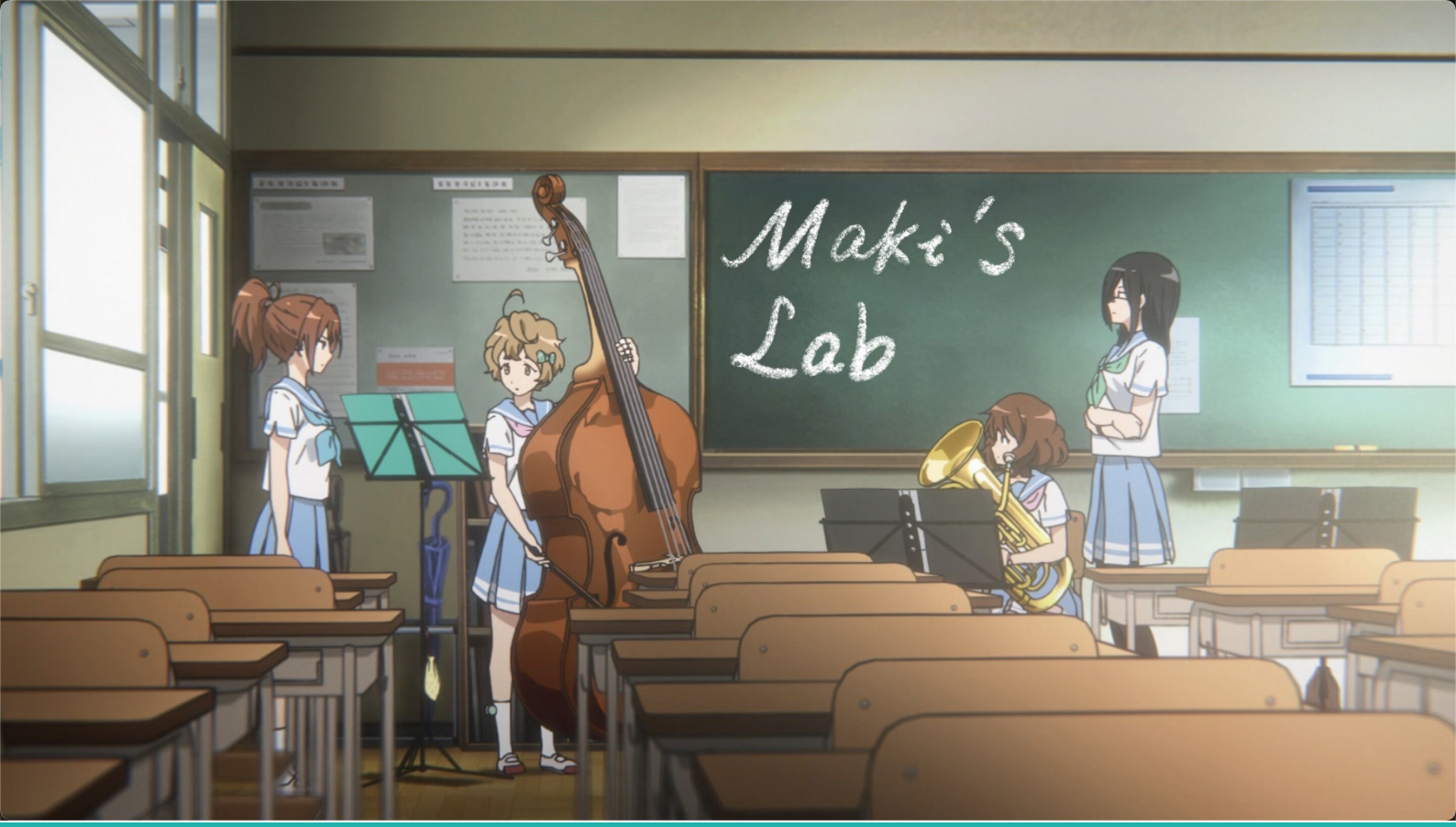
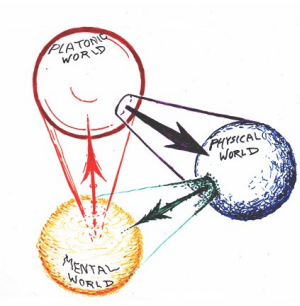


抽象代数/抽象代数 II
MAT2B10/MAT2B20

作者：抽象代数委员会
组织：Maki's Lab
时间：July 9, 2022
版本：1.0



"九万里风鹏正举。风休住，蓬舟吹取三山去。"——【宋】李清照

目录

第一部分

抽象代数 I
基本的代数结构

第 1 章 群论 I——Group Theory I

1.1 幺半群

定义 1.1

我们说 $(S,*)$ 是一个幺半群，当该二元运算满足结合律，且具有单位元。此即，

$$\forall x,y,z\in S, x*(y*z)=(x*y)*z \tag{1.1}$$

$$\exists e\in S, \forall x\in S, e*x=x*e=x \tag{1.2}$$

♣

结合律不难理解，而单位元是什么呢？首先，单位元是一个元素；其次，其左乘或右乘在任何元素上都不会改变其取值。最简单的例子在实数集上，其中 0 是加法单位元，1 是乘法单位元。

例如，$(\mathbb{N},+),(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ 是（加法）幺半群，其中（加法）单位元是 0；$(\mathbb{N},*),(\mathbb{Z},*),(\mathbb{Q},*),(\mathbb{R},*),(\mathbb{C},*)$ 是（乘法）幺半群，（乘法）单位元是 1。

讲到结合律，自然会想到交换律。对于一般的幺半群，我们不要求其运算满足交换律。而满足交换律的幺半群叫做交换幺半群。

定义 1.2

我们说 $(S,*)$ 是一个交换幺半群，当其是一个幺半群，且该运算满足交换律，即

$$\forall x,y\in S, x*y=y*x \tag{1.3}$$

♣

上述例子中所有的幺半群都是交换幺半群。很自然的一个问题是，有没有不交换的幺半群呢？答案是肯定的。假如你熟悉线性代数，你一定知道，$n*n$ 实矩阵对乘法构成结合律，且具有乘法单位元（单位矩阵），但不是交换的，于是所有 $n*n$ 实矩阵对乘法构成非交换的幺半群。

在抽象代数中，我们常常会通过非常少的公理得到很多结论。这里的第一个例子便是，幺半群的单位元是唯一的。为了方便起见，在熟悉定义的情况下，我们经常用 $\cdot$ 来表示乘法。

命题 1.1

若 $(S,\cdot)$ 是一个幺半群，则单位元是唯一的。此即，若 e,e' 都是单位元，则 $e=e'$。

♠

证明 假设 e,e' 都是 $(S,\cdot)$ 的单位元。考虑乘积 $e\cdot e'$，一方面 e 是单位元，所以它等于 e'，但另一方面 e' 也是单位元，因此同理它等于 e，故

$$e=e\cdot e'=e' \tag{1.4}$$

这就证明了幺半群中单位元的唯一性。

在这一节中，如非特别说明，我们假设 $(S,\cdot)$ 是一个幺半群。

假如 $(S,\cdot)$ 满足结合律，我们可以用数学归纳法证明其满足广义结合律。如果 $x_1,\cdots,x_n\in S$，我们想要求按这个顺序下的乘积。我们有不同添加括号的方式来规定乘法的顺序，广义结合律说的是，无论如何加括号，只要元素顺序规定了，这个乘积的值就是不变的。即在元素连续乘积中，无论按什么顺序添加括号，得到的值是一样的。首先，我们给出任意一个方便的（等价）定义，接下来用这个定义证明广义结合律。

定义 1.3

令 $x_1,\cdots,x_n\in S$，我们递归地定义

$$x_1\cdot x_2\cdot\cdots\cdot x_n=(x_1\cdot x_2\cdot\cdots\cdot x_{n-1})\cdot x_n \tag{1.5}$$

令 $x\in S, n\in\mathbb{N}$。若 $n>0$，我们定义 $x^n=x\cdots x$，而 $x^0=e$。

♣

要证明广义结合律，事实上我们只要证明以下的命题。

命题 1.2

令 $x_1,\cdots,x_n,y_1,\cdots,y_m\in S$，则

$$x_1\cdot x_2\cdot\cdots\cdot x_n\cdot y_1\cdot y_2\cdot\cdots\cdot y_m=(x_1\cdot x_2\cdot\cdots\cdot x_n)\cdot(y_1\cdot y_2\cdot\cdots\cdot y_m) \tag{1.6}$$

证明 对 m 做数学归纳。当 $m=1$ 时，由定义直接得到。

接下来，假设

$$x_1\cdot x_2\cdot\cdots\cdot x_n\cdot y_1\cdot y_2\cdot\cdots\cdot y_k=(x_1\cdot x_2\cdot\cdots\cdot x_n)\cdot(y_1\cdot y_2\cdot\cdots\cdot y_k)$$

则我们有

$$x_1\cdot x_2\cdot\cdots\cdot x_n\cdot y_1\cdot y_2\cdot\cdots\cdot y_{k+1} \tag{1.7}$$

Q: 为什么是结合律而不是交换律?

$$=((x_1\cdot x_2\cdot\cdots\cdot x_n)\cdot(y_1\cdot y_2\cdot\cdots\cdot y_k))\cdot y_{k+1} \tag{1.8}$$

$$=(x_1\cdot x_2\cdot\cdots\cdot x_n)\cdot((y_1\cdot y_2\cdot\cdots\cdot y_k)\cdot y_{k+1}) \tag{1.9}$$

$$=(x_1\cdot x_2\cdot\cdots\cdot x_n)\cdot(y_1\cdot y_2\cdot\cdots\cdot y_{k+1}) \tag{1.10}$$

接下来，我们就有了广义结合律，只要 $x_1,\cdots,x_n$ 的顺序是固定的，无论怎么添加括号，我们都可以利用命题 1.2 的结论，将括号重排至从前往后依次乘的顺序而保持结果不变。注意，我们没有用到单位元的条件。因此，只要一个集合上的二元运算满足结合律，就会立刻满足广义结合律。所以，如果一个集合上的二元运算有结合律，我们就可以在连续元素的乘积中不加括号，也可以按照我们的需要随意加括号。

若所有 x_i 和 y_j 都相等，我们就得到以下的推论。

命题 1.3

令 $x\in S,m,n\in\mathbb{N}$，则

$$x^{m+n}=x^m\cdot x^n \tag{1.11}$$

我们很容易发现，比如说，$(\mathbb{N},+)$ 是 $(\mathbb{Z},+)$ 的子集，而且它们都是幺半群。我们称前者是后者的子幺半群。

定义 1.4

令 $(S,\cdot)$ 是一个幺半群，若 $T\subset S$，我们说 $(T,\cdot)$ 是 $(S,\cdot)$ 的一个子幺半群，若 $e\in T$，且 T 在乘法下封闭，即

$$e\in T \tag{1.12}$$

$$\forall x,y\in T,x*y\in T \tag{1.13}$$

这个定义是很有价值的，其价值在于子幺半群必定仍然是个幺半群。

命题 1.4

若 $(T,\cdot)$ 是 $(S,\cdot)$ 的一个子幺半群，则 $(T,\cdot)$ 是个幺半群。

证明 就二元运算的定义而言，子群第一个条件（封闭性）就满足了，这使得我们后面的谈论是有意义的。首先，结合律对于 S 中元素都满足，当然对 T 中元素也满足（T 是子集）。接下来，类似地，e 对于所有 S 中元素都是单位元，固然对于 T 中元素亦是单位元。

抽象代数中，一类重要的数学映射叫做“同态”。同态指的是“保持某些运算”的映射。我们常常会加上前缀，如“群同态”，“环同态”，等等。为了让你更早接触到这一重要概念（或者概念族），我们并不刻意略过，而是刻意将其早点讲解。这里，我们介绍幺半群同态。

定义 1.5

假设 $(S,\cdot)$，$(T,*)$ 是两个幺半群，且 $f:S\to T$ 是一个映射，我们称 f 是一个幺半群同态，当 f 保持了乘法运算，且把单位元映到了单位元。

$$\forall x,y\in S, f(x\cdot y)=f(x)*f(y) \tag{1.14}$$

$$f(e)=e' \tag{1.15}$$

其中，e 和 e' 分别是 $(S,\cdot)$ 和 $(T,*)$ 的单位元。

♣

假设 $(S,\cdot)$ 是一个幺半群，令 $x\in S$。我们定义 $f:(\mathbb{N},+)\to(S,\cdot)$，使 $f(n)=x^n$，则根据广义结合律不难发现，这就是一个最朴素的幺半群同态。因为一方面，根据自然的定义，$f(0)=x^0=e$，把单位元映到单位元。而另一方面，利用广义结合律，$f(m+n)=x^{m+n}=x^m\cdot x^n=f(m)\cdot f(n)$。未来，我们在群论中也会看到类似的群同态，也是通过一个元素“引出”的同态。

从这里，我们有两个延伸。第一个延伸是，什么是“引出”？我们可以从一个元素引出一个同态，实际上，也可以从任何一个元素引出一个原幺半群的子幺半群。另一方面，其实每一个子集都可以引出一个子幺半群。第二个延伸是“同构”。这个词是常见的，即便从未学过的同学也应当至少听说过这个词。如果说同态的含义仅仅是保持运算，那么同构的含义便是完全一致的运算。一个同构首先是一个双射，这意味着你可以在元素之间建立一一对应，即可以给每个元素贴上唯一的标签；在双射的基础上，同构的含义是，换了标签下，运算是不变的——也就是说，这两个结构（比如幺半群）的唯一区别就是“标签不同”。

请读者原谅上一段落可能造成的理解上的困扰。实际上这是为了缓解未来更大的困扰而提前给各位做一些介绍，并且让大家做好心理准备。下面，请听进一步的讲解。

定义 1.6

假设 $(S,\cdot)$ 是一个幺半群，而 $A\subset S$ 是一个子集。我们定义由 A 生成的子幺半群，记作 $\langle A\rangle$，是指 S 中所有包含了 A 的子幺半群的交集。

$$\langle A\rangle=\bigcap\{T\subset S:T\supset A,T\text{ 是子幺半群}\} \tag{1.16}$$

♣

对于第一次看到满足条件的一堆结构的交集的观众而言，这个概念是令人生畏的。看到这样的交集，首先要问自己，我们取交集的集族是否是非空的。答案往往是显然非空的。在这里，我们考虑全集 S，这就是一个包含了 A 的子幺半群，因此这个集族是非空的。接下来要问自己，这些子幺半群交在一起，还是不是子幺半群。初学者一定要注意，这个结论并不是极其显然的。因为当你取了交集以后，交集的性质未必像集族中每个集合的性质那么好。幸运的是，大部分时候下，交集的性质确实这么好。在幺半群的情况下，上面说的便是下面的命题。

命题 1.5

假设 $(S,\cdot)$ 是一个幺半群，而 $A\subset S$ 是一个子集。则 $\langle A\rangle$ 也是一个子幺半群。因此，这是包含了 A 的最小的子幺半群。

♠

注意，这里说的“最小”，指的是在包含关系下最小的，也就是，它包含于所有包含 A 的子幺半群。

证明 要证明 $\langle A\rangle$ 是子幺半群，只需要证明它包含了 e，并在乘法运算下封闭。首先，因为集族中每一个 T，作为子幺半群，都会包含 e；因此 $\langle A\rangle$ 作为这些集合的交集也会包含 e，这就证明了第一点。而对于第二点，我们首先假设 $x,y\in\langle A\rangle$，而想要证明 $x\cdot y\in\langle A\rangle$。注意到，因为 $x,y\in\langle A\rangle$，任取一个包含了 A 的子幺半群 T（集族中的集合），我们都有 $x,y\in T$，于是有 $x\cdot y\in T$。而 $x\cdot y\in T$ 对于所有这样的 T 都成立，我们就有 $x\cdot y$ 属于它们的交集，也就是 $\langle A\rangle$。这样，我们就证明了第二点。综上，由一个幺半群 S 的任意子集 A 生成的子幺半群都确实是一个子幺半群。

未来，我们也会看到由子集生成的子群，子环，等等。定义是完全一样的。一般来说，结构 S 中，由一个子集 A 生成的子结构，就是 S 中所有包含了 A 的子结构的交集。要注意，每一次你想用这样一个概念，都要证明这个交集依然是子结构——正如我们证明包含了 A 的子幺半群的交集还是子幺半群一样。证明也是类似的，逐

条证明即可。只是未来的结构会更复杂，条件更多，要证明的也越多。不过一旦你掌握证明方法的核心，无论结构多么复杂，你都不会乱了分寸。

接下来，我们看幺半群最后一个内容，也就是上面所说的第二个延伸，即同构，具体来说，幺半群同构。同构的含义上文已经解释过了，这里直接给出定义。

定义 1.7

假设 $(S,\cdot)$，$(T,*)$ 是两个幺半群，且 $f:S\to T$ 是一个映射，我们称 f 是一个幺半群同构，当 f 是一个双射，且是一个同态。

$$f \text{ 是双射} \tag{1.17}$$

$$\forall x,y\in S, f(x\cdot y)=f(x)*f(y) \tag{1.18}$$

$$f(e)=e' \tag{1.19}$$

其中，e 和 e' 分别是 $(S,\cdot)$ 和 $(T,*)$ 的单位元。

♣

大家需要注意，同构这个概念和相等、全等、相似等概念一样，是一个等价关系，因此一定满足对称性。而这里我们只要求了 f 是幺半群同态，却不要求 f^{-1} 也是幺半群同态（因为 f 是双射，所以 f^{-1} 一定存在）。这实际上就暗示了下列命题——每个幺半群同构的逆映射还是幺半群同态。因而，每个幺半群同构的逆映射还是幺半群同构。未来我们会看到，同样的命题对于群，环，等等常见的结构都是成立的。正如刚才子集生成的子结构要证明是子结构一样，这里我们为了严格起见，需要证明同构的逆映射依然是同态。

命题 1.6

若 $f:(S,\cdot)\to(T,*)$ 是一个幺半群同构，则 $f^{-1}:T\to S$ 是一个幺半群同态。因此，f^{-1} 也是个幺半群同构。

♠

事实上，这个证明是不难的。而重要的是在于上面段落中提到的数学思想。当我们给出“同构”这个词，就通过“同”暗示了是等价关系，而等价关系需要有对称性。可是定义中没有对称性，这该怎么办呢？通过命题证明对称性。

证明 令 $x',y'\in T$，我们只需证明 $f^{-1}(x'*y')=f^{-1}(x')\cdot f^{-1}(y')$。为了方便起见，根据 f 是一个双射，我们可以令 $x=f^{-1}(x'),y=f^{-1}(y')$。我们只需证明 $f^{-1}(x'*y')=x\cdot y$。而由于 f 是幺半群同态，所以 $f(x\cdot y)=f(x)*f(y)=x'*y'$。反过来说，$f^{-1}(x'*y')=x\cdot y=f^{-1}(x')\cdot f^{-1}(y')$。这就证明了这个命题。

更一般地来说，我们应当定义的同构，其实应该是满足三个条件：双射，原函数是同态，逆函数也是同态。在这里，因为第三个条件往往可以通过前两条推出来，所以我们把他作为结论而不是条件。这也解释了为什么在抽象代数中的同构，我们只会看到前面两条。

事实上，进一步补充来说，例如在拓扑学中，我们用“连续函数”对应“同态”，用“同胚”对应“同构”。在拓扑学中，要定义“同胚”，我们必须定义三条：双射，原函数连续，逆函数连续。这也进一步加深了我们对于同构的理解。

1.2 群

上一节中，我们已经学习了幺半群。在这里，我们首先在幺半群中定义可逆元素及其逆元。

定义 1.8

令 $(S,\cdot)$ 是一个幺半群，$x\in S$。我们称 x 是可逆的，当

$$\exists y\in S, x\cdot y=y\cdot x=e \tag{1.20}$$

其中 y 被称为 x 的逆元，记作 x^{-1}。

♣

首先，根据 e 的定义，e 一定是可逆的，而 e 是它的逆元。这是因为 $e = e \cdot e$。接下来，例如在加法幺半群 $(\mathbb{N}, +)$ 中，若 $x \in \mathbb{N}$，则逆元 y 应当满足 $x + y = 0$（根据交换律我们只需要 $x + y = 0$ 即可），那么 $y = -x$。可是 $\mathbb{N}$ 中只有 0 的相反数在其中，因此这个幺半群中只有 0 有逆元。也正因为这个原因，我们在加法群中，记逆元为 $-x$。

在乘法幺半群 $(\mathbb{Z}, \cdot)$ 中，若 $x \in \mathbb{Z}$，则逆元 y 应当满足 $x \cdot y = 1$（同样利用交换律），所以 $y = x^{-1}$。而 $\mathbb{Z}$ 中，只有 ± 1 的逆元在其中（也是他们自身），其中 1 还是乘法单位元。其他元素在 $\mathbb{Z}$ 中都没有逆元。

接下来，我们要问这样的逆元是否是唯一的（正如当时我们问单位元是否是唯一的）。回答是肯定的。

命题 1.7

令 $(S, \cdot)$ 是一个幺半群。假设 $x \in S$ 是可逆的，则其逆元唯一。也就是说，如果 $y, y' \in S$ 都是它的逆元，则 $y = y'$。

♠

证明 假设 y, y' 都是 x 的逆元。则 $y \cdot x = e$，$x \cdot y' = e$。我们接下来利用一个巧妙的连续“代数变形”来证明 $y = y'$。

$$y = y \cdot e = y \cdot x \cdot y' = e \cdot y' = y' \tag{1.21}$$

其中我们利用了 e 是单位元，以及（广义）结合律（因为我们直接不加括号了）。

我们最喜欢的幺半群是那些所有元素都具有逆元的（不仅是单位元），对于这样的代数结构，我们称为群。这也是著名的代数结构。后面我们会发现，群的性质很好，使其具有价值；但也不是特别好，使其会很普遍（性质特别好的结构不会普遍）。事实上，群在数学中比比皆是，我们在哪里都会看到它的身影，因此对于群的研究并不是空中楼阁，而是有实打实的意义的。下面是定义。

定义 1.9

令 $(G, \cdot)$ 是一个幺半群，我们说它是一个群，当 G 中所有元素都是可逆的。换言之，若 $\cdot$ 是 G 上的一个二元运算，则我们称 $(G, \cdot)$ 是个群，或 G 对 $\cdot$ 构成群，当这个运算满足结合律，存在单位元，且每个元素具有逆元。再进一步展开来说，同样等价地，若 $\cdot$ 是 G 上的一个二元运算，则我们称 $(G, \cdot)$ 是个群，当

$$\forall x, y, z \in G, x \cdot (y \cdot z) = (x \cdot y) \cdot z \tag{1.22}$$

$$\exists e \in G, \forall x \in G, x \cdot e = e \cdot x = x \tag{1.23}$$

$$\forall x \in G, \exists y \in G, x \cdot y = y \cdot x = e \tag{1.24}$$

♣

注意，对于群，我们常用字母 G，以及挨着的 H, K 等，因为群的英文是 group。另外，我们把 x 的逆元记作 x^{-1}。一个自然的推论便是，每个元素的逆元都是唯一的（从幺半群中得到这个结论）。

那么逆元的逆元是否一定是自身呢？答案是肯定的。

命题 1.8

令 $(G, \cdot)$ 是一个群，令 $x \in G$，则 $\left(x^{-1}\right)^{-1} = x$。

♠

证明 方便起见，我们令 $y = x^{-1}$，于是有 $x \cdot y = y \cdot x = e$。我们要证明 $y^{-1} = x$，而这就是 $y \cdot x = x \cdot y = e$，显然成立。这就证明了逆元的逆元是自身，符合了我们的预期。

命题 1.9

令 $(G, \cdot)$ 是一个群，令 $x, y \in G$，则 $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$。

♠

证明 我们利用定义来证明。一方面，利用广义结合律，$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = e$；另一方面，同理可以得到另一边的等式，这就告诉我们 $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$。

我们同样定义交换群，指的是那些运算满足交换律的群。因为历史上阿贝尔对交换群的贡献，交换群更有名的别称是阿贝尔群。

定义 1.10

若 $(G,\cdot)$ 是一个群，我们称它是阿贝尔群，或交换群，当该运算满足交换律，即

$$\forall x,y\in G, x\cdot y=y\cdot x \tag{1.25}$$

♣

接下来，我们要给出几个常见的群的例子。最基础的群是只有一个元素的群，称为平凡群，记作 $\{e\}$，其中的乘法是 $e\cdot e=e$。常见的加法群有 $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ 等。常见的乘法群有 $(\mathbb{Q}^\times,\cdot),(\mathbb{R}^\times,\cdot),(\mathbb{C}^\times,\cdot)$ 等，这里 $\mathbb{Q}^\times=\mathbb{Q}\setminus\{0\}$，类似地定义其余的两个集合。这些群分别叫做整数加群，有理数加群，实数加群，复数加群；有理数乘群，实数乘群，以及复数乘群。

线性代数中，加法群比较简单，事实上所有向量空间都对加法构成群，例如 n 维欧氏空间 $(\mathbb{R}^n,+)$ 对加法构成群，类似地也有 $(\mathbb{C}^n,+)$，甚至还有 $(\mathbb{Q}^n,+)$ 和 $(\mathbb{Z}^n,+)$。对于这些常见向量构成的空间，单位元是零向量，加法逆元则是对每个坐标取相反数，如 $(x_1,\cdots,x_n)$ 的加法逆元是 $(-x_1,\cdots,-x_n)$。未来我们会看到，这样的例子可以推广到群的直积。

不止这些常见向量，实际上所有 $m*n$ 矩阵也对加法构成群，单位元是零矩阵（每个项都是 0），加法逆元则是对每一项取相反数。对于 $n*n$ 的实矩阵加法群，我们记作 $(M(n,\mathbb{R}),+)$，类似地你也可以定义复矩阵加法群等。

对于矩阵乘法群，则会复杂一些。事实上，我们需要一个引理。这个引理构建了幺半群与群的一个联系。

引理 1.1

令 $(S,\cdot)$ 是一个幺半群，令 G 是其所有可逆元素构成的子集。则 $(G,\cdot)$ 是个群。

♡

我们称呼幺半群中的可逆元素为“单位”，因此 G 是由所有该运算下的单位构成的集合（在这里甚至是群）。

证明 首先结合律完全继承自 S，不需要证明。而单位元是可逆的，因此 $e\in G$。剩下要证明 G 中每个元素都有（G 中的）逆元，而这几乎是显然的。假设 $x\in G$，则 x 是可逆元素，我们取 $y\in S$，使得 $x\cdot y=y\cdot x=e$(这里要注意我们只能首先保证 y 在全集 S 中)。接下来我们要证明 $y\in G$，即 y 可逆，而这是显然的，因为 x 正是它的逆。所以 $y\in G$。这样，就证明了 $(G,\cdot)$ 是个群。

例如，在上面的例子中，$(\mathbb{Z},\cdot)$ 所有可逆元素构成的群就是 $(\pm1,\cdot)$，非常简单，但也很重要。

定义 1.11

我们对于那些 $n*n$ 可逆实矩阵构成的乘法群，称为（实数上的）n 阶一般线性群，记作 $(GL(n,\mathbb{R}),\cdot)$。由于一个矩阵可逆当且仅当其行列式不为零，因此

$$GL(n,\mathbb{R})=\{A\in M(n,\mathbb{R}):\det(A)\neq0\} \tag{1.26}$$

♣

注意，这的确是个群，因为本身 $n*n$ 实矩阵对乘法构成幺半群（单位元是单位矩阵），接下来我们取所有可逆元素，就得到了一般线性群。当然，我们也有复数上的，有理数上的，等更多的一般线性群。

提到了一般线性群很难不去提特殊线性群。

定义 1.12

(实数上的)n 阶特殊线性群是由那些行列式恰好是 1 的 $n*n$ 实矩阵构成的乘法群，记作 $(SL(n,\mathbb{R}),\cdot)$，即

$$SL(n,\mathbb{R})=\{A\in M(n,\mathbb{R}):\det(A)=1\} \tag{1.27}$$

♣

注意，这个定义是尚且不良好的，因为我们并没有证明特殊线性群是个群。实际上，它是个子群。我们为什么不给出子群的条件呢？正如我们给出子幺半群的条件那样。

定义 1.13

令 $(G,\cdot)$ 是一个群，且 $H\subset G$。我们称 H 是 G 的子群，记作 $H<G$，当其包含了单位元，在乘法和逆运

算下都封闭，即

$$e \in H \tag{1.28}$$

$$\forall x, y \in H, x \cdot y \in H \tag{1.29}$$

$$\forall x \in H, x^{-1} \in H \tag{1.30}$$

♣

类似地，我们定义子群的根本目的是证明其是个群。因此我们效仿幺半群的做法，证明子群是个群。

命题 1.10

令 $(G, \cdot)$ 是一个群。若 H 是 G 的子群，则 $(H, \cdot)$ 也是个群。

♠

证明 就二元运算的良定义性而言，子群第一个条件（封闭性）就满足了，这使得我们后面的谈论是有意义的。首先，结合律肯定满足，因为它是个子集。其次，根据子群的第二个条件，$e \in H$ 是显然的。再次，我们要证明每个 H 中元素有 H 中的逆元，而这是子群的第三个条件。

命题 1.11

有时为了方便起见，我们把子群的后两个条件合并，缩成两个条件，即

$$e \in H \tag{1.31}$$

$$\forall x, y \in H, x \cdot y^{-1} \in H \tag{1.32}$$

$$\tag{1.33}$$

这条命题说的便是，这是子群的等价条件。

♠

证明 假设原来的子群条件。令 $x, y \in H$，利用逆元封闭性得到 $y^{-1} \in H$，再利用乘法封闭性得到 $x \cdot y^{-1} \in H$。

反过来，假设这里的条件。令 $x \in H$，则 $e \cdot x^{-1} = x^{-1} \in H$，这证明了逆元封闭性。

接下来，令 $x, y \in H$，则利用逆元封闭性，$y^{-1} \in H$，故 $x \cdot (y^{-1})^{-1} = x \cdot \in H$。这就证明了乘法封闭性。综上，这的确是子群的等价条件。

命题 1.12

$(SL(n, \mathbb{R}), \cdot)$ 是个群。

♠

证明 根据定义，$SL(n, \mathbb{R})$ 首先是 $GL(n, \mathbb{R})$ 的子集，那么只要证明它是个子群即可。首先，乘法单位元单位矩阵的行列式恰好是 1（这也是为什么我们定义特殊线性群是行列式是 1 的矩阵构成的群），这就证明了 $I \in SL(n, \mathbb{R})$（I=I_n 指的是 n 阶单位矩阵）。另外，我们要证明 $SL(n, \mathbb{R})$ 在乘法下封闭。令 A, B 是两个行列式为 1 的 $n * n$ 实矩阵。由于行列式满足 $\det(AB) = \det(A)\det(B)$，因此 AB 的行列式也是 1，也就在特殊线性群中。这就证明了特殊线性群确实是个群。至于逆元封闭性，我们利用 $\det(A^{-1}) = \frac{1}{\det(A)}$。假设 $\det(A) = 1$，则 $\det(A^{-1}) = 1$，于是 $A^{-1} \in SL(n, \mathbb{R})$。综上，特殊线性群确实是个群。

通过这个例子，我们其实第一次学习了如何利用子群条件来证明群的条件。未来，我们会常常看到这样的证明。等到未来这样的证明出现太多次以后，我们甚至会直接用“显然”来略过这样的一段证明。大家不必感到恐惧，因为当你理解了证明思路的核心，就算你只能看到“显然”两个字，也能很快想到证明证明方法。反过来，这也需要你在每次学习新知识的时候更脚踏实地。

这里要格外注意，行列式的这个性质，其实就是群同态性质。很妙的是，群同态的定义和幺半群同态非常相似。

定义 1.14

令 $(G,\cdot),(G',*)$ 是两个群，且 $f:G\to G'$ 是一个映射。我们称 f 是一个群同态，当其保持了乘法运算，即

$$\forall x,y\in G, f(x\cdot y)=f(x)*f(y) \tag{1.34}$$

命题 1.13

若 $f:(G,\cdot)\to(G',*)$ 是一个群同态，则 $f(e)=e'$，$f(x^{-1})=f(x)^{-1}$。

也就是，f 不仅把乘积映到乘积，而且把单位元映到单位元，把逆元映到逆元。在这个意义下，实际上 f 将所有群 G 的“信息”都保持到了 G' 上，包括单位元，乘法和逆元。至于结合律（或者更基础的封闭性），显然两边本来就有，就不必再提。

证明 首先，因为 $e\cdot e=e$，所以利用同态的性质，$f(e)=f(e\cdot e)=f(e)*f(e)$。这时，两边同时左乘 $f(e)^{-1}$，就可以各约掉一个 $f(e)$，得到 $e'=f(e)$，这就证明了 f 把单位元映到单位元。

另一方面，令 $x\in G$，则 $e'=f(e)=f(x\cdot x^{-1})=f(x)*f(x^{-1})$。同理 $e'=f(x^{-1})*f(x)$。于是由定义，$f(x^{-1})$ 就是 $f(x)$ 的逆元，即 $f(x^{-1})=f(x)^{-1}$。这就证明了这个命题。

这里，要注意幺半群同态有额外的把单位元映到单位元这个条件。那为什么群同态不需要这个条件呢？因为只是保持乘法就可以得到条件。仔细看上面的证明，我们会发现取 $f(x)$ 的逆元是必要的一步，而这在幺半群中是行不通的。这就是为什么在幺半群的同态中，我们要有两个条件。

这样，我们又进一步理解了一般的结构的同态应该满足什么条件。一个一般结构的同态应该把所有运算都保持，把所有“特殊元素”都映射到对应的“特殊元素”上，例如这里的乘法单位元。未来我们会学习更多的同态，而最终每个同态都会有这些性质。微妙的地方便在于，有时条件很多，有时条件很少，这是因为这个结构本身的性质“好坏”决定的。因此我们不严谨地说，从同态的角度而言，群的性质比幺半群的性质要更“好”。同时，这也从一个侧面说明了，为什么很多书上，都会略提幺半群，甚至不提。我们在这里提，是为了对幺半群及衍生的刻画，为后面的复杂结构做铺垫，且让大家做好心理准备（之前也提过了）。

接下来，我们再回到特殊线性群这个重要的例子。我们注意到，在证明它是子群的时候，我们严格依赖了行列式函数的同态性质。而 1 又是乘法的单位元，这提醒我们行列式其实是从一般线性群到实数乘群的（乘法）群同态。

命题 1.14

$\det:GL(n,\mathbb{R})\to(\mathbb{R}^\times,\cdot)$ 是一个乘法群同态。

这是线性代数的重要结论，在这里，我们不给出任何证明。那么特殊线性群是什么呢？它恰好就是由那些映到单位元的元素（矩阵）构成的集合（子群）。那么一般来说，是不是群同态中映到单位元的元素构成的集合是子群呢？回答是肯定的。而且未来我们会知道，这样的集合不仅是子群，而且是正规子群，而这 a 就是后话了。与之类似地，群同态的像，是陪域的子群。对于这两个重要的子群，我们起了名字。我们未来会常常看到这样的子群，甚至刻意构造群同态，使得某个群成为这两个子群之一。下面我们介绍这两个子群。

定义 1.15

令 $f:(G,\cdot)\to(G',*)$ 是一个群同态。则我们定义 f 的核与像，记作 $\ker(f)$ 与 $\mathrm{im}(f)$，分别为

$$\ker(f)=\{x\in G:f(x)=e'\}\subset G \tag{1.35}$$

$$\mathrm{im}(f)=\{y\in G':\exists x\in G, y=f(x)\}=\{f(x):x\in G\}]\subset G' \tag{1.36}$$

在这里，我们要注意核是在定义域中的，而像是在陪域中的。实际上，像就是值域，我们换了个名字而已。正如刚才说的，我们有两个重要性质。

命题 1.15

令 $f:(G,\cdot)\to(G',*)$ 是一个群同态，则核是定义域的子群，像是陪域的子群，即

$$\ker(f)<G \tag{1.37}$$

$$\mathrm{im}(f)<G' \tag{1.38}$$

♠

未来我们会有更重要的结论，即每一个同态都隐含着一个同构，这被称为群同构第一定理，而为了到达那里，我们还有一段路要走。

证明 在这个证明中，我们都会有更简单的那个证明方法（两个条件的版本）。从这里开始，我们也可以在上下文语境清晰的情况下，在乘群中省略所有的乘法。

先证明第一个子群关系。我们利用 $f(e)=e'$ 来说明 $e\in\ker(f)$。接着，假设 $x,y\in\ker(f)$，只需证明 $xy^{-1}\in\ker(f)$。利用同态的性质，$f(xy^{-1})=f(x)f(y)^{-1}=e'e'^{-1}=e'$，这就证明了 $xy^{-1}\in\ker(f)$。第一个子群关系得证。

再证明第二个子群关系。同样由于 $f(e)=e'$，我们有 $e'\in\mathrm{im}(f)$。接着，假设 $y=f(x),y'=f(x')\in\mathrm{im}(f)$，只需证明 $yy'^{-1}\in\mathrm{im}(f)$。同样利用同态的性质，$yy'^{-1}=f(x)f(x')^{-1}=f(xx'^{-1})\in\mathrm{im}(f)f$。第二个子群关系也得证。这样我们就证完了整个命题。

这个命题的直接推论便是 $(SL(n,\mathbb{R}),\cdot)<(GL(n,\mathbb{R}),\cdot)$。可惜我们在这个例子中不能得到非平凡的像的子群结论，因为上述的行列式函数是一个满射。正因为满射的同态和单射的同态都很常见且重要，因此我们给他们分别起了名字，叫做满同态和单同态。

定义 1.16

令 $f:(G,\cdot)\to(G',*)$ 是一个群同态。我们称 f 是一个满同态当 f 是满的，称 f 是一个单同态当 f 是单的。

♣

在这里，我们非常合适地插入单同态的极简单的充要条件。

命题 1.16

令 $f:(G,\cdot)\to(G',*)$ 是一个群同态，则 f 是一个单同态当且仅当 $\ker(f)=\{e\}$。也就是说，一个群同态是单的当且仅当是核是平凡的。

♠

证明 假设 f 是单的，那么因为 $f(e)=e'$，因此若 $f(x)=e'$，则利用单射的性质我们一定有 $x=e$，这就证明了核是平凡的。（这个方向是显然的）

另一个方向不那么显然。我们假设 $\ker(f)=\{e'\}$。假设 $x,x'\in G$，使得 $f(x)=f(x')$，我们只须证明 $x=x'$。在这里，我们同时右乘 $f(x')^{-1}$，得到 $f(x)f(x'^{-1})=f(xx'^{-1})=e'$。而因为核是平凡的，所以必须有 $xx'^{-1}=e$。接下来同时右乘 x'，我们就得到 $x=x'$。这就证明了这个命题。

注意，在这个证明的后半段，我们把简单的两个值相等的条件，借助群的性质（如逆元）转化到核的条件上，进而大规模化简命题（要知道，找到核还是相对容易的）。未来，我们会多次使用这个结论，请大家务必尽早记在心里。同样，这个命题也应该依赖了群的性质（如逆元）。不难想象，这个命题在幺半群中是未必成立的。

讲了群同态，那么当然要提群同构。这个定义和当时的幺半群同构是类似的。

定义 1.17

令 $f:(G,\cdot)\to(G',*)$ 是一个映射，我们称 f 是一个群同构，当 f 既是一个双射，又是一个群同态。简单来说，同构就是双射的同态。

♣

类似地，我们也可以证明若 f 是群同构，则 f^{-1} 是群同态，故也是群同构。

命题 1.17

若 $f:(G,\cdot)\to(G,*)$ 是一个群同构，则 f^{-1} 也是群同构。

证明 因为 f^{-1} 也是双射，所以我们只须证明 f^{-1} 是群同态。令 $x',y'\in G'$，假设 $x'=f(x),y'=f(y)$。则 $x'*y'=f(x\cdot y)$，故 $f^{-1}(x'*y')=x\cdot y=f^{-1}(x)\cdot f^{-1}(y)$。这就完成了证明。

我们短暂地回到刚才，提到 $(\mathbb{R}^n,+),(\mathbb{C}^n,+)$ 是群的时候。我们刚才说了，这样的群其实是用群的笛卡尔乘积作成的，称为群的直积。那么是否对于任意的一族群，我们都可以在它们的笛卡尔乘积上赋予群的结构呢？这个问题非常自然，也就是说结构是否可以拓展到笛卡尔乘积上。回答是肯定的。我们先看一个简单的例子。

定义 1.18

令 $(G,\cdot_1),(G',\cdot_2)$ 是两个群，我们构造它们的直积，不妨记 $(G\times G',*)$。对于 $(x,y),(x',y')\in G\times G'$，我们定义逐坐标的乘积，为

$$(x,y)*(x',y')=(x\cdot_1 x',y\cdot_2 y') \tag{1.39}$$

命题 1.18

若 $(G,\cdot_1),(G',\cdot_2)$ 是两个群，则它们的直积 $(G\times G',*)$ 还是一个群。

证明 封闭性：因为 G 在 $\cdot_1$ 下封闭，G' 在 $\cdot_2$ 下封闭，而 $G\times G'$ 的元素乘积是逐坐标定义的，则 $G\times G'$ 在 $*=(\cdot_1,\cdot_2)$ 下也是封闭的。

结合律：同样，逐坐标有结合律，故整体也有结合律。

单位元：不难想象，(e,e') 是直积的单位元。对于任意 $(x,y)\in G\times G'$，我们有 $(x,y)*(e,e')=(x\cdot_1 e,y\cdot_2 e')=(x,y)$，另一边也是同理，这就证明了 (e,e') 是直积的单位元。

逆元：同样不难想象，对于任意 $(x,y)\in G\times G'$，(x^{-1},y^{-1}) 是 (x,y) 的逆元。证明是类似的，这里省略。

既然有了两个群的直积，我们就可以类似地定义有限多个群的直积，同样通过逐坐标的乘法。甚至进一步，我们可以对于任意一族群，定义它们的直积。未来我们也会看到其他结构的直积。

定义 1.19

令 $(G_i,\cdot_i)_{i\in I}$ 是一族群，其中 I 是一个指标集。我们定义它们的直积为 $(\prod_{i\in I}G_i,*)$，同样通过逐点的乘积。对于 $(x_i)_{i\in I},(y_i)_{i\in I}\in\prod_{i\in I}G_i$，我们定义

$$(x_i)_{i\in I}*(y_i)_{i\in I}=(x_i\cdot_i y_i)_{i\in I} \tag{1.40}$$

类似地，我们有

命题 1.19

若 $(G_i,\cdot_i)_{i\in I}$ 是一族群，则它们的直积 $(\prod_{i\in I}G_i,*)$ 还是一个群。

证明 证明是完全同理的，故我们只列出一些重点。封闭性与结合律是显然的。单位元是 $(e_i)_{i\in I}$，而 $(x_i)_{i\in I}$ 的逆元是 $(x_i^{-1})_{i\in I}$。

最经典的例子就是通过 n 个实数加群 $(\mathbb{R},+)$ 得到的 $(\mathbb{R}^n,+)$。我们正是通过逐点的加法来定义向量的加法的，而这样的向量加法也被记作加法。未来，在不容易造成歧义的情况下，我们也会省略这些乘法（加法）的区别，统称为乘法（或加法）。

我们有了笛卡尔乘积，就一定有投影到各个坐标的映射。要提醒大家的是，这个定义在任意笛卡尔乘积中都存在。

在这里，若 $(G_i,\cdot_i)_{i\in I}$ 是一族群，$j\in I$ 是任意指标，我们定义映射到指标 j 的投影映射为

$$p_j:\prod_{i\in I}G_i\to G_j \tag{1.41}$$

对于 $(x_i)_{i\in I}$，我们定义其投影

$$p_j((x_i)_{i\in I}) = x_j \tag{1.42}$$

为了结论的一般性，我们会一直用任意笛卡尔乘积来展开后面的讨论。当然，对于任意笛卡尔乘积（直积）的结论都会适用于有限笛卡尔乘积（直积）上。目前，我们要说的只有这个事实：从直积到任意一个坐标的投影映射都是一个群同态。未来，我们会有别的结论。

命题 1.20

若 $(G_i,\cdot_i)_{i\in I}$ 是一族群，$j\in I$ 是任意指标，则投影映射 $p_j:\prod_{i\in I}G_i\to G_j$ 是个群同态。

♠

证明是极其简单的，但这不会改变这个结论的重要性。从某种程度上说，这提醒我们不能看轻任何一个概念。“直积，这个简单，每个坐标相乘就好了。”但凡抱有这样轻率的想法，就不容易想到投影映射是群同态。因此，对于看似简单的数学概念抱有一定的敬畏之心，能让我们更脚踏实地地学习。

证明 令 $(x_i)_{i\in I},(y_i)_{i\in I}\in\prod_{i\in I}G_i$，则

$$p_j((x_i)_{i\in I}) = x_j,\quad p_j((y_i)_{i\in I}) = y_j \tag{1.43}$$

$$p_j((x_i)_{i\in I} * (y_i)_{i\in I}) = p_j((x_i\cdot_i y_i)_{i\in I}) = x_j\cdot_j y_j = p_j((x_i)_{i\in I})\cdot_j p_j((y_i)_{i\in I}) \tag{1.44}$$

1.3 有限群

这一节的标题是有限群，我们当然会说很多与“有限”有关的话题，但我们的讨论绝不是停留于有限群的。正如我们借助特殊线性群引出了同态和子群，我们会借助有限群引出一系列有趣而实用的概念与结论。

什么是有限群呢？顾名思义，有限群就是有限的群。

定义 1.20

令 $(G,\cdot)$ 是一个群。我们称 G 是一个有限群，若 G 是有限的。

♣

第一个概念是元素的阶，这与循环群密切相关，我们会慢慢引出循环群的概念。

定义 1.21

若 $x\in G$，则 x（在 G 中）的阶，记作 $|x|$，定义为那个最小的正整数 $n\in\mathbb{N}_1$，使得 $x^n=e$。若这样的 n 不存在，则记 $|x|=\infty$。

♣

命题 1.21

若 $(G,\cdot)$ 是有限群，且 $x\in G$，则 $|x|<\infty$。换言之，有限群的每一个元素通过自乘有限多次，都可以得到单位元。

♠

证明 我们用反证法，假设 $|x|=\infty$，那么根据定义，对于任意的 $n\in\mathbb{N}_1$，我们都有 $x^n\neq e$。我们要说明的是，这会导致一个事实，就是所有的 $x^n(n\in\mathbb{N}_1)$ 都是不同的。在这里，我们不借助同态，直接利用定义来证明这个事实。假设但凡有一对 $n\neq m\in\mathbb{N}_1$ 使得 $x^n=x^m$，不失一般性我们假设 $n>m$。则通过反复的消元，我们可以得到 $x^{n-m}=e$，其中 $n-m\in\mathbb{N}_1$，而这与假设是矛盾的，因为我们假设 x 的阶是无穷的。因此，这个事实是对的——所有的 $x^n(n\in\mathbb{N}_1)$ 都是不同的。那么很遗憾，这是个有限群，你怎么可以有无穷多个不相等的元素呢？这就证明了这个命题。

