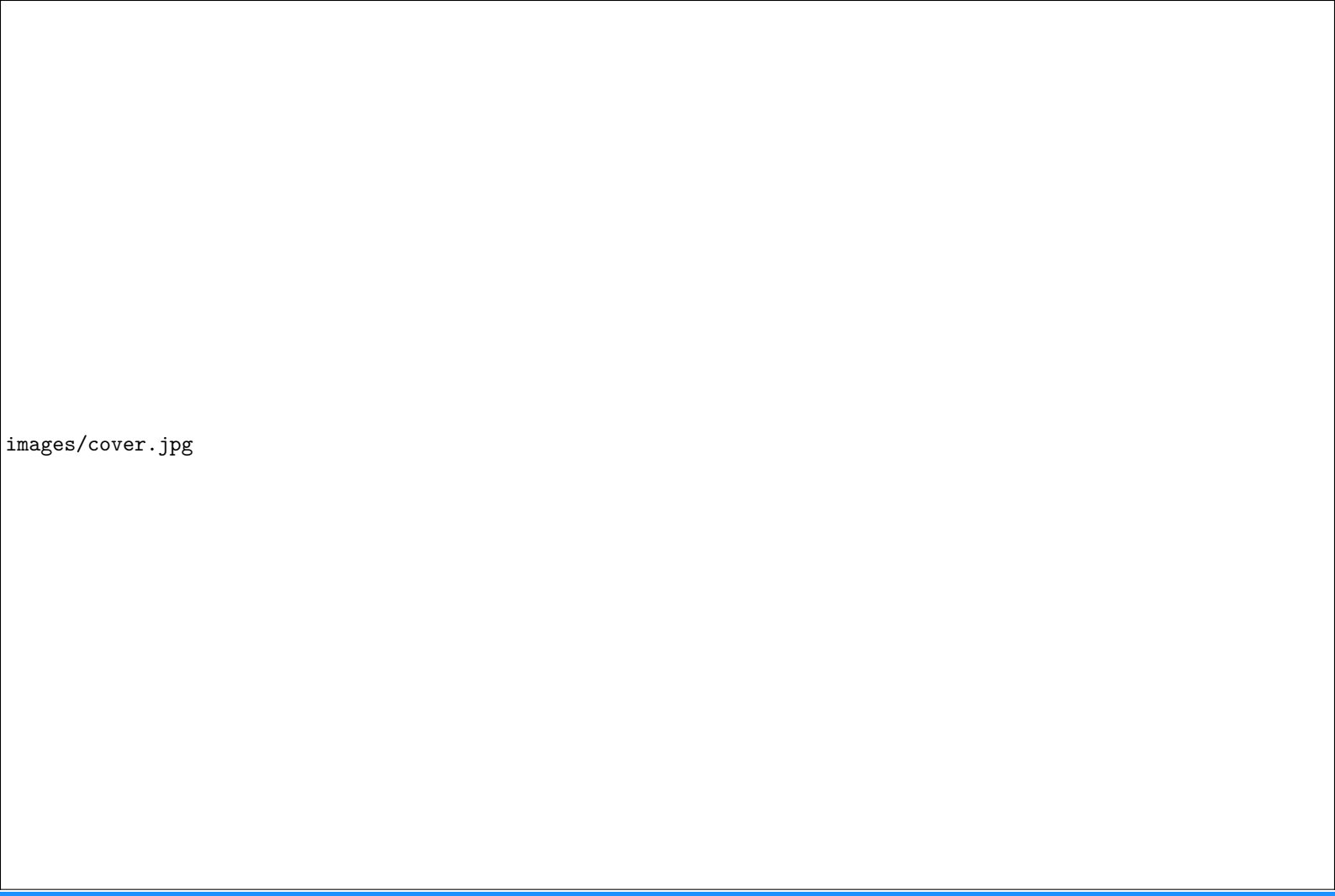

抽象代数解题指南 I

作者：Victor Zhong (Maki's Lab 代数分部)

时间：2022.5.6

版本：2.0 (2023.3.5)

“积土成山，风雨兴焉；积水成渊，蛟龙生焉。”——荀子

目录

第一版前言

解题，一直是数学学习的核心问题与热门话题之一. 从小学到大学，凡是学数学的地方，就有解题，就有“解题高手”和“解题苦手”. 那么，你有没有想过，是什么因素，导致了解题能力的高低之别?

是“聪明”么? 是“天赋”么?

不可否认，有的人确实很有数学方面的天赋，这在各行各业都是正常现象. 然而，这样的人毕竟是极少数. 笔者在此斗胆提出一个暴论：我们的解题能力不尽如人意，是因为没有在数学学习的过程中，体会到数学的学科特点，总结出解题的基本理念. 于是乎，我们虽然解了成千上万道题，却仍然不清楚自己究竟有什么样的解题工具，仍然没有勇气面对全新的问题，甚至于不知道自己为什么能够解出一道题.

这实际上是一个看起来有一些反逻辑的现象. “解题”的过程，我们已经经历了无数次，但是，我们对“解题”本身，却缺乏一个清晰的认知. 模糊的中心思想，必然带来飘忽不定的行动，于是产生仿佛“碰运气”一般的不确定结果，其直接的体现就是，考试的成绩与卷面的相关性极强，卷面的题目“落在自己的范围”内，成绩就高，反之，成绩就无法掌控了.

回到我们现在面对的大学课程，也许考试成绩没有那么重要了，但是学习的过程仍然是读教材、做练习、应对期中期末考试，同时立志于为数学学科添砖加瓦的同志们，还要为将来的研究做准备. 于是，独立的解题，就成为了迈向研究的第一步. “解题，是极简的研究”.

因此，不论从哪个角度来说，只要谈到数学，解题，就是绕不开的环节.

0.1 解题是什么？

笔者的理解是：解题，就是应用“所学知识”，结合“题设”，逻辑地获得“答案”的思维过程.

首先，哪些是“所学知识”? 众所周知，教材、参考书中的“定义、引理、定理、性质、推论……”是我们的所学知识. 除此之外，笔者认为，我们所读的每一份知识材料，所做的每一道题，都应该纳入我们的知识体系之中.

也许有人会因此感到害怕：我们做过的题浩如烟海，阅读的参考书也不少，怎么可能都记得呢? 实际上，由于数学学科高度的逻辑性，归纳和记忆是一件极其简单的事情，我们只需要抓住为数不多的组织知识的线索，就可以轻松记住一大片知识，形成自己的知识体系，并且很容易不断地向其中添加新的知识点.

例如，在抽象代数的群论中，我们都学了什么东西呢? 首先，我们的研究对象，是群；为了研究群的结构，我们使用“生成元 + 关系”的模式描述一个群；我们讨论了子群和陪集，子群有两条等价定义，而陪集是利用子群，划分了一个群；两个典型的子群是正规化子与中心化子；这里还有 Lagrange 定理，描述了子群和群的阶的关系；我们注意到有一种特殊的子群：正规子群，正规子群有四五条等价定义；基于正规子群的陪集的全体，又形成了一个群，是为商群. 我们研究了群和群之间的特殊的映射：群同态（以及同构），同态将幺元映射到幺元，逆映射到逆；由同态产生了两个特殊的群：核与象，它们之间的关系即为第一同构定理；我们还学习了其他三个同构定理，他们从不同的角度应用了第一同构定理. 我们可以利用群，去研究集合的结构，这就是群作用，由群作用得到了 Cayley 定理和轨道公式；典型的群作用包括左乘作用和共轭作用；由群作用我们得到了研究有限群的结构的有力工具：Sylow 定理. 在学习上述理论知识的过程中，我们经常使用一些典型的群结构，比如模 n 同余类、二面体群、四元数群、矩阵群、对称群……；我们也研究了一些结构简单的群：循环群、有限生成 Abel 群、可解群. 以上这些还只是泛泛地描述，具体到每个要点，我们还可以给出有哪些定义定理和性质、有哪些常见的处理问题的思路.

于是，从这个角度而言，一个注意各种细节、注意积累的学生学到的数学知识，远比简单学学地学生学到的要多得多，即便只是一天多注意了一两个点，日积月累下来，也是巨大的区别.

第二方面，如何结合“题设”? 一方面，我们要从给定“条件”的角度，重新梳理我们的知识体系. 例如，题设条件中给了一个正规子群，你会想到如何使用它呢? 我们就要回到我们的知识体系中，哪些知识点涉及到了正规子群? 正规子群的定义与等价定义是显然能想到的；除此之外，我们可以利用正规子群构造商群，从而简

化群的结构（因为群的阶下降了）；可以寻找一个合适的群同态使得其定义域为给定群，核为给定正规子群，从而同构定理也有可能应用起来；还有，如果讨论的是交换群，那么任意子群都是正规子群，子群的性质也可能用起来. 如果进一步考虑群作用，还会有更多的思路，这里就不再列举了.

另一方面，需要我们证明的结论的特性，也会让我们从不同的视角审视我们的知识体系. 例如，我们有时候需要通过一些群的阶的特征，来确定群的结构特征（经典的例子是 Cauchy 定理与 Sylow 定理，他们都是“某种意义下”的 Lagrange 定理的逆定理）. 当我们遇到此类问题时，我们有什么思路呢？我们当然有 Cauchy 定理与 Sylow 定理可以使用；我们知道素数 p 阶群必为 p 阶循环群；我们有一些群的阶的性质，可以帮助我们缩小可能情况的数量……限于篇幅，这里不再给出更多的思路，相关内容读者可以在正文的相关章节找到. 笔者建议大家每接触到一个新的思路，就把它整理下来，并且试着应用在其他问题中，本书也会尽可能在每个新方法下，给出几个可以使用该方法的例子，供读者练习.

从而，能否有效地结合题设的关键，还是我们日常构建的知识体系是否足够全面. 我们不依赖“灵光乍现”来面对难题，而是扎扎实实地做好日常的学习与积累.

最后一方面，逻辑的获得答案. 这里所说的就是正确利用数学语言表达我们的思路，给出答案. 无须讳言，我们在高考之后，就不再有人严格的要求我们的“解题格式”了，笔者认为这对于数学学习是很危险的. 随意的证明书写，往往意味着不严谨的解答过程，反应出解答的书写者对某些知识有着不同程度的错误理解，情况严重时会导致写出的证明完全错误. Maki’s Lab 会在每一门数学课程中，给出尽可能严谨的证明过程，格式的要求会遵循目前国际通行的数学证明书写规范.

总而言之，解题，是一项系统工程，是对我们日常学习效果的综合考察. 我们应当重视解题过程，时刻总结我们获得的经验，并纳入我们的知识体系之中. 笔者认为，只有如此，我们才能够充分发挥解题的作用，不断提高我们的数学能力.

0.2 解题有绝招？

笔者很负责任地表示：解题没有绝招.

我们不妨把讨论的内容扩大一些. 现在社会的发展越来越快，我们似乎越来越越来越不愿意花太多时间完整地做事. 比如，走路我们要走“捷径”，吃饭我们要吃“快餐”，读书我们要读“精编版”、“缩略版”，看电视剧我们要看“精讲”，甚至于学习我们也要学别人整理好的“知识图表”与“习题精选”. 我们希望花更少的时间，快速地掌握“干货”，这样就有更多的时间做更多的事，有更多的产出了.

这样的追求是否合理呢？笔者认为，每个人都会基于自己的价值观，有自己的判断，笔者无意批判. 不过，快速获得的东西，永远只能解决燃眉之急；要想深入全面的了解一些事，就必须老老实实地按照事物的发展规律，花时间学习和体验.

回到解题上来，市面上有不少的书籍或者视频，针对各个知识点，都总结了一些“题型”，然后较为死板的给出了一些解题程序. 读者只需要按照这些整理好的“套路”，就可以把同样类型的题解出来了. 这么做的好处，自然是读者不需要花太多的时间，就可以掌握大部分题目的解法，如果是为了通过一些考试，这么做确有合理之处. 然而，如果是为了日常学习，那么这样的做法，就十分不可取了. 我们解题的核心目的，不是为了一题两题的答案，而是通过解题的过程，训练我们应用知识解决问题的能力. 因此，思考与总结的过程，远比获得答案要重要得多；掌握思考和总结的方法，才是我们受益终身的东西.

同时，解题是一个高度经验化的东西. 正如我们前一节所描述的那样，笔者的解题，依赖自主构建的“知识体系”，而其他的人，也会有自己关于解题理论的论述，这些都是合理的. 对笔者来说自然的思路，也许其他人就接受不了. 因此，笔者不认为直接从他人那里继承一套相对完整的解题经验，是一种有效的学习解题的方式. 参考别人的思考方法，结合自己的情况，去逐步形成自己习惯的解题经验，这才是正招.

0.3 让我来到你身边

本书取名《抽象代数解题指南》，主要呈现的是抽象代数课程中较为典型的定理使用方法、解决问题的常见思路和经验、以及一些容易出错的细节. 本书的定位是一本教材辅导书，而不是代替教材的材料，因此建议读者先根据“任何一本”教材学习，再使用本书训练、复习、提高. 笔者尤其推荐使用 Maki’s Lab 抽象代数课程组编写的抽象代数系列教材，本书的知识体系基本上与该系列教材相同.

为了方便笔者行文以及读者阅读，每小节的开篇，会简单列举本节所需的定义和定理，而后列举的所有例题、习题，均不超出所列知识点之范围. 第二部分是较为有特色的一个板块：“从定理证明中学解题”，我们会把对解题有启发意义的定理证明，拿出来重新梳理一遍，这时我们将站在解题者的角度，或分析证明的思考过程，或总结实用的解题“套路”. 第三部分是例题讲解部分，我们给出若干典型例题进行讲解分析. 在第二、第三部分，每一个证明的后面，都会配有相应的习题，它们的解题过程与前述证明有强烈的相关性. 第四部分是习题，列举读者应知应会，但没在前三节呈现的习题. 最后一部分是思考题，包含一些有难度的、或者跨学科的一些问题，这些问题不要求读者初学即可做出，读者完全可以先跳过，留待以后思考练习.

本书的主要目的，是笔者想要透过《抽象代数》这样一门具体的课程，“引导”【笔者：“可能大言不惭了一些. ”】读者逻辑地思考，自然地获得解题思路. 我们的论述核心是抽象代数，但思考的步伐却绝不应该止于抽象代数这一门课. 笔者期待，读者在这里体会到了思考的乐趣和妙处，初步形成了属于自己的思考方法，然后把这些方法应用在别的学习环境之中. 从人生的角度来看，抽象代数只是众多课程中的一门课而已，学习也只是生活的一部分，他们都没有那么的重要. 但是，思考的能力与解决问题的意识和策略，是我们时时刻刻都要面对的，影响一生的关键话题，我们只能从每一次的生命活动中，不断地体会和总结.

0.4 用途说明

本书由 Maki’s Lab 代数分部的 Victor 编著，当前 Maki’s Lab 官网为唯一发布渠道. 读者可作为学习资料免费使用，但不可用于任何商业用途. 如若发现，笔者将从即日起不再公开更新.

笔者的本意是希望本书能够帮助到更多有需要的同学，而不是作为牟利的工具. 良好的分享环境，需要我们每一个人共同维护!

Victor Zhong
2022.5.6

第 1 章 群论 I

1.1 幺半群

1.1.1 课前思考

1. 存在不包含正整数的 $(\mathbb{Z},+)$ 的子幺半群.（T/F）
2. 设 $(S,\cdot),(T,\circ)$ 是两个幺半群，且有 $\varphi: S\to T$. 若对任意的 $s,s'\in S$ 都满足
$$\varphi(s\cdot s')=\varphi(s)\circ\varphi(s')$$
则 φ 是幺半群同态.（T/F）
3. 考虑 n 阶实方阵的乘法运算，下列说法正确的有（　）：
A. $R^{n\times n}$ 上的二元运算；　B. 满足交换律；　C. 满足结合律；　D. 每个元素都有自己的逆.
4. 以下代数结构是幺半群的有（　）：
A. $(\mathbb{Q},+)$　B. $(\mathbb{Q},\cdot)$　C. $(\mathbb{Q}_+,+)$　D. $(\mathbb{Q}_+,\cdot)$.
5. 以下集合（连同加法）是 $(\mathbb{Z},+)$ 的子幺半群的有（　）：
A. $A=\{3k:\ k\in\mathbb{Z}_+\}$；　B. $B=\{n\in\mathbb{Z}:\ n\geqslant -1\}$；　C. $C=\{n\in\mathbb{Z}:\ n\leqslant 1\}$；　D. $D=\{-3k:\ k\in\mathbb{Z}\}$.
6. 写出由如下元素生成的 $(\mathbb{Z},+)$ 的子幺半群.
   (a). 1：____；
   (b). -2：____；
   (c). $-2,4$：____.

解

1. T. 例如 $(\mathbb{Z}_-\cup\{0\},+)$.
2. F. 例如 $\varphi:(\mathbb{Z},\cdot)\to(\mathbb{Z},\cdot), n\mapsto 0$. 其满足题设条件，但它不是幺半群同态，因为它不满足 $\varphi(1)=1$.
3. AC. 方阵乘法不满足交换律，且行列式等于 0 的方阵没有逆.
4. ABD. C 选项只能是半群，没有幺元 0.
5. BD. A 选项缺少幺元，C 选项不满足运算封闭性.
6. (a). $S=\{n\in\mathbb{Z}:\ n\geqslant 0\}$；
   (b). $S=\{n=2k:\ k\leqslant 0\}$；
   (c). $S=\{n=2k:\ k\in\mathbb{Z}\}$.

1.1.2 知识要点

（一）二元运算与半群结构

1. 集合 A 上的二元运算：函数
$$\cdot: A\times A\to A,\qquad (a,b)\mapsto a\cdot b$$
$a\cdot b$ 可以简单写做 ab.
   (a). 二元运算是结合的：对任意 $a,b,c\in A$，有 $a(bc)=(ab)c$.
   (b). 二元运算是交换的：对任意 $a,b\in A$，有 $ab=ba$.
2. 半群 $(S,\cdot)$：集合 S 及其上的二元运算 “$\cdot$”，满足：
（结合律）：对任意 $a,b,c\in S$，有 $a(bc)=(ab)c$.
3. 交换半群 $(S,\cdot)$：半群 $(S,\cdot)$，且满足：
（交换律）：对任意 $a,b\in S$，有 $ab=ba$.
4. 幺半群 $(S,\cdot)$：半群 $(S,\cdot)$，且满足：

(幺元)：存在 $e \in S$，对任意 $a \in S$，满足 $ea = ae = a$.
S 的幺元：e，在没有误解时简写为 1，或 1_S.

5. 逆：幺半群 $(S, \cdot)$ 中，满足 $st = ts = 1$ 的元素 $t \in S$ 称为 s 的逆.
6. (幺半群的基本性质)：设 $(S, \cdot)$ 是幺半群.
   (a). (幺元唯一)：S 的幺元是唯一的；
   (b). (唯一的逆)：对 S 的每个元素 s，若其逆存在，则唯一.（s 的逆记作 s^{-1}）

(二)、子幺半群

1. 幺半群 $(S, \cdot)$ 的子幺半群 $(T, \cdot)$：$T \subset S$，T 包含 S 的幺元，且 T 在乘法下封闭.
   子幺半群为幺半群.

(三)、生成

1. 由子集 A 生成的子幺半群：所有包含 A 的幺半群 S 的子幺半群的交集

$$\langle A \rangle = \bigcap_{\substack{A \subset T \\ T\text{是子幺半群}}} T.$$

2. (包含 A 的最小子幺半群)：设 A 是幺半群 S 的子集，则 $\langle A \rangle$ 是 S 中包含 A 的最小的子幺半群.

(四)、幺半群间的特殊映射

1. 幺半群同态：设 $(S, \cdot), (T, \circ)$ 为两个幺半群. 映射 $\varphi : S \to T$，且对任意的 $s, s' \in S$ 有

$$\varphi(s \cdot s') = \varphi(s) \circ \varphi(s') \qquad \forall s, s' \in S$$
$$\varphi(1_S) = 1_T.$$

2. 幺半群同构：映射 $\varphi : S \to T$ 是幺半群同态，且为双射.
3. (同构的逆映射)：若 $\varphi : S \to T$ 是幺半群同构，则其逆映射存在（记为 $\varphi^{-1} : T \to S$），且 φ^{-1} 也是同构.

1.1.3 知识要点解读

(一) 代数结构公理的使用：代数变形

抽象代数是一门代数课程，因此代数变形的能力既是核心，又是基本功.

需要注意的是，我们所能使用的，仅仅是我们学过的知识点，换句话说，虽然我们对结合律、交换律等运算律非常的熟悉，但是绝不可想当然地认为他们都自然成立. 例如在下面的几例中，幺半群 S 并不假定是交换的，所以证明时不能使用交换律. 建议初学者做每一步证明或运算时，都先考虑一下："自己使用是的哪条运算律，在当前题设下可以使用吗?" 我们所做的每一步代数运算，都应该是有理有据的.

问题 1.1 (幺元唯一)：幺半群 S 的幺元是唯一的.

注 这也许是每个抽象代数的初学者，所接触的第一个代数证明，因此具有相当的纪念意义.

本例有一点值得关注：唯一性的证明. 这是一个很普遍的命题类型，常见的证明思路有：

1. 使用确保唯一性的定理或性质；
2. 假设有两个满足条件的对象，证明它们相等；
3. 假设有两个满足条件的不相等的对象，找出矛盾.

证明 假设 e, e' 均为 S 的幺元，于是有：

$$\begin{aligned} e &= ee' && (e' \text{ 是幺元}) \\ &= e' && (e \text{ 是幺元}) \end{aligned}$$

从而 S 的幺元唯一.

问题 1.2 （唯一的逆）：对幺半群 S 的每个元素 s，若其逆存在，则唯一.

证明 对 S 的每个元素 s，假设 b,c 均为 s 的逆，于是有：

$$\begin{aligned} b &= be && (e \text{ 是幺元}) \\ &= b(sc) && (c \text{ 是 } s \text{ 的逆}) \\ &= (bs)c && (\text{结合律}) \\ &= ec && (b \text{ 是 } s \text{ 的逆}) \\ &= c && (e \text{ 是幺元}) \end{aligned}$$

从而 s 的逆唯一.

（二）代数结构的子结构

我们在学习集合的时候，一定会学子集的概念. 一般的，对于任何一种代数结构，我们都会寻求定义其子结构，并且期待子结构满足这样两个条件：

1. 集合上是子集；
2. 尽可能保留原代数结构的核心特征.

例如，子幺半群就是幺半群的子集，并且继承了乘法、幺元、封闭性等核心特征，最终我们可以证明子幺半群本身也是幺半群.

另一方面，在条件允许的情况下，我们也寻求在子集的基础上，构造出我们想要的子代数对象，这就引出了一个重要的概念：生成. 我们在定义中给出的是从大到小的构造子代数对象的方法：取交. 我们后面还会看到从小到大的构造方法.

问题 1.3 （包含 A 的最小子幺半群）：设 A 是幺半群 S 的子集，则 $\langle A\rangle$ 是 S 中包含 A 的最小的子幺半群.

证明 先证明：$\langle A\rangle$ 是 S 的子幺半群.

我们有

$$\langle A\rangle = \bigcap_{\substack{A\subset T\\ T\text{是子幺半群}}} T.$$

一方面，对任意包含 A 的子幺半群 T，$1\in T$，所以 $1\in\langle A\rangle$. 另一方面，对任意的 $x,y\in\langle A\rangle$，和任意的包含 A 的子幺半群 T，有 $x,y\in T$，从而 $xy\in T$，也就有

$$xy\in \bigcap_{\substack{A\subset T\\ T\text{是子幺半群}}} T=\langle A\rangle .$$

从而 $\langle A\rangle$ 是 S 的子幺半群.

再证明：若 T 是任意一个 S 中包含 A 的子幺半群，则 $\langle A\rangle\subset T$. （从而得出 $\langle A\rangle$ 的最小性）

因为 T 是任意一个 S 中包含 A 的子幺半群，所以由 $\langle A\rangle$ 的定义可知，T 是参与定义中交集运算的若干个集合之一，从而得到的交集也必然是 T 的子集.

笔记 读者可以利用此题熟悉子幺半群的证明方法.

1.1.4 典型例题

（一）半群的判定

例题 1.1 设 S 是非空集，$\mathscr{P}(S)$ 是由 S 的所有子集构成的集合（称为 S 的幂集），证明：

1. $\mathscr{P}(S)$ 连同集合的求并运算 $\cup$ 构成交换幺半群；
2. $\mathscr{P}(S)$ 连同集合的求交运算 $\cap$ 构成交换幺半群.

证明

1. 先证明：$\varnothing$ 是 $\mathscr{P}(S)$ 的幺元. 对任意的 $A \in \mathscr{P}(S)$，有
$$\varnothing \cup A = A = A \cup \varnothing$$
再证明：$\mathscr{P}(S)$ 在运算 $\cup$ 下封闭. 对任意的 $A, B \in \mathscr{P}(S)$，有
$$A \cup B \subset S$$
从而 $A \cup B \in \mathscr{P}(S)$.
最后证明：运算 $\cup$ 是交换的. 对任意的 $A, B \in \mathscr{P}(S)$，有
$$A \cup B = B \cup A$$
综上，$(\mathscr{P}(S), \cup)$ 是交换幺半群.
2. 证明过程与第一小问几乎一致，留给读者作为练习.

✍ **练习 1.1*** 设 $S = \{1, 2, \cdots, n\}$，定义集合 $M(S) = \{f : S \to S\}$（即定义域和陪域均为 S 的映射的集合），$M(S)$ 上的运算为映射的复合运算 $\circ$.

1. 试求出 $M(S)$ 中的元素个数；
2. 证明 $(M, \circ)$ 是幺半群，幺元是 S 上的恒等映射 id_S.

（二）同态与同构

同态最重要的特性就是“保持运算”，即 $f(xy) = f(x)f(y)$，下面给出的例子都紧紧围绕这一特性的使用.

例题 1.2 令 $(S, \cdot)$ 和 $(S', \cdot)$ 是两个幺半群，而 $f : S \to S'$ 是个满射，证明：f 是个幺半群同态，当且仅当对任意 $x, y \in S$，满足 $f(xy) = f(x)f(y)$.

注 已知 f 是幺半群同态时，由定义即知命题成立.

而反方向的证明，需要我们注意到特殊条件：满射，满射意味着我们可以将象集中的运算放到原象集中去考虑，这是应用满射的常见思路之一，我们以后还会经常用到这一思路.

证明 “$\to$”：由定义即可得证.

“$\leftarrow$”：结合幺半群同态的定义，我们只需证：若满射 $f : S \to S'$ 满足 $\forall x, y \in S, f(xy) = f(x)f(y)$，则 $f(1) = 1'$，即 $f(1)$ 为 S' 幺元.

对任意 $x' \in S'$，由于 f 为满射，从而存在 $x \in S$，使得 $f(x) = x'$，于是 $x'f(1) = f(x)f(1) = f(x \cdot 1) = f(x) = x'$. 同理可证 $f(1)x' = x'$，从而 $f(1)$ 为 S' 幺元. 原命题得证.

✍ **练习 1.2** 试给出一个幺半群间的映射，它可以保持运算，但不能将幺元映到幺元.（因此它不是幺半群同态，例题中给出的满射要求是必不可少的）

解 考虑幺半群 $M = (\mathbb{N}, \cdot)$，以及映射：$\varphi : M \to M,\ n \mapsto 0$.

✍ **练习 1.3** 令 $(S, \cdot)$ 和 $(S', \cdot)$ 是两个幺半群，则 $f : S \to S'$ 是个幺半群同构，当且仅当 f 是双射，且对任意 $x, y \in S$，满足 $f(xy) = f(x)f(y)$.

1.1.5 习题

（一）半群结构

✍ **练习 1.4** 设 S 是集合，定义 S 上的运算：$ab := b$.

1. 证明：S 是一个半群.
2. 在什么条件下，S 是幺半群?

提示 第二小问中，设 1 是 S 中的幺元，则对任意的 $s \in S$ 有
$$s = s1 = 1$$

练习 1.5 设 $M=\mathbb{Z}^2$，定义 M 上的运算

$$(x_1,x_2)(y_1,y_2):=(x_1y_1+2x_2y_2,x_1y_2+x_2y_1)$$

证明：

1. $(M,\cdot)$ 是交换幺半群，幺元为 $(1,0)$；
2. 若 $(x_1,x_2)\neq(0,0)$，且 $(x_1,x_2)(y_1,y_2)=(x_1,x_2)(z_1,z_2)$，则 $(y_1,y_2)=(z_1,z_2)$.

练习 1.6 设 (M,p) 是幺半群，$m\in M$. 定义 M 上的运算 p_m：

$$p_m(a,b)=amb$$

1. 证明：(M,p_m) 是半群；
2. 在什么条件下，(M,p_m) 是幺半群?

证明

1. 先证明，运算 p_m 在 M 上封闭. 对任意的 $a,b\in M$，有 $p_m(a,b)=amb\in M$.
   再证明：运算 p_m 满足结合律. 对任意的 $a,b,c\in M$，有

$$\begin{aligned}p_m(p_m(a,b),c)&=p_m(amb,c)\\&=ambmc\\&=am(bmc)\\&=p_m(a,bmc)\\&=p_m(a,p_m(b,c))\end{aligned}$$

2. 假设 (M,p_m) 存在一个幺元 x，则对任意的 $a\in M$ 需要满足

$$p_m(x,a)=a=p_m(a,x)$$

   也就是

$$xma=a=amx$$

   注意到 $(M,\cdot)$ 有唯一的幺元 1，且满足 $1a=a=a1$，所以必有 $xm=mx=1$，即 $m=x^{-1}$. 所以当 m 可逆时 (M,p_m) 为幺半群，且幺元为 m^{-1}.

笔记 读者可能比较习惯形如 $a+b$ 的二元运算表达式，而对于映射形式 $f(a,b)$ 较为生疏，此题即是一个很好的适应性练习.

第二小问有一点难度，关键问题在于读者能否注意到幺元的唯一性.

练习 1.7 设 $(S,\cdot)$ 是半群，u 不是 S 中的元素. 定义 $M=S\cup\{u\}$，且定义 M 上的运算 $\circ$：

$$\begin{aligned}a\circ b&:=ab,\quad a,b\in S\\a\circ u&:=a,\quad a\in M\\u\circ a&:=a,\quad a\in M\end{aligned}$$

证明：$(M,\circ)$ 是幺半群.

笔记 此题说明，我们总可以将一个半群改造为幺半群.

（二）幺半群同态

练习 1.8 定义整数集 $\mathbb{Z}$ 上的运算 $\circ$：$a\circ b:=a+b-ab$. 证明：

1. $(\mathbb{Z},\circ)$ 是幺半群，幺元为 0；

2. 定义映射

$$\begin{aligned}\varphi : (\mathbb{Z}, \cdot) &\to (\mathbb{Z}, \circ)\\ a &\mapsto 1 - a\end{aligned}$$

则 φ 是幺半群同构.

（三）生成的闭包定义 *

✍ **练习 1.9** 设 S 为幺半群，$a \in S$，证明：$\langle a \rangle = \{a^n : n \in \mathbb{N}\}$. 其中规定 $a^0 = 1$.

注 根据生成的定义，我们需要证明：

$$\langle a \rangle := \bigcap_{\substack{a \in T \\ T\text{是}S\text{的子幺半群}}} T = \{a^n : n \in \mathbb{N}\}.$$

记 $A := \{a^n : n \in \mathbb{N}\}$，则我们需要证明：

1. $(A, \cdot)$ 是幺半群，从而 $\langle a \rangle \subset A$.
2. 对任意 S 的子幺半群 T，若 $a \in T$，则 $A \subset T$，从而 $A \subset \langle a \rangle$.

证明

1. 先证明：$A := \{a^n : n \in \mathbb{N}\}$ 是幺半群.

   封闭性：对任意的 $a^i, a^j \in A$，有 $a^i a^j = a^{i+j} \in A$.

   结合律：对任意的 $a^i, a^j, a^k \in A$，有

   $$\begin{aligned}(a^i a^j)a^k &= a^{i+j}a^k\\ &= a^{i+j+k}\\ &= a^i a^{j+k}\\ &= a^i(a^j a^k)\end{aligned}$$

   幺元：对任意的 $a^i \in A$，有

   $$a^i a^0 = a^i = a^0 a^i$$

   从而 a^0 是幺元.

   综上，A 为 S 的子群.

2. 再证明：对任意 S 的子幺半群 T，若 $a \in T$，则 $A \subset T$. 也就是，对任意的 $n \in \mathbb{N}$，有 $a^n \in T$.

   我们对 n 采用数学归纳法.

   当 $n = 0$ 时，$a^0 = 1 \in T$，命题成立.

   设 $n = k$ 时，有 $a^k \in T$. 当 $n = k + 1$ 时，由子幺半群的运算封闭性可得：$a^n = a^{k+1} = a^k a \in T$.

   综上，对任意的 $n \in \mathbb{N}$，有 $a^n \in T$，即 $A \subset T$.

   综合前面的讨论，原命题得证.

✍ **练习 1.10** 设 S 为幺半群，$A \subset S$. 证明：$\langle A \rangle = \{x = a_1 \cdots a_n : a_1, \cdots, a_n \in A, n \in \mathbb{N}\}$. 其中规定

1. 当 $A = \varnothing$ 时，$\langle A \rangle = \langle 1 \rangle$.
2. 当 $n = 0$ 时，$x = 1$.

注 换言之，由幺半群中有限多个元素生成的子幺半群就是由这些元素的有限乘积所构成的.

证明 和前一题的证明是类似的.

一方面，这是个子幺半群. 它对乘法是封闭的，因为

$$(a_1 \cdots a_m)(b_1 \cdots b_n) = a_1 \cdots a_m b_1 \cdots b_n$$

仍然是 A 中元素的有限乘积，它包含幺元 $a^0 = 1$.

另一方面，假设 $T < S$ 是个子幺半群，而且 $A \subset T$. 对任意 $a_1, \cdots, a_n \in A$，我们有 $a_1, \cdots, a_n \in T$. 因为 T 是个子幺半群，所以在乘法下封闭，因此 $a_1 \cdots a_n \in T$. 这就证明了 $\{a_1 \cdots a_n : a_1, \cdots, a_n \in A, n \in \mathbb{N}\} \subset T$.

综上所述，我们就证明了幺半群中一个子集所生成的子幺半群是由子集中元素的有限乘积所构成的.

1.2 群

1.2.1 课前思考

1. 定义实数集 $\mathbb{R}$ 上的运算“$\circ$”

$$r \circ s := r + s + k$$

其中 $k \in \mathbb{R}$ 是常数. 则代数系统 $(\mathbb{R}, \circ)$ 中的幺元为____，任意元素 r 的逆为____.

2. 设 $(G, \cdot)$ 为群，$a, b, c, x \in G$，且有 $x^2 a = bxc^{-1}, acx = xac$，则 $x =$____（用只含 a, b, c 的代数式表示）.

解

1. 幺元：$-k$，元素 r 的逆：$-r - 2k$.
2. $x = bc^{-1}a^{-1}$.
   由第一式可得 $x(xac) = bx$，再利用第二式可得 $xacx = bx$，从而 $xac = b$，即得结果.

1.2.2 知识要点

（一）群及其基本性质

1. 群 $(G, \cdot)$：幺半群 $(G, \cdot)$，且满足：
   （逆）：对任意 $a \in G$，存在 $a^{-1} \in G$，满足 $a^{-1}a = aa^{-1} = 1$.
   （若不做特殊声明，以后 G 连同的运算均为“$\cdot$”）
2. 交换群（Abel 群）G：满足交换律的群 G.
3. （群的基本性质）：设 G 是群.
   (a). （双重逆）：若 $g \in G$，则 $(g^{-1})^{-1} = g$.
   (b). （穿脱原理）：若 $g, h \in G$，则 $(gh)^{-1} = h^{-1}g^{-1}$.
   (c). （消去律）：设 $a, b, g, h \in G$，
   I. 若 $ag = ah$，则 $g = h$;
   II. 若 $gb = hb$，则 $g = h$.
4. （幺半群中的群）：记幺半群 $(S, \cdot)$ 中所有可逆元构成的集合为 $S^\times$，则 $(S^\times, \cdot)$ 构成群.
5. 群 $(A, \cdot), (B, *)$ 的直积：A, B 的笛卡尔积 $A \times B = \{(a, b) : a \in A, b \in B\}$，连同运算：

$$(a, b)(c, d) = (a \cdot c, b * d)$$

形成群.（记为 $A \times B$）

（二）子群

1. 群 $(G, \cdot)$ 的子群 H：$H \subset G$，H 包含 G 的幺元，且 H 在乘法和逆下封闭.（记为 $H < G$）
   子群为群.
   真子群：G 的子群 H 满足 $H \neq G$.
   G 的平凡子群：$\{1\}$ 和 G.
2. （子群的等价定义）：对于群 G 的子集 H，$H < G$，当且仅当
   (a). $H \neq \varnothing$;
   (b). 对任意的 $x, y \in H$，有 $xy^{-1} \in H$（或 $x^{-1}y \in H$）.
3. $\mathbb{R}$ 上的 n 阶一般线性群：

$$GL_n(\mathbb{R}) = \left\{A \in \mathbb{R}^{n \times n} : \det A \neq 0\right\}.$$

（$GL_n(\mathbb{C})$ 可类似定义）

（三）生成

1. （子群的交）：若 $\mathcal{A}$ 是群 G 的一些子群组成的集族，则
$$\bigcap_{H\in\mathcal{A}} H < G.$$
2. 由子集 A 生成的子群：所有包含 A 的群 G 的子群的交集
$$\langle A\rangle = \bigcap_{\substack{A\subset H\\ H<G}} H.$$

（四）群间的特殊映射

1. 群同态：设 $(G,\cdot),(H,\circ)$ 为两个群. 映射 $\varphi: G\to H$，满足：
$$\varphi(g\cdot g') = \varphi(g)\circ\varphi(g') \qquad \forall g,g'\in G.$$
2. 群同构：映射 $\varphi: G\to H$ 是群同态，且为双射.（记作 $G\simeq H$）
3. （同构的逆映射）：若 $\varphi: G\to H$ 是群同构，则其逆映射存在（记为 $\varphi^{-1}: H\to G$），且 φ^{-1} 也是群同构.
4. （同态的基本性质）：若 $\varphi: G\to H$ 是群同态，则
   (a). $\varphi(1_G) = 1_H$；
   (b). 对任意的 $g\in G$，有 $\varphi(g^{-1}) = \varphi(g)^{-1}$.
5. 同态 φ 的象：$\operatorname{im}\varphi = \{\varphi(g): g\in G\}$.（也可以记为 $\varphi(G)$.）
   同态 φ 的核：$\ker\varphi = \{g\in G: \varphi(g) = 1_H\}$.
6. （子群关系）：$\ker\varphi < G$，且 $\operatorname{im}\varphi < H$.
7. （单射与满射）：
   (a). φ 为单同态，当且仅当 $\ker\varphi = \{1_G\}$；
   (b). φ 为满同态，当且仅当 $\operatorname{im}\varphi = H$.

1.2.3 知识要点解读

（一）群的运算性质

群相对于幺半群来说，多出的条件只有一个，即每个元素都有逆，从而我们可以在计算过程中随意的引入任意一个元素的逆.

问题 1.4（双重逆）：设 G 为群. 若 $g\in G$，则 $(g^{-1})^{-1} = g$.

证明

$$\begin{aligned}
(g^{-1})^{-1} &= (g^{-1})^{-1}e && (e\text{是幺元})\\
&= (g^{-1})^{-1}(g^{-1}g) && (g^{-1}\text{是 } g \text{ 的逆})\\
&= ((g^{-1})^{-1}g^{-1})g && (\text{结合律})\\
&= eg && ((g^{-1})^{-1}\text{是 } g^{-1} \text{ 的逆})\\
&= g && (e\text{是幺元}).
\end{aligned}$$

✍ **练习 1.11** 设 G 为群，且令 $x,y\in G$，证明以下命题等价：

1. $xy = yx$；
2. $y^{-1}xy = x$；
3. $x^{-1}y^{-1}xy = 1$.

练习 1.12 设 G 为群，$g,n\in G$.

1. 已知 $gng^{-1}=1$，证明：$n=1$;
2. 已知 $g^{-1}ng=1$，证明：$n=1$.

笔记 本题非常简单，但其中出现的 gng^{-1} 的形式非常重要，我们称之为 n 的共轭形式. 共轭形式有很多美妙的性质，我们将在日后的学习中逐步接触到. 大家可以回想在线性代数中学过的相似变换 $A^{-1}BA$，也是这样的形式哦.

有关代数变形进一步的问题和想法，我们将利用一个专题详细论述之.

（二）群结构的证明

验证该集合连同给定的运算，满足群结构所需的各条公理即可. 注意：要验证给定的运算确实是集合上的二元运算（我们称这一性质称为运算的“封闭性”）.

例题 1.3（幺半群中的群）：记幺半群 $(S,\cdot)$ 中所有可逆元构成的集合为 $S^\times$，则 $(S^\times,\cdot)$ 构成群.

证明

1. （封闭性）：对任意的 $s,t\in S^\times$，由 $S^\times$ 的定义，s,t 均存在各自的逆 s^{-1},t^{-1}. 而对于 st，因为
$$(t^{-1}s^{-1})(st)=1=(st)(t^{-1}s^{-1})$$
所以 $t^{-1}s^{-1}$ 是 st 的逆，即 $st\in S^\times$.
2. （结合律）：因为 S 中结合律成立，所以 $S^\times$ 中结合律也成立.
3. （幺元）：S 中的元素 1 有逆 1，所以 $1\in S^\times$. 而对任意的 $s\in S^\times\subset S$，有 $1s=s1=s$，所以 1 也为 $S^\times$ 中的幺元.
4. （逆）：由 $S^\times$ 的定义，其中的每个元素均有逆.

综上，$(S^\times,\cdot)$ 是一个群.

例题 1.4（子群的等价定义）：对于群 G 的子集 H，$H<G$，当且仅当

1. $H\neq\varnothing$;
2. 对任意的 $x,y\in H$，有 $xy^{-1}\in H$（或 $x^{-1}y\in H$）.

注 此处是全书中唯一一次使用子群的定义来证明一个结构是子群，绝大多数情况下，我们采用更为简洁的等价等义.（即本题所证之结论）

证明 一方面，如果 $H<G$，则命题易证.

另一方面，设 $H\neq\varnothing$，且对任意的 $x,y\in H$，有 $xy^{-1}\in H$.

1. 幺元存在：因为 $H\neq\varnothing$，所以存在 $h\in H$，从而 $1=hh^{-1}\in H$.
2. 逆存在：对任意的 $h\in H$，有 $h^{-1}=1h^{-1}\in H$.
3. 乘法封闭性：对任意的 $x,y\in H$，有 $y^{-1}\in H$，从而 $xy=x(y^{-1})^{-1}\in H$.

综上，$H<G$.

笔记 作者展示这一定理的证明，并不是鼓励大多家使用子群的定义. 请大家关心证明的后半部分，我们如何利用 xy^{-1} 反复取特殊值变形，得到我们想要的代数形式. 取特殊值，是代数变形的另一个维度，一般来说，优先考虑幺元、涉及到的元素及其逆.

问题 1.5（子群的交）：若 $\mathcal{A}$ 是群 G 的一些子群组成的集族，则
$$\bigcap_{H\in\mathcal{A}}H<G$$

证明 首先，对任意的 $x\in\bigcap_{H\in\mathcal{A}}H$，有 $x\in H\subset G$，从而 $\bigcap_{H\in\mathcal{A}}H\subset G$.

其次，对任意的 $H\in\mathcal{A}$，有 $1\in H$，从而 $1\in\bigcap_{H\in\mathcal{A}}H$，即 $\bigcap_{H\in\mathcal{A}}H\neq\varnothing$.

最后，对任意的 $x,y\in\bigcap_{H\in\mathcal{A}}H$，则对任意的 $H\in\mathcal{A}$，$x,y\in H$，有 $xy^{-1}\in H$. 所以，$xy^{-1}\in\bigcap_{H\in\mathcal{A}}H$.

综上，$\bigcap_{H\in\mathcal{A}}H<G$.

笔记 一般的，我们总可以将交集理解为“任意”，将并集理解为“存在”，这是因为：

$$x \in \bigcap_{i\in I} A_i \iff \forall i \in I, x \in A_i$$

$$x \in \bigcup_{i\in I} A_i \iff \exists i \in I, x \in A_i$$

我们后面还会多次碰到交和并的问题.

（三）同态的基本性质

幺半群同态和群同态之间有一个关键性的差别：是否需要额外指定“幺元”映到“幺元”. 群同态不需要额外指定，因为保持运算的群映射自然满足这一点.

问题 1.6 设 $\varphi : G \to H$ 是群同态，证明：$\varphi(1_G) = 1_H$.

证明 因为 $\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G)\varphi(1_G)$，从而由消去律，等式两边同时乘 $(\varphi(1_G))^{-1}$，即得 $1_H = \varphi(1_G)$.

练习 1.13 设 $\varphi : G \to H$ 是群同态，$g \in G$. 证明：

1. $\varphi(g^{-1}) = (\varphi(g))^{-1}$；
2. 对任意整数 n，$\varphi(g^n) = (\varphi(g))^n$.

利用群同态，可以得到定义域和陪域的特殊的子群：象与核，这两个子群对于群同态的性质的描述有关键意义.

问题 1.7 已知群同态 $\varphi : G \to H$，则 $\ker\varphi < G$.

证明 一方面，$\varphi(1_G) = 1_H$，从而 $1 \in \ker\varphi$. 即 $\ker\varphi \neq \varnothing$.

另一方面，对任意的 $x, y \in \ker\varphi$，有

$$\begin{aligned}\varphi(xy^{-1}) &= \varphi(x)\varphi(y^{-1}) \\ &= \varphi(x)\varphi(y)^{-1} \\ &= 1\end{aligned}$$

从而 $xy^{-1} \in \ker\varphi$.

综上，$\ker\varphi$ 是 G 的子群.

问题 1.8 φ 为单同态，当且仅当 $\ker\varphi = \{1_G\}$.

证明 一方面，设 φ 为单同态. 由于 $\varphi(1_G) = 1_H$，所以若 $\varphi(x) = 1_H$，则必有 $x = 1_G$，从而 $\ker\varphi = \{1_G\}$.

另一方面。设 $\ker\varphi = \{1_G\}$. 对任意的 $x, y \in G$，若 $f(x) = f(y)$，则 $1_H = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$. 从而 $xy^{-1} \in \ker\varphi = \{1_G\}$，即 $xy^{-1} = 1_G$，也就有 $x = y$.

1.2.4 典型例题

（一）群的证明

我们再通过一个例子，说明群证明的方法. 读者需要通过这些基础练习，快速进入抽象代数的大门.

例题 1.5 设 $G = \{z \in \mathbb{C} : \exists n \in \mathbb{Z}_+, z^n = 1\}$. 证明 G 连同乘法是一个群（复数域中的单位根群）.

证明

1. （封闭性）对任意的 $g, h \in G$，由 G 的定义，存在正整数 m, n，使得 $g^m = 1, h^n = 1$. 于是 $(gh)^{mn} = (g^m)^n(h^n)^m = 1$，也就是 $gh \in G$.
2. （结合律）：复数域中，结合律显然成立.
3. （幺元）：G 中有元素 1，使得对任意 $g \in G$，$g \cdot 1 = 1 \cdot g = g$.

4. (逆)：取任意 $g \in G$，于是存在正整数 m，使得 $g^m = 1$. 考察元素 $1/g$，因为 $(1/g)^m = 1/g^m = 1$，从而 $1/g \in G$，且满足 $g \cdot 1/g = 1/g \cdot g = 1$. 从而 $1/g$ 为 g 的逆.

综上，$(G, \cdot)$ 是一个群.

✍ **练习 1.14** 设 $G = \{a + b\sqrt{2} \in \mathbb{R} : a, b \in \mathbb{Q}\}$.

1. 证明 G 连同实数的加法是一个群；
2. 记 $G^\times$ 是 G 中的非零元素，证明 $G^\times$ 连同实数的乘法是一个群.【感谢 Mamoe1 的校对.】

✍ **练习 1.15** 设 $G = [0, 1)$. 对任意的 $x, y \in G$，定义 $x * y$ 为 $x + y$ 的小数部分 (即 $x * y = x + y - [x + y]$). 证明 $(G, *)$ 是一个交换群.

（二）由子集生成子群

例题 1.6 设 G 为群，$A, B \subset G$.

1. 证明：若 $A \subset B$，则 $\langle A \rangle < \langle B \rangle$；
2. 给出一个例子，使得 $A \subset B$ 且 $A \neq B$，但 $\langle A \rangle = \langle B \rangle$.

证明

1. 因为 $\langle A \rangle$，$\langle B \rangle$ 都是群，所以我们只需证：$\langle A \rangle \subset \langle B \rangle$.

   对任意的 $g \in \langle A \rangle$，考虑任意包含 B 的 G 的子群 H，我们有 $A \subset B \subset H$，于是由生成的定义，$g \in H$. (g 属于每一个包含 A 的 G 的子群) 所以有：

   $$g \in \bigcap_{\substack{B \subset H \\ H < G}} H = \langle B \rangle$$

   命题即证.
2. 取 $A = \mathbb{Z} - \{0\}$，$B = \mathbb{Z}$，则 $A \subset B$ 且 $A \neq B$，但 $\langle A \rangle = \mathbb{Z} = \langle B \rangle$.

✍ **练习 1.16** 若 H 是群 G 的子群，证明：

1. $\langle H \rangle = H$；
2. $\langle H - \{1\} \rangle = H$.

（三）数集的结构关系

作为对群和群同态的概念的基本应用，我们来考察数集的结构关系. 这里需要注意的是，几个数集的一些核心区别. 例如，整数的除法不一定得到整数（一般是有理数）；正有理数的开平方不一定得到有理数（一般是实数）；负实数的开平方一定不是实数（是复数）.

例题 1.7 证明：群 $(\mathbb{Q}, +)$ 与群 $(\mathbb{Q}_+, \cdot)$ 不同构.

注 我们想要证明的是一个否定性命题：说明两个群不为同构. 结合我们学过的知识，从定义来看，可能以下两种证明途径：（当然可以结合反证法）

1. 两个群之间不存在双射；
2. 对两个群之间的任意双射，都存在两个元素不能够“保持运算”.

从同态/同构的性质来看，我们还有其他可能的证明途径：

1. 两个群里指定阶的元素个数不相同；
2. 两个群有某种性质不相同（比如交换性）；
3. ……

随着我们学习的知识不断增多，我们还会有其他的思路.

我们在这里列出诸多的思路，并不是希望读者机械地把这些点一条一条背下来，然后遇到新的题目逐个套用；而是借此展示解题思路的可能来源，即解题的思路都有对应的知识点加以启发. 我们需要在平时学习的过程中多加思考与积累，我们也希望读者能从这个例子的分析中，体会一些自己寻找思路的方法.

证明 假设映射 $f:(\mathbb{Q},+)\to(\mathbb{Q}_+,\cdot)$ 为群同构，于是必存在一个 $q\in\mathbb{Q}$，使得 $f(q)=2$. 考虑 $f(q/2)$，令 $f(q/2)=m\in\mathbb{Q}_+$，于是 $f(q)=f(q/2+q/2)=(f(q/2))^2=m^2$，从而 $2=m^2$. 然而 $m=\pm\sqrt{2}$，不是 $\mathbb{Q}_+$ 内的元素，矛盾！从而假设错误，即两群不同构.

笔记 我们回过头看一看，这一思路是如何寻到的，实际上是抓住了有理数集的关键特点，即对有理数开方，往往不再是有理数. 这样的思路是具有普遍性的，即我们可以关注特殊性，这种思路尤其对于反证法或者否定性结论十分有用.

练习 1.17 证明：

1. 群 $(\mathbb{Q},+)$ 与群 $(\mathbb{Q}^*,\cdot)$ 不同构；
2. 群 $(\mathbb{R},+)$ 与群 $(\mathbb{R}_+,\cdot)$ 同构.

提示 考虑指数运算.

证明

1. 假设 $\varphi:\mathbb{Q}\to\mathbb{Q}^*$ 是群同构，对任意 $x\in\mathbb{Q}$，$\varphi(x)=\varphi(\frac{x}{2})^2>0$，从而 φ 的像包含于 $\mathbb{Q}_+$，此时 φ 必不是同构，矛盾！从而不存在群 $(\mathbb{Q},+)$ 与群 $(\mathbb{Q}^*,\cdot)$ 的同构.
2. 定义映射

$$\begin{aligned}\varphi:\mathbb{R}&\to\mathbb{R}_+\\ r&\mapsto e^r\end{aligned}$$

易证这是一个群同构.

1.2.5 习题

（一）群的证明

练习 1.18 下列代数结构中，哪些是半群，哪些是幺半群，哪些是群？证明你的结论.

1. $(\mathbb{Z},+)$；
2. $(\mathbb{Z},\cdot)$；
3. $(\mathbb{N},+)$；
4. $(\mathbb{Q},+)$；
5. $(\mathbb{Q},\cdot)$；
6. $(\mathbb{Q}^*,\cdot)$；
7. $(\mathbb{Q}_+,+)$.

解

1. 半群：$(\mathbb{Q}_+,+)$
2. 幺半群：$(\mathbb{Z},\cdot),(\mathbb{N},+),(\mathbb{Q},\cdot)$
3. 群：$(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{Q}^*,\cdot)$

练习 1.19 试举出一个半群的例子，它不是幺半群；再给出一个幺半群的例子，它不是群.

注 请参见前一题的答案.

练习 1.20 下列集合中，哪些连同有理数加法构成群？若是，证明之；反之，指出其不满足哪些群公理.

1. 既约的有理数集（包含 $0:=0/1$），其元素的分母为奇数；
2. 既约的有理数集（包含 $0:=0/1$），其元素的分母为偶数；
3. 有理数集，其元素的绝对值 <1；
4. 有理数集，其元素的绝对值 $\geqslant 1$，或为 0；
5. 有理数集，其元素的分母为 1 或 2；
6. 有理数集，其元素的分母为 $1,2$ 或 3.

注

1. 该集合是群. 注意到，对任意分母为奇数的既约分数 $\frac{n}{m}$ 和 $\frac{q}{p}$，有：
$$\frac{n}{m}+\frac{q}{p}=\frac{np+mq}{mp}$$
注意到 mp 必为奇数，所以 $\frac{np+mq}{mp}$ 对应的既约分数，分母依然是奇数.
2. 该集合不是群. 反例：
$$\frac{1}{6}+\frac{1}{6}=\frac{1}{3}$$
3. 该集合不是群. 反例：
$$\frac{2}{3}+\frac{2}{3}=\frac{4}{3}$$
4. 该集合不是群. 反例：
$$\frac{3}{2}-1=\frac{1}{2}$$
5. 该集合是群.
6. 该集合不是群. 反例：
$$\frac{1}{3}+\frac{1}{2}=\frac{5}{6}$$

✍ **练习 1.21** 设 $G=\{(a,b):a\in\mathbb{R}^*,b\in\mathbb{R}\}$. 在 G 上定义
$$(a,b)(c,d):=(ac,ad+b)$$
证明：G 是群.

✍ **练习 1.22*** 设 G 是群，S 是个非空集合，则所有从 S 到 G 的映射，在映射的乘法下构成一个群，记为 $M(S,G)$. 其中映射乘法是指，对 $f,g:S\to G$，定义 $fg:S\to G,x\mapsto f(x)g(x)$.

证明 （封闭性）：因为群在乘法下的封闭性，对任意 $x\in S$，$(fg)(x):=f(x)g(x)\in G$，于是 $fg\in M(S,G)$.

（结合律）：若 $f,g,h\in M(S,G)$，则对任意 $x\in S$，我们有
$$((fg)h)(x)=(fg)(x)h(x)=(f(x)g(x))h(x)=f(x)(g(x)h(x))=f(x)(gh)(x)=(f(gh))(x)$$
因此 $(fg)h=f(gh)$.

（幺元）：为了方便，我们滥用符号，令 $e:S\to G$，指的是恒等映射 $\forall x\in S,e(x)=e$. 则对于任意 $f\in M(S,G)$ 和任意 $x\in S$，我们有
$$(fe)(x)=f(x)e(x)=f(x)e=f(x).$$
同理，$(ef)(x)=f(x)$. 这就证明了（恒等映射）e 是 $M(S,G)$ 上的单位元.

（逆）：假设 $f\in M(S,G)$，我们定义 $f^{-1}\in M(S,G)$：对任意 $x\in S$，有
$$f^{-1}(x)=f(x)^{-1}.$$
（注意，这里的 f^{-1} 不是逆映射，而是 f 的乘法逆元.）

我们很容易检验，f^{-1} 确实是 f 在 $M(S,G)$ 中的逆，这是因为对任意 $x\in S$，我们有
$$f^{-1}(x)f(x)=f(x)^{-1}f(x)=e.$$
同理，我们有 $f(x)f^{-1}(x)=e$. 因此，在 $M(S,G)$ 中，我们有
$$f\cdot f^{-1}=f^{-1}\cdot f=e.$$
其中 e 是 $M(S,G)$ 中的单位元，即把 S 中所有元素映到单位的映射.

综上所述，$M(S,G)$ 确实是个群.

（二）子群的证明

✍ **练习 1.23** 设 G 是交换群.

1. 证明：$\{g\in G:|g|<\infty\}$ 是 G 的子群.（被称为 G 的挠子群（torsion subgroup））

2. 当 G 不是交换群时，试给出一个反例.

提示 第一小问中，注意在交换群上有 $(gh)^n = g^n h^n$.

第二小问，在 $GL_2(\mathbb{R})$ 中，考虑元素 $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ -3 & -2 \end{pmatrix}$.

✍ **练习 1.24** 定义 $\mathbb{R}$ 上的 n 阶特殊线性群：

$$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$$

证明：$SL_n(\mathbb{R}) < GL_n(\mathbb{R})$.

✍ **练习 1.25** 证明：集合 $\{(a_{ij}) \in GL_n(\mathbb{R}) : a_{ij} = 0 \, \forall \, i > j\}$ 连同矩阵的乘积运算，是 $GL_n(\mathbb{R})$ 的子群.

✍ **练习 1.26** 证明：集合 $\{(a_{ij}) \in GL_n(\mathbb{R}) : \forall \, i > j, a_{ij} = 0; \forall \, i, a_{ii} = 1\}$ 连同矩阵的乘积运算，是 $GL_n(\mathbb{R})$ 的子群.

✍ **练习 1.27** 设 H 是群 $(\mathbb{Q}, +)$ 的子群，且满足性质：对任意 $x \in H - \{0\}$，$1/x \in H$. 证明：$H = \{0\}$ 或 $\mathbb{Q}$.

提示 反复利用性质：若 $x \in H$，则对任意整数 n 都有 $nx \in H$.

证明 设 $H \neq \{0\}$，则存在非零有理数 $p/q \in H$，其中 $p \in \mathbb{Z}^*, q \in \mathbb{Z}_+$. 根据加法的封闭性，$q$ 个 p/q 之和

$$p = q \cdot \frac{p}{q} = \frac{p}{q} + \frac{p}{q} + \cdots + \frac{p}{q} \in H$$

从而 $1/p \in H$，类似地有 $1 = p \cdot 1/p \in H$.

所以任意整数 $n = n \cdot 1 \in H$，从而 $1/n \in H$，最终任意有理数 $m/n = m \cdot 1/n \in H$.

综上所述，$H = \{0\}$ 或 $\mathbb{Q}$.

✍ **练习 1.28** 设 G, H 为群，证明以下集合都是 $G \times H$ 的子群（与 $G \times H$ 使用同样的运算）：

1. $\{(g, 1) : g \in G\}$;
2. $\{(1, h) : h \in H\}$;
3. $\{(g, g) : g \in G\}$，其中 $G = H$.

✍ **练习 1.29** 设 G 是交换群，且取定 $n \in \mathbb{Z}$. 证明以下集合都是 G 的子群（与 G 使用同样的运算）：

1. $\{g^n : g \in G\}$;
2. $\{g \in G : g^n = 1\}$.

✍ **练习 1.30*** 群 G 被称作有限生成的，若存在一个有限集 A，使得 $H = \langle A \rangle$. 证明：

1. 每个有限群都是有限生成的;
2. $\mathbb{Z}$ 是有限生成的;
3. 每个有限生成的 $(\mathbb{Q}, +)$ 子群都是循环群;
4. $(\mathbb{Q}, +)$ 不是有限生成的.

提示 第三小问，设 $\mathbb{Q}$ 的有限生成子群 $H = \langle p_1/q_1, \cdots, p_k/q_k \rangle$，设 $q = q_1 \cdots q_k$，则

$$H = \left\langle \frac{1}{q} \cdot \gcd\left(\frac{p_1 q}{q_1}, \cdots, \frac{p_k q}{q_k} \right) \right\rangle$$

（三）同态的基本性质

✍ **练习 1.31** 设 $\varphi : G \to H$ 是群同构，证明：G 是交换群，当且仅当 H 是交换群.

✍ **练习 1.32** 设 G 是一个群. 证明：映射 $\varphi : G \to G$, $g \mapsto g^2$ 是群同态，当且仅当 G 是交换群.

证明 一方面，设 φ 是群同态. 对任意的 $g, h \in G$，有：

$$\begin{aligned} g^2 h^2 &= f(g) f(h) \\ &= f(gh) \\ &= (gh)^2 \\ &= ghgh \end{aligned}$$

从而 $gh=hg$，即 G 是交换群.

另一方面，设 G 是交换群. 对任意的 $g,h\in G$，有：

$$\begin{aligned}f(g)f(h)&=g^2h^2\\&=gghh\\&=g(hg)h\\&=(gh)^2\\&=f(gh)\end{aligned}$$

即 φ 是群同态.

综上，命题得证.

✍ **练习 1.33** 设 G 是一个群. 证明：映射 $\varphi:G\to G,\ g\mapsto g^{-1}$ 是群同态，当且仅当 G 是交换群.

证明 一方面，设 φ 是群同态. 对任意的 $g,h\in G$，有：

$$\begin{aligned}gh&=f(g^{-1})f(h^{-1})\\&=f(g^{-1}h^{-1})\\&=f((hg)^{-1})\\&=hg\end{aligned}$$

即 G 是交换群.

另一方面，设 G 是交换群. 对任意的 $g,h\in G$，有：

$$\begin{aligned}f(g)f(h)&=g^{-1}h^{-1}\\&=h^{-1}g^{-1}\\&=(gh)^{-1}\\&=f(gh)\end{aligned}$$

即 φ 是群同态.

综上，命题得证.

注 本题和前一题的核心都是交换群的运算特性. 交换性的定义是非常简单的：

$$gh=hg$$

而在具体问题中，他会以各种各样的等价形式呈现，比如本题的“逆形式”

$$g^{-1}h^{-1}=(gh)^{-1}$$

或者前一题的“平方形式”

$$g^2h^2=(gh)^2$$

又比如“换位子形式”

$$g^{-1}h^{-1}gh=1$$

其中 $g^{-1}h^{-1}gh$ 被称为 g,h 的“换位子”.

再比如“交错形式”

$$h^{-1}ghg^{-1}=1.$$

✍ **练习 1.34*** 设 G 为有限群，$\varphi:G\to G$ 是群同构，且满足：

1. 对任意 G 的元素 $g\neq 1$，有 $\varphi(g)\neq g$；
2. $\varphi^2=id.$（恒等映射）.

证明：G 是奇数阶交换群.

证明

1. (奇数阶)：任取一个元素 $g \neq 1$ 有：

$$\varphi(g) = \varphi(g)$$
$$\varphi(\varphi(g)) = g$$

且 $g \neq \varphi(g)$. 从而 G 中的元素，除了幺元 1，总是 $g, \varphi(g)$ 两两分组，从而 G 的阶为奇数.

2. (交换性)：定义集合 $H = \{g^{-1}\varphi(g) : g \in G\}$，且定义映射

$$f : G \to H$$
$$g \mapsto g^{-1}\varphi(g)$$

f 显然是满射，而若有 $g^{-1}\varphi(g) = h^{-1}\varphi(h)$，则

$$\varphi(g)(\varphi(h))^{-1} = gh^{-1}$$
$$\varphi(g)\varphi(h^{-1}) = gh^{-1}$$
$$\varphi(gh^{-1}) = gh^{-1}$$

结合 φ 的第一条性质，此时必然有 $gh^{-1} = 1$，即 $g = h$. 从而 f 是单射，于是 f 是双射. 又 G 是有限集，所以必然有 $G = H$.

对任意的 $g \in G$，存在 $a \in G$，使得 $g = a^{-1}\varphi(a)$，于是有：

$$\begin{aligned}\varphi(g) &= \varphi(a^{-1}\varphi(a)) \\ &= \varphi(a^{-1})\varphi^2(a) \\ &= \varphi(a^{-1})a \\ &= \varphi(a)^{-1}(a^{-1})^{-1} \\ &= (a^{-1}\varphi(a))^{-1} \\ &= g^{-1}\end{aligned}$$

利用前一题的结论，即可证明 G 是交换群.

注 本题的思路来源，笔者目前没有想明白，有知道的读者还望不吝赐教.

✍ **练习 1.35*** 证明：

1. 群 $(\mathbb{R}^*, \cdot)$ 与群 $(\mathbb{C}^*, \cdot)$ 不同构；
2. 群 $(\mathbb{Z}, +)$ 与群 $(\mathbb{Q}_+, \cdot)$ 不同构；
3. 群 $(\mathbb{Q}, +)$ 与群 $(\mathbb{R}_+, \cdot)$ 不同构.

证明

1. 第一小问，假设 φ 是群 $(\mathbb{R}^*, \cdot)$ 到群 $(\mathbb{C}^*, \cdot)$ 的一个同构映射，则 $\varphi(1) = 1$. 注意到 $\varphi(-1)^2 = \varphi(1) = 1$ 而 $\varphi(-1) \neq \varphi(1)$，只能有 $\varphi(-1) = -1$.

   设 $\sqrt{-1}$ 的原象为 x，即 $\varphi(x) = \sqrt{-1}$，那么 $\varphi(x^2) = \varphi(x)^2 = -1 = \varphi(-1)$，于是 $x^2 = -1$，矛盾.

   综上所述，群 $(\mathbb{R}^*, \cdot)$ 与群 $(\mathbb{C}^*, \cdot)$ 不同构.

2. 第二小问，假设 φ 是群 $(\mathbb{Z}, +)$ 到群 $(\mathbb{Q}_+, \cdot)$ 的一个同构映射，设 $\varphi(1) = a$，那么对任意整数 n，$\varphi(n) = a^n$. 当 $a > 1$ 时，$\cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots$ 严格单调递增，于是 $(a + a^2)/2$ 没有原象；当 $a < 1$ 时，$\cdots, a^{-2}, a^{-1}, 1, a, a^2, \cdots$ 严格单调递减，$(a + a^2)/2$ 同样没有原象.

   综上所述，群 $(\mathbb{Z}, +)$ 与群 $(\mathbb{Q}_+, \cdot)$ 不同构.

3. 第三小问，由于 $\mathbb{Q}$ 是可数集，$\mathbb{R}_+$ 是不可数集，不存在 $\mathbb{Q}$ 到 $\mathbb{R}_+$ 的双射，所以群 $(\mathbb{Q}, +)$ 与群 $(\mathbb{R}_+, \cdot)$ 不同构.

1.2.6 拓展

练习 1.36 设 G 为群，$s \in G$，证明：$\langle s \rangle = \left\{ s^k : k \in \mathbb{Z} \right\}$，其中令 $s^0 = e$.

练习 1.37 设 G 为群，$S \subset G$ 是个非空子集，则 $\langle S \rangle = \left\{ a_1^{k_1} \cdots a_n^{k_n} : a_1, \cdots, a_n \in S, k_1, \cdots, k_n \in \mathbb{Z}, n \in \mathbb{N} \right\}$. 其中 $a_i^0 = e$.

注 注意，这里的结论和幺半群中的区别在于指数可以是负数. 原因是子群不仅在乘法下封闭，而且在逆元下也封闭.

证明过程是类似的. 首先，这确实是一个群.

1. 封闭性：和幺半群的证明是同样的；
2. 单位元：因为对任意 $a \in S$，我们有 $e = a^0 \in \left\{ a_1^{k_1} \cdots a_n^{k_n} : a_1, \cdots, a_n \in S, k_1, \cdots, k_n \in \mathbb{Z}, n \in \mathbb{N} \right\}$；
3. 逆元：根据上面的练习，我们知道

$$\left(a_1^{k_1} \cdots a_n^{k_n} \right)^{-1} = a_n^{-k_1} \cdots a_1^{-k_1} \in \left\{ a_1^{k_1} \cdots a_n^{k_n} : a_1, \cdots, a_n \in S, k_1, \cdots, k_n \in \mathbb{Z}, n \in \mathbb{N} \right\}.$$

其次，假设 $H < G$ 是个子群，并且 $S \subset H$. 令 $a_1, \cdots, a_n \in S$. 因此对任意 i 都有 $\langle a_i \rangle \subset H$. 特别地，对于 $k_1, \cdots, k_n \in \mathbb{Z}$，我们有 $a_1^{k_1}, \cdots, a_n^{k_n} \in H$. 因为 H 是个子群，所以在乘法下封闭，因此 $a_1^{k_1} \cdots a_n^{k_n} \in H$. 这就证明了 $\left\{ a_1^{k_1} \cdots a_n^{k_n} : a_1, \cdots, a_n \in S, k_1, \cdots, k_n \in \mathbb{Z}, n \in \mathbb{N} \right\} \subset H$.

练习 1.38（有限群的子群的等价定义）：对于有限群 G 的子集 A，$A < G$，当且仅当 $A \neq \varnothing$ 且 $\forall x, y \in A, xy \in A$.

证明 一方面，当 A 是 G 的子群时，A 中乘法的封闭性是显然的.

另一方面，假设 $A \subset G$ 是个有限的非空子集，且对乘法封闭. 我们只需证明，对任意 $a, b \in A$，方程 $xa = b$ 和 $ay = b$ 在 A 中有解.（见下一节“群的等价定义”）

令 $a \in A$，令 $\phi : A \to A$，对任意 $x \in A$，定义为 $\phi(x) = xa$.

利用乘法的封闭性，这是良定义的. 又因为消去律，即 $xa = ya \implies x = y$，我们知道 ϕ 是个单射. 在这里，因为 A 是个有限集，所以这样的单射必须是双射.

因此对任意 $a, b \in A$，我们知道方程 $xa = b$ 在 A 中有解，同理 $ay = b$ 在 A 中也有解. 又因为 A 显然是个半群，所以这就告诉我们 A 是个子群.

笔记 注意，子群一般需要对乘法封闭和对逆运算封闭两个条件. 在这里，对于有限的非空子集，我们只需要前者，因此这显然是个不大平凡的结论. 相比起具体能让我们在解题中省下多少时间，这个结论本身就应该让人感到惊喜.

1.3 专题：代数变形

在一般的群中，交换律并不满足，由此产生了许多不同于数的运算的代数运算特性，例如，在实数的乘法运算中，我们不加思索地就会写出：

$$xyxy = (xy)^2 = x^2y^2$$

$$xyx^{-1} = y$$

然而这些在不满足交换律的群中，往往是不成立的，这是导致我们对群的认识和研究有困难的核心矛盾. 通过后面的学习我们会知道，有限生成的交换群有统一的同构型；特别的，给定一个有限交换群的阶，我们很容易就能知道它的可能的所有同构型，这些在非交换群中是没有的.

那么，我们为什么还要研究相对而言性质“不太优美”的非交换群呢？请大家思考一下，在我们的数学学习生涯中，有没有不满足交换性封闭的二元运算？有的，而且有一类不交换的二元运算我们经常使用：映射的复合运算.（需要说明的是，如果所给的映射的集合不合适，复合运算有可能不封闭）诸如函数的复合运算、矩阵的乘积、线性映射的复合……他们都属于这一类. 而映射是数学的核心概念，离开映射就没有办法构建数学的大厦了. 笔者认为，仅从这一点而言，我们就必须研究非交换群. 事实上，由 Cayley 定理（读者会在群作用的部分学到这一定理），任意一个群中的元素，都可以视为某个集合到自身的双射，而一个集合到自身的全体双射，连

同复合运算构成了对称群，于是群天然地被打上了“映射”的烙印，也就是说，我们不能回避不交换带来的各种问题.

但是，交换毕竟比不交换的性质要好，因此我们总是尽可能地在非交换的群中寻找（部分或全体的）交换性. 请读者注意，我们对交换性地关注贯穿群论的学习和研究，而此处，就是我们探讨交换性的起点.

1.3.1 幺元的性质

不管一个群全局的交换性有多差（事实上我们现在也没有一个指标衡量全局交换性，以后我们会学到若干衡量指标），我们总会有一个元素，它和群中每个元素都交换，这个元素就是幺元.

幺元的交换性我们不必多说，定义展示的非常清楚，而接下来的事实，则是我们经常忽略的. 在群的定义中，和幺元联系最紧密的概念，是一个元素的逆，由定义不难看出，一个元素和它的逆是交换的，我们先看下例.

例题 1.8 群 G 中有两个元素 x,y，且 $xy=1$，证明：$yx=1$.

证明 [1：利用方程的特性] 我们有

$$\begin{aligned} xy&=1\\ xyy^{-1}&=y^{-1}\\ x&=y^{-1} \end{aligned}$$

所以有 $yx=yy^{-1}=1$.

证明 [2：直接代数变形]

$$yx=yx1=yx(yy^{-1})=y(xy)y^{-1}=y1y^{-1}=yy^{-1}=1$$

此即得证.

笔记 方法一是最直接最简单的做法，没有进一步分析的必要.

方法二在这里略显复杂，但是其处理手法是非常基本的，我们有必要做一点分析：

我们想要证 $yx=1$，同时要利用 $xy=1$，以及 G 为群. 观察 yx，通过它，至少有两种简单的方式产生 xy，即 $x(yx)=(xy)x$，以及 $(yx)y=y(xy)$，而为了确保所作变形为恒等变形，我们不好直接乘 x 或 y，从而我们想到利用幺元“无中生有”，即 $yx=yx1=yx(yy^{-1})$，注意到 y^{-1} 的出现由群 G 所保证. 进一步的，$yx(yy^{-1})$ 的形式，让我们很自然地想要“过河拆桥”：$yx(yy^{-1})=y(xy)y^{-1}=yy^{-1}$，利用幺元约去了 xy，从而有效地化简了式子，最终得到了结果.

我们也可以使用 $yx=1yx$ 来解决此题，请读者自行写出解题过程.

需要强调的是，笔者并不赞同为了炫技而故意将问题解的复杂的方式，从这一角度而言，如果读者在练习或者测试中遇到本题，方法一一定是最优的选择. 方法二在一些更复杂的题目中有其优势（甚至是只能这样做），因此我们予以详细解释.

此例告诉我们，在一个群中，一个元素如果有左逆，左逆就是逆（同理，右逆也就是逆，读者可以作为练习自己尝试）. 事实上，读者对比两种解法就可以发现，本例就是逆的性质的变形而已，它和逆的性质是等价的. 而例题中这种写法的妙处，在于实际操作时，不必引入一个元素的逆，就可以直接换位. 我们在后面较为复杂的题中就会发现，减少一个中间环节，得到的不仅仅是节省的时间，更包含审视等式的不同的视角（逆的视角，或者交换性的视角）. 下面我们来看一些应用这一结论得到的简单但不显然的结论.（以下系列习题由 Maki 与 Victor 发现并讨论）

练习 1.39 群 G 中有 n 个元素 $x_1,x_2,\cdots,x_n$，且 $x_1x_2\cdots x_n=1$，证明：$x_2\cdots x_nx_1=x_3\cdots x_nx_1x_2=\cdots=x_nx_1\cdots x_{n-1}=1$.

证明 因为

$$x_1x_2\cdots x_n=x_1(x_2\cdots x_n)=1$$

所以 $(x_2\cdots x_n)x_1=1$.

其他等式可类似得证.

笔记 我们看到 $x_1x_2\cdots x_n=1$ 具有轮换性.

练习 1.40 设 x,y 是群 G 的元素，n 是正整数.

1. 若 $(xy)^n=1$，证明：$(yx)^n=1$；
2. 若 $(xy)^nx=1$，证明：$xy=yx$.

证明

1. 因为：

$$1=(xy)^n=xyxy\cdots xy=x(yxy\cdots xy)$$

所以

$$1=x(yxy\cdots xy)=(yxy\cdots xy)x=(yx)^n$$

2. 因为：

$$1=(xy)^nx=xy((xy)^{n-1}x)$$
$$1=(xy)^nx=((xy)^{n-1}x)yx$$

所以 $xy=yx$.

练习 1.41 群 G 中有两个元素 x,y，且 $xy=1$，证明：

1. $x^2y^2=y^2x^2=1$；
2. 对任意正整数 n，有 $x^ny^n=y^nx^n=1$.

证明

1. 因为 $xy=1$，所以 $y=x^{-1}$，从而 $x^2y^2=x^2x^{-2}=1$，y^2x^2 同理可证.
2. 因为 $xy=1$，所以 $y=x^{-1}$，从而 $x^ny^n=x^nx^{-n}=1$，y^nx^n 同理可证.

练习 1.42 群 G 中有三个元素 a,g,n，且 $a^m=1,agng^{-1}=1$，证明：$n^m=1$.

证明 因为 $agng^{-1}=1$，所以 $gng^{-1}=a^{-1}$，即 $gn^mg^{-1}=(gng^{-1})^m=a^{-m}=1$，从而 $n^m=g^{-1}g=1$.

笔记 这里我们发现了共轭形式的一个性质：$(gng^{-1})^m=gn^mg^{-1}$.

练习 1.43* 幺半群 G 中有三个元素 x,y,z，且 $xy=yz=1$，证明：$x=z$.（也就是说，若某个幺半群中的元素同时有左逆和右逆，那么它们是相等的）

证明 我们有：

$$x=x1=x(yz)=(xy)z=1z=z.$$

笔记 本例告诉我们，当一个元素的逆不知道是否存在的时候，由左逆和右逆，仍然能得到元素的逆. 从这一角度而言，本小节的第一题中，方法二更贴近逆的定义核心，本质上一个元素和其逆的交换性，依赖于幺元和任意元素的交换性.

1.3.2 等式的使用方法

在群中，给定一个等式 $a=b$，我们可以如何使用它呢?

显然的，我们可以做代入操作. 注意到等号是双向的，所以我们既可以在其他的代数式中，将 a 替换成 b，或者将 b 替换成 a. 同时我们还可以做归边操作，即将右侧的代数式全部移动到左边（或者反之），此时我们会得到

$$ab^{-1}=b^{-1}a=a^{-1}b=ba^{-1}=1.$$

我们再考虑复杂一点的情况，例如给定等式 $a=bc$，此时归边操作的可能性会变得很多，因为我们可以“部

分归边”，比如将等式改写为 $b^{-1}a=c$，$ac^{-1}=b$，而完全归边的情况也多了起来，我们有：

$$b^{-1}ac^{-1}=c^{-1}b^{-1}a=ac^{-1}b^{-1}=1$$

事实上这三个式子是轮换的，所以上一小节的讨论已经展示了这一点.

以上是一些泛泛而谈，实际情况下，究竟使用哪些形式更为简单，这一点没有定论. 我们需要根据代数变形的目标，以及自己的解题经验，进行一个综合判断.

✍ **练习 1.44*** 设 u,v 是群 G 中的元素，满足：

$$uv=v^2u^2,\ u^4=1,\ v^3=1$$

证明：$u=v=1$.

注 本题我们将尽可能使用各种代数变形方法来解决，读者可以从中了解它们的特点.

证明 [1：直接代入化简] 因为

$$\begin{aligned}u&=uv^3=(uv)v^2\\&=v^2u^2v^2=v^2u(uv)v\\&=v^2uv^2u^2v=v^2(uv)vu^2v\\&=v^4u^2vu^2v=vu(uv)u^2v\\&=vuv^2u^4v=vuv^3=vu\end{aligned}$$

所以 $v=1$. 代入 $uv=v^2u^2$ 可得 $u=u^2$，从而 $u=1$. 命题得证.

笔记 方法一的关键在于反复从“同一个方向”（本例为从左至右）使用 $uv=v^2u^2$，且利用剩下两个等式简化等式. 只要坚持变形到最后，且不要计算错误，获得结果是必然的.

证明 [2: 归边操作] 因为 $uv=v^2u^2$，所以 $(vu)(vu^2)=v(uv)u^2=v^3u^4=1$. 由逆的交换性可得 $(vu^2)(vu)=1$，结合前式可得：

$$\begin{aligned}vuvu^2&=vu^2vu\\(vu)^{-1}(vu)vuuu^{-1}&=(vu)^{-1}(vu)uvuu^{-1}\\vu&=uv\end{aligned}$$

从而代回原式可得 $vu=v(vu)u$，即 $vu=1$. 所以 $1=(vu)^4=v^4u^4=v$【请读者思考，第二个等号为什么成立？】，从而也就有 $u=1$.

笔记 方法二利用等于 1 的等式的轮换性化简条件. 当然这样的方法有其局限，比如将条件改为 $uv=v^2u^3$，此时我们会得到 $vuvu=1$，再按照前述的思路处理，就只能得到 $1=1$ 了.

证明 [3：等式取逆] 因为 $uv=v^2u^2$，所以两侧都取逆可得 $v^2u^3=u^2v$，于是：

$$\begin{aligned}uvu&=v^2u^3=u^2v\\vu&=uv\end{aligned}$$

以下步骤和证法 2 相同.

笔记 我们同样将条件改为 $uv=v^2u^3$，此时取逆，我们会得到 $v^2u^3=uv$，同样无法再处理下去.

此题我们使用了三种解题方法，一般来说，方法一的思路初学者比较容易想到，但显然化简得过程较为复杂，容易出错. 方法二和方法三都更灵活的应用了条件 $uv=v^2u^2$，但是我们也在评注中给出了方法“失效”的例子. 事实上，我们会在下一小节更详细的讨论该题，并且试图说明，这些方法的“失效”，是因为所给条件原本就无法化简到更简单的形式，而不是方法出了问题. 我们在遇到新的问题时，总可以先尝试更为简单的后两种方法，实在没办法时，再考虑方法一。

✍ **练习 1.45** 证明：b 是含幺半群 G 中元素 a 的逆，当且仅当下式成立：

$$aba=a,\ ab^2a=1$$

证明 一方面，已知 $b=a^{-1}$，则 $aba=aa^{-1}a=a$，且 $ab^2a=aa^{-1}a=1$.

另一方面，已知 $aba=a$, $ab^2a=1$，则有：

$$\begin{aligned} ab &= ab(ab^2a) \\ &= (aba)b^2a \\ &= ab^2a \\ &= 1 \end{aligned}$$

$ba=1$ 同理可证，从而 $b=a^{-1}$.

综上，原命题得证.

✍ **练习 1.46*** 设 G 为群，$a_1,a_2,b_1,b_2\in G$，整数 m,n 互素，且满足

$$\begin{aligned} a_1b_1=b_1a_1=a_2b_2=b_2a_2 \\ a_1^m=a_2^m=b_1^n=b_2^n \end{aligned}$$

证明：$a_1=a_2,\quad b_1=b_2$.

证明 注意到 m,n 互素，以及 $a_1^m=a_2^m$，我们只须证明 $a_1^n=a_2^n$.

因为

$$\begin{aligned} &(a_1b_1)^n=a_1^nb_1^n \qquad (\text{注意到}a_1,b_1\text{是交换的，从而这一等号成立，下面一个等号也是如此}) \\ &(a_2b_2)^n=a_2^nb_2^n \end{aligned}$$

而 $a_1b_1=a_2b_2$，所以 $a_1^nb_1^n=a_2^nb_2^n$，又因为 $b_1^n=b_2^n$，所以 $a_1^n=a_2^n$. 同理我们可以证明 $b_1=b_2$. 此题即证.

笔记 本题利用了数论中一个非常重要的定理：Bézout 定理，即对任意非零整数 m,n，存在整数 k,l，使得 $km+ln=\gcd(m,n)$.

在本题中，若已知 $a_1^m=a_2^m$ 和 $a_1^n=a_2^n$，因为 $\gcd(m,n)=1$，所以存在整数 k,l，使得 $km+ln=1$，于是我们有：

$$\begin{aligned} a_1 &= a_1^{km+ln} \\ &= a_1^{km}a_1^{ln} \\ &= (a_1^m)^k(a_1^n)^l \\ &= (a_2^m)^k(a_2^n)^l \\ &= a_2^{km}a_2^{ln} \\ &= a_2^{km+ln} \\ &= a_2. \end{aligned}$$

✍ **练习 1.47**** 设 a,b 是群 G 中的元素，满足：

$$aba=ba^2b,\ a^3=1,\ b^{2n-1}=1$$

证明：$b=1$.

注 笔者认为，此题初学者经过仔细思考后实在做不出也没有关系，可以先跳过.

以下两种解法，第一种来自于《近世代数三百题》，第二种综合了 Maki 与 Victor 的思考与讨论而来，我们会分析方法二的思路.

证明 [1] 因为 $ab^2a=aba^3ba=(aba)a^2ba=(ba^2b)a^2ba=ba^2(ba^2b)a=ba^2(aba)a=b^2a^2$，于是 $ab^2=b^2a$.

设 $ab^{2r}=b^{2r}a$，则 $ab^{2(r+1)}=ab^{2r}b^2=b^{2r}ab^2=b^{2r}b^2a=b^{2(r+1)}a$，于是对任一正整数 k 有 $ab^{2k}=b^{2k}a$. 特别的，$ab^{2n}=b^{2n}a$.

因为 $b^{2n-1}=1$，所以 $b^{2n}=b$，从而 $ab=ba$，于是 $ba^2=aba=ba^2b$，即 $b=1$.

证明 [2] 因为 $aba = ba^2b$，从而

$$\begin{aligned} aba &= ba^2b = ba(aba)a^2 \\ &= baba^2ba^2 = b(aba)(aba)a \\ &= b^2a^2b^2a^2ba = b^2a^2b^2a(aba) \end{aligned}$$

即 $b^2a^2b^2a = 1$. 因为 $a^3 = 1$，从而 $b^2(a^{-1}b^2a) = 1$，于是 $(b^2)^n(a^{-1}b^2a)^n = 1$，即 $b^{2n}(a^{-1}b^{2n}a) = 1$. 因为 $b^{2n-1} = 1$，从而 $b^{2n} = b$，也就是 $ba^{-1}ba = 1$.

注意到 $a^{-1} = a^2$，于是 $1 = ba^{-1}ba = (ba^2b)a = aba^2$，从而 $a = (aba^2)a = ab$，即 $b = 1$.

笔记 我们的思路来源非常简单，先从“同一个方向”使用最复杂的关系 $aba = ba^2b$，然后得到了一个简单一些的关系：$b^2a^2b^2a = 1$. 注意到 $a^{-1} = a^2$，于是原式的的形式进一步被简化，包含了我们喜欢的共轭形式.

1.3.3 应用：“拟交换”条件的使用

【注：本小节涉及生成元、有限交换群的结构定理等后续知识，读者如果初学群论，建议先跳过讨论，只做习题即可.】

我们拿出上一小节的第一题，进行进一步的分析. 为讨论方便，我们不妨直接讨论由 u, v 生成的群：

$$G = \langle u, v \mid u^4 = 1, v^3 = 1, u^av^b = v^cu^d \rangle$$

其中 a, d 是 0 到 3 之间的整数，b, c 是 0 到 2 之间的整数，且 a, b, c, d 不全为 0，我们不妨称 $u^av^b = v^cu^d$ 为拟交换条件. 此时，我们会有以下疑问：群 G 的阶是否确定？群 G 的同构型有哪些？

1. $(c = d = 0)$：拟交换条件简化为 $u^av^b = 1$：

拟交换条件	G 的构型
$u = 1$	$G = \langle v \mid v^3 = 1 \rangle \simeq \mathbb{Z}_3$
$u^2 = 1$	$G = \mathbb{Z}_2 * \mathbb{Z}_3$
$v = 1$	$G = \langle u \mid u^4 = 1 \rangle \simeq \mathbb{Z}_4$
$uv = 1$	$G = 1$
$uv^2 = 1$	$G = 1$
$u^2v = 1$	$G = \langle u \mid u^2 = 1 \rangle \simeq \mathbb{Z}_2$

这些讨论同时包含了 a, b, c, d 中至少有一个为 0 的情况，以下设 a, b, c, d 均不为 0.

我们只需要考虑 $a \leqslant 2, b \leqslant 1$ 的情况，这是因为当 $a \geqslant 3$ 时将 u 替换成 u^{-1}，当 $b \geqslant 2$ 时将 v 替换成 v^{-1}，就可以把条件转化为 $a \leqslant 2, b \leqslant 1$ 的情况.

2. $(a = b = 1)$：拟交换条件为 $uv = v^cu^d$：

拟交换条件	G 的构型
$uv = vu$	$G \simeq \mathbb{Z}_{12}$
$uv = v^2u$	$G \simeq \mathbb{Z}_3 \rtimes \mathbb{Z}_4$
$uv = vu^2$	$G = \langle v \mid v^3 = 1 \rangle \simeq \mathbb{Z}_3$
$uv = v^2u^2$	$G = 1$
$uv = vu^3$	$G = \langle u, v \mid u^2 = v^3 = 1, uv = vu \rangle \simeq \mathbb{Z}_6$
$uv = v^2u^3$	$G = \langle u, v \mid u^4 = 1, v^3 = 1, (uv)^2 = 1 \rangle$?

3. $(a = 2, b = 1)$：拟交换条件为 $u^2v = v^cu^d$：

拟交换条件	G 的构型
$u^2v=vu$	$G=\langle v\mid v^3=1\rangle\simeq\mathbb{Z}_3$
$u^2v=v^2u$	$G=1$
$u^2v=vu^2$	?
$u^2v=v^2u^2$	$G=\langle u,v\mid u^4=1,v^3=1,(vu^2)^2=1\rangle$?
$u^2v=vu^3$	$G=\langle v\mid v^3=1\rangle\simeq\mathbb{Z}_3$
$u^2v=v^2u^3$	$G=1$

✍ **练习 1.48** 设 u,v 是群 G 中的元素，满足：

$$u^4=1,\ v^3=1$$

试证明以下结论：

1. 若 $uv=1$，则 $u=v=1$；
2. 若 $uv^2=1$，则 $u=v=1$；
3. 若 $u^2v=1$，则 $u^2=v=1$；
4. 若 $uv=vu^2$，则 $u=1$；
5. 若 $uv=v^2u^2$，则 $u=v=1$；
6. 若 $uv=vu^3$，则 $u^2=1$，且 u,v 可交换；
7. 若 $u^2v=vu$，则 $u=1$；
8. 若 $u^2v=vu^3$，则 $u=1$；
9. 若 $u^3v=vu$，则 $u^2=1$，且 u,v 可交换；
10. 若 $u^3v=vu^2$，则 $u=1$；
11. 若 $uv^2=vu^2$，则 $u=v=1$；
12. 若 $uv^2=v^2u^2$，则 $u=1$；
13. 若 $u^2v^2=vu$，则 $u=v=1$；
14. 若 $u^2v^2=v^2u$，则 $u=1$

提示 我们这里针对一类特殊条件给出一个相对简单的做法.

我们考虑 $uv=vu^2$ 的情形，此时可以按如下方式变形

$$\begin{aligned}v&=vu^4=(vu^2)u^2\\&=uvu^2=u(vu^2)\\&=u^2v\end{aligned}$$

所以有 $u^2=1$，回代可得 $uv=v$，即 $u=1$.

这个代数式的特殊之处在于，v 在左右交换的时候，次数不变，此时我们进行化简时会变得简单. 条件 $uv=vu^3$，$u^2v=vu$ 等也具有类似性质，从而也可同样处理.

1.3.4 应用：群的等价定义

✍ **练习 1.49*** 设 G 是半群，且对任意 $a\in G$，存在唯一的 $a'\in G$，使得对任意的 $b\in G$，有

$$a'(ab)=b=(ba)a'$$

证明：G 是群.

证明 先证明：$a'a=aa'$.

题设中取 $b=a$，有 $a'a^2=a=a^2a'$，于是：

$$\begin{aligned} a'a &= a'(a^2a') \\ &= (a'a^2)a' \\ &= aa' \end{aligned}$$

再证明：对任意的 $a\in G$，$a'a=aa'$ 是 G 的幺元.

对任意的 $b\in G$，有：

$$(a'a)b=a'(ab)=b$$
$$b(a'a)=b(aa')=(ba)a'=b$$

于是 $a'a$ 为 G 的幺元（不妨记为 1）.

最后，对任意的 $a\in G$，存在 $a'\in G$，使得 $a'a=aa'=1$，从而 a' 为 a 的逆，即 G 的任一元素均有逆.

综上，半群 G 为群.

注：请读者按顺序做以下三题. 且如果感觉有难度，可以跳过.

练习 1.50 设 G 是一个半群，若满足：

1. （左幺元）：存在 $e\in G$，使得对任意的 $g\in G$，有 $eg=g$；
2. （左逆）：对任意的 $g\in G$，存在 $h\in G$，使得 $hg=e$.

证明 G 是群.

注 分析：我们需要证明的结论有两个：左幺元也是右幺元（即对所有的 $g\in G$ 有 $ge=g$）；左逆也是右逆. 先证明哪个呢？

我们先分析题设中给的条件：半群就是保证结合律可用，而且不用担心运算的结果不是 G 中的元素；剩下的无论是左幺还是左逆，都是在元素的左边添上新的元素并作计算. 此时，假定我们先尝试证明 $ge=g$，你会发现，如果我们选择处理 ge，则 e 只能选择变为 hg，而 gh 无法计算；如果选择处理 g，在 g 的左边添上 e 之后，得到的 eg 还是没有进一步处理的方式. 而过程中出现的 gh 提示我们，可能要先处理逆的问题.

于是，我们先考虑“左逆也是右逆”的问题. 此时又一个新的问题出现了，我们要证明的式子是什么？也许读者会考虑证明 $gh=e$，但是尝试一下之后就会发现 gh 也是很难处理的. 那我们该怎么办呢？

事实上，我们忽略了一个条件，因为题设只保证左逆的存在，所以 g 的左逆 h 自己也是有一个左逆的！我们不妨记 h 的左逆为 g'，于是，我们再处理 gh 时就容易了，读者做过前文中的代数变形的练习，即可独立解决问题.

证明 任取 G 的一个左幺元 e. 且对任意的 $g\in G$，记 g 的左逆为 h，h 的左逆为 g'. 先证明：$gh=e$.（从而每个元素都有一个左幺元意义下的逆.）

我们有：

$$\begin{aligned} gh &= egh && (e\text{ 是左幺元}) \\ &= g'hgh && (g'\text{ 是 }h\text{ 的左逆，从而 }g'h=e) \\ &= g'(hg)h && (\text{半群的运算满足结合律}) \\ &= g'eh && (h\text{ 是 }g\text{ 的左逆，从而 }hg=e) \\ &= g'(eh) && (\text{结合律}) \\ &= g'h && (e\text{ 是左幺元}) \\ &= e && (g'\text{ 是 }h\text{ 的左逆，从而 }g'h=e) \end{aligned}$$

再证明：左幺元 e 也是右幺元. 对任意的 $g \in G$，设 $h \in G$ 是 g 的一个逆（即 $hg = gh = e$），从而有：

$$\begin{aligned} ge &= g(hg) && (h \text{ 是 } g \text{ 的逆}) \\ &= (gh)g && (\text{结合律}) \\ &= eg && (h \text{ 是 } g \text{ 的逆}) \\ &= g && (e \text{ 是左幺元}) \end{aligned}$$

综上，G 中有一个幺元，且每个元素都有一个逆，从而半群 G 是群.

✍ **练习 1.51** 设 G 是一个半群，且对任意的 $g, h \in G$，方程 $xg = h$ 和方程 $gy = h$ 在 G 内有解. 证明 G 是群.

注 分析：利用上题的结论，我们只需证明 G 中有左幺元，且每个元素都有其（左幺元意义下）的左逆即可. 而由于左逆的定义依赖于左幺元的存在性，所以我们势必要先构造出一个左幺元. 一旦左幺元存在（不妨记为 e），则由关于 x 的方程 $xg = e$ 的解的存在性，即可“解出” g 的左逆.

注意到，我们由关于 x 的方程 $xg = g$，可以得到一个解，不妨记为 e（事实上我们知道这就是 G 的左幺元，所以采用了这个记号）. 接下来我们需要证明对任意 $h \in G$，有 $eh = h$. 为了让 e 参与运算，我们势必要利用条件构造 g 和 h 之间的关系式，请读者想一想，应该构造什么样的关系式呢？想清楚这一点后，此题即可迎刃而解.

证明 根据上题，我们只须证明 G 中有左幺元，且每个元素的都有自己的左逆.

任取 $g \in G$，则由题设，关于 x 的方程 $xg = g$ 的解存在，记解为 $x = e$. 下证：e 是 G 的左幺元，即对任意的 $h \in G$，有 $eh = h$.

由题设，关于 y 的方程 $h = gy$ 有解存在，不妨将解仍记为 y，即有 $h = gy$. 此时我们有：

$$eh = e(gy) = (eg)y = gy = h$$

然后，对任意的 $g \in G$，关于 x 的方程 $xg = e$ 总是有解的，所以每个元素都有（左幺元意义下的）左逆存在.

综上，半群 G 是一个群.

✍ **练习 1.52** 设 G 是一个有限半群，且在 G 内消去律成立. 证明 G 是群.

注 分析：初看此题，笔者是不知道该如何下手的，因为所给条件看起来无法联系到一起，消去律怎么用呢？半群有限这个条件又怎么用呢？

好吧，我们先来做一点简单的事情，不妨设半群为 $G = \{g_1, \cdots, g_n\}$. 为了能用上消去律，我们得构造乘积和等式，于是随便找一个元素 $g \in G$ 和半群里的每个元素都左乘一下好了，此时我们得到了集合 $A = \{gg_1, \cdots, gg_n\}$. 这时候我们发现，因为消去律的存在，$A$ 中的元素两两不同，因为若有 $gg_1 = gg_2$，则必要 $g_1 = g_2$，矛盾！又因为半群保证了运算的封闭性，所以任意 $gg_i \in G$，即 $A \subset G$，又 $|A| = n = |G|$，所以只能有 $A = G$.

此时我们想到了上一题的结论. 任取 G 的元素 g, h，存不存在 $x \in G$，使得 $xg = h$ 呢？答案是肯定的，上一段的讨论已经说明了这一点，我们不妨再论述一下：考虑集合 $Gg := \{g_1g, \cdots, g_ng\}$（记号 Gg 我们以后会经常用到），因为它等于 G，所以 $h \in Gg$，即存在一个 x_i，使得 $h = x_ig$. 类似地，也存在 $y \in G$，使得 $gy = h$. 所以有限半群 G 是群.

证明 半群 G 有限，所以不妨记 $G = \{g_1, \cdots, g_n\}$（注意到其中的元素两两不同）. 对任意的 $g, h \in G$，下证：关于 x 的方程 $xg = h$ 在 G 中有解.（同理可证关于 y 的方程 $gy = h$ 在 G 中有解，从而由上题结论可知，G 是群）

令集合 $Gg := \{g_1g, \cdots, g_ng\}$，若其中存在两个相等的元素 $g_ig = g_jg$，则由消去律可得 $g_i = g_j$，矛盾！所以 $|Gg| = n$. 由因为 G 是半群，所以其上的运算满足封闭性，即对任意的 $g_ig \in Gg$，有 $g_ig \in G$，于是 $Gg \subset G$. 而 $|G| = n = |Gg|$，所以必有 $G = Gg$. 从而，对于 $h \in G = Gg$，存在 $g_i \in G$，使得 $h = g_ig$. 命题得证.

1.4 拓展：群的例子

这一小节在 Maki 的讲义中是没有的，内容也散见于讲义的各个部分. 笔者认为，如果读者想要处理各式各样的抽象代数的练习，一些常见的、简洁的群的例子是必须提前熟知的. 本节主要呈现了几种典型的群结构. 我们通过各种练习展示了这些典型群的一些特征，这些群在我们今后的学习中也会经常碰到，希望大家熟练掌握.

阅读提示：本节并不想过于深入的分析各个群的来源以及性质，主要是提供一些相对抽象的群的例子，便于大家练习与应用. 因此读者此处无需纠结群的来源背景，而是将注意力放在群的生成元和元素的运算关系上.

1.4.1 知识要点

（一）“生成元 + 关系”表达法

1. G 由子集 S 生成：G 的子集 S 满足，每个 G 的元素，都可以写为 S 的元素和其逆的有限积.（记作：$G=\langle S\rangle$，S 中的元素称为 G 的生成元）
2. G 中的关系：G 的生成元满足的方程.
3. “生成元 + 关系”表达法：若 S 为生成元集，$R_1,R_2,\cdots,R_m$ 为关系，则 G 可以表达为：

$$G=\langle S\mid R_1,R_2,\cdots,R_m\rangle$$

（二）一些经典的群

1. 生成元为单一元素的群，即 $G=\langle g\rangle$.
2. 模 n 同余类加群：$\mathbb{Z}_n=\{\bar{0},\bar{1},\cdots,\overline{n-1}\}$，连同加法构成群.（其中 n 为不小于 2 的正整数）
3. $2n$ 阶二面体群：

$$D_{2n}=\left\langle r,s\mid r^n=s^2=1,\ rs=sr^{-1}\right\rangle$$

4. Klein 四元群：$K_4=\langle a,b\mid a^2=b^2=(ab)^2=1\rangle$.（或记为 V）
5. 四元数群：

$$Q_8=\{1,-1,i,-i,j,-j,k,-k\}$$

运算法则为：

$$\begin{gathered}\forall a\in Q_8,1\cdot a=a\cdot 1=a\\(-1)^2=1;\forall a\in Q_8,(-1)a=a(-1)=-a\\i^2=j^2=k^2=-1\\ij=k,ji=-k\\jk=i,kj=-i\\ki=j,ik=-j\end{gathered}$$

1.4.2 典型例题

（一）典型群之间的同态

现在，我们了解了很多群的结构，我们自然就可以利用同态来进一步研究他们. 更细致的研究，我们将在子群之后再做展开.

例题 1.9 证明：D_8 和 Q_8 不同构.

注 我们在上一小节“数集的结构关系”部分，曾经展示过证明两个群不同构的一些思路. 本题我们继续做类似的尝试.

证明 我们考虑两个群中阶数为 4 的元素个数.（如果两个群同构，那么由于对应元素的阶相同，从而两个群中同阶元素的个数必然相同）

在 D_8 中，有两个元素：r, r^3；

在 Q_8 中，有六个元素：$i, -i, j, -j, k, -k$.

从而 D_8 和 Q_8 不同构.

1.4.3 习题

（一）二面体群

✍ **练习 1.53** 写出以下各群的元素，并分别计算这些元素的阶.

1. D_6
2. D_8
3. D_{10}

注 二面体群的元素形式较为简单，我们一般习惯表达为 $s^k r^i$, $k \in \{0,1\}$, $i \in \{0,1,\cdots,n-1\}$ 的形式.

读者通过此问，对二面体群的元素特性有了直观的认知，这为我们接下来抽象的考察元素特性是有帮助的.

解 以 D_8 为例，剩下两群由读者完成.

元素：$D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$.

对应的阶数：$\{1,4,2,4,2,2,2,2\}$.

✍ **练习 1.54** x 是 D_{2n} 中不是 r 的幂的元素. 证明：

1. $rx = xr^{-1}$；
2. $|x| = 2$.

注 x 若不是 r 的幂，则只能为 sr^i, $i \in \{0,1,\cdots,n-1\}$. 余下的证明就是很自然的了.

证明 由题设，$x = sr^i$，其中 $i \in \{0,1,\cdots,n-1\}$.

1. $rx = rsr^i = sr^{-1}r^i = sr^i r^{-1} = xr^{-1}$.
2. 一方面，$x \neq 1$. 另一方面，注意到：$r^i s = r^{i-1}sr^{-1} = r^{i-2}sr^{-2} = \cdots = sr^{-i}$. 于是 $x^2 = sr^i sr^i = ssr^{-i}r^i = 1$. 从而 $|x| = 2$.

✍ **练习 1.55** 证明：D_{2n} 可由 s, sr 生成.

证明 只需证明 s, sr 可生成 D_{2n} 的生成元 r, s. 注意到 $r = s(sr)$，于是命题得证.

✍ **练习 1.56** 设 $n = 2k$ 是不小于 4 的偶数，考察群 D_{2n}，证明：

1. $z = r^k$ 是 2 阶元素；
2. z 与 D_{2n} 中的任意元素都交换；
3. 除幺元外，z 是 D_{2n} 中唯一与任意元素都交换的元素.

证明

1. 由 r 是 $n = 2k$ 阶元素可得 $z = r^k$ 是 2 阶元素.
2. D_{2n} 中的元素可分为两类：r^i, sr^i，这里 $0 \leq i \leq n-1$. r^i 显然与 r^k 可交换；并且
$$r^k(sr^i) = (r^k s)r^i = (sr^{-k})r^i = (sr^k)r^i = (sr^i)r^k$$
所以 r^k 与 D_{2n} 中任意元素可交换.
3. 考虑 D_{2n} 中元素与 r 和 s 的交换性：
$$r^i s = sr^{-i}, \quad sr^i = sr^i$$
$$(sr^i)r = sr^{i+1}, \quad r(sr^i) = sr^{i-1}$$
那么 r^i 型元素与 s 都可交换当且仅当 $sr^{-i} = sr^i$，即 $i = 0$ 或 $i = k$；sr^i 型元素与 r 不可交换. 结合第二小问结论得知 D_{2n} 中与任意元素都交换的元素只有幺元和 z.

✍ **练习 1.57** 设 n 是不小于 3 的奇数，考察群 D_{2n}，证明：幺元是 D_{2n} 中唯一与任意元素都交换的元素.

证明 考虑 D_{2n} 中元素与 r 和 s 的交换性：

$$r^i s = sr^{-i}, \quad sr^i = sr^i$$
$$(sr^i)r = sr^{i+1}, \quad r(sr^i) = sr^{i-1}$$

那么 r^i 型元素与 s 都可交换当且仅当 $sr^{-i} = sr^i$，即 $i = 0$；sr^i 型元素与 r 不可交换. 所以 D_{2n} 中与任意元素都交换的元素只有幺元.

