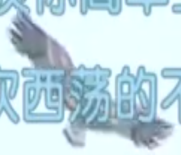
纸鸢啊纸鸢！我羡你高举空中。



可是你为什么东吹西荡的不自在?

莫非是上受微风的吹动，下受麻线的牵扯，

所以不能干青云而直上，向平阳而直下。

但是可怜的你！为什么这样的不自由呢?

原来你没有自动的能力?才落得这样的苦恼。

在你的 $1/\sqrt{2}$ 方向上

Lie

2024.08.23

黎曼，高斯，拉格朗日，鲁菲尼，阿贝尔，勒贝格，拉普拉斯，克莱因，泰勒，诺特，希尔伯特，怀尔斯，亚历山德罗夫，伽罗瓦，闵可夫斯基，哈代，格罗特迪克，姜立夫，华罗庚，陈景润，陈省身，丘成桐，陶哲轩，李，罗素，哥德尔，拉马努金，刘维尔，柯西，傅里叶，泊松，欧拉，牛顿，韦达，笛卡尔，庞加莱，怀尔，冯诺依曼，柯尔莫哥洛夫，康托尔，图灵，李特尔伍德，嘉当，尹依，维纳，仙农，柯朗，阿蒂亚，巴拿赫，爱尔特希，爱森斯坦因，马尔可夫.

如你所看到到我在上面列出了一些数学家的名字.

还有下面的几个句子，以此来表达对他们的尊敬，以及复杂的情感.

数学不是沿着清理干净的公路谨慎行进的，而是进入一个陌生荒原的旅行，在那里探险者往往会迷失方向。撰史者应该注意这样的严酷事实：绘就的是地图，而真正的探险者却已消失在别处。

数学家的模式，像画家或诗人的一样，必须是美的；各种思想，像色彩或辞藻一样，必须以和谐的方式组合在一起。美是首要的标准，丑陋的数学不可能永世长存。

证明是一个偶像，数学家在这个偶像前折磨自己。

此页故意留白

目录

第 1 章 胡言乱语

尽管还有许多格式问题与字体问题，还有一些过于僵硬的表达叙述，姑且维持现状吧。请忽略这些问题.....

本文使用 LaTeX 编写，顺利阅读本篇内容，需要一款合适的 PDF 阅读器。（WPS 带的就行，其他的没测试过）

1.1 胡言乱语

今天是 2024 年 6 月 7 日，星期五

早 6 点，被下水道的不明生物吵醒，嗯，真烦

好久没早起了。

向窗外望去，天气不算好，也不算差

万事开头难，就让我先开个头吧！

2017 年 9 月 1 日，早九点，数学课（多么巧，也是星期五），

没记错的话应该是在学一元二次方程的公式解法，40 多岁的马老师怎么也没想到，她的一段话竟会引导一个学生长达 7 年的长考。

这七年间，我在某些方面有所进步，不过在另一些方面退步了。但我还没进步到足以成为一名数学家；同样，我也没有退步到幻想自己已经是一名数学家.....

就在昨天，我终于学习完抽象代数的课程和伽罗瓦理论简介，“行色匆匆”我对其中的内容还未有深刻的理解，但也明白个七八成。在学习的过程中也曾深入的去探索过一个问题，并且得到了一些“不错的结果”.....

“一个高超的问题解答者必须具备两种不协调的素质——永不安分的想象和极具耐心的执拗。”这两个“素质”在我身上的体现极为“抽象”，和我相处的人大概都知道这点.....

回想 2022-2023 年，这是我数学水平提高最多的时间段，在这两年的时间里我学会了很多的数学知识，虽然这些知识看起来毫无作用，当我和别人谈论起这些时，他们问的最多的问题就是“这有什么用呢?”。我相信这一定有用——尽管我不知道这些到底有什么用。

“旅途中最美丽的地方，便是我未曾涉足之地，因此我一直追寻着，我追寻着梦想，我的心如此沉重，无论我的归宿在何方，我的眷恋从未改变，它像诅咒压在心里，让我的一些追求都遥不可及。”

拍摄于 2023 年 12 月 22 日

不知从何时起，我便喜欢在上课的时候看头顶的时钟，2023 下半年到 2024 前几个月看的次数最多，时间最长，为什么我时常看钟呢？看还有多长时间下课???

当然不是，“事实上”我在考虑“时钟巡

回”问题，和“12 的质因数分解及其等式关　系”。

事实上这个说法并不准确，先卖个官子，让我从 2022 年讲起。

1.2 二〇二二

1.2.1 fuck you!5

2022 年 2 月 25 日，按农历算是正月二十五，真巧又是星期五..... 不巧的是这天手机坏了，在买新手机的陆上，又碰见了各种 5.....

唉，明天又是星期五（2024.8.26）.....

这 buff 叠太多了.....

这么多的 5 是怎么回事？我不知道。但，我相信，如果两个看起来毫无关系的事物发生了如此巧合，那么这一定蕴含某种真理。不过这 5 是怎么回事？我不知道.....

写到这发现写错个字前面那个陆，本来想改成五的，但是敲键盘的一瞬间想到在某些地方会用陆来表示五，唉，不改了，叠 buff 去吧.....

2023 年 12 月 22 日也是星期五.....

fuck you！5

1.2.2 胡言乱语 2.0

大一学习了一点高等数学。高等数学对于一些人的来说，可能是他们学习到的数学知识最后的一点内容了。这对于刚毕业的，一些想摆脱数学的高中生来说大概是非人的折磨.....

不过对于我来说还想继续学一点数学，大概是理想，兴趣，固执，还是要证明什么.....

随便什么的吧.....

找个差不多的理由罢了.....