这个结论实际上非常美妙，让我给大家分析一下。比如在复数上，自乘有限多次能得到乘法单位元 1 的叫做单位根，这样的数是非常少的（复数乘群是无限群，不矛盾），而在实数加群上，只有加法单位元 0，可以做到自加有限多次得到 0（实数加群也是无限群，不矛盾）。可是对于有限群，我们居然有这样的结论——每一个元素有限多次自乘后都会回到单位元。这正是因为群的性质很“好”，我们才能有这样的结论。以上这一段是一

段数学欣赏，我们学数学并不只是枯燥乏味的，而应当品味其中的奥妙和乐趣，这样才是寓教于乐。

刚才的证明中我们提到了同态。也就是说通过同态也可以证明这个结论。事实上，对于代数性质敏感的同学已经注意到了，我们仿佛有一个很自然的同态尚未提及。我们放在这里说，正是为了自然地引出。与幺半群中的结论相类似（幺半群中用的是非负整数的幺半群），我们有以下群论的命题（用整数加群）。

命题 1.22

令 $(G,\cdot)$ 是一个群，任取 $x\in G$。则 $f:(\mathbb{Z},+)\to(G,\cdot)$，定义为 $f(n)=x^n$，是一个群同态。

事实上，我们还未定义过 x 的非正幂次，因此这个命题尚且是不良好定义的。在这里，我们立刻补上定义。

定义 1.22

令 $(G,\cdot)$ 是一个群，且 $x\in G$。若 $n\in\mathbb{N}_1$，我们定义 $x^{-n}=\left(x^{-1}\right)^n$，另外定义 $x^0=e$。

现在，我们给出上述命题的证明。

证明 取定 $x\in G$。令 $m,n\in\mathbb{Z}$，我们只须证明 $f(m+n)=f(m)\cdot f(n)$，也即 $x^{m+n}=x^m\cdot x^n$。

首先注意到，如果 $m,n\in\mathbb{N}_1$，则从广义结合律中就立刻得到这个性质。若 m 或 n 是 0，利用单位元的性质也是显然的。故我们可以不失一般性，假设 $m<0$，记 $m'=-m$，则 $x^m=x^{-m'}=\left(x^{-1}\right)^{m'}$。

若 $n<0$，记 $n'=-n$，则同理，$x^n=\left(x^{-1}\right)^{n'}$，故 $x^{m+n}=\left(x^{-1}\right)^{m'+n'}$，这里 $m',n'\in\mathbb{N}_1$，于是就得证了。

若 $0<n<m'$，则 $x^{m+n}=x^{-(m'-n)}=\left(x^{-1}\right)^{m'-n}$。而 $x^m\cdot x^n=\left(x^{-1}\right)^{m'}\left(x^{-1}\right)^{-n}$。这里一正一负，利用刚才证过的，也得证了。

若 $n\geqslant m'$，用 x^n 去约掉一些 $\left(x^{-1}\right)$，具体的证明过程与前一种情况非常类似，故这里略去证明，留给读者练习。

注意，这里的证明其实并不有趣，也有些许复杂，而事实上我们没有更好的方法可以简化证明。就算通过一些引理，还是不可避免要进行各种分类讨论。我们一定要记住，这样的“复杂”在数学中有时也是必须的，正是通过一些不可避免的步骤，我们可以得到一些好用的结论。如果读者愿意，也可以证明下面的命题（我们留作习题）。

命题 1.23

令 $(G,\cdot)$ 是一个群，且 $x\in G$。令 $m,n\in\mathbb{Z}$，则 $x^{mn}=(x^m)^n$。

证明 证明留作练习。方法不唯一。

接下来，利用同态的性质，我们有的直接推论就是，刚才提到的同态的像，也就是

$$\{x^n:n\in\mathbb{Z}\}\tag{1.45}$$

是一个子群，被称为由 x 生成的群。

定义 1.23

令 $(G,\cdot)$ 是一个群，且 $x\in G$，则 $\langle x\rangle$，被称为由 x 生成的群，定义为

$$\langle x\rangle=\{x^n:n\in\mathbb{Z}\}\tag{1.46}$$

还记得我们在幺半群一节中提到了可以用幺半群的任何一个子集生成一个子幺半群吗？我们当时特别提到，每当你要说明由子集生成的子结构，一定要证明那个集族的交仍然是一个子结构。在这里，我们也给出定义。

定义 1.24

令 $(G,\cdot)$ 是一个群，且 $S\subset G$。则由 S 生成的群，记作 $\langle S\rangle$，定义为

$$\langle S\rangle=\bigcap\{H\subset G:H\supset S,H<G\}\tag{1.47}$$

当然，我们要检验上面的 $\langle S\rangle$ 确实是个群。

命题 1.24

令 $(G,\cdot)$ 是一个群，且 $S\subset G$，则 $\langle S\rangle < G$。

证明 在这里，我们只要证明其包含单位元，在乘法和逆元下封闭。

根据定义，$\langle S\rangle$ 是由所有包含了 S 的 G 中子群全部取交集得到的。

单位元：每个这样的子群 H 都包含单位元，故它们的交集也包含单位元。

乘法封闭性：假设 $x,y\in\langle S\rangle$，任取一个包含了 S 的子群 H，则 $x,y\in H$。因为 H 是子群，故 $xy\in H$，所以 $xy\in\langle S\rangle$。

逆元封闭性：与上面这一条非常类似，略证就是 $\langle S\rangle$ 中所有逆元都在每一个这样的 H 中，故在他们的交集 $\langle S\rangle$ 中。

因此，G 中由 S 生成的子群，确实是包含了 S 的最小子群。

有的群是由一个元素生成的，这样的群就叫做循环群。

定义 1.25

令 $(G,\cdot)$ 是一个群。若存在 $x\in G$，使得 $G=\langle x\rangle$，则 G 被称为一个循环群，而 x 被称为 G 的一个生成元。

我们要证明这两个概念是吻合的，也即

命题 1.25

令 $(G,\cdot)$ 是一个群，则 $\langle x\rangle=\langle\{x\}\rangle$。

证明 根据定义和性质，$\langle\{x\}\rangle$ 是包含了 $\{x\}$ 的最小的子群。因此要证明这个最小的子群就是 $\langle x\rangle$，我们只须证明两点。一，$\langle x\rangle$ 是个子群；二，如果一个子群 H 包含了 $\{x\}$，那么它一定要包含整个 $\langle x\rangle$。

首先，刚才我们已经利用同态的性质，证明了 $\langle x\rangle$ 是个子群。这就证明了第一点。

第二点几乎也是显然的。我们假设 H 是个子群，且 $x\in H$。那么根据子群包含单位元，且有乘法和逆元的封闭性，我们有 $e\in H$，并且递归地，对于 $n\in\mathbb{N}_1$，$x^n=x\cdots x\in H$，$x^{-n}=x^{-1}\cdots x^{-1}\in H$。这就证明了 $H\supset\langle x\rangle$。

好了，上面这个命题美妙地证明了这个由 x 生成的群，确实就是由子集 $\{x\}$ 生成的子群。未来我们也会看到很多类似的命题。我们一定要注意，不要被一些定义所误导了，例如这里 $\langle x\rangle$ 的定义本身，实际上不能说明这就是由子集 $\{x\}$ 生成的子群，所以我们是需要用命题来证明的，这并不是完全平凡的结论（虽然证明不难）。

我们接下来看看有限循环群，毕竟这一节叫有限群。当然，有限循环群就是有限的循环群，这里不赘述了。

命题 1.26

令 $G=\langle x\rangle$ 是有限循环群，假设 $|x|=n$，则 $G=\{e,x,x^2,\cdots,x^{n-1}\}$，其中枚举法中的这些元素是两两不同的。我们称这样的有限循环群的阶是 n。

这是什么意思呢？就是说，每个有限循环群，都可以用从 0 开始的前 n 项幂来准确的描述，其中 $n=|x|$。

证明 我们来证明两件事。第一，每一个 G 中元素都可以写成从 0 开始的前 n 项幂的形式；第二，从 0 开始的前 n 项幂是两两不同的。

我们来证明第一点。任取 G 中元素 x^m，其中 $m\in\mathbb{Z}$。根据带余除法，我们有 $m=qn+r$，其中 $q\in\mathbb{Z}$，$0\leqslant r\leqslant n-1$。那么因为 $x^n=e$，所以 $x^m=x^{qn+r}=(x^q)^n\cdot x^r=x^r$，而这就属于从 0 开始的前 n 项幂。

我们来证明第二点。用反证法，假设 $0\leqslant m'<m\leqslant n-1$，使得 $x^m=x^{m'}$，则 $x^{m-m'}=e$。其中 $1\leqslant m-m'\leqslant n-1<n$，可是 $n=|x|$ 是最小的正整数 k 使 $x^k=e$，这就导致了矛盾。

综上所述，$G=\{e,x,x^2,\cdots,x^{n-1}\}$，其中枚举法中的这些元素是两两不同的。

有限循环群的结构是非常简单的，我们有下列命题。

命题 1.27

对于任意的 $n\in\mathbb{N}_1$，所有 n 阶的循环群都是互相同构的。

证明 假设 $G=\langle x\rangle, G'=\langle y\rangle$ 都是 n 阶循环群。令 $f: G\to G'$，对于 $0\leqslant m\leqslant n-1$，定义为

$$f(x^m)=y^m \tag{1.48}$$

这显然是个同态。

此外，它是个双射，因为我们可以明确地找到其逆映射

$$f^{-1}(y^m)=x^m \tag{1.49}$$

这样，f 既是双射，也是同态，这就证明了 f 是个同构。

下面，我们来看无限循环群。很显然，$(\mathbb{Z},+)$ 就是一个无限循环群，生成元是 1 或者 -1（这两个元素都能生成整数加群）。我们实际上可以证明，每一个无限的循环群，都只有两个对应的生成元。

命题 1.28

令 $G=\langle x\rangle$ 是无限循环群，则 $x^n(n\in\mathbb{Z})$ 是两两不同的，且 G 只有两个生成元，分别是 x 与 x^{-1}。

证明 首先证明 $x^n(n\in\mathbb{Z})$ 是两两不同的。假设有两个相同，不失一般性假设 $m>n\in Z, x^m=x^n$，则 $x^{m-n}=e$，故 x 是有有限阶的。这就矛盾了。

接着，如果 $x^n(n\in\mathbb{Z})$ 可以生成这个群，那么 $x\in\langle x^n\rangle$，于是存在 $m\in\mathbb{Z}$ 使得 $x=(x^n)^m$，于是 x^{nm-1}=0。由于 x 是无限阶的，所以 $nm=1$，那么这样的 n 只能是 ±1。另外，显然 x^{-1} 也可以生成这个群。这就证明了恰好是这两个生成元。

和有限循环群一样，我们有以下命题。

命题 1.29

所有的无限循环群是彼此同构的。

证明 证明是非常相似的，故留做练习。

这个命题告诉我们，要研究无限循环群，只要研究整数加群就可以了。是否是整数非常特殊呢？其实，我们不要忘记，整数就是这么定义出来的——我们一个一个数数，为了减法或加法逆元又定义了负整数，共同组成了整数，从定义上，整数就是个无限循环群。在数学中，整数集是个最常见的集合，而这个结论告诉我们，平时司空见惯的整数加群，实际上代表着所有的无限循环群。

我们把目光转回有限循环群。我们想知道 n 阶循环群中有几个生成元，而每一个元素的阶既然是有限的，又分别是多少。第二个问题可以回答第一个问题，因为生成元就是阶为 n 的元素。

命题 1.30

令 $G=\langle x\rangle$ 是一个 n 阶循环群。假设 $1\leqslant m\leqslant n$，则 x^m 的阶为

$$|x^m|=\frac{n}{\gcd(n,m)} \tag{1.50}$$

证明 假设 $1\leqslant m\leqslant n-1$，我们希望找到最小的正整数 k 使得 $(x^m)^k=x^{mk}=e$。由于 $|x|=n$，故这等价于 $n|mk$。接下来我们要利用简单的初等数论。通过同时除以 n 和 m 的最大公因数，我们得到

$$\frac{n}{\gcd(n,m)}\left|\frac{m}{\gcd(n,m)}\cdot k\right. \tag{1.51}$$

而因为 $\frac{n}{\gcd(n,m)}$ 和 $\frac{m}{\gcd(n,m)}$ 是互素的，所以这个条件进一步等价于

$$\frac{n}{\gcd(n,m)}\left|k\right. \tag{1.52}$$

也就是说，最小的这个正整数 k 正是 $\frac{n}{\gcd(n,m)}$。这就完成了证明。

这个命题的直接推论便是有限群的生成元的个数。

命题 1.31

令 $G=\langle x\rangle$ 是一个 n 阶循环群，则 $x^m(1\leqslant m\leqslant n)$ 是个生成元，当且仅当

$$\gcd(m,n)=1 \tag{1.53}$$

根据欧拉 ϕ 函数的定义，这些生成元的个数正是 $\phi(n)$。

证明 这是直接推论，证明是显然的。

我们换一个话题，因为循环群说的差不多了。我们要给出陪集的概念。在这一节中的主要目的是为了帮助我们计数。我们先给一个简单的定义。

定义 1.26

令 H 是 G 的子群，则 H 的阶，记作 $|H|$，定义为 H 的集合大小。若 H 是无限群则记 $|H|=\infty$。

一个可能会令初学者惊讶的命题是这样的。

命题 1.32

若 H 是 G 的子群，则 H 的阶整除 G 的阶，即

$$|H|\Big||G| \tag{1.54}$$

这意味着所有有限群的子群的阶都不是随意的，它必须是所在的更大的群的因数。这个命题可以被称为拉格朗日定理（也可以认为是拉格朗日定理的推论）。要证明这个命题，我们需要一些定义和引理。

定义 1.27

令 G 是一个群，$H<G$ 是一个子群，$a\in G$。则 aH 是 H 的一个左陪集（由 a 引出），定义为

$$aH=\{ax:x\in H\} \tag{1.55}$$

也就是说，由 a 引出的 H 的左陪集，就是用 a 左乘了 H 中的每一个元素所得到的。特别地，$eH=H$ 也是一个左陪集，未来我们会知道，在 H 是正规子群的时候，我们可以定义陪集的乘法，而此时这个特殊的陪集 $eH=H$ 就会起到单位元的作用。

我们继续说有限群的左陪集。

引理 1.2

令 G 是一个有限群，$H<G$ 是一个子群，$a\in G$。我们通过左乘 a 来定义 $f:H\to aH$

$$f(x)=ax \tag{1.56}$$

则 f 是一个双射。特别地，$|H|=|aH|$。

这告诉我们这些陪集都是一样大小的。而更妙的是，所有的左陪集实际上构成了 G 的一个分拆，也就是说，我们有下列命题。

命题 1.33

令 G 是一个有限群，$H<G$ 是一个子群，$a,b\in G$。则左陪集 aH 和 bH 要么相等，要么无交。也就是说，我们有 $aH=bH$，或 $aH\cap bH=\emptyset$。

证明 假设 $a,b\in G$。不妨假设 $aH\cap bH\neq\emptyset$，假设 $ah_1=bh_2\in aH\cap bH$，其中 $h_1,h_2\in H$。我们只须证明 $aH=bH$，而根据对称性，我们只须证明 $aH\subset bH$ 即可。任取 aH 中的元素 $ah(h\in H)$，则 $ah=(bh_2h_1^{-1})h=b(h_2h_1^{-1}h)\in bH$。这就完成了证明。

既然这样，那么我们就可以把 G 分拆成 H 的一系列左陪集。我们称这个由左陪集构成的集族为商集 G/H。

我们记这些左陪集的个数为 $[G:H]$，称为 H 在 G 中的指数。

定义 1.28

令 G 是一个有限群，$H<G$ 是一个子群。则商集 G/H 定义为

$$G/H=\{aH:a\in G\} \tag{1.57}$$

我们把这个商集的大小称为 H 在 G 中的指数，记为 $[G:H]$，即

$$[G:H]=|G/H| \tag{1.58}$$

根据上面所说的，我们就有直接推论

命题 1.34 (拉格朗日定理)

令 G 是一个有限群，$H<G$ 是一个子群，则

$$|G|=[G:H]|H| \tag{1.59}$$

特别地，

$$|H|\Big||G| \tag{1.60}$$

我们插入一个很简单的引理，这个引理很好用，接下来也会用到。

引理 1.3

令 G 是一个群，$H<G$ 是一个子群，$x\in G$，则我们有充要条件

$$xH=H\iff x\in H \tag{1.61}$$

一般地，对于 $x,y\in G$，我们有充要条件

$$xH=yH\iff y^{-1}x\in H \tag{1.62}$$

证明 后半个命题可以通过对 $xH=yH$ 两边同时左乘 y^{-1} 得到 $y^{-1}xH=H$，进而转化为前半个命题。因此我们只须证明前半个命题。

一方面，假设 $xH=H$，不妨取 $x=xe\in xH=H$，因此 $x\in H$。

另一方面，假设 $x\in H$，则根据乘法封闭性，$xH=\{xh:h\in H\}\subset H$。根据逆元封闭性，$x^{-1}\in H$。同理可得 $x^{-1}H\subset H$。对这个式子同时左乘 x，我们就得到 $xH=H$。

这里有两个很自然的问题可以问。第一个问题是，如果我们有嵌套的子群，那么有没有指数的关系。第二个问题是，这个商集有没有可能赋予上群的结构。第一个问题的答案是肯定的，而第二个问题的答案是有时可以——在 H 是 G 的正规子群的时候。正规子群相关的内容我们放到下一节讲，这里我们把第一个问题回答了，通过一个命题。

命题 1.35

令 $K<H<G$ 是三个有限群，则

$$[G:K]=[G:H][H:K] \tag{1.63}$$

证明 [证法一] 直接利用拉格朗日定理。把指数写成阶的商，等号右边约分后就立刻得证了。

证明 [证法二] 我们想要把这个性质形象地用陪集嵌套子陪集的方式来刻画，进而把这个命题作为推论。假设 $G/H=\{a_iH\}_{i\in I}$，$H/K=\{b_jK\}_{j\in J}$。有没有一种可能，我们有 $G/K=\{a_ib_jK\}_{i\in I,j\in J}$ 呢？——这里的含义是，枚举法中的这些陪集都是两两不同的。答案是肯定的。我们只要证明了这个条件，原命题就成为直接推论了。

我们要证明两件事。第一，这些 a_ib_jK 枚举尽了所有 K 在 G 中的左陪集；第二，这些 a_ib_jK 是两两无交的。

第一：令 $aK\in G/K(a\in G)$。假设 $a\in a_iH$，其中 $a=a_ih(h\in H)$。进一步假设 $h\in b_jK$，故 $aK=a_ihK\subset a_ib_jK$。因为左陪集要么相等，要么无交，故 $aK=a_ib_jK$，这就证明了第一点。

第二：假设 $a_ib_jK = a_{i'}b_{j'}K$。同时右乘上 H（指在集合意义上，同时右乘上 H 的所有元素），由于 $b_j, b_{j'} \in H$ 以及 $k \in K$，我们有 $a_iH = a_{i'}H$。这就告诉我们 $a_i = a_{i'}$，所以我们可以在 $a_ib_jK = a_{i'}b_{j'}K$ 上同时左乘 a_i^{-1}，得到 $b_jK = b_{j'}K$。这就告诉我们 $b_j = b_{j'}$，这就证明了第二点。

综上所述，嵌套子群的陪集也是如我们预期的那样嵌套，这样，作为推论，我们证明了原命题。

接下来，假设我们有两个子群 $H, K < G$，那么我们就有了它们的乘积

$$HK = \{hk : h \in H, k \in K\} \tag{1.64}$$

和交集 $H \cap K$。对于这些子集（或子群），我们有没有什么大小关系呢？答案是肯定的。

命题 1.36

令 $(G, \cdot)$ 是一个群。若 $H, K < G$ 是两个有限子群，则

$$|HK| = \frac{|H||K|}{|H \cap K|} \tag{1.65}$$

♠

证明 我们微调至

$$\frac{|HK|}{|K|} = \frac{|H|}{|H \cap K|} \tag{1.66}$$

因为 $H \cap K < H$，我们可以假设 $H/(H \cap K) = \{a_i(H \cap K)\}_{i \in I}$，其中 $a_i \in H (i \in I)$ 是两两不同的。我们只须证明 $HK/K = \{a_iK\}_{i \in I}$，其中 a_iK 要么相等，要么无交。

任取 $hkK = hK \in HK/K$，其中 $h \in H$，故存在 $i \in I$ 使得 $h \in a_i(H \cap K)$。假设 $h = a_ix$，其中 x 既在 H，也在 K。这样，$hkK = hK = a_ixK = a_iK$，因为 $x \in K$。这就证明了第一点。

接着，假设 $a_iK = a_jK$，其中 $i, j \in I$。我们只须证明 $a_i(H \cap K) = a_j(H \cap K)$。根据上面的引理 $a_j^{-1}a_i \in K$，可是 $a_i = a_j \in H$，于是 $a_j^{-1}a_i \in H \cap K$。同样根据上面的引理，我们知道 $a_i(H \cap K) = a_j(H \cap K)$。这就证明了第二点。

综上所述，尽管 HK 不需要成为一个群，但是 HK/K 完全可以通过 $H/(H \cap K)$ 来明确地构造出来，它们的大小相等，这就完成了这个命题的证明。

1.4 正规子群

我们在这一节会定义一个群的正规子群。正规子群首先是个子群，但是又满足更多的性质。因此正规子群一定是子群，反过来不一定。

假设 $H < G$，我们的一个重要的目标是赋予 $G/H = \{aH : a \in G\}$ 以群结构。我们当然希望对于 $a, b \in G$，定义

$$(aH) \cdot (bH) = (ab)H \tag{1.67}$$

可是注意到一个陪集的表达式不唯一的，根据上一节的引理，若 $a, b \in G$，则

$$aH = a'H \iff a^{-1}a' \in H \tag{1.68}$$

我们希望上面的乘法是良定义的，所以要给子群一些额外的条件，变成所谓的正规子群。这额外的条件便是正规性，即左右陪集全部相等。我们指的是，

定义 1.29

令 $(G, \cdot)$ 是一个群，且 $N \subset G$。我们称 N 是个正规子群，记作 $N \lhd G$，若

$$N \text{ 是个子群} \tag{1.69}$$

$$\forall a \in G, aN = Na \tag{1.70}$$

♣

首先要证的便是上面的陪集乘法是良定义的。

命题 1.37

令 $(G,\cdot)$ 是一个群，且 $N \lhd G$，$a,b \in G$，则

$$(aN)\cdot(bN) = (ab)N \tag{1.71}$$

是良定义的。

证明 [证法一] 假设 $aN = a'N, bN = b'N$，则 $a^{-1}a', b^{-1}b' \in N$，我们只须证明 $abN = a'b'N$，即 $(ab)^{-1}a'b' = b^{-1}a^{-1}a'b' \in N$。首先中间这个部分，即 $a^{-1}a'$，是在 N 中的。接着，利用 N 是个正规子群，我们可以得到 $b^{-1}Nb = N$，因此，$b^{-1}a^{-1}a'b' \in b^{-1}Nb' = N$。进一步地，$abN = a'b'N$。这就证明了良定义性。

证明 [证法二] 事实上，这个乘法可以简单地理解成子集乘法，即 $(aN)(bN) = \{xy : x \in aN, y \in bN\}$。我们只须说明，这从集合意义上，等于 abN。而这几乎是显然的。由于 $Nb = bN$，我们有 $aNbN = abNN = abN$。其中最后一步的 $NN = N$，一边是因为乘法封闭性，$NN \subset N$；而另一边是因为乘法单位元，$N = Ne \subset NN$。这样，既然从集合意义上相等，那么自然就是良定义的。(因为我们不必选取单位元)。

以上两个证明各有利弊。当然，都理解是最好的。下面，我们要说一个重要的结论，这个结论也是我们期待的，那就是，当 $N \lhd G$ 时，G/N 在这个陪集乘法下构成群，称为商群。

命题 1.38

令 $(G,\cdot)$ 是一个群，且 $N \lhd G$，则 $(G/N,\cdot)$ 构成一个群，称为（G 在 N 上的）商群，其中的单位元是 $eN = N$，每个陪集 aN 的逆元是 $a^{-1}N$。

证明 事实上，我们会发现，良定义性是最难证的。一旦证明了良定义性，利用乘法的定义，上面这些结论几乎都是显然的。我们一条条来证。

封闭性：在讲陪集的时候已经证过了。

结合律：令 $a,b,c \in G$，则利用乘法的定义，$(aNbN)cN = (abN)(cN) = ((ab)c)N$。利用 G 对乘法的结合律，得到这是等于 $(a(bc))N$ 的。类似地，这最终等于 $aN(bNcN)$。

单位元：令 $a \in G$，则 $aNeN = (ae)N = aN$，类似地 $eNaN = aN$。

逆元：令 $a \in G$，则 $aNa^{-1}N = (aa^{-1})N = eN$，类似地 $a^{-1}NaN = eN$。

综上，若 $N \lhd G$，则 G/N 在这个自然的乘法下构成群，称为一个商群。

我们这里补充一个引理，帮助我们更好地判别正规子群。

引理 1.4

令 $(G,\cdot)$ 是一个群，且 $N < G$，则下列命题等价

1. N 是 G 的正规子群，即

$$\forall a \in G, aN = Na \tag{1.72}$$

2.

$$\forall a \in G, aNa^{-1} \subset N \tag{1.73}$$

3.

$$\forall a \in G, \forall n \in N, ana^{-1} \in N \tag{1.74}$$

证明 显然第二个条件和第三个条件等价。我们只要证明第一个条件与第二个条件等价即可。

一方面，我们假设 N 是 G 的正规子群。令 $a \in G$，则 $aN = Na$。同时右乘 a^{-1} 并取一半的包含关系，我们得到了 $aNa^{-1} \subset N$。

另一方面，我们假设第二个条件。令 $a \in G$，则由 $aNa^{-1} \subset N$ 得到 $aN \subset Na$，由 $a^{-1}N\left(a^{-1}\right)^{-1} \subset N$ 得到 $Na \subset aN$。因此，$aN = Na$。

事实上，第二个条件和第三个条件都很好用，唯独第一个条件很少用。

一个简单的命题是，一族正规子群的任意交还是正规子群。

命题 1.39

令 $(N_i)_{i\in I}$ 是一族 G 的正规子群，则它们的交集仍然是 G 的正规子群，即

$$\bigcap_{i\in I} N_i \lhd G \tag{1.75}$$

证明 首先，我们可以知道子群的任意交是子群。这个证明与子集可以生成子群的证明是几乎完全一致的，故这里略去证明。检验三条或精简的两条即可。

因此我们只需要检查正规性。我们利用引理的第三条。令 $a\in G, n\in \bigcap_{i\in I} N_i$，我们只须证明 $ana^{-1}\in \bigcap_{i\in I} N_i$。任取 $i\in I$，则 $n\in N_i$。由于 $N_i\lhd G$，我们有 $ana^{-1}\in N_i$。因此，$ana^{-1}\in \bigcap_{i\in I} N_i$。这就证明了 $\bigcap_{i\in I} N_i \lhd G$。

那么十分类似地，读者也可以证明，每一个子集都可以生成一个正规子群，定义为所有包含那个子集的正规子群的交集，而这个交集仍然是一个正规子群。在这里，我们一笔带过，感兴趣的读者可以花一点时间证明。

我们应当举一些正规子群的例子。首先，对于任意群 $(G,\cdot)$，平凡子群 $\{e\}$ 和整个群 G 都是正规子群，即

命题 1.40

令 $(G,\cdot)$ 是一个群，则

$$\{e\}\lhd G \tag{1.76}$$

$$G\lhd G \tag{1.77}$$

证明 我们实际也没有给过它们是子群的证明，这里一并给了。

平凡群：怎么乘都是单位元，所以对乘法封闭；包含单位元；唯一的元素的逆元还是单位元；在这个群中，a 的左右陪集都是 $a\{e\}=\{e\}a=\{a\}$。因此，$\{e\}\lhd G$。

整个群：子群是显然的；在整个群 G 中，每个元素的左右陪集都是全集，即 $aG=Ga=G$，这是因为 $a\in G$。因此，$G\lhd G$。

而对于阿贝尔群而言，子群就是正规子群，正规子群也就是子群，这是因为其乘法是交换的，因此左陪集当然，作为结论，等于右陪集。

命题 1.41

令 $(G,\cdot)$ 是个阿贝尔群，则子群就是正规子群，正规子群也就是子群，即

$$H<G \iff H\lhd G \tag{1.78}$$

证明 证明只需一行。根据交换律，$aH=\{ah:h\in H\}=\{ha:h\in H\}=Ha$。

到这里，我们已经万事俱备了，是时候介绍群同构第一定理了。这个定理可以从每一个群同态中都找到一个群同构，而其中的一个群就是商群。（这就是为什么我们必须先说商群。）

命题 1.42 (群同构第一定理)

令 $f:G\to G'$ 是一个群同态，则 $\ker(f)\lhd G$，且 G 在 $\ker(f)$ 上的商群同构于 $\mathrm{im}(f)$，即

$$G/\ker(f)\simeq \mathrm{im}(f) \tag{1.79}$$

特别地，若 f 是满同态，则

$$G/\ker(f)\simeq G' \tag{1.80}$$

若 f 是单同态，则

$$G/\{e\}\simeq G\simeq \mathrm{im}(f) \tag{1.81}$$

若 G 是有限群，则

$$\frac{|G|}{|\ker(f)|}=|\mathrm{im}(f)| \tag{1.82}$$

证明 这三条推论都是显然的，唯一要说明的是 $G/\{e\}$ 为什么同构于 G。这是因为 $a\{e\} \mapsto a$ 是一个同构（很容易检验其既是双射也是同态），这就意味着我们只须证明原命题即可。

首先要说明每个同态的核都是定义域的正规子群。要注意，同态的像未必是正规子群，往往只是普通的子群。我们只须证明，若 $a \in G$，$n \in \ker(f)$，则 $ana^{-1} \in \ker(f)$。注意到

$$f(ana^{-1}) = f(a)e'f(a)^{-1} = e' \tag{1.83}$$

因此 $ana^{-1} \in \ker(f)$。这就证明了 $\ker(f) \lhd G$。

接下来，我们要找到一个从商群 $G/\ker(f)$ 到像集 $\mathrm{im}(f)$ 的同构映射。我们称这个映射叫 $\tilde{f} : G/\ker(f) \to \mathrm{im}(f)$，对于 $a \in G$，定义为

$$\tilde{f}(a\ker(f)) = f(a) \tag{1.84}$$

为了方便起见，在不会引起歧义的情况下，我们令 $N = \ker(f)$，也即

$$\tilde{f}(aN) = f(a) \tag{1.85}$$

考虑到陪集代表元的不唯一性，我们要证明良定义性。假设 $aN = a'N$，或 $a^{-1}a' \in N$，只须证明 $f(a) = f(a')$，而这是因为

$$f(a') = f(aa^{-1}a') = f(a)f(a^{-1}a') = f(a)e' = f(a) \tag{1.86}$$

这就证明了良定义性。

接下来，我们要证明 $\tilde{f}$ 既是同态，也是双射（单射 + 满射）。

同态：令 $a, b \in G$，则 $\tilde{f}(aN) = f(a)$，$\tilde{f}(bN) = f(b)$，而

$$\tilde{f}\left((aN)(bN)\right) = \tilde{f}(abN) = f(ab) = f(a)f(b) = \tilde{f}(aN)\tilde{f}(bN) \tag{1.87}$$

这就证明了 $\tilde{f}$ 是一个同态。

单射：只须证明 $\ker\left(\tilde{f}\right) = \{N\}$。假设 $\tilde{f}(aN) = e'$，则根据定义，$f(a) = e'$，故 $a \in \ker(f) = N$，所以 $aN = N$，这就证明了 $\tilde{f}$ 是一个单射。

满射：令 $a' \in \mathrm{im}(f)$，取 $a \in G$ 使得 $a' = f(a)$。因此，$\tilde{f}(aN) = f(a) = a'$，这就证明了 $\tilde{f}$ 是一个满射。

综上所述，$\tilde{f}$ 是一个从商群 $G/\ker(f)$ 到像集 $\mathrm{im}(f)$ 的同构。作为结论，

$$G/\ker(f) \simeq \mathrm{im}(f) \tag{1.88}$$

至于推论，我们在开头已经证过了。这就完成了整个命题的证明。

我们举一个例子，你知道一般线性群 $GL(n,\mathbb{R})$ 在特殊线性群 $SL(n,\mathbb{R})$ 中的商群是什么结构吗？现在你知道了，因为

$$\det : GL(n,\mathbb{R}) \to \mathbb{R}^\times \tag{1.89}$$

是个满同态，且 $\ker(\det) = SL(n,\mathbb{R})$，则由群同构第一定理，我们有

$$GL(n,\mathbb{R})/SL(n,R) \simeq \mathbb{R}^\times \tag{1.90}$$

讲了群同构第一定理，不讲第二、第三定理好像有点说不过去。后面两个定理的难度都会低很多，所以不要被数量吓到了。下面，我们来讲剩下两个定理。

命题 1.43 (群同构第二定理)

令 $(G,\cdot)$ 是一个群，且 $N \lhd G$，$H < G$。则 $H \cap N \lhd H$，$N \lhd HN$，且

$$H/(H \cap N) \simeq HN/N \tag{1.91}$$

这和之前两个子群乘积的阶的公式是类似的。

证明 第一，要证明 $H \cap N \lhd H$。令 $h \in H$，而 $x \in H \cap N$，则 $hxh^{-1} \in H$，而且因为 $N \lhd G$，$hxh^{-1} \in N$，因此 $hxh^{-1} \in H \cap N$。

第二，要证明 $N \lhd HN$。令 $hn \in HN$，而 $n' \in N$。则 $hnn'(hn)^{-1} = h(nn'n^{-1})h^{-1} \in hNh^{-1} = N$。

第三，要证明 $H/(H\cap N)\simeq HN/N$。令 $f:H\to HN/N$，定义为

$$f(h)=hN \tag{1.92}$$

这显然是良定义的同态（因为 $N\lhd G$）。根据 $HN/N=\{hnN:h\in H,n\in N\}=\{hN:h\in H\}$，这还是个满同态。接下来，它的核是 $\ker(f)=\{h\in H:hN=eN\}=\{h\in H:h\in N\}=H\cap N$。因此，根据群同构第一定理，

$$H/(H\cap N)\simeq HN/N \tag{1.93}$$

这就证明了群同构第二定理。

注意到，实际上我们曾经在计算有限群的阶的时候，暗示过这个定理。不过当时两边尚且不一定是群，又怎么能同构呢。

命题 1.44 (群同构第三定理)

令 $(G,\cdot)$ 是一个群，且 $N\lhd G$，$M\lhd G$，$M<N$。则 $N/M\lhd G/M$，且

$$(G/M)/(N/M)\simeq G/N \tag{1.94}$$

♠

证明 首先根据定理，$N/M\subset G/M$。我们要注意 N/M 是个群，是要证明的。我们只须证明 $M\lhd N$。这几乎是显然的。令 $n\in N$，$m\in N$，则 $nmn^{-1}\in M$。因此 N/M 是个群。

因为这两个都是群，所以当然有 $N/M<G/M$。接下来我们可以先证明正规性（只利用同态的核也可以证明，不过下面的证明也是便于读者理解正规子群的概念，故保留），这也几乎是显然的。令 $nM\in N/M(n\in N)$，$gM\in G/M(g\in G)$，则

$$(gM)(nM)(gM)^{-1}=(gng^{-1})M\in\{nM:n\in N\}=N/M \tag{1.95}$$

因此 $N/M\lhd G/M$。

那么，我们要定义 $f:G/M\to G/N$，定义为

$$f(gM)=gN \tag{1.96}$$

要证明良定义性。假设 $gM=g'M$，则 $g^{-1}g'\in M$，故 $g^{-1}g'\in N$，所以 $gN=g'N$。

同态是显然的：

$$(gMg'M)=f(gg'M)=gg'N=gNg'N=f(gM)g(g'M) \tag{1.97}$$

满同态几乎也是显然的。任取 $gN\in G/N(g\in G)$，则 $f(gM)=gN$。

最后，核是什么呢？

$$\ker(f)=\{gM:f(gM)=gN=eN\}=\{gM:g\in N\}=N/M \tag{1.98}$$

根据群同构第一定理，这就告诉我们

$$(G/M)/(N/M)\simeq G/N \tag{1.99}$$

综上所述，我们就证明了群同构第三定理。

1.5 群作用

群作用是个较为抽象的概念。为了让大家理解这一概念，请允许我们为大家以更多的概念和例子做些铺垫。这些铺垫不会是无关信息的堆砌，而是为了在重要的概念登场前，让大家做好准备。

第一个概念是对称群，或置换群。

定义 1.30

令 S 是一个集合，则 S 上的置换群（或对称群），记作 $(\mathrm{Perm}(S),\circ)$，由所有 S 到自身的双射构成，而这

里的运算是映射的复合运算。

$$\mathrm{Perm}(S) = \{f : S \to S \text{ 双射}\} \tag{1.100}$$

证明 首先，映射的复合是满足结合律的。这是根据定义立刻可知的。

单位元是恒等映射，记作 id，对所有 $s \in S$，定义为

$$id(x) = x \tag{1.101}$$

故显然有，对所有 $f \in \mathrm{Perm}(S)$，$f \circ id = id \circ f = f$。

逆元是根据双射可知的。假如 f 是一个从 S 到自身的双射，则存在其逆映射 f^{-1}，使得 $f \circ f^{-1} = f^{-1} \circ f = id$。

综上所述，$(\mathrm{Perm}(S), \circ)$ 是个群，称为 S 上的置换群（或对称群）。

还记得我们是怎么在有限群中证明 $|xH| = |H|$ 的吗（$H < G$，$x \in G$）？我们是构造了一个双射 $\phi_x : H \to xH$，定义为，对于 $h \in H$，

$$\phi_x(h) = xh \tag{1.102}$$

则其逆为 $\phi_{x^{-1}} : xH \to H$。

我们将上面的 ϕ_x 延拓到整个群 G，还用 ϕ_x 来表示，即 $\phi_x : G \to G$，定义为左乘 x 的运算，即对于 $y \in G$，

$$\phi_x(y) = xy \tag{1.103}$$

这显然是一个双射（但一般来说不是同态，请大家自行验证），因为我们可以找到它的逆映射，及 $\phi_{x^{-1}}$。这是因为

$$(\phi_x \circ \phi_{x^{-1}})(y) = x(x^{-1}y) = y \tag{1.104}$$

$$(\phi_{x^{-1}} \circ \phi_x)(y) = x^{-1}(xy) = y \tag{1.105}$$

所以，我们就得到了下面的式子，希望大家可以迅速理解其含义。

$$(\phi_x)^{-1} = \phi_{x^{-1}} \tag{1.106}$$

由于我们对于每一个 $x \in G$，都定义了一个双射 $\phi_x : G \to G$，即 $\phi_x \in \mathrm{Perm}(G)$，所以这其实给出了一个映射 $\phi : G \to \mathrm{Perm}(G)$，即对于 $x \in G$，我们定义

$$\phi(x) = \phi_x \in \mathrm{Perm}(G) \tag{1.107}$$

要注意，这个映射 ϕ 的定义域和陪域都是群。所以，难道说这是个群同态？答案是肯定的。否则我们就没有讲的必要了。

命题 1.45

令 $(G, \cdot)$ 是一个群，我们通过上面的方法定义 $\phi : (G, \cdot) \to (\mathrm{Perm}(G), \circ)$，则 ϕ 是个群同态。

证明 证明是很简单的。令 $x, y \in G$，对于 $z \in G$，我们有

$$(\phi_x \circ \phi_y)(z) = x(yz) = (xy)z = \phi_{xy}(z) \tag{1.108}$$

由于这对于所有 $z \in G$ 都成立，故

$$\phi_x \circ \phi_y = \phi_{xy} \tag{1.109}$$

即

$$\phi(xy) = \phi(x) \circ \phi(y) \tag{1.110}$$

这就证明了 $\phi : G \to \mathrm{Perm}(G)$ 是个群同态。

即使证明很简单，但这样的结论无疑会给每个初学者以“美的体会”。这便是代数这一门学科美的地方。它常常给你一些好的结论，而证明不会太难。事实上，它的“美”，蕴含在对称之中，而群论讲的就是对称的故事。对于这一种“美”，我们为它起名，称作“群作用”。

定义 1.31

令 $(G,\cdot)$ 是一个群，S 是一个集合，而 $\phi: G \to \mathrm{Perm}(S)$。若 ϕ 是一个群同态，则我们说 ϕ 是 G 在（集合）S 上的群作用。

根据上面的命题，我们就知道，“左乘”是一个 G 在其自身的群作用 (也就是 $S=G$ 的特例)。

左乘作用似乎过于显然，因此我们给一个稍微不那么显然的例子，也是在自身的作用，叫做“共轭作用”。

定义 1.32

令 $(G,\cdot)$ 是一个群，我们对 $x \in G$，定义 $\phi_x \in \mathrm{Perm}(G)$，对 $y \in G$，定义为

$$\phi_x(y) = xyx^{-1} \tag{1.111}$$

则 $\phi: G \to \mathrm{Perm}(G)$，对 $x \in G$，定义为 $\phi(x) = \phi_x$，被称为 G 的共轭作用。

命题 1.46

令 $(G,\cdot)$ 是一个群，则 G 的共轭作用是 G 在自身的一个群作用。

证明 首先，我们要说明 ϕ_x 是双射，而这是显然的，因为其逆是 $\phi_{x^{-1}}$。而这是因为，对于 $y \in G$，

$$(\phi_x \circ \phi_{x^{-1}})(y) = \phi_x(x^{-1}yx) = x(x^{-1}yx)x^{-1} = y \tag{1.112}$$

$$(\phi_{x^{-1}} \circ \phi_x)(y) = \phi_{x^{-1}}(xyx^{-1}) = x^{-1}(xyx^{-1})x = y \tag{1.113}$$

这样，$\phi: G \to \mathrm{Perm}(G)$ 就是良定义的。接下来，我们证明 ϕ 是个同态。令 $x,y \in G$，$z \in G$，则

$$(\phi_x \circ \phi_y)(z) = \phi_x(yzy^{-1}) = x(yzy^{-1})x^{-1} = (xy)z(xy)^{-1} = \phi_{xy}(z) \tag{1.114}$$

这对所有 $z \in G$ 都成立，故

$$\phi_{xy} = \phi_x \circ \phi_y \tag{1.115}$$

即

$$\phi(xy) = \phi(x) \circ \phi(y) \tag{1.116}$$

这就证明了共轭作用确实是一个群在自身的群作用。

事实上，我们必须要注意，共轭作用比左乘作用更“好”，虽然其看上去更复杂一些。好在什么地方呢？我们知道，左乘作用的 ϕ_x，大部分不是群同态，可是共轭作用的 ϕ_x，个个都是同构。因为这一额外的性质，我们补充一个命题。

命题 1.47

令 $(G,\cdot)$ 是一个群，$x \in G$，则 $\phi_x: G \to G$，对 $y \in G$，定义为

$$\phi_x(y) = xyx^{-1} \tag{1.117}$$

是一个群 G 的自同构（即到自身的同构）。

证明 我们已经说明，ϕ_x 一定是双射，因为它的逆是 $\phi_{x^{-1}}$。因此我们只须证明 ϕ_x 本身还是个同态（不是说 ϕ 是同态，而是说每个 ϕ_x 是同态）。因此我们令 $y,z \in G$，只须证明 $\phi_x(yz) = \phi_x(y)\phi_x(z)$。而这是因为

$$\phi_x(y)\phi_x(z) = (xyx^{-1})(xzx^{-1}) = x(yz)x^{-1} = \phi_x(yz) \tag{1.118}$$

恰好约掉。这就证明了共轭作用下的每一个 ϕ_x 都是群 G 的自同构。

注意，我们对这样的自同构很感兴趣。因此再给它们一个特殊的名字，叫做“内自同构”，意指由群 G 内的元素引出的自同构。而所有其他的自同构，就叫做“外自同构”。

定义 1.33

令 $(G,\cdot)$ 是一个群，则一个 G 的（由 $x\in G$ 引出的）内自同构，指的是 $\phi_x:G\to G$，对 $y\in G$，定义为

$$\phi_x(y)=xyx^{-1} \tag{1.119}$$

而其他所有 G 上的自同构，则称为 G 上的外自同构。

我们回到群作用。囿于篇幅，我们希望再讲述一个定理，称为“轨道-稳定化子定理”。

注意，一般来说，令 $\phi:(G,\cdot)\to(\mathrm{Perm}(S),\circ)$ 是一个 G 在 S 的群作用，$x\in G$，$s\in S$，则我们会用 $x\cdot s$，甚至 xs，来代表 $\phi_x(s)$，或 $\phi(x,s)$。在这样的记号下，群作用的性质等价地变成下面两条。

命题 1.48

令 $\phi:(G,\cdot)\to(\mathrm{Perm}(S),\circ)$ 是一个 G 在 S 的群作用，假如我们用 $x\cdot s$，甚至 xs，来代表 $\phi_x(s)$，或 $\phi(x,s)$（其中 $x\in G$，$s\in S$），则我们等价地，可以把群作用的性质，记作

$$\forall s\in S, e\cdot s=s \tag{1.120}$$

$$\forall x,y\in G, x\cdot(y\cdot s)=(xy)\cdot s \tag{1.121}$$

或者进一步地，在不会引起歧义的情况下，记作

$$\forall s\in S, es=s \tag{1.122}$$

$$\forall x,y\in G, x(ys)=(xy)s \tag{1.123}$$

证明 若 ϕ 是一个群作用，则显然利用同态的性质我们有第二条。而根据同态把单位元映到单位元，我们有 $\phi_e=id$，即对所有 $s\in S$，$es=s$。这就证明了一个方向。