✍ **练习 1.58** 证明：$D_{2n} = \langle a, b |\, a^2 = b^2 = (ab)^n = 1 \rangle$

提示 取 $a = s, b = sr$ 即可.

（二）四元数群

✍ **练习 1.59** 试用“生成元 + 关系”表达法表达 Q_8.

解 $Q_8 = \langle i, j \mid i^2 = j^2, i^4 = 1, ij = -ji \rangle$

（三）典型群之间的同态

✍ **练习 1.60** 若 A, B 是群，证明：$A \times B \simeq B \times A$.

提示 考虑 : $(a, b) \mapsto (b, a)$.

✍ **练习 1.61** 若 A, B, C 是群，证明：$(A \times B) \times C \simeq A \times (B \times C)$.

提示 考虑 : $((a, b), c) \mapsto (a, (b, c))$.

✍ **练习 1.62** 证明：$K_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

提示 考虑 $a \mapsto (1, 0); b \mapsto (0, 1)$.

1.5 子群与陪集

1.5.1 课前思考

1. 下列说法正确的有（　　）：
   A. 两个子群的乘积是子群；
   B. 两个子群的交是子群；
   C. 两个子群的并不是子群；
   D. 任意子群的交是子群；
   E. 任意子群的并是子群；
2. 设 H 是群 G 的 5 阶子群，且 G 中 H 不同的左陪集为 H, g_1H, g_2H，则 G 的阶为____. 写出 G 中 H 的三个不同的右陪集____.

解

1. BD.
2. G 的阶为 15. 因为 $|G| = |H|[G : H] = 5 \times 3 = 15$.
   不同的右陪集可以是 H, Hg_1, Hg_2. 由题设，$g_1, g_2 \notin H$，且 $g_1^{-1}g_2 \notin H$. 所以 H 不等于 Hg_1, Hg_2，且 Hg_1 不等于 Hg_2，这就得到了三个不同的右陪集.

1.5.2 知识要点

（一）子群的运算

1. 元素与集合的运算：对于群 G 的子集 A, B，元素 g, h，定义：
   (a). $gB = \{gb : b \in B\}$；
   (b). $Ah = \{ah : a \in A\}$.
   (c). $AB = \{ab : a \in A, b \in B\}$.
2. （子群的乘积）：H, K 为 G 的子群，则 $HK < G$ 当且仅当 $HK = KH$.

（二）阶

1. 元素 $g \in G$ 的阶：最小的正整数 n，使得 $g^n = 1$.（记作 $|g|$ 或 $o(g)$，本书采用第一种记法.）若这样的正整数不存在，则称 $|g| = +\infty$.
2. 群 G 的阶：集合 G 的元素个数.（记作 $|G|$.）若 G 为无穷集，则称 $|G| = +\infty$.

（三）陪集

1. 陪集：设 $H < G$，$g \in G$，定义
   (a). 由 g 引出的 H 的左陪集：gH；
   (b). 由 g 引出的 H 的右陪集：Hg.
2. （陪集的性质）：设 $H < G$，$g_1, g_2 \in G$：
   (a). （相等的陪集）：$Hg_1 = Hg_2 \iff g_1 g_2^{-1} \in H$；
   (b). （等价关系）：G 上有等价关系：
   $$g_1 \sim g_2 \iff g_1 g_2^{-1} \in H$$
   从而对于 g_1，其所在的等价类为右陪集 Hg_1；
   (c). （G 的分拆）：H 的右陪集全体，构成了 G 的分拆；（即两个右陪集 Hg_1, Hg_2，要么 $Hg_1 = Hg_2$，要么 $Hg_1 \cap Hg_2 = \varnothing$）
   (d). （陪集的阶）：$|Hg_1| = |H|$.
   【注：以上结论均可自然推广到左陪集上，在此不赘述.】
3. 子群 H 的指数：群 G 中，子群 H 的右陪集（或左陪集）的个数.（记为 $[G : H]$）

（四）Lagrange 定理及其应用

1. （Lagrange 定理）：若 G 为有限群，且 $H < G$，则 $|G| = [G : H] \cdot |H|$.
2. （元素的阶与群的阶）：对有限群 G 的任意元素 g，$|g|$ 总是整除 $|G|$.
   特别的，$g^{|G|} = 1$.【对这一定理的进一步说明，我们留到“循环群”一节讲解.】
3. （子群乘积的阶）：设 G 为群，A, B 为 G 的有限子群，则 $|AB| = \dfrac{|A| \cdot |B|}{|A \cap B|}$.
4. （嵌套的子群）：设 G 为群，$A < B < G$，且 $[G : A]$ 是有限的，则 $[G : A] = [G : B][B : A]$.
5. （子群的交）：设 G 为群，A, B 为 G 的有限子群，且 $[G : A] = m$，$[G : B] = n$，则 $\operatorname{lcm}(m, n) \leqslant [G : A \cap B] \leqslant mn$.
   特别的，若 $\gcd(m, n) = 1$，则 $[G : A \cap B] = mn$，且 $AB = G$.

（五）Lagrange 定理的“部分逆”定理 *

1. （Cauchy 定理 *）：G 是有限群，p 是一个素数且整除 $|G|$，则 G 有一个 p 阶元素.【我们会在习题里给出一个证明】

2. (Sylow 定理 *)：G 是有限群，且阶为 $p^\alpha m$, 其中 p 是素数，p 不整除 m, 于是 G 有阶为 p^α 的子群.【我们将在以后学习该定理的一些使用】

1.5.3 知识要点解读

（一）子群的证明

一般来说，使用等价定义证明子群，会比使用子群的定义简洁很多.

问题 1.9 （子群的乘积）：H, K 为 G 的子群，则 $HK < G$ 当且仅当 $HK = KH$.

证明 一方面，设 $HK = KH$，显然 $1 = 1 \cdot 1 \in HK$，则需证：对任意的 $a, b \in HK$，$ab^{-1} \in HK$.

因为 $a, b \in HK$，则存在 $h_1, h_2 \in H$，$k_1, k_2 \in K$，使得 $a = h_1k_1, b = h_2k_2$. 于是 $ab^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. 因为 $k_1, k_2 \in K$，于是存在 $k = k_1k_2^{-1} \in K$. 又因为 $HK = KH$，于是存在 $h' \in H, k' \in K$，使得 $kh_2^{-1} = h'k'$，从而：

$$\begin{aligned} ab^{-1} &= h_1k_1k_2^{-1}h_2^{-1} \\ &= h_1kh_2^{-1} \\ &= h_1h'k' \\ &= (h_1h')k' \in HK \end{aligned}$$

另一方面，设 $HK < G$. 因为 $H < HK$，$K < HK$，则 $KH \subset HK$. 我们需证：$HK \subset KH$.

对任意的 $h \in H, k \in K$, 因为 HK 为群, 于是 $(hk)^{-1} \in HK$, 从而存在 $h_1 \in H, k_1 \in K$, 使得 $(hk)^{-1} = h_1k_1$. 进一步变形可得：

$$\begin{aligned} hk &= (h_1k_1)^{-1} \\ &= k_1^{-1}h_1^{-1} \in KH \end{aligned}$$

这样就证明了 $HK \subset KH$.

笔记 这一结论的证明，对于初学者来说是较难想到的. 在前一部分的证明中，我们反复使用条件 $HK = KH$，当然实际上这一条件也只有“子集乘积的定义”可以使用，所以它考验的是读者敢不敢去用. 而后一部分的证明，我们需要想到穿脱原理.

练习 1.63 （子群的并）：

1. 设 $H, K < G$. 证明：$H \cup K < G$，当且仅当 $H \subset K$ 或 $K \subset H$.

* 设 $H_1 \subset H_2 \subset \cdots$ 是 G 的子群的升链，证明：$\cup_{i=1}^{\infty} H_i < G$.

（二）元素、集合混合运算

我们将元素的运算，自然地推广到了集合上. 于是我们在遇到涉及集合的运算时，我们就有了两个视角：最基本、也是最通用的，将集合拆开，直接考虑元素的运算；另一种方式，我们可以利用已知的一些结论，将集合整体考虑. 两种方式各有利弊.

笔者想在此说一些题外话. 实际上单看集合运算的定义，它就是一个记号而已，是可有可无的. 如果我们就是不想用这个记号，实际上也是可以的. 但是有了这个记号，却对后续群论的构建，有着不可或缺的作用，且为我们多提供了一种处理问题的思路. 因此，理论的简洁性、精炼性，是数学研究中非常重要的.

问题 1.10 （相等的陪集）：设 $H < G$，$g_1, g_2 \in G$. $Hg_1 = Hg_2 \iff g_1g_2^{-1} \in H$.【简记为 $(C1)$】

注 我们从这一命题开始，逐步构建我们未来常用的一些集合运算的结论. 当然此处我们只能老老实实地回归定义.

证明 “$\to$”：若 $Hg_1 = Hg_2$，则对于任意的 $h_1 \in H$，存在 $h_2 \in H$，使得 $h_1g_1 = h_2g_2$，于是 $g_1g_2^{-1} = h_1^{-1}h_2 \in H$.

“←”：一方面，若 $g_1g_2^{-1}\in H$，则对任意的 $h_1\in H$，有 $h_1(g_1g_2^{-1})\in H$. 于是存在 $h_2\in H$，使得 $h_1(g_1g_2^{-1})=h_2$，即 $h_1g_1=h_2g_2$，从而 $Hg_1\subset Hg_2$. 另一方面，若 $g_1g_2^{-1}\in H$，则 $g_2g_1^{-1}=(g_1g_2^{-1})^{-1}\in H$，于是与前面的证明过程类似地，有 $Hg_2\subset Hg_1$，从而 $Hg_1=Hg_2$.

笔记 我们在证明过程中，反复使用的是群对运算的封闭性，以及逆的存在性.

另一方面，这一结论未来的使用频率极高.

问题 1.11 （等价关系）：设 $H<G$，$g_1,g_2\in G$.

1. G 上有等价关系：
$$g_1\sim g_2\iff g_1g_2^{-1}\in H$$
2. 对于 g_1，其所在的等价类为右陪集 Hg_1.

注 我们先简单回顾一下，一个等价关系需要满足三个条件：自反性、对称性、传递性. 同时，一个集合上地等价关系对应着一个对集合的划分，他们将集合分割成无交的若干等价类.

证明

1. 自反性：对任意 $g\in G$，因为 $gg^{-1}=1\in H$，所以 $g\sim g$.
对称性：对任意的 $g,h\in G$，若 $g\sim h$，则 $gh^{-1}\in H$. 于是 $hg^{-1}=(gh^{-1})^{-1}\in H$，即 $h\sim g$.
传递性：对任意的 $g,h,k\in G$，若 $g\sim h$，$h\sim k$，则 $gh^{-1}\in H$ 且 $hk^{-1}\in H$，从而 $gk^{-1}=(gh^{-1})(hk^{-1})\in H$，即 $g\sim k$.
综上，我们定义的 $\sim$ 确为等价关系.
2. 对于确定的 g_1，我们有：
$$\begin{aligned}g_2\sim g_1&\iff g_2g_1^{-1}\in H\\&\iff (g_2g_1^{-1})g_1\in Hg_1\\&\iff g_2\in Hg_1\end{aligned}$$
从而 g_1 的等价类确为 Hg_1.

笔记 在第二小问地证明过程中，我们实际使用了一个小结论：若 $H<G$，则 $g'\in H\iff g'g\in Hg$，我们将在习题中给出一个更一般地命题.

练习 1.64 证明：若 $A\subset G$，$g,h\in G$，则 $gh\in gA\iff h\in A\iff hg\in Ag$.【简记为 (C_2)】

练习 1.65 证明：若 $A,B\subset G$，$g,h\in G$，则 $hA\subset hB\iff A\subset B\iff Ag\subset Bg$.【简记为 (C_3)】

练习 1.66 证明：若 $A,B\subset G$，$g,h\in G$，则 $hA=hB\iff A=B\iff Ag=Bg$.【简记为 (C_4)】

（三）群的陪集分解

陪集分解为我们提供了一个认识群结构的视角：从子群的角度理解群结构. 利用子群，我们将群分割成了大小相同的若干小版块，其中一个小板块包含幺元，即为子群本身.

问题 1.12 （Lagrange 定理）：若 G 为有限群，且 $H<G$，则 $|G|=[G:H]\cdot|H|$.

解 设 H 的全部右陪集为 $\{Hg_1,\cdots,Hg_n\}$，其中由指数的定义可得：$n=[G:H]$. 对 G 做 H 的右陪集分解：（我们用 $\sqcup$ 表示无交并，下同）
$$G=\bigsqcup_{i=1}^{n}Hg_i$$
因为上式是无交并，所以对等式两边的元素个数计数：
$$|G|=\sum_{i=1}^{n}|Hg_i|$$

注意到每个 $|Hg_i| = |H|$，于是：

$$\begin{aligned} |G| &= \sum_{i=1}^{n} |Hg_i| \\ &= \sum_{i=1}^{n} |H| \\ &= n|H| \\ &= [G:H] \cdot |H| \end{aligned}$$

下面将要展示的，是笔者非常喜欢的定理证明之一，它将陪集分解的精华完全呈现了出来. 请读者朋友跟随笔者的思路，一起来赏析.

问题 1.13 （子群乘积的阶）：设 G 为有限群，$A, B < G$，则 $|AB| = \dfrac{|A| \cdot |B|}{|A \cap B|}$.

注 该命题的证明，完全可以在讲完 Lagrange 定理之后，作为习题留给学生.

我们从解体的角度来思考，看到此题，我们能想些什么？先看条件，已知两个子群，我们目前所学的知识中，子群的使用只有两个方向，一个是把子群当一个群来用，另一个就是利用子群构造群的陪集. 而从结论来看，需要我们计数，因此利用子群构造陪集，应该是我们的首选思路.

然而，思考至此，我们仍然会感到有一些头疼，题设没有给任何群的阶的性质，我们如何计数呢？注意到结论的形式，是若干集合的阶的关系，而不必求出（也没法求出）阶的绝对值. 进一步，我们回想 Lagrange 定理的证明过程，我们将大集合拆成了若干不相交的小集合（即划分），然后两边计数，这样的思路应当是具有借鉴意义的，我们不妨在这里再试一试.

于是，下一个需要考虑的问题是，我们对哪个集合做划分呢？再看一遍需证结论：$|AB| = \dfrac{|A| \cdot |B|}{|A \cap B|}$，你有没有一种冲动，想把该式改写成这样的形式：$|AB|/|A| = |B|/|A \cap B|$？（或对称的 $|AB|/|B| = |A|/|A \cap B|$）这样做的主要理由在等式右侧，我们已经知道 $A \cap B < B$，于是右侧就等于 $[B : A \cap B]$，也就暗示了我们一个陪集分解：对 B 做 $A \cap B$ 的陪集分解，等式右侧即为 $A \cap B$ 的右陪集的个数.

那么，等式左侧呢？AB 一般来说不是群，但有趣的是，我们仍然可以对 AB 做类似陪集分解的操作：对所有的 $b \in B$，Ab 的并集即为 AB，去掉所有 Ab 中重复的集合，剩下的即为 AB 的无交并，也就是对 AB 的划分了【请读者先思考，为什么可以这么做，我们将在解答中给出原因】. 分析至此，解题思路已经呼之欲出了，我们来看解答.

证明 由定义，我们有 $AB = \cup_{b \in B} Ab$. 因为每个 Ab 都是 G 中 A 的右陪集，因此对 $b, b' \in B$，Ab, Ab' 要么相同，要么不相交. 又因为 B 是有限的，因此我们总可以去掉所有 Ab 中重复的集合，若记剩下的集合为集族 $\mathcal{A} := \{Ab_1, \cdots, Ab_n\}$，则 AB 可以表达为一个无交并：

$$AB = \bigsqcup_{i=1}^{n} Ab_i$$

对等式两边计数，就有 $|AB| = n|A|$. （因为每个 $|Ab_i| = |A|$）

另一方面，设 B 中 $A \cap B$ 的右陪集全体为集族 $\mathcal{B} := \{(A \cap B)b_1, \cdots, (A \cap B)b_m\}$，从而由 Lagrange 定理：$|B| = m|A \cap B|$. 从而我们只需证明：$m = n$.

定义映射 $\varphi : \mathcal{A} \to \mathcal{B}$, $Ab \mapsto (A \cap B)b$. 于是我们只需证该映射为双射. 进一步，由单射的定义，我们只需证：对任意的 $b_1, b_2 \in B$，$Ab_1 = Ab_2$ 当且仅当 $(A \cap B)b_1 = (A \cap B)b_2$.

我们有

$$\begin{aligned} Ab_1 = Ab_2 &\iff b_1 b_2^{-1} \in A && (C1) \\ &\iff b_1 b_2^{-1} \in A \cap B && (b_1 b_2^{-1} \in B) \\ &\iff (A \cap B)b_1 = (A \cap B)b_2 && (C1) \end{aligned}$$

从而命题得证.

笔记 不知道读者至此有没有理解，为什么我们只需证：对任意的 $b_1, b_2 \in B$，$Ab_1 = Ab_2$ 当且仅当 $(A \cap B)b_1 =$

$(A\cap B)b_2$，就可以说明 φ 为双射了？

这是因为，φ 为双射，当且仅当 φ,φ^{-1} 均有定义且均为单射，而一个映射 $f:A\to B$ 为单射，当且仅当对于任意 $a,a'\in A$，若 $f(a)=f(a')$，则 $a=a'$. 从而，我们把上面的两个结论结合一下，就变成了：一个映射 $f:A\to B$ 为双射，当且仅当 f,f^{-1} 均有定义，且对于任意 $a,a'\in A$，有 $a=a'\iff f(a)=f(a')$.

回到我们的证明中，若 $\varphi:Ab\mapsto(A\cap B)b$，我们自然有 $\varphi^{-1}:(A\cap B)b\mapsto Ab$. 从而解答中的证明是合理的.

我们对 AB 的处理，启发我们深入理解“陪集分解”的本质：陪集分解是一种特殊的集合划分，只不过由于群和子群的特殊性（集合 + 封闭的运算），才使得这样的划分有特殊性质（Lagrange 定理）. 于是，只要集合是合适的，“陪集分解”完全可以利用在不是群的集合上（例如本题的 AB）.

本题还展示了命题 $(C1)$ 的巨大作用，读者要学会熟练使用它.

✍ **练习 1.67**（嵌套的子群）：设 G 为群，$H<K<G$，且 $[G:H]$ 是有限的，则 $[G:H]=[G:K][K:H]$.

证明 由陪集分解可得：（其中 I,J 为指标集）

$$\begin{aligned}G&=\bigsqcup_{i\in I}g_iK\\&=\bigsqcup_{i\in I}g_i(\bigsqcup_{j\in J}k_jH)\\&=\bigsqcup_{i\in I,j\in J}g_ik_jH\end{aligned}$$

其中欲使最后一个等号成立，我们需要证明：若 $g_i\neq g_{i'},i,i'\in I$，或 $k_j\neq k_{j'},j,j'\in J$，则 $g_ik_jH\neq g_{i'}k_{j'}H$. 我们转而证明其逆否命题：若 $g_ik_jH=g_{i'}k_{j'}H$，则 $g_i=g_{i'}$ 且 $k_j=k_{j'}$.

因为 $g_ik_jH=g_{i'}k_{j'}H$，所以 $k_i^{-1}g_i^{-1}g_{i'}k'_{j'}\in H$. 因为 $H<K$，所以 $k_i^{-1}g_i^{-1}g_{i'}k'_{j'}\in K$，即 $g_i^{-1}g_{i'}\in K$，从而 $g_iK=g_{i'}K$. 又因为我们选取的指标集 I，使得不同的 K 的左陪集对应于不同的 g_i，相同的 K 的左陪集对应于相同的 $g_{i'}$，所以 $g_i=g_{i'}$.

另一方面，因为 $g_i=g_{i'}$，所以 $k_jH=k_{j'}H$，与前面的讨论类似地，此时必有 $k_j=k_{j'}$，原命题得证.

从而 G 被分割成若干个 H 的左陪集，左陪集个数为 $|I||J|$，于是 $|G:H|=|I||J|=|G:K||K:H|$.

笔记 请读者注意，在对 G 做陪集分解时，$\sqcup_{i\in I}g_i(\sqcup_{j\in J}k_jH)=\sqcup_{i\in I,j\in J}g_ik_jH$ 并不是显然成立的，这里面包含隐藏的信息，即当 i,j 的指标组合不相等时，g_ik_jH 表示不同的 H 的左陪集. 于是我们在解答的后半部分补充了一个证明.

另一方面，我们取指标集 I,J 的作用，就是使得陪集与代表元构成一一对应关系，正是由于这种关系，才使得我们后面的证明能够进行下去.

✍ **练习 1.68****（子群的交）：设 G 为群，A,B 为 G 的有限子群，且 $[G:A]=m$，$[G:B]=n$，则 $\operatorname{lcm}(m,n)\leqslant[G:A\cap B]\leqslant mn$.

特别的，若 $\gcd(m,n)=1$，则 $[G:A\cap B]=mn$，且 $AB=G$.

证明

1. 先证明：$[A:A\cap B]\leqslant[G:B]$.（从而 $[G:A\cap B]=[G:A][A:A\cap B]\leqslant[G:A][G:B]=mn$.）
   记 A 中 $A\cap B$ 的右陪集的集合为 $\mathcal{A}$，G 对 B 的右陪集的集合为 $\mathcal{B}$. 给定一个映射 $\mathcal{A}\to\mathcal{B}:(A\cap B)a\mapsto Ba$. 于是只需证明该映射为单射即可.
   对任意 $a,a'\in A$，我们有：
   $$\begin{aligned}(A\cap B)a\neq(A\cap B)a'&\to A\cap Ba\neq A\cap Ba'\\A\cap Ba\neq A\cap Ba'&\to Ba\neq Ba'\end{aligned}\qquad(C4)$$
   从而 $(A\cap B)a\neq(A\cap B)a'\to Ba\neq Ba'$ 该映射确为单射.
   再证明：$[G:A]$ 整除 $[G:A\cap B]$.（类似地，$[G:B]$ 整除 $[G:A\cap B]$）
   因为 $[G:A\cap B]=[G:A][A:A\cap B]$，从而 $[G:A]$ 整除 $[G:A\cap B]$. 因此 $[G:A\cap B]$ 被 $\operatorname{lcm}(m,n)$ 整除，从而 $\operatorname{lcm}(m,n)\leqslant[G:A\cap B]$.
2. 若 $\gcd(m,n)=1$，则 $\operatorname{lcm}(m,n)=mn$，从而结合第一小问可得 $[G:A\cap B]=mn$.

于是，因为 $[G:A\cap B]=[G:A][G:B]$，所以 $1/|A\cap B|=|G|/(|A|\cdot|B|)$，即 $|G|=|A|\cdot|B|/|A\cap B|=|AB|$，结合 $AB\subset G$ 可得：$AB=G$.

笔记 命题 $(C4)$ 是指：$(A\cap B)c=Ac\cap Bc$，且 $c(A\cap B)=cA\cap cB$，其证明留给读者，读者可以参考“典型例题”-“元素、集合混合运算”一节展示的方法.

另一方面，为什么 $A\cap Ba\neq A\cap Ba'\to Ba\neq Ba'$？我们不妨考虑更一般地情况：$A\cap B\neq A\cap C\to B\neq C$. 我们考虑其逆否命题：$B=C\to A\cap B=A\cap C$，而这是显然的.（这里终于可以用显然这个词，而不至于被读者诟病笔者“偷懒”了）

1.5.4 典型例题

（一）元素的阶

元素的阶的定义中，最重要的特性是“最小的正整数”，我们常常利用这一点构造矛盾，或者建立不等关系. 另外，这一部分也会涉及简单的初等数论知识，建议读者了解一点初等数论中关于“整除性”和“同余”的知识，他们在群论中将会被多次使用.

例题 1.10 证明：设 G 为群，$g\in G$，整数 $m\neq 0$. 证明：g 的阶整除 m，当且仅当 $g^m=1$.

注 读者千万仔细，由 $g^m=1$ 不能随意地得到 $|g|=m$.

证明 不妨记 $|g|=n$.

一方面，若 $n|m$，则存在整数 k，使得 $kn=m$，于是 $g^m=g^{kn}=(g^n)^k=1^k=1$.

另一方面，设 $g^m=1$ $(m\neq 0)$. 由带余除法，我们有：$m=kn+r$，其中 $r\in[0,n-1]$. 于是 $1=g^m=g^{kn+r}=g^rg^{kn}=g^r$. 由于 r 是小于 n 的非负整数，若 $r\neq 0$，则 $n=|g|\leqslant r$，矛盾！从而只能有 $r=0$，于是 $m=kn$，即 $n|m$.

例题 1.11 设 G 为群，$x,g\in G$. 试证明：

1. $|x|=|g^{-1}xg|$；
2. 对任意的 $a,b\in G$，有 $|ab|=|ba|$.

证明

1. 记 $|x|=n$.

   一方面，

   $$\begin{aligned}(g^{-1}xg)^n&=(g^{-1}xg)(g^{-1}xg)\cdots(g^{-1}xg)\\&=g^{-1}x(gg^{-1})x\cdots xg\\&=g^{-1}x^ng=1.\end{aligned}$$

   从而 $|g^{-1}xg|\leqslant n$.

   另一方面，对任意小于 n 的正整数 m，若 $(g^{-1}xg)^m=1$，则有 $1=(g^{-1}xg)^m=g^{-1}x^mg$. 于是 $g1g^{-1}=gg^{-1}x^mgg^{-1}$，即 $x^m=1$. 从而 $|x|\leqslant m<n$，与 $|x|=n$ 矛盾！从而 $|g^{-1}xg|\geqslant n$. 综上，$|g^{-1}xg|=n=|x|$.
2. 利用第一小问的结论，取 $x=ab,g=a$，则 $|ab|=|a^{-1}aba|=|ba|$.

练习 1.69 设 x 是群 G 的元素. 证明：

1. x 与 x^{-1} 有同样的阶；
2. $x^2=1$ 当且仅当 $|x|=1,2$；
3. 若 $|x|=n<\infty$. 且存在正整数 s,t，满足 $n=st$，则 $|x^s|=t$.

1.5.4.1 元素、集合混合运算

我们现在已经有了 $(C1)-(C4)$ 四条结论结论，这些结论将极大地简化我们的证明过程. 试看下例.

例题 1.12 设 A,B 是群 G 的子群，若存在 $g,h\in G$，使得 $Ag=Bh$，试证明：$A=B$.

注 初看此题，我们可能会感觉有些懵，找不到方向. 我们来分析一下，一共有以下几种使用条件等式 $Ag = Bh$ 的方法：

1. 利用 $(C3)$，将元素 g, h 凑到一起：$A = B(hg^{-1})$，或 $A(gh^{-1}) = B$；
2. 对等式的一半“元素化”处理：对任意的 $a \in A$，有 $ag \in Bh$；或对任意的 $b \in B$，有 $bh \in Ag$；
3. 对等式两边都“元素化”处理：对任意的 $a \in A$，存在 $b \in B$，有 $ag = bh$；或对任意的 $b \in B$，存在 $a \in A$，有 $ag = bh$.

我们分别给出一个对应的解法.

证明 [1] 由 $Ag = Bh$ 可得，$A = B(gh^{-1})$. 因为 $1 \in B$，所以 $gh^{-1} \in A$，于是 $Ag = Ah$，即 $Ah = Bh$，于是 $A = B$.

证明 [2] 由 $Ag = Bh$ 可得，对任意的 $b \in B$，有 $bh \in Ag$. 因为 $1 \in B$，所以可取 $b = 1$，从而 $h \in Ag$，从而 $hg^{-1} \in A$. 由此可得 $Ag = Ah$，即 $Ah = Bh$，于是 $A = B$.

证明 [3] 由 $Ag = Bh$ 可得，或对任意的 $b \in B$，存在 $a \in A$，有 $ag = bh$. 于是对 $1 \in B$，存在 $a \in A$，有 $ag = h$，于是 $hg^{-1} = a \in A$. 由此可得 $Ag = Ah$，即 $Ah = Bh$，于是 $A = B$.

笔记 我们看到，本题的关键在于，关注子群中的特殊元素：幺元. 因此三种思路最终会回到同一条路上. 当然，思路 1 相对来说更清晰一些，这也是尽可能“整体处理集合”的方法的优势.

练习 1.70 设 A, B, C 是群 G 的子集，$g \in G$，证明：

1. $g(A \cap B) = gA \cap gB$（同样的有 $(A \cap B)g = Ag \cap Bg$，记为 $C5$）；
2. $g(A \cup B) = gA \cup gB$（同样的有 $(A \cup B)g = Ag \cup Bg$）；
3. $C(A \cap B) \subset CA \cap CB$，并给出一个等号不成立的例子（同样的有 $(A \cap B)C \subset AC \cap BC$）；
4. $C(A \cup B) = CA \cup CB$（同样的有 $(A \cup B)C = AC \cup BC$）

注 提示：第三小问的例子，可以考虑 D_8 中，$A = \{s, sr\}$，$B = \{1, r^2\}$，$C = \{s, r\}$.

练习 1.71（吸收律）：设 A, B, C 是群 G 的子群，且 $A < C$，证明：$C(A \cap B) = C \cap CB$，$(A \cap B)C = C \cap BC$.

注 提示：本题可以看作是上题第三小问的特殊情况.

练习 1.72 设 A, B 是群 G 的子群，且 $G = AB$. 证明：若 $A < C$，则 $C = A(B \cap C)$.

注 提示：本题用吸收律去做是非常简单的. 读者也可以尝试不使用吸收律，直接证明.

练习 1.73 证明：群 G 中 H 的右陪集个数，与 G 中 H 的左陪集个数相同.

注 提示：考虑右陪集 Hg 和左陪集 $g^{-1}H$ 之间的对应关系.

1.5.4.2 Lagrange 定理的应用

Lagrange 定理的关键，在于联系了群和其子群的阶的关系：整除关系，结合数论的整除理论，我们能得到一些很有趣的结论.

例题 1.13 证明：若 H, K 是 G 的有限子群，且 H, K 的阶互素，则 $H \cap K = \{1\}$.

证明 因为 $H \cap K < H$，所以 $|H \cap K|$ 整除 $|H|$，同理 $|H \cap K|$ 整除 $|K|$，从而 $|H \cap K|$ 整除 $\gcd(|H|, |K|) = 1$，于是 $|H \cap K| = 1$，则 $H \cap K$ 只能为 $\{1\}$.

笔记 本例虽然简单，但是“整除性分析”是我们解决问题的重要手段，我们会在抽象代数的各个章节看到它的身影.

更多的应用，我们将在后续的学习中多次展示.

1.5.5 习题

练习 1.74 请找出 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 的加群以及 $\mathbb{Q}^+, \mathbb{Q}^\times, \mathbb{R}^+, \mathbb{R}^\times, \mathbb{C}^\times$ 中所有有限阶的元素，以及它们的阶.

证明 实际上，我们只要找到在这些群中方程 $x^m = e$ 的解即可. 同时注意到 $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ 以及 $\mathbb{Q}^+ < \mathbb{Q}^\times < \mathbb{R}^\times < \mathbb{C}^\times$ 的子群关系，我们只须考虑 $\mathbb{C}, \mathbb{C}^\times$.

注意到在加群中，我们要找到的是 $mx = x + \cdots + x = 0$ 的解. 在 $\mathbb{C}$ 中，唯一的可能性便是 $x = 0$，这就意味着唯一有有限阶的元素是单位元 0 自身.

在乘群中，我们要找到的是 $x^m = x \cdots x = 1$ 的解. 注意到在 $\mathbb{C}^\times$ 中，$z^m = 1$ 的解被称为 m 次单位根，对于每个 m 都有 m 个不同的解. 特别地，在 $\mathbb{Q}^\times, \mathbb{R}^\times$ 中，这样的单位根只有 ± 1 两个，其中 1 作为单位元，阶是 1，而 -1 的阶是 2，因为 $(-1)^2 = 1$. 而在 $\mathbb{Q}^+, \mathbb{R}^+$ 中，唯一的具有有限阶的元素只有单位元 1 了.

✍ **练习 1.75** 计算 Q_8 中各元素的阶.

解 1 阶元素：

$$1$$

2 阶元素：

$$-1$$

4 阶元素：

$$i, -i, j, -j, k, -k$$

✍ **练习 1.76** 设 x 是群 G 中的 $n \in \mathbb{Z}_+$ 阶元素. 证明：$1, x, \cdots, x^{n-1}$ 都是不同的，且 $|x| \leqslant |G|$.

✍ **练习 1.77** 设 x 是群 G 中的 $n \in \mathbb{Z}_+$ 阶元素. 试证明：

1. 若 n 是奇数，则对于任意 $i = 1, 2, \cdots, n-1$ 有 $x^i \neq x^{-i}$；
2. 若 $n = 2k$（k 为正整数），且整数 $i \in [1, n)$，于是 $x^i = x^{-i}$ 当且仅当 $i = k$.

✍ **练习 1.78** 设 x 是群 G 中的无穷阶元素，证明：元素 x^n, $n \in \mathbb{Z}$ 都是不同的.

✍ **练习 1.79*** 证明：若对所有的 $x \in G$，均有 $x^2 = 1$，则 G 是交换群.

注 提示：注意到 $(xy)^2 = xyxy = x^{-1}yxy^{-1} = 1$.

✍ **练习 1.80** 设 $\varphi : G \to H$ 是群同构，证明：$\forall x \in G, |\varphi(x)| = |x|$.

✍ **练习 1.81** 设 $f : G \to H$ 是群同态. 证明：若 $g \in G$ 的阶为 $n < \infty$，则 $|f(g)|$ 整除 $|g|$.

证明 因为 $|g| = n$，所以 $g^n = 1$，从而 $f(g^n) = f(1) = 1$，也就是 $(f(g))^n = 1$. 由“元素的阶”部分的例题可知，$|f(g)|$ 整除 $n = |g|$.

✍ **练习 1.82** 设 G 为群，$H \subset G$. 证明：

1. $H < G$，当且仅当 $HH^{-1} = H$（或 $H^{-1}H = H$）；
2. $HH^{-1} = H$，当且仅当 $HH^{-1} \subset H$；
3. 若 $H < G$，则 $HH = H$；
4. 当 $HH = H$ 时，是否有 $H < G$?

注 提示：第四小问，考虑 $(\mathbb{Z}, +)$ 的子集 $(\mathbb{N}, +)$.

1.5.6 拓展

1.5.6.1 阶

✍ **练习 1.83** 设 G 为偶数阶群，证明：存在 $x \in G$，使得 $|x| = 2$.

证明 注意到，$|x| = 2$ 的充要条件是 $x \neq e$ 且 $x^2 = e$. 我们还知道 $x^2 = e$ 当且仅当 $x^{-1} = x$. 进一步地，我们不难发现

$$x \mapsto x^{-1} \tag{1.1}$$

是个从 G 到 G 的双射，其逆映射就是这个映射本身. 因为对任意 $x \in G$，我们都有 $\left(x^{-1}\right)^{-1}$. 也就是说，如果 $x \mapsto y$，则 $y \mapsto x$.

因此，我们可以将 G 分成两组. 第一组是由映到自身的元素所组成的，第二组是由不映到自身的元素所组成的. 根据上面对于这个双射的讨论，我们知道第二组是成双成对出现的，因为 x 映到 y 等价于 y 映到 x，对第二组的元素来说我们有 $x \neq y$，因此自然是成双成对的.

由于 $n = |G|$ 是个偶数，第二组也是有偶数个元素. 因此第一组也有偶数个元素. 我们注意到 $e \mapsto e^{-1} = e$. 这告诉我们第一组至少还有个别的元素，即存在某个 $x \in G$，使得 $x \neq e$ 且 $x^{-1} = x$. 而这就等价于说 $|x| = 2$. 此即得证.

✍ **练习 1.84** 设 G 为有限群. 证明：群 G 中 $x^2 = e$ 的解的个数与 $|G|$ 有着一样的奇偶性.（也就是说，如果 $|G|$ 是偶数，则 $x^2 = e$ 在 G 中有偶数个解，反之，则有奇数个解.）

证明 注意到 $x^2 = e \iff x = x^{-1}$. 因此我们只须研究 $x \mapsto x^{-1}$ 的这个映射，称其为 ϕ. 注意到 ϕ 是个双射，而且 $\phi \circ \phi = id$，也就是说

$$y = x^{-1} \iff x = y^{-1} \tag{1.2}$$

这就告诉了我们，如果 $x \neq x^{-1}$，则 x 和 x^{-1} 是配对的.

因此，我们将 G 中所有元素分成两类，一类是使得 $x = x^{-1}$ 的元素，另一类是使得 $x^{-1} \neq x$ 的元素. 根据上面的讨论，第二类元素总是成双成对地出现，因此第二类元素的个数一定是个偶数. 又因为 $x = x^{-1} \iff x^2 = e$，所以 $x^2 = e$ 的解的个数与 $|G|$ 有着相同的奇偶性.

✍ **练习 1.85** 设 G 为有限群，$m \geqslant 3$. 证明：G 中阶为 m 的元素一定是偶数个.

证明 我们同样研究 $x \mapsto x^{-1}$ 的映射，这是个双射. 注意到 $|x| = \left|x^{-1}\right|$，所以 x 的阶是 m 当且仅当 x^{-1} 的阶是 m. 特别地，因为 $m \geqslant 3$，所以 $x \neq x^{-1}$. 同样利用一一配对，这就证明了 G 中阶为 m 的元素一定是偶数个.

✍ **练习 1.86** 设 A, B 是有限群 G 的两个非空子集，且 $|A| + |B| > |G|$，证明：$G = AB$.

证明 对任意的 $g \in G$，$|A^{-1}g| = |g^{-1}A| = |A|$，因为 $|A| + |B| > |G|$，则 $|A^{-1}g| + |B| > |G|$，所以 $A^{-1}g \cap B \neq \varnothing$. 从而，存在 $a \in A$，$b \in B$，使得 $a^{-1}g = b$，即 $g = ab$. 所以 $G = AB$.

✍ **练习 1.87** 设 S 是有限群 G 的一个子集，使得 $|S| > |G|/2$. 求证 $G = SS$，即每一个 G 中元素，都可以写成 S 中某两个元素的乘积.

证明 我们来计算一些集合的大小. 令 $x \in G$，要证明 $x \in SS$，我们只须证明 $xS^{-1} \cap S \neq \emptyset$，其中 $S^{-1} = \{s^{-1} : s \in S\}$.

我们注意到

$$\left|xS^{-1}\right| = \left|S^{-1}\right| = |S|$$

又因为 $|S| > |G|/2$，因此这两个集合必须有交集. 取 $a \in S \cap xS^{-1}$，$b \in S$，使得 $a = xb^{-1}$. 同时右乘 b，就得到了 $x = ab \in SS$. 这就证明了这个命题.

笔记 直接利用前一小问也可快速得到答案.

✍ **练习 1.88** 设有限群 G 的阶为 n. 任取 $a_1, \cdots, a_n \in G$，证明：存在 $1 \leqslant k \leqslant l \leqslant n$，使得 $a_k \cdots a_l = e$.

证明 用反证法，假设对所有这样的 k, l，都有 $a_k \cdots a_l \neq e$，则特别地，对所有 $1 \leqslant l \leqslant n$，都有 $a_1 \cdots a_l \neq e$. 因此这 n 个 $a_1 \cdots a_l$ 只有 $n-1$ 个可能性（因为都取不到 e）. 根据鸽笼原理，我们知道一定有两个这样的乘积相等，即存在 $1 \leqslant k < l \leqslant n$，使得 $a_1 \cdots a_k = a_1 \cdots a_l$.

注意到 $k+1 \leqslant l$，因此从左到右依次约掉相同的元素，我们就得到了

$$a_{k+1} \cdots a_l = e$$

这就导致了一个矛盾. 因此，我们就证明了这个命题.

1.5.6.2 Cauchy 定理的证明

✍ **练习 1.89** 该习题给出了 Cauchy 定理的一种证明思路.

设 G 是有限群，p 是 $|G|$ 的素因子. 记

$$S=\{(x_1,x_2,\cdots,x_p):\ x_i\in G,\ x_1x_2\cdots x_p=1\}.$$

并定义 S 上的关系 $\sim$：$\alpha\sim\beta$ 当且仅当 β 是 α 的一个循环置换. （即若 $\alpha=(x_1,x_2,\cdots,x_p)$，则

$$\beta=(x_{1+k},x_{2+k},\cdots,x_p,x_1,\cdots,x_k)$$

其中 $k\in[0,p-1]$ 为整数.）试证明：

1. $|S|=|G|^{p-1}$，从而 $|S|$ 被 p 整除；
2. S 中元素的循环置换仍然是 S 的元素；
3. $\sim$ 为 S 上的等价关系；
4. 等价类只包含一个元素，当且仅当该元素形如 $(x,x,\cdots,x)$，且 $x^p=1$；
5. 任意一个等价类的阶为 1 或 p. 从而 $|S|=k+pd$，其中 k 为阶为 1 的等价类的个数，d 为阶为 p 的等价类的个数；
6. G 必包含一个阶为 p 的元素.

注 提示：第六小问中，$\{(1,1,\cdots,1)\}$ 必是阶为 1 的等价类，所以 $k\neq 0$. 由第五小问的结论可知，$p|k$，所以 $k\geqslant p>1$，从而必有另一个阶为 1 的等价类 $\{(x,x,\cdots,x):x\neq 1,x^p=1\}$.

1.5.6.3 Lagrange 定理在初等数论中的应用

我们考虑数论中的模 n 同余类 $\mathbb{Z}_n:=\mathbb{Z}/n\mathbb{Z}$：完全剩余系连同加法 $(\mathbb{Z}_n,+)$ 构成交换群，既约剩余系连同乘法 $(\mathbb{Z}_n^\times,\cdot)$ 构成交换群. 对同余知识不太熟悉的读者，可以参考任意一本初等数论教程，以下我们简单列举一下常用的结论：

1. a,b 模 n 同余：$n\mid(a-b)$，记为 $a\equiv b\mod n$；【这里我们默认 $n\in\mathbb{Z}_+$】
2. （运算性质）：若 $a\equiv b\mod n$，$c\equiv d\mod n$，则
   (a). $a\pm c\equiv b\pm d\mod n$
   (b). $ac\equiv bd\mod n$
3. （模的性质）：设 $a\equiv b\mod n$，
   (a). 若 $d|n$，则 $a\equiv b\mod d$
   (b). 若 $d>0$，则 $da\equiv db\mod dn$
4. r 所在的模 n 同余类：$r\mod n:=\{r+kn:k\in\mathbb{Z}\}$.（有时简记为 $\bar r$）
5. 模 n 的完全剩余系：$\mathbb{Z}_n:=\{\bar 0,\cdots,\overline{n-1}\}$.
6. 模 n 的既约剩余系：$\mathbb{Z}_n^\times:=\{\bar i:\gcd(i,n)=1\}$.
7. Euler 函数 $\varphi(n)$：$1,2,\cdots,n$ 中与 n 的最大公因数为 1 的整数个数.（即模 n 的既约剩余系的元素个数）

✍ **练习 1.90** 证明 Fermat 小定理：若 p 是素数，那么对任意的 $a\in\mathbb{Z}$ 有 $a^p\equiv a\mod p$.

注 我们从群论的角度重新描述这一问题：若 p 是素数，那么对任意的 $a\in\mathbb{Z}_p$，有 $a^p=a$. 于是我们所学的 Lagrange 定理就派上了用场.

证明 因为 p 为素数，所以 $\mathbb{Z}_p^\times=\{\bar 1,\cdots,\overline{p-1}\}$. 若 $a=\bar 0$，则 $a^p=\bar 0=a$.

下设 $a\in\mathbb{Z}_p^\times$. 因为 $|\mathbb{Z}_p^\times|=p-1$，于是由 Lagrange 定理的推论 $a^{p-1}=\bar 1$，即 $a^p=a$. 于是原命题得证.

✍ **练习 1.91** 设 p 是素数，n 是正整数.

1. 找出 $\bar p$ 在群 $(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times$ 中的阶；
2. 证明：$n\mid\varphi(p^n-1)$.

证明

1. 一方面，我们显然有 $p^n-1\equiv 0\mod p^n-1$，即 $(\bar p)^n=\bar 1$. 另一方面，对任意的 $k<n$，$p^k-1<p^n-1$，所以 $\overline{p^k-1}=p^k-1\neq 0$，即 $(\bar p)^k\neq\bar 1$. 从而 $|\bar p|=n$.
2. 由 Lagrange 定理的推论，$|\bar p|$ 整除 $|(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times|$，即 $n\mid\varphi(p^n-1)$.

✍ **练习 1.92** 证明 Euler 定理：若 $\gcd(a,n)=1$，则 $a^{\varphi(n)}\equiv 1 \mod n$.

注 提示：考虑 $a\in\mathbb{Z}_n^\times$.

✍ **练习 1.93** 确定 $3^{3^{100}}$ 的最末两位数字.

注 求一个数的末两位数字，就是求其模 100 的同余类.

解 由 Euler 定理：因为 $\gcd(3,100)=1$，所以 $3^{\varphi(100)}\equiv 1 \mod 100$. 以下先求 $\varphi(100)$.

因为 $100=2^2\times 5^2$，所以 $\varphi(100)$ 为 100 以内没有素因子 2 和 5 的正整数个数. 100 以内 2 的倍数有 50 个，5 的倍数有 20 个，10 的倍数有 10 个，因此根据容斥原理，100 以内 2 或 5 的倍数有 $50+20-10=60$ 个，从而 $\varphi(100)=100-60=40$. 也就有 $3^{40}\equiv 1 \mod 100$.

我们进一步考察 $3^{100} \mod 40$. 因为 $3^4=81\equiv 1 \mod 40$，所以 $3^{100}=(3^4)^25\equiv 1^25\equiv 1 \mod 40$，即存在整数 k，满足 $3^{100}=40k+1$.

综上，$3^{3^{100}}\equiv 3^{40k+1}\equiv 3(3^{40})^k\equiv 3 \mod 100$. 即 $3^{3^{100}}$ 的最末两位数字是 03.

1.6 循环群

1.6.1 课前思考

1. 设 G 为有限群，$g\in G$ 的阶为 10，则下列结论中正确的有____，不正确的有____：
   A. G 的阶为 12；
   B. G 的阶为 20；
   C. g^4 的阶为 5；
   D. G 有 2 阶子群.
2. 设 G 的阶为 7，则下列说法正确的有（　　）：
   A. G 为交换群；
   B. G 的所有不等于 1 的元素，其阶都为 7；
   C. G 的子群有 3 个；
   D. G 到自身的群同态，除了恒等映射，都是群同构.

解

1. 正确：CD，2 阶子群可以为 $\langle g^5\rangle$.
   错误：A，G 的阶只能为 10 的倍数.
2. ABD：注意到 7 阶群只能为 7 阶循环群 $(\mathbb{Z}_7,+)$ 即可.

1.6.2 知识要点

（一）循环群的生成元与循环群的结构

设 G 为循环群：$G=\langle g\rangle$.

1. （生成元的阶）：$|g|=|G|$.
2. （生成元的幂）：
   (a). 若 $|g|=\infty$，则 $G\simeq(\mathbb{Z},+)$，且 $G=\langle g^a\rangle$，当且仅当 $a=\pm 1$；
   (b). 若 $|g|=n<\infty$，则 $G\simeq(\mathbb{Z}_n,+)$，且 $G=\langle g^a\rangle$，当且仅当 $(a,n)=1$；于是 G 的生成元共有 $\varphi(n)$ 个.

（二）元素的阶的性质

设 g,h 是群 G 的元素.

1. （g^a 的阶）：
   (a). 若 $|g|=\infty$，则 $|g^a|=\infty$；

(b). 若 $|g|=n<\infty$，则 $|g^a|=\dfrac{n}{\gcd(n,a)}$.

2. (乘积的阶)：若 $gh=hg$，且 $|g|$, $|h|$ 互素，则 $|gh|=|g|\cdot|h|$.

(三) 循环群的子群结构

1. (循环群的子群)：$G=\langle g\rangle$ 的子群为 $K=\{1\}$ 或 $\langle g^d\rangle$，其中 d 为最小的正整数，使得 $g^d\in K$. 具体地说：
   (a). 若 G 为无限群：则对任意的正整数 m，G 恰有一个指数为 m 的子群 $\langle g^m\rangle$，且 $\langle g^m\rangle=\langle g^{-m}\rangle$；
   (b). 若 G 为阶 n 的有限群：则对任意的 $a|n$，G 恰有一个指数为 d 的子群 $\langle g^d\rangle$，$d=n/a$，且 $\langle x^m\rangle=\langle x^{(m,n)}\rangle$.

1.6.3 知识要点解读

循环群与同余类的关系非常密切，于是这一部分的定理证明中，也大量的出现初等数论的基础知识. 同时，我们把元素的阶的性质放到本节呈现，是因为 $|g|=|\langle g\rangle|$，从而我们对元素的阶的解读，有两个角度：

1. 指数的角度：根据定义，元素的阶为最小的正整数满足 $g^{|g|}=1$，此时需结合同余类、Bézout 定理等初等数论知识加以讨论；
2. 群的角度：元素的阶为由该元素生成的循环群的阶，此时可以通过 Lagrange 定理等子群的性质，得到阶的一些信息.

问题 1.14 (生成元的阶)：设 G 为循环群：$G=\langle g\rangle$，则 $|g|=|G|$.

证明 若 $|g|=\infty$，则对任意的 $i\in\mathbb{Z}$，g^i 都是不相同的. (否则，若存在 $i<j$，使得 $g^i=g^j$，则 $g^{j-i}=1$，于是 $|g|\leqslant j-i$，这与 $|g|=\infty$ 相矛盾!) 而所有的 $g^i\in G$，所以 $|G|=\infty$.

下设 $|g|=n$. 由同余类的性质可知，对任意的整数 k，都存在整数 $i\in[0,n-1]$，以及整数 m，使得 $k-i=nm$，于是 $g^k=g^{i+nm}=g^i$. 从而 G 中的元素至多为 $\{g^0=1,\cdots,g^{n-1}\}$. 同时，若存在 0 到 $n-1$ 中的整数 $i<j$，使得 $g^i=g^j$，则 $g^{j-i}=1$，从而 $n=|g|\leqslant j-i$. 然而 $j-i$ 必然小于 n，矛盾! 从而集合中的元素 $\{g^0=1,\cdots,g^{n-1}\}$ 两两不同，即 $G=\{g^0=1,\cdots,g^{n-1}\}$，于是 $|G|=n=|g|$.

问题 1.15 (g^a 的阶)：设 g 是群 G 的元素，若 $|g|=n<\infty$，则 $|g^a|=\dfrac{n}{\gcd(n,a)}$.

证明 记 $|g^a|=k$.

一方面：(注意到 $\gcd(n,a)\mid a$)

$$(g^a)^{\frac{n}{\gcd(n,a)}}=(g^n)^{\frac{a}{\gcd(n,a)}}=1$$

从而 $k\leqslant\frac{n}{\gcd(n,a)}$.

另一方面，因为 $(g^a)^k=1$，于是 $g^{ak}=1$，从而必有 $n\mid ak$，于是 $\frac{n}{\gcd(n,a)}\mid\frac{a}{\gcd(n,a)}k$，由于 $\frac{n}{\gcd(n,a)}$ 与 $\frac{a}{\gcd(n,a)}$ 互素，从而有 $\frac{n}{\gcd(n,a)}\mid k$，所以 $k\geqslant\frac{n}{\gcd(n,a)}$.

综上，$|g^a|=k=\frac{n}{\gcd(n,a)}$.

✍ **练习 1.94** 设群 G 中元素 a 的阶为 $n<\infty$，对任意的整数 m，证明：

$$|a^m|=|a|\iff\gcd(n,m)=1$$

问题 1.16* (乘积的阶)：设 g,h 是群 G 的元素，若 $gh=hg$，且 $|g|$, $|h|$ 互素，则 $|gh|=|g|\cdot|h|$.

证明 记 $|g|=m$, $|h|=n$, $|gh|=k$.

一方面，因为 g,h 可交换，所以

$$\begin{aligned}(gh)^{mn}&=g^{mn}h^{mn}\\&=(g^m)^n(h^n)^m\\&=1\end{aligned}$$

从而 $k\leqslant mn$.

另一方面，考察元素 $(gh)^m$ 的阶，我们有 $|(gh)^m| = \frac{k}{\gcd(m,k)}$. 同时，因为 $(gh)^m = g^m h^m = h^m$，我们有 $|h^m| = \frac{n}{\gcd(m,n)} = n$，从而 $n = \frac{k}{\gcd(m,k)}$，即 $n\gcd(m,k) = k$，也就是 $n \mid k$. 同理，考察 $(gh)^n$ 的阶可得 $m \mid k$，于是 $mn = \mathrm{lcm}(m,n)$ 整除 k，即 $k \geqslant mn$.

综上，$|gh| = mn = |g| \cdot |h|$.

1.6.4 典型例题

循环群也许是我们接触过的最简单的群了，由于其生成元只有一个，因此它的结构非常清晰，它的子群的结构也很清晰. 而且，对任意一个群，它总是有一系列的循环子群 $\langle g \rangle$，其中 g 是任意元素. 我们可以利用这一点研究群的结构. 我们来看一个非常有用的结论.

例题 1.14 若群 G 的阶为素数 p，则 $G \simeq \mathbb{Z}_p$.

证明 任取 G 的非幺元素 g，因为 $|g| \neq 1$ 整除素数 p，所以 $|g| = p$. 于是 G 包含由 g 生成的子群 $H = \langle g \rangle \simeq \mathbb{Z}_p$. 而因为 $|G| = p = |H|$，所以必有 $G = H \simeq \mathbb{Z}_p$.

1.6.5 习题

（一）循环群的结构

✍ **练习 1.95** 考虑 $\mathbb{Z}_{45} = \langle x \rangle$.

1. 找出 $\mathbb{Z}_{45}$ 的所有子群，并分别给出一个生成元.；
2. 描述这些子群之间的包含关系；
3. 写出所有能生成 $\mathbb{Z}_{45}$ 的元素.

✍ **练习 1.96** 写出 D_8 的所有循环子群，并找出 D_8 的一个非循环的真子群.

注 提示：$\langle r^2, s \rangle$.

✍ **练习 1.97*** 证明：下列的群均不循环：

1. $\mathbb{Z}_2 \times \mathbb{Z}_2$；
2. $\mathbb{Z}_2 \times \mathbb{Z}$；
3. $\mathbb{Z} \times \mathbb{Z}$；
4. $\mathbb{Q} \times \mathbb{Q}$.

注 由于循环群的结构可以由其阶完全确定，所以我们总可以找到对应阶的循环群的“原型”：$\mathbb{Z}_n$ 或 $\mathbb{Z}$，从而我们继续考察已知群和“原型”是否同构即可.

证明

1. 如果 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 为循环群，由于其为 4 阶，从而必同构于 $\mathbb{Z}_4$. 然而 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 中的每个元素，都为 1 阶或 2 阶，而 $\mathbb{Z}_4$ 中存在 4 阶元素，于是两个群必定不同构.
2. 如果 $\mathbb{Z}_2 \times \mathbb{Z}$ 为循环群，由于其为无限群，从而必同构于 $\mathbb{Z}$. $\mathbb{Z}$ 中只有一个有限阶元素 0，而 $\mathbb{Z}_2 \times \mathbb{Z}$ 中至少有两个有限阶元素 $(0,0),(1,0)$，于是两个群必定不同构.
3. 如果 $\mathbb{Z} \times \mathbb{Z}$ 为循环群，于是可设 $\mathbb{Z} \times \mathbb{Z} = \langle (a,b) \rangle$. 考察元素 $(1,0),(0,1)$，必存在两个非零整数 m,n，使得
$$(1,0) = (ma, mb)$$
$$(0,1) = (na, nb)$$
而由方程 1：$b = 0$；由方程 2：$b \neq 0$，矛盾！
4. 与第三问的证明过程基本一致.

✍ **练习 1.98** 证明：对任意的正整数 $n \geqslant 3$，$G = (\mathbb{Z}_{2^n})^\times$ 不是循环群.

注 提示：对于循环群，同阶的子群只有一个，而 $\langle 2^n - 1 \rangle$ 和 $\langle 2^{n-1} + 1 \rangle$ 都是 G 的二阶子群.

（二）循环群的应用

✍ **练习 1.99** 若 x 是有限群 G 的元素，且 $|x|=|G|$，证明：$G=\langle x\rangle$. 若 G 是无限群，试给出一个反例.

注 提示：考虑 $\mathbb{Z}$ 中的元素 2.

✍ **练习 1.100** 设 H 为群，$h\in H$.

1. 证明：存在唯一的群同态 $f:\mathbb{Z}\to H$，满足 $1\mapsto h$；
2. 若存在 $n\in\mathbb{Z}_+$ 使得 $h^n=1$，证明：存在唯一的群同态 $f:\mathbb{Z}_n=\langle x\rangle\to H$，满足 $x\mapsto h$.

✍ **练习 1.101** 设 G 是有限群，$x\in G$. 证明：$g\in N_G(\langle x\rangle)$，当且仅当存在 $a\in\mathbb{Z}$，使得 $gxg^{-1}=x^a$.

证明 一方面，若 $g\in N_G(\langle x\rangle)$，则 $g\langle x\rangle g^{-1}=\langle x\rangle$，于是 $gxg^{-1}\in\langle x\rangle$，即存在 $a\in\mathbb{Z}$，使得 $gxg^{-1}=x^a$.

另一方面，设存在 $a\in\mathbb{Z}$，使得 $gxg^{-1}=x^a$. 对任意的 $x^i\in\langle x\rangle$，有：

$$\begin{aligned} gx^ig^{-1}&=gx(g^{-1}g)x\cdots x(g^{-1}g)xg^{-1}\\ &=(gxg^{-1})^i\\ &=x^{ai}\in\langle x\rangle \end{aligned}$$

于是 $g\langle x\rangle g^{-1}\subset\langle x\rangle$，由“正规子群”一节的习题可知：$g\langle x\rangle g^{-1}=\langle x\rangle$，也就有 $g\in N_G(\langle x\rangle)$.

✍ **练习 1.102*** 设 G 是 n 阶循环群，k 与 n 互素. 证明：映射 $x\mapsto x^k$ 是满射.

注 提示：由 Bézout 定理，存在整数 p，使得 $kp\equiv 1 \mod n$. 从而对任意的 $g\in G$，$g^p\in G$，使得 $(g^p)^k=g^{pk}=g\in G$.

✍ **练习 1.103*** 设 G 是 n 阶群，k 与 n 互素. 证明：映射 $x\mapsto x^k$ 是满射.

注 提示：注意到对任意 $g\in G$，$g^n=1$. 然后使用上题的证明过程即可.

✍ **练习 1.104** 设 $\mathbb{Z}_n$ 是 n 阶循环群. 对任意整数 a，定义映射

$$\begin{aligned} \sigma_a:\mathbb{Z}_n&\to\mathbb{Z}_n\\ x&\mapsto a\cdot x \end{aligned}$$

证明：

1. σ_a 是 $\mathbb{Z}_n\to\mathbb{Z}_n$ 的同构，当且仅当 $\gcd(a,n)=1$；
2. $\sigma_a=\sigma_b$，当且仅当 $a\equiv b \mod n$；
3. 对任意的同构 $\varphi:\mathbb{Z}_n\to\mathbb{Z}_n$，存在整数 a，使得 $\varphi=\sigma_a$；
4. $\sigma_a\circ\sigma_b=\sigma_{ab}$；
5. 映射 $\bar{a}\mapsto\sigma_a$ 是群 $(\mathbb{Z}_n)^\times$ 到群 $\mathrm{Aut}(\mathbb{Z}_n)$ 的同构.【读者没学自同构之前，该小问可以先跳过】

✍ **练习 1.105*** 证明：群 G 只有平凡子群（即 $\{1\}$ 和 G）的充要条件是 $G=\{1\}$，或为素数阶循环群.

注 提示：若 G 只有平凡子群，我们只需证明：$|G|$ 为 1 或素数. 若 $|G|$ 是合数，考虑 G 中的元素 $g\neq 1$. 由 Lagrange 定理，$|g|$ 是 G 的因子，若 $|g|\neq|G|$，则 $\langle g\rangle$ 是非平凡子群. 若 $|g|=|G|$，则 $G=\langle g\rangle$ 为循环群，于是 $|G|$ 的每个不等于 1 的真因子，都对应着一个 G 的非平凡子群. 从而 $|G|$ 只能为素数或 1.

✍ **练习 1.106** 试给出一个无限群的例子，它的任意阶不为 1 的子群，都具有有限指数.

注 提示：考虑 $\mathbb{Z}$.

✍ **练习 1.107** 证明：若一个群只有有限多个子群，则它必为有限群.

注 提示：考虑证明逆否命题：若群 G 为无限群，则 G 有无限多个子群.

一方面，若 G 中有一个无穷阶的元素 g，则 G 有子群 $\langle g\rangle\simeq\mathbb{Z}$，而 $\mathbb{Z}$ 有无限多个子群.

另一方面，若 G 中的所有元素均为有限阶，我们做如下操作：取 $x_1\in G$，则 $H_1=\langle x_1\rangle<G$，且为有限阶，于是 $|G-H_1|=\infty$. 在 $G-H_1$ 中取 x_2，则 $H_2=\langle x_2\rangle<G$，且为有限阶，于是 $|G-H_1\cup H_2|=\infty$. 按这样的方式操作下去，对任意的 $n\in\mathbb{Z}_+$，我们都有一个不同的子群 H_n，从而 G 有无限多个子群.

（三）元素的阶

✍ **练习 1.108** 设 x,y 为群 G 的两个元素，且 $|x|=n,|y|=m$.

1. 证明：若 $xy=yx$，则 $|xy|$ 整除 $\operatorname{lcm}(x,y)$；
2. 若 $xy\neq yx$，则第一小问的命题成立么？
3. 试给出一例，满足 $xy=yx$，且 $|xy|\neq\operatorname{lcm}(x,y)$.

注 提示：

1. 第一小问，参考“从定理证明中学解题”所示例题；
2. 第二小问，在 D_6 中，$|r|=3$，$|s|=2$，且 $|rs|=2$；
3. 第三小问，在 $\mathbb{Z}_4$ 中，取 $x=y=2$，于是 $x+y=y+x$ 且 $|x|=|y|=2$，但 $|0|=|x+y|=1\neq 2$.

✍ **练习 1.109** 设 x 是群 G 的元素，p 是素数，n 是正整数. 证明：若 $x^{p^n}=1$，则存在某个 $m\leqslant n$，使得 $|x|=p^m$.

✍ **练习 1.110*** 证明：$(\mathbb{Q},+)$ 不是循环群，但其任意有限生成的子群都是循环群.

注 第一小问，$\langle q\rangle=\{nq:\ n\in\mathbb{Z}\}$.

第二小问，若生成元为既约分数 $p_i/q_i,(i=1,\cdots,n)$，则他们生成子群的生成元可以按如下方式选取：将这些分数通分 $p_i'/\operatorname{lcm}(q_1,\cdots,q_n)$，于是生成元取 $\gcd(p_1',\cdots,p_n')/\operatorname{lcm}(q_1,\cdots,q_n)$.

✍ **练习 1.111** 设有限群 G 的阶为 n，证明：若对 n 的每一个因子 m，G 中至多有一个 m 阶子群，则 G 为循环群.

注 ？

✍ **练习 1.112** 证明：群 G 是循环群，当且仅当 G 的任一子群形如 $\{g^m:\ g\in G\}$，其中 m 是非负整数.

注 ？

1.6.6 思考题

完全剩余系与简化剩余系

✍ **练习 1.113** 定义：

$$\mathbb{Z}_n^\times:=\{\bar a:\ (a,n)=1,a\in\{0,\cdots,n-1\}\}$$

证明：$\mathbb{Z}_n^\times$ 连同剩余类的乘法构成群.

✍ **练习 1.114** 证明：$\mathbb{Z}_5^\times,\mathbb{Z}_9^\times,\mathbb{Z}_{18}^\times$ 是循环群.

注 证明一个有限群 G 是循环群，只需找到一个元素 g，满足 $|g|=|G|$ 即可.

解

$$\mathbb{Z}_5^\times=\langle\bar 2\rangle$$
$$\mathbb{Z}_9^\times=\langle\bar 2\rangle$$
$$\mathbb{Z}_{18}^\times=\langle\bar 5\rangle$$

✍ **练习 1.115** 证明：$(\mathbb{Z}_{24}^\times,\times)\simeq(\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,+)$.

证明 为简单起见，我们将 $\bar a$ 简记为 a. 首先

$$\mathbb{Z}_{24}^\times:=\{1,5,7,11,13,17,19,23\}.$$

计算每个元素的阶可得：$\mathbb{Z}_{24}^\times$ 中不等于 1 的元素，都是二阶元素. 又因为 $\mathbb{Z}_{24}^\times$ 是 8 阶交换群，所以 $\mathbb{Z}_{24}^\times$ 只能同构于 $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$.

另一方面，定义映射 $\varphi:\mathbb{Z}_{24}^{\times}\to\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$：

$$5\mapsto(1,0,0)$$
$$7\mapsto(0,1,0)$$
$$13\mapsto(0,0,1)$$

可以验证 φ 确实是群同构.

笔记 在群论 II 中我们会知道，8 阶交换群有三种构型：$\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,\mathbb{Z}_4\times\mathbb{Z}_2,\mathbb{Z}_8$. 区别这三个群，只需关注元素的阶的最大值即可. 也就是说，$\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ 中元素的最高阶为 2，$\mathbb{Z}_4\times\mathbb{Z}_2$ 中元素的最高阶为 4，$\mathbb{Z}_8$ 中元素的最高阶为 8.

练习 1.116 设 p 是奇素数，$n\geqslant 2$ 是正整数.

1. 证明：$(1+p)^{p^{n-1}}\equiv 1 \mod p^n$，但 $(1+p)^{p^{n-2}}\not\equiv 1 \mod p^n$.
2. 证明：$(1+p)$ 是群 $(\mathbb{Z}_{p^n})^{\times}$ 中阶为 p^{n-1} 的元素.

注 提示：利用二项式定理.

练习 1.117 设 $n\geqslant 2$ 是正整数.

1. 证明：$(1+2^2)^{2^{n-2}}\equiv 1 \mod 2^n$，但 $(1+2^2)^{2^{n-3}}\not\equiv 1 \mod 2^n$.
2. 证明：5 是群 $(\mathbb{Z}_{2^n})^{\times}$ 中阶为 2^{n-2} 的元素.

1.7 正规子群与同构定理

1.7.1 课前思考

1. 设 $f:G\to H$ 是群同态，则下列说法正确的有（　　）：
   A. 若 M 是 G 的子群，则 $f(M)$ 是 H 的子群.
   B. 若 N 是 H 的子群，则 $f^{-1}(N)$ 是 G 的子群.
   C. 若 M 是 G 的正规子群，则 $f(M)$ 是 H 的正规子群.
   D. 若 N 是 H 的正规子群，则 $f^{-1}(N)$ 是 G 的正规子群.
2. 非交换群的最小阶数为____. 试写出该阶数的一个交换群____，以及一个非交换群____.

解

1. ABD.
2. $6,\mathbb{Z}_6,D_6$.
   $1,2,3,5$ 阶均为循环群，4 阶群有两个：$\mathbb{Z}_4$ 和 $\mathbb{Z}_2\times\mathbb{Z}_2$. 同时 6 阶群中有非交换群 D_6.

1.7.2 知识要点

设 G,H 为群.

（一）共轭关系

1. 共轭：
   (a). 对于 $g,h\in G$，g 与 h 共轭：存在 $n\in G$，有 $n^{-1}gn=h$；
   (b). 对于 $A,B\subset G$，A 与 B 共轭：存在 $n\in G$，有 $n^{-1}An=B$.
2. （等价关系）：不论是元素还是集合，共轭关系都是等价关系.
3. （子群的共轭）：若 $H<G$，则对任意的 $g\in G$，有 $gHg^{-1}<G$.

（二）正规子群与商群

1. G 的正规子群 N：$N<G$，且满足：对任意的 $g\in G$，有 $gNg^{-1}=N$.（记作 $N\lhd G$）
2. （正规子群的等价定义）：已知 $N<G$，则以下条件等价：
   (a). $N\lhd G$;
   (b). 对任意的 $g\in G$，有 $gN=Ng$;
   (c). 对任意的 $g\in G$，有 $gNg^{-1}\subset N$;
   (d). 对任意的 $g\in G$ 与任意的 $n\in N$，有 $gng^{-1}\in N$.
3. 单群：正规子群只有 $\{1\}$ 和其自身的群.
4. $N\lhd G$，G 对 N 的商群：N 的全体右陪集（或左陪集），连同 G 的运算构成的群.（记作 G/N，商群中的元素 gN 有时简记为 $\bar{g}$）
5. $N\lhd G$，G 到 G/N 上的自然映射（同态）：$\pi:G\to G/N,\ g\mapsto gN$.
6. $\bar{H}<G/N,\bar{H}$ 在 G 中的完全原象（complete preimage）：$\bar{H}$ 在自然映射下的原象.

（三）同构定理

1. （第一同构定理）：已知群同态 $\varphi:G\to H$，则 $\ker\varphi\lhd G$，且 $G/\ker\varphi\simeq\operatorname{im}\varphi$;
2. （第二同构定理，“钻石”）：设 $A,B<G$，对任意的 $a\in A$，有 $aB=Ba$，于是：
   (a). $AB<G$;
   (b). $B\lhd AB$;
   (c). $A\cap B\lhd A$;
   (d). $AB/B\simeq A/(A\cap B)$.
   注：当我们学过正规化子的知识后，条件“对任意的 $a\in A$，有 $aB=Ba$”可以记为 $A<N_G(B)$.
3. （第三同构定理）：设 $H,K\lhd G$，$H<K$，于是：
   (a). $H\lhd K$;
   (b). $(G/H)/(K/H)\simeq G/K$.
4. （第四同构定理，“格栅”*）：设 $N\lhd G$，并令 $\mathcal{H}=\{H<G:N\subset H\}$，$\bar{\mathcal{H}}=\{H<G/N\}$. 于是存在从 $\mathcal{H}$ 到 $\bar{\mathcal{H}}$ 的双射：$H\mapsto H/N$.（即每个 G/N 的子群都形如 H/N，其中 H 为包含 N 的 G 的子群.）
5. （第四同构定理的推论 *）：$N\lhd G$，于是对任意的包含 N 的 G 的子群 H,K 有：
   (a). $H<K\iff H/N<K/N$;
   (b). 若 $H<K$，则 $[K:H]=[K/N:H/N]$;
   (c). $\langle H,K\rangle/N=\langle H/N,K/N\rangle$;
   (d). $(H\cap K)/N=H/N\cap K/N$;
   (e). $H\lhd K\iff H/N\lhd K/N$.

1.7.3 从定理证明中学解题

1.7.3.1 正规子群的等价定义

我们先来证明正规子群最重要的等价定义 (c)（(d) 是其元素形式，两者明显等价），这也展示了正规子群定义的使用.

问题 1.17（正规子群的等价定义）：已知 $N<G$，则 $N\lhd G$ 当且仅当对任意的 $g\in G$，有 $gNg^{-1}\subset N$.

证明 一方面，若 $N\lhd G$，则对任意的 $g\in G$，有 $gNg^{-1}=N$，从而 $gNg^{-1}\subset N$ 显然成立.

另一方面，若对任意的 $g\in G$，有 $gNg^{-1}\subset N$，则：$N\subset g^{-1}Ng$. 由 g 的任意性，将前式中的 g 替换为 g^{-1} 可得：$N\subset gNg^{-1}$. 从而 $gNg^{-1}\subset N\subset gNg^{-1}$，于是必有 $N=gNg^{-1}$.

笔记 我们在本题中，看到了共轭形式的某种“稳定性”，即 gNg^{-1} 与 $g^{-1}Ng$ 在一定条件下是等价的（例如 g 取遍某个群中的全部元素）. 实际上在不同的抽象代数参考书中，有的将 A 的共轭定义为 gAg^{-1}，有的则定义为 $g^{-1}Ag$. 这二者在具体的使用过程中，没有本质区别，但会有一些细节上的差异，这一点希望读者注意.

正规子群的等价定义是很容易使用的，我们在“典型例题”部分作进一步的解读.

1.7.3.2 第一同构定理的证明

问题 1.18 （第一同构定理）：设群同态 $\varphi: G \to H$，则 $G/\ker\varphi \simeq \operatorname{im}\varphi$.

注 第一同构定理的证明非常具有代表性，其中蕴含着初学者容易忽视和感到困惑的点：映射的良定义问题. 其实读者不必把这一问题想的很复杂，说穿了就是映射不允许“一对多”，即一个元素不能映到多个象，而这是我们一开始学映射的时候就知道的事情. 只不过，在具体问题中，可能的“一对多”的情况会有一点点隐蔽，需要读者留心.

回到第一同构定理中，我们要证：$G/\ker\varphi \simeq \operatorname{im}\varphi$，于是我们需要定义映射：$f: G/\ker\varphi \to \operatorname{im}\varphi$，想办法证明 f 是群同态、且是双射. 给定 $g\ker\varphi \in G/\ker\varphi$，我们很自然地想将 f 定义为 $g\ker\varphi \mapsto \varphi(g)$. 于是，良定义的问题就悄然间出现了，读者可以先想一想问题出在哪，我们先看解答.

证明 定义映射 $f: G/\ker\varphi \to \operatorname{im}\varphi$, $g\ker\varphi \mapsto \varphi(g)$.

我们先证明：f 是良定义的，即对任意的 $g, g' \in G$，若 $g\ker\varphi = g'\ker\varphi$，则 $\varphi(g) = \varphi(g')$. 因为 $g\ker\varphi = g'\ker\varphi$，所以 $g^{-1}g' \in \ker\varphi$，即 $\varphi(g^{-1}g') = 1$. 而 $1 = \varphi(g^{-1}g') = \varphi(g)^{-1}\varphi(g')$，从而 $\varphi(g) = \varphi(g')$.

接下来证明：f 是群同态. 对任意的 $g\ker\varphi, g'\ker\varphi \in G/\ker\varphi$，我们有：

$$\begin{aligned} f(g\ker\varphi g'\ker\varphi) &= f(gg'\ker\varphi) \\ &= \varphi(gg') \\ &= \varphi(g)\varphi(g') \\ &= f(g\ker\varphi)f(g'\ker\varphi) \end{aligned}$$

从而 f 为群同态.

最后证明：f 是双射. 对任意的 $g\ker\varphi, g'\ker\varphi \in G/\ker\varphi$，我们有：

$$\begin{aligned} g\ker\varphi = g'\ker\varphi &\iff g^{-1}g' \in \ker\varphi \\ &\iff \varphi(g^{-1}g') = 1 \\ &\iff \varphi(g) = \varphi(g') \end{aligned}$$

从而 f 是双射.

笔记 一般的，涉及等价类的映射，容易产生因为选择不同代表元而产生的、“形式上”不同的象.

1.7.3.3 第一同构定理的应用

第二、三同构定理的证明，是第一同构定理的应用的绝佳的例子.

问题 1.19 （第二同构定理）：设群同态 $\varphi: G \to H$，$A, B < G$，对任意的 $a \in A$，有 $aB = Ba$，于是：

1. $AB < G$;
2. $B \lhd AB$;
3. $A \cap B \lhd A$;
4. $AB/B \simeq A/(A \cap B)$.

证明

1. 因为对任意的 $a \in A$，有 $aB = Ba$，从而 $AB = BA$，于是 $AB < G$.
2. 需证：对任意的 $a \in A, b \in B$，任意的 $h \in B$，有 $abh(ab)^{-1} \in B$. 前面已经证明 $aB = Ba$，所以 $aBa^{-1} = B$. 于是对于 $bhb^{-1} \in B$，有 $abh(ab)^{-1} = a(bhb^{-1})a^{-1} \in aBa^{-1} = B$. 即 $abh(ab)^{-1} \in B$.

3. 对任意的 $a \in A$，有 $a(A \cap B) = A \cap aB = A \cap Ba = (A \cap B)a$.
4. 定义映射 $f : A \to AB/B,\ a \mapsto aB$.
   先证明：f 是群同态. 对任意的 $a, a' \in A$，有

$$\begin{aligned} f(aa') &= aa'B \\ &= aa'BB && (B \text{ 是子群.}) \\ &= aBa'B && (a'B = Ba'.) \\ &= f(a)f(a') \end{aligned}$$

   于是 f 为群同态.
   再证明：f 是满射. 这是显然的，因为对任意的 $aB \in AB/B$，有 $f(a) = aB$.
   最后求 $\ker f$.

$$\begin{aligned} \ker f &= \{a \in A : f(a) = 1\} \\ &= \{a \in A : aB = B\} \\ &= \{a \in A : a \in B\} \\ &= A \cap B \end{aligned}$$

   从而由第一同构定理：$A/(A \cap B) \simeq AB/B$.

笔记 本例中可能会让读者感到迷惑的点，是 AB/B 中的元素形式，其实我们只需按照定义，对任意的 $ab \in AB$，$abB = aB \in AB/B$.

练习 1.118（第三同构定理）：设 $H, K \lhd G$，$H < K$，于是：

1. $H \lhd K$;
2. $(G/H)/(K/H) \simeq G/K$.

注 提示：考虑映射 $f : G/H \to G/K, gH \mapsto gK$，注意良定义的问题.

练习 1.119 设 $\varphi : G \to H$ 是群同态.

1. 设 $E < H$，证明：$\varphi^{-1}(E) < G$;
2. 设 $E \lhd H$，证明：$\varphi^{-1}(E) \lhd G$.
3. 设 $F \lhd G$，命题 $\varphi(F) \lhd H$ 成立吗？[*]

注 读者需要熟悉“象、原象”的概念，而且往往求原象的“操作” φ^{-1}，比映射 φ 本身，具有更好的性质.

证明

1. 一方面，因为 $\varphi(1_G) = 1_H \in E$，所以 $1_G \in \varphi^{-1}(E)$，从而 $\varphi^{-1}(E) \neq \varnothing$.
   另一方面，对任意的 $g_1, g_2 \in \varphi^{-1}(E)$，分别存在 $h_1, h_2 \in E$，使得 $\varphi(g_1) = h_1, \varphi(g_2) = h_2$. 从而 $\varphi(g_1 g_2^{-1}) = h_1 h_2^{-1} \in E$，即 $g_1 g_2^{-1} \in \varphi^{-1}(E)$.
   从而命题得证.
2. 由第一问的结论，我们只需证：对任意的 $x \in G$，$g \in \varphi^{-1}(E)$，有 $xgx^{-1} \in \varphi^{-1}(E)$，也就是 $\varphi(xgx^{-1}) \in E$.
   注意到 $\varphi(g) \in E$，且 $E \lhd G$，于是 $\varphi(x)\varphi(g)\varphi(x^{-1}) \in E$（等价定义 (d)）.
3. 取群同态为 $\varphi : \mathbb{Z}_2 = \langle s \rangle \to D_8 = \langle r, s \rangle, s \mapsto s$. 从而 $\langle s \rangle \lhd \langle s \rangle$，但 $\varphi(\langle s \rangle) = \langle s \rangle$ 却并不是 D_8 的正规子群.

1.7.4 典型例题

1.7.4.1 共轭形式

共轭形式的出现，与一般不成立的交换性有直接的联系，显然，若 G 为交换群，则成立平凡的结论 $gag^{-1} = a, gAg^{-1} = A$，此时也就没有研究共轭形式的必要了. 而一般情况下，我们会发现，研究对象与其共轭形式的性质有很大的相似性，例如若 A 为子群，则 gAg^{-1} 也为子群. 一般的，我们有如下结论.

例题 1.15 设 a, b 为群 G 的元素. 证明：

1. ab 的共轭形式，等于 a 的共轭形式乘 b 的共轭形式；
2. a 的阶，等于 a 的共轭形式的阶；
3. a^{-1} 的共轭形式，等于 a 的共轭形式的逆.

证明

1. 对任意的 $g \in G$，有 $g(ab)g^{-1} = (gag^{-1})(gbg^{-1})$.
2. 见“基本概念”一节的例题.
3. 对任意的 $g \in G$，有 $ga^{-1}g^{-1} = (gag^{-1})^{-1}$.

✍ **练习 1.120** 设 A, B 为群 G 的子集. 证明：

1. AB 的共轭形式，等于 A 的共轭形式乘 B 的共轭形式；
2. A 的阶，等于 A 的共轭形式的阶；
3. A^{-1} 的共轭形式，等于 A 的共轭形式的逆.

✍ **练习 1.121** 设 G 为群. 证明：

1. 设 $N = \langle S \rangle$，其中 $S \subset G$. 则 $N \lhd G$，当且仅当对任意的 $g \in G$，有 $gSg^{-1} \subset N$；
2. 设 $N = \langle x \rangle$ 是循环群. 则 $N \lhd G$，当且仅当对任意的 $g \in G$，存在整数 k，有 $gxg^{-1} = x^k$；
3. 设 n 是正整数. 证明：由 G 的所有 n 阶元素生成的子群 N，是 G 的正规子群.

证明

1. 一方面，若 $N \lhd G$，则对任意的 $g \in G$，有 $gSg^{-1} \subset gNg^{-1} = N$.
   另一方面，设对任意的 $g \in G$，满足 $gSg^{-1} \subset N$. 因为 $N = \langle S \rangle$，所以对任意的 $n \in N$，存在 $s_1, \cdots, s_n \in S$，有 $n = s_1 s_2 \cdots s_n$. 利用例题第一小问的结论，可知 $gng^{-1} = (gs_1g^{-1})(gs_2g^{-1}) \cdots (gs_ng^{-1}) \in (gSg^{-1})^n \subset N^n = N$. 于是 $N \lhd G$.
2. 直接利用第一小问结论即证.
3. 注意到元素的阶与其共轭形式的阶相同，所以对 N 的任意生成元 a，有 $gag^{-1} \in N$，利用第一小问结论即证.

1.7.4.2 正规子群的证明

想必大家现在有了这样的经验：子群的定义不如其等价定义的使用频率高. 对与正规子群，情况就不一定了，几种证明思路各有所长：等价定义 (b) 和定义本身几乎一致，注重于集合视角整体处理问题. 利用等价定义 (c)，我们不用证明集合相等，只需证明集合包含，这样至少减少了一半的工作量；利用等价定义 (d)，证明元素属于集合一般来说不一定简单，但是群（或子群）的封闭性容易导出属于关系. 面对具体问题的时候，谁更好用是不确定的，因此我们都需要熟练掌握. 我们来看一些例题.

例题 1.16 证明：若 $H, K \lhd G$，则 $H \cap K \lhd G$.

证明 [1]：利用正规子群的定义（等价定义 (b),(c) 的证明过程基本相同）

对任意的 $g \in G$，有：

$$\begin{aligned} g(H \cap K)g^{-1} &= g(Hg^{-1} \cap Kg^{-1}) \\ &= gHg^{-1} \cap gKg^{-1} \\ &= H \cap K \end{aligned}$$

于是命题得证.

证明 [2]：利用正规子群的等价定义 (d)

我们只需证：对任意的 $x \in H \cap K$ 和任意的 g，有 $gxg^{-1} \in H \cap K$.

因为 $x \in H$，所以 $gxg^{-1} \in H$. 同理，因为 $x \in K$，所以 $gxg^{-1} \in K$. 于是 $gxg^{-1} \in H \cap K$.

笔记 证法一是集合视角的证明，证法二是元素视角的证明. 在子群的部分，我们已经点出了两种证明思路的区别和联系，这里也没有新的内容.

✍ **练习 1.122** 定义群 G 的中心 $Z(G)$，

$$Z(G) := \{x \in G : xg = gx, g \in G\}$$

证明：$Z(G)$ 是 G 的正规子群.

✍ **练习 1.123** 对群 G 的任意多个正规子群，证明：

1. 这些正规子群的交，是 G 的正规子群；
2. 由这些正规子群生成的子群，也是 G 的正规子群.

✍ **练习 1.124** 证明：若 $N \lhd G$ 且 $H < G$，则 $N \cap H \lhd H$.

证明 对任意的 $h \in H$ 有：

$$\begin{aligned} h(N \cap H) &= hN \cap hH \\ &= Nh \cap H \\ &= Nh \cap Hh \\ &= (N \cap H)h \end{aligned}$$

我们接下来要看一个有趣的问题，它也是我们经常使用的命题.

例题 1.17 设 G 为群，$N < G$. 证明：若 N 的指数为 2，则 $N \lhd G$.

证明 因为 N 的指数为 2，所以取 $g \in G - N$，则 N 的左陪集为 $\{N, gN\}$，右陪集为 $\{N, Ng\}$. 由陪集分解，我们有以下无交并：$G = N \cup gN = N \cup Ng$. 因为 $N = N$，从而 $gN = Ng$.

笔记 本题的证明方式在“正规子群的证明”中比较另类. 不过他提醒我们关注陪集分解，实际上，到现在我们所学的研究群结构的工具，根源都来自于陪集分解. 因此我们在学了很多“高大上”的方法之后，也不要忘记了“起点”和“初心”.

1.7.4.3 利用商群简化群结构

在“知识要点”里，商群的内容不过寥寥几行字而已. 但是，商群的概念及其背后联系的思想，是非常重要的.

首先，商群是通过正规子群的陪集来定义的，于是我们将一个较大的群 G，“分”成了两个较小的群 N 和 G/N. 一般来说，小群的结构总是相对简单的，也是我们较为熟悉的，于是我们利用商群“化繁为简”.

其次，如果我们尝试思考逆过程“三生万物”：即给定两个小群，构造出一个大群，我们可以预计会存在商群的结构. 这一部分的内容在直积、半直积的部分呈现.

同时，商群的结构启发我们，在一个群 G 里，正规子群 N，和幺元 1 的性质，其实是很相似的，我们来看：

1. 元素 e 为 G 的幺元，当且仅当对任意的 $g \in G$，满足 $ge = eg = g$；
2. 子群 N 为 G 的正规子群，当且仅当对任意的 $g \in G$，满足 $gN = Ng$
3. 元素 $\bar{e}$ 为 G/N 的幺元，当且仅当对任意的 $\bar{g} \in G/N$，满足 $\bar{g}\bar{e} = \bar{e}\bar{g} = \bar{g}$.

这种相似性笔者称之为“普遍交换性”：即与群中的每一个元素都交换.

事实上，我们学过的很多内容，都和“交换性”有着深刻的联系. 如果一个群本身就满足交换性，那么它的结构非常简单，我们有“有限生成交换群的结构定理”，对任意阶的交换群，我们很清楚它的结构是怎样的（至少是若干种备选类型中的一种）. 如果一个群不交换，我们有满足“普遍交换性”的元素和子群，有考察“部分交换性”的中心化子（与给定集合中的每个元素交换的元素集合）与更弱的正规化子（与给定集合交换的元素集合）. 而且，因为不交换，我们有不平凡的共轭形式、交换子（形如 $x^{-1}y^{-1}xy$，我们在可解群的部分会接触到，这与 Galois 理论有紧密的关联）. 不交换也使得群结构变得更加丰富，目前数学家们也没有完全破解群结构的秘密.

从现在开始，我们将“构造商群”视为正规子群的应用方法之一. 构造商群的本质，就是将正规子群当作幺元用，我们来看下例.

例题 1.18 设 $H<G$，$N\lhd G$. 证明：若 $|H|$ 和 $[G:N]$ 互素，则 $H<N$.

注 此题需证 $H<N$，即需证 $H\subset N$. 于是需证对于任意的 $h\in H$，有 $h\in N$. 我们来看题设的三个条件：$H<G$，$N\lhd G$，$|H|$ 和 $[G:N]$ 互素，他们怎样与目标 $h\in N$ 联系呢？至此我们发现，我们先前积累的解题经验，不足以处理这一问题（这也是笔者把此题作为例题的原因）. 我们来看解答.

证明 考虑商群 G/N，由商群的定义：$|G/N|=[G:N]$. 对任意的 $h\in H$，有 $h^{|H|}=1$，从而 $(\bar{h})^{|H|}=\bar{1}$（这一结论留作习题）. 另一方面，因为 $\bar{h}\in G/N$，所以 $(\bar{h})^{|G/N|}=\bar{1}$. 注意到 $|H|$ 和 $[G:N]$ 互素，即 $|H|$ 和 $|G/N|$ 互素，而由数论中的 Bézout 定理可得，存在整数 a,b，使得 $a|H|+b|G/N|=1$，于是 $\bar{h}=(\bar{h})^{a|H|+b|G/N|}=((\bar{h})^{|H|})^a((\bar{h})^{|G/N|})^b=\bar{1}^a\bar{1}^b=\bar{1}$. 所以 $h\in N$. 命题得证.

笔记 本题的突破口在于考虑商群 G/N，一方面 $|G/N|$ 联系了条件里的 $[G:N]$，另一方面 hN 联系了 $h\in N$. 由此题我们得到了一个证明元素 g 属于正规子群 N 的思路：尝试证明 $\bar{g}=\bar{1}$.

本题也可以使用第二同构定理证明.

练习 1.125 设 $N\lhd G$，$g\in G$. 证明：若 $|g|$ 和 $|G/N|$ 互素，则 $g\in N$.

练习 1.126 设 N 是有限群 G 的正规子群，且 $|N|$ 和 $[G:N]$ 互素. 证明：N 是 G 中 $|N|$ 阶的唯一子群.

注 提示：假设 H 也是 $|N|$ 阶子群，于是 $|H|$ 和 $[G:N]$ 互素.

1.7.4.4 第一同构定理的应用

第一同构定理至少告诉我们两个重要的信息：

1. 每个群同态都可以产生一个对应的同构，从而如果我们将一个结构简单的群和一个结构复杂的群用同态关联起来，则可以构造一个同构：简单群同构于复杂群的商群，从而研究复杂群的结构；
2. 每个群同态都可以产生一个定义群的商群，即群同态的核；反过来，每给出一个定义群的商群，都可以通过构造自然映射，使得这个商群是该群同态的核.

于是第一同构定理，颇有一点“借力打力”的意味，也意味着“从已知到未知”. 这些数学思想是我们经常遇见的.

例题 1.19 定义“行列式映射”：$\det: GL_n(\mathbb{R})\to(\mathbb{R}^*,\cdot), A\mapsto\det(A)$. 试证明：

1. 映射 det 是群同态，且是满同态.
2. 证明：$GL_n(\mathbb{R})/SL_n(\mathbb{R})\simeq(\mathbb{R}^*,\cdot)$.

注 相信读者此时已经学过了线性代数，因而对于求方阵的行列式必定是手到擒来. 我们在这里，要从抽象代数的角度审视这个熟悉的对象. 我们需要回忆起行列式的一个重要性质：$\det(AB)=\det(A)\det(B)$.

证明

1. 因为 $\det(AB)=\det(A)\det(B)$，所以映射 det 为群同态. 同时，对任意的 $a\in\mathbb{R}^*$，我们总能找到：
$$\begin{vmatrix} a & 0 & \cdots & 0\\ 0 & 1 & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & 1 \end{vmatrix}=a$$
于是 det 为满射.
2. 我们来求 $\ker\det$. 我们有：
$$\begin{aligned}\ker\det&=\{A\in GL_n(\mathbb{R}):\ \det(A)=1\}\\&=SL_n(\mathbb{R})\end{aligned}$$
所以由第一同构定理可得：$GL_n(\mathbb{R})/SL_n(\mathbb{R})\simeq(\mathbb{R}^*,\cdot)$.

练习 1.127 定义“倍乘映射”：$f:\mathbb{Z}\to n\mathbb{Z}, a\mapsto na$. 试证明：

1. 映射 f 是群同态，且是满同态.
2. 求此映射的核，并由此导出同构关系.

1.7.5 习题

1.7.5.1 正规子群的例子

✍ **练习 1.128** 设 $G=D_{16}=\langle r,s\mid r^8=s^2=1,\ rs=sr^{-1}\rangle$，$\bar{G}=G/\langle r^4\rangle$.

1. 证明：$|\bar{G}|=8$；
2. 将 $\bar{G}$ 中的元素均改写为 $\bar{s}^a\bar{r}^b$ 的形式，其中 a,b 为自然数；
3. 求 $\bar{G}$ 中每个元素的阶；
4. 将下列元素改写为 $\bar{s}^a\bar{r}^b$ 的形式，其中 a,b 为自然数：

$$\overline{rs},\ \overline{sr^{-2}s},\ \overline{s^{-1}r^{-1}sr}$$

5. 证明：$\bar{H}=\langle\bar{s},\bar{r}^2\rangle$ 是 $\bar{G}$ 的正规子群，且 $\bar{H}\cong V_4$. 求 $\bar{H}$ 在 G 中的完全原象；
6. 求 $\bar{G}$ 的中心 $Z(\bar{G})$，并求出 $\bar{G}/Z(\bar{G})$.

注 提示：第五小问：注意到 $[\bar{G}:\bar{H}]=2$，$\bar{H}$ 的完全原象为 $\langle s,r^2\rangle\simeq D_8$. 第六小问：$Z(\bar{G})=\langle\bar{r}^2\rangle$，于是 $\bar{G}/Z(\bar{G})\simeq V_4$.

✍ **练习 1.129** 设 $G=QD_{16}=\langle\sigma,\tau\mid\sigma^8=\tau^2=1,\sigma\tau=\tau\sigma^3\rangle$，$\bar{G}=G/\langle\sigma^4\rangle$.

1. 证明：$|\bar{G}|=8$；
2. 将 $\bar{G}$ 中的元素均改写为 $\bar{\tau}^a\bar{\sigma}^b$ 的形式，其中 a,b 为自然数；
3. 求 $\bar{G}$ 中每个元素的阶；
4. 将下列元素改写为 $\bar{\tau}^a\bar{\sigma}^b$ 的形式，其中 a,b 为自然数：

$$\overline{\sigma\tau},\ \overline{\tau\sigma^{-2}\tau},\ \overline{\tau^{-1}\sigma^{-1}\tau\sigma}$$

5. 证明：$\bar{G}\simeq D_8$.

✍ **练习 1.130** 设 $G=M=\langle u,v\mid u^2=v^8=1,vu=uv^5\rangle$，$\bar{G}=G/\langle v^4\rangle$.

1. 证明：$|\bar{G}|=8$；
2. 将 $\bar{G}$ 中的元素均改写为 $\bar{u}^a\bar{v}^b$ 的形式，其中 a,b 为自然数；
3. 求 $\bar{G}$ 中每个元素的阶；
4. 将下列元素改写为 $\bar{u}^a\bar{v}^b$ 的形式，其中 a,b 为自然数：

$$\overline{vu},\ \overline{uv^{-2}u},\ \overline{u^{-1}v^{-1}uv}$$

5. 证明：$\bar{G}\simeq Z_2\times Z_4$.

✍ **练习 1.131** 设 $G=\mathbb{Z}/24\mathbb{Z}$，$\tilde{G}=G/\langle\overline{12}\rangle$，其中对每个整数 a，将 $\tilde{a}$ 简记为 $\tilde{a}$.

1. 证明：$\tilde{G}=\{\tilde{0},\tilde{1},\cdots,\widetilde{11}\}$；
2. 求 $\tilde{G}$ 中每个元素的阶；
3. 证明：$\tilde{G}\simeq\mathbb{Z}/12\mathbb{Z}$.

✍ **练习 1.132** 设 $G=Z_4\times Z_4=\{x,y\mid x^4=y^4=1,xy=yx\}$，$\bar{G}=G/\langle x^2y^2\rangle$.

1. 证明：$|\bar{G}|=8$；
2. 将 $\bar{G}$ 中的元素均改写为 $\bar{x}^a\bar{y}^b$ 的形式，其中 a,b 为自然数；
3. 求 $\bar{G}$ 中每个元素的阶；
4. 证明：$\bar{G}\simeq Z_4\times Z_2$.

1.7.5.2 正规子群的证明与应用

✍ **练习 1.133** 证明：若 $N\lhd H$ 且 $H<G$，则 $H<N_G(N)$.

✍ **练习 1.134** 证明：若 $N<H<G$，且 $N\lhd G$，则 $N\lhd H$.

✍ **练习 1.135*** 若 $N\lhd H$ 且 $H\lhd G$，我们是否可以说明：$N\lhd G$?

解 考虑 $\mathbb{Z}_2 \lhd K_4 \lhd S_4$.

✍ **练习 1.136** G 是交换群，且 $N < G$. 证明：G/N 是交换群.

注 注意到交换群的子群都是正规子群.

✍ **练习 1.137** 试给出一个非交换群 G 及其正规子群 $N \neq G$，使得 G/N 是交换群.

解

$$D_6/\langle s|s^2=1\rangle = \langle r|r^3=1\rangle$$

✍ **练习 1.138** 证明：在商群 G/N 中，对任意正整数 n 有 $(gN)^n = g^nN$.

✍ **练习 1.139** 设 G 是群，且 $N \lhd G$. 证明：若 n 是最小的正整数使得 $g^n \in N$，则 $gN \in G/N$ 的阶为 n.

✍ **练习 1.140** 试给出一个群 G，和它的一个正规子群 N、元素 $g \in G$，满足 $|gN| < |g|$.

注 提示：任取 N 中的元素 $g \neq 1$，则 $|gN| = 1$，而 $|g| \geqslant 2$.

✍ **练习 1.141** 设 G 是群，且 $N \lhd G$，记 $\bar{G} = G/N$. 证明：

1. 若 $G = \langle x, y\rangle$，则 $\bar{G} = \langle \bar{x}, \bar{y}\rangle$；
2. 一般地，若 $G = \langle S\rangle$，则 $\bar{G} = \langle \bar{S}\rangle$.

注 提示：$(a_1 \cdots a_n)N = (a_1N)\cdots(a_nN)$.

✍ **练习 1.142** 证明：若 $G/Z(G)$ 是循环群，则 G 是交换群.

注 提示：设 $G/Z(G) = \langle \bar{x}\rangle$，于是任意 $g \in G$ 可表示为 x^kz，其中 k 为整数，$z \in Z(G)$.

✍ **练习 1.143** 设 H 是 G 的子群. 证明：若 H 是 G 中阶为 $|H|$ 的唯一的子群，则 $H \lhd G$.

证明 因为 $gHg^{-1} < G$，且 $|gHg^{-1}| = |H|$，所以由 H 的唯一性可得 $gHg^{-1} = H$.

✍ **练习 1.144** 证明：若 $|G| = pq$，其中 p, q 为素数，则要么 G 是交换群，要么 $Z(G) = 1$.

注 提示：我们已经在“正规子群”一节中证明：若 $G/Z(G)$ 是循环群，则 G 是交换群.

✍ **练习 1.145** 证明：若 H 是 G 的正规子群，且指数为素数 p，于是对任意 $K < G$，或者 $K < H$，或者 $G = HK$ 且 $|K : H \cap K| = p$.

证明 商群 G/H 的阶为素数 p，从而 $G/H \simeq \mathbb{Z}_p$. 于是必有一元素 $x \in G - H$，使得 $G/H = \langle \bar{x}\rangle$.

考虑 K 和 H 的关系，若 K 不是 H 的子群，则 K 中必有一个不属于 H 的元素 k，也就是 $\bar{k} \neq \bar{1}$. 又因为 $\bar{k} \in G/H = \langle \bar{x}\rangle$，于是 $|\bar{k}|$ 必为 p 的因子，且不为 1，从而只能有 $|\bar{k}| = p$，即有 $\langle \bar{k}\rangle = \langle \bar{x}\rangle$.

对任意的 $g \in G$，有 $gH \in G/H = \langle \bar{x}\rangle = \langle \bar{k}\rangle$，所以存在自然数 m，使得 $gH = (\bar{k})^m = k^mH$. 由此可得：

$$g \in gH = k^mH \subset \langle k\rangle H \subset KH = HK$$

从而 $G \subset HK$，而 $HK \subset G$ 是显然的，于是 $G = HK$.

由 $|HK| = |H||K|/|H \cap K|$ 可得：$|HK : H| = |K : H \cap K|$，即 $p = |G : H| = |HK : H| = |K : H \cap K|$.

1.7.5.3 共轭形式

✍ **练习 1.146** 设 N 是群 G 的有限子群.

1. 取 $g \in G$. 证明：$gNg^{-1} = N$ 当且仅当 $gNg^{-1} \subset N$；
2. 证明：$N_G(N) = \{g \in G : gNg^{-1} \subset N\}$；
3. 设 $N = \langle S\rangle$，其中 $S \subset G$. 证明：对于 $g \in G$，$gNg^{-1} = N$ 当且仅当 $gSg^{-1} \subset N$；
4. 设 $G = \langle T\rangle$，$N = \langle S\rangle$，其中 $S, T \subset G$. 证明：$N \lhd G$ 当且仅当对任意的 $t \in T$，$tSt^{-1} \subset N$.

注 提示：第一小问中，注意到 $|N| = |gNg^{-1}|$.

✍ **练习 1.147*** 设 H, K 是有限群 G 的两个子群，$g \in G$，证明：

$$|HgK| = |H|[K : K \cap g^{-1}Hg] = |K|[H : H \cap gKg^{-1}]$$

证明 因为对任意的 $h\in H$，hgK 是 K 的左陪集，于是 HgK 总可以分解为无交并：

$$HgK=\bigsqcup_{i=1}^{m}h_igK$$

从而 $|HgK|=m|K|$. 于是我们只需证：$m=[H:H\cap gKg^{-1}]$.

因为 K 是子群，于是 gKg^{-1} 也是子群，从而 $H\cap gKg^{-1}$ 是 H 的子群. 于是我们只需证：H 中 $H\cap gKg^{-1}$ 的左陪集的个数等于 m. 即证明：对任意的 $h,h'\in H$，$hgK=h'gK\iff h(H\cap gKg^{-1})=h'(H\cap gKg^{-1})$. (请读者参考上一节“群的陪集分解”)

我们有：

$$\begin{aligned}
hgK=h'gK&\iff (h'g)^{-1}(hg)\in K && (C1)\\
&\iff g^{-1}h'^{-1}hg\in K\\
&\iff h'^{-1}h\in gKg^{-1} && (C2)\\
&\iff h'^{-1}h\in H\cap gKg^{-1} && (h'^{-1}h\in H)\\
&\iff h(H\cap gKg^{-1})=h'(H\cap gKg^{-1})
\end{aligned}$$

另一个等式 $|HgK|=|H|[K:K\cap g^{-1}Hg]$ 的证明过程基本相同，这里略去. 于是命题即证.

笔记 若 $H,K<G$，我们对形如 $HgK(g\in G)$ 的集合称为 G 的一个 $H-K$ 双陪集. 我们可以证明，所有的 $H-K$ 双陪集，也构成 G 的一个分拆. 这就是我们下面要证的.

练习 1.148 设 G 为群，$H,K<G$. 证明：任意的 $H-K$ 双陪集全体，构成了 G 的一个分拆.

证明 首先注意到因为 $H,K<G$，所以 $e\in H$，$e\in K$. 令 $g\in G$，我们一定有

$$g=ege\in HgK$$

接着，我们只要证明对任意 $g_1,g_2\in G$，对应的两个双陪集 Hg_1K 和 Hg_2K 要么相等，要么无交. 实际上，我们可以证明

$$Hg_1K=Hg_2K\iff g_1\in Hg_2K.$$

充分性是显然的，因为 $g_1\in Hg_1K$. 我们来证明必要性. 假设 $g_1\in Hg_2K$. 同时左乘 H，右乘 K，我们就得到了 $Hg_1K\subset Hg_2K$. 另一方面，因为我们可以找到 $h\in H$，$k\in K$，使得 $g_1=hg_2k$，所以

$$g_2=h^{-1}g_1k^{-1}\in Hg_1K.$$

我们同理可以证明 $Hg_2K\subset Hg_1K$. 因此 $Hg_1K=Hg_2K$，这就证明了必要性.

现在，假设 $Hg_1K\cap Hg_2K\neq\emptyset$，令 $g_3\in Hg_1K\cap Hg_2K$. 则

$$Hg_3K=Hg_1K$$

$$Hg_3K=Hg_2K$$

这就证明了 $Hg_1K=Hg_2K$.

综上所述，我们就证明了所有的 $H-K$ 双陪集构成了 G 的一个分拆.

1.7.5.4 象与核

练习 1.149 定义 $\varphi:(\mathbb{R}^*,\cdot)\to(\{\pm1\},\cdot)$，$x\mapsto x/|x|$. 证明 φ 是群同态，并求其象与核.

练习 1.150 定义 $\varphi:\mathbb{Z}/8\mathbb{Z}\to\mathbb{Z}/4\mathbb{Z}$，$\bar{a}\mapsto\bar{a}$. 证明 φ 是群满同态，并求其象与核.

练习 1.151 设 $G=\left\{\begin{pmatrix}a&b\\0&c\end{pmatrix}:a,b,c\in\mathbb{R},ac\neq0\right\}<GL_2(\mathbb{R})$.

1. 证明 $\varphi:G\to\mathbb{R}^*$，$\begin{pmatrix}a&b\\0&c\end{pmatrix}\mapsto a$ 是群满同态，并求其象与核；

2. 证明 $\psi: G \to \mathbb{R}^* \times \mathbb{R}^*$, $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a,c)$ 是群满同态，并求其象与核；
3. 设 $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}$. 证明：$H \simeq (\mathbb{R}, +)$.

✍ **练习 1.152** 设 $S^1 = \{e^{2\pi i r} : r \in \mathbb{R}\}$. 定义 $\varphi: (\mathbb{R}, +) \to (S^1, \cdot)$, $r \mapsto e^{2\pi i r}$. 证明 φ 是群满同态，并求其象与核.

✍ **练习 1.153** 设 $f: G \to H$ 是群同态，$M < G$. 证明：$f^{-1}(f(M)) = KM$，其中 $K = \ker f$.

证明 一方面，对任意的 $k \in K, m \in M$，$f(km) = f(k)f(m) = f(m) \in f(M)$，从而 $km \in f^{-1}(f(M))$. 即 $KM \subset f^{-1}(f(M))$.