于是，在大一学完了高数后，我自学了一点高等代数。学到什么程度呢？我的目标是：能看懂主要定义，定理，试着作一点点题目，并且了解定理的证明，知识的历史背景等等。

然后我在哔哩哔哩上，键入了“高等数学”这四个字，刚好看见了丘维声老师的高等代数视频课。感觉他讲的非常好，然后就利用暑假刷视频，一个暑假把涉及行列式和矩阵基本运算和性质的内容看了一下（这是我们专业要学的高等代数里的内容，不过我们专业学的和数学专业的高等代数有较大区别，我们专业学的大部分是计算，以及一些简单的证明，内容与高等代数相比也差很多），剩下的内容在大二学习线性代数时看完了。

ok我们思考这样一个☝问题：假设存在一个空间 ϕ（在此只讨论牛顿力学，而不考虑量子力学），ϕ 中存在一些原子，且 ϕ 的温度是绝对零度，当然这是不可能的，但这里我们认为 ϕ 的温度就是绝对零度。那么可以推测（这些推测不一定准确）ϕ 中的所有粒子都是静止的，包括电子绕核子的运动和他自身的运动，1这样他们之间存在万有引力，又驱使这些粒子相互靠近，在这个过程中由于粒子的运动 ϕ 就不在是绝对零度

大二应该是我在大学这四年里最快乐，高兴的一学年，当然这一年里也有一些不太愉快的事。（不过我想我已经快忘光了，现在能想起来的大概只有英语了）。我很高兴，学校能安排一点大学物理课程，虽然大部分内容是高

中学到的，但是大学物理确实让我学习到了一些高中没有的知识物理确实让我学习到了一些高中没有的知识，比如角动量守恒什么的。重要的是在上大学物理课的时候我思考了上一页图片所展示的，虽然这在物理中并不现实，可能这样的思考也毫无意义，不过在与大物老师的交谈中了解到了量子，这对于后来的专业课：结构化学起到了深远的影响，不过那是一年后的事情了。

紧接着的就是大三了，那段时间大概是发生了一些事情，让原本制定的计划，想做事情变得一团遭。

1.3 阅读 (一)

1.3.1 数学女孩

从 2022 年起，我开始阅览江南图书馆二楼的一些书籍，一开始我只是在里面瞎转，并没有明确要看的书，直到我发现了一本叫“数学女孩”的书。这本书到目前为止一共有五册，第一册讲的很杂，第二册讲的是费马大定理，第三册讲哥德尔不完备定理，第四册讲随机算法，第五册讲伽罗瓦理论。这本书以小说式的方法叙述数学，在高中时已经听到这本书了，可惜当时没条件看，大学算是能看了，不过我当时没在图书馆找到第一册，似乎图书馆里没有引进第一册，不知道现在有没有。

当时只看了第二册和费马大定理相关的，不过我也没想到，这本书里的一些内容会，对我以后尝试解决的一个问题起到指导性的作用。其中提到了时钟巡回（蕴涵时钟算法），勾股定理，素数，群，模，归纳法，模形式，椭圆函数等等。我对这其中感兴趣的便是素数和群了，于是便去学了一点初等数论和抽象代数。现在，还是让我们暂时把中心放在费马大定理上。

1.3.2 费马大定理

不过一周的时间，我便把数学女孩的第二册看完了，在还书时想着“让我挑下一本书吧”，于是又在图书馆里面瞎转。转着转着就发现一本叫“费马大定理”的书，从书架上把它拿下来看了几眼，心想“大概是采访了怀尔斯吧”。（事实上，还讲了费马大定理的由来，人们尝试证明费马大定理的历史，以及解决这个问题的大致思想等等。如果你想问我“怀尔斯是谁的话”.....）

随即眼睛转动了几下，又发现了一本关于费马大定理的书，不过它的作者似乎是位“民科”，看了这本书后最大的感受和想法就是“数学不能与政治挂钩”，我的某位好友曾质疑这个想法（我当时不能说服他），还好在不久之后，我的线代老师肯定了这个想法。

对了，重点是这节所说的第一本书，它的完整中文书名叫“费马大定理：一个困惑了世间智者 358 年的谜”，它的作者是“西蒙 • 辛格 SIMON SINGH”，译者是“薛密”。其核心内容是探讨是否存在正整数 x、y、z，使得 $x^n + y^n = z^n$ 成立，其中 n 是大于 2 的正整数。这个问题最初由法国数学家费马在 1637 年提出，他在一本数学书的空白处写下了一段话，暗示了

一个无法证明的数学定理，并表示自己有一个“十分美妙的证明”，但遗憾的是，他并没有给出这个证明。这段话成为了数学史上著名的未解之谜，吸引了无数数学家前赴后继地研究。

费马大定理的解决过程充满了曲折和挑战。欧拉、索非·热尔曼、勒让德、狄利克雷、加布里尔·拉梅等数学家都曾尝试证明或部分证明这个定理，但都未能成功。直到 1995 年，英国数学家安德鲁·怀尔斯经过多年的艰苦努力，终于找到了费马大定理的完整证明。他的证明方法基于椭圆曲线和模形式的理论，这一成就被认为是 20 世纪数学界的重大突破之一。

最后让我摘抄这本书里的一段话来结束这一节。

> 30 年后，安德鲁·怀尔斯已经准备好了。站在牛顿研究所的演讲厅里，他在黑板上飞快地写着，然后，努力克制住自己的喜悦，凝视着他的听众。演讲正在达到它的高潮，而听众也明白这一点。他们之中有几个人事先已将照相机带进了演讲厅，闪光灯频频亮起，记录下了他最后的论述。
>
> 手中拿着粉笔，他最后一次转向黑板。这最后的几行逻辑演绎完成了证明。300 多年来第一次，费马的挑战被征服了。更多的相机闪烁着拍下了这个历史性的时刻。怀尔斯写上了费马大定理的结论，转向听众，平和地说道：“我想我就在这里结束。”
>
> 两百多位数学家鼓起掌来，欢庆着。就连那些曾期望得到这个结果的人也难以置信地笑了起来。30 年后，安德鲁·怀尔斯终于相信他已经实现了他的梦想，历经了 7 年的孤寂，他终于可以对外透露他的秘密的计算。
>
> (.....)