另一方向，若 $\cdot:G\times S\to S$ 满足这两条性质，我们想要定义 $\phi:G\to\mathrm{Perm}(S)$。当然对于 $x\in G, s\in S$，定义

$$\phi(x)(s)=\phi_x(s)=xs \tag{1.124}$$

我们当然也证明这样的 ϕ_x 是双射，否则都不是良定义的。但这几乎是显然的。

$$x(x^{-1}s)=(xx^{-1})s=es=sx^{-1}(xs)=(x^{-1}x)s=es=s \tag{1.125}$$

注意，上面两行的最后一步我们用到了命题中的第一条性质，为了证明 ϕ_x 是双射，这一条性质是不可或缺的。接下来，我们当然有

$$\phi_x^{-1}=\phi_{x^{-1}} \tag{1.126}$$

这就证明了每一个 ϕ_x 都是双射。而同态的性质是显然的，把第二个条件翻译一下即可。

因此命题中的第一条性质，是说明 ϕ 是良定义的（ϕ_x 是双射），而第二条性质是说明 ϕ 是同态。二者缺一不可。这两条性质加起来，就是群作用的定义。

接下来，我们举一个例子，地球的自转。我们知道地球是沿着一根轴自传的，我们固定这个轴。那么每一种自传对应着一个角度，其自由度为 1。我们把所有的自传构成的群叫做 G。而每一个自传，都会把地球表面的一个地方，带到另一个地方。

什么是轨道呢？我们取定地球上一个地点。那么每一个自传都会作用在这个地点，把它带到另一个地点。所有能够在群作用下“去到的地方”，就构成了轨道。我们不难发现，地球表面每个地方的轨道，就是纬度相同的一圈。

稳定化子是什么呢？我们同样取定地球上一个地点。有没有哪个自传作用在这个地点后位置还不变的？有的。那些转了 $2\pi n(n\in\mathbb{Z})$ 弧度的自传，是那些“固定”了这个地点的自传，也可以说“稳定”了这个地点。

假如记得没错的话，这是我们第一次引入借助生活中的例子来理解抽象代数。希望大家可以认识到，群作用是一个普遍的现象。下面我们给出严格定义。

定义 1.34

令 $\phi:(G,\cdot)\to(\mathrm{Perm}(S),\circ)$ 是一个 G 在 S 的群作用。若 $s\in S$。则我们定义 s 的轨道，记作 $\mathrm{Orb}(s)$，定义为

$$\mathrm{Orb}(s)=\{s'\in S:\exists x\in G,s'=xs\}=\{xs:x\in G\} \tag{1.127}$$

我们定义 s 的稳定化子，记作 $\mathrm{Stab}(s)$，定义为

$$\mathrm{Stab}(s)=\{x\in G:xs=s\} \tag{1.128}$$

♣

我们借地球自转的例子，可以发现轨道与轨道之间应当是要么相等，要么无交的。我们来证明这一命题。

命题 1.49

令 $\phi:(G,\cdot)\to(\mathrm{Perm}(S),\circ)$ 是一个 G 在 S 的群作用，而 $s,s'\in S$，则 $\mathrm{Orb}(s)$ 与 $\mathrm{Orb}(s')$ 要么相等，要么无交。因此，S 可以写成轨道的无交并。

♠

证明 假设它们有交集，即假设 $s''\in\mathrm{Orb}(s)\cap\mathrm{Orb}(s')$。进一步，我们找到 $x,x'\in G$，使得 $s''=xs=x's'$。根据对称性，我们只须证明 $\mathrm{Orb}(s)\subset\mathrm{Orb}(s')$。

任取 $ys\in\mathrm{Orb}(s)(y\in G)$，则

$$ys=(yx^{-1})xs=(yx^{-1})x's'=(yx^{-1}x')s'\in\mathrm{Orb}(s') \tag{1.129}$$

根据对称性，我们就知道 $\mathrm{Orb}(s)=\mathrm{Orb}(s')$。

我们应该注意到稳定化子中的元素是群中的元素，所以很自然会去想这是不是子群。答案是肯定的。

命题 1.50

令 $\phi:(G,\cdot)\to(\mathrm{Perm}(S),\circ)$ 是一个 G 在 S 的群作用，而 $s\in S$，则 s 的稳定化子是 G 的子群，即

$$\mathrm{Stab}(s)<G \tag{1.130}$$

♠

证明 一，$es=s$。二，若 $x,y\in\mathrm{Stab}(s)$，则 $(xy)s=x(ys)=xs=s$。三，若 $xs=s$，则左乘 x^{-1}，得到 $x^{-1}s=s$。

注意稳定化子一般不是正规子群。这里我们省略反例。

引理 1.5

令 $\phi:(G,\cdot)\to(\mathrm{Perm}(S),\circ)$ 是一个 G 在 S 的群作用，$s\in S$，$x,y\in G$，则 $xs=ys$ 当且仅当 $x^{-1}y\in\mathrm{Stab}(s)$。

♡

证明 对 $xs=ys$ 两边同时左乘 x^{-1}，就显然了。

这个引理的作用即在于下面的轨道-稳定化子定理

命题 1.51 (轨道-稳定化子定理)

令 $\phi:(G,\cdot)\to(\mathrm{Perm}(S),\circ)$ 是一个 G 在 S 的群作用，$s\in S$，则存在 $G/\mathrm{Stab}(s)$ 到 $\mathrm{Orb}(s)$ 的双射。

特别地，若 G 是有限群，则

$$|G|=|\mathrm{Stab}(s)|\cdot|\mathrm{Orb}(s)| \tag{1.131}$$

♠

证明 令 $f:G/\mathrm{Stab}(s)\to\mathrm{Orb}(s)$，定义为 $f(x\,\mathrm{Stab}(s))=xs$。

首先证明 f 是良定义的。根据上面的引理，若 $x\,\mathrm{Stab}(s)=y\,\mathrm{Stab}(s)$，则 $x^{-1}y\in\mathrm{Stab}(s)$，故 $xs=ys$。

根据 $\mathrm{Orb}(s)$ 的定义，f 显然是一个满射。

单射则是再次利用上面的引理。若 $xs=ys$，则 $x^{-1}y\in\mathrm{Stab}(s)$，故 $x\,\mathrm{Stab}(s)=y\,\mathrm{Stab}(s)$。

假如 G 是有限群，则同时取集合大小，就得到了

$$|G|=|\mathrm{Stab}(s)|\cdot|\mathrm{Orb}(s)| \tag{1.132}$$

综上，我们就证明了轨道-稳定化子定理。

有时，我们不知道一个有限群 G 的大小，但知道它作用在一个集合 S 上，那我们就可以利用轨道-稳定化子定理，找到某一个点 $s \in S$ 的轨道和稳定化子，进而算出 G 的阶。除了算出阶，其实也可以通过完全知道一个群的元素有哪些。例如 G 有 n 个元素，而你恰好找到了 n 个不相等的元素，那么这个群 G 一定就是由你找到的那些元素来构成的，无一例外，无一多余。

我们来看一个例子，二面体群 D_{2n}，它是由所有正 n 边形到自身的对称变换所构成的。什么是对称变换？就是把自身映到自身，而且是保距的。保距指的是，原先距离相同的点，变换后距离仍然相同。事实上，每一个对称变换由其 n 个顶点的像唯一确定，因为其余的点都可以通过顶点来找到位置。很明显，在初中的时候我们就知道，这是个轴对称图形，有 n 个翻折变换；这还是个中心对称图形，有 n 个旋转变换。那么问题来了，这些是不是所有的对称变换呢？回答是肯定的。我们可以利用轨道-稳定化子定理来证明。

命题 1.52

$|D_{2n}| = 2n$

♠

证明 任取正多边形的一个顶点 s，考虑其轨道 $\mathrm{Orb}(s)$。最多只有 n 个顶点可以去，而 n 个旋转变换恰好带 s 去了这些顶点，因此 $|\mathrm{Orb}(s)| = n$。

接下来，考虑其稳定化子 $\mathrm{Stab}(s)$。如果 $x \in D_{2n}$ 把 s 映射到 s，但又有保证是一个等距变换，则 s 相邻的两个顶点一定要被映射到这两个顶点。其中一个是恒等变换，而另一个是沿 s 所在的对称轴的翻折变换。不难看出，这两个是唯二的 s 的稳定化子。因此 $|\mathrm{Stab}(s)| = 2$。

根据轨道-稳定化子定理，$|D_{2n}| = |\mathrm{Orb}(s)| \cdot |\mathrm{Stab}(s)| = 2n$。这就证明了这个命题。

因此，二面体群 D_{2n} 就是恰好由 n 个翻折变换和 n 个旋转变换所组成的群。

1.6 群论与数论

为了让大家看到群论的应用，这里我们不妨举数论的例子。事实上，讲了群论以后不讲（初等）数论是很可惜的。因为利用群论，（初等）数论中的不少结论都变得非常简单。我们逐一来看。

我们首先定义整除。

定义 1.35

令 $n \in \mathbb{Z} \setminus \{0\}$，而 $m \in \mathbb{Z}$。我们说 n 整除 m，记作 $n|m$，若

$$m \in n\mathbb{Z} = \{kn : k \in \mathbb{Z}\} \tag{1.133}$$

♣

不难发现，对任何 $n \in \mathbb{Z}$，$n\mathbb{Z} < \mathbb{Z}$。事实上 $n\mathbb{Z} \lhd \mathbb{Z}$。最好的证明方法可能是通过同态。

命题 1.53

若 $n \in \mathbb{Z}$，则 $n\mathbb{Z} \lhd \mathbb{Z}$。

♠

证明 令 $f : \mathbb{Z} \to \mathbb{Z}$，对 $m \in \mathbb{Z}$，定义为

$$f(m) = mn \tag{1.134}$$

则 f 显然是群同态。因此 $n\mathbb{Z} = \mathrm{im}(f) < \mathbb{Z}$。又因为 $\mathbb{Z}$ 是阿贝尔群，因此 $n\mathbb{Z} \lhd \mathbb{Z}$。

接下来，我们定义模 n 的同余。

定义 1.36

令 $n \in \mathbb{N}_1$，而 $a, b \in \mathbb{Z}$。我们说 a 同余 b（模 n），记作 $a \equiv b \bmod n$，若

$$a + n\mathbb{Z} = b + n\mathbb{Z} \tag{1.135}$$

或

$$a-b\in n\mathbb{Z} \tag{1.136}$$

注意，从 $a+n\mathbb{Z}=b+n\mathbb{Z}$ 中，我们能得到 $-b+a\in n\mathbb{Z}$，利用 $n\mathbb{Z}$ 是阿贝尔群，交换后得到 $a-b\in n\mathbb{Z}$。

正因为 $n\mathbb{Z}\lhd\mathbb{Z}$，我们就得到了一个极其重要的商群，即 $\mathbb{Z}/n\mathbb{Z}$，在不引起歧义的情况下，也记作 $\mathbb{Z}_n$

定义 1.37

令 $n\in\mathbb{N}_1$，则 $\mathbb{Z}_n$ 定义为

$$\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z} \tag{1.137}$$

$\mathbb{Z}_n$ 中的每个元素，被称为一个模 n 的同余类。

不难发现，$0,\cdots,n-1$ 分别代表了 n 个同余类。

命题 1.54

$$\mathbb{Z}_n=\{k+n\mathbb{Z}:0\leqslant k\leqslant n-1\} \tag{1.138}$$

其中枚举法中的这些陪集是两两不同的。

证明 首先证明这里列完了所有的陪集。令 $m\in\mathbb{Z}$，根据带余除法，我们可以找到 $q\in\mathbb{Z}$，以及 $0\leqslant r\leqslant n-1$，使得

$$m=qn+r \tag{1.139}$$

由于

$$qn\in n\mathbb{Z} \tag{1.140}$$

因此 $m+n\mathbb{Z}=r+n\mathbb{Z}\in\{k+n\mathbb{Z}:0\leqslant k\leqslant n-1\}$。这就证明了最多只有这 n 个同余类。

接下来证明这 n 个同余类是互异的。假如 $k+n\mathbb{Z}=k'+n\mathbb{Z}$，其中 $0\leqslant k,k'\leqslant n-1$，则 $k-k'\in n\mathbb{Z}$。但是 $-(n-1)\leqslant k-k'\leqslant(n-1)$。而在这个范围内唯一 n 的倍数就是 0，于是 $k-k'=0$，或 $k=k'$。这就证明了这 n 个同余类是互异的。

综上所述，

$$\mathbb{Z}_n=\{k+n\mathbb{Z}:0\leqslant k\leqslant n-1\} \tag{1.141}$$

那么这个群的结构是什么呢？我们一句话就说完了。

命题 1.55

令 $n\in\mathbb{N}_1$，则 $\mathbb{Z}_n$ 是个 n 阶循环群。

还记得吗？给定 n，所有 n 阶循环群都是同构的。因此我们只要研究了 $\mathbb{Z}_n$，就研究了所有的有限循环群。

证明 我们只须证明 $\mathbb{Z}_n=\langle 1+n\mathbb{Z}\rangle$ 即可。而这几乎是显然的。因为（利用数学归纳法）k 个 $1+n\mathbb{Z}$ 相加，就是 $k+n\mathbb{Z}$（注意 0 个 $1+n\mathbb{Z}$ 相加规定为 $0+n\mathbb{Z}=n\mathbb{Z}$）。而这个群又是 n 阶的，因此是 n 阶循环群。

注意，接下来在不引起歧义的情况下，我们简单地将这个群记作

$$(\mathbb{Z}_n,+)=(\{0,1,\cdots,n-1\},+) \tag{1.142}$$

我们要注意的是，未来会知道，假如再考虑乘法，$(\mathbb{Z}_n,+,\cdot)$ 是个环。特别地，$(\mathbb{Z}_n,\cdot)$ 是个幺半群。

注意到，我们如果定义乘法 $\cdot:\mathbb{Z}_n\times\mathbb{Z}_n\to\mathbb{Z}_n$，当然定义为

$$(a+n\mathbb{Z})\cdot(b+n\mathbb{Z})=ab+n\mathbb{Z} \tag{1.143}$$

命题 1.56

$(\mathbb{Z}_n,\cdot)$ 是个幺半群。

♠

证明 我们先证明乘法是良定义的。假设 $a'+n\mathbb{Z}=a+n\mathbb{Z}$，$b'+n\mathbb{Z}=b+n\mathbb{Z}$。故 $a'=a+nk$，$b'=b+nl$，其中 $k,l\in\mathbb{Z}$。我们只须证明 $a'b'-ab\in n\mathbb{Z}$。而这是因为

$$a'b'-ab=(a+nk)(b+nl)-ab=anl+bnk+n^2kl=n(al+bk+nkl)\in n\mathbb{Z} \tag{1.144}$$

单位元显然是 $1+n\mathbb{Z}$。这是因为 $(a+n\mathbb{Z})(1+n\mathbb{Z})=a+n\mathbb{Z}$。

结合律也是显然的，因为 $(\mathbb{Z},\cdot)$ 是幺半群。

逆元是不必要的，因为我们只要证明是幺半群。

这样，我们就证明了 $(\mathbb{Z}_n,\cdot)$ 是个幺半群。

我们曾经在群论一节的开头证明了幺半群中所有可逆元素构成了群。我们把 $(\mathbb{Z}_n,\cdot)$ 中所有可逆元素构成的群记作 $\mathbb{Z}_n^\times$。

定义 1.38

令 $n\in\mathbb{N}_2$，则 $\mathbb{Z}_n^\times$，定义为由 $(\mathbb{Z}_n,\cdot)$ 中所有可逆元素构成的群。即

$$\mathbb{Z}_n^\times=\{k+n\mathbb{Z}:0\leqslant k\leqslant n-1,\exists l\in\mathbb{Z},kl\equiv 1 \bmod n\} \tag{1.145}$$

♣

我们很好奇 $(\mathbb{Z}_n,\cdot)$ 中的可逆元素是什么样子的。因此我们需要一个引理，称为裴蜀定理。其证明可以通过辗转相除法得到，这与群论的内容无关，故省略证明。

引理 1.6

若 $a,b,c\in\mathbb{N}_1$，则 $ax+by=c$ 有整数解 x,y 当且仅当 $\gcd(a,b)|c$。

特别地，对任意 $a,b\in\mathbb{N}_1$，我们可以找到 $x,y\in\mathbb{Z}$，使得 $\gcd(a.b)=ax+by$。

♡

利用这个引理，我们巧妙地算出了 $(\mathbb{Z}_n,\cdot)$ 的样子。

命题 1.57

令 $n\in\mathbb{N}_2$，则

$$\mathbb{Z}_n^\times=\{k+n\mathbb{Z}:1\leqslant k\leqslant n-1,\gcd(a,n)=1\} \tag{1.146}$$

因此

$$\left|\mathbb{Z}_n^\times\right|=\phi(n) \tag{1.147}$$

特别地，若 p 是一个素数，则

$$\mathbb{Z}_p^\times=\{1+p\mathbb{Z},2+p\mathbb{Z},\cdots,(p-1)+p\mathbb{Z}\} \tag{1.148}$$

因此

$$\left|\mathbb{Z}_p^\times\right|=p-1 \tag{1.149}$$

♠

证明 我们只须证明，若 $0\leqslant k\leqslant n-1$，则

$$(\exists l\in\mathbb{Z},kl\equiv 1 \bmod n)\iff\gcd(k,n)=1 \tag{1.150}$$

分两类情况。若 $k=0$，则显然左边是错的，而右边甚至是没有定义的，当然也是错的。即便你考虑 k 是 n 的倍数，那么 $\gcd(k,n)=n$，也是错的。

若 $1 \leqslant k \leqslant n-1$，则

$$\exists l \in \mathbb{Z}, kl \equiv 1 \bmod n \tag{1.151}$$

$$\iff \exists l \in \mathbb{Z}, \exists m \in \mathbb{Z}, kl + mn = 1 \tag{1.152}$$

$$\iff \gcd(k, n) = 1 \tag{1.153}$$

其中第一个充要条件是因为同余的定义，第二个充要条件是因为裴蜀定理。

这样我们就证明了 $\mathbb{Z}_n^\times$ 是由那些那 n 互素的数所在的陪集所构成的。特别地，这样的陪集的数量就是由欧拉 ϕ 函数给出的，即

$$\phi(n) = |\{1 \leqslant k \leqslant n-1 : \gcd(k, n) = 1\}| \tag{1.154}$$

接下来，若 p 是一个素数，则

$$\gcd(k, p) = 1 \iff p \nmid k \tag{1.155}$$

当然，从 1 到 $p-1$ 的这些数，都和 p 互素。因此，

$$\mathbb{Z}_p^\times = \{1 + p\mathbb{Z}, 2 + p\mathbb{Z}, \cdots, (p-1) + p\mathbb{Z}\} \tag{1.156}$$

故

$$\left|\mathbb{Z}_p^\times\right| = p - 1 \tag{1.157}$$

这就证明了这个命题。

同样，在不引起歧义的情况下，我们记

$$(\mathbb{Z}_n^\times, \cdot) = (\{1 \leqslant k \leqslant n-1 : \gcd(k, n) = 1\}, \cdot) \tag{1.158}$$

$$\left(\mathbb{Z}_p^\times, \cdot\right) = (\{1, 2, \cdots, p-1\}, \cdot) \tag{1.159}$$

根据拉格朗日定理，每个有限群的子群的阶整除这个群的阶。特别地，每个元素的阶，作为其生成的循环子群的阶，也整除整个群的阶。因此，我们有下面的引理。

引理 1.7

令 $(G, \cdot)$ 是个有限群，则对任意 $a \in G$，$a^{|G|} = e$。♡

证明 令 $\langle a \rangle$ 是由 a 生成的循环子群。则由拉格朗日定理，

$$|\langle a \rangle| \Big| |G| \tag{1.160}$$

而我们知道

$$|a| = |\langle a \rangle| \tag{1.161}$$

因此，

$$a^{|G|} = \left(a^{|a|}\right)^{|G|/|a|} = e^{|G|/|a|} = e \tag{1.162}$$

这就证明了这个引理。

这个引理在（初等）数论中有两个极其重要的推论，分别称为费马小定理和欧拉定理。

命题 1.58 (费马小定理)

令 p 是一个素数，而 $p \nmid a$，则

$$a^{p-1} \equiv 1 \bmod p \tag{1.163}$$

同时左乘 a，也可以得到

$$a^p \equiv a \bmod p \tag{1.164}$$

♠

证明 根据 $(\mathbb{Z}_p,\cdot)$ 中乘法的良定义性，我们不失一般性，假设

$$1 \leqslant a \leqslant p-1 \tag{1.165}$$

因此 $a \in \mathbb{Z}_p^\times$。根据上面的引理，

$$a^{|\mathbb{Z}_p^\times|} = e \tag{1.166}$$

此即

$$a^{p-1} \equiv 1 \bmod p \tag{1.167}$$

同时左乘后的结论是显然的。综上所述，我们用群论证明了费马小定理。

命题 1.59 (欧拉定理)

令 $n \in \mathbb{N}_2$，而 $\gcd(a,n)=1$，则

$$a^{\phi(n)} \equiv 1 \bmod n \tag{1.168}$$

证明 这个定理叫欧拉定理，这也在一定程度上解释了为什么 ϕ 函数被称为欧拉函数。欧拉定理显然是费马小定理的推广。通过群论来证明的思路是一致的。

首先，根据 $(\mathbb{Z}_n,\cdot)$ 中乘法的良定义性，我们不失一般性，假设

$$1 \leqslant a \leqslant n-1, \gcd(a,n)=1 \tag{1.169}$$

利用上面的引理，

$$a^{|\mathbb{Z}_n^\times|} = a^{\phi(n)} = e \tag{1.170}$$

此即

$$a^{\phi(n)} \equiv 1 \bmod n \tag{1.171}$$

这就证明了欧拉定理。

注意，当 $n=p$ 的时候，欧拉定理就退化为费马小定理。

最后，我们要介绍的定理是威尔逊定理。

命题 1.60 (威尔逊定理)

若 p 是一个奇素数（即除了 2 以外的素数），则

$$(p-1)! \equiv -1 \bmod p \tag{1.172}$$

其中 ! 表示阶乘。

证明

我们令 p 是一个奇素数，故 $\mathbb{Z}_p^\times$ 包含 $p-1$（偶数）个元素。

我们希望将逆元进行配对。注意到每一个元素都对应了一个逆元。而元素和逆元相等当且仅当这个元素的平方是单位元，即

$$a = a^{-1} \iff a^2 \equiv 1 \bmod p \tag{1.173}$$

而这就是

$$p|(a^2-1) = (a-1)(a+1) \tag{1.174}$$

所以要么 $p|(a-1)$，要么 $p|(a+1)$。

这就说明了所有逆元是自己的元素恰好是 1 和 $p-1$ 这两个。我们去掉这两个元素，剩下 $p-3$（偶数）个元素一定是两两配对的。因此剩下所有元素的乘积是 1。

因此

$$(p-1)! \equiv 1 \cdot (p-1) \cdot (1) \cdot \cdots \cdot (1) \equiv p-1 \equiv -1 \bmod p \tag{1.175}$$

这就证明了威尔逊定理。

为了方便大家理解，我们举一个可能不太恰当的例子。这就好比说有 $p-1$（偶数）个人，其中有两个编号是 1 和 $p-1$ 的人是单身，它们的对象不能是别人，硬要说也只能是自己。而剩下所有人都有（不是自己的）对象。

当然，我们必须说，在这个例子中有对象也不是什么好事，因为你和对象相乘就会约掉，失去踪影，仿佛失去了“个性”一般。1 是单位元，本身也没什么个性，可以无视。倒是 $p-1$，有个性却没有依附他人，因此是唯一留下踪影的人。

综上所述，从某个非常侧面的角度来看，威尔逊定理的一个间接推论便是：如果有了对象，我们一定要给彼此一个独立发展和生活的空间。

命题 1.61 (威尔逊定理的间接推论 *)

如果有了对象，我们一定要给彼此一个独立发展和生活的空间。

第 2 章 环论 I——Ring Theory I

2.1 环

注意到，环实际上有两种定义。一种是有乘法单位元的，而另一种是没有乘法单位元的。我们在这里假设环都是有乘法单位元的。

定义 2.1

我们说 $(R,+,\cdot)$ 是一个环，当 $(R,+)$ 是个阿贝尔群，$(R,\cdot)$ 是个幺半群，且乘法对加法有左右分配律，即

$$\forall a,b,c\in R, a(b+c)=ab+ac \tag{2.1}$$

$$\forall a,b,c\in R, (a+b)c=ac+bc \tag{2.2}$$

♣

R 指代的是英文单词 *ring*，即环。

那么什么是一个环呢？我们可以这样理解。对加法封闭，有交换、结合律，有单位元和逆元；对乘法封闭，有结合律，有单位元（有的定义中不需要有乘法单位元）。乘法不需要有逆元。

同时，我们不要求乘法有交换律。对于那些有乘法交换律的环，我们称之为交换环。

定义 2.2

令 $(R,+,\cdot)$ 是一个环，我们说 R 是一个交换环，当 R 对乘法有交换律，即

$$\forall a,b\in R, ab=ba \tag{2.3}$$

♣

注意，在交换环中，因为乘法是交换的，因此，左右分配律变成分配律。（只要证明任何一边，就可以利用乘法交换律得到另一边）。

环仍然是很常见的概念。最常见的环是整数环 $(\mathbb{Z},+,\cdot)$。不难检验这是一个环。我们结合上一章提到过的。我们实际上，也知道 $(\mathbb{Z}_n,+,\cdot)$ 是一个环。唯一要检验的便是分配律。考虑到 $\mathbb{Z}_n$ 中加法和乘法的良定义性，我们可以直接把 $\mathbb{Z}$ 中乘法对加法的分配律直接转移到 $\mathbb{Z}_n$ 中。具体的证明可以留给大家作为练习。

另一个经典的例子是 $n*n$ 实矩阵环 $(M(n,\mathbb{R}),+,\cdot)$。这是一个非交换环——乘法是不交换的。实际上，环是很常见的。仅仅是环的性质其实往往不够好，所以我们会给环加上各种更多的公理，比如得到整环，唯一分解整环，主理想整环，欧几里得整环，域等等。未来，我们会分别研究这些特别的环，以及它们之间的联系。

正如在幺半群、群论的开始我们证明了一些性质。环论的定义给了以后，有一些简单的小练习，我们用命题的形式给出。

命题 2.1

令 $(R,+,\cdot)$ 是一个环，而 $a,b,c\in R$，则

$$a0=0a=0 \tag{2.4}$$

$$a(-b)=(-a)b=-(ab) \tag{2.5}$$

$$(-a)(-b)=ab \tag{2.6}$$

♠

证明 一：首先，利用分配律，

$$a0=a(0+0)=a0+a0 \tag{2.7}$$

因此 $a0=0$。根据对称性，$0a=a$。

二：根据对称性，我们只须证明 $a(-b)=-(ab)$。而这是因为

$$a(-b)+ab=a(-b+b)=a0=0 \tag{2.8}$$

三：利用两次性质二，我们就得到

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab \tag{2.9}$$

有一个重要的环是零环，它是最平凡的环，即 $(0,+,\cdot)$。它只有一个元素，既是加法单位元也是乘法单位元，定义为

$$00 = 0 \tag{2.10}$$

$$0+0 = 0 \tag{2.11}$$

很容易检验这是一个环。

我们要说明的一个结论是，一个环是零环当且仅当加法单位元等于乘法单位元，即 $0 = 1$。

命题 2.2

令 $(R,+,\cdot)$ 是一个环，则 $R = \{0\}$ 当且仅当 $0 = 1$。

证明 充分性是显然的。

我们来证明必要性。假设 $0 = 1$，我们只须证明对所有 $a \in R$，都有 $a = 0$。

$$a = a1 = a0 = 0 \tag{2.12}$$

这就证明了这个命题。

我们在前一章学习了，每一个幺半群的所有可逆元素构成了一个群。由于每一个环 $(R,+,\cdot)$ 都包含了一个幺半群 $(R,\cdot)$。因此我们也定义所有乘法可逆元素构成的群，记作 $R^\times$。

定义 2.3

令 $(R,+,\cdot)$ 是一个环，则 $(R^\times,\cdot)$，是由 R 中所有乘法可逆元素构成的群。R 中的乘法可逆元素又被称为 R 中的单位。

我们知道，对于一般的环（不是零环的环），$0 \neq 1$。因此 0 永远是没有乘法逆元的，这是因为对所有 $a \in R$，我们有 $0a = 0 \neq 1$。所以最好的情况可能就是 $R \setminus \{0\} = R^\times$，即所有非零元素都有乘法逆元。这样的环的性质是很好的，我们称它为一个除环。

定义 2.4

令 $(R,+,\cdot)$ 是一个环，我们称 $(R,+,\cdot)$ 是一个除环，若

$$R \setminus \{0\} = R^\times \tag{2.13}$$

也即，所有非零元素都是单位。

不难发现，除环的充要条件是对加法构成阿贝尔群，对乘法构成群，且乘法对加法有左右分配律。

更好的环便是域。一个域是指交换的除环。

定义 2.5

令 $(R,+,\cdot)$ 是一个环，我们称 $(R,+,\cdot)$ 是一个域，若它是一个交换的除环。

命题 2.3

$(R,+,\cdot)$ 是一个域，当且仅当

$$(R,+) \text{ 是一个阿贝尔群} \tag{2.14}$$

$$(R \setminus \{0\},+) \text{ 是一个阿贝尔群} \tag{2.15}$$

$$\text{乘法对加法有分配律} \tag{2.16}$$

证明 根据定义，这是显然的。

我们发现 $(Z,+,\cdot)$ 是交换环，但不是域，因为 2 的乘法逆元 $\frac{1}{2}$ 显然不是整数。当我们扩充到所有的有理数以后，$(\mathbb{Q},+,\cdot)$ 就成为域。类似地，$(\mathbb{R},+,\cdot)$，$(\mathbb{C},+,\cdot)$ 也是域。我们下一个章节就会专门讨论域。域的性质比环好太多，但这也大大限制了域的范围——域完全没有环常见。因为域是特殊的环，所以环的大多性质都可以转移到域上，但反过来确实完全不可以的。从另一个方面说，因为域的性质太好，所以可以研究的内容，也和环并不一样。未来，大家会从学习中体会到这一段中所说的内容。

讲了环，当然要讲子环。

定义 2.6

令 $(R,+,\cdot)$ 是一个环，而 $S\subset R$。我们说 S 是 R 的子环，记作 $S<R$，若

$$0,1\in S \tag{2.17}$$

$$\forall a,b\in S, a+b, ab\in S \tag{2.18}$$

$$\forall a\in S, -a\in S \tag{2.19}$$

♣

事实上，这就是说 $(S,+)$ 是 $(R,+)$ 的子群，$(S,\cdot)$ 是 $(R,\cdot)$ 的子幺半群。我们当然有简单一些的等价条件。

引理 2.1

令 $(R,+,\cdot)$ 是一个环，而 $S\subset R$，则 $S<R$ 当且仅当

$$1\in S \tag{2.20}$$

$$\forall a,b\in S, a-b, ab\in S \tag{2.21}$$

♡

证明 假如满足了这两个条件，那么 $0=1-1\in S$。而 $-a=0-a\in S$，$a+b=a-(-b)\in S$。这就证明了这是个子环。

另一个方向是显然的。假如 S 是子环，那么 $a-b=a+(-b)\in S$。

例如 $\mathbb{Z}$ 就是 $\mathbb{Q}$ 的子环。

有了子环，我们就想知道是否用子集可以生成子环。答案还是肯定的。因为我们已经在幺半群和群中都做过类似的操作了，所以我们不赘述了。

定义 2.7

令 $(R,+,\cdot)$ 是一个环，而 $A\subset R$，则 A 生成的子环，记作 $\langle A\rangle$，定义为所有包含了 A 的子环的交集，即

$$\langle A\rangle=\bigcap\{S\subset R: S\supset A, S<R\} \tag{2.22}$$

♣

命题 2.4

令 $(R,+,\cdot)$ 是一个环，而 $A\subset R$，则 $\langle A\rangle<R$。

♠

证明 首先这个集族是非空的，因为 R 本身就是一个包含了 A 的子环。

接下来，我们利用上面的引理。令 S 是一个包含了 A 的子环。因为 1 在每一个这样的 S 中，所以 $1\in\langle A\rangle$。

令 $a,n\in\langle A\rangle$，则 $a-b, ab$ 在每一个这样的 S 中，因为每一个 S 都是子环。因此 $a-b, ab\in\langle A\rangle$。

综上所述，$\langle A\rangle<R$。

说完了子环，我们也要想到环的直积。和幺半群、群一样，环的直积是个群这一点也是需要证明的。

定义 2.8

令 $((R_i,+_i,\cdot_i)_{i\in I}$ 是一族环。我们定义它们的直积，为 $(\prod_{i\in I}R_i,+,\cdot)$。对于 $(x_i)_{i\in I},(y_i)_{i\in I}\in\prod_{i\in I}R_i$，我们

定义

$$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i +_i y_i)_{i\in I} \tag{2.23}$$

$$(x_i)_{i\in I} \cdot (y_i)_{i\in I} = (x_i \cdot_i y_i)_{i\in I} \tag{2.24}$$

♣

命题 2.5

令 $((R_i, +_i, \cdot_i)_{i\in I}$ 是一族环，则它们的直积 $(\prod_{i\in I} R_i, +, \cdot)$ 还是一个环。

♠

证明

根据幺半群和群论对直积是保持的，我们立刻知道 $\prod_{i\in I} R_i$ 对加法构成群，对乘法构成幺半群。因此只须检验乘法对加法的左右分配律。根据对称性，我们只证明左分配律。

令 $(x_i)_{i\in I}, (y_i)_{i\in I}, (z_i)_{i\in I} \in \prod_{i\in I} R_i$，则

$$(x_i)_{i\in I} \cdot ((y_i)_{i\in I} + (z_i)_{i\in I}) \tag{2.25}$$

$$=(x_i \cdot_i (y_i +_i z_i))_{i\in I} \tag{2.26}$$

$$=(x_i)_{i\in I} \cdot ((y_i)_{i\in I} + (z_i)_{i\in I}) \tag{2.27}$$

$$=(x_i)_{i\in I} \cdot (y_i)_{i\in I} + (x_i)_{i\in I} \cdot (z_i)_{i\in I} \tag{2.28}$$

因此，$(\prod_{i\in I} R_i, +, \cdot)$ 是一个环。这就证明了这个命题。

2.2 环同态

因为第一章的铺垫足够多，所以我们可以快速地进入环同态的讨论。更妙的是，环同构第一定理与群同构第一定理非常相似（在加法上是一致的，而在乘法上还是有微妙的区别的）。这意味着我们讨论在环同态上不会花太多的时间。

定义 2.9

令 $f : (R, +, \cdot) \to (R', +', *)$ 是一个映射，我们说 f 是个环同态，若

$$f(1) = 1' \tag{2.29}$$

$$f(a + b) = f(a) +' f(b) \tag{2.30}$$

$$f(ab) = f(a) * f(b) \tag{2.31}$$

♣

未来，在不引起歧义的情况下，我们会忽略两个环中加法与乘法的区别，都记作 + 和 ·，称环同态是

$$f : (R, +, \cdot) \to (R', +, \cdot) \tag{2.32}$$

注意到，这其实就是说，f 既是加法的群同态，又是乘法的幺半群同态。不要忘记，幺半群同态我们是要保持单位元的。而群同态因为逆元的存在，不需要额外的保持单位元的条件。这是个很小的细节。但通过这个细节，就能看出你是否真正理解了幺半群和群的重要区别。

要注意，因为我们定义了环是有乘法单位元的，因此 $\ker(f)$ 不一定是子环。所以，假如我们用群论作对比，在群论中正规子群是子群，可是在环论中的“正规子群”式的结构甚至几乎永远不是子环（除非是整个环）。我们管环论中的“正规子群”式的结构叫“理想”。这也是一个非常有名的概念，当然很多人只是听过了这个术语而已。和群论类似，$\mathrm{im}(f)$ 依然是子结构（在这里是子环）。那么，我们希望有的环同构第一定理，便是希望

$$R/\ker(f) \simeq \mathrm{im}(f) \tag{2.33}$$

我们现在有几件事情要做：定义理想，证明环同态的核一定是理想，定义商环，定义环同构，证明上述的同构关系。

理想在一定程度上，是一个“奇怪的”概念，原因便是初学者是很难一下子理解这样定义的好处。当时讲正规子群的时候，我们可以说因为希望左陪集的乘法是良定义的。这里虽然也是一样的道理，但是定义方法却并不类似。我们要提醒大家的是，理想这个概念，和数学中许多重要的概念一样，是经历了几年乃至几十年的研究后，才慢慢确定下来的——因此初学者不必立刻“理解”。事实上，在学完环同构第一定理的瞬间，应当就对这个概念有一定认识了。在学习得越来越深入后，对这一概念的熟悉便加深了。实际上，对所有抽象概念，人的认知都有类似的过程。我们铺垫这么多，就是为了在很大程度上提醒大家，下一个定义的重要性。

定义 2.10

令 $(R,+,\cdot)$ 是一个环，而 $I\subset R$。我们定义，称 I 是 R 的左理想，若

$$(I,+)<(R,+) \tag{2.34}$$

$$\forall r\in R,\forall a\in I,ra\in I \tag{2.35}$$

类似地，我们称 I 是 R 的右理想，若

$$(I,+)<(R,+) \tag{2.36}$$

$$\forall a\in I,\forall r\in R,ar\in I \tag{2.37}$$

如果 I 既是左理想又是右理想，我们就称 I 是 R 的一个理想，记作 $I\lhd R$。

我们刚才提过，一个理想一般不是子环。实际上，一个理想是子环当且仅当它是整个环。

引理 2.2

令 $(R,+,\cdot)$ 是一个环，而 $I\lhd R$。则 $I<R$ 当且仅当 $I=R$。

证明 必要性是显然的，因为一个环当然是自己的子环。

我们来证明充分性。假设 $I<R$，则特别地，$1\in I$。可是 $I\lhd R$，因此对任何 $r\in R$，我们有

$$r=r\cdot 1\in I \tag{2.38}$$

这就证明了 $I=R$。

综上所述，一个理想是子环当且仅当它是整个环。

注意，对于一个交换环来说，左理想等价于右理想，也就等价于理想。我们只需要证明左理想或右理想中的一条就可以证明另一条。

命题 2.6

假设 $(R,+,\cdot)$ 是一个交换环，则 I 是一个左理想当且仅当 I 是一个右理想，又当且仅当 I 是一个理想。

证明

根据交换环对乘法的交换律，这是显然的。

我们可以说，理想的第二条性质指的是：理想在乘法下“吸收”了整个环到理想上，也就是说

$$RI\subset I \tag{2.39}$$

$$IR\subset I \tag{2.40}$$

其中子集的乘法，当然指所有元素乘积的集合。

我们举一个重要的例子：$n\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想。通过这个例子，我们来体会一下，理想是怎么“吸收”整个环的乘法到其自身的。

命题 2.7

令 $n\in\mathbb{N}_1$，则 $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想，即

$$n\mathbb{Z}\lhd\mathbb{Z} \tag{2.41}$$

证明 首先，我们知道 $(n\mathbb{Z},+)$ 是 $(\mathbb{Z},+)$ 的（加法）子群。这可以通过构造 $m\mapsto mn$ 的（加法）群同态来得到（我们上一章证明过）。

其次，注意到 $\mathbb{Z}$ 是一个交换环，故我们只须证明 $RI\subset I$，在这里就是 $\mathbb{Z}\cdot n\mathbb{Z}\subset n\mathbb{Z}$。什么意思呢？就是说，一个整数乘上一个 n 的倍数，还是 n 的倍数。这是显然的，但这种显然蕴藏着一种微妙。数学家们通过体会这一种微妙，找到了理想的正确定义。这告诫我们，不要被看似简单的事实或现象蒙蔽双眼。我们应当从中找到数学的规律，而不是找到自己的傲慢。

要证明 $\mathbb{Z}\cdot n\mathbb{Z}\subset n\mathbb{Z}$，我们只须令 $m\in\mathbb{Z}$，$nk\in n\mathbb{Z}(k\in\mathbb{Z})$，只要证明 $mnk\in n\mathbb{Z}$ 即可。而这是因为

$$mnk=n(mk)\in n\mathbb{Z} \tag{2.42}$$

综上所述，这就证明了 $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想。

我们发现，正如正规子群可以从群同态中定义（群同态的核），理想也可以从环同态中定义（环同态的核）。我们用一个小引理来强调这个事实。

引理 2.3

令 $n\in\mathbb{N}_1$，我们要定义映射 $f:(\mathbb{Z},+,\cdot)\to(\mathbb{Z}_n,+,\cdot)$。对 $m\in\mathbb{Z}$，我们定义

$$f(m)=m+n\mathbb{Z} \tag{2.43}$$

则 f 是一个环同态，而 $\ker(f)=n\mathbb{Z}\lhd R$。♡

证明

我们在上一章中证明了 f 是加法的群同态。因此只须证明 f 是乘法的幺半群同态。

第一，$f(1)=1+n\mathbb{Z}$ 是 $\mathbb{Z}_n$ 的乘法单位元。

第二，若 $m,m'\in\mathbb{Z}$，则利用上一章中我们证明过的 $\mathbb{Z}_n$ 对乘法的良定义性，我们有

$$f(m)f(m')=(m+n\mathbb{Z})(m'+n\mathbb{Z})=mm'+n\mathbb{Z}=f(mm') \tag{2.44}$$

综上所述，f 是一个从 $\mathbb{Z}$ 到 $\mathbb{Z}_n$ 的环同态。

事实上，通过这个例子，我们想要引出的便是，每一个环同态的核都是理想。刚才我们也说了，每一个环同态的像都是子环。现在，我们来证明。

命题 2.8

令 $f:(R,+,\cdot)\to(R',+,\cdot)$ 是一个环同态，则 f 的核是 R 的理想，f 的像是 R' 的子环。此即，

$$\ker(f)=\{a\in R:f(a)=0\}\lhd R \tag{2.45}$$

$$\mathrm{im}(f)=\{b\in R':\exists a\in R,b=f(a)\}=\{f(a)\mathbb{R}':a\in R\}<R' \tag{2.46}$$

♠

证明 我们先证明 $\ker(f)\lhd R$。根据群同态的性质，我们知道 $\ker(f)$ 是加法的（正规）子群。为了方便起见，令 $I=\ker(f)$。我们只须证明 $RI\subset I$ 以及 $IR\subset I$。

令 $a\in R$，$b\in I=\ker(f)$，故 $f(b)=0'$。因此，$f(ab)=f(a)f(b)=f(a)0'=0'$，从而 $ab\in\ker(f)=I$。这就证明了 $RI\subset I$。而另一个包含关系是非常类似的，这里略去证明。这样，我们就证明了 $\ker(f)\lhd R$。

我们再证明 $\mathrm{im}(f)<R'$。第一，$1'=f(1)\in\mathrm{im}(f)$。

第二，令 $a',b'\in\mathrm{im}(f)$，不妨设 $a'=f(a)$，$b'=f(b)$。只须证明 $a'-b',a'b'\in\mathrm{im}(f)$。而这分别是因为

$$a'-b'=f(a)-f(b)=f(a-b)\in\mathrm{im}(f) \tag{2.47}$$

$$a'b'=f(a)f(b)=f(ab)\in\mathrm{im}(f) \tag{2.48}$$

这就证明了 $\mathrm{im}(f)<R'$。

综上所述，我们证明了这个命题。

接下来，我们想要给出商环的定义。注意，对加法群而言，商群是由加法的陪集所构成。在环中，我们既有加法，又有乘法，但是商环（群）仍然是由加法的陪集所构成。这是非常重要的一个出发点：商环，从集合意义

上来说，等于加法的商群。从这个出发点开始，我们来定义环对于理想的商环。

定义 2.11

令 $(R,+,\cdot)$ 是一个环，而 $I \lhd R$。我们定义 R 对 I 的商环，定义为 $(R/I,+,\cdot)$，其中

$$R/I = \{a+I : a \in R\} \tag{2.49}$$

而加法和乘法分别对 $a+I, b+I \in R/I (a,b \in R)$，定义为

$$(a+I)+(b+I) = (a+b)+I \tag{2.50}$$

$$(a+I)(b+I) = (ab)+I \tag{2.51}$$

♣

这个定义是不良好的。我们将其良定义性，和商环是个环这个事实，一并写进下一个命题中。

命题 2.9

令 $(R,+,\cdot)$ 是一个环，而 $I \lhd R$，则上述的加法和乘法是良定义的，且商环 $(R/I,+,\cdot)$ 是一个环。

♠

证明 因为环对加法构成阿贝尔群，而理想对加法构成子群，因此理想对加法构成正规子群。根据上一章的内容，正规子群这样的陪集加法是良定义的。

我们要证明商环对乘法是良定义的。令 $a+I = a'+I$，$b+I = b'+I$，即 $a-a' \in I, b-b' \in I$。我们只须证明 $ab+I = a'b'+I$，即 $ab-a'b' \in I$。而这是因为

$$ab-a'b' = (ab-a'b)+(a'b-a'b') = (a-a')b+a'(b-b') \in IR+RI = I+I = I \tag{2.52}$$

其中倒数第二个等号是根据理想对乘法的“吸引”性质，而最后一个等号是根据理想对加法的封闭性。这样，我们就证明了商环对乘法是良定义的。

接下来，要证明商环是个环，其实只要将 R 上环的结构（利用良定义性）照搬过来即可。

利用 I 对加法构成正规子群，因此利用上一章的内容，R/I 对加法构成群。我们只须证明 R/I 对乘法构成幺半群，且乘法对加法有左右分配律。

乘法单位元是 $1+I$，因为对任意 $a+I (a \in R)$，我们有

$$(a+I)(1+I) = (1+I)(a+I) = a+I \tag{2.53}$$

R/I 对乘法有结合律，这是因为对任意 $a+I, b+I, c+I (a,b,c \in R)$，我们有

$$((a+I)(b+I))(c+I) = (ab+I)(c+I) = (ab)c+I = a(bc)+I = (a+I)((b+I)(c+I)) \tag{2.54}$$

最后，我们要证明乘法对加法有左右分配律。利用对称性，我们只证明左分配律。对任意 $a+I, b+I, c+I (a,b,c \in R)$，我们有

$$(a+I)((b+I)+(c+I)) = (a+I)((b+c)+I) = a(b+c)+I = (ab+ac)+I = (a+I)(b+I)+(a+I)(c+I) \tag{2.55}$$