另一方面，对任意的 $x \in f^{-1}(f(M))$，我们有 $f(x) \in f(M)$，从而存在 $m \in M$ 使得 $f(x) = f(m)$. 于是 $f(xm^{-1}) = 1$，即 $xm^{-1} \in K$，也就是 $x \in Km \subset KM$. 这就证明了 $f^{-1}(f(M)) \subset KM$.

综上，$f^{-1}(f(M)) = KM$.

1.7.5.5 第一同构定理

✍ **练习 1.154** 设群 $G = \{(a,b) : a \in \mathbb{R}^*, b \in \mathbb{R}\}$. G 上的运算为 $(a,b)(c,d) := (ac, ad+b)$. 证明：$K = \{(1,b) : b \in \mathbb{R}\}$ 是 G 的正规子群，且 $G/K \simeq (\mathbb{R}^*, \cdot)$.

✍ **练习 1.155** 考虑商群 $(\mathbb{Q}/\mathbb{Z}, +)$. 证明：

1. $\mathbb{Q}$ 中每个 $\mathbb{Z}$ 的陪集，恰好有一个代表元 $q \in \mathbb{Q}$，满足 $q \in [0,1)$；
2. $\mathbb{Q}/\mathbb{Z}$ 中的每个元素都是有限阶，且对任意大正整数 n，都有元素的阶为 n；
3. $\mathbb{Q}/\mathbb{Z}$ 是 $\mathbb{R}/\mathbb{Z}$ 的挠子群；【挠子群的定义见“子群”一节的习题】
4. $\mathbb{Q}/\mathbb{Z}$ 同构于 $\mathbb{C}^\times$ 上的单位根群. 【单位根群的定义见“基本概念”一节的例题】

✍ **练习 1.156** 设 A, B 是群. 证明：$N = \{(a,1) : a \in A\}$ 是 $A \times B$ 的正规子群，且 $(A \times B)/N \simeq B$.

✍ **练习 1.157** 设 A 是交换群，$D = \{(a,a) : a \in A\}$. 证明：$D \lhd A \times A$，且 $(A \times A)/D \simeq A$.

✍ **练习 1.158** 设 $D = \{(a,a) : a \in S_3\}$. 证明：$D$ 不是 $S_3 \times S_3$ 的正规子群.

✍ **练习 1.159** 设 $C \lhd A$ 且 $D \lhd B$. 证明：

1. $(C \times D) \lhd (A \times B)$；
2. $(A \times B)/(C \times D) \simeq (A/C) \times (B/D)$.

注 提示：定义映射

$$\varphi: A \times B \to (A/C) \times (B/D)$$
$$(a,b) \mapsto (aC, bD).$$

✍ **练习 1.160** 设 M, N 是 G 的正规子群，且满足 $G = MN$. 证明：$G/(M \cap N) \simeq (G/M) \times (G/N)$.

注 提示：定义映射

$$\varphi: G \to (G/M) \times (G/N)$$
$$mn \mapsto (nM, mN).$$

✍ **练习 1.161** 设 p 是素数，$G = \{z \in \mathbb{C} : z^{p^n} = 1 \text{ for some } n \in \mathbb{Z}_+\}$. 证明：映射 $z \mapsto z^p$ 是满同态.

✍ **练习 1.162** 设 N 是群 G 的正规子群，且 $N < M < G$，证明：

$$N_G(M)/N = N_{\bar{G}}(\bar{M})$$

其中 $\bar{G} = G/N$, $\bar{M} = M/N$.

注 定义映射：$\varphi: N_G(M) \to N_{\bar{G}}(\bar{M})$, $g \mapsto gN$. 我们需要证明：

1. φ 是良定义的，即若 $g \in N_G(M)$，则 $gN \in N_{\bar{G}}(\bar{M})$.

2. φ 是满射.
3. φ 是群同态.
4. $\ker\varphi = N$.

1.7.6 拓展

1.7.6.1 Hall 子群

我们称有限群 G 的子群 H 为 G 的 Hall 子群，如果 H 的指数和阶互素. 例如在循环群 $\mathbb{Z}_6$ 中，子群 $\mathbb{Z}_2$ 为 Hall 子群，因为他的指数为 3，而阶为 2.

✍ **练习 1.163** 设 H 是 G 的 Hall 子群，$N \lhd G$. 证明：

1. $H \cap N$ 是 N 的 Hall 子群；
2. HN/N 是 G/N 的 Hall 子群.

证明

1. 因为 $N \lhd G$，所以 $HN = NH$，从而 HN 是 G 的子群. 于是 $|HN| = |H||N|/|H \cap N|$ 整除 $|G|$，即 $|HN|/|H| = [N : H \cap N]$ 整除 $|G|/|H| = [G : H]$.
   又因为 $H \cap N$ 是 H 的子群，从而 $|H \cap N|$ 整除 $|H|$.
   由于 H 是 G 的 Hall 子群，于是 $\gcd(|H|, [G : H]) = 1$，由此得到 $\gcd(|H \cap N|, [N : H \cap N]) = 1$. 即 $H \cap N$ 是 N 的 Hall 子群.
2. 由第三同构定理：$[G/N : HN/N] = [G : HN]$，而由第二同构定理：$[G : HN] = [G : H]/[N : H \cap N]$，所以 $[G/N : HN/N] = [G : H]/[N : H \cap N]$.
   由第二同构定理：$|NH/N| = |H|/|H \cap N|$.
   由于 H 是 G 的 Hall 子群，于是 $(|H|, [G : H]) = 1$，由此得到 $(|H|/|H \cap N|, [G : H]/[N : H \cap N]) = 1$，即 $(|NH/N|, [G/N : HN/N]) = 1$，从而 HN/N 是 G/N 的 Hall 子群.

笔记 看到题设中的 $H \cap N$，HN/N 等形式，我们就要有意识地联想到第二、第三同构定理.

✍ **练习 1.164** 设 p 是素数，群 G 的阶为 $p^a m$，其中 $p \nmid m$. 设 P 是 G 的 p^a 阶子群，N 是 G 的 $p^b n$ 阶正规子群，其中 $p \nmid n$. 证明：$|P \cap N| = p^b$，且 $|PN/N| = p^{a-b}$.

证明 因为 $|P| = p^a$，$[G : P] = m$，而 $p \nmid m$ 且 p 为素数，从而 $\gcd(m, p) = 1$，也就是说，P 是 G 的 Hall 子群. 由前一题的结论可知，$P \cap N$ 是 N 的 Hall 子群，即 $(|P \cap N|, |N : P \cap N|) = 1$.

因为 $P \cap N < P$，所以 $|P \cap N|$ 只能为 p 的幂. 若 $|P \cap N| = p^i < p^b$，则 $\gcd(|P \cap N|, |N : P \cap N|) \geqslant p$，矛盾！从而只能有 $|P \cap N| = p^b$.

第二小问利用第二同构定理即得.

1.7.6.2 交换子的简单性质

对于群 G 的元素 x, y，定义 x, y 的交换子 $[x, y] = x^{-1}y^{-1}xy$.（有的教科书会定义为 $xyx^{-1}y^{-1}$，读者通过后面的练习可以理解，两种定义虽然不同，但是本核心思想是一致的）

我们先看定义交换子的意义：

✍ **练习 1.165** 证明：

1. $xy = yx[x, y]$；
2. x, y 交换，当且仅当 $[x, y] = 1$.

✍ **练习 1.166** 设 $N \lhd G$，$\bar{G} = G/N$. 证明：$\bar{x}, \bar{y}$ 交换，当且仅当 $[x, y] \in N$. 特别的，G/N 为交换群，当且仅当 $G' < N$.

✍ **练习 1.167*** 证明：$G' = \langle [x, y] : x, y \in G \rangle$ 是 G 的正规子群，且 G/G' 是交换群.

证明

1. 只需证：对任意的 $x,y\in G$ 和任意的 $g\in G$，有 $g[x,y]g^{-1}\in G'$.
   我们有：
$$\begin{aligned} g[x,y]g^{-1} &= gx^{-1}y^{-1}xyg^{-1} \\ &= gx^{-1}(g^{-1}g)y^{-1}(g^{-1}g)x(g^{-1}g)yg^{-1} \\ &= (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) \\ &= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) \\ &= [gxg^{-1},gyg^{-1}]\in G' \end{aligned}$$
2. 对任意的 $\bar{x},\bar{y}\in G/G'$，因为 $[x,y]\in G'$，所以由上一题的结论可知，$\bar{x},\bar{y}$ 交换.

另一方面，通过简单观察就可以发现，交换子的形式非常有趣：$x^{-1}y^{-1}xy=(x^{-1}y^{-1}x)y=x^{-1}(y^{-1}xy)$，它同时包含了 x 和 y 的共轭形式，这一点往往是我们探究其性质的突破口.

✍ **练习 1.168*** 设 $H,K\lhd G$，$H\cap K=\{1\}$. 证明：对任意 $x\in H$ 与任意 $y\in K$，有 $xy=yx$.

证明 [1] 对任意的 $x\in H,y\in K$，有 $xy\in xK=Kx$，所以存在 $y'\in K$，使得 $xy=y'x$. 又 $y'x\in y'H=Hy'$，所以存在 $x'\in H$，使得 $xy=y'x=x'y'$. 进一步的，我们有
$$y(y')^{-1}=x^{-1}x'$$
左式属于 K，右式属于 H，从而 $y(y')^{-1}=x^{-1}x'\in H\cap K=\{1\}$，即 $y(y')^{-1}=x^{-1}x'=1$. 求得 $x=x',y=y'$，所以 $xy=y'x=yx$.

证明 [2] 一方面，由于 $x^{-1}y^{-1}x\in x^{-1}Kx=Kx^{-1}x=K$，所以 $x^{-1}y^{-1}xy=(x^{-1}y^{-1}x)y\in K$. 另一方面，$y^{-1}xy\in y^{-1}Hy=Hy^{-1}y=H$，所以 $x^{-1}y^{-1}xy=x^{-1}(y^{-1}xy)\in H$. 从而 $x^{-1}y^{-1}xy\in K\cap H$，即 $x^{-1}y^{-1}xy=1$，从而得到 $xy=yx$.

✍ **练习 1.169** 设 $H,K\lhd G$，且 H,K 均为有限群，它们的阶互素. 证明：对任意 $x\in H$ 与任意 $y\in K$，有 $xy=yx$.

注 提示：考虑 $|H\cap K|$ 的阶.

✍ **练习 1.170** 设 $N\lhd G$，$N\cap G'=\{1\}$，证明：$N<Z(G)$.

注 提示：对任意的 $n\in N$ 和 $g\in G$，有 $n^{-1}g^{-1}ng\in G'$，且 $n^{-1}(g^{-1}ng)\in N$.

第 2 章 环论

2.1 环

2.1.1 课前思考

1. 集合
$$R=\left\{\begin{pmatrix}a & 0\\ 0 & b\end{pmatrix}:\ a,b\in\mathbb{Z}\right\}$$
连同矩阵的加法和乘法构成交换环.（T/F）
2. 设集合 $S=\{0,3,6,9,12\}$，定义 S 上的加法和乘法运算，为 $\mathbb{Z}_{15}$ 上的加法和乘法运算，则 $(S,+,\cdot)$ 为域.（T/F）
3. 下列说法中正确的有（　　）：
A. 环 R 中，加法幺元 0 和乘法幺元 1 是不同的元素.
B. 存在一个不少于三个元素的环，其中不是 0 和 1 的元素都是零因子.
C. 存在一个环，其中不是 0 的元素都是单位.
D. 存在一个环，使得一个元素既是零因子，又是单位.
4. 环 $\mathbb{Z}[\sqrt{-1}]$ 中有____ 个单位.
5. 环 $(\mathbb{Z}_{10},+,\cdot)$ 的单位有____；零因子有____；子环有____.
6. 设环 R 有左消去律 (即对任意的 $a\in R^*$ 和 $b,c\in R$, 若 $ab=ac$, 则 $b=c$), 则下列说法中不正确的有（　　）：
A. 右消去律也成立.
B. R 中非零元都有乘法逆.
C. R 中没有零因子.
D. R 中非零元对加法的阶都一样.

解

1. T.
2. T. S 是交换环. 6 是 S 的乘法幺元，$3,12$ 互为乘法逆，9 的乘法逆是其自身，所以 S 是域.
3. BC.
A 选项：零环 $\{0\}$ 中加法和乘法幺元是同一个.
B 选项：考虑环的直积 $\mathbb{Z}_2\times\mathbb{Z}_2$，其中 $(1,0),(0,1)$ 都是零因子.
C 选项：任意一个的域都满足这一命题.
D 选项：假设 $u\in R$ 是单位，且存在 $v\in R$，使得 $uv=0$，从而 $u^{-1}uv=0$，即 $v=0$. 从而 u 不是零因子.
4. 4：环 $\mathbb{Z}[\sqrt{-1}]$ 中的单位恰为范数等于 1 的元素，从而有 4 个：$\pm1,\pm\sqrt{-1}$.（参见“二次域”一节）
5. 单位：$1,3,7,9$；零因子：$2,4,5,6,8$；子环：$\mathbb{Z}_{10}$（本书的子环要求继承父结构中的乘法幺元，更详细地解释请阅读后文）.
6. B.
先证明：R 中没有零因子. 对任意的 $a,b\in R$，若 $ab=0$，则 $ab=a0$. 此时，如果 $a\neq0$，利用左消去律可得 $b=0$. 从而 $ab=0$，可得 $a=0$ 或 $b=0$. 从而 R 中没有零因子. 由此马上判断选项 A, C 正确.
选项 B 错误，考虑整环 $\mathbb{Z}$，其中 2 不是零因子，但也没有乘法逆.
对于选项 D. 先证明：对任意 R 的元素 $r,s\neq0$，以及正整数 n，若 $n\cdot r=0$（$n\cdot r$ 即 n 个 r 相加），则 $n\cdot s=0$. 我们有：
$$0=n\cdot r=(n\cdot1)r$$

由于 $r \neq 0$，所以由消去律可得：$n \cdot 1 = 0$，于是：

$$n \cdot s = (n \cdot 1)s = 0s = 0.$$

从而，若 $|r| = n$，则必有 $|s| = n$，否则，如果 $|s| = m < n$，则也会有 $m \cdot r = 0$，于是 $n = |r| \leqslant m$，矛盾！$m > n$ 的情况类似可证. 此外，若 $|r| = \infty$，则同样有 $|s| = \infty$. 综上，R 中所有的非零元，加法阶必须一致，D 选项正确.

2.1.2 知识要点

（一）基本概念与运算性质

1. 环 $(R, +, \cdot)$：集合 R 与其上的二元运算 $+, \cdot$，且满足：
   (a). $(R, +)$ 是交换群；
   (b). $(R, \cdot)$ 是幺半群；
   (c). （乘法分配律）：对任意的 $a, b, c \in R$ 有

$$(a + b)c = ac + bc$$

$$c(a + b) = ca + cb$$

   则称 R 为环.（其中一个元素 a 的加法逆记为 $-a$，乘法逆（如果存在的话）记为 a^{-1}.）
   （注：在本书与 Maki 的抽代讲义中，我们始终约定，所谓的环是“含幺环”，即 R 中一定有乘法幺元，不同的书对此有不同的处理方式，请读者留意.）
2. （环的运算性质）：设 R 是环，则
   (a). 对任意的 $a \in R$，有 $0a = a0 = 0$；
   (b). 对任意的 $a, b \in R$，有 $(-a)b = a(-b) = -(ab)$；
   (c). 对任意的 $a, b \in R$，有 $(-a)(-b) = ab$；
   (d). 对任意的 $a \in R$，有 $-a = (-1)a$.

（二）环中的特殊元素

1. 有左逆的元素：对于环 R 中的元素 a，存在 $b \in R$，使得 $ba = 1$.
   有右逆的元素：对于环 R 中的元素 a，存在 $b \in R$，使得 $ab = 1$.
   单位：环 R 中有乘法逆元的元素.（其全体记为 $R^\times$）
2. 左零因子：对于环 R 中的非零元素 a，存在非零的 $b \in R$，使得 $ab = 0$.
   右零因子：对于环 R 中的非零元素 a，存在非零的 $c \in R$，使得 $ca = 0$.
   左零因子和右零因子统称零因子.
   （注：有的教材不要求零因子非零.）

（三）特殊的环

1. 整环：R 是交换环，且没有零因子.
   （注：有些比较久远的教材中，整环不要求满足乘法交换性.）
2. （乘法消去律）：设 a, b, c 是环 R 的元素，且 a 不是零因子. 若 $ab = ac$，则 $a = 0$ 或 $b = c$.（$ba = ca$ 同理）
   特别的，设 a, b, c 是整环 R 的元素，若 $ab = ac$，则 $a = 0$ 或 $b = c$.（$ba = ca$ 同理）
3. 斜域（或称为除环、体）：R 是环，且 $(R^*, \cdot)$ 是群.
4. 域：R 是环，且 $(R^*, \cdot)$ 是交换群.
5. （有限整环）：任意有限的整环都是域.
6. 子环：我们称 $(S, +, \cdot)$ 是 $(R, +, \cdot)$ 的子环（记作 $S < R$），如果满足

(a). $S \subset R$;

(b). $(S,+) < (R,+)$;

(c). S 对于乘法封闭，且 $1 \in S$.

7. 环 $R_1, \cdots, R_n$ 的直积：集合

$$R_1 \times \cdots \times R_n := \{(r_1, \cdots, r_n) : r_1 \in R_1, \cdots, r_n \in R_n\}.$$

其上的加法和乘法定义为按分量做对应的计算：

$$(r_1, \cdots, r_n) + (r_1', \cdots, r_n') := (r_1 + r_1', \cdots, r_n + r_n')$$
$$(r_1, \cdots, r_n)(r_1', \cdots, r_n') := (r_1 r_1', \cdots, r_n r_n').$$

（四）环的例子

1. $M_n(R)$：分量是 R 的元素的 $n \times n$ 的矩阵全体，连同矩阵的加法和乘法构成环.
2. （矩阵环的单位）：$M_n(R)^\times = GL_n(R)$.

2.1.3 知识要点解读

（一）环的运算性质

虽然环有两个二元运算，比群要复杂，但是由于我们从小学习四则运算，所以反而对有两种运算的环感到更为习惯一些.

问题 2.1 （环的运算性质）：设 R 是环，则

1. 对任意的 $a \in R$，有 $0a = a0 = 0$;
2. 对任意的 $a, b \in R$，有 $(-a)b = a(-b) = -(ab)$;
3. 对任意的 $a, b \in R$，有 $(-a)(-b) = ab$;
4. 对任意的 $a \in R$，有 $-a = (-1)a$.

证明

1. 对任意的 $a \in R$，有：

$$\begin{aligned} 0a + 0a &= (0+0)a && \text{(乘法分配律)} \\ &= 0a && \text{(加法幺元)} \end{aligned}$$

所以由加法群的消去律可得：$0a = 0$，同理可证 $a0 = 0$.

2. 对任意的 $a, b \in R$，有：

$$\begin{aligned} (-a)b + ab &= (-a+a)b && \text{(乘法分配律)} \\ &= 0b && \text{(加法逆)} \\ &= 0 \end{aligned}$$

从而由加法逆的唯一性可知：$(-a)b = -(ab)$，同理可证 $a(-b) = -(ab)$.

3. 对任意的 $a, b \in R$，有

$$\begin{aligned} (-a)(-b) + (-a)b &= (-a)(-b+b) && \text{(乘法分配律)} \\ &= (-a)0 \\ &= 0 \end{aligned}$$

所以 $(-a)(-b)$ 是 $(-a)b$ 的加法逆. 而上一小题我们已经证明：$(-a)b$ 的加法逆是 ab，从而由逆的唯一性可得 $(-a)(-b) = ab$.

4. 对任意的 $a \in R$，有

$$\begin{aligned} a+(-1)a &= 1a+(-1)a && \text{(乘法幺元的性质)} \\ &= (1+(-1))a \\ &= 0a \\ &= 0 \end{aligned}$$

而 a 的加法逆为 $-a$，从而有 $-a=(-1)a$.

笔记 这一证明中多次利用的，是群中元素的逆的唯一性. 大家在学习环论的时候，不要把群论的知识，都还给老师了哟.

练习 2.1 在环 R 中，证明：

1. $(-1)^2=1$；
2. 若 $u \in R^\times$，则 $-u \in R^\times$.

证明

1. 我们有：

$$(-1)^2 = 1 \cdot 1 = 1$$

2. 我们有：

$$(-u)(-u^{-1}) = uu^{-1} = 1$$

所以 $-u \in R^\times$.

（二）环中的特殊元素与特殊的环

我们知道，环 R 对于乘法运算而言是幺半群，而且其中还包含了加法幺元 0，所以我们会关心两类特殊的方程：$ab=1$，或者 $ab=0$.

针对 $ab=1$ 的讨论，我们在幺半群的部分已经有所涉猎. 这里我们更明确的引入了单侧逆的概念. 根据环中元素逆的存在特性，我们给出了两类特殊的环：斜域和域，区分两者的是乘法是否满足交换律.

针对 $ab=0$ 的讨论，则是比较新颖的内容，初学者可能一时对于零因子没有很直观的认识，因为我们熟悉的各种数集，连同加法和乘法，绝大多数都是整环起步. 即使对于不是整环的 $\mathbb{Z}_n$（n 是合数），它也是交换环，从而零因子没有左右的区分. 实际上，存在这样的环，其中有一个元素，它是左零因子却不是右零因子；类似的，存在这样的环，其中有两个元素 a,b，满足 $ab=1$ 且 $ba \neq 1$. 请看以下几个例子.

例题 2.1 在 2 阶实方阵环 $M_2(\mathbb{R})$ 中，取

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 1 & -1 \end{pmatrix}$$

则：

$$AB = 0, \quad BA = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}$$

例题 2.2 定义集合

$$R = \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} : x,z \in \mathbb{Z}, y \in \mathbb{Z}_2 \right\}$$

容易验证 R 连同矩阵的加法和乘法构成环.

考虑元素

$$a := \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$$

则 a 是左零因子，因为：

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & \bar{1} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

但是 a 不是右零因子，因为对任意 R 中的元素有：

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2x & y \\ 0 & z \end{pmatrix}$$

如果想让计算结果等于零矩阵，则只能有 $x = y = z = 0$，此时 a 左乘的是零矩阵.

例题 2.3 定义 $\mathbb{R}$ 上无穷序列集合 $\mathbb{R}^\infty := \{(x_1, x_2, \cdots) : x_i \in \mathbb{R}\}$，并且定义映射集合

$$R := \{f : \mathbb{R}^\infty \to \mathbb{R}^\infty\}$$

可以证明，R 连同映射的加法和复合构成环.

取 R 中的两个元素：

$$f : (x_1, x_2, \cdots) \mapsto (0, x_1, x_2, \cdots)$$
$$g : (x_1, x_2, \cdots) \mapsto (x_2, x_3, \cdots)$$

则

$$gf : (x_1, x_2, \cdots) \mapsto (x_1, x_2, \cdots)$$
$$fg : (x_1, x_2, \cdots) \mapsto (0, x_2, x_3, \cdots)$$

也就是 $gf = 1$（恒等映射）而 $fg \neq 1$.

进一步考察可以发现，f 永远不可能是左逆，因为对任意的 $h \in R$，不论 h 将定义域中的元素映成什么象，f 总会进一步将这个象映成第一分量为零的元素，而 $\mathbb{R}^\infty$ 一定有第一分量不为零的元素，从而 fh 不等于 1.

类似地，g 也不可能是右逆，请读者自己写出这一结论的证明.

笔记 我们反复强调过，不论是群的运算，还是环的乘法，都不一定满足交换性. 然而，回顾我们接触过的所有二元运算，不满足交换性的实际上只有一类：映射的复合运算（矩阵乘法、置换乘法均属于特殊映射的复合运算）. 所以当我们需要非交换的例子时，各种映射集就是我们唯一的选择.

练习 2.2 试举一例说明：在含幺环中，一个右可逆元可以有多于一个右逆.

注 提示：利用前一例.

由于环 R 对于加法而言是交换群，所以对于加法也成立消去律，即已知 $a + b = a + c$ 可得 $b = c$. 而乘法的消去律是比较麻烦的，一般的我们总是要考虑零因子以及 0 的特殊情况，这一点在中学阶段的代数训练中经常作为易错点出现，例如下面的经典问题.

例题 2.4 在实数域内，已知

$$\frac{x+y}{z} = \frac{y+z}{x} = \frac{z+x}{y} = k$$

试求 k 的值.

解 由题设条件可得：

$$x + y = kz$$
$$y + z = kx$$
$$z + x = ky$$

三式相加有 $2(x + y + z) = k(x + y + z)$.

1. 若 $x + y + z \neq 0$，则 $k = 2$.
2. 若 $x + y + z = 0$，则 $x + y = -z$，于是 $k = -1$.

综上，$k = 2$ 或 -1.

笔记 相信大家不会因为没有注意到 $x + y + z = 0$ 的情况，从而漏掉 $k = -1$ 这个解. 笔者想借此题唤醒大家对

于零的注意. 同时，在环中，一旦考虑乘法，不但要注意零，还要注意有弱化版零的性质的零因子.

问题 2.2（乘法消去律）：设 a,b,c 是环 R 的元素，且 a 不是零因子. 若 $ab=ac$，则 $a=0$ 或 $b=c$.

证明 我们对 $ab=ac$ 做代数变形：

$$\begin{aligned} ab &= ac \\ ab-ac &= 0 && \text{(加法运算的逆)} \\ a(b-c) &= 0 && \text{(乘法分配律)} \end{aligned}$$

若 $a=0$，则命题成立. 若 $a\neq 0$，则 $b-c$ 必须为 0（否则 a 是零因子，矛盾!），命题亦成立.

笔记 我们在有理数或实数的代数变形中，经常用到一个结论：若 $xy=0$，则 $x=0$ 或 $y=0$. 但是在环里一般不成立. 事实上，由于有理数集和实数集都是域，从而没有零因子，所以由本例的证明保证了该结论的正确性.

我们很容易能从其他的环中找出这一结论不成立的例子. 例如，在环 $\mathbb{Z}_6$ 中，$\bar{2}\bar{3}=\bar{0}$. 能找到这样的元素，是因为 $\mathbb{Z}_6$ 连整环也不是.

问题 2.3* （有限整环）：任意有限的整环 R 都是域.

证明 设 R 是有限整环，$a\in R^*$，定义映射：

$$\begin{aligned} f: R &\to R \\ x &\mapsto ax \end{aligned}$$

先证明：f 是双射.

对任意的 $x,y\in R$，若 $ax=ay$，则由消去律可知 $x=y$. 从而 f 是单射，即 $|f(R)|\geqslant|R|$. 同时我们很自然地有 $f(R)\subset R$，即 $|f(R)|\leqslant|R|$，从而 $|f(R)|=|R|$. 另一方面，由于 R 是有限集，所以 $f(R)=R$，从而 f 是满射. 于是 f 为双射.

因为 f 是双射，所以对于 $1\in R=f(R)$，存在 $y\in R$，使得 $1=f(y)=ay$，即 a 是单位. 这说明，R^* 中的每个元素都是 R 的单位，从而 R 为域.

笔记 同样的技巧，我们在证明“满足消去律的有限半群是群”这一命题时，已经使用过一次了.

练习 2.3* 有限环 R 若没有零因子，则 R 是斜域.

注 证明思路与前面的例题一致.

进一步地，我们有 Wedderburn 定理：有限斜域必是域.（证明需要用到分圆多项式，我们在抽代一的部分不需要掌握）于是，我们发现，有限环的情况非常简单：

1. 有零因子
2. 无零因子：此时只能为域.

（三）环、子环的定义

目前有两个版本的环定义，狭义上要求环包含乘法幺元，广义上则不做要求. 应该说，不论采用哪一种定义，环论在整体上是没有什么变化的，只是有一些细节会有所区别. 虽然本书（连同 Maki 的讲义）采用狭义定义，不过由于市面上许多流行的教材采用广义定义，因此本书会在有区别的部分做出说明，这里我们着重说明一个概念：子环.

我们回忆子群、子幺半群的定义（包括我们在线性代数里学过的子空间），可以发现，定义子结构的逻辑内涵都是一致的：

1. 元素视角：子集；
2. 运算视角：继承父结构的运算和基本特性（例如封闭性、结合律、幺元、逆等等）.

例如对于子群的定义：$H<G$

1. 元素视角：$H\subset G$；
2. 运算视角：H 上的加法运算继承于 G，且有同样的封闭性、结合律、幺元（从而 $1_H=1_G$）、逆.

回到子环上，对应于狭义的环定义，我们可以这样定义子环：$S < R$

1. 元素视角：$S \subset R$；
2. 运算视角：
   (a). 加法：S 继承 R 的加法，且有同样的封闭性、结合律、交换律、加法幺元（从而 $0_S = 0_R$）、加法逆；
   (b). 乘法：S 继承 R 的乘法，且有同样的封闭性、结合律、乘法幺元（从而 $1_S = 1_R$）.

如果我们使用广义的环定义（即不要求乘法幺存在），则定义子环：$S < R$

1. 元素视角：$S \subset R$；
2. 运算视角：
   (a). 加法：S 继承 R 的加法，且有同样的封闭性、结合律、交换律、加法幺元（从而 $0_S = 0_R$）、加法逆；
   (b). 乘法：S 继承 R 的乘法，且有同样的封闭性、结合律.

我们用一个例子来说明，两个版本的子环定义的微妙区别：

例题 2.5 考虑环 $(\mathbb{Z}_{10}, +, \cdot)$，按照狭义定义，子环有一个：$\mathbb{Z}_{10}$ 自身.

按照广义定义，子环有四个：$\{0\}, \mathbb{Z}_{10}, \{0,2,4,6,8\}, \{0,5\}$. 考察子环 $S = \{0,2,4,6,8\}$（连同加法、乘法），其中并没有包括 $\mathbb{Z}_{10}$ 中的乘法幺元 1，但是这并不意味着 S 中没有乘法幺元. 事实上，我们有

$$0 \cdot 6 = 0 = 6 \cdot 0$$
$$2 \cdot 6 = 2 = 6 \cdot 2$$
$$4 \cdot 6 = 4 = 6 \cdot 4$$
$$6 \cdot 6 = 6 = 6 \cdot 6$$
$$8 \cdot 6 = 8 = 6 \cdot 8$$

从而 6 是 S 中的乘法幺元.

于是，如果采用广义定义，子环中可以没有乘法幺元，也可以有乘法幺元；有乘法幺元时，它可以继承于父结构（例如 $\mathbb{Z}_{10}$ 之于 $\mathbb{Z}_{10}$），也可以不继承（例如 S 之于 $\mathbb{Z}_{10}$）.

同时，在 $\mathbb{Z}_{10}$ 中，$2,4,6,8$ 都是零因子，但是在 S 中，$2,4,6,8$ 都是单位，其中 $2,8$ 互为乘法逆，4 的乘法逆是其自身，6 是乘法幺元.

2.1.4 典型例题

（一）环的例子

例题 2.6 设 $(G, +)$ 为交换群，$\mathrm{End}(G)$ 为 G 的所有自同态构成的集合. 定义 $\mathrm{End}(G)$ 上的运算：对任意的 $x \in G$，定义

$$(f+g)(x) := f(x) + g(x)$$
$$(fg)(x) := f(g(x))$$

证明：$(\mathrm{End}(G), +, \cdot)$ 为环.

证明 先证明：$(\mathrm{End}(G), +)$ 为交换群.

1. 加法封闭性：对任意的 $f, g \in \mathrm{End}(G)$ 和 $x \in G$，有 $(f+g)(x) = f(x) + g(x) \in G$，从而 $f + g : G \to G$. 并且，对任意的 $x, y \in G$，有：

$$\begin{aligned}(f+g)(x+y) &= f(x+y) + g(x+y) \\ &= f(x) + f(y) + g(x) + g(y) \\ &= f(x) + g(x) + f(y) + g(y) \\ &= (f+g)(x) + (f+g)(y)\end{aligned}$$

从而 $f+g$ 是群同态，即 $f + g \in \mathrm{End}(G)$.

2. 加法结合律：对任意的 $f,g,h\in \mathrm{End}(G)$ 和 $x\in G$，有：

$$\begin{aligned}((f+g)+h)(x)&=(f+g)(x)+h(x)\\&=(f(x)+g(x))+h(x)\\&=f(x)+(g(x)+h(x))\\&=f(x)+(g+h)(x)\\&=(f+(g+h))(x)\end{aligned}$$

从而 $(f+g)+h=f+(g+h)$.

3. 加法幺元：考虑 G 上的平凡映射

$$\begin{aligned}e:G&\to G\\x&\mapsto 0_g\end{aligned}$$

其中 0_g 是 G 中的幺元. 先证明：$e\in \mathrm{End}(G)$. 对任意的 $x,y\in G$，有：

$$\begin{aligned}e(x+y)&=0_g\\&=0_g+0_g\\&=e(x)+e(y)\end{aligned}$$

从而 $e\in \mathrm{End}(G)$.

再证明：e 是 $\mathrm{End}(G)$ 的加法幺元. 对任意的 $f\in \mathrm{End}(G)$ 和 $x\in G$，有：

$$\begin{aligned}(f+e)(x)&=f(x)+e(x)\\&=f(x)+0_g\\&=f(x)\\&=0_g+f(x)\\&=e(x)+f(x)\\&=(e+f)(x)\end{aligned}$$

从而 $f+e=f=e+f$.

4. 加法逆：对任意的 $f\in \mathrm{End}(G)$，定义映射

$$\begin{aligned}-f:G&\to G\\x&\mapsto -f(x)\end{aligned}$$

下证：$-f\in \mathrm{End}(G)$. 对任意的 $x\in G$，有：

$$\begin{aligned}(f+(-f))(x)&=f(x)+(-f)(x)\\&=f(x)+(-f(x))\\&=0_g\\&=e(x)\\((-f)+f)(x)&=(-f)(x)+f(x)\\&=(-f(x))+f(x)\\&=0_g\\&=e(x)\end{aligned}$$

从而 $f+(-f)=e=(-f)+f$.

5. 加法交换律：对任意的 $f,g\in \mathrm{End}(G)$ 和 $x\in G$，有：

$$\begin{aligned}(f+g)(x)&=f(x)+g(x)\\&=g(x)+f(x)\\&=(g+f)(x)\end{aligned}$$

从而 $f+g=g+f$.

综上，$(\mathrm{End}(G),+)$ 为交换群.

再证明：$(\mathrm{End}(G),\cdot)$ 为幺半群.

1. 乘法封闭性：对任意的 $f,g\in \mathrm{End}(G)$ 和 $x\in G$，有 $(fg)(x)=f(g(x))\in G$，从而 $fg:G\to G$. 并且，对任意的 $x,y\in G$，有：

$$\begin{aligned}(fg)(x+y)&=f(g(x+y))\\&=f(g(x)+g(y))\\&=f(g(x))+f(g(y))\\&=fg(x)+fg(y)\end{aligned}$$

从而 fg 是群同态，即 $fg\in \mathrm{End}(G)$.

2. 乘法结合律：对任意的 $f,g,h\in \mathrm{End}(G)$ 和 $x\in G$，有：

$$\begin{aligned}((fg)h)(x)&=(fg)(h(x))\\&=f(g(h(x)))\\&=f((gh)(x))\\&=(f(gh))(x)\end{aligned}$$

从而 $(fg)h=f(gh)$.

3. 乘法幺元：考虑 G 上的恒等映射

$$\begin{aligned}1:G&\to G\\x&\mapsto x.\end{aligned}$$

先证明：$1\in \mathrm{End}(G)$. 对任意的 $x,y\in G$，有：

$$\begin{aligned}1(x+y)&=x+y\\&=1(x)+1(y)\end{aligned}$$

从而 $1\in \mathrm{End}(G)$.

再证明：1 是 $\mathrm{End}(G)$ 的乘法幺元. 对任意的 $f\in \mathrm{End}(G)$ 和 $x\in G$，有：

$$\begin{aligned}(f1)(x)&=f(1(x))\\&=f(x)\\&=1(f(x))\\&=(1f)(x)\end{aligned}$$

从而 $f1=f=1f$.

综上，$(\mathrm{End}(G),\cdot)$ 为幺半群. 结合前面的证明，我们有：$(\mathrm{End}(G),+,\cdot)$ 为环.

笔记 本题从技术角度而言，并不是难题，但是笔者仍然建议每一位初学者严格地证明一遍该命题. 这是因为本题的细节较多，如果读者对于相关基本概念不熟悉，或者做题时不小心，就很容易漏掉几个需要证明的结论.

所以虽然我们的解题指南并不面向考试，但是如果有机会笔者出一套抽象代数的测试卷，本题一定会入选. 而且笔者敢断言，此题拿满分的学生会非常少.

（二）环的代数变形

例题 2.7 证明：

1. 若 a 是环 R 中的单位，则 a 一定不是零因子；（从而域中没有零因子）
2. 若 a 是环 R 中的零因子，则 a 一定不是单位.

证明

1. 设存在非零的 $b\in R$，使得 $ab=0$（$ba=0$ 可类似求证），则有：
$$b=1b=(a^{-1}a)b=a^{-1}(ab)=a^{-1}0=0$$
矛盾！
2. 因为 a 是环 R 中的零因子，所以存在非零的 $b\in R$，使得 $ab=0$（$ba=0$ 可类似求证）. 设 a 是单位，则有：
$$b=1b=(a^{-1}a)b=a^{-1}(ab)=a^{-1}0=0$$
矛盾！

笔记 虽然两个小问的证明过程非常类似，但是待证命题不同，请读者留意.

练习 2.4 设 R 是环，$u\in R$. 证明：

1. u 是单位，当且仅当 u 有左逆和右逆.
2. 若 u 有右逆，则 u 不是右零因子.（类似地有：若 u 有左逆，则 u 不是左零因子.）
3. 若 u 有多于一个右逆，则 u 是左零因子.（类似地有：若 u 有多于一个左逆，则 u 是右零因子.）
4. 若 u 是左零因子，且有右逆，则 u 有多于一个右逆.（类似地有：若 u 是右零因子，且有左逆，则 u 有多于一个左逆.）
5. 若 u 有右逆，且不是左零因子，则 u 有唯一的右逆.（类似地有：若 u 是左零因子，且有右逆，则 u 有多于一个右逆.）
6. 若 R 是有限环，则每个有右逆的元素是单位.（类似地有：若 R 是有限环，则每个有左逆的元素是单位.）

证明

1. 一方面，当 u 是单位时，u^{-1} 既是 u 的左逆，也是右逆.
另一方面，设 $au=ub=1$，则 $a=aub=b$，从而 a 是 u 的乘法逆.【读者有没有对此感到熟悉？】
2. 设 $uv=1$，且设 $au=0$（$a\neq 0$），于是 $a=auv=0v=0$，矛盾！
3. 设 $ua=ub=1$，且 $a\neq b$，则 $u(a-b)=0$，即 u 为左零因子.
4. 设存在 $a,b\neq 0$，使得 $ua=0$，且 $ub=1$，则 $u(a+b)=1$，且 $a+b\neq b$，即 $a+b$ 为不同于 b 的右逆.
5. 设存在 $v\neq 0$，使得 $uv=1$. 假设 u 有不止一个右逆，则存在 $w\neq 0$ 且 $w\neq v$，使得 $uw=1$. 从而 $u(v-w)=0$，且 $v-w\neq 0$，即 u 是左零因子，矛盾！从而 u 有唯一的右逆.
6. 任取一有右逆的元素 u，由于 u 不是右零因子，所以 $au=bu$ 可推证 $a=b$，即 R 中的每个元素与 u 左乘的结果均不相同，由于 R 有限，所以即有 $|R|=|Ru|$. 从而对于 $1\in R$，存在 $v\in R$，使得 $1=vu$，即 u 有左逆. 于是由第一小问的结论可知，u 是单位. 命题得证.

2.1.5 习题

（一）环的例子

练习 2.5 设 $R=\{f:[0,1]\to\mathbb{R}\}$，证明：$R$ 连同函数的加法、乘法运算是一个交换群.
以下哪些集合（连同同样的运算）是 R 的子环？哪些集合除了没有乘法幺元外，满足其他所有环的公理？

1. $A=\{f\in R:f(q)=0,\forall q\in\mathbb{Q}\cap[0,1]\}$；
2. $B=\{f\in R:\ f$是多项式$\}$；
3. $C=\{f\in R:\ f$有有限个零点，或者$=0\}$；
4. $D=\{f\in R:\ \lim_{x\to 1_-}f(x)=0\}$；
5. $E=\{f=\sum_{n=0}^{\infty}a_n\sin(nx)+\sum_{m=0}^{\infty}b_m\cos(mx):x\in[0,1],a_i,b_j\in\mathbb{R},$只有有限个 a_i,b_j 不为零$\}$.

注 提示：证明 $(R,+,\cdot)$ 是环，可参考例题 2.6. 其中乘法幺元记为 $1:x\mapsto 1$.

1. A 没有乘法幺元，但满足其他环公理.
2. B 是 R 的子环.
3. C 是 R 的子环.（没有零点，也就是有 0 个零点，属于“有限个零点”的范畴）
4. D 没有乘法幺元，但满足其他环公理.（利用极限的运算性质，可以证明 D 对加法和乘法封闭）
5. E 是 R 的子环. 我们有：

$$\begin{aligned}\sin(mx)\cos(nx)&=\frac{1}{2}\sin((m+n)x)+\frac{1}{2}\sin((m-n)x)\\ \sin(mx)\sin(nx)&=-\frac{1}{2}\cos((m+n)x)+\frac{1}{2}\cos((m-n)x)\\ \cos(mx)\cos(nx)&=\frac{1}{2}\cos((m+n)x)+\frac{1}{2}\cos((m-n)x)\end{aligned}$$

由此可证 E 对乘法的封闭性.

✍ **练习 2.6** 设 R 是整数序列 $(a_1,a_2,a_3,\cdots)$ 的集合，每个序列中只有有限个数不为零. 证明：R 连同按分量的加法和乘法，满足环的公理，除了没有乘法幺元.

注 提示：对于序列 $a=(a_1,a_2,a_3,\cdots),b=(b_1,b_2,b_3,\cdots)$，记 a 中不为零的分量的下标构成有限集 I，b 中不为零的分量的下标构成有限集 J，则 $a+b$ 中不为零的分量的下标包含于集合 $I\cup J$，ab 中不为零的分量的下标构成集合 $I\cap J$.

另外，与 R 中元素交换的元素，只能为全一序列 $(1,1,1,\cdots)$，但他不是 R 中的元素.

（二）子环

✍ **练习 2.7** 设 R 是环，S 是 R 的子环. 证明：若 u 是 S 的单位，则一定是 R 的单位. 举例说明，反之则不然.

注 提示：考虑 $\mathbb{Z}$ 和 $\mathbb{Q}$，2 在 $\mathbb{Q}$ 中是单位，但在 $\mathbb{Z}$ 中不是.

✍ **练习 2.8** 证明：任意多个环 R 的子环的交，仍然是 R 的子环.

注 提示：回顾子群、正规子群中类似命题的证明方式.

✍ **练习 2.9** 定义环 R 的中心

$$Z(R)=\{z\in R:\ zr=rz,\forall r\in R\}.$$

证明：

1. $Z(R)$ 是 R 的子环；
2. 若 R 是除环，则 $Z(R)$ 是域.

证明

1. 先证明：$Z(R)$ 是 R 的加法子群. 首先 $1\in Z(R)$（$1r=r1=r$）. 其次，对任意的 $s,t\in Z(R)$，和任意的 $r\in R$，有

$$\begin{aligned}(s-t)r&=sr-tr\\ &=rs-rt\\ &=r(s-t)\end{aligned}$$

从而 $s-t\in Z(R)$，即 $Z(R)$ 是 R 的加法子群.

再证明：$Z(R)$ 是乘法幺半群. 前面已经证明 $1\in Z(R)$. 对任意的 $s,t\in Z(R)$，和任意的 $r\in R$，有

$$\begin{aligned}(st)r&=s(tr)\\ &=srt\\ &=r(st)\end{aligned}$$

于是 $st\in Z(R)$. 从而 $Z(R)$ 是 R 的乘法幺半群.

综上，$Z(R)$ 是 R 的子环.

2. 先证明：若 $s\in Z(R)$，则 $s^{-1}\in Z(R)$. 对任意的 $r\in R$，若 $r=0$，则有 $s^{-1}r=0=rs^{-1}$. 若 $r\neq 0$，则有

$$\begin{aligned} s^{-1}r &= s^{-1}(r^{-1})^{-1} && (R\text{ 是除环，所以任意非零元素都有乘法逆.})\\ &= (r^{-1}s)^{-1}\\ &= (sr^{-1})^{-1} && (s\text{ 和 }R\text{ 中的任意元素都交换.})\\ &= rs^{-1} \end{aligned}$$

从而 $s^{-1}\in Z(R)$. 上一小题已经证明 $Z(R)$ 是环，于是 $Z(R)$ 是除环.

再证明：对任意的 $s,t\in Z(R)$，有 $st=ts$. 因为 s 和 R 中的任意元素都交换，所以 $st=ts$. 于是 $Z(R)$ 是域.

笔记 注意到在加法群中，对应于乘法群中 gh^{-1} 的元素应写作 $g-h$.

练习 2.10 取定环 R 中的元素 a，定义

$$C(a)=\{r\in R: ra=ar\}.$$

证明：

1. $C(a)$ 是 R 的子环，且包含 a；
2. $Z(R)=\cap_{a\in R}C(a)$；
3. 若 R 是除环，则 $C(a)$ 是除环.

注 提示：与前一题的思路基本一致.

（三）环中的特殊元素

练习 2.11 若 R 是整环，$x\in R$，$x^2=1$，证明：$x=\pm 1$.

证明 我们有：

$$\begin{aligned} 0 &= x^2-1\\ &= x^2-x+x-1\\ &= x(x-1)+(x-1)\\ &= (x+1)(x-1) \end{aligned}$$

由于 R 是整环，所以只能有 $x+1=0$ 或 $x-1=0$，即 $x=\pm 1$.

笔记 思路的来源是我们在实数域中学过的平方差公式，但是不可以直接在整环中使用，需要先证明. 因此在解答中干脆回归了最原始的添项法，以避免麻烦.（实际上添项也不复杂，思路是显然的.）

练习 2.12 证明：域的子环是整环.

注 提示：域中没有零因子.

练习 2.13 设 a 是环 R 中的非零元，证明：

1. a 不是左零因子，当且仅当对任意的 $b,c\in R$，有 $ab=ac\to b=c$.
2. a 不是右零因子，当且仅当对任意的 $b,c\in R$，有 $ba=ca\to b=c$.

证明 题中的两个待证结论显然具有对称性，我们只证明第一条.

一方面，设 a 不是左零因子. 对任意的 $b,c\in R$，若 $ab=ac$，则 $a(b-c)=0$. 由于 a 不是左零因子，所以若 $b-c\neq 0$，则 $a(b-c)\neq 0$，矛盾！从而 $b-c=0$，即 $b=c$.

另一方面，设对任意的 $b,c\in R$，若 $ab=ac$，则 $b=c$. 假设 a 是左零因子，则存在非零的 $u\in R$，使得 $au=0$. 于是对任意的 $x\in R$，有 $ax=a(x+u)$，从而 $x=x+u$，即 $u=0$，矛盾！所以 a 不是左零因子.

综上，原命题成立.

练习 2.14** 证明：R 是非零环，$u \in R$ 是单位，且 $v = u^{-1}$，当且仅当 $uvu = u$，R 的元素中只有 v 满足这一条件.

证明 一方面，若 $u \in R$ 是单位，且 $v = u^{-1}$，则 $uvu = (uv)u = 1u = u$. 设 $x \in R$ 满足条件 $uxu = u$. 则有

$$v(uxu) = vu$$
$$xu = 1$$

并且

$$(uxu)v = uv$$
$$ux = 1$$

于是 x 只能为 u 的乘法逆，即 $x = u^{-1} = v$. 于是 R 中只有 v 满足 $uvu = u$.

另一方面，我们需要证明："若 $uvu = u$，且 R 的元素中只有 v 满足这一条件，则 $u \in R$ 是单位，且 $v = u^{-1}$"

.

首先，假设 $u \in R$ 不是单位. 由于 $uvu = u$，所以有：

$$u(1 - vu) = 0$$
$$(1 - uv)u = 0$$

我们接下来讨论使两式成立的所有情况：

1. 若 $u = 0$，则对 R 中的任意元素 r，均有 $uru = 0 = u$，这与 v 的唯一性矛盾！
2. 下设 $u \neq 0$. 由于 u 不是单位，所以 $1 - vu, 1 - uv$ 不可能都为零（否则 $uv = vu = 1$，u 有乘法逆 v，矛盾！）.

   如果 $1 - uv \neq 0$，则由 $(1 - uv)u = 0$ 可得 $u(1 - uv)u = 0$，于是：

$$\begin{aligned} u &= u + 0 \\ &= uvu + u(1 - uv)u \\ &= u(v + 1 - uv)u \end{aligned}$$

   从而 R 中有两个不相同的元素 $x = v, v + 1 - uv$，满足 $uxu = u$，这与 v 的唯一性矛盾！

   类似地，如果 $1 - vu \neq 0$，则由 $u(1 - vu) = 0$ 可得 $u(1 - vu)u = 0$，于是：

$$\begin{aligned} u &= u + 0 \\ &= uvu + u(1 - vu)u \\ &= u(v + 1 - vu)u \end{aligned}$$

   从而 R 中有两个不相同的元素 $x = v, v + 1 - vu$，满足 $uxu = u$，这与 v 的唯一性矛盾！

综上，$u \in R$ 一定是单位.

其次，假设 $v \neq u^{-1}$，则 R 中有两个不相同的元素 $x = v, u^{-1}$，满足 $uxu = u$. 这与 v 的唯一性矛盾！由此可得，$u \in R$ 一定是单位，且 $v = u^{-1}$.

综合前面的证明，原命题得证.

笔记 本题的要点，在于找到不等于零的元素 r，满足 $uru = 0$，此时就可以构造出两个满足 $uxu = u$ 的元素 $x = v, v + r$. 实际上，若 u 有乘法逆，则满足 $uru = 0$ 的元素只有 $r = 0$.

练习 2.15** 证明：若 $1 - ab$ 是环 R 中的单位，则 $1 - ba$ 也是 R 中的单位.

证明 设 $1 - ab$ 的乘法逆是 r，从而

$$r - abr = 1 = r - rab$$

即

$$abr = r - 1 = rab$$

于是有：

$$\begin{aligned}(1-ba)(1+bra) &= 1-ba+bra-babra\\ &= 1-ba+bra-b(r-1)a\\ &= 1-ba+bra-bra+ba\\ &= 1\end{aligned}$$

且

$$\begin{aligned}(1+bra)(1-ba) &= 1+bra-ba-braba\\ &= 1+bra-ba-b(r-1)a\\ &= 1+bra-ba+ba-bra\\ &= 1\end{aligned}$$

即 $1-ba$ 的乘法逆为 $1+bra$，从而 $1-ba$ 是 R 中的单位.

注 本题是如何想到 $1+bra$ 这个元素的，笔者目前没有想明白.

✍ **练习 2.16*** 设 $r\in R$ 有多于一个右逆，证明：r 有无数个右逆.

（四）幂零元

环 R 中的元素 r 被称为是幂零的，如果存在正整数 m，使得 $r^m=0$.

✍ **练习 2.17** 设 $R=\mathbb{Z}_n$.

1. 若 $n=a^kb$，其中 a,k,b 均为整数，证明：$\overline{ab}$ 是幂零的；
2. 设 $a\in\mathbb{Z}$，证明：$\bar{a}\in R$ 是幂零的，当且仅当每个 n 的素因子，都是 a 的素因子.
3. 写出 $\mathbb{Z}_{72}$ 的全部幂零元.

证明

1. 因为 $(ab)^k=(a^kb)b^{k-1}=nb^{k-1}$，所以 $(ab)^k$ 是 n 的倍数，即 $\overline{(ab)^k}=\bar{0}$，从而
$$(\overline{ab})^k=\overline{(ab)^k}=\bar{0}.$$
2. 设 n 的素因子分解为
$$n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}.$$
其中任意 α_i 都是正整数，p_i 是素数. 记
$$\alpha:=\max\{\alpha_1,\cdots,\alpha_k\}.$$
一方面，若每个 n 的素因子，都是 a 的素因子，则 a 是 $p_1\cdots p_n$ 的倍数，不妨记为 $a=up_1\cdots p_n$，其中 u 为整数. 于是 $a^\alpha=u^\alpha(p_1\cdots p_n)^\alpha$，而 $(p_1\cdots p_n)^\alpha$ 是 n 的倍数，所以 a^α 是 n 的倍数，即 $(\bar{a})^\alpha=\overline{a^\alpha}=\bar{0}$.
另一方面，假设 n 有一个素因子不是 a 的素因子，不妨认为这个素因子是 p_1. 因为 $p_1\nmid a$，所以任意的 a 的幂次 a^m 都不能整除 p_1，从而 a^m 不可能整除 n，即 $\overline{a^m}\neq\bar{0}$，也就是说，$a$ 不是幂零的. 去逆否命题即得：若 a 是幂零的，则每个 n 的素因子，都是 a 的素因子.
综上，原命题得证.
3. $72=2^3\times3^2$，由上一小问的结论，$\mathbb{Z}_{72}$ 的幂零元必形如 $\overline{6k}$，其中 k 为整数，从而 $\mathbb{Z}_{72}$ 的全体幂零元为：
$$\{\overline{6k}:k\in\{0,1,\cdots,11\}\}.$$

✍ **练习 2.18** 设 $R=\{f:X\to F:F\text{为域}\}$. 证明：$R$ 中没有非零的幂零元.

证明 设 $f\neq0$ 是幂零元，则存在一点 $x\in X$，使得 $f(x)\neq0$，且存在正整数 m，使得 $f^m=0$. 于是必有 $(f(x))^m=0$. 下证：对任意的正整数 n，$(f(x))^n\neq0$.（从而矛盾！）

对 n 采用数学归纳法. 首先，当 $n=1$ 时，$(f(x))^n=f(x)\neq0$，命题得证.

假设当 $n=k$ 时，$(f(x))^n \neq 0$，则当 $n=k+1$ 时，有

$$(f(x))^n = f(x)(f(x))^k$$

由于 $f(x),(f(x))^k$ 都是域 K 中的元素，所以它们均不为零因子，于是二者的乘积不为零，命题得证.

综上，对任意的正整数 n，都有 $(f(x))^n \neq 0$.

✍ **练习 2.19** 证明：若 R 是整环，则 R 中的幂零元只有 0.

证明 设 $r \in R$ 是幂零的，则存在 $m \in \mathbb{Z}_+$，有 $r^m = 0$，也就是 $r \cdot r^{m-1} = 0$. 由于 R 是整环，所以必有 $r=0$，或 $r^{m-1}=0$. 如果 $r=0$，原命题得证；如果 $r^{m-1}=0$，重复前面的讨论. 由于 m 是一个有限的整数，所以这样的讨论不可能无限持续下去，最终我们将得到 $r=0$.

✍ **练习 2.20** 设 x 是交换环 R 的幂零元，证明：

1. $x=0$，或 x 是零因子；
2. 对任意的 $r \in R$，rx 都是幂零元；
3. $1+x$ 是 R 的单位；
4. 若 u 是 R 的单位，则 $u+x$ 是 R 的单位.

证明

1. 当 $x=0$ 时，x 显然为幂零元 $(x^1 = x = 0)$. 下设 $x \neq 0$. 由于 x 幂零，所以存在正整数 m，使得 $x^m = 0$. 记 $A = \{n \in \mathbb{Z}_+ : x^n = 0\}$，由于 A 非空，且为 $\mathbb{N}$ 的子集，所以必有最小元，不妨仍记为 m，于是 $xx^{m-1}=0$，且 $x^{m-1} \neq 0$，从而 x 是零因子.
2. 由于 x 幂零，所以存在正整数 m，使得 $x^m = 0$，于是
$$(rx)^m = r^m x^m = r^m 0 = 0.$$
3. 由于 x 幂零，所以存在正整数 m，使得 $x^m = 0$. 又因为
$$\begin{aligned} -1 &= x^{2m} - 1 \\ &= (x^2-1)(x^{2(m-1)} + x^{2(m-2)} + \cdots + 1) \\ &= (x+1)(x-1)(x^{2(m-1)} + x^{2(m-2)} + \cdots + 1) \\ &:= (x+1)p(x) \end{aligned}$$
于是 $(x+1)(-p(x)) = 1$，即 $1+x$ 是 R 的单位.
4. 由于 x 幂零，所以存在正整数 m，使得 $x^m = 0$. 又因为
$$\begin{aligned} -u^{2m} &= x^{2m} - u^{2m} \\ &= (x+u)(x-u)(x^{2(m-1)} + x^{2(m-2)}u^2 + \cdots + u^{2(m-1)}) \\ &:= (x+u)p(x) \end{aligned}$$
于是 $(x+u)(-p(x)/u^{2m}) = 1$ （显然 $u^{2m} \neq 0$），即 $u+x$ 为 R 的单位.

笔记 本题的难点实际上在于因式分解. 我们有如下常用的乘法公式：

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$$
$$x^{2n+1} + y^{2n+1} = (x+y)(x^{2n} - x^{2n-1}y + x^{2n-2}y^2 - \cdots + y^{2n})$$

证明也很简单，只需要从等式右侧化简即可.

（五）幂等元

环 R 中的元素 r 被称为是幂等的，如果满足 $r^2 = r$.

✍ **练习 2.21** 证明：若 R 是整环，则 R 中的幂等元只有 $0,1$.

证明 设 $r \in R$ 是幂等的，则有 $r^2 = r$，即 $r(r-1)=0$. 由于 R 是整环，所以必有 $r=0$ 或 $r-1=0$，也就是 $r=0,1$.

（六）Bool 环

环 R 称之为 Bool 环：对任意的 $a \in R$，有 $a^2 = a$.

✍ **练习 2.22** 设 R 是 Bool 环. 证明：

1. R 中每个元素的加法逆元，都是其自身；
2. R 是可交换的.

证明

1. 对任意的 $x \in R$，有：

$$\begin{aligned} x + x &= (x + x)^2 \\ &= x^2 + xx + xx + x^2 \\ &= x + x + x + x \end{aligned}$$

于是 $x + x = 0$，即 $x = -x$.

2. 对任意的 $x, y \in R$，我们有

$$\begin{aligned} x + y &= (x + y)^2 \\ &= x^2 + xy + yx + y^2 \\ &= x + xy + yx + y \end{aligned}$$

从而 $xy + yx = 0$，即 $xy = -yx = yx$. 命题得证.

✍ **练习 2.23** 证明：唯一的 Bool 整环是 $\mathbb{Z}_2$.

证明 若 R 是 Bool 环，且为整环，则对任意的 $a \in R$ 有：

$$\begin{aligned} a^2 &= a \\ a^2 - a &= 0 \\ a(a-1) &= 0 \end{aligned}$$

由乘法消去律可得：$a = 0$ 或 $a = 1$. 从而 R 中只有两个元素 $0, 1$. 考虑加法群 $(R, +)$，二阶加法群只有一个 $\mathbb{Z}_2$. 经验证，$\mathbb{Z}_2$ 是 Bool 环. 从而唯一的 Bool 整环是 $\mathbb{Z}_2$.

✍ **练习 2.24** 设 X 是非空集，$\mathcal{P}(X)$ 是 X 的幂集（即 X 的子集全体构成的集合），定义 $\mathcal{P}(X)$ 上的加法和乘法：

$$\begin{aligned} A + B &:= (A - B) \cup (B - A) \\ A \times B &:= A \cap B \end{aligned}$$

试证明：

1. $\mathcal{P}(X)$ 连同如上定义的加法和乘法构成环.
2. $\mathcal{P}(X)$ 是 Bool 环.

证明

1. 先证明：$(\mathcal{P}(X), +)$ 是交换群. 运算封闭性、结合律、交换律都是显然成立的. 幺元为空集 $\varnothing$，因为

$$\begin{aligned} A + \varnothing &= A \cup \varnothing = A \\ \varnothing + A &= \varnothing \cup A = A \end{aligned}$$

一个元素 A 的逆元为其自身，因为

$$A + A = \varnothing \cup \varnothing = \varnothing$$

从而 $(\mathcal{P}(X), +)$ 是交换群.

再证明：$(\mathcal{P}(X),\cdot)$ 是幺半群. 运算封闭性、结合律显然成立. 乘法幺元为全集 X，因为

$$A\times X=A\cap X=A$$
$$X\times A=X\cap A=A$$

从而 $(\mathcal{P}(X),\cdot)$ 是幺半群.

最后证明：乘法满足分配律. 对任意的 $A,B,C\subset X$，有：

$$\begin{aligned}(A+B)\times C&=((A-B)\cup(B-A))\cap C\\&=((A-B)\cap C)\cup((B-A)\cap C)\\&=(A\cap C-B\cap C)\cup(B\cap C-A\cap C)\\&=A\cap C+B\cap C\\&=A\times C+B\times C\end{aligned}$$

同理可证 $C\times(A+B)=C\times A+C\times B$.

综上，$(\mathcal{P}(X),+,\cdot)$ 是环.

2. 对任意的 $A\subset X$，有

$$A^2=A\cap A=A$$

命题得证.

✍ **练习 2.25** 试举出一个无限的 Bool 环.

注 提示：考虑整数集的全体子集，按前一题的方法构造环.

（七）环的直积

✍ **练习 2.26** 设 R,S 是环. 证明

1. 集合 $R\times S$ 连同按分量的加法和乘法构成环；
2. $R\times S$ 是交换环，当且仅当 R,S 都是交换环.

注 第一小问按分量讨论即可，我们给出第二小题的证明.

证明 一方面，若 $R\times S$ 是交换环，则对任意的 $r,r'\in R$，有：

$$(r,1)(r',1)=(r',1)(r,1)$$
$$(rr',1)=(r'r,1)$$

从而 $rr'=r'r$，即 R 是交换的. 同理可证 S 是交换的.

另一方面，若 R,S 是交换环，则对任意的 $(r,s),(r',s')\in R\times S$，有：

$$\begin{aligned}(r,s)(r',s')&=(rr',ss')\\&=(r'r,s's)\\&=(r',s')(r,s)\end{aligned}$$

从而 $R\times S$ 是交换的.

✍ **练习 2.27** 设 I 是任意非空指标集，$R_i,i\in I$ 都是环. 证明：直积 $\prod_{i\in I}R_i$ 连同按分量的加法和乘法构成环.

✍ **练习 2.28** 证明：$\{(r,r):r\in R\}$ 是 $R\times R$ 的子环.

2.2 环同态、商环

2.2.1 课前思考

1. 设 R,S 为环，则零映射：$0:R\to S,r\mapsto 0$ 是环同态.（T/F）
2. 整数环 $\mathbb{Z}$ 的理想为____.
3. 举例说明：环 R 的子集 A 对 R 的元素有乘法吸收性，但 A 不是理想.

解

1. F：解释见“知识要点解读”的第二部分.
2. $n\mathbb{Z}$，其中 $n\in\mathbb{N}$.
3. 整数环 $\mathbb{Z}$ 的子集 $A:=\{\pm(2k+2):k\in\mathbb{Z}_+\}\cup\{0\}$.

2.2.2 知识要点

1. 环同态：环 R,S 间的映射 $\varphi:R\to S$，且对任意的 $a,b\in R$ 满足
   (a). $\varphi(a+b)=\varphi(a)+\varphi(b)$;
   (b). $\varphi(ab)=\varphi(a)\varphi(b)$;
   (c). $\varphi(1_r)=1_s$.
   环同态的核：$\ker\varphi=\{r\in R:\ \varphi(r)=0_s\}$.
   环同态的象：$\operatorname{im}\varphi=\varphi(R):=\{\varphi(r):r\in R\}$.
   环同构：一个环同态，且为双射.
2. 元素、集合混合乘法运算记号：设 A,B 是环 R 的子集，$r\in R$，定义
$$Ar:=\{ar:\ a\in A\}$$
$$rA:=\{ra:\ a\in A\}$$
$$AB:=\left\{\sum_{i=1}^{n}a_ib_i:\ a_i\in A,b_i\in B,n\in\mathbb{Z}_+\right\}$$
   （注：加法运算即为群中的混合运算，按群中的方式处理即可.）
3. 环 R 的左（或右/双侧）理想 I：$I\subset R$，且满足：
   (a). I 是加群 R 的子群，且;
   (b). 对任意的 $r\in R$，有 $rI\subset I$.（右理想：$Ir\subset I$；双侧理想：既是左理想，又是右理想. 以后不妨称这一性质为“吸收性”.）
   注：以后不加说明，“理想”均特指双侧理想. A 是 R 的理想，记作 $A\lhd R$.
4. 商环：设 R 为环，I 是 R 的理想，于是加法商群 R/I 上可定义加法和乘法运算：
$$(r+I)+(s+I):=(r+s)+I$$
$$(r+I)(s+I):=rs+I$$
   此时称 $(R/I,+,\cdot)$ 为商环.
   注 1：考虑代数式 II，如果将其理解为理想的乘法，则 II 一般不等于 I（例如对于 $\mathbb{Z}$ 的理想 $2\mathbb{Z}$，有 $(2\mathbb{Z})(2\mathbb{Z})=4\mathbb{Z}$）.；而如果将其理解为商环 R/I 中的元素的乘法运算，则 $II=I$. 所以两种乘法运算并不相同，在实际应用中读者需要通过上下文判断到底是哪一种乘法. 在本书中，为了避免使用语义含混的符号，我们总是认为 II 表示理想的乘法运算，而将商环元素的乘法运算记为 $\bar{0}\bar{0}=\bar{0}$. 一般的，我们将商环中的运算记为：
$$\bar{r}+\bar{s}:=\overline{r+s}$$
$$\bar{r}\cdot\bar{s}:=\overline{rs}$$
   注 2：我们有时也会采用 $\bmod$ 的记法（抽代里几乎不用）表示 $\bar{r}$，即 $r\mod I$，而 $r-s\in I$ 则可记为

$r \equiv s \mod I$. 这样的记法利用到整数环 $\mathbb{Z}$ 上，就成为了我们熟悉的同余.

5. (环同构定理)：
   (a). (第一同构定理)：设 $\varphi : R \to S$ 是环同态，则
      I. $\ker \varphi \lhd R$;
      II. $\operatorname{im} \varphi < S$;
      III. $R/\ker \varphi \simeq \operatorname{im} \varphi$.
   (b). (自然映射)：设 $I \lhd R$，则自然映射
   $$\psi : R \to R/I$$
   $$r \mapsto \bar{r}$$
   是环满同态.
   (c). (第二同构定理)：设 $A < R$，$B \lhd R$，则
      I. $A + B < R$;
      II. $A \cap B \lhd A$;
      III. $(A + B)/B \simeq A/(A \cap B)$.
   (d). (第三同构定理)：设 $I, J \lhd R$，且 $I \subset J$，则 $J/I \lhd R/I$，且 $(R/I)/(J/I) \simeq (R/J)$.
   (e). (第四同构定理)：设 $I \lhd R$，则 R 中包含 I 的理想和 R/I 的理想有一一对应的关系：$A \mapsto A/I$. 换句话说，A 是 R 中包含 I 的理想，当且仅当 $A/I \lhd R/I$.

2.2.3 知识要点解读

(一) 理想的概念

环论中的理想，其角色有点类似于群论中的正规子群，但是在下一节，我们将会看到，理想之于环论的意义更为巨大. 本节中最重要的任务是熟悉理想的定义和基本运算，而且请注意，理想一般来说不是子环（因为理想不一定包含乘法幺元）.

问题 2.4 (第二同构定理)：设 $A < R$，$B \lhd R$，则

1. $A + B < R$;
2. $A \cap B \lhd A$;
3. $(A + B)/B \simeq A/(A \cap B)$.

证明

1. 先证明：$A + B$ 是 R 的加法子群. 首先，$0 = 0 + 0 \in A + B$. 其次，对任意的 $a, a' \in A$，$b, b' \in B$，有
   $$(a + b) - (a' + b') = (a - a') + (b - b') \in A + B$$
   得证.
   再证明：$A + B$ 是乘法幺半群. 首先，$1 = 1 + 0 \in A + B$. 其次，对任意的 $a, a' \in A$，$b, b' \in B$，有
   $$\begin{aligned}(a + b)(a' + b') &= aa' + ab' + ba' + bb' \\ &= aa' + (ab' + ba' + bb') \in A + B\end{aligned}$$
   (因为 B 是 R 的理想，所以 $ab', ba', bb' \in B$) 得证.
   最后，$A + B$ 上的乘法分配律由 R 的运算性质保证. 综上，$A + B$ (连同 R 上的加法和乘法运算) 是 R 的子环.
2. 首先，由于 A, B 都是 R 的加法子群，所以 $A \cap B$ 也是 R 的加法子群.
   下证：对任意的 $a \in A$，有 $a(A \cap B) \subset A \cap B$. ($(A \cap B)a \subset A \cap B$ 同理可证)

我们有

$$\begin{aligned} a(A\cap B) &= aA\cap aB \\ &\subset A\cap B \qquad\qquad (aA\subset A, aB\subset B). \end{aligned}$$

即证.

3. 定义环的映射:

$$\begin{aligned} \varphi : A &\to (A+B)/B \\ a &\mapsto \bar{a} \end{aligned}$$

先证明: φ 是环同态. 对任意的 $a_1, a_2\in A$, 我们有:

$$\begin{aligned} \varphi(a_1+a_2) &= \overline{a_1+a_2} \\ &= \overline{a_1}+\overline{a_2} \\ &= \varphi(a_1)+\varphi(a_2) \end{aligned}$$

$$\begin{aligned} \varphi(a_1a_2) &= \overline{a_1a_2} \\ &= \overline{a_1a_2} \\ &= \varphi(a_1)\varphi(a_2) \end{aligned}$$

$$\varphi(1) = \bar{1}$$

而 $\bar{1}$ 是 $(A+B)/B$ 的乘法幺元 (可以验证 $\bar{1}\bar{a}=\bar{a}=\bar{a}\bar{1}$) .

综上, φ 是环同态. 同时, φ 是满射, 因为对任意的象 $\bar{a}$, 都有对应的原象 a. 计算 φ 的核:

$$\begin{aligned} \ker\varphi &= \{a\in A : \bar{a}=\bar{0}\} \\ &= \{a\in A : a\in B\} \\ &= A\cap B \end{aligned}$$

于是由第一同构定理可得:

$$A/(A\cap B)\simeq (A+B)/B$$

笔记 读者可以通过第二同构定理的证明, 熟悉环同态的证明, 以及理想的运算性质, 尤其是理想对于乘法运算的“吸收性”, 这一点也是无法对标正规子群的特殊性质. 这种差别是因为, 在一般的环中, 乘法的性质 (幺半群甚至是半群) 比加法 (交换群) 弱, 从而涉及乘法的条件, 往往需要给的强一些.

注意到第三小问中, 商环 $(A+B)/B$ 的元素形如 $\bar{a}:=a+B$, 这是因为, 对任意的 $a\in A, b\in B$, 有

$$\overline{a+b} = \bar{a}+\bar{b} = \bar{a}+\bar{0} = \bar{a}$$

问题 2.5 (第三同构定理): 设 $I, J\lhd R$, 且 $I\subset J$, 则 $J/I\lhd R/I$, 且 $(R/I)/(J/I)\simeq (R/J)$.

证明 先证明: $J/I\lhd R/I$. 显然, J/I 是 R/I 的加法子群 (群的第四同构定理), 下证: J/I 对 R/I 中元素有吸收性.

记 $\bar{r}=r+I$. 对任意的 $r\in R$ 和 $j\in J$, 有:

$$\bar{r}\bar{j} = \overline{rj} = rj+I\in J+I$$

$\bar{j}\bar{r}\in J+I$ 同理可证. 从而对任意的 $r\in R$, 有

$$\begin{aligned} \bar{r}(J/I) &\subset J/I \\ (J/I)\bar{r} &\subset J/I. \end{aligned}$$

吸收性得证.

定义环的映射：

$$\varphi : R/I \to R/J$$
$$\bar{r} \mapsto r'$$

其中 $\bar{r} := r + I, r' := r + J$.

下证：φ 是环同态.

1. 良定义：当 $\overline{r_1} = \overline{r_2}$ 时，有

$$r_1 - r_2 \in I \subset J$$

从而 $r_1' = r_2'$.

2. 保持加法：对任意的 $r, s \in I$，有

$$\begin{aligned}\varphi(\bar{r} + \bar{s}) &= \varphi(\overline{r+s}) \\ &= (r+s)' \\ &= r' + s' \\ &= \varphi(\bar{r}) + \varphi(\bar{s})\end{aligned}$$

3. 保持乘法：对任意的 $r, s \in I$，有

$$\begin{aligned}\varphi(\bar{r}\bar{s}) &= \varphi(\overline{rs}) \\ &= (rs)' \\ &= r's' \\ &= \varphi(\bar{r})\varphi(\bar{s})\end{aligned}$$

4. 幺元对幺元：

$$\varphi(\bar{1}) = 1'$$

综上，φ 是环同态. 且对任意的象 r'，都有对应的原象 $\bar{r}$，从而 φ 是满射. 求 φ 的核：

$$\begin{aligned}\ker\varphi &= \{\bar{r} : r' = 0'\} \\ &= \{\bar{r} : r \in J\} \\ &= J/I\end{aligned}$$

从而利用环第一同构定理，有：

$$(R/I)/(J/I) \simeq R/J.$$

笔记 读者可以通过第三同构定理的证明，熟悉理想的判定方法.

问题 2.6（第四同构定理）：设 $I \lhd R$，则 R 中包含 I 的理想和 R/I 的理想有一一对应的关系：$A \mapsto A/I$. 也就是说，A 是 R 中包含 I 的理想，当且仅当 A/I 是 R/I 的理想.

证明 一方面，设 A 是 R 中包含 I 的理想.

1. 先证明：A/I 是 R/I 的加法子群. 由群的第四同构定理直接得证.
2. 再证明：A/I 对 R/I 元素的吸收性. 对任意的 $r \in R$，以及任意的 $a \in A$，有

$$\bar{r}\bar{a} = \overline{ra}$$
$$\bar{a}\bar{r} = \overline{ar}$$

由于 $A \lhd R$，所以 $ar, ra \in A$，于是 $\overline{ra}, \overline{ar} \in A/I$，吸收性即证.

综上，$A/I \lhd R/I$.

另一方面，先证明，R/I 的理想，都形如 A/I，其中 A 是 R 中包含 I 的理想. 设 J 是 R/I 的理想，定义集

合：

$$A := \{a \in R : \bar{a} \in J\}.$$

下证：$A \lhd R$，且 $I \subset A$. 首先，$0 \in A$，且对任意 $a, b \in A$，有 $\bar{a}, \bar{b} \in J$，于是 $\overline{a-b} = \bar{a} - \bar{b} \in J$，即 $a - b \in A$. 所以 A 是 R 的加法子群.

其次，对任意的 $r \in R$ 和 $a \in A$，有 $\overline{ra} = \bar{r}\bar{a} \in \bar{r}J \subset J$，从而 $ra \in A$. 同理可证 $ar \in A$，所以 A 对 R 有吸收性. 综上所述，$A \lhd R$.

另外，对任意的 $i \in I$，$\bar{i} = \bar{0} \in J$，所以 $i \in A$，从而 $I \subset A$.

于是，$A/I \lhd R/I$，必有 $A \lhd R$，且 $A \subset R$.

笔记 第四同构定理向我们展示了 A 与 A/I 结构之间的联系. 后半部分证明中，对 A 的构造非常巧妙，我们在交换代数中还会再遇到.

（二）环同态

和子环的概念类似的，不同的环的定义，将导致不同的环同态的定义. 简而言之，如果我们要求环中含有乘法幺元，则环同态的定义中，就需要有 $\varphi(1) = 1$（我们不妨称此为环同态的严格定义）. 反之，如果环中不要求含幺，那么也无法讨论甚至给定幺元的像（此时称为环同态的宽松定义）. 不同的书中对此有不同的处理，请读者一定小心.

例题 2.8 考虑零映射：$0 : R \to S, r \mapsto 0$. 在宽松定义下，它始终是环同态；而在严格定义下，只有 S 为零环时，它才为环同态.

2.2.4 典型例题

（一）环同态的判定

不论给定的映射形式有多复杂，判定环同态方法总是不变的，利用定义就好.

例题 2.9 设 X 是非空集，$\mathcal{P}(X)$ 是 X 的幂集（从而是 Bool 环，见第一小节的习题）. 设映射的集合 $R = \{f : X \to \mathbb{Z}_2\}$，且对任意的 $A \in \mathcal{P}(X)$，定义映射 $\chi_A : X \to \mathbb{Z}_2$：（也称之为 A 的特征函数）

$$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

证明：映射

$$\begin{aligned} \varphi : \mathcal{P}(X) &\to R \\ A &\mapsto \chi_A \end{aligned}$$

是环同态.

证明

1. （保持加法）：对任意的 $A, B \in \mathcal{P}(X)$（即 $A, B \subset X$），有：

$$\varphi(A + B) = \chi_{(A-B)\cup(B-A)}$$
$$\varphi(A) + \varphi(B) = \chi_A + \chi_B$$

考察两个映射在全集 X 上的的取值情况：

$x \in$	$\overline{A \cup B}$	$A - B$	$B - A$	$A \cap B$
$\chi_{(A-B)\cup(B-A)}$	0	1	1	0
$\chi_A + \chi_B$	$0+0=0$	$1+0=1$	$0+1=1$	$1+1=0$

从而有 $\chi_{(A-B)\cup(B-A)} = \chi_A + \chi_B$，即 $\varphi(A + B) = \varphi(A) + \varphi(B)$.

2. (保持乘法): 对任意的 $A, B \in \mathcal{P}(X)$ 有:

$$\varphi(A \times B) = \chi_{A\cap B}$$
$$\varphi(A)\varphi(B) = \chi_A\chi_B$$

考察两个映射在全集 X 上的的取值情况:

$x \in$	$\overline{A \cup B}$	$A - B$	$B - A$	$A \cap B$
$\chi_{A\cap B}$	0	0	0	1
$\chi_A\chi_B$	$0\cdot 0 = 0$	$1\cdot 0 = 0$	$0\cdot 1 = 0$	$1\cdot 1 = 1$

从而有 $\chi_{A\cap B} = \chi_A\chi_B$, 即 $\varphi(AB) = \varphi(A)\varphi(B)$.

3. (幺元到幺元): $\mathcal{P}(X)$ 中的乘法幺元为 X, R 中的乘法幺元是 1 映射: $1(x) = 1, \forall x \in X$. 且对任意的 $x \in X$, 我们有:

$$\varphi(X)(x) = \chi_X(x) = 1 = 1(x).$$

从而 $\varphi(X) = 1$.

综上: φ 是环同态.

笔记 本题的题面比较怪异, 里面涉及了集合论、映射等相关知识, 但是对环同态的处理仍然是朴素的, 没有新的花样. 希望读者不要被这些花架子劝退.

2.2.5 习题

(一) 环同态的例子

练习 2.29 证明: 环 $\mathbb{Z}[x]$ 和 $\mathbb{Q}[x]$ 不同构.

提示 提示: 如果 $\varphi : \mathbb{Q}[x] \to \mathbb{Z}[x]$ 是环同构, 则 $0 \mapsto 0$, $1 \mapsto 1$, 于是必须将 $\mathbb{Q}$ 同构地映到 $\mathbb{Z}$, 而加群 $\mathbb{Q}$ 和 $\mathbb{Z}$ 之间没有群同构, 从而也没有环同构, 矛盾!

练习 2.30 写出所有 $\mathbb{Z}$ 到 $\mathbb{Z}$ 的环同态.

解 对任意的环同态 $\varphi : \mathbb{Z} \to \mathbb{Z}$, 有:

$$\varphi(1) = 1$$

所以对任意的 $n \in \mathbb{Z}_+$, 有

$$\begin{aligned}\varphi(n) &= \varphi(1 + \cdots + 1)\\ &= \varphi(1) + \cdots + \varphi(1)\\ &= 1 + \cdots + 1\\ &= n\end{aligned}$$

且

$$\varphi(-n) = -\varphi(n) = -n$$

结合 $\varphi(0) = 0$ 可知, φ 只能为恒等映射.

练习 2.31 设 R 是 $[0, 1]$ 上所有连续实函数的集合 (从而连同函数的加法和乘法运算构成环). 证明: 映射

$$\varphi : R \to \mathbb{R}$$
$$f \mapsto \int_0^1 f(t)dt$$

是加群的群同态, 但不是环同态.

证明 先证明：φ 是加群的群同态. 对任意的 $f,g\in R$ 有：

$$\begin{aligned}\varphi(f+g)&=\int_0^1(f+g)(t)dt\\&=\int_0^1(f(t)+g(t))dt\\&=\int_0^1f(t)dt+\int_0^1g(t)dt\\&=\varphi(f)+\varphi(g)\end{aligned}$$

得证.

再证明：φ 不保持乘法运算，从而不是环同态. 取 $f(t)=g(t)=t$，则

$$\begin{aligned}\varphi(f)\varphi(g)&=\left(\int_0^1tdt\right)\left(\int_0^1tdt\right)\\&=\frac{1}{2}\frac{1}{2}\\&=\frac{1}{4}\\\varphi(fg)&=\int_0^1t^2dt\\&=\frac{1}{3}\end{aligned}$$

即 $\varphi(f)\varphi(g)\neq\varphi(fg)$. 于是 φ 不保持乘法运算.

笔记 此题并不难，但是启发我们：分析学中随处可见代数结构，读者可以对此留意一二.

练习 2.32 指出下列哪些是 $M_2(\mathbb{Z})$ 到 $\mathbb{Z}$ 的环同态，并证明之.

1. (投影)：
$$f:\begin{pmatrix}a&b\\c&d\end{pmatrix}\mapsto a$$
2. (迹)：
$$g:\begin{pmatrix}a&b\\c&d\end{pmatrix}\mapsto a+d$$
3. (行列式)：
$$h:\begin{pmatrix}a&b\\c&d\end{pmatrix}\mapsto ad-bc$$

解

1. 不是环同态. 取
$$A=B=\begin{pmatrix}1&1\\1&1\end{pmatrix}$$
则
$$AB=\begin{pmatrix}2&2\\2&2\end{pmatrix}$$
于是：
$$f(AB)=2\neq1=f(A)f(B).$$
2. 是环同态，一般的，对任意的 $A,B\in F^{n\times n}$ 有
$$\begin{aligned}\operatorname{tr}(A+B)&=\operatorname{tr}(A)+\operatorname{tr}(B)\\\operatorname{tr}(AB)&=\operatorname{tr}(A)\operatorname{tr}(B)\end{aligned}$$

3. 不是环同态. 取

$$A=\begin{pmatrix}1&1\\0&1\end{pmatrix},\ B=\begin{pmatrix}1&1\\1&1\end{pmatrix}$$

则

$$A+B=\begin{pmatrix}2&2\\1&2\end{pmatrix}$$

于是:

$$h(A)+h(B)=1\neq 2=h(A+B).$$

✍ **练习 2.33** 定义二阶上三角方阵的集合:

$$R=\left\{\begin{pmatrix}a&b\\0&d\end{pmatrix}:\ a,b,d\in\mathbb{Z}\right\}$$

证明:

1. R 是 $M_2(\mathbb{Z})$ 的子环;
2. 映射 $\varphi:R\to\mathbb{Z}\times\mathbb{Z}$

$$\begin{pmatrix}a&b\\0&d\end{pmatrix}\mapsto(a,d)$$

是环满同态，并求其核.

提示 使用定义即可.

✍ **练习 2.34** 证明：环 $M_2(\mathbb{R})$ 包含一个子环同构于 $\mathbb{C}$.

注 提示：考虑集合

$$R=\{\lambda I:\lambda\in\mathbb{C}\}$$

其中 $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$.

✍ **练习 2.35*** 证明：环 $M_4(\mathbb{R})$ 包含一个子环同构于 Hamilton 四元数环 $\mathbb{H}$.

注 提示：考虑映射

$$i\mapsto\begin{pmatrix}0&-1&0&0\\1&0&0&0\\0&0&0&-1\\0&0&1&0\end{pmatrix}$$

$$j\mapsto\begin{pmatrix}0&0&-1&0\\0&0&0&1\\1&0&0&0\\0&-1&0&0\end{pmatrix}$$

笔记 以上两例我们在群表示论中会再一次遇见.

（二）环同态的性质

✍ **练习 2.36** 设 $\varphi:R\to S$ 是环满同态. 证明：$\varphi(Z(R))\subset Z(S)$.

证明 对任意的 $r \in Z(R)$，和任意的 $s = \varphi(r') \in S$（满射确保这样的 r' 存在），有

$$\begin{aligned} \varphi(r)s &= \varphi(r)\varphi(r') \\ &= \varphi(rr') \\ &= \varphi(r'r) && (r \in Z(R)) \\ &= \varphi(r')\varphi(r) \\ &= s\varphi(r) \end{aligned}$$

从而 $r \in Z(S)$，即 $\varphi(Z(R)) \subset Z(S)$.

✍ **练习 2.37** 设 $\varphi : R \to S$ 是环同态，$u \in R^\times$. 证明：$\varphi(u) \in S^\times$，且 $\varphi(u^{-1}) = \varphi(u)^{-1}$.

证明 我们有：

$$\begin{aligned} 1 &= \varphi(1) \\ &= \varphi(uu^{-1}) \\ &= \varphi(u)\varphi(u^{-1}) \end{aligned}$$

所以 $\varphi(u) \in S^\times$. 同时可得 $\varphi(u)$ 的乘法逆为 $\varphi(u^{-1})$. 由于 $\varphi(u)^{-1}$ 也是 $\varphi(u)$ 的乘法逆，所以由逆的唯一性可得 $\varphi(u^{-1}) = \varphi(u)^{-1}$.

（三）理想的例子

✍ **练习 2.38** 指出以下哪些是环 $R = \mathbb{Z} \times \mathbb{Z}$ 的理想，并证明之：

1. $I_1 = \{(a, a) : a \in \mathbb{Z}\}$;
2. $I_2 = \{(2a, 2b) : a, b \in \mathbb{Z}\}$;
3. $I_3 = \{(2a, 0) : a \in \mathbb{Z}\}$;
4. $I_4 = \{(a, -a) : a \in \mathbb{Z}\}$.

解

1. I_1 不是 R 的理想，因为
$$(2,1)(1,1) = (2,1) \notin I_1$$
2. I_2 是 R 的理想. 首先，I_2 是 R 的加法子群，因为 I_2 非空，且对任意的 $(2a, 2b), (2c, 2d) \in I_2$，有：
$$(2a, 2b) - (2c, 2d) = (2(a-c), 2(b-d)) \in I_2.$$
其次，I_2 有吸收性. 因为对任意的 $(r, s) \in R$ 和 $(2a, 2b) \in I_2$，有：
$$(2a, 2b)(r, s) = (r, s)(2a, 2b) = (2ra, 2sb) \in I_2$$
综上，I_2 是 R 的理想.
3. I_3 是 R 的理想. 首先，I_3 是 R 的加法子群，因为 I_3 非空，且对任意的 $(2a, 0), (2c, 0) \in I_3$，有：
$$(2a, 0) - (2c, 0) = (2(a-c), 0) \in I_3.$$
其次，I_3 有吸收性. 因为对任意的 $(r, s) \in R$ 和 $(2a, 0) \in I_3$，有：
$$(2a, 0)(r, s) = (r, s)(2a, 0) = (2ra, 0) \in I_3$$
综上，I_3 是 R 的理想.
4. I_4 不是 R 的理想，因为
$$(2,1)(1,-1) = (2,-1) \notin I_4.$$

✍ **练习 2.39** 指出以下哪些是多项式环 $\mathbb{Z}[x]$ 的理想，并证明之：（可以在学完“多项式理论”的第一小节之后再来做此题）

1. $I_1=\{p(x)\in\mathbb{Z}[x]:3\mid a_0\}$;
2. $I_2=\{p(x)\in\mathbb{Z}[x]:3\mid a_2\}$;
3. $I_3=\{p(x)\in\mathbb{Z}[x]:a_0=a_1=a_2=0\}$;
4. $I_4=\mathbb{Z}[x^2]$;
5. $I_5=\{p(x)=\sum_{i=0}^n a_ix^i\in\mathbb{Z}[x]:\sum_{i=0}^n a_i=0\}$;
6. $I_6=\{p(x)\in\mathbb{Z}[x]:p'(0)=0\}$，其中 $p'(x)$ 为 $p(x)$ 的（形式）导数.

解

1. I_1 是理想.
2. I_2 不是理想，因为 $x(3x^2+x)=3x^3+x^2\notin I_2$.
3. I_3 是理想.
4. I_4 不是理想，因为 $x\cdot x^2=x^3\notin I_4$.
5. I_5 是理想.

   首先，对任意的 $p(x)=\sum_{i=0}^n a_ix^i$，有 $\sum_{i=0}^n a_i=p(1)$. 从而 $I_5=\{p(x)\in\mathbb{Z}[x]:p(1)=0\}$.

   其次，I_5 是加法子群，因为 $0\in I_5$，且对任意的 $p,q\in I_5$，有：

   $$(p-q)(1)=p(1)-q(1)=0.$$

   即 $p-q\in I_5$.

   最后，I_5 对 $Z[x]$ 中的元素有吸收性. 因为对任意的 $f\in\mathbb{Z}[x]$ 和 $p\in I_5$，有：

   $$(fp)(1)=f(1)p(1)=f(1)\cdot 0=0$$
   $$(pf)(1)=p(1)f(1)=p(1)\cdot 0=0$$

   即 $fp,pf\in I_5$.

   综上，$I_5<\mathbb{Z}[x]$.
6. I_6 不是理想. 因为 $1\in I_6$，但是 $(x\cdot 1)'=1$，所以 $x\cdot 1\notin I_6$.

练习 2.40* 设 R 是环，$M_n(R)$ 的子集 L_j 中的元素都是除第 j 列以外其余分量为零的矩阵，矩阵 $E_{ij}\in M_n(R)$ 只有 (i,j) 位置的分量为 1，其他分量为 0. 证明：

1. L_j 是 $M_n(R)$ 的左理想；
2. 对任意的指标 i，有 $L_j=M_n(R)E_{ij}$.

证明

1. 首先，$0\in L_j$，且对任意的 $A=(a_{ij}),B=(b_{ij})\in L_j$，若 $k\neq j$，则：

   $$a_{ik}-b_{ik}=0-0=0$$

   即 $A-B$ 第 j 列之外的分量均为 0，从而 $A-B\in L_j$. 因此 L_j 是 $M_n(R)$ 的加法子群.

   其次，对任意的 $X=(x_{ij})\in M_n(R)$ 和 $A=(a_{ij})\in L_j$，$C=XA$ 不在第 j 列的任意分量 c_{ik} 为：

   $$c_{ik}=\sum_{l=1}^n x_{il}a_{lk}=\sum_{l=1}^n x_{il}\cdot 0=0$$

   故 $XA=C\in L_j$. 从而 X 对 $M_n(R)$ 中的元素有左吸收性. 综上，L_j 是 $M_n(R)$ 的左理想.
2. 一方面，对任意的 $X=(x_{ij})\in M_n(R)$，$C=XE_{ij}$ 不在第 j 列的元素 c_{km} 为：

   $$c_{km}=\sum_{l=1}^n x_{kl}e_{lm}$$

   由于 e_{lm} 当且仅当 $(l,m)=(i,j)$ 时不为零，所以有：

   $$c_{km}=\sum_{l=1}^n x_{kl}e_{lm}=\sum_{l=1}^n x_{kl}\cdot 0=0$$

   于是 $XE_{ij}\in L_j$，即 $M_n(R)E_{ij}\subset L_j$.

   另一方面，对任意的 $A=(a_{ij})\in L_j$，取 $X=(x_{ij})\in M_n(R)$ 满足对任意的 k 有 $x_{ki}=a_{kj}$，则 $C=XE_{ij}$

的分量 c_{km} 为：

$$c_{km}=\sum_{l=1}^{n}x_{kl}e_{lm}$$

若 $m\neq j$，则 $e_{lm}=0$，此时 $c_{km}=0$，若 $m=j$，则：

$$\begin{aligned}c_{kj}&=\sum_{l=1}^{n}x_{kl}e_{lj}\\&=x_{ki}e_{ij}\\&=a_{kj}\end{aligned}$$

从而 $A=C=XE_{ij}\in M_n(R)E_{ij}$，即 $L_j\subset M_n(R)E_{ij}$.

综上，对任意的指标 i，有 $L_j=M_n(R)E_{ij}$.

✍ **练习 2.41**** 证明：每个 $M_n(R)$ 的理想都等于 $M_n(J)$，其中 J 是 R 的某个理想.

证明 一方面，设 $J<R$ 的理想. 首先，$0\in M_n(J)$，且对任意的 $A=(a_{ij}),B=(b_{ij})\in M_n(J)$，有：

$$a_{ij}-b_{ij}\in J$$

所以 $A-B=(a_{ij}-b_{ij})\in M_n(J)$. 于是 $M_n(J)$ 是 $M_n(R)$ 的加法子群.

其次，对任意的 $X=(x_{ij})\in M_n(R)$ 和 $A=(a_{ij})\in M_n(J)$，有：

$$c_{ij}:=\sum_{k=1}^{n}a_{ik}xkj\in J$$

$$d_{ij}:=\sum_{k=1}^{n}x_{ik}akj\in J$$

从而 $AX=(c_{ij})\in M_n(J),XA=(d_{ij})\in M_n(J)$. 即 $M_n(J)$ 对 $M_n(R)$ 的元素有吸收性. 综上，$M_n(J)<M_n(R)$.

另一方面，我们要证明，$M_n(R)$ 的理想 I 都形如 $M_n(J)$，其中 $J<R$. 令：

$$J:=\{r\in R:\ \exists A\in I,i,j\in\{1,\cdots,n\},r=a_{ij}\}.$$

(即 J 为 I 中任意元素的任意分量的集合.)

1. 定义 $E_{pq}\in M_n(R)$ 是这样的方阵，它的第 p 行第 q 列的分量为 1，其他位置均为 0. 于是对任意的 $A=(a_{ij})\in M_n(R)$，有：

   $$E_{pq}AE_{rs}=(\sum_{k}\sum_{j}e_{ij}a_{jk}e'_{kl})$$

   其中只有 e_{pq} 和 $e'kl$ 等于 1，其他均为 0，所以矩阵 $E_{pq}AE_{rs}$ 中只有一个分量不为零：

   $$e_{pq}a_{qr}e'_{rs}=a_{qr}$$

   所以 $E_{pq}AE_{rs}$ 是这样的矩阵，它在第 p 行第 s 列的分量为 a_{qr}，其他分量均为 0.
2. 设 $r\in J$，定义矩阵 $A_r\in M_n(R)$ 在第 1 行第 1 列的分量为 r，其他分量均为 0，证明：$A_r\in I$.

   由 J 的定义，一定存在一个矩阵 $B\in I$，和指标 i,j，使得它在第 i 行第 j 列的分量为 r. 因为 $I<M_n(R)$，所以 $E_{1i}BE_{j1}\in I$. 而由前述命题可得：$A_r=E_{1i}BE_{j1}$，即证.

   由此我们可将 J 重新定义为：

   $$J:=\{r\in R:\ A_r\in I\}.$$
3. 证明：$J<R$. 首先，$0\in J$（因为 $A_0=0\in I$），且对任意的 $r,s\in J$，有：

   $$A_{r-s}=A_r-A_s\in I$$

   即 $r-s\in J$，所以 J 是 R 的加法子群.

其次，对任意的 $x \in R$ 和 $r \in J$，有：

$$A_{rs} = A_r A_s \in I$$
$$A_{sr} = A_s A_r \in I$$

所以 $rs, sr \in J$. 所以 J 对 R 的元素有吸收性. 故 $J < R$.

4. 最后证明：$I = M_n(J)$. 一方面，因为 I 中的元素的分量均在 J 中，所以 $I \subset M_n(J)$. 另一方面，对任意的 $X \in M_n(J)$，有：

$$X = \sum_{i=1}^{n} \sum_{j=1}^{n} A_{x_{ij}}$$

因为 $x_{ij} \in J$，所以 $A_{x_{ij}} \in I$，于是它们的和也在 I 中，即 $X \in I$，从而 $M_n(J) \subset I$. 综上，$I = M_n(J)$.

✍ **练习 2.42** 设 a 是环 R 的元素. 证明：

1. $I = \{x \in R : ax = 0\}$ 是右理想（称为 a 的右零化子）；
2. $J = \{y \in R : ya = 0\}$ 是左理想（称为 a 的左零化子）；
3. 若 L 是 R 的左理想，则 $K = \{x \in R : xa = 0, \forall a \in L\}$ 是理想（称为 L 的左零化子）.

证明

1. 先证明：I 是加法子群. 因为 I 非空（$0 \in I$），且对任意的 $x, y \in I$，有 $a(x-y) = ax - ay = 0 - 0 = 0$，即 $x - y \in I$.
   再证明：I 有右吸收性. 对任意的 $r \in R$，$x \in I$，有 $a(xr) = (ax)r = 0r = 0$，从而 $xr \in I$，即 $Ir \subset I$.
   综上，I 是 R 的右理想.
2. 和第一小问的证明过程类似.
3. 先证明：K 是加法子群. 因为 K 非空（$0 \in K$），且对任意的 $x, y \in K$ 和任意的 $a \in L$，有 $(x-y)a = xa - ya = 0$，即 $x - y \in K$.
   再证明：K 有吸收性. 对任意的 $r \in R$，$x \in K$，以及任意的 $a \in L$，有：
   $$(rx)a = r(xa) = r0 = 0$$
   $$(xr)a = x(ra) = 0 \quad (ra \in rL \subset L)$$
   从而 $rx, xr \in K$，即 $rK, Kr \in K$.
   综上，K 是 R 的理想.

✍ **练习 2.43** 设 S 是环 R 的子环，I 是 R 的理想. 证明：若 $S \cap I = 0$，则 $\bar{S} \simeq S$，其中 $\bar{S} = \{s + I : s \in S\}$.

证明 由环的第二同构定理可得：$I \lhd S + I$，$S \cap I \lhd S$. 考虑商环

$$\begin{aligned}(S+I)/I &= \{\overline{s+i} : s \in S, i \in I\} \\ &= \{\bar{s} : s \in S\} \\ &= \bar{S}\end{aligned}$$
$$S/(S \cap I) = S/\{0\} \simeq S$$

还是由第二同构定理：$(S+I)/I \simeq S/(S \cap I)$，从而 $\bar{S} \simeq S$.

笔记 注意商环 $(S+I)/I$ 中的元素形如 $\overline{s+i} = (s+i) + I = s + I = \bar{s}$.

✍ **练习 2.44** 设 $\varphi : R \to S$ 是环同态. 证明：

1. 若 J 是 S 的理想，则 $\varphi^{-1}(J)$ 是 R 的理想；
2. 若 R 是 S 的子环，J 是 S 的理想，则 $J \cap R$ 是 R 的理想；
3. 若 φ 是满射，I 是 R 的理想，则 $\varphi(I)$ 是 S 的理想. 举例说明，当 φ 不是满射时，该命题不成立.

证明

1. (a). （加法子群）：由于 J 是 S 的加法子群，所以 $\varphi^{-1}(J)$ 也是 R 的加法子群.

(b). (吸收性): 对任意的 $r\in R$ 和 $r'\in\varphi^{-1}(J)$,

$$\varphi(rr')=\varphi(r)\varphi(r')\in\varphi(r)J\subset J$$
$$\varphi(r'r)=\varphi(r')\varphi(r)\in J\varphi(r)\subset J$$

从而 $rr',r'r\in\varphi^{-1}(J)$, 即对任意的 $r\in R$, $r\varphi^{-1}(J),\varphi^{-1}(J)r\subset\varphi^{-1}(J)$.

综上, $\varphi^{-1}(J)$ 是 R 的理想.

2. 考虑嵌入映射 $\varphi:R\to S,r\mapsto r$ (容易验证这是一个环同态). 则 $\varphi^{-1}(J)=J\cap R$, 利用第一小题的结论即可.

3. (a). (加法子群): 首先, $\varphi(I)$ 非空, 因为 I 非空. 其次, 对任意的 $x,y\in I$, 有:

$$\varphi(x)-\varphi(y)=\varphi(x-y)\in\varphi(I)$$

从而 $\varphi(I)$ 是 S 的加法子群.

(b). (吸收性): 对任意的 $s\in S$, 存在 $r\in R$, 使得 $s=\varphi(r)$. 对任意的 $x\in I$ 有:

$$s\varphi(x)=\varphi(rx)\in\varphi(I)$$
$$\varphi(x)s=\varphi(xr)\in\varphi(I)$$

从而对任意的 $s\in S$, 有 $s\varphi(I),\varphi(I)s\subset\varphi(I)$.

综上, $\varphi(I)$ 为 S 的理想.

当 φ 不是满射时, 例如取 φ 为

$$\varphi:\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}$$
$$x\mapsto(x,x)$$

取 $I=2\mathbb{Z}$, 则 $\varphi(I)=\{(2a,2a):a\in\mathbb{Z}\}$ 并不是 $\mathbb{Z}\times\mathbb{Z}$ 的理想, 因为 $(1,2)\varphi(I)=\{(2a,4a):a\in\mathbb{Z}\}\notin\varphi(I)$.

(四) 诣零根

✍ **练习 2.45** 设 R 是交换环, 证明: R 的幂零元全体构成理想. (称其为 R 的诣零根, 记作 $Nil(R)$)

证明

1. (加法子群): 首先 $Nil(R)$ 非空, 因为 $0\in Nil(R)$. 其次, 对任意的 $a,b\in Nil(R)$, 存在正整数 m,n, 使得 $a^m=b^n=0$, 从而有:

$$\begin{aligned}(a-b)^{m+n}&=\sum_{k=0}^{m+n}(-1)^{m+n-k}C_{m+n}^k a^k b^{m+n-k}\\&=\sum_{k=0}^{m}(-1)^{m+n-k}C_{m+n}^k a^k b^{m+n-k}+\sum_{k=m+1}^{m+n}(-1)^{m+n-k}C_{m+n}^k a^k b^{m+n-k}\\&=\sum_{k=0}^{m}(-1)^{m+n-k}C_{m+n}^k a^k b^{m+n-k}+\sum_{l=1}^{n}(-1)^{n-l}C_{m+n}^{m+l}a^{m+l}b^{n-l},\quad(l=k-m)\\&=b^n\sum_{k=0}^{m}(-1)^{m+n-k}C_{m+n}^k a^k b^{m-k}+a^m\sum_{l=1}^{n}(-1)^{n-l}C_{m+n}^{m+l}a^l b^{n-l}\\&=0\end{aligned}$$

也就是说, $a-b\in Nil(R)$. 从而 $Nil(R)$ 是加法子群.

2. (吸收性): 对任意的 $r\in R$, $a\in Nil(R)$, 存在正整数 n, 使得 $a^n=0$, 从而

$$(ra)^n=r^n a^n=r^n 0=0$$

也就是说, $ra\in Nil(R)$, 即 $Nil(R)$ 对 R 中的元素有吸收性.

综上, $Nil(R)$ 是 R 的理想.

✍ **练习 2.46** 试举一例说明, $r+s$ 是交换环 R 中的幂零元, 但 r,s 不是幂零的.

解 Z_{10} 中，$5+5=0$ 是幂零元，但 5 不是，因为 $5^2=5$，所以 5 的任意非零次幂都是 5.

✍ **练习 2.47** 设 R 是交换环，证明：$R/Nil(R)$ 中唯一的幂零元是 $\bar{0}$.

证明 只需证：对任意的 $r\in R$，若存在整数 n 使得 $(\bar{r})^n=\bar{0}$，则 $r\in Nil(R)$.

因为 $\bar{0}=(\bar{r})^n=\overline{r^n}$，所以 $r^n\in Nil(R)$，于是存在正整数 m，使得 $(r^n)^m=0$，从而 $r^{mn}=0$，即 $r\in Nil(R)$.

✍ **练习 2.48** 证明：

1. $M_2(\mathbb{Z})$ 的幂零元

$$\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix}$$

的和不是幂零元.

2. $M_2(\mathbb{Z})$ 的全体幂零元不构成它的理想.（从而诣零根的性质只在交换环中考察）

证明

1. 两个元素的和为

$$a=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

而利用数学归纳法可得：

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}^{2k}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

$$\begin{pmatrix}0&1\\1&0\end{pmatrix}^{2k+1}=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

其中 $k\in\mathbb{N}$. 从而 a 不是幂零元.

2. 由第一小问可知，$M_2(\mathbb{Z})$ 的幂零元集合上的加法不封闭，从而不是加法子群，也就不是理想.

✍ **练习 2.49** 设 $\varphi:R\to S$ 是环同态. 证明：若 x 是 R 的幂零元，则 $\varphi(x)$ 是 S 中的幂零元.

证明 设正整数 n 使得 $x^n=0$，则 $\varphi(x)^n=\varphi(x^n)=\varphi(0)=0$，从而 $\varphi(x)$ 是 S 中的幂零元.

✍ **练习 2.50**** 设 R 是交换环，$p(x)=\sum_{k=0}^n a_kx^k\in R[x]$. 证明：

1. $p(x)$ 是 $R[x]$ 的单位，当且仅当 a_0 是 R 的单位，且 $a_1,\cdots,a_n$ 是 R 的幂零元；
2. $p(x)$ 是 $R[x]$ 的幂零元，当且仅当 $a_0,\cdots,a_n$ 是 R 的幂零元.

证明

1. 一方面，设 a_0 是 R 的单位，且 $a_1,\cdots,a_n$ 是 R 的幂零元. 对任意非零指标 i，a_i 是幂零的，意味着存在正整数 n，使得 $a_i^n=0$. 于是 $(a_ix^i)^n=a_i^nx^{in}=0$，从而 $a_ix^i\in Nil(R[x])$，于是 $\sum_{k=1}^n a_kx^k\in Nil(R[x])$. 对于 a_0，它是 R 中的单位，则必然也是 $R[x]$ 中的单位. 利用第一节练习 2.20 的结论可得，$p(x)=a_0+\sum_{k=1}^n a_kx^k$ 是 $R[x]$ 中的单位.