第 2 章 一点准备

2.1 预备知识：集合，映射，代数运算及关系，集合的划分与等价类

2.1.1 集合

我们把指定的某些对象的全体称为集合，集合中的每个对象叫做这个集合的元素。

如果两个集合所含的元素完全相同（即 A 中的元素都是 B 的元素，B 中的元素也都是 A 的元素），那么称这两个集合相等。

如果 a 是集合 A 的元素，那么就记作 $a \in A$, 读作“a 属于 A”。

含有有限个元素的集合叫作有限集；含有无限个元素的集合叫作无限集。

我们把不含任何元素的集合称为空集，记作 $\varnothing$

如果集合 A 的任意一个元素都是集合 B 的元素, 那么集合 A 称为集合 B 的子集, 记作 $A \subseteq B$ 或 $B \subseteq A$, 读作“集合 A 包含于集合 B”或“集合 B 包含集合 A”。

根据子集的定义，任何一个集合是它本身的子集。

我们规定，$\varnothing \subseteq A$，即空集是任何集合的子集。

显然，对于任何集合 A, 都有子集 A 和子集 $\varnothing$，我们称 A 和 $\varnothing$ 是集合 A 的平凡子集。(如果某事看起来是“显然的”，那么我就使用“平凡的”“平凡”字样。)

集合中元素的个数叫作集合的阶数。

2.1.1.1 集合的基本运算

一. 交集与并集

既属于集合 A 又属于集合 B 的所有元素组成的集合，叫作集合 A 与集合 B 的交集, 记作 $A \cap B$，读作“A 交 B”，即，

$$A \cap B = \{x \mid x \in A, \text{且} x \in B\}$$

由属于集合 A 或属于集合 B 的元素组成的集合，叫作集合 A 与集合 B 的并集，记作 $A \cup B$，读作“A 并 B”。

二. 补集与全集

这两者的概念不在叙述，重要的是集合经过以上四种基本运算得到的结果仍然是集合，并且是全集的子集。

2.1.1.2 集合运算的一些性质

关于集合的交与并，有

$$\complement(A \cap B) = \complement A \cup \complement B \qquad \complement(A \cup B) = \complement A \cap \complement B$$

类似的，有:（其中，$\complement$ 表示补集。）

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

2.1.1.3 一些拓展

设 B 是 A 的非空子集，定义 B 到 A 的映射 i：对任意的 a 属于 A，i 把 a 映射过去得到 a 自己，则称 i 为 B 到 A 的嵌入映射。

设 A_0 是 A 的非空子集，f 是 A_0 到集合 B 的映射，若有 A 到 B 的映射 g，使 $g(x) = f(x), \forall x \in A_0$, 则称 g 为 f 的开拓映射，fg 在 A_0 上的限制映射。

直观上，开拓映射是把一个映射的定义域扩大; 限制映射是把一个映射的定义域缩小，从这个意义上将，嵌入映射是把一个恒等映射值域所在的集合扩大。嵌入映射一定是单射，不一定是满射。开拓映射既不一定是单射，也不一定是满射。

笛卡尔直积集合：设 A,B 是两个集合，则称

$$A \times B = \{(a, b) \,|\, a \in A, b \in B\}$$

为 A 与 B 的直积。

集合 A 中元素的个数一般用 $card(A)$ 表示，有一重要结论在此给出：$card(A \cup B) = card(A) + card(B) - card(A \cap B)$

2.1.2 映射

2.1.2.1 映射概念

设 X、Y 是两个非空集合，如果存在一个法则 f，使得对 X 中的每个元素 x，按法则 f，在 Y 中有唯一确定的元素 y 与之对应，则称 f 为从 X 到 Y 的映射，记作 f：X→Y。

其中，X 叫作定义域，Y 叫陪域，y 称为元素 x 在映射 f 下的象，记作：y=f(x)；x 称为 y 关于映射 f 的原象。集合 X 中所有元素的象的集合称为映射 f 的值域，记作 f(X) 或 Imf(X)。这里要注意：值域是陪域的子集。比如指数函数 $y = e^x$，它的定义域是全体实数，但值域是 $(0, +\infty)$，它的陪域是全体实数。当值域和陪域相等时，我们把 f 叫做满射。

若 f 和 g 的定义域，陪域，对应法则相同（$f(a) = g(a), \forall a \in A$），那么称 f 与 g 相等，记作 f=g。

2.1.2.2 满射，单射，双射，逆映射

若 Y 中的任一元素 y 都是 X 中某元素的像，则称 f 为从 X 到 Y 的满射。$\Longleftrightarrow \forall b \in B, \exists a \in A$使得$b = f(a)$

若 X 中的任一两个不同元素 $(x_1 \neq x_2)$，对应的 $(y_1 \neq y_2)$，则称 f 为从 X 到 Y 的单射。$\Longleftrightarrow \forall x_1,x_2 \in X$ 从 $f(x_1) = f(x_2)$可以推出$x_1 = x_2$

如果一个映射既是单射又是满射，那么称这个映射是双射。

若 f 把任意的 a 映射到 a 自己，那么 f 就是恒等映射，恒等映射一般计为 I。如果一个映射既是单射又是满射，那么称这个映射是双射。

设 f：X→Y，如果存在 g：Y→X. 使得 fg=I_B 且 gf=I_A，那么称 f 是可逆映射，把 g 称为 f 的逆映射。可以证明 f 的逆映射是唯一的。另外 f 是可逆映射当且仅当 f 是双射。

对于有限集上的映射 f 而言，可以证明：一方面，如果 f 是满射，那么 f 是单射；另一方面，如果 f 是单射，那么 f 是满射。从而 f 是双射。于是，我们便得到了定理：

有限集上的单射或满射是双射. (2.1)