综上所述，我们就证明了 R/I 是个环。这个环被叫做 R 对 I 的商环。

我们为了环同构第一定理，补充环同构的定义。

定义 2.12

令 $f : (R,+,\cdot) \to (R',+,\cdot)$ 是一个映射，我们称 f 是一个环同构，若 f 既是双射，又是环同态。

♣

和之前一样，我们应当出于对对称性的考虑，证明每个环同构 f 的逆映射仍然是环同态，进而也是环同构。

引理 2.4

令 $f : (R,+,\cdot) \to (R',+,\cdot)$ 是个环同构，则 f^{-1} 是个环同态，进而也是环同构。

♡

证明 事实上，f 是环同构，当且仅当 f 对加法是群同构，而对乘法是幺半群同构。因为我们对群同构和幺半群

同构都证明了逆映射仍然是同构。因此环同构的逆映射也是环同构，也就是环同态。这就证明了这个引理。

现在，我们终于做好环同构第一定理的准备了。让我们毫不犹豫地开始证明环同构第一定理吧！

命题 2.10 (环同构第一定理)

令 $f:(R,+,\cdot)\to(R',+,\cdot)$ 是一个环同态，则 R 对 $\ker(f)$ 构成的商环，同构于 $\mathrm{im}(f)$。此即，

$$R/\ker(f)\simeq \mathrm{im}(f) \tag{2.56}$$

证明

我们的定义方式和群同构定理是一致的。令 $\tilde{f}:R/\ker(f)\to\mathrm{im}(f)$，对 $a+\ker(f)$，定义为

$$\tilde{f}(a+\ker(f))=f(a) \tag{2.57}$$

我们在上一章证明了 $\tilde{f}$ 是良定义的，且对加法构成群同构。要证明 $\tilde{f}$ 是环同构，只须证明它对乘法是幺半群同态。

令 $a+\ker(f),b+\ker(f)\in R/\ker(f)(a,b\in R)$，则

$$\tilde{f}((a+\ker(f))(b+\ker(f)))=\tilde{f}(ab+\ker(f))=f(ab)=f(a)f(b)=\tilde{f}(a+\ker(f))\tilde{f}(b+\ker(f)) \tag{2.58}$$

综上所述，$\tilde{f}$ 给出了一个从商环 $R/\ker(f)$ 到像 $\mathrm{im}(f)$ 的环同构。这就证明了这个定理。

我们发现，上面的证明其实是之前的众多命题所铺垫的。真正证明的时候，已经非常简单了。这也是数学学习或研究的一个方法。我们只要把基础打扎实了，证明定理的时候，就不会很困难。

下面是环同构第二与第三定理。

命题 2.11 (环同构第二定理)

令 $(R,+,\cdot)$ 是一个环，而 $S<R$，$I\lhd R$。则 $S+I<R$，$S\cap I\lhd S$，$I\lhd S+I$，且

$$S/(S\cap I)\simeq (S+I)/I \tag{2.59}$$

证明 我们先证明 $S+I<R$。对加法而言，S 和 I 都是子群，因此我们只须证明 $S+I$ 对乘法构成子幺半群，即对乘法是封闭的，且包含单位元。第一，$1=1+0\in S+I$。第二，只须证明 $(S+I)(S+I)\subset(S+I)$，而这是因为

$$(S+I)(S+I)=SS+SI+IS+II\subset S+I+I+I=S+I \tag{2.60}$$

倒数第二个等号是根据 S 与 I 对乘法的封闭性，及 I 对乘法的“吸收”性。最后一个等号是根据 I 对加法的封闭性。

我们再证明 $S\cap I\lhd S$。同样根据上一章，$S\cap I$ 对加法构成子群。我们只须证明 $S\cap I$ 对乘法的“吸收”性，即 $(S\cap I)S\subset S\cap I$，及 $S(S\cap I)\subset S\cap I$。根据对称性，我们证明前面这个包含关系。

$$(S\cap I)S\subset SS\cap IS=S\cap I \tag{2.61}$$

根据对称性，$S\cap I\lhd S$。

我们接着证明 $I\lhd S+I$。根据上一章，加法的子群关系是显然的。我们只须证明 $I(S+I)\subset I$，及 $(S+I)I\subset I$。根据对称性，我们证明前面这个包含关系。

$$I(S+I)\subset IS+II=I+I=I \tag{2.62}$$

根据对称性，$I\lhd S+I$。

我们最后证明 $S/(S\cap I)\simeq(S+I)/I$。和群同构第二定理的证明一样，我们定义 $f:S\to(S+I)/I$，对 $a\in S$，定义为

$$f(a)=a+I\in(S+I)/I \tag{2.63}$$

根据上一章的结论，f 一个是良定义的满射，对加法构成群同态，且 $\ker(f)=S\cap I$。因此我们只要证明 f 对乘法是幺半群同态，就可以利用环同构第一定理证明这个命题了。而这是显然的，因为若 $a,b\in S$，则

$$f(a)f(b) = (a+I)(b+I) = ab+I = f(ab) \tag{2.64}$$

因此，由环同构第一定理，我们得到了

$$S/(S\cap I) \simeq (S+I)/I \tag{2.65}$$

综上所述，我们就证明了这个命题。

命题 2.12 (环同构第三定理)

令 $(R,+,\cdot)$ 是一个环，而 $I,J \lhd R$，且 $I \subset J$。则 $J/I \lhd R/I$，且

$$(R/I)/(J/I) \simeq R/J \tag{2.66}$$

♠

证明

我们先证明 $J/I \lhd R/I$。对加法而言 J 是 R 的子群，因此 J/I 是 R/I 的加法子群。我们只须证明 $(J/I)(R/I) \subset J/I$，及 $(R/I)(J/I) \subset J/I$。根据对称性，我们证明前面这个包含关系。因为 $J \lhd R$，所以

$$(J/I)(R/I) = (JR)/I \subset J/I \tag{2.67}$$

这就证明了 $J/I \lhd R/I$。

和上一章一样，我们令 $f: R/I \to R/J$，对 $a+I(a\in R)$，定义为

$$f(a+I) = a+J \tag{2.68}$$

根据上一章的结论，f 是一个良定义的满射，对加法构成群同态，且 $\ker(f) = J/I$。因此我们只要证明 f 对乘法是幺半群同态，就可以利用环同构第一定理证明这个命题了。而这是显然的，因为若 $a+I, b+I \in R/I (a,b\in R)$，则

$$f(a+I)f(b+I) = (a+J)(b+J) = ab+J = f(ab+I) \tag{2.69}$$

因此，由环同构第一定理，我们得到了

$$(R/I)/(J/I) \simeq R/J \tag{2.70}$$

综上所述，我们就证明了这个命题。

我们做个简单的复盘。实际上，我们会发现，环同构三定理，在良定义性和加法上，是完全照搬了群同构三定理的结论的，而对乘法的幺半群同态则是几乎显然的。因此，环同构定理实际上是群同构三定理的升级版。未来我们还会看到模论中的模同构三定理。到时候我们会注意到，证明也是类似的。

2.3 理想

这一节中，我们来谈谈理想（好像没有什么问题）。

首先还是生成的问题，我们要证明生成的理想还是理想，老生常谈了。

定义 2.13

令 $(R,+,\cdot)$ 是一个环，而 $A \subset R$。则 (A)，称为由 A 生成的理想，定义为所有 R 中包含 A 的理想的交集，即

$$(A) = \bigcap \{I \subset R : I \supset A, I \lhd R\} \tag{2.71}$$

♣

这里，我们用圆括号来区分尖括号，后者生成的是子环。

命题 2.13

令 $(R,+,\cdot)$ 是一个环，而 $A\subset R$，则 $(A)\lhd R$。

证明 首先，取交集的集族非空，因为整个环 R 是包含了 A 的一个理想（对加法构成子群，且“吸收”了乘法）。

由于集族中每一个理想都是加法子群。因此根据前一章的结论，它们的交还是加法子群。我们只须检验乘法的“吸收”性，即 $R(A)\subset(A)$，及 $(A)R\subset(A)$。根据对称性，我们证明第一个包含关系。假设 $r\in R$，$a\in(A)$，则对于任意集族中的理想 I，我们都有 $a\in I$。故 $ra\in I$。这对于任意这样的理想 I 都是成立的，因此 $ra\in(A)$。这就证明了 (A) 是 R 的子环。

假如我们有环 R 中的一个元素 $a\in R$，那么我们很自然会问，由一个元素生成的理想是什么。一般地，假如我们有有限多个元素 $a_1,\cdots,a_n\in R$，那么由有限多个元素生成的理想又是什么。对于交换环，答案是简单的，下面的命题给出了交换环中的答案。

定义 2.14

令 $(R,+,\cdot)$ 是一个环，而 $a\in R$，则我们定义

$$(a)=(\{a\}) \tag{2.72}$$

称为由 a 生成的主理想。一般地，若一个理想能被一个元素生成，我们就称其为主理想。

对于 $a_1,\cdots a_n\in R$，我们定义

$$(a_1,\cdots,a_n)=(\{a_1,\cdots,a_n\}) \tag{2.73}$$

一般地，若一个理想能被有限个元素生成，我们就称其为有限生成的理想。

命题 2.14

令 $(R,+,\cdot)$ 是一个交换环，而 $a\in R$，则

$$(a)=Ra=\{ra:r\in R\} \tag{2.74}$$

一般地，若 $a_1,\cdots,a_n\in R$，则

$$(a_1,\cdots,a_n)=Ra_1+\cdots+Ra_n=\{r_1a_1+\cdots r_na_n:r_1,\cdots,r_n\in R\} \tag{2.75}$$

证明 显然有限生成的理想是主理想的特例，故我们只须证明第二个等式。

要证明 $(A)=I$，我们只须证明两点。一，I 是包含 A 的理想；二，每一个理想包含 A 的理想都会包含 A。

首先，要证明 $Ra_1+\cdots+Ra_n$ 是个理想。对加法而言，$0=0a_1+\cdots+0a_n\in Ra_1+\cdots+Ra_n$，而且对 $r_1a_1+\cdots+r_na_n,s_1a_1+\cdots+s_na_n(r_i,s_i\in R)$，我们有

$$(r_1a_1+\cdots+r_na_n)-(s_1a_1+\cdots+s_na_n)=(r_1-s_1)a_1+\cdots(r_n-s_n)a_n\in Ra_1+\cdots+Ra_n \tag{2.76}$$

因此 $Ra_1+\cdots+Ra_n$ 对加法构成子群。

接下来，因为 R 是交换环，我们只须证明 $R(Ra_1+\cdots+Ra_n)\subset(Ra_1+\cdots+Ra_n)$。而这是因为

$$R(Ra_1+\cdots+Ra_n)=RRa_1+\cdots RRa_n=Ra_1+\cdots+Ra_n \tag{2.77}$$

这样，我们就证明了 $Ra_1+\cdots+Ra_n$ 是个理想，而且显然包含 $\{a_1,\cdots,a_n\}$。

另一方面，若 I 是一个包含了 $a_1,\cdots,a_n$ 的理想，那么根据加法的封闭性及乘法的“吸收”性，

$$I\supset Ra_1+\cdots+Ra_n \tag{2.78}$$

综上所述，这就证明了这个命题。

理想可以定义加法。

定义 2.15

令 $(R,+,\cdot)$ 是一个环，而 $I,J \lhd R$，则

$$I+J=\{a+b:a\in I,b\in J\} \tag{2.79}$$

命题 2.15

令 $(R,+,\cdot)$ 是一个环，而 $I,J \lhd R$，则 $I+J$ 还是个理想，即

$$I+J \lhd R \tag{2.80}$$

证明 加法子群的部分是显然的。我们只须证明乘法的“吸收”性。

$$R(I+J)=RI+RJ\subset I+J \tag{2.81}$$

$$(I+J)R=IR+JR\subset I+J \tag{2.82}$$

这就证明了

$$I+J \lhd R \tag{2.83}$$

事实上，理想的和，是由并所生成的理想。这个结论非常重要，未来我们会常常用到。

命题 2.16

令 $(R,+,\cdot)$ 是一个环，而 $I,J \lhd R$，则 $I+J$ 是由 $I\cup J$ 生成的理想，即

$$I+J=(I\cup J) \tag{2.84}$$

证明 首先，我们证明了 $I+J$ 是一个理想。而 $I+J\supset I+\{0\}=I$，同理 $I+J\supset J$，故 $I+J\supset I\cup J$。这就证明了 $I+J$ 是一个包含了 $I\cup J$ 的理想。

接着，如果 K 是包含了 $I\cup J$ 的理想，那么根据加法封闭性，我们当然有

$$K\supset I+J \tag{2.85}$$

综上所述，我们就证明了

$$I+J=(I\cup J) \tag{2.86}$$

在一个交换环中，我们可以简单地表示出两个理想的乘积。注意，为了理想乘积的计算方便，我们并没有定义为元素乘积的集合，而是定义为前者所生成的理想。根据下面的命题，这个理想就是由交换环中元素乘积的有限和所构成的集合。这个定义迫使了理想的乘积还是一个理想，进而可以得到一系列简洁的结论。为了未来不引起歧义，除非特别指明，否则我们每次在交换环中引用理想的乘积，就是在表示由集合乘积所生成的那个理想。

定义 2.16

令 $(R,+,\cdot)$ 是一个交换环，而 $I,J \lhd R$，则

$$IJ=(\{ab:a\in I,b\in J\}) \tag{2.87}$$

上面的圆括号表示生成的理想。

命题 2.17

令 $(R,+,\cdot)$ 是一个交换环，而 $I,J \lhd R$，则

$$IJ=\{a_1b_1+\cdots+a_nb_n:a_1,\cdots,a_n\in I,b_1,\cdots,b_n\in J\} \tag{2.88}$$

证明

首先，如果 K 是交换环 R 中包含了 $\{ab : a \in I, b \in J\}$ 的理想，则根据加法的封闭性，

$$K \supset \{a_1b_1 + \cdots + a_nb_n : a_1, \cdots, a_n \in I, b_1, \cdots, b_n \in J\} \tag{2.89}$$

接着，我们要证明 IJ 确实是包含了 $\{ab : a \in I, b \in J\}$ 的一个理想。包含关系是显然的，这就是有限和中只有一项的特例。

我们先证明加法是子群。$0 = 00 + \cdots + 00$，而且对于 $a_1b_1 + \cdots a_nb_n, c_1d_1 + \cdots + c_md_m \in IJ$，我们有

$$(a_1b_1 + \cdots a_nb_n) - (c_1d_1 + \cdots + c_md_m) = a_1b_1 + \cdots a_nb_n + (-c_1)d_1 + \cdots + (-c_m)d_m \in IJ \tag{2.90}$$

我们再证明乘法的“吸收性”。令 $a_1b_1 + \cdots a_nb_n \in IJ$，而 $r \in R$，则 $ra_i \in I$，不妨令 $a_i' = ra_i \in I$，则

$$r(a_1b_1 + \cdots a_nb_n) = ra_1b_1 + \cdots ra_nb_n = a_1'b_1 + \cdots a_n'b_n \in IJ \tag{2.91}$$

综上所述，由交换环中的两个理想 I，J 的乘积所生成的理想，就是它们元素乘积的有限和所构成的集合。

我们来看上面这个命题。即便是在交换环中，理想的乘积也不是我们所希望的元素乘积构成的集合——原因在于加法未必封闭。在这样的情况下，我们略微修改一下，发现有限和便可以满足。未来我们也会看到类似的处理。

我们说了交换环中理想的加法和乘法，那么我们是否对这两个运算有一些简单的运算律呢？答案是肯定的。

命题 2.18

令 $(R, +, \cdot)$ 是一个交换环，而 $I, J, K \lhd R$，则

$$I + J = J + I \tag{2.92}$$

$$I + (J + K) = (I + J) + K \tag{2.93}$$

$$I(J + K) = IJ + IK \tag{2.94}$$

$$I(JK) = (IJ)K \tag{2.95}$$

$$I = RI = IR \tag{2.96}$$

证明 前两条是显然的。因为加法就是定义为集合元素的加法，利用前一章的知识就可以证明。

我们来证明第三条。一方面，$I(J + K) \supset I(J + \{0\}) = IJ$，同理 $I(J + K) \supset IK$，故 $I(J + K) \supset IJ + IK$。另一方面，令 $\sum_i (a_i(b_i + c_i)) \in I(J + K)$，则

$$\sum_i (a_i(b_i + c_i)) = \sum_i (a_ib_i) + \sum_i (a_ic_i) \in IJ + IK \tag{2.97}$$

因此 $I(J + K) \subset IJ + IK$。

我们来证明第四条。根据对称性，我们证明 $I(JK) \subset (IJ)K$。因为理想的乘积是有元素乘积的集合所生成的，故只须证明 $\{ad : a \in I, d \in JK\} \subset (IJ)K$。

令 $a \in I$，$d = \sum_i (b_ic_i) \in JK$。则

$$ab = a\sum_i (b_ic_i) = \sum_i ((ab_i)c_i) \tag{2.98}$$

其中 $ab_i \in IJ$，故 $ab \in (IJ)K$。这就证明了第四条。

第五条根据对称性或交换性，我们只证明 $I = RI$。一方面，根据理想的定义，$I \supset RI$。另一方面，$I = 1I \subset RI$，因为 $1 \in R$。

综上所述，我们证明了这个命题。

我们之前也证明过，理想的交集仍是理想。我们用下一个引理来刻画理想的交，和，与乘积之间的大小关系。

引理 2.5

令 $(R,+,\cdot)$ 是一个交换环，而 $I,J \lhd R$，则

$$IJ \subset I \cap J \subset I + J \tag{2.99}$$

♡

证明 证明是简单的。因为 R 是一个交换环，而 I 是一个理想，故

$$IJ \subset IR = I \tag{2.100}$$

对 J 是类似的，故

$$IJ \subset I \cap J \tag{2.101}$$

另外，$I \cap J \subset I$，而且 $I \cap \subset J$，故

$$I \cap J \subset (I \cup J) = I + J \tag{2.102}$$

这就证明了这个引理。

注意到，这个引理告诉我们理想的乘积是非常小的，甚至比交集还小。而理想的和，作为理想并集所生成的理想，则是非常大的。我们再补充一个引理。

引理 2.6

令 $(R,+,\cdot)$ 是一个交换环，而 $I,J \lhd R$，则

$$(I \cap J)(I + J) \subset IJ \tag{2.103}$$

♡

证明 证明是不难的。令 $a_i(b_i + c_i) \in (I \cap J)(I + J)$，其中 $a_i \in I \cap J, b_i \in I, c_i \in J$，则

$$\sum_i (a_i(b_i + c_i)) = \sum_i (a_i b_i) + \sum_i (a_i c_i) \subset JI + IJ = IJ + IJ = IJ \tag{2.104}$$

倒数第二步是根据交换环对乘法的交换律，最后一步是根据理想的乘积对加法的封闭性。这就证明了这个命题。

我们再举一个理想的交与和之间的关系。

命题 2.19

令 $(R,+,\cdot)$ 是一个交换环，而 $I,J,K \lhd R$，则

$$I \cap (J + K) \supset I \cap J + I \cap K \tag{2.105}$$

特别地，如果 $J \subset K$，则

$$I \cap (J + K) = I \cap J + I \cap K \tag{2.106}$$

♠

证明 因为 $I \cap (J + K) \supset I \cap J$，且 $I \cap (J + K) \supset I \cap K$，所以

$$I \cap (J + K) \supset I \cap J + I \cap K \tag{2.107}$$

这就证明了第一点。

接下来，我们假设 $J \subset K$。我们只须证明

$$I \cap (J + K) \subset I \cap J + I \cap K \tag{2.108}$$

而这是因为

$$I \cap (J + K) \subset I \cap (K + K) = I \cap K \subset I \cap J + I \cap K \tag{2.109}$$

这就证明了这个命题。

我们下面定义交换环中互素的理想。

定义 2.17

令 $(R,+,\cdot)$ 是一个交换环，而 $I,J\lhd R$。我们称 I，J 互素，若其和为整个环，即

$$I+J=R \tag{2.110}$$

命题 2.20

令 $(R,+,\cdot)$ 是一个交换环，而 $I,J\lhd R$。则 I，J 互素，当且仅当

$$\exists a\in I,\exists b\in J,a+b=1 \tag{2.111}$$

证明 一方面，若 $I+J=R$，则 $1\in R=I+J$，故我们能找到 $a\in I$，$b\in J$，使得 $a+b=1$。

另一方面，假设 $a+b=1(a\in I,b\in J)$，则对任何 $r\in R$，

$$r=r1=r(a+b)=ra+rb\in RI+RJ=I+J \tag{2.112}$$

这就证明了 $I+J=R$。

综上所述，两个理想互素当且仅当 1 可以写成这两个理想中元素的和。

命题 2.21

令 $(R,+,\cdot)$ 是一个交换环，而 $I,J\lhd R$ 互素，则

$$IJ=I\cap J \tag{2.113}$$

证明 我们刚才已经证明了

$$IJ\subset I\cap J \tag{2.114}$$

故只须证明

$$I\cap J\subset IJ \tag{2.115}$$

而这是因为根据上面的引理，

$$I\cap J=(I\cap J)R=(I\cap J)(I+J)\subset IJ \tag{2.116}$$

这就证明了这个命题。

我们还能结合理想与环同态。很自然地可以问，在一个同态下，理想的像是不是理想，理想的原像是不是理想。前一个是否定的（因为陪集可以很大），后一个是肯定的。我们来证明后一个结论。在后续的课程中，我们会看到更多关于理想的原像，以及理想的像所生成的理想相关的讨论。囿于篇幅，我们只证明一个小命题。

命题 2.22

令 $(R,+,\cdot)$ 和 $(R',+,\cdot)$ 是两个交换环，令 $f:(R,+,\cdot)\to(R',+,\cdot)$ 是一个环同态，而 $I'\lhd R'$，则 $f^{-1}(I')\lhd R$。

证明 就加法子群而言，一个是 $0=f^{-1}(0)\in R$，另一个是若 $a=f^{-1}(a'),b=f^{-1}(b')\in f^{-1}(I)$，则

$$a-b=f^{-1}(a'-b')\in f^{-1}(R) \tag{2.117}$$

就乘法的“吸收”性来说。我们只须证明 $Rf^{-1}(I')\subset f^{-1}(I')$，而这是因为

$$Rf^{-1}(I')\subset f^{-1}(R')f^{-1}(I')=f^{-1}(R'I')=f^{-1}(I') \tag{2.118}$$

这样，我们就证明了这个命题，即交换环中，理想在环同态下的原像还是理想。

2.4 素理想与极大理想

为了不把所有理想相关的内容放在同一节，我们在适当的时候分出一节来，以讨论素理想与极大理想的名义，将其它一些有关理想本身的重要定义、结论放在这一节中讲。类似的处理方法我们在第一章的“有限群”一

节中也见过。为了将纷乱的定义和结论有机地结合起来，对初学者更友好，以一种讲故事的方法智慧地串联知识，希望大家可以理解这种编排知识的方式。同样地，虽然叫素理想与极大理想，但范围远远不止这两个概念。

我们先定义整环。

注意到在整数环 $(\mathbb{Z},+,\cdot)$ 中，我们有

$$\forall a,b\in\mathbb{Z},(ab=0\implies a=0\text{或}b=0) \tag{2.119}$$

可是在 $(\mathbb{Z}_6,+,\cdot)$ 中

$$2\cdot 3=0 \tag{2.120}$$

或者严谨地说，

$$(2+6\mathbb{Z})(3+6\mathbb{Z})=0+6\mathbb{Z} \tag{2.121}$$

这个重要的区别给出了一个定义，我们称满足上面这条性质的非零交换环为整环。

定义 2.18

令 $(R,+,\cdot)$ 是一个环，则我们称 R 是个整环，若它是个非零交换环，且没有零因子，即

$$R\neq\{0\} \tag{2.122}$$

$$R\text{是个交换环。} \tag{2.123}$$

$$\forall a,b\in R,(ab=0\implies a=0\text{或}b=0) \tag{2.124}$$

若 $a\neq 0$ 满足 $\exists b\neq 0$ 使得 $ab=0$，我们就称其为一个零因子。

♣

注意到在环 $\mathbb{Z}_6$ 中，2 和 3 就是零因子。（严格地说是 $2+6\mathbb{Z}$ 和 $3+6\mathbb{Z}$，为了方便我们简称为 2 和 3）。

什么是素理想呢？我们来看整数环上的例子。

根据初等数论，我们知道

引理 2.7

若 p 是一个素数，$a,b\in\mathbb{Z}$，则

$$p|ab\iff p|a\text{或}p|b \tag{2.125}$$

♡

注意到这个命题对于合数 n 是错的，即

引理 2.8

若 n 是一个合数，则存在 $a,b\in\mathbb{Z}$，使得

$$n|ab \tag{2.126}$$

$$n\nmid a \tag{2.127}$$

$$n\nmid b \tag{2.128}$$

♡

证明 证明是简单的。若 n 是一个合数，我们可以取一个非平凡分解 $n=ab$，其中 $a,b\neq\pm1$。则 $n|ab$，可是 $|n|>|a|$，故 $n\nmid a$（因为若一个数整除另一个数，则这个数的绝对值必须小于等于另一个数）。同理 $n\nmid b$。这样，我们就证明了这个引理。

根据上面这两个引理，我们就知道了，在整数中，这个性质是只对素数成立的。实际上，如果我们用理想来看，这个性质也可以改为

$$\forall a,b\in\mathbb{Z},(ab\in p\mathbb{Z}\iff a\in p\mathbb{Z}\text{或}b\in p\mathbb{Z}) \tag{2.129}$$

因此，在一般的交换环中，我们定义素理想就是既满足这个性质（如果两个元素的乘积在理想中，则至少有一个元素在这个理想中），又不是整个环的理想。

定义 2.19

令 $(R,+,\cdot)$ 是一个交换环，而 $\mathfrak{p}\lhd R$，则我们称 $\mathfrak{p}$ 是个素理想，若

$$\forall a,b\in\mathbb{Z},(ab\in\mathfrak{p}\iff a\in\mathfrak{p}\text{或}b\in\mathfrak{p}) \tag{2.130}$$

$$\mathfrak{p}\neq R \tag{2.131}$$

♣

对代数结构敏感的同学可能已经注意到了素理想和整环之间的微妙联系。事实上，我们通过一个命题来将谜底揭开。

命题 2.23

令 $(R,+,\cdot)$ 是一个交换环，而 $\mathfrak{p}\lhd R$。则 $\mathfrak{p}$ 是一个素理想，当且仅当商环 $R/\mathfrak{p}$ 是一个整环。

♠

证明 先证充分性。令 $\mathfrak{p}$ 是一个素理想。因为 R 是交换环，则显然 $R/\mathfrak{p}$ 也是交换环。因为对 $a,b\in R$，我们有

$$(a+\mathfrak{p})(b+\mathfrak{p})=ab+\mathfrak{p}=ba+\mathfrak{p}=(b+\mathfrak{p})(a+\mathfrak{p}) \tag{2.132}$$

而且因为 $\mathfrak{p}\neq R$，所以 $R/\mathfrak{p}$ 不是零环。

我们只须证明 $R/\mathfrak{p}$ 中没有零因子。假设

$$(a+\mathfrak{p})(b+\mathfrak{p})=0+\mathfrak{p} \tag{2.133}$$

则 $ab\in\mathfrak{p}$。根据 $\mathfrak{p}$ 是素理想，不失一般性假设 $a\in\mathfrak{p}$。则

$$a+\mathfrak{p}=0+\mathfrak{p} \tag{2.134}$$

这就证明了 $R/\mathfrak{p}$ 是一个整环。

再证必要性。假设 $R/\mathfrak{p}$ 是一个整环。类似地，我们知道因为 $R/\mathfrak{p}$ 不是零环，所以 $\mathfrak{p}\neq R$。

再令 $a,b\in R$，使得 $ab\in\mathfrak{p}$，则

$$ab+\mathfrak{p}=(a+\mathfrak{p})(b+\mathfrak{p})=0+\mathfrak{p} \tag{2.135}$$

由于 $R/\mathfrak{p}$ 是一个整环，故不失一般性假设 $a+\mathfrak{p}=0+\mathfrak{p}$，这就证明了 $a\in\mathfrak{p}$，即 $\mathfrak{p}$ 是一个素理想。

讲了素理想，我们来讲极大理想。

定义 2.20

令 $(R,+,\cdot)$ 是一个交换环，而 $\mathfrak{m}\lhd R$。则我们称 $\mathfrak{m}$ 是一个极大理想，若 $\mathfrak{m}\neq R$，且它是个极大的理想，即对于任意 $I\lhd R$，如果 $I\supsetneq\mathfrak{m}$，则

$$I=R \tag{2.136}$$

这就是说，唯一严格大于 $\mathfrak{m}$ 的理想，是整个环。

♣

实际上，正如素理想的充要条件，我们也有极大理想的充要条件。

命题 2.24

令 $(R,+,\cdot)$ 是一个交换环，而 $\mathfrak{m}\lhd R$。则 $\mathfrak{m}$ 是一个极大理想，当且仅当商环 $R/\mathfrak{m}$ 是一个域。

♠

证明 先证充分性。令 $\mathfrak{m}$ 是一个极大理想。因为 $R/\mathfrak{m}$ 是交换环，我们只须证明每个非零元素都有逆元。令 $a+\mathfrak{m}\in R/\mathfrak{m}(a+\mathfrak{m}\neq 0+\mathfrak{m})$，也就是说 $a\notin\mathfrak{m}$。只须证明存在 $b+\mathfrak{m}\in R/\mathfrak{m}(b\in R)$，使得 $ab+\mathfrak{m}=1+\mathfrak{m}$。

等价地，我们只须证明存在 $b\in R,m\in\mathfrak{m}$，使得

$$1=ab+m \tag{2.137}$$

考虑到 $a\in\mathfrak{m}$，所以 $\mathfrak{m}+Ra=(\mathfrak{m},a)$，是一个严格包含了 $\mathfrak{m}$ 的理想。因为 $\mathfrak{m}$ 是极大理想，所以 $\mathfrak{m}+Ra=R$。右边取 $1\in R$，我们就得到了，存在 $b\in R$，使得 $1=ab+m$，这就证明了充分性。

再证必要性。如果 $R/\mathfrak{m}$ 是一个域，那么对于假设理想 $I\supsetneq\mathfrak{m}$。任取 $a\in I\setminus\mathfrak{m}$。则 $a+\mathfrak{m}\neq 0+\mathfrak{m}$，故存在

$b \in R$，使得 $ab + \mathfrak{m} = 1 + \mathfrak{m}$。因此，也存在 $m \in \mathfrak{m}$，使 $1 = ab + m$。

因此，对任意 $r \in R$，我们都有

$$r = r(ab + m) = rab + rm \in Ib + \mathfrak{m} \subset I + I = I \tag{2.138}$$

这就证明了 $I = R$。因此 $\mathfrak{m}$ 是一个极大理想。

综上所述，我们就证明了这个命题。

我们想要证明每一个极大理想都是素理想。一个便捷的方法是证明每一个域都是整环。

引理 2.9

令 $(R, +, \cdot)$ 是一个域，则 R 是一个整环。

♡

证明 一个域当然是一个交换环。令 $a, b \in R$，使 $ab = 0$。我们只须证明 $a = 0$ 或 $b = 0$。

假设 $a \neq 0, b \neq 0$，而 $ab = 0$。我们取 $c, d \in R$，使 $ac = bd = 1$。则

$$1 = 11 = acbd = abcd = 0cd = 0 \tag{2.139}$$

于是 $R = \{0\}$。这和我们假设的存在 $a \neq 0$ 是矛盾的。因此每一个域都是整环。

利用这个引理，我们就得到下面的推论。

命题 2.25

令 $(R, +, \cdot)$ 是一个交换环，则每一个极大理想都是素理想。

♠

证明 [证法 1] 令 $\mathfrak{m}$ 是一个极大理想，则 $R/\mathfrak{m}$ 是一个域。根据上面的引理，$R/\mathfrak{m}$ 是一个整环，而这就告诉我们 $\mathfrak{m}$ 是一个素理想。这就证明了这个命题。[证法 2]

令 $\mathfrak{m}$ 是一个极大理想。假设 $a, b \in R$，使得 $ab \in \mathfrak{m}$，我们只须证明 $a \in \mathfrak{m}$ 或 $b \in \mathfrak{m}$。用反证法，假设 $a, b \notin \mathfrak{m}$。则 $\mathfrak{m} + Ra$ 是一个严格包含 $\mathfrak{m}$ 的理想。因为 $\mathfrak{m}$ 是极大理想，这就迫使

$$R = \mathfrak{m} + Ra \tag{2.140}$$

于是存在 $m \in \mathfrak{m}$ 与 $r \in R$，使

$$1 = m + ra \tag{2.141}$$

则由于 $ab \in \mathfrak{m}$，我们有

$$b = bm + r(ab) \in \mathfrak{m} + r\mathfrak{m} \subset \mathfrak{m} + \mathfrak{m} = \mathfrak{m} \tag{2.142}$$

可是这与 $b \notin \mathfrak{m}$ 相矛盾。

因此，$\mathfrak{m}$ 是一个素理想。

接下来，我们把重心转移到中国剩余定理。这个以“中国”命名的定理到今天仍然重要。

我们首先定义在一个交换环中模一个理想的同余。

定义 2.21

令 $(R, +, \cdot)$ 是一个交换环，而 $I \lhd R$。令 $a, b \in R$，我们称 a, b 模 I 同余，记作

$$a \equiv b \bmod I \tag{2.143}$$

若它们的差在 I 中，即

$$a - b \in I \tag{2.144}$$

或等价地，

$$a + I = b + I \tag{2.145}$$

♣

则利用商环的性质，我们知道

命题 2.26

令 $(R,+,\cdot)$ 是一个交换环，而 $I \lhd R$。假设 $n \in \mathbb{N}_1$。令 $a,b,c,d \in R$，假设

$$a \equiv b \bmod I \tag{2.146}$$

$$c \equiv d \bmod I \tag{2.147}$$

则

$$a+c \equiv b+d \bmod I \tag{2.148}$$

$$ac \equiv bd \bmod I \tag{2.149}$$

$$a^n \equiv b^n \bmod I \tag{2.150}$$

♠

证明 根据商环的性质，这是显然的。

接着，我们来陈述并证明中国剩余定理。

命题 2.27 (中国剩余定理)

令 $(R,+,\cdot)$ 是一个交换环，而 $(I_i)_{1\leqslant i\leqslant n}$ 是一族两两互素的理想，即对任何 $i \neq j$ 都有 $I_i + I_j = R$。则对任何 $a_1,\cdot,a_n \in R$，我们可以找到 $x \in R$，使

$$x \equiv a_1 \bmod I_1 \tag{2.151}$$

$$\cdots \tag{2.152}$$

$$x \equiv a_n \bmod I_n \tag{2.153}$$

♠

证明 令 $a = (a_1,\cdots,a_n)$，则

$$a = a_1(1,0,\cdots,0) + \cdots + a_n(0,\cdots,0,1) \tag{2.154}$$

假如 $x_i (1 \leqslant i \leqslant n)$ 分别满足

$$x_i \equiv 1 \bmod I_i \tag{2.155}$$

$$若 j \neq i,\quad x_i \equiv 0 \bmod I_j \tag{2.156}$$

则根据上面的命题，$x = a_1x_1 + \cdots + a_nx_n$ 就一定满足了同余方程组

$$x \equiv a_1 \bmod I_1 \tag{2.157}$$

$$\cdots \tag{2.158}$$

$$x \equiv a_n \bmod I_n \tag{2.159}$$

因此我们只须证明对任何 $1 \leqslant i \leqslant n$，我们能找到 $x_i \in R$，使得

$$x_i \equiv 1 \bmod I_i \tag{2.160}$$

$$若 j \neq i,\quad x_i \equiv 0 \bmod I_j \tag{2.161}$$

不失一般性，我们假设 $i = 1$。由于 I_1 与 $I_j (j \neq 1)$ 都互素，则存在 $b_j \in I_1, c_j \in I_j (j \neq 1)$，使得

$$b_2 + c_2 = 1 \tag{2.162}$$

$$\cdots \tag{2.163}$$

$$b_n + c_n = 1 \tag{2.164}$$

令 $x_1 = c_2 \cdots c_n \in R$。则对任何 $j \neq 1$，我们有

$$x_1 \equiv c_2 \cdots c_j \cdots c_n \equiv 0 \bmod I_j \tag{2.165}$$

并且

$$1 - c_2 \cdots c_n = (b_2 + c_2) \cdots (b_n + c_n) - (c_2 \cdots c_n) \tag{2.166}$$

根据分配律，上面的每一项都包含至少某个 $b_i \in I_1$ 作为因子，因此

$$1 - c_2 \cdots c_n \in I_1 \tag{2.167}$$

于是

$$x_1 = c_2 \cdots c_n \equiv 1 \bmod I_1 \tag{2.168}$$

这就完成了 x_1 的构造。类似地，我们可以构造出所有的 $x_i (1 \leqslant i \leqslant n)$，因此

$$x \equiv a_1 x_1 + \cdots + a_n x_n \tag{2.169}$$

给出了原命题所需的解。

综上所述，我们通过线性性对原同余方程组进行了化简，并不失一般性地证明了 $i = 1$ 的情形，这就完成了中国剩余定理的证明。

事实上，我们有以下的推论，也可以叫做中国剩余定理，因为它们是等价的。

命题 2.28

令 $(R, +, \cdot)$ 是一个交换环，而 $(I_i)_{1 \leqslant i \leqslant n}$ 是一族两两互素的理想，即对任何 $i \neq j$ 都有 $I_i + I_j = R$。则

$$\pi : R \to \prod_{i=1}^{n} (R/I_i) \tag{2.170}$$

$$\pi(a) = (a + I_1, \cdots, a + I_n) \tag{2.171}$$

是个满同态。

特别地，

$$R \Big/ \bigcap_{i=1}^{n} I_i \simeq \prod_{i=1}^{n} (R/I_i) \tag{2.172}$$

因此在以上的条件下，π 是个同构当且仅当

$$\bigcap_{i=1}^{n} I_i = \{0\} \tag{2.173}$$

证明 π 的每一个坐标都是环同态，因此 π 也是环同态。上面的中国剩余定理证明的就是 π 是个满同态。

我们只须找到 π 的核即可。根据 π 的定义，

$$\pi(a) = 0 \iff \forall i, a + I_i = 0 + I_i \tag{2.174}$$

$$\iff \forall i, a \in I_i \tag{2.175}$$

$$\iff a \in \bigcap_{i=1}^{n} I_i \tag{2.176}$$

根据环同态第一定理，这就证明了

$$R \Big/ \bigcap_{i=1}^{n} I_i \simeq \prod_{i=1}^{n} (R/I_i) \tag{2.177}$$

因此在以上的条件下，π 是同构当且仅当 π 是单的，当且仅当 $\ker(\pi) = \{0\}$，当且仅当

$$\bigcap_{i=1}^{n} I_i = \{0\} \tag{2.178}$$

因此，最特殊的情况即 R 中有有限多个两两互素且总的交集为 $\{0\}$ 的理想。在这种情况下，

$$R \simeq \prod_{i=1}^{n} (R/I_i) \tag{2.179}$$

综上所述，我们证明了这个命题。

2.5 环的局部化

接着讲理想似乎有些枯燥。我们换个新鲜而有趣的话题——环的局部化。什么是局部化呢?

我们用一句话来做引子：请问整数是怎么变成有理数的?

这个问题，越是数学的新手越觉得简单。其实，这背后是有奥秘的。我们无论怎样定义出无限循环阿贝尔群——整数群，无论怎样定义上面的乘法使其成为我们熟知的整数环，都不能简单地说有理数的结构是自然得到的。其实，有理数的定义就是比值的形式，而我们一定要模掉一些等价关系，例如

$$\frac{2}{4} \sim \frac{1}{2} \tag{2.180}$$

我们马上就知道，因为整数环是个整环，因此用某种方法定义出来的结构是个美妙的域（在整数环的例子中，给出的就是有理数域）。而一般地，对于交换环，我们也能构造出一个由分数的等价类（或在不引起歧义的情况下简化为分数）构成的环。

我们要问三个问题。分子是谁? 分母是谁? 分数的等价关系怎么定义? 下面，我们来通过定义和命题来回答这三个问题。

第一个问题，分子是谁? 一般来说，任何一个交换环自身都可以（非交换环的结构太差，很多概念都不方便定义）。

第二个问题，分母是谁? 我们当然希望分母可以是 1，这样可以使

$$r = \frac{r}{1} \tag{2.181}$$

我们当然也希望分母在乘法下封闭，这样才能有

$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} \tag{2.182}$$

而满足这两个条件就可以了——我们要求的不多。事实上，满足这两个条件的，根据第一章第一节所说的，不就是 $(R \setminus \{0\}, \cdot)$ 的子幺半群吗? 在这里，我们称其为乘法子集。

定义 2.22

令 $(R, +, \cdot)$ 是一个交换环，而 $S \subset R$。则我们称 S 是一个乘法子集，若 S 是 $(R \setminus \{0\}, \cdot)$ 的（乘法）子幺半群，即

$$1 \in S \tag{2.183}$$

$$\forall a, b \in S, ab \in S \tag{2.184}$$

♣

第三个问题，什么时候两个分数等价? 假设乘法子集是 S，我们或许希望

$$\frac{a}{b} \sim \frac{c}{d} \iff ad - bc = 0 \tag{2.185}$$

可是上面的式子一般来说不是一个等价关系，因为若 $a/b = c/d$，且 $c/d = e/f$，我们就只能得到 $ad = bd$，且 $cf = de$，可是从环的结构来说，我们完全不能说明 $af = be$。因此一般来说，我们修改定义，变成

$$\frac{a}{b} \sim \frac{c}{d} \iff \exists s \in S, s(ad - bc) = 0 \tag{2.186}$$

下面，我们给出完整的定义。

定义 2.23

令 $(R,+,\cdot)$ 是一个交换环，而 S 是乘法子集。则 R 对 S 的局部化，记作 $(S^{-1}R,+,\cdot)$，定义为

$$S^{-1}R=\left\{\frac{r}{s}:r\in R,s\in S\right\}/\sim \tag{2.187}$$

其中

$$\frac{r}{s}\sim\frac{r'}{s'}\iff\exists t\in S,t(rs'-r's)=0 \tag{2.188}$$

若 $r,r'\in R,s,s'\in S$，我们定义

$$\frac{r}{s}+\frac{r'}{s'}=\frac{rs'+sr'}{ss'} \tag{2.189}$$

$$\frac{r}{s}\frac{r'}{s'}=\frac{rr'}{ss'} \tag{2.190}$$

♣

和商环的证明一样，我们把良定义性和环的性质一并放进下一个命题中来证。

命题 2.29

令 $(R,+,\cdot)$ 是一个交换环，而 S 是乘法子集。则 R 对 S 的局部化，即 $\left(S^{-1}R,+,\cdot\right)$，是个交换环。

♠

证明 我们先证明 $\sim$ 是个等价关系，再证明加法和乘法是良定义的，最后证明 $S^{-1}R$ 是个环。

第一，我们来证明 $\sim$ 是个等价关系。$r/s=r/s$ 是显然的，这是因为 $1(rs-rs)=0(1\in S)$。假设 $r/s\sim r'/s'$，则存在 $t\in S$，使得

$$t(rs'-r's)=0 \tag{2.191}$$

则

$$(-t)(r's-rs')=0 \tag{2.192}$$

故 $r'/s'=r/s$。最后，如果 $r/s\sim r'/s'$，$r'/s'\sim r''/s''$，只须证明 $r/s\sim r''/s''$。我们取 $t,t'\in S$，使

$$t(rs'-r's)=0 \tag{2.193}$$

$$t'(r's''-r''s')=0 \tag{2.194}$$

则我们可以通过不断的尝试，凑出一个美妙的 $t''=tt's'$。于是 $t''(rs''-r''s)=0$，这是因为

$$(tt's')rs''=t's''(trs')=t's''(tr's)=ts(t'r's'')=ts(t'r''s')=(tt's')r''s \tag{2.195}$$

由于 S 是乘法子群，故 $t''=tt's'\in S$。接下来，即使局部化中的每个元素实际上是等价类，我们还是为了方便起见，用等于号来代替所有的等价号。

第二，我们来证明加法和乘法是良定义的。假设

$$\frac{r_1}{s_1}\sim\frac{r_1'}{s_1'} \tag{2.196}$$

$$\frac{r_2}{s_2}\sim\frac{r_2'}{s_2'} \tag{2.197}$$

故存在 $t,t'\in S$，使得

$$t(r_1s_1'-r_1's_1)=0 \tag{2.198}$$

$$t'(r_2s_2'-r_2's_2)=0 \tag{2.199}$$

我们只须证明

$$\frac{r_1}{s_1}+\frac{r_2}{s_2}=\frac{r_1s_2+r_2s_1}{s_1s_2}\sim\frac{r_1's_2'+r_2's_1'}{s_1's_2'}=\frac{r_1'}{s_1'}+\frac{r_2'}{s_2'} \tag{2.200}$$

$$\frac{r_1}{s_1}\cdot\frac{r_2}{s_2}=\frac{r_1r_2}{s_1s_2}\sim\frac{r_1'r_2'}{s_1's_2'}=\frac{r_1'}{s_1'}\cdot\frac{r_2'}{s_2'} \tag{2.201}$$

根据重新分组，对于 $tt' \in S$，我们有

$$tt'\left((r_1s_2+r_2s_1)s_1's_2'-(r_1's_2'+r_2's_1')s_1s_2\right) \tag{2.202}$$

$$=tt'\left((r_1s_1'-r_1's_1)s_2s_2'+(r_2s_2'-r_2's_2)s_2s_1'\right) \tag{2.203}$$

$$=0+0=0 \tag{2.204}$$

根据拆项补项，同样对于 $tt' \in S$，我们有

$$tt'\left(r_1r_2s_1's_2'-r_1'r_2's_1s_2\right) \tag{2.205}$$

$$=tt'\left(r_1r_2s_1's_2'-r_1'r_2s_1s_2'\right)+tt'\left(r_1'r_2s_1s_2'-r_1'r_2's_1s_2\right) \tag{2.206}$$

$$=tt'\left(r_1s_1'-r_1's_1\right)r_2s_2'+tt'\left(r_2s_2'-r_2's_2\right)r_1's_1' \tag{2.207}$$

$$=0+0=0 \tag{2.208}$$

第三，我们来证明 $S^{-1}R$ 是个环。根据定义，加法和乘法的封闭性和交换律是显然的。而加法单位元是 $0/1$，乘法单位元是 $1/1$，因为对于任何 $r/s \in S^{-1}R$，我们有

$$\frac{0}{1}+\frac{r}{s}=\frac{0s+1r}{1s}=\frac{r}{s} \tag{2.209}$$

$$\frac{1}{1}\cdot\frac{r}{s}=\frac{1r}{1s}=\frac{r}{s} \tag{2.210}$$

乘法的结合律是显然的，而加法的结合律也很简单，我们很容易检验

$$\left(\frac{r_1}{s_1}+\frac{r_2}{s_2}\right)+\frac{r_3}{s_3}=\frac{r_1s_2s_3+s_1r_2s_3+s_1s_2r_3}{s_1s_2s_3}=\frac{r_1}{s_1}+\left(\frac{r_2}{s_2}+\frac{r_3}{s_3}\right) \tag{2.211}$$