另一方面，设 $p(x)$ 是 $R[x]$ 的单位. 则存在 $q(x)=\sum_{k=0}^m b_kx^k$，使得 $p(x)q(x)=1$. 对比等式两侧多项式的系数可得，常数项 $a_0b_0=1$，从而 a_0,b_0 是 R 的单位. x^k 单项的系数为

$$\sum_{\substack{i\in[0,n]\\j\in[0,m]\\i+j=k}}a_ib_j=0$$

以下用数学归纳法证明：对于 $j\in[0,m]$，$a_n^{j+1}b_{m-j}=0$.

当 $j=0$ 时，a_nb_m 即是最高次单项 x^{m+n} 的系数，所以等于 0，命题成立.

假设 $j \leqslant k$，时 $a_n^{j+1} b_{m-j} = 0$，$j = k+1$ 时，考虑单项 x^{m+n-j} 的系数：

$$\begin{aligned} 0 &= \sum_{\substack{i\in[0,n]\\ l\in[0,m]\\ i+l=m+n-j}} a_i b_l \\ &= \sum_{i=n-j}^{n} a_i b_{m+n-j-i} \\ &= \sum_{i=0}^{j} a_{n-i} b_{m-j+i} \\ &= a_n b_{m-j} + a_{n-1} b_{m-j+1} + \cdots + a_{n-j} b_m \\ &= a_n b_{m-k-1} + a_{n-1} b_{m-k} + \cdots + a_{n-k-1} b_m \end{aligned}$$

等式两侧同乘 a_n^{k+1} 可得：

$$\begin{aligned} 0 &= a_n^{k+2} b_{m-k-1} + a_{n-1} a_n^{k+1} b_{m-k} + \cdots + a_{n-k-1} a_n^{k+1} b_m \\ &= a_n^{(k+1)+1} b_{m-(k+1)} + a_{n-1} a_n (a_n^k b_{m-k}) + \cdots + a_{n-k-1} a_n^k (a_n b_m) \\ &= a_n^{(k+1)+1} b_{m-(k+1)} && \text{利用归纳假设.} = a_n^{j+1} b_{m-j} \end{aligned}$$

命题成立. 综上，对于 $j \in [0, m]$，$a_n^{j+1} b_{m-j} = 0$. 于是 $a_n^{m+1} b_0 = 0$，由于 b_0 是单位，所以 $a_n^{m+1} = 0$，即 a_n 是 R 的幂零元.

由于 a_n 是幂零的，所以 $a_n x^n$ 是幂零的，从而 $p(x) - a_n x^n$ 是幂零的. 利用前面的讨论可知，$p(x) - a_n x^n$ 最高次项的系数 a_{n-1} 也是幂零的. 由此可以一直证明：$a_{n-2}, \cdots, a_1$ 都是幂零的. 于是命题得证.

综上，原命题成立.

2. 一方面，若 $a_0, \cdots, a_n$ 都是幂零元，则 $a_i x^i$ 也都是幂零元，所以 $p(x) = \sum a_i x^i$ 也是幂零元.

另一方面，若 $p(x)$ 是幂零的，则存在正整数 k，使得 $(p(x))^k = 0$. 考察他的最低次项，有 $a_0^k = 0$，即 a_0 是幂零的. 于是 $p(x) - a_0$ 也是幂零的.

继续考察幂零元 $p(x) - a_0 = x\left(\sum_{i=1}^{n} a_i x^{i-1}\right) := x p_1(x)$，存在正整数 k_1，使得 $x^{k_1} p_1(x)^{k_1} = 0$. 由于 x^{k_1} 不等于零，也不是零因子，所以 $p_1(x)^{k_1} = 0$，即 $p_1(x)$ 是幂零元. 由前面的讨论可知，他的常数项 a_1 也是幂零的.

重复前面的讨论，可以得到，$a_0, \cdots, a_n$ 都是幂零元，命题得证.

2.2.6 思考题

下题呈现的是，当环同态 φ 不要求 $\varphi(1) = 1$ 时，φ 的特殊性质.

练习 2.51 设 R, S 是非零环，非零映射 $\varphi : R \to S$ 保持加法和乘法运算. 证明：

1. 若 $\varphi(1) \neq 1$，则 $\varphi(1)$ 是 S 的零因子.
2. 若 S 是整环，则 φ 必为环同态.

证明

1. 我们有：

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$$

即 $\varphi(1)(\varphi(1) - 1) = 0$. 由于 $\varphi(1) \neq 1$，所以 $\varphi(1) - 1 \neq 0$，从而 $\varphi(1)$ 是零因子.

2. 前一小问的证明过程可得 $\varphi(1)(\varphi(1) - 1) = 0$，当 S 是整环时，必有 $\varphi(1) = 0$ 或 $= 1$. 若 $\varphi(1) = 0$，则对任意的 $r \in R$，有 $\varphi(r) = \varphi(1r) = \varphi(1)\varphi(r) = 0$，从而 φ 为零映射，矛盾！从而只能有 $\varphi(1) = 1$，结合题设即得 φ 是环同态.

2.3 理想的性质

2.3.1 课前思考

1. 域的理想有____ 个；斜域的理想有____ 个.
2. 环 R 中，由 $a \in R$ 生成的理想形如____.

解

1. $2, 2$. 域 F 的理想有 $\{0\}, F$ 两个，斜域亦然. 因为环中包含单位的理想只能为环本身.
2. $RaR = \{rar' : r, r' \in R\}$.

2.3.2 知识要点

（一）理想的结构

1. 生成：A 是环 R 的子集，定义由 A 生成的理想为 R 中包含 A 的最小的理想.（记作 (A)，生成的左理想、右理想可类似定义）
   有限生成理想：由有限集生成的理想.
   主理想：由一个元素生成的理想.
2. （生成的理想）：环 R 中由子集 A 生成的左理想为 RA，由 A 生成的右理想为 AR，由 A 生成的理想为 $(A) = RAR$. 特别的，当 R 为交换环时，$(A) = RA = AR = RAR$.
3. （包含单位的理想）：设 I 是 R 的理想.
   (a). $I = R$，当且仅当 I 包含一个单位；
   (b). 设 R 是交换环，则 R 是域，当且仅当它的理想只有 $\{0\}$ 和 R.
4. （域上的环同态）：设 R 是域，则从 R 到任意非零的环同态都是单射.

（二）两类特殊的理想

1. 环 R 的极大理想 M：R 的理想 $M \neq R$，且 R 中包含 M 的理想只有 M 和 R.
2. （极大理想的存在性 *）：环中任意真理想都包含于某个极大理想之中.
3. （交换环的极大理想）：设 R 是交换环，则理想 M 是 R 的极大理想，当且仅当 R/M 是域.
4. 交换环 R 的素理想 P：交换环 R 的理想 $P \neq R$，且对任意的 $a, b \in R$，当 $ab \in P$ 时，a, b 中至少有一个元素属于 P.
5. （交换环的素理想）：设 R 是交换环，则理想 P 是 R 的素理想，当且仅当 R/P 是整环. 从而，每个 R 的极大理想都是素理想.

2.3.3 知识要点解读

（一）环的确定

区别各种性质的环（交换环、整环、斜域、域），关键还是要回到定义，抓住一种环与其他环的本质区别，具体地说：

1. 整环：证明乘法的交换性、以及不存在非零的零因子. 此时涉及到形如 $xa = 0$ 的代数式的变形；
2. 斜域、域：证明所有的非零元都是单位，此时涉及到形如 $uv = 1$ 的代数式的变形. 斜域和域的区别在于乘法的交换性，这一点往往是中比较容易验证的.

通过以上分析可知，代数变形是基本功，环中的代数变形又以群（幺半群）中的代数变形为基础.

问题 2.7（包含单位的理想）：设 I 是环 R 的理想.

1. $I = R$，当且仅当 I 包含一个单位；

2. 设 R 是交换环. R 是域，当且仅当它的理想只有 $\{0\}$ 和 R.

证明

1. 一方面，当 $I=R$ 时，$1\in R=I$，从而 I 包含单位 1.

   另一方面，设 I 包含单位 u，从而存在 $v\in R$，使得 $vu=1$. 对任意的 $r\in R$，有

   $$r=r1=r(vu)=(rv)u\in(rv)I\subset I$$

   从而 $R\subset I$，同时显然有 $I\subset R$，即 $I=R$.

2. 一方面，当 R 是域时，理想 I 要么包含一个单位，此时 $I=R$；要么不包含单位，此时 I 只有唯一的元素 0，即 $I=\{0\}$.

   另一方面，当 R 的理想只有 $\{0\}$ 和 R 时，对任意的 $r\in R$，对应的主理想 $(r)=Rr$ 只能等于 $\{0\}$ 和 R. 若 $Rr=\{0\}$，则 $r=1r=0$；若 $Rr=R$，则存在 $s\in R$，使得 $sr=1$，从而 r 为单位. 于是，R 中除了 0 都是单位，结合 R 是交换环可知，R 是域.

笔记 对于斜域 D 而言，它的理想也只有 $\{0\}$ 和 D，但是反之则不然，例如 $M_n(F)$ 只有理想 $\{0\}$ 和 $M_n(F)$，但他不是斜域（因为它有非零的零因子）. 这是因为斜域中的主理想形如 RaR，此时第二小问的证明过程将不再适用.

练习 2.52 证明：R 是斜域，当且仅当其左理想只有 (0) 和 R.（“左理想”替换为“右理想”，命题亦成立）

证明 一方面，设 R 是斜域. (0) 显然是 R 的左理想，而当 R 的左理想中包含非零元 u 时，由于 u 为单位，所以该左理想为 R. 从而 R 的左理想只有 (0) 和 R.

另一方面，设环 R 的左理想只有 (0) 和 R. 对任意的 $u\in R$，由其生成的左理想为 Ru，从而 $Ru=\{0\}$ 或 R. 若 $Ru=\{0\}$，则 $u=1u=0$. 若 $Ru=R$，则存在 $v\in R$，使得 $vu=1$，即 u 为单位. 所以 R 中所有的非零元都是单位，即 R 为斜域.

综上，命题得证.

问题 2.8（交换环的极大理想）：设 R 是交换环，则理想 M 是 R 的极大理想，当且仅当 R/M 是域.

证明 M 是 R 的极大理想，当且仅当 R/M 只有理想 $\{\bar0\}$ 或 R/M（利用第四同构定理），当且仅当 R/M 是域.

问题 2.9（交换环的素理想）：设 R 是交换环，则理想 P 是 R 的素理想，当且仅当 R/P 是整环. 从而，每个 R 的极大理想都是素理想.

证明 一方面，若 P 是素理想，则对任意的 $a,b\in R$，当 $ab\in P$ 时，有 a 或 b 属于 P. 也就是说，对任意的 $\bar a,\bar b\in R/P$，若 $\bar a\bar b=\bar0$，则必有 $\bar a=\bar0$ 或 $\bar b=\bar0$. 结合 R/P 可交换得知，R/P 是整环.

另一方面，若 R/P 是整环，假设 P 不是 R 的素理想，则存在 $a,b\in R$，使得 $ab\in P$，且 $a,b\notin P$. 也就是说，$\bar a,\bar b\in R/P$，$\bar a\bar b=\bar0$，且 $\bar a,\bar b\neq\bar0$，从而 $\bar a,\bar b$ 是 R/P 的零因子，这与 R/P 是整环矛盾！所以 P 是 R 的素理想.

综上，原命题成立.

对于 R 的每个极大理想 M，R/M 是域，从而也是整环，由此可得 M 是素理想.

笔记 素理想的概念看起来不如极大理想直观，不过本例提供了一个不错的理解角度. 另一方面，读者可以尝试寻找 $\mathbb{Z}$ 中的素理想，从而体会素理想与素数的关系.

2.3.4 典型例题

（一）构造商环

判断（或者应用）一个交换环的素理想和极大理想，考虑对应的商环往往要比直接使用定义容易一些.

例题 2.10 在环 $\mathbb{Z}$ 中，取素数 p，证明：

1. 主理想 (p) 是极大理想，从而也是素理想；
2. 主理想 (0) 是素理想，但不是极大理想.

证明

1. 因为 $\mathbb{Z}$ 是交换环，所以 $(p)=p\mathbb{Z}$，于是 $\mathbb{Z}/p\mathbb{Z}\simeq\mathbb{Z}_p$. 由同余类的知识，我们知道 $\mathbb{Z}_p$ 是个域，从而 (p) 是极大理想，从而也是素理想.
2. $(0)=0\mathbb{Z}=\{0\}$，从而 $\mathbb{Z}/(0)=\mathbb{Z}$ 是个整环，于是 (0) 是素理想，但不是极大理想.

笔记 p 为素数时，$\mathbb{Z}_p$ 是域，为了说明这一点，我们只需说明对任意非零的 $\bar{m}\in\mathbb{Z}_p$，存在 $\bar{n}\in\mathbb{Z}_p$ 使得 $\bar{m}\bar{n}=\bar{1}$. 而这等价于对任意非零的正整数 m，存在整数 n,k，使得 $nm+kp=1$，这即是数论中的 Bézout 定理.

练习 2.53 设 R 是交换环. 证明：R 是域，当且仅当 (0) 是极大理想.

证明 (0) 是极大理想，当且仅当 $R\simeq R/(0)$ 是域.

练习 2.54 设 R 是交换环. P 是 R 的素理想，且不包含零因子. 证明：R 是整环.

证明 设 R 有零因子 a，从而存在非零的 b，使得 $ab=0$. 考虑商环 R/P，则有 $\bar{a}\bar{b}=\bar{0}$. 由于 P 是 R 的素理想，所以 R/P 是整环，也就有 $\bar{a}=\bar{0}$，或 $\bar{b}=\bar{0}$.

若 $\bar{a}=\bar{0}$，则 $a\in P$，但 P 中没有零因子，矛盾！$\bar{b}=\bar{0}$ 同样得到矛盾. 从而 R 没有零因子，即 R 是整环.

（二）理想的运算

我们定义了理想的加法、乘积、交三种运算，由此可导出很多的关系式. 在抽象代数的体系下，我们不要求读者利用这些关系式作进一步的推导，但是要能够利用理想的定义证明这些关系.

从思路上而言，此类问题没有什么难点，核心在于搞清楚理想表达式中的元素形式，然后利用理想的定义进行代数变形即可.

例题 2.11 设 I,J,K 是 R 的理想. 证明：

1. $I(J+K)=IJ+IK$，且 $(J+K)I=JI+KI$；
2. 若 $J\subset I$，则 $I\cap(J+K)=J+(I\cap K)$.

证明

1. 一方面，对任意的 $i\in I,j\in J,k\in K$，
$$i(j+k)=ij+ik\subset IJ+IK$$
从而由理想的加法封闭性可得：对一系列的 $i_n\in I,j_n\in J,k_n\in K$，有 $\sum_n i_n(j_n+k_n)\in IJ+IK$，即 $I(J+K)\subset IJ+IK$.
另一方面，对任意的 $i\in I,j\in J,k\in K$，
$$ij=i(j+0)\in I(J+K)$$
$$ik=i(0+k)\in I(J+K)$$
从而由理想的加法封闭性可得：对一系列的 $i_n\in I,j_n\in J,k_n\in K$，有 $\sum_n i_nj_n\in I(J+K),\sum_n i_nk_n\in I(J+K)$，即 $IJ,IK\subset I(J+K)$，从而 $IJ+IK\subset I(J+K)$.
综上，$I(J+K)=IJ+IK$.（另一式同理可证）
2. 一方面，对任意的 $i\in I\cap(J+K)$，存在 $j\in J,k\in K$，使得 $i=j+k$. 因为 $i\in I,j\in J\subset I$，所以 $k=i-j\in I$，即 $k\in I\cap K$，从而 $i=j+k\in J+(I\cap K)$. 也就是 $I\cap(J+K)\subset J+(I\cap K)$.
另一方面，对任意的 $j\in J,k\in I\cap K$，$j+k\in J+I\subset I$，且 $j+k\in J+K$，从而 $j+k\in I\cap(J+K)$. 也就是 $J+(I\cap K)\subset I\cap(J+K)$.
综上，$I\cap(J+K)=J+(I\cap K)$.

笔记 问题的核心在于，搞清楚复杂集合 $(J+K)I,I\cap(J+K)$ 中的元素形式. 其他证明过程都是常规操作，不再分析.

2.3.5 习题

（一）理想的性质

✍ **练习 2.55** 设 $\{I_n\}_n$ 是环 R 的一族理想，证明：$I := \cap_n I_n$ 也是 R 的理想.

证明

1. (加法子群)：I_n 都是 R 的加法子群，从而 $\cap_n I_n$ 也是 R 的加法子群. (子群的交仍是子群)
2. (吸收性)：对任意的 $r \in R$ 和 I_n，有 $rI_n \subset I_n$，从而

$$rI = \cap_n (rI_n) \subset \cap_n I_n = I.$$

同理可得 $Ir \subset I$，从而 I 对 R 的元素有吸收性.

综上，$I \lhd R$.

✍ **练习 2.56** 设 $I_1 \subset I_2 \subset \cdots$ 都是环 R 的理想，证明：$I = \cup_{n=1}^{\infty} I_n$ 是 R 的理想.

证明

1. (加法子群)：首先，I 非空，因为 I_1 是理想，非空. 其次，对任意的 $i, j \in I$，存在指标 m, n，使得 $i \in I_m, j \in I_n$. 由于所有的 I_n 构成包含链，所以不妨设 $I_m \subset I_n$，此时 $i, j \in I_n$. 于是有：

$$i - j \in I_n \subset I$$

即 I 是 R 的加法子群.

2. (吸收性)：任取 $r \in R$. 对任意的 $i \in I$，都存在一个指标 m（与 i 相关），使得 $i \in I_m$，于是：

$$ri \in rI_m \subset I_m \subset I$$

$$ir \in I_m r \subset I_m \subset I$$

从而 $rI \subset I$ 且 $Ir \subset I$.

综上，I 为 R 的理想.

✍ **练习 2.57** 设 I 是环 R 的理想，S 是 R 的子环.

1. 证明：$I \cap S$ 是 S 的理想.
2. 举例说明：S 的理想可以不形如 $I \cap S$.

解 第一小问由环的第二同构定理直接推证.

第二小问，取 $R = \mathbb{Q}$，$S = \mathbb{Z}$. $\mathbb{Q}$ 是域，其理想 I 只可能为 (0) 和 (1)，从而 $S \cap I$ 可能为 (0) 和 $\mathbb{Z}$. 而 $\mathbb{Z}$ 理想 $2\mathbb{Z}$ 不等于 (0) 或 $\mathbb{Z}$，从而 $2\mathbb{Z}$ 不形如 $I \cap S$.

✍ **练习 2.58** 设 I, J 是 R 的理想. 证明：

1. $I + J$ 是包含 I, J 的最小的 R 的理想；
2. IJ 是包含于 $I \cap J$ 的理想；
3. 给出一例满足：$IJ \neq I \cap J$；
4. 若 R 交换，且 $I + J = R$，则 $IJ = I \cap J$.

证明

1. (a). (加法子群)：首先，$I + J$ 非空，因为 I, J 非空. 其次，对任意的 $i, i' \in I$, $j, j' \in J$

$$(i + j) - (i' + j') = (i - i') + (j - j') \in I + J$$

从而 $I + J$ 是 R 的加法子群.

(b). (吸收性)：对任意的 $r \in R$ 和 $i \in J \in J$，有

$$r(i + j) = ri + rj \in rI + rJ \subset I + J$$

从而 $r(I + J) \subset I + J$. 同理可证 $(I + J)r \subset I + J$.

综上 $I + J < R$.

再设 K 是包含 I, J 的 R 的理想. 对任意的 $i \in I, j \in J$，i, j 都是 K 中的元素，所以 $i + j \in K$，从而 $I + J < K$. 这就说明，$I + J$ 是包含 I, J 的最小的 R 的理想.

2. (a). (加法子群)：首先，IJ 非空，因为 I,J 非空. 其次，对任意的 $\sum_n i_n j_n, \sum_m i'_m j'_m \in IJ$，$\sum_n i_n j_n - \sum_m i'_m j'_m \in IJ$（由 IJ 的定义可得）. 从而 IJ 是 R 的加法子群.

   (b). (吸收性)：对任意的 $r \in R$ 和 $\sum_n i_n j_n \in IJ$，有

$$r\sum_n i_n j_n = \sum_n (ri_n) j_n$$

   因为 $I \lhd R$，所以 $ri_n \in I$，于是 $\sum_n (ri_n) j_n \in IJ$. 同理可证，$(\sum_n i_n j_n) r \in IJ$.

   (c). (包含关系)：对任意的 $i_k \in I, j_k \in J$ 有

$$i_k j_k \in i_k J \subset J$$

$$i_k j_k \in I j_k \subset I$$

   从而 $\sum_k i_k j_k \in I \cap J$，也就是 $IJ \subset I \cap J$.

   综上，命题得证.

3. 考虑 $\mathbb{Z}$ 的理想 $2\mathbb{Z}, 4\mathbb{Z}$，则

$$(2\mathbb{Z})(4\mathbb{Z}) = 8\mathbb{Z}$$

$$(2\mathbb{Z}) \cap (4\mathbb{Z}) = 4\mathbb{Z}$$

   从而 $(2\mathbb{Z})(4\mathbb{Z}) \neq (2\mathbb{Z}) \cap (4\mathbb{Z})$.

4. 因为 $R = I + J$，所以存在 $i \in I$, $j \in J$，使得 $1 = i + j$. 对任意的 $s \in I \cap J$，有（注意到 $s \in I$ 且 $s \in J$.）

$$s = s1 = s(i+j) = si + sj = is + sj \in IJ$$

   即 $I \cap J \subset IJ$. 结合前一小问的 $IJ \subset I \cap J$，可得 $IJ = I \cap J$.

✍ **练习 2.59** 设 R 是交换环. $I = (a_1, \cdots, a_n), J = (b_1, \cdots, b_m)$ 是 R 的两个有限生成的理想. 证明：理想 IJ 可由元素 $a_i b_j, i \in \{1, \cdots, n\}, j \in \{1, \cdots, m\}$ 生成.

证明 由元素 $a_i b_j, i \in \{1, \cdots, n\}, j \in \{1, \cdots, m\}$ 生成的理想为 $K := \langle a_i b_j \rangle_{i \in \{1,\cdots,n\}, j \in \{1,\cdots,m\}}$.

一方面，对任意 K 中的元素 $r := \sum_k a_k b_k$，因为 $a_k \in I, b_k \in J$，所以 $r \in IJ$，从而 $K \subset IJ$.

另一方面，对任意的 IJ 中的元素 $r := \sum_k a_k b_k$，同样它是 K 中的元素，所以 $IJ \subset K$.

综上，$IJ = K$.

（二）素理想、极大理想

✍ **练习 2.60** 设 R 是 $[0,1]$ 上全体连续实函数构成的环，定义函数的集合 I

$$I := \{f \in R : f(1/3) = f(1/2) = 0\}$$

证明：I 是 R 的理想，但不是素理想.

证明 先证明：$I \lhd R$.

1. (加法子群)：首先，零映射在 I 中. 其次，对任意的 $f, g \in I$，

$$(f-g)\left(\frac{1}{3}\right) = f\left(\frac{1}{3}\right) - g\left(\frac{1}{3}\right) = 0$$

$$(f-g)\left(\frac{1}{2}\right) = f\left(\frac{1}{2}\right) - g\left(\frac{1}{2}\right) = 0$$

   即 $f - g \in I$. 从而 I 是 R 的加法子群.

2. (吸收性)：对任意的 $r \in R, f \in I$，有

$$(rf)\left(\frac{1}{3}\right) = r\left(\frac{1}{3}\right) f\left(\frac{1}{3}\right) = 0$$

$$(rf)\left(\frac{1}{2}\right) = r\left(\frac{1}{2}\right) f\left(\frac{1}{2}\right) = 0$$

   即 $rf \in I$. 类似可证 $fr \in I$. 从而 I 对 R 的元素有吸收性.

综上，$I \lhd R$.

下证 I 不是素理想. 考虑商环 R/I，并考虑元素 $\overline{x-\frac{1}{3}}$ 和 $\overline{x-\frac{1}{2}}$，二者均不等于 $\bar{0}$，但乘积 $\overline{(x-\frac{1}{3})(x-\frac{1}{2})}$ 是 $\bar{0}$，所以二者是 R/I 的零因子，从而 R/I 不是整环，I 不是素理想.

✍ **练习 2.61*** 设 R 是 Bool 环，证明：

1. R 的每个素理想 P 都是极大理想；
2. R 的每个有限生成理想，都是主理想.

证明

1. 首先，R 是交换环. 其次，对任意非零的 $\bar{x} \in R/P$，因为 $x^2 = x$，所以 $(\bar{x})^2 = \bar{x}$，即 $\bar{x}(\bar{x}-\bar{1}) = \bar{0}$. 由于 R/P 是整环，所以 $\bar{x}-\bar{1} = \bar{0}$，即 $\bar{x} = \bar{1}$，也就是说，所有非零的 $\bar{x}$ 都是 R/P 中的单位，所以 R/P 是域，即 P 是 R 的极大理想.
2. 先证明：对任意的 $x, y \in R$，有 $(x,y) = (xy+x+y)$. 一方面，显然有 $xy+x+y \in (x,y)$，所以 $(xy+x+y) \subset (x,y)$. 另一方面：

$$x(xy+x+y) = x^2y + x^2 + xy = xy + x + xy = x$$
$$y(xy+x+y) = xy^2 + xy + y^2 = xy + xy + y = y$$

于是 $x, y \in (xy+x+y)$，从而 $(x,y) \subset (xy+x+y)$. 综上，$(x,y) = (xy+x+y)$.

对于 R 的有限生成理想 $(a_1, \cdots, a_n)$，取

$$b_1 := a_1$$
$$b_i := b_i + a_{i+1} + b_i a_{i+1} \quad (i \in \{2, \cdots n-1\})$$

利用先证的结论可得：

$$\begin{aligned}(a_1, \cdots, a_n) &= (b_2, a_3, \cdots, a_n) \\ &= (b_3, a_4, \cdots, a_n) \\ &= (b_{n-1})\end{aligned}$$

即有限生成理想是主理想.

✍ **练习 2.62** 设 R 是环，M 是 R 的理想，R/M 是域. 证明：M 是极大理想.

证明 对任意包含 M 的 R 的理想 I，由于 $M \subset I \subset R$，所以 $M/M \subset I/M \subset R/M$，即 I/M 是 R/M 的理想（第四同构定理）. 由于 R/M 是域，所以其理想只有可能是 $\{\bar{0}\}$ 或 R/M，从而 $I/M = \{\bar{0}\}$ 或 R/M. 所以 $I = M$ 或 R，即 M 是极大理想.

笔记 此题中没有假设 R 是交换环.

✍ **练习 2.63** 设 R 是整环，$a, b \in R$. 证明：$(a) = (b)$，当且仅当存在单位 $u \in R$，使得 $a = ub$.

证明 一方面，若 $(a) = (b)$，则存在 $u, v \in R$，使得 $a = ub$ 且 $va = b$. 于是 $a = ub = uva$，即 $(uv-1)a = 0$.

1. 若 $a = 0$，则 $(b) = (0)$，即 $b = 1b = 0$，此时 $a = 1b$.
2. 若 $a \neq 0$，则 $uv - 1 = 0$，即 $uv = 1$，从而存在单位 u，使得 $a = ub$.

综上，存在 $u \in R^\times$，使得 $a = ub$.

另一方面，若存在 $u \in R^\times$，使得 $a = ub$，则 $(a) = Ra = Rub \subset Rb = (b)$. 另一方面，$u^{-1}a = u^{-1}ub = b$，则 $(b) = Rb = Ru^{-1}a \subset Ra = (a)$. 于是 $(a) = (b)$.

✍ **练习 2.64** 设 R 是交换环，I, J 是 R 的理想，P 是 R 的素理想，且包含 IJ. 证明：I 或 J 包含于 P.

证明 假设 I, J 都不包含于 P，也就是说，存在 $i \in I, j \in J$，$i, j \notin P$. 考虑商环 R/P，因为 $ij \in IJ \subset P$，所以 $\bar{i}\bar{j} = \bar{0}$. 因为 P 是素理想，所以 R/P 是整环，从而必有 $\bar{i} = \bar{0}$ 或 $\bar{j} = \bar{0}$. 如果 $\bar{i} = \bar{0}$，则 $i \in P$，矛盾！同理 $\bar{j} = \bar{0}$ 一样导出矛盾！. 原命题得证.

✍ **练习 2.65** 设 $\varphi : R \to S$ 是交换环的环同态. 证明：

1. 若 P 是 S 的素理想，则 $\varphi^{-1}(P)$ 要么等于 R，要么是 R 的素理想；

2. 若 R 是 S 的子环，P 是 S 的素理想，则 $P\cap R$ 要么等于 R，要么是 R 的素理想；
3. 若 M 是 S 的极大理想，φ 是满射，则 $\varphi^{-1}(M)$ 是 R 的极大理想. 当 φ 不是满射时，试举一反例.

证明

1. 首先，$\varphi^{-1}(P)$ 确实是 R 的理想（参见上一节习题）. 其次，对任意的 $a,b\in R$，若 $ab\in\varphi^{-1}(P)$，则 $\varphi(ab)\in P$，从而 $\varphi(a)\varphi(b)\in P$. 由于 P 是 S 的素理想，所以 $\varphi(a)\in P$ 或 $\varphi(b)\in P$，即 $a\in\varphi^{-1}(P)$ 或 $b\in\varphi^{-1}(P)$. 从而当 $\varphi^{-1}(P)\neq R$ 时，其为素理想. 否则 $\varphi^{-1}(P)=R$.
2. 取 $\varphi:R\to S$ 是嵌入映射 $r\mapsto r$，则 $\varphi^{-1}(P)=P\cap R$，利用第一小题的结论即证.
3. 首先，$\varphi^{-1}(M)$ 确实是 R 的理想. 其次，对 R 的任意理想 I，若 $\varphi^{-1}(M)\subset I\subset R$，则 $M\subset\varphi(I)\subset S$. 由于 φ 为满射，所以 $\varphi(I)$ 是 S 的理想（参见上一节习题）. 又因为 M 是 S 的极大理想，所以 $\varphi(I)=M$ 或 S，也就是说，$I=\varphi^{-1}(M)$ 或 R，即 $\varphi^{-1}(M)$ 是 R 的极大理想.

   当 φ 不是满射时，例如取 φ 为

$$\varphi:\mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}$$
$$x\mapsto(x,0)$$

   再取 $M=\mathbb{Z}\times 2\mathbb{Z}$，则 $(\mathbb{Z}\times\mathbb{Z})/M\simeq\mathbb{Z}_2$ 为域，从而 M 是 $\mathbb{Z}\times\mathbb{Z}$ 的极大理想. 而 $\varphi^{-1}(M)=\mathbb{Z}$，不是 $\mathbb{Z}$ 的极大理想.

✍ **练习 2.66** 设 R 是有限交换群，证明：R 的每个素理想都是极大理想.

证明 设 P 是 R 的素理想，从而 R/P 是整环（即为有限整环）. 而有限整环都是域，从而 P 是极大理想.

✍ **练习 2.67** 设 R 是交换环，且对任意的 $a\in R$，都存在正整数 $n>1$，使得 $a^n=a$. 证明：R 的每个素理想都是极大理想.

证明 设 P 是 R 的素理想，则 R/P 是整环. 下证：R/P 是域.（从而 P 是极大理想）

对任意的 $\bar a\in R/P$，因为存在正整数 $n>1$，使得 $a^n=a$，所以 $(\bar a)^n=\bar a$，即 $((\bar a)^{n-1}-\bar 1)(\bar a)=\bar 0$. 由于 R/P 是整环，所以 $\bar a=\bar 0$，或 $(\bar a)^{n-1}=\bar 1$. 当 $\bar a\neq\bar 0$ 时，$\bar a=\bar 1$ $(n=2)$，或者 $\bar a(\bar a)^{n-2}=\bar 1$ $(n>2)$，不论哪一种情况，$\bar a$ 都为 R/P 中的单位. 从而 R/P 中的所有非零元都是单位，即 R/P 是域. 由此即证 P 是 R 的极大理想，原命题得证.

（三）多项式环的商环

✍ **练习 2.68** 设 $x^2+x+1\in R:=\mathbb{Z}_2[x]$，考虑商环 $\bar R:=\mathbb{Z}_2[x]/(x^2+x+1)$.

1. 证明：$\bar R$ 有四个元素 $\bar 0,\bar 1,\bar x,\overline{x+1}$；
2. 证明：加群 $(\bar R,+)$ 同构于 V_4；
3. 证明：乘群 $(\bar R^\times,\cdot)$ 同构于 $\mathbb{Z}_3$. 从而 $\bar R$ 是域.

笔记 读者可以把元素的加法表和乘法表列出，从而熟悉商环的元素运算.

✍ **练习 2.69** 设 R 是交换环. 证明：

1. 主理想 (x) 是 $R[x]$ 中的素理想，当且仅当 R 是整环；
2. 主理想 (x) 是 $R[x]$ 中的极大理想，当且仅当 R 是域.

注 提示：证明 $R[x]/(x)\simeq R$.

✍ **练习 2.70** 设 R 是交换环，x 是未定元，$f(x)\in R[x]$ 是次数 $n\geqslant 1$ 的首一多项式. 考虑商环 $R[x]/(f(x))$. 证明：

1. 商环 $R[x]/(f(x))$ 中的元素都形如 $\overline{p(x)}$，其中多项式 $p(x)\in R[x]$ 的次数小于 n；
2. 若 $p(x),q(x)\in R[x]$ 不相同，且次数均小于 n，则 $\overline{p(x)}\neq\overline{q(x)}$；
3. 若 $f(x)=a(x)b(x)$，且 $a(x),b(x)$ 的次数均小于 n，则 $\overline{a(x)}$ 是 $R[x]/(f(x))$ 的零因子；
4. 若 $f(x)=x^n-a$，且 $a\in R$ 是幂零元，则 $\bar x$ 是 $R[x]/(f(x))$ 的幂零元；
5. 设 p 是素数，$R=\mathbb{Z}_p$，$f(x)=x^p-a$，$a\in\mathbb{Z}_p$，则 $\overline{x-a}$ 是 $R[x]/(f(x))$ 的幂零元.

注 提示：

第一小题：设 $f(x)=x^n+b_{n-1}x^{n-1}+\cdots+b_0$，则 $\overline{x^n}=-\overline{b_{n-1}x^{n-1}}-\cdots-\overline{b_0}$. 从而，当 $p(x)$ 的次数大于 n 时，反复利用前式即可将 $\overline{p(x)}$ 的次数降至不超过 $n-1$ 次.

第二小题：若 $\overline{p(x)}=\overline{q(x)}$，则

$$\overline{p(x)-q(x)}=\bar{0}$$

即 $p(x)-q(x)\in(f(x))$，从而 $p(x)-q(x)$ 为 $f(x)$ 的倍元. 当 $p(x)-q(x)\neq 0$ 时，它的次数只能为 $\deg f=n$ 的倍数. 但是 p,q 的次数都小于 n，所以它们的差的次数也必然小于 n，矛盾！所以只能有 $p(x)=q(x)$.

第三小题：我们有

$$\begin{aligned}\bar{0}&=\overline{f(x)}\\&=\overline{a(x)b(x)}\\&=\overline{a(x)b(x)}.\end{aligned}$$

第四小题：因为 a 幂零，所以存在正整数 k，使得 $a^k=0$，从而 $(\bar{a})^k=\bar{0}$. 又因为 $(\bar{x})^n=\bar{a}$，所以 $(\bar{x})^{nk}=(\bar{a})^k=\bar{0}$.

第五小题：Z_p 中有：

$$\begin{aligned}(\overline{x-a})^p&=(\bar{x}-\bar{a})^p\\&=\sum_{i=0}^{p}C_p^i(\bar{x})^i(-\bar{a})^{p-i}\\&=(\bar{x})^p+(-\bar{a})^p\qquad\qquad(i\neq 0,p\text{时，}C_p^i\text{是 }p\text{ 的倍数，从而为零})\end{aligned}$$

若 $p=2$，则 $(-\bar{0})^2=-\bar{0},(-\bar{1})^2=-\bar{1}$，从而有 $(-\bar{a})^p=-\bar{a}$.

若 p 为其他素数，则必是奇数，从而有

$$(-\bar{a})^p=-(\bar{a})^p=-\bar{a}$$

其中最后一个等号成立，是因为费马小定理.

综上，原式可进一步化简为：

$$\begin{aligned}(\overline{x-a})^p&=(\bar{x})^p+(-\bar{a})^p\\&=(\bar{x})^p-\bar{a}\\&=\overline{x^p-a}\\&=\bar{0}.\end{aligned}$$

2.4 拓展：Zorn 引理、极大子群和极大理想

2.4.1 任意笛卡尔积

给定两个集合 A,B，它们的笛卡尔积我们是非常熟悉的：

$$A\times B:=\{(a,b):a\in A,b\in B\}$$

类似地，给定一族集合 $\{A_i\}_{i\in I}$，其中 I 是指标集，我们可类似定义它们的笛卡尔积：

$$\prod_{i\in I}A_i:=\{(a_i)_{i\in I}:a_i\in A_i\}$$

其中描述元素的方式 $(a_i)_{i\in I}$ 多少有些抽象，我们可以借助选择函数来描述. 一般的，对于一族集合 $\{A_i\}_{i\in I}$，我们定义一个选择函数为

$$f:I\to\cup_{i\in I}A_i$$

使得对任意的 $i \in I$ 都有 $f(i) \in A_i$. 从而笛卡尔积 $\prod_{i\in I} A_i$ 中的元素 $(a_i)_{i\in I}$ 总是和选择函数 $f : i \mapsto a_i$ 是一一对应的.

同时，已知一个笛卡尔积 $\prod_{i\in I} A_i$，就必然会有投影映射：

$$\pi_i : \prod_{j\in I} A_j \to A_i$$
$$(a_j)_{j\in I} \mapsto a_i$$

2.4.2 偏序集和 Zorn 引理

在一些集合上，我们可以对其中的元素排序（例如 $\mathbb{R}$），有些集合就没有这样的性质（例如 $\mathbb{C}$），受此启发，我们定义集合的某种序关系.

定义 2.1 (偏序关系)

非空集合 A 的一个关系 $\leqslant$ 被称为是偏序的，若其满足如下条件：

1. (自反性)：对任意的 $a \in A$，有 $a \leqslant a$；
2. (反对称性)：对任意的 $a, b \in A$，若 $a \leqslant b$ 且 $b \leqslant a$，则 $a = b$；
3. (传递性)：对任意的 $a, b, c \in A$，若 $a \leqslant b$ 且 $b \leqslant c$，则 $a \leqslant c$.

♣

定义 2.2 (全序关系)

非空集合 A 的一个关系 $\leqslant$ 被称为是全序的，若其满足如下条件：

1. (完全性)：对任意的 $a, b \in A$，都有 $a \leqslant b$ 或 $b \leqslant a$；
2. (反对称性)：对任意的 $a, b \in A$，若 $a \leqslant b$ 且 $b \leqslant a$，则 $a = b$；
3. (传递性)：对任意的 $a, b, c \in A$，若 $a \leqslant b$ 且 $b \leqslant c$，则 $a \leqslant c$.

♣

定义 2.3 (良序关系)

非空集合 A 的一个关系 $\leqslant$ 被称为是良序的，若其满足如下条件：

1. (全序)：$\leqslant$ 是 A 上的全序关系；
2. (极小元)：A 的任意非空子集都有极小元（即对任意的 $B \subset A$，都存在 $s \in B$，使得任意的 $b \in B$ 都满足 $s \leqslant b$）.

♣

我们在抽代里学到了不少的偏序关系：

例题 2.12 定义集合 S 为群 G 的所有子群构成的集合. 关系“$<$”定义为：$M < N$ 当且仅当 M 是 N 的子群. 则“$<$”为 S 上的偏序关系.

例题 2.13 定义集合 S 为环 R 的所有理想构成的集合. 关系“$<$”定义为：$M < N$ 当且仅当 M 包含于 N. 则“$<$”为 S 上的偏序关系.

例题 2.14 任取一个整环 R，关系“$|$”定义为：$r|s$ 当且仅当 r 整除 s. 则“$|$”为 R 上的偏序关系.

例题 2.15 定义集合 S 为循环群 $\mathbb{Z}_{p^n}$ 的所有子集构成的集合，其中 p 为素数，n 为正整数. 关系“$<$”定义为：$M < N$ 当且仅当 M 是 N 的子群. 则“$<$”为 S 上的全序关系. 进一步的，他也是良序关系.

在给定偏序关系后，马上就会有如下相关概念：

定义 2.4 (链、上界、极大元)

设 A 为非空集合，$\leqslant$ 为其上的一个偏序关系.

1. A 的子集 B 被称作是一个链（或全序子集），如果对任意的 $x, y \in B$，有 $x \leqslant y$ 或 $y \leqslant x$.
2. A 的子集 B 的一个上界，指的是元素 $u \in A$，且对任意的 $b \in B$，有 $b \leqslant u$.

3. A 的极大元指的是元素 $m \in A$，其满足：对任意的 $a \in A$，若 $m \leqslant a$，则 $m = a$. ♣

再经过上述铺垫后，我们就可以介绍 Zorn 引理了.

定理 2.1 (Zorn 引理)

若 A 是非空偏序集，且每个链都有上界，则 A 必有极大元. ♡

有意思的是，Zorn 引理名为“引理”，实际上在集合论中（Zermelo-Fraenkel 系统）是以公理形式出现的. 我们还有两个和 Zorn 引理等价的命题，它们也非常常见.

定理 2.2 (选择公理)

任意由非空集合构成的集族的笛卡尔积是非空的. 换言之，若 I 是任意非空指标集，对任意的 $i \in I$，A_i 都是非空集，则存在一个从 I 到 $\cup_{i\in I}A_i$ 的选择函数. ♡

定理 2.3 (良序原则)

每个非空集合 A 都有一个其上的良序. ♡

利用 Zorn 引理就可以进行群的极大子群和环的极大理想的讨论了.

2.4.3 极大子群

练习 2.71 群 G 的子群 M 被称为是极大子群，如果 $M \neq G$，且唯一包含 M 的 G 的子群是 G. 证明：

1. 若 H 是有限群 G 的真子群，则存在一个包含 H 的 G 的极大子群；
2. 在二面体群 $D_{2n} = \langle r, s\rangle$ 中，$\langle r\rangle$ 是 D_{2n} 的极大子群；
3. 设 $G = \langle x\rangle$ 是 n 阶循环群，则子群 H 是极大子群，当且仅当 $H = \langle x^p\rangle$，其中素数 p 整除 n.

证明

1. 首先，存在一个 G 的子群 N，使得 H 真包含于 N（取 $N = G$ 即可）. 如果 N 只能取 G，则 H 即为 G 的极大子群，原命题成立. 下设 H 不是 G 的极大子群，从而存在 G 的子群 N_1，使得 H 真包含于 N_1，且 N_1 真包含于 G，从而 $|H| < |N_1| < |G|$. 以下对 N_1 做类似地讨论：若 N_1 已经是 G 的极大子群，则讨论停止；否则又存在一个 G 的真子群 N_2，使得 N_1 真包含于 N_2，并且 $|N_1| < |N_2| < |G|$. 注意到每多一次这样的讨论，得到的新的更大的真子群的阶数都要增加（至少加一），而 G 是有限群，从而这样的过程不可能一直持续下去，于是我们就得到了一个有限的升链：
$$H < N_1 < N_2 < \cdots < N_k < G$$
此时 N_k 即为 G 的极大子群，且包含 H. 综上，原命题得证.
2. 首先，$H = \langle r\rangle$ 是 D_{2n} 的真子群. 其次，若存在一个 D_{2n} 的子群 M 真包含 H，由于 H 中包含了所有的 r 的幂次，从而 M 中必然存在一个元素 sr^i，于是 $s = (sr^i)r^{-i} \in M$，即 $r, s \in M$，从而 $M = D_{2n}$. 于是 H 为 D_{2n} 的真子群.
3. 首先，G 的子群都可以写为 $\langle x^m\rangle$，其中 m 为 n 的因子. 下证：$\langle x^m\rangle$ 是 $\langle x^l\rangle$ 的真子群，当且仅当 $l|m$，且 $l \neq m$. 一方面，当 $l|m$，且 $l \neq m$ 时，$x^m = x^{kl} \in \langle x^l\rangle$（存在某个整数 k），从而 $\langle x^m\rangle$ 是 $\langle x^l\rangle$ 的子群. 结合 $l \neq m$ 可知，两个子群并不相等，所以是真包含. 另一方面，若 $\langle x^m\rangle$ 是 $\langle x^l\rangle$ 的真子群，则 $m \neq l$，且 $x^m \in \langle x^l\rangle$，从而 $x^m = x^{kl-an}$，其中 k, a 都是整数，并且使得 $kl - an \in [0, n)$（这一点可以由整数的带余除法保证），从而有 $m = kl - an$. 注意到 $l|n$，从而等式右侧整除 l，从而 $l|m$，且 $m \neq l$.
回到原题，若 $H = \langle x^p\rangle$ 是极大子群，假设 p 不是素数，从而有真因子分解 qr，于是子群 $M = \langle x^q\rangle$ 真包含 H，且不等于 G，与极大子群的定义矛盾！从而若 $H = \langle x^p\rangle$ 是极大子群，则 p 是素数. 另一方面，若 p 是素数，由于 p 的真因子只有 1，所以真包含 $H = \langle x^p\rangle$ 的 G 的子群只有 $G = \langle x\rangle$，于是 H 为极大子群. 综

上，原命题得证.

✍ **练习 2.72** 设 $G=\langle g_1,g_2,\cdots,g_n\rangle$ 是有限生成群，S 是 G 的所有真子群构成的集合.

1. 证明：集合的包含关系“$\subset$”是集合 S 上的偏序关系.
   以下记 C 是 S 中的一个链.
2. 证明：$H=\cup_{N\in C}N$ 是 G 的子群.
3. 证明：H 是 G 的真子群.
4. 证明：S 有极大元.

证明

1. 容易验证，S 上的关系“$\subset$”满足自反性、反对称性和传递性，所以是偏序关系.
2. 首先，C 是非空集，所以 H 非空. 其次，对任意的 $x,y\in H$，必然存在 $M,N\in C$，使得 $x\in M,y\in N$. 由于 C 为链，所以必有 $M\subset N$ 或 $N\subset M$. 不妨设 $M\subset N$，于是 $x,y\in N$. 又因为 N 为子群，所以
   $$x^{-1}y\in N\subset H.$$
   综上，$H<G$.
3. 假设 $H=G$，于是每个 $g_i\in H$，从而存在 C 中的子群 $N_1,\cdots,N_n$，使得每个 $g_i\in N_i$. 由于 C 是链，所以所有的 N_i 之间都有包含关系，不妨设 $N_1\subset N_2\subset\cdots\subset N_n$，于是所有的 $g_i\in N_n$，即 $G=\langle g_1,g_2,\cdots,g_n\rangle\subset N_n$. 而 N_n 是 G 的真子群，矛盾！所以 H 是 G 的真子群.
4. 由前一小题可知，S 中的每个链都有上界 H，从而由 Zorn 引理可知，S 有极大元.（并且这一极大元就是 G 的一个极大子群：记 M 为 S 的极大元，从而对 S 中的任意元素 N，若 $M\subset N$，则 $M=N$，即 G 中包含 M 的真子群只有 G.）

2.4.4 极大理想

我们以环中极大理想的存在性作为本节的结束.

定理 2.4 (极大理想的存在性)

环中任意真理想都包含于某个极大理想之中.

♡

证明 设环为 R，I 是 R 的一个真理想.，S 是 R 的所有包含 I 的真理想构成的集合. 于是 S 非空（$I\in S$），且集合的包含关系“$\subset$”是 S 上的偏序关系. 记 C 是 S 中的一个链，并记 $J=\cup_{A\in C}A$.

1. 证明：J 是 R 的理想.
   首先，J 非空（因为 S 非空，所以 C 非空）.
   其次，对任意的 $a,b\in J$，存在 C 中的理想 A,B，使得 $a\in A,b\in B$. 并且由于 C 是链，所以必有 $A\subset B$ 或 $B\subset A$. 不妨设 $A\subset B$，从而 $a,b\in B$，于是 $a-b\in B\subset J$，即 J 是加法子群.
   最后，对于任意的 $r\in R$，$a\in J$，必有 C 中的理想 A，使得 $a\in A$，从而 $ra\in rA\subset A\subset J$，且 $ar\in Ar\subset A\subset J$，即 J 有乘法的吸收性.
   综上，J 是 R 的理想.
2. 证明：乘法逆元 1 不是 J 中的元素（从而 J 是 R 的真理想）.
   假设 $1\in J$，则必然存在 C 中的理想 A，使得 $1\in A$. 而 A 是 R 的真理想，所以不包含 1，矛盾！
3. 证明：S 有极大元（按定义即为极大理想）.
   由前两小题可知，S 中的每个链都有上界 J，从而由 Zorn 引理可知，S 有极大元.

2.5 中国剩余定理

2.5.1 知识要点

1. 互素（或互极大）：交换环 R 的理想 I, J 是互素的，如果 $I + J = R$.
2. （中国剩余定理）：设 R 是交换环，$\{I_i\}_{i\in[1,n]}$ 是一族两两互素的 R 的理想. 定义映射

$$\pi : R \to R/I_1 \times R/I_2 \times \cdots \times R/I_n$$
$$a \mapsto (a + I_1, \cdots, a + I_n)$$

则有：

(a). π 是环满同态，核为 $\cap_{i=1}^{n} I_i = I_1 \cdots I_n$.

(b). 有环同构

$$R/(I_1 \cdots I_n) \simeq R/I_1 \times \cdots \times R/I_n$$

3. （同余形式的中国剩余定理）：设 R 是交换环，$\{I_i\}_{i\in[1,n]}$ 是一族两两互素的 R 的理想. 则对任意的 $a_1, \cdots, a_n \in R$，都存在 $x \in R$，使得

$$\begin{cases} x & \equiv a_1 \mod I_1 \\ & \cdots \\ x & \equiv a_n \mod I_n \end{cases}$$

4. （整数环上的中国剩余定理）：设正整数 n 的素因子分解为 $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$，于是有环同构

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$$

特别的，有乘群的同构

$$\mathbb{Z}_n^{\times} \simeq \mathbb{Z}_{p_1^{\alpha_1}}^{\times} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}^{\times}$$

2.5.2 知识要点解读

（一）中国剩余定理的证明

本节的核心知识点就是中国剩余定理，这一名称的来源我们放到本节的最后做简单的介绍，同时给出一次同余方程组的一种解法.

如果我们简单的概括中国剩余定理讲了一个什么结论，那就是：交换环对理想乘积的商，同构于交换环对理想的商的直积. 这里我们给出一个不依赖于“同余方程有解”的中国剩余定理的证法.

问题 2.10 （中国剩余定理）：设 R 是交换环，$\{I_i\}_{i\in[1,k]}$ 是一族两两互素的 R 的理想. 定义映射

$$\pi : R \to R/I_1 \times R/I_2 \times \cdots \times R/I_k$$
$$a \mapsto (a + I_1, \cdots, a + I_k)$$

则有：

1. π 是环满同态，核为 $\cap_{i=1}^{k} I_i = I_1 \cdots I_k$.
2. 有环同构

$$R/(I_1 \cdots I_k) \simeq R/I_1 \times \cdots \times R/I_k$$

证明

1. （互素理想的性质）：先证明：若 R 的理想 A, B, C 两两是互素的，则 A 和 BC 也是互素的. 由于 $A + BC$ 是理想，从而只需证：$1 \in A + BC$. 因为 $A + B = R, A + C = R$，所以存在 $a, a' \in A, b \in B, c \in C$，使得

$a+b=1, a'+c=1$，于是：

$$\begin{aligned}1&=(a+b)(a'+c)\\&=(aa'+ac+a'b)+bc\\&\in A+BC\end{aligned}$$

由此利用数学归纳法不难得到：对于一族互素的理想 $\{I_i\}_{i=1}^{m+1}$，I_{m+1} 和 $I_1\cdots I_m$ 是互素的.

2. (π 是环同态)：略.
3. (π 是满射，以及导出的同构)：以下对理想的个数 k 做数学归纳.

我们先证明 $k=2$ 的情形. 记 $I_1=A, I_2=B$. 从而下证：

$$\begin{aligned}\pi: R&\to R/A\times R/B\\a&\mapsto (a+A, a+B)\end{aligned}$$

是环满同态，且有同构：

$$R/(AB)\simeq R/A\times R/B.$$

因为 $A+B=R$，所以存在 $x\in A, y\in B$，使得 $x+y=1$. 我们有

$$\begin{aligned}\pi(x)&=\pi(1-y)=(\bar{0},\bar{1})\\\pi(y)&=\pi(1-x)=(\bar{1},\bar{0})\end{aligned}$$

从而对任意的 $(r+A, s+B)\in R/A\times R/B$，有：

$$\begin{aligned}\pi(ry+sx)&=\pi(r)\pi(y)+\pi(s)\pi(x)\\&=(\bar{r},\bar{r})(\bar{1},\bar{0})+(\bar{s},\bar{s})(\bar{0},\bar{1})\\&=(\bar{r},\bar{s})\end{aligned}$$

即 π 是满射.

$A\cap B=AB$ 的证明参见 2.3 节练习 2.53，从而 $\ker\varphi=A\cap B=AB$，然后利用环第一同构定理即得：

$$R/(AB)\simeq R/A\times R/B.$$

假设 $k=m$ 时，$\pi: R\to R/I_1\times\cdots\times R/I_m$ 是环满同态，且有同构

$$R/(I_1\cdots I_m)\simeq R/I_1\times\cdots\times R/I_m$$

当 $k=m+1$ 时，令 $A=I_1\cdots I_m, B=I_{m+1}$，我们有：

$$\begin{aligned}\varphi: R&\to R/A\times R/B\\a&\mapsto (a+A, a+B)\end{aligned}$$

是环满同态. 核为 AB. 由归纳假设，有环同构

$$\psi: R/A\xrightarrow{\sim} R/I_1\times\cdots\times R/I_m$$

从而可以有环同构

$$\psi': R/A\times R/B\xrightarrow{\sim} R/I_1\times\cdots\times R/I_{m+1}$$

取 $\pi:=\psi'\circ\varphi$，则 π 是环满同态，核为 AB，进而导出欲证环同构.

综上，原命题成立.

笔记 $k=2$ 这个特殊情况的证明中，难点在于证明满射，也就是为任意的 $(\bar{r},\bar{s})$ 寻找一个原象. 我们利用 $x+y=1$，巧妙地构造出了“基” $(\bar{0},\bar{1}), (\bar{1},\bar{0})$，然后找出了原象 $ry+sx$（他是一个关于 x, y 的线性组合，而线性组合是我们喜欢看到的东西，我们有很多的处理技巧）. 这一技巧以后也是用得到的，所以读者一定要理解它. 从这里我们也能看出“互素”这个条件的意义，它确保了这样对 1 的拆分是可行的.

然后在进行归纳递推的时候，我们想办法把一般情况变形为 $k=2$ 时的情形. 这里的变形思路不是很容易独

立想出，需要我们对理想的运算非常熟悉，因此读者只需对照前文理清思路即可，不用过于关注这里的处理细节（笔者目前没有在其他地方看到类似思路的应用）.

2.5.3 习题

环 R 的元素 e 被称为幂等的，如果 $e^2=e$.

环 R 的元素 e 被称为中心幂等的，如果 $e^2=e$，且 $e\in Z(R)$（即对任意的 $r\in R$，有 $er=re$）.

练习 2.73 设 e 是环 R 的中心幂等元，证明：

1. $Re, R(1-e)$ 都是 R 的理想；
2. $Re, R(1-e)$ 都是环，其中 e 是环 Re 的乘法幺元，$1-e$ 是环 $R(1-e)$ 的乘法幺元.
3. $R\simeq Re\times R(1-e)$.

证明

1. 我们只验证乘法的封闭性，其余未尽事宜留给读者. 对任意的 $r\in R$，有
$$\begin{aligned} r(Re)&=(rR)e\subset Re\\ (Re)r&=Rre\subset Re\\ r(R(1-e))&=(rR)(1-e)\subset R(1-e)\\ R(1-e)r&=Rr(1-e)\subset R(1-e)\end{aligned}$$
所以 $Re, R(1-e)$ 都是 R 的理想.
2. 我们只验证乘法的封闭性和幺元，其余未尽事宜留给读者. 在 Re 中，对任意的 $r,r'\in R$ 有
$$\begin{aligned}(re)(r'e)&=r(er')e=rr'e^2=rr'e\in Re\\ (re)e&=re^2=re=ree=ere=e(re)\end{aligned}$$
而在 $R(1-e)$ 中，对任意的 $r,r'\in R$ 有
$$\begin{aligned}r(1-e)r'(1-e)&=rr'(1-e)^2=rr'(1-2e+e^2)=rr'(1-e)\in R(1-e)\\ (r(1-e))(1-e)&=r(1-e)=r(1-e)(1-e)=(1-e)(r(1-e))\end{aligned}$$
3. 定义“自然映射”
$$\begin{aligned}\varphi: R&\to Re\times R(1-e)\\ r&\mapsto (re, r(1-e))\end{aligned}$$
容易验证 φ 是环同态. 下证：φ 是满射. 我们有
$$\begin{aligned}\varphi(e)&=(e,0)\\ \varphi(1-e)&=(0,1-e)\end{aligned}$$
所以对于任意的 $(re, s(1-e))\in Re\times R(1-e)$，有
$$\begin{aligned}\varphi(re+s(1-e))&=\varphi(re)+\varphi(s(1-e))\\ &=\varphi(r)\varphi(e)+\varphi(s)\varphi(1-e)\\ &=(re,r(1-e))(e,0)+(se,s(1-e))(0,1-e)\\ &=(re,0)+(0,s(1-e))\\ &=(re,s(1-e))\end{aligned}$$
从而 φ 是满同态.

最后求 φ 的核：

$$\begin{aligned}\ker\varphi &= \{r\in R : (re, r(1-e)) = (0,0)\}\\ &= \{0\}\end{aligned}$$

所以 φ 是单射，即有同构 $R \simeq Re \times R(1-e)$.

笔记 读者可以证明：环 Re 是以 e 为乘法幺元的环，$R(1-e)$ 是以 $1-e$ 为乘法幺元的的环，但是他们不是 R 的子环（因为乘法幺元不一样）.

练习 2.74 环 R 中的幂等元 e, e' 被称为正交的，如果 $ee' = 0 = e'e$. 设 $R, R_1, \cdots, R_n$ 是环，则下列条件等价：

1. $R \simeq R_1 \times \cdots \times R_n$；
2. R 具有两两正交的中心幂等元 $e_1, \cdots, e_n$，使得 $e_1 + \cdots + e_n = 1_R$，且 $Re_i \simeq R_i$.

注 提示：考虑 $e_i \in R_i$ 和 $(0, \cdots, 0, 1_{R_i}, 0, \cdots, 0) \in R_1 \times \cdots \times R_n$（只有第 i 个位置不为 0）之间的对应关系即可.

练习 2.75* 设 R, S 是环. 证明：$R \times S$ 的理想都形如 $I \times J$，其中 I 是 R 的理想，J 是 S 的理想.

证明 设 M 是 $R \times S$ 的理想.

1. 先证明：若 $(r,s) \in M$，则 $(r,0), (0,s) \in M$.
   我们有
   $$\begin{aligned}(r,0) &= (r,s)(1,0) \in M(1,0) \subset M\\ (0,s) &= (r,s)(0,1) \in M(0,1) \subset M\end{aligned}$$
2. 再证明：定义集合
   $$I = \{r \in R : (r,0) \in M\}$$
   则 I 是 R 的理想.
   首先，对任意的 $r, r' \in I$，有 $(r,0), (r',0) \in M$，从而 $(r-r', 0) \in M$，即 $rr' \in I$，并且 I 非空（因为 M 非空）. 于是 I 是 R 的加法子群.
   其次，对任意的 $r \in I$ 和 $u \in R$，我们有 $(ru, 0) = (r,0)(u,0) \subset M(u,0) \subset M$，从而 $ru \in I$. 同理可证 $ur \in I$. 所以 I 对 R 的元素有吸收性.
   综上，$I \lhd R$.
   同理，定义集合
   $$J = \{s \in S : (0,s) \in M\}$$
   则 J 是 S 的理想.
3. 最后证明：$M = I \times J$.
   一方面，对任意的 $(r,s) \in M$，我们有 $(r,0), (0,s) \in M$，从而 $r \in I$，$s \in J$，即 $M \subset I \times J$.
   另一方面，对任意的 $r \in I, s \in J$，有 $(r,0), (0,s) \in M$，从而 $(r,s) = (r,0) + (0,s) \in M$，即 $I \times J \subset M$.
   综上，$M = I \times J$.

笔记 此题的核心思路，是利用任意的理想 M 构造出 I 和 J，然后证明 $M = I \times J$. 类似的方法我们在证明环的第四同构定理时也用过（请参见 2.2 节），当时利用任意的理想 J 构造 A，然后证明 $J = A/I$.

练习 2.76 证明：若 R, S 都是非零环，则 $R \times S$ 不可能是域.

证明 由上题，$R \times \{0\}$ 和 $\{0\} \times S$ 都是 $R \times S$ 的理想. 由于 R, S 都是非零环，于是它们既不是零理想，也不是 $R \times S$，从而 $R \times S$ 不是域（因为域的理想只有零理想以及自身）.

练习 2.77** 设 R 是有限 Bool 环. 证明：$R \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \mathbb{Z}_2$.

证明 先证明：任意 $r \in R$ 都是中心幂等元. 因为 R 是 Bool 环，所以 $r^2 = r$. 并且由于 Bool 环都是交换的，所以 $R = Z(R)$，从而 $r \in Z(R)$，得证.

利用本节第一题的结论可得：任取 $R \simeq Rr \times R(1-r)$，且 $Rr, R(1-r)$ 各自为环. 又因为 R 是有限环，且

$Rr, R(1-r)$ 非空，于是由 $|R| = |Rr| \cdot |R(1-r)|$ 可知，$Rr, R(1-r)$ 是阶小于 R 的环.

再证明：Rr 也是 Bool 环.（同理可证：$R(1-r)$ 也是 Bool 环）对任意的 $sr \in Rr$，有：

$$(sr)^2 = srsr = ssrr = sr$$

从而 Rr 是 Bool 环.

于是，有限 Bool 环 R 被分解为两个阶更低的 Bool 环 $Rr, R(1-r)$ 的直积. 对 $Rr, R(1-r)$ 可做类似操作，可将他们分解为阶更低的 Bool 的直积. 这样的分解过程直到所有的分量 Bool 环 R' 不能再被分解为止. 此时，对任意的 $t \in R'$，只能有 $R' \simeq R't$ 或 $R' \simeq R'(1-t)$. 若 $R' \simeq R't$，则 $1 \in R't$，于是 t 是 R' 中的单位. 若 $R' \simeq R'(1-t)$，则同理可得，$(1-t)$ 是 R' 中的单位，从而存在 $u \in R'$，使得 $(1-t)u = 1$，即 $u - tu = 1$. 等式两侧同乘 u，可得 $u^2 - tu^2 = u$，再利用 Bool 环的性质可得：$u - tu = u$. 于是 $1 = u - tu = u$，而 $1 - t = 1$ 即 $t = 0$. 因此，R' 中的元素，除了零都是单位，即 R' 是域. 而作为整环的 Bool 环只有 $\mathbb{Z}_2$，这样就得到了 $R' \simeq \mathbb{Z}_2$.

综上，R 总会被表示为若干个 $\mathbb{Z}_2$ 的直积，原命题得证.

2.5.4 拓展：同余方程的求解

我们将中国剩余定理应用到整数环 $\mathbb{Z}$ 上，即得以下命题：

✍ **练习 2.78** 设 $n_1, \cdots, n_k$ 是两两互素的正整数，则对于任意的 k 个整数 $a_1, \cdots, a_k$，同余方程组

$$\begin{cases} x & \equiv a_1 \mod n_1 \\ & \cdots \\ x & \equiv a_k \mod n_k \end{cases}$$

必有整数解，且所有解构成陪集 $x \mod n_1 \cdots n_k$.

注 提示：注意到若 m, n 互素，则 $(m) + (n) = \mathbb{Z}$. 这是因为 $(m) + (n) = (m, n) = (1)$.

这里想给大家介绍一些有趣的数学史. 我国有一本著名的数学著作《孙子算经》，大约成书于南北朝时期，作者生平已不可考. 但是其中有不少我们耳熟能详的经典问题. 比如“鸡兔同笼问题”：今有雉兔同笼，上有三十五头，下有九十四足，问雉兔各几何？而我们今天要看的，是另一个经典问题“物不知其数”（也正是因为有了这一问题，我们本节的定理被称作“中国剩余定理”）：今有物不知其数，三三之数剩二，五五之数剩三，七七之数剩二，问物几何？

利用同余的记号，这一问题可以重新被表述为：

✍ **练习 2.79** 求同余方程组的解：

$$\begin{cases} x & \equiv 2 \mod 3 \\ x & \equiv 3 \mod 5 \\ x & \equiv 2 \mod 7 \end{cases}$$

中国剩余定理的证明，实际上提供了一种求解同余方程组的方法，即我们先求出以下三个同余方程的一个特解：

$$\begin{cases} r_1 & \equiv 1 \mod 3 \\ r_1 & \equiv 0 \mod 5 \\ r_1 & \equiv 0 \mod 7 \end{cases}$$

$$\begin{cases} r_2 & \equiv 0 \mod 3 \\ r_2 & \equiv 1 \mod 5 \\ r_2 & \equiv 0 \mod 7 \end{cases}$$

$$\begin{cases} r_3 & \equiv 0 \mod 3 \\ r_3 & \equiv 0 \mod 5 \\ r_3 & \equiv 1 \mod 7 \end{cases}$$

我们以第一个方程组为例求解 r_1，由后两个方程可得 r_1 是 35 的倍数，从而可设 $r_1 = 35k$，再由第一个方程可得，存在整数 l，使得 $35k = 3l + 1$. 问题转化为求不定方程的一个特解，而这是简单的（我们将在“因子分解”一节中给出相关结论）. 实际上我们通过简单的实验也可以找出一个特解 $r_1 = 70$.

类似地，另外两个方程可以找到特解 $r_2 = 21, r_3 = 15$. 由此可得原同余方程组的一个特解为 $x = 2r_1 + 3r_2 + 2r_3 = 140 + 63 + 30 = 233$. 从而利用中国剩余定理可得，方程组的任意解满足 $x \equiv 233 \mod (3 \cdot 5 \cdot 7)$，即 $x \equiv 23 \mod 105$.

为什么我们可以这么做呢？我们利用中国剩余定理将上述过程转述一遍：$(3), (5), (7)$ 是两两互极大的 $\mathbb{Z}$ 的理想，从而有环同构：

$$\mathbb{Z}/((3)(5)(7)) \simeq \mathbb{Z}/(3) \times \mathbb{Z}/(5) \times \mathbb{Z}/(7)$$

也就是

$$\mathbb{Z}_{105} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$$

从而，一定存在 x，使得 $x + (105)$ 对应于 $(2 + (3), 3 + (5), 2 + (7))$. 换句话说，我们要求解 x，就是寻找 $(2 + (3), 3 + (5), 2 + (7))$ 的一个原象. 我们在证明中国剩余定理的过程中，是如何寻找这一原象的呢？我们说明了 $\pi(r_1) = (1, 0, 0), \pi(r_2) = (0, 1, 0), \pi(r_3) = (0, 0, 1)$ 的存在性，然后说明 $\pi(2r_1 + 3r_2 + 2r_3) = (2, 3, 2)$. 于是问题就转化为求解前述的三个更简单一些的同余方程组.

✍ **练习 2.80** 求同余方程组的解：

$$\begin{cases} x & \equiv 1 \mod 4 \\ x & \equiv 2 \mod 3 \\ x & \equiv 3 \mod 5 \end{cases}$$

注 提示：求出 $r_1 = 45, r_2 = 20, r_3 = 36$，从而解可取

$$45 + 2 \times 20 - 2 \times 36 \equiv 13 \mod 60$$

✍ **练习 2.81** 求同余方程组的解：

$$\begin{cases} x & \equiv 4 \mod 11 \\ x & \equiv 3 \mod 17 \end{cases}$$

注 提示：求出 $r_1 = 34, r_2 = 154$，从而解可取

$$4 \times 34 + 3 \times 154 \equiv 37 \mod 187$$

2.6 分式环

本节均设 R 是交换环.

2.6.1 知识要点

1. (分式环)：设 D 是 R 的非空子集，且满足
   (a). $0 \notin D$;
   (b). D 中没有零因子，且对乘法封闭.
   从而存在一个交换环 Q（记作 $Q := D^{-1}R$，称作 R 的分式环），使得
   (a). R 是 Q 的子环，且 $D \subset Q^\times$.
   (b). Q 的元素形如 rd^{-1}，其中 $r \in R, d \in D$.
   特别的，若 $D = R^*$，则 $D^{-1}R$ 是域（称作 R 的分式域）.
   (c). Q 是最小的包含 R，且使 D 中的元素均为单位的环.
   也就是说，设 S 是交换环，$\varphi : R \to S$ 是任意环单同态，使得 $\varphi(D) \subset S^\times$. 于是存在环单同态 $\Phi : Q \to S$，使得 $\Phi|_R = \varphi$.

2.6.2 知识要点解读

分式环的构造过程，与利用整数环 $\mathbb{Z}$ 构造有理数域 $\mathbb{Q}$ 的过程非常类似.

问题 2.11 (分式环)：设 D 是 R 的非空子集，且满足

1. $0 \notin D$;
2. D 中没有零因子，且对乘法封闭.

从而存在一个交换环 Q（记作 $Q := D^{-1}R$，称作 R 的分式环），使得

1. R 是 Q 的子环，且 $D \subset Q^\times$.
2. Q 的元素形如 rd^{-1}，其中 $r \in R, d \in D$.
   特别的，若 $D = R^*$，则 $D^{-1}R$ 是域.
3. Q 是最小的包含 R，且使 D 中的元素均为单位的环.
   也就是说，设 S 是交换环，$\varphi : R \to S$ 是任意环单同态，使得 $\varphi(D) \subset S^\times$. 于是存在环单同态 $\Phi : Q \to S$，使得 $\Phi|_R = \varphi$.

证明

1. (定义“分式”)：设 $\mathcal{F} = \{(r, d) : r \in R, d \in D\}$，定义 $\mathcal{F}$ 上的关系“$\sim$”：
$$(r, d) \sim (s, e) \iff re = sd$$
   显然这一关系是自反和对称的，下证它是传递的. 设 $(r, d) \sim (s, e)$，$(s, e) \sim (t, f)$. 于是 $re - sd = 0$，$sf - te = 0$. 即 $(rf - td)e = f(re - sd) + d(sf - te) = 0$，因为 $e \in D$ 非零且不是零因子，所以只能有 $rf - td = 0$，即 $(r, d) \sim (t, f)$. 综上，关系 $\sim$ 是等价关系，记 (r, d) 所在的等价类为：
$$\frac{r}{d} := \{(a, b) \in \mathcal{F} : (a, b) \sim (r, d)\}$$
   且设 Q 为所有等价类的集合.
2. (构造分式环)：定义 Q 上的加法和乘法运算：
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$$
   下证：Q 是交换环.
   (a). (运算良定义)：设 $\frac{a}{b} = \frac{a'}{b'}$，$\frac{c}{d} = \frac{c'}{d'}$，则：
$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a'}{b'} + \frac{c'}{d'} = \frac{a'd' + b'c'}{b'd'}$$

而

$$\begin{aligned}(ad+bc)(b'd') &= ab'dd' + bb'cd' \\ &= a'bdd' + bb'c'd \\ &= (a'd' + b'c')(bd)\end{aligned}$$

即

$$\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$$

加法是良定义的.

同时

$$\frac{a}{b} \times \frac{c}{d} = \frac{ab}{cd}$$
$$\frac{a'}{b'} \times \frac{c'}{d'} = \frac{a'b'}{c'd'}$$

上下两式显然相等，从而乘法也是良定义的.

(b). (加法交换群): Q 中的加法满足结合律、交换律、有幺元 $\frac{0}{d}, d \in D$ (注意所有的 $\frac{0}{d}$ 都相等，因此实际上只有一个)，任意元素 $\frac{a}{b}$ 都有对应的逆 $\frac{-a}{b}$. (证明细节留给读者)

(c). (乘法交换幺半群): Q 中的乘法满足结合律、交换律、有幺元 $\frac{d}{d}, d \in D$ (注意所有的 $\frac{d}{d}$ 都相等，因此实际上只有一个) . (证明细节留给读者)

综上，Q 是交换环.

3. (R 是 Q 的子环，D 中的每个元素都是 Q 的单位): 定义映射

$$\iota : R \to Q$$
$$r \mapsto \frac{rd}{d}, d \in D$$

首先，ι 是良定义的，因为对任意的 $d, e \in D$，$\frac{rd}{d} = \frac{re}{e}$. 其次，容易验证 ι 是环同态. 最后，ι 是单射，因为若 $\frac{rd}{d} = \frac{r'd}{d}$，则 $(r-r')d = 0$，由于 d 非零且不是零因子，所以 $r = r'$. 于是 $\iota(R)$ 同构于 Q 的子环，即可将 R 视为 Q 的子环.

同时，对任意 $e \in D$，$\frac{ed}{d}$ 有乘法逆 $\frac{1}{e}$，从而 e 可视为 Q 中的单位.

4. (Q 的元素形式): 对任意元素 $\frac{1}{d}$，其逆为 $d := \frac{d}{1}$，因此可将 $\frac{1}{d}$ 记作 d^{-1}，$\frac{r}{d}$ 记作 rd^{-1}.

5. ($D = R^*$ 的特殊情形): 当 $D = R^*$ 时，Q 中的任意非零元素 $\frac{r}{d}$ 都有乘法逆 $\frac{d}{r}$. 从而 Q 为域.

6. (分式环的唯一性): 设 S 是交换环，$\varphi : R \to S$ 是任意环单同态，使得对任意的 $d \in D$ 有 $\varphi(d) \in S^\times$. 将 φ 扩展为映射:

$$\Phi : Q \to S$$
$$rd^{-1} \mapsto \varphi(r)\varphi(d)^{-1}$$

下证: Φ 是良定义的. 对任意的 $rd^{-1} = se^{-1}$，有 $re = sd$，从而 $\varphi(r)\varphi(e) = \varphi(s)\varphi(d)$，即 $\varphi(r)\varphi(d)^{-1} = \varphi(s)\varphi(e)^{-1}$. 于是

$$\begin{aligned}\Phi(rd^{-1}) &= \varphi(r)\varphi(d)^{-1} \\ &= \varphi(s)\varphi(e)^{-1} \\ &= \Phi(se^{-1})\end{aligned}$$

进一步可以验证 Φ 为环单同态 (证明留给读者)，于是命题得证.

笔记 这一命题看起来复杂，其实非常好理解，因为我们熟知一个例子: 由整数得到有理数的过程. 实际上，命题的证明过程就是和构造有理数一样地构造“分式”，进而构造相似于有理数集的“分式环”，换句话说，就是将构造有理数的过程，在一般的交换群中抽象的复现. 这一思路应当引起我们的重视，即从熟悉的实例中寻找一般化的思路，“从特殊性看问题”.

另一方面，我们在证明过程中，着重展示了运算和映射良定义的证明. 这是初学者容易忽略的地方. 这里通

常来说有一个经验，即一旦涉及到等价类，往往会牵扯良定义的问题，因为同一个等价类可以有不同的代表元，从而对同一个等价类，产生在“形式上”不同的像.

本命题的证明还有一个重要的意义，即我们在命题中没有具体给出 $D^{-1}R$ 的形式，但是通过证明我们知道，它的形式是唯一的. 所以在具体使用中我们更多的会应用证明中给出的 $D^{-1}R$ 形式，对命题本身的应用反而少了.

当我们将 D 的约束条件放的宽些，允许其中含有 R 的零因子时，仍然能够类似地构造出环 Q，但是要修改等价关系. 相关内容将在交换代数部分详细展开.

2.6.3 习题

练习 2.82 证明：任意 $\mathbb{R}$ 的子域必须包含 $\mathbb{Q}$.

注 $\mathbb{R}$ 中包含 1，从而 $\mathbb{R}$ 中包含由 1 生成的域，即为 $\mathbb{Q}$.

2.7 环中的因子分解

2.7.1 课前思考

1. 试写出以下几种环之间的包含关系：整环，主理想整环，域，唯一因子分解整环，交换环，欧几里得整环.

——

解

1. 域 $\subset$ 欧几里得整环 $\subset$ 主理想整环 $\subset$ 唯一因子分解整环 $\subset$ 整环 $\subset$ 交换环.

2.7.2 知识要点

（一）整环上的整除关系

1. a 整除 b（或 a 是 b 的因子，或 b 是 a 的倍元）：整环 R 中的元素 $a\neq 0, b\in R$，且存在 $c\in R$，使得 $b=ac$. 若 a,c 均不为单位，则 a,c 称为 b 的真因子.
2. a 和 b 相伴（记作 $a\sim b$）：整环 R 中的元素 $a,b\neq 0$，且 $a|b$，$b|a$.
3. （整除的主理想表达）：设 a,b 为整环 R 中的元素，且 $a\neq 0$. 则 $a|b$ 当且仅当 $(b)\subset(a)$.
4. （相伴的主理想表达）：设整环 R 中的元素 $a,b\neq 0$，则 $a\sim b$，当且仅当 $(a)=(b)$，当且仅当 $a=ub$，其中 u 为 R 的单位.

（二）不可约元与素元

1. 整环 R 上的可约元 x：$x\in R-\{0\}$，且存在两个不是单位的元素 $a,b\in R$，使得 $x=ab$.（反之称之为不可约元）
2. 整环 R 上的素元 p：p 非零、不是单位，且对任意的 $a,b\in R$，若 $p|ab$，则 $p|a$ 或 $p|b$.
   （注：在一般的交换环中，可同样定义整除、相伴、素元以及不可约元的概念.）
3. （素元与素理想）：设 R 是整环，$p\in R$，则 p 是素元，当且仅当 (p) 是非零的素理想.
4. （素元与不可约元）：设 R 是整环，$p\in R$ 是素元，则 p 不可约.

（三）最大公因子

1. 最大公因子：整环 R 中的元素 $a,b\neq 0$，称 d 是 a,b 的最大公因子（记作 $\gcd(a,b)$ 或 (a,b)），若
   (a). d 是 a,b 的因子；
   (b). 若 e 是 a,b 的因子，则 e 整除 d.

2. 最小公倍元：整环 R 中的元素 $a,b\neq 0$，称 m 是 a,b 的最小公倍数（记作 $\operatorname{lcm}(a,b)$ 或 $[a,b]$），若
   (a). m 是 a,b 的倍元；
   (b). 若 n 是 a,b 的倍元，则 n 是 m 的倍元.
3. （相伴）：设整环 R 中的元素 $a,b\neq 0$，若 d,d' 均为 a,b 的最大公因子，则 $d\sim d'$. 类似地，若 m,m' 均为 a,b 的最小公倍元，则 $m\sim m'$.
   （注：一般的，两个元素的最大公因子和最小公倍元既可以不存在，也可以有很多，所以本书中我们使用 (a,b) 表示任意的最大公因子，并且 $d\sim(a,b)$ 表示 d 是 a,b 的一个最大公因子.）

（四）唯一因子分解整环

1. 唯一因子分解整环：R 是整环，且每个非零元 x 都有不可约元分解
$$x=ux_1\cdots x_n$$
   其中 u 为单位，x_i 均为不可约元. 且不计元素顺序时，该分解（在相伴意义下）唯一.
2. （没有无限升链，U1*）：设 R 为唯一因子分解整环，则 R 中不存在无限的元素序列 $a_1,a_2,\cdots,a_n,\cdots$，使得每个 a_{i+1} 都是 a_i 的真因子.
   等价地说，若对所有的 i 均有 $a_{i+1}|a_i$，则存在正整数 N，使得 $a_N\sim a_{N+1}\sim\cdots$.
3. （素元与不可约元，U2*）：设 R 是唯一因子分解整环，则 p 不可约，当且仅当 p 是素元.
4. （最大公因子的存在性，U3*）：唯一因子分解整环中的任意两个非零元都有最大公因子.
5. （唯一因子分解整环的等价定义 ***）：设 R 是整环，则下列命题等价
   (a). R 是唯一因子分解整环；
   (b). R 满足 U1 和 U3；
   (c). R 满足 U1 和 U2.

（五）主理想整环

1. 主理想整环：R 是整环，且每个理想 I 都是主理想.
2. （素理想也是极大理想）：若 P 是主理想整环 R 的素理想，则 P 是极大理想.
3. （唯一因子分解整环）：每个主理想整环都是唯一因子分解整环.

（六）欧几里得整环

1. 欧几里得整环：R 是整环，且存在映射 $f:R^*\to\mathbb{N}$（f 称为欧几里得映射），使得对任意的 $a\in R,b\in R^*$，都存在 $q,r\in R$，满足
$$a=qb+r$$
   其中 $r=0$ 或 $f(r)<f(b)$.
2. （主理想整环）：每个欧几里得整环都是主理想整环.
3. （域）：每个域都是欧几里得整环.

2.7.3 从定理证明中学解题

2.7.3.1 整环上的整除关系

整环上的整除关系的概念可以类比于整数的整除关系，但是二者有相当程度的区别，主要在于一般整环的单位可能有很多，从而对于相伴关系的讨论有意义，而整数环中的单位只有 ±1，所以与整数 n 相伴的整数只有 $\pm n$. 当我们进一步限制在正整数范围内讨论整除关系后，相伴关系与相等关系没有区别，从而也就失去了讨论的意义.

问题 2.12 （整除的主理想表达）：设 a,b 为整环 R 中的元素，且 $a\neq 0$. 则 $a|b$ 当且仅当 $(b)\subset(a)$.

证明 一方面，若 $a|b$，则存在 $r\in R$，使得 $b=ra$，从而 $b\in(a)$，于是 $(b)\subset(a)$.

另一方面，若 $(b)\subset(a)$，则 $b\in(a)$，从而存在 $r\in R$，使得 $b=ra$，即 $a|b$.

笔记 整环上元素的整除关系有两套等价的表述方式：代数式表达（$b=ra$）和主理想表达（$(b)\subset(a)$），前者进一步与代数变形相联系，而后者往往与理想的相关性质相联系（尤其是涉及素理想与极大理想时）.

练习 2.83 （相伴的主理想表达）：设整环 R 中的元素 $a,b\neq 0$，则 $a\sim b$，当且仅当 $(a)=(b)$，当且仅当 $a=ub$，其中 u 为 R 的单位.

练习 2.84 (最大公因子等价)：设整环 R 中的元素 $a,b\neq 0$，若 d,d' 均为 a,b 的最大公因子，则 $d\sim d'$. 类似地，若 m,m' 均为 a,b 的最小公倍数，则 $m\sim m'$.

2.7.3.2 素元与不可约元

素元和不可约元在整数环中没有区别. 而实际上，对于一般的环而言，素元与素理想几乎是捆绑在一起的概念，不可约元则更多的充当了“积木”的角色，成为了构成所有元素的基本部件.

问题 2.13 （素元与素理想）：设 R 是整环，$p\in R$，则 p 是素元，当且仅当 (p) 是非零的素理想.

证明 一方面，设 p 是素元. 考虑商环 $R/(p)$，对任意的 $\bar{a},\bar{b}\in R/(p)$，若 $\bar{a}\bar{b}=\bar{0}$，则 $ab\in(p)$，即 $p|ab$. 由于 p 是素元，则必有 $p|a$ 或 $p|b$，从而有 $\bar{a}=\bar{0}$ 或 $\bar{b}=\bar{0}$. 即 $R/(p)$ 是整环，从而 (p) 是素理想.

反之，设 (p) 是非零的素理想. 证明过程只需将前述过程倒过来即可，此处从略.

问题 2.14 （素元与不可约元）：设 R 是整环，$p\in R$ 是素元，则 p 不可约.

证明 设素元 p 可约，于是存在不是单位的 $a,b\in R$，使得 $p=ab$，从而 $p|ab$. 由于 p 是素元，从而 $p|a$，或 $p|b$.

若 $p|a$，结合 $p=ab$ 可知 $a|p$，从而 $p\sim a$，于是 b 为单位，矛盾！$p|b$ 可类似得到矛盾. 从而 p 不可约.

2.7.3.3 唯一因子分解整环

唯一因子分解整环为我们提供了一个很好的讨论因子分解的环境，因为我们在数论中熟知的“素因子分解”摇身一变，成为了“不可约元分解”，两者的内涵是相同的. 而应用不可约元的分解，主要也就是应用分解的“唯一性”. 换句话说，通过两种不同的方式，得到同一个元素的不可约元分解，于是就可以得到不可约元的个数的信息，以及相伴的信息.

问题 2.15 （素元与不可约元）：设 R 是唯一因子分解整环，则 p 不可约，当且仅当 p 是素元.

证明 在整环中，素元总是不可约的. 下证：在 R 中，若 p 是不可约的，则 p 是素元.

设 $p|ab$，则有 $pc=ab,c\in R$. 对 a,b,c 做不可约元分解：

$$a=up_1\cdots p_l$$
$$b=vq_1\cdots q_m$$
$$c=wr_1\cdots r_n$$

其中 u,v,w 是 R 的单位，于是

$$wpr_1\cdots r_n=uvp_1\cdots p_lq_1\cdots q_m$$

由不可约元分解的唯一性可知：p 与某个 p_i 或 q_j 相伴，从而 $p|a$ 或 $p|b$，即 p 是素元.

练习 2.85 （最大公因子的存在性）：唯一因子分解整环中的任意两个非零元都有最大公因子.

注 提示：对任意的非零元 a,b 有：

$$a=up_1^{\alpha_1}\cdots p_n^{\alpha_n}$$
$$b=vp_1^{\beta_1}\cdots p_n^{\beta_n}$$

这里 u,v 为单位，p_i 为不同的不可约元，指数 α_i 和 β_i 可以为零.（这样处理可以使 a,b 在形式上体现出相同的不可约元因子. 具体操作时，可以先列出出现在 a,b 中的所有不相伴的不可约元，再给他们赋予对应的指数，实际不包含的给零指数即可.）

从而，可取 $\gcd(a,b)$ 为：

$$d=p_1^{\min\{\alpha_1,\beta_1\}}\cdots p_n^{\min\{\alpha_n,\beta_n\}}.$$

进一步的，可取 $\operatorname{lcm}(a,b)$ 为：

$$m=p_1^{\max\{\alpha_1,\beta_1\}}\cdots p_n^{\max\{\alpha_n,\beta_n\}}.$$

✍ **练习 2.86**（没有无限升链）：设 R 为唯一因子分解整环，则 R 中不存在无限的元素序列 $a_1,a_2,\cdots,a_n,\cdots$，使得每个 a_{i+1} 都是 a_i 的真因子.

注 提示：记 a_i 得素因子个数为 $n(a_i)$，则易证 $n(a_{i+1})<n(a_i)$（严格成立小于号），然而 a_1 得素因子个数总是有限的，所以这样的过程只能在有限步停止.

2.7.3.4 主理想整环

主理想的形式 (a) 是很好的，因为其中的每个元素都可以写为很简单的形式 ra. 主理想整环则充分利用了这一优势，我们构造出的任意理想都是主理想. 实际应用主理想整环，也往往紧扣这一特点.

问题 2.16（素理想也是极大理想）：若 P 是主理想整环 R 的非零的素理想，则 P 是极大理想.

证明 任取 R 的理想 I，满足 $P\subset I\subset R$. 由于 R 是主理想整环，所以可记 $P=(p),I=(a)$. 由于 $(p)\subset(a)$，所以 $p\in(a)$，从而存在 $b\in R$，使得 $p=ab$. 由于 P 是素理想，所以必有 $a\in P$ 或 $b\in P$. 若 $a\in P$，则 $I=(a)\subset P$，也就有 $I=P$.

而当 $b\in P=(p)$ 时，就会存在 $r\in R$，使得 $b=rp$，从而 $p=ab=arp$，即 $p(1-ar)=0$. 显然 $p\neq0$，从而 $ar=1$，即 a 为单位，从而 $I=R$.

综上，P 即为 R 的极大理想.

✍ **练习 2.87** 证明：p 是素数，当且仅当 $\mathbb{Z}_p$ 是域.

证明 p 是素数，当且仅当 $p\mathbb{Z}$ 是 $\mathbb{Z}$ 的素理想，由于 $\mathbb{Z}$ 是主理想整环，从而当且仅当 $p\mathbb{Z}$ 也是 $\mathbb{Z}$ 的极大理想，当且仅当 $\mathbb{Z}_p$ 为域.

2.7.3.5 欧几里得整环

欧几里得整环中，欧几里得映射相当于给整环的元素进行了排序，由此整数环中有关大小关系的命题，就有可能借此移植到整环上.

问题 2.17（主理想整环）：每个欧几里得整环 R 都是主理想整环.

证明 设 I 是 R 的理想. 若 $I=(0)$，则 I 是主理想. 以下设 $I\neq(0)$.

记 R 对应的欧几里得映射为 f. 由于 $f(I-\{0\})$ 为 $\mathbb{N}$ 的子集，从而 $f(I-\{0\})$ 必然存在一个最小的自然数 n，并设 $f(b)=n$ $\left(b\in I-\{0\}\right)$. 下证：$I=(b)$.

一方面，$b\in I$，所以 $(b)\subset I$. 另一方面，对任意的 $a\in I$，必存在 $q,r\in R$，使得

$$a=qb+r$$

且 $f(r)<f(b)$ 或 $r=0$. 然而 $f(b)$ 已经是最小值，所以只能有 $r=0$，从而 $a=qb\subset(b)$，即 $I\subset(b)$. 于是 $I=(b)$.

综上，任意 I 都是主理想，从而 R 是主理想整环.

2.7.4 典型例题

2.7.4.1 典型的环结构

我们已经证明了一个环结构的包含链条：

整环 ⊃ 唯一因子分解整环 ⊃ 主理想整环 ⊃ 欧几里得整环 ⊃ 域

而下面的这些例子说明，这里的包含都是“真包含”，即存在着是前一个结构而不是后一个结构的实际例子.

例题 2.16 $\mathbb{Z}$ 是欧几里得整环，但不是域.

笔记 证明过程参见 Maki 的抽象代数 I 讲义.

例题 2.17 $\mathbb{Z}[(1+\sqrt{-19})/2]$ 是主理想整环，但不是欧几里得整环.

笔记 对这一命题的证明已经已经超出我们这里所学的知识范围，此处从略. 感兴趣的同学可以参考 Dummit 第 282 页的相关内容.

例题 2.18 $\mathbb{Z}[x]$ 是唯一因子分解整环，但不是主理想整环.

证明 命题的前半部分将放在“多项式”一章加以解释，这里证明后半部分.

下证：$(2,x)$ 不是主理想.（从而 $\mathbb{Z}[x]$ 不是主理想整环）

假设存在 $p(x)\in\mathbb{Z}[x]$，使得 $(p(x))=(2,x)$. 一方面，因为 $2\in(p(x))$，所以存在 $q(x)\in\mathbb{Z}[x]$，使得 $2=p(x)q(x)$，从而利用待定系数法对比常数项可得，$p(x)=1$ 或 2.

若 $p(x)=1$，则 $(2,x)=(1)$，于是 $1\in(2,x)$，即存在 $f(x),g(x)\in\mathbb{Z}[x]$，使得 $1=2f(x)+xg(x)$，利用待定系数法对比常数项可得：$1=2f(0)$（其中 $f(0)$ 为 $f(x)$ 的常数项，故而为整数），然而这在整数环中是不成立的.

若 $p(x)=2$，则 $(2,x)=(2)$，于是 $x\in(2)$，即存在 $f(x)\in\mathbb{Z}[x]$，使得 $x=2f(x)$，利用待定系数法对比一次项系数可得：$1=2a_1$，其中 a_1 是 $f(x)$ 的一次项系数，从而为整数，但是这在整数环中同样不成立.

综上，假设错误，即原命题成立.

例题 2.19 $\mathbb{Z}[\sqrt{-5}]$ 是整环，但不是唯一因子分解整环.

笔记 证明过程参见 Maki 的抽象代数 I 讲义.

2.7.4.2 整除

问题 2.18 设 R 为唯一因子分解整环，$a,b,c\in R$ 为非零元，则：

1. $((a,b),c)\sim(a,(b,c))$；
2. 若 $a\sim b$，则 $(c,a)\sim(c,b)$；
3. $c(a,b)\sim(ca,cb)$；
4. $(a,b)\sim 1$ 且 $(a,c)\sim 1$，则 $(a,bc)\sim 1$.

证明

1. $((a,b),c)$ 和 $(a,(b,c))$ 都表示 a,b,c 的最大公因子，故而相伴.
2. 由对称性，只需证 $(c,a)|(c,b)$. 而显然 $(c,a)|c$，$(c,a)|a$. 由于 a 和 b 相伴，从而存在单位 u，使得 $au=b$，从而 $(c,a)u|au$，即 $(c,a)u|b$，也就有 $(c,a)|b$. 所以有 $(c,a)|(c,b)$.
3. 记 $(a,b)=d$，$(ca,cb)=e$. 则 $cd|ca$ 且 $cd|cb$，从而 $cd|(ca,cb)$. 设 $e=cdu$，且 $ca=ea'$，从而 $ca=cdua'$，即 $a=dua'$，$du|a$. 类似地，$du|b$，从而 $du|d$，即 u 是 R 的单位. 所以 $(ca,cb)\sim c(a,b)$.
4. 因为 $(a,b)\sim 1$，所以 $(ac,bc)\sim c$. 又因为 $(a,c)\sim 1$，所以 $(a,(ac,bc))\sim 1$，即 $1\sim(a,(ac,bc))\sim((a,ac),bc)\sim(a(1,c),bc)\sim(a,bc)$.

笔记 四个小问都可以利用不可约元分解去证明，读者可以尝试以下. 并且他们实际上给出了最大公因子“算符” $(\cdot,\cdot)$ 的一些性质，从而我们可以直接对 $(\cdot,\cdot)$ 进行代数变形.

有细心地读者可能会发现，证明过程中没有直接使用“唯一因子分解”这一条件. 事实上，它保证了我们讨论的所有最大公因子都存在. 于是，环 R 的条件可以弱化为“整环 + 任意两个元素存在最大公因子”. 但是，在

任意整环中，已知 (a,b) 并不意味着 ca 和 cb 就有最大公因子.

✍ **练习 2.88** 设 R 为唯一因子分解整环，$a,b,c\in R$ 为非零元，且 $a|bc$，证明：

1. 若 $(a,b)\sim 1$，则 $a|c$；
2. 若存在非零的 $k\in R$，使得 $k(a,b)\sim a$，则 $k|c$.

证明

1. 因为 $a|bc$，所以 $(a,bc)\sim a$. 又 $(a,b)\sim 1$，所以 $(ac,bc)\sim c$. 从而有：

$$\begin{aligned}(a,c)&\sim(a,(ac,bc))\\&\sim((a,ac),bc)\\&\sim(a(1,c),bc)\\&\sim(a,bc)\\&\sim a\end{aligned}$$

   即 $a|c$.

2. 设 $b=l(a,b)$，则 $(a,b)(k,l)\sim(a,b)$，即 $(k,l)\sim 1$. 而由 $a|bc$ 可得 $k|lc$. 从而由第一小题的结论可知：$k|c$.

2.7.4.3 主理想整环

例题 2.20 设 R 是主理想整环，$a,b,d\in R$ 是非零元. 证明：$d\sim(a,b)$，当且仅当 $(a,b)=(d)$.

证明 先设 $d\sim(a,b)$. 一方面，因为 $d|a$ 且 $d|b$，于是 $a,b\in(d)$，即 $(a,b)\subset(d)$. 另一方面，因为 R 是主理想整环，所以存在 $d'\in R$，使得 $(a,b)=(d')$，即 $d'\in(d)$，$d|d'$. 而 $a,b\in(d')$，于是 $d'|a,d'|b$，从而 $d'|d$，于是 $d\sim d'$，即 $(a,b)=(d')=(d)$.

再设 $(a,b)=(d)$. 一方面易得 $d|a,d|b$. 另一方面，若 $d'|a$ 且 $d'|b$，则 $a,b\in(d')$，即 $(d)=(a,b)\subset(d')$，从而 $d'|d$. 于是 $d\sim(a,b)$.

笔记 由此题我们可知，在主理想整环中，a,b 的最大公因子，可表达为 a,b 的线性组合形式 $d=ax+by$，其中 $x,y\in R$. 此结论应用在整数环中即为 Bézout 定理.

✍ **练习 2.89** 设 R 是主理想整环，$a,b,m\in R$ 是非零元. 证明：$m\sim[a,b]$，当且仅当 $(a)\cap(b)=(m)$.

2.7.5 习题

2.7.5.1 整除

✍ **练习 2.90** 设 R 为唯一因子分解整环，$a,b,c\in R$ 为非零元，证明：$ab\sim(a,b)[a,b]$.

✍ **练习 2.91** 设 R 为整环，$a,b\in R$ 为非零元，$a\sim b$，证明：

1. 若 a 不可约，则 b 不可约；
2. 若 a 为素元，则 b 为素元.

2.7.5.2 主理想整环

✍ **练习 2.92** 设 R 是主理想整环，$a,b,m\in R$ 是非零元. 证明：

1. $(a)\cap(b)=(a)(b)$，当且仅当 $(a,b)\sim 1$；
2. 方程 $ax+by=m$ 在 R 中有解 x,y。当且仅当 $(a,b)|c$.

✍ **练习 2.93** 设 R 是主理想整环，P 是其素理想. 证明：R/P 仍然是主理想整环.

证明 设 $\bar{I}$ 是 R/P 的理想. 定义集合：

$$I:=\{i\in R:\ i+P\in\bar{I}\}$$

1. 证明：$P\subset I$ 且 I 是 R 的理想.
   首先，I 非空，因为对任意的 $p\in P$，$p+P=P$ 是 R/P 的零元，所以理想 $\bar{I}$ 必然包含 P，从而 $p\in I$. 由此也证明了 $P\subset I$.
   其次，对任意的 $i,j\in I$，因为 $i+P,j+P\in\bar{I}$，所以 $(i+P)-(j+P)\in\bar{I}$，即 $(i-j)+P\in\bar{I}$. 从而 $i-j\in I$.
   综上，I 是 R 的加法子群.
   另一方面，对任意的 $r\in R,i\in I$，有：
   $$ri+P=(r+P)(i+P)\in(r+P)\bar{I}\subset\bar{I}$$
   从而 $ri\in I$，类似地 $ir\in I$.（注意到 $\bar{I}$ 是 R/P 的理想，且 $r+P\in R/P$，所以 $(r+P)\bar{I}\subset\bar{I}$.）从而 I 为 R 的理想.
2. 证明：$\bar{I}=I/P$.
   一方面，对任意的 $i+P\in\bar{I}$，根据 I 的定义即得 $i\in I$，从而 $i+P\in I/P$.
   另一方面，对任意的 $i+P\in I/P$，即任意的 $i\in I$，根据 I 的定义有 $i+P\in\bar{I}$.
3. 证明：I/P 是主理想（从而 R/P 中的每个理想都是主理想）. 因为 R 是主理想整环，所以必存在 $i\in R$，使得 $I=(i)$. 下证：$I/P=(\bar{i})$，其中 $\bar{i}:=i+P$.
   一方面，因为 $i+P\in I/P$，所以 $(\bar{i})\subset I/P$. 另一方面，对任意的 $r+P\in I/P$，即 $r\in I$，于是存在 $s\in R$，使得 $r=si$，从而 $r+P=si+P=(s+P)(i+P)\in(\bar{i})$. 于是 $I/P=(\bar{i})$.
4. 证明：R/P 是主理想整环. 因为 P 为 R 的素理想，所以 R/P 为整环. 又 R/P 中的每个理想都是主理想，所以 R/P 是主理想整环，命题得证.

笔记 在证明 R/P 为主理想整环时，不要忘记证明 R/P 是整环.
请读者思考，为什么 $i+P\in I/P$，当且仅当 $i\in I$？

练习 2.94 设 R 是整环. 证明：若 R 满足以下两个条件，则 R 是主理想整环：
1. 任意两个非零元素 $a,b\in R$ 都有最大公因数，且可以表达为 $ra+sb$，其中 $r,s\in R$；
2. 若 $a_1,a_2,\cdots$ 都是 R 中的非零元，并且对任意的下标 i 有 $a_{i+1}|a_i$，则存在一个正整数 N，使得对任意的 $n\geqslant N$，有 $a_n\sim a_N$.

证明 ？

练习 2.95 设 R 是二次整数环 $\mathbb{Z}[\sqrt{-5}]$. 定义理想 $I_2=(2,1+\sqrt{-5})$，$I_3=(3,2+\sqrt{-5})$ 和 $I_3'=(3,2-\sqrt{-5})$.
1. 证明：I_2,I_3,I_3' 都不是 R 的主理想；
2. 证明：$I_2^2=(2)$，$I_2I_3=(1-\sqrt{-5})$，$I_2I_3'=(1+\sqrt{-5})$.

证明 放到高斯整数环的专题中去用。利用 norm

2.7.5.3 未分类

练习 2.96 考虑整数环中的丢番图方程（不定方程）：$ax+by=N$，其中 a,b,N 是整数且 a,b 不为零. 记 $(a,b)=d$
1. 设 x_0,y_0 是原方程的一组整数解（特解），证明：方程的任意整数解（通解）都有如下形式：
   $$x=x_0+m\frac{b}{d}$$
   $$y=y_0-m\frac{a}{d}$$
   其中 $m\in\mathbb{Z}$.
2. 原方程有整数解，当且仅当 $d|N$.

证明

1. 因为 x_0, y_0 为一组解，所以有 $ax_0 + by_0 = N$. 与原方程相减可得：

$$a(x - x_0) = b(y_0 - y)$$
$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$$

从而可得

$$\frac{b}{d} \Big| \frac{a}{d}(x - x_0)$$

并且由于 $(a/b, b/d) = (a, b)/d = 1$，所以只能有

$$\frac{b}{d} \Big| (x - x_0)$$

即存在 $m \in \mathbb{Z}$（注意，此时的 m 不是遍历 $\mathbb{Z}$ 的），使得

$$m\frac{b}{d} = (x - x_0)$$
$$x = x_0 + m\frac{b}{d}$$

代入方程 $a(x - x_0) = b(y_0 - y)$ 即得

$$y = y_0 - m\frac{a}{d}$$

另一方面，对于任意的 $m \in \mathbb{Z}$，不难验证

$$x = x_0 + m\frac{b}{d}$$
$$y = y_0 - m\frac{a}{d}$$

都是原方程的解，所以命题得证.

2. 一方面，若原方程有整数解 x_0, y_0，则 $ax_0 + by_0 = N$，即

$$d\left(\frac{a}{d}x_0 + \frac{b}{d}y_0\right) = N$$

从而 $d|N$.（注意到 $a/d, b/d$ 均为整数）

另一方面，若 $d|N$，则原方程变形为：

$$\frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{N}{d}$$

由于 $\mathbb{Z}$ 为主理想整环，所以由 $(a/d, b/d) = 1$ 可得 $(a/d, b/d) = (1)$（左右两侧均为理想），于是存在整数 x_0, y_0，使得

$$\frac{a}{d}x_0 + \frac{b}{d}y_0 = 1$$
$$a\left(\frac{N}{d}x_0\right) + b\left(\frac{N}{d}y_0\right) = d\frac{N}{d} = N$$

即 $\frac{N}{d}x_0, \frac{N}{d}y_0$ 为原方程的一组整数解.

综上，原命题得证.

✍ **练习 2.97*** 设 a, b 是互素的正整数，$n = ab - a - b$，证明：

1. 不定方程 $ax + by = n$ 没有非负整数解；
2. 对任意的 $N > n$，不定方程 $ax + by = N$ 有非负整数解.

证明 TBD

2.7.6 思考题

2.7.6.1 欧几里得整环上的“辗转相除法”

✍ **练习 2.98**

1. 试找出一个 $a \in \mathbb{Z}[i]$，使得 $(85, 1+13i) = (a)$；
2. 试找出一个 $a \in \mathbb{Z}[i]$，使得 $(47-13i, 53+56i) = (a)$；

解 注意到 $\mathbb{Z}[i]$ 上的欧几里得映射为 $f(a+bi) = a^2+b^2$.

1. 我们有：

$$85 = (-6i)(1+13i) + (7+6i)$$
$$1+13i = (1+i)(7+6i)$$

所以 a 可取 $7+6i$.

2. 我们有：

$$53+56i = (1+i)(47-13i) + (-7+22i)$$
$$47-13i = (-1-i)(-7+22i) + (18+2i)$$
$$-7+22i = i(18+2i) + (-5+4i)$$
$$18+2i = (-2-2i)(-5+4i)$$

所以 a 可取 $-5+4i$.

2.8 专题：二次域与二次整环

例题 2.21（二次域）：设有理数 D 不是 $\mathbb{Q}$ 中的完全平方数（即不存在有理数 q，使得 $D = q^2$）. 定义

$$\mathbb{Q}(\sqrt{D}) := \{a+b\sqrt{D} : a, b \in \mathbb{Q}\} \subset \mathbb{C}$$

证明：$\mathbb{Q}(\sqrt{D})$ 连同复数的加法和乘法运算构成域.

证明 首先，验证 $(\mathbb{Q}(\sqrt{D}), +)$ 是交换群. 对任意的 $a+b\sqrt{D}$, $c+d\sqrt{D} \in \mathbb{Q}(\sqrt{D})$，有：

$$(a+b\sqrt{D}) + (c+d\sqrt{D}) = (a+c) + (b+d)\sqrt{D} \in \mathbb{Q}(\sqrt{D})$$

从而加法是封闭的. 结合性、交换性、加法幺元、元素的加法逆都很容易验证，此处从略.