2.1.2.3 函数

函数是一类特殊的映射，函数的陪域是数域的非空子集，定义域可以是任何集合。两个函数相同的充分必要条件是定义域，陪域，对应法则相同。

在高中阶段，我们认为两个（单值）函数相同的充分必要条件是定义域，对应法则相同。这是因为在高中阶段所讨论的函数的自变量都取实数，默认为陪域都是实数集，在这个前提条件下定义域，对应法则相同就可以了，但严格的说法是定义域，陪域，对应法则相同。一个函数的逆函数存在的前提条件是，$\forall x_1,x_2 \in X$ 从 $f(x_1) = f(x_2)$可以推出$x_1 = x_2$，它是单射。

2.1.3 运算

2.1.3.1 代数运算和二元运算

设 A,B,C 是非空集合，则 A 与 B 的直积集合 $A \times B$ 到 C 的一个映射 f，称为 A 与 B 到 C 的一个代数运算。

这就是说，若有 $a \in A, b \in B$，则 $(a,b) \in A \times B, f((a,b)) = c \in C$，即 a 与 b 惟一确定 c，我们就说 a 与 b 运算的结果是 c。为了简单，常记 $f((a,b))$ 为 $a \circ b$，于是上面的运算就写成了 $a \circ b = c$。为了区别不同的运算法则，我们有时也把代数运算的符号“∘”改写为“+”或“×”，于是就有了

$$3+5=8 \quad 3 \times 5 = 15$$

的写法，也就有了“加法”，“乘法”的叫法

通常较多用到的代数运算，是 A=B=C 时的情形，即 A 与 A 到 A 的代数运算, 也称为 A 中的“二元运算”或“运算”。此时也说“集合 A 对该运算是封闭的”

2.1.3.2 运算律

设集合 A 中有一种二元运算“∘”，如果

$$(a \circ b) \circ c = a \circ (b \circ c), \forall a, b, c \in A,$$

则称该运算满足结合律。

设集合 A 中有一种二元运算“∘”，如果

$$a \circ b = b \circ a,$$

则称该运算满足交换律。

设集合 A 中有两种代数运算“∘”和“+”，如果，

$$a \circ (b + c) = a \circ b + a \circ c, \text{或}$$

$$(b + c) \circ a = b \circ a + c \circ a,$$

则称该运算满足“∘”对“+”的左分配律或右分配律。

结合律的一个重要作用，是使表达式 $a_1 \circ a_2 \circ \cdots \circ a_n$ 有意义，因为这时无论怎样加括号，运算的结果都是一样的，这给我们带来了方便。

交换律的一个重要作用，是使等式 $(a \circ b)^n = a^n \circ b^n$ 成立。

分配律的一个重要作用，是使一个集合中的两种运算之间产生一种联系。

在研究集合时，有时要把集合划分成一些子集来讨论，这时就要用到集合的分类，集合的分类又和“等价关系”密切相关，为了讲清“等价关系”，我们先来介绍“关系”关系的概念。

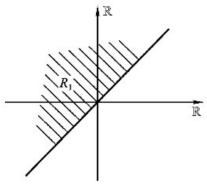
2.1.4 关系

我们知道，现实生活当中有许许多多的关系，例如“同学关系”，“师生关系”，“上下级关系”等等，我们也知道实数集合中“大于”，“小于”“等于”这些关系，还有 n 阶复方阵集合中“相和”“相似”这些关系。现在，我们把这些关系抽象出来得到数学中“关系”的定义：

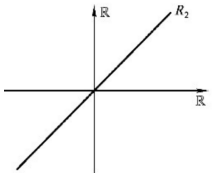
如果有一种性质 R，使集合 A 中任意两元素 a,b，或者有性质 R，或者没有性质 R，二者必居其一，我们就说 R 给定了 A 中的一个“关系”。当 a,b 有性质 R 时，称 a 与 b 有（R）关系，计为 aRb；当 a，b 没有性质 R 时，称 a 与 b 没有关系，记为 $a \not R b$。

设 A 是一个非空集合，R 是 A 与 A 的笛卡尔直积集合的子集，$a, b \in A$, 若 $(a, b) \in R$, 则称 a 与 b 有 R 关系，记为 aRb, 且称 R 为 A 的一个关系（二元关系）。在不引起混淆时，aRb 也可以记为 $a \sim b$。

例：实数集 R 中的小于等于关系，可以用 $\mathbb{R} \times \mathbb{R}$ 中的子集 R_1 来刻画；等于关系也可以用 $\mathbb{R} \times \mathbb{R}$ 中的子集 R_2 来刻画。



R_1



R_2

图 2.1

2.1.4.1 等价关系

实数集中的等于关系可以推广为等价关系。

定义：若集合 A 的一个关系 R 满足

(1) 反身性 $aRa \Rightarrow \forall a \in A$

(2) 对称性 $aRb \Rightarrow bRa, \forall a, b \in A$

(3) 传递性 $aRb, bRc, \Rightarrow aRc, \forall a, b, c \in A$

则称 R 为 A 的一个“等价关系”。

例如：n 阶方阵的相似关系就是等价关系，图形的相似关系也是等价关系，现实生活中的同班关系，血缘关系，晶体学当中的同晶系关系等都是等价关系。实数的等于关系是等价关系，但不等关系都不是等价关系。

2.1.5 集合的划分与等价类

图 2.2

上图是 2023 年 5 月份的月历。

显然，星期一是由无穷多天组成的集合，星期二……星期日也是如此。如何表示星期一这个集合呢？用列举法无法把属于星期一的无穷多天都写出来，于是想到用描述法。那么属于星期一的那些天的特征是什么呢？我们把 2023 年 5 月一日对应到一，5 月 2 日对应到二……。这个对应法则把时间长河中所有的日子组成的集合到整数集的一个一一的对应。观察 2023 年五月份的月历可以看出，星期一是由被七除后余数为一的整数组成的子集，星期二是由被七除后余二的整数组成的子集,……, 星期六是由被七除后余数为 6 的整数组成的子集, 星期日是由被七除后余数为零的整数组成的子集，把这些子集依次记成 $H_1, H_2, \ldots H_6, H_0$。即：

$$H_1 = \{7k+1 \,|\, k \in Z\},$$

$$H_2 = \{7k+2 \,|\, k \in Z\},$$

$$\cdots \qquad \cdots\cdots$$

$$H_6 = \{7k+6 \,|\, k \in Z\},$$

$$H_7 = \{7k \,|\, k \in Z\}.$$

于是 $\mathbb{Z}$ 被分成了七个子集，显然有：

$$\mathbb{Z} = H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5 H_6 \cup H_7, H_i \cap H_j = \varnothing 当 i = j.$$