加法的逆元也是显然的。r/s 的加法逆元当然是 $(-r)/s$。

最后，我们只须证明乘法对加法的分配律。令 $r_1/s_1, r_2/s_2, r_3/s_3 \in S^{-1}R$，则我们很容易检验

$$\frac{r_1}{s_1}\cdot\left(\frac{r_2}{s_2}+\frac{r_3}{s_3}\right)=\frac{r_1(r_2s_3+r_3s_2)}{s_1s_2s_3}=\frac{r_1r_2s_3}{s_1s_2s_3}+\frac{r_1r_3s_2}{s_1s_2s_3}=\frac{r_1}{s_1}\cdot\frac{r_2}{s_2}+\frac{r_1}{s_1}\cdot\frac{r_3}{s_3} \tag{2.212}$$

综上所述，我们就证明了 R 对 S 的局部化 $S^{-1}R$ 是个交换环。

在一般的交换环上的局部化似乎过于复杂。我们来看一个在整环上的简化版本。

命题 2.30

令 $(R,+,\cdot)$ 是一个整环，而 S 是一个乘法子集，则

$$\frac{a}{b}\sim\frac{c}{d} \iff ad-bc=0 \tag{2.213}$$

证明 先证必要性。假如 $ad-bc=0$，那么我们取 $s=1$，则 $1(ad-bc)=1\cdot 0=0$，这就证明了

$$\frac{a}{b}\sim\frac{c}{d} \tag{2.214}$$

再证充分性。假如 $a/b=c/d$，则存在 $s\in S$（于是 $s\neq 0$），使得 $s(ad-bc)=0$。可是因为 R 是个整环，而且 $s\neq 0$，所以 $ad-bc=0$。

这就证明了这个命题。

这个命题的意义在于，把我们熟知的分数相等的条件，在整环的情况下重新展示了一遍。

接下来，我们要讲一个重要的命题。那就是说，假如 R 是一个整环，而 $S=R\setminus\{0\}$，则 $S^{-1}R$ 是一个域，被称为 R 上的分式域。事实上，有理数域就是整数环的分式域。

定义 2.24

令 $(R,+,\cdot)$ 是一个整环，我们定义 R 上的分式域，记作 $\mathrm{Frac}(R)$，定义为 $S^{-1}(R)$，其中 $S=R\setminus\{0\}$。

命题 2.31

令 $(R,+,\cdot)$ 是一个整环，则 R 上的分式域 $\mathrm{Frac}(R)$ 是个域。

证明 令 $S = R \setminus \{0\}$。

我们已经证明了 $\mathrm{Frac}(R) = S^{-1}R$ 是个交换环，因此只须证明对任意非零元素

$$\frac{r}{s} \in S^{-1}R \tag{2.215}$$

我们都能找到逆元即可。

而这是因为由

$$\frac{r}{s} \neq 0 \tag{2.216}$$

我们可以得知 $r \neq 0$。

因此，

$$\frac{s}{r} \in S^{-1}R \tag{2.217}$$

而且

$$\frac{r}{s}\frac{s}{r} = \frac{s}{r}\frac{r}{s} = \frac{sr}{sr} = \frac{1}{1} = 1 \tag{2.218}$$

这就证明了 $\mathrm{Frac}(R)$ 是个域。

因此，在一个整环 R 中，每一个由乘法子集 S 给出的 $S^{-1}R$，都是 $\mathrm{Frac}(R)$ 的子环。

在实际应用中，乘法子集 S 除了是整个 $R \setminus \{0\}$，还有两种常见的可能。

第一种是由某个非零元素生成的子幺半群，即 $s \in R \setminus \{0\}$，而

$$S = \langle s \rangle = \{1, s, s^2, \cdots, \} \tag{2.219}$$

第二种是由某个素理想的补集得到的，即 $\mathfrak{p} \lhd R$ 是个素理想，而

$$S = R \setminus \mathfrak{p} \tag{2.220}$$

我们称这样的局部化为在素理想 $\mathfrak{p}$ 上的局部化。当然，我们需要一个引理来证明交换环中每一个素理想的补集都是乘法子集，这样才能使这个概念是良定义的。

引理 2.10

令 $(R, +, \cdot)$ 是一个交换环，而 $\mathfrak{p} \lhd R$ 是一个素理想，则 $S = R \setminus \mathfrak{p}$ 是一个乘法子集。 ♡

证明 首先，若 $1 \in \mathfrak{p}$，则 $\mathfrak{p} = R$，可是素理想根据定义是不能等于整个环的。因此 $1 \in S$。

接着，假设 $s_1, s_2 \in S$，我们只须证明 $s_1 s_2 \in S$。

因为 $s_1 \notin \mathfrak{p}$，$s_2 \notin \mathfrak{p}$，所以根据逆否命题，

$$s_1 s_2 \notin \mathfrak{p} \tag{2.221}$$

也就是说，

$$s_1 s_2 \in S \tag{2.222}$$

这就巧妙地证明了素理想的补集是一个乘法子集。

2.6 主理想整环与唯一分解整环

有一种性质非常好的整环，它的每一个理想都是主理想，即可以只由一个元素生成。我们称这样的整环为主理想整环。

定义 2.25

令 $(R, +, \cdot)$ 是一个交换环，则我们称 R 是个主理想整环，若 R 是一个整环，而且每一个理想 $I \lhd R$ 都是主理想，即可以写成

$$I = (a) = Ra \tag{2.223}$$

的形式。 ♣

主理想整环的性质非常好，但是当然没有域好。最常见的一个主理想整环就是整数环 $(\mathbb{Z},+,\cdot)$。

下面，我们来证明 $(\mathbb{Z},+,\cdot)$ 是个主理想整环。

命题 2.32

$(\mathbb{Z},+,\cdot)$ 是个主理想整环。 ♠

实际上，我们有更好的结论，即 $\mathbb{Z}$ 的某个（加法）子群都具有 $n\mathbb{Z}$ 的形式。

引理 2.11

$(\mathbb{Z},+,\cdot)$ 的每个子群都具有 $n\mathbb{Z}$ 的形式。 ♡

证明 不妨令 $I<\mathbb{Z}$ 是加法子群。

假如 I 只包含了 0 一个元素，那么 $I=\{0\}=0\mathbb{Z}$。

假设 I 包含了 0 以外的元素，那么根据逆元的封闭性，I 一定包含了一个正整数。根据自然数集的良序公理，我们可以取到最小的那个正整数，称其为 n。下面，我们只须证明

$$I=n\mathbb{Z} \tag{2.224}$$

一方面，因为 $n\in I$，则 n 生成的（加法）子群也包含于 I，而前者正是 $n\mathbb{Z}$，因此

$$n\mathbb{Z}\subset I \tag{2.225}$$

另一方面，假设存在 $I\setminus n\mathbb{Z}$ 的元素，我们任取 $m\in I\setminus n\mathbb{Z}$。则根据带余除法，我们有

$$m=qn+r \tag{2.226}$$

其中 $1\leqslant r\leqslant n-1$。

则根据子群的性质，

$$r=m-qn=m+(-q)n\in I \tag{2.227}$$

而这与 n 是 I 最小的正整数的事实相矛盾。这就证明了这个引理，进而证明了上面的命题，即 $(\mathbb{Z},+,\cdot)$ 是个主理想整环。

我们再做一个小练习，即每一个域都是主理想整环。

命题 2.33

若 $(R,+,\cdot)$ 是一个域，则 R 是一个主理想整环。 ♠

实际上，我们也有更好的结论，即每个域只有两个理想：零和自身。更妙的是，满足这个条件（只有零和自身两个理想）的环一定是域。

引理 2.12

若 $(R,+,\cdot)$ 是一个环，则 R 是一个域当且仅当 $\{0\}$ 和 R 是 R 中唯二的理想（$R\neq\{0\}$）。 ♡

证明 先证充分性。假设 R 是一个域，而 I 是一个理想。假设 $I\neq\{0\}$，任取 $a\neq 0$。则存在 $b\in R$，使得

$$ab=1 \tag{2.228}$$

因此

$$1\in Ra\subset RI\subset I \tag{2.229}$$

所以 $I=R$。

再证必要性。假设 R 唯二的理想是零和整个环。令 $a \neq 0$，则 $(a) \neq 0$，因此 $(a) = R$。于是存在 $b, c \in R$，使得

$$ab = 1 \in R \tag{2.230}$$

$$ca = 1 \tag{2.231}$$

下面我们只须证明 $b = c$，而证明方法和我们当时证明逆元是唯一时是一样的。

$$b = 1b = cab = c1 = c \tag{2.232}$$

这样，就证明了 R 是一个域。

还记得在交换环中，每一个极大理想都是素理想。我们要证明，在主理想整环中，每一个素理想也是极大理想。

命题 2.34

令 $(R, +, \cdot)$ 是一个主理想整环，而 $\mathfrak{p} \lhd R$ 是一个素理想，则 $\mathfrak{p}$ 是一个极大理想。

证明 用反证法。假设 $\mathfrak{p}$ 是素理想，而不是极大理想，则存在 $I \lhd R$，使得 $\mathfrak{p} \subsetneq I \neq R$。

因为 R 是主理想整环，我们记 $\mathfrak{p} = (p)$，$I = (a)$。则由于 $\mathfrak{p} \subset I$，我们有

$$p \in I = (a) \tag{2.233}$$

故存在 $b \in R$，使得

$$p = ab \tag{2.234}$$

显然，b 不能是单位（即存在乘法逆元的元素），因为不然的话我们就可以写 $a = pb^{-1}$，进而 $\mathfrak{p} = I$，导致矛盾。因此，b 没有乘法逆元。

另外，由于 I 是真理想，故 a 也不是单位——否则 $1 \in (a)$，进而 $(a) = R$。

现在 $ab \in \mathfrak{p}$，则 $a \in \mathfrak{p}$ 或 $b \in \mathfrak{p}$。假如 $a \in \mathfrak{p} = (p)$，则不难证明 b 就是一个单位，而这是不可能的。假如 $b \in \mathfrak{p}$，则同理，a 就是一个单位，而这也是不可能的。无论如何，我们都会得到矛盾。

因此，我们就证明了，在主理想整环中，每一个素理想都是极大理想，因此两个概念在主理想整环中是等价的。

命题 2.35

若 p 是一个素数，则 $\mathbb{Z}_p$ 是一个域。

命题 2.36

我们知道 $p\mathbb{Z} \lhd \mathbb{Z}$ 是个素理想，而 $\mathbb{Z}$ 是个主理想整环，因此 $p\mathbb{Z}$ 是 $\mathbb{Z}$ 的极大理想。根据之前的引理，这就证明了 $\mathbb{Z}_p$ 是一个域。

定义 2.26

若 p 是一个素数，则我们把 $\mathbb{Z}_p$ 记作 $\mathbb{F}_p$。特别地，这是一个有限域，即只有有限多个元素的域。

未来我们会知道，所有的有限域的阶都是素数的幂次，而恰好是具有素数的阶的有限域，就是这里的 $\mathbb{F}_p$。

同理，我们也可以通过整数环中素理想和极大理想的等价性证明

引理 2.13

若 n 是一个合数，则 $\mathbb{Z}_n$ 不是一个域。

证明 证明是类似的，故留做练习。

下面，我们慢慢地进入到唯一分解整环的环节。唯一分解整环依然是整环的一种，它的性质也很好，但是不如主理想整环好。未来我们会知道，每一个主理想整环都是唯一分解整环，而反之则不一定。

刚才证明素理想是极大理想的时候，我们注意到如果把一个交换环中的元素写成两个非单位的元素的乘积似乎是一个不平凡的条件（在反证法的过程中，我们的核心步骤是把 p 写成 $p=ab$，而 a,b 都不是单位）。在一个整环中，我们称这样的元素为可约的元素。反之，就称之为不可约的元素。

定义 2.27

令 $(R,+,\cdot)$ 是一个整环，而 $x\in R\setminus\{0\}$。我们称 x 是可约的，若存在两个非单位的元素 $a,b\in R$，使得

$$x=ab \tag{2.235}$$

反之，则称 x 是不可约的。此即，对于任意分解 $x=ab$，我们一定有 a 是一个单位或者 b 是一个单位。

在整数环 $\mathbb{Z}$ 中，可约的元素是（正负）合数。不可约的元素是（正负）素数和 ±1。

我们同样以整数环作比，在一个整环中，我们定义一个非零元素整除另一个元素，若后者是前者的倍数，即前者乘上某一个环中的元素。

定义 2.28

令 $(R,+,\cdot)$ 是一个整环，而 $a\neq0$，$b\in R$。我们称 a 整除 b，记作 $a|b$，若存在 $c\in R$，使得

$$b=ac \tag{2.236}$$

假如整环中的两个元素互相整除，我们就称它们等价。

定义 2.29

令 $(R,+,\cdot)$ 是一个整环，而 $a,b\neq0$。我们称 $a\sim b$，若 $a|b$ 且 $b|a$。

为了像在整数环中熟悉整除一样，我们借助下面的一些引理来熟悉整环中的整除关系。

引理 2.14

令 $(R,+,\cdot)$ 是一个整环，而 $a\neq0,b\in R$，则下列命题等价

$$a|b \tag{2.237}$$

$$(b)\subset(a) \tag{2.238}$$

举个例子，在整数环中 $2|6$，因此 $6\mathbb{Z}\subset2\mathbb{Z}$，即 6 的倍数都是 2 的倍数。在这里，我们要注意这个等价条件中 a 与 b 的顺序是反的。

证明 一方面，假设 $a|b$，故存在 $c\in R$，使得

$$b=ac \tag{2.239}$$

因此

$$(b)=Rb=Rac=Rca\subset Ra=(a) \tag{2.240}$$

另一方面，假设 $(b)\subset(a)$，则特别地，$b\in(a)$。故我们可以找到 $c\in R$，使得

$$b=ac \tag{2.241}$$

而这就证明了 $a|b$。

综上所述，我们就证明了这个引理。

引理 2.15

令 $(R,+,\cdot)$ 是一个整环，而 $a,b\neq 0$，则下列命题均等价。

$$a\sim b \tag{2.242}$$

$$(a)=(b) \tag{2.243}$$

$$a=ub,\text{ 其中 } u \text{ 是一个单位} \tag{2.244}$$

♡

证明 假设 $a,b\neq 0$ 都在整环 R 中。

第一，假设 $a\sim b$，则 $a|b$，$b|a$。根据上面的引理，我们就知道 $(a)\subset(b)$，而且 $(b)\subset(a)$，这就证明了 $(a)=(b)$。

第二，假设 $(a)=(b)$，则存在 $u,v\in R$，使得

$$a=ub \tag{2.245}$$

$$b=va \tag{2.246}$$

因此 $b=va=vub=uvb$，根据环的性质，我们有

$$b(uv-1)=0 \tag{2.247}$$

而根据整环的性质，上面的因子至少有一个是 0，而 $b\neq 0$，因此 $uv=1$。这就告诉我们 u,v 都是单位。特别地，u 是一个单位。

第三，假设 $a=ub$，其中 u 是一个单位，则我们取 $v\in R$，使得 $uv=1$，两边同时乘上 v，就得到了 $b=va$。因此，$a|b$ 而且 $b|a$。根据定义，我们就证明了

$$a\sim b \tag{2.248}$$

综上所述，我们证明了这个引理。

注意，我们要求 R 是整环的原因就在于要在上面的关键一步中分离出 $b=0$ 或者 $uv-1=0$。

我们在整数环中有最大公因数和最小公倍数，在主理想整环中，最大公因数和最小公倍数一定存在，至多差一个等价关系（指互相整除的等价）。

我们先定义最大公因数。

定义 2.30

令 $(R,+,\cdot)$ 是一个整环，而 $a,b\neq 0$。则我们称 d 是 a,b 的一个最大公因数，记作 $d=\gcd(a,b)$，若 d 整除了 a 与 b，并且对于任何整除了 a 与 b 的元素 e，我们都有 $d|e$（因为 d 是“最大”的公因数）。此即，

$$d|a\text{ 且 }d|b \tag{2.249}$$

$$\forall e\in R,(d|a\text{ 且 }d|b\implies e|d) \tag{2.250}$$

♣

要注意，我们没有说最大公因数（或最小公倍数）是唯一的，因此上面的 $d=\gcd(a,b)$ 中的等号只是形式的等号，它不满足传递性。下面我们会证明最大公因数（或最小公倍数）若存在，则彼此之间都是等价的。

类似地，我们定义最小公倍数。

定义 2.31

令 $(R,+,\cdot)$ 是一个整环，而 $a,b\neq 0$。则我们称 m 是 a,b 的一个最小公倍数，记作 $m=\operatorname{lcm}(a,b)$，若 a 与 b 都整除 m，并且对于任何被 a 与 b 整除的元素 n，我们都有 $m|n$（因为 m 是“最小”的公倍数）。此即，

$$a|m\text{ 且 }b|m \tag{2.251}$$

$$\forall n\in R,(a|n\text{ 且 }a|n\implies m|n) \tag{2.252}$$

♣

我们来证明，若最大公因数（或最小公倍数）若存在，则在等价关系下是唯一的。

引理 2.16

令 $(R,+,\cdot)$ 是一个整环，而 $a,b\neq 0$。假如 $d=\gcd(a,b)$，而 $d'=\gcd(a,b)$，则 $d\sim d'$。

类似地，假如 $m=\mathrm{lcm}(a,b)$，而 $m'=\mathrm{lcm}(a,b)$，则 $m\sim m'$。

♡

证明 我们证明最大公因数的部分。

假设 $a,b\neq 0$，而 d 与 d' 都是 a 与 b 的最大公因数，则它们都整除 a 和 b。因为它们都是“最大”的公因数，因此 $d|d'$，而且 $d'|d$。这就证明了 $d\sim d'$。

最小公倍数的部分是非常类似的，留做练习。

接着，我们是时候来证明一个有意义的命题，即最大公因数和最小公倍数在主理想整环中是存在的（对任意 $a,b\neq 0$）。

命题 2.37

令 $(R,+,\cdot)$ 是一个主理想整环，而 $a,b\neq 0$，则存在 $\gcd(a,b)$ 与 $\mathrm{lcm}(a,b)$。

♠

证明 假设 $a,b\neq 0$，则根据主理想整环的条件，我们可以找到 $d\in R$ 使得

$$(a)+(b)=(d) \tag{2.253}$$

这样，特别地，就能找到 $x,y\in R$，使得

$$ax+by=d \tag{2.254}$$

并且

$$(a)\subset(a)+(b)=(d) \tag{2.255}$$

因此

$$d|a \tag{2.256}$$

类似地，$d|b$。因此 d 是 a 与 b 的一个公因数。

另外，假设 e 也是 a 与 b 的一个公因数，则 $e|a$，$e|b$。我们记 $a=em$，$b=en$，则

$$d=ax+by=emx+eny=e(mx+ny) \tag{2.257}$$

因此 $e|d$。这就证明了 d 是 a 与 b 的最大公因数。

另外，要证明最小公倍数，我们去找 $(a)\cap(b)$。同理，根据主理想整环的条件，我们可以找到 $m\in R$ 使得

$$(a)\cap(b)=(m) \tag{2.258}$$

因此

$$(m)=(a)\cap(b)\subset(a) \tag{2.259}$$

即 $a|m$。同理 $a|m$。这就证明了 m 是一个公倍数。

假如 n 也是一个公倍数，则 $a|n$，$b|n$，这就得到了 $(n)\subset(a)\cap(b)=(m)$。这就证明了 $m|n$，即 m 是最小公倍数。

综上所述，我们证明了最大公因数和最小公倍数在主理想整环中是存在的。

实际上，我们有一个有趣的定义，即最大公因数整环。它指的就是那些对于非零的一对数都有最大公因数的整环。

定义 2.32

令 $(R,+,\cdot)$ 是一个整环，则我们称 R 是个最大公因数整环，若对于任何 $a,b\neq 0$，我们都能找到 $\gcd(a,b)\in R$。

♣

上面的命题就告诉我们，每一个主理想整环都是最大公因数整环。

命题 2.38

令 $(R,+,\cdot)$ 是一个主理想整环，则 R 是一个最大公因数整环。

有人可能会问，那为什么不定义最小公倍数整环呢？实际上，这两个定义将是等价的。我们利用一个整环中最大公因数和最小公倍数的关系（假如它们都存在）来回答这个问题。

注意到，在整数中，我们根据初等数论可以知道，两个数的最大公因数与最小公倍数的乘积，等于原本这两个数的乘积。而在整环中，最多差一个等价关系，即最多差一个单位。

命题 2.39

令 $(R,+,\cdot)$ 是一个整环，而 $a,b\neq 0$。则 $\gcd(a,b)$ 存在，当且仅当 $\operatorname{lcm}(a,b)$ 存在。假如有一个存在（或两个都存在），那么它们的乘积等价于原本元素的乘积，即

$$\gcd(a,b)\operatorname{lcm}(a,b)\sim ab \tag{2.260}$$

证明

首先，我们证明后半个命题，即，如果 $\gcd(a,b)$ 和 $\operatorname{lcm}(a,b)$ 都存在，那么

$$\gcd(a,b)\operatorname{lcm}(a,b)\sim ab \tag{2.261}$$

这里的证明和初等数论中的证明是一致的。为了照顾没有学过初等数论的读者，我们列出证明的重点。

我们先证明

$$\gcd(a,b)\operatorname{lcm}(a,b)\Big|ab \tag{2.262}$$

我们只须证明

$$\operatorname{lcm}(a,b)\Big|\frac{ab}{\gcd(a,b)} \tag{2.263}$$

注意，我们可以写出右边的分数，是因为 $\gcd(a,b)$ 整除 a（或 b），故整除 ab。

而根据最小公倍数的性质，我们只须证明

$$a\Big|\frac{ab}{\gcd(a,b)} \tag{2.264}$$

$$b\Big|\frac{ab}{\gcd(a,b)} \tag{2.265}$$

而这是因为

$$a\Big|a\cdot\frac{b}{\gcd(a,b)}=\frac{ab}{\gcd(a,b)} \tag{2.266}$$

b 的条件是类似的。因此，我们证明了一边。

另一边等价于

$$\frac{ab}{\operatorname{lcm}(a,b)}\Big|\gcd(a,b) \tag{2.267}$$

注意，我们可以写出左边的分数，是因为 ab 也是 a 和 b 的公倍数，因此是 $\operatorname{lcm}(a,b)$ 的倍数。

根据最大公因数的性质，我们只须证明

$$\frac{ab}{\operatorname{lcm}(a,b)}\Big|a \tag{2.268}$$

$$\frac{ab}{\operatorname{lcm}(a,b)}\Big|b \tag{2.269}$$

$$\tag{2.270}$$

而这是因为，根据 $b|\operatorname{lcm}(a,b)$，我们有

$$a=\frac{ab}{\operatorname{lcm}(a,b)}\frac{\operatorname{lcm}(a,b)}{b} \tag{2.271}$$

b 的条件是类似的。这样，我们就证明了另一边。我们就证明了后半个命题。

接下来，我们来证明前半个命题。即 $\gcd(a,b)$ 存在，当且仅当 $\mathrm{lcm}(a,b)$ 存在。

首先假设 $\gcd(a,b)$ 存在。根据后半个命题的暗示（明示），我们只须证明

$$\frac{ab}{\gcd(a,b)} = \mathrm{lcm}(a,b) \tag{2.272}$$

上面的证明过程中有可以再次使用的结论（尽管这里我们还不知道最小公倍数是存在的），即

$$a \left| \frac{ab}{\gcd(a,b)} \right. \tag{2.273}$$

$$b \left| \frac{ab}{\gcd(a,b)} \right. \tag{2.274}$$

这就说明了 $ab/\gcd(a,b)$ 是 a 和 b 的公倍数。因此，我们只须证明对于任意 a 和 b 的公倍数 n，一定有 $\mathrm{lcm}(a,b)|n$。

假设 $a|n$，$b|n$，只须证明 $ab/\gcd(a,b)|n$，而这等价于 $ab|n\gcd(a,b)$。我们不难证明一个引理，即 $n\gcd(a,b) = \gcd(an,bn)$（证明留做练习，可以利用定义直接证明）。因此只须证明 $ab|\gcd(an,bn)$。根据最大公因数的性质，我们只须证明 $ab|an$，$ab|bn$，而根据 $a|n$，$b|n$ 的条件，这也是显然的。

这就证明了若 $\gcd(a,b)$ 存在，则 $\mathrm{lcm}(a,b)$ 存在。反过来的情况是非常类似的，我们留给读者作为练习。

综上所述，我们就证明了这个命题。

根据上面的命题，最大公因数整环和最小公倍数整环是等价的，因此我们只须定义最大公因数整环即可。不要忘记，每一个主理想整环都是最大公因数整环。

特别地，我们还是回到整数环的例子，根据上面的一系列命题，我们得到了推论，即

引理 2.17

若 $m,n \in \mathbb{N}_1$，则

$$(m) + (n) = (\gcd(m,n)) \tag{2.275}$$

$$(m) \cap (n) = (\mathrm{lcm}(m,n)) \tag{2.276}$$

♡

证明 根据上面的一系列命题，这是显然的。

刚才，我们讲解了许许多多整环上整除的例子与性质。实际上，除了让大家熟悉起整环的整除以外，我们也是有目的地给唯一分解整环做铺垫——这一节的标题是主理想整环与唯一分解整环——在唯一分解整环的部分我们也会大量运用整除的性质以大幅简化证明过程。下面，我们是时候进入这一节的最后一部分了——唯一分解整环。

首先回忆我们刚才提到的，整环中的不可约元素就是那些可以表示成非单位乘积的元素。我们现在定义素元素。一般来说，两者不等价。

定义 2.33

令 $(R,+,\cdot)$ 是一个整环，而 $p \in R$。我们称 p 是一个素元素，若 $p \neq 0$，p 不是单位，而且对于任何 $a,b \in R$，

$$p|ab \iff p|a \text{ 或 } p|b \tag{2.277}$$

♣

不难看出，素元素几乎就是说它生成的主理想是素理想。微妙的区别在于我们要求素元素是非零的（这在整环的分解中是重要的）。因此，我们有以下的引理。

引理 2.18

令 $(R,+,\cdot)$ 是一个整环，而 $p \in R$。则 p 是一个素元素，当且仅当 (p) 是一个非零的素理想。

♡

证明 根据素元素和素理想的定义，这是显然的。

那么，如何联系素元素和不可约元素呢？原来，素元素一定是不可约的。

命题 2.40

令 $(R,+,\cdot)$ 是一个整环，而 p 是一个素元素，则 p 是不可约的。

♠

证明 证明是简单的。假如 p 是可约的素元素，那么我们记 $p=ab$，其中 a 与 b 都不是单位。则 $p\nmid a$，因为否则的话 $a\sim p$，就会得到 b 是一个单位。这就告诉我们 $p\nmid a$，同理 $p\nmid b$。然而 $p=ab|ab$，这与素元素的性质相矛盾。因此，整环中的每一个素理想都是可约的。

反过来，是否在整环中所有的不可约元素都是素元素呢？答案是否定的。我们很快就知道，在唯一分解整环中，不可约元素都是素元素，进而就等价了。我们可以在非唯一分解整环的 $\mathbb{Z}\left[\sqrt{-5}\right]$ 中找到反例。下面，我们给出定义。

定义 2.34

我们定义 $\mathbb{Z}\left[\sqrt{-5}\right]=\left\{a+b\sqrt{-5}:a,b\in\mathbb{Z}\right\}$

♣

引理 2.19

$\mathbb{Z}\left[\sqrt{-5}\right]$ 是 $\mathbb{C}$ 的子环。

♡

证明 为了方便，令 $R=\mathbb{Z}\left[\sqrt{-5}\right]$。

我们有 $0=0+0\sqrt{-5},1=1+0\sqrt{-5}\in R$。加法的封闭性是显然的，而加法逆元的封闭是因为 $-\left(a+b\sqrt{-5}\right)=(-a)+(-b)\sqrt{-5}\in R$。

乘法的封闭性是因为，若 $a,b,c,d\in\mathbb{Z}$，则

$$\left(a+b\sqrt{-5}\right)\left(c+d\sqrt{-5}\right)=(ac-5bd)+(ad+bc)\sqrt{-5}\in R \tag{2.278}$$

类似地，你可以定义任意的 $\mathbb{Z}\left[\sqrt{n}\right]$ $(n\in\mathbb{Z})$。为了使其不平凡，可以假设 n 不是完全平方数。

下面，我们来证明在 $\mathbb{Z}\left[\sqrt{-5}\right]$ 中，有不可约的元素不是素元素。

引理 2.20

$\mathbb{Z}\left[\sqrt{-5}\right]$ 中存在不可约的非素元素。

♡

证明 注意到

$$3^2=9=\left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right) \tag{2.279}$$

我们可以证明 $3,2+\sqrt{-5},2-\sqrt{-5}$ 都是不可约的非单位的元素，而 3 就是不可约的非素元素。这是因为 3 整除 $2+\sqrt{-5}$ 和 $2-\sqrt{-5}$ 的乘积，但是不整除它们中的任何一个。

上面这一段的证明，我们可以直接暴力地利用定义证明，但这样太复杂了。利用下一节的知识，我们可以简单地证明上面这一段的事实，因此暂时将证明省略，在下一节中证明。注意，这不会引起任何循环论证的问题，因为下一节的任何一个定义或命题都不会依赖于这个反例。

我们要补充一点。正因为在上面这样的例子中，要证明不可约或者非单位是很复杂的，所以我们才需要下一节的知识。这就是我们必须要讲欧几里得整环及相关知识的原因——它们不是复杂化了问题，而是简化了问题。这是至关重要的，请大家记在心里。

下面，我们给出唯一分解整环的定义。

定义 2.35

令 $(R,+,\cdot)$ 是一个整环，则我们称 R 是一个唯一分解整环，若每一个非零元素 $x\in R\setminus\{0\}$ 都可以写成

$$x=ux_1\cdots x_n \tag{2.280}$$

的形式，其中 u 是单位，而 $x_1,\cdots,x_n$ 是环中（有限多个）不可约的元素；并且每一个元素的分解都是唯一的，即如果 x 还可以写成

$$x = vy_1\cdots y_m \tag{2.281}$$

的形式，那么我们必须有 $m=n$（即不可约元素的个数相等），而且 x_i 与 y_j 之间，存在一个双射，使它们对应等价，即存在某一个

$$\pi:\{1,\cdots,n\}\to\{1,\cdots,n\} \tag{2.282}$$

使得

$$\forall i\in\{1,\cdots,n\}, x_i\sim y_{\pi(i)} \tag{2.283}$$

这里的第二个条件，等价于说，假如一个非零元素有两个分解成单位乘上有限多个不可约元素的乘积的形式，那么不可约元素的个数必须相等，并且在某一个（下标的）置换下，x_i 和 y_j 之间对应等价。

不难发现，这个定义仿照了整数中的算术基本定理的形式。

看回刚才的例子，我们不难发现 $\mathbb{Z}\left[\sqrt{-5}\right]$ 不是唯一分解整环，因为 9 有两个非平凡分解（严格证明依赖于 $3, 2+\sqrt{-5}, 2-\sqrt{-5}$ 都是不可约元素的事实，而这一事实会在下一节中证明）。

$$9 = 3^2 = \left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right) \tag{2.284}$$

这一节中最重要的结论是：主理想整环是唯一分解整环。一个推论便是整数环是唯一分解整环（而这几乎就是算术基本定理，唯一的可能区别在于不可约和素元素的区别）。我们在这一节中很快就会看到证明。

现在，我们要利用唯一分解整环证明的第一个命题就是，在唯一分解整环中，每一个不可约元素都是素元素。

命题 2.41

令 $(R,+,\cdot)$ 是一个唯一分解整环，而 p 是一个不可约元素，则 p 是素元素。

证明 假设 p 是一个不可约元素，则 $p\neq 0$ 而 $p|ab$，我们只须证明 $p|a$ 或者 $p|b$。由于 $p|ab$，故存在 $x\in R$，使得

$$px = ab \tag{2.285}$$

因为唯一分解整环（按定义要求）一定是整环，所以我们可以假设 $a,b\neq 0$（否则利用整环的性质显然有 $p|a$ 或 $p|b$）。因此 $px=ab\neq 0$

根据唯一分解整环的性质，因为 p 是不可约的，所以我们必须有 p 与 a 或 b 中的一个等价。而这就证明了 $p|a$ 或 $p|b$。

综上所述，我们就证明了在唯一分解整环中，不可约元素也都是素元素。这就证明了在唯一分解整环中，不可约元素就是素元素，素元素也就是不可约元素。

因此，唯一分解整环中，每一个非零元素都可以分解成一个单位与有限多个素元素的乘积（因为不可约元素也是素元素）。更进一步，在我们选取了每一个素元素的等价类中的一个 p 后，每一个元素 x 都可以分解成

$$x\sim\prod_p p^{v_p(x)} \tag{2.286}$$

的形式。其中 $v_p(x)$ 称为 x 在 p 的阶。由分解的有限性可知，除了有限项以外的所有 $v_p(x)$ 都等于 0。

为了更熟悉唯一分解整环的概念，我们不妨再结合上面提到的最大公因数整环，证明一下，每一个唯一分解整环都是最大公因数整环。

命题 2.42

令 $(R,+,\cdot)$ 是一个唯一分解整环，则 R 是一个最大公因数整环。

证明 令 $a,b\neq 0$，利用上面的记号，我们记

$$a\sim\prod_p p^{v_p(a)} \tag{2.287}$$

$$b\sim\prod_p p^{v_p(b)} \tag{2.288}$$

正如初等数论中所熟知的，我们只须证明

$$(a)+(b)=\left(\prod_p p^{\min(v_p(a),v_p(b))}\right) \tag{2.289}$$

或等价地，

$$\gcd(a,b)=\prod_p p^{\min(v_p(a),v_p(b))} \tag{2.290}$$

我们先来证明右边是良定义的。因为除了有限项以外的所有 $v_p(a)$ 和 $v_p(b)$ 都等于 0，因此除了有限项以外的所有 $\min v_p(a),v_p(b)$ 都等于 0，因此右边实际上是个有限乘积。

一方面，由于对所有素元素等价类中的代表元素 p，我们都有 $\min v_p(a),v_p(b)\leqslant v_p(a)$，因此

$$\prod_p p^{\min(v_p(a),v_p(b))}\Bigg|\prod_p p^{v_p(a)}=a \tag{2.291}$$

同理

$$\prod_p p^{\min(v_p(a),v_p(b))}\Bigg|\prod_p p^{v_p(b)}=b \tag{2.292}$$

另一方面，如果 $e|a$ 且 $e|b$，我们同样将 e 写成在这组代表元素 $\{p\}$ 下的分解，即

$$e\sim\prod_p p^{v_p(e)} \tag{2.293}$$

根据唯一分解整环的性质，由于 $e|a$，我们可以把 a 写作 e 和某个元素的乘积，则必须有，对所有素元素的代表元素 p

$$v_p(e)\leqslant v_p(a) \tag{2.294}$$

同理，对所有 p，我们有 $v_p(e)\leqslant v_p(b)$。因此 $v_p(e)\leqslant\min(v_p(a),v_p(b))$。

这就证明了

$$e\Bigg|\prod_p p^{\min(v_p(a),v_p(b))} \tag{2.295}$$

综上所述，我们证明了

$$\gcd(a,b)=\prod_p p^{\min(v_p(a),v_p(b))} \tag{2.296}$$

这也就证明了每个唯一分解整环都是最大公因数整环。

注意，我们也可以表示出最小公倍数。一种方式就是利用它们的乘积，以及在整数（甚至实数）中，

$$\min(a,b)+\max(a,b)=a+b \tag{2.297}$$

另一种方式就是和上面的证明类似。无论用哪种方式，我们都可以证明，在唯一分解整环中，

$$\operatorname{lcm}(a,b)=\prod_p p^{\max(v_p(a),v_p(b))} \tag{2.298}$$

现在，我们已经充分熟悉了唯一分解整环。最后，让我们来证明这一节中最重要的结论：每一个主理想整环都是唯一分解整环，进而将这两个看似毫无联系的概念串联起来。我们先证明一个小引理，再证明这个定理。

引理 2.21

令 $(R,+,\cdot)$ 是一个最大公因数整环，而 p 是一个不可约元素，则 p 是素元素。 ♡

证明 令 $a,b \in R$，使得 $p|ab$，我们只须证明 $p|a$ 或 $p|b$。假设 $p \nmid a$，则与初等数论中一样，我们可以证明 $\gcd(a,p)=1$。因为我们在一个最大公因数整环中，故可以找到 $d=\gcd(a,p)$，而我们只须证明 d 是个单位。

假设 d 不是单位。因为 p 是不可约的，所以当我们写成 $p=de$ 后，e 必须是单位，这就告诉我们 $p \sim d$。所以 $(p)=(d)$。根据最大公因数的性质，我们有

$$(a)+(p)=(d)=(p) \tag{2.299}$$

因此

$$(a)=(p) \tag{2.300}$$

则 $p|a$，因此矛盾。

综上，我们在 $p \nmid a$ 的假设下证明了 $\gcd(a,p)=1$。接着，我们就能找到 $x,y \in R$，使得

$$ax+py=1 \tag{2.301}$$

我们知道 $p|ab$，现在只须证明 $p|b$ 即可。对上式两边同时乘上 b，则

$$abx+bpy=b \tag{2.302}$$

注意到左面的两项都是 p 的倍数，故右边也是 p 的倍数，即 $p|b$。

综上所述，我们就证明了这个引理。

命题 2.43

令 $(R,+,\cdot)$ 是一个主理想整环，则 R 是一个唯一分解整环。

证明 这是一个著名的定理，一般证明的方法是用（理想升链下的）极值原理。

假设 R 是一个主理想整环。我们先证明每一个非零元素都可以分解成一个单位和有限多个不可约元素的乘积，再证明这样的分解是唯一的。

令 S 为 $R \setminus \{0\}$ 中所有不能被这样分解的元素所构成的集合。假设 $S \neq 0$。我们希望构造出反例，而反例不是那么好构造的，所以我们需要用到极值原理。任取 $a_1 \in S$，考虑所有可能的 S 中元素所生成的主理想升链。

$$(a_1) \subsetneq (a_2) \subsetneq \cdots (a_n) \subsetneq \cdots \tag{2.303}$$

我们先证明这样的升链只能有有限项，即不存在无穷的严格递增的理想链。

用反证法，假如

$$(a_1) \subsetneq (a_2) \subsetneq \cdots \tag{2.304}$$

是个无穷升链。则不难证明

$$I=\bigcup_{n=0}^{\infty}(a_n) \tag{2.305}$$

是个理想。注意，一般来说理想的并不是理想，这里是因为升链的条件才成立。完整的证明留做练习，这里只给一个重要的提示——两个 I 中元素的加法，可以考虑成在较大的那个理想中进行，用较大的理想是理想来证明。

然而，I 作为一个主理想整环中的理想，也一定可以写成

$$I=(a) \tag{2.306}$$

假设 $a \in (a_n)$，那么

$$I=(a) \subset (a_n) \subset \bigcup_{n=0}^{\infty}(a_n)=I \tag{2.307}$$

这就证明了 $a \sim a_n$，即这个链条在第 n 项时就停下了。事实上，用同样的方法我们可以证明主理想整环中任何的理想升链都会在有限项停下，这样的环被叫做诺特环。特别地，在这里，我们可以取到 $a \sim a_n$，是 a_1 所在的一个升链的最大的理想中的一个元素。

注意，这里的 $a_1, a_2, \cdots, a_n$ 都是 S 中元素，故它们都不可以写成一个单位和有限多个不可约元素的乘积。特别地，$a \sim a_n$ 一定不是一个不可约元素（否则 a_n 就不属于 S 了）。因此我们找到两个非单位 $b, c \in R$，使得

$$a = bc \tag{2.308}$$

可是这样，我们就有

$$(a) \subsetneq (b) \tag{2.309}$$

$$(a) \subsetneq (c) \tag{2.310}$$

因此，根据 (a) 的极大性，我们必须有 $b, c \neq S$。也就是说，b, c 可以写成单位与有限多个不可约元素的乘积。可是这样，a 也当然可以这样写了，这就说明了 $a \in S$。于是，我们得到了一个矛盾。

综上所述，我们利用反证法，证明了在主理想整环中，每一个非零元素都可以写成一个单位和有限多个不可约元素的乘积。

下面，我们来证明这种写法的唯一性。注意，这里的证明和算术基本定理中的证明是相似的。

假设

$$x = up_1 \cdots p_m = vq_1 \cdots q_n \tag{2.311}$$

其中 u, v 是单位，p_i 和 q_j 都是不可约元素。不失一般性假设 $m \leqslant n$。因为主理想整环都是最大公因数整环，再利用上面的引理，我们就知道这里的 p_i 和 q_j 都是素元素。

因为 p_1 整除左边，就整除右边，在一个重排后不失一般性假设 $p_1 | q_1$。因为 p_1 和 q_1 都是不可约的，故 $p_1 \sim q_1$。重复这样的过程，我们就在重排后得到 $p_1 \sim q_1, \cdots, p_m \sim q_m$。因为等价下，我们可以对应做除法而得到单位，因此在对应着除完 p_i 与 q_i 后，我们必须两边都剩下单位，这就证明了 $m = n$，也就证明了这样的分解对每一个非零元素都是唯一的。

综上所述，我们证明了这个定理，即每一个主理想整环都是唯一分解整环。

我们用一个逻辑链条来做一个小结。

命题 2.44

域 $\Longrightarrow$ 主理想整环 $\Longrightarrow$ 唯一分解整环 $\Longrightarrow$ 最大公因数整环 $\Longrightarrow$ 整环 $\Longrightarrow$ 交换环 $\Longrightarrow$ 环。

2.7 欧几里得整环

在这一节中，我们要补充上一节中没有证明的有关 $\mathbb{Z}\left[\sqrt{-5}\right]$ 的事实，并且将欧几里得整环从逻辑上插在域和主理想整环之间。这就是说，欧几里得整环的性质比主理想整环还要好，但是没有域好。

我们在证明整数环是唯一分解整环的时候用到了带余除法。欧几里得整环和带余除法的推广密切相关。下面，我们给出定义。

定义 2.36

令 $(R, +, \cdot)$ 是一个整环，则我们称 R 是个欧几里得整环，若存在 $f : R \setminus \{0\} \to \mathbb{N}_0$，使得对任意 $a \in R$，$b \in R \setminus \{0\}$，我们都能找到 $q, r \in R$，使得

$$a = qb + r \tag{2.312}$$

其中 $r = 0$ 或 $f(r) < f(b)$。

这里的 f 被称为欧几里得函数。

这里有两个注意点。一个是这里的 q, r 不需要是唯一的。另一个是我们单独把 $r = 0$ 的情况拿出来，而且不定义 $f(0)$。在整数环中，余数的条件是

$$0 \leqslant r \leqslant |b| - 1 \tag{2.313}$$

这里实际上将其分为两条，即 $r = 0$ 或 $r < |b|$。因此，我们立刻证明了整数环是一个欧几里得整环。

命题 2.45

整数环 $\mathbb{Z}$ 是个欧几里得整环。

证明 令 $f:\mathbb{Z}\setminus\{0\}\to\mathbb{N}_0$，定义为

$$f(x)=|x| \tag{2.314}$$

则根据带余除法，对于任意 $a\in\mathbb{Z}$，$b\in\mathbb{Z}\setminus\{0\}$，我们可以找到 $q,r\in\mathbb{Z}$，使得

$$a=qb+r \tag{2.315}$$

$$r=0\text{ 或}r=|r|<|b| \tag{2.316}$$

即

$$r=0\text{ 或}f(r)<f(b) \tag{2.317}$$

这就证明了整数环是个欧几里得整环。

实际上，我们也可以证明域上的多项式环是欧几里得整环。对应的欧几里得函数是众所周知的多项式的次数。为了知识的连贯性，我们选择克制所有在环中对多项式的讨论，而将多项式相关的讨论放到下一章中，因此这个结论也会在下一章中证明。

我们迫不及待地想要证明域是欧几里得整环，而且欧几里得整环是主理想整环。

命题 2.46

令 $(F,+,\cdot)$ 是一个域，则 F 是一个欧几里得整环。

证明 注意到域的性质是非常好的——每一个非零元素都有乘法逆元。令 $a\in F$，$b\in F\setminus\{0\}$。取 $c\in F$，使得 $bc=1$。因此

$$a=a\cdot 1=abc+0=(ac)b+0 \tag{2.318}$$

我们令 $q=ac$，$r=0$。这就证明了 F 是一个欧几里得整环（无论怎么定义欧几里得函数都可以）。

命题 2.47

令 $(R,+,\cdot)$ 是一个欧几里得整环，则 R 是一个主理想整环。

证明 令 $I\lhd R$ 是一个理想。假如 $I=\{0\}=(0)$，则 I 显然是个理想。因此我们假设 $I\neq\{0\}$，即 $I\setminus\{0\}\neq\emptyset$。

因为我们定义的欧几里得函数 f 的陪域是自然数集，而自然数集是有良序公理的。根据良序公理，我们可以找到 $I\setminus\{0\}$ 中取值最小的某个 b（不一定是唯一的），使得

$$f(b)=\min_{x\in I}f(x) \tag{2.319}$$

我们只须证明

$$I=(b) \tag{2.320}$$

首先因为 $b\in R$，所以 $I\supset(b)$。

假设 $a\in I\setminus(b)$，则

$$a=qb+r \tag{2.321}$$

$$r\neq 0 \tag{2.322}$$

因此 $f(r)<f(a)$。并且

$$r=a-qb\in I+(b)\subset I \tag{2.323}$$

又因为 $r\neq 0$，这就和 b 的取法相矛盾。

综上所述，我们就证明了每一个欧几里得整环都是主理想整环。

我们进一步补全了环论中的逻辑链条，得到

命题 2.48

域 $\Longrightarrow$ 欧几里得整环 $\Longrightarrow$ 主理想整环 $\Longrightarrow$ 唯一分解整环 $\Longrightarrow$ 最大公因数整环 $\Longrightarrow$ 整环 $\Longrightarrow$ 交换环 $\Longrightarrow$ 环。