其次，验证 $(\mathbb{Q}(\sqrt{D}) - \{0\}, \cdot)$ 是交换群. 对任意的 $a+b\sqrt{D}$, $c+d\sqrt{D} \in \mathbb{Q}(\sqrt{D})$，有：

$$(a+b\sqrt{D})(c+d\sqrt{D}) = (ac+bdD) + (ad+bc)\sqrt{D} \in \mathbb{Q}(\sqrt{D})$$

从而乘法是封闭的. 结合性、交换性由复数的乘法性质所保证. 乘法幺元是 $1 = 1+0\sqrt{D}$. 下证：任意非零元素 $a+b\sqrt{D}$ 都有其逆元. 不妨设 $c+d\sqrt{D}$ 是 $a+b\sqrt{D}$ 的逆，于是有：

$$1 = (a+b\sqrt{D})(c+d\sqrt{D}) = (ac+bdD) + (ad+bc)\sqrt{D}$$

对比有理数项和根号项的系数，我们有：

$$ac+bdD = 1$$
$$ad+bc = 0$$

从而解得：

$$c = \frac{a}{a^2-b^2D}$$
$$d = \frac{-b}{a^2-b^2D}$$

注意到这里 $a^2-b^2D \neq 0$（否则 $D = (a/b)^2$，违反前提；或者 $a = b = 0$，为零元）. 从而每个非零元都有其逆元. 于是 $(\mathbb{Q}(\sqrt{D}) - \{0\}, \cdot)$ 是交换群.

最后，乘法分配律由复数的运算性质保证. 综上，$\mathbb{Q}(\sqrt{D})$ 连同复数的加法和乘法运算构成域.

✍ **练习 2.99** 前述例题中，将 D 限定为无平方因子的整数（即素因子分解后，每个素因子只出现一次），结论依然成立，请证明之.（事实上两者是同一个域，以后我们定义的二次域都将 D 限定为无平方因子的整数.）

✍ **练习 2.100** （二次整环）：设 D 是无平方因子的整数.

1. 定义：

$$\mathbb{Z}[\sqrt{D}]=\{a+b\sqrt{D}:a,b\in\mathbb{Z}\}$$

证明：$\mathbb{Z}[\sqrt{D}]$ 是二次域 $\mathbb{Q}(\sqrt{D})$ 的子环；

2. 若 $D\equiv 1 \mod 4$，设 $\omega=\frac{1+\sqrt{D}}{2}$，并定义

$$\mathbb{Z}[\omega]=\{a+b\omega:\ a,b\in\mathbb{Z}\}$$

证明：$\mathbb{Z}[\omega]$ 是二次域 $\mathbb{Q}(\sqrt{D})$ 的子环；

定义 $\mathbb{Z}[\omega]$ 是二次域 $\mathbb{Q}(\sqrt{D})$ 的二次整数环，其中

$$\omega=\begin{cases}\sqrt{D} & D\equiv 2,3,0 \mod 4\\ \frac{1+\sqrt{D}}{2} & D\equiv 1 \mod 4\end{cases}$$

✍ **练习 2.101** 定义二次域上的域模：

$$\begin{aligned}N:\mathbb{Q}(\sqrt{D})&\to\mathbb{Q}\\ a+b\sqrt{D}&\mapsto a^2-Db^2\end{aligned}$$

证明，对任意的 $\alpha,\beta\in\mathbb{Q}(\sqrt{D})$，有 $N(\alpha\beta)=N(\alpha)N(\beta)$；

✍ **练习 2.102** 证明：α 是整数环 $\mathbb{Z}[\omega]$ 的单位，当且仅当 $N(\alpha)=\pm 1$.

问题 2.19 证明：$\mathbb{Z}[\sqrt{-1}]$ 是欧几里得整环，其中欧几里得函数为 $N(a+b\sqrt{-1})=a^2+b^2$.

注 这一问题的证法是经典证法.

证明 设 $\alpha=a+b\sqrt{-1},\beta=c+d\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}]$，且 $\beta\neq 0$. 下证：存在 $q,r\in\mathbb{Z}[\sqrt{-1}]$，使得 $\alpha=\beta q+r$，且 $r=0$ 或 $N(r)<N(\beta)$.

在 $\mathbb{Z}[\sqrt{-1}]$ 的分式域中有

$$\begin{aligned}\frac{\alpha}{\beta}&=e+f\sqrt{-1}\\ e&=\frac{ac+bd}{c^2+d^2}\\ f&=\frac{bc-ad}{c^2+d^2}\end{aligned}$$

其中 $e,f\in\mathbb{Q}$. 取 u 是最接近 e 的整数，v 是最接近 f 的整数，于是

$$|e-u|\leqslant\frac{1}{2},\ |f-v|\leqslant\frac{1}{2}$$

从而有：

$$\begin{aligned}\alpha&=\beta(e+f\sqrt{-1})\\ &=\beta(u+v\sqrt{-1})+\beta((e-u)+(f-v)\sqrt{-1})\end{aligned}$$

令 $q=u+v\sqrt{-1},r=\beta((e-u)+(f-v)\sqrt{-1})$. 由于 $\alpha,\beta,q\in\mathbb{Z}[\sqrt{-1}]$，所以 $r=\alpha-\beta q\in\mathbb{Z}[\sqrt{-1}]$. 而且当 $r\neq 0$ 时我们有：

$$\begin{aligned}N(r)&=N(\beta)N((e-u)+(f-v)\sqrt{-1})\\ &=N(\beta)((e-u)^2+(f-v)^2)\\ &\leqslant\frac{1}{2}N(\beta)\\ &<N(\beta)\end{aligned}$$

从而命题成立.

✍ **练习 2.103** 利用例题的方法，证明 $\mathbb{Z}[\sqrt{-2}],\mathbb{Z}[\frac{1+\sqrt{-3}}{2}],\mathbb{Z}[\frac{1+\sqrt{-7}}{2}],\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$ 是欧几里得整环.

✍ **练习 2.104** 证明：$\mathbb{Z}[\sqrt{2}]$ 是欧几里得整环.

问题 2.20 求 $\mathbb{Z}[\sqrt{-1}]$ 的单位群.

解 设 $\gamma = a + b\sqrt{-1}$ 是 $\mathbb{Z}[\sqrt{-1}]$ 的单位，从而存在 $c + d\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$，使得：

$$(a + b\sqrt{-1})(c + d\sqrt{-1}) = 1$$

对等式两侧作用欧几里得函数可得：

$$(a^2 + b^2)(c^2 + d^2) = 1$$

由于等式左侧的两个因子均为正整数，所以只能有 $a^2 + b^2 = 1$，从而可得 $\gamma = 1, -1, \sqrt{-1}$ 或 $-\sqrt{-1}$. 即

$$(\mathbb{Z}[\sqrt{-1}])^\times = \{\pm 1, \pm\sqrt{-1}\}.$$

问题 2.21 对 $\mathbb{Z}[\sqrt{-1}]$ 任意的理想 I，证明：商环 $\mathbb{Z}[\sqrt{-1}]/I$ 是有限的.

证明 因为 $\mathbb{Z}[\sqrt{-1}]$ 是欧几里得整环，所以它也是主理想整环. 对 $\mathbb{Z}[\sqrt{-1}]$ 任意的理想 $I = (\alpha)$，由带余除法可知，$\bar{\beta} \in \mathbb{Z}[\sqrt{-1}]/I$ 中必有 $N(\beta) < N(\alpha)$ 或 $\beta = 0$，从而 $\mathbb{Z}[\sqrt{-1}]/I$ 是有限的.

问题 2.22 证明：$\mathbb{Z}[\sqrt{-5}]$ 不是唯一因子分解整环.

证明 我们有：$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

1. 先证明：$2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ 都是 $\mathbb{Z}[\sqrt{-5}]$ 中的不可约元.
   假设 2 可约，即有 $2 = ab$，其中 a, b 都不是单位（即 $N(a), N(b) > 1$）. 取域模可得：
   $$4 = N(2) = N(a)N(b)$$
   从而只能有 $N(a) = N(b) = 2$. 设 $a = x + y\sqrt{-5}$，从而 $x^2 + 5y^2 = 2$. 然而这一方程没有整数解，从而 2 不可约.
   其他三个数的不可约证明与之类似，留给读者作为练习.
2. 再证明：2 和 $1 \pm \sqrt{-5}$ 不相伴.
   首先，假设存在 $x + y\sqrt{-5}$，使得 $2 = (x + y\sqrt{-5})(1 + \sqrt{-5})$，从而有 $4 = (x^2 + y^2)6$，而这是矛盾的！同理也不存在 $x + y\sqrt{-5}$，使得 $2(x + y\sqrt{-5}) = 1 + \sqrt{-5}$. 从而 2 和 $1 + \sqrt{-5}$ 不相伴. 类似可证 2 和 $1 - \sqrt{-5}$ 不相伴.

综上，6 有不唯一的不可约元分解，从而 $\mathbb{Z}[\sqrt{-5}]$ 不是唯一因子分解整环.

✍ **练习 2.105** 设 D 是非完全平方的整数，定义

$$S := \left\{ \begin{pmatrix} a & b \\ Db & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

证明：

1. S 是 $M_2(\mathbb{Z})$ 的子环；
2. 映射
   $$\varphi : \mathbb{Z}[\sqrt{D}] \to S$$
   $$a + b\sqrt{D} \mapsto \begin{pmatrix} a & b \\ Db & a \end{pmatrix}$$
   是环同态；
3. 若 $D \equiv 1 \mod 4$，则集合
   $$T := \left\{ \begin{pmatrix} a & b \\ (D-1)b/4 & a+b \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$
   是 $M_2(\mathbb{Z})$ 的子环，且同构于二次整数环 $\mathbb{Z}[\omega]$.

第 3 章 多项式理论

注：若无特殊声明，本章中 R 均为交换环，F 为域，x 为未定元.

3.1 一元多项式环

3.1.1 课前思考

判断下列命题的正误，并说明理由：

1. $0, 0x+0, 0x^2+0x+0 \in R[x]$ 是同一个元素.
2. 若 $f, g \in R[x]$ 均不是零多项式，则 $\deg fg = \deg f + \deg g$.
3. 若 $f, g \in R[x]$ 均不是零多项式，则 $\deg fg = \deg f \cdot \deg g$.
4. 若 $r \in R$，则 $\deg r = 0$.

解

1. T.
2. F: 在 $\mathbb{Z}_6[x]$ 中,$(2x)(3x) = 6x^2 = 0$.
3. F: 在 $\mathbb{R}[x]$ 中,$\left(x^2\right) \cdot \left(x^3\right) = x^5$.
4. F: 零多项式的次数不是零.

3.1.2 知识要点

（一）一元多项式环

1. R 上 (关于 x) 的形式幂级数：f 为形式和
$$f = \sum_{i=0}^{\infty} a_i x^i, \quad a_i \in R.$$
2. R 上 (关于 x) 的一元多项式：f 为形式和
$$f = \sum_{i=0}^{\infty} a_i x^i, \quad a_i \in R.$$
其中除有限项外的所有的 a_i 均为零. 换句话说，f 等价于一个无穷序列
$$(a_0, a_1, \cdots, a_n, 0, 0, \cdots)$$
3. 零多项式: 等价于无穷序列 $(0, 0, \cdots)$.
4. 多项式的加法和乘法运算：设 f, g 为 R 上的两个关于 x 的多项式
$$f = \sum_{i=0}^{\infty} a_i x^i, \quad g = \sum_{i=0}^{\infty} b_i x^i$$
则定义
$$f + g = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$
$$fg = \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k b_{i-k} \right) x^i$$
5. R 上 (关于 x) 的一元多项式环：R 上的全体多项式的集合（记为 $R[x]$），连同多项式的加法和乘法构成交换环.

(二)、多项式的次数

1. 一元多项式的次数：设
$$p=\sum_{i=0}^{\infty}a_ix^i\in R[x]$$
   (a). p 的次数：p 不为零多项式时，定义为最大的使得 $a_i\neq 0$ 的下标 i（记作 $\deg p=i$）.
   (b). p 的首项：若非零多项式 p 的次数为 n，则其首项为 p 的最高次项, 即 a_nx^n，其中 a_n 叫做 p 的首项系数.
   (c). 首一多项式：首项系数为 1 的多项式.
2. (多项式的和与积的次数)：设 $f,g\in R[x]$，则
   (a). $\deg(f+g)\leqslant\max\{\deg f,\deg g\}$.
   特别地，若 $\deg f\neq\deg g$，则 $\deg(f+g)=\max\{\deg f,\deg g\}$.
   (b). $\deg(fg)\leqslant\deg f+\deg g$.
   特别地，若 f 或 g 的首项系数不为零因子，则 $\deg(fg)=\deg f+\deg g$.

(三)、代入

1. (代入同态)：任取 $r\in R$，则映射
$$\begin{aligned}\varphi_r:R[x]&\to R\\ \sum_{i=0}^{\infty}a_ix^i&\mapsto\sum_{i=0}^{\infty}a_ir^i\end{aligned}$$
   为环同态.（注意到序列 a_i 中只有有限项不为 0，所以像 $\sum_{i=0}^{\infty}a_ir^i$ 的表达是合理的.）
   从而，对于 $f\in R[x]$，我们一般记 $f(x):=f$，$f(a):=\varphi_a(f)$.
2. (环同态“诱导”多项式环的同态)：设 R,R' 均为交换环，$\varphi:R\to R'$ 为环同态，则映射
$$\begin{aligned}\bar{\varphi}:R[x]&\to R'[x]\\ \sum_{i=0}^{\infty}a_ix^i&\mapsto\sum_{i=0}^{\infty}\varphi(a_i)x^i\end{aligned}$$
   也是一个环同态.（约定：我们以后称 $\bar{\varphi}$ 是由 φ 诱导的同态）

3.1.3 知识要点解读

(一) 多项式的定义

多项式是我们刚刚进入代数学的大门时就开始接触的一个概念. 我们这里不采用相对常见的定义多项式的方式 $\sum_{i=0}^{n}a_ix^i$，而是绕了一个弯，从形式幂级数说起，主要用意在于回避了零多项式带来的烦恼.

考虑多项式
$$\begin{aligned}z_0&=0\\ z_1&=0+0x\\ z_2&=0+0x+0x^2\\ &\cdots\end{aligned}$$
粗看之下，它们不都是零吗？但是，以 z_1 为例，我们认为它等于零，是因为默认有 $0x=0$. 那么，这个等式为什么成立？我们似乎是找不到理由的. 事实上这个等式也确实没有道理，因为我们学过的性质：“0 与任何元素相乘都得 0”是在一个环中成立的. 然而 x 作为未定元, 并不是环 R 中的元素！(注意：我们更不能说 0 是多项式环 $R[x]$ 中的元素，因为此时多项式环尚未定义.）因此, $z_0,z_1,z_2,\cdots$ 并不是相同的. 然而，麻烦的是，如果我们

姑且就认为这些多项式不相同，按通常的多项式运算定义了加法和乘法，把 z_0 视为加法幺元，则 $z_1, z_2, \cdots$ 也满足加法幺元的性质. 若 $R[x]$ 是环，则 $(R[x], +)$ 是加法交换群，此时只能有唯一的加法幺元，这就产生了矛盾!

如何解决这样的矛盾呢? 我们熟悉的多项式的运算中，总是默认 $z_0, z_1, z_2, \cdots$ 都是相等的，我们不妨就将它们视作同一个多项式，并且在此基础上再构造多项式环，这就产生了借助形式幂级数定义的方式. 当然，如果你是初学者，可以暂且不管这些，就按照你熟悉的多项式的定义去处理，只要附加一条“所有的 z_i 都是相等的”就可以了.

还有一个方面是读者容易产生误解的：多项式不是映射. 一个对应关系 f 要想成为映射，必须要有定义域 A 和良定义的对应法则 f（此时才有映射 $f : A \to f(A)$）. 而多形式的定义中，x 是一个形式上的记号，他没有任何含义，更谈不上“取值”.

例如，考虑

$$f_1(x) = x$$
$$f_2(x) = x^3$$

作为多项式而言，二者必然不相同，我们从直观上就可以判定. 然而，如果我们给定 x 的取值范围 $\{-1, 0, 1\} \subset \mathbb{Z}$，则此二者是同一个映射. 这从侧面说明了多项式并不是映射. 当然，这个例子也说明，如果我们赋予 x 一个取值范围，就可以把一个多项式转化为映射.

（二）零多项式的次数

零多项式的次数究竟是多少? 这是一个没有标准答案的问题，不同的教材有不同的看法. 有不定义次数的（Artin, Dummit, Waerden），有记为 $-\infty$ 的（冯克勤，Jacobson，GTM211）. 笔者认为使用记号 $-\infty$（不要理解为极限中的负无穷）较为方便，且不容易产生误解，其中规定（这些规定都是很自然地，不需要额外记忆）：

$$(-\infty) + (-\infty) = -\infty$$
$$n + (-\infty) = -\infty$$
$$(-\infty)(-\infty) = -\infty$$
$$n(-\infty) = -\infty$$
$$-\infty < n$$

其中 n 为自然数.

（三）有关未定元

正如其名字一样，未定元其实就是表示一个“无法确定的元素”（至少站在系数环 R 的角度来说是这样）. 未定元不是环 R 中的元素，但是它在形式上和 R 中的元素做着类似地加法和乘法运算. 甚至于，有时候我们会人为地将未定元设为 R 中的某个元素 (进行代入操作).

在本章中，为了讨论问题方便，我们令 R 是交换环. 实际上，当 R 不是交换环时，我们仍然可以完全相同地定义多项式环 $R[x]$，但是其中有一个问题就暴露了出来. 考虑多项式 $f = x + a \in R[x]$，则根据乘法的定义有 $h := f^2 = x^2 + 2ax + a^2$. 然后我们做代入操作 $x = b$，并且设 b 和 a 不可交换，此时：

$$f(b)f(b) = (b + a)(b + a) = b^2 + ba + ab + a^2$$
$$h(b) = b^2 + 2ab + a^2$$

可以发现虽然 $f^2 = h$，但 $f(b)f(b) \neq h(b)$（读者可以尝试将 R 取为某个矩阵环，从而会找到更为具体且常见的例子）. 这个例子告诉我们，我们在多项式环的乘法定义中，隐式地规定了：未定元和系数环中的元素都是可交换的. 并且，若 R 不是交换环，则代入映射将不再是一个同态.

3.1.4 习题

练习 3.1 设 $p(x)=2x^3-3x^2+4x-5$, $q(x)=7x^3+33x-4$, 在下列给定的系数环中计算 $p(x)+q(x)$ 和 $p(x)q(x)$:

1. $R=\mathbb{Z}$: $p(x)+q(x)=9x^3-3x^2+37x-9$, $p(x)q(x)=14x^6-21x^5+94x^4-142x^3+144x^2-181x+20$.
2. $R=\mathbb{Z}_2$:$p(x)=x^2+1$, $q(x)=x^3+x$, $p(x)+q(x)=x^3+x^2+x+1$, $p(x)q(x)=x^5+x$.
3. $R=\mathbb{Z}_3$: $p(x)=2x^3+x+1$, $q(x)=x^3+2$. $p(x)+q(x)=x$, $p(x)q(x)=2x^6+x^4+2x^3+2x+2$.

练习 3.2 设 I 是 R 的理想, 证明:

1. $I[x]$ 是 $R[x]$ 的理想;
2. $R[x]/I[x]\simeq(R/I)[x]$;
3. 若 I 是 R 的素理想, 则 $I[x]$ 是 $R[x]$ 的素理想.

证明

1. 容易验证 $I[x]$ 是 $R[x]$ 的加法子群.
   任取 $f\in I[x], g\in R[x]$, 设
   $$f=\sum_{i=0}^{m}a_ix^i,\quad a_i\in I$$
   $$g=\sum_{i=0}^{n}b_ix^i,\quad b_i\in R$$
   则
   $$fg=\sum_{i=0}^{m+n}c_ix^i$$
   $$c_i=\sum_{k=0}^{i}a_kb_{i-k}$$
   注意到 fg 的每一项系数 c_i 都在 $IR\subset I$ 中, 所以 $fg\in I[x]$, 即 $I[x]$ 有吸收性. 故 $I[x]$ 是 $R[x]$ 的理想.
2. 定义映射
   $$\varphi: R[x]\to(R/I)[x]$$
   $$\sum_{i=0}^{n}a_ix^i\mapsto\sum_{i=0}^{n}\overline{a_i}x^i$$
   不难验证 φ 是环同态, 且核为
   $$\begin{aligned}\ker\varphi&=\left\{\sum_{i=0}^{n}a_ix^i:\sum_{i=0}^{n}\overline{a_i}x^i=0\right\}\\&=\left\{\sum_{i=0}^{n}a_ix^i:a_i\in I\right\}\\&=I[x]\end{aligned}$$
   这就是我们需要的环同态.
3. 若 I 是 R 的素理想, 则 R/I 是整环, 从而 $R[x]/I[x]\simeq(R/I)[x]$ 是整环, 故 $I[x]$ 是 $R[x]$ 的素理想.

练习 3.3* 设 $p(x)=\sum_{i=0}^{n}a_ix^i\in R[x]$. 证明: $p(x)$ 是 $R[x]$ 的零因子当且仅当存在非零的 $b\in R$ 使得 $bp(x)=0$.

证明

1. 若存在 $b\neq0$, 使得 $bp(x)=0$, 则 $p(x)$ 显然是一个零因子.
2. 反过来, 设 $p(x)$ 是 $R[x]$ 的零因子, 则存在 $q(x)\in R[x]-\{0\}$, 使得 $p(x)q(x)=0$. 假设 $q_0(x)$ 是这些 $q(x)$ 中次数最低的多项式. 用反证法, 设 $\deg q_0(x)\geq1$.

3.1.5 拓展：形式幂级数环

3.2 域上的一元多项式环

3.2.1 课前思考

判断下列命题的正误，并说明理由：

1. $\mathbb{Z}_3[x]$ 是欧几里得整环.
2. $\mathbb{Z}[x]$ 中任意两个非零多项式都可以做带余除法.

解

1. T;
2. F：除式的首项系数必须为 ± 1

3.2.2 知识要点

1. (整环上的一元多项式环)：设 R 是整环，x 则
   (a). $R[x]$ 的单位也为 R 的单位；
   (b). $R[x]$ 是整环.
2. (多项式的带余除法)：设 $f,g \in R[x]$ 为非零多项式，且 g 的首项系数为 R 中的单位，则存在唯一的 $q,r \in R[x]$，使得 $f = qg + r$，且 $\deg r < \deg g$.
3. (域上的一元多项式环)：$F[x]$ 为欧几里得整环，其中欧几里得函数为 deg.

3.2.3 知识要点解读

(一) 多项式的带余除法

我们先来看确保带余除法可以进行的证明：

问题 3.1 (多项式的带余除法)：设 $f,g \in R[x]$ 为非零多项式，且 g 的首项系数为 R 中的单位，则存在唯一的 $q,r \in R[x]$，使得 $f = qg + r$，且 $\deg r < \deg g$.

证明 (存在性)：若 $\deg g > \deg f$，则取 $q = 0, r = f$ 即可满足题设要求. 以下设 $\deg g \leqslant \deg f$，此时令

$$f = \sum_{i=0}^{n} a_i x^i, \quad a_n \neq 0$$

$$g = \sum_{i=0}^{m} b_i x^i, \quad b_m \in R^\times$$

其中 $m \leqslant n$. 以下对非负整数 n 用数学归纳法.

1. $n = 0$ 时，$m = 0$，此时 $f = a_0 \in R, g = b_0 \in R^\times$. 于是可取 $q = a_0 b_0^{-1}, r = 0$.
2. 假设 $n \leqslant k$ 时均存在带余除法. 当 $n = k+1$ 时，考虑多项式

$$f - a_{k+1} b_m^{-1} x^{k+1-m} g$$

其次数显然不超过 $k+1$ 次，且 x^{k+1} 项的系数为 $a_{k+1} - a_{k+1} = 0$，从而其次数不超过 k 次. 利用归纳假设，存在 $q', r' \in R[x]$，使得

$$f - a_{k+1} b_m^{-1} x^{k+1-m} g = q'g + r'$$

且 $\deg r' < \deg g$. 从而我们取 $q = q' + a_{k+1} b_m^{-1} x^{k+1-m}, r = r'$，即得 $f = qg + r$，且 $\deg r < \deg g$.

综上，带余除法总是存在的.

(唯一性): 设 $f=q_1g+r_1=q_2g+r_2$, 其中 $\deg r_1,\deg r_2$ 均小于 $\deg g$. 于是有 $(q_1-q_2)g=r_2-r_1$. 考虑它们的次数: (注意第二个式子的等号是成立的, 因为 g 的首项系数不是零因子)

$$\deg(r_2-r_1)=\deg(q_1-q_2)g=\deg(q_1-q_2)+\deg g$$

并且

$$\deg(r_2-r_1)\leqslant\max\{\deg r_1,\deg r_2\}<\deg g$$

结合两式即得

$$\deg(q_1-q_2)<0$$

于是只能有 $q_1-q_2=0$, 从而 $r_2-r_1=(q_1-q_2)g=0$. 唯一性即证.

多项式的带余除法似乎和欧几里得整环里的带余除法非常相似, 但是两者是有区别的. 对于不能够作为欧几里得整环的多项式环 (例如 $\mathbb{Z}[x]$, 下一节我们会讨论) 来说, 带余除法是有限制的, 即除式的首项系数必须为系数环中的单位. 反例也很好找出, 比如 $\mathbb{Z}[x]$ 中的 x^2 就不能去 "除" $2x$. 事实上, 如果我们设存在 $q,r\in\mathbb{Z}[x]$, 使得 $x^2=q(x)(2x)+r(x)$, 且 $\deg r<1$, 则 r 只能取常数, 由次数关系, $\deg q=1$, 然而这样的话, 右侧多项式中 x^2 的系数必为 2 的倍数, 从而与左侧不可能相等, 矛盾!

另一方面, 多项式的次数是多项式的一个重要特征, 他常常作为讨论问题的突破口 (例如前面的讨论), 并且由于它取自然数 (不考虑零多项式), 所以也很有可能作为数学归纳法的指标.

3.2.4 典型例题

(一) 多项式的带余除法

多项式的带余除法是非常重要的算法, 我们在讨论多项式的可约性时经常需要用到, 我们用下面这道例题说明这一算法的操作流程.

例题 3.1 在 $\mathbb{Q}[x]$ 内求 $f=x^3-2$, $g=x+1$ 的最大公因式, 并表达成 f,g 的线性组合 (系数在 $\mathbb{Q}$ 内).

注 求最大公因子的过程依然是辗转相除法, 具体做法在 "环上的因子分解" 一节中已有具体描述. 对于读者来说可能的难点是如何做多项式的带余除法. 也就是说, 我们要找到 $q,r\in\mathbb{Q}[x]$, 使得 $f=qg+r$, 且 $\deg r<\deg g$.

首先, 由次数关系可知, q 为不超过 2 次的式子, r 为不超过 0 次的式子, 所以设 $q=ax^2+bx+c$, $r\in\mathbb{Q}$. 则有

$$\begin{aligned}x^3-2&=(ax^2+bx+c)(x+1)+r\\&=ax^3+(a+b)x^2+(b+c)x+c+r\end{aligned}$$

从而利用待定系数法可得:

$$\begin{aligned}a&=1\\a+b&=0\\b+c&=0\\c+r&=-2\end{aligned}$$

从而求得: $a=1,b=-1,c=1,r=-3$.

不过, 我们并不需要这么麻烦的做这件事. 实际上, 做带余除法, 就是尽可能地利用除式 g, 将被除式 f 不断地降次, 直至次数小于 $\deg g$ 而获得 r 的过程. 我们来看:

1. 对于 $f=x^3-2$, 显然可以利用 $ax^2g=a(x^3+x^2)$ (a 为待定系数) 将 f 降为不超过 2 次的式子, 也就是说, 让 $a(x^3+x^2)$ 的三次项系数等于 f 的三次项系数, 此时 $f_1:=f-ax^2g$ 的次数就不超过二次了. 于是利用简单的除法就可得: $a=1$, 此时 $f_1=-x^2-2$.
2. 对于 f_1 继续重复第一步的过程, 即让 $f_2=f_1-bxg$ 的最高此项系数等于 0, 于是 $b=-1$, 此时 $f_2=x-2$.
3. 最后, 对 f_2 重复第一步的过程, 即让 $f_3=f_2-cg$ 的最高此项系数等于 0, 于是 $c=1$, 此时 $f_3=-3=r$.

整合前面的过程，我们就得到了：$f=(x^2-x+1)g-3$.
我们可以将上述的机械过程表达为竖式：

$$\begin{array}{r|l} & x^2-1x+1 \\ \cline{2-2} x+1 & x^3+0x^2+0x-2 \\ & \underline{x^3+1x^2} \\ & -x^2+0x-2 \\ & \underline{-x^2+0x-1} \\ & x-2 \\ & \underline{x+1} \\ & -3 \end{array}$$

读者熟练掌握之后，可以使用更简洁的只保留系数的竖式：

$$\begin{array}{r|l} & 1-1+1 \\ \cline{2-2} 1+1 & 1+0+0-2 \\ & \underline{1+1} \\ & -1+0-2 \\ & \underline{-1+0-1} \\ & 1-2 \\ & \underline{1+1} \\ & -3 \end{array}$$

解 辗转相除法的过程如下：

$$x^3-2=(x^2-x+1)(x+1)-3$$
$$x+1=(-\frac{1}{3}x-\frac{1}{3})(-3)$$

从而 $(f,g)=-3$，且有：

$$-3=1\cdot(x^3-2)+(-x^2+x-1)(x+1)$$

✍ **练习 3.4** 在 $\mathbb{Q}[x]$ 内求下列各组多项式 $f=x^5+2x^3+x^2+x+1$, $g=x^5+x^4+2x^3+2x^2+2x+1$ 的最大公因式，并表达成 f,g 的线性组合（系数在 $\mathbb{Q}$ 内）.

解 辗转相除法的过程如下：

$$x^5+x^4+2x^3+2x^2+2x+1=1(x^5+2x^3+x^2+x+1)+(x^4+x^2+x)$$
$$x^5+2x^3+x^2+x+1=x(x^4+x^2+x)+(x^3+x+1)$$
$$x^4+x^2+x=x(x^3+x+1)$$

从而 $(f,g)=x^3+x+1$，且有：

$$\begin{aligned} x^3+x+1&=f-x(x^4+x^2+x)\\ &=f-x(g-f)\\ &=(x+1)f-xg \end{aligned}$$

3.2.5 习题

✍ **练习 3.5** 设 $f\in F[x]$ 的次数 n 为正整数，考虑商环 $F[x]/(f)$. 证明：

1. 对任意的 $g\in F[x]$，存在次数不超过 $n-1$ 的 $g_0\in F[x]$，使得 $\bar{g}=\bar{g}_0$.（记 $\bar{g}=g+(f)\in F[x]$）
2. 若 F 的阶为 q，则 $F[x]/(f)$ 的元素个数为 q^n.

注 提示：利用带余除法，对任意的 g 和 f，存在 $q,r\in F[x]$，使得 $g=qf+r$，其中 $\deg r<\deg f$，于是 $\bar{g}=\bar{r}$. 取 $g_0=r$ 即可.

✍ **练习 3.6** 设 $f\in F[x]$，证明：$F[x]/(f)$ 是域，当且仅当 f 不可约.

注 提示：$F[x]/(f)$ 是域，当且仅当 (f) 是极大理想，当且仅当 (f) 是素理想（$F[x]$ 为主理想整环），当且仅当 f 是素元，当且仅当 f 不可约（$F[x]$ 为唯一因子分解整环）.

✍ **练习 3.7*** 设 F 是有限域，证明：$F[x]$ 中有无穷多个素元.

注 提示：假设 $F[x]$ 中只有有限个素元 $p_1,\cdots,p_n$，考虑元素 $p=p_1\cdots p_n+1$，p 不能被任意 p_i 整除，从而只能为新的素元，矛盾!

✍ **练习 3.8*** 设 $f\in F[x]$，试写出 $F[x]/(f)$ 的所有理想.

解 利用第四同构定理可知，$F[x]/(f)$ 的理想均有形式 $I/(f)$，其中 I 为 $F[x]$ 的理想. 由于 $F[x]$ 为欧几里得整环，所以为主理想整环，于是 I 总可以表达为 $(g),g\in F[x]$.

若 $(g)/(f)$ 为 $F[x]/(f)$ 的理想，则对任意的 $\bar{h}\in F[x]/(f)$，和任意的 $r\in F[x]$，有

$$\bar{h}\overline{rg}\in(g)/(f)$$

即存在 $s\in F[x]$，使得 $\overline{hrg}=\overline{sg}$，也就是有 $f|(hr-s)g$.

若 $f|g$，则 $(g)/(f)=\{\bar{0}\}$. 若 $f|hr-s$，则由 hr 的任意性，只能有 $hr-s=0$

？

✍ **练习 3.9** 试求出环 $\mathbb{Z}[x]/(2,x^3+1)$ 的所有理想.

证明 先证明：$\mathbb{Z}[x]/(2,x^3+1)\simeq\mathbb{Z}_2[x]/(x^3+1)$.

定义映射

$$\varphi:\mathbb{Z}[x]\to\mathbb{Z}_2[x]/(x^3+1)$$
$$\sum_{i=0}^{n}a_ix^i\mapsto\sum_{i=0}^{n}\overline{a_i}x^i+(x^3+1)$$

其中对任意的 $a_i\in\mathbb{Z}$，$\overline{a_i}=a_i+(2)$.

从而易证 φ 是环满同态. 下面求 φ 的核. 设 $f=\sum_{i=0}^{n}a_ix^i\in\ker\varphi$，则存在 $r\in\mathbb{Z}_2[x]$，使得

$$\sum_{i=0}^{n}\overline{a_i}x^i=r(x^3+1)$$

将 $\overline{a_i}\in\mathbb{Z}_2$ 视为其在 $\mathbb{Z}$ 中的对应数值（例如将 $\bar{1}$ 视作 1），则存在 $q\in\mathbb{Z}[x]$，使得 $f=\sum_{i=0}^{n}\overline{a_i}x^i+2q$，从而（此处将 r 的系数也视做 $\mathbb{Z}$ 中的数值）

$$f-2q=r(x^3+1)$$

即 $f\in(2)+(x^3+1)$. 另一方面，对任意的 $g\in(2)+(x^3+1)$，显然 $\varphi(g)=0$. 所以有 $\ker\varphi=(2)+(x^3+1)=(2,x^3+1)$. 从而有 $\mathbb{Z}[x]/(2,x^3+1)\simeq\mathbb{Z}_2[x]/(x^3+1)$.

又因为 $\mathbb{Z}_2$ 是域，所以 $\mathbb{Z}_2[x]$ 是欧几里得整环（从而为主理想整环）. $\mathbb{Z}_2[x]$ 中的每个元素都对应着一个主理想，从而也是全部的理想，于是 $\mathbb{Z}[x]/(2,x^3+1)$ 中的理想都形如 (ax^2+bx+c)，其中 $a,b,c\in\mathbb{Z}_2$.

笔记 此题证明过程不严谨.

✍ **练习 3.10** 证明以下环同构：

1. $\mathbb{Z}[x]/(2)\simeq\mathbb{Z}_2[x]$；
2. $\mathbb{Z}[x]/(x)\simeq\mathbb{Z}$；

✍ **练习 3.11** 试描述商环 $\mathbb{Z}[x]/(x^2)$ 的结构.（它包含哪些元素，其上的计算如何定义?）

3.2.6 作者的话：“计算题”与“证明题”谁更重要？

本章中出现了很多非证明的计算题，比如求多项式的最大公因式、因式分解等等. 读者可以看到，计算题的解题思路与证明题完全不一样（显然如此），考察或者训练的能力也有区别. 一个学生在学完 Maki 的讲义之后，或许可以把至少一半的证明题解出来，但是如果不经过额外的学习，可能一道计算题也做不出.

在笔者看来，不论是计算题还是证明题，都是对所学理论知识的实际应用. 那么它们之间的区别在哪呢？在于直接处理的对象不一样. 证明题，更多的是处理基本、抽象的概念，所讨论的问题也往往比较抽象，也就是说，基本上是讲义知识体系的直接延伸，以抽象对抽象. 而计算题处理的主要是具体的实例，而且往往是非常具体的，所以它们距离所学的知识体系实际上有一点远，往往所需要的思想方法也不会在讲义中呈现，这大概是有时候计算题比证明题“难”的关键所在.

例如，当你学完唯一因子分解整环的时候，你应该已经知道，$\mathbb{Z}, \mathbb{Z}[x]$ 都是唯一因子分解整环. 在理论教材中，对这一问题的描述到此为止，不再展开. 而实际应用中呢？需要你再证明一遍同样的结论吗？显然不会了，也没有意义，实际问题只会是诸如“$x^3+y^3+z^3-3xyz$ 是否可约”这样的类型. 于是我们发现，我们学过的理论知识，为我们讨论这些问题打下了基础，但是不能够帮助我们解决这些问题.

说到这里，大家应该已经明白两种类型问题的区别和关联所在了. 笔者认为，两种类型的问题没有包含关系，你熟悉一种问题的同时，可以对另一种问题没有任何办法. 也就是说，两种问题的地位相同，仅从问题的角度而言，也没有重要性排序. 当然对于具体的每个读者来说，重要性是很有可能不一样的. 如果读者更关心实际应用，那他甚至于可以不用深入地学理论，搞清楚计算的方法就好；反之，如果读者更关心理论证明，那么他也可以不用很关心不太常用的计算方法. 一切取决于读者的实际需求.

而如果你和笔者一样，目前没有特别明确的应用场景，学习的目的是为了提高自己的数学的综合能力，那么笔者真诚地建议你，重视计算题的作用和价值. 一般来说，证明题能帮助我们更好的理解概念，计算题能更好的帮助我们熟悉抽象理论下沉到具体情境中的情形，从而为抽象概念的存在找到依据. 因为我们生活在具体的世界中，我们所构建的每一种抽象的知识体系，都是为了帮助我们更深刻地认识世界、理解世界、改造世界，如果我们不熟悉抽象概念在具体世界中的应用情形，我们又何谈利用抽象概念认识世界呢？打个比方说，这就像一个小学一年级的孩子，他已经知道整数连同加法和乘法构成欧几里得整环，但是不知道 $1+1$ 等于几. 他可以在抽象的概念世界里走得很远，但是在现实世界中将寸步难行.

所以，笔者的观点是，理论证明和实际计算都很重要，在没有特定需求的情况下，我们应该做到两者同步训练同步发展，避免出现一条腿走路的情况. 换句话说，既不要不懂理论，“知其然而不知其所以然”；更不要站在理论的“高峰”上俯瞰计算，甚至于产生了某种轻视计算的心态. 只关心实际计算，思维能力很难提升；只关心理论证明，又终将会陷入概念的“乐园”中而脱离世界.

3.3 唯一因子分解整环上的多项式环

3.3.1 课前思考

判断下列命题的正误，并说明理由：

1. x^2+2 是不可约多项式.
2. 设 $f \in \mathbb{Z}[x]$. 若 f 在 $\mathbb{Q}[x]$ 上不可约，则 f 在 $\mathbb{Z}[x]$ 上不可约.
3. $\mathbb{Q}[x]$ 是唯一因子分解整环.

解

1. F：没有说明多项式所在的环，从而讨论可约性是没有意义的；
2. F：$f=2x+4$ 在 $\mathbb{Q}[x]$ 上不可约，但是在 $\mathbb{Z}[x]$ 上可约 $f=2(x+2)$（这里 $2, x+2$ 均不是单位，所以都是 f 的真因子）；
3. T.

3.3.2 知识要点

1. 容量：设 R 是唯一因子分解整环，$f=\sum_{i=0}^{n}a_ix^i\in R[x]-\{0\}$. 定义 f 的容量为
$$\operatorname{cont}(f):=\gcd(a_0,\cdots,a_n)$$
本原多项式：多项式的容量为 1.
2. （高斯引理）：设 R 是唯一因子分解整环，$f,g\in R[x]$. 则 $\operatorname{cont}(fg)=\operatorname{cont}(f)\operatorname{cont}(g)$.
特别的，$R[x]$ 中两个本原多项式的乘积仍为本原多项式.
3. （分式域上的多项式环）：设 R 是唯一因子分解整环，F 是 R 的分式域，$f\in R[x]$ 是本原多项式且 $\deg f\geqslant 1$，则 f 在 $R[x]$ 中不可约，当且仅当 f 在 $F[x]$ 中不可约.
4. （唯一因子分解整环上的多项式环）：设 R 是唯一因子分解整环，则 $R[x]$ 是唯一因子分解整环.

3.3.3 知识要点解读

（一）本原多项式的可约性

考察多项式 $2x+4$，在 $\mathbb{Z}[x]$ 内，它是可约的 $2x+4=2(x+2)$，而在 $\mathbb{Q}[x]$ 内，它就变得不可约了，因为此时 $2\in\mathbb{Q}$ 是单位. 我们在研究多项式的可约性时，系数的公因子（即多项式的容量）总是容易率先提取出来，然后得到容量为 1 的本原多项式. 而考察本原多项式的可约性时，我们可以把系数环扩展到对应的分式环中，下面的定理确保了这样操作的合理性.

问题 3.2 （分式域上的多项式环）：设 R 是唯一因子分解整环，F 是 R 的分式域，$f\in R[x]$ 是本原多项式且 $\deg f\geqslant 1$，则 f 在 $R[x]$ 中不可约，当且仅当 f 在 $F[x]$ 中不可约.

注 我们首先要考虑一个问题：系数环的扩张（从 R 到分式域 F）对 $R[x]$ 中多项式的可约性有什么影响？取可约多项式 $f=gh\in R[x]$. 如果 g,h 都是次数至少为 1 的多项式，那么扩张系数环后，真因子仍然为真因子. 但是，如果某个因子（不妨其设为 g）是 R 中的元素，那么扩张系数环后，R 中的非零元均变成了 F 中的单位，此时 g 不再是 f 的真因子，这就有可能改变 f 的可约性. 前面提到的 $2x+4\in\mathbb{Z}[x]$ 就是这样的情况。【Victor: 122】

回到本题，我们发现题设中要求 f 是本原多项式，这就杜绝了 f 在 $R[x]$ 中有属于 R 的真因子的情况，从而我们马上就能够知道：若 f 在 $R[x]$ 中可约，则 f 在 $F[x]$ 中可约. 也就是说：若 f 在 $F[x]$ 中不可约，则 f 在 $R[x]$ 中不可约.

另一个方向的命题我们该如何考虑？请先看解答.

证明 一方面，设 f 在 $F[x]$ 中不可约. 此时，如果 f 在 $R[x]$ 中可约，即 $f=gh$，$g,h\in R[x]$. 首先 g,h 不可能是 R 中的元素（否则 $\operatorname{cont}(f)\neq 1$），从而 g,h 都是至少一次的多项式. 而 $g,h\in R[x]\subset F[x]$，所以 f 在 $F[x]$ 中可约，矛盾！从而 f 在 $R[x]$ 中不可约.

另一方面，设 f 在 $R[x]$ 中不可约，假设 f 在 $F[x]$ 中可约，由前一段的讨论可知 f 没有 R 中的真因子，所以设 $f=gh$，且 $g,h\in F[x]$ 都是至少一次的多项式. 取 g 的系数（均约化为既约分式）的分母的最小公倍元 b 和 h 的系数的分母的最小公倍元 d，并且令
$$g'=bg/\operatorname{cont}(bg)$$
$$h'=dh/\operatorname{cont}(dh)$$
从而 $g',h'\in R[x]$，且 $\operatorname{cont}(g'),\operatorname{cont}(h')$ 均与 1 相伴. 并且有
$$f=gh=\frac{\operatorname{cont}(bg)\operatorname{cont}(dh)}{bd}g'h'$$
由于 $\operatorname{cont}(f)$ 为单位，从而
$$bd\sim bd\operatorname{cont}(f)\sim\operatorname{cont}(bdf)\sim\operatorname{cont}(\operatorname{cont}(bg)\operatorname{cont}(dh)g'h')\sim\operatorname{cont}(bg)\operatorname{cont}(dh)$$
也就有 $f\sim g'h'$，从而 f 在 $R[x]$ 中可约，矛盾！从而 f 在 $F[x]$ 中不可约.

综上，命题得证.

笔记 另一个方向得命题，处理起来有一定的技巧上的困难，不过思路其实是很明确的，我们想要证明：假如 f 在 $F[x]$ 中可约，则必然可以找到其在 $R[x]$ 中的真因式. 而整个的证明过程就是在找这样的因式：若本原多项式 f 在 $F[x]$ 中可约，且 $f=gh$，则 f 在 $R[x]$ 中亦可约，且 $f\sim g'h'$，其中 $g',h'\in R[x]$ 可如下构造：取 g 的系数的分母的最小公倍元 b 和 h 的系数的分母的最小公倍元 d，并令

$$g'=bg/\operatorname{cont}(bg)$$
$$h'=dh/\operatorname{cont}(dh)$$

我们用一个实例来解释这一过程：设 $g=\frac{9}{2}x^2+\frac{3}{4}x+3\in\mathbb{Q}[x]$，我们要想办法把 f 转化到 $\mathbb{Z}[x]$ 中，所以我们要对系数去分母，于是我们取 $4g=18x^2+3x+12$. 不过仅仅去分母是不够的，因为我们讨论的是本原多项式，所以还要约去系数的最大公因子，从而我们最终取 $g'=4g/\operatorname{cont}(4g)=6x^2+x+4$.

在我们按前述方法取了 g',h' 后，最后就是想办法说明：在 $R[x]$ 中，$gh\sim g'h'$，这就要用到高斯引理了. 当然这一过程是很直白的，没有理解上的障碍.

此外，我们发现一个有趣的事实：若 b,d 不是单位，则有 $\operatorname{cont}(bg)\nmid b$ 和 $\operatorname{cont}(dh)\nmid d$（在我们举的例子中，$b=4,\operatorname{cont}(bg)=3$）. 假如 $\operatorname{cont}(bg)|b$，则因为 $(b^{-1}\operatorname{cont}(bg))\in R[x]$，所以 $b^{-1}\operatorname{cont}(bg)$ 也必为 g 的系数的分母的公倍元，于是由最小公倍元的定义可得 $b|b^{-1}\operatorname{cont}(bg)$，即 $b^2|\operatorname{cont}(bg)$. 这就说明，$g$ 的系数的分子有公因子 b，从而 g 的系数都是 R 的元素，也就是说，g 的系数的分母都是单位，从而 b 是单位，矛盾！

3.3.4 习题

练习 3.12 设 R 是唯一因子分解整环，F 是 R 的分式域，$p\in R[x]$. 若 $p=fg$，其中 $f,g\in F[x]$ 均不是常数多项式，则存在 $r,s\in F^*$，使得 $f'=rf,g'=sg$ 都是 $R[x]$ 中的元素，且 $p=f'g'$.

证明 因为 $p\in R[x]$，从而令 $q=p/\operatorname{cont}(p)\in R[x]$，这样 $\operatorname{cont}(q)=1$，且有 $q=f(g/\operatorname{cont}(p))$. 由于 f,g 均不是常系数，从而 q 在 $F[x]$ 内可约，于是 q 在 $R[x]$ 内可约. 取 f 的系数的分母的公倍元 b 和 g 的系数的分母的最小公倍元 d（于是 $g/\operatorname{cont}(p)$ 的系数的分母的最小公倍元为 $\operatorname{cont}(p)d$）. 令

$$f'=bf/\operatorname{cont}(bf)$$
$$h=dg/\operatorname{cont}(dg)$$

从而 $q\sim f'h$，即 $p=f'u\operatorname{cont}(p)h:=f'g',u\in R^\times$. 其中

$$f'=\frac{b}{\operatorname{cont}(bf)}f$$
$$g'=\frac{du\operatorname{cont}(p)}{\operatorname{cont}(dg)}g$$

都是 $R[x]$ 中的元素.

练习 3.13 设 R 是整环，F 是 R 的分式域，$f\in R[x]$ 是首一的，并且有 $f=gh$，其中 $g,h\in F[x]$ 也是首一的，次数低于 f. 证明：若 $g\notin R[x]$，则 R 不是唯一因子分解整环.

证明 若 R 是唯一因子分解整环，则 $R[x]$ 是唯一因子分解整环. 由定理“分式域上的多项式环”的证明过程可得，取 g 的系数的分母的最小公倍元 b 和 h 的系数的分母的最小公倍元 d，并令

$$g'=bg/\operatorname{cont}(bg)$$
$$h'=dh/\operatorname{cont}(dh)$$

从而有 $f=ug'h',u\in R^\times,g',h'\in R[x]$. 下证：$\operatorname{cont}(bg)\sim 1$.（从而 $\operatorname{cont}(dh)\sim 1$）

假设 $\operatorname{cont}(bg)=c$ 不是单位，则 $(c^{-1}b)g\in R[x]$，从而 $c^{-1}b$ 是 g 的系数的分母的公倍元，从而必有 $b|c^{-1}b$，即 $c\sim 1$，矛盾！

由于 $\operatorname{cont}(bg)\sim\operatorname{cont}(dh)\sim 1$，于是有 $f\sim g'h'=bdgh=bdf$，即 $bd\sim 1$，也就是 $b\sim d\sim 1$. 于是 $g=b^{-1}g'\in R[x]$，与题设矛盾！

练习 3.14 利用前一题的结论证明：环 $R=\mathbb{Z}[2\sqrt{2}]$ 不是唯一因子分解整环.

证明 考虑多项式 $x^2+2\sqrt{2}x+2\in R[x]$，我们有：

$$x^2+2\sqrt{2}x+2=(x+\sqrt{2})^2$$

由于 $\sqrt{2}=(2\sqrt{2})/2$，所以 $x+\sqrt{2}\in F[x]$，其中 F 为 R 的分式域. 然而 $x+\sqrt{2}\notin R[x]$，所以由前一题的结论可得：R 不是唯一因子分解整环.

✍ **练习 3.15** 设 F 是域，定义集合

$$R:=\{\sum_{i=0}^{n}a_ix^i\in F[x]:a_1=0,n\in\mathbb{N}\}$$

证明：R 是 $F[x]$ 的子环，且不是唯一因子分解整环.

注 提示：$x^6=(x^2)^3=(x^3)^2$，而 x^2,x^3 在 R 内都是不可约元.

✍ **练习 3.16*** 设 $f,g\in\mathbb{Q}[x]$，且 $fg\in\mathbb{Z}[x]$. 证明：任取 f 的一个系数和 g 的一个系数相乘，得到的都是整数.

证明 取 f 的系数（均约化为既约分数）的分母的最小公倍数 b 和 g 的系数的分母的最小公倍数 d，并且令

$$f'=bf/\operatorname{cont}(bf)$$
$$g'=dg/\operatorname{cont}(dg)$$

于是 $f',g'\in\mathbb{Z}[x]$ 的容量均为 1，从而 $f'g'$ 的容量为 1. 进一步的，因为

$$fg=\frac{\operatorname{cont}(bf)\operatorname{cont}(dg)}{bd}f'g'\in\mathbb{Z}[x]$$

所以 $q=\frac{\operatorname{cont}(bf)\operatorname{cont}(dg)}{bd}\in\mathbb{Z}$（否则其既约形式的分母需要被 $f'g'$ 的所有系数整除，从而 $f'g'$ 的容量不为 1，矛盾！）

注意到 f 中的任意系数 a_i 都可以表达成 $\frac{\operatorname{cont}(bf)}{b}a_i'$，其中 a_i' 是 f' 中对应项的系数，类似地，g 中的任意系数 b_j 都可以表达成 $\frac{\operatorname{cont}(dg)}{d}b_j'$，其中 b_j' 是 g' 中对应项的系数，于是有：

$$\begin{aligned}a_ib_j&=\frac{\operatorname{cont}(bf)}{b}a_i'\frac{\operatorname{cont}(dg)}{d}b_j'\\&=qa_i'b_j'\end{aligned}$$

由于 $f',g'\in\mathbb{Z}[x]$，所以 $a_i',b_i'\in\mathbb{Z}$，前面又已证明 $q\in\mathbb{Z}$，所以 $a_ib_j\in\mathbb{Z}$，原命题得证.

笔记 本题的证明过程稍加改造，即可证明更一般地命题：“设 R 是交换环，F 为其分式域. $f,g\in F[x]$，且 $fg\in R[x]$. 证明：任取 f 的一个系数和 g 的一个系数相乘，得到的都是 R 中的元素.”

3.3.5 综合题：环 $R=\mathbb{Z}+x\mathbb{Q}[x]$ 的性质

✍ **练习 3.17** 证明：R 是整环.

证明 设 $m+xf(x),n+xg(x)\in\mathbb{Z}+x\mathbb{Q}[x]$ 满足 $(m+xf(x))(n+xg(x))=0$. 首先，左式的常数项为 mn，于是 $mn=0$，注意到 $m,n\in\mathbb{Z}$，从而只能有 $m=n=0$，于是原式化简为 $x^2f(x)g(x)=0$，又 $\mathbb{Q}[x]$ 为整环，且 $x^2\neq0$，所以 $f(x)g(x)=0$，从而只能有 $f(x)$ 或 $g(x)$ 为零多项式. 然而此时必有 $m+xf(x)$ 或 $n+xg(x)$ 等于零. 从而 R 是整环.

✍ **练习 3.18** 证明：R 的单位为 ±1.

证明 设 $m+xf(x),n+xg(x)\in\mathbb{Z}+x\mathbb{Q}[x]$ 满足 $(m+xf(x))(n+xg(x))=1$. 首先，左式的常数项为 mn，于是 $mn=1$，注意到 $m,n\in\mathbb{Z}$，从而只能有 $m=n=1$ 或 -1.

一方面，若 $m=n=1$，则 $xf(x)+xg(x)+x^2f(x)g(x)=0$. 又 $\mathbb{Q}[x]$ 为整环，且 $x\neq0$，所以 $f(x)+g(x)+xf(x)g(x)=0$. 考虑等式两侧的多项式次数：

$$\deg f+\deg g+1=-\infty$$

所以 f,g 中至少有一个为零多项式，不妨设 $f=0$，从而可得 $g=0$.

另一方面，若 $m=n=-1$，同理可证 $f=g=0$.

综上，只能有 $1\cdot 1=1$ 或 $(-1)\cdot(-1)=1$. 即 R 的单位为 ± 1.

✍ **练习 3.19** 证明：R 中的不可约元可以分为两类：

1. $\pm p$，其中 p 为 $\mathbb{Z}$ 中的素数；
2. $\mathbb{Q}[x]$ 中的不可约多项式 $h(x)$，其中 h 的常数项为 ± 1.

证明

1. 先证明：$\mathbb{Z}$ 中的素数 p 是 R 中的不可约元. 若存在 $m+xf(x),n+xg(x)\in\mathbb{Z}+x\mathbb{Q}[x]$，使得 $(m+xf(x))(n+xg(x))=p$，则必有

$$mn=p$$
$$mxg(x)+nxf(x)+x^2f(x)g(x)=0$$

和前一题的证明过程类似的，可得 $f=g=0$，从而只能有 $p=mn$. 而 p 在 $\mathbb{Z}$ 内不可约，所以 $m+xf(x),n+xg(x)$ 只能取 $\pm p,\pm 1$，均不是 p 的真因子，从而 p 在 R 上不可约.

类似可证 $-p$ 是 R 中的不可约元.

2. 再证明：若 $h(x)$ 是 $\mathbb{Q}[x]$ 中的不可约多项式，且 h 的常数项为 1，则 $h(x)$ 在 R 内不可约. 设 $m+xf(x),n+xg(x)\in\mathbb{Z}+x\mathbb{Q}[x]$，使得

$$(m+xf(x))(n+xg(x))=h(x).$$

由于 $h(x)\in\mathbb{Q}[x]$ 不可约，且 $m+xf(x),n+xg(x)\in\mathbb{Q}[x]$，所以 $m+xf(x),n+xg(x)$ 中必有一个为 $\mathbb{Q}[x]$ 中的单位，也就是 $\mathbb{Q}^*$ 中的元素，不妨设 $m+xf(x)\in\mathbb{Q}$，则 $f=0$，于是有：

$$m(n+xg(x))=h(x)$$

对比等式两侧的常数项可得 $mn=1$，即 $m=\pm 1\in R^\times$. 于是 $h(x)$ 在 R 中亦不可约.

类似可证：若 $h(x)$ 是 $\mathbb{Q}[x]$ 中的不可约多项式，且 h 的常数项为 -1，则 $h(x)$ 在 R 内不可约.

3. 最后证明：若 $h(x)\in R$ 不属于题设描述的两类元素，则 $h(x)$ 必在 R 中可约. 也就是说，若 $h(x)$ 的常数项不是 $\mathbb{Z}$ 中的素数，则 $h(x)$ 必在 R 中可约.

设 $h(x)=xu(x)+n$，其中 n 不是 $\mathbb{Z}$ 中的素数，则 n 有因子分解 $n=pq$，其中 p,q 都是 n 的真因子. 取

$$f(x)=x(u(x)/p)+q$$
$$g(x)=x0+p=p$$

则 $f,g\in R$ 都不是单位，且 $fg=h$，从而 h 在 R 上可约.

综上，R 中的不可约元只有题设中描述的两类元素.

✍ **练习 3.20** 证明：R 中的不可约元都是素元.

证明 我们将两类不可约元分别讨论即可.

1. 先证明：$\mathbb{Z}$ 中的素数 p 是 R 中的素元.

设 $p|(m+xf(x))(n+xg(x))=(mn+(mg(x)+nf(x))x+x^2f(x)g(x))$，其中 $m+xf(x),n+xg(x)\in\mathbb{Z}+x\mathbb{Q}[x]$，则 p 必然整除右侧多项式的各项系数. 首先就有 $p|mn$，由于 p 是素数，所以由 $\mathbb{Z}$ 的性质可得 $p|m$ 或 $p|n$. 不妨设 $p|m$，即存在 $k\in\mathbb{Z}$，使得 $pk=m$，于是 $m+xf(x)=p(k+xf(x)/p)$，即 $p|m+xf(x)$. 同理，若设 $p|n$ 则可证明 $p|n+xg(x)$，从而 p 是 R 中的素元.

2. 再证明：若 $h(x)$ 是 $\mathbb{Q}[x]$ 中的不可约多项式，且 h 的常数项为 1，则 $h(x)$ 为素元.

设 $h(x)|(m+xf(x))(n+xg(x))$，其中 $m+xf(x),n+xg(x)\in\mathbb{Z}+x\mathbb{Q}[x]$. 由于 h 在 $\mathbb{Q}[x]$ 不可约，从而在 $\mathbb{Q}[x]$ 中为素元，于是在 $\mathbb{Q}[x]$ 中必有 $h(x)|m+xf(x)$ 或 $h(x)|n+xg(x)$. 不妨设 $h(x)|m+xf(x)$，即存在 $u(x)\in\mathbb{Q}[x]$，使得 $h(x)q(x)=m+xf(x)$，比较两侧的常数项可得

$$\pm 1q(0)=m$$

即 $q(0)=\pm m\in\mathbb{Z}$，于是 $q(x)\in\mathbb{Z}+x\mathbb{Q}[x]$. 从而在 R 中有 $h(x)|m+xf(x)$. 同理，若在 $\mathbb{Q}[x]$ 中有 $h(x)|n+xg(x)$，则其同样可在 R 中成立，从而 $h(x)$ 是 R 中的素元.

结合前一题的结论可得：R 中的不可约元都是素元.

✍ **练习 3.21** 证明：x 不可写做 R 中一些不可约元的乘积，从而 R 不是唯一因子分解整环.

证明 假设 x 可以在 R 中做不可约元分解：$x=p_1\cdots,p_n$. 由前面的问题可知，任意的 p_i 只可能为 $\mathbb{Z}$ 中的素数，或者 $\mathbb{Q}[x]$ 中常数项为 ±1 的不可约多项式. 然而不论哪一种情况，p_i 的常数项均不为 0，从而乘积 $p_1\cdots,p_n$ 的常数项也必不为 0. 但是 x 的常数项为 0，矛盾！所以这样的不可约元分解不存在.

由此可以说明，R 不是唯一因子分解整环.

✍ **练习 3.22** 证明：x 不是 R 中的素元. 描述商环 $R/(x)$ 的结构.

证明 整环中，素元都是不可约元. 而由前面的问题可知，x 不是 R 中的不可约元，从而也不是 R 中的素元.

由于 $(x)=Rx$ 为 $\mathbb{Q}[x]$ 中常数项为 0，一次项系数为整数的多项式的集合，所以 $R/(x)=\{ax+b:a\in[0,1),b\in\mathbb{Z}\}$.

笔记 我们也可以回归定义说明 x 不是素元. 考虑 $x|(\frac{1}{2}x+0)(x+1)$，然而在 R 中 $x\nmid\frac{1}{2}x$，且 $x\nmid(x+1)$.

3.4 拓展：不可约判定

注：本节在 Maki 的讲义的基础上增加了余数定理等内容. 笔者的意图是构建一个相对完整的处理多项式因子分解的知识体系：寻找一次因式可以利用因式定理，寻找高次根式利用单代数扩域（留待下一章讲解）；以及判定一些特殊的不可约多项式的方法：系数取模法，同时说明 Eisenstein 判别法是系数取模思想的特例.

3.4.1 课前思考

判断下列命题的正误，并说明理由：

1. $x^4+4\in\mathbb{Z}[x]$ 是可约的.
2. $x^4+1\in\mathbb{Z}_2[x]$ 是不可约的.
3. $x^{100}+2x^{50}-2\in\mathbb{Q}[x]$ 没有有理根.

解

1. T：$x^4+4=(x^2+2x+2)(x^2-2x+2)$；
2. F：$x^4+1=(x+1)^4$；
3. T：原式若有有理根，则只能为 $\pm1,\pm2$，显然它们都不是原始的根.

3.4.2 知识要点

1. （余数定理）：设 $f\in R[x]$，则对任意的 $c\in R$，均有唯一的 $q\in R[x]$，使得 $f=q(x-c)+f(c)$.（即 f 除以 $x-c$ 的余数为 $f(c)$）
2. （因式定理）：设 $f\in R[x],c\in R$，则 $(x-c)|f$，当且仅当 $f(c)=0$.
3. （$\mathbb{Z}$ 上多项式的有理根）：$p(x)=\sum_{i=0}^n a_ix^i\in\mathbb{Z}[x]$. 若既约分数 $r/s\in\mathbb{Q}$ 是 $p(x)$ 的根，则 $r\mid a_0$，$s\mid a_n$.
4. （不可约判定：系数取模）：I 是整环 R 的真理想. $p(x)$ 是 $R[x]$ 内的首一多项式，且不为常数. 若 $p(x)$ 在 $(R/I)[x]$ 内的象（即 $p(x)$ 的系数均模 I 得到的多项式）不能被分解为两个次数更低的多项式，则 $p(x)$ 在 $R[x]$ 内不可约.
5. （Eisenstein 判别法）：P 是唯一因子分解整环 R 的素理想，F 是 R 的分式域，$f(x)=\sum_{i=0}^n a_ix^i$ 是 $R[x]$ 中的多项式（$n\geqslant1$）. 若 $a_n\notin P$，$a_{n-1},\cdots,a_0\in P$，且 $a_0\notin P^2$，则 $f(x)$ 在 $F[x]$ 内不可约.
   进一步的，若 f 在 $R[x]$ 内本原，则 f 在 $R[x]$ 内不可约.

3.4.3 知识要点解读

（一）一次根式的搜索：因式定理

寻找一个多项式的一次因式，本质是就是在寻找它的根，因为我们有余数定理及其推论：因式定理.

问题 3.3（余数定理）：设 $f\in R[x]$，则对任意的 $c\in R$，均有唯一的 $q\in R[x]$，使得 $f=(x-c)q+f(c)$.（即 f 除以 $x-c$ 的余数为 $f(c)$）

证明 由多项式的带余除法可知，对被除式 f 和除式 $x-c$，存在唯一的 $q,r\in R[x]$，使得 $f=(x-c)q+r$，且 $\deg r<\deg(x-c)$，从而 $r\in R$. 等式两侧代入 $x=c$ 可得：$f(c)=0+r$，即 $r=f(c)$. 原命题得证.

余数定理很容易得到因式定理：$f(c)=0$ 等价于 $(x-c)|f(x)$. 这一定理在初等数学的因式分解中，初场频率特别高，而且有一个非常玄学的名称“试根法”. 实际上，那些看起来奇奇怪怪的尝试，都是有对应的命题在背后支撑，比如单位根、二次根式（这些都有域的代数扩张的知识背景，我们会在下一章提及），又比如下面提到的有理根的判定.

问题 3.4（$\mathbb{Z}$ 上多项式的有理根）：$p(x)=\sum_{i=0}^n a_ix^i\in\mathbb{Z}[x]$. 若既约分数 $r/s\in\mathbb{Q}$ 是 $p(x)$ 的根，则 $r\mid a_0$，$s\mid a_n$.

注 这一定理的证明非常简单，但是对于寻找整系数多项式的有理根特别有用，进一步说，对于寻找整系数多项式在 $\mathbb{Z}[x]$ 内的一次因式特别有用.

证明 由于既约分数 $r/s\in\mathbb{Q}$ 是 $p(x)$ 的根，所以

$$0=p(r/s)=\sum_{i=0}^n a_ir^is^{-i}$$

等式两侧同时乘 s^n 可得：

$$\sum_{i=0}^n a_ir^is^{n-i}=0$$

一方面有：

$$a_0s^n=\sum_{i=1}^n a_ir^is^{n-i}=r\sum_{i=1}^n a_ir^{i-1}s^{n-i}$$

从而 $r|a_0s^n$，而 $r\nmid s$，从而 $r|a_0$.

另一方面有

$$a_nr^n=\sum_{i=0}^{n-1} a_ir^is^{n-i}=s\sum_{i=0}^{n-1} a_ir^is^{n-1-i}$$

从而 $s|a_nr^n$，而 $s\nmid r$，从而 $s|a_n$.

笔记 涉及到唯一因子分解整环 R(及其分式域 F) 的问题，考虑整除性总是一个可选的思路.

（二）不可约判定：系数取模思想

一般意义上的因式分解问题，最终都要依靠分裂域，将多项式的根（等价地说是一次因式）全部包括进数环中才能得以解决. 比如 $x^2-2\in\mathbb{Q}[x]$ 是不可约的，但是将 $\sqrt{2}$ 扩充到系数环中，即考虑系数环 $\mathbb{Q}[\sqrt{2}]$，此时 x^2-2 就变得可约.

对于一类特殊的多项式，我们有“取巧”的处理方法，可以直接判定它不可约，这就是下面介绍的系数取模的方法，以及经典的 Eisenstein 判别法.

问题 3.5（不可约判定：系数取模）：I 是整环 R 的真理想. $p(x)$ 是 $R[x]$ 内的首一多项式，且不为常数. 若 $p(x)$ 在 $(R/I)[x]$ 内的象 $q(x)$ 不能被分解为两个次数更低的多项式，则 $p(x)$ 在 $R[x]$ 内不可约.

证明 记 $p(x)=x^n+\sum_{i=0}^{n-1}a_ix^i$，则 $q(x)=x^n+\sum_{i=0}^{n-1}\overline{a_i}x^i$. 假设 $p(x)$ 在 $R[x]$ 内可约，则 $p(x)=f(x)g(x)$，其中 $f(x),g(x)$ 均为真因子. 由于 $p(x)$ 的首项系数为 1，所以 f,g 的首项系数均为单位，从而 f,g 不能是常数. 不妨记 $\deg f=k$，则 $\deg g=n-k$，其中 $k\in[1,n-1]$.

对等式 $p(x)=f(x)g(x)$ 两侧的多项式的系数做模 I 的操作【由于 $\overline{ab}=\bar{a}\bar{b}$，所以这样的操作保持等式. 或者理解为 $R[x]/I[x]$，参见第一节的习题 3.2】. 由于 I 是 R 的真理想，所以 f,g 的首项系数（也就是单位）均不属

于 I，从而取模之后 f,g 不降次，即为 q 的真因子. 所以 q 可约，这与题设矛盾！

笔记 这一命题的意义在于，我们可以通过对系数环取模，使得系数环的形式非常简单（例如有限域），从而简化对问题的讨论.

问题 3.6（Eisenstein 判别法）：P 是唯一因子分解整环 R 的素理想，F 是 R 的分式域，$f(x)=\sum_{i=0}^{n}a_ix^i$ 是 $R[x]$ 中的多项式（$n\geqslant 1$）. 若 $a_n\notin P$，$a_{n-1},\cdots,a_0\in P$，且 $a_0\notin P^2$，则 $f(x)$ 在 $F[x]$ 内不可约.

证明 假设 f 在 $F[x]$ 中可约，则有 $f=gh$，其中 g,h 为 f 的真因子，从而 f,g 均不是常数. 记

$$g=\sum_{i=0}^{k}b_ix^i$$

$$h=\sum_{i=0}^{n-k}c_ix^i$$

其中整数 $k\in[1,n-1]$. 对等式两边多项式的系数模 P，可得 $\overline{a_n}x^n=g'h'$，其中

$$g'=\sum_{i=0}^{k}\overline{b_i}x^i$$

$$h'=\sum_{i=0}^{n-k}\overline{c_i}x^i$$

对比等式常数项可得：$\overline{b_0}\overline{c_0}=\bar{0}$. 由于 P 是唯一因子分解整环 R 的素理想，所以 R/P 是整环，于是必有 $\overline{b_0}$ 或 $\overline{c_0}$ 是 $\bar{0}$，即 b_0 或 c_0 是 P 中的元素. 如果两者都是 P 中的元素，则 $a_0=b_0c_0\in P^2$，矛盾！所以不妨设 $b_0\in P,c_0\notin P$.

继续对比一次项可得：$\overline{b_1}\overline{c_0}+\overline{b_0}\overline{c_1}=\bar{0}$，由于 $b_0\in P$，所以 $\overline{b_0}\overline{c_1}=\bar{0}$，即 $\overline{b_1}\overline{c_0}=\bar{0}$. 由于 $c_0\notin P$，所以 $b_1\in P$. 以此类推可以得到每个 $b_i\in P$，于是 $a_n=b_kc_{n-k}\in P$，矛盾！

综上，f 不可约.

笔记 我们将其利用在 $\mathbb{Z}[x]$ 上，即可得到更为常用的形式：

p 是 $\mathbb{Z}$ 的素数，$f(x)=\sum_{i=0}^{n}a_ix^i$ 是 $\mathbb{Z}[x]$ 中的本原多项式（$n\geqslant 1$，请读者思考为什么这里要有本原这个条件）. 若 $p\nmid a_n$，$a_{n-1},\cdots,a_0$ 均整除 p，且 $p^2\nmid a_0$，则 $f(x)$ 在 $\mathbb{Z}[x]$ 内不可约.

3.4.4 典型例题

练习 3.23 证明：$f=x^4+1$ 在 $\mathbb{Z}[x]$ 上不可约.

注 本题是利用 Eisenstein 判别法的经典问题，处理手法是换元法. 我们很容易证明：在给定的环 $R[x]$ 上，$f(x)$ 和 $f(x+1)$ 的可约性相同. 类似的，$f(x)$ 和 $f(x+c),c\in R$ 的可约性也是相同的. 读者可以把此题的处理手法，作为利用 Eisenstein 判别法的典型手法之一积累下来.

证明 若 $f(x)$ 在 $\mathbb{Z}[x]$ 上可约，则 $f(x+1)$ 也在 $\mathbb{Z}[x]$ 上可约. 而

$$f(x+)=(x+1)^4+1=x^4+4x^3+6x^2+4x+2$$

由于首项系数不是素数 2 的倍数，其他各项系数都是 2 的倍数，常数项不是 2^2 的倍数，所以根据 Eisenstein 判别法可得，$f(x+1)$ 在 $\mathbb{Z}[x]$ 上不可约，矛盾！

从而 $f(x)$ 在 $\mathbb{Z}[x]$ 上不可约.

3.4.5 习题

练习 3.24 设 α 是 $\mathbb{Z}[x]$ 中某个首一多项式的有理数解. 证明：α 是整数.

解 设 $\alpha=\dfrac{r}{s}$，由于其为首一多项式的解，于是必有 $s|1$，从而 $s=1$，即 $\alpha=r\in\mathbb{Z}$.

练习 3.25 确定以下多项式在给定环中是否可约. 若可约，则将其分解为不可约因子的积；若不可约，说明理由.

1. $f=x^2+x+1\in\mathbb{Z}_2[x]$;

2. $f=x^3+x+1\in\mathbb{Z}_3[x]$;
3. $f=x^4+1\in\mathbb{Z}_5[x]$;
4. $f=x^4+10x^2+1\in\mathbb{Z}[x]$.

证明

1. 若 f 可约，其真因子只能为一次因式 $x-a,a\in\mathbb{Z}_2[x]$. 而
$$f(0)=f(1)=1$$
从而 f 不可能有一次因子，矛盾！所以 f 不可约.
2. 若 f 可约，其真因子至少有一个一次因式 $x-a,a\in\mathbb{Z}_3[x]$. 因为 $f(0)=1,f(1)=0,f(2)=2$，所以 $x-1$ 为 f 唯一的一次因式，做带余除法可得：
$$x^3+x+1=(x-1)(x^2+x+2)$$
进一步考虑 $g:=x^2+x+2$ 的可约性. 若其可约，则因式也只能为一次因式 $x-a,a\in\mathbb{Z}_3[x]$，然而 $g(0)=2,g(1)=1,g(2)=2$，均不为零，所以 g 没有一次因式，即不可约.
综上，f 的因子分解为
$$x^3+x+1=(x-1)(x^2+x+2)$$
3. 注意到 $1=-4$，所以
$$\begin{aligned}x^4+1&=(x^2)^2-2^2\\&=(x^2+2)(x^2-2)\end{aligned}$$
而 x^2+2,x^2-2 均为不可约多项式（请读者利用前两小问的思路证明这一点），所以上式即为最终分解结果.
4. 首先，如果 f 有一次因式 $x-c\in\mathbb{Z}[x]$，则 c 为 f 的整数根. f 的整数根只可能为 ±1，然而经过验证他们均不是 f 的根，所以 f 不存在一次因式，从而也就不存在三次因式. 因此，假如 f 可约，f 只能为两个二次因式的乘积，不妨设 $f=pq$. 又因为 f 的首项是 1，所以 p,q 的首项也只能为 1.（均为 -1 亦可，但是这时候我们可取 $-p$ 与 $-q$，首项系数仍然为 1）
设 $p=x^2+ax+b,q=x^2+cx+d$，于是：
$$\begin{aligned}x^4+10x^2+1&=(x^2+ax+b)(x^2+cx+d)\\&=x^4+(a+c)x^3+(ac+b+d)x^2+(ad+bc)x+bd\end{aligned}$$
首先对比三次项和常数项的系数可得：$a=-c$ 且 b,d 同时等于 1 或 -1. 而不论哪一种情况，对比二次项系数有 $-a^2\pm2=10$，即 $-a^2=8,12$，而这是不可能的.
综上，x^4+10x^2+1 在 $\mathbb{Z}[x]$ 内不可约.

✍ **练习 3.26** 证明下列各式在 $\mathbb{Z}[x]$ 内不可约：

1. $f=x^4-4x^3+6$;
2. $f=x^6+30x^5-15x^3+6x-120$;
3. $f=x^4+4x^3+6x^2+2x+1$;
4. $f=\frac{(x+2)^p-2^p}{x}$，其中 p 为奇素数.

注 提示：四小问均使用 Eisenstein 判别法：

1. 第一小问，取素数 2;
2. 第二小问，取素数 3;
3. 第三小问，考虑 $f(x-1)=x^4-2x+2$，取素数 2;
4. 第四小问，取素数 p.

✍ **练习 3.27*** 证明：对任意的正整数 n，多项式 $f=(x-1)\cdots(x-n)-1$ 在 $\mathbb{Z}[x]$ 内不可约.

证明 ？

✍ **练习 3.28*** 证明：对任意不等于 4 的正整数 n，多项式 $f=(x-1)\cdots(x-n)+1$ 在 $\mathbb{Z}[x]$ 内不可约.

证明 ？

✍ **练习 3.29**

1. 试给出 $\mathbb{Z}_2[x]$ 中所有次数不超过 4 的不可约首一多项式；
2. 试给出 $\mathbb{Z}_3[x]$ 中所有次数不超过 3 的不可约首一多项式；

解

1. $\mathbb{Z}_2[x]$ 中次数不超过 3 的不可约首一多项式有：

$$\begin{aligned}1\\ x\\ x{+}1\\ x^2+x{+}1\\ x^3+x{+}1\\ x^3+x^2{+}1\\ x^4+x{+}1\\ x^4+x^3{+}1\\ x^4+x^3+x^2+x{+}1\end{aligned}$$

2. $\mathbb{Z}_3[x]$ 中次数不超过 3 的不可约首一多项式有：

$$\begin{aligned}1\\ x\\ x{+}1\\ x{+}2\\ x^2{+}1\\ x^2+x{+}2\\ x^2+2x{+}2\\ x^3+2x{+}1\\ x^3+2x{+}2\\ x^3+x^2{+}2\\ x^3+x^2+x{+}2\\ x^3+x^2+2x{+}1\\ x^3+2x^2{+}1\\ x^3+2x^2+x{+}1\\ x^3+2x^2+2x{+}2\end{aligned}$$

✍ **练习 3.30** 证明：$f=x^2-\sqrt{2}$ 在 $\mathbb{Z}[\sqrt{2}]$ 内不可约.

证明 若 f 在 $\mathbb{Z}[\sqrt{2}]$ 内可约，由于 f 首一，所以不是单位的常数不可能为 f 的真因子，从而 f 的因子只能为一次因式 $x-c, c\in\mathbb{Z}[\sqrt{2}]$. 由因式定理可得 $f(c)=0$. 设 $c=m+n\sqrt{2}$，其中 $m,n\in\mathbb{Z}$，则有：

$$\begin{aligned}0&=(m+n\sqrt{2})^2-\sqrt{2}\\ &=(m^2+2n^2)+(2mn-1)\sqrt{2}\end{aligned}$$

于是必有 $m^2+2n^2=0$，即 $m=n=0$，而由此可得 $c=0$，从而 $0=f(c)=-\sqrt{2}$，矛盾！故 $f=x^2-\sqrt{2}$ 在

$\mathbb{Z}[\sqrt{2}]$ 内不可约.

✍ **练习 3.31** 证明：$f = x^{n-1} + x^{n-2} + \cdots + x + 1 \in \mathbb{Z}[x]$ 不可约，当且仅当 n 是素数.

证明 一方面，当 n 不是素数时，记 $n = pq$，其中 $p, q > 0$ 均不为 1，则 f 可以分解为

$$f = (1 + x + \cdots + x^{p-1})(1 + x^p + x^{(q-1)p})$$

另一方面，当 n 是素数时，我们来求 $f(x+1)$. 注意到 $(x-1)f(x) = x^n - 1$，所以有

$$(x + 1 - 1)f(x + 1) = (x + 1)^n - 1$$

即

$$f(x + 1) = \frac{(x + 1)^n - 1}{x}$$

考虑 $f(x+1)$ 的各项系数，首项系数为 1，其余各项系数均为素数 p 的倍数（由组合数的性质可以得知），而常数项 n 不是 n^2 的倍数，所以由 Eisenstein 判别法可知，$f(x+1)$ 不可约，即 $f(x)$ 不可约.

综上，n 不是素数，当且仅当 f 可约. 取逆否即得待证命题.

✍ **练习 3.32** 证明：当 $n \neq -1, 3, 5$ 时，$f(x) = x^3 - nx + 2 \in \mathbb{Z}[x]$ 不可约.

解 假设 $f(x)$ 可约，由于 $f(x)$ 为 3 次多项式，因此其只能分解为三个一次式的乘积，或一个一次式与一个二次式的乘积. 不论哪一种情形，$f(x)$ 都必然存在一个一次因式，不妨设为 $x - r$，于是 $r \in \mathbb{Z}$ 为 $f(x)$ 的根. 从而 $r|2$. 从而 $r = \pm 1, \pm 2$.

当 $r = 1$ 时，$0 = f(1) = 3 - n$，即 $n = 3$，此时 $f(x) = (x-1)^2(x+2)$.

当 $r = -1$ 时，$0 = f(-1) = 1 + n$，即 $n = -1$，此时 $f(x) = (x+1)(x^2 - x + 2)$.

当 $r = 2$ 时，$0 = f(2) = 10 - 2n$，即 $n = 5$，此时 $f(x) = (x-2)(x^2 + 2x - 1)$.

当 $r = -2$ 时，$0 = f(-2) = -6 + 2n$，即 $n = 3$，此时 $f(x) = (x-1)^2(x+2)$.

综上，$f(x)$ 可约当且仅当 $n = -1, 3, 5$. 取逆否命题即可.

✍ **练习 3.33** 在给定系数环中分解多项式 $f = x^8 - 1$ 和 $g = x^6 - 1$：

1. $\mathbb{Z}$；
2. $\mathbb{Z}_2$；
3. $\mathbb{Z}_3$.

注 提示：$x^4 + 1$ 在 $\mathbb{Z}_3[x]$ 内是可约的，我们容易判断它没有一次因式，所以假如可约也只能是两个二次因式，利用待定系数法即可求出结果.

解

$$f = (x^4 + 1)(x^2 + 1)(x + 1)(x - 1) \qquad \in \mathbb{Z}[x]$$
$$f = (x + 1)^8 \qquad \in \mathbb{Z}_2[x]$$
$$f = (x^2 + 2x + 2)(x^2 + x + 2)(x^2 + 1)(x + 2)(x + 1) \qquad \in \mathbb{Z}_3[x]$$

$$g = (x^2 + x + 1)(x^2 - x + 1)(x + 1)(x - 1) \qquad \in \mathbb{Z}[x]$$
$$g = (x^2 + x + 1)^2(x + 1)^2 \qquad \in \mathbb{Z}_2[x]$$
$$g = (x + 2)^3(x + 1)^3 \qquad \in \mathbb{Z}_3[x]$$

✍ **练习 3.34** 证明下列各式在 $\mathbb{Q}[x]$ 内不可约：

1. $f = 6x^5 + 14x^3 - 21x + 35$；
2. $f = 18x^5 - 30x^2 + 120x + 360$.

证明

1. 因为 f 在 $\mathbb{Z}[x]$ 中本原，所以 f 在 $\mathbb{Z}[x]$ 内的可约性等价于在 $\mathbb{Q}[x]$ 内的等价性. 由 Eisenstein 判别法可知，f 在 $\mathbb{Z}[x]$ 内不可约（考虑素数 7），从而 f 在 $\mathbb{Q}[x]$ 内不可约.
2. 在 $\mathbb{Q}[x]$ 中，$f \sim f' := 3x^5 - 5x^2 + 20x + 60$. 与前一小题类似地，由于 f' 在 $\mathbb{Z}[x]$ 内不可约（考虑素数 5），所以 f' 在 $\mathbb{Q}[x]$ 内不可约，从而 f 在 $\mathbb{Q}[x]$ 内不可约.

3.5 多元多项式环

3.5.1 知识要点

1. 多重指标记号：记多重指标 $\alpha := (\alpha_1, \cdots, \alpha_n)$，其加法为分量加法. 未定元 $x := (x_1, \cdots, x_n)$，$x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.
2. R 上关于 $x_1, \cdots, x_n$ 的 n 元多项式：f 为形式和
$$f(x_1, \cdots, x_n) = \sum_{\alpha=0}^{\infty} a_\alpha x^\alpha$$
其中除有限项外所有的 a_α 均为 0.
3. 多项式的加法和乘法运算：设 f, g 为 R 上的两个关于 $x = (x_1, \cdots, x_n)$ 的多项式
$$f = \sum_{\alpha=0}^{\infty} a_\alpha x^\alpha$$
$$g = \sum_{\alpha=0}^{\infty} b_\alpha x^\alpha$$
则定义
$$f + g = \sum_{\alpha=0}^{\infty} (a_\alpha + b_\alpha) x^\alpha$$
$$fg = \sum_{\alpha=0}^{\infty} \left(\sum_{\beta+\gamma=\alpha} a_\beta b_\gamma \right) x^\alpha$$
4. 单项式：形如 $g = x^\alpha$ 的多项式，其次数定义为
$$\deg g := |\alpha| := \sum_{i=1}^{n} \alpha_i$$
5. 多项式的次数：$\deg f$ 定义为它的每个单项式的次数的最大值.
6. 齐次多项式：多项式的所有单项的次数相同.
7. R 上关于 $x_1, \cdots, x_n$ 的 n 元多项式环：R 上的关于 $x_1, \cdots, x_n$ 的全体多项式的集合（记为 $R[x_1, \cdots, x_n]$），连同多项式的加法和乘法构成交换环.
注：也可以归纳定义为
$$R[x_1, \cdots, x_n] = R[x_1, \cdots, x_{n-1}][x_n]$$
8. （唯一因子分解整环）：设 R 是唯一因子分解整环，则 $R[x_1, \cdots, x_n]$ 也是唯一因子分解整环.

3.5.2 习题

✍ **练习 3.35** 设 $x_1, \cdots, x_n$ 是不同的未定元. 证明：对任意 $\pi \in S_n$，都有
$$R[x_{\pi(1)}, x_{\pi(2)}, \cdots, x_{\pi(n)}] \simeq R[x_1, \cdots, x_n]$$

注 提示：考虑映射

$$\varphi : R[x_1, \cdots, x_n] \to R[x_{\pi(1)}, x_{\pi(2)}, \cdots, x_{\pi(n)}]$$
$$f(x_1, \cdots, x_n) \mapsto f(x_{\pi(1)}, \cdots, x_{\pi(n)}).$$

✍ **练习 3.36** 证明：

1. 理想 (x, y) 是 $\mathbb{Q}[x, y]$ 的极大理想；
2. 理想 (x) 是 $\mathbb{Q}[x, y]$ 的素理想，但不是极大理想.

注 提示：$\mathbb{Q}[x, y]/(x, y) \simeq \mathbb{Q}$ 是域，所以 (x, y) 是极大理想；而 $\mathbb{Q}[x, y]/(x) \simeq \mathbb{Q}[y]$ 是欧几里得整环，不是域，所以 (x) 只能是素理想.

✍ **练习 3.37** 证明：

1. 理想 $(x, y, 2)$ 是 $\mathbb{Z}[x, y]$ 的极大理想；
2. 理想 (x, y) 是 $\mathbb{Z}[x, y]$ 的素理想，但不是极大理想.

注 提示：$\mathbb{Z}[x, y]/(x, y, 2) \simeq \mathbb{Z}_2$ 是域；而 $\mathbb{Z}[x, y]/(x, y) \simeq \mathbb{Z}$ 是欧几里得整环.

✍ **练习 3.38** 设 F 是域，$R = F[x, x^2y, x^3y^2, \cdots, x^ny^{n-1}, \cdots]$. 证明：

1. R 的分式域和 $F[x, y]$ 的分式域相同；
2. R 存在一个不可有限生成的理想.

证明

1. 一方面，$R \subset F[x, y]$，于是 $R \subset \mathrm{Frac}(F[x, y])$，利用分式域的极小性可得 $\mathrm{Frac}(R) \subset \mathrm{Frac}(F[x, y])$. 以下只需证：$\mathrm{Frac}(F[x, y]) \subset \mathrm{Frac}(R)$.
   注意到 $F \subset \mathrm{Frac}(R)$，$x \in \mathrm{Frac}(R)$ 且 $y = x^2y/(x^2) \in \mathrm{Frac}(R)$，于是 $F[x, y] \subset \mathrm{Frac}(R)$，从而利用分式域的极小性可得 $\mathrm{Frac}(F[x, y]) \subset \mathrm{Frac}(R)$.
2. 先证明：对任意 $n \in \mathbb{Z}_+$ 有 $x^{n+1}y^n \notin F[x, x^2y, \cdots, x^ny^{n-1}]$. 由 x 的次数和系数关系，假设 $x^{n+1}y^n \in F[x, x^2y, \cdots, x^ny^{n-1}]$，则其只能由若干个集合 $A = \{x, x^2y, \cdots, x^ny^{n-1}\}$ 中的单项式相乘而得. 再考虑 x 和 y 的次数差，$x^{n+1}y^n$ 为 1，集合 A 中每个单项式也都为 1，若有 n 个 A 中的元素相乘，则 x 和 y 的次数差就为 n. 所以要使 $x^{n+1}y^n$ 为若干个 A 中元素的乘积，就只能有 $n = 1$，即 $x^{n+1}y^n \in A$，这显然是错误的.
   所以，R 作为 R 的理想是不可有限生成的.

✍ **练习 3.39** 设 F 是域，证明：环 $F[x, y]/(y^2 - x)$ 和环 $F[x, y]/(y^2 - x^2)$ 不同构.

注 提示：$F[x, y]/(y^2 - x)$ 至少为整环，而 $F[x, y]/(y^2 - x^2)$ 显然有零因子 $\overline{y - x}$.

✍ **练习 3.40*** 设 R 是整环，i, j 是互素的整数，证明：理想 $(x^i - y^j)$ 是 $R[x, y]$ 的素理想.

证明 定义映射：

$$\varphi : R[x, y] \to R[t]$$

对应规则为：

$$\varphi|_R = id.$$
$$x \mapsto t^j$$
$$y \mapsto t^i$$

1. 证明：φ 是环同态.【证明留给读者】
2. 证明：φ 是满射. 因为 i, j 是互素的，所以由 Bézout 定理可知，存在整数 k, l，使得 $ki + lj = 1$，从而
$$\varphi(x^l y^k) = t^{lj+ki} = t$$
于是对于任意的 $f(t) \in R[t]$，都有 $\varphi(f(x^l y^k)) = f(t)$.
3. 证明：$\ker\varphi = (x^i - y^j)$. 一方面，$\varphi(x^i - y^j) = 0$，所以 $(x^i - y^j) \subset \ker\varphi$. 另一方面，对任意的 $f(x, y) \in \ker\varphi$，有 (...) ？

4. 由前面的结论可得环同构：

$$R[x,y]/(x^i-y^j)\simeq R[t]$$

因为 R 是整环，所以 $R[t]$ 是整环，从而 (x^i-y^j) 是素理想.

✍ **练习 3.41** 设 $p(x_1,x_2,\cdots,x_n)\in R[x_1,x_2,\cdots,x_n]$ 是 k 次齐次多项式. 证明：对任意的 $\lambda\in R$，有

$$p(\lambda x_1,\lambda x_2,\cdots,\lambda x_n)=\lambda^k p(x_1,x_2,\cdots,x_n)$$

✍ **练习 3.42** 证明：两个齐次多项式的乘积还是齐次多项式.

✍ **练习 3.43*** 设 R 是任意环（不一定交换），$\mathrm{Func}(R)$ 是 R 到自身的映射构成的环. 若 $p(x)\in R[x]$ 是多项式，定义 $f_p\in\mathrm{Func}(R), f_p(r)=p(r)$.

1. 对于固定的 $a\in R$，证明：映射

$$\begin{aligned}\varphi:&\mathrm{Func}(R)\to R\\ &f_p\mapsto f_p(a)\end{aligned}$$

是环同态.

2. 定义映射

$$\begin{aligned}\psi:R[x]&\to\mathrm{Func}(R)\\ p&\mapsto f_p\end{aligned}$$

证明：ψ 一般不是环同态.

3. 对于固定的 $a\in R$，证明：

$$\begin{aligned}\varphi\circ\psi:R[x]&\to R\\ p&\mapsto f_p(a)\end{aligned}$$

是环同态，当且仅当 $a\in Z(R)$.

✍ **练习 3.44*** 证明：环 $\mathbb{Z}[x_1,x_2,\cdots]/(x_1x_2,x_3x_4,\cdots)$ 包含无穷多个素理想.

证明 ？

第 4 章 域论

4.1 域的基本概念

4.1.1 课前思考

判断下列命题的正误，并说明理由：

1. 环 $\mathbb{Z}_n$（其中 $n \geqslant 2$ 为正整数）的特征是 n.
2. 存在特征为 6 的整环.
3. 存在 $\mathbb{Z}_8$ 到 $\mathbb{Z}_{13}$ 的非平凡环同态.
4. 在 $\mathbb{Z}_3$ 中，对任意的元素 a, b，有 $(a+b)^9 = a^9 + b^9$.

解

1. T：$\bar{1}$ 必须乘 n 才可得 $\bar{0}$，且任意元素乘 n 都得 $\bar{0}$.
2. F：整环的特征只能是 0 和素数.
3. F：不存在 $\mathbb{Z}_8$ 到 $\mathbb{Z}_{13}$ 的非平凡群同态，从而也不能存在环同态.
4. T：$(a+b)^9 = ((a+b)^3)^3 = (a^3+b^3)^3 = a^9 + b^9$.

4.1.2 知识要点

（一）域和域同态的基本概念

1. 域 $(F, +, \cdot)$：$(F, +, \cdot)$ 是个交换环，且 F 的每个非零元素都是单位.
2. $(F, +, \cdot)$，$(F', +, \cdot)$ 是两个域，域同态 $f : F \to F'$：f 是个环同态.
3. （域到环的同态）：若 $f : F \to R$ 是个环同态，其中 F 是个域，$R \neq \{0\}$，且 $f \neq 0$，则 f 是个单射.
   特别的，域同态一定是单射.（我们也称单同态为嵌入）
4. 域 F 的子域 E：$E \subset F$，且 E 在与 F 相同的运算下为域.
5. 由 $A \subset F$ 生成的子域：F 中包含 A 的最小的子域，即 $(A) = \bigcap_{A \subset E < F} E$（记作 (A)）.

（二）环的特征

1. 环 R 的特征：最小的正整数 n，满足 $n \cdot 1 = 1 + \cdots + 1 = 0$（$n$ 个 1 相加），记作 $\mathrm{char}(R)$.
   若不存在这样的正整数，定义 $\mathrm{char}(R) = 0$.
2. （环的“特征”同态）：设 R 是环，定义映射 $\varphi : \mathbb{Z} \to R, k \mapsto k \cdot 1$，则 φ 是环同态，且
   (a). 若 $\mathrm{char}(R) = 0$，则 φ 是嵌入同态（即单同态）；
   (b). 若 $\mathrm{char}(R) = n \in \mathbb{Z}_+$，则 $\ker \varphi = n\mathbb{Z}$.
3. （整环的特征）：整环 R 的特征只能为素数或 0.

（三）域的特征

1. 域 F 的素子域：由 1 生成的子域.
2. （素子域的结构）：F 的素子域同构于 $\mathbb{Q}$（若 $\mathrm{char}(F) = 0$）或 $\mathbb{Z}_p$（若 $\mathrm{char}(F) = p$）.
3. （域的“特征”同态）：设 F 是域：
   (a). 若 $\mathrm{char}(F) = 0$，则 $\varphi : \mathbb{Q} \to F, a/b \mapsto (a \cdot 1)(b \cdot 1)^{-1}$ 是嵌入映射；
   (b). 若 $\mathrm{char}(F) = p \in \mathbb{Z}_+$，则 $\varphi : \mathbb{Z}_p \to F, a \mapsto a \cdot 1$，是嵌入映射.
4. （Frobenius 自同态）：设域 F 的特征为 p，则映射 $f : F \to F$, $a \mapsto a^p$ 为 F 的自同态.（称 f 为 F 的 Frobenius 自同态）

特别的，对任意的 $a,b\in F$，有 $(a+b)^p=a^p+b^p$.

5. (元素的特征次方根)：设有限域 F 的特征为 p，则 F 中的每个元素，都是 F 中某个元素的 p 次幂.（也就是 $F=F^p$）

4.1.3 知识要点解读

（一）域到环的同态

我们在学习群和环的时候，都是沿着“从大到小、由此及彼”的路线来展开的. 也就是说，我们先学习子结构（子群、子环），然后学习商结构与对应的特殊子集（商群与正规子群、商环与理想），最后学习同态与同构定理. 但是域的学习路线并不是如此，因为这些内容在域上会变得非常简单. 比如，域的理想只有自己和 (0)，对应的“商域”也变得非常简单. 又比如在环中研究的因子分解问题，在域中没有意义，因为所有非零元都是单位，不需要分解. 域同态也非常简单，只有零同态、单射（嵌入）和同构三种情况.

问题 4.1 (域到环的同态)：若 $f:F\to R$ 是个环同态，其中 F 是个域，$R\neq\{0\}$，且 $f\neq 0$，则 f 是个单射.

证明 假设 $\ker f\neq\{0\}$. 取非零的 $a\in\ker f$，从而 $a^{-1}\in\ker f$，于是 $1=aa^{-1}\in\ker f$，即 $f(1)=0'$.
由于 $R\neq\{0\}$，且 $f\neq 0$，于是 $\mathrm{im}f\neq\{0\}$，从而象集中 $1'\neq 0'$. 由环同态的性质可知 $f(1)=1'$. 矛盾！
从而 $\ker f$ 只能为零环，即 f 为单射.

如前所述，先前的学习路径已经很难再学到域的性质，所以域论部分将采用“从小到大”的路线进行，即给定一个域，再加入某些额外的元素，我们想办法构造新的域. 请读者一定注意这种学习思路上的转换.

（二）环的特征

环的特征本质上是环的乘法幺元的加法特性，即寻找满足 $n\cdot 1=0$ 的最小的正整数 n. 由此我们构造出环中的一个子环.

问题 4.2 (环的“特征”同态)：设 R 是环，定义映射 $\varphi:\mathbb{Z}\to R,k\mapsto k\cdot 1$，则 φ 是环同态，且

1. 若 $\mathrm{char}(R)=0$，则 φ 是嵌入同态（即单同态）；
2. 若 $\mathrm{char}(R)=n\in\mathbb{Z}_+$，则 $\ker\varphi=n\mathbb{Z}$.

证明

1. 先证明：φ 是环同态.
首先，对任意的 $m,n\in\mathbb{Z}$，有：
$$\begin{aligned}\varphi(m+n)&=(m+n)\cdot 1\\&=m\cdot 1+n\cdot 1\\&=\varphi(m)+\varphi(n)\end{aligned}$$
其次，对任意的 $m,n\in\mathbb{Z}$，有：
$$\begin{aligned}\varphi(mn)&=(mn)\cdot 1\\&=(m\cdot 1)(n\cdot 1)\\&=\varphi(m)\varphi(n)\end{aligned}$$
最后：
$$\varphi(1)=1\cdot 1=1$$
综上，φ 是环同态.
2. 再证明：若 $\mathrm{char}(R)=0$，则 φ 是单同态.

若 $\mathrm{char}(R)=0$，则：

$$\begin{aligned}\ker\varphi &:= \{n\in\mathbb{Z} : n\cdot 1=0\}\\ &= \{0\}\end{aligned}$$

从而 φ 是单同态.

3. 最后证明：若 $\mathrm{char}(R)=n\in\mathbb{Z}_+$，则 $\ker\varphi=n\mathbb{Z}$.

若 $\mathrm{char}(R)=n\in\mathbb{Z}_+$，则：

$$\begin{aligned}\ker\varphi &:= \{n\in\mathbb{Z} : n\cdot 1=0\}\\ &= n\mathbb{Z}.\end{aligned}$$

笔记 如果环 R 的特征为零，则 R 中包含一个同构于 $\mathbb{Z}$ 的子环；而若 R 的特征为 n，则 R 中包含一个同构于 $\mathbb{Z}_n$ 的子环.

问题 4.3 （整环的特征）：整环 R 的特征只能为素数或 0.

证明 设 R 的特征为正整数 k，考虑映射 $\varphi:\mathbb{Z}\to R, k\mapsto k\cdot 1$，其核为 $k\mathbb{Z}$，于是由第一同构定理可得 $\mathbb{Z}_k$ 同构于 R 的某个子环. 由于 R 是整环，所以没有零因子，从而 $\mathbb{Z}_k$ 中也没有零因子，于是 k 只能为素数.

另一方面，特征为零的整环存在，例如 $\mathbb{Z}$，所以整环的特征只能为素数或 0.

笔记 这一性质非常重要，不过一般我们并不在整环中使用这一性质，而是在域中使用.

（三）域的特征

前一节我们已经知道，整环的特征是零或素数. 从而域的特征也是如此. 同时域又是交换的，从而我们能够在域上定义一个自同态.

问题 4.4 （Frobenius 自同态）：设域 F 的特征为 p，则映射 $f:F\to F, a\mapsto a^p$ 为 F 的自同态.

特别的，对任意的 $a,b\in F$，有 $(a+b)^p=a^p+b^p$.

证明

1. 证明：在任意交换环 R 上，对任意的 $a,b\in R$ 和 $n\in\mathbb{Z}_+$，有二项展开式：

$$(a+b)^n=\sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i.$$

其中二项式系数为

$$\binom{n}{i}:=\frac{n!}{i!(n-i)!}.$$

当 $n=1$ 时，$a+b=a+b$. 原命题成立.

假设 $n=k$ 时原命题成立，当 $n=k+1$ 时：

$$\begin{aligned}(a+b)^{k+1} &= (a+b)(a+b)^k \\ &= (a+b)\sum_{i=0}^{k}\binom{k}{i}a^{k-i}b^i \\ &= \sum_{i=0}^{k}\binom{k}{i}a^{k+1-i}b^i + \sum_{i=0}^{k}\binom{k}{i}a^{k-i}b^{i+1} \\ &= a^{k+1} + \sum_{i=1}^{k}\binom{k}{i}a^{k+1-i}b^i + \sum_{i=0}^{k-1}\binom{k}{i}a^{k-i}b^{i+1} + b^{k+1} \\ &= a^{k+1} + \sum_{i=1}^{k}\binom{k}{i}a^{k+1-i}b^i + \sum_{i=1}^{k}\binom{k}{i-1}a^{k+1-i}b^i + b^{k+1} \\ &= a^{k+1} + \sum_{i=1}^{k}\left(\binom{k}{i} + \binom{k}{i-1}\right)a^{k+1-i}b^i + b^{k+1} \\ &= a^{k+1} + \sum_{i=1}^{k}\binom{k+1}{i}a^{k+1-i}b^i + b^{k+1} \\ &= \sum_{i=0}^{k+1}\binom{k+1}{i}a^{k+1-i}b^i\end{aligned}$$

原命题成立.

综上，命题成立.

2. 证明：对任意的 $a,b\in F$，有 $f(a+b)=f(a)+f(b)$，即 $(a+b)^p=a^p+b^p$.

   只需证明，在整数环 $\mathbb{Z}$ 中，对任意的 $i\in\{1,2,\cdots,p-1\}$，$\binom{p}{i}$ 是 p 的倍数.

   显然，二项式系数

   $$\binom{p}{i}=\frac{p!}{i!(p-i)!}.$$

   为整数. 分子中有因子 p，而分母 $i!(p-i)!$ 中没有超过 p 的素因子，所以因子 p 不会被约去，即 $\binom{p}{i}$ 是 p 的倍数.

   回到域 F 中，由于 $\operatorname{char}F=p$，所以对任意的 $i\in\{1,2,\cdots,p-1\}$，$\binom{p}{i}=0$，从而 $(a+b)^p=a^p+b^p$.

3. 证明：对任意的 $a,b\in F$，有 $f(ab)=f(a)f(b)$，即 $(ab)^p=a^pb^p$. 由于域 F 是交换环，所以 $(ab)^p=a^pb^p$ 显然成立.

4. 证明：$f(1)=1$. 我们有 $f(1)=1^p=1$.

综上，f 是 F 的自同态.

笔记 Frobenius 自同态中最常用的就是其保持加法的性质，即 $(a+b)^p=a^p+b^p$.

问题 4.5（元素的特征次方根）：设有限域 F 的特征为 p，则 F 中的每个元素，都是 F 中某个元素的 p 次幂.

证明 考虑 F 的 Frobenius 自同态 f. 由于 f 不是零映射，所以 f 是单射. 又因为 F 是有限域，所以 $|f(F)|=|F|$，而 $f(F)\subset F$，从而必有 $f(F)=F$，即 f 是满射. 从而，对任意的 $u\in F=f(F)$，存在 $v\in F$，使得 $v^p=u$.

4.1.4 习题

练习 4.1 设环 R 的特征为 n，证明：对任意的 $r\in R$，$n\cdot r=0$.

证明 我们有

$$\begin{aligned} n \cdot r &= n \cdot (1r) \\ &= (n \cdot 1)r \\ &= 0r \\ &= 0 \end{aligned}$$

✍ **练习 4.2** 求下列环的特征：

1. $\mathbb{Z}$;
2. $\mathbb{Z}_n$;
3. $\mathbb{Q}$;
4. $\mathbb{Z}[x]$;
5. $\mathbb{Z}_n[x]$.

解

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{Z}[x]$ 的特征为 0，因为对任意的正整数 n，$n \cdot 1 = n \neq 0$.
2. $\mathbb{Z}_n, \mathbb{Z}_n[x]$ 的特征为 n. 一方面，$n \cdot \bar{1} = \bar{n} = \bar{0}$. 另一方面，对任意的正整数 $m < n$，$m \cdot \bar{1} = \bar{m} \neq \bar{0}$.

✍ **练习 4.3** 证明：非零 Bool 环的特征为 2.

注 提示：布尔环中的任意元素 x 有性质：$x + x = 0$.

4.2 域的扩张

注：如无特殊声明，本节均设 F/K 是扩域.

4.2.1 课前思考

判断下列命题的正误，并说明理由：

1. 有限生成扩张一定是有限扩张.
2. 有限扩张一定是代数扩张.
3. 若 $p(x) \in K[x]$ 有一根为 $a \in F$，则 $K(a) \simeq K[x]/(p(x))$.
4. 若 a 是 K 上的代数元素，则有 $K[a] = K(a)$.
5. 未定元 x 是 K 上的超越元素.

解

1. F：$\mathbb{Q}(\pi)/\mathbb{Q}$ 是有限生成扩张，也是无限扩张（因为 π 是 $\mathbb{Q}$ 上的超越数）;
2. T;
3. F：$p(x)$ 不可约时命题才成立;
4. T;
5. T：因为 $K[x]$ 中没有以 x 为根的多项式.