从这个例子中我们不难抽象出定义：

如果集合 S 是它的一些非空子集的并集，其中每两个不相等的子集的交为空集，那么把这些子集组成的集合称为 S 的一个划分。

显然，这个划分给出了一个等价关系；因为对于某一天要么是星期 x，要么是星期 y，二者只据其一，并且只据其一；这样就有了一个二元关系。

又因为：

1. 同一天 t 是同一星期 x。
2. t 和 m 是星期 x，那么 m 和 t 就是星期 x。而
3. t 和 m 是星期 x，m 和 v 是星期 x，就能得到 t 和 v 是星期 x。

从而这个二元关系就是等价关系。如果你还有点注意力的话，就不难发现:

S 上的一个划分给出了 S 上的一个等价关系。

如果你有不错的注意力的话，就不难发现：

S 上的一个等价关系给出了 S 上的一个划分。

设 ~ 是集合 S 上的等价关系，任给 $a \in S$,S 的子集

$$\{x \in S | x \sim a\}$$

称为由 a 确定的等价类，记作 $\bar{a}$。

等价类有如下四条性质：

$$a \in \bar{a}, \forall a \in S$$

$$a \in \bar{a} \Longleftrightarrow a \in \bar{a}$$

$$\bar{x} = \bar{y} \Longleftrightarrow x = y$$

若 a 与 b 是集合 S 中的元素，那么 a 的等价类与 b 的等价类要么相等，要么不相交。

一元多项式方程

2.2 多项式

2.2.1 数域

设 F 是由一些数成的集合，其中包括数 0 和数 1，如果 F 中任意两个数（这两个数可以相同）的和、差、积、商（除数不为 0）仍是 F 中的数，则称 F 为一个数域。

常见数域：复数域 C；实数域 R；有理数域 Q。

（1）任意数域 F 都包括有理数域 Q；即，有理数域为最小数域。

（2）两个数域之交也构成一个数域。

2.2.2 一元多项式

设 $a_0, a_1, \ldots, a_n$ 都是数域 F 中的数，n 是非负整数，那么表达式 $f(x) = a_n x^n + a_{n-1}x^{n-1} + + a_2 x^2 + a_1 x + a_0 (a_n \neq 0)$ 叫做数域 F 上一个文字 x 的多项式或一元多项式。

x 称为不定元，$a_0, a_1, \ldots, a_n$ 称为系数。“两个多项式相等，当且仅当它们有完全相同的项（除去系数为零的项）。”

$a_n x^n$ 叫做多项式 f(x) 的最高次项或首项。a_n 称为首项系数，非负整数 n 叫做多项式的次数，记作 $deg f(x)$。a_0 叫零次项或常数项。

零次多项式：最高次项是零次项的多项式，即 $a(a \neq 0)$ 的次数为零，叫零次多项式。

零多项式：系数全为零的多项式没有次数，这个多项式叫零多项式，零多项式总可记为 0。有些地方也将零多项式的次数定义为负无穷。

零化多项式：若有 $x = x_0$，使得 $a_n x^n + a_{n-1}x^{n-1} + + a_2 x^2 + a_1 x + a_0 (a_n \neq 0)$，则称 f 是 x_0 的零化多项式。易见 x_0 的零化多项式有无穷多个。

形如“$a_n x^n + a_{n-1}x^{n-1} + + a_2 x^2 + a_1 x + a_0 (a_n \neq 0)$”的等式，称之为一元 n 次（多项式）方程，若 f 是 x_0 的零化多项式，那么 $x = x_0$ 是一元 n 次（多项式）方程 f=0 的一个根，也就是方程的一个解。

代数学是数学中的一个重要的基础性的分支学科。初等代数学是由古代的算术推广和发展而来的，抽象代数学则是在初等代数学的基础上于十九世纪发展形成的。初等代数学亦称古典代数学，是实数和复数及以它们为系数的多项式的代数运算的理论和方法。初等代数学的中心问题就是多项式方程（代数方程）和方程组的求解问题。因此，初等代数学有时也称为方程论。

2.2.3 一元 n 次方程根的性质

1. 代数基本定理 n 次多项式函数 $f(x) = a_n x^n + a_{n-1}x^{n-1} + + a_2 x^2 + a_1 x + a_0$，在复平面内有 n 个零点。

2. 奇数次方程至少有一个实数根
3. 虚数根总是以共轭复根的形式成对出现
4. 韦达定理

   如果 n 次方程 $f(x)=a_nx^n+a_{n-1}x^{n-1}++a_2x^2+a_1x+a_0(a_n\neq 0)$ 的 n 个根是 $x_1,x_2,\ldots,x_n$，那么

$$\begin{cases} x_1+x_2+\ldots+x_n= & -\dfrac{a_{n-1}}{a_n} \\ x_1x_2+x_1x_3+\ldots+x_{n-1}x_n= & \dfrac{a_{n-2}}{a_n} \\ \ldots\quad\ldots\quad\ldots\quad= & \ldots \\ x_1x_2x_3\ldots x_{n-1}x_n= & (-1)^n\dfrac{a_0}{a_n} \end{cases}$$

5. 有理根定理如果整系数方程 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_2x^2+a_1x+a_0(a_n\neq 0)$ 的一根为 $x=\dfrac{q}{p}$，那么 $q|a_0,p|a_n$。