我们在实际情况中，会遇到一种范数。

定义 2.37

令 $(R,+,\cdot)$ 是一个整环，我们称 $N:R\to\mathbb{R}^{\geqslant 0}$ 是一个范数，若

$$N(x)=0 \iff x=0 \tag{2.324}$$

$$N(x)=1 \iff x \text{ 是一个单位} \tag{2.325}$$

$$\forall a,b\in R, N(ab)=N(a)N(b) \tag{2.326}$$

注意，范数在分析学中有另一种含义。在这一门课程中，在不引起歧义的情况下，我们用“范数”来指代如上所述的类似于同态的映射。

例如在高斯整数环 $\mathbb{Z}[i]=\mathbb{Z}\left[\sqrt{-1}\right]=\{a+bi:a,b\in\mathbb{Z}\}$ 中，我们可以定义

$$N(a+bi)=a^2+b^2 \tag{2.327}$$

则利用复数的性质或直接利用定义，我们都可以证明这个例子中的 N 是一个范数。囿于篇幅，我们将证明留做练习。

考虑到在高斯整数环中 $a+bi\in\mathbb{Z}[i]$ 满足 $a,b\in\mathbb{Z}$，因此 $N:R\to\mathbb{N}_0$ 是个映射到自然数的函数。我们下面来证明 N 是一个欧几里得函数函数。

命题 2.49

高斯整数环 $\mathbb{Z}[i]$ 是一个欧几里得整环。

证明 令 $a=x+iy,b=z+iw\in\mathbb{Z}[i](x,y,z,w\in\mathbb{Z})$。则在复数域 $\mathbb{C}$ 中，我们可以取到

$$\frac{a}{b}=\frac{x+iy}{z+iw}=\frac{(xz-yw)+i(xw+yz)}{z^2+w^2}=\frac{xz-yw}{z^2+w^2}+i\frac{xw+yz}{z^2+w^2}\in\mathbb{Q}[i] \tag{2.328}$$

其中 $\mathbb{Q}[i]=\{a+ib:a,b\in\mathbb{Q}\}$。

尽管如此，我们依然可以找到离这两个有理数最近的两个整数，称为 $m,n\in\mathbb{Z}$，使得

$$\left|m-\frac{xz-yw}{z^2+w^2}\right|\leqslant\frac{1}{2} \tag{2.329}$$

$$\left|n-\frac{xw+yz}{z^2+w^2}\right|\leqslant\frac{1}{2} \tag{2.330}$$

我们令

$$q=m+in \tag{2.331}$$

是 a/b 的一个很好的（可以是最好的）高斯整数逼近。

而

$$r=a-qb \tag{2.332}$$

我们只须证明 $r=0$ 或者 $N(r)<N(b)$。假设 $r\neq 0$，只须证明 $N(r)<N(b)$。而这是因为

$$r=a-qb=b\left(\frac{a}{b}-q\right)=\left(m-\frac{xz-yw}{z^2+w^2}\right)+i\left(n-\frac{xw+yz}{z^2+w^2}\right) \tag{2.333}$$

因此

$$N(r)\leqslant\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2=\frac{1}{2} \tag{2.334}$$

并且因为 $b \neq 0$，所以

$$N(b) \geqslant 1 > \frac{1}{2} \geqslant N(r) \tag{2.335}$$

这就证明了这个命题。

实际上，对于映射到自然数的范数，我们有一条很好的性质，即

命题 2.50

令 $(R,+,\cdot)$ 是一个整环，$N : R \to \mathbb{N}_0$ 是一个范数，而 $x \in R$。若 $N(x)$ 是一个素数，则 x 是一个不可约元素。

证明 用反证法。假设 $x = ab$，其中 a、b 都是非单位，则根据范数的条件，$N(a), N(b) > 1$。这就给出了正整数 $N(x)$ 的一个非平凡分解，与 $N(x)$ 是素数的条件相矛盾。

综上，我们就证明了这个命题。

现在，我们来证明上一节中留下的问题。

引理 2.22

$N : \mathbb{Z}\left[\sqrt{-5}\right] \to \mathbb{N}_0$，

$$N\left(a+\sqrt{-5}b\right) = a^2 + 5b^2 \tag{2.336}$$

是 $\mathbb{Z}\left[\sqrt{-5}\right]$ 上的一个范数。

证明 令 $x = a + \sqrt{-5}b \in \mathbb{Z}\left[\sqrt{-5}\right]$。

第一条是显然的。若 $\left|a^2 + 5b^2\right| = 0$，则 $a = b = 0$。

我们来证明第三条。不难发现

$$N\left(a+\sqrt{-5}b\right) = N\left(a+i\left(\sqrt{5}b\right)\right) = a^2 + 5b^2 = \left(a+i\left(\sqrt{5}b\right)\right)^2 \tag{2.337}$$

就是复数上的模长平方，故 N 显然是乘性映射。

我们来证明第二条。利用一点点数论，$N(x) = 1$ 当且仅当 $x = \pm 1$。± 1 显然是单位。我们只须证明，若 x 是个单位，则 $x = \pm 1$。假设

$$xy = \left(a+\sqrt{-5}b\right)\left(c+\sqrt{-5}d\right) = 1 \tag{2.338}$$

两边同时取范数，得到

$$N(xy) = N(x)N(y) = 1 \tag{2.339}$$

因此 $N(x) = \pm 1$，故 $x = \pm 1$。

综上所述，我们就证明了 N 是 $\mathbb{Z}\left[\sqrt{-5}\right]$ 上的一个范数。

现在，我们来证明上一节留下的练习，即 $3, 2+\sqrt{-5}, 2-\sqrt{-5}$ 是这个环中的不可约元素。

引理 2.23

$3, 2+\sqrt{-5}, 2-\sqrt{-5}$ 是 $\mathbb{Z}\left[\sqrt{-5}\right]$ 中的不可约元素。

证明 一方面，我们计算得到 $N(3) = 9$，因此如果 3 可以分解成两个非单位 x, y 的乘积，即 $3 = xy$，则必须有

$$N(x) = N(y) = \pm 3 \tag{2.340}$$

然而显然对于任意 $a, b \in \mathbb{Z}$，我们有

$$a^2 + 5b^2 \neq 3 \tag{2.341}$$

这就导致了矛盾。因此 3 是环 $\mathbb{Z}\left[\sqrt{-5}\right]$ 中的不可约元素。

另一方面，我们计算得到

$$N\left(2\pm\sqrt{-5}\right)=2^2+5=9 \tag{2.342}$$

同理，$2+\sqrt{-5},2-\sqrt{-5}$ 也是环 $\mathbb{Z}\left[\sqrt{-5}\right]$ 中的不可约元素。

命题 2.51

$\mathbb{Z}\left[\sqrt{-5}\right]$ 不是一个唯一分解整环。

♠

证明 因为

$$9=3^2=\left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right) \tag{2.343}$$

利用上一条引理所说的，$3,2+\sqrt{-5},2-\sqrt{-5}$ 是 $\mathbb{Z}\left[\sqrt{-5}\right]$ 中的不可约元素。因此，$\mathbb{Z}\left[\sqrt{-5}\right]$ 不是一个唯一分解整环。

命题 2.52

在 $\mathbb{Z}\left[\sqrt{-5}\right]$ 中，存在是不可约元素却不是素元素的元素。

♠

证明 例如 3 是不可约的，而且

$$3|9=\left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right) \tag{2.344}$$

然而

$$3\nmid 2\pm\sqrt{-5} \tag{2.345}$$

这就证明了 3 不是素元素。类似地，我们也可以证明 $2\pm\sqrt{-5}$ 是不可约的，却不是素元素。

第 3 章 多项式理论——Polynomial Theory

3.1 多项式环

我们从初中就学过多项式，可是，有多少人真正理解了多项式呢？我们用最经典的一个问题来尝试证明你不懂多项式。请问，多项式是映射吗？

如果你说是，那你就是不懂多项式的。因为多项式并不是映射，尽管每个多项式确实可以引出一个映射。什么意思？我们来看一个例子，首先定义二元域

定义 3.1

$\mathbb{F}_2 = \mathbb{Z}_2$，被称为一个二元域。事实上，所有的二元域都彼此同构。

我们在上一章中，证明了对任意素数 p，$\mathbb{Z}_p$ 都是域，因此二元域当然是个域。在这个域中，运算非常简单，即

$$0 + 0 = 0 \tag{3.1}$$

$$0 + 1 = 1 \tag{3.2}$$

$$1 + 1 = 0 \tag{3.3}$$

$$0 \cdot 0 = 0 \tag{3.4}$$

$$0 \cdot 1 = 0 \tag{3.5}$$

$$1 \cdot 1 = 1 \tag{3.6}$$

我们现在定义两个 $\mathbb{F}_2$ 上的多项式，令

$$f(x) = x \tag{3.7}$$

$$g(x) = x^2 \tag{3.8}$$

假如多项式就是映射，那么从映射的角度来看，$f = g$。这是因为

$$f(0) = 0 = 0^2 = g(0) \tag{3.9}$$

$$f(1) = 1 = 1^2 = g(1) \tag{3.10}$$

可是这两个多项式显然是不同的。或者说，我们希望这两个多项式是不同的——有谁希望我们将一次式和二次式混为一谈呢？这就通过一个反例说明了，多项式并不是映射。

那么多项式是什么呢？下面我们要说，多项式是一个形式的记号，而且必须要定义在一个环上（否则没有自然的加法和乘法去做运算）。为了方便，我们一般假设 R 是交换环。

定义 3.2

令 $(R, +, \cdot)$ 是一个交换环，我们称 f 是 R 上的一个多项式，若 f 具有以下形式的表达式

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \tag{3.11}$$

其中 $n \in \mathbb{N}_0$，所有 $a_i \in R$。不失一般性，我们可以假设 $a_n \neq 0$。这里的 a_n 被称为 f 的首项系数。

大家一定要注意，这里的 f 只是一个形式的记号，包括这里的 x 也是形式的记号。也就是说，按照定义，我们要求两个多项式相等，当且仅当所有的系数都相等。这就说明，在刚才的二元域的例子中，f 和 g 作为映射是相等的，但作为多项式是不相等的。

学习抽象代数的学生一定学过数学分析。实际上，我们也有形式幂级数，不妨也定义一下。

定义 3.3

令 $(R,+,\cdot)$ 是一个交换环，我们称 f 是 R 上的一个形式幂级数，若 f 具有以下形式的表达式

$$f(x)=\sum_{i=0}^{\infty}a_ix^i \tag{3.12}$$

其中所有 $a_i\in R$。

那么多项式就有另外一个等价定义，即除了有限项外的所有 a_i 都等于 0 的形式幂级数。

定义 3.4

令 $(R,+,\cdot)$ 是一个交换环，则 f 是 R 上的一个多项式，当且仅当 f 可以写成

$$f(x)=\sum_{i=0}^{\infty}a_ix^i \tag{3.13}$$

的形式，并且除了有限项外，所有的 a_i 都等于 0。

假如 $f\neq 0$，我们称最大的使得 $a_i\neq 0$ 的 i 为 f 的次数，记作 $\deg(f)$。

零多项式 0 的次数，我们在这里定义为 -1。

注意，零多项式的次数，在不同的书上有不同的定义，有人定义成 -1（正如我们的定义），有人定义成 0，有人定义成 ∞ 甚至 $-\infty$，还有人索性不给出定义。这里，我们想说明零多项式的特殊性，以区分非零常多项式，却又不给一个极端的正负无穷的次数，所以 -1 是最好的选择。一般来说，零多项式是特殊的情况，我们无论怎么定义，只要分类讨论时小心一点，都不会造成太大的问题。

既然有了多项式，我们就有两件事可以做。一是引出一个以这个环本身为定义域的映射，二是赋予多项式的集合一个环的结构。

第一件事是很好做的，我们直接同样形式地定义

$$f(x)=\sum_{i=0}^{n}a_ix^i \tag{3.14}$$

为一个从 R 到 R 的映射即可。

第二件事有点难度，有不少细节可能会出问题。我们慢慢向前进。

定义 3.5

令 $(R,+,\cdot)$ 是一个交换环，而 f,g 是 R 上的两个多项式。令

$$f(x)=\sum_{i=0}^{\infty}a_ix^i \tag{3.15}$$

$$g(x)=\sum_{i=0}^{\infty}b_ix^i \tag{3.16}$$

则我们定义它们的和与积，记作 $f+g$ 和 fg，定义为

$$(f+g)(x)=\sum_{i=0}^{\infty}c_ix^i \tag{3.17}$$

$$(fg)(x)=\sum_{i=0}^{\infty}d_ix^i \tag{3.18}$$

$$\tag{3.19}$$

其中，对所有 $i \geqslant 0$，我们定义

$$c_i = a_i + b_i \tag{3.20}$$

$$d_i = \sum_{j=0}^{i} a_j b_{i-j} \tag{3.21}$$

♣

加法是很好理解的，各位相加就好了。那么多项式的乘法，为什么看上去这么奇怪呢？原来，我们希望，这些哪怕是形式记号的多项式，乘起来以后，也在各位是对齐的。恰好是从 0 到 i 的这些 j 所给出的 a_j 与 b_{i-j} 所在的项，做了乘积后便得到了 x^i 所在的项，即

$$\left(a_j x^j\right)\left(b_{i-j} x^{i-j}\right) = \left(a_j b_{i-j}\right) x^i \tag{3.22}$$

所以，这里（形式的）多项式乘法，与我们之前熟知的整系数，实系数，甚至复系数多项式乘法都是一致的。

假如你愿意的话，也可以将多项式乘法下系数（这里是 d_i）的公式改写为更优美的形式，即

$$d_i = \sum_{j+k=i} a_j b_k \tag{3.23}$$

因为在计算中非常有用，所以我们单独将这个结论列为一个引理。

引理 3.1

令 $(R,+,\cdot)$ 是一个交换环，而 f,g 是 R 上的两个多项式。令

$$f(x) = \sum_{i=0}^{\infty} a_i x^i \tag{3.24}$$

$$g(x) = \sum_{i=0}^{\infty} b_i x^i \tag{3.25}$$

$$(fg)(x) = \sum_{i=0}^{\infty} d_i x^i \tag{3.26}$$

$$\tag{3.27}$$

则对所有 $n \geqslant 0$，我们有

$$d_n = \sum_{i+j=n} a_i b_j \tag{3.28}$$

♡

证明 根据 d_i 的定义，这是显然的。

未来，我们一定会知道，这样的记号和众所周知的“卷积”就联系起来了。实际上，各种“卷积”的概念，都可以用类似的方式来定义。有时因为考虑的是连续的空间，所以我们会用积分来代替求和，但本质还是一致的。注意，所有的卷积运算都是结合的，因此自然地，多项式的乘法也应当是结合的；在这里，因为我们要求环本身是交换的，所以多项式的乘法也应当是交换的。至于加法的交换、结合等性质就过于显然了，我们几乎没有什么要补充的。

下面，我们证明所有交换环 R 上的多项式，在上面给出的加法和乘法下，构成一个交换环，称为（交换环）R 上的多项式环。

定义 3.6

令 $(R,+,\cdot)$ 是一个交换环，我们定义 R 上的多项式环，记作 $(R[x],+,\cdot)$（其中 x 是形式变量），定义为

$$R[x]=\{f:f \text{ 是 } R \text{ 上的一个多项式}\} \tag{3.29}$$

$$=\left\{f(x)=\sum_{i=0}^{n}a_ix^i:n\in\mathbb{N}_0,\forall i,a_i\in R\right\} \tag{3.30}$$

$$=\left\{f(x)=\sum_{i=0}^{\infty}a_ix^i:\forall i,a_i\in R,\text{除了有限项外，所有的 } a_i \text{ 都等于 } 0\right\} \tag{3.31}$$

♣

命题 3.1

令 $(R,+,\cdot)$ 是一个交换环，则 R 上的多项式环 $R[x]$，是个交换环。

♠

证明 首先，根据定义，加法和乘法是良定义的。就算是乘法，我们在每一项中也用的是有限的加乘得到 d_i，所以良定义是自明的。

多项式的加法因为是逐位相加，所以太显然。整个多项式环上的交换律和结合律从多项式每一项的交换律和结合律就可以得到。而加法单位元显然是零多项式 0，加法逆元显然是每一位都取加法逆元（即相反数）。具体的证明过程，留给有兴趣的读者来证明。

乘法的单位元显然是常多项式 1，因为无论从严格的定义还是我们上面介绍的直观的定义（为了让 x^i 幂次对应相等），都能简单地证明对任意 $f\in R[x]$，都有

$$1\cdot f=f\cdot 1=f \tag{3.32}$$

下面，我们重点证明 $R[x]$ 上的乘法是交换和结合的。为了方便起见，我们用 $a_i(f)$ 来指代多项式 f 在第 i 项的系数。注意，有时我们也会用 $a_f(i)$ 的记号，它们的含义是相同的。令 $f,g,h\in R[x]$。我们只须证明，对任意 $n\geqslant 0$，我们有

$$a_n(fg)=a_n(gf) \tag{3.33}$$

$$a_n((fg)h)=a_n(f(gh)) \tag{3.34}$$

我们先证明乘法交换律。

$$a_n(fg)=\sum_{i+j=n}a_i(f)a_j(g) \tag{3.35}$$

$$=\sum_{j+i=n}a_j(g)a_i(f) \tag{3.36}$$

$$=a_n(gf) \tag{3.37}$$

我们再证明乘法结合律。

$$a_n((fg)h) = \sum_{l+k=n} a_l(fg)a_k(h) \tag{3.38}$$

$$= \sum_{l+k=n} \left(\sum_{i+j=l} a_i(f)a_j(g) \right) a_k(h) \tag{3.39}$$

$$= \sum_{i+j+k=n} a_i(f)a_j(g)a_k(h) \tag{3.40}$$

$$= \sum_{i+l=n} a_i(f) \left(\sum_{j+k=l} a_j(g)a_k(h) \right) \tag{3.41}$$

$$= \sum_{i+l=n} a_i(f)a_l(gh) \tag{3.42}$$

$$= a_n(f(gh)) \tag{3.43}$$

综上所述，我们就证明了交换环 R 上的多项式环 $R[x]$ 是个交换环。

实际上，我们用几乎完全一样的方法，可以证明交换环 R 上的形式幂级数，在几乎完全一样的加法和乘法下，构成交换环，记作 $R[[x]]$。囿于篇幅，我们在整个抽代 I 中，不会进一步讨论形式幂级数了。感兴趣的读者可以参考其他的材料。

接下来，我们问一个几乎显然的问题，假设 $f, g \neq 0$，那么

$$\deg(f+g) = \max(\deg(f), \deg(g)) \tag{3.44}$$

$$\deg(fg) = \deg(f)\deg(g) \tag{3.45}$$

是否是成立的呢?

答案是否定的。下面给出两个反例。

在任意交换环中，

$$\deg(x) = 1 \tag{3.46}$$

$$\deg(-x) = 1 \tag{3.47}$$

$$\deg(x + (-x)) = \deg(0) = -1 \tag{3.48}$$

如果 R 不是整环，我们可以找到 $a, b \in R$，使得 $ab = 0$，而 $a, b \neq 0$，则

$$\deg(ax) = 1 \tag{3.49}$$

$$\deg(bx) = 1 \tag{3.50}$$

$$\deg(abx^2) = \deg(0) = -1 \tag{3.51}$$

显然不相等。

那么一般来说，我们有什么结论呢？在什么情况下，我们会有更好的结论呢？我们用两个命题来给出答案。

命题 3.2

令 $(R, +, \cdot)$ 是一个交换环，$f, g \in R[x] \setminus \{0\}$，则

$$\deg(f+g) \leqslant \max(\deg(f), \deg(g)) \tag{3.52}$$

假如我们还有 $\deg(f) \neq \deg(g)$ 的条件，那么

$$\deg(f+g) = \max(\deg(f), \deg(g)) \tag{3.53}$$

♠

证明 我们依然采用之前的记号，用 $a_i(f)$ 表示多项式 f 在第 i 项的系数。

不失一般性，假设 $m = \deg(f) \leqslant \deg(g) = n$。

那么显然，对任意 $k \geqslant n+1$，我们有 $a_k(f) = a_k(g) = 0$，因此 $a_k(f+g) = 0$。这就证明了

$$\deg(f+g) \leqslant \max(\deg(f), \deg(g)) \tag{3.54}$$

假如 $\deg(f) \neq \deg(g)$，我们依然不失一般性地假设 $m = \deg(f) < \deg(g) = n$。
同理，我们可以证明对任意 $k \geqslant n+1$，我们有 $a_k(f+g) = 0$。
除此以外，因为 $a_n(f) = 0$，而 $a_n(g) \neq 0$，所以

$$a_n(f+g) \neq 0 \tag{3.55}$$

这就证明了

$$\deg(f+g) = \max(\deg(f), \deg(g)) \tag{3.56}$$

综上所述，我们就证明了这个命题。

命题 3.3

令 $(R, +, \cdot)$ 是一个整环，则对任意 $f, g \in R[x] \setminus \{0\}$，我们有

$$\deg(fg) = \deg(f)\deg(g) \tag{3.57}$$

证明 假设 $f, g \neq 0$。不失一般性，假设 $m = \deg(f) \leqslant \deg(g) = n$。
利用乘法的定义，我们不难证明对任意 $k \geqslant mn+1$，我们有

$$a_k(fg) = 0 \tag{3.58}$$

因此我们一定有

$$\deg(fg) \leqslant mn = \deg(f)\deg(g) \tag{3.59}$$

另一方面，根据乘法的定义，我们不难证明

$$a_{mn}(fg) = a_m(f)a_n(g) \tag{3.60}$$

因为 m 和 n 分别是 f 和 g 的次数，所以 $a_m(f) \neq 0$，$a_n(g) \neq 0$。又因为 R 是个整环，所以

$$a_{mn}(fg) = a_m(f)a_n(g) \neq 0 \tag{3.61}$$

这就证明了

$$\deg(fg) = \deg(f)\deg(g) \tag{3.62}$$

综上所述，我们就证明了这个命题。
接着，我们要说一个重要的同态。

命题 3.4

令 $(R, +, \cdot)$ 是一个交换环，而 $a \in R$。则 $\phi_a : R[x] \to R$，定义为

$$\phi_a(f(x)) = f(a) \tag{3.63}$$

是一个环同态。这个环同态被称为代入同态。

证明 证明是不难的。显然 $\phi_a(1) = 1(a) = 1$。令

$$f(x) = \sum_{n=0}^{\infty} b_n x^n \tag{3.64}$$

$$g(x) = \sum_{n=0}^{\infty} c_n x^n \tag{3.65}$$

则

$$\phi_a(f(x)) = \sum_{n=0}^{\infty} b_n a^n \tag{3.66}$$

$$\phi_a(g(x)) = \sum_{n=0}^{\infty} c_n a^n \tag{3.67}$$

因此

$$\phi_a(f(x)+g(x)) = \phi_a\left(\sum_{n=0}^{\infty}(b_n+c_n)x^n\right) = \sum_{n=0}^{\infty}(b_n+c_n)a^n = \phi_a(f(x)) + \phi_a(g(x)) \tag{3.68}$$

而且

$$\phi_a(f(x)g(x)) = \phi_a\left(\sum_{n=0}^{\infty}\left(\sum_{i+j=n} b_i c_j\right)x^n\right) = \sum_{n=0}^{\infty}\left(\sum_{i+j=n} b_i c_j\right)a^n = \left(\sum_{n=0}^{\infty} b_n a^n\right)\left(\sum_{n=0}^{\infty} c_n a^n\right) = \phi_a(f(x))\phi_a(g(x)) \tag{3.69}$$

综上所述，这就证明了每个 $\phi_a(a \in R)$ 都是一个环同态。

对于交换环而言，正如每个元素可以引出一个多项式环上的环同态，每个环同态也可以引出多项式环的环同态。

命题 3.5

令 $(R,+,\cdot)$，$(R',+,\cdot)$ 是两个交换环，而 $f: R \to R'$ 是个环同态，则 $\phi: R[x] \to R'[x]$，定义为

$$\phi\left(\sum_{n=0}^{\infty} a_n x^n\right) = \sum_{n=0}^{\infty} f(a_n)x^n \tag{3.70}$$

是个环同态。

证明 因为 f 是环同态，所以 $f(1)=1$，$f(0)=0$，而这就告诉我们 $\phi(1)=1$。令

$$g(x) = \sum_{n=0}^{\infty} b_n x^n \tag{3.71}$$

$$h(x) = \sum_{n=0}^{\infty} c_n x^n \tag{3.72}$$

则

$$\phi(g(x)) = \sum_{n=0}^{\infty} f(b_n)x^n \tag{3.73}$$

$$\phi(h(x)) = \sum_{n=0}^{\infty} f(c_n)x^n \tag{3.74}$$

$$\tag{3.75}$$

因此

$$\phi(g(x)+h(x)) = \sum_{n=0}^{\infty} f(b_n+c_n)x^n = \sum_{n=0}^{\infty} f(b_n)x^n + \sum_{n=0}^{\infty} f(c_n)x^n = \phi(g(x)) + \phi(h(x)) \tag{3.76}$$

而且

$$\phi(g(x)h(x)) = \sum_{n=0}^{\infty} f\left(\sum_{i+j=n} b_i c_j\right)x^n = \sum_{n=0}^{\infty}\sum_{i+j=n} f(b_i)f(c_j)x^n = \left(\sum_{n=0}^{\infty} f(b_n)x^n\right)\left(\sum_{n=0}^{\infty} f(c_n)x^n\right) = \phi(g(x))\phi(h(x)) \tag{3.77}$$

综上所述，这就证明了 $\phi: R[x] \to R'[x]$ 是个环同态。

上面介绍的多项式环是只有一个变量 x 的，所以全称是单变量多项式环。我们在初中时就学习了有两个或更多变量的多项式。类似地，我们也可以定义多变量多项式环。我们一般用 $x_1, \cdots, x_n$ 来表示这些变量。

定义 3.7

令 $(R,+,\cdot)$ 是一个交换环，则我们称 f 是一个关于 $x_1,\cdots,x_n$ 的多变量多项式，若

$$f(x_1,\cdots,x_n)=\sum_{\alpha_1=0}^{\infty}\cdots\sum_{\alpha_n=0}^{\infty}a_{\alpha_1,\cdots,\alpha_n}x_1^{\alpha_1}\cdots x_n^{\alpha_n} \tag{3.78}$$

其中，除了有限项外的所有 $a_{\alpha_1,\cdots,\alpha_n}$ 都等于 0。

为了方便起见，我们常常用多重指标

$$\alpha=(\alpha_1\cdots\alpha_n) \tag{3.79}$$

作为指标的推广。

对于这样的 α，我们定义其次数为

$$|\alpha|=\alpha_1+\cdots+\alpha_n \tag{3.80}$$

对于多重变量 $x=(x_1,\cdots,x_n)$，我们定义它的在多重指标下的幂次为

$$x^{\alpha}=x_1^{\alpha_1}\cdots x_n^{\alpha_n} \tag{3.81}$$

多重指标的加法、减法都是自明的，我们不必赘述。

假如用多重指标，我们可以大幅简化多变量多项式的定义。

定义 3.8

令 $(R,+,\cdot)$ 是一个交换环，则我们称 f 是一个关于 $x_1,\cdots,x_n$ 的多变量多项式，若

$$f(x_1,\cdots,x_n)=\sum_{\alpha=(\alpha_1,\cdots\alpha_n)}a_{\alpha}x^{\alpha} \tag{3.82}$$

其中，除了有限项外的所有 a_{α} 都等于 0。

我们用 $a_{\alpha}(f)$ 来表示多变量多项式 f 在多重指标 α 下的系数。用这样的记号，我们类似地定义多变量多项式的加法与乘法，定义为

$$a_{\alpha}(f+g)=a_{\alpha}(f)+a_{\alpha}(g) \tag{3.83}$$

$$a_{\alpha}(fg)=\sum_{\beta+\gamma=\alpha}a_{\beta}(f)a\gamma(g) \tag{3.84}$$

现在，我们定义 R 上的多变量多项式环。

定义 3.9

令 $(R,+,\cdot)$ 是一个交换环，我们定义 R 上的多变量多项式环，记作 $(R[x_1,\cdots,x_n],+,\cdot)$（其中 $x_1,\cdots,x_n$ 是形式变量），定义为

$$R[x]=\{f:f\text{ 是 }R\text{ 上的一个关于 }x_1,\cdots,x_n\text{ 的多变量多项式}\} \tag{3.85}$$

$$=\left\{f(x)=\sum_{\alpha=(\alpha_1,\cdots\alpha_n)}a_{\alpha}x^{\alpha}:\forall\alpha,a_{\alpha}\in R,\text{除了有限项外，所有的 }a_{\alpha}\text{ 都等于 }0\right\} \tag{3.86}$$

完全同理地，我们可以证明下面的命题。

命题 3.6

令 $(R,+,\cdot)$ 是一个交换环，则 R 上的多变量多项式环 $R[x_1,\cdots,x_n]$，是个交换环。

证明 和（单变量）多项式环的证明极其类似。故留给有兴趣的读者作为练习。

3.2 多项式环的结构

从上一节中，我知道了，交换环上的多项式环是个交换环，整环上的多项式环是个整环。我们很想知道，比如说域上的多项式环，或者唯一分解整环上的多项式环，分别是什么环。在这一节中，我们将会给出答案。

首先，域上的多项式环，不大可能是域。以实数域为例，实数域上的多项式环

$$\mathbb{R}[x] = \left\{ f(x) = \sum_n a_n x^n : \text{除有限项外的所有 } a_n \text{ 都等于 } 0 \right\} \tag{3.87}$$

不是一个域。我们用一个引理来证明这个结论。

引理 3.2

实数域上的多项式环 $\mathbb{R}[x]$ 不是一个域。

证明 对于 $x \in \mathbb{R}[x]$ 和任意 $f(x) \in \mathbb{R}[x] \setminus 0$，我们有

$$\deg(xf(x)) = \deg(f) + 1 \geqslant 1 \tag{3.88}$$

因此

$$xf(x) \neq 1 \tag{3.89}$$

所以 x 没有乘法逆元。因此 $\mathbb{R}[x]$ 不是一个域。

类似地，我们可以证明每个域上的多项式环都不是一个域。

可是，我们还是有非常好的结论，那就是每个域上的多项式环都是一个欧几里得整环。

要证明这个命题，我们可以先证明一个非常重要的引理，那就是多项式的长除法。

引理 3.3

令 $(R, +, \cdot)$ 是一个交换环，而 $f, g \in R[x] \setminus \{0\}$，假设 g 的首项系数是 R 中的一个单位，则存在唯一的 $q, r \in R[x]$，使得

$$f = qg + r \tag{3.90}$$

$$\deg(r) < \deg(g) \tag{3.91}$$

注意，在这里，我们将 $r = 0$ 的可能性融入在 $\deg(r) = -1 < \deg(g)$ 中了。

证明

实际上，这个引理可以用多项式长除法的算法来证明。我们将这个众所周知的算法用数学归纳法来证明。

先证存在性。取定 $m = \deg(g)$。令 $n = \deg(f)$。假如 $n < m$，则取

$$q = 0 \tag{3.92}$$

$$r = f \tag{3.93}$$

即可。因为此时我们有

$$\deg(r) = \deg(f) = n < m = \deg(g) \tag{3.94}$$

接下来，假设 $n \geqslant m$。令 $d = n - m \geqslant 0$，对 d 做数学归纳法。为了方便，令 $u = a_m(g)$ 是 g 的首项系数。根据条件，u 是 R 中的一个单位。

假如 $d = 0$，则 $m = n$，我们取

$$q = a_m(f)u^{-1} \tag{3.95}$$

$$r = f - qg \tag{3.96}$$

于是 f 与 qg 有相等的首项系数，因为

$$a_m(f) = a_m(f)u^{-1} \cdot u \tag{3.97}$$

因此 $\deg(r) < \deg(g)$。

接下来，假设对所有 $0 \leqslant d < l$，命题都成立。我们假设 $d = l$，只须证明 q 与 r 在这种情形的存在性即可。

类似地，我们取

$$q' = a_n(f)u^{-1} \tag{3.98}$$

$$r' = f - q'g \tag{3.99}$$

若 $r' = 0$ 则得证。所以我们假设 $r' \neq 0$。因此同理可得 $\deg(f - q'g) < n$。因为 $d = l$，所以特别地，

$$\deg(r') < l \tag{3.100}$$

利用数学归纳法的假设，我们可知，r' 可以进一步分解为

$$r' = qg + r \tag{3.101}$$

$$\deg(r) < \deg(g) \tag{3.102}$$

因此，此时我们有

$$f = q'g + r' = q'g + (qg + r) = (q' + q)g + r \tag{3.103}$$

$$\deg(r) < \deg(g) \tag{3.104}$$

这就证明了存在性。

再证唯一性。假设

$$f = qg + r = q'g + r' \tag{3.105}$$

$$\deg(r) < \deg(g) \tag{3.106}$$

$$\deg(r') < \deg(g) \tag{3.107}$$

我们只须证明 $q = q'$，$r = r'$。

注意到

$$(q - q')g = r' - r \tag{3.108}$$

而

$$\deg(r' - r) \leqslant \max(\deg(r), \deg(r')) < \deg(g) \tag{3.109}$$

可是 $r - r'$ 又是 g 的因式，因此我们必须有

$$q - q' = 0 \tag{3.110}$$

所以 $q = q'$，$r = r'$。这就证明了唯一性。

综上所述，我们就证明了这个引理。

命题 3.7

令 $(F, +, \cdot)$ 是一个域，则 $F[x]$ 是个欧几里得整环。

证明 令 $f \in F[x]$，$g \in F[x] \setminus \{0\}$。

假如 $f = 0$，则取 $q = 0$，$r = f$，我们就证明了 $r = 0$ 的结论。

假如 $f \neq 0$。因为 g 是非零的多项式，因此其首项系数是非零的，因为 F 是个域，所以 g 的首项系数是个单位。根据上面的引理，我们就可以找到（唯一的）$q, r \in F[x]$，使得

$$f = qg + r \tag{3.111}$$

$$\deg(r) < \deg(f) \tag{3.112}$$

假如 $r = 0$，则是显然的。假如 $r \neq 0$，则 $0 \leqslant \deg(r) < \deg(f)$。

综上所述，我们就证明了 $F[x]$ 是个欧几里得整环。

特别地，我们就得到下面两个推论。

引理 3.4

令 $(F,+,\cdot)$ 是一个域，则 $F[x]$ 是个主理想整环。 ♡

引理 3.5

令 $(F,+,\cdot)$ 是一个域，则 $F[x]$ 是个唯一分解整环。 ♡

我们很自然会问一个问题，那就是域上的多变量多项式环，是不是欧几里得整环。实际上，一般来说，连主理想整环都不是。

我们需要一个小引理作为铺垫。

引理 3.6

令 $(R,+,\cdot)$ 是一个整环，而 $f,g\in R[x]$，使得

$$x=f(x)g(x) \tag{3.113}$$

则 $f(x)=ux$ 或 u，其中 u 是 R 上的一个单位。 ♡

证明 因为 R 是个整环，因此

$$1=\deg(x)=\deg(f)\deg(g) \tag{3.114}$$

故 $\deg(f)=0$ 或1。假如 $\deg(f)=0$，则 $\deg(g)=1$，故 f 是 R 上的一个单位。

假如 $\deg(f)=1$，则 $\deg(g)=0$，同理，$f(x)=ux$，其中 u 是 R 上的一个单位。

利用这个引理，我们可以证明下面的命题。

命题 3.8

若 $n\geqslant 2$，则实数域上的多变量多项式环 $\mathbb{R}[x_1,\cdots,x_n]$ 不是一个主理想整环。 ♠

证明 假设 $n\geqslant 2$。令 I 是由 n 个单项式 $x_1,\cdots,x_n$ 生成的理想，即

$$I=(x_1,\cdots,x_n)=\mathbb{R}[x_1,\cdots,x_n]x_1+\cdots+\mathbb{R}[x_1,\cdots,x_n]x_n \tag{3.115}$$

我们只须证明，对任意 $f\in\mathbb{R}[x_1,\cdots,x_n]$，我们都有

$$I\neq(f)=\mathbb{R}[x_1,\cdots,x_n]f \tag{3.116}$$

而这几乎是显然的。因为某个主理想整环都是最大公因数环，所以根据数学归纳法，$(f)=(x_1,\cdots,x_n)$ 的充要条件是 $f=\gcd(x_1,\cdots,x_n)$。现在假设 $f=\gcd(x_1,\cdots,x_n)$，因此 f 能整除所有的单项式 x_i。

以 $i=n$ 为例，我们将在 R 上含有 n 个变量的多变量多项式 f 视作在 $R[x_1,\cdots,x_{n-1}]$ 上只含有一个变量 x_n 的单变量多项式。注意到因为整环上的多项式环还是整环，因此由数学归纳法，$R[x_1,\cdots,x_{n-1}]$ 是个整环。利用上面的引理，这里，因为 f 整除单项式 x_n，故 f 关于 x_n 必须是一个单项式，且关于 x_n 的次数小于等于 1。

类似地，对于其它的 i 我们也有类似的结论。因此，这个多项式 f 必定是一个单项式，而且它关于每一个变量的次数必须小于等于 1。可是因为 f 要生成每一个单项式 x_i，这就迫使其关于每一个变量的次数都不能等于 1，所以 f 必须是常值函数。然而常值函数是不能生成任何一个单项式 x_i 的。这就导致了矛盾。

因此，只要 $n\geqslant 2$，$\mathbb{R}[x_1,\cdots,x_n]$ 就不是一个主理想整环。

注意，这个命题可以推广。我们可以完全同理地证明，整环上的多变量多项式环都不是主理想整环。

另一个显然的推论则是

命题 3.9

若 $n\geqslant 2$，则实数域上的多变量多项式环 $\mathbb{R}[x_1,\cdots,x_n]$ 不是一个欧几里得整环。 ♠

因为我们想要知道一些特殊的环上的多项式环是什么结构，而我们刚刚仅仅知道了实数域上的多变量多项式环不是一个主理想整环，所以我们的问题一定还没有问完。因此，我们继续问，实数域上的多变量多项式环，

是不是唯一分解整环呢?

这时，答案是肯定的。我们只须证明唯一分解整环上的多项式环是唯一分解整环，就可以利用数学归纳法，递推地证明，任意唯一分解整环上的多变量多项式环都是唯一分解整环。而这就是我们接下来要证明的方向。

接下来，为了方便起见，我们考虑的环都是唯一分解整环。

首先，我们给出唯一分解整环上多项式容量与本原多项式的定义。

定义 3.10

令 $(R,+,\cdot)$ 是一个唯一分解整环，而 $f=\sum_n a_n x^n \in R[x]\setminus\{0\}$，则我们定义 f 的多项式容量，记作 $\mathrm{cont}(f)$，定义为 f 上所有系数的最大公因数，即

$$\mathrm{cont}(f)=\gcd(a_0,\cdots,a_n) \tag{3.117}$$

其中 a_n 是 f 的首项系数。而 $\mathrm{cont}(f)$ 是不一定唯一的，但是最多相差一个单位。

假如 $\mathrm{cont}(f)=1$，我们就称 f 是个本原多项式。

♣

注意，当我们说 $\mathrm{cont}(f)=1$ 的时候，我们其实在说 f 的各项系数的最大公因数是个单位。

很显然，我们可以将每一个非零多项式写成一个常数与一个本原多项式的乘积。

引理 3.7

令 $(R,+,\cdot)$ 是一个唯一分解整环，而 $f=\sum_n a_n x^n \in R[x]\setminus\{0\}$，则

$$f(x)=\mathrm{cont}(f)\frac{f(x)}{\mathrm{cont}(f)} \tag{3.118}$$

其中 $f(x)/\mathrm{cont}(f)$ 是个本原多项式。

♡

证明 证明是显然的，我们只须注意到

$$\frac{\gcd(a_0,\cdots,a_n)}{\mathrm{cont}(f)}=\gcd\left(\frac{a_0}{\mathrm{cont}(f)},\cdots,\frac{a_n}{\mathrm{cont}(f)}\right) \tag{3.119}$$

即可。因为这立刻告诉我们

$$\frac{f(x)}{\mathrm{cont}(f)} \tag{3.120}$$

是本原的。

我们对本原多项式有个极为重要的引理，称为高斯引理。它的论述非常简单，即唯一分解整环上两个本原多项式的乘积仍是本原的。

命题 3.10 (高斯引理)

令 $(R,+,\cdot)$ 是一个唯一分解整环，而 $f,g\in R[x]\setminus\{0\}$ 是两个本原多项式，则 fg 也是本原多项式。

♠

证明 假设 R 是个唯一分解整环。假设 f,g 是 R 上的两个非零本原多项式，只须证明 fg 是本原多项式。

用反证法，假设 p 是一个素元素，并且 p 整除 fg 的所有系数。令

$$f(x)=a_0+\cdots+a_m x^m \tag{3.121}$$

$$g(x)=b_0+\cdots+b_n x^n \tag{3.122}$$

则

$$f(x)g(x)=a_0b_0+(a_0b_1+a_1b_0)x+\cdots+(a_mb_n)x^{m+n} \tag{3.123}$$

利用极值原理。考虑到 p 不可能整除所有的 a_i，也不可能整除所有的 b_j，因此 p 一定不整除某些 a_i 和某些 b_j。我们令 r,s 分别是最小的 i,j 使得 $p\nmid a_i$ 及 $p\nmid b_j$。因此 $r\leqslant m$，$r\leqslant n$。

根据假设，

$$p|a_{r+s}(fg)=\sum_{i+j=r+s}a_ib_j=a_0b_{r+s}+\cdots+a_{r-1}b_{s+1}+a_rb_s+a_{r+1}b_{s-1}+\cdots+a_{r+s}b_0 \tag{3.124}$$

可是，$p|a_0,\cdots,a_{r-1}$，且 $p|b_{s-1},\cdots,b_0$，故

$$p|\left((a_0b_{r+s}+\cdots+a_{r-1}b_{s+1})+(a_{r+1}b_{s-1}+\cdots+a_{r+s}b_0)\right) \tag{3.125}$$

因此，

$$p|a_rb_s \tag{3.126}$$

而这是不可能的。因为 $p\nmid a_r$，$p\nmid b_s$。

综上所述，我们就证明了高斯引理，即唯一分解整环上两个本原多项式的乘积仍然是一个本原多项式。

特别地，高斯引理实际上告诉我们一个重要的推论，那就是含量函数 cont 是个乘性函数，即

引理 3.8

令 $(R,+,\cdot)$ 是一个唯一分解整环，而 $f,g\in R[x]\setminus\{0\}$，则 f 与 g 乘积的含量是它们含量之积，即

$$\operatorname{cont}(fg)=\operatorname{cont}(f)\operatorname{cont}(g) \tag{3.127}$$

♡

证明 令 f,g 是唯一分解整环 R 上的两个非零多项式。我们分别将 f 和 g 写成

$$f(x)=\operatorname{cont}(f)f_1(x) \tag{3.128}$$

$$g(x)=\operatorname{cont}(f)g_1(x) \tag{3.129}$$

其中 f_1 和 g_1 是本原的。

故

$$f(x)g(x)=\operatorname{cont}(f)\operatorname{cont}(g)f_1(x)g_1(x) \tag{3.130}$$

其中 f_1g_1 是本原的，因此 f_1g_1 各项系数的最大公因数是 1，而 fg 各项系数的最大公因数是 $\operatorname{cont}(f)\operatorname{cont}(g)$。根据定义，这就等于 $\operatorname{cont}(fg)$。故

$$\operatorname{cont}(fg)=\operatorname{cont}(f)\operatorname{cont}(g) \tag{3.131}$$

综上所述，我们就证明了这个引理。

有人也将上面这个引理称为高斯引理。不难发现，它们之间是等价的。我们把证明留给感兴趣的读者。

下面，我们要介绍另一个重要的引理，我们介绍它的目的也是为了证明唯一分解整环上的多项式环是唯一分解整环。我们要证明这样的多项式环是唯一分解整环，但是我们尚且不知道对于一个 $R[x]$（R 是唯一分解整环）上的多项式来说，我们可以怎么分解，更不用提怎么证明唯一分解了。可是，我们不要忘记，在上一章中我们曾经学过，每一个整环都可以构造出一个域，称为分式域。在这里，唯一分解整环 R 是一个整环，因此其分式域 $\operatorname{Frac}(R)$ 是个域，而它上面的多项式环则是主理想整环，进而是唯一分解整环。所以一个重要的思路，就是通过 $\operatorname{Frac}(R)[x]$ 上的分解，来构造出 $R[x]$ 上的分解，并且证明唯一性。

引理 3.9

令 $(R,+,\cdot)$ 是一个唯一分解整环，令 $F=\operatorname{Frac}(R)$ 是 R 的分式域。令 $f\in R[x]\subset F[x]$，则我们有以下结论

1. 若 $f=c$ 是常值函数，则 f 在 $R[x]$ 上不可约当且仅当 c 在 R 上不可约。
2. 若 f 不是常值函数，即 $\deg(f)\geqslant 1$，则 f 在 $R[x]$ 上不可约，当且仅当 f 是本原多项式且 f 在 $F[x]$ 上不可约。

♡

证明 第一，先假设 $f=c$ 是常值函数。充分性是显然的，因为如果 c 在 R 上可约，那么 c 一定在 $R[x]$ 上也可约（因为我们可以认为 R 是 $R[x]$ 的子环）。

我们来证必要性，而只须证明其逆否命题。假设 $f=c$ 在 $R[x]$ 上可约，我们只须证明 f 在 R 上可约。

而这几乎是显然的。因为此时 $c=g(x)h(x)$。根据多项式次数的关系，我们有

$$\deg(gh)=\deg(g)+\deg(h)=\deg(c)\leqslant 0 \tag{3.132}$$

因此 g 和 h 都必须是常值函数。因此 $g,h\in R$ 是环 $R[x]$ 上的非单位。于是 g,h 也是环 R 上的非单位。这是因为如果 g 在 R 中有乘法逆元，那么因为 R 可以看成 $R[x]$ 的子环，所以 g 在 $R[x]$ 中也会有乘法逆元，这就矛

盾了。所以 g,h 必须是 R 上的非单位，而这就证明了 $f=c$ 在 R 上可约。这就证明了必要性，也就证明了整个第一点。

第二，再假设 f 不是常值函数。必要性是显然的，因为如果 f 在 $R[x]$ 上可约，那么 f 在 $F[x]$ 上也可约（因为我们可以认为 $R[x]$ 是 $F[x]$ 的子环）。