4.2.2 知识要点

（一）作为向量空间的扩域

1. K，F 是两个域. F/K 是个域扩张（或 F 是 K 的扩域）：K 是 F 的子域.
2. （向量空间）：若 F/K 是个域扩张，则 F 是 K 上的向量空间.
3. 域扩张 F/K 的维数（或扩张次数）：K 上的线性空间 F 的维数.（$\dim_K F$，或记作 $[F : K]$. ）
   有限扩张：$[F : K] < \infty$.

无限扩张：$[F:K]=\infty$.

（二）域的生成

1. 生成：设 F/K 是域扩张，S 是 F 的子集，则 F 中包含 $K\cup S$ 的最小子域被称作 S 在 K 上生成的域，记作 $K(S)$，也就是
$$K(S)=\bigcap_{\substack{(K\cup S)\subset E\\ E\text{是 }F\text{ 的子域}}} E.$$
类似地可以定义 S 在 K 上生成的环 $K[S]$：F 中包含 $K\cup S$ 的最小子环.
2. 有限生成扩张：设 $a_1,\cdots,a_n\in F$，则域 $K(a_1,\cdots,a_n)$ 被称为 K 的有限生成扩张.
单扩张：只有一个生成元的域扩张（例如 $K(a_1)$）.
3. （有限生成扩张的递归 *）：$K(a_1,a_2)=(K(a_1))(a_2)$.
4. （扩域、扩环的显式 *）：设 $u,u_i\in F$，$S\subset F$，x,x_i 均为未定元，则有：
   (a). （扩环）：
$$\begin{aligned}K[u]&=\{f(u):f(x)\in F[x]\}\\ K[u_1,\cdots,u_n]&=\{f(u_1,\cdots,u_n):f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]\}\\ K[S]&=\{f(u_1,\cdots,u_n):f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n],\forall u_i\in S,n\in\mathbb{Z}_+\}\end{aligned}$$
   (b). （扩域）：
$$\begin{aligned}K(u)&=\{(f/g)(u):f,g\in F[x],g(u)\neq 0\}\\ K(u_1,\cdots,u_n)&=\{(f/g)(u_1,\cdots,u_n):f,g\in F[x_1,\cdots,x_n],g(u_1,\cdots,u_n)\neq 0\}\\ K[S]&=\{(f/g)(u_1,\cdots,u_n):f,g\in F[x_1,\cdots,x_n],g(u_1,\cdots,u_n)\neq 0,\forall u_i\in S,n\in\mathbb{Z}_+\}\end{aligned}$$

（三）代数扩张

1. $a\in F$ 是 K 上的代数元素：$K(a)/K$ 是有限扩张.
$a\in F$ 是 K 上的超越元素：$K(a)/K$ 是无限扩张.
2. （代数元素的全体 *）：F 中 K 上的代数元素全体构成 F 的子域.
3. （代数元素、超越元素与多项式的根）：设 $a\in F$.
   (a). a 在 K 上是个代数元素，当且仅当存在某个非零多项式 $p(x)\in K[x]$，使得 $p(a)=0$；
   (b). a 在 K 上是个超越元素，当且仅当对任意非零多项式 $p(x)\in K[x]$，我们都有 $p(a)\neq 0$.
4. 代数扩张 F/K：F/K 为域扩张，且任意 $a\in F$ 都是 K 上的代数元素.
超越扩张 F/K：F/K 为域扩张，且存在至少一个 $a\in F$ 是 K 上的超越元素.
5. （代数扩张的性质）
   (a). （有限生成代数扩张）：F/K 是个有限扩张，当且仅当它既是有限生成扩张，又是代数扩张.
   (b). （代数扩张的传递性）：若 E 为域，且 $F/E,E/K$ 均为代数扩张，则 F/K 也为代数扩张.
   特别的，若 $F/E,E/K$ 均为有限扩张，则 F/K 也为有限扩张，且 $[F:K]=[F:E][E:K]$.
6. （单代数扩张的性质）：F/K 为域扩张，$a\in F$ 为 K 上的代数元素.
   (a). （最小多项式）：存在唯一的首一非零多项式 $p(x)$，使得每个有根为 a 的多项式 $f(x)\in K[x]$，被 $p(x)$ 整除.（称 $p(x)$ 为 a 在域 F 上的最小多项式（或极小多项式），也可以表示为 $m_{a,K}(x)$）.
   从而最小多项式是不可约的，且 $\{f(x)\in K[x]:f(a)=0\}=(p(x))$.
   (b). （$K(a)$ 的结构-商环）：$K[x]/(p(x))\simeq K(a)$
   (c). （$K(a)$ 的结构-线性空间）：若 $\deg p=n$，则 $\{1,a,\cdots,a^{n-1}\}$ 是 $K(a)$ 在 E 上的一组基，即 $K(a)=K[a]$.
7. （同构的单代数扩张）：$\varphi:F\xrightarrow{\sim}F'$ 是一个域同构. $p(x)=\sum_{i=0}^n a_ix^i\in F[x]$ 是一个不可约多项式，且 $p'(x)=\sum_{i=0}^n\varphi(a_i)x^i\in F'[x]$. α 是 $p(x)$ 的一个根 (在 F 的某个扩域中)，β 是 $p'(x)$ 的一个根 (在 F' 的某

个扩域中). 于是存在一个同构:

$$\sigma : F(\alpha) \xrightarrow{\sim} F'(\beta)$$
$$\alpha \mapsto \beta$$

使得 $\sigma|_F = \varphi$.

（四）超越扩张

1. 域 F 上的有理函数域 $F(x)$: 多项式环 $F[x]$ 的分式域，即 $F(x) = \mathrm{Frac}(F[x])$.
   也就是说，任意一个 $r(x) \in F(x)$，都可以在一个显然的等价关系下（形式地）写成
   $$r(x) = \frac{f(x)}{g(x)} \tag{4.1}$$
   其中 $f(x) \in F[x]$，$g(x) \in F[x] - \{0\}$.
2. (单超越扩张的性质): F/K 为域扩张，$a \in F$ 为 K 上的超越元素.
   (a). ($K(a)$ 的结构): $K(a) \simeq K(x)$.
   (b). (无限扩张): $[K(a) : K] = \infty$.

4.2.3 知识要点解读

（一）扩域的结构

利用多项式环和分式环的知识，我们可以显式地表达扩域、扩环的元素. 我们先以单扩张为例，说明这种显式表达的合理性.

问题 4.6 (扩域、扩环的显式): 设 $u \in F$，x 为未定元，则有:

$$K[u] = \{f(u) : f(x) \in F[x]\}$$
$$K(u) = \{(f/g)(u) : f, g \in F[x], g(u) \neq 0\}$$

证明

1. (扩环): 首先，集合 $A := \{f(u) : f(x) \in F[x]\}$ 确实是一个环【笔者: 相信读者此处不需要我再证明这个命题了】，且 A 包含域 K 和元素 u，所以由扩环的定义，$F[u] \subset A$.
   另一方面，对任意的 $f(u) = \sum_{i=0}^{n} a_i u^i \in A$，由 A 的定义，任意 $a_i \in K$. 因为 $u \in K[u]$，则任意 $u^i \in K[u]$，从而任意的 $a_i u^i \in K[u]$，所以 $f(u) \in K[u]$（这里利用的是环对于加法和乘法的封闭性，而多项式中只涉及这两种运算）. 从而 $A \subset K[u]$.
   综上，$K[u] = A = \{f(u) : f(x) \in F[x]\}$.
2. (扩域): 首先，集合 $B := \{(f/g)(u) : f, g \in F[x], g(u) \neq 0\}$ 确实是一个域，且 B 包含域 K 和元素 u，所以由扩域的定义，$F(u) \subset B$.
   另一方面，对任意的
   $$\left(\frac{f}{g}\right)(u) = \frac{\sum_{i=0}^{m} a_i u^i}{\sum_{j=0}^{n} b_j u^j} \in B$$
   由 B 的定义，任意 $a_i, b_j \in K$. 因为 $u \in K(u)$，则任意 $u^i \in K[u]$，从而任意的 $a_i u^i, b_j u^j \in K(u)$，进一步有 $f(u) = \sum a_i u^i, g(u) = \sum b_j u^j \in K(u)$. 由于 $K(u)$ 是域，$g(u) \neq 0$，所以 $g(u)$ 有乘法逆 $g(u)^{-1}$，最终有 $(f/g)(u) = f(u)/g(u) \in K(u)$. 即 $B \subset K(u)$.
   综上，$K(u) = B = \{(f/g)(u) : f, g \in F[x], g(u) \neq 0\}$.

根据这一命题，我们对于扩环和扩域可以有更为直观的理解:

在一个给定的域 K 中，我们拿一个元素 u（一般不是 K 中的元素，否则扩域还是它自己，这个过程就没什么意义了），并且想办法构造一个新的域（而且尽可能小），此时你会怎么做呢? 我们一定是考虑“不得不放进

扩域中”的元素，比如若干个 u 的和、积等等，此时我们可以按运算法则逐条考虑：

首先，扩域对加法封闭，且要有加法逆，于是所有与 u 相关的和以及它们的加法逆，都要放进扩域中. 其次，扩域乘法封闭，且每个非零元素都要有乘法逆，于是所有与 u 相关的积以及它们的乘法逆，都要放进扩域中. 此时我们不由的就会想到以 u 为“变量”的（形式上的）“有理函数” $\sum a_i u^i / \sum b_j u^j$【编者：这种说法不严谨，但是比较形象】. 从而我们构造出了前述问题中呈现的扩域的形式. 扩环的构造也是如此.

这一过程和我们在初中学习的尺规作图有点神似：我们在一些基本图形和基本操作的基础上，作图的范围有多广阔呢？可以做出正十七边形，但是不能三等分角. 前面所述的单扩域我们就可以理解成：给定基本元素集：$K \cup \{u\}$，以及基本的运算：$\{+, -, \cdot, (\,)^{-1}\}$，我们能够构造出的元素全体是 $K(u)$，这是一个域. 在这一观点下，尺规作图也可以理解为是域的扩张，“三等分角、倍立方”等问题可以用扩域的知识研究.

另一方面，我们看到，域 K 上的扩环（或扩域），都在 K 上构造了一个线性空间.

（二）单代数扩张

单代数扩张的结构也是笔者非常喜欢的几个命题之一，尤其是它的证明过程（上一个得到笔者青睐的命题是 Lagrange 定理）. 它的巧妙之处在于，一个形如扩环的结构，本质上却是个扩域. 而且进一步的，它给我们一个重要的启发：即对于一个代数数而言，它是谁不重要，它所对应的最小多项式才是核心. 这里再一次印证了笔者对于代数结构的一个论述：在一个代数结构里，元素本身是什么不重要，它和其他元素的联系才是这个元素的本质内涵.

问题 4.7 （单代数扩张的性质）：F/K 为域扩张，$a \in F$ 为 K 上的代数元素.

1. （最小多项式）：存在唯一的首一非零多项式 $p(x)$，使得每个有根为 a 的多项式 $f(x) \in K[x]$，被 $p(x)$ 整除.（称 $p(x)$ 为 a 在域 F 上的最小多项式（或极小多项式），也可以表示为 $m_{a,K}(x)$）.
   从而最小多项式是不可约的，且 $\{f(x) \in K[x] : f(a) = 0\} = (p(x))$.
2. （$K(a)$ 的结构-商环）：$K[x]/(p(x)) \simeq K(a)$
3. （$K(a)$ 的结构-线性空间）：若 $\deg p = n$，则 $\{1, a, \cdots, a^{n-1}\}$ 是 $K(a)$ 在 K 上的一组基，即 $K(a) = K[a]$.

证明

1. 定义映射：$\varphi : K[x] \to K(a), f \mapsto f(a)$. 很容易证明，$\varphi$ 是一个环同态，从而核为：
$$\ker \varphi := \{f \in K[x] : f(a) = 0\}$$
因为 a 是 K 上的代数元素，所以存在以 a 为一根的非零多项式 $g \in K[x]$，也就是说，$\ker \varphi \neq (0)$. 由于 E 是域，所以 $K[x]$ 是欧几里得整环，也是主理想整环，从而存在 $p \in K[x] - \{0\}$，使得 $\ker \varphi = (q(x))$. 记 $q(x)$ 的首项系数为 $c \in K$，从而可取首一多项式 $p(x) = c^{-1} q(x)$. 由于 c 是单位，所以 $\ker \varphi = (q(x)) = (p(x))$.

   一方面，由 $\ker \varphi$ 的定义，所有有根为 a 的多项式都位列其中，从而都是 $(p(x))$ 的元素，也就都被 p 整除. 另一方面，若 $r(x)$ 也是 a 的最小多项式，由于 $(p(x)) = (r(x))$，所以 $p(x) \sim r(x)$，他们只相差一个单位. 而又因为他们都是首一多项式，所以这个单位只能是 1，从而两者相等. 即 p 是唯一的.

   p 的不可约性也很容易证明：若 $p = fg$，且 f, g 都是其真因子，则有 $0 = p(a) = f(a)g(a)$. 由于 $K[x]$ 为整环，所以必有 $f(a) = 0$ 或 $g(a) = 0$. 不妨设 $f(a) = 0$，则由最小多项式的性质可知：$p | f$，这与 f 是 p 的真因子矛盾！

2. 由于 p 是主理想整环 $K[x]$ 中的不可约元，所以 p 是素元，从而 $\ker \varphi = (p(x))$ 是 $K[x]$ 中的素理想，也就是极大理想，所以 $K[x]/(p(x))$ 是域. 我们有域的嵌入 $\bar{\varphi} : K[x]/(p(x)) \to K(a)$，即 $\bar{\varphi}(K[x]/(p(x))) \subset K(a)$.

   注意到 $K(a)$ 是包含 $K \cup \{a\}$ 的最小域，而 $\bar{\varphi}(K[x]/(p(x)))$ 中包含 $a = \bar{\varphi}(\bar{x})$ 和任意 K 中的元素 $e = \bar{\varphi}(\bar{e})$，所以 $K(a) \subset \bar{\varphi}(K[x]/(p(x)))$. 综上，$K(a) = \bar{\varphi}(K[x]/(p(x)))$，也就是 $K(a) \simeq K[x]/(p(x))$.

3. 由前一小问有域同构 $\bar{\varphi} : K[x]/(p(x)) \xrightarrow{\simeq} K(a)$，所以任意 $K(a)$ 中的元素都可以表示为 $\bar{\varphi}(\bar{f})$. 由于 p 是 n 次多项式，所以由带余除法，必存在一个次数小于 n 的多项式 $g = \sum_{i=0}^{n-1} b_i x^i$（这里各项系数都可以为零），

满足 $\bar{f}=\bar{g}$. 从而有：

$$\begin{aligned}\bar{\varphi}(\bar{f}) &= \bar{\varphi}(\bar{g})\\ &= \bar{\varphi}\left(\sum_{i=0}^{n-1} b_i(\bar{x})^i\right)\\ &= \sum_{i=0}^{n-1} b_i(\bar{\varphi}(\bar{x}))^i\\ &= \sum_{i=0}^{n-1} b_i a^i\\ &= g(a)\in K[a]\end{aligned}$$

即 $K(a)\subset K[a]$，而显然有 $K[a]\subset K(a)$，从而 $K[a]=K(a)$.

笔记 证明过程中有一个细节值得注意，就是商环 $K[x]/(p(x))$ 与域 $K(a)$ 的同构中，对应于 a 的是 $\bar{x}$，也就是说，我们将未定元 x 所在的陪集映到了代数元素 a 上，从而我们将 a 与 $p(x)$ 的根联系在一起，因为：

$$\begin{aligned}0 &= \bar{\varphi}(\bar{0})\\ &= \bar{\varphi}\left(\overline{p(x)}\right)\\ &= \bar{\varphi}(p(\bar{x}))\\ &= p(\bar{\varphi}(\bar{x}))\\ &= p(a)\end{aligned}$$

虽然这一性质早在我们预料之中，但是通过同构的方式重新验证，还是能让我们体会到这一定理（以及这一结构 $K(a)\simeq K[x]/(p(x))$）的美妙之处.

利用单代数扩张，我们可以延拓任意的域同构：

问题 4.8（同构的单代数扩张）：$\varphi: F\xrightarrow{\sim} F'$ 是一个域同构. $p(x)=\sum_{i=0}^{n} a_i x^i\in F[x]$ 是一个不可约多项式，且 $p'(x)=\sum_{i=0}^{n}\varphi(a_i)x^i\in F'[x]$. α 是 $p(x)=0$ 的一个根 (在 F 的某个扩域中)，β 是 $p'(x)=0$ 的一个根 (在 F' 的某个扩域中). 于是存在一个同构：

$$\begin{aligned}\sigma: F(\alpha) &\xrightarrow{\sim} F'(\beta)\\ \alpha &\mapsto \beta\end{aligned}$$

使得 $\sigma|_F=\varphi$.

注 证明的过程是很直接的，我们可以从 φ 诱导出环同构 $\varphi: F[x]\xrightarrow{\sim} F'[x]$，然后定义映射：

$$\begin{aligned}\psi: F[x]/(p(x)) &\to F'[x]/(p'(x))\\ \bar{f} &\mapsto \overline{\varphi(f)}\end{aligned}$$

容易证明这是一个域同构（注意要先说明良定义）. 再利用单代数扩张的性质可得：

$$F(\alpha)\simeq F[x]/(p(x))\simeq F'[x]/(p'(x))\simeq F'(\beta).$$

此即得证.

如果我们取 $F'=F$，φ 为恒等映射，则 $p'=p$. 取 $p(x)=0$ 的两个根（在 F 的某个扩域内）α_1 和 α_2，利用刚刚证明的命题即得：

$$F(\alpha_1)\simeq F[x]/(p(x))\simeq F(\alpha_2)$$

4.2.4 典型例题

（一）单代数扩张

对于单代数扩张，有 $K(a)=K[a]$. 因此 $K(a)$ 中的每个非零元素，都有一个逆元，并且也是多项式的形式. 我们通过一个例子，说明求逆的方法.

例题 4.1 证明：$p(x)=x^3-2$ 在 $\mathbb{Q}[x]$ 中不可约. 令 θ 是 $p(x)$ 的一个根，求 $1+\theta$ 在 $\mathbb{Q}(\theta)$ 中的逆.

笔记 回忆环论中的内容：证明一个多项式不可约，我们可以尝试使用 Eisenstein 判别法.

而求逆可以使用待定系数法，我们在解答中展示过程，这一过程可以很自然地应用到任意情形之下.

证明 利用 Eisenstein 判别法，$2\mid(-2)$，且 $2^2\nmid(-2)$，从而 $p(x)=x^3-2$ 在 $\mathbb{Q}[x]$ 中不可约.

由单代数扩张的性质，$\mathbb{Q}(\theta)=\{a+b\theta+c\theta^2:a,b,c\in\mathbb{Q}\}$. 于是可设 $(1+\theta)^{-1}=a+b\theta+c\theta^2$，从而有：（注意到 $\theta^3=2$）

$$\begin{aligned}1&=(1+\theta)(1+\theta)^{-1}\\&=(1+\theta)(a+b\theta+c\theta^2)\\&=a+(a+b)\theta+(c+b)\theta^2+c\theta^3\\&=(2c+a)+(a+b)\theta+(c+b)\theta^2\end{aligned}$$

由待定系数法：

$$\begin{aligned}a+2c&=1\\a+b&=0\\b+c&=0\end{aligned}$$

解得：

$$a=\frac{1}{3},\ b=-\frac{1}{3},\ c=\frac{1}{3}$$

即：$(1+\theta)^{-1}=\dfrac{1}{3}(1-\theta+\theta^2)$.

练习 4.4 证明：$p(x)=x^3+9x+6$ 在 $\mathbb{Q}[x]$ 中不可约. 令 θ 是 $p(x)$ 的一个根，求 $1+\theta$ 在 $\mathbb{Q}(\theta)$ 中的逆.

练习 4.5 证明：$p(x)=x^2+x+1$ 在 $\mathbb{F}_2[x]$ 中不可约. 令 θ 是 $p(x)$ 的一个根，求 $1+\theta$ 在 $\mathbb{F}_2(\theta)$ 中的逆.

对于单代数扩张，我们还有同构 $F[x]/(p(x))\simeq F[a]$，其中 $p(x)$ 为 a 在 F 上的最小多项式. 于是 a 与 $p(x)$ 的对应关系也是我们所关注的问题.

一方面，给定 F 上的不可约多项式 $p(x)$，找 a 就是求 $p(x)$ 的根，不论是有求根公式的低次多项式，还是一般需要依赖数值求解的高次多项式，求 a 总是不困难的.

而另一方面，已知 a，求对应的、给定 F 上的不可约多项式 $p(x)$，就是一个相对较为困难，且具有一定技巧性的事情了.

例题 4.2 求元素 $\theta=\sqrt[6]{2}$ 在下列域中的最小多项式 $p(x)$：

1. $K=\mathbb{Q}(\sqrt[6]{2})$；
2. $K=\mathbb{Q}(\sqrt[3]{2})$；
3. $K=\mathbb{Q}(\sqrt{2})$；
4. $K=\mathbb{Q}$.

注 由最小多项式的定义，元素 a 在给定数域（或环）R 中的最小多项式 $p(x)$ 需要满足：

1. $p(x)$ 为首一多项式，系数在 R 中；
2. $p(a)=0$；
3. $p(x)$ 在 $R[x]$ 中不可约.

解

1. 考虑首一多项式 $p(x)=x-\theta\in K[x]$. 因为 p 为一次式，所以必然是不可约多项式，且 $p(\theta)=0$. 故 $x-\theta$ 是 a 在 K 中的最小多项式.

2. 考虑首一多项式 $p(x)=x^2-\theta^2\in K[x]$. $p(\theta)=0$ 是显然的. 下证：$p(x)\in K[x]$ 不可约.
   假设 $p(x)\in K[x]$ 可约，由于 p 为二次式，所以其真因子中必有一次式 $x-c\in K[x]$，也就是 $p(x)=0$ 有一根 $c\in K$. 而我们知道，$p(x)=0$ 有且只有两根 $\pm\theta$（将 $p(x)=0$ 置于复数域中，考察它的根，并且由代数基本定理可知他只有两个根），而两根均不在 K 中，矛盾！所以 $p(x)\in K[x]$ 不可约.
   综上，$x^2-\theta^2$ 是 a 在 K 中的最小多项式.
3. 考虑首一多项式 $p(x)=x^3-\theta^3\in K[x]$. $p(\theta)=0$ 是显然的. 下证：$p(x)\in K[x]$ 不可约.
   假设 $p(x)\in K[x]$ 可约，由于 p 为三次式，所以其真因子中必有一次式 $x-c\in K[x]$，也就是 $p(x)=0$ 有一根 $c\in K$. 而我们知道，$p(x)=0$ 有且只有三根 $\theta,\theta\omega,\theta\omega^2$（其中 ω 为不等于 1 的任意三次单位根），它们均不在 K 中，矛盾！所以 $p(x)\in K[x]$ 不可约.
   综上，$x^3-\theta^3$ 是 a 在 K 中的最小多项式.
4. 考虑首一多项式 $p(x)=x^6-2\in K[x]$. $p(\theta)=0$ 是显然的. 注意到 p 的首项系数不是 2 的倍数，其他各项系数为 2 的倍数，常数项不为 2^2 的倍数，所以由 Eisenstein 判别法可知 $p(x)\in K[x]$ 不可约.
   综上，x^6-2 是 a 在 K 中的最小多项式.

笔记 一般来说，证明一个多项式不可约，有如下的思路：

1. 对于二次、三次多项式，证明它没有一次因式；
2. 利用系数取模法（包括 Eisenstein 判别法）证明多项式不可约；
3. 假设该多项式可约，利用分解式制造矛盾.

例题 4.3 求 $t=1+\sqrt[3]{2}+\sqrt[3]{4}$ 在 $\mathbb{Q}$ 上的最小多项式.

解 考虑首一多项式 $p(x)=x^3-3x^2-3x-1$. 记 $a=\sqrt[3]{2}$，从而可得：

$$t(a-1)=(a-1)(a^2+a+1)=a^3-1=2-1=1$$

即

$$a=\frac{t+1}{t}$$

一方面：

$$\begin{aligned}p(t)&=2t^3-(t+1)^3\\&=t^3\left(2-\left(\frac{t+1}{t}\right)^3\right)\\&=t^3\left(2-a^3\right)\\&=0\end{aligned}$$

另一方面，考虑 $p(y-1)=y^3-6y^2+6y-2$. 由于首项系数不为 2 的倍数，其余各项系数均为 2 的倍数，且常数项不为 2^2 的倍数，所以由 Eisenstein 判别法可知，$p(y-1)$ 在 $\mathbb{Q}[x]$ 内不可约，也就是 $p(x)$ 在 $\mathbb{Q}[x]$ 内不可约.

综上，t 在 $\mathbb{Q}$ 上的最小多项式为 x^3-3x^2-3x-1.

笔记 想必读者看完答案之后一定有一个疑问，这里的最小多项式 $p(x)=x^3-3x^2-3x-1$ 是怎么找到的呢？下面就来揭示寻找的过程.

首先，观察 t 的结构：$t=1+a+a^2$. 我们想以此为基础，构造一个只包含 t 和有理数的多项式，从而要想办法将 a 转化成有理数. 我们知道，$a^3=2$，而 $1+a+a^2$ 又非常容易让人联想到立方差公式 $a^3-1=(a-1)(1+a+a^2)$，于是我们得到：

$$t(a-1)=a^3-1=1$$

上式可以解出 a 的表达式：

$$a=\frac{t+1}{t}$$

然后利用 $a^3=2$，即可使得等式中只包含 t 和有理数，再去分母移项就可得到我们想要的多项式：

$$\begin{aligned} 2=a^3&=\frac{(t+1)^3}{t^3}\\ 2t^3&=(t+1)^3\\ t^3-3t^2-3t-1&=0 \end{aligned}$$

然后剩下的工作就写道解答里去了.

请读者注意，本题最核心、最困难的思考部分，并没有呈现在解答中，也不需要（且不应该）写到解答里. 这可能是一部分难题不容易看懂解答的原因，“功夫在解答之外”.

✍ **练习 4.6** 求元素 $2+\sqrt{3}$ 在 $\mathbb{Q}$ 上的最小多项式.

✍ **练习 4.7** 求元素 $1+i$ 在 $\mathbb{Q}$ 上的最小多项式.

注 利用代数方程的复根成对共轭的性质，构造以给定元素为根的方程 $p(x)=0$. 然后证明 $p(x)$（或者它的某个以给定元素为根的因式）不可约，从而找出最小多项式.

本题中，取 $x=1+i$，$y=1-i$. 于是 $x+y=2$，$xy=2$，从而构造出多项式 x^2-2x+2.

解 考虑首一多项式 $p(x)=x^2-2x+2$. 一方面，$p(1+i)=0$. 另一方面，由于 $p(x)$ 为二次式，若其可约，则必然有 $\mathbb{Q}[x]$ 内的一次因式，从而 $p(x)=0$ 有有理根. 然而 $p(x)=0$ 没有有理根，所以在 $\mathbb{Q}[x]$ 内不可约. 从而 x^2-2x+2 是所需的最小多项式.

✍ **练习 4.8** 求元素 $t=1+\sqrt[3]{2}+2\sqrt[3]{4}$ 在 $\mathbb{Q}$ 上的最小多项式.

解 考虑首一多项式 $p(x)=x^3-3x^2-9x-23$. 一方面，可以验证 $p(t)=0$. 另一方面，由于 $p(x)$ 为三次式，若其可约，则必然有 $\mathbb{Q}[x]$ 内的一次因式，从而 $p(x)=0$ 有有理根，且有理根只可能为 ± 23，不过 $p(\pm 23)\neq 0$，于是 $p(x)=0$ 没有有理根，矛盾！所以 $p(x)$ 不可约，也就是我们想要的最小多项式.

笔记 记 $u=\sqrt[3]{2}$，于是 $t=1+u+2u^2$. 我们似乎不太能够发现处理 t 的简单办法，于是考虑使用待定系数法. 注意到 t 中出现的各个单项，至少需要求三次方，才能够将其变为有理数，所以我们不妨猜想，t 对应的最小多项式是三次式.

设首一多项式 $f(x)=x^3+ax^2+bx+c$ 以 t 为一根，由于：

$$\begin{aligned} t&=2u^2+u+1\\ t^2&=4u^4+4u^3+5u^2+2u+1=5u^2+10u+9\\ t^3&=10u^4+25u^3+33u^2+19u+9=33u^2+39u+59 \end{aligned}$$

从而可得：

$$\begin{aligned} 0&=f(t)\\ &=(33u^2+39u+59)+(5u^2+10u+9)a+(2u^2+u+1)b+c\\ &=(33+5a+2b)u^2+(39+10a+b)u+(59+9a+b+c) \end{aligned}$$

于是由待定系数法得到方程组：

$$\begin{aligned} 5a+2b&=-33\\ 10a+b&=-39\\ 9a+b+c&=-59 \end{aligned}$$

解得：

$$\begin{aligned} a&=-3\\ b&=-9\\ c&=-23 \end{aligned}$$

接下来的过程就呈现在解答里了.

待定系数法是通法，但是计算过程较为繁杂，一不小心也容易算错，所以我们当然还是想找一找，有没有更简单的找到最小多项式的办法. 通过观察，我们发现：

$$t = 2u^2 + u + 1$$
$$ut = 2u^3 + u^2 + u = u^2 + u + 4$$

于是有：

$$2ut - t = u + 7$$

也就是：

$$(2t - 1)u = t + 7$$

从而等式两边同时求三次方，就把 u 消去了：

$$2(2t - 1)^3 = (t + 7)^3$$

化简此式会更容易一些，我们展示一下化简过程，注意有些式子不必先求值：

$$\begin{aligned} 2(8t^3 - 12t^2 + 6t - 1) &= t^3 + 21t^2 + 3 \cdot 7^2 t + 7^3 \\ 15t^3 - 45t^2 - 3(7^2 - 2^2)t - (2 + 7^3) &= 0 \\ t^3 - 3t^2 - 3 \cdot 5 \cdot 9/15t - (2 + 7 \cdot 4 + 7 \cdot 45)/15 &= 0 \\ t^3 - 3t^2 - 9t - (30 + 21 * 15)/15 &= 0 \\ t^3 - 3t^2 - 9t - 23 &= 0 \end{aligned}$$

这样做不但避免了繁琐的多项式乘法，计算更简单，而且我们得到了一个非常重要的关系：

$$(2t - 1)u = t + 7.$$

（二）有限扩张的嵌套

对于嵌套的有限扩张 F/E，E/K，维数公式 $[F : K] = [F : E][E : K]$ 有时会提供一些奇妙的信息，因为它是整数乘积 $a = bc$ 的形式，从而素因子分析（包括其特殊形式：奇偶分析）这一常用手法再现江湖. 对此我们并不陌生，群论中的 Lagrange 定理、轨道公式，环论中素理想的性质，都有类似的形式和通用的处理思路.

例题 4.4 设域扩张 F/K 的维数为某个素数 p，证明：任意包含 K 的 F 的子域是 K 或者 F.

证明 任意包含 K 的 F 的子域 E，我们有 $[F : K] = [F : E][E : K]$，所以 $p = [F : E][E : K]$，因为 p 只能分解为 $1 \cdot p$，所以 $[F : E] = 1$ 或 $[E : K] = 1$，即 $E = F$ 或 $E = K$.

例题 4.5 证明：若 $[F(a) : F]$ 是奇数，则 $F(a) = F(a^2)$.

注 注意到 $F(a)/F(a^2)$，$F(a^2)/F$ 为嵌套的有限扩域，从而我们可以利用维数公式分析.

证明 因为 $a^2 \in F(a)$，所以 $F(a^2)$ 为 $F(a)$ 的子域. 又因为 $F(a^2)$ 为 F 的扩域，所以有 $[F(a) : F(a^2)][F(a^2) : F] = [F(a) : F]$.

考虑 a 在 $F(a^2)[x]$ 中的最小多项式，若 $a \in F(a^2)$，则最小多项式为 $x - a$，即 $[F(a) : F(a^2)] = 1$；若 $a \notin F(a^2)$，则最小多项式为 $x^2 - a^2$，即 $[F(a) : F(a^2)] = 2$. 然而，第二种情况是不成立的，因为此时等式 $[F(a) : F(a^2)][F(a^2) : F] = [F(a) : F]$ 的左边为偶数，右边为奇数，矛盾！所以只能是 $[F(a) : F(a^2)] = 1$，从而 $F(a) = F(a^2)$.

笔记 一般来说，我们看到待证命题 $F(a) = F(a^2)$，想到的往往是先证明 $a^2 \in F(a)$（显然成立），再证明 $a \in F(a^2)$，然而到此这一思路也就无法继续发展下去了. 此时我们回头看题设，维数关系 $[F(a) : F]$ 我们还没有用起来，于是经过进一步的思考，解答中呈现的方法也就顺理成章的出现了.

因此，例题也告诉我们，在思考代数扩张的相关问题时，维数关系总是一个思考的角度.

练习 4.9 设 $F = \mathbb{Q}(a_1, a_2, \cdots, a_n)$，其中每个 $a_i^2 \in \mathbb{Q}$. 证明：$\sqrt[3]{2} \notin F$.

注 提示：容易求得 $\sqrt[3]{2}$ 在 $\mathbb{Q}$ 中的最小多项式为 $x^3-2=0$，从而 $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$. 若 $\sqrt[3]{2}\in F$，则 $\mathbb{Q}(\sqrt[3]{2})$ 为 F 的子域，于是有：

$$[F:\mathbb{Q}]=[F:\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$$

可得 $3|[F:\mathbb{Q}]$.

然而，$[F:\mathbb{Q}]$ 只能为 2 的幂次，这是因为

1. 若 $a_i\in\mathbb{Q}(a_1,\cdots,a_{i-1})$，则 $[\mathbb{Q}(a_1,\cdots,a_{i-1})(a_i):\mathbb{Q}(a_1,\cdots,a_{i-1})]=1$；
2. 若 $a_i\notin\mathbb{Q}(a_1,\cdots,a_{i-1})$，则 $[\mathbb{Q}(a_1,\cdots,a_{i-1})(a_i):\mathbb{Q}(a_1,\cdots,a_{i-1})]=2$.

然后 F 可以在 $\mathbb{Q}$ 上从 a_1 到 a_n 依次归纳生成.

由此导出矛盾！

4.2.5 习题

（一）代数扩张

✍ **练习 4.10** 证明：$\mathbb{R}[x]/(x^2+1)\simeq\mathbb{C}$.

注 提示：$\mathbb{R}[x]/(x^2+1)\simeq\mathbb{R}[\sqrt{-1}]\simeq\mathbb{C}$.

✍ **练习 4.11** 设 p 为素数，分别求 $e^{\frac{2\pi i}{p}}$ 和 $e^{\frac{2\pi i}{8}}$ 在 $\mathbb{Q}$ 上的最小多项式.

注 提示：

1. 第一小问，需要证明
$$\frac{x^p-1}{x-1}$$
是 $\mathbb{Q}[x]$ 上的不可约多项式.（我们在多项式一章不可约判定一节处理过此类问题）
2. 第二小问，需要证明
$$x^4+1$$
是 $\mathbb{Q}[x]$ 上的不可约多项式.

✍ **练习 4.12**

1. 证明：$p(x)=x^3-2x-2$ 在 $\mathbb{Q}[x]$ 中不可约；
2. 令 u 是 $p(x)$ 的一个根，化简 $(u+1)(u^2+u+1)$；
3. 化简 $(u+1)/(u^2+u+1)$.

证明

1. 因为 p 的首项系数为 1，$-2,-2$ 是素数 2 的倍数，而 -2 不是 2^2 的倍数，所以利用 Eisenstein 判别法可知，p 在 $\mathbb{Q}[x]$ 中不可约.
2. 因为 $u^3-2u-2=0$，所以
$$\begin{aligned}(u+1)(u^2+u+1)&=u^3+2u^2+2u+1\\&=(2u+2)+2u^2+2u+1\\&=2u^2+4u+3\end{aligned}$$
3. 设 u^2+u+1 的乘法逆为 au^2+bu+c，于是有：
$$\begin{aligned}1&=(u^2+u+1)(au^2+bu+c)\\&=au^4+(b+a)u^3+(c+b+a)u^2+(b+c)u+c\\&=2au(u+1)+2(a+b)(u+1)+(c+b+a)u^2+(b+c)u+c\\&=(3a+b+c)u^2+(4a+3b+c)u+(2a+2b+c)\end{aligned}$$

对比等式两边系数有

$$3a+b+c=0$$
$$4a+3b+c=0$$
$$2a+2b+c=1$$

解得：

$$a=-\frac{2}{3}$$
$$b=\frac{1}{3}$$
$$c=\frac{5}{3}$$

即

$$\frac{1}{u^2+u+1}=\frac{1}{3}(-2u^2+u+5)$$

所以有

$$\begin{aligned}\frac{u+1}{u^2+u+1}&=\frac{1}{3}(u+1)(-2u^2+u+5)\\&=\frac{1}{3}(-2u^3-u^2+6u+5)\\&=\frac{1}{3}(-u^2+2u+1)\end{aligned}$$

✍ **练习 4.13** 证明：$p(x)=x^3+x+1$ 在 $\mathbb{Z}_2[x]$ 中不可约. 令 u 是 $p(x)$ 的一个根，求 $1+u+u^2$ 在 $\mathbb{Z}_2(u)$ 中的逆.

✍ **练习 4.14** 设 u 是多项式 x^3-6x^2+9x+3 的一个实根.

1. 证明：$[\mathbb{Q}(u):\mathbb{Q}]=3$；
2. 将 $u^4,(u+1)^{-1},(u^2-6u+8)^{-1}$ 表示成 $1,u,u^2$ 的 $\mathbb{Q}$-线性组合.

✍ **练习 4.15** 设 $u=x^3/(x+1)$，求 $[\mathbb{Q}(x):\mathbb{Q}(u)]$.

注 提示：注意到 $\mathbb{Q}(x)=\mathbb{Q}(u,x)=(\mathbb{Q}(u))(x)$. 而利用所给条件代数变形可得

$$x^3-ux-u=0$$

换句话说，x 是多项式环 $\mathbb{Q}(u)[t]$ 中的代数元素.

由于 u 是 $\mathbb{Z}[u]$ 中的不可约元，所以利用 Eisenstein 判别法可得，多项式 t^3-ut-u 在 $\mathbb{Z}[u]$ 中不可约. 再由 Gauss 引理，本原多项式 t^3-ut-u 在 $\mathbb{Q}(u)$（$\mathbb{Z}[u]$ 的分式域）中不可约. 从而 t^3-ut-u 是 x 的最小多项式，于是 $[\mathbb{Q}(x):\mathbb{Q}(u)]=[\mathbb{Q}(u)(x):\mathbb{Q}(u)]=3$.

✍ **练习 4.16** 设 $F=\mathbb{Q}(i)$，证明：x^3-2 与 x^3-3 在 F 上不可约.

注 提示：三次多项式一定会有一个一次因式，从而只需考察该多项式等于零时在给定域内有没有根即可.

证明 对于 $f(x)=x^3-2$，$f(x)=0$ 在 $\mathbb{C}$ 上的三个根为 $\sqrt[3]{2}\zeta_3$，其中 $\zeta_3\neq 1$ 为三次单位根. 由于这三个根均不在 F 内（读者写出 ζ_3 的显式即可验证这一点），从而 $f(x)$ 在 $F[x]$ 内没有一次因式，所以 $f(x)$ 在 $F[x]$ 内不可约.

$g(x)=x^3-3$ 在 $F[x]$ 内不可约可类似证明.

✍ **练习 4.17** 考察 $\mathbb{Q}$ 的一个扩域 $\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

1. 证明：$\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$；
2. 证明：$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$；
3. 求 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}$ 上的最小多项式；
4. 求 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{2})$ 上的最小多项式；
5. 证明：$[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}(\sqrt{6})]=2$；
6. 求 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{6})$ 上的最小多项式.

证明

1. 一方面，$\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$，从而 $\mathbb{Q}(\sqrt{2}+\sqrt{3})\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$.
   另一方面，记 $u=\sqrt{2}+\sqrt{3}$，则 $u^{-1}=\sqrt{3}-\sqrt{2}$，从而
   $$\sqrt{2}=\frac{1}{2}(u-u^{-1})\in\mathbb{Q}(u)$$
   $$\sqrt{3}=\frac{1}{2}(u+u^{-1})\in\mathbb{Q}(u)$$
   于是 $\mathbb{Q}(\sqrt{2},\sqrt{3})\subset\mathbb{Q}(\sqrt{2}+\sqrt{3})$.
   综上，$\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$.
2. 首先，$x^2-2\in\mathbb{Q}[x]$ 是不可约多项式，所以是 $\sqrt{2}$ 在 $\mathbb{Q}$ 上的最小多项式，于是 $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$. 其次，$x^2-3\in\mathbb{Q}(\sqrt{2})[x]$ 同样是不可约多项式，所以是 $\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{2})$ 上的最小多项式，于是 $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$.
   注意到 $\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$，所以有
   $$\begin{aligned}[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]&=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]\\&=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]\\&=4.\end{aligned}$$
3. 因为 $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=4$，所以 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}$ 上的最小多项式的次数是 4. 考虑首一多项式 $f(x)=x^4-10x^2+1$，我们有：
   $$f(\sqrt{2}+\sqrt{3})=0$$
   从而 x^4-10x^2+1 就是欲求最小多项式.
4. 由于 $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$，所以 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{2})$ 上的最小多项式的次数是 4. 考虑首一多项式 $g(x)=x^2-2\sqrt{2}x-1$，我们有
   $$g(\sqrt{2}+\sqrt{3})=0$$
   从而 $x^2-2\sqrt{2}x-1$ 就是欲求最小多项式.
5. 容易证明：$[\mathbb{Q}(\sqrt{6}):\mathbb{Q}]=2$（考虑多项式 x^2-6），且 $\mathbb{Q}(\sqrt{6})\in\mathbb{Q}(\sqrt{2},\sqrt{3})$，所以有维数关系：
   $$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{6})][\mathbb{Q}(\sqrt{6}):\mathbb{Q}]$$
   从而求得 $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{6})]=2$.
6. 由于 $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{6})]=2$，所以 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{6})$ 上的最小多项式的次数是 2. 考虑首一多项式 $h(x)=x^2-(5+2\sqrt{6})$，我们有
   $$h(\sqrt{2}+\sqrt{3})=0$$
   从而 $x^2-(5+2\sqrt{6})$ 就是欲求最小多项式.

笔记 本题的解答中，需要额外解释的内容比较丰富.

1. 第一小问的证法，是此类问题的一般思路.
2. 第二小问借助最小多项式求扩域维数. 由于这里的最小多项式很好找，而维数关系不好说明，所以从最小多项式推证到维数. 有时这一过程也会逆转.
3. 第三小问实际上就是一个逆转过程，这里的最小多项式不容易一下子找到，而维数已知的情况下，就可以给出最小多项式的次数，然后通过待定系数法求解.
   不过，待定系数法是求最小多项式的通法，换句话说，也就是没有办法的办法，而本题的难度还远没有那么大，所以可以借助其他手段给出. 笔者是通过两步“观察法”找到最小多项式的：
   首先，考虑以 $\sqrt{3}\pm\sqrt{2}$ 为根的实系数一元二次方程，利用 Vieta 定理很容易得到它：$x^2-2\sqrt{3}x+1=0$.
   然后，将左式分组改写为 $(x^2+1)-2\sqrt{3}x$，再乘上它的“共轭”式 $(x^2+1)+2\sqrt{3}x$，就有
   $$((x^2+1)-2\sqrt{3}x)((x^2+1)+2\sqrt{3}x)=(x^2+1)^2-(2\sqrt{3}x)^2=x^4-10x^2+1.$$
   请读者思考，这一方法的合理性.
4. 第四小问考虑以 $\sqrt{2}\pm\sqrt{3}$ 为根的实系数一元二次方程即可. 请注意，这里我们关注 $\sqrt{3}$ 的共轭，这是因为

$\sqrt{2}$ 是 $\mathbb{Q}(\sqrt{2})$ 中的元素，最终所求的最小多项式的系数中可以有 $\sqrt{2}$.

5. 第五小问是维数公式的典型应用.
6. 第六小问的思路来源是完全平方公式 $(\sqrt{2}+\sqrt{3})^2=5+2\sqrt{6}$，至于想到它的原因，则是因为 $\sqrt{6}=\sqrt{2}\sqrt{3}$.

总结一下本题呈现的主要思路：

1. 利用共轭式和 Vieta 定理，联系二次根式与二次多项式；
2. 扩域的维数，与扩充的某些代数元素最小多项式的次数相等. 在实际问题中两者都有可能更容易求得，从而两个方向的转化都很常见.

✍ **练习 4.18** F 是一个特征不等于 2 的域. 设 $d_1,d_2\in F$，且不为 F 中的平方. 证明：

1. 如果 d_1d_2 不是 F 中的平方，则 $F(\sqrt{d_1},\sqrt{d_2})$ 在 F 上的维数为 4（称为 F 上的四次幂扩张，biquadratic extension）；
2. 如果 d_1d_2 是 F 中的平方，则 $F(\sqrt{d_1},\sqrt{d_2})$ 在 F 上的维数为 2.

注 提示：若 $d_1d_2=c^2$，则 $\sqrt{d_2}=c/\sqrt{d_1}$，从而 $F(\sqrt{d_1},\sqrt{d_2})=F(\sqrt{d_1})$. 细心的读者可能会有疑问，为什么 $\mathrm{char}(F)$ 不能为 2？我们将在有限域的部分回答这一问题，目前读者的知识储备不足以回答这一问题.

✍ **练习 4.19** F 是一个特征不等于 2 的域. 设 $a,b\in F$，且 b 不是 F 中的平方. 证明：

1. 存在 $m,n\in F$，有 $\sqrt{a+\sqrt{b}}=\sqrt{m}+\sqrt{n}$，当且仅当 a^2-b 是 F 中的平方.
2. 当 a,b 满足什么条件时，$\mathbb{Q}(\sqrt{a+\sqrt{b}})$ 是 $\mathbb{Q}$ 上的四次幂扩张？

✍ **练习 4.20** 求域扩张 $\mathbb{Q}(\sqrt{3+2\sqrt{2}})$ 的维数.

注 提示：注意到 $\sqrt{3+2\sqrt{2}}=1+\sqrt{2}$.

✍ **练习 4.21**

1. 设 $\sqrt{3+4i}$ 表示位于第一象限的 $3+4i$ 的平方根，$\sqrt{3-4i}$ 表示位于第四象限的 $3-4i$ 的平方根. 证明：$[\mathbb{Q}(\sqrt{3+4i}+\sqrt{3-4i}):\mathbb{Q}]=1$.
2. 求域扩张 $\mathbb{Q}(\sqrt{1+\sqrt{-3}}+\sqrt{1-\sqrt{-3}})/\mathbb{Q}$ 的维数.

注 提示：第一小问，证明 $\sqrt{3+4i}+\sqrt{3-4i}\in\mathbb{Q}$ 即可. 第二小问的思路与第一题相同.

✍ **练习 4.22** 设 K/F 是域的代数扩张. 令 R 是包含 F 的 K 的子环，证明：R 是包含 F 的 K 的子域.

证明 R 的含幺交换性是显然的. 对任意 $r\in R$，我们只需证明：r 的逆在 R 中.

若 $r\in F$，由于 F 是域，命题显然成立.

若 $r\notin F$，因为 $r\in R\subset K$，所以 r 是 F 的代数元素. 因此，$K(r)/K$ 是个有限单扩张，$K[r]=K(r)$，从而 $K[r]$ 中包含了 r 的逆. 又 $K\subset R$，$r\in R$，从而 $K[r]\in R$，也就是说，r 的逆也在 R 中. 命题成立.

综上所述，原命题得证.

笔记 单代数扩张的性质非常好，它在一个线性空间上产生了域结构，我们对此要加以利用.

✍ **练习 4.23*** 设 u 属于域 F 的某个扩域，且 x^n-a 是 u 在 F 上的最小多项式. 试求 u^m 在 F 上的最小多项式，其中 $m\mid n$.

✍ **练习 4.24** 证明：映射

$$\begin{aligned}\varphi:\mathbb{Q}(\sqrt{2})&\to\mathbb{Q}(\sqrt{2})\\ a+b\sqrt{2}&\mapsto a-b\sqrt{2}\end{aligned}$$

是域同构.

✍ **练习 4.25** 若域 K 有子域 $\mathbb{Z}_p$，其中 p 为素数，证明：K 是特征 p 域.

证明 因为 K 有子域 $\mathbb{Z}_p$，所以 K 是子域 $\mathbb{Z}_p$ 上的线性空间，从而在 K 上存在一组基 $\{e_i\}_{i\in I}$，使得 K 中的任意元素 k 可唯一的表达为：

$$k=\sum_{i\in I}a_ie_i$$

其中 $a_i \in \mathbb{Z}_p$，且只有有限个 a_i 不等于 0. 从而：

$$\begin{aligned} p \cdot k &= \sum_{i \in I} p \cdot (a_i e_i) \\ &= \sum_{i \in I} (p a_i) e_i \\ &= \sum_{i \in I} 0 e_i \\ &= 0 \end{aligned}$$

即 $\operatorname{char} K = \mathbb{Z}_p$.

（二）超越扩张

练习 4.26 F 是域，$F[x]$ 为其多项式环，证明：未定元 x 为 F 上的超越元素.

笔记 本题颇有一点脑筋急转弯的味道.

练习 4.27 给出域扩张 F/K 的例子，使得 $F = K(u, v)$，u, v 均是 K 上的超越元素，但是 F 和有理函数域 $K(x, y)$ 不同构.

解 取 $u = \pi$，$v = \pi^2$，于是 $K(u, v) \simeq K(\pi) \simeq K(x)$，但是 $K(x)$ 和 $K(x, y)$ 不同构.

笔记 在多项式环和有理函数域中，各个未定元之间没有任何关系.

练习 4.28 F 是域，u 是有理函数域 $F(x)$ 中的元素，且 $u \notin F$，求证：未定元 x 是域 $F(u)$ 上的代数元素.

证明 因为 $u \in F(x)$，所以存在互素的 $P(x), Q(x) \in F[x]$，使得 $u = P(x)/Q(x)$. 于是 $P(x) - Q(x)u = 0$，这是一个关于 u 的，系数在 $F(u)$ 中的多项式方程. 命题即证.

（三）待定区

练习 4.29 域 F 被称为是“形式实”（formally real）的，如果 -1 不能被表示为 F 中平方的和. 设 F 是形式实域，$f(x) \in F[x]$ 是奇数 k 次不可约多项式，且 α 是 $f(x)$ 的根. 证明：$F(\alpha)$ 也是形式实域.

证明 假设 α 是使 $F(\alpha)$ 不是形式实域的、维数最小的数，且为某个不可约多项式的根，则存在 $f_1, \cdots, f_n \in F[x]$，使得 $f_1^2(x) + \cdots + f_n^2(x) \equiv 1 \mod (f(x))$. 不妨设每个 f_i 的次数都小于 k，（否则总可以对 f_i 进一步用 f 模化）且将其表达为等式，即存在 $g(x) \in F[x]$，使得 $f_1^2(x) + \cdots + f_n^2(x) = 1 + f(x)g(x)$，注意到等式左侧的多项式次数至多为 $2(k-1)$ 次，从而 $g(x)$ 的次数，至多为 $k - 2 < k$ 次，换句话说，对于 $g(x)$ 的某个不可约因式 $h(x)$，有 $f_1^2(x) + \cdots + f_n^2(x) \equiv 1 \mod (h(x))$，于是对于 $h(x)$ 的任意根 β，其次数比 α 小，且使 $F(\beta)$ 不为形式实域，这就与 α 的最小性矛盾！从而 $F(\alpha)$ 必为形式数域.

笔记 此题的思路颇有一些组合学的意味. 我们利用的是“极端原理”：一个自然数集的子集中，必有最小数. 无穷递降法（证明 $\sqrt{2}$ 为无理数的一种方法）也属于这样的思路.

练习 4.30 设 $f(x)$ 是域 F 上次数为 n 的不可约多项式，且 $g(x)$ 是 F 上的任意多项式. 证明：$f(g(x))$ 的每个不可约因子，其次数都能被 n 整除.

证明 设 $\beta \in \bar{F}$ 是 $f(g(x))$ 的任意一个根，我们只需证明：β 在 F 上的最小多项式的次数能被 n 整除，也就是 $[F(\beta) : F]$ 能被 n 整除.

对于 β，一定存在一个 $f(x)$ 的根 α，使得 $g(\beta) = \alpha$. 从而 $F(\alpha) \subset F(\beta)$，于是有 $[F(\beta) : F] = [F(\beta) : F(\alpha)][F(\alpha) : F] = [F(\beta) : F(\alpha)]n$，原命题得证.

笔记 我们举一个例子，使得 $f(x)$ 不可约，而 $f(g(x))$ 可约：在有理数范围内，$f(x) = x^2 + 64$ 不可约.

我们先取 $g(x) = x^2$，则 $f(g(x)) = x^4 + 64 = (x^4 + 16x^2 + 64) - (4x)^2 = (x^2 + 8)^2 - (4x)^2 = (x^2 + 4x + 8)(x^2 - 4x + 8)$ 可约.

再取 $g(x) = x^3$，则 $f(g(x)) = x^6 + 64 = (x^2)^3 + 4^3 = (x^2 + 4)(x^4 - 4x^2 + 16)$，同样可约.

练习 4.31 证明：$K_1 = \mathbb{Z}_{11}[x]/(x^2 + 1)$ 和 $K_2 = \mathbb{Z}_{11}[y]/(y^2 + 2y + 2)$ 都是域，且同构.

注 提示：考虑域同构 $\varphi: K_1 \to K_2, f(x) \to f(y+1)$.

练习 4.32 E 为域，$f \in E[x]$，$\deg f = n \geqslant 1$. 求证：存在 E 的某个扩域 F，使得 $[F:E] \leqslant n!$，并且 $f(x)$ 在 $E(x)$ 中分解成 n 个一次多项式之积.

注 提示：在 E 的代数闭域中给出 f 的不可约分解

$$f = (x-a_1)\cdots(x-a_n)$$

考虑 a_1 在 $E[x]$ 中的最小多项式，其次数不可能超过 n；然后考虑 a_2 在 $E(a_1)[x]$ 中的最小多项式，其次数不可能超过 $n-1$（因为 a_2 是多项式 $(x-a_2)\cdots(x-a_n) \in E(a_1)[x]$ 的根.）……

按前述过程依次讨论至 a_n 为止，所得扩域 $E(a_1,\cdots,a_n)$ 相对 E 的次数不超过 $n!$，且 f 在该扩域中有不可约分解 $f = (x-a_1)\cdots(x-a_n)$.

4.3 有限域的构造

注：本节的主要目的是让读者熟悉有限群的结构和基本性质，其中大多数定理的理论性证明，我们将在后续章节中逐步给出.

本节均设 F 是有限域.

4.3.1 课前思考

判断下列命题的正误，并说明理由：

1. 存在 15 阶的有限域.
2. $\mathbb{Z}_2[x]/(x^3+x^2+1)$ 是域.
3. $\mathbb{Z}_2[x]/(x^3+x^2+1)$ 与 $\mathbb{Z}_2[x]/(x^3+x+1)$ 同构.
4. 设 $x^3+x^2+1, x^3+x+1 \in \mathbb{Z}_2[x]$. 在 $\mathbb{Z}_2$ 的某个扩域中，取 $x^3+x^2+1=0$ 的一根为 u，$x^3+x+1=0$ 的一根为 v，则存在域同构 $\varphi: \mathbb{Z}_2[x]/(x^3+x^2+1) \to \mathbb{Z}_2[x]/(x^3+x+1)$，使得 $\varphi(u)=v$.

解

1. F：有限域的阶必为 p^n，其中 p 为素数.
2. T
3. T：他们都是 8 阶域，同阶的域总是同构的.
4. F：若 $\varphi(u)=v$，则 $0=\varphi(0)=\varphi(u^3+u^2+1)=v^3+v^2+1=v^2-v$，而 v^2-v 必然不等于零（否则 v 在 $\mathbb{Z}_2[x]$ 内的最小多项式就是至多二次，但是 v 的最小多项式是 x^3+x+1，矛盾!）.

4.3.2 知识要点

（一）线性结构

1. （特征）：$\mathrm{char}(F)=p$ 是个素数，并且 $F/\mathbb{Z}_p$ 是有限扩张.
2. （线性空间）：F 是 $\mathbb{Z}_p$ 上的线性空间. 记 $n := [F:\mathbb{Z}_p]$，则 $|F| = p^n$，且 F 作为加法群是 n 个 p 阶循环群的直积.
3. （Frobenius 自同态）：若 F 为有限域，则其 Frobenius 自同态为同构.

（二）乘法结构 *

1. （乘法循环群）：$(F^\times, \cdot)$ 为 p^n-1 阶循环群. 若 $F^\times$ 由元素 u 生成，则 $F=\mathbb{Z}_p(u)$.
2. （方程的根）：对任意 $x \in F$，有 $x^{p^n}=x$. 换言之，F 中的每个元素，都是方程 $x^{p^n}-x=0$ 的根.
3. （存在性和唯一性）：对任意的素数 p 和自然数 n，p^n 阶有限域必然存在，且（在同构意义下）唯一.

4. (子域)：p^m 阶域是 p^n 阶域的子域，当且仅当 $m|n$.

4.3.3 知识要点解读

(一) 线性结构

我们在域的扩张部分知道，一旦有扩域关系 F/K，则 F 是 K 上的线性空间. 同时，由域的特征，我们总是可以得到域的一个素子域（同构于 $\mathbb{Z}_p$ 或者 $\mathbb{Z}$），从而可以得到素子域上的一个线性空间. 结合有限域的本质特征：有限，我们得到如下命题.

问题 4.9 (特征)：$\mathrm{char}(F)=p$ 是个素数，并且 $F/\mathbb{Z}_p$ 是有限扩张.

证明 域的特征只能为 0 或某个素数 p. 若 F 的特征为 0，则 F 有素子域 $\mathbb{Z}$，从而 F 必为无限域，矛盾！所以 $\mathrm{char}(F)=p$. 由有限扩张的定义，$F/\mathbb{Z}_p$ 是有限扩张.

问题 4.10 (线性空间)：F 是 $\mathbb{Z}_p$ 上的线性空间. 记 $n:=[F:\mathbb{Z}_p]$，则 $|F|=p^n$，且 F 作为加法群是 n 个 p 阶循环群的直积.

证明 由于 $\mathrm{char}(F)=p$，从而 F 有一个子域 $\mathbb{Z}_p$. 于是 F 是 $\mathbb{Z}_p$ 上的线性空间. 因为 $[F:\mathbb{Z}_p]=n$，于是可取 $\{e_1,\cdots,e_n\}\subset F$ 为 F 在 $\mathbb{Z}_p$ 上的一组基，F 中的每个元素都可唯一表达为：

$$\sum_{i=1}^{n} a_i e_i,\ \forall a_i\in\mathbb{Z}_p.$$

从而有：$|F|=|\mathbb{Z}_p|^n=p^n$.

4.3.4 典型例题

(一) 有限域的构造

对于一个阶为 p^n 的有限域 F，我们知道 $\mathbb{Z}_p$ 为其子域，然后我们选择一个 n 次首一不可约多项式 $f(x)\in\mathbb{Z}_p[x]$，并取 $f(x)$ 的任意一根 u（这样的 u 总是可以在 $\mathbb{Z}_p$ 的一个扩域中找到，我们将这一扩域称为 $\mathbb{Z}_p$ 的“代数闭包”. 代数闭包的一个典型例子是，有理数域 $\mathbb{Q}$ 的代数闭包是复数域 $\mathbb{C}$）. 从而 $\mathbb{Z}_p(u)\simeq\mathbb{Z}_p[x]/(p(x))$ 为 $\mathbb{Z}_p$ 的扩域，且阶为 p^n，即 $\mathbb{Z}_p(u)$ 就是我们需要的 F.

有一个细节需要指出，所谓的“n 次首一不可约多项式 $f(x)\in\mathbb{Z}_p[x]$”是否一定是存在的？答案是肯定的，证明将留在后续章节给出.

例题 4.6 构造一个 8 元域.

解 因为 $8=2^3$，于是我们先给出一个二元域 $\mathbb{Z}_2=\{0,1\}$. 然后，选择 $\mathbb{Z}_2$ 上的一个三次不可约多项式 $f(x)=x^3+x+1$（因为 $f(0)=f(1)=1$，所以 $f(x)$ 没有 $\mathbb{Z}_2$ 上的一次因式，也就在 $\mathbb{Z}_2[x]$ 内不可约）.

在 $\mathbb{Z}_2$ 的代数闭包中，取 $f(x)=0$ 的一个根 u，于是 $\mathbb{Z}_2[x]/(f(x))\simeq\mathbb{Z}_2(u)$ 为一个 8 元域.

笔记 构造的过程给出了 8 元域的线性结构. 进一步，8 元域对应的乘法群是一个循环群：

$$\begin{aligned}
u^0&=1\\
u^1&=u\\
u^2&=u^2\\
u^3&=u+1\\
u^4&=u^2+u\\
u^5&=u^2+u+1\\
u^6&=u^2+1\\
u^7&=1=u^0
\end{aligned}$$

即 $\mathbb{Z}_2(u)^*$ 是 7 阶循环群.

练习 4.33 构造一个 4 元域，一个 9 元域. 给出域的对应乘法群的结构.

解

1. 4 元域：$\mathbb{Z}_2[x]/(f(x))$，$f(x)$ 只能取 x^2+x+1.
   取 $x^2+x+1=0$ 在 $\mathbb{Z}_2$ 的代数闭包里的一根 u，则：
   $$\begin{aligned} u^0 &= 1 \\ u^1 &= u \\ u^2 &= u+1 \\ u^3 &= u^0 \end{aligned}$$
   即 $\mathbb{Z}_2(u)^*$ 是 3 阶循环群.
2. 9 元域：$\mathbb{Z}_3[x]/(f(x))$，$f(x)$ 可取 x^2+1, x^2+x+2, x^2+2x+2；
   以 $f(x)=x^2+x+2$ 为例，取 $x^2+x+2=0$ 在 $\mathbb{Z}_3$ 的代数闭包里的一根 v，则：
   $$\begin{aligned} v^0 &= 1 \\ v^1 &= v \\ v^2 &= 2v+1 \\ v^3 &= 2v+2 \\ v^4 &= 2 \\ v^5 &= 2v \\ v^6 &= v+2 \\ v^7 &= v+1 \\ v^8 &= v^0 \end{aligned}$$
   即 $\mathbb{Z}_3(v)^*$ 是 8 阶循环群.

（二）有限域上多项式的可约性

考察有限域上多项式的可约性，往往比 $\mathbb{Q}$ 上要容易得多，因为有限域上低次因式的个数十分有限.

例题 4.7 试写出 $\mathbb{Z}_3$ 上全部二次多项式的因式分解形式.

笔记 $\mathbb{Z}_3$ 上二次多项式一共有 $2\times3\times3=18$ 个，我们按照顺序以此讨论即可. 注意到二次多项式若可约，则因式必为一次. 考察 $\mathbb{Z}_3$ 上的一次多项式：

$$x, x+1, x+2$$

$$2x, 2x+1=2(x+2), 2x+2=2(x+1)$$

根据因式定理，我们只需验证二次多项式有无 $\mathbb{Z}_3$ 内的根，有根即可约，无根即不可约. 需要注意的是，$2x, 2x+1, 2x+2$ 是 $\mathbb{Z}_3[x]$ 中的不可约因式，所以 $2x^2$ 的分解式可以写成 $2x\cdot x$. 这里笔者为了形式上的美观，在多项式的最高次项系数为 2 时，统一将 2 作为“公因子”提出.

以下我们直接给出答案.

解

$$
\begin{aligned}
x^2 &= x^2 \\
x^2+1 &\text{ 不可约} \\
x^2+2 &= (x+1)(x+2) \\
x^2+x &= x(x+1) \\
x^2+x+1 &= (x+2)^2 \\
x^2+x+2 &\text{ 不可约} \\
x^2+2x &= x(x+2) \\
x^2+2x+1 &= (x+1)^2 \\
x^2+2x+2 &\text{ 不可约} \\
2x^2 &= 2x^2 \\
2x^2+1 &= 2(x+1)(x+2) \\
2x^2+2 &= 2(x^2+1) \text{ 不可约} \\
2x^2+x &= 2x(x+2) \\
2x^2+x+1 &= 2(x^2+2x+2) \text{ 不可约} \\
2x^2+x+2 &= 2(x+1)^2 \\
2x^2+2x &= 2x(x+1) \\
2x^2+2x+1 &= 2(x^2+x+2) \text{ 不可约} \\
2x^2+2x+2 &= 2(x+2)^2
\end{aligned}
$$

笔记 我们知道，若 $f(x)\in\mathbb{Z}_3[x]$ 不可约，则 $f(x+1), f(x+2)$ 也不可约（这是我们利用 Eisenstein 判别法的常用技巧）. 有趣的是，取 $f(x)=x^2+1$，则

$$
\begin{aligned}
f(x+1) &= (x+1)^2+1 = x^2+2x+2 \\
f(x+2) &= (x+2)^2+1 = x^2+x+2
\end{aligned}
$$

他们恰好是三个首一的三次不可约多项式.

练习 4.34 试写出 $\mathbb{Z}_2$ 上全部不超过五次的多项式的因式分解形式.

4.3.5 习题

练习 4.35 试构造一个 16 元域.

解 答案：$\mathbb{Z}_2[x]/(f(x))$，$f(x)$ 可取 $x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1$.

练习 4.36 将 x^8-x 在给定域上做因式分解：

1. $\mathbb{Q}$;
2. $\mathbb{Z}_2$

解

1. $x^8-x=x(x^7-1)=x(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$.（在多项式一章，我们已经证明，$x^6+x^5+x^4+x^3+x^2+x+1=(x^7-1)/(x-1)$ 不可约）
2. $x^8-x=x(x^7-1)=x(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)=x(x-1)(x^3+x+1)(x^3+x^2+1)$.（$x^3+x+1$，$x^3+x^2+1$ 在 $\mathbb{Z}_3$ 中没有根，所以不可约）

笔记 第二小问中的两个三次因式其实不难发现. 我们已经在前面的练习中寻找了所有 $\mathbb{Z}_2$ 上的不可约多项式，由于 $x^6+x^5+x^4+x^3+x^2+x+1$ 为六次，从而我们只需将 $\mathbb{Z}_2$ 上的不超过 3 次的不可约多项式逐个验证即可.

练习 4.37 在 $\mathbb{Z}_2$ 上分解因式：$x^{16}-x$.

解

$$\begin{aligned}x^{16}-x&=x(x^{15}-1)\\&=x(x^5-1)((x^5)^2+x^5+1)\\&=x(x-1)(x^4+x^3+x^2+x+1)((x^5)^2+x^5+1)\\&=x(x-1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^8+x^7+x^5+x^4+x^3+x+1)\\&=x(x-1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)\\&=x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)\end{aligned}$$

笔记 请读者参考 3.4 节的练习 3.29.

进一步可以发现，$x^{16}-x$ 是 $\mathbb{Z}_2$ 上所有不可约多项式的乘积.

练习 4.38 证明：$d|n$，当且仅当 $(x^d-1)|(x^n-1)$. 其中 $d,n\in\mathbb{Z}_+$

证明 一方面，若 $d|n$，则存在正整数 k，有 $n=dk$. 由乘法公式

$$t^k-1=(t-1)(t^{k-1}+\cdots+1)$$

取 $t=x^d$ 就有

$$x^dk-1=(x^d-1)(x^{d(k-1)}+x^{d(k-2)}+\cdots+1)$$

从而 $(x^d-1)|(x^n-1)$.

另一方面，假设 $(x^d-1)|(x^n-1)$. 由带余除法，存在 q,r，使得

$$n=qd+r$$

其中 $r\in\{0,\cdots,d-1\}$.

我们有

$$\begin{aligned}x^n-1&=x^{qd+r}-1\\&=(x^{qd+r}-x^{(q-1)d+r})+(x^{(q-1)d+r}-x^{(q-2)d+r})+\cdots+(x^r-1)\\&=(x^d-1)(x^{(q-1)d+r}+\cdots+x^r)+(x^r-1)\end{aligned}$$

由于 $(x^d-1)|(x^n-1)$，所以 $(x^d-1)|(x^r-1)$. 而 $r<d$，所以只能有 $x^r-1=0$，即 $r=0$. 于是 $n=qd$，即 $d|n$.

综上，原命题成立.

练习 4.39 给出域 $\mathbb{Z}_3[x]/(x^2+x+2)$ 到域 $\mathbb{Z}_3[x]/(x^2+2x+2)$ 的一个同构.

解 定义映射：

$$\begin{aligned}\varphi:\mathbb{Z}_3[x]/(x^2+x+2)&\to\mathbb{Z}_3[x]/(x^2+2x+2)\\\overline{f(x)}&\mapsto\overline{f(x+2)}\end{aligned}$$

下证：φ 是域同构.

1. (保持加法)：对任意的 $f,g\in\mathbb{Z}_3[x]$，有

$$\begin{aligned}\varphi(\overline{f(x)})+\varphi(\overline{g(x)})&=\overline{f(x+2)}+\overline{g(x+2)}\\&=\overline{f(x+2)+g(x+2)}\\&=\overline{(f+g)(x+2)}\\&=\varphi(\overline{(f+g)(x)})\\&=\varphi(\overline{f(x)+g(x)})\\&=\varphi(\overline{f(x)}+\overline{g(x)})\end{aligned}$$

2. (保持乘法)：对任意的 $f,g\in\mathbb{Z}_3[x]$，有

$$\begin{aligned}\varphi(\overline{f(x)})\cdot\varphi(\overline{g(x)})&=\overline{f(x+2)}\cdot\overline{g(x+2)}\\&=\overline{f(x+2)\cdot g(x+2)}\\&=\overline{(f\cdot g)(x+2)}\\&=\varphi(\overline{(f\cdot g)(x)})\\&=\varphi(\overline{f(x)\cdot g(x)})\\&=\varphi(\overline{f(x)}\cdot\overline{g(x)})\end{aligned}$$

3. (保持乘法幺元)：根据对应关系，我们有

$$\varphi(\bar{1})=\bar{1}$$

综上，φ 是环同态. 再求 φ 的核：

$$\begin{aligned}\ker\varphi&=\{\overline{f(x)}\in\mathbb{Z}_3[x]/(x^2+x+2):f(x+2)\in(x^2+2x+2)\}\\&=\{\overline{f(x)}\in\mathbb{Z}_3[x]/(x^2+x+2):f(t)\in((t-2)^2+2(t-2)+2)\}\quad(t:=x+2)\\&=\{\overline{f(x)}\in\mathbb{Z}_3[x]/(x^2+x+2):f(t)\in(t^2+t+2)\}\\&=\{\overline{f(x)}=\bar{0}\in\mathbb{Z}_3[x]/(x^2+x+2)\}\\&=\{\bar{0}\}\end{aligned}$$

从而 φ 为环同构，即为域同构.

练习 4.40* 证明：有限域 $F=\mathbb{Z}_{p^n}$ 上的没有四次幂扩张. 【四次幂扩张的定义，请见第二节 “练习 5.16”】

笔记 所谓 F 上的四次幂扩张，指的是 $F(\sqrt{d_1},\sqrt{d_2})/F$，其中 $d_1,d_2\in F$，且 d_1,d_2,d_1d_2 均不为 F 中的平方. (由此该扩张的维数为 4.)

解

1. 若 $p=2$，我们证明：每个元素都是平方.
   首先，$0=0^2$，为平方.
   以下考虑 $F^\times$ 中的元素，我们知道存在一个乘法生成元 u，使得 $F^\times=\langle u\mid u^{2^n-1}=1\rangle$. 于是所有非零元都可表示为 $u^i,i\in\{0,\cdots,2^n-2\}$.
   若 $i=2k$，则 $u^i=(u^k)^2$ 为平方；若 $i=2k+1$，则 $u^i=u^{2k+1}\cdot u^{2^n-1}=u^{2(k+n)}=(u^{k+n})^2$ 也为平方，命题得证.
2. 以下考虑素数 p 为奇数的情形. 我们证明：若 a,b 不是 F 中的平方，则 ab 必为 F 中的平方.
   首先，$0=0^2$，为平方.
   以下考虑 $F^\times$ 中的元素，我们知道存在一个乘法生成元 u，使得 $F^\times=\langle u\mid u^{p^n-1}=1\rangle$. 于是所有非零元都可表示为 $u^i,i\in\{0,\cdots,p^n-2\}$. 从而有 $a=u^k,b=u^j$.
   因为 a,b 不为 F 中的平方，从而 k,j 均为奇数，且 u 不为 F 中的平方，不妨设 $k=2k'+1,j=2j'-1$. (k,j 为偶数时，a,b 显然为平方；k,j 为奇数时，$a=(u^{k'})^2u$，从而要求 u 也不能为平方数) 于是 $ab=u^{2k'+2j'}=(u^{k'+j'})^2$，为 F 中的平方，命题得证.

综上，域 F 上不可能有四次幂扩张.

练习 4.41* 设 $\mathbb{Q}(\sqrt{D_1},\sqrt{D_2})/\mathbb{Q}$ 是一个四次幂扩张，其中 D_1,D_2 是整数. 令 $\theta=a+b\sqrt{D_1}+c\sqrt{D_2}+d\sqrt{D_1D_2}$，其中 a,b,c,d 为整数，且 $\mathbb{Q}(\sqrt{D_1},\sqrt{D_2})=\mathbb{Q}(\theta)$，证明：

1. θ 在 $\mathbb{Q}$ 上的最小多项式 $f(x)$ 为 $\mathbb{Q}$ 上的 4 次不可约多项式.
2. $f(x)$ 模任意素数 p 后，在 $\mathbb{F}_p$ 上可约.

解

1. 由四次幂扩张的定义即证.
2. $f(x)$ 在模 p 之后，实际上就称为了 $\mathbb{F}_p[x]$ 的元素（不妨记为 $\bar{f}(x)$）. 且我们有 $\mathbb{F}_p(\sqrt{D_1},\sqrt{D_2})=\mathbb{F}_p(\theta)$. 若 $\bar{f}(x)$ 在 $\mathbb{F}_p$ 上不可约，则 $\mathbb{F}_p(\theta)/\mathbb{F}_p$ 的扩张维数依旧是 4，(TBD)

4.4 分裂域

本节均设 F,E,K 为域.

4.4.1 知识要点

（一）分裂域

1. 分裂域：$f\in F[x]$. 称 F 的扩域 E 是 f 在 F 上的分裂域，若 E 满足：
   (a). $f(x)=c(x-a_1)\cdots(x-a_n)$，所有的 $a_i\in E$，且 c 是 f 的首项系数；
   (b). E 是使得 f 在其上有 n 个根的最小的 F 的扩域.
2. (分裂域的存在性)：对任意的域 F 和多项式 $f\in F[x]$，总是存在一个 f 在 F 上的分裂域.

（二）域同构的延拓

1. (同构在根上的延拓)：设 $\varphi:F\to F'$ 是域同构，$E/F,E'/F'$ 都是域的扩张. $r\in E$ 是 F 上的代数元素，其最小多项式为 $f\in F[x]$，则
   (a). φ 可延拓成域的嵌入 $\psi:F(r)\to E'$，当且仅当 $g:=\varphi(f)$ 在 E' 内有根.
   (b). φ 的这种延拓的个数，等于 g 在 E' 中不同根的个数.
2. (分裂域的同构)：设 $\varphi:F\to F'$ 是域同构，$f\in F[x]$. E 是 f 在 F 上的分裂域，E' 是 $g:=\varphi(f)$ 在 F' 上的分裂域. 则
   (a). φ 可延拓为域同构 $\psi:E\to E'$.
   (b). 设 r 为这种延拓的个数，则 $1\leqslant r\leqslant[E:F]$.
   (c). 若 g 在 E' 内无重根，则 $r=[E:F]$.
3. (分裂域的唯一性)：对任意的域 K 和多项式 $f\in K[x]$，f 在 K 上的分裂域互相同构.

（三）代数闭域

1. 域 F 的代数闭域 $\bar{F}$：$\bar{F}/F$ 是代数扩张，且对任意 $f\in F[x]$，$f=0$ 的根都在 $\bar{F}$ 内.
2. 代数封闭：域 K 是代数封闭的，如果对任意的 $f\in K[x]$，$f=0$ 都有一根在 K 内.
3. (代数闭域总是代数封闭的)：设 $\bar{F}$ 是域 F 的代数闭域，则 $\bar{F}$ 是代数封闭的.
4. (存在性)：对任意域 F，存在一个包含 F 的代数封闭的域 K.
5. (唯一性)：设 K 是代数封闭的，F 是 K 的子域. 则 F 的所有代数元素构成的域 $\bar{F}$ 是 F 的一个代数闭域，且 F 的代数闭域在同构意义下唯一.

4.4.2 从定理证明中学解题

（一）分裂域的性质

分裂域的思想来源，是我们熟悉的单代数扩张. 给定域 K 和一个多项式 $f \in K[x]$，如果 $f(x)=0$ 在 K 的某个扩域上有根 $u \notin K$，我们可以在 K 上找到 u 对应的最小多项式 $p(x)$（此时必然有 $p|f$），然后构造域 $K(u) \simeq K[x]/(p(x))$. 此时 $f(x)=0$ 会有更多的根包含在新构造的域中. 由于根的个数总是有限的，所以最终我们会得到一个 K 的扩域，包含 $f(x)=0$ 的所有根. 将这一过程利用数学归纳法表述出来，实际上就证明了分裂域的存在性.

问题 4.11 对任意的域 K 和多项式 $f \in K[x]$，总是存在一个 f 在 K 上的分裂域 E.

证明 对 f 的次数做归纳. 当 $\deg f=1$ 时，则取 $E=F$ 即可.

假设 $\deg f \leqslant n$ 时命题均成立（n 是某个正整数）. 当 $\deg f=n+1$ 时：

1. 若 f 在 $K[x]$ 中可约，则 $f=gh$，并且由于 K 是域，所以 g,h 都不是常数，从而 $\deg g, \deg h \leqslant n$. 由归纳假设，存在 g 在 K 上的分裂域 E_1；且存在 h 在 E_1 上的分裂域 E_2，从而 E_2 是 f 在 K 上的分裂域.
2. 若 f 在 $K[x]$ 中不可约，则令 $E_1=K[x]/(f(x))$，于是 F 自然嵌入域 E_1，且 $f(x)$ 有一根 $a_1:=\bar{x} \in E_1$，从而在 E_1 中 $f=(x-a_1)g$，其中 $\deg g=n$. 利用归纳假设，存在 g 在 E_1 上的分裂域 E_2，从而 E_2 是 f 在 K 上的分裂域.

综上，原命题得证.

笔记 证明过程中对于不可约多项式的处理是该问题的本质，即利用扩域 $E_1=K[x]/(f(x))$ 产生 $f(x)=0$ 的一根（也就是 $\bar{x} \in K[x]/(f(x))$），进而产生 $f(t) \in E_1[t]$ 的一个因式 $t-\bar{x}$，这就达到了降次的目的.

我们也可以从另一个角度理解分裂域. 由分裂域的存在性，我们总能找到包含 $f=0$ 的全部根的 K 的扩域 F. 记这些根为 $x_1,\cdots,x_m$，则包含 K 和 $x_1,\cdots,x_m$ 的最小的 F 的子域，是代数扩域 $K(x_1,\cdots,x_n)$. 而 $K(x_1,\cdots,x_n)$ 显然是 f 在 K 上的分裂域. 这样我们就得到了一个求 f 在 K 上的分裂域的方法. 这一点看起来是反逻辑的：在分裂域存在性的证明中，我们是先构造的分裂域，在构造的过程中实际上把 $f=0$ 的根也构造出来了. 从而是先有的分裂域，再有的（全部的）根. 然而这里分裂域的构造方法，是先有的根，再有的分裂域. 在实际应用中，这种情况非常常见. 比如，对于 $f \in \mathbb{Q}[x]$，我们总能知道 $f=0$ 在 $\mathbb{C}$ 内的所有根，然后再构造 f 在 $\mathbb{Q}$ 上的分裂域.

（二）域同构的延拓

问题 4.12（同构在根上的延拓）：设 $\varphi: F \to F'$ 是域同构，$E/F, E'/F'$ 都是域的扩张. $r \in E$ 是 F 上的代数元素，其最小多项式为 $f \in F[x]$，则

1. φ 可延拓成域的嵌入 $\psi: F(r) \to E'$，当且仅当 $g:=\varphi(f)$ 在 E' 内有根.
2. φ 的这种延拓的个数，等于 g 在 E' 中不同根的个数.

证明

1. 记

$$f=\sum_{i=1}^{n} a_i x^i.$$

一方面，设 φ 可延拓成域的嵌入 $\psi: F(r) \to E'$，从而

$$\begin{aligned} 0 &= \psi(0) \\ &= \psi(f(r)) \\ &= \psi\left(\sum_{i=1}^{n} a_i r^i\right) \\ &= \sum_{i=1}^{n} \psi(a_i)\psi(r)^i \\ &= \sum_{i=1}^{n} \varphi(a_i)\psi(r)^i \\ &= g(\psi(r)) \end{aligned}$$

即 g 在 E' 内有根 $\psi(r)$.

另一方面，假设 g 在 E' 内有根 d. 定义映射

$$\begin{aligned} \eta: F(r) &\to E' \\ f(r) &\mapsto \varphi(f)(d). \end{aligned}$$

任取 $F(r)$ 中的两个元素 $h(r), i(r)$，我们有：

$$\begin{aligned} \eta(h(r)+i(r)) &= \eta((h+i)(r)) \\ &= \varphi(h+i)(d) \\ &= \varphi(h)(d)+\varphi(i)(d) \quad (\varphi: F[x] \to F'[x]\text{是环同构}) \\ &= \eta(h(r))+\eta(i(r)) \end{aligned}$$

$$\begin{aligned} \eta(h(r)i(r)) &= \eta((hi)(r)) \\ &= \varphi(hi)(d) \\ &= (\varphi(h)\varphi(i))(d) \\ &= \varphi(h)(d)\cdot\varphi(i)(d) \\ &= \eta(h(r))\eta(i(r)) \end{aligned}$$

$$\eta(1) = \varphi(1) = 1$$

从而 η 是域同态. 注意到 η 在 F 上的限制为域同构 φ，所以 η 不是零映射，从而作为域同态的 η 只能为嵌入映射.

2. 对于 g 在 E 中的两个不同根 d, d'，分别存在域同态：

$$\begin{aligned} \eta: F(r) &\to E' \\ f(r) &\mapsto \varphi(f)(d) \end{aligned}$$

和

$$\begin{aligned} \eta': F(r) &\to E' \\ f(r) &\mapsto \varphi(f)(d') \end{aligned}$$

由于 $\eta(r) = d \neq d' = \eta'(r)$，所以 η, η' 是不同的映射. 从而 φ 的延拓个数，等于 g 在 E' 中不同根的个数.

笔记 以上证明过程也可以证明：若取 E, E' 是 F, F' 的分裂域，则 φ 的延拓 ψ 总是将不可约多项式 f 的根，映到 $g := \varphi(f)$ 的根. 换句话说，g 的不同根的个数，决定了延拓的个数.

✍ **练习 4.42** 设 f 是 $F[x]$ 中的不可约多项式，E 为 f 在 F 上的分裂域，$r\in E$ 是 f 的一根. 证明：存在域的嵌入 $\psi:F(r)\to E$，使得 ψ 在 F 上是恒等映射. 且这种嵌入的个数，等于 f 在 E 中不同根的个数.

注 提示：取前一定理中的 $F'=F,E'=E$，$\varphi=id$. 即可.

问题 4.13（分裂域的同构）：设 $\varphi:F\to F',a\mapsto\bar{a}$ 是域同构，$f\in F[x]$. E 是 f 在 F 上的分裂域，E' 是 $g:=\varphi(f)$ 在 F' 上的分裂域. 则

1. φ 可延拓为域同构 $\psi:E\to E'$.
2. 设 r 为这种延拓的个数，则 $1\leqslant r\leqslant[E:F]$.
3. 若 g 在 E' 内无重根（也就是 f 在 E 内无重根），则 $r=[E:F]$.

证明 对 $[E:F]$ 做归纳. 当 $[E:F]=1$ 时，$E=F$，从而 f 在 $F[x]$ 内只有一次因式

$$f=a(x-x_1)\cdots(x-x_m)$$

其中 $a,x_i\in F$，于是

$$g=\varphi(f)=\bar{a}(x-\overline{x_1})\cdots(x-\overline{x_m})$$

从而 $E'=F'(\overline{x_1},\cdots,\overline{x_m})=F'$，$\psi$ 恰好等于 φ，即 $r=1$.

假设当 $[E:F]<n$ 时原命题均成立. 当 $[E:F]=n>1$ 时，f 在 $F[x]$ 内必有超过一次的不可约因子，不妨记为 p，从而 $q:=\varphi(p)\in F'[x]$ 是 g 的超过一次的不可约因子.

设 $a\in E$ 是 p 的一个根，则对任意满足题设的 φ 的延拓 $\psi:E\to E'$，ψ 在 $F(a)$ 上的限制可得域同构 $\tau:F(a)\to F'(b)$，其中 b 为 q 在 E' 内的某个根. 由前一定理可得，该同构的个数等于 q 在 E' 内不同的根的个数. 由于 $\deg q=\deg p=[F(a):F]$，所以该同构同态的个数不超过 $[F(a):F]$.

由于 E 也是 f 在 $F(a)$ 上的分裂域，E' 是 g 在 $F'(b)$ 上的分裂域，且 $[E:F(a)]<[E:F]=n$，所以由归纳假设，τ 可延拓为域同构 ψ，且延拓个数不小于 1，不超过 $[E:F(a)]$.

由前述，φ 延拓到 σ 的过程，被分成了两个阶段，第一阶段从 φ 延拓到 τ，延拓个数 $r_1\leqslant[F(a):F]$，第二阶段从任意 τ 延拓到 ψ，延拓个数 $r_2\leqslant[E:F(a)]$. 于是，根据乘法原理，φ 到 σ 的延拓个数 $r\leqslant[E:F(a)][F(a):F]=[E:F]$. $r=[E:F]$ 时，当且仅当 $r_1=[F(a):F]$，且每个 $r_2=[E:F(a)]$. 前一个等号的成立条件，是 q 无重根，后一个等号的成立条件，是 g 无重根，从而 $r=[E:F]$，当且仅当 g 无重根. 原命题成立.

综上，原命题成立.

✍ **练习 4.43** 设 $f\in F[x]$. E 是 f 在 F 上的分裂域，则存在域同构 $\psi:E\to E$，使得 ψ 在 F 上是恒等映射. 记 r 为可能的 ψ 的个数，则 $1\leqslant r\leqslant[E:F]$. 进一步地，若 f 在 E 内无重根，则 $r=[E:F]$.

注 提示：取前一定理中的 $F'=F,E'=E$，$\varphi=id$. 即可.

在“Galois 扩张”一节，我们将用更简洁的数学语言重新叙述此定理.

（三）代数闭域

虽然我们到此才接触到代数闭域这个概念，但是实际上从我们学单代数扩张开始，就在应用着这个概念. 每当我们需要考察不可约多项式 $f\in K[x]$，且要取 $f=0$ 的一个根时，我们就需要请出“域 F 的某个扩域”这样一个含混不清，又很不讲道理的说法. 众所周知，数学中，是不能允许这样奇葩的描述存在的，所以就有了“代数闭域”.

代数闭域要满足两个条件：首先是域 F 的代数扩展，其次他要包含所有方程 $f=0$ 的根，其中 $f\in F[x]$. 第二个条件也可以等价地描述为：代数闭域包含了 F 上的所有代数元素. 显然，代数闭域是分裂域地进一步延伸，分裂域只针对一个多项式，而代数闭域针对所有的多项式. 同时，由代数闭域引申出一个概念：代数封闭.

代数封闭的要求看起来是不高的：对每个多项式 $f\in K[x]$，$f=0$ 有一根在 K 中即可. 但是实际上，要求有一个，也就要求了全部. 这是因为当 $f=0$ 有一根 $\alpha\in K$ 时，f 在 $K[x]$ 内就有一个因式 $x-\alpha$，从而 $f/(x-\alpha)\in k[x]$. 进一步考察 $f/(x-\alpha)=0$，由代数封闭性，该方程也得有一根 β 在 K 内，而 β 也是 $f=0$ 的另一个根. 以此类推，最终 $f=0$ 的所有根都必须在 K 内.

问题 4.14（代数闭域总是代数封闭的）：设 $\bar{F}$ 是域 F 的代数闭域，则 $\bar{F}$ 是代数封闭的.

证明 设 $f \in \bar{F}[x]$，α 是 $f=0$ 的一根. 从而 $\bar{F}(\alpha)/\bar{F}$ 是代数扩张. 由于 $\bar{F}/F$ 是代数扩张，所以 $\bar{F}(\alpha)/F$ 是代数扩张. 由此可得，α 是 F 上的代数元素，结合代数闭域的定义可知，$\alpha \in \bar{F}$.

注 由此命题立即得：$\overline{\bar{F}} = \bar{F}$.

我们回到代数闭域上来. 我们首先试图找到一个包含给定域的代数封闭的域，而这一点依赖于极大理想的存在性，我们将其证明放到本节的附录中，供有兴趣的读者参考. 然后我们再将这个域缩小，这样就得到了给定域的代数闭域.

问题 4.15 （唯一性）：设 K 是代数封闭的，F 是 K 的子域. 则 F 的所有代数元素构成的域 $\bar{F}$ 是 F 的一个代数闭域，且 F 的代数闭域在同构意义下唯一.

证明 由 $\bar{F}$ 的定义，$\bar{F}/F$ 是代数扩张，且对任意的 $f \in F[x]$，$f=0$ 的根都是 F 的代数元素，于是都在 $\bar{F}$ 内，从而 $\bar{F}$ 是 F 的代数闭域.

代数闭域的唯一性的证明，与分裂域的唯一性的证明几乎一致，此处从略.

4.4.3 典型例题

例题 4.8 设 $f(x)=x^4-2 \in \mathbb{Q}[x]$. 试确定 f 在 $\mathbb{Q}$ 上的分裂域，以及该分裂域相对于 $\mathbb{Q}$ 的次数.

注 分析：由代数基本定理可知，$\mathbb{C}[x]$ 中的元素总能在 $\mathbb{C}$ 上找到根. 所以我们讨论此类问题时，往往已经知道了根的形式，主要是确定扩域中需要扩哪些元素.

证明 在 $\mathbb{C}$ 上，我们有

$$\begin{aligned} f(x) &= (x^2+\sqrt{2})(x^2-\sqrt{2}) \\ &= (x+\sqrt{-1}\sqrt[4]{2})(x-\sqrt{-1}\sqrt[4]{2})(x+\sqrt[4]{2})(x-\sqrt[4]{2}) \\ &= (x+ab)(x-ab)(x+b)(x-b) \end{aligned}$$

其中 $a=\sqrt{-1}, b=\sqrt[4]{2}$. 根据定义我们有 f 在 $\mathbb{Q}$ 上的分裂域为 $\mathbb{Q}(ab,-ab,b,-b)=\mathbb{Q}(ab,b)$. 而我们也很容易证明：$\mathbb{Q}(ab,b)=\mathbb{Q}(a,b)$（因为 $a=ab/b$）. 所以所求的分裂域即为 $\mathbb{Q}(a,b)=\mathbb{Q}(\sqrt{-1},\sqrt[4]{2})$.

注意到 $\sqrt[4]{2}$ 在 $\mathbb{Q}$ 上的最小多项式即是 $f:=x^4-2$（因为 f 不可约），从而

$$[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=\deg f=4$$

进一步地，$\sqrt{-1}$ 在 $\mathbb{Q}(\sqrt[4]{2})$ 上的最小多项式是 $g:=x^2+1$，所以

$$[\mathbb{Q}(\sqrt[4]{2})(\sqrt{-1}):\mathbb{Q}(\sqrt[4]{2})]=\deg g=2$$

于是：

$$[\mathbb{Q}(\sqrt{-1},\sqrt[4]{2}):\mathbb{Q}]=[\mathbb{Q}(\sqrt[4]{2})(\sqrt{-1}):\mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=8.$$

✍ **练习 4.44** 设 $f(x)=x^4+2 \in \mathbb{Q}[x]$. 试确定 f 在 $\mathbb{Q}$ 上的分裂域，以及该分裂域相对于 $\mathbb{Q}$ 的次数.

4.4.4 习题

✍ **练习 4.45** 设 $f(x)=x^4+x^2+1 \in \mathbb{Q}[x]$. 试确定 f 在 $\mathbb{Q}$ 上的分裂域，以及该分裂域相对于 $\mathbb{Q}$ 的次数.

注 提示：设 $\zeta_3=e^{\frac{2\pi i}{3}}$（三次单位根），$\zeta_6=e^{\frac{1\pi i}{3}}$（六次单位根），则

$$\begin{aligned} f(x) &= (x^2-\zeta_3)(x^2-\zeta_3^2) \\ &= (x+\zeta_6)(x-\zeta_6)(x+\zeta_3)(x-\zeta_3) \end{aligned}$$

✍ **练习 4.46** 设 $f(x)=x^6-4 \in \mathbb{Q}[x]$. 试确定 f 在 $\mathbb{Q}$ 上的分裂域，以及该分裂域相对于 $\mathbb{Q}$ 的次数.

✍ **练习 4.47** 设 F 是域，$f \in F[x]$. $\deg f=n$，f 在 F 上的分裂域为 E. 证明：$[E:F] \leqslant n!$.

注 提示：考虑 f 在 F 的代数扩域中的根，其中不同的根至多有 n 个，不妨记为 $x_1,\cdots,x_n$.

对于 x_1，x_1 在 F 上的最小多项式，一定是 f 的因子，所以其次数必然不超过 n，即 $[F(x_1):F] \leqslant n$.

进一步，f 在 $F(x_1)$ 上至少有一个一次的因式 $(x-x_1)$，所以 x_2 在 $F(x_1)$ 上的最小多项式，一定是 $f/(x-x_1)$ 的因子，所以其次数必然不超过 $n-1$，即 $[F(x_1,x_2):F(x_1)]\leqslant n-1$.

重复上述过程直至所有根讨论完毕，此时可得：

$$\begin{aligned}[F(a_1,\cdots,a_n):F] &= [F(a_1,\cdots,a_n):F(a_1,\cdots,a_{n-1})]\cdots[F(a_1):F]\\ &\leqslant 1\cdots n\\ &= n!\end{aligned}$$

✍ **练习 4.48** 设 F 是域，$f\in F[x]$. $\deg f=n$，f 在 F 上的分裂域为 E. 证明：$[E:F]|n!$.

证明 对 n 做归纳. 当 $n=1$ 时，显然 $E=F$，于是 $[E:F]=1$，$n!=1$，从而 $[E:F]|n!$，原命题成立.

假设 $[E:F]\leqslant k$ 时原命题均成立. 当 $[E:F]=k+1$ 时：

1. 若 f 在 F 上可约，则有 $f=gh$，其中 g,h 为 f 的真因子. 记 $\deg g=l$，则 $\deg h=k+1-l$. 由归纳假设，g 在 F 上的分裂域

✍ **练习 4.49*** 设 K/F 是域的有限扩张. 证明：K 是 F 的一个分裂域（即存在 $h\in F[x]$，使得 F 是 h 在 K 上的分裂域），当且仅当对于 $F[x]$ 中的任意不可约多项式 f，若 $f=0$ 至少有一根在 K 内，则 $f=0$ 的所有根都在 K 内（称作 f 在 K 中完全分裂）.

✍ **练习 4.50*** 证明：代数闭域必为无限域.

4.5 可分扩张

本节均设 K 是域.

4.5.1 知识要点

（一）多项式的单根与重根

1. 单根、重根：$f\in K[x]$. 在 f 在 K 上的分裂域 F 内，f 可被分解为一次因式的乘积
$$f(x)=\prod_{i=1}^{k}(x-a_i)^{n_i}$$
其中 $a_1,\cdots,a_k\in F$ 是不同的元素，任意 $n_i\in\mathbb{Z}_+$.
   (a). 单根：若 $n_i=1$，则称 a_i 是 f 的单根.
   (b). 重根：若 $n_i\geqslant 2$，则称 a_i 是 f 的重根.
   (c). 重数：n_i 称为根 a_i 的重数.
2. （形式）导数：设
$$f=\sum_{i=0}^{n}a_ix^i\in K[x]$$
则定义 f 的（形式）导数为
$$D_xf=\sum_{i=0}^{n-1}(i+1)a_{i+1}x^i.$$
3. （导数的基本性质）：设 $f,g\in K[x]$，$c\in K$，则
   (a). $D_x(f+g)=D_xf+D_xg$;
   (b). $D_x(cf)=cD_xf$;
   (c). $D_x(fg)=f(D_xg)+(D_xf)g$.
4. 可分多项式：域 K 上的多项式 f 是可分的，如果它（在 f 在 K 上的分裂域内）没有重根.（反之被称为不可分的）

5. (重根的判定)：$f \in K[x]$ 有重根 a，当且仅当 a 是 $D_x f$ 的根. 也就是说，设 a 在 K 上的最小多项式为 $m_a(x)$，则 f 和 $D_x f$ 有公因子 $m_a(x)$.
   特别的，f 是可分的，当且仅当 $\gcd(f, D_x f) = 1$.

(二) 可分多项式与不可约多项式的关系

1. (不可约多项式的重根)：设 K 是域，$f \in K[x]$ 不可约.
   (a). 若 $\operatorname{char} K = 0$，则 f 无重根.(从而是可分的)
   (b). 若 $\operatorname{char} K = p$，则 f 有重根，当且仅当存在 $g \in K[x]$，使得 $f(x) = g(x^p)$.
2. 完全域：特征为 p 的域 K 是完全域，如果 $K = K^p$.(记号见第一节) 特征为 0 的域也定义为完全域.
3. (完全域的可分多项式)：设 K 是完全域，则
   (a). 不可约多项式都是可分的.
   (b). f 是可分的，当且仅当 f 是不同的不可约多项式的积.
4. (可分次数)：设 K 是特征 p 域，$f \in K[x]$ 是不可约多项式，则存在唯一的自然数 k 和唯一的不可约可分多项式 $f_{sep} \in K[x]$，使得 $f(x) = f_{sep}(x^{p^k})$.
   f 的可分次数：$\deg f_{sep}$，记为 $\deg_s f$.
   f 的不可分次数：p^k，记为 $\deg_i f$.
   两者的关系为：$\deg f = \deg_s f \cdot \deg_i f$.

(三) 可分扩张

1. 可分(代数)扩张：K/F 是可分扩张，如果 K 中的每个元素，都是 F 上的某个可分多项式的根.
2. (可分扩张的等价定义)：K/F 是可分扩张，当且仅当对 K 中每个元素在 F 上的最小多项式 f，f 是可分的.
3. (完全域上的扩张)：完全域上的有限扩张都是可分扩张.

4.5.2 知识要点解读

(一) 可分多项式

可分多项式的概念看似简单，实际上有一些容易产生错误理解的细节.

首先，我们给定一个多项式 f，必须要给定他所在的多项式环 $K[x]$(也就是他的系数所在的域 K). 那么，当我们讨论 f 的根 a 的时候，a 又是哪里的元素呢？一种错误的理解是，我们只讨论位于 K 内的根. 实际上我们讨论的是位于 f 在 K 上的分裂域内的根.(读者可以回顾 f 的单根、重根的定义)

第二，除了本书给出的定义外，还有一种可分多项式的定义：f 在 $K[x]$ 中的每个不可约因式均没有重根(冯克勤《近世代数引论》即是此种定义). 两种定义是有冲突的.

例题 4.9 考虑 $f = (x-1)^2 \in \mathbb{Q}[x]$. 如果根据本书采用的定义，$f$ 是不可分的，因为有重根 1. 如果采用另一版本的定义，则 f 是可分的，因为它的所有不可约因式 $x-1$ 均没有重根.

当然，对于不可约多项式而言，两种定义是一致的. 由于不可约多项式的地位远超可约多项式，因此读者不必过于在意两种定义的区别.

第三，也是我们前面所强调的，想要给出完整的 f，必须给出他所在的多项式环. f 的可分性，与其所在环是直接关联的.

例题 4.10 考虑 $f = x^2 - 1$. 如果 $f \in \mathbb{Q}[x]$，则 f 是可分多项式，因为它的根为 ± 1，无重根.

如果 $f \in \mathbb{Z}_2[x]$，则 f 是不可分的，因为 $f = (x-1)^2$，即 f 有重根 1.

回到可分多项式的定义上，我们借用分析学中的导数，研究多项式的重根特性. 需要注意的是，我们只是利用了导数的形式(从而我们称之为形式导数)，并没有在多项式环上定义拓扑，从而也不存在取极限的过程.

形式导数完全保留了导数的基本性质，没有违反我们认知的性质. 利用形式导数，可以方便的判定多项式有无重根.

问题 4.16（重根的判定）：$f \in K[x]$ 有重根 a，当且仅当 a 是 $D_x f$ 的根.

特别的，f 是可分的，当且仅当 $\gcd(f, D_x f) = 1$.

证明 一方面，设 a 是 f 的 n 重根（$n \geqslant 2$），则在 f 的分裂域中有

$$f(x) = (x-a)^n g(x).$$

于是 f 的形式导数为：

$$D_x f(x) = n(x-a)^{n-1} g(x) + (x-a)^n D_x g(x)$$

从而 a 是 $D_x f$ 的根.

另一方面，设 a 是 f 和 $D_x f$ 的根，则在 f 的分裂域中有

$$f(x) = (x-a)h(x)$$

于是 f 的形式导数为：

$$D_x f(x) = h(x) + (x-a)D_x h(x)$$

由于 a 是 $D_x f$ 的根，所以：

$$0 = D_x f(a) = h(a)$$

即 h 有根 a. 从而 f 有重根 a.

笔记 请注意，我们不能说，f 有重根 a，当且仅当 f 和 $D_x f$ 有公因子 $x-a$. 因为 $f, D_x f$ 都是 $K[x]$ 中的元素，而 $x-a$ 只能说是 f 在 K 上的分裂域中的元素. 虽然我们不能使用 $x-a$，但是我们可以替代的使用最小多项式 $m_a(x)$. 这一点在单代数扩域的部分已经详细讨论了.

（二）可分多项式与不可约多项式的关系

借助于形式导数判别法，不可约多项式的可分性是容易判定的.

问题 4.17（不可约多项式的重根）：设 K 是域，$f \in K[x]$ 不可约，$\deg f := n \geqslant 1$.

1. 若 $\operatorname{char} K = 0$，则 f 无重根.（从而是可分的）
2. 若 $\operatorname{char} K = p$，则 f 有重根，当且仅当存在 $g \in K[x]$，使得 $f(x) = g(x^p)$.

证明

1. 由于 f 是不可约的，假设 f 有重根，则 $(D_x f, f) \neq 1$，于是只能有 $(D_x f, f) = f$，也就是 $f | D_x f$. 然而 $\deg D_x f = n - 1 < \deg f$，于是只能有 $D_x f = 0$. 从而 $\deg f = 0$，与 $\deg f \geqslant 1$ 矛盾！从而 f 无重根.
2. 与第一小问的证明相同，f 有重根，当且仅当 $D_x f = 0$. 记

$$f = \sum_{i=0}^{n} a_i x^i$$

于是

$$D_x f = \sum_{i=1}^{n} i a_i x^{i-1}$$

$D_x f = 0$，当且仅当对任意的 $i \in \{1, \cdots, n\}$，$i a_i = 0$. 由于 K 为特征 p 域，所以若 $p | i$，则 $i a_i$ 自然为 0. 若 $p \nmid i$，则有 $a_i = 0$. 设 0 到 n 区间最大的 p 的倍数是 lp，则：

$$\begin{aligned} f &= \sum_{j=0}^{l} a_{jp} x^{jp} \\ &= g(x^p) \end{aligned}$$

其中令

$$g(x)=\sum_{j=0}^{l}a_{jp}x^j.$$

进一步的，任意多项式总是不可约多项式的乘积，我们自然希望，通过不可约多项式的可分性判定，构建任意多项式的可分性判定，这比利用定义或者利用形式导数判定可分性，更具有操作性. 这一问题的被分成两个部分加以解决，分割的标准是完全域.

完全域的定义看起来是很奇怪的，它把两种没有关系的域强行定义到了一起：满足 $K^p=K$ 的特征 p 域，以及特征 0 域. 促使他们结合的，正是不可约多项式.

问题 4.18 （完全域的可分多项式）：设 K 是完全域，则

1. 不可约多项式都是可分的.
2. f 是可分的，当且仅当 f 是不同的不可约多项式的积.

注 很显然，这一命题就是前一命题的直接推广.

证明

1. 对于特征 0 域，不可约多项式都是可分的.

   对于满足 $K=K^p$ 的特征 p 域 K，假设不可约多项式 $f\in K[x]$ 不可分，即 f 有重根，则存在 $g\in K[x]$，满足 $f(x)=g(x^p)$. 记

   $$g(x)=\sum_{j=0}^{l}a_jx^j.$$

   对于任意的 $a_j\in K=K^p$，存在 $b_j\in K$，使得 $a_j=b_j^p$，于是：

   $$\begin{aligned}f(x)&=g(x^p)\\&=\sum_{j=0}^{l}a_j(x^p)^j\\&=\sum_{j=0}^{l}b_j^p(x^j)^p\\&=(\sum_{j=0}^{l}b_jx^j)^p\quad(\text{利用}(a+b)^p=a^p+b^p)\end{aligned}$$

   此时 f 是可约多项式，这与 f 是不可约的矛盾！从而 f 必是可分多项式.

   综上，完全域中，不可约多项式均可分.
2. 首先，两个不相同的不可约多项式，必然没有相同的根，否则它们必有不相伴于 1 的公因子（即相同根的最小多项式），从而它们均可约，矛盾.

   其次，两个没有相同根的的不可约多项式，也必然是不相同的.

   因为 f 总可以被分解成不可约多项式的积，从而 f 可分，当且仅当 f 没有重根，当且仅当 f 的各不可约因子之间没有相同根（不可约因子自己没有重根），当且仅当各不可约因子不相同. 原命题得证.