2.2.4 多元多项式与对称多项式

2.2.4.1 多元多项式

设 p 是一个数域，$x_1,x_2,\ldots,x_n$ 是 n 个文字。形式为 ax_1 设 p 是一个数域，$x_1,x_2,\ldots,x_n$ 是 n 个文字。形如 $ax_1{}^{k_1}x_2{}^{k_2}\ldots x_n{}^{k_n}$ 的式子，称为一个单项式。

其中，a 属于 p，$k_1,k_2,\ldots,k_n$ 是非负整数。如果两个单项式中相同文字有相同的次数，就称它们为同类项。

一些单项式的和：$\sum_{k_1,k_2,\ldots,k_n}a_{k_1,k_2,\ldots,k_n}x_1{}^{k_1}x_2{}^{k_2}\ldots x_n{}^{k_n}$ 称为多多项式，简称多项式。

2.2.4.2 对称多项式

对称多项式是多元多项式中常见的一种。

n 元多项式 $f(x_1,x_2,\ldots,x_n)$，如果对任意的 $i,j,1\leqslant i<j\leqslant n$，都有

$$f\left(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n\right)=f\left(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n\right),$$

那么这个多项式称为对称多项式。也就是说，对换两个文字，f 不变，那么 f 就是对称多项式。

由对称多项式的定义可知，对称多项式的和，积，以及对称多项式的多项式还是对称多项式。

定理：任意一个 n 元对称多项式都可以表示成初等对称多项式的多项式，并且这个多项式是唯一的。

2.2.4.3 初等对称多项式

$\sigma_1=x_1+x_2+\ldots+x_n$

$\sigma_2 = x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n$

. . . .

$\sigma_n = x_1x_2x_3 \ldots x_{n-1}x_n$，称为初等对称多项式。

2.3 一元低次方程求根公式

这一节将给出一元低次方程求根公式，1-4 次方程是有求根公式的，而五次和五次以上方程一般而言没有求根公式。

对于一次和二次方程他们的求根公式是简单的，只给出公式而不进行推导。

对三次方程求根公式给出了一些推导思路，和具体的公式。

四次方程但具体公式过于繁琐，也不美观，因此只给出了思路，需要求解时用方法进行推导比直接套用公式更有意义。

2.3.1 一元一次方程

一次方程，总可以转化为 ax+b=0 的形式，求根公式为

$$x = -\frac{b}{a}$$

2.3.2 一元二次方程

二次方程，总可以转化为 $ax^2 + bx + c = 0$ 的形式，求根公式为

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

2.3.3 一点准备

三次和四次方程需要用到一些技巧，方法和概念在本节介绍。

2.3.3.1 契尔恩豪森转换

令 $t = x + \frac{a_{n-1}}{na_n}$，对于一元 n 次方程 $a_nx^n + a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x + a_0 = 0$，将 t 带入到原方程中，就可以将 n-1 次项消除，从而达到简化方程的目的。

2.3.3.2 欧拉公式

欧拉公式：$\cos\theta + i\sin\theta = e^{i\theta}$

2.3.3.3 n 次单位根

方程 $x^n = 1$，显然有且只有一实数根 $x_1 = 1$，但根据代数基本定理：“n 次多项式函数 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 = 0$，在复平面内有 n 个零点。”这表明他还有其他 n-1 个复根，它们是谁呢？让我们利用欧拉公式给出结论。

令 $\cos\theta + i\sin\theta = e^{i\theta} = x^n = 1$，得到方程组：$cos\theta = 1, sin\theta = 0$ 从而 $\theta = 2k\pi, k \in Z$。代入得到：$e^{2k\pi i} = x^n$，因此 $x = e^{\frac{2k\pi i}{n}} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ 其中 $k = 0, 1, \ldots, n-1$

2.3.4 一元三次方程

对于一元三次方程 $ax^3 + bx^2 + cx + d = 0$，利用契尔恩豪森转换可以将二次项消除掉。

令 $t = x + \frac{b}{3a}$，将 t 带入得：

$$(t - \frac{a}{3})^3 + a(t - \frac{a}{3})^2 + b(t - \frac{a}{3}) + c = 0$$

展开，化简得到：

$$t^3 + \frac{3ac - b^2}{3a^2}t + \frac{27a^2d - 9abc + 2b^3}{27a^3} = 0$$

令 $p = \frac{3ac - b^2}{3a^2}$，$q = \frac{27a^2d - 9abc + 2b^3}{27a^3}$。原方程化为:

$$t^3 + pt + q = 0$$

此方程中已无二次项，要求得原方程的根，只需要解此方程。

到此为止，有多种方法求解三次方程，本节只介绍一种。

Cardan 法：

对于方程 $t^3 + pt + q = 0$，令 t=m+n，方程化为：

$$m^3 + n^3 + (3mn + p)(m + n) + q = 0$$

选取合适的 m,n 使得 $3mn+p = 0$,即 $mn = -\frac{p}{3}$, 得到 $m^3n^3 = -(\frac{p}{3})^3$, 方程化简为 $m^3+n^3 = -q$。可以观察到 m，n 是方程 $X^2 + qX - (p/3)^3 = 0$ 的两个根，

$$X_1 = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}, \quad X_2 = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

不妨取，$m^3 = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$, $n^3 = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$

其解为：m=M，$M\omega$，$M\omega^2$，n=N，$N\omega$，$N\omega^2$。（利用欧拉公式和 n 次单位根）

其中：$\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$,

$$M=\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}},\quad N=\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}$$

立方根 M，N 满足约束条件 $MN=-\frac{p}{3}$，显然只有下面 3 种情况满足条件：

$$\begin{cases} m=M \\ n=N \end{cases}\qquad \begin{cases} m=M\omega \\ n=N\omega^2 \end{cases}\qquad \begin{cases} m=M\omega^2 \\ n=N\omega \end{cases}$$