我们来证充分性。假设 f 在 $R[x]$ 上是不可约的。

我们先证明 f 是本原多项式。这是很简单的。假如 f 不是本原多项式，那么 f 的各项系数的最大公因数是个非单位。又因为 $\deg(f(x)/\mathrm{cont}(f))=\deg(f(x))\geqslant 1$，故

$$f(x)=\mathrm{cont}(f)\frac{f(x)}{\mathrm{cont}(f)} \tag{3.133}$$

给出了 f 在 $R[x]$ 上的一个非平凡分解。这就导致了矛盾。因此，f 必须是（$R[x]$ 上的）本原多项式。

我们再证明 f 在 $F[x]$ 上是不可约的。假如 $f(x)=g(x)h(x)$，其中 $g,h\in F(x)$。根据分式域的定义以及多项式非零系数的有限性，我们可以通过乘上某些 $a,b\in R$，使得 $ag(x),bh(x)\in R[x]$。一般来说，我们可以选择分母的最大公因数作为这里的 a 和 b。因此，我们就知道，在环 $R[x]$ 中，

$$f(x)=abg(x)h(x) \tag{3.134}$$

两边同时取容量，我们就得到了

$$1=\mathrm{cont}(f)=ab\,\mathrm{cont}(g)\,\mathrm{cont}(h) \tag{3.135}$$

这就迫使了 a,b 是单位，而 g,h 是 $R[x]$ 上本原多项式。这就给出了 f 在 $R[x]$ 上的非平凡分解，而这与我们假设的 f 在 $R[x]$ 上不可约是矛盾的。因此，我们就证明了 f 在 $R[x]$ 上是不可约的。这就证明了充分性，也就证明了整个第二点。

综上所述，我们就证明了这个引理。

下面，我们终于可以证明唯一分解整环上的多项式环是个唯一分解整环。

命题 3.11

令 $(R,+,\cdot)$ 是一个唯一分解整环，则 $R[x]$ 是个唯一分解整环。

证明 假设 R 是个唯一分解整环，而 f 是 R 上的一个多项式。令 $F=\mathrm{Frac}(R)$ 是 R 的分式域。因为 $R\subset F$，所以 f 可以被视作 F 上的多项式。

先证分解的存在性。

因为 $F[x]$ 是主理想整环，进而是唯一分解整环，故存在 $F[x]$ 上的（唯一）分解

$$f(x)=cg_1(x)\cdots g_n(x) \tag{3.136}$$

其中 $c\in F$，而 $g_1,\cdots,g_n\in F[x]$。通过对 $g_1,\cdots,g_n$ 乘上一些 R 中的常数 $a_1,\cdots,a_n$，我们可以得到 $h_1(x)=a_1g_1(x),\cdots,h_n(x)=a_ng_n(x)\in R[x]$。再假设 $h_1(x)=\mathrm{cont}(h_1)f_1(x),\cdots,h_n(x)\,\mathrm{cont}(h_n)f_n(x)$，则 $f_1,\cdots,f_n$ 是 R 上的本原多项式。为了方便，记

$$d=c\frac{a_1\cdots a_n}{\mathrm{cont}(h_1)\cdots\mathrm{cont}(f_n)} \tag{3.137}$$

故我们有

$$\mathrm{cont}(f)\frac{f(x)}{\mathrm{cont}(f)}=f(x)=df_1(x)\cdots f_n(x) \tag{3.138}$$

其中 $f/\mathrm{cont}(f)$ 是个本原多项式。因此

$$d\sim\mathrm{cont}(f)\in R \tag{3.139}$$

这告诉我们，f 可以分解成 R 中的一个常数与若干个 R 上本原多项式的乘积。要注意，这里的 $f_1,\cdots,f_n$ 在 $F[x]$ 上仍是不可约的，因为 $g_1\cdots,g_n$ 是 $F[x]$ 上不可约的，而 $f_1,\cdots,f_n$ 只是它们的（F 中）标量倍而已。于是，根据上面介绍的引理，因为 $f_1,\cdots,f_n$ 是 R 上本原多项式，且在 $F[x]$ 上不可约，所以它们在 $R[x]$ 上也不可约。

进一步地，利用 R 的唯一分解性质，我们可以找到 d 的唯一分解

$$d = d_1 \cdot d_m \tag{3.140}$$

同样根据上面的引理，我们知道 $d_1, \cdots, d_m$ 在 $R[x]$ 中也是不可约的。这就证明了分解的存在性。

再证分解的唯一性。假设

$$f(x) = c_1 \cdots c_m g_1(x) \cdots g_n(x) = d_1 \cdots d_{m'} h_1(x) \cdots h_{n'}(x) \tag{3.141}$$

其中所有 c_i, d_j 在 $R[x]$ 中不可约，故在 R 中不可约；所有 g_i, h_j 在 $R[x]$ 不可约，故都在 $F[x]$ 中不可约，且都是 $R[x]$ 上本原多项式。因此，通过对上式同时取含量，我们可以得到

$$c_1 \cdots c_m \sim d_1 \cdots d_{m'} \tag{3.142}$$

利用 R 是个唯一分解整环，我们证明了这些元素在一个重排下是两两等价的。

另一方面，因为 $F[x]$ 是个唯一分解整环，所以 g_i 和 h_j 也在一个重排下两两等价。而这就证明了分解的唯一性。

综上所述，我们证明了 $R[x]$ 上的多项式存在唯一分解。因此，我们就证明了这个命题，即每一个唯一分解整环上的多项式环都是唯一分解整环。

更妙的是，利用数学归纳法，我们就可以递归地证明，唯一分解整环上的多变量多项式环都是唯一分解整环，即

命题 3.12

令 $(R, +, \cdot)$ 是一个唯一分解整环，而 $n \geqslant 1$，则 $R[x_1, \cdots, x_n]$ 是个唯一分解整环。

证明 利用数学归纳法，这是显然的。

于是，我们就回答了前面提出的问题，即 $\mathbb{R}[x_1, \cdots, x_n] (n \geqslant 2)$ 是什么结构。答案便是唯一分解整环。

引理 3.10

若 $n \geqslant 1$，则 $\mathbb{R}[x_1, \cdots, x_n]$ 是个唯一分解整环。特别地，若 $n = 1$，则 $\mathbb{R}[x]$ 是个主理想整环。

证明 这是显然的。

3.3 不可约多项式

在这一节中，我们会介绍著名的艾森斯坦判别法。这个判别法给出了在唯一分解整环上不可约多项式的充分条件，而这个充分条件是很好检验的。而且更妙的是，就算多项式本身不能通过这个充分条件的检查，我们仍然可以对多项式作一些简单的变换，使变换后的多项式满足充分条件，而根据不可约在这类变换下的不变形，我们就能证明本来的多项式也是不可约的。

下面，我们直接给出这个命题。

命题 3.13 (艾森斯坦判别法)

令 $(R, +, \cdot)$ 是一个唯一分解整环，而 $F = \mathrm{Frac}(R)$ 是它的分式域。令 $f(x) \in R[x]$ 是一个非常数多项式，即 $\deg(f) \geqslant 1$。令 $n = \deg(f)$，则 $f(x)$ 可以写成

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \tag{3.143}$$

假如存在某个素元素 $p \in R$，使得

$$p \nmid a_n \tag{3.144}$$

$$p | a_{n-1}, \cdots, p | a_0 \tag{3.145}$$

$$p^2 \nmid a_0 \tag{3.146}$$

则 $f(x)$ 在 $F[x]$ 上是不可约的。进一步地，如果 $f(x)$ 是 $R[x]$ 上的本原多项式，那么 $f(x)$ 在 $R[x]$ 上也是不可约的。

证明 用反证法，假设 $f(x)$ 在 $F[x]$ 上是可约的，则存在 $g(x), h(x) \in F[x]$，使得

$$g(x) = b_0 + \cdots + b_m x^m \tag{3.147}$$

$$h(x) = c_0 + \cdots + c_l x^l \tag{3.148}$$

$$f(x) = g(x)h(x) \tag{3.149}$$

因为 $p|a_0$ 而 $p^2 \nmid a_0$，所以 p 整除 b_0 和 c_0 中的恰好一个，不失一般性，假设 $p|b_0$，而 $p \nmid c_0$。接下来，我们用数学归纳法，证明对于任意 $0 \leqslant k \leqslant n-1$，我们有 $p|b_k$。

假设对于所有 $0 \leqslant k < l \leqslant n-1$，我们有 $p|b_k$，则当 $k = l$ 时，由于

$$p|a_l = b_0 c_l + b_1 c_{l-1} + \cdots + b_{l-1} c_1 + b_l c_0 \tag{3.150}$$

其中 $p|b_0, \cdots, b_{l-1}$，所以 $p|(b_l c_0)$。可是 $p \nmid c_0$，因此我们有 $p|b_l$。这就证明了 $p|b_0, \cdots, p|b_{n-1}$。

同理，因为 $p \nmid a_n$，而

$$a_n = b_0 c_n + b_1 c_{n-1} + \cdots + b_{n-1} c_1 + b_n c_0 \tag{3.151}$$

所以 $p \nmid b_n$，这就迫使 $m = \deg(g) = \deg(f) = n$，因此 $h(x) = c \in F \setminus \{0\}$ 是个非零常数。于是，在 $F[x]$ 上，$f(x)$ 只能被分解为

$$f(x) = cg(x) \tag{3.152}$$

可是 $c \in F \setminus \{0\}$ 在 F 上是个单位，在 $F[x]$ 上也是个单位，所以 $f(x)$ 在 $F[x]$ 上一定是不可约的。这就导致了一个矛盾。因此，$f(x)$ 在 $F[x]$ 上是不可约的。

进一步地，根据上面讲过的引理，当 $f(x)$ 在 $R[x]$ 上是本原多项式，即含量为 1 时，我们就知道 $f(x)$ 在 $R[x]$ 上也是不可约的。

我们来看一个具体的例子。

例题 3.1 证明 $f(x) = x^3 + 20x^2 - 6x + 2$ 在 $\mathbb{Z}[x]$ 是不可约的。

证明 注意到首项系数是 1，其余系数都是 2 的倍数，而常数项系数不是 4 的倍数。因此，我们可以使用艾森斯坦判别法。令 $R = \mathbb{Z}$，而 $p = 2$，则所有条件都满足。又因为 f 的含量显然是 1（因为首项系数是 1），所以 $f(x)$ 不仅在 $\mathbb{Q}[x]$ 上不可约，更在 $\mathbb{Z}[x]$ 上不可约。此即得证。

第 4 章 域论——Field Theory

4.1 域

这一章是抽代 I 的最后一章，我们会讲解域论。由于伽罗瓦理论对初学者的难度很大，我们会放到抽代 II 再讲。为了保证我们讲义在逻辑和认知上的连贯性，我们会尽力在这一章中为伽罗瓦理论铺，同时又不给大家带来困惑。这样做是非常需要智慧的，我们会尽心尽力为之。

域的定义早在环论就讲过，我们再提一次。

定义 4.1

令 $(F,+,\cdot)$ 是一个环，则我们称 $(F,+,\cdot)$ 是个域，若

1. F 是个交换环。
2. F 的每个非零元素都是单位（即都有逆元）。

♣

等价地，我们有以下的定义。

引理 4.1

我们称 $(F,+,\cdot)$ 是个域，若

1. $(F,+)$ 是个阿贝尔群。
2. $(F\setminus\{0\},\cdot)$ 是个阿贝尔群。
3. F 中的乘法对加法有分配律。

♡

注意到域是特殊的环，所以有不少定义和结论和环论是一致的。当然，有一些结果是更好的。我们先来看域同态。

定义 4.2

令 $(F,+,\cdot)$，$(F',+,\cdot)$ 是两个域，则我们称 $f:F\to F'$ 是个域同态，若 f 是个环同态，即

$$f(1)=1' \tag{4.1}$$

$$\forall x,y\in F, f(x+y)=f(x)+f(y) \tag{4.2}$$

$$\forall x,y\in F, f(xy)=f(x)f(y) \tag{4.3}$$

♣

由于域同态和环同态的定义是几乎完全一样的，所以我们大部分时候不区分这两个词，统一用环同态这个词。同理，我们不需要再列出域同构三定理，因为其形式和结论也是几乎完全一样的。而且，一般来说域同态是很少见的。我们往往是用环同态构造出域同构的。

事实上，任何一个域同态都是一个单射。

命题 4.1

若 $f:F\to F'$ 是个域同态，则 f 是个单射。

♠

要证明这个命题，我们只须证明一个更一般的引理，即从域到非零环的环同态都是单射。

引理 4.2

若 $f:F\to R$ 是个环同态，其中 F 是个域，R 不是零环，则 f 是个单射。

♡

证明 用反证法。假设 f 不是单射，则 $\ker(f)\neq\{0\}$。任取非零元素 $a\in F$，使得

$$f(a)=0 \tag{4.4}$$

因为 F 是个域，所以 a 有乘法逆元 a^{-1}。因此

$$f(1) = f(aa^{-1}) = f(a)f(a^{-1}) = 0 \cdot f(a^{-1}) = 0 \tag{4.5}$$

因为 R 不是零环，所以 $f(1) = 0 \neq 1$。可是环同态要求把乘法单位元映到乘法单位元。这就导致了一个矛盾。

综上所述，我们就证明了这个引理，即每一个从域到非零环的环同态都是单射。

那么利用这个引理，我们当然可以证明每个域同态都是单射。注意，这实际上是个非常好的性质。因为在环论中，我们有数不清的环同态都不是单射，而在这里，只要定义域是个域，而陪域是个非零环，任何一个环同态都是单射了。从这里，也能看出域这个结构“好”的地方。

讲了域同态，我们来讲子域。同样的，一个域的子域就是既要是子集又要是域。和以往一样，我们也要简单的判别准则。

定义 4.3

令 $(F,+,\cdot)$ 是一个域，而 $E \subset F$，则我们称 E 是 F 的子域，若

1. E 在相同的加法和乘法下构成一个域。

命题 4.2

令 $(F,+,\cdot)$ 是一个域，而 $E \subset F$，则 E 是 F 的子域，当且仅当

$$1 \in E \tag{4.6}$$

$$\forall a,b \in E, a+b, -b, a*b \in E \tag{4.7}$$

$$\forall b \in E \setminus \{0\}, \frac{1}{b} \in E \tag{4.8}$$

简单来说，就是包含了乘法单位元，又在加、乘及加乘的逆运算下封闭。等价地，就是说包含了乘法单位元，又在加减乘除下都封闭。

证明 如果 E 是个子域，那么 $(E,+,\cdot)$ 就是个域，所以这些条件当然都满足。

另一方面，假设 E 满足这些条件，我们只须证明 E 是个子域。

不难发现，通过这些条件，我们可以知道

$$0 = 1 - 1 \in E \tag{4.9}$$

所以实际上，我们可以将其分为两组。一组是包含加法单位元、在加法下封闭以及每个元素有加法逆元；另一组是包含乘法单位元、在乘法下封闭以及每个非零元素有乘法逆元。

实际上，这分别告诉我们 $(E,+)$ 是个子群，以及 $(E \setminus \{0\},\cdot)$ 是个子群。特别地，由于 F 对加法和乘法是交换的，所以这两个群都是阿贝尔群。又因为 F 上的乘法对加法有分配律，所以 E 上也存在这样的分配律。这就证明了 E 是个子域。

综上所述，这就证明了这个命题。我们通过这个命题，找到了子域的充要条件。

和之前几章类似，我们也可以定义由一个域的非空子集所生成的子域。

定义 4.4

令 $(F,+,\cdot)$ 是一个域，而 $A \subset F$ 是个非空子集，则我们定义由 A 生成的子域，记作 (A)，定义为 F 中包含 A 的最小的子域，即

$$(A) = \bigcap_{A \subset E < F} E \tag{4.10}$$

和以往一样，我们要证明这里的 (A) 确实是个子域。

命题 4.3

令 $(F,+,\cdot)$ 是一个域，而 $A\subset F$ 是个非空子集，则 $(A)<F$。

证明 假设 E 是任意一个包含了 A 的 F 中子域。显然 0 和 1 属于每一个这样的 E，因此 $0,1\in(A)$。

令 $a,b\in(A)$，$c\in(A)\setminus\{0\}$。则对任意这样的 E，我们有

$$a+b,-a,\frac{1}{c}\in E \tag{4.11}$$

所以

$$a+b,-a,\frac{1}{c}\in(A) \tag{4.12}$$

综上所述，这就证明了 (A) 是个子域（$(A)\subset F$ 是显然的）。

现在，假设 F 是个域，我们给出特征的定义。在域论中，域的特征是极其重要的。无论我们是否在意，它都会自然而然地出现在域的讨论中。事实上，通过特征，我们在每个域中都能找到我们熟悉的域的影子，要么是有理数域 $\mathbb{Q}$，要么是有 p 个元素（p 是素数）的有限域 $\mathbb{F}_p$。下面，我们给出定义。

定义 4.5

令 $(F,+,\cdot)$ 是一个域，若存在某个正整数 n，使得

$$n\cdot 1=1+\cdots+1=0 \tag{4.13}$$

则我们称最小的这个正整数为 F 的特征，记作 $\mathrm{char}(F)$。

假如不存在这样的正整数，我们称 F 的特征为零，即 $\mathrm{char}(F)=0$

实际上，一个域的特征要么是 0，要么是某个素数 p。我们先证明一个引理。

引理 4.3

令 $(F,+,\cdot)$ 是一个域。定义 $f:\mathbb{Z}\to F$，定义为

$$f(n)=n\cdot 1 \tag{4.14}$$

则这是个环同态。因此 $\ker(f)$ 是 $\mathbb{Z}$ 中的某个理想，即存在 $n\in\mathbb{N}_0$，使得 $\ker(f)=(n)$。

证明 根据群论的知识及数学归纳法，我们不难证明这是个环同态。根据群论，$\ker(f)$ 作为 $\mathbb{Z}$ 的子群，必须是 (n) 的形式。

实际上，一个域的特征，基本上就是这个域的加法子群中 1 的阶（除非它是特征零的）。

引理 4.4

令 $(F,+,\cdot)$ 是一个域。令 n 是 F 的加法子群中 1 的阶。若 $n<\infty$，则 $\mathrm{char}(F)=n$；若 $n=\infty$，则 $\mathrm{char}(F)=0$。

证明 根据阶与特征的定义，这是自明的。

注意，我们在这里罗列上面的引理，目的是为了让大家联系起群论和环论的知识，更好地掌握域论的知识。

下面，我们证明，若一个域的特征非零（即我们反复地加 1，总能在有限次内得到 0），则特征必须是某个素数。

命题 4.4

令 $(F,+,\cdot)$ 是一个域，而 $\mathrm{char}(F)\neq 0$，则 $\mathrm{char}(F)=p$ 是一个素数。

证明 假设 $\mathrm{char}(F)$ 是个合数，则存在整数上的非平凡分解 $\mathrm{char}(F)=ab$，其中 $a,b\geqslant 2$。则不难发现，

$$(a\cdot 1)(b\cdot 1)=(ab)\cdot 1=0 \tag{4.15}$$

然而

$$a \cdot 1 \neq 0 \tag{4.16}$$

$$b \cdot 1 \neq 0 \tag{4.17}$$

这就告诉我们 F 不是整环。这显然和域的条件矛盾。因此，$\mathrm{char}(F)$ 要么是零，要么是个素数。

我们如何进一步刻画特征零或特征是素数的域呢？大家来看下面两个命题。

命题 4.5

令 $(F,+,\cdot)$ 是一个域，而 $\mathrm{char}(F)=0$。则存在一个域同态 $f:\mathbb{Q}\to F$。由于域同态总是单射，因此 $f(\mathbb{Q})<F$，给出了一个有理数域在域 F 中的嵌入。

注意，我们没有给过嵌入的定义。简单地解释一下，在代数中，A 到 B 的一个嵌入就是 A 到 B 的单同态。在几何中我们也有嵌入的概念，当然也希望是单射，并且保留一些结构（在几何中则是几何结构）。几何的话题当然不是我们的重点，我们来证明这个命题。

证明 假设 F 是个特征为零的域，我们定义 $f:\mathbb{Q}\to F$，对任意 $a\in\mathbb{Z}$，$b\in\mathbb{Z}\setminus\{0\}$，定义为

$$f\left(\frac{a}{b}\right)=\frac{a\cdot 1}{b\cdot 1} \tag{4.18}$$

注意到，这里的分母 $b\cdot 1$ 永远不等于 0，这恰恰是因为 F 是特征为零的。因此，这是良定义的。我们只须证明 f 是个环同态。这样 f 就必须是域同态，进而是个单射。

不难发现，

$$f(1)=\frac{1\cdot 1}{1\cdot 1}=1 \tag{4.19}$$

另一方面，利用

$$a\mapsto a\cdot 1 \tag{4.20}$$

是个从 $\mathbb{Z}$ 到 F 的环同态，及 F 域的性质，我们很容易证明 f 在加、乘及加乘的逆运算下都封闭。具体的证明我们完全可以留做练习，因为没有任何新的难点，只需要逐条检验即可。事实上，大家如果去尝试，很快就会发现，靠 $a\mapsto a\cdot 1$ 是个环同态这个信息，我们完全足够证明这个 f 是环同态了。

这样，我们就证明了这个命题，即每个特征零的域都可以被有理数域嵌入。

另一方面，每个特征为（素数）p 的域都可以被 $\mathbb{F}_p\simeq\mathbb{Z}_p$ 嵌入。

命题 4.6

令 $(F,+,\cdot)$ 是一个域，而 $\mathrm{char}(F)=p$，其中 p 是个素数。则存在一个域同态 $f:\mathbb{Z}_p\to F$。由于域同态总是单射，因此 $f(\mathbb{Z}_p)<F$，给出了一个有 p 个元素的有限域 $\mathbb{F}_p$（或 $\mathbb{Z}_p$）在域 F 中的嵌入。

证明 我们可以利用之前证明过的 $f:\mathbb{Z}\to F$ 的环同态，即

$$a\mapsto a\cdot 1 \tag{4.21}$$

因为 $\mathrm{char}(F)=p$，所以等价地，我们有 $\ker(f)=(p)$。根据环同构第一定理，我们就得到了一个域同态

$$\tilde{f}:\mathbb{Z}_p\to F \tag{4.22}$$

这显然是个单射（域同态都是单射）。

综上所述，我们就证明了这个命题，即每个特征为素数 p 的域都可以被 $\mathbb{Z}_p$ 嵌入。

实际上，我们有一个极其重要的 Frobenius（环）自同态。Frobenius 自同态不仅在特征 p 的域上有定义，甚至在特征 p 的交换环都有定义（p 是个素数）。为了得到更一般的结论，我们先定义环的特征，再定义特征 p 的交换环上的 Frobenius 自同态。

环的特征的定义是一模一样的。

定义 4.6

令 $(R,+,\cdot)$ 是一个环，若存在某个正整数 n，使得

$$n\cdot 1 = 1+\cdots+1 = 0 \tag{4.23}$$

则我们称最小的这个正整数为 R 的特征，记作 $\mathrm{char}(R)$。

假如不存在这样的正整数，我们称 R 的特征为零，即 $\mathrm{char}(R)=0$

定义 4.7

若 R 是个特征为素数 p 的交换环，则我们定义 R 上的 Frobenius 自同态为 $f:R\to R$，对于 $a\in R$，定义

$$f(a)=a^p \tag{4.24}$$

这个定义看似很普通，但其实暗藏玄机。最重要的惊人性质是一个在一般的实数或复数域上不可能成立的性质，即对于任何 $a,b\in R$，我们会有

$$(a+b)^p = a^p+b^p \tag{4.25}$$

连小学生都知道，这样的式子一般是不成立的。然而在特征为素数 p 的交换环中，这就是成立的。我们把这个结论放在自同态的性质中一起证明。

命题 4.7

令 R 是个特征为素数 p 的交换环，则 R 上的 Frobenius 自同态 $a\mapsto a^p$ 是个环同态。

证明 第一，$f(1)=1^p=1$。

第二，$f(a+b)=(a+b)^p$，利用交换环上的二项式定理（我们为了主线的连贯性，没有证明过交换环上的这个定理，请感兴趣的读者自行验证，方法是数学归纳法），我们有

$$(a+b)^p = a^p+\binom{p}{1}a^{p-1}b^1+\cdots+\binom{p}{p-1}a^1b^{p-1}+b^p \tag{4.26}$$

为了照顾不熟悉初等数论的读者，我们来证明一个众所周知的结论，即对于素数 p 和 $1\leqslant k\leqslant p-1$，我们有

$$p\left|\binom{p}{k}\right. \tag{4.27}$$

这是因为

$$\binom{p}{k}=\frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1} \tag{4.28}$$

是个整数。注意到分子是 p 的倍数，而分母不是 p 的倍数，因此这个整体是 p 的倍数。因为我们假设 R 是特征 p 的，因此中间的所有项都等于 0 了。因此，我们就有

$$f(a+b)=(a+b)^p=a^p+b^p=f(a)+f(b) \tag{4.29}$$

另一方面，同样因为 R 是交换环，我们有

$$f(ab)=(ab)^p=a^pb^p=f(a)f(b) \tag{4.30}$$

综上所述，我们就证明了 f 是个环自同态。

特别地，对于特征有限（即为素数 p）的域，我们也有 Frobenius 自同态。

引理 4.5

令 $(F,+,\cdot)$ 是一个域，而 $\mathrm{char}(F)=p$ 是个素数，则 $f:F\to F$，定义为 $a\mapsto a^p$，是个自同态，称为（特征为素数 p 的）域 F 上的 Frobenius 自同态。

证明 因为每个域都是交换环，所以这是显然的。

实际上，对于有限域来说（我们马上给出定义），Frobenius 自同态会变成 Frobenius 自同构，即加入了双射的结论。这是更加美妙的。我们来定义有限域，并证明这个优美的结论。

定义 4.8

令 $(F,+,\cdot)$ 是一个域，则我们称 F 是个有限域，若 F 是个有限集。 ♣

这是自明的定义。我们在下一节中就会证明，每一个有限域的阶不是任意的，而一定是某个素数的幂次，即具有 p^n 的形式，其中 p 是个素数而 n 是个正整数。一般来说，我们用 q 来表示素数的幂次，即记成 $q=p^n$。未来，我们还会证明，如果两个有限域的大小一样，那么它们是同构的，因此，正如我们有 $\mathbb{F}_p=\mathbb{Z}_p$ 来表示有 p 个元素的有限域那样，我们会用 $\mathbb{F}_q=\mathbb{F}_{p^n}$ 来表示有 $q=p^n$ 个元素的有限域。

对于特征为素数 p 的有限域 $\mathbb{F}$ 来说，Frobenius 自同态变成 Frobenius 自同构。

命题 4.8

令 $(F,+,\cdot)$ 是个有限域，而 $\mathrm{char}(F)=p$，则 Frobenius 自同态 $a\mapsto a^p$ 是个 F 上的自同构。 ♠

证明 证明是非常简单的。注意到 f 是 F 上的环自同态，而定义域和陪域都是域 F，所以这是个域同态。我们知道每一个域同态都是单射，所以 f 是个单射。

又因为 f 的定义域和陪域都是有限集，且大小相等，因此这样的单射一定是双射。这就证明了 f 是一个双射的域自同态，而这就是域自同构的定义。我们称其为（特征为素数 p 的有限域）F 上的域自同构。

4.2 域扩张

在域论中，我们特别关注所谓的“域扩张”。假如说子域是从大的域到小的域，那么域扩张就是从小的域到大的域。定义是极其简单的。但是这个区别实际上是本质的，它表明了我们的核心意图——不是在乎子域，而是在乎扩域。我们不满足于域本身的性质，而想要更好的性质。

在一定程度上，这代表了我们对知识的贪婪。域的性质太好，不像环论那样，环的结构本身可以探讨很久。域不一样，域的结构很简单，性质很好，难道我们就不研究域了吗？不，我们还是要研究，只不过换一个角度。还记得我们在环论开头时刚提到域时就讲的吗？虽然域是特别的环，但是环论和域论探究的问题是很不一样的。具体还有什么区别呢，请听我们继续为大家讲述。我们先给出域扩张的定义。

定义 4.9

令 E，F 是两个域。我们称 F/E 是个域扩张，或 F 是 E 的扩域，当

$$E\text{ 是 }F\text{ 的子域。} \tag{4.31}$$

♣

所以我们有一个显然的引理。

引理 4.6

令 E，F 是两个域，则 F/E 是个域扩张当且仅当 E 是 F 的子域。 ♡

证明 根据定义，这是显然的。

我们一定要注意域扩张的左右顺序，写在左边的是大的域，写在右边的是小的域。这个记号并不表示一个“商结构”，而只是形式地表示左边的域是右边的扩域（或右边的域是左边的子域）。在某种程度上，用这种记号就是为了方便。比起说 E,F 是两个域，E 是 F 的子域，我们只用说 F/E 是个域扩张。的确方便很多。因为初学者可能会误解，以为 F/E 是个新的结构，所以我们特别花一些笔墨在这里解释一下。

从这里开始，我们假设大家学习过严格的线性代数，例如抽象的（建立在域上的）向量空间。

我们回顾向量空间的定义。用抽代的语言来说，我们会知道，向量空间就是域上的模（我们会在抽代 II 中介绍模论）。什么意思呢？下面，我们用群论的语言简化定义。

定义 4.10

令 F 是一个域，而 $(V,+)$ 是个阿贝尔群。假如存在标量乘法 $\cdot : F\times V\to V$，使得

$$\forall v\in V, 1v=v \tag{4.32}$$

$$\forall a,b\in F,\forall v\in V,(a+b)v=av+bv \tag{4.33}$$

$$\forall a\in F,v,w\in V,a(v+w)=av+aw \tag{4.34}$$

$$\forall a,b\in F,\forall v\in V,a(bv)=(ab)v \tag{4.35}$$

则我们称 V 是 F 上的向量空间。我们称 V 中的元素为向量，而 F 中的元素为标量。

我们很快注意到，若 F/E 是个域扩张，则 F 是 E 上的向量空间。

命题 4.9

令 F/E 是个域扩张，则 F 是 E 上的向量空间。

证明 首先 $(E,+,\cdot)$ 当然是个域，而 $(F,+)$ 当然是个阿贝尔群。我们定义 F 上的标量乘法是 F 上的乘法限制在 $E\times F$，即对于任意 $a\in E,v\in F$，我们定义

$$a\cdot v=av \tag{4.36}$$

因此，剩下四个条件都可以从 F 的域的条件中轻易得到。我们把具体的证明留给感兴趣的读者。

综上所述，我们证明了这个命题。

既然说了向量空间，我们快速复习一下张成、维数、线性组合、线性相关与线性无关的概念和性质。

定义 4.11

令 V 是域 F 上的向量空间，而 $v_1,\cdots,v_m\in V$，则我们定义它们的张成为

$$\operatorname{span}(v_1,\cdots,v_m)=\{a_1v_1+\cdots+a_mv_m:a_1,\cdots,a_m\in F\}=Fv_1+\cdots+Fv_m \tag{4.37}$$

定义 4.12

令 V 是域 F 上的向量空间，则我们称 V 是有限维的，或有限生成的，若存在有限多个 $v_1,\cdots,v_m$，使得

$$V=\operatorname{span}(v_1,\cdots,v_m) \tag{4.38}$$

命题 4.10

若 V 是域 F 上的有限维向量空间，则我们称 V 的维数是 n，记作 $\dim(V)=n$，若 n 是最小的 m，使得 V 可以被 m 个向量张成（或生成）。特别地，我们记 $\dim(V)=0$，若 $V=\{0\}$，我们可以认为 V 被零个向量张成。

定义 4.13

若 V 是域 F 上的向量空间，而 $v_1,\cdots,v_m\in V$。假如 $v\in V$，则我们称 v 是 $v_1,\cdots,v_m$ 的一个线性组合，若 v 可以写成

$$v=a_1v_1+\cdots+a_mv_m \tag{4.39}$$

的形式。其中 $a_1,\cdots,a_m\in F$ 是 m 个标量。

因此，张成就是由所有线性组合所构成的集合。

定义 4.14

若 V 是域 F 上的向量空间，而 $v_1,\cdots,v_m\in V$。我们称这些向量是线性无关的，若

$$\forall a_1\cdots,a_n\in F,(a_1v_1+\cdots+a_nv_n=0\implies a_1=\cdots=a_n=0) \tag{4.40}$$

换言之，对 $v_1,\cdots,v_m$ 来说，只有平凡的线性组合能得到 0。

定义 4.15

若 V 是域 F 上的有限维向量空间，而 $v_1,\cdots,v_m\in V$。我们称 $v_1,\cdots,v_m$ 构成了 V 上的一组基，若它们张成了整个向量空间 V，并且是线性无关的。

命题 4.11

若 V 是域 F 上的有限维向量空间，则任意一组基的元素个数都是相等的，就是 V 的维数。

更妙的是，在有限维向量空间中，任何一组线性无关的向量都可以通过添加某些向量（或者不添加）变成一组基，任何一组张成了整个向量空间的向量都可以通过删除某些向量（或者不删除）变成一组基。

命题 4.12

若 V 是域 F 上的有限维向量空间，其中 $\dim(V)=n$，而 $v_1,\cdots,v_m\in V$ 是线性无关的一组向量。则我们一定有 $m\leqslant n$，并且存在 $v_{m+1},\cdots,v_n\in V$，使得 $v_1,\cdots,v_n$ 是 V 的一组基。

命题 4.13

若 V 是域 F 上的有限维向量空间，其中 $\dim(V)=n$，而 $v_1,\cdots,v_m\in V$ 张成了整个向量空间 V，即 $\operatorname{span}(v_1,\cdots,v_m)=V$。则我们一定有 $m\geqslant n$，并且可以删掉其中的 $n-m$ 个向量，在一个重排下可以假设删掉的是最后 $n-m$ 个向量，使得 $v_1,\cdots,v_n$ 是 V 的一组基。

我们可以定义一个向量空间的子向量空间。当然，我们也有简单的判别准则。

定义 4.16

令 V 是域 F 上的一个向量空间，而 $U\subset V$，则我们称 U 是 V 的子向量空间，记 $U<V$，若 U 也是域 F 上的向量空间。

命题 4.14

令 V 是域 F 上的一个向量空间，而 $U\subset V$，则 U 是 V 的子向量空间当且仅当

$$0\in U \tag{4.41}$$

$$\forall u,v\in U,u+v\in U \tag{4.42}$$

$$\forall a\in F,\forall u\in U,au\in U \tag{4.43}$$

换言之，子向量空间就是包含了单位元 0，而且在加法和标量乘法下封闭。

现在，我们回到域论的讨论。我们刚才已经证过，如果 F/E 是个域扩张，那么 F 就是 E 上的向量空间。也就是说，我们认为 E 是一个域，而 F 是一个向量空间（虽然它也是一个域），那么我们就可以谈论 F 在 E 上的维数，成为这个域扩张的扩张次数。维数要么是有限的，要么是无限的。

定义 4.17

令 F/E 是个域扩张，则 F 在 E 上的扩张次数，记为 $[F:E]$，定义为 F 作为一个向量空间，在 E 上的维数。

若 F 是 E 上的有限维向量空间，则称 F 是 E 的有限扩张。反之，则称 F 是 E 的无限扩张。

如果 F/E 的扩张次数是 2，我们可以说 F 是 E 的二次扩域。如果这个扩张次数是 3，我们可以说 F 是 E 的三次扩域，以此类推。

假如 E/k 是个域扩张，而 F/E 也是个域扩张，那么 E/k 当然也是域扩张（因为子域的包含关系），我们很在意，这些扩张次数之间，是否有着子群般的联系。回答是肯定的。

命题 4.15

令 F/E，E/k 是两个有限的域扩张（在不引起歧义的情况下我们可以称 $F/E/k$ 是个嵌套的域扩张），则我们有

$$[F:k]=[F:E][E:k] \tag{4.44}$$

证明 假设 $[F:E]=m$，$[E:k]=n$。注意到维数是一组基的元素个数。我们假设 F 在 E 上有一组基，称为 $\{f_1,\cdots,f_m\}$；假设 E 在 k 上有一组基，称为 $\{e_1,\cdots,e_n\}$。

我们只须证明，$B=\{f_ie_j\}_{i,j}$ 是 F 在 k 上的一组基。

一方面，我们要证明在域 k 上，这组向量 B 张成了整个 F。令 $v\in F$。由于 $\{f_1,\cdots,f_m\}$ 是一组 F 在 E 上的基，则存在 $a_1,\cdots,a_m\in E$，使得

$$v=a_1f_1+\cdots+a_mf_m \tag{4.45}$$

又因为对于任意的 $i\in\{1,\cdots,m\}$，我们有 $a_i\in E$. 同理，由于 $\{e_1,\cdots,e_n\}$ 是一组 E 在 k 上的基，我们可以找到 $b_{i1},\cdots,b_{in}\in k$，使得

$$a_i=b_{i1}e_1+\cdots+b_{in}e_n \tag{4.46}$$

因此

$$v=\sum_i a_if_i=\sum_i\left(\sum_j a_{ij}e_j\right)f_i=\sum_{i,j}a_{ij}f_ie_j \tag{4.47}$$

这就证明了 $B=\{f_ie_j\}_{i,j}$ 在 k 上张成了 F。

另一方面，我们要证明这些 f_ie_j 是线性无关的，即 $B=\{f_ie_j\}_{i,j}$ 在 k 上是线性无关的。假设对 $1\leqslant i\leqslant m$，$1\leqslant j\leqslant n$，我们有 $a_{ij}\in k$，使得

$$\sum_{i,j}a_{ij}f_ie_j=0 \tag{4.48}$$

我们只须证明所有的 a_{ij} 都是 0。

注意到所有的 f_i 是在 E 线性无关的。我们可以将上式改写成

$$\sum_i\left(\sum_j a_{ij}e_j\right)f_i \tag{4.49}$$

其中对任意 $1\leqslant i\leqslant m$，我们都有 $\sum_j a_{ij}e_j\in E$。所以利用 $\{f_1,\cdots,f_m\}$ 在 E 上的线性无关性，我们可以得到，对任意 $1\leqslant i\leqslant m$，我们有

$$\sum_j a_{ij}e_j=0 \tag{4.50}$$

同理，又因为 $\{e_1,\cdots,e_n\}$ 在 k 上的线性无关性，我们可以得到所有的 a_{ij} 都等于 0。而这就证明了 $B=\{f_ie_j\}_{i,j}$ 在 k 上是线性无关的。

综上所述，$B=\{f_ie_j\}_{i,j}$ 是 F 在 k 上的一组基。因此我们就证明了这个命题，即对于任意嵌套的域扩张 $F/E/k$，我们有 $[F:k]=[F:E][E:k]$。

特别地，我们知道了两个有限域扩张的嵌套还是有限的域扩张，即

引理 4.7

若 F/E 和 E/k 都是有限的域扩张，那么 F/k 也是有限的域扩张。

证明 利用上面的命题，我们甚至可以找到 F/k 的扩域维数。我们当然有

$$[F:k]=[F:E][E:k]<\infty \tag{4.51}$$

实际上，讲了向量空间以后，我们可以进一步探索有限域的结构。在这里，我们几乎可以轻描淡写地证明，每个有限域的阶（即元素个数）必须是某个素数的幂次，即 $q=p^n$ 的形式。

命题 4.16

令 $(F,+,\cdot)$ 是一个域。若 F 是个有限域，则 $\mathrm{char}(F)=p$ 是个素数。特别地，存在 $n\in\mathbb{N}$，使得 $|F|=p^n$。

证明 我们在上一节中已经证明了有限域的特征一定是个素数，在这里设 F 的特征为 p。实际上，我们也证明过有限域 $\mathbb{F}_p\simeq\mathbb{Z}_p$ 可以嵌入到 F 中。因此 $\mathbb{F}_p$ 的同构的像，作为一个 p 阶的有限域，是 F 的子域。因此，为了方便起见，我们可以（在同构的意义下）认为 F 是 $\mathbb{F}_p$ 的一个扩域。由于 F 是个有限域，所以扩域次数 $[F:\mathbb{F}_p]<\infty$。令 $n=[F:\mathbb{F}_p]$，取 $\{e_1,\cdots,e_n\}\subset F$ 是 F 在 $\mathbb{F}_p$ 下的一组基。则每个 F 的元素可以唯一地写成

$$a_1e_1+\cdots+a_ne_n \tag{4.52}$$

其中 $a_1,\cdots,a_n\in\mathbb{F}_p$。因为 $|\mathbb{F}_p|=p$，所以

$$|F|=|\mathbb{F}_p|^n=p^n \tag{4.53}$$

综上所述，这就证明了这个命题，即每个有限域的阶都是某个素数的幂次，即 $q=p^n$。

我们很在乎一种重要的域扩张 F/E，其中 F 是由 F 中的有限多个元素和域 E 所生成的（子域）。对于这样的域扩张，我们称为有限生成域扩张。我们先定义一个域 F 中由有限多个元素和一个子域 $E<F$ 所生成的域，再定义并刻画有限生成域扩张。

定义 4.18

令 F/E 是一个域扩张，若 $a_1,\cdots,a_n\in F$，则我们定义由 $a_1,\cdots,a_n$ 和域 E 生成的子域，记为 $E(a_1,\cdots,a_n)$，定义为域 F 中最小的包含了 $a_1,\cdots,a_n$ 和 E 的子域。按上一节的记号，此即

$$E(a_1,\cdots,a_n)=(E\cup\{a_1,\cdots,a_n\}) \tag{4.54}$$

进一步展开，等价地说，这就是

$$E(a_1,\cdots,a_n)=\bigcap_{\substack{a_1,\cdots,a_n\in k\\ E\subset k<F}}k \tag{4.55}$$

定义 4.19

令 F/E 是一个域扩张，若存在 $a_1,\cdots,a_n\in F$，使得 $F=E(a_1,\cdots,a_n)$，则我们称 F 在 E 上是有限生成的，或称 F/E 是个有限生成的域扩张。特别地，如果 $n=1$，则 F 可以写成 $F=E(a_1)$，此时我们称 F/E 是个单扩张（或简单扩张）。

这里的重难点就是有限生成域扩张和有限域扩张的区别。我们现在就要指出，有限生成的性质未必是“好”的：有时候，连单扩张都会是无限扩张（我们马上会知道，这样的生成元素 a_1 叫做超越元素），因此有限生成的域扩张一般来说不是有限的。可是反过来，有限的域扩张的性质很“好”：每一个有限域扩张都是有限生成的。下面，我们尽量按照逻辑顺序，不紧不慢地证明这些重要的性质。

我们先来证明，每个有限的域扩张都是有限生成的。

命题 4.17

令 F/E 是一个域扩张。若 F/E 是有限的，则它是有限生成的。

证明 假设 F/E 是个有限域扩张，即 F 是 E 上的有限维向量空间。令 $n=[F:E]$，我们取一组基 $\{f_1,\cdots,f_n\}\in F$。

要证明 F/E 是有限生成的，我们只须证明

$$E(f_1,\cdots,f_n)=F \tag{4.56}$$

因为等号左边是包含了 E 和 $f_1,\cdots,f_n$ 的最小的域，所以我们只需证明等号右边是一个域，而且每一个包含了 E 和 $f_1,\cdots,f_n$ 的域都会包含整个 F。

注意到等号右边的 F 本身就是一个域。另外，如果 k 是个包含了 E 和 $f_1,\cdots,f_n$ 的域。令 $a_1,\cdots,a_n\in E$，则利用加法和乘法封闭性，我们有

$$a_1f_1+\cdots+a_nf_n\in k \tag{4.57}$$

由于 $f_1,\cdots,f_n$ 张成了 F，所以

$$F\subset k \tag{4.58}$$

综上所述，这就证明了

$$E(f_1,\cdots,f_n)=F \tag{4.59}$$

下面，我们来介绍单扩张。我们来看几个例子。因为这块研究的历史原因，以及本身就是最直观、最好理解的，我们选定域扩张中的那个子域是有理数域 $\mathbb{Q}$。我们设生成元是 $a\in\mathbb{C}$。

第一个例子：生成元 $a\in\mathbb{Q}$。

引理 4.8

若 $a\in\mathbb{Q}$，则 $\mathbb{Q}(a)=\mathbb{Q}$。因此，$[\mathbb{Q}(a):\mathbb{Q}]=1$。♡

证明 一方面，$\mathbb{Q}$ 是个域。

另一方面，若 F 是 $\mathbb{C}$ 的子域，且包含了 $\mathbb{Q}$ 和 a。我们只须证明 F 包含 $\mathbb{Q}$。可是因为 $a\in\mathbb{Q}$，所以这是显然的。

综上所述，我们就证明了这个引理。

第二个例子：若 $a=\sqrt{d}$，其中 $d\in\mathbb{Z}$，而且 $|d|$ 不是完全平方数（这样假设的两个原因：一个是 $\sqrt{d}$ 是最简二次根式，另一个是使得 $\mathbb{Q}(a)$ 不是 $\mathbb{Q}$）。

引理 4.9

若 $a=\sqrt{d}$，其中 $d\in\mathbb{Z}$，而且 $|d|$ 不是完全平方数，则

$$\mathbb{Q}(a)=\{r+sa:r,s\in\mathbb{Q}\} \tag{4.60}$$

其中 $1,a$ 在 $\mathbb{Q}$ 上是线性无关的。特别地，$[\mathbb{Q}(a):\mathbb{Q}]=2$。♡

证明 一方面，如果 F 是包含了 $\mathbb{Q}$ 和 a 的域，那么显然对任意 $r,s\in\mathbb{Q}$，我们有

$$r+sa\in F \tag{4.61}$$

因此，我们只须证明 $\{r+sa:r,s\in\mathbb{Q}\}$ 是个域。注意到 $1,a$ 在 $\mathbb{Q}$ 上是线性无关的。本质上是因为 $a\notin\mathbb{Q}$。假如

$$r+sa=0 \tag{4.62}$$

假如 $s=0$，那么显然 $r=0$。假如 $s\neq0$，那么 $a=-r/s\in\mathbb{Q}$，而这是不可能的。因此 $1,a$ 在 $\mathbb{Q}$ 上确实是线性无关的。

所以，$\mathbb{Q}(a)$ 作为 $\mathbb{Q}$ 上以 $\{1,a\}$ 为基的向量空间，对加法构成子群。等到我们证明了这是个域，就可以证明 $[\mathbb{Q}(a):\mathbb{Q}]=2$ 了。

接下来，我们证明它包含了 1，且在乘法下封闭。$1=1+0a\in\{r+sa:r,s\in\mathbb{Q}\}$。若 $r+sa,r'+s'a\in\{r+sa:r,s\in\mathbb{Q}\}$，则

$$(r+sa)(r'+s'a)=(rr'+ss'd)+(rs'+r's)a\in\{r''+s''a:r'',s''\in\mathbb{Q}\} \tag{4.63}$$