在本章的第一节中，我们证明了有限 p 域满足 $K^p=K$，从而所有的有限域都是完全域. 于是，从特征以及是否有限的角度衡量，只有无限 p 域的可分多项式的形式还没有搞清楚. 我们先举一例，说明这样的域是存在的，且在这样的域上，前述命题并不成立.

例题 4.11 设有理函数域 $K:=\mathbb{Z}_p(t)$，其中 p 是素数，则 K 是无限 p 域.（请读者自证之）

考虑多项式 $f=x^p-t\in K[x]$，利用 Eisenstein 判别法（关于不可约元 t）可得，f 是不可约的. 进一步，存在 $g(x):=x-t\in K[x]$，使得 $f(x)=g(x^p)$，从而 f 有重根，是不可分的.

笔记 有理函数域 $\mathbb{Z}_p(t)$ 是我们已知的最简单的无限 p 域，也是最简单的非完全域.

前面的例子中，f 不可分，但是与之相关的 g 是可分的. 由此启发我们定义有限 p 域上不可约多项式的可分次数和不可分次数.

问题 4.19 （可分次数）：设 K 是特征 p 域，$f \in K[x]$ 是不可约多项式，则存在唯一的自然数 k 和唯一的不可约可分多项式 $f_{sep} \in K[x]$，使得 $f(x) = f_{sep}(x^{p^k})$.

证明 若 f 是可分多项式，则可取 $k = 0, f_{sep} = f$，原命题成立.

假设 f 是不可分的，则 f 有重根，于是存在 $f_1 \in K[x]$，使得 $f(x) = f_1(x^p)$. 进一步的，假设 f_1 仍然不可分，则存在 $f_2 \in K[x]$，使得 $f_1(x) = f_2(x^p)$，从而 $f(x) = f_2(x^{p^2})$.

1. 先证明：以上的过程不可能无限的进行下去. 换句话说，存在一个自然数 k，使得
$$f(x) = f_k(x^{p^k}).$$
因为 $f(x) = f_k(x^{p^k})$，考虑两侧多项式的次数可得 $\deg f = \deg f_k \cdot p^k \geqslant p^k$. 由于 f 的次数是确定的，所以 k 不可能取无限大，从而取 f_i 的过程只能进行有限次.
2. 再证明：假设取 f_i 的过程进行到第 k 次停止，则 f_k 是可分多项式，从而前述的 k 是唯一的. 假设 f_k 仍然是不可分的，则存在 $f_{k+1}(x) = f_k(x^p)$，从而取 f_i 过程没有在第 k 次停止，矛盾！从而 f_k 必然可分，且 k 唯一确定.
3. 最后证明：f_k 是不可约的. 假设 $f_k(x) = g(x)h(x)$，其中 g, h 都是真因子，则 $f(x) = g(x^{p^k})h(x^{p^k})$，从而 f 是可约的，这与 f 的不可约性矛盾！

综上，可取 $f_{sep} = f_k$，就有 $f(x) = f_{sep}(x^{p^k})$. 且由 k 的唯一性，可得 f_{sep} 的可约性.

笔记 这一命题告诉我们，无限 p 域上的对任意的不可约多项式 f，总可以找到一个与之对应的可分多项式 f_{sep}. 并且，f 可分，当且仅当 $f = f_{sep}$，当且仅当 $k = 0$，当且仅当 f 的不可分次数为 1，当且仅当 f 的可分次数为 f 的次数.

由于无限 p 域 K 上不可约多项式的可分性较为复杂，因此与完全域不同，K 上的可分多项式与不可约多项式之间没有办法建立一个很简明的对应关系.

例题 4.12 继续以有理函数域 $K := \mathbb{Z}_p(t)$ 为例，考虑其上的多项式 $f(x) = (x^{p^2} - t)(x^p - t)$. 由于 f 的两个因子都是不可分多项式，从而 f 不可分. 我们尝试拆解出 “f_{sep}”：
$$f(x) = f_1(x^p)$$
$$f_1(x) = (x^p - t)(x - t)$$
此时 f_1 不能够继续拆分 f_2 了，但是 f_1 仍然不可分，且 f_1 是可约的.

这一例子也说明，K 上不同的不可约多项式的乘积，仍然可能是不可分多项式.

（三）可分多项式与有限域

利用分裂域和可分多项式的性质，我们可以进一步深化对有限域的研究.

问题 4.20 （存在性和唯一性）：对任意的素数 p 和自然数 n，p^n 阶有限域必然存在，且（在同构意义下）唯一.

证明

1. 证明：$f := x^{p^n} - x \in \mathbb{Z}_p[x]$ 是可分多项式.

f 的形式导数为：
$$D_x f = p^n x^{p^n - 1} - 1$$
$$= -1$$
于是 $\gcd(f, D_x f)$ 只能等于 1，从而 f 没有重根，即 f 可分.

2. 证明：f 所有根的集合 K 是域，从而 f 在 $\mathbb{Z}_p$ 上的分裂域即是域 K.

因为 f 在 $\mathbb{Z}_p$ 上的分裂域 F 包含 $\mathbb{Z}_p$，所以该分裂域的特征为 p. 并且 $K \subset F$.

(a). 证明：$(K, +)$ 是交换群.

I. 封闭性：对任意的 $c,d\in K$

$$\begin{aligned}(c+d)^{p^n}-(c+d)&=(c^{p^n}-c)+(c^{p^n}-c)\\&=0\end{aligned}$$

从而 $c+d\in K$.

II. 结合律、交换律：显然成立.

III. 加法幺元：显然 $0\in K$，且对任意的 $c\in K$ 有

$$c+0=c=0+c$$

IV. 加法逆：对任意的 $c\in K$ 有：

$$\begin{aligned}(-c)^{p^n}-(-c)&=-(c^{p^n}-c)\\&=0\end{aligned}$$

从而 $-c\in K$. 且 $c+(-c)=0=(-c)+c$.

(b). 证明：$(K^\times,\cdots)$ 是交换群.

I. 封闭性：对任意的 $c,d\in K$

$$\begin{aligned}(cd)^{p^n}-cd&=c^{p^n}d^{p^n}-cd\\&=cd-cd\\&=0\end{aligned}$$

从而 $cd\in K$.

II. 结合律、交换律：显然成立.

III. 乘法幺元：显然 $1\in K$，且对任意的 $c\in K$ 有

$$c1=c=1c$$

IV. 乘法逆：对任意的 $c\in K$ 有：

$$\begin{aligned}(c)^{-p^n}-c^{-1}&=c^{-p^n-1}(c-c^{p^n})\\&=0\end{aligned}$$

从而 $c^{-1}\in K$. 且 $cc^{-1}=1=c^{-1}c$.

综上，K 是域. 因为分裂域是包含 f 所有根的最小的域，所以 $F\subset K$，即 $K=F$.

3. 证明：p^n 阶域必然存在.

因为 f 是可分多项式，所以 f 的根的个数为 p^n，即 $|K|=p^n$. 于是，p^n 阶域必然存在.

4. 证明：在同构意义下，p^n 阶域是唯一的.

假设 L 是特征 p 域，且 $[L:\mathbb{Z}_p]=n$，则 L 是 p^n 阶域. 由于 $(L^\times,\cdot)$ 是 p^n-1 阶群，所以对任意的 $c\in L^\times$，有

$$c^{p^n-1}=1$$

从而对任意的 $c\in L$，有 $c^{p^n}=c$，于是 L 中的所有元素，都是方程 $x^{p^n}=x$ 的根. 即 L 是 $f:=x^{p^n}-x$ 在 $\mathbb{Z}_p$ 上的分裂域，于是由分裂域的唯一性可知，p^n 阶域在同构意义下唯一.

笔记 这一证明过程是构造性的，它给出了构造 p^n 阶有限域的另一种方法.

问题 4.21 （子域）：p^m 阶域是 p^n 阶域的子域，当且仅当 $m|n$.

注 我们在有限域一节曾经证明：$d|n$，当且仅当 $(x^d-1)|(x^n-1)$. 其中 $d,n\in\mathbb{Z}_+$.

证明 p^m 阶域是 p^n 阶域的子域，当且仅当 $x^{p^m}-x$ 的根，都是 $x^{p^n}-x$ 的根，当且仅当 $(x^{p^m}-x)|(x^{p^n}-x)$，当且仅当 $(x^{p^m-1}-1)|(x^{p^n-1}-1)$，当且仅当 $(p^m-1)|(p^n-1)$，当且仅当 $m|n$.

（四）可分扩张

和之前代数扩张的定义类似的，我们将扩域的元素和域中多项式的根联系起来：设 F/K 是域的扩张

1. F/K 是代数扩张：F 中的每个元素都是 K 上**非零**多项式的根.
2. F/K 是可分扩张：F 中的每个元素都是 K 上**可分**多项式的根.

问题 4.22 （完全域上的扩张）：完全域上的有限扩张都是可分扩张.

证明 设 F/K 是有限扩张，且 K 是有限域. 对 F 中的任意元素 c，若 $c\in K$，则 c 是不可约多项式 $x-c$ 的根. 若 $c\in F-K$，则 c 是其 K 上最小多项式的根. 于是，c 总是 K 上某个不可约多项式的根. 由于 K 是完全域，所以 K 上的不可约多项式都是可分的. 从而对 F 中的任意元素 c，c 是 K 上某个可分多项式的根，即 F/K 是可分扩张.

笔记 此定理进一步体现“完全域”这一概念的意义：完全域上域的扩张特性比一般域更优.

另一方面，我们理解代数扩域的思路，仍然是多项式的根（或者元素的最小多项式）.

4.5.3 习题

（一）有限域

练习 4.51Fermat 小定理 对任意素数 p，以及 $a\in\mathbb{Z}_p$，证明：$a^p=a$.

证明 因为 $\mathbb{Z}_p$ 中的元素都是 x^p-x 的根，所以必有 $a^p-a=0$，即 $a^p=a$.

笔记 数论中的 Fermat 小定理叙述为：对任意的素数 p 和整数 a，有 $a^p\equiv a \mod p$.

练习 4.52 对任意的 $f\in\mathbb{Z}_p[x]$，$(f(x))^p=f(x^p)$.

证明 设

$$f(x)=\sum_{i=0}^{n}a_ix^i\in\mathbb{Z}_p[x]$$

由于 $\mathbb{Z}_p[x]$ 包含子域 $\mathbb{Z}_p$，所以 $\mathbb{Z}_p[x]$ 是特征 p 域，从而：

$$\begin{aligned}(f(x))^p&=(\sum_{i=0}^{n}a_ix^i)^p\\&=\sum_{i=0}^{n}(a_ix^i)^p\\&=\sum_{i=0}^{n}a_i^px^{ip}\\&=\sum_{i=0}^{n}a_i(x^p)^i\quad(a_i^p=a_i)\\&=f(x^p)\end{aligned}$$

笔记 注意到 $a_i\in\mathbb{Z}_p$，所以 $a_i^p=a_i$.

练习 4.53 设 $f(x_1,\cdots,x_n)\in\mathbb{Z}[x_1,\cdots,x_n]$. 证明：对任意的素数 p，多项式

$$g(x_1,\cdots,x_n):=(f(x_1,\cdots,x_n))^p-f(x_1^p,\cdots,x_n^p)$$

的所有系数都是 p 的倍数.

证明 记 $\bar f=f+Z_p\in\mathbb{Z}[x_1,\cdots,x_n]/\mathbb{Z}_p\simeq\mathbb{Z}_p[x_1,\cdots,x_n]$，只需证：$\bar g=\bar 0$.

设

$$\bar f:=\sum a_{c_1,\cdots,c_n}x_1^{c_1}\cdots x_n^{c_n}\in\mathbb{Z}_p[x_1,\cdots,x_n]$$

注意到 $\mathbb{Z}_p[x_1,\cdots,x_n]$ 是特征 p 域，我们有：

$$\begin{aligned}\bar{g}&=\overline{(f(x_1,\cdots,x_n))^p-f(x_1^p,\cdots,x_n^p)}\\&=\overline{(f(x_1,\cdots,x_n))^p}-\overline{f(x_1^p,\cdots,x_n^p)}\\&=(\bar{f}(x_1,\cdots,x_n))^p-\bar{f}(x_1^p,\cdots,x_n^p)\\&=\left(\sum a_{c_1,\cdots,c_n}x_1^{c_1}\cdots x_n^{c_n}\right)^p-\sum a_{c_1,\cdots,c_n}(x_1^p)^{c_1}\cdots(x_n^p)^{c_n}\\&=\sum a_{c_1,\cdots,c_n}x_1^{c_1p}\cdots x_n^{c_np}-\sum a_{c_1,\cdots,c_n}(x_1)^{c_1p}\cdots(x_n)^{c_np}\\&=\bar{0}\end{aligned}$$

从而原命题得证.

笔记 注意到 $a_{c_1,\cdots,c_n}\in\mathbb{Z}_p$，所以 $a^p_{c_1,\cdots,c_n}=a_{c_1,\cdots,c_n}$.

（二）可分多项式

练习 4.54 对任意的素数 p 和任意非零的 $a\in\mathbb{Z}_p$，证明：$f:=x^p-x+a\in\mathbb{Z}_p[x]$ 是不可约多项式，并且是可分多项式.

证明 先证明：若 c 是 f 的一个根，则 $c+1$ 也是 f 的一个根. 假设 $f(c)=0$，即 $c^p-c+a=0$，则

$$\begin{aligned}f(c+1)&=(c+1)^p-(c+1)+a\\&=\sum_{i=0}^{p}\binom{p}{i}c^i-(c+1)+a\\&=c^p+1-c-1+a\quad\left(\binom{p}{i}=0,i\in\{1,\cdots,p-1\}\right)\\&=c-a+1-c-1+a\\&=0\end{aligned}$$

于是，若 c 是 f 的一个根，则 $c+1,c+2,\cdots$ 都是 f 的根. 由于 $c+p=c$，所以 f 一共有 p 个根：$c,c+1,\cdots,c+p-1$.

首先，f 没有一次因式. 假设 f 有一次因式，则 $c,c+1,\cdots,c+p-1$ 中一定有某个元素属于 $\mathbb{Z}_p$，于是 $c\in Z_p$，从而 $c,c+1,\cdots,c+p-1$ 就是 $\mathbb{Z}_p$ 中的所有元素，即 0 是 f 的一个根. 然而 $0=f(0)=0-0+a\neq 0$，矛盾！

假设 f 有某个大于一次的因式 $g\in\mathbb{Z}_p[x]$（此时 $p\geqslant 3$ 为奇数），则必然有 f 的若干个根 $c_1,\cdots,c_m$，使得 $g(x)=(x-c_1)\cdots(x-c_m)$. 由于 f 的根的特性，f 在 $\mathbb{Z}_p$ 上必然有 p 个不相同的因式：

$$\begin{aligned}g(x)&=(x-c_1)\cdots(x-c_m)\\g(x-1)&=(x-c_1-1)\cdots(x-c_m-1)\\&\cdots\\g_{p-1}(x)&=(x-c_1-p+1)\cdots(x-c_m-p+1)\end{aligned}$$

然而这些因式的乘积的次数，已经大于 f 次数，矛盾！所以 f 也不能有超过一次的因式.

综上，f 在 $\mathbb{Z}_p$ 中没有因式，是不可约的. 进一步的，由于 $\mathbb{Z}_p$ 是完全域，所以 f 是可分多项式.

笔记 本题证明不可约的方式不是常规方式.

练习 4.55 设 K/F 是域的扩张，F 是完全域，$f\in F[x]$ 没有重复的不可约因子. 证明：f 在 $K[x]$ 内没有重复的不可约因子.

证明 因为 F 是完全域，所以 f 是可分多项式，从而 f 没有重根. 假设 f 在 $K[x]$ 内有重复的不可约因子，则 f 有重复的不可约因子对应的重根，矛盾！

4.6 拓展 A：单位根与分圆域

笔者的话：笔者对于单位根的知识有一种特殊的感情，这还要从一位老师和一套书说起。

笔者在很多场合都提到过高中时期的数学老师，是他的教导让笔者初步认识到了思考的重要性。后来它给了笔者两套数学专题类的丛书：中学生文库和数学小丛书，这些书的作者都是大家耳熟能详的大家：常庚哲、苏淳、史济怀、谷超豪……而他们所写的内容是“纯粹”的初等数学，比如奇偶数、三角恒等变换等等，里面的知识非常丰富，而且不枯燥。可以说，正是在这两套书的指引下，笔者逐渐有了做数学教育、写数学书的想法。

回到我们的主题上来，大家看到的这本书通常都会被算到“高等”数学的范畴，但是“高等”和“初等”的分界线在哪里呢，我们在使用数学知识的时候，会刻意区分它是“高等”的知识还是“初等”的只是么？显然是不会的。我想这大概就是数学的妙处，从一个小学生水平的数学知识出发，也可以引申到非常深刻的数学话题（我们谈到的各种运算律，想必大家都是在小学四年级的时候就学过的吧）。

从而笔者想表达的是，我们学习数学的过程，有时候我们在学习新的知识，有时候我们在将旧的知识和新的知识联系起来。这种“增材 + 联系”的循环往复，使得我们逐渐将所掌握的知识编织成了一张大网，而不再是一条一条孤立的线索了。

4.6.1 单位根及其基本性质

我们在前面的章节中已经介绍过，n 次单位根，指的是方程

$$x^n = 1$$

的根. 而且我们已经证明

1. n 次单位根全体连同乘法构成循环群；
2. 所有的单位根全体连同乘法构成交换群.

利用复数的知识，我们知道 n 次单位根的全体是

$$\{e^{\frac{2\pi ik}{n}}\}_{k=0}^{n-1}$$

很多时候，我们并不需要直接使用单位根的显式. 一方面，我们可以利用 n 次单位根的循环群，来完成元素之间的乘法运算. 另一方面，我们知道有如下乘法公式

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + 1)$$

所以除了 1 之外，其他的 n 次单位根都是方程 $x^{n-1} + x^{n-2} + \cdots + 1$ 的根，从而我们有一个重要的性质。

定理 4.1

对 n 次单位根 $\zeta_n = e^{\frac{2\pi ik}{n}}$，若 $(n,k) = 1$，则有

$$\sum_{k=0}^{n-1} \zeta_n^k = 0$$

♡

这一点常常帮助我们做一些特殊的因式分解.

例题 4.13 在 $\mathbb{Z}[x]$ 内做因式分解：$f = x^5 + x + 1$.

证明 考虑不是 1 的三次单位根 ω，我们有：

$$f(\omega) = \omega^2 + \omega + 1 = 0$$

从而 f 有因子 $x^2 + x + 1$. 再由多项式的带余除法求得：

$$f = (x^2 + x + 1)(x^3 - x^2 + 1)$$

进一步考虑 $x^3 - x^2 + 1$ 的可约性. 若其可约，则必然有一次因式，而其首项和常数项都是 1，所以可能的整数根只有 ± 1. 简单的验证即可知 ± 1 都不是 $x^3 - x^2 + 1$ 的根，从而其在 $\mathbb{Z}[x]$ 上不可约.

综上，f 的不可约元分解为 $(x^2 + x + 1)(x^3 - x^2 + 1)$.

✍ **练习 4.56** 在 $\mathbb{Z}[x]$ 内做因式分解：$f = x^8 + x^4 + 1$.

例题 4.14 设 $P(x), Q(x), R(x), S(x) \in \mathbb{R}[x]$，且满足条件

$$P(x^5) + xQ(x^5) + x^2R(x^5) = (x^4 + x^3 + x^2 + x + 1)S(x)$$

证明：$(x-1)|P(x)$.

注 等式右侧的因子 $(x^4 + x^3 + x^2 + x + 1)$ 强烈的“明示”我们使用五次单位根.

证明 记 ω 为任意不等于 1 的五次单位根，则 $x^4 + x^3 + x^2 + x + 1$ 的四个根恰好为 $\omega, \omega^2, \omega^3, \omega^4$（因为 5 是素数，所以和每个小于五的正整数互素）. 分别代入 $x = \omega, \omega^2, \omega^3, \omega^4$ 可得

$$\begin{aligned} P(1) + \omega Q(1) + \omega^2 R(1) &= 0 \\ P(1) + \omega^2 Q(1) + \omega^4 R(1) &= 0 \\ P(1) + \omega^3 Q(1) + \omega R(1) &= 0 \\ P(1) + \omega^4 Q(1) + \omega^3 R(1) &= 0 \end{aligned}$$

四式相加即得 $P(1) = 0$，从而由因式定理可知 $(x-1)|P(x)$.

n 次单位根中有一些特殊的元素，由它可以直接生成整个 n 次单位根群，我们把这样的元素称为“原始的”（primitive）n 次单位根. 利用循环群的知识，我们知道一个 n 次单位根 $e^{\frac{2\pi ik}{n}}$ 是原始的，当且仅当 $(k, n) = 1$. 以下为了行文方便，我们总是记 $\zeta_n = e^{\frac{2\pi i}{n}}$.

4.6.2 分圆域

所谓 n 次单位根的分圆域，指的是 $\mathbb{Q}$ 的扩域 $\mathbb{Q}(\zeta_n)$. 之所以称之为“分圆”，因为 n 次单位根总是均匀的分布在单位圆上. 利用前面学过的域扩张的知识，我们可以轻松解决下列问题.

✍ **练习 4.57** $f = x^n - 1 \in \mathbb{Q}[x]$ 在 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}(\zeta_n)$.

✍ **练习 4.58** 证明：当 p 为素数时，$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

注 提示：只需证明多项式

$$\frac{x^p - 1}{x - 1}$$

在 $\mathbb{Q}[x]$ 内不可约.

✍ **练习 4.59** 求 $[\mathbb{Q}(\zeta_4) : \mathbb{Q}]$ 的值.

注 提示：注意到 ζ_4 在 $\mathbb{Q}[x]$ 内的最小多项式是 $x^2 + 1$，而不是 $x^4 - 1$.

✍ **练习 4.60** 在 $\mathbb{Q}[x]$ 内因式分解 $x^9 - 1$，并求 $[\mathbb{Q}(\zeta_9) : \mathbb{Q}]$ 的值.

注 提示：因式分解的结果为

$$x^9 - 1 = (x-1)(x^2 + x + 1)(x^6 + x^3 + 1)$$

✍ **练习 4.61** 设 p 是素数，求 $x^p - 2$ 在 $\mathbb{Q}$ 上的分裂域.

注 提示：$x^p - 2$ 的所有复根可表示为 $\sqrt[p]{2}\zeta_p^k, k = 0, \cdots, p-1$. 接下来证明：

$$\mathbb{Q}(\sqrt[p]{2}, \sqrt[p]{2}\zeta_p, \cdots, \sqrt[p]{2}\zeta_p^{p-1}) = \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$$

即可.

4.7 拓展 B：一元三次方程的求根公式

我们首先来看一个因式分解问题：

例题 4.15 在 $\mathbb{C}[x]$ 上因式分解：$x^3 + y^3 + z^3 - 3xyz$.

解 我们有：

$$\begin{aligned}x^3+y^3+z^3-3xyz&=(x+y)(x^2-xy+y^2)+z^3-3xyz\\&=(x+y+z)(x^2-xy+y^2)-x^2z+xyz-y^2z+z^3-3xyz\\&=(x+y+z)(x^2-xy+y^2)-(x^2+2xy+y^2)z+z^3\\&=(x+y+z)(x^2-xy+y^2)-((x+y)^2-z^2)z\\&=(x+y+z)(x^2-xy+y^2)-(x+y+z)(x+y-z)z\\&=(x+y+z)(x^2+y^2+z^2-xy-yz-zx)\end{aligned}$$

然后，对于因式 $x^2+y^2+z^2-xy-yz-zx$，我们可以将其视作是关于 x 的一元二次方程（即 $x^2-(y+z)x+(y^2+z^2-yz)=0$），直接求解：

$$\begin{aligned}x_1,x_2&=\frac{(y+z)\pm\sqrt{(y+z)^2-4(y^2+z^2-yz)}}{2}\\&=\frac{(y+z)\pm\sqrt{-3(y-z)^2}}{2}\end{aligned}$$

y,z 对称，于是不妨设 $y\geqslant z$，进一步化简可得：

$$\begin{aligned}x_1,x_2&=\frac{(y+z)\pm\sqrt{-3}(y-z)}{2}\\&=\frac{1+\sqrt{-3}}{2}y+\frac{1-\sqrt{-3}}{2}z,\ \frac{1-\sqrt{-3}}{2}y+\frac{1+\sqrt{-3}}{2}z\\&=-(\omega^2y+\omega z),\ -(\omega y+\omega^2z)\end{aligned}$$

其中

$$\begin{aligned}\omega&:=-\frac{1}{2}+\frac{\sqrt{-3}}{2}\\\omega^2&=-\frac{1}{2}-\frac{\sqrt{-3}}{2}\end{aligned}$$

是三次单位根（下同）. 从而有：

$$x^2+y^2+z^2-xy-yz-zx=(x+\omega y+\omega^2z)(x+\omega^2y+\omega z)$$

这是两个一次因式了，从而没办法继续因式分解.

最终，我们得到了因式分解的最终结果：

$$x^3+y^3+z^3-3xyz=(x+y+z)(x+\omega y+\omega^2z)(x+\omega^2y+\omega z).$$

笔记 本题的解答是在已知部分答案的情况下写出的（很明显，如果笔者不是事先知道 $x^3+y^3+z^3-3xyz$ 有因式 $x+y+z$，一定不会做这样的代数变形），那么答案是如何事先知道的呢？

注意到 $x^3+y^3+z^3-3xyz$ 是一个对称多项式，从而它的因式可以通过合理的分组，变成若干个对称多项式的乘积. 我们从最简单的情形开始验证，也就是考虑一次对称多项式 $x+y+z$. 将原多项式视作以 x 为变量，y,z 为参数的多项式：

$$f(x)=x^3-(3yz)x+(y^3+z^3)$$

然后代入 $x=-y-z$ 可得：

$$f(-y-z)=-(y+z)^3+(3yz)(y+z)+(y^3+z^3)=-(y+z)^3+(y+z)^3=0$$

从而验证了 $x+y+z$ 确为一个因式. 然后做多项式的除法，即可得到另一个二次的因式. 如果是在 $\mathbb{Q}[x]$ 内做因式分解，到这一步就可以结束了，而现在是 $\mathbb{C}[x]$，从而再对二次因式做一个解方程的操作即可.

这一因式分解的结果，实际上是一种特殊形式的一元三次方程的解，即关于 x 的一元三次方程：

$$x^3-(3yz)x+(y^3+z^3)=0$$

有三个根为：

$$x_1=-y-z, x_2=-\omega y-\omega^2 z, x_3=-\omega^2 y-\omega z.$$

这一结果启发我们，对于一般的没有二次项的一元三次方程 $x^3-3px+q=0$，我们能不能利用这一结果找到它的三个根呢？实际上这就得到了著名的卡尔达诺（Cardano）公式. 在说明这一公式的形式之前，我们也做一个澄清，正如洛必达法则是由伯努利发现的一样，卡尔达诺公式是由塔塔利亚发现的.

定理 4.2 (Cardano 公式)

关于 x 的一元三次方程 $x^3-3px+q=0$，它的三个根形如：

$$x_1=-y-z$$
$$x_2=-\omega y-\omega^2 z$$
$$x_3=-\omega^2 y-\omega z$$

其中：

$$\omega=-\frac{1}{2}+\frac{\sqrt{-3}}{2}$$
$$y=\sqrt[3]{\frac{q+\sqrt{q^2-4p^3}}{2}}$$
$$z=\sqrt[3]{\frac{q-\sqrt{q^2-4p^3}}{2}}$$

♡

证明 令 $p=yz, q=y^3+z^3$，下面先解出 y,z 关于 p,q 的表达式. 我们有：

$$y^3z^3=p^3$$
$$y^3+z^3=q$$

从而 y^3,z^3 是关于 u 的一元二次方程 $u^2-qx+p^3=0$ 的两个根，解之可得：

$$u_1,u_2=\frac{q\pm\sqrt{q^2-4p^3}}{2}$$

由于 y^3,z^3 是对称的，所以不妨取

$$y^3=\frac{q+\sqrt{q^2-4p^3}}{2}$$
$$z^3=\frac{q-\sqrt{q^2-4p^3}}{2}$$

于是 y,z 各自就可以表达为：

$$y_i=\sqrt[3]{\frac{q+\sqrt{q^2-4p^3}}{2}}\omega^i$$
$$z_i=\sqrt[3]{\frac{q-\sqrt{q^2-4p^3}}{2}}\omega^i$$

注意到 $yz=p$，所以组合考虑 y,z 的取值，我们得到三组解：

$$y_1,z_1=\sqrt[3]{\frac{q+\sqrt{q^2-4p^3}}{2}},\sqrt[3]{\frac{q-\sqrt{q^2-4p^3}}{2}}$$
$$y_2,z_2=\sqrt[3]{\frac{q+\sqrt{q^2-4p^3}}{2}}\omega,\sqrt[3]{\frac{q-\sqrt{q^2-4p^3}}{2}}\omega^2$$
$$y_3,z_3=\sqrt[3]{\frac{q+\sqrt{q^2-4p^3}}{2}}\omega^2,\sqrt[3]{\frac{q-\sqrt{q^2-4p^3}}{2}}\omega$$

进一步，利用前述因式分解的结果，我们可得方程 $x^3-3px+q=0$（即 $x^3-(3yz)x+(y^3+z^3)=0$）的解

为：

$$x_1 = -y - z$$
$$x_2 = -\omega y - \omega^2 z$$
$$x_3 = -\omega^2 y - \omega z$$

分别带入 y, z 的三组可能取值，发现最终原方程也就只有三个解，他们是：

$$x_1 = -y - z$$
$$x_2 = -\omega y - \omega^2 z$$
$$x_3 = -\omega^2 y - \omega z$$

其中：

$$y = \sqrt[3]{\frac{q + \sqrt{q^2 - 4p^3}}{2}}$$
$$z = \sqrt[3]{\frac{q - \sqrt{q^2 - 4p^3}}{2}}$$

有的读者此时一定会有疑问，对于不缺二次项的一元三次方程 $x^3 + ax^2 + bx + c = 0$，我们应该怎么办呢？取 $x = y - u$，其中 u 是参数，则原方程变为：

$$\begin{aligned} 0 &= x^3 + ax^2 + bx + c \\ &= (y-u)^3 + (y-u)x^2 + (y-u)x + c \\ &= y^3 + (-3u + a)y^2 + (3u^2 - 2au + b)y + (-u^3 + au^2 - bu + c) \end{aligned}$$

我们取 $u = \frac{a}{3}$，则可得关于 y 的一元三次方程

$$y^3 + (-\frac{a^2}{3} + b)y + (\frac{2a^3}{27} - \frac{ab}{3} + c) = 0$$

这是一个缺二次项的方程，从而可以利用 Cardano 公式求解.

到此我们彻底解决了一元三次方程的求根问题. 比起具体的求解某个一元三次方程的根，笔者认为，Cardano 公式最重要的是揭示了一元三次方程根的形式，即

$$x_1 = a + b + c$$
$$x_2 = a + b\omega + c\omega^2$$
$$x_3 = a + b\omega^2 + c\omega$$

我们可以试着用韦达定理，来构造以 $y_i := x_i - a$ 为根的一元三次方程，我们有

$$y_1 + y_2 + y_3 = 0$$
$$y_1y_2 + y_2y_3 + y_3y_1 = 3bc(\omega + \omega^2) = -3bc$$
$$y_1y_2y_3 = b^3 + c^3$$

我们发现，最终我们还是回归了我们本节开篇所讲的因式分解，即方程

$$(x-a)^3 - 3bc(x-a) - (b^3 + c^3) = 0$$

有三个根为 x_1, x_2, x_3. 利用这一点我们可以解决一些问题.

例题 4.16 求 $t = 1 + \sqrt[3]{2} + 2\sqrt[3]{4}$ 在 $\mathbb{Q}$ 上的最小多项式.

注 这是我们在代数扩域一节（第二节）中的一个例题，利用一元三次方程的知识，我们可以更轻松的解决.

设：

$$t_1 = 1 + \sqrt[3]{2} + 2\sqrt[3]{4}$$
$$t_2 = 1 + \sqrt[3]{2}\omega + 2\sqrt[3]{4}\omega^2$$
$$t_3 = 1 + \sqrt[3]{2}\omega^2 + 2\sqrt[3]{4}\omega^2$$

则以他们为根的一个一元三次方程为

$$\begin{aligned} 0 &= (x-1)^3 - 3(\sqrt[3]{2})(2\sqrt[3]{4})(x-1) + (\sqrt[3]{2})^3 + (2\sqrt[3]{4})^3 \\ &= (x-1)^3 - 12(x-1) - 34 \\ &= x^3 - 3x - 9x - 23 \end{aligned}$$

这就得到了我们想要的最小多项式了.

解答我们在第二节已经展示了，此处从略.

例题 4.17 求以 $t = 1 + \sqrt[3]{2} + \sqrt[3]{3}$ 为一根的多项式方程，要求最高此项系数为 1，且系数均为有理数.

注 与前一题的思路一样，我们可以先构造出一个一元三次方程

$$(y-1)^3 - 3\sqrt[3]{6}(y-1) - 5 = 0$$

虽然它还不满足题设要求，但是此时式子里只有一个根式了，从而求立方可以处理掉.

$$(y-1)^3 - 5 = 3\sqrt[3]{6}(y-1)$$
$$((y-1)^3 - 5)^3 = 162(y-1)^3$$
$$((y-1)^3 - 5)^3 - 162(y-1)^3 = 0$$

最终的式子就是我们需要的方程.（请原谅，笔者实在不想化简这样一个复杂的式子）

第 5 章 群论 II

5.1 对称群与交错群

5.1.1 课前思考

1. 设 A 是 m 阶集合，B 是 n 阶集合，则从 A 到 B 的映射有____ 个.
2. 设 A 是 n 阶集合，则 $\mathrm{Perm}(A)$ 的阶数为____.

解

1. n^m. A 中的每个元素，都有 n 种可能的象.
2. $n!$.

5.1.2 知识要点

（一）置换与对称群

1. 集合 Ω 上的置换：从 Ω 映到 Ω 上的一个双射.
2. 集合 Ω 上的对称群：Ω 上的全体置换 $\mathrm{Perm}(\Omega)$（或记作 S_Ω），连同映射的复合运算，构成的群.
3. n 阶对称群：$S_n := \mathrm{Perm}(\Omega)$，其中 $\Omega = \{1, 2, \cdots, n\}$.
4. 轮换：一列元素 $(a_1\ a_2\ \cdots\ a_m)$，它表达了一个置换，将每个 a_i 映到 a_{i+1}（$i \in [1, m-1]$），且将 a_m 映到 a_1.
   (a). 轮换的长度：一个轮换中包含的元素个数.
   (b). t-轮换：长度为 t 的轮换.
   (c). 两个轮换不交：两个轮换不包含公共元素.（不交的两个轮换可以交换顺序.）
5. （轮换分解）：不计轮换次序，任意 $\sigma \in S_n$ 可以被唯一的分解为若干个不交的轮换的乘积.
6. 置换的轮换型：置换的轮换分解中，所有的轮换长度构成的一列整数.（所有的 1 都省略，除了幺元对应的轮换型，他只能表达为 1）
7. 对换：S_n 中的 2-轮换.
8. （轮换与对换的关系）：对任意 m-轮换有 $(a_1\ a_2\ \cdots\ a_m) = (a_1\ a_m)(a_1\ a_{m-1})\cdots(a_1\ a_2)$.
9. （S_n 的生成元）：$S_n = \langle T \rangle$，$T = \{(i\ j) : 1 \leqslant i < j \leqslant n\}$.

（二）置换的奇偶性

1. 置换群：对称群的任意子群.
2. “判别式”：定义“判别式”

$$\Delta = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)$$

对每个 $\sigma \in S_n$，定义

$$\sigma(\Delta) = \prod_{1 \leqslant i < j \leqslant n} \left(x_{\sigma(i)} - x_{\sigma(j)}\right)$$

于是 $\sigma(\Delta) = \pm\Delta$.

3. 置换的奇偶性：对任意 $\sigma \in S_n$，定义 $\epsilon : S_n \to (\{\pm 1\}, \cdot)$

$$\epsilon(\sigma) = \begin{cases} +1, & \text{if } \sigma(\Delta) = \Delta \\ -1, & \text{if } \sigma(\Delta) = -\Delta \end{cases}$$

于是定义：

(a). σ 为奇置换：$\epsilon(\sigma)=-1$；
(b). σ 为偶置换：$\epsilon(\sigma)=1$

4. (对换的奇偶性)：任意对换都是奇置换.
5. (奇偶性的等价定义)：对任意 $\sigma\in S_n$，
   (a). σ 为奇置换，当且仅当 σ 为奇数个对换的积；
   (b). σ 为偶置换：当且仅当 σ 为偶数个对换的积.
6. (轮换的奇偶性)：m-轮换是奇置换，当且仅当 m 是偶数.
7. (同态 ϵ)：ϵ 为满同态.

(三) 交错群

1. n 阶交错群 A_n：同态 $\epsilon:S_n\to(\{\pm1\},\cdot)$ 的核.
2. (交错群的等价定义)：$A_n=\{\sigma\in S_n:\sigma$是偶置换.$\}$
3. (单群)：对任意不小于 5 的整数 n，A_n 是非交换的单群.

5.1.3 知识要点解读

(一) 置换与对称群

置换本质上就是特殊的映射：一个集合到自身的双射，因此我们对它并不陌生. 在抽象代数的范围内，我们通常只研究有限集上的置换，以及它们构成的对称群. (一个例外是，考虑 n 维线性空间 V，则 V 到自身的置换，是一个 n 阶的可逆方阵，这是我们研究的对象之一，不过 V 是无限集.)

有限集上的置换，我们有一个非常简便的表达方法：轮换分解法. 可以这么表达是因为有如下命题作为保证：

问题 5.1 (轮换分解)：不计轮换次序，任意 $\sigma\in S_n$ 可以被唯一的分解为若干个不交的轮换的乘积.
注 证明过程我们将在群作用一节中予以展示. 由此也体现出群作用和置换，轨道和轮换之间的联系.

置换的计算是基本功，同时也是容易让初学者感到困惑的难点之一，笔者也曾经为此辗转反侧. 我们会在“典型例题”部分，详细地给出轮换分解的操作方式和理解思路.

(二) 置换的奇偶性

置换奇偶性有两种定义方法，一种是将置换分解成若干个对换的积，然后由对换个数的奇偶性决定置换的奇偶性。这种做法容易操作，但是在理论上需要更多的补充说明，因为一个置换分解成对换的方式不是唯一的，例如

$$\begin{aligned}(1\ 2)&=(1\ 3)(2\ 3)(1\ 3)\\&=(1\ 4)(3\ 4)(1\ 4)(2\ 3)(1\ 3)\\&\cdots\end{aligned}$$

另一种定义方法看起来比较绕. 我们定义了一个“判别式”：

$$\Delta=\prod_{1\leqslant i<j\leqslant n}(x_i-x_j).$$

我们在学习一元二次方程的时候，也定义了一个判别式（一般的，一元三次、四次方程也有自己的判别式），这两个判别式在本质上是一件事. 首先，对于两个元素 x_1,x_2，判别式为：

$$\Delta=x_1-x_2$$

假如我们令 x_1, x_2 为一元二次方程 $ax^2+bx+c=0$ 的两个根. 由于 x_1, x_2 是任意的，因此一般会有两种情况，为了保持对称性，我们考虑代数式 $(x_1-x_2)^2$，由 Vieta 定理可得:

$$\begin{aligned}(x_1-x_2)^2 &= (x_1+x_2)^2-4x_1x_2\\ &= \frac{b^2-4ac}{a^2}\end{aligned}$$

由于 a^2 不影响整个式子的正负性，所以就判别的需求来说，起作用的是 b^2-4ac，也就是我们熟悉的判别式了.

对于一元三次、四次方程，类似地讨论也是存在的，我们将会在 Galois 理论的部分展开论述.

回到奇偶性的话题上，考虑 n 个元素对应的判别式 Δ，可以发现，任意一个 S_n 中的置换作用于 Δ 上，只能得到两个结果 $\pm\Delta$. 由此引申出了一个非常重要的群同态 ϵ，以及该同态的核：n 阶交错群 A_n，进而得到 $A_n \lhd S_n$. 由于 S_n 的复杂性，当 n 比较大时，S_n 的子群（乃至于正规子群）情况，是不容易搞清楚的，而交错群天然地提供了一个正规子群，这对于我们研究 S_n 地结构，是很有帮助的.

两种定义最终能够统一起来，出发点是如下命题：

问题 5.2 （对换的奇偶性）：任意对换都是奇置换.

证明 取 S_n 中的任意对换 $\sigma=(m\ n)$，考察 σ 对 Δ 各因式 x_i-x_j 的作用.

1. 如果 i,j 中没有 m,n，则 σ 对 x_i-x_j 没有影响.
2. 如果 i,j 中包含 m,n 其中之一，不妨设 $i=m$，则 $x_i-x_j=x_m-x_j$. 对应的考虑因子 x_n-x_j，则

$$\begin{aligned}\sigma((x_m-x_j)(x_n-x_j)) &= \sigma(x_m-x_j)\sigma(x_n-x_j)\\ &= (x_n-x_j)(x_m-x_j)\end{aligned}$$

   σ 保持两个因子的乘积不变.
3. 如果 i,j 等于 m,n，则

$$\sigma(x_m-x_n)=-(x_m-x_n)$$

综上所述，σ 对 Δ 的作用，只会使 Δ 的一个因式变号，从而 $\sigma(\Delta)=-\Delta$，即 σ 是奇置换.

上述命题启发我们，判断一个置换的奇偶性，只需要将置换分解成对换的乘积，在对对换的个数计数即可. 由于置换的奇偶性总是确定的，因此不论做怎样的分解，对换个数的奇偶性总是不变，从而两种定义就统一起来了.

5.1.4 典型例题

（一）置换的轮换分解与计算

为了研究 S_n 的性质，我们首先需要熟悉 S_n 的元素. 我们当然可以使用列表法，表达每一个置换，但是我们还有更简单的表达方式：轮换分解. 轮换分解是一个机械性的算法，笔者曾写过一个 python 小程序操作轮换分解. 我们用一个例子展示具体的做法.

例题 5.1 设 σ 是置换：

$$1\mapsto 3\quad 2\mapsto 4\quad 3\mapsto 5\quad 4\mapsto 2\quad 5\mapsto 1$$

并且设 τ 是置换：

$$1\mapsto 5\quad 2\mapsto 3\quad 3\mapsto 2\quad 4\mapsto 4\quad 5\mapsto 1.$$

试给出下列置换的轮换分解：$\sigma, \tau, \sigma^2, \sigma\tau, \tau\sigma, \tau^2\sigma, \sigma^{-1}, \tau^{-1}$.

注 我们先以 σ 为例，展示如何对一个置换做轮换分解.

σ 包含五个元素，其中号码最小的为 1，于是我们从 1 开始考虑. 1 映到 3，3 映到 5，5 映回 1. 于是我们有了第一个轮换 (1 3 5).

剩下的元素中，号码最小的为 2，于是我们从 2 开始寻找新的轮换. 2 映到 4，4 映回 2. 于是我们有了第二个轮换 (2 4).

此时不剩下其他元素了，于是轮换分解结束，我们得到：$\sigma = (1\,3\,5)(2\,4)$. （或者 $(2\,4)(1\,3\,5)$，不交的轮换，先后顺序无所谓）

我们再以 σ^2 为例，展示如何做置换的复合运算.

首先写出需要复合的全部轮换：$\sigma^2 = (1\,3\,5)(2\,4)(1\,3\,5)(2\,4)$.

然后，和前例类似地，我们先从 1 开始考虑. 由于映射是从最右边开始先做的，于是我们从右往左以此考虑每个轮换. 1 经过第一个轮换不变，仍为 1；1 经过第二个轮换，变为 3；3 经过第三个轮换不变，仍为 3；3 经过第四个轮换，变为 5. 于是 σ^2 将 1 变为 5.

我们继续从 5 开始上述流程，可得：$5 \mapsto 5 \mapsto 1 \mapsto 1 \mapsto 3$，于是 σ^2 将 5 变为 3. 而 $3 \mapsto 3 \mapsto 5 \mapsto 5 \mapsto 1$，于是 σ^2 将 3 变为 1. 至此我们找到了 σ^2 的第一个轮换 $(1\,5\,3)$.

在剩下的元素中，我们从 2 开始继续考虑. $2 \mapsto 4 \mapsto 4 \mapsto 2 \mapsto 2$，于是 σ^2 将 2 变为 2. 注意在轮换分解中，恒等映射略去不写，于是我们找到了 σ^2 的第二个轮换 $id.$，省略不写. 类似地，剩下的一个元素 4 也映回自身，同样省略.

于是，$\sigma^2 = (1\,5\,3)$.

最后，我们展示以下，如何求置换的逆. 从元素的角度看，如果一个置换 f 将 a 映到 b，那么 f^{-1} 将 b 映到 a. 从而，对于一个轮换 $(a\,b\,c)$ 来说，其逆就是 $(c\,b\,a)$.

因此，$\sigma^{-1} = ((1\,3\,5)(2\,4))^{-1} = (2\,4)^{-1}(1\,3\,5)^{-1} = (4\,2)(5\,3\,1)$. 由轮换的定义，我们可以进一步整理为：$\sigma^{-1} = (2\,4)(1\,5\,3)$.

剩下的部分我们在解答中展示.

解

$$\begin{aligned}
\sigma &= (1\,3\,5)(2\,4)\\
\tau &= (1\,5)(2\,3)\\
\sigma^2 &= (1\,3\,5)(2\,4)(1\,3\,5)(2\,4) = (1\,5\,3)\\
\sigma\tau &= (1\,3\,5)(2\,4)(1\,5)(2\,3) = (2\,5\,3\,4)\\
\tau\sigma &= (1\,5)(2\,3)(1\,3\,5)(2\,4) = (1\,2\,4\,3)\\
\tau^2\sigma &= (1\,5)(2\,3)(1\,5)(2\,3)(1\,3\,5)(2\,4) = (1\,3\,5)(2\,4)\\
\sigma^{-1} &= (1\,5\,3)(2\,4)\\
\tau^{-1} &= (1\,5)(2\,3)
\end{aligned}$$

笔记 在熟悉了基本过程之后，我们可以通过一些简单的小结论简化运算. 例如，对任意不同的 i, j，有 $(i\,j) = (i\,j)^{-1}$，从而 $(i\,j)(i\,j) = 1$. 进一步结合“不交的两个轮换可以交换顺序”的性质，于是：

$$\begin{aligned}
\sigma^2 &= (1\,3\,5)(2\,4)(1\,3\,5)(2\,4)\\
&= (1\,3\,5)(1\,3\,5)(2\,4)(2\,4)\\
&= (1\,3\,5)(1\,3\,5)\\
&= (1\,5\,3).
\end{aligned}$$

练习 5.1 设 σ 是置换：

$$\begin{array}{lllll}
1 \mapsto 13 & 2 \mapsto 2 & 3 \mapsto 15 & 4 \mapsto 14 & 5 \mapsto 10\\
6 \mapsto 6 & 7 \mapsto 12 & 8 \mapsto 3 & 9 \mapsto 4 & 10 \mapsto 1\\
11 \mapsto 7 & 12 \mapsto 9 & 13 \mapsto 5 & 14 \mapsto 11 & 15 \mapsto 8
\end{array}$$

并且设 τ 是置换：

$$1\mapsto 14 \quad 2\mapsto 9 \quad 3\mapsto 10 \quad 4\mapsto 2 \quad 5\mapsto 12$$
$$6\mapsto 6 \quad 7\mapsto 5 \quad 8\mapsto 11 \quad 9\mapsto 15 \quad 10\mapsto 3$$
$$11\mapsto 8 \quad 12\mapsto 7 \quad 13\mapsto 4 \quad 14\mapsto 1 \quad 15\mapsto 13$$

试给出下列置换的轮换分解：$\sigma,\tau,\sigma^2,\sigma\tau,\tau\sigma,\tau^2\sigma,\sigma^{-1},\tau^{-1}$，并且计算它们的阶.

✍ **练习 5.2** 设 $\sigma=(1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12)$，对每个正整数 i，计算每个 σ^i 并轮换分解，计算它们的阶.

5.1.5 习题

（一）置换与对称群

✍ **练习 5.3** 写出 S_4 的每个元素的轮换分解，并计算它们的阶.

解 1 阶元素：

$$1$$

2 阶元素：

$$(1\,2),(1\,3),(1\,4),(2\,3),(2\,4),(3\,4)$$
$$(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)$$

3 阶元素：

$$(1\,2\,3),(1\,2\,4),(1\,3\,4),(2\,3\,4),(1\,3\,2),(1\,4\,2),(1\,4\,3),(2\,4\,3)$$

4 阶元素：

$$(1\,2\,3\,4),(1\,2\,4\,3),(1\,3\,2\,4),(1\,3\,4\,2),(1\,4\,2\,3),(1\,4\,3\,2)$$

✍ **练习 5.4** 设 $\sigma=(a_1\,a_2\cdots a_m)$ 是一个 m-轮换.

1. 证明：对任意 $i\in\{1,2,\cdots,m\}$，有 $\sigma^i(a_k)=a_{k+i}$，其中当 $k+i>m$ 时，$k+i$ 由其模 m 剩余类替换.
2. 证明：$|\sigma|=m$.

✍ **练习 5.5** 设 $\sigma=(a_1\,a_2\cdots a_m)$ 是一个 m-轮换. 证明：σ^i 是 m-轮换，当且仅当 $(i,m)=1$.

✍ **练习 5.6** 对给定的 τ，考虑是否存在一个 n-轮换 σ，使得 $\tau=\sigma^k$：

1. $\tau=(1\,2)(3\,4)(5\,6)$. $(n\geqslant 6)$
2. $\tau=(1\,2)(3\,4\,5)$. $(n\geqslant 5)$

解

1. 可取 $\sigma=(1\,3\,5\,2\,4\,6)$，此时 $k=3$.
2. 由轮换 $(1\,2)$ 可知：$2k\equiv 0 \mod n$，因为 $\sigma^k(1)=2,\sigma^{2k}(1)=1$，且 σ 为轮换. 而由轮换 $(3\,4\,5)$ 可知：$3k\equiv 0 \mod n$. 于是 $k=in,i\in\mathbb{Z}$. 但是，$\sigma^k=(\sigma^n)^i=1$. 于是不存在满足条件的 σ.

✍ **练习 5.7** 证明：S_n 中的元素 σ 的阶为 2，当且仅当其轮换分解为 2-轮换的乘积.

✍ **练习 5.8**

1. p 是素数. 证明：S_n 中的元素 σ 的阶为 p，当且仅当其轮换分解为 p-轮换的乘积.
2. 若 p 不是素数，试给出一个反例.

注 提示：在 S_6 中，$(1\,2)(3\,4\,5\,6)$ 的阶为 4.

✍ **练习 5.9** 证明：S_n 中的元素的阶，等于其轮换分解中所有轮换长度的最小公倍数.

✍ **练习 5.10** 找出所有的整数 n，满足 S_5 中有一个阶为 n 的元素.

笔记 由上一题，我们只需考虑 S_5 的元素的所有可能轮换型即可.

解

轮换型	对应的阶数
5	5
4	4
3, 2	6
3	3
2, 2	2
2	2
1	1

从而 $n \in \{1,2,3,4,5,6\}$.

✍ **练习 5.11** 找出所有的整数 n，满足 S_7 中有一个阶为 n 的元素.

解

轮换型	对应的阶数
7	7
6	6
5, 2	10
5	5
4, 3	12
4, 2	4
4	4
3, 3	3
3, 2, 2	6
3, 2	6
3	3
2, 2, 2	2
2, 2	2
2	2
1	1

从而 $n \in \{1,2,3,4,5,6,7,10,12\}$.

✍ **练习 5.12** 证明：若 $n \geqslant m$，则 S_n 中的 m-轮换一共有：

$$\frac{n(n-1)(n-2)\cdots(n-m+1)}{m}$$

注 提示：首先，从 n 个数中，取 m 个数进行排列. 然后，注意到对一个特定的 m-轮换，有 m 种排列方式，于是得证.

✍ **练习 5.13** 证明：若 $n \geqslant 4$，则 S_n 中形如两个不相交的 2-轮换乘积的元素，一共有

$$n(n-1)(n-2)(n-3)/8$$

✍ **练习 5.14** 证明：若 $m \neq n$，则 S_m 和 S_n 不同构.

✍ **练习 5.15** 试用“生成元 + 关系”表达法表达 S_3.

【提示：$S_3 \simeq D_6$】

✍ **练习 5.16** 证明：D_{24} 和 S_4 不同构.

注 提示：考虑阶为 2 的元素个数.

✍ **练习 5.17*** 证明：对任意两个有限集 Δ, Ω，若 $|\Delta| = |\Omega|$，则 $\mathrm{Perm}(\Delta) \simeq \mathrm{Perm}(\Omega)$.

注 读者可以依次证明下列命题.

1. 证明：存在一个双射 $\theta : \Delta \to \Omega$；
2. 定义

$$\varphi : \mathrm{Perm}(\Delta) \to \mathrm{Perm}(\Omega)$$
$$\sigma \mapsto \theta\sigma\theta^{-1}$$

. 证明：$\theta\sigma\theta^{-1} \in \mathrm{Perm}(\Omega)$；（从而 φ 是良定义的）
3. φ 是双射；
4. φ 是群同态.

（二）置换的奇偶性

✍ **练习 5.18** 证明：对任意置换 σ，σ^2 是偶置换.

（三）对称群的生成元

✍ **练习 5.19** 证明：S_n 可由 $\{(1 \quad i) | \, 2 \leqslant i \leqslant n-1\}$ 生成.

注 提示：$(i\ j) = (1\ i)(1\ j)(1\ i)$.

✍ **练习 5.20** 证明：S_n 可由 $\{(i \quad i+1) | \, 1 \leqslant i \leqslant n-1\}$ 生成.

注 提示：$(i\ i+1)(1\ i)(i\ i+1) = (1\ i+1)$.

✍ **练习 5.21** 对任意 $n \geqslant 2$，证明：$S_n = \langle (1\ 2), (1\ 2\ 3\ \cdots\ n) \rangle$.

证明 对 n 使用数学归纳法：

$n = 2$ 时显然成立.

假设 $n = k$ 时成立，当 $n = k+1$ 时，因为

$$(1\ 2)(1\ 2\ 3\ \cdots\ n) = (2\ 3\ \cdots\ n)$$
$$(1\ 2\ 3\ \cdots\ n)(1\ 2) = (1\ 3\ \cdots\ n)$$
$$(2\ 3\ \cdots\ n)(1\ 3\ \cdots\ n)^{-1} = (1\ 2\ 3)$$
$$(1\ 2)(1\ 2\ 3) = (2\ 3).$$

而由归纳假设，$\langle (2\ 3), (2\ 3\ \cdots\ n) \rangle = S(\{2, 3, \cdots, n\})$。从而可以生成 $(2\ 3), \cdots, (n-1\ n)$. 结合 $(1\ 2)$，利用上一题的结论可得 $n = k+1$ 时成立.

综上所述，原命题成立.

✍ **练习 5.22** 对任意素数 p，证明：$S_p = \langle \sigma, \tau \rangle$. 其中 σ 是任意对换，τ 是任意 p-轮换.

注 提示：不妨记 $\tau = (a_1\ a_2\ \cdots\ a_p)$，$\sigma = (a_i\ a_{i+j})$，于是 $\tau^j = (a_i\ a_{i+j}\ a_{\overline{i+2j}} \cdots)$，利用上一题的结论即证.

✍ **练习 5.23** 证明：由 A_4 的任意一个 2 阶和 3 阶元素生成的子群，为 A_4 本身.

注 提示：任取 A_4 中的 2 阶元素 $(1\ 2)(3\ 4)$。我们只需证明：$\langle (1\ 2\ 3), (1\ 2)(3\ 4) \rangle = A_4$，$\langle (2\ 1\ 3), (1\ 2)(3\ 4) \rangle = A_4$. （其他组合可以通过置换 $1, 2, 3, 4$ 获得）

以 $\langle (1\ 2\ 3), (1\ 2)(3\ 4) \rangle = A_4$ 为例.

$$(1\ 2\ 3) = (1\ 3)(1\ 2)$$
$$(1\ 2\ 3)^{-1} = (1\ 2)(1\ 3)$$
$$(1\ 2\ 3)(1\ 2)(3\ 4) = (1\ 4)(1\ 3)$$
$$((1\ 4)(1\ 3))^{-1} = (1\ 3)(1\ 4)$$
$$(1\ 2)(1\ 3)(1\ 3)(1\ 4) = (1\ 2)(1\ 4)$$
$$(1\ 4)(1\ 3)(1\ 3)(1\ 2) = (1\ 4)(1\ 2)$$

由以上六个元素，即可生成 A_4.

✍ **练习 5.24** 证明：若 x, y 是 S_4 中不同的 3-轮换，且满足 $x \neq y^{-1}$，则 $\langle x, y\rangle = A_4$.
注 提示：只需证明：$\langle (1\,2\,3), (1\,2\,4)\rangle = A_4$.

$$
\begin{aligned}
(1\,2\,3) &= (1\,3)(1\,2)\\
(1\,2\,3)^{-1} &= (1\,2)(1\,3)\\
(1\,2\,4) &= (1\,4)(1\,2)\\
(1\,2\,4)^{-1} &= (1\,2)(1\,4)\\
(1\,4)(1\,2)(1\,2)(1\,3) &= (1\,4)(1\,3)\\
(1\,3)(1\,2)(1\,2)(1\,4) &= (1\,3)(1\,4)
\end{aligned}
$$

由以上六个元素，即可生成 A_4。

✍ **练习 5.25** 设 x, y 是 S_n 中的 3-轮换. 证明：$\langle x, y\rangle$ 同构于 $\mathbb{Z}_3, A_4, A_5$ 或 $\mathbb{Z}_3 \times \mathbb{Z}_3$.

（四）对称群的子群结构

✍ **练习 5.26** 证明：$G = \langle (1\,3), (1\,2\,3\,4)\rangle \simeq D_8$，从而 G 是 S_4 的真子群.
注 提示：令 $r = (1\,2\,3\,4)$，$s = (1\,3)$，于是

$$\langle (1\,3), (1\,2\,3\,4)\rangle = \left\langle r, s \middle| s^4 = s^2 = 1,\ rs = sr^{-1}\right\rangle \simeq D_8.$$

✍ **练习 5.27** 证明：A_4（唯一的）4 阶子群是正规子群，且同构于 V_4.
注 提示：这一子群为 $\langle (1\,2)(3\,4), (1\,3)(2\,4)\rangle$.

✍ **练习 5.28** 证明：S_4 没有子群同构于 Q_8.
证明 假设存在群单同态 $\varphi : Q_8 \to S_4$. 考虑 Q_8 中的 2 阶元素 -1，有三个不同的 4 阶元素 i, j, k，使得 $i^2 = j^2 = k^2 = -1$.

而 S_4 中的 2 阶元素有两种共轭类，分别考虑其代表元 $(1\,2), (1\,2)(1\,3)$. 对于 $(1\,2)$，没有元素满足其平方为 $(1\,2)$. 对于 $(1\,2)(3\,4)$，只有两个元素 $(1\,3\,2\,4), (1\,4\,2\,3)$ 满足其平方为 $(1\,2)(3\,4)$.

于是，-1 不可能与任何一个 S_4 中的元素对应，即这样的群单同态不存在.

✍ **练习 5.29*** 证明：对任意 $n \geqslant 3$，A_n 包含一个同构于 S_{n-2} 的子群.
注 提示：考虑映射：

$$
\begin{aligned}
\varphi : S_{n-2} &\to A_n\\
(1\,i) &\mapsto (1\,i)(n-1\,n)
\end{aligned}
$$

此为群单同态.

✍ **练习 5.30** 证明：每个 A_n 中的 2 阶元素，都是 S_n 中某个 4 阶元素的平方.
注 提示：对 A_n 中的每个元素做轮换分解，于是阶为 2 的元素只能包含偶数个（记为 $2k$）对换，不妨记为

$$\sigma = (a_1\ a_1') \cdots (a_{2k}\ a_{2k}')$$

考虑 S_n 中的元素

$$(a_1\ a_2\ a_1'\ a_2') \cdots (a_{2k-1}\ a_{2k}\ a_{2k-1}'\ a_{2k}')$$

容易验证其阶为 4，且平方 $= \sigma$.

5.2 群作用

5.2.1 知识要点

（一）群作用的概念

1. 群 G 对集合 A 的左作用：映射 $\psi: G\times A\to A$, $(g,a)\mapsto g\cdot a$,（在不混淆的情形下，可以简记为 ga）满足：
   (a). 对任意的 $g,h\in G$，$a\in A$，有 $g\cdot(h\cdot a)=(gh)\cdot a$；
   (b). 对任意的 $a\in A$ 与幺元 $1\in G$，有 $1\cdot a=a$.
2. 置换表示（左作用的等价定义）：定义群同态 $\varphi: G\to \mathrm{Perm}(A)$, $g\mapsto \sigma_g$，且定义置换 $\sigma_g: A\to A$, $a\mapsto g\cdot a$.

（二）轨道与稳定化子

1. 作用的核：同态 $\varphi: G\to S_A$ 的核，即
$$\ker\varphi=\{g\in G:\ \forall a\in A,\ g\cdot a=a\}.$$
2. 群作用忠实：作用的核为 $\{1\}$.
3. 群 G 中，元素 $a\in A$ 的稳定化子：（有的采用记号 G_a，本书使用 $\mathrm{Stab}(a)$）
$$\mathrm{Stab}(a):=\{g\in G:\ g\cdot a=a\}$$
4. （稳定化子的性质）：
   (a). （子群）：对任意 $a\in A$，有 $\mathrm{Stab}(a)<G$.
   (b). （交）：$\cap_{a\in A}\mathrm{Stab}(a)=\ker\varphi$.
5. 元素 $a\in A$ 的轨道：（有的采用记号 $\mathcal{O}$ 或 Ga，本书使用 $\mathrm{Orb}(a)$）
$$\mathrm{Orb}(a):=\{g\cdot a:\ g\in G\}.$$
6. （轨道的性质）：
   (a). （等价类）：定义在 A 上的关系
$$a\sim b\iff \exists g\in G, a=g\cdot b$$
   是等价关系. 等价类即为各不同的轨道.
   (b). （轨道公式）：对任意 $a\in A$，有 $|\mathrm{Orb}(a)|=[G:\mathrm{Stab}(a)]$.
7. 群作用传递：群作用只有一个轨道.

5.2.2 知识要点解读

（一）群作用的概念

群作用的概念，对于初学者来说较为复杂，我们先来看它的两种定义的等价性，在此过程中进一步熟悉群作用.

问题 5.3 （等价定义）：证明群作用的两个定义（“公理定义”、“置换表示”）等价.

注 其实这里对于每个读者来说，都是没有难度的，只需要按照定义的字面意思，利用最基本的处理手法就可以了. 于是这一问题的难度主要在于读者内心的胆怯. 笔者认为，一个人对于自己不熟悉的事情，总会有本能的一点点担心，这是正常的，但是抱着担心不再前进，就比较遗憾了.

证明

1. 首先，已知“公理定义”，我们定义映射
$$\varphi: G\to(\mathrm{Perm}(A),\circ)$$
$$g\mapsto\sigma_g$$

且每个置换 σ_g 定义为：

$$\begin{aligned}\sigma_g : A &\to A\\ a &\mapsto g\cdot a\end{aligned}$$

我们需要证明：φ 是群同态.
对任意的 $g,h\in G$，和任意的 $a\in A$，有：

$$\begin{aligned}\varphi(gh)(a) &= \sigma_{gh}(a)\\ &= (gh)\cdot a\\ &= g\cdot(h\cdot a)\\ &= g\cdot(\sigma_h(a))\\ &= \sigma_g(\sigma_h(a))\\ &= (\sigma_g\circ\sigma_h)(a)\\ &= (\varphi(g)\circ\varphi(h))(a)\end{aligned}$$

也就是 $\varphi(gh)=\varphi(g)\circ\varphi(h)$. 命题得证.

2. 另一方面，已知置换表示 φ 和 σ_g（与前面的证明使用同一套符号），我们需要证明通过 σ_g 定义的 $g\cdot a$，满足群作用的两条公理.
首先，由 σ_g 的定义可知，映射 $(g,a)\mapsto g\cdot a$ 存在.
其次，对任意的 $g,h\in G$，我们有

$$\begin{aligned}g\cdot(h\cdot a) &= g\cdot(\sigma_h(a))\\ &= \sigma_g(\sigma_h(a))\\ &= (\sigma_g\circ\sigma_h)(a)\\ &= (\varphi(g)\circ\varphi(h))(a)\\ &= \varphi(gh)(a)\\ &= \sigma_{gh}(a)\\ &= (gh)\cdot a\end{aligned}$$

最后，对 $1\in G$，根据同态的性质“幺元对幺元”，我们有 σ_1 为群 $\mathrm{Perm}(A)$ 的幺元，即 $\sigma(1)$ 为 A 上的恒等映射，因此

$$1\cdot a=\sigma_1(a)=a$$

综上，命题得证.

笔记 笔者在这里，刻意把计算过程写的非常详细，甚至是有一些🅵嗦，我们希望借此向读者详细地展示各种符号在计算过程中的变化，从而避免一些不必要的误解. 我们建议初学者仔细地把每个等号成立的原因都思考清楚.

（二）轨道与稳定化子

笔者认为，轨道这个词非常的形象，我们先用一个例子感受一下.

例题 5.2 取 S_4 的一个子群 $H=\langle(1\ 2),(3\ 4)\rangle$，定义 H 对集合 $A=\{1,2,3,4\}$ 的作用为（实际上就是最直白的那种）：

$$(a_1\ a_2\ a_3\ a_4)(a_1)=a_2.$$

于是，该群作用一共有两条轨道：

$$\begin{aligned}O_1&=\{1,2\}\\ O_2&=\{3,4\}\end{aligned}$$

得到这两条轨道也并不难，首先给出 H 中的所有元素：

$$H=\{1,(1\ 2),(3\ 4),(1\ 2)(3\ 4)\}$$

然后，我们考虑 $1\in A$ 所在的轨道（记为 O_1）. 分别考虑 H 中的元素作用在 1 上的结果，可得 O_1 中包含 $1,2$ 两个元素. 也许有读者会想，我们还需不需要继续考虑 H 的诸元素作用在 2 上的结果？实际上是不需要的，因为：

$$2=(1\ 2)(1)$$

所以对任意的 $h\in H$ 有

$$h\cdot 2=h\cdot((1\ 2)(1))=(h(1\ 2))\cdot 1$$

而 $h(1\ 2)\in H$. 所以 H 对 2 作用的结果，已经包含在了 H 对 1 作用的结果中，由此我们可得 $O_1=\{1,2\}$.（O_2 也可类似求得）

笔记 本例想说明的一个问题是，对于一般意义下群 G 对集合 A 作用而言，包含元素 $a\in A$ 的轨道是 $\mathrm{Orb}(a)$. 而对任意 $b\in\mathrm{Orb}(a)$，b 所在的轨道还是 $\mathrm{Orb}(a)$（也就是 $\mathrm{Orb}(a)=\mathrm{Orb}(b)$）. 通俗的说法就是：同一轨道中的元素共享同一个轨道.（很明显，这是一句正确的废话，当然读者需要意识到这是一句废话才好）

由于有了轨道的概念，群作用提供了一个集合 A 的划分（等价地说，定义了 A 上的一个等价关系）. 也就是说，$a\in A$ 的轨道，揭示了 a 与其他 A 中的元素的联系，从而呈现了集合 A 的结构. 但是，我们更关心的，并不是集合 A 的结构（对于集合而言，讨论它的结构似乎也没有什么意义），而是群 G 的结构. 于是，我们反过来站在元素 a 的角度，考察群 G 中的元素的性质. 稳定化子就是这样性质的一个概念.

稳定化子的概念是不难理解的. 站在元素 a 的角度，我们把对他作用“无效”的元素挑出来，就构成了 a 的稳定化子. 由于群作用本身具有的性质较好，所以这些元素构成了一个群.

问题 5.4（轨道化子是子群）：对任意 $a\in A$，有 $\mathrm{Stab}(a)<G$.

证明 首先，$1\cdot a=a$，所以 $1\in\mathrm{Stab}(a)$.

其次，对任意的 $h\in\mathrm{Stab}(a)$，有

$$\begin{aligned}h\cdot a&=a\\ h^{-1}\cdot(h\cdot a)&=h^{-1}\cdot a\\ (h^{-1}h)\cdot a&=h^{-1}\cdot a\end{aligned}$$

即 $h^{-1}\cdot a=a$. 所有对任意的 $g,h\in\mathrm{Stab}(a)$，有

$$\begin{aligned}(gh^{-1})\cdot a&=g\cdot(h^{-1}\cdot a)\\ &=g\cdot a\\ &=a.\end{aligned}$$

综上，$\mathrm{Stab}(a)<G$.

笔记 请读者注意，千万不要不假思索地写出

$$h^{-1}\cdot a=(h\cdot a)^{-1}$$

这样贻笑大方的式子.

因为 a 的稳定化子是子群，所以可以对其应用 Lagrange 定理：

$$|G|=[G:\mathrm{Stab}(a)]\,|\mathrm{Stab}(a)|$$

其中 $\mathrm{Stab}(a)$ 的指数，还可以有另一种解读的方式，这就是轨道公式.

问题 5.5（轨道公式）：对任意 $a\in A$ 与 $g\in G$，定义群 G 对 A 的作用 $g\cdot a$，则 $|\mathrm{Orb}(a)|=[G:\mathrm{Stab}(a)]$.

证明 定义从 a 的轨道到 $\mathrm{Stab}(a)$ 的左陪集全体的映射：

$$f:g\cdot a\mapsto g\,\mathrm{Stab}(a).$$

下证：f 是双射. 我们只需证明：对任意的 $g,h\in G$，$g\cdot a=h\cdot a$，当且仅当 $g\,\mathrm{Stab}(a)=h\,\mathrm{Stab}(a)$.

我们有：

$$\begin{aligned} g\cdot a=h\cdot a &\iff h^{-1}\cdot(g\cdot a)=h^{-1}\cdot(h\cdot a)\\ &\iff (h^{-1}g)\cdot a=a\\ &\iff h^{-1}g\in \mathrm{Stab}(a)\\ &\iff g\,\mathrm{Stab}(a)=h\,\mathrm{Stab}(a). \end{aligned}$$

a 的轨道中的元素个数为 $|\mathrm{Orb}(a)|$，$\mathrm{Stab}(a)$ 的左陪集全体中的元素个数为 $[G:\mathrm{Stab}(a)]$，所以有 $|\mathrm{Orb}(a)|=[G:\mathrm{Stab}(a)]$.

笔记 构造双射的做法，我们在陪集一节已经使用多次了.

5.2.3 典型例题

（一）群作用的例子

例题 5.3 已知群 G，定义群对自身的“左乘作用”：对任意的 $g,a\in G$，有 $g\cdot a:=ga$（ga 表示群 G 内的乘法），证明：“左乘作用”是群 G 对自身的群作用.

注 以下我们对两种定义分别验证.

证明 [1]（公理定义）：首先，对任意 $g,h,a\in G$，我们有：

$$\begin{aligned} g\cdot(h\cdot a)&=g\cdot(ha)\\ &=g(ha)\\ &=(gh)a\\ &=(gh)\cdot a. \end{aligned}$$

其次，对于 $1\in G$，有：$1\cdot a=1a=a$.

综上，命题得证.

证明 （置换表示）：“左乘作用”定义了映射：

$$\begin{aligned} \varphi: G&\to(\mathrm{Perm}(G),\circ)\\ g&\mapsto\sigma_g \end{aligned}$$

且每个 σ_g 定义为：

$$\begin{aligned} \sigma_g: G&\to G\\ a&\mapsto g\cdot a \end{aligned}$$

我们首先要证明，σ_g 确为 G 上的置换，从而 $\sigma_g\in\mathrm{Perm}(G)$. 而对任意的 $g,a,b\in G$，有：

$$\begin{aligned} \sigma_g(a)=\sigma_g(b) &\iff g\cdot a=g\cdot b\\ &\iff ga=gb\\ &\iff a=b \end{aligned}$$

从而 σ_g 为 G 上的置换.

再验证 φ 是个同态，这是因为：对任意的 $g,h,a\in G$，

$$\begin{aligned}\varphi(gh)(a)&=\sigma_{gh}(a)\\&=(gh)\cdot a\\&=gha\\&=g(ha)\\&=g\cdot(ha)\\&=\sigma_g(ha)\\&=\sigma_g(h\cdot a)\\&=\sigma_g(\sigma_h(a))\\&=\sigma_g\circ\sigma_h(a)\\&=\varphi(g)\circ\varphi(h)(a)\end{aligned}$$

从而有：$\varphi(gh)=\varphi(g)\circ\varphi(h)$.

笔记 笔者个人认为，公理定义形式上简洁一些，实际应用也更方便一些，但是对于初学者来说不那么好理解；而置换表示则恰恰相反，它联系了我们前面已经很熟悉的同态，所以更好理解，但是形式上相对繁琐. 两种定义读者都需要很熟悉.

（二）轨道与稳定化子

例题 5.4 设群 G 作用于 A. 证明：

1. 若 $a,b\in A$，存在 $g\in G$ 使得 $b=g\cdot a$，则 $\mathrm{Stab}(b)=g\,\mathrm{Stab}(a)g^{-1}$；
2. 若 G 对 A 的作用传递，则该作用的核 N 为 $\cap_{g\in G}g\,\mathrm{Stab}(a)g^{-1}$.

证明

1. 一方面，对任意的 $h\in\mathrm{Stab}(a)$，有：

$$\begin{aligned}(ghg^{-1})\cdot b&=ghg^{-1}\cdot(g\cdot a)\\&=gha\\&=ga\\&=b\end{aligned}$$

从而 $ghg^{-1}\in\mathrm{Stab}(b)$，即 $g\,\mathrm{Stab}(a)g^{-1}\subset\mathrm{Stab}(b)$.

另一方面，对任意的 $k\in\mathrm{Stab}(b)$，有：

$$\begin{aligned}(g^{-1}kg)\cdot a&=g^{-1}kg(g^{-1}\cdot b)\\&=g^{-1}\cdot(k\cdot b)\\&=g^{-1}\cdot b\\&=a\end{aligned}$$

从而 $g^{-1}kg\in\mathrm{Stab}(a)$，即 $g^{-1}\,\mathrm{Stab}(b)g\subset\mathrm{Stab}(a)$，也就是 $\mathrm{Stab}(b)\subset g\,\mathrm{Stab}(a)g^{-1}$.

综上：$\mathrm{Stab}(b)=g\,\mathrm{Stab}(a)g^{-1}$.

2. 若 G 对 A 的作用传递，则 $\mathrm{Orb}(a)=A$，从而：

$$\begin{aligned} N &= \bigcap_{a'\in A} \mathrm{Stab}(a') \\ &= \bigcap_{g\cdot a\in \mathrm{Orb}(a)} \mathrm{Stab}(g\cdot a) \\ &= \bigcap_{g\in G} g\,\mathrm{Stab}(a)g^{-1} \end{aligned}$$

笔记 第二小问连等式的第二个等号是一次指标变换，其道理在于，遍历集合 A 中的元素就相当于遍历 $\mathrm{Orb}(a)$ 中的元素，因为 $A=\mathrm{Orb}(a)$. 而 $\{g\cdot a\}_{g\in G}$ 可以遍历 $\mathrm{Orb}(a)$. 我们在后面的学习中还会碰到很多各式各样的指标变换.

练习 5.31 设群 G 在集合 A 上的作用传递，$N\lhd G$，证明：A 在 N 的作用下的轨道有同样多的元.

证明 只需证：在 N 的作用下，对任意的 $a,b\in A$，有 $|\mathrm{Orb}(a)|=|\mathrm{Orb}(b)|$. 即证：$|\mathrm{Stab}(a)|=|\mathrm{Stab}(b)|$.

由于 G 对 a 的作用传递，所以对于 $a,b\in A$，存在 $g\in G$，使得 $g\cdot b=a$（从而 $g^{-1}\cdot a=b$）. 定义映射

$$\begin{aligned} f:\mathrm{Stab}(a) &\to \mathrm{Stab}(b) \\ n &\mapsto g^{-1}ng \end{aligned}$$

1. 先证明：当 $n\in\mathrm{Stab}(a)$ 时有 $g^{-1}ng\in\mathrm{Stab}(b)$.

   首先，$\mathrm{Stab}(a),\mathrm{Stab}(b)$ 是在 N 的作用下定义的，由于 $N\lhd G$，所以 $g^{-1}ng\in N$. 然后：

$$\begin{aligned} (g^{-1}ng)\cdot b &= (g^{-1}n)\cdot(g\cdot b) \\ &= g^{-1}\cdot(n\cdot a) \\ &= g^{-1}\cdot a \\ &= b \end{aligned}$$

   于是 $g^{-1}ng\in\mathrm{Stab}(b)$.
2. 再证明：f 是双射. 也就是说，证明：对于任意的 $n_1,n_2\in\mathrm{Stab}(a)$，$n_1=n_2$，当且仅当 $g^{-1}n_1g=g^{-1}n_2g$. 而这是显然成立的.

综上，$|\mathrm{Stab}(a)|=|\mathrm{Stab}(b)|$，原命题即证.

笔记 本题如果直接从轨道的角度破题，会比较繁琐. 先利用轨道公式，将轨道的关系转换成稳定化子的关系再破题，则相对简单.

5.2.4 习题

以下均假设 G 是群，A 是非空集.

（一）群作用的基本概念

练习 5.32 定义 $\mathbb{Z}$ 对自身的作用：对任意 $z,a\in\mathbb{Z}$，$z\cdot a:=z+a$. 证明：这是一个群作用.

练习 5.33 定义 $\mathbb{R}$ 对 $\mathbb{R}^2$ 的作用：对任意的 $r\in\mathbb{R},(x,y)\in\mathbb{R}^2$，$r\cdot(x,y):=(x+ry,y)$. 证明：这是一个群作用.

练习 5.34 定义 $(\mathbb{R}^*,\cdot)$ 对群 $(\mathbb{R}^n,+)$ 的作用：$\alpha(r_1,\cdots,r_n):=(\alpha r_1,\cdots,\alpha r_n)$. 这是一个群作用.

注 本题实际上来源于线性空间 $\mathbb{R}^n$ 的性质. 以后我们会知道，线性空间即为“域对加群的作用”.

练习 5.35 设正整数 $k\leqslant|A|$，集族 $\mathcal{B}=\{C\subset A:|C|=k\}$. 定义 $\mathrm{Perm}(A)$ 对 $\mathcal{B}$ 的作用：

$$\sigma\cdot\{a_1,\cdots,a_k\}:=\{\sigma(a_1),\cdots,\sigma(a_k)\}.$$

1. 证明：这是一个群作用；
2. 设 $A=\{1,2,3,4\}$，$k=2$，试给出 $(1\,2)$ 和 $(1\,2\,3)$ 对 $\mathcal{B}$ 中每个元素的作用结果.

3. 当 k 取何值时，该群作用为忠实的?

证明

1. 首先，对任意 $\sigma,\tau\in \mathrm{Perm}(A)$ 和任意 $\{a_1,\cdots,a_k\}\in\mathcal{B}$，有

$$\begin{aligned}\sigma(\tau\{a_1,\cdots,a_k\}) &= \sigma\{\tau(a_1),\cdots,\tau(a_k)\}\\ &= \{\sigma(\tau(a_1)),\cdots,\sigma(\tau(a_k))\}\\ &= \{(\sigma\tau)(a_1),\cdots,(\sigma\tau)(a_k)\}\\ &= (\sigma\tau)\{a_1,\cdots,a_k\}.\end{aligned}$$

   其次，对 $1\in\mathrm{Perm}(A)$ 和任意 $\{a_1,\cdots,a_k\}\in\mathcal{B}$，有

$$\begin{aligned}1\{a_1,\cdots,a_k\} &= \{1(a_1),\cdots,1(a_k)\}\\ &= \{a_1,\cdots,a_k\}\end{aligned}$$

   综上，有题设定义的作用为群作用.

2. 按定义计算即可，结果为:

$$\begin{aligned}(1\ 2)\{1,2\}&=\{1,2\}\\ (1\ 2)\{1,3\}&=\{2,3\}\\ (1\ 2)\{1,4\}&=\{2,4\}\\ (1\ 2)\{2,3\}&=\{1,3\}\\ (1\ 2)\{2,4\}&=\{1,4\}\\ (1\ 2)\{3,4\}&=\{3,4\}\\ (1\ 2\ 3)\{1,2\}&=\{2,3\}\\ (1\ 2\ 3)\{1,3\}&=\{1,2\}\\ (1\ 2\ 3)\{1,4\}&=\{2,4\}\\ (1\ 2\ 3)\{2,3\}&=\{1,3\}\\ (1\ 2\ 3)\{2,4\}&=\{3,4\}\\ (1\ 2\ 3)\{3,4\}&=\{1,4\}\end{aligned}$$

3. 若 $k=n$，则任意 $\sigma\in\mathrm{Perm}(A)$ 都是核中的元素，因为 $\sigma\cdot A=A$.
   而 $k<n$ 时，对任意不等于 1 的 $\sigma=(a_1'\ \cdots\ a_l')\in\mathrm{Perm}(A)$，都有集合 $C\in\mathcal{B}$，使得 $a_1'\in C$，而 $a_2'\notin C$，从而 $\sigma\cdot C\neq C$，也就是说，σ 不是核中的元素，于是核只能为 $\{1\}$.
   综上，$k<n$ 时，表示都是忠实的.

✍ **练习 5.36** 设正整数 $k\leqslant|A|$，$B=\{(a_1,\cdots,a_k):\ a_i\in A,\forall i\}$. 定义 $\mathrm{Perm}(A)$ 对 B 的作用:

$$\sigma\cdot(a_1,\cdots,a_k):=(\sigma(a_1),\cdots,\sigma(a_k)).$$

1. 证明: 这是一个群作用;
2. 设 $A=\{1,2,3,4\}$，$k=2$，试给出 $(1\ 2)$ 和 $(1\ 2\ 3)$ 对 B 中每个元素的作用结果.
3. 当 k 取何值时，该群作用为忠实的?

注 提示: 解题过程与前一题基本一致，注意两题的不同: 这里 B 的元素是有序数组，而前一题 $\mathcal{B}$ 的元素为集合(从而本质为无序数组)，于是两题的结果并不相同.

第三小问，$k\leqslant n$ 均可.

✍ **练习 5.37** 设 R 是变量为 x_1, x_2, x_3, x_4 的整系数多项式的集合. 定义 S_4 对 R 的作用：

$$\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}). \tag{5.1}$$

求给定 $p(x)$ 的稳定化子，及其所在的轨道

1. $p(x) = x_1 + x_2$;
2. $p(x) = x_1x_2 + x_3x_4$;
3. $p(x) = (x_1 + x_2)(x_3 + x_4)$.

✍ **练习 5.38** 证明：群 G 对 A 的作用的核 $N = \{g \in G : ga = a, \forall a \in A\}$.

证明 设 G 对 A 的作用为同态 $\varphi : G \to \mathrm{Perm}(A)$，由定义，$N = \ker \varphi$，于是有：

$$\begin{aligned} N &= \ker \varphi \\ &= \{g \in G : \varphi(g) = 1\} \\ &= \{g \in G : ga = a, \forall a \in A\} \end{aligned}$$

（二）轨道与稳定化子

✍ **练习 5.39** 设 $A = \{(i, j) : i, j \in \{1, 2, 3\}\}$，定义 S_3 对 A 的作用：$\sigma((i, j)) = (\sigma(i), \sigma(j))$.

1. 求出 S_3 在 A 上的所有轨道;
2. 求 $\mathrm{Stab}((1, 1))$ 和 $\mathrm{Stab}((1, 2))$.

注 参考答案：

1. 一共有两条轨道：

$$\begin{aligned} O_1 &:= \{(i, i) : i \in \{1, 2, 3\}\} \\ O_2 &:= \{(i, j) : i, j \in \{1, 2, 3\}, i \neq j\}. \end{aligned}$$

2.

$$\begin{aligned} \mathrm{Stab}((1, 1)) &= \{1, (2\ 3)\} \\ \mathrm{Stab}\,(1, 2) &= \{1\} \end{aligned}$$

✍ **练习 5.40** 设 $A = \{\{i, j\} : i, j \in \{1, 2, 3\}\}$，定义 S_3 对 A 的作用：$\sigma(\{i, j\}) = \{\sigma(i), \sigma(j)\}$.

1. 求出 S_3 在 A 上的所有轨道;
2. 求 $\mathrm{Stab}(\{1, 1\})$ 和 $\mathrm{Stab}(\{1, 2\})$.

注 参考答案：

1. 一共有两条轨道：

$$\begin{aligned} O_1 &:= \{\{i, i\} : i \in \{1, 2, 3\}\} \\ O_2 &:= \{\{i, j\} : i, j \in \{1, 2, 3\}, i < j\}. \end{aligned}$$

2.

$$\begin{aligned} \mathrm{Stab}(\{1, 1\}) &= \{1, (2\ 3)\} \\ \mathrm{Stab}\,\{1, 2\} &= \{1, (1\ 2)\} \end{aligned}$$

请读者体会本题与上一题的区别.

此外，如果读者需要更多的练习来熟悉轨道与稳定化子的定义，可以将本题与上题中的 A 替换为更大的集族或有序列的集合（例如 $\{C \subset \{1, 2, 3\} : C \neq \varnothing\}$），然后重做后续的题目.

✍ **练习 5.41** 设群 G 是 A 的置换群（即 $G < \mathrm{Perm}(A)$）. 证明：

1. 设 $\sigma \in G, a \in A$，则 $\mathrm{Stab}(\sigma(a)) = \sigma\,\mathrm{Stab}(a)\sigma^{-1}$;

2. 若 G 对 A 的作用传递，则：

$$\cap_{\sigma\in G}\sigma\,\mathrm{Stab}(a)\sigma^{-1}=\{1\}.$$

注 提示：本题是前一题结论的直接应用，注意到 G 对 A 的作用必然为忠实的，于是该作用的核为 $\{1\}$.

✍ **练习 5.42** 设交换群 G 是 A 的置换群（即 $G<\mathrm{Perm}(A)$），且 G 对 A 的群作用传递. 证明：

1. 对任意的 $\sigma\in G-\{1\}$ 和 $a\in A$，有 $\sigma(a)\neq a$；
2. $|G|=|A|$.

注 提示：利用前一题的结论，注意到 G 是交换群，所以

$$\begin{aligned}\mathrm{Stab}(\sigma(a))&=\sigma\,\mathrm{Stab}(a)\sigma^{-1}\\&=\sigma\sigma^{-1}\,\mathrm{Stab}(a)\\&=\mathrm{Stab}(a).\end{aligned}$$

而该群作用又传递，从而

$$\begin{aligned}\{1\}&=\cap_{\sigma\in G}\sigma\,\mathrm{Stab}(a)\sigma^{-1}\\&=\cap_{\sigma\in G}\mathrm{Stab}(a)\\&=\mathrm{Stab}(a).\end{aligned}$$

以下两个命题就都容易证明了.

✍ **练习 5.43*** （Burnside 引理）：设群 G 作用在集合 A 上，t 是 A 在 G 的作用下的轨道个数. 对任意的 $g\in G$，定义 $F(g)=|\{a\in A:\ g\cdot a=a\}|$. 证明：

$$t|G|=\sum_{g\in G}F(g).$$

注 这是一道“抽象计数”类的问题，我们以前学过的“陪集”一节就包含了很多这样的问题（例如 Lagrange 定理的证明）.

计数问题的关键，直白地说，就在于按什么方式数数. 比如 Lagrange 定理 $|G|=|H|[G:H]$，等式左侧是从群的视角数元素的个数，等式右侧是分别数子群的元素个数和陪集的个数，然后再乘起来（能相乘是因为，事先证明了所有陪集大小一样）. 这也启发我们，建立数量等式的一个方式是：采用两种不同的计数策略，计算同一个数量.

回到本题，所给条件非常少，一个抽象的群作用对于计数似乎是没有什么用的，轨道的个数我们目前也不知道怎么用起来（毕竟轨道的大小一般是参差不齐的）. 那么破题的关键来到了临时定义的 $F(g)$ 身上. $F(g)$ 对于我们而言是个新概念，但是其中有一个我们很熟悉的方程：$g\cdot a=a$. 我们在稳定化子的定义中见过这个方程：

$$\mathrm{Stab}(a):=\{g\in G:g\cdot a=a\}$$

对比 $\{a\in A:\ g\cdot a=a\}$ 来看，两个集合分别固定了方程中的 g 和 a. 实际上这里就在启发我们，如果存在一个需要计数的对象，计数的两个角度分别是遍历 g 和遍历 a. 这句话看起来可能有点模糊，我们举一个例子.

我们将一堆苹果排成两排四列，那么数这堆苹果就有两种方式，一种是先计算每列的苹果个数（2），再将所有列中苹果的个数相加 $2+2+2+2$，就是苹果的个数. 另一种是先计算每行的苹果个数（4），再将所有行中苹果的个数相加 $4+4$，也是这堆苹果的个数.

同样的道理，我们发现：

$$\begin{aligned}\sum_{g\in G}F(g)&=\sum_{g\in G}|\{a\in A:\ g\cdot a=a\}|\\&=\sum_{a\in A}|\{g\in G:g\cdot a=a\}|\\&=\sum_{a\in A}|\,\mathrm{Stab}(a)|.\end{aligned}$$

由此也不难得到计数对象是集合 $P:=\{(g,a)\in G\times A:g\cdot a=a\}$ 中元素的个数.

到此，我们处理了等式右侧的代数式，将之转换成了我们熟悉的稳定化子. 等式左侧出现了轨道的个数 t，“轨道 + 稳定化子”的组合，总是能让我们自然地想起轨道公式. 此时本题也就得以破解.

证明

1. 先证明：$\sum_{g\in G} F(g) = \sum_{a\in A} |\operatorname{Stab}(a)|$.
   定义集合 $P := \{(g,a) \in G \times A : g\cdot a = a\}$. 一方面：
   $$\begin{aligned} |P| &= \sum_{g\in G} |\{a \in A : g\cdot a = a\}| \\ &= \sum_{g\in G} F(g) \end{aligned}$$
   另一方面：
   $$\begin{aligned} |P| &= \sum_{a\in A} |\{g \in G : g\cdot a = a\}| \\ &= \sum_{a\in A} |\operatorname{Stab}(a)| \end{aligned}$$
   所以有 $\sum_{g\in G} F(g) = \sum_{a\in A} |\operatorname{Stab}(a)|$.
2. 再证明：设 G 对 A 作用的一条轨道是 $O = \{a_i\}_{i\in I}$（I 是指标集），则 $|G| = \sum_{i\in I} |\operatorname{Stab}(a_i)|$.
   对任意的 $a_i \in O$，由轨道公式可得 $|G|/|O| = |\operatorname{Stab}(a_i)|$. 所以对任意的 $a_i, a_j \in O$，有 $|\operatorname{Stab}(a_i)| = |\operatorname{Stab}(a_j)|$. 注意到 $|O| = |I|$，于是
   $$\begin{aligned} |G| &= |O||\operatorname{Stab}(a_i)| \\ &= \sum_{i\in I} |\operatorname{Stab}(a_i)| \end{aligned}$$
3. 最后证明原命题. 记 A 的 t 条轨道分别为 $O_1, \cdots, O_t$. 记轨道 $O_j\{a_{j,i}\}_{i\in I_j}$，则有：
   $$\begin{aligned} t|G| &= \sum_{j=1}^{t} |G| \\ &= \sum_{j=1}^{t} \sum_{i\in I_j} |\operatorname{Stab}(a_{j,i})| \end{aligned}$$
   由于所有的轨道构成 A 的划分，所以前式遍历了 A 中的所有元素，从而有：
   $$\begin{aligned} t|G| &= \sum_{a\in A} |\operatorname{Stab}(a)| \\ &= \sum_{g\in G} F(g). \end{aligned}$$

笔记 “抽象计数”类的问题，形式上是各种求和指标的转换，实质是计数策略的变化.

5.2.5 思考题

练习 5.44* 设 G 是有限群 A 的置换群，且 G 对 A 的作用传递. 定义块（block）：A 的非空子集 B，使得对任意的 $\sigma \in G$，有 $\sigma(B) = B$ 或 $\sigma(B) \cap B = \varnothing$.

1. 证明：若 B 是块，且包含 $a \in A$，则
   $$G_B = \{\sigma \in G : \sigma(B) = B\} \tag{5.2}$$
   是 G 的子群，且包含 $\operatorname{Stab}(a)$；
2. 证明：若 B 是块，且 $\sigma_1(B), \cdots, \sigma_n(B)$ 是 B 在 G 的元素下的全部不同的象，则 $\sigma_1(B), \cdots, \sigma_n(B)$ 是 A 的划分；
3. 我们称 G 在 A 上是本原的（G 同时满足题设条件），当且仅当 A 的块只有 A 和 1 阶子集. 取 $A = \{1,2,3,4\}$，证明：S_4 是本原的，但 D_8 不是本原的；

4. 证明：G 在 A 上是本原的，当且仅当对任意的 $a\in A$，包含 $\mathrm{Stab}(a)$ 的子群只有 $\mathrm{Stab}(a)$ 和 G.

证明

1. 首先，$1\in G_B$，所以 G_B 非空. 其次，对任意的 $\sigma,\tau\in G_B$，有：
$$\begin{aligned}\sigma\tau^{-1}(B)&=\sigma(B)\\&=B\end{aligned}$$
从而 $\sigma\tau^{-1}\in G_B$，于是 $G_B<G$.
对于任意 $\rho\in\mathrm{Stab}(a)$，有 $a\in B$，且 $a=\rho a\in\rho(B)$，从而 $\rho(B)\cap B$ 非空，而 B 为块，所以只能有 $\rho(B)=B$，即 $\rho\in G_B$. 所以 $\mathrm{Stab}(a)\subset G_B$.
2. 先证明：若 $\sigma_i(B)\cap\sigma_j(B)$ 非空，则 $\sigma_i(B)=\sigma_j(B)$. 设 $a\in\sigma_i(B)\cap\sigma_j(B)$，则存在 $b_1,b_2\in B$，使得 $a=\sigma_ib_1=\sigma_jb_2$，于是 $b_1=\sigma_i^{-1}\sigma_jb_2\in B$，即 $\sigma_i^{-1}\sigma_j(B)\cap B$ 非空. 由于 B 是块，所以只能有 $\sigma_i^{-1}\sigma_j(B)=B$，即 $\sigma_j(B)=\sigma_i(B)$.
再证：所有的 $\sigma_i(B)$ 的并等于 A. 由于任意 $\sigma_i(B)$ 和 $\sigma_j(B)$ 不相交，因此
$$\cup_{i=1}^n\sigma_i(B)=\cup_{g\in G}g(B)$$
而由于 G 对 A 的作用传递，所以任取 $b\in B$，有 $Gb=A$，于是：
$$A=Gb=\cup_{g\in G}\{gb\}\subset\cup_{g\in G}g(B)=\cup_{i=1}^n\sigma_i(B).$$
另一方面：任意的 $\sigma_i(B)\subset A$，于是 $\cup_{i=1}^n\sigma_i(B)\subset A$，从而只能有
$$\cup_{i=1}^n\sigma_i(B)=A$$
综上，A 是所有的 $\sigma_i(B)$ 的无交并，即所有的 $\sigma_i(B)$ 是 A 的划分.
3. 对 S_4，考虑 A 的子集 $B=\{a,b\}$ 和 $C=\{a,b,c\}$，于是 $(b\ d)(B)=\{a,d\}$（既不等于 B，也不是和 B 无交），$(b\ d)(C)=\{a,b,d\}$，从而 A 没有 2 阶或 3 阶的块，即 S_4 在 A 上本原.
对 $D_8=\langle r=(1\,2\,3\,4),s=(2\,4)\rangle$，考虑 $B=\{2,4\}$，记 $C=\{1,3\}$，有：
$$\begin{aligned}1(B)&=B\\r(B)&=C\quad(\cap B=\varnothing)\\r^2(B)&=B\\r^3(B)&=C\\s(B)&=B\\rs(B)&=C\\r^2s(B)&=B\\r^3s(B)&=C\end{aligned}$$
于是 B 是 A 的块，从而 D_8 在 A 上不是本原的.
4. ?

✍ **练习 5.45** 群 G 对 A 的传递的作用被称为是双传递（或 2-传递）的，如果对任意的 $a\in A$，$\mathrm{Stab}(a)$ 在集合 $A-\{a\}$ 上传递. 证明：

1. 对任意的整数 $n\geqslant 2$，S_n 对 $A=\{1,2,\cdots,n\}$ 的作用是双传递的；
2. 若 G 对 A 的作用双传递，则也是本原的；
3. D_8 对集合 $A=\{1,2,3,4\}$ 的作用不是双传递的.

证明

1. 对任意的 $k\in A$，$\mathrm{Stab}(k)$ 由所有不包含 k 的置换构成，从而 $\sigma:=(1\,2\,\cdots\,k-1\,k+1\,\cdots\,n)\in\mathrm{Stab}(k)$. 而 σ 对 $A-\{k\}$ 的作用是传递的，即 $\mathrm{Stab}(k)$ 对 $A-\{k\}$ 的作用传递，命题即证.
2. 设 $B\subset A$，$B\neq G$ 且包含至少两个元素. 设 $x,y\in B$，$z\notin B$. 因为 $\mathrm{Stab}(x)$ 在 $A-\{x\}$ 上传递，所以总存

在一个 $g \in \mathrm{Stab}(x)$，使得 $gx = x, gy = z$. 从而 $g(B) \cap B$ 非空且不等于 B，于是 B 不是块. 也就是说，不存在除一元集和 A 自身的块，于是 G 对 A 的作用本原.

3. 由上题，D_8 对 A 的作用不是本原的，从而也不是双传递的.

✍ **练习 5.46** 设 G 对有限集 A 的作用传递，$H \lhd G$. 设 $O_1, \cdots, O_r$ 是 H 在 A 上的轨道. 证明：

1. 对任意的 $g \in G$，$i \in \{1, \cdots, r\}$，存在 $j \in \{1, \cdots, r\}$，使得 $gO_i = O_j$.（从而 G 在 $\{O_1, \cdots, O_r\}$ 上传递，且所有的 $|O_i|$ 都相等）；
2. 若 $a \in O_1$，则 $|O_1| = |H : H \cap \mathrm{Stab}(a)|$，且 $r = [G : H\,\mathrm{Stab}(a)]$.

证明

1. 任取一个 $g \in G$ 和 $a \in O_i$. 若 $ga \in O_i$，则对任意的 $b \in O_i$，由于 H 在 O_i 上的作用传递，所以存在 $h \in H$，使得 $b = ha$，而因为 $H \lhd G$，所以存在 $h' \in H$，使得 $ghg^{-1} = h'$，从而 $gb = gha = h'ga = h'b \in O_i$. 于是 $gO_i \in O_i$.
   若 $ga \in O_j$
   (TBD)

5.3 群作用的例子

5.3.1 知识要点

（一）左乘作用与 Cayley 方程

1. 群 G 对自身的左乘作用：对任意 $g, a \in G$，$g \cdot a := ga$.
2. （左乘作用的性质）：群 G 对自身的左乘作用忠实且传递.
3. 群 G 对子群左陪集全体的左乘作用：设 $H < G$，A 为 H 左陪集的集合. 对任意 $g \in G, aH \in A$，定义
$$g \cdot aH := gaH \tag{5.3}$$
4. （广义左乘作用的性质）：
   (a). G 对 A 的作用传递；
   (b). $\mathrm{Stab}(1H) = H$；
   (c). 作用的核 $K = \cap_{x \in G} xHx^{-1}$，且 K 是 H 内最大的 G 的正规子群.
5. （Cayley 定理）：任意群 G 都同构于对称群的某个子群. 特别的，若 $|G| = n$，则 G 同构于 S_n 的某个子群.
6. （群的阶的最小素因子）：若有限群 G 的阶为 n，且 p 是 n 的最小素因子，则任意指数为 p 的子群都是正规的.

（二）共轭作用与类方程

1. 群 G 对自身的共轭作用：对任意 $g, a \in G$，$g \cdot a := gag^{-1}$.
2. 群 G 对自身幂集的共轭作用：设 $\mathscr{P}(G) = \{S \subset G\}$ 为 G 的幂集，对任意 $g \in G, S \in \mathscr{P}(G)$，定义 $g \cdot S := gSg^{-1}$.
3. （共轭子集的个数）：群 G 中与 $S \subset G$ 共轭的子集个数为 $[G : N_G(S)]$. 特别的，群 G 中与 $s \in G$ 共轭的元素个数为 $[G : C_G(s)]$.
4. （类方程）：设 G 是有限群，$g_1, \cdots, g_r$ 是 G 中不在 $Z(G)$ 内的不同共轭类的代表元，则
$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)]$$

（三）对称群对自身的共轭作用

1. （置换的共轭 I）：设 $\sigma,\tau\in S_n$，且 σ 有轮换分解

$$\sigma=(a_1\ a_2\ \cdots\ a_{k_1})(b_1\ b_2\ \cdots\ b_{k_2})\cdots.$$

于是 $\tau\sigma\tau^{-1}$ 有轮换分解

$$\tau\sigma\tau^{-1}=(\tau(a_1)\ \tau(a_2)\ \cdots\ \tau(a_{k_1}))(\tau(b_1)\ \tau(b_2)\ \cdots\ \tau(b_{k_2}))\cdots.$$

2. （置换的共轭 II）：设 $\sigma,\tau\in S_n$，则 σ,τ 共轭，当且仅当它们轮换分解的轮换型相同.
3. （单群）：A_5 是单群.

5.3.2 从定理证明中学解题

我们这里给出的典型群作用，其运算本质还是群的元素与子集的混合运算，所以此处没有新的技巧，读者可以将各种命题的证明，作为以前学过的知识的复习.

5.3.2.1 左乘作用

问题 5.6 （广义左乘作用的性质）：设 $H<G$，A 为 H 左陪集的集合，G 对 A 的左乘作用如前所述，则：

1. G 对 A 的作用传递；
2. $\mathrm{Stab}(1H)=H$；
3. 作用的核 $K=\cap_{x\in G}xHx^{-1}$，且 K 是 H 内最大的 G 的正规子群.

证明

1. 对任意 $aH,bH\in A$，存在 $g=ba^{-1}$，使得 $g\cdot aH=bH$，于是 A 只包含一个轨道.
2. 对任意 $h\in H$，有 $h\cdot 1H=hH=H$. 且对任意 $g\notin H$，有 $g\cdot 1H=gH\neq H$，从而 $\mathrm{Stab}(1H)=H$.
3. 我们有

$$\begin{aligned}K&=\{g\in G:\ g\cdot xH=xH,\forall xH\in A\}\\&=\{g\in G:\ gxH=xH,\forall xH\in A\}\\&=\{g\in G:\ gxH=xH,\forall x\in G\}\\&=\{g\in G:\ x^{-1}gx\in H,\forall x\in G\}\\&=\{g\in G:\ g\in xHx^{-1},\forall x\in G\}\\&=\cap_{x\in G}xHx^{-1}.\end{aligned}$$

由定义，$K\lhd G$. 且因为对任意的 $k\in K$，有 $kH=k\cdot H=H$，于是 $k\in H$，从而 $K<H$.

最后证明：若 $N\lhd G$ 且 $N<H$，则 $N<K$. 对任意 $x\in G$，有 $N=xNx^{-1}<xHx^{-1}$. 从而

$$N<\cap_{x\in G}xHx^{-1}=K.$$

问题 5.7 （群的阶的最小素因子）：若有限群 G 的阶为 n，且 p 是 n 的最小素因子，则任意指数为 p 的子群都是正规的.

证明 设 $H\leqslant G$，且 $[G:H]=p$. 考虑 G 对 H 左陪集全体 A 的左乘作用 $\pi_H:G\to\mathrm{Perm}(A)$，并记 K 为作用的核，$[H:K]=k$. 于是 $[G:K]=pk$，从而 k 是 n 的因子. 由于 n 的最小素因子为 p，从而若 k 不为 1，则其素因子一定不小于 p.

而另一方面，因为 $|A|=p$，所以 G/H 同构于 $\mathrm{Perm}(A)\simeq S_p$ 的某个子群. 于是由 Lagrange 定理可知，$pk=|G/H|$ 整除 $p!=|S_p|$，即 $k\mid(p-1)!$，然而 $(p-1)!$ 中的每个素因子都小于 p，于是 k 如果不为 1，其素因子必小于 p.

综上，k 只能为 1，从而 $H=K\lhd G$.

5.3.2.2 共轭作用

问题 5.8 （共轭子集的个数）：群 G 中与 $S\subset G$ 共轭的子集个数为 $[G:N_G(S)]$. 特别的，群 G 中与 $s\in G$ 共轭的元素个数为 $[G:C_G(s)]$.

证明 群 G 中与 $S\subset G$ 共轭的子集全体，构成了 S 所在的共轭作用的轨道. 我们有：

$$\begin{aligned}\mathrm{Stab}(S)&=\{g\in G:\ gSg^{-1}=S\}\\&=\{g\in G:\ g\in N_G(S)\}&&=N_G(S).\end{aligned}$$

从而利用轨道公式有 $|\mathrm{Orb}(S)|=[G:N_G(S)]$.

特别的，当 $S=\{s\}$ 时，由定义，$N_G(\{s\})=C_G(s)$，从而命题即证.

✍ **练习 5.47** （类方程）：设 G 是有限群，$g_1,\cdots,g_r$ 是 G 中不在 $Z(G)$ 内的不同共轭类的代表元，则

$$|G|=|Z(G)|+\sum_{i=1}^{r}[G:C_G(g_i)]$$

注 提示：将 G 划分为共轭类的无交并，分别计数求和即可.

5.3.3 典型例题

5.3.3.1 类方程的应用

例题 5.5 若群 G 的阶为 $p^\alpha,\alpha\geqslant 1$，其中 p 是素数，证明：$Z(G)\neq\{1\}$.