带入原方程，便得到方程 $t^3+pt+q=0$ 的三个根（Cardan 公式）：

$$\begin{cases} t_1=M+N=\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}} \\ t_2=M\omega+N\omega^2=\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}\omega+\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}\omega^2 \\ t_3=M\omega^2+N\omega=\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}\omega^2+\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}}\omega \end{cases}$$

2.3.5 一元四次方程

$y^4+py^2+qy+r=\left(y^2-ky+s\right)\left(y^2+ky+t\right)$

将等式的右边展开可以得到

$y^4+(s+t-k^2)y^2+(ks-kt)x-st=0$

对照系函数可以得到

$$\begin{cases} s+t=k^2+p \\ ks-kt=q \\ st=r \end{cases}$$

由前两个方程得可以到

$$\begin{cases} s=\frac{k^3+pk+q}{2k} \\ t=\frac{k^3+pk-q}{2k} \end{cases}$$

带入到第三个方程中化简可以得到方程

$$k^6+2pk^4+(p^2-4r)k^2-q^2=0$$

显然这是一个一元三次方程 (关于 k 的)，通过求解这个方程可以得到最初方程的解。

由于四次方程的求根公式实在太长就不放上去了，从这个过程中可以看出，四次方程求根公式里肯定包含着平方根和三次方根。

2.3.6 一元高次方程

当数学家解决了三次方程四次方程的代数解问题之后，当然会继续研究五次方程的解法，而几百年间，这个问题一直没有被攻破，于是有人开始怀疑五次及五次以上方程没有代数解，经过拉格朗日、阿贝尔、伽罗瓦等人的努力，五次以上方程无代数解的问题终于被彻底解决。

次数大于等于 5 的多项式方程一般不能用根式求解。

一个染色问题

还记得我曾说，经常在上课看头顶的时钟，考虑所谓“时钟巡回”问题吗？现在让我来叙述一下这个问题。不过我是在设法解决另外一个问题时发现它的。这一节我将简要聊一聊正 n 边形染色问题（这个名字是我自己起的，可能会和其他一些名称冲突），并由此引出“时钟巡回”“数论”及“群”，首先让我们简要复习一下高中所学的排列与组合。

2.4 排列与组合

从 n 个不同元素中，每次取出 m 个元素为一组，如果该组内对每个元素的位置是有要求的（位置不同代表意义不同的）即排列，无要求（位置不同代表意义相同）的即组合。

2.4.1 排列

从 n 个不同元素中取出 m 个元素，按照一定的顺序排成一列，叫做从 n 个元素中取出 m 个元素的一个排列。这样的全部的排列个数，叫做排列数，写做：A_n^m。

2.4.2 组合

从 n 个不同元素中，不重复地选出 m 个元素的一个组合，这样的组合的总数叫做组合数，写做：C_n^m。

2.5 一个染色问题

考虑一个规则的几何体，例如正 n 边形，使用 n 种不同的颜色对其顶点进行染色，每种颜色可以使用多次（对顶点染色），也可以一次都不用，正 n 边形的每个顶点都要进行染色，如果正 n 边形经过刚体运动，使得两种不同状态最后看起来是一样的（重合），那么称这两种状态是一个方案。（当然，需要保证每个三角形都是一样的边长）

问题是：对于一个确定的 n，由 n 确定的方案总数 S 是多少；对于 n 来说，S 有通项公式吗？

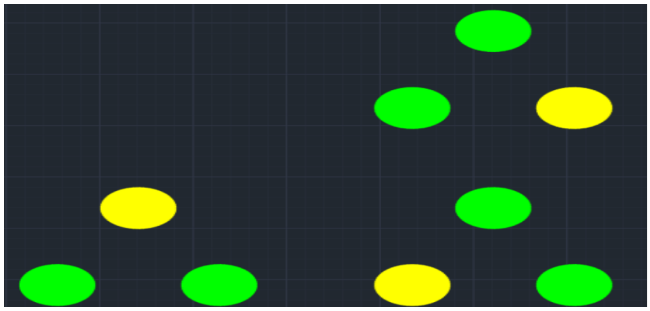


图 2.3

为了理解这个问题，上图展示出了对于正三边形的三种染色状态，按照定义他们是同一个染色方案因为经过刚体运动他们可以完全重合。

下图展示了正三边形所有不同的方案：

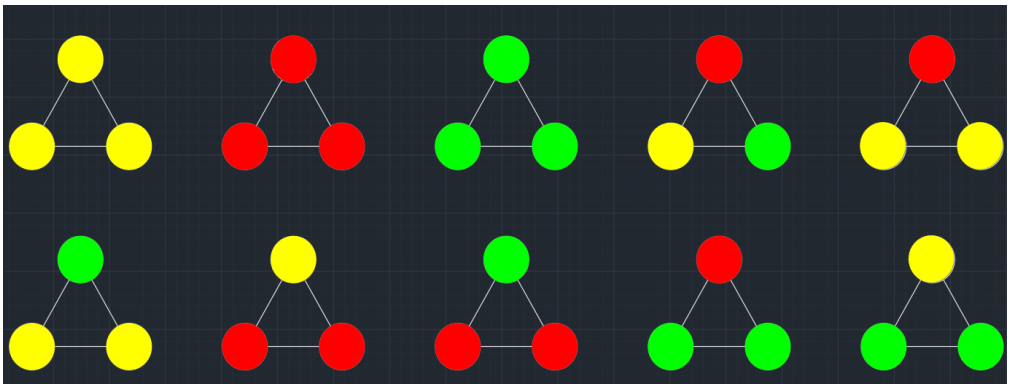


图 2.4

共十种方案，这是通过枚举法得出的, 经过简单计算也可以得到相同结论。

分类讨论：

1. 三种颜色只取一种（颜色）涂染，则只有三种（不同的）方案 $C_3^1 = 3$；
2. 三种颜色取三种涂染，有 $C_3^3 = 1$ 种方案；
3. 三种颜色取两种，那么就会有一种颜色用了两次，这种颜色将占据（涂染）两个顶点，并且这两个顶点的位置只能相邻，另外一种颜色只占据一个顶点，可知所有不同的染色方案完全被两种颜色的取法和具体的用法决定，因此有 $C_3^2 C_2^1 = 3 \times 2 = 6$ 种方案。