最后，要证明非零元素在乘法逆元下封闭。假设 $r+sa\neq 0$，则 r,s 不都等于 0，所以 $r-sa\neq 0$。因此

$$\frac{1}{r+sa}=\frac{r-sa}{(r+sa)(r-sa)}=\frac{r-sa}{r^2-s^2d}\in\{r'+s'a:r',s'\in\mathbb{Q}\} \tag{4.64}$$

所以 $\{r+sa:r,s\in\mathbb{Q}\}$ 是个域。因此，结合证明刚开始提到的，我们就证明了 $\mathbb{Q}(a)=\{r+sa:r,s\in\mathbb{Q}\}$。证明之中，我们也证明了 $[\mathbb{Q}(a):\mathbb{Q}]=2$。

下面是一些在数论中被称为二次数域的例子。

$$\mathbb{Q}(i)=\{r+si:r,s\in\mathbb{Q}\} \tag{4.65}$$

$$\mathbb{Q}\left(\sqrt{2}\right)=\left\{r+s\sqrt{2}:r,s\in\mathbb{Q}\right\} \tag{4.66}$$

$$\mathbb{Q}\left(\sqrt{-5}\right)=\left\{r+s\sqrt{-5}:r,s\in\mathbb{Q}\right\} \tag{4.67}$$

接下来，我们留给感兴趣的读者证明

引理 4.10

$\mathbb{Q}\left(\sqrt[3]{2}\right)=\left\{r+s\sqrt[3]{2}+t\left(\sqrt[3]{2}\right)^2:r,s,t\in\mathbb{Q}\right\}$，其中 $\left[\mathbb{Q}\left(\sqrt[3]{2}\right):\mathbb{Q}\right]=3$。 ♡

证明 我们把几乎全部的证明留给感兴趣的读者作为练习。但是我们会给一个最重要的提示，那就是在证明乘法逆元时，我们可以利用完全立方公式

$$(a+b)\left(a^2-ab+b^2\right)=a^3+b^3 \tag{4.68}$$

将分母有理化。剩余的证明，对于认真学习的大家，一定不是问题。

下面，我们来证明一个更一般的结论，即在每一个有限单扩张 $E(a)/E$ 中，都可以找到某个 $n\in\mathbb{N}_1$，使得 $\{1,a,\ldots,a^{n-1}\}$ 是 $E(a)$ 在 E 上的一组基，其中 $n=[E(a):E]$。而每一个无限的单扩张 $E(a)/E$，实际上同构于 E 上的有理函数域，即 E 上多项式环 $E[x]$ 的分式域，记作 $E(x)$。

命题 4.18

令 F/E 是一个域扩张，而 $a\in F$。若 $E(a)/E$ 是个有限扩张，则存在唯一的首一非零多项式 $p(x)$，使得

$$\forall f(x)\in E[x],(f(a)=0\implies p(x)|f(x)) \tag{4.69}$$

我们称这个多项式为 a 在域 F 上的最小多项式。 ♠

注意，首一多项式指的是最高次系数是 1 的多项式。

证明 我们构造代入同态 $\phi:E[x]\to E(a)$，定义为

$$\phi(f(x))=f(a) \tag{4.70}$$

根据上一章节的讨论，因为 E 是个域，所以 $E[x]$ 是个主理想整环。我们在乎的是 ϕ 的核，因为它就是由所有在 a 点取值为 0 的多项式所组成的理想。因为 $E[x]$ 是个主理想整环而 $\ker(\phi)\lhd E[x]$，所以 $\ker(f)$ 是个主理想。

第一类情况，我们假设这个主理想不是 (0)，则 $\ker(f)$ 由一个非零多项式生成。考虑到在域 E 上的多项式环 $E[x]$ 中，所有的单位就是 E 中的单位，即 E 中的非零元素。那么，我们可以通过乘上某个单位，得到唯一的代表元素，即唯一的首一多项式 $p(x)$，使得

$$\ker(\phi)=(p(x)) \tag{4.71}$$

而这就证明了，所有使得 $f(a)=0$ 的 $E[x]$ 中的非零多项式 $f(x)$，必须整除这个唯一的首一多项式 $f(x)$。

第二类情况，假如这个主理想是 (0)。那么不存在任何非零多项式 $f(x)$，使得 $f(a)=0$。为了得到矛盾，我们只须证明对任意 $n\in\mathbb{N}_1$，$\{1,a,\cdots,a^{n-1}\}$ 都是在 E 上线性无关的。而这是因为，如果 $n\in\mathbb{N}_1$，而 $e_0,\cdots,e_{n-1}\in F$，使得

$$e_0+e_1a+\cdots+e_{n-1}a^{n-1}=0 \tag{4.72}$$

则由于不存在任何非零多项式 $f(x)$，使得 $f(a)=0$，所以 $e_1=\cdots=e_{n-1}=0$，而这就迫使 $e_0=0$，而这就证明了对所有 $n\in\mathbb{N}_1$，$\{1,a,\cdots,a^{n-1}\}$ 都是在 E 上线性无关的。那么这样 $[E(a):E]$ 就不可能是有限的，而这与 $E(a)/E$ 是有限扩张相矛盾。所以 $\ker(\phi)$ 不可能是 (0)。

综上所述，我们就证明了这个命题。

一个显而易见的引理是：这样的最小多项式是不可约的。

引理 4.11

令 F/E 是一个域扩张，而 $a\in F$。若 $E(a)/E$ 是个有限扩张，则 a 在 E 上的最小多项式 $p(x)$ 是不可约的。♡

证明 用反证法。假设 $p(x)=f(x)g(x)$，其中 f 和 g 是 $E[x]$ 中的非常数多项式。由于 $p(a)=f(a)g(a)=0$，我们可以不失一般性假设 $f(a)=0$，然而 $\deg(f)<\deg(p)$，就导致了一个矛盾。因此 $p(x)$ 在 $E[x]$ 上是不可约的。

根据有限单扩张上最小多项式的存在性和不可约性，我们可以证明刚才所说的：每一个有限单扩张 $E(a)/E$ 中，都可以找到某个 $n\in\mathbb{N}_1$，使得 $\{1,a,\ldots,a^{n-1}\}$ 是 $E(a)$ 在 E 上的一组基，其中 $n=[E(a):E]$。

注意，这个结论美妙的地方就在于用多项式的形式刻画了扩域的样子。这说明了上面举的几个例子并非特例，而是有限单扩张的普遍情形，例如若 $a\in\mathbb{Q}$，则 a 在 $\mathbb{Q}$ 上的最小多项式是 $x-a$；若 $a=\sqrt{d}$，而 $|d|$ 不是完全平方数，则 a 在 $\mathbb{Q}$ 上的最小多项式是 x^2-d；$\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的最小多项式是 x^3-2。

我们还需要一个引理。

引理 4.12

令 F/E 是一个域扩张，而 $a\in F$。假设 $E(a)/E$ 是个有限扩张，令 $p(x)$ 是 a 在 E 上的最小多项式，则

$$E[x]/(p(x))\simeq E(a) \tag{4.73}$$

♡

证明 考虑同样的代入同态，即 $\phi:E[x]\to E(a)$，定义为

$$\phi(f(x))=f(a) \tag{4.74}$$

根据上一命题，我们知道若 $p(x)$ 是 a 在 E 上的最小多项式，则

$$\ker(\phi)=(p(x)) \tag{4.75}$$

根据环同构第一定理，我们有

$$E[x]/(p(x))\simeq \mathrm{im}(\phi)<E(a) \tag{4.76}$$

因为 $p(x)$ 是不可约的，所以 $(p(x))$ 是个素理想。注意到 $E[x]$ 是个主理想整环，所以 $(p(x))$ 是个极大理想，因此 $E[x]/(p(x))$ 是个域。因此它的同构的像 $\mathrm{im}(\phi)$ 也是个域。这个域显然包含 E 和 a，因此根据 $E(a)$ 是最小的包含了 E 和 a 的 F 中子域，我们就得到了 $E(a)<\mathrm{im}(\phi)$。又因为 $\mathrm{im}(\phi)<E(a)$，所以 $\mathrm{im}(\phi)=E(a)$，此即

$$E[x]/(p(x))\simeq E(a) \tag{4.77}$$

这就证明了这个命题。

命题 4.19

令 F/E 是一个域扩张，而 $a\in F$。假设 $E(a)/E$ 是个有限扩张，令 $p(x)$ 是 a 在 E 上的最小多项式，而 $\deg(p)=n$，则 $\{1,a,\cdots,a^{n-1}\}$ 是 $E(a)$ 在 E 上的一组基，即

$$E(a)=\left\{e_0+e_1a+\cdots+e_{n-1}a^{n-1}:e_0,\cdots,e_{n-1}\in E\right\} \tag{4.78}$$

其中描述法中的这些元素是两两不同的。特别地，我们有

$$E(a)=E[a] \tag{4.79}$$

♠

证明 假设 $[E(a):E]=n$，根据上面的引理，我们知道

$$E[x]/(p(x))\simeq E(a) \tag{4.80}$$

其中 $\deg(p) = n$。因此我们只须研究 $E[x]/(p(x))$ 的结构即可。利用带余除法，我们很快发现，每一个 $E[x]/(p(x))$ 的元素，可以唯一地表示成

$$f(x) + (p(x)) \tag{4.81}$$

其中 $0 \leqslant \deg(f) < \deg(p) = n$，这就证明了

$$E[x]/(p(x)) = \left\{(e_0 + e_1 x + \cdots + e_{n-1}x^{n-1}) + (p(x)) : e_0, \cdots, e_{n-1} \in E\right\} \tag{4.82}$$

因此，

$$E(a) = \left\{e_0 + e_1 a + \cdots + e_{n-1}a^{n-1} : e_0, \cdots, e_{n-1} \in E\right\} \tag{4.83}$$

下面，我们来证明这些元素是两两不同的。假如 $f(x), g(x) \in E[x]$，其中 $0 \geqslant \deg(f), \deg(g) < n$，使得 $f(a) = g(a)$。我们只须证明 $f = g$。注意到 $(f-g)(a) = 0$，所以根据最小多项式的性质，$p(x)|(f-g)(x)$，因此 $n|\deg(f-g)$。又因为 $0 \leqslant \deg(f-g) < n$，所以 $f - g = 0$，即 $f(x) = g(x)$。这就证明了这些元素是两两不同的。

综上所述，我们就证明了

$$E(a) = E[a] = \operatorname{span}(1, a, \cdots, a^{n-1}) = \left\{e_0 + e_1 a + \cdots + e_{n-1}a^{n-1} : e_0, \cdots, e_{n-1} \in E\right\} \tag{4.84}$$

实际情况中，我们应该如何找到一个有限单扩张中元素的逆呢？其实等价地，我们可以问，如果 E 是一个域，而 $p(x) \in E[x]$ 是一个不可约多项式，我们怎么找到 $f(x) + (p(x)) \in E[x]/(p(x))$ 的逆呢？我们用一个引理来表达。

引理 4.13

令 $(E, +, \cdot)$ 是一个域，$p(x) \in E[x]$ 是个不可约多项式，而 $\deg(p) = n$。令 $f(x) + (p(x)) \in E[x]/(p(x))$，不失一般性，假设 $0 \leqslant \deg(f) < n$。因为 $\gcd(f(x), p(x)) = 1$，则存在 $g(x) \in E[x]$，使得

$$f(x)g(x) \equiv 1 \bmod (p(x)) \tag{4.85}$$

因此 $g(x) + (p(x))$ 是 $E[x]/(p(x))$ 中 $f(x) + (p(x))$ 的逆。 ♡

证明 证明的本质实际上就是数论中著名的裴蜀定理的翻版。因为 $E[x]$ 是个欧几里得整环，所以我们可以对一对多项式 $f(x)$ 和 $p(x)$ 做辗转相除法，直到得到它们的最大公因式 $\gcd(f, p)$。在这里因为 $p(x)$ 是不可约的，而 $f(x)$ 的次数是小于 $p(x)$ 的次数的，因此 $\gcd(f, p) = 1$。所以我们可以找到多项式的线性组合

$$f(x)g(x) + p(x)h(x) = 1 \tag{4.86}$$

其中 $g(x), h(x) \in E[x]$。特别地，这就告诉我们

$$f(x)g(x) \equiv 1 \bmod (p(x)) \tag{4.87}$$

综上所述，我们就证明了这个引理。

由这个引理，我们就可以找到有限单扩张中元素的逆了。

引理 4.14

令 F/E 是一个域扩张，而 $a \in F$。假设 $E(a)/E$ 是个有限扩张，令 $p(x)$ 是 a 在 E 上的最小多项式，而 $\deg(p) = n$。假设 $f = e_0 + e_1 a + \cdots + e_{n-1}a^{n-1} \in E(a)$，令 $f(x) = e_0 + e_1 x + \cdots + e_{n-1}x^{n-1} \in E[x]$，而 $g(x) + (p(x)) \in E[x]/(p(x))$ 是 $f(x) + (p(x))$ 的逆，则在 $E(a)$ 中，

$$\frac{1}{f} = \frac{1}{e_0 + e_1 a + \cdots + e_{n-1}a^{n-1}} = \frac{1}{f(a)} = g(a) \in E(a) \tag{4.88}$$

♡

证明 我们只须注意到同样的事实，即 $f(x) \mapsto f(a)$ 给出了从 $E[x]/(p(x))$ 到 $E(a)$ 的双射。因为在左边，我们有

$$(f(x) + (p(x)))(g(x) + (p(x))) = 1 + (p(x)) \tag{4.89}$$

所以

$$f(a)g(a) = 1 \tag{4.90}$$

而这就完成了证明。

注意，上面这两个引理在实际的计算中是非常有用的。因为在实践中，比起存在性，我们更在乎如何计算。对于单扩张中元素的逆，我们将元素的问题转化为多项式的问题，再借助多项式的理论来解决这个问题。你说，这是不是非常美妙呢？在抽象代数中，我们常常会将问题转化。因此，要真正理解这一门学科，必须要拥有大局观，即所谓的“Big Picture”，不能花太多时间去了解所有的细枝末节——在很多时候，知道一些重要的定理和方法就足够了，你会在具体的练习和问题中进一步锻炼自己。事实上，在数学研究中，有不少重要的定理是通过跨领域的知识来解决的。因此，越有大局观的人，就越容易找到概念与概念间隐藏的关系。找到这样关系的过程，就是数学研究。

下面，我们准备好讲解代数扩张了。讲了代数扩张，我们终于可以把之前遗留的关于有限扩张和有限生成扩张关联的问题给解决了。

首先，我们给出定义。

定义 4.20

令 F/E 是一个域扩张，而 $a \in F$。如果 $E(a)/E$ 是个有限扩张，则我们称 a 在 E 上是个代数数。反之，若 $E(a)/E$ 是个无限扩张，那么我们称 a 在 E 上是个超越数。 ♣

根据上面的讨论，我们立刻得到下面的引理。

引理 4.15

令 F/E 是一个域扩张，而 $a \in F$。则 a 在 E 上是个代数数当且仅当存在某个非零多项式 $p(x) \in E[x]$，使得

$$p(a) = 0 \tag{4.91}$$

相反，a 在 E 上是个超越数当且仅当对任意非零多项式 $p(x) \in E[x]$，我们都有

$$p(a) \neq 0 \tag{4.92}$$

♡

事实上，我们知道两个重要的无理数 e 和 π 都是（$\mathbb{Q}$ 上的）超越数。当然，对这两个超越数的证明不在我们这节课要讨论的范围之中。感兴趣的读者可以自行参考相关的材料。我们容易证明常见的 $i, \sqrt{2}, \sqrt[3]{2}$ 这类数都是（$\mathbb{Q}$ 上的）代数数。

下面，我们给出代数扩张的定义。这个定义几乎是自明的。

定义 4.21

令 F/E 是一个域扩张。我们称 F/E 是个代数扩张，若任意 $f \in F$ 都是 E 上的代数数。反之，我们称 F/E 是个超越扩张，若存在至少一个 $f \in F$ 是 E 上的超越数。 ♣

下面我们要证明一个重要的命题，即一个扩张是有限扩张当且仅当它既是有限生成扩张，又是代数扩张。

命题 4.20

令 F/E 是一个域扩张，则 F/E 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。 ♠

证明 先证充分性。假设 F/E 是个有限扩张，则我们知道它一定是有限生成扩张。我们只须证明它是代数扩张。令 $a \in F$。用反证法，假设 a 是个超越数。则不存在任何非零多项式 $p(x) \in E[x]$，使

$$p(a) = 0 \tag{4.93}$$

这立刻就说明了 $\{1, a, a^2, \cdots, a^{n-1}\}$ 对任何 $n \in \mathbb{N}_1$ 都是线性无关的，这和 F/E 是个有限扩张相矛盾（有限扩张就是说维数是有限的）。因此，F/E 一定是个代数扩张。

再证必要性。我们假设 F/E 是个有限生成的代数扩张，即 $F = E(a_1, \cdots, a_m)$，其中每一个 a_i 在 E 上都是代数数。用数学归纳法。假如 $m = 1$，而 $F = E(a)$，其中 a 在 E 上是代数的，则我们知道 $E(a) = E[a] =$

$\mathrm{span}(1,a,\cdots,a_{n-1})$，其中 $n=[E(a):E]$，这就证明了 $E(a)/E$ 是有限的（即维数有限）。接着，假设命题对 $m=k$ 成立，则当 $m=k+1$ 时，若 $F=E(a_1,\cdots,a_{k+1})$，则我们知道 $F=(E(a_1,\cdots,a_k))(a_{k+1})$。其中 $a_1,\cdots,a_k$ 在 E 上是代数的，所以根据归纳假设，我们有 $E(a_1,\cdots,a_k)/E$ 是有限的。接着，因为 a_{k+1} 在 E 上是代数的，则它在 $E(a_1,\cdots,a_k)$ 上也是代数的（因为我们可以取相同的非零多项式），因此，我们就知道 $F=(E(a_1,\cdots,a_k))(a_{k+1})$ 在 E 上是个代数扩张。这样，我们就证明了每个有限生成的代数扩张都是有限扩张。

综上所述，我们就证明了这个命题，即一个域扩张是有限扩张的充要条件是它既是有限生成扩张，又是代数扩张。

在结束这一节前，我们还剩一个内容没有讨论，那就是 E 上无限的单扩域 $E(a)$ 与有理函数域 $E(x)$ 是同构的。首先我们定义域上的有理函数域。

定义 4.22

令 $(E,+,\cdot)$ 是一个域，则 E 上的有理函数域，记作 $E(x)$，定义为 E 上多项式环 $E[x]$ 的分式域，即

$$E(x)=\mathrm{Frac}(E[x]) \tag{4.94}$$

也就是说，任意一个 $r(x)\in E(x)$，都可以在一个显然的等价关系下（形式地）写成

$$r(x)=\frac{f(x)}{g(x)} \tag{4.95}$$

其中 $f(x)\in E[x]$，$g(x)\in E[x]\setminus\{0\}$。

命题 4.21

令 $(F,+,\cdot)$ 是一个域，则 E 上的有理函数域是个域。

证明 注意到 $E[x]$ 是个主理想整环，因此显然是整环。所以 $E[x]$ 的分式环是个域，即分式域 $E(x)$，在这里就是有理函数域。

下面，我们来证明 E 上无限的单扩域 $E(a)$ 与有理函数域 $E(x)$ 是同构的。

命题 4.22

令 F/E 是一个域扩张，而 $a\in F$。若 $E(a)/E$ 是个无限扩张，即 $[E(a):E]=\infty$，则

$$E(a)\simeq E(x) \tag{4.96}$$

证明 我们还是构造代入同态 $\phi:E[x]\to E(a)$，定义为

$$\phi(f(x))=f(a) \tag{4.97}$$

因为 $E(a)$ 是无限扩张，所以 $\ker(\phi)$ 必须是 (0)，也就是说对于任意非零多项式 $f(x)\in E[x]$，我们都有

$$f(a)\neq 0 \tag{4.98}$$

所以我们可以将这个代入同态延拓到有理函数域 $E(x)$ 中，即定义 $\tilde{\phi}:E(x)\to E(a)$，对任意 $f(x)/g(x)\in E(x)$，定义为

$$\tilde{\phi}\left(\frac{f(x)}{g(x)}\right)=\frac{f(a)}{g(a)} \tag{4.99}$$

因为 $g(x)\neq 0$，所以分母不为零；又因为如果 $f/g=h/l$，那么 $fl=gh$，则 $f(a)l(a)=g(a)h(a)$，所以 $\tilde{\phi}$ 是良定义的。

我们同样很容易验证这是个域同态，即保持了 1，加法和乘法。域同态都是单射，所以 $\tilde{\phi}$ 是个单射。我们只须证明 $\tilde{\phi}$ 是个满射。

因为 $E(a)$ 定义为包含了 E 和 a 的最小的域，所以我们只须证明

$$\tilde{\phi}(E(x))=\left\{\frac{f(a)}{g(a)}:f(x)\in E[x],g(x)\in E[x]\setminus\{0\}\right\} \tag{4.100}$$

是个包含了 E 和 a 的域。

注意 $\tilde{\phi}(E(x))$ 是由所有 a 的所有有理表达式构成的集合。我们很容易证明它包含了 $0,1$，且在加减乘除下都封闭（除法要求除数不为零）。最重要的是除法，我们发现

$$\left(\frac{f(a)}{g(a)}\right)^{-1}=\frac{g(a)}{f(a)} \tag{4.101}$$

这就证明了 $\tilde{\phi}(E(x))$ 是个包含了 E 和 a 的域，所以它就是 $E(a)$。因此 $\tilde{\phi}$ 是一个域同构。因此，

$$E(a)\simeq E(x) \tag{4.102}$$

综上所述，我们就证明了这个命题，即 E 上无限的单扩域 $E(a)$ 与有理函数域 $E(x)$ 是同构的。

换言之，若 a 在 E 上是个超越数，那么 $E(a)\simeq E(x)$。

我们举一个小小的例子，我们知道 π（在 $\mathbb{Q}$ 上）是个超越数，所以 $\mathbb{Q}(\pi)\sim\mathbb{Q}(x)$。更具体地，$\mathbb{Q}(\pi)$ 就是由所有 π 在 $\mathbb{Q}$ 上的有理表达式所构成的域。

4.3 有限域与分裂域

我们仿照着之前的做法，借有限域而讨论分裂域。

假如 F 是个有限域，我们知道它的特征一定是某个素数 p（这是因为它是个整环）。此时，又因为 F 可以认为是 F_p 的一个扩域，因此（至少在同构意义下）作为 $\mathbb{F}_p$ 上的向量空间，它的元素个数必定是 p 的某个幂次，记作 $q=p^n$。我们在这一节的一个重要目标是证明阶相等的有限域是两两同构的，即如果 F_1 和 F_2 都是有 $q=p^n$ 个元素的有限域，那么

$$F_1\simeq F_2 \tag{4.103}$$

我们首先回顾 Frobenius 同态 $a\mapsto a^p$，因为 F 是特征 p，所以它是个单同态。又因为 F 是有限的，所以这是个双射，即同构。

一个美妙的事实便是，Frobenius 同态的复合具有 $a\mapsto a^{p^m}$ 的形式。我们用一个引理来强调这个美妙的事实。

引理 4.16

令 $(R,+,\cdot)$ 是一个整环，假设 R 是特征 p 的。令 $f:R\to R$ 是 Frobenius 同态，即对任意 $a\in R$，我们有

$$f(a)=a^p \tag{4.104}$$

则对任意 $m\in\mathbb{N}_1$，f 与自己复合 m 次的映射是

$$f^m(a)=(f\circ\cdots\circ f)(a)=a^{p^m} \tag{4.105}$$

♡

证明 用数学归纳法，若 $m=1$，则 $f(a)=a^p$。

假设当 $m=k$ 时，$f^k(a)=a^{p^k}$，则当 $m=k+1$ 时，

$$f^{k+1}(a)=f\left(f^k(a)\right)=f\left(a^{p^k}\right)=\left(a^{p^k}\right)^p=a^{p^{k+1}} \tag{4.106}$$

这就证明了这个引理。

当然，这个引理最重要的便是告诉我们，对特征 p 的整环 R，$a,b\in R$，以及任意的 $m\in\mathbb{N}_1$，我们有

$$(a+b)^{p^m}=a^{p^m}+b^{p^m} \tag{4.107}$$

即将这个奇妙的结论复合了 m 次，得到了新的奇妙的结论。这个结论在特征 p 的有限域中当然也成立。而更美妙地，注意到同构的复合还是同构（证明留给感兴趣的读者），因此在特征 p 的有限域中，对每一个 $m\in\mathbb{N}_1$，我们都有 $a\mapsto a^{p^m}$ 是一个域同构。

引理 4.17

令 $(F,+,\cdot)$ 是一个域，若 F 是个特征 p 的有限域，则对任意 $m\in\mathbb{N}_1$，$a\mapsto a^{p^m}$ 都是个域同构。

♡

证明 只需要利用有限域中 $a \mapsto a^p$ 是个同构，同构的复合是同构，以及给出 $a \mapsto a^{p^m}$ 的这个映射是

$$f^m = f \circ \cdots \circ f \tag{4.108}$$

我们就知道，$a \mapsto a^{p^m}$ 是个域同构。此即得证。

下面，我们来证明，若有限域 F 的阶是 $q = p^n$，则 F 中的每个元素，都是多项式 $x^{p^n} - x$ 的根。

命题 4.23

令 $(F, +, \cdot)$ 是一个域。若 F 是个有限域，而 $|F| = p^n$，则对任意 $x \in F$，我们有 $x^{p^n} = x$。换言之，F 中的每个元素，都是多项式 $x^{p^n} - x$ 的根。

♠

证明 若 $x = 0$，则 $x^{p^m} = 0^{p^m} = 0$。假设 $x \neq 0$，则 $x \in F^\times$。因为 F 是个域，所以 $F^\times = F \setminus \{0\}$ 在乘法下构成一个群，这个群的阶是 $p^n - 1$。利用拉格朗日定理，因为 $x \in F^\times$，所以

$$x^{p^m - 1} = x \tag{4.109}$$

两边同时乘上 x，我们就得到了 $x^{p^m} = x$。

综上所述，我们就证明了这个命题，即阶为 p^n 的有限域中的每个元素都是 $x^{p^n} - x$ 的根。

既然讲到了有限域 F 的乘群 $F^\times$，我们就要讲一个对初学者来讲惊人的事实，那就是任何有限域 F 的乘群 $F^\times$ 都是个循环群，即可以用一个元素来生成。

这个命题证明，本质上是数论的，我们要用到欧拉函数的性质。我们回顾欧拉函数 $\phi(n)$，指的是从 1 到 n 的与 n 互素的整数的个数，即

$$\phi(n) = |\{1 \leqslant a \leqslant n : \gcd(a, n) = 1\}| = \sum_{\substack{a=1 \\ \gcd(a,n)=1}}^{n} 1 \tag{4.110}$$

举个例子，若 p 是个素数，则 $\phi(p) = p - 1$。为了证明有限域 F 的乘群 $F^\times$ 是个循环群，我们需要一个数论中的引理。

引理 4.18

若 $n \in \mathbb{N}_1$，则

$$n = \sum_{d|n} \phi(d) \tag{4.111}$$

这里的求和下标指的是对 n 的正因子 $d \geqslant 1$ 求和（一般来说我们会省略写 $d \geqslant 1$）。

♡

证明 我们令 $n \in \mathbb{N}_1$，则

$$n = \sum_{a=1}^{n} 1 \tag{4.112}$$

每一个从 1 到 n 的数 a 都与 n 有最大公因数，记作 $d = \gcd(a, n)$，这个数必须整除 n，故我们可以先取这样的 $d|n$，再去找对应的 $a \in \{1, \cdots, n\}$，使得 $\gcd(a, n) = d$。此即

$$n = \sum_{a=1}^{n} 1 = \sum_{d|n} \sum_{\substack{a=1 \\ \gcd(a,n)=d}}^{n} 1 \tag{4.113}$$

假如 $\gcd(a, n) = d$，我们可以令 $b = a/d$，则 $\gcd(b, n/d) = 1$，而且 $1 \leqslant b \leqslant n/d$，此即

$$n = \sum_{d|n} \sum_{\substack{a=1 \\ \gcd(a,n)=d}}^{n} 1 = \sum_{d|n} \sum_{\substack{b=1 \\ \gcd(b,n/d)=1}}^{n/d} 1 = \sum_{d|n} \phi(d) \tag{4.114}$$

这就证明了这个引理。

除此以外，我们还需要一个几乎显然的引理，即域上的 n 次多项式最多有 n 个根。

引理 4.19

令 $(F,+,\cdot)$ 是一个域。若 $p(x)\in F[x]$ 是个 n 次多项式（$n\geqslant 1$），则 $p(x)$ 在 F 上最多有 n 个根。♡

证明 我们只须利用因式定理。因为 F 是个域，所以若 a 是 $p(x)$ 在 F 上的一个根，则 $x-a$ 作为一个 F 上的多项式，整除 $p(x)$。即存在 $q(x)\in F[x]$，使得

$$p(x)=(x-a)q(x) \tag{4.115}$$

因为每个域都是整环，所以 $\deg(q)=\deg(p)-1$。因此，若 p 在 F 上有 n 个根，称为 $a_1,\cdots,a_n\in F$，则

$$p(x)=c(x-a_1)\cdots(x-a_n) \tag{4.116}$$

其中 $c\in F\setminus\{0\}$。因此，p 不可能有第 $n+1$ 个根了（因为次数不够了）。这就证明了若 $n\in\mathbb{N}_1$，则任何一个 n 次多项式 $p(x)$ 在域 F 上最多有 n 个根。

下面，我们来证明有限域上的乘群一定是循环群。

命题 4.24

令 $(F,+,\cdot)$ 是一个域。若 F 是个有限域，则 $F^\times=F\setminus\{0\}$ 在乘法下构成一个循环群。♠

证明 我们采用一个经典的证明。这个证明的直接推论是由模 p 的非零同余类所构成的群有生成元，称为模 p 的原根。感兴趣的读者可以进一步去学习原根相关的知识，我们在这里不再深入讲了。

为方便起见，令 $G=F^\times$，则 $(G,\cdot)$ 构成一个（乘）群。我们令 n 是它的阶，即 $n=|F^\times|=|F|-1=p^n-1$。我们只须证明存在一个元素 $a\in G$，使得 $|a|=n$。

我们注意到一个重要的事实，即任意元素 $a\in G$ 的阶必须整除群 G 的阶（拉格朗日定理），所以 $|a|$ 必须整除 n。

令 $d|n$。我们分两类情况讨论。

第一类情况，若存在 $a\in G$，使得 $|a|=d$，则 $a^d=1$。特别地，利用群论的知识，我们知道 $\langle a\rangle=\{1,a,\cdots,a^{d-1}\}$。还是利用群论的知识，因为 G 是个阿贝尔群（交换群），所以我们知道对任意 $0\leqslant i\leqslant d-1$，我们有

$$(a^i)^d=\left(a^d\right)^i=1^i=1 \tag{4.117}$$

因此（两两不同的）$1,a,\cdots,a^{d-1}$ 给出了 $x^d-1=0$ 的 d 个根。又因为 F 是个域，所以 $x^d-1=0$ 在 F 上最多有 d 个根。因此，$1,a,\cdots,a^{d-1}$ 恰好就是 $x^d-1=0$ 的 d 个根。

进一步地，我们想知道 G 中有多少元素的阶恰好是 d。假设 $|b|=d$，则 $b^d=1$，所以 b 是 x^d-1 的一个根。我们记 $b=a^k$。根据群论，我们知道

$$|b|=\left|a^k\right|=\frac{d}{\gcd(k,d)} \tag{4.118}$$

因此 $|b|=\left|a^k\right|=d$ 当且仅当 $\gcd(k,d)=1$。这样的 b 的个数当然是 $\phi(d)$。

第二类情况，若不存在 $a\in G$，使得 $|a|=d$，则当然对于任何 $a\in G$，我们都有 $a^d-1\neq 1$，即 G 中不存在 $x^d-1=0$ 的根。

结合两类情况，我们定义一个函数 ψ。对任意 $d|n$，我们定义 $\psi(d)$ 是 F 上 $x^d-1=0$ 的根的个数。

因此，根据上面的分类讨论，$\psi(d)$ 要么是 $\phi(d)$，要么是 0。特别地，对任意 $d|n$，我们有 $\psi(d)\leqslant\phi(d)$。

注意到，G 中每一个元素的阶，一定整除 n，所以

$$n=\sum_{g\in G}\sum_{\substack{d|n\\|g|=d}}1=\sum_{d|n}\sum_{\substack{g\in G\\|g|=d}}1=\sum_{d|n}\psi(d) \tag{4.119}$$

另一方面，根据数论，我们知道

$$n=\sum_{d|n}\phi(d) \tag{4.120}$$

注意到不等式 $\psi(d)\leqslant\phi(d)$。所以这迫使所有的 $\psi(d)$ 都等于 $\phi(d)$，其中 $d|n$。因此特别地，对 $d=1$，$\psi(d)=\phi(d)>0$，因此在群 G 中存在至少一个元素 g，使得 $|g|=n$。这就证明了群 $G=F^\times$ 是个循环群。

综上所述，我们就证明了这个命题，即有限域上的乘群一定是循环群。

注意，在证明的过程中，我们实际上也证明了，若 $n = |F^\times| = |F| - 1$，则对任意 $d|n$，群 $F^\times$ 中阶为 d 的元素个数恰好是 $\phi(d)$

而这个结论仅通过 $F^\times$ 是乘群的事实也可以证明，证明是非常简单的，我们留给感兴趣的读者作为练习。

我们回到有限域的讨论。我们很容易发现，阶为 p^n 的有限域 F，作为 $\mathbb{F}_p$ 的扩域，包含了 $x^{p^n} - x$ 的每个根，而且因为 $x^{p^n} - x$ 在每个域中最多有 p^n 个根，以及 $|F| = p^n$，所以 F 是 $\mathbb{F}_p$ 的极小的一个包含了 $x^{p^n} - x$ 的所有根的扩域。我们称这样的域为分裂域。特别地，阶为 p^n 有限域 F 是 $x^{p^n} - x$ 在 $\mathbb{F}_p$ 上的一个分裂域。我们如何证明在阶相等的情况下，有限域都是同构的呢？只须证明有限域确实是这样的分裂域，以及分裂域是彼此同构的即可，这就是我们剩下的证明目标。

定义 4.23

令 $(E, +, \cdot)$ 是一个域，而 $f(x) \in E[x]$ 是个 E 上的多项式。若 F 是 E 的扩域，则我们称 F 是 $f(x)$ 在 E 上的一个分裂域，若

1. f(x) 在 F 上有 n 个解，即 $f(x)$ 可以在 F 上分解为 $f(x) = c(x - a_1)\cdots(x - a_n)$，其中 $a_1, \cdots, a_n \in F$。
2. 若 k 是个中间域，即 $F/k/E$ 是个嵌套的域扩张，而 $f(x)$ 在 k 上有 n 个解，则 $F = k$。

也就是说，F 是一个“极小的”使得 $f(x)$ 在其上有 n 个解的 E 的扩域。 ♣

我们做一个小练习，那就是阶为 $q = p^n$ 的有限域是 $x^{p^n} - x$ 在 $\mathbb{F}_p$ 上的一个分裂域。为了这个练习，我们引入多项式的形式导数这一概念。

定义 4.24

令 $(R, +, \cdot)$ 是一个环，而 $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$，则我们定义 $f(x)$ 的形式导数 $f'(x)$ 为

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \tag{4.121}$$

♣

尽管求导一般来说不是一个环同态，但是它满足所有微积分中熟知的结论。

引理 4.20

令 $(R, +, \cdot)$ 是一个环，则

$$\forall c \in R, \forall f(x) \in R[x], (cf(x))' = cf'(x) \tag{4.122}$$

$$\forall f(x), g(x) \in R[x], (f(x) + g(x))' = f'(x) + g'(x) \tag{4.123}$$

$$\forall f(x), g(x) \in R[x], (f(x)g(x))' = f'(x)g(x) + f(x)g'(x) \tag{4.124}$$

♡

证明 证明是比较机械的，我们留给既感兴趣又充满耐心的读者作为额外的练习。

引理 4.21

令 $(F, +, \cdot)$ 是个阶为 $q = p^n$ 的有限域。则 F 是 $x^{p^n} - x$ 在 $\mathbb{F}_p$ 上的一个分裂域。 ♡

证明 令 $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$。

一方面，因为 F 的阶是 $q = p^n$，所以 F 是特征 p 的（若是其他素数 q，则 q 不整除 p^n，会导致矛盾）。因此我们可以认为 F 是 $\mathbb{F}_p$ 的一个扩域（至少在同构意义下是一个扩域）。而且我们证明过 F 中的每个元素都是 $f(x) = x^{p^n} - x$ 的根，考虑到 $x^{p^n} - x$ 的次数是 p^n，因此我们有

$$f(x) = \prod_{a \in F} (x - a) \tag{4.125}$$

另一方面，假设 k 是一个严格比 F 更小的，有 p^n 个根的中间域 k，即 $k \subsetneq F$，而 $f(x)$ 在 k 上有 p^n 个根。因为 $|k| < |F| = p^n$，所以 $f(x)$ 在 k 中必须有重根，即存在 $a \in k$，使得 $(x - a)^2 | f(x)$。记 $f(x) = (x - a)^2 g(x)$，则

$$f'(x) = 2(x - a)g(x) + (x - a)^2 g'(x) \tag{4.126}$$

特别地，$(x-a)|f'(x)$，而且 $(x-a)|f(x)$，所以 $\gcd(f,f')\neq 1$。

可是 $f(x)$ 在 $\mathbb{F}_p[x]$ 中的形式导数是 $f'(x)=p^n x^{p^n-1}-1=0-1=-1$。因此在 $\mathbb{F}_p[x]$ 中显然有

$$\gcd(f,f')=1 \tag{4.127}$$

这是矛盾的。因此，任意使得 $f(x)=x^{p^n}-x$ 在其上有 p^n 个根的 F 与 $\mathbb{F}_p$ 的中间域 k 必须满足 $k=F$。

综上所述，我们就证明了阶为 $q=p^n$ 的有限域是 $x^{p^n}-x$ 在 $\mathbb{F}_p$ 上的一个分裂域。

现在，我们来证明同一个多项式在同一个域上的分裂域之间是两两等价的。实际上，我们可以证明更好的结论，即

命题 4.25

令 $(E,+,\cdot)$ 和 $(F,+,\cdot)$ 是两个域，而 $\phi: E\to F$ 是个域同构。令 $f(x)\in E[x]$ 是个 E 上的多项式，令 $g=\tilde{\phi}(f)$，其中 $\tilde{\phi}: E[x]\to F[x]$ 是 ϕ 引出的同态（我们在上一章中讲过）。假设 $n=\deg(f)=\deg(g)$。若 E' 是 $f(x)$ 在 E 上的分裂域，而 F' 是 $g(x)$ 在 F 上的分裂域，则它们同构，即

$$E'\simeq F' \tag{4.128}$$

♠

证明 因为 $\phi: E\to F$ 是个域同构，所以 $\tilde{\phi}: E[x]\to F[x]$ 显然是个环同构（环同态的部分我们在上一章中已经证明，而双射则是因为系数的一一对应）。假设 E' 是 $f(x)$ 在 E 上的分裂域，而 F' 是 $g(x)$ 在 F 上的分裂域。

我们递归地证明（即可以用数学归纳法）。若 $f(x)$ 是常数多项式，则是显然的。因此假设 $f(x)=c(x-a_1)\cdots(x-a_m)f_1(x)\cdots f_k(x)$，其中 $c\neq 0$，$a_1,\cdots,a_m\in E$，$f_1,\cdots,f_k$ 在 E 上是不可约的，且 $\deg(f_1),\cdots,\deg(f_k)\geqslant 2$。

首先，因为 f_1 在 E 上是不可约的，所以 $E[x]/(f_1(x))$ 是个域。令 α_1 是 f_1 在 E' 上的一个根，则 α_1 在 E 上是代数的，我们可以取到它在 E 上的最小多项式。这个最小多项式是不可约的，且整除 f_1，又因为 f_1 本身是不可约的，所以 f_1 就是 α_1 在 E 上的最小多项式。利用前一节的知识，我们就知道

$$E(\alpha_1)\simeq E[x]/(f_1(x)) \tag{4.129}$$

同理，令 β_1 是 $\tilde{\phi}(f_1(x))$ 在 F' 上的一个根。因为 ϕ 是个域同构，$\tilde{\phi}$ 是个环同构，所以 $\tilde{\phi}(f_1(x))$ 在 $E'[x]$ 中也是不可约的。因此

$$E(\alpha_1)\simeq E[x]/(f_1(x))\simeq E'[x]/(\tilde{\phi}(f_1(x)))\simeq E'(\beta_1) \tag{4.130}$$

递归地，我们可以重复这个过程，直到

$$E(\alpha_1,\cdots,\alpha_l)\simeq E'(\beta_1,\cdots,\beta_l) \tag{4.131}$$

使得 $f_1,\cdots,f_k$ 都在 $E(\alpha_1,\cdots,\alpha_l)$ 中完全分解，因此 $\tilde{f}_1,\cdots,\tilde{f}_k$ 在 $E'(\beta_1,\cdots,\beta_l)$ 中也完全分解，所以 $f(x)$ 在 $E(\alpha_1,\cdots,\alpha_l)$ 中有 n 个根，$g(x)$ 在 $E'(\beta_1,\cdots,\beta_l)$ 中也有 n 个根。又因为 $\alpha_1,\cdots,\alpha_l\in E'$，所以

$$E'=E(\alpha_1,\cdots,\alpha_l)\simeq E'(\beta_1,\cdots,\beta_l)=F' \tag{4.132}$$

综上所述，我们就证明了这个命题，即在题设下 $E'\simeq F'$。

特别地，如果 $E=F$，则我们就得到了下面的推论。

引理 4.22

令 $(F,+,\cdot)$ 是一个域，而 $f(x)\in F[x]$ 是个 F 上的多项式，则 $f(x)$ 在 F 上的分裂域在同构下是唯一的。

♡

证明 只须令 $E=F$，我们就立刻得到了这个推论。

因此，我们就证明了阶相等的有限域之间是两两等价的，即

命题 4.26

令 $(F_1,+,\cdot)$ 和 $(F_2,+,\cdot)$ 是阶相等的有限域，则 $F_1\simeq F_2$。假设 $|F_1|=|F_2|=q=p^n$，则我们在同构的意义下，记 $\mathbb{F}_q=\mathbb{F}_{p^n}$ 为这样的有限域。

♠

证明 因为阶为 $q=p^n$ 的有限域是 $x^{p^n}-x$ 在 $\mathbb{F}_p$ 上的分裂域，而分裂域是彼此同构的，因此 F_1 和 F_2 也是同构

的。这就证明了这个命题。

第二部分

抽象代数 II
结合代数与 Galois 理论

第 5 章 群论 II——Group Theory II

5.1 对称群

在群论 I 的讨论中，我们略去了一个重要的群，那就是对称群。

定义 5.1

令 $n \in \mathbb{N}_1$，则对称群 S_n，定义为

$$S_n = \{\sigma : \{1, \cdots, n\} \to \{1, \cdots, n\} : \sigma\text{是双射}\} \tag{5.1}$$

对称群 S_n 中的每一个元素，我们称为 $\{1, \cdots, n\}$ 的一个置换，简称为一个置换。

显然，利用双射的性质，对称群在复合运算下构成一个群。

命题 5.1

令 $n \in \mathbb{N}_1$，则对称群 S_n，在复合下构成一个群。

证明 这是自明的。我们留给感兴趣的读者作为练习。S_n 中的单位元是恒等映射，即将 $\{1, \cdots, n\}$ 中的每个元素映到自身的那个双射，我们记恒等映射为 id_n，简记为 id。

如何表示 S_n 中的一个置换呢？我们有两种方法。第一种方法是写成两行的一个矩阵，其中第一行是从 1 到 n 的数字，第二行是对应的 $\sigma(i)$。

定义 5.2

令 $\sigma \in S_n$，则我们形式地将 σ 记作

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix} \tag{5.2}$$

很显然，一个写成这样形式的映射是一个置换，当且仅当第二行的数字取遍了 $1, \cdots, n$，是两两不同的数字。因为映射的复合是从右到左计算的，因此我们采用的规则是从右到左进行置换的复合运算。实际上，也有一种约定是从左到右计算。正如自然数集是否包含 0 并没有广泛的共识，置换的乘积也没有“正确”的顺序。在这本教材中，我们按照映射的本质，一概约定从右到左计算。

下面我们举一个例子。

练习 5.1 求证

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \tag{5.3}$$

证明 只须看 1,2,3 分别被映射到哪里去了即可。在右边的置换中，1 被映射到了 2；在左边的置换中，2 又被映射到了 3。因此，这两个置换的乘积，就将 1 映射到了 3，所以我们在 1 的下面写 3。同理，我们也可以得到 2 和 3 分别被映射到了 2 和 1。

下面，我们讲一个简单的引理，那就是每一个较小的对称群都可以嵌入到一个较大的对称群。

引理 5.1

令 $m \leqslant n$ 是两个正整数，则 S_m 可以被嵌入到 S_n 中，即存在一个单同态 $f : S_m \to S_n$。

证明 对于任意 $\sigma \in S_m$，我们想要定义 $f(\sigma) \in S_n$，而这就需要对任意 $i \in \{1, \cdots, n\}$，给出 $f(\sigma)(i)$ 的定义。我们是这么定义的。

如果 $1 \leqslant i \leqslant m$，我们定义 $f(\sigma)(i) = \sigma(i)$。如果 $m+1 \leqslant i \leqslant n$，我们定义 $f(\sigma)(i) = i$ 自身。

也就是说，我们将一个 m 个元素的置换视作一个 n 个元素的置换的一种方法，就是将其视为前 m 个元素的置换，而后 $n-m$ 个元素的恒等置换。

要证明 f 是个同态，只须对 i 分两类情况讨论。若 $i \leqslant m$，那么利用 S_n 是个群的条件即可；若 $i > m$，那么恒等映射显然会给出同态。

要证明 f 是个单射，只须证明它的核是平凡的，即 $\ker(f) = \{id\}$。那么，如果 $f(\sigma) = id$，显然后 $n-m$ 个单位是映到自身的，而且前 m 个元素，在 σ 下也要映到自身。这就迫使 $\sigma = id_m = id$。

综上所述，我们就证明了若 $m < n$ 是两个正整数，就存在一个从 S_m 到 S_n 的单同态，即 S_m 可以嵌入到 S_n 中。

(1 2 3)

第 6 章 环论 II——Ring theory II