证明 由类方程：$|G|=|Z(G)|+\sum_{i=1}^{r}[G:C_G(g_i)]$，其中 $g_1,\cdots,g_r$ 是 G 中不在 $Z(G)$ 内的不同共轭类的代表元. 因为 $[G:C_G(g_i)]\mid|G|=p^\alpha$，且 $C_G(g_i)\neq G$（否则 $g_i\in Z(G)$，矛盾），即 $[G:C_G(g_i)]\neq 1$，所以 $[G:C_G(g_i)]\mid p$. 回到类方程中，左侧 $|G|$ 是 p 的倍数，右侧 $\sum_{i=1}^{r}[G:C_G(g_i)]$ 也是 p 的倍数，从而 $|Z(G)|\geqslant 1$ 必是 p 的倍数，于是 $|Z(G)|\geqslant p$，即 $Z(G)\neq\{1\}$.

✍ **练习 5.48** 若群 G 的阶为 p^2，其中 p 是素数，证明：

1. G 是交换群；
2. G 同构于 $\mathbb{Z}_{p^2}$ 或 $\mathbb{Z}_p\times\mathbb{Z}_p$.

5.3.4 习题

5.4 群的自同构、正规化子与中心化子

5.4.1 知识要点

（一）正规化子与中心化子

设 A 为群 G 的非空子集.

1. A 的正规化子：$N_G(A)=\{g\in G:\ gAg^{-1}=A\}$.
2. A 的中心化子：$C_G(A)=\{g\in G:\ \forall a\in A,gag^{-1}=a\}$
3. 群 G 的中心：$Z(G)=C_G(G)=\{g\in G:\ \forall x\in G,gx=xg\}$
4. （群的中心是正规子群）：$Z(G)\lhd G$.
5. （子集的“子”）：对群 G 的任意子集 A，有 $Z(G)\lhd C_G(A)<N_G(A)<G$.
6. （子群的“子”）：对任意的 $H<G$，有 $H\lhd N_G(H)$.

（二）自同构与内自同构

1. 群 G 的自同构：G 到自身的同构.

G 的自同构全体记为 $\mathrm{Aut}(G)$.

2. (自同构群): $\mathrm{Aut}(G)$ 连同映射的复合运算构成群, 从而 $\mathrm{Aut}(G) < \mathrm{Perm}(G)$.
3. (循环群的自同构群): $\mathrm{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^\times$.
4. (共轭作用是自同构): 设 H 是群 G 的正规子群, 则对任意 $g \in G$, 映射

$$\begin{aligned} \varphi_g : H &\to H \\ h &\mapsto ghg^{-1} \end{aligned}$$

是 H 的自同构. 于是 G 对 H 的共轭作用即为同态

$$\begin{aligned} \varphi : G &\to \mathrm{Aut}(H) \\ g &\mapsto \varphi_g \end{aligned}$$

其核为 $C_G(H)$.

5. (子群的共轭还是子群): 设 K 是群 G 的子群, 则对任意 $g \in G$ 有 $K \simeq gKg^{-1}$.
6. (正规化子模中心化子): 设 H 是群 G 的子群, 则 $N_G(H)/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的某个子群.
7. G 的内自同构: 对任意固定的 $g \in G$, 同构 $G \to G, h \mapsto ghg^{-1}$.
8. (内自同构的性质): G 的内自同构全体构成 $\mathrm{Aut}(G)$ 的子群. (记为 $\mathrm{Inn}(G)$) 且 $G/Z(G) \simeq \mathrm{Inn}(G)$.

(三) 特征子群

1. 群 G 的特征子群 H: $H < G$, 且 G 的每个自同构都将 H 映到自身, 即对任意的 $\sigma \in \mathrm{Aut}(G)$, 有 $\sigma(H) = H$. (记为 $H \operatorname{char} G$)
2. (正规): 特征子群都是正规子群.
3. (给定阶的唯一子群): 若 H 是 G 的给定阶的唯一子群, 则 $H \operatorname{char} G$.
4. (特征传递正规): 若 $K \operatorname{char} H$, $H \lhd G$, 则 $K \lhd G$.

5.4.2 知识要点解读

(一) 正规化子与中心化子

正规化子、中心化子 (包括群的中心) 都是对群的 "部分交换性" 的描述. 首先我们要注意到, 在交换群中, 研究这些概念并没有什么意义.

✍ **练习 5.49** 设 G 为交换群, $A \subset G$, 证明: $N_G(A) = C_G(A) = Z(G) = G$.

对于非交换的群, 任意元素的交换性不再成立, 此时我们转而考察弱化的交换条件. 取群的一个子集 A, 与 A 整体交换的所有元素, 我们称之为 A 的正规化子; 与 A 的每个元素都交换的所有元素, 我们称之为 A 的中心化子. 看起来这样的定义没有什么了不起, 但是得到的这些 "子", 却都是子群.

问题 5.9 (正规化子): 对群 G 的任意非空子集 A, 有 $N_G(A) < G$.

证明 首先, 由正规化子的定义, $N_G(A) \subset G$.

其次, 因为 $1A = A1$, 所以 $1 \in N_G(A)$, 从而 $N_G(A) \neq \varnothing$.

最后, 对于任意的 $x, y \in N_G(A)$ 有:

$$(xy^{-1})A(xy^{-1})^{-1} = x(y^{-1}Ay)x^{-1} = xAx^{-1} = A$$

从而 $xy^{-1} \in N_G(A)$.

综上, $N_G(A) < G$.

✍ **练习 5.50** (中心化子): 对群 G 的任意非空子集 A, 有 $C_G(A) < N_G(A)$.

✍ **练习 5.51** (中心): 对群 G 的任意非空子集 A, 有 $Z(G) < N_G(A)$.

我们也可以从映射的角度，重新审视这些“子”. 记 $\mathfrak{p}^*(G)$ 为 G 的幂集（不包含空集），$s(G)$ 为 G 的全体子群构成的集合（非官方记号），则 N_G, C_G 都可以视作是从 $\mathfrak{p}^*(G)$ 到 $s(G)$ 的映射. 当然这一视角能不能带来更多的性质，笔者目前还没有进一步的思考.

（二）群的自同构

自同构的概念本身是很直白的，没有什么需要解释. 而由自同构，很自然地引出了两个问题：

1. 一个群的自同构群是什么?
2. 一个群的自同构有哪些类型?

第一个问题显然是“因群而异”的，不同类型的群有不同的自同构群. 由于群的分类是一个复杂的问题，进而群的自同构群也很复杂. 对于最简单的一类群——循环群，我们有如下结论：

问题 5.10 （循环群的自同构群）：$\mathrm{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^\times$.

证明

1. (G 的自同态)

   先证明：对任意的整数 $k \in \{0, 1, \cdots, n-1\}$，映射

   $$\begin{aligned} \varphi_k : G &\to G \\ x^i &\mapsto (x^i)^k \end{aligned}$$

   是一个群同态.（证明略）

   另一方面，设 $\varphi : G \to G$ 是一个群同态，则 $\varphi(x) \in G$，即存在一个整数 $k \in \{0, 1, \cdots, n-1\}$，使得 $\varphi(x) = x^k$，此时 $\varphi = \varphi_k$. 从而 $\varphi_k, k \in \{0, 1, \cdots, n-1\}$ 是所有的 G 的自同态.

2. (G 的自同构)

   对固定的 k，以及 $i \in \{0, 1, \cdots, n-1\}$，方程 $x^{ik} = 0$，当且仅当 $n | ik$.

   若 $(k, n) = 1$，则 i 只能 $= 0$，此时 $\ker \varphi_k = \{0\}$，即 φ_k 是群同构.

   若 $(k, n) = m$，则可取 $i = n/m$，此时 $\ker \varphi_k \neq 0$，即 φ_k 不是群同构.

   从而

   $$\mathrm{Aut}(G) = \{\varphi_k : (k, n) = 1\}.$$

   定义映射

   $$\begin{aligned} f : \mathrm{Aut}(G) &\to Z_n^\times \\ \varphi_k &\mapsto k \end{aligned}$$

   容易证明 f 是群同构，即得 $\mathrm{Aut}(G) \simeq Z_n^\times$.

我们总可以遵循这样的讨论思路，求出任意给定群的自同构群，从而第一个问题总是可以解决的.（我们将在例题部分做一点讨论）

对于第二个问题，我们首先将一类特殊的自同构（共轭作用）拿出来讨论.

问题 5.11 （共轭作用是自同构）：设 H 是群 G 的正规子群，则对任意 $g \in G$，映射

$$\begin{aligned} \varphi_g : H &\to H \\ h &\mapsto ghg^{-1} \end{aligned}$$

是 H 的自同构. 于是 G 对 H 的共轭作用即为同态

$$\begin{aligned} \varphi : G &\to \mathrm{Aut}(H) \\ g &\mapsto \varphi_g \end{aligned}$$

其核为 $C_G(H)$.

证明

1. ($ghg^{-1} \in H$)：先证明，对任意的 $h \in H$，$ghg^{-1} \in H$. 因为 $H \lhd G$，所以存在 $h' \in H$，使得 $gh = h'g$. 于是 $ghg^{-1} = h'gg^{-1} = h' \in H$.
   同理可得，$g^{-1}hg \in H$.
2. (φ_g 是群同态)：对任意的 $x, y \in H$，有：
$$\begin{aligned}\varphi_g(xy) &= gxyg^{-1}\\ &= gxg^{-1} \cdot gyg^{-1}\\ &= \varphi_g(x)\varphi_g(y)\end{aligned}$$
   所以 φ_g 是群同态.
3. (φ_g 是群同构)：一方面，对任意的 $x, y \in H$，若 $gxg^{-1} = gyg^{-1}$，则 $x = y$，从而 φ 是单射.
   另一方面，对任意的 $h \in H$，有 $g^{-1}hg \in H$，使得
$$\varphi_g(g^{-1}hg) = g(g^{-1}hg)g^{-1} = h$$
   从而 φ 是满射.
   综上，φ_g 是群同构，即 φ_g 是 H 的自同构.
4. (φ 是群同态)：对任意的 $g_1, g_2 \in G$，和任意的 $h \in H$，有：
$$\begin{aligned}\varphi_{g_1g_2}(h) &= (g_1g_2)h(g_1g_2)^{-1}\\ &= g_1(g_2hg_2^{-1})g_1^{-1}\\ &= g_1\varphi_{g_2}(h)g^{-1}\\ &= \varphi_{g_1}(\varphi_{g_2}(h))\\ &= (\varphi_{g_1}\varphi_{g_2})(h)\end{aligned}$$
   从而总是有 $\varphi_{g_1g_2} = \varphi_{g_1}\varphi_{g_2}$，即 φ 是群同态.
5. (φ 的核)：我们有
$$\ker\varphi = \{g \in G : \varphi_g = id.\}$$
   而 $\varphi_g = id. \in \mathrm{Aut}(H)$，当且仅当对任意的 $h \in H$，有
$$\begin{aligned}h &= \varphi_g(h)\\ &= ghg^{-1}\end{aligned}$$
   即对任意的 $h \in H$，有 $hg = gh$. 于是当且仅当 $g \in C_G(H)$.
   综上，$\ker\varphi = C_G(H)$.

笔记 这一命题涉及到两层同态关系：φ_g 和 φ. 读者如果对群作用的概念足够熟悉，那么处理这样的同态关系应该是游刃有余的.

这一命题有两个方面的应用. 首先，考虑 G 作为自身的正规子群，于是每个 $\varphi_g : G \to G$ 都是群自同构（这就是内自同构）. 我们知道，同构是保持子群的，于是对任意的 $K < G$，$\varphi_g(K) \simeq K$，也就有如下命题.

练习 5.52（子群的共轭还是子群）：设 K 是群 G 的子群，则对任意 $g \in G$ 有 $K \simeq gKg^{-1}$.

另一方面，对任意的 $H < G$，H 总是 $N_G(H)$ 的正规子群. 于是将原命题中的 G 替换为 $N_G(H)$，即得

练习 5.53（正规化子模中心化子）：设 H 是群 G 的子群，则 $N_G(H)/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的某个子群.

进一步地，将这一命题中的 H 换成 G，就会得到：$G/Z(G)$ 同构于 $\mathrm{Aut}(H)$ 的某个子群. 事实上，我们有更强的结论.

问题 5.12（内自同构的性质）：G 的内自同构全体构成 $\mathrm{Aut}(G)$ 的子群.（记为 $\mathrm{Inn}(G)$）且 $G/Z(G) \simeq \mathrm{Inn}(G)$.

证明 记 G 关于元素 g 的内自同构为 $\varphi_g : G \to G, h \mapsto ghg^{-1}$.

1. (内自同构构成子群)：首先，G 的恒等映射是 G 的内自同构：

$$\begin{aligned} id.: G &\to G \\ g &\mapsto g = 1g1^{-1} \end{aligned}$$

从而 $\mathrm{Inn}(G)$ 非空.

其次，对任意的 $x, y \in G$，有：

$$\begin{aligned} \varphi_x \varphi_y^{-1} &= \varphi_x \varphi_{y^{-1}} \\ &= \varphi_{xy^{-1}} \in \mathrm{Inn}(G) \end{aligned}$$

所以 $\mathrm{Inn}(G)$ 连同映射的复合构成 $\mathrm{Aut}(G)$ 的子群.

2. (同构关系)：令映射

$$\begin{aligned} \psi: G &\to \mathrm{Inn}(G) \\ g &\mapsto \varphi_g \end{aligned}$$

先证明：ψ 是群同态. 对任意的 $x, y \in G$，有

$$\begin{aligned} \psi(xy) &= \varphi_{xy} \\ &= \varphi_x \varphi_y \\ &= \psi(x)\psi(y) \end{aligned}$$

从而 ψ 是群同态.

再证明：ψ 是群满同态. 这是因为 $\mathrm{Inn}(G)$ 中的元素，必然形如 φ_g，从而他有原象 g.

最后证明：$\ker \psi = Z(G)$. 我们有

$$\ker \psi = \{g \in G : \varphi_g = id.\}$$

而 $\varphi_g = id. \in \mathrm{Inn}(G)$，当且仅当对任意的 $h \in G$，有

$$\begin{aligned} h &= \varphi_g(h) \\ &= ghg^{-1} \end{aligned}$$

即对任意的 $h \in G$，有 $hg = gh$. 于是当且仅当 $g \in Z(G)$.

综上，$\ker \psi = Z(G)$.

最后，利用群的第一同构定理，可得：

$$G/Z(G) = G/\ker \psi \simeq \psi(G) = \mathrm{Inn}(G).$$

原命题即证.

(三) 特征子群的性质

从自同构的角度来看，正规子群相当于是群的内自同构的“稳定子”，特征子群则是群的所有自同构的“稳定子”. 也就是说：

1. $H \lhd G$：对任意的 $\sigma \in \mathrm{Inn}(G)$，$\sigma(H) = H$. (因为内自同构总是形如 $h \mapsto ghg^{-1}$.)
2. $H \operatorname{char} G$：对任意的 $\sigma \in \mathrm{Aut}(G)$，$\sigma(H) = H$.

从而特征子群是正规子群的加强版. 正如正规子群的基本使用离不开共轭形式一样，特征子群的基本使用，也离不开自同构.

问题 5.13 (正规)：若 H 是群 G 的特征子群，则 $H \lhd G$.

证明 对任意的 $g \in G$，g 对 G 的共轭作用都是 G 的自同构. 由于 $H \operatorname{char} G$，所以 $gHg^{-1} = H$，命题即证.

问题 5.14 (给定阶的唯一子群)：若 H 是 G 的给定阶的唯一子群，则 $H \operatorname{char} G$.

证明 对任意的 $\sigma \in \mathrm{Aut}(G)$，先证明：$\sigma(H) < G$，且 $\sigma(H) \simeq H$.

首先，$\sigma(H)$ 必然非空，因为 $1=\sigma(1)\in\sigma(H)$. 其次，对任意的 $x,y\in H$，有：

$$\begin{aligned}\sigma(x)(\sigma(y))^{-1}&=\sigma(x)\sigma(y^{-1})\\&=\sigma(xy^{-1})\in\sigma(H)\end{aligned}$$

于是 $\sigma(H)<G$.

定义映射 $\psi:H\to\sigma(H),h\mapsto\sigma(h)$. 很容易证明 ψ 为同构. 于是 $\sigma(H)\simeq H$.

因为阶为 $|H|$ 的 G 的子群是唯一的，所以只能有 $\sigma(H)=H$，于是 $H\operatorname{char}G$.

问题 5.15（特征传递正规）：若 $K\operatorname{char}H$，$H\lhd G$，则 $K\lhd G$.

注 分析：此题曾困扰笔者很长时间，思考过程中的主要问题在于，题目中看起来没有显式的 H 的自同构，那么我们如何使用 $K\operatorname{char}H$ 这个条件呢?

从待证结论分析，我们需证 $gKg^{-1}=K$. 注意到在正规子群一节中，我们曾经分析过，一般证明正规子群，更多的会去证明更弱一点的结论 $gKg^{-1}\subset K$. 这里为什么不这样做？这是因为我们需要将一切线索都尽量和问题的核心“自同构”联系起来，而 $gKg^{-1}=K$ 表达的含义，可以理解为 g 对 K 的共轭作用保持 K 不变. 我们知道，共轭作用是可以理解为自同构的. 一般的，我们只能理解为 G 的自同构，但是，由于 $H\lhd G$，所以 g 的共轭作用也是 H 的自同构. 想到这里，此题就解开了，因为 H 的自同构会保持 K 不变，这正是 $K\operatorname{char}H$ 想要告诉我们的. 到此，整理一下思路，我们即可写出如下解答.

证明 因为 $H\lhd G$，所以 $\varphi:h\mapsto ghg^{-1}$ 是 H 的自同构. 又 $K\operatorname{char}H$，所以 $\varphi(K)=K$，即 $gKg^{-1}=K$，即 $K\lhd G$.

5.4.3 典型例题

（一）正规化子与中心化子

例题 5.6 设 G 为群. 证明：若 $A\subset B\subset G$，则 $C_G(B)<C_G(A)$.

证明 因为 $C_G(A)$，$C_G(B)$ 都是群，所以我们只需证：$C_G(B)\subset C_G(A)$.

对任意 $g\in C_G(B)$，由正规化子的定义，对所有 $b\in B$，有 $gb=bg$. 因为 $A\subset B$，即所有的 $a\in A$，都有 $a\in B$，于是 $ga=ag$. 从而 $g\in C_G(A)$. 由此即证 $C_G(B)\subset C_G(A)$.

练习 5.54 H 是群 G 的子群. 证明：

1. $H\lhd N_G(H)$；
2. $H\lhd C_G(H)$，当且仅当 H 是交换的.

证明

1. 首先，对任意的 $h\in H$，$hH=H=Hh$，所以 $H<N_G(H)$.
   然后，对任意的 $g\in N_G(H)$，由正规化子的定义可得：$gH=Hg$，从而 $H\lhd N_G(H)$.
2. 一方面，若 $H\lhd C_G(H)$，则对任意的 $h,h'\in H$，有 $hh'=h'h$，从而 H 是交换的.
   另一方面，若 H 是交换的，则对任意的 $h,h'\in H$，有 $hh'=h'h$，从而 $H<C_G(H)$. 又因为 $H\lhd N_G(H)$，$C_G(H)<N_G(H)$，所以 $H\lhd C_G(H)$.
   综上，原命题成立.

笔记 本题要求读者掌握正规化子、中心化子、正规子群的定义.

（二）群的自同构群

当我们给出自同构群的概念之后，如何求一个群的自同构群，就是一个呼之欲出的问题了. 我们首先考虑较为简单的情形：有限群. 由于有限群 G 总是有有限个生成元，所以对于任意的一个以 G 为定义域的群自同态，只需要给出生成元的象，就可以确定 G 中任意元素的象. 此外，我们知道，如果 $\varphi\in\operatorname{Aut}(G)$，则 $g\in G$ 和 $\varphi(g)$ 的阶总是一样的. 再结合群同构的核 $=\{0\}$，我们就可以从所有的群自同态中筛选出所有的群自同构，进而给出自同构群的构型（已知群的所有元素，群的构型总是可以确定的）.

例题 5.7 求 D_8 的自同构群和内自同构群的构型.

解 先计算 $D_8 = \langle r, s | r^4 = s^2 = 1, rs = sr^{-1} \rangle$ 的所有元素的阶：

$$1 : 1$$
$$2 : r^2, s, sr, sr^2, sr^3$$
$$4 : r, r^3$$

对任意的 $\sigma \in \mathrm{Aut}(D_8)$，我们只需要给定合适的 $\sigma(r), \sigma(s)$，就可确定 σ. 因为 $|r| = 4$，所以 $\sigma(r) = r, r^3$. 因为 $|s| = 2$，所以 $\sigma(s) = r^2, s, sr, sr^2, sr^3$. 以下我们分别讨论这些情况.

1. 设 $\sigma(r) = r$，则对任意的整数 n，有 $\sigma(r^n) = r^n$，于是 $\sigma(s)$ 不能等于 r^2（否则 $\sigma(r^2)$ 也等于 r^2，σ 必然不是群同构）. 我们列出所有可能的自同构，及其阶数：
   (a). $\sigma(s) = s$：此时 σ 为恒等映射.
   (b). $\sigma(s) = sr$：此时对任意的 $r^i, r^i s \in D_8$，有
   $$\sigma(r^i) = r^i$$
   $$\sigma(r^i s) = r^i sr = r^{i-1} s$$
   注意到 $\sigma^4 r^i s = r^{i-4} s = r^i s$，所以 $|\sigma| = 4$.
   (c). $\sigma(s) = sr^2$：此时对任意的 $r^i, r^i s \in D_8$，有
   $$\sigma(r^i) = r^i$$
   $$\sigma(r^i s) = r^i sr^2 = r^{i-2} s$$
   注意到 $\sigma^2 r^i s = r^{i-4} s = r^i s$，所以 $|\sigma| = 2$.
   (d). $\sigma(s) = sr^3$：此时对任意的 $r^i, r^i s \in D_8$，有
   $$\sigma(r^i) = r^i$$
   $$\sigma(r^i s) = r^i sr^3 = r^{i-3} s$$
   注意到 $\sigma^4 r^i s = r^{i-12} s = r^i s$，所以 $|\sigma| = 4$.
2. 设 $\sigma(r) = r^3$，则对任意的整数 n，有 $\sigma(r^n) = r^{4-n}$，从而 $\sigma(s)$ 也不能等于 r^2，且 $\sigma^2(r^i) = r^i$.
   (a). $\sigma(s) = s$：此时对任意的 $r^i, r^i s \in D_8$，有
   $$\sigma(r^i) = r^{4-i}$$
   $$\sigma(r^i s) = r^{4-i} s$$
   注意到 $\sigma^2(r^i s) = r^i s$，所以 $|\sigma| = 2$.
   (b). $\sigma(s) = sr$：此时对任意的 $r^i, r^i s \in D_8$，有
   $$\sigma(r^i) = r^{4-i}$$
   $$\sigma(r^i s) = r^{4-i} sr = r^{3-i} s$$
   注意到 $\sigma^2(r^i s) = r^i s$，所以 $|\sigma| = 2$.
   (c). $\sigma(s) = sr^2$：此时对任意的 $r^i, r^i s \in D_8$，有
   $$\sigma(r^i) = r^{4-i}$$
   $$\sigma(r^i s) = r^{4-i} sr^2 = r^{2-i} s$$
   注意到 $\sigma^2(r^i s) = r^i s$，所以 $|\sigma| = 2$.
   (d). $\sigma(s) = sr^3$：此时对任意的 $r^i, r^i s \in D_8$，有
   $$\sigma(r^i) = r^{4-i}$$
   $$\sigma(r^i s) = r^{4-i} sr^3 = r^{1-i} s$$
   从而 $|\sigma| = 2$.

综上，$|\mathrm{Aut}(D_8)|=8$，且有 1 阶元素 1 个，2 阶元素 5 个，4 阶元素 2 个，从而 $\mathrm{Aut}(D_8)\simeq D_8$.

另外，由于 $Z(D_8)=\langle r^2\rangle$，所以

$$\mathrm{Inn}(D_8)\simeq D_8/\langle r^2\rangle=\{\bar{1},\bar{r},\bar{s},\overline{sr}\}.$$

不难验证，$\mathrm{Inn}(D_8)\simeq V_4$.

笔记 解决本题的基础，在于我们对于小阶群的结构有充分的了解. 对于 8 阶群，我们是了解的，其种类也不算多. 所以，当我们确定 $\mathrm{Aut}(D_8)$ 是 8 阶群后，最简明的做法，就是算出其中每个元素的阶，然后和几种 8 阶群对比一下，看看能对上哪一种 8 阶群的构型.

例题 5.8 求 $G=\mathbb{Z}_2\times\mathbb{Z}_8$ 的自同构群的阶数.

注 $\mathbb{Z}_2\times\mathbb{Z}_8$ 可以表达为：

$$\mathbb{Z}_2\times\mathbb{Z}_8=\langle(1,0),(0,1)\rangle.$$

计算 $\mathbb{Z}_2\times\mathbb{Z}_8$ 的所有元素的阶：

$$\begin{aligned}&1:(0,0)\\&2:(0,4),(1,0),(1,4)\\&4:(0,2),(0,6),(1,2),(1,6)\\&8:(0,1),(0,3),(0,5),(0,7),(1,1),(1,3),(1,5),(1,7)\end{aligned}$$

结合本小节前言的论述，我们必须将 $(1,0)$ 对应到任意一个 2 阶元素，$(0,1)$ 对应到任意一个 8 阶元素，再从中筛选群同构即可.

解 $\mathbb{Z}_2\times\mathbb{Z}_8$ 可以表达为：

$$\mathbb{Z}_2\times\mathbb{Z}_8=\langle(1,0),(0,1)\rangle.$$

对于任意的群同态：$\varphi:G\to G$，显然 $\varphi((1,0)),\varphi((0,1))\in G$. 且对任意的 $g,h\in G$，易证如下定义的映射

$$(x,y)\mapsto xg+yh$$

是 G 到自身的群同态.

进一步的，对于任意的 G 的自同构 φ，有

$$\begin{aligned}|\varphi((1,0))|&=|(1,0)|=2\\|\varphi((0,1))|&=|(0,1)|=8.\end{aligned}$$

对任意的 $g,h\in G$，$|g|=2,|h|=8$，考虑群同态

$$\begin{aligned}\varphi:G&\to G\\(x,y)&\mapsto xg+yh\end{aligned}$$

考虑方程 $xg+yh=(0,0),(x,y)\in G$.

1. 当 $x=0$ 时，由于 $|h|=8$，所以 $yh=0$ 当且仅当 $y=0$，即有一个解 $(0,0)$.
2. 当 $x=1$ 时，$|xg|=|g|=2$，从而 $|xg|=|-yh|=|yh|=2$. 由于 $|h|=8$，所以 $|yh|=|h|/(|h|,y)$，即 $(|h|,y)=(8,y)=4$，即 $y=4$. 此时 $g=xg=-yh=-4h$. 注意到对任意的 h，$h^4=(0,4)$（对 8 个 8 阶元素计算检验即可），所以当 $g=(0,4)$ 时，原方程有非零解；其他情况下，即 $g=(1,0),(1,4)$ 时，均不存在 h，使得 $g=-4h$.

综上，当 $g=(1,0),(1,4)$，h 为任意 8 阶元素时，前面定义的 φ 是群同构. 并且这些也是 $\mathrm{Aut}(G)$ 的所有元素. 从而 $|\mathrm{Aut}(G)|=2\times8=16$.

笔记 $\mathrm{Aut}(G)$ 的具体形式不好确定，因为 16 阶群的种类太多了.

5.4.4 习题

（一）正规化子与中心化子

练习 5.55 分别计算 D_8 和 Q_8 中，各个元素的中心化子.

注 提示：也就是计算与各个元素交换的元素集合.

练习 5.56 设 $n \geqslant 3$ 是正整数，证明：

1. 若 n 是奇数，则 $Z(D_{2n}) = 1$；
2. 若 $n = 2k$，$k \geqslant 2$ 是正整数，则 $Z(D_{2n}) = \{1, r^k\}$.

注 提示：由定义我们知道：$Z(G) = \cap_{g\in G} N_G(g)$，从而若 $g, h \in G$ 满足 $gh \neq hg$，则 $g, h \notin Z(G)$.

练习 5.57 设 G 为群，$H \lhd G$，且 $N_G(H) = C_G(H)$. 证明：$H < Z(G)$.

证明 因为 $H \lhd G$，所以对任意的 $g \in G$，有 $gH = Hg$，即 $g \in N_G(H)$. 从而 $g \in C_G(H)$. 也就是说，对任意的 $g \in G$ 和任意的 $h \in H$，有 $gh = hg$，所以 $h \in Z(G)$. 从而 $H \subset Z(G)$，即 $H < Z(G)$.

练习 5.58 设 G 为群，证明：

1. $C_G(Z(G)) = G$；
2. $N_G(Z(G)) = G$.

证明

1. 一方面，$Z(G) < G$，所以 $C_G(Z(G)) < G$. 另一方面，对任意的 $g \in G$ 和任意的 $h \in Z(G)$，有 $gh = hg$，所以 $g \in C_G(Z(G))$，即 $G < C_G(Z(G))$. 综上，$C_G(Z(G)) = G$.
2. 一方面，$Z(G) < G$，所以 $N_G(Z(G)) < G$. 另一方面，对任意的 $g \in G$ 和任意的 $h \in Z(G)$，有 $gh = hg$，从而 $gZ(G) = Z(G)g$，所以 $g \in N_G(Z(G))$，即 $G < N_G(Z(G))$. 综上，$N_G(Z(G)) = G$.

练习 5.59 设 G 为群，对任意 $H < G$ 和任意非空 $A \subset G$，定义 $N_H(A) = \{h \in H : hAh^{-1} = A\}$. 证明：$N_H(A) = N_G(A) \cap H$.

证明 一方面，设 $h \in N_H(A)$，则 $h \in H$，且由于 $hA = Ah$，所以 $h \in N_G(A)$，从而 $h \in N_G(A) \cap H$.

另一方面，设 $h \in N_G(A) \cap H$，则 $h \in H$，且 $hA = Ah$，所以 $h \in N_H(A)$.

综上：$N_H(A) = N_G(A) \cap H$.

练习 5.60 设 H 是群 G 的阶为 2 的子群，证明：

1. $N_G(H) = C_G(H)$；
2. 若 $N_G(H) = G$，则 $H < Z(G)$.

证明

1. 一方面，$C_G(H) < N_G(H)$. 于是我们只需证 $N_G(H) \subset C_G(H)$.
   因为 $|H| = 2$，所以设 $H = \{1, h\}$，且 $h^2 = 1$. 对任意的 $g \in N_G(H)$，有 $gH = Hg$，于是 $\{g, gh\} = \{g, hg\}$. 而 $g = g$，所以只能有 $gh = hg$，于是 $g \in C_G(H)$.
2. 因为 $N_G(H) = G$，所以对任意 $g \in G$，有 $gH = Hg$，由第一小问的证明过程可得 $gh = hg$，于是 $h \in Z(G)$，从而 $H \subset Z(G)$. 又因为 H 是群，从而 $H < Z(G)$.

练习 5.61* 设 $H < G$，证明：$C_G(C_G(C_G(H))) = C_G(H)$.

证明 先证明：对任意的子群 $H < G$，$H < C_G(C_G(H))$.

对任意的 $h \in H$，由中心化子的定义得：对任意的 $a \in C_G(H)$，有 $ah = ha$. 于是，对任意的 $a \in C_G(H)$，有 $ah = ha$，也就是，$h \in C_G(C_G(H))$. 命题得证.

于是，一方面，因为 $H < C_G(C_G(H))$，所以 $C_G(C_G(C_G(H))) < C_G(H)$.

另一方面，因为 $C_G(H) < G$，从而可以将 $H < C_G(C_G(H))$ 中的 H 替换成 $G_G(H)$，即得 $C_G(H) < C_G(C_G(C_G(H)))$.

两相结合即得：$C_G(C_G(C_G(H))) = C_G(H)$.

笔记 本题的形式十分有趣. 笔者不得不承认，一开始看到 $C_G(C_G(C_G(H)))$ 的时候，笔者不由的心头一震：“这什么奇怪的形式哟”，一下子不知道如何是好. 冷静下来之后，我们得想了，我们从哪里寻找思路呢？

正规化子的定义，应该是我们先想到的，不过显然地，展开描述 $x \in C_G(C_G(C_G(H)))$，并不是一件容易的事情，因此这一想法先搁置一旁. 还有别的思路吗？

我们来想办法联系一下等式左右两侧的代数式的形式. 等式右侧没啥说的，子群 H 的中心化子 $C_G(H)$，左侧呢？有两种视角可以联系 $C_G(H)$：

1. 视角一，$C_G(C_G(C_G(H)))$ 是 $C_G(C_G(H))$ 的中心化子；
2. 视角二，$C_G(C_G(C_G(H)))$ 是对 $C_G(H)$ 再做两次“中心化”.

为什么要这样去看呢？因为我们前面做过一个练习：若 $A \subset B$，则 $C_G(B) \subset C_G(A)$. 那么如果 H 和 $C_G(C_G(H))$ 之间有包含关系的话，利用视角一，我们能得到 $C_G(H)$ 和 $C_G(C_G(C_G(H)))$ 的某种包含关系；同时，利用视角二，我们将 $C_G(H)$“代入”H 中，也能得到 $C_G(H)$ 和 $C_G(C_G(C_G(H)))$ 的某种包含关系. 然后解答中呈现的结果告诉我们，这两种处理方式得到的包含关系刚好相反，于是巧妙地获得了相等关系.

同样的处理思路，我们在 Galois 理论中还会再次遇到.

✍ **练习 5.62**

1. 证明：若 H 是群 G 的子群，且 H 是交换群，则 $\langle H, Z(G)\rangle$ 是交换的.
2. 给出一个例子，使得 H 是群 G 的子群，H 是交换群，且 $\langle H, C_G(H)\rangle$ 不是交换的.

注 提示：第二小问，考虑 $G = D_8, H = \{1, r^2\}$，此时 $C_G(H) = D_8$.

✍ **练习 5.63** 设 G 为群，$H < G$ 且 $g \in G$. 证明：若右陪集 Hg 等于某个 H 在 G 中的左陪集，则其必等于左陪集 gH，且 $g \in N_G(H)$.

证明 若 $Hg = g'H$，则 $1 \cdot g \in Hg = g'H$，从而 $g'^{-1}g \in H$，于是 $gH = g'H = Hg$. 再由正规子群定义立即得 $g \in N_G(H)$.

（二）自同构群

✍ **练习 5.64** 证明：

1. $\mathrm{Inn}(Q_8) \simeq V_4$；
2. $\mathrm{Inn}(S_3) \simeq S_3$.

✍ **练习 5.65** 设 G 为群，$\sigma \in \mathrm{Aut}(G)$. 定义：

$$\begin{aligned} \varphi_g : G &\to G \\ h &\mapsto ghg^{-1} \end{aligned}$$

证明：

1. $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$；
2. $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

注 定义 $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ 为 G 的外自同构群.

证明

1. 对任意的 $h \in G$，有

$$\begin{aligned} \sigma\varphi_g\sigma^{-1}(h) &= \sigma(g\sigma^{-1}(h)g^{-1}) \\ &= \sigma(g)h\sigma(g^{-1}) \\ &= \sigma(g)h(\sigma(g))^{-1} \\ &= \varphi_{\sigma(g)}(h) \end{aligned}$$

从而 $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$.

2. 由前一小问，对任意的 $\sigma \in \mathrm{Aut}(G)$ 和任意的 $\varphi_g \in \mathrm{Inn}(G)$，有 $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)} \in \mathrm{Inn}(G)$，从而 $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

✍ **练习 5.66** 证明：如果 G 是 pq 阶交换群，其中 p, q 是不同的素数，那么 G 是循环群.

注 本题是使用 Cauchy 定理的一个经典例子.

证明 不妨设 $p<q$，则由 Cauchy 定理，G 必然存在 p 阶子群 H. 由于 p 是素数，所以 H 只能是 p 阶循环群，从而设 $H=\langle h|h^p=1\rangle$.

又因为 G 是交换群，所以其子群都是正规子群，也就有 $H\lhd G$. 考虑商群 G/H，由 Lagrange 定理，$|G/H|=|G|/|H|=pq/p=q$. 由于 q 也是素数，所以 G/H 只能为 q 阶循环群，从而 $G/H=\langle\bar{g}|(\bar{g})^q=\bar{1}\rangle$. 因为 $(\bar{g})^q=\bar{1}$，也就是 $H=(gH)^q=g^qH$，所以 $g^q\in H$.

下证：$|gh|=pq$. 一方面

$$(gh)^pq=(g^q)^p(h^p)^q\quad(G\text{ 是循环群，所以该等式成立.})\tag{5.4}$$

$$=(g^q)^p\tag{5.5}$$

由于 $g^q\in H$，而 H 是 p 阶群，所以 $(g^q)^p=1$，从而 $(gh)^pq=1$.

另一方面，假设 $|gh|<pq$. 由于 $|gh|$ 是 $|G|=pq$ 的因子，而 p,q 均为素数，所以 $|gh|$ 可能等于 $1,p,q$. 以下分别讨论这几种情况：

1. 若 $|gh|=1$，则 $gh=1$，从而 $h=g^{-1}$，于是 $q=|h|=|g^{-1}|=|g|=p$，矛盾！
2. 若 $|gh|=p$，则 $1=(gh)^p=g^p$，从而 $(\bar{g})^p=\bar{1}$，即 $q=|\bar{g}|\leqslant p$，矛盾！
3. 若 $|gh|=q$，则 $1=(gh)^q=h^q$. 又因为 $|h|=p$，所以 p 是 q 的因子. 由于 q 是素数，所以 $p=1$ 或 $p=q$，而这两种情况都不可能成立！

综上，$|gh|\geqslant pq$. 结合 $(gh)^pq=1$ 可得：$|gh|=pq$.

因为 $|gh|=pq$，所以 $\langle gh\rangle$ 是 G 的 pq 阶子群. 然而 G 是 pq 阶群，所以必有 $G=\langle gh\rangle$，从而 G 是循环群.

✍ **练习 5.67** 证明：$|\operatorname{Aut}(Q_8)|\leqslant 24$.

注 提示：Q_8 可以认为有两个生成元 i,j. i,j 都是 4 阶元素. Q_8 中一共有 6 个四阶元素 $i,-i,j,-j,k,-k$. 对任意的 $\sigma\in\operatorname{Aut}(Q_8)$，分别考虑 $\sigma(i),\sigma(j)$.

1. $\sigma(i)=i$：此时 $\sigma(i^3)=-i$，于是 $\sigma(j)$ 还有至多 4 种可能的选择 $\pm j,\pm k$.
2. $\sigma(i)=-i$：此时 $\sigma(i^3)=i$，于是 $\sigma(j)$ 还有至多 4 种可能的选择 $\pm j,\pm k$.
3. $\sigma(i)=j$：此时 $\sigma(i^3)=-j$，于是 $\sigma(j)$ 还有至多 4 种可能的选择 $\pm i,\pm k$.
4. $\sigma(i)=-j$：此时 $\sigma(i^3)=j$，于是 $\sigma(j)$ 还有至多 4 种可能的选择 $\pm i,\pm k$.
5. $\sigma(i)=k$：此时 $\sigma(i^3)=-k$，于是 $\sigma(j)$ 还有至多 4 种可能的选择 $\pm j,\pm k$.
6. $\sigma(i)=-k$：此时 $\sigma(i^3)=k$，于是 $\sigma(j)$ 还有至多 4 种可能的选择 $\pm i,\pm j$.

综上，$|\operatorname{Aut}(Q_8)|\leqslant 24$.

笔记 实际上，$\operatorname{Aut}(Q_8)\simeq S_4$.

✍ **练习 5.68** 设 G 是群，H,K 是 G 的子群，$H<K$.

1. 证明：若 $H\operatorname{char}K,K\operatorname{char}G$，则 $H\operatorname{char}G$.
2. 试举一例说明：若 $H\lhd K$，$K\operatorname{char}G$，则 H 不一定是 G 的正规子群.

证明

1. 因为 $K\operatorname{char}G$，所以对任意的 $\sigma\in\operatorname{Aut}(G)$，有 $\sigma(K)=K$. 由于 σ 是同构，所以 $\sigma|_K\in\operatorname{Aut}(K)$. 又因为 $H\operatorname{char}K$，所以 $\sigma|_K(H)=H$. 由于 $H\subset K$，所以 $\sigma(H)=\sigma|_K(H)=H$. 即 $H\operatorname{char}G$.
2. ?

✍ **练习 5.69** 设 $D_{2n}=\langle r,s|r^n=s^2=1,rs=sr^{-1}\rangle$，证明：$H=\langle r\rangle$ 的每个子群，都是 D_{2n} 的正规子群.

证明 若 $n=2$，则 $D_{2n}\simeq V_4$，是循环群，所以其子群都是正规子群. 下设 $n\geqslant 3$.

先证明：$H\operatorname{char}D_{2n}$. 对任意的 $\sigma\in\operatorname{Aut}(D_{2n})$，$\sigma(r)$ 必须和 r 同阶. 注意到所有的 $sr^i\in D_{2n}$ 都是 2 阶，所以 $\sigma(r)$ 只能等于某个 r^k，并且 $(k,n)=1$. 从而 $\sigma(r)$ 也是 $\langle r\rangle$ 的一个生成元，即 $\sigma(H)=H$. 这就证明了 $H\operatorname{char}D_{2n}$.

由于 H 是循环群，所以其子群 K 都是 H 的正规子群. 从而必有 $K\lhd D_{2n}$.

✍ **练习 5.70** 设 G 是群，$A\lhd G$，且 A 是交换群. 记 $\bar{G}=G/A$.

1. 证明：$\bar{G}$ 对 A 有左作用 $\bar{g}\cdot a:=gag^{-1}$，其中 g 是陪集 $\bar{g}$ 的任意代表元.

2. 试举一例说明：如果 A 不是交换群，则前述作用不是良定义.

证明

1. 先证明：$\bar{g}\cdot a := gag^{-1}$ 是良定义. 也就是说，对于 $g,h\in G$，若 $\bar{g}=\bar{h}$，则 $gag^{-1}=hah^{-1}$.
因为 $\bar{g}=\bar{h}$，所以 $h^{-1}g\in A$. 对任意的 $a\in A$，有：
$$\begin{aligned}(h^{-1}g)a(h^{-1}g)^{-1}&=(h^{-1}g)(h^{-1}g)^{-1}a\\&=a\end{aligned}$$
于是
$$h^{-1}gag^{-1}h=a$$
也就是
$$gag^{-1}=hah^{-1}.$$
再证明：$\bar{g}\cdot a := gag^{-1}$ 是 $\bar{G}$ 对 A 的左作用.
一方面，对任意的 $g,h\in G$，有
$$\begin{aligned}\bar{g}\cdot(\bar{h}\cdot a)&=\bar{g}\cdot(hah^{-1})\\&=ghah^{-1}g^{-1}\\&=(gh)a(gh)^{-1}\\&=\overline{gh}\cdot a\\&=(\bar{g}\bar{h})\cdot a\end{aligned}$$
另一方面，
$$\begin{aligned}\bar{1}\cdot a&=1a1^{-1}\\&=a\end{aligned}$$
从而 $\bar{g}\cdot a$ 是左作用.

2. 考虑 S_4 及其子群 A_4. 由于 A_4 的指数为 2，所以必为 S_4 的正规子群. 沿用前一小问的符号，取 $A=A_4$，则 $\bar{1}=\overline{(1\,2)(1\,3)}$. 不过，对于 $a=(1\,2)(3\,4)$，
$$\begin{aligned}1a1^{-1}&=(1\,2)(3\,4)\\(1\,2)(1\,3)a((1\,2)(1\,3))^{-1}&=(1\,2)(1\,3)(1\,2)(3\,4)(1\,3)(1\,2)\\&=(1\,3)(2\,4)\end{aligned}$$
两者不相等，所以前一小问中的作用，在此处不是良定义.

✍ **练习 5.71** 设 G 是 3825 阶群. 证明：若 H 是 G 的 17 阶正规子群，则 $H<Z(G)$.

证明 由于 H 是 17 阶群，所以 $H\simeq\mathbb{Z}_{17}$，从而 $\mathrm{Aut}(H)\simeq(\mathbb{Z}_{17})^\times$，即 $|\mathrm{Aut}(H)|=|(\mathbb{Z}_{17})^\times|=\varphi(17)=16$.

另一方面，由于 $H\lhd G$，所以 $N_G(H)=G$. 因为 $N_G(H)/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的子群，所以 $G/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的子群，从而
$$|G/C_G(H)|\,|\,|\mathrm{Aut}(H)|$$
G 的阶为 $3825=3^2\times5^2\times17$，从而 $|G/C_G(H)|$ 为 3825 的因子. 同时，$|\mathrm{Aut}(H)|=16=2^4$，从而 $|G/C_G(H)|$ 为 16 的因子. 由于 $(3825,16)=1$，所以只能有 $|G/C_G(H)|=1$，即 $G=C_G(H)$. 这就说明，对任意的 $g\in G,h\in H$，有 $gh=hg$，从而 $H\subset Z(G)$，即 $H<Z(G)$.

笔记 破题的关键在于我们所熟悉的素因子分析，只不过这里结合了本节的新知识：$N_G(H)/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的子群. 读者对此应有一定的敏感性，也就是说，任何群的同态（同构）关系，都有可能作为素因子分析的素材.

✍ **练习 5.72** 设 G 是 203 阶群. 证明：

1. 若 H 是 G 的 7 阶正规子群，则 $H<Z(G)$.

2. 在前一小问的条件下，G 是交换群.

证明

1. 由于 H 是 7 阶群，所以 $H \simeq \mathbb{Z}_7$，从而 $\mathrm{Aut}(H) \simeq (\mathbb{Z}_7)^\times$，即 $|\mathrm{Aut}(H)| = |(\mathbb{Z}_7)^\times| = \varphi(7) = 6$.
   另一方面，由于 $H \lhd G$，所以 $N_G(H) = G$. 因为 $N_G(H)/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的子群，所以 $G/C_G(H)$ 同构于 $\mathrm{Aut}(H)$ 的子群，从而
   $$|G/C_G(H)| \mid |\mathrm{Aut}(H)|$$
   G 的阶为 $203 = 7 \times 29$，从而 $|G/C_G(H)|$ 为 203 的因子. 同时，$|\mathrm{Aut}(H)| = 6$，从而 $|G/C_G(H)|$ 为 6 的因子. 由于 $(203, 6) = 1$，所以只能有 $|G/C_G(H)| = 1$，即 $G = C_G(H)$. 这就说明，对任意的 $g \in G, h \in H$，有 $gh = hg$，从而 $H \subset Z(G)$，即 $H < Z(G)$.
2. 考虑商群 G/H，$|G/H| = |G|/|H| = 29$ 为素数，所以 $G/H \simeq \mathbb{Z}_{29}$. 设 $H = \langle h \rangle$，$G/H = \langle \bar{g} \rangle$.
   首先，$H < Z(G)$，所以 $gh = hg$. 其次，G/H 中的任意元素，都可表示为 $(\bar{g})^k = \overline{g^k}$，从而 G 中的任意元素，都可表示为 $g^k h^l$. 从而，对 G 的任意两个元素 $g^i h^j, g^k h^l$，有：
   $$(g^i h^j)(g^k h^l) = g^{i+k} h^{j+l} = (g^k h^l)(g^i h^j)$$
   所以，G 是交换群.

✍ **练习 5.73*** 设 G 是 1575 阶群. 证明：若 H 是 G 的 9 阶正规子群，则 $H < Z(G)$.

待定

✍ **练习 5.74** 设 p 是素数，P 是 S_p 的 p 阶子群. 证明：$N_{S_p}(P)/C_{S_p}(P) \simeq \mathrm{Aut}(P)$.

5.5 Sylow 定理

5.5.1 知识要点

设 G 是群，p 是素数.

1. p-群：阶为 $p^\alpha, \alpha \in \mathbb{Z}_+$ 的群.
2. G 的 p-子群：G 的为 p-群的子群.
3. G 的 Sylow p-子群：$|G| = p^\alpha m$，其中 $p \nmid m$，G 的 $= p^\alpha$ 阶子群.
   G 的 Sylow p-子群的集合记为 $Syl_p(G)$，其阶记为 $n_p(G)$.
4. (Sylow 定理)：设 $|G| = p^\alpha m$，$p \nmid m$. 则
   (a). G 一定有 Sylow p-子群；
   (b). 若 P 是 G 的 Sylow p-子群，Q 是 G 的 p-子群，于是存在 $g \in G$，使得 $Q < gPg^{-1}$. 特别的，任意两个 G 的 Sylow p-子群共轭；
   (c). $n_p \equiv 1 \mod p$，且 $n_p \mid m$.
5. (只有一个 Sylow p-子群)：设 P 是 G 的 Sylow p-子群，则以下命题等价
   (a). $n_p = 1$；
   (b). $P \lhd G$；
   (c). P char G；
   (d). 若 $X = \{x \in G : |x| = p^k, k \in \mathbb{N}\}$，则 $\langle X \rangle$ 是 p-子群.

5.5.2 从定理证明中学解题

5.5.3 典型例题

5.5.3.1 Sylow 定理的应用：讨论给定阶群的结构性质

我们知道，给定一个群的阶，如果阶数不是很特别（比如素因子很少），那么我们对于该群的结构认知，仅限于 Cauchy 定理，即阶的每个素因子阶的子群存在. 而 Sylow 定理提供了另一个方向的性质，即阶的每个素因子的最高次幂的阶的子群存在，这样的子群个数为 p 的倍数加 1，且整除阶的不含 p 因子的部分. 我们用几个例子来展示这些信息综合起来的威力.

例题 5.9 证明：30 阶群 G 必有一正规子群同构于 $\mathbb{Z}_{15}$.

注 分析：$30=2\times3\times5$，由于我们是首次使用 Sylow 定理，没有任何经验，我们不妨对 30 的三个素因子 $2,3,5$ 挨个使用一遍 Sylow 定理，看看能得到什么结论：

1. $n_2=2k_2+1$，且 $n_2|15$；
2. $n_3=3k_3+1$，且 $n_3|10$；
3. $n_5=5k_5+1$，且 $n_5|6$.

可以看到我们给出了 n_p 和 k_p 的不定方程组，分别在 $n_p>0,k_p\geqslant0$ 的范围下解之：

$$(k_2,n_2)=(0,1),(2,5),(7,15)$$
$$(k_3,n_3)=(0,1),(3,10)$$
$$(k_5,n_5)=(0,1),(1,6)$$

当然，我们最喜欢的是 $(0,1)$，此时 Sylow p-子群是特征子群，性质很强. 而面对其他情形，就要结合别的条件综合分析了. 另一方面，当 p 越大时，n_p 的可能取值种类越少，此时分类讨论越方便. 于是在没有特殊情况时，先考虑大的素因子总是更有利的.

证明 因为 $30=2\times3\times5$，所以设 $P\in Syl_5(G),Q\in Syl_3(G)$. 下证：$P,Q$ 至少有一个为 G 的正规子群.（从而 PQ 为 G 的 15 阶群，即 $PQ\simeq\mathbb{Z}_{15}$. 该命题的证明见下题）若 G 只有一个 Sylow 3-子群或 Sylow 5-子群，则命题立证.

而若 Sylow 3-子群或 Sylow 5-子群都不止一个，则由分析中的讨论可知，$n_3=10$ 且 $n_5=6$. 考虑 G 的阶为 3 或 5 的元素个数. 在每个 Sylow 3-子群中，都有两个不同的阶为 3 的元素，且不同的 Sylow 3-子群，包含的元素除 1 意外均不相同（为什么？）. 所以 G 中一共有 20 个 3 阶元素. 同理，G 中共有 $6*4=24$ 个 5 阶元素. 3 阶和 5 阶元素显然不相同，所以 G 中至少有 $20+24+1=45$ 个不同的元素，而 G 一共只有 30 个元素，矛盾！

综上，原命题成立.

笔记 “对特定阶的元素计数”这一手法，我们在证明两个群不同构时已经使用过，相信读者对此不会感到陌生.

例题 5.10 设 G 是 12 阶群，证明：G 有一个正规的 3 阶子群，或 $G\simeq A_4$.

证明 由 Sylow 定理，G 必有一 3 阶 Sylow 子群，且 $n_3=1,4$.

若 $n_3=1$，则 3 阶 Sylow 子群必为正规子群.

若 $n_3=4$，取 $P\in Syl_3(G)$. 又 $[G:N_G(P)]=n_3=4$，所以 $N_G(P)$ 的阶为 3，又因为 $P<N_G(P)$，且 $|P|=3$，所以 $N_G(P)=P$. 定义 G 对 $Syl_3(G)$ 的共轭作用 φ，则有对应的群同态

$$\varphi:G\to S_4$$

（因为 $Syl_3(G)$ 里有 4 个元素）

作用的核 K 是 G 的正规子群，且对任意 $k\in K,Q\in Syl_3(G)$ 有 $k\cdot Q:=kQk^{-1}=Q$. 特别的，取 $Q=P$，则 $kPk^{-1}=P$，即 $k\in N_G(P)$，于是 $K<N_G(P)=P$. 而 P 为 3 阶群，于是 K 只能为 $\{1\}$ 或 P. 注意到 $K\lhd G$，但是 P 不是 G 的正规子群，所以 $K=\{1\}$. 这就说明，φ 是单同态. 从而 $G\simeq\operatorname{im}\varphi<S_4$.

由于每个 3 阶群中都有两个 3 阶元素，且互不相同（否则他们所在的 3 阶群就相同了），所以 G 有 8 个 3 阶

元素. 而我们已经知道，S_4 中恰有 8 个 3 阶元素【参看 2.2 节练习 2.54】，且都包含于 A_4 中，所以

$$|\operatorname{im}\varphi \cap A_4| \geqslant 8$$

同时必须满足 $|\operatorname{im}\varphi \cap A_4|$ 是 12 的因子，所以只能有

$$|\operatorname{im}\varphi \cap A_4| = 12$$

即 $G \simeq \operatorname{im}\varphi = A_4$.

综上，原命题即证.

笔记 本题的突破口在于，当 $n_3 = 4$ 时，发现了 $P = N_G(P)$. 而这一情况的出现并不唯一，即如果 $|G| = pq$，p 为素数，且 $p \mid (q-1)$，则 n_p 有可能取到 q，此时 $[G : N_G(P)] = n_p = q$，从而 $|N_G(P)| = p = |P|$，即 $P = N_G(P)$.

例题 5.11 设群 G 的阶为 pq，其中 p, q 均为阶数，且 $p < q$. 证明：

1. G 必有一阶为 q 的子群 Q，且 $Q \lhd G$；
2. G 必有一阶为 p 的子群 P. 进一步，若 $p \nmid q-1$，则 $P \lhd G$，且 G 为循环群.

证明

1. 由 Sylow 定理，G 必有一阶为 q 的子群 Q，且 $n_q = kq+1$，$n_q \mid p$. 由于 $q > p$，所以 k 只能取 0，从而 $n_q = 1$. 于是 $Q \lhd G$.
2. 由 Sylow 定理，G 必有一阶为 p 的子群 P，且 $n_p = kp+1$，$n_p \mid q$. 由于 q 是素数，所以 $n_p = 1, q$. 而若 $kp+1 = n_p = q$，则 $q-1 = kp$，即 $p \mid q-1$，与题设矛盾. 从而 $n_p = 1$，即 $P \lhd G$.
   因为 p, q 是素数，所以 P, Q 都为循环群，记 $P = \langle x \rangle$，$Q = \langle y \rangle$. 由于 $P, Q \lhd G$，且 $P \cap Q = 1$【为什么 ?】，所以任意的 $a \in P, b \in Q$ 都满足 $ab = ba$.（参见 2.5 节习题 2.153）于是有 $|xy| = |x| \cdot |y| = pq$，从而 G 必为循环群（同构于 $\mathbb{Z}_{pq}$.）

练习 5.75 设 G 是 p^2q 阶群，其中 p, q 是不同的素数. 证明：G 必有正规的 Sylow 子群.

证明 TBD

练习 5.76 证明：132 阶群 G 不是单群.

证明 假设 G 是单群，因为 $132 = 2^2 \times 3 \times 11$. 由 Sylow 定理：

1. G 必有 11 阶子群，且 $n_{11} = 1, 12$，由于 G 是单群，所以不存在除 $\{1\}, G$ 以外的正规子群，从而 $n_{11} \neq 1$，即 $n_{11} = 12$.
2. G 必有 3 阶子群，且 $n_3 = 1, 4, 22$，同理 $n_3 \neq 1$，于是 $n_3 \geqslant 4$.
3. G 必有 $2^2 = 4$ 阶子群，且 $n_2 \geqslant 3$.

考虑 G 的 12 个 11 阶群，其中阶为 11 的元素一共有 $12 \times 10 = 120$ 个. 再考虑 G 的至少 4 个 3 阶群，则其中阶为 3 的元素一共有 $4 \times 2 = 8$ 个. 最后考虑 G 的至少 2 个 4 阶群，其中至少有 5 个不同的元素（4 阶群只有 $\mathbb{Z}_4$ 和 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 两种同构型，分类讨论即可），且阶为 $1, 2, 4$，所以与前述的元素都不相同. 综合以上讨论，G 中至少有 $120 + 8 + 5 = 133$ 个元素，但 $|G| = 132 < 133$，矛盾！所以 G 不是单群.

5.5.4 习题

以下均设 G 是有限群，p 是素数.

5.5.4.1 群的 Sylow 子群

练习 5.77

1. 证明：若 P 是 G 的 Sylow p-子群，$H < G$ 且 $P < H$，则 P 是 H 的 Sylow p-子群；
2. 举例说明：G 的 Sylow p-子群的子群，不一定是 G 的 Sylow p-子群.

证明

1. 记 $|G| = p^\alpha m$，其中 $p \nmid m$，于是 $|P| = p^\alpha$. 因为 $P < H$，所以 $p^\alpha \mid |H|$，又因为 $H < G$，所以 $|H| \mid p^\alpha m$，所以 $|H|$ 中 p 因子只能为 α 幂次，从而 $P \in Syl_p(H)$.

2. $\mathbb{Z}_{12}=\langle x\rangle$ 中，$\langle x^3\rangle\simeq\mathbb{Z}_4$ 是 $\mathbb{Z}_{12}$ 的 Sylow 2-子群，但它的子群 $\langle x^6\rangle\simeq\mathbb{Z}_2$ 不是 $\mathbb{Z}_{12}$ 的 Sylow 2-子群.

✍ **练习 5.78** 证明：若 $H<G$，$Q\in Syl_p(H)$，则对任意的 $g\in G$，有 $gQg^{-1}\in Syl_p(gHg^{-1})$.

✍ **练习 5.79** 写出 $D_{12}, S_3\times S_3$ 的 Sylow 2-子群和 Sylow 3-子群.

注 提示：两个群的阶都是 $12=2^2\times 3$，所以 Sylow 2-子群是 4 阶子群，Sylow 3-子群是 3 阶子群. 寻找子群的方法我们已经有一个专题讲过，大家可以参考，这里我们给出针对 D_{12} 的思考方法.

大家如果对小阶群的种类非常熟悉的话，就会知道，4 阶群只有两种同构型 $\mathbb{Z}_4$ 和 $V_4\simeq\mathbb{Z}_2\times\mathbb{Z}_2$，前者会包含两个 4 阶元素，后者包含 3 个 2 阶元素. 而 D_{12} 里没有 4 阶元素，所以 4 阶子群只能同构于 V_4，从而我们找出 D_{12} 所有的 2 阶元素

$$r^3$$

$$s, sr, sr^2, sr^3, sr^4, sr^5$$

两两组合看看能否生成同构于 V_4 的群即可.

3 阶群只有一种同构型 $\mathbb{Z}_3$，其中有两个 3 阶元素. 找出 D_{12} 中的所有 3 阶元素

$$r^2, r^4$$

写出由他们分别生成的不同的 3 阶群即可.

$S_3\times S_3$ 可类似讨论，这里不赘述.

解

1. $D_{12}=\langle r,s\mid r^6=s^2=1, rs=sr^{-1}\rangle$

   Sylow 2-子群：

   $$\langle r^3,s\rangle, \langle r^3,sr\rangle, \langle r^3,sr^2\rangle$$
   $$\langle sr,sr^4\rangle, \langle sr^2,sr^5\rangle$$

   Sylow 3-子群：

   $$\langle r^2\rangle$$

2. $G=S_3\times S_3$

   Sylow 2-子群：记 $\sigma_1=(1\ 2), \sigma_2=(1\ 3), \sigma_3=(2\ 3)$，则对任意的 $i,j\in\{1,2,3\}$

   $$\langle(\sigma_i,\sigma_j)\rangle$$

   都是 G 的 4 阶子群.

   Sylow 3-子群：记 $\rho=(1\ 2\ 3)$（则 $(1\ 3\ 2)=\rho^2$），于是

   $$\langle(1,\rho)\rangle, \langle(1,\rho^2)\rangle$$
   $$\langle(\rho,1)\rangle, \langle(\rho^2,1)\rangle$$

   为 G 的全部 3 阶子群.

✍ **练习 5.80** 写出 A_4, S_4 的 Sylow 3-子群.

✍ **练习 5.81** 写出 S_4 的 Sylow 2-子群，并找出 S_4 中的元素 σ，使得存在 $P,Q\in Syl_2(S_4)$，满足 $P=\sigma Q\sigma^{-1}$.

✍ **练习 5.82** 写出 S_5 的两个 Sylow 2-子群 P,Q，并找出 S_5 中的元素 σ，使得 $P=\sigma Q\sigma^{-1}$.

✍ **练习 5.83** 证明：对每个奇素数 p，D_{2n} 的 Sylow p-子群都是循环且正规的.

注 提示：D_{2n} 中每个 sr^i 都是 2 阶，因此它们不能作为 Sylow p-子群的元素，从而任意 Sylow p-子群只能为循环群 $\langle r\mid r^n=1\rangle$ 的子群. 而我们在循环群一节已经学过，有限循环群的阶的每个正因子，都对应唯一的相应阶的循环子群. 从而 $n_p=1$，即 Sylow p-子群正规.

✍ **练习 5.84** 设 $2n=2^ak$，其中 k 为奇数. 证明：D_{2n} 的 Sylow 2-子群的个数为 k.

证明 以下证明：若 $P\in Syl_2(D_{2n})$，则 $N_{D_{2n}}(P)=P$.（从而 $n_2=[D_{2n}:N_{D_{2n}}(P)]=k$.）

设 $P\in Syl_2(D_{2n})$. 因为 $P<N_{D_{2n}}(P)$，所以只需证 $N_{D_{2n}}(P)<P$. 设 $x\in N_{D_{2n}}(P)$，于是 $xP=Px$？D_{2n} 的特殊性在哪？

若 $a=1$，则 $P=\langle sr^i\rangle$，其中 $i\in\{0,\cdots,k-1\}$. 于是

$$sP\neq Ps$$
$$r^jP\neq Pr^j$$
$$sr^jP\neq Psr^j\quad(j\neq i)$$

从而 $N_{D_{2n}}(P)=P$，命题得证.

若 $a>1$. 因为 $|r|=2^{a-1}k$，于是 $r^k,r^{2k},\cdots,r^{2^{a-2}k}$ 的阶为 2 的幂次. 这样 P 中包含的元素只能形如 $r^{2^ik},i\in\{0,\cdots,k-2\}$，和 sr^u. 并且，若 P 中包含 sr^u 和 $sr^v,u>v$，则 $u-v$ 必须等于某个 2^ik.

我们进一步考虑 P 的生成元，首先，如果 P 中包含 r 的幂次，则只需选择指数最小的一个（不妨设为 r^{2^ik}），即可生成其他幂次高的元素. 其次，考虑形如 sr^j 的元素，因为 sr^u 和 $sr^v,u>v$ 会生成 r^{u-v}，于是我们考察所有形如 sr^j 的元素的 r 的指数差，并记最小的差为 nk. 再取 r 的指数最小的元素为 $sr^i\cdots\cdots$

【知道怎么做了，但是太复杂，回头再考虑有没有简单做法.】

TBD

5.5.4.2 寻找有限群的正规子群

✍ **练习 5.85** 证明：56 阶群有一个正规的 Sylow p-子群.

注 提示：$n_7=8$ 且 8 阶群不唯一时，7 阶元素有 48 个，2 的幂次阶元素至少有 $8+1=9$ 个，从而矛盾！

✍ **练习 5.86** 证明：312 阶群有一个正规的 Sylow p-子群.

✍ **练习 5.87** 证明：351 阶群有一个正规的 Sylow p-子群.

✍ **练习 5.88** 证明：105 阶群有一个正规的 Sylow 5-子群或正规的 Sylow 7-子群.

✍ **练习 5.89** 证明：200 阶群有一个正规的 Sylow 5-子群.

✍ **练习 5.90** 设 G 的阶为 pqr，其中 $p<q<r$ 均为素数. 证明：G 必有一个正规的 p、q 或 r 阶 Sylow 子群.

证明 设 G 没有正规的 p、q 或 r 阶 Sylow 子群. 先考虑 r 阶 Sylow 子群的个数 $n_r=kr+1,k>0$，由于 $n_r\mid pq$，但是由于 $r>p,r>q$，所以 $kr+1\nmid p,kr+1\nmid q$，于是只能有 $kr+1=pq$. 从而 G 中 r 阶的元素有 $(r-1)pq$ 个.

此外，$n_p\geqslant p+1,n_q\geqslant q+1$，于是 G 中 p 阶元素至少有 $(p-1)(p+1)$ 个，q 阶元素至少有 $(q-1)(q+1)$ 个，再算上幺元，G 中的元素至少有 $n:=(r-1)pq+(p-1)(p+1)+(q-1)(q+1)+1$ 个. 但是我们有：

$$\begin{aligned}n&=pqr+(p^2+q^2-pq)-1\\&>pqr+pq-1\quad(\text{对 }p,q\text{ 使用均值不等式，且二者不同，所以取不到等号})\\&>pqr\quad(p,q\geqslant 2)\end{aligned}$$

矛盾！所以原命题成立.

5.5.5 思考题

5.5.5.1 Sylow 定理的证明

✍ **练习 5.91** 引理：设 $P\in Syl_p(G)$. 若 Q 是 G 的 p-子群，则 $Q\cap N_G(P)=Q\cap P$.

证明 因为 $P<N_G(P)$，所以 $Q\cap P<Q\cap N_G(P)$. 下证：$H:=Q\cap N_G(P)<Q\cap P$. 又因为 $H<Q$，所以只需证：$H<P$.

因为 $H<N_G(P)$，所以 $HP=PH$，从而 PH 是 G 的子群. 同时

$$|PH|=\frac{|P||H|}{|P\cap H|}.$$

由于 $|P|,|H|$ 都是 p 的幂次，所以 $|PH|$ 也只能为 p 的幂次，即 $|PH|$ 是 p-子群.

又因为 $P<PH$，所以 p^α 整除 $|PH|$. 而 G 的 p-子群的阶至多为 p^α，所以只能有 $|PH|=p^\alpha$，即 $P=PH$，由此可得：$H<P$.（对任意的 $h\in H$，有 $hP\in P$，即 $h\in P$.）

笔记 本题的解题要点在于，如何使用条件 $P\in Syl_p(G)$.

我们来分析 Sylow p-子群 P 的特点（或者说，相对于 P 是子群，多出的特点有哪些），它主要有两个：一个是 P 的阶非常简单，只有一个素因子 p，从而“等式的因子分析”之类的手法就很容易使用. 另一个是指数 α 的最大性，这就会使得每个包含 P 的 p-子群，只能是 P 本身.

练习 5.92（Sylow 定理）：设 $|G|=p^\alpha m$，$p\nmid m$. 则

1. G 一定有 Sylow p-子群；
2. 若 P 是 G 的 Sylow p-子群，Q 是 G 的 p-子群，于是存在 $g\in G$，使得 $Q<gPg^{-1}$. 特别的，任意两个 G 的 Sylow p-子群共轭；
3. $n_p\equiv 1 \mod p$，且 $n_p\mid m$.

证明

1. 对 $|G|$ 做数学归纳法.

   若 $|G|=1$，则命题平凡的成立.

   以下设：所有阶小于 $|G|$ 的群都有 Sylow p-子群. 欲证：G 有 Sylow p-子群.

   考虑 G 的中心 $Z(G)$. 一方面，若 p 整除 $|Z(G)|$，则由 Cauchy 定理可知，$Z(G)$ 有一个 p 阶子群 N. 设 $\bar G=G/N$，则 $|\bar G|=p^{\alpha-1}m$. 由归纳假设，$\bar G$ 有 $p^{\alpha-1}$ 阶子群 $\bar P$，于是存在包含 N 的子群 P 使得 $\bar P=P/N$（第四同构定理），此时 $|P|=|\bar P|\cdot|N|=p^\alpha$，即 P 是 G 的 Sylow 子群.

   另一方面，设 p 不整除 $|Z(G)|$. 设 $g_1,\cdots,g_r$ 是 G 的不属于 $Z(G)$ 的共轭类的代表元，则 G 的类方程为：

   $$|G|=|Z(G)|+\sum_{i=1}^{r}[G:C_G(g_i)]$$

   若所有的 $[G:C_G(g_i)]$ 都被 p 整除，则 $|Z(G)|$ 也被 p 整除，矛盾！于是必有一个 $[G:C_G(g_j)]$ 不被 p 整除. 记 $H=C_G(g_j)$，则 $|H|=p^\alpha k$，其中 $p\nmid k$. 因为 $g_j\notin Z(G)$，所以 $|H|<|G|$. 由归纳假设，H 有 p^α 阶子群 P，而 $P<H<G$，所以 P 也是 G 的 Sylow p-子群.

   综上，G 一定有 Sylow p-子群.

2. 记 P 的共轭类的集合为 $\mathscr{S}:=\{P_1,\cdots,P_r\}$，且设 Q 是 G 的任意 p-子群. 先证明：$r\equiv 1 \mod p$.（注意到 Q 的选择与 r 无关.）

   考虑 Q 对 $\mathscr{S}$ 的共轭作用，并设所有不同的轨道为 $O_1,\cdots,O_s$，于是

   $$\mathscr{S}=\bigsqcup_{i=1}^{s}O_i$$

   $$r=|\mathscr{S}|=\sum_{i=1}^{s}|O_i|$$

   在每个 O_i 中取一代表元 P_i，于是 $|O_i|=[Q:N_Q(P_i)]$. 又因为

   $$N_Q(P_i)=N_G(P_i)\cap Q=P_i\cap Q$$

   所以 $|O_i|=[Q:P_i\cap Q],1\leqslant i\leqslant s$.

   由于 Q 是任取的，不妨设 $Q=P_1$，于是 $O_1=\{P_1\}$，即 $|O_1|=1$. 对任意 $i>1$，由于 $P_1\neq P_i$，所以 $P_1\cap P_i<P_1$，从而

   $$|O_i|=[P_1:P_i\cap P_1]>1$$

   由于 P_1,P_i 都是 Sylow p-子群，所以 $P_i\cap P_1$ 的阶必为 p 的幂次，从而 p 整除 $|O_i|$. 于是我们有：

   $$r=|O_1|+\sum_{i=2}^{s}|O_i|\equiv 1 \mod p$$

   回到到原命题的证明过程. 假设 p-子群 Q 不包含于任何一个 P_i（即命题 (2) 不成立），此时对所有的 i，

$Q\cap P_i$ 都是 Q 的真子群，从而

$$|O_i|=[Q:P_i\cap Q]>1$$

即 p 整除 $|O_i|$，于是 $p\mid r$，这与 $r\equiv 1 \mod p$ 矛盾! 从而任意 p-子群 Q 总包含于某个 P 的共轭.

特别的，若 Q 也为 Sylow p-子群，由于其为 p-子群，所以 Q 包含于 P 的某个共轭 P_i. 同时 $|Q|=p^\alpha=|P_i|$，所以 $Q=P_i$，即 Q 与 P 共轭.

3. 由第二小问，$\mathscr{S}=Syl_p(G)$，从而 $n_p=r\equiv 1 \mod p$. 因为 $n_p=|\mathscr{S}|=[G:N_G(P)]$，且 $P<N_G(P)$（即 $|N_G(P)|$ 被 p^α 整除，不妨设 $|N_G(P)|=p^\alpha k$），于是 $n_p=m/k$，即 $n_p\mid m$.

5.5.5.2 60 阶群的性质

5.6 群的直积

5.6.1 知识要点

1. 群 $G_1,\cdots,G_n$ 的直积：定义集合

$$G_1\times\cdots\times G_n:=\{(g_1,\cdots,g_n):\ g_i\in G_i,\forall i\}$$

其上的运算定义为 $(g_1,\cdots,g_n)(h_1,\cdots,h_n)=(g_1h_1,\cdots,g_nh_n)$.

2. （直积的分量）：设 $G_1,\cdots,G_n$ 为群，$G=G_1\times\cdots\times G_n$.
   (a). $G_i\simeq\{(1,\cdots,1,g_i,1,\cdots,1):\ g_i\in G_i\}$；（以后我们视二者相等，用 G_i 指代后者）
   (b). $G/G_i\simeq G_1\times\cdots\times G_{i-1}\times G_{i+1}\times G_n$；
   (c). （投影）：对每个 i，定义 $\pi_i:G\to G_i$

$$(g_1,\cdots,g_n)\mapsto g_i$$

   于是 π_i 是满同态；
   (d). 若 $x\in G_i,y\in G_j,i\neq j$，则 $xy=yx$.
3. （识别定理 recognition theorem）：设 G 是群，$H,K\lhd G$，且 $H\cap K=1$，则 $HK\simeq H\times K$.（此时我们称 HK 为 H 和 K 的内直积，$H\times K$ 称为外直积）

5.6.2 从定理证明中学解题

问题 5.16 （识别定理）：设 G 是群，$H,K\lhd G$，且 $H\cap K=1$，则 $HK\simeq H\times K$.

证明 我们在 2.5 节练习 2.152 中已经证明，对任意的 $h\in H,k\in K$，有 $hk=kh$. 且由于 $HK=KH$，所以 $HK<G$.

下证：HK 中的每个元素，都可唯一的表达为 hk 的形式，其中 $h\in H,k\in K$. 设 $h_1k_1=h_2k_2$，则 $h_2^{-1}h_1=k_2k_1^{-1}\in K$，即 $h_2^{-1}h_1\in K\cap H=\{1\}$，也就是 $h_1=h_2$. 同理可证 $k_1=k_2$，命题得证.

定义映射

$$\varphi:HK\to H\cap K$$
$$hk\mapsto(h,k)$$

由前述引理，φ 是良定义的.【编者问：这里良定义的问题出在哪儿？】我们只需证：φ 是同构.

首先，对任意 $hk,h'k'\in HK$，有：

$$\begin{aligned}\varphi(hkh'k')&=\varphi(hh'kk')\\&=(hh',kk')\\&=(h,k)(h',k')\\&=\varphi(hk)\varphi(h'k')\end{aligned}$$

于是 φ 是同态.

其次，对任意 $(h,k)\in H\times K$，都有 $hk\in HK$，使得 $\varphi(hk)=(h,k)$，于是 φ 是满射.

最后，因为

$$\begin{aligned}\ker\varphi&=\{hk\in HK:\ \varphi(hk)=(1,1)\}\\&=\{hk\in HK:\ (h,k)=(1,1)\}\\&=\{hk\in HK:\ h=1,k=1\}\\&=\{1\in HK\}\quad(\text{注意到 }1\in HK\text{ 只能唯一的表达为 }1\cdot 1.)\qquad\qquad=\{1\}\end{aligned}$$

所以 φ 为单射.

综上，φ 为同构，即 $HK\simeq H\times K$.

笔记 这一定理的证明，没有使用任何新的知识点和技巧，读者只要熟练掌握了截至群同态部分的知识，就可以熟练的证明它. 建议读者先独立地证明一下这个定理，以此检验自己之前知识的学习情况.

5.6.3 典型例题

5.6.4 习题

以下各题均设 $G_1,\cdots,G_n$ 为群，$G=G_1\times G_n$.

5.6.4.1 直积的例子

练习 5.93 证明：

1. $Z(G_1\times\cdots\times G_n)=Z(G_1)\times\cdots\times Z(G_n)$；
2. 群的直积是交换群，当且仅当它的每个分量也是交换群.

证明

1. 一方面，设 $(g_1,\cdots,g_n)\in Z(G_1\times\cdots\times G_n)$. 考虑 g_1，由群的中心的定义可得，对任意 $h_1\in G_1$ 有：

$$(h_1,1,\cdots,1)(g_1,\cdots,g_n)=(g_1,\cdots,g_n)(h_1,1,\cdots,1)$$

$$(h_1g_1,g_2,\cdots,g_n)=(g_1h_1,g_2,\cdots,g_n)$$

即 $h_1g_1=g_1h_1$，于是 $g_1\in Z(G_1)$. 同理，对任意 i 都有 $g_i\in Z(G_i)$，这就说明：

$$(g_1,\cdots,g_n)\in Z(G_1)\times\cdots\times Z(G_n).$$

即

$$Z(G_1\times\cdots\times G_n)\subset Z(G_1)\times\cdots\times Z(G_n).$$

另一方面，设 $(g_1,\cdots,g_n)\in Z(G_1)\times\cdots\times Z(G_n)$，即对每个 i 有 $g_i\in Z(G_i)$. 于是对任意的 $(h_1,\cdots,h_n)\in G_1\times\cdots\times G_n$ 有：

$$\begin{aligned}(g_1,\cdots,g_n)(h_1,\cdots,h_n)&=(g_1h_1,\cdots,g_nh_n)\\&=(h_1g_1,\cdots,h_ng_n)\\&=(h_1,\cdots,h_n)(g_1,\cdots,g_n)\end{aligned}$$

从而 $(g_1,\cdots,g_n)\in Z(G_1\times\cdots\times G_n)$，即

$$Z(G_1)\times\cdots\times Z(G_n)\subset Z(G_1\times\cdots\times G_n).$$

综上，$Z(G_1\times\cdots\times G_n)=Z(G_1)\times\cdots\times Z(G_n)$.

2. 一个群为交换群，当且仅当它等于它的中心，结合第一小问的结论即证.

5.6.4.2 直积的子群

✍ **练习 5.94** 设 I 是集合 $A=\{1,\cdots,n\}$ 的非空真子集，$J=A-I$. 定义：

$$G_I=\{(g_1,\cdots,g_n)\in G:\ g_j=1,\forall j\in J\}.$$

试证明：

1. $G_I\simeq\prod_{i\in I}G_i$；
2. $G_I\simeq G$，且 $G/G_I\simeq G_J$；
3. $G\simeq G_I\times G_J$.
4. 设 K 也是 A 的非空真子群，且 $K\cap I=\varnothing$，则对任意的 $x\in G_I,y\in G_J$ 有 $xy=yx$.

✍ **练习 5.95** 设 A,B 是有限群，p 是素数. 证明：

1. $A\times B$ 的 Sylow p-子群都形如 $P\times Q$，其中 $P\in Syl_p(A),Q\in Syl_p(B)$；
2. $n_p(A\times B)=n_p(A)n_p(B)$.

注 提示：注意到 $|A\times B|=|A||B|$，且 Sylow p-子群的阶必须取到 p 的最高次幂.

笔记 一般的，该结论对任意有限个群的直积都成立.

✍ **练习 5.96*** 试举出 $Q_8\times\mathbb{Z}_4$ 的不正规的子群.

解 ？

笔记 注意到 $A\times B$ 的子群并不一定形如 $P\times Q,P<A,Q<B$.

✍ **练习 5.97** 证明：$Q_8\times\mathbb{Z}_2^n$ 的任意子群都正规.

证明 ？

5.6.4.3 未分类

✍ **练习 5.98** 取固定的 $\pi\in S_n$. 证明映射：

$$\begin{aligned}\varphi_\pi:G_1\times\cdots\times G_n&\to G_{\pi^{-1}(1)}\times\cdots\times G_{\pi^{-1}(n)}\\(g_1,\cdots,g_n)&\mapsto(g_{\pi^{-1}(1)},\cdots,g_{\pi^{-1}(n)})\end{aligned}$$

是同构.

注 提示：注意到 $\pi^{-1}\in S_n$.

5.7 群的半直积

5.7.1 知识要点

1. 群 H 和 K 关于 φ 的半直积：$H\rtimes_\varphi K=\{(h,k):\ h\in H,k\in K\}$，连同运算 $(h,k)(h',k')=(h(k\cdot h'),kk')$. 其中 $\varphi:K\to\mathrm{Aut}(H)$ 是群同态，且记 $k\cdot h:=\varphi(k)(h)$.
2. （半直积的基本性质）：设 H,K 为群，$\varphi:K\to\mathrm{Aut}(H)$ 是群同态，记 $G=H\rtimes_\varphi K$.
   (a). （群的幺和逆）：G 的幺：$(1,1)$，(h,k) 的逆：$(k^{-1}\cdot h^{-1},k^{-1})$；
   (b). （群的阶）：$|G|=|H||K|$；
   (c). （“分量群”是子群）：$H\simeq\{(h,1):h\in H\}\lhd G$，$K\simeq\{(1,k):k\in K\}<G$；（以下视这些同构为相等）
   (d). （“分量群”的交）：$H\cap K=1$；
   (e). （共轭形式）：对任意的 $h\in H$ 和任意的 $k\in K$，有 $khk^{-1}=k\cdot h$.
3. （半直积与直积）：设 H,K 为群，$\varphi:K\to\mathrm{Aut}(H)$ 是群同态，则下列命题等价：
   (a). $H\rtimes K$ 到 $H\times K$ 的恒等映射是群同态；
   (b). φ 是平凡的；（即对任意的 $k\in K$，有 $\varphi(k)=1$）

(c). $K \lhd H \rtimes K$.

4. (半直积与积)：设 G 为群，$H \lhd G$，$K < G$，$H \cap K = 1$. 定义 K 对 H 的作用为 $k \cdot h = khk^{-1}$，且对应的群同态为 $\varphi : K \to \mathrm{Aut}(H)$，则 $HK \simeq H \rtimes K$.
5. 设 $H, K < G$. K 是 H 在 G 中的补（complement)：满足 $G = HK$ 且 $H \cap K = 1$.

5.7.2 从定理证明中学解题

5.7.2.1 半直积的基本性质

笔者强烈建议读者把下列定理独立的证明一遍！它可以帮助读者熟悉半直积的定义方式，同时能够综合的复习前面学过的子群、正规子群、群作用、自同构等基础知识. 如果读者对于证明该定理感到有一定的难度，建议有针对的复习前面学过的知识.

问题 5.17 (半直积的基本性质)：设 H, K 为群，$\varphi : K \to \mathrm{Aut}(H)$ 是群同态，记 $G = H \rtimes_\varphi K$.

1. (群的幺和逆)：G 的幺：$(1,1)$，(h,k) 的逆：$(k^{-1} \cdot h^{-1}, k^{-1})$;
2. (群的阶)：$|G| = |H||K|$;
3. (“分量群”是子群)：$H \simeq \{(h,1) : h \in H\} \lhd G$，$K \simeq \{(1,k) : k \in K\} < G$;（以下视这些同构为相等）
4. (“分量群”的交)：$H \cap K = \{1\}$;
5. (共轭形式)：对任意的 $h \in H$ 和任意的 $k \in K$，有 $khk^{-1} = k \cdot h$.

证明

1. 我们证明：G 是群. 设 $(h,k), (h_1,k_1), (h_2,k_2), (h_3,k_3) \in G$:
   (a). (封闭性)：$(h_1,k_1)(h_2,k_2) = (h_1k_1 \cdot h_2, k_1k_2) \in G$.
   (b). (结合律)：因为

$$\begin{aligned}((h_1,k_1)(h_2,k_2))(h_3,k_3) &= (h_1k_1 \cdot h_2, k_1k_2)(h_3,k_3)\\ &= (h_1(k_1 \cdot h_2)(k_1k_2 \cdot h_3), k_1k_2k_3)\end{aligned}$$

且

$$\begin{aligned}(h_1,k_1)((h_2,k_2)(h_3,k_3)) &= (h_1,k_1)(h_2k_2 \cdot h_3, k_2k_3)\\ &= (h_1k_1 \cdot (h_2k_2 \cdot h_3), k_1k_2k_3)\end{aligned}$$

注意到：

$$\begin{aligned}h_1k_1 \cdot (h_2k_2 \cdot h_3) &= h_1(k_1 \cdot h_2)(k_1 \cdot (k_2 \cdot h_3))\\ &= h_1(k_1 \cdot h_2)(k_1k_2 \cdot h_3)\end{aligned}$$

从而

$$((h_1,k_1)(h_2,k_2))(h_3,k_3) = (h_1,k_1)((h_2,k_2)(h_3,k_3))$$

   (c). (幺元)：考虑元素 $(1,1) \in G$，有

$$\begin{aligned}(1,1)(h,k) &= (1(1 \cdot h), 1k) = (h,k)\\ (h,k)(1,1) &= (hk \cdot 1, k)\end{aligned}$$

因为 $\varphi_k \in \mathrm{Aut}(H)$，所以 $k \cdot 1 = \varphi_k(1) = 1$，从而 $(hk \cdot 1, k) = (h,k)$，即 $(1,1)(h,k) = (h,k) = (h,k)(1,1)$，从而 $(1,1)$ 为 G 的幺元.

(d). (逆): 对元素 (h,k)，考虑 $(k^{-1}\cdot h^{-1},k^{-1})$ (显然它是 G 中的元素)，有

$$\begin{aligned}(h,k)(k^{-1}\cdot h^{-1},k^{-1}) &= (hk\cdot(k^{-1}\cdot h^{-1}),kk^{-1})\\ &= (h1\cdot h^{-1},1)\\ &= (hh^{-1},1)\\ &= (1,1)\end{aligned}$$

$$\begin{aligned}(k^{-1}\cdot h^{-1},k^{-1})(h,k) &= ((k^{-1}\cdot h^{-1})k^{-1}\cdot h,k^{-1}k)\\ &= (k^{-1}\cdot(h^{-1}h),1)\\ &= (k^{-1}\cdot 1,1) \qquad\qquad = (1,1)\end{aligned}$$

即 $(h,k)(k^{-1}\cdot h^{-1},k^{-1})=(k^{-1}\cdot h^{-1},k^{-1})(h,k)=(1,1)$，从而 $(k^{-1}\cdot h^{-1},k^{-1})$ 为 (h,k) 的逆.

综上，G 是群.

2. 先证明：对于 $(h_1,k_1),(h_2,k_2)\in G$，二者相等当且仅当 $h_1=h_2$, $k_1=k_2$.

一方面，$h_1=h_2$, $k_1=k_2$ 时，$(h_1,k_1)=(h_2,k_2)$ 是显然的.

另一方面，若 $(h_1,k_1)=(h_2,k_2)$，则有：

$$\begin{aligned}1=(1,1) &= (h_1,k_1)(h_2,k_2)^{-1}\\ &= (h_1,k_1)(k_2^{-1}\cdot h_2^{-1},k_2^{-1})\\ &= (h_1k_1k_2^{-1}\cdot h_2^{-1},k_1k_2^{-1})\end{aligned}$$

因为 $(1,1)$ 是幺元，而 G 中幺元唯一，从而必有

$$\begin{aligned}h_1k_1k_2^{-1}\cdot h_2 &= 1\\ k_1k_2^{-1} &= 1\end{aligned}$$

后者可得 $k_1=k_2$，代入前者即得 $h_1=h_2$. 从而命题得证.

回到原命题，因为 G 中的元素都形如 (h,k)，且两元素相等当且仅当两个分量都对应相等，于是 $|G|$ 等于两分量位置可取元素个数之乘积，即 $|H||K|$.

3. $H\simeq\{(h,1):h\in H\},K\simeq\{(1,k):k\in K\}$ 几乎是显然的，在此不赘述. (与群的直积部分类似，以后我们将这两个“同构”关系视为“相等”关系).

先证明：$H\lhd G$.

对任意的 $(h_1,1)\in H$ 和 $(h_2,k)\in G$，有：

$$\begin{aligned}(h_2,k)(h_1,1)(h_2,k)^{-1} &= (h_2k\cdot h_1,k)(k^{-1}\cdot h_2^{-1},k^{-1})\\ &= (h_2(k\cdot h_1)(k\cdot(k^{-1}\cdot h_2^{-1})),kk^{-1})\\ &= (h_2(k\cdot h_1)h_2^{-1},1)\in H\end{aligned}$$

从而 $H\lhd G$.

再证明：$K<G$.

首先，$(1,1)\in K$. 其次，对任意的 $(1,k_1),(1,k_2)\in K$，有：

$$\begin{aligned}(1,k_1)(1,k_2)^{-1} &= (1,k_1)(k_2^{-1}\cdot 1,k_2^{-1})\\ &= (1,k_1)(1,k_2^{-1})\\ &= (1k_1\cdot 1,k_1k_2^{-1})\\ &= (1,k_1k_2^{-1})\in K\end{aligned}$$

从而 $K<G$.

4. 对任意的 $(h,k)\in H\cap K$，因为 $(h,k)\in H$，所以 $h=1$；又因为 $(h,k)\in K$，所以 $k=1$，于是有

$(h,k)=(1,1)=1$，即 $H\cap K=\{1\}$.

5. 为了表达清晰，此处我们用分量形式表达元素. 对任意的 $(h,1)\in H,(1,k)\in K$，有：

$$\begin{aligned} khk^{-1} &:= (1,k)(h,1)(1,k)^{-1} \\ &= (k\cdot h,k)(1,k^{-1}) \\ &= (k\cdot h,1) \\ &:= k\cdot h \end{aligned}$$

问题 5.18 （半直积与直积）：设 H,K 为群，$\varphi:K\to \mathrm{Aut}(H)$ 是群同态，则下列命题等价：

1. $H\rtimes K$ 到 $H\times K$ 的恒等映射是群同态；
2. φ 是平凡的；（即对任意的 $k\in K$，有 $\varphi(k)=1$）
3. $K\lhd H\rtimes K$.

证明

1. $(1)\to(2)$：设

$$\begin{aligned} \psi: H\rtimes K &\to H\times K \\ (h,k) &\mapsto (h,k) \end{aligned}$$

是群同态. 从而对任意的 $h_1,h_2\in H$，$k_1,k_2\in K$，有 $\psi((h_1,k_1)(h_2,k_2))=\psi((h_1,k_1))\psi((h_2,k_2))$.（请注意，等号两侧的元素运算不相同！前者是在半直积内的运算，后者是在直积内的运算.）而

$$\begin{aligned} LHS &= \psi((h_1k_1\cdot h_2,k_1k_2)) \\ &= (h_1k_1\cdot h_2,k_1k_2) \\ RHS &= (h_1h_2,k_1k_2) \end{aligned}$$

对比两个元素的分量，可得 $h_1k_1\cdot h_2=h_1h_2$，即 $k_1\cdot h_2=h_2$，于是 K 对 H 的作用平凡，即 φ 平凡.

2. $(2)\to(3)$：设 φ 是平凡的，则对任意的 $k\in K,h\in H$，有 $k\cdot h=h$.
从而，对任意的 $(1,k_1)\in K,(h,k_2)\in H\rtimes K$，有：

$$\begin{aligned} (h,k_2)(1,k_1)(h,k_2)^{-1} &= (h,k_2)(1,k_1)(k_2^{-1}\cdot h^{-1},k_2^{-1}) \\ &= (hk_2\cdot 1,k_2k_1)(h^{-1},k_2^{-1}) \\ &= (h,k_2k_1)(h^{-1},k_2^{-1}) \\ &= (hk_2k_1\cdot h^{-1},k_2k_1k_2^{-1}) \\ &= (hh^{-1},k_2k_1k_2^{-1}) \\ &= (1,k_2k_1k_2^{-1})\in K \end{aligned}$$

即 $K\lhd H\rtimes K$.

3. $(3)\to(1)$：设 $K\lhd H\rtimes K$，且定义

$$\begin{aligned} \psi: H\rtimes K &\to H\times K \\ (h,k) &\mapsto (h,k) \end{aligned}$$

显然 ψ 是双射，下证：ψ 是同态.
由于 $K\lhd H\rtimes K$，所以对任意的 $(1,k_1)\in K,(h,k_2)\in H\rtimes K$，有

$$\begin{aligned} (h,k_2)(1,k_1)(h,k_2)^{-1} &= (h,k_2)(1,k_1)(k_2^{-1}\cdot h^{-1},k_2^{-1}) \\ &= (h,k_2k_1)(k_2^{-1}\cdot h^{-1},k_2^{-1}) \\ &= (hk_2k_1k_2^{-1}\cdot h^{-1},k_2k_1k_2^{-1})\in K \end{aligned}$$

即 $hk_2k_1k_2^{-1}\cdot h^{-1}=1$，进一步化简得：

$$\begin{aligned}1&=hk_2k_1k_2^{-1}\cdot h^{-1}\\&=h(k_2k_1k_2^{-1}\cdot h)^{-1}\end{aligned}$$

即 $h=k_2k_1k_2^{-1}\cdot h$. 注意到 k_2 是任意的，于是取 $k_2=1$，即有 $h=k_1\cdot h$，从而 K 对 H 的作用是平凡的.

从而，对任意的 $h_1,h_2\in H$，$k_1,k_2\in K$，有

$$\begin{aligned}\psi((h_1,k_1)(h_2,k_2))&=(h_1k_1\cdot h_2,k_1k_2)\\&=(h_1h_2,k_1k_2)\\&=\psi(h_1,k_1)\psi(h_2,k_2)\end{aligned}$$

命题得证.

综上，三个命题是等价的.

问题 5.19 （半直积与积）：设 G 为群，$H\lhd G$，$K<G$，$H\cap K=1$. 定义 K 对 H 的作用为 $k\cdot h=khk^{-1}$，且对应的群同态为 $\varphi:K\to\mathrm{Aut}(H)$，则 $HK\simeq H\rtimes K$.

证明 定义“自然”的映射：

$$\begin{aligned}\psi:HK&\to H\rtimes K\\hk&\mapsto(h,k)\end{aligned}$$

显然 ψ 为满射. 下证：ψ 是群同态，且为单射.

对任意的 $h_1,h_2\in H,k_1,k_2\in K$，有：

$$\begin{aligned}\psi(h_1k_1)\psi(h_2k_2)&=(h_1k_1\cdot h_2,k_1k_2)\\&=(h_1k_1h_2k_1^{-1},k_1k_2)\end{aligned}$$

因为 $H\lhd G$，所以对 $h'\in H$，使得 $k_1h_2=h'k_1$，即 $h'=k_1h_2k_1^{-1}$，于是

$$\begin{aligned}\psi(h_1k_1h_2k_2)&=\psi(h_1h'k_1k_2)\\&=(h_1h',k_1k_2)\\&=(h_1k_1h_2k_1^{-1},k_1k_2)\\&=\psi(h_1k_1)\psi(h_2k_2)\end{aligned}$$

从而 ψ 是群同态.

考虑 ψ 的核：

$$\begin{aligned}\ker\psi&=\{hk\in HK:(h,k)=1\}\\&=\{1\}\end{aligned}$$

从而 ψ 为单射.

综上，$HK\simeq H\rtimes K$.

5.7.3 典型例题

5.7.4 习题

5.7.4.1 半直积的例子 - 利用半直积构造大群

练习 5.99 设 $H=\langle r|\,r^n=1\rangle$，$n$ 为整数，$K=\langle s|\,s^2=1\rangle$，定义 K 对 H 的作用为 $s\cdot r=r^{-1}$. 证明：$H\rtimes K\simeq D_{2n}$.

注 提示：注意到 $r^{-1}=s\cdot r=srs^{-1}$，即 $sr=r^{-1}s$，从而

$$H\rtimes K\simeq\langle r,s|\,r^n=s^2=1,sr=r^{-1}s\rangle\simeq D_{2n}.$$

另外，H 也可取 $\mathbb{Z}$，此时记 $D_\infty=\mathbb{Z}\rtimes\mathbb{Z}_2$.

✍ **练习 5.100** 设 $G = H \rtimes K$，其中 $H = \mathbb{Z}_3 K = \mathbb{Z}_4$，且定义 K 对 H 的作用为 $k \cdot h = h^{-1}$. 证明：G 是 12 阶非交换群，且不同构于 A_4 或 D_{12}.

注 提示：考虑三个群里的 4 阶群的情况，$\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ 中有 4 阶群 $\mathbb{Z}_4$，而 A_4, D_{12} 中只包含同构型为 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 的子群，从而不可能同构.

值得注意的是，12 阶非交换群只有这三种.

5.7.4.2 半直积的应用 - 全形

对任意的群 H，$\mathrm{Aut}(H)$ 对 H 的作用是自然的，由此定义 H 的全形（holomorph）：$\mathrm{Hol}(H) := H \rtimes \mathrm{Aut}(H)$.

✍ **练习 5.101** 证明：$\mathrm{Hol}(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq S_4$.

证明

5.8 常见的小阶群

5.9 群的阿贝尔化

5.10 可解群

5.11 有限生成交换群的结构

5.11.1 知识要点

1. 秩为 r 的自由交换群：$\mathbb{Z}^r := \mathbb{Z} \times \cdots \times \mathbb{Z}$.（$r$ 个同构于 $\mathbb{Z}$ 的群的直积）
2. （有限生成交换群基本定理，不变因子分解）：若 G 是有限生成交换群，则
$$G \simeq \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$$
其中 $r \geqslant 0, n_i \geqslant 2$ 均为整数，且 $n_{i+1} \mid n_i$ $(i \in \{1, \cdots, s-1\})$. 不计直积各分量的顺序时，该表达式唯一.
r 称为 G 的自由秩（或 Betti 数），n_i 称为 G 的不变因子.
当 $r = 0$ 时，称 s 为 G 的秩.
3. （不同素因子的乘积）：若交换群 G 的阶 n 为不同素因子的乘积，则 $G \simeq \mathbb{Z}_n$.
4. （基本因子分解）：若 G 的阶为 $n > 1$，且 n 的素因子分解为
$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$
则
$$G \simeq A_1 \times \cdots \times A_k$$
$$A_i \simeq \mathbb{Z}_{p_i^{\beta_{i,1}}} \times \cdots \times \mathbb{Z}_{p_i^{\beta_{i,t}}}$$
其中 $\beta_{i,1} \geqslant \beta_{i,2} \geqslant \cdots \geqslant \beta_{i,t} \geqslant 1$，且 $\beta_{i,1} + \beta_{i,2} + \cdots + \beta_{i,t} = \alpha_i$. 不计直积各分量的顺序时，该表达式唯一.
$p_i^{\beta_{i,j}}$ 称为 G 的基本因子.
5. （互素因子的乘积）：设 $m, n \in \mathbb{Z}_+$，则 $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$，当且仅当 $\gcd(m, n) = 1$.

5.11.2 典型例题

例题 5.12 试写出阶为 1800 的交换群的所有可能的情况（分别用不变因子与基本因子分解的方式）.

注 分析：毫无疑问，本节的核心内容，就是明确有限交换群的结构. 换句话说，给定一个交换群的阶，我们要能够知道这个群可能有哪几种同构型. 我们将以本题为例，展示如何找到一个一个交换群的不变因子与基本因子.

首先，需要将阶数做素因子展开（相信所有的读者都有能力完成这一步）

$$1800 = 2^3 \times 3^2 \times 5^2.$$

然后，我们先做不变因子分解. 不变因子需要满足的条件是：n_1 是 n_2 的倍数，n_2 是 n_3 的倍数，以此类推，且 $n_1 \cdots n_k = n$. 我们先考虑 n_1，n_1 必须包含 n 的每一个不同的素因子，本例中即为 $2,3,5$，否则，假如 n_1 中不包含 5，那么不管其他的哪个 n_i 包含因子 5，都将破坏前述的倍数关系. 选定 n_1 之后，n_2 又必须包含剩下的素因子中每一个不同的素因子，以此类推，直到安排完所有的素因子.

这样的描述仍显空泛，我们具体来看，对于 $n = 2^3 \times 3^2 \times 5^2$ 来说，n_1 必须包含因子 $2,3,5$，从而 n_1 可能的取值情况有：

$$\begin{aligned}
&2^1 \times 3^1 \times 5^1, \quad 2^2 \times 3^1 \times 5^1\\
&2^3 \times 3^1 \times 5^1, \quad 2^1 \times 3^2 \times 5^1\\
&2^2 \times 3^2 \times 5^1, \quad 2^3 \times 3^2 \times 5^1\\
&2^1 \times 3^1 \times 5^2, \quad 2^2 \times 3^1 \times 5^2\\
&2^3 \times 3^1 \times 5^2, \quad 2^1 \times 3^2 \times 5^2\\
&2^2 \times 3^2 \times 5^2, \quad 2^3 \times 3^2 \times 5^2
\end{aligned}$$

然后我们就需要挨个考虑 n_2 的取值了：

1. $n_1 = 2^1 \times 3^1 \times 5^1$ 时：

素因子/幂次	2	3	5
幂次累计	3	2	2
n_1	1	1	1
n_2	1	1	1
n_3	1	0	0

于是不变因子为 $30, 30, 2$.

2. $n_1 = 2^2 \times 3^1 \times 5^1$ 时：

素因子/幂次	2	3	5
幂次累计	3	2	2
n_1	2	1	1
n_2	1	1	1

于是不变因子为 $60, 30$.

3. $n_1 = 2^3 \times 3^1 \times 5^1$ 时：

素因子/幂次	2	3	5
幂次累计	3	2	2
n_1	3	1	1
n_2	0	1	1

于是不变因子为 $120, 15$.

4. $n_1 = 2^1 \times 3^2 \times 5^1$ 时：

素因子/幂次	2	3	5
幂次累计	3	2	2
n_1	1	2	1
n_2	1	0	1
n_3	1	0	0

于是不变因子为 $90, 10, 2$.

5. $n_1 = 2^2 \times 3^2 \times 5^1$ 时：

素因子/幂次	2	3	5
幂次累计	3	2	2
n_1	2	2	1
n_2	1	0	1

于是不变因子为 $180, 10$.

6. $n_1 = 2^3 \times 3^2 \times 5^1$ 时：

素因子/幂次	2	3	5
幂次累计	3	2	2
n_1	3	2	1
n_2	0	0	1

于是不变因子为 $360, 5$.

7. $n_1 = 2^1 \times 3^1 \times 5^2$ 时：

素因子/幂次	2	3	5
幂次累计	3	2	2
n_1	1	1	2
n_2	1	1	0
n_3	1	0	0

于是不变因子为 $150, 6, 2$.

8. $n_1 = 2^2 \times 3^1 \times 5^2$ 时：

素因子/幂次	2	3	5
幂次累计	3	2	2
n_1	2	1	2
n_2	1	1	0

于是不变因子为 $300, 6$.

9. $n_1 = 2^3 \times 3^1 \times 5^2$ 时：

素因子/幂次	2	3	5
幂次累计	3	2	2
n_1	3	1	2
n_2	0	1	0

于是不变因子为 $600, 3$.

10. $n_1 = 2^1 \times 3^2 \times 5^2$ 时：

素因子/幂次	2	3	5
幂次累计	3	2	2
n_1	1	2	2
n_2	1	0	0
n_3	1	0	0

于是不变因子为 $450, 2, 2$.

11. $n_1 = 2^2 \times 3^2 \times 5^2$ 时：

素因子/幂次	2	3	5
幂次累计	3	2	2
n_1	2	2	2
n_2	1	0	0

于是不变因子为 $900, 2$.

12. $n_1 = 2^3 \times 3^2 \times 5^2$ 时：

素因子/幂次	2	3	5
幂次累计	3	2	2
n_1	3	2	2

于是不变因子为 1800.

综上，1800 阶交换群的不变因子分解的所有情形为：

$$\mathbb{Z}_{30} \times \mathbb{Z}_{30} \times \mathbb{Z}_2$$

$$\mathbb{Z}_{60} \times \mathbb{Z}_{30}$$

$$\mathbb{Z}_{120} \times \mathbb{Z}_{15}$$

$$\mathbb{Z}_{90} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$$

$$\mathbb{Z}_{180} \times \mathbb{Z}_{10}$$

$$\mathbb{Z}_{360} \times \mathbb{Z}_5$$

$$\mathbb{Z}_{150} \times \mathbb{Z}_6 \times \mathbb{Z}_2$$

$$\mathbb{Z}_{300} \times \mathbb{Z}_6$$

$$\mathbb{Z}_{600} \times \mathbb{Z}_3$$

$$\mathbb{Z}_{450} \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\mathbb{Z}_{900} \times \mathbb{Z}_2$$

$$\mathbb{Z}_{1800}$$

最后，我们再考虑基本因子分解的情况. 基本因子的分解是每个素因子分解进行的，我们只需考虑其幂次的所有划分种类即可. 先看素因子 2，一共有 3 个，从而可能的划分为：

$$\mathbb{Z}_{2^3}$$

$$\mathbb{Z}_{2^2} \times \mathbb{Z}_2$$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

对于素因子 3，一共有 2 个，从而可能的划分为：

$$\mathbb{Z}_{3^2}$$

$$\mathbb{Z}_3 \times \mathbb{Z}_3$$

对于素因子 5，一共有 2 个，从而可能的划分为：

$$\mathbb{Z}_{5^2}$$

$$\mathbb{Z}_5 \times \mathbb{Z}_5$$

然后，在每个素因子里选一个可能的构型组合起来，就得到了全部的基本因子分解的结果：

$$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}$$
$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}$$
$$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$$
$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$$
$$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$
$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$
$$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$
$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

解 参见分析.

笔记 注意到，不变因子分解和基本因子分解只是分解形式不同，但得到的群构型应当是一致的. 例如：

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{30} \times \mathbb{Z}_{30} \times \mathbb{Z}_2$$

请读者思考这是为什么？【提示：m, n 互素时，$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$，且任意调换直积的分量顺序得到的群都是同构的.】

练习 5.102 试写出给定阶的交换群的所有可能的情况（分别用不变因子与基本因子分解的方式）.

1. $|G| = 1155$;
2. $|G| = 270$
3. $|G| = 576$;
4. $|G| = 9801$;
5. $|G| = 44100$.