共有 3+1+6=10 种方案。这与图 4 展示相同。

你可以尝试使用高中所学的排列组合来计算 n=4，5，6，7 时的方案总数，不过我不推荐你这么干，n=4 时还好，对于其他情况这是一个非常痛苦的过程。

n=4，5 时方案数分别为 55，377，我可以一直写到 n=10 时的具体方案数，不过对于 n=11 之后我就无能为力了（这个数字太大，我的计算机算不出它，但别人的似乎可以，怎么回事呢？我不知道.....），不过我可以给一种形式上的表达，我把它放在了第 9 节的最后面。

2.6 钟面引出的两个问题

2.6.1 钟面上的时钟巡回问题

我们观察钟面上的时针，它开始时指向 12，以 1 个小时为一个单位，时针每过一个小时顺时针旋转 30°，指向下一个数，时针依次经过的数为 12-1-2-3-4-5-6-7-8-9-11-12，它从 12 开始经过了钟面上的每一个数最终回到了 12。

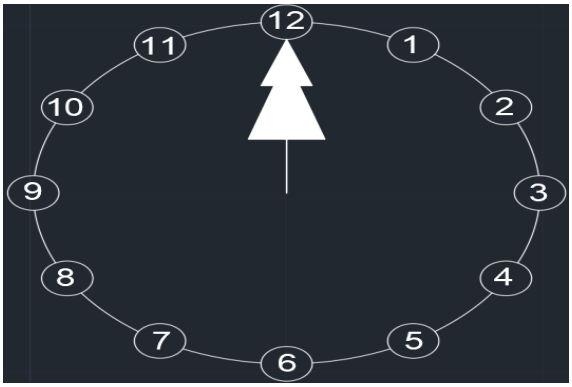


图 2.5

（若以）2 小时为（一个）单位，（时针每过两个小时旋转 60°，指向下一个数）依次经过的数为 12-2-4-6-8-10-12，不会经过钟上所有的数

3 个小时为单位依次经过的数为 12-3-6-9-12（不会经过钟上所有的数）

（4 个小时为单位，依次）经过的数为 12-4-8-12

.....

做表如下：

单位	经过的数	经过的数的个数
1	12-1-2-3-4-5-6-7-8-9-11-12	12
2	12-2-4-6-8-10-12	6
3	12-3-6-9-12	4
4	12-4-8-12	3
5	12-5-10-3-8-1-6-11-4-9-2-7-12	12
6	12-6-12	2
7	12-7-2-9-4-11-6-1-8-3-10-5-12	12
8	12-8-4-12	3
9	12-9-6-3-12	4
10	12-10-8-6-4-2-12	6
11	12-11-10-9-8-7-6-5-4-3-2-1-12	12
12	12-12	1

表 2.1: 12-时钟巡回

我们把时钟表盘上所有的数都绕一遍的现象称为完全巡回，那么我们自然会问完全巡回的条件是什么？或者说完全巡回的规律是什么？

如果你有惊人的注意力的话，你就会发现以下事实：

每一个单位与经过的数的个数的乘积都是十二的倍数。

当且仅当单位不是 12 的因数时，完全巡回。换句话说就是单位与 12 互素。

如果两个数有相同的属于 12 的因数，那么他们所对应的经过的数相同，并且顺序相反，经过的数的个数也相同。

如果你想得到严谨的证明的话，可以去学一点初等数论。不过初等数论不是这里的重点，所以这里只展示结论，最后要说的是这个结论对于任意的 n 都成立。（或许之后会详细介绍）

从物理的角度来讲物体的运动是相对的，那么假设我们让指针不动，将钟固定在一个平面上，让标记着数字的圆盘转动。

如果你把这个钟面的边界当作一个圆的话，那么不论转多少度，它都能与自身重合；但如果这个边界是个正 12 边形的话，那么只有转一些固定角度，它才能与自身重合；如果边界是正八边形的话，那么它又得转另外的一些角度才能与自身重合。

这表明圆，正 12 边形，正八边形有着不同的性质，为了描述这种性质，让我来介绍群的概念。

2.6.2 群

群是数学中用来度量（衡量）对称性的“语言”。

用群来度量对称性的重要意义在于: 我们可以通过研究群的分类，来对具有对称性的客观事物进行分类。

钟面上，指针绕圆心的旋转组成的集合就可以看作是一个关于旋转操作的群，这个群有一个专有名词，其中的抽象运算就是“旋转”，而“指针的指向”就是群中的元素。

我们很容易看出，等边三角形比等腰三角形 (它的腰与底不相等) 更具有对称性，道理是什么呢？

设等腰三角形底边上的垂直平分线为 (图 6), 则平面上关于 l 的反射 τ 把等腰三角形变成与它自己重合的图形。显然，平面的恒等变换 I 也具有这个性质。

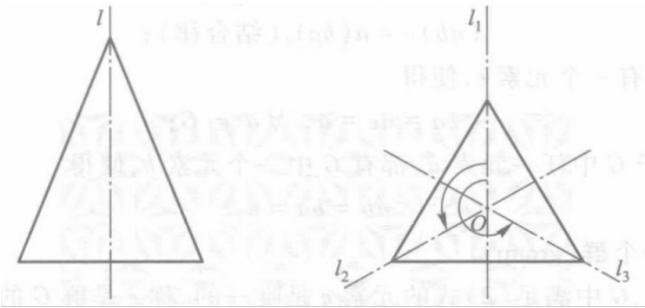


图 2.6

设等边三角形的中心为 O，三条边上的垂直平分线分别为 l_1, l_2, l_3(图 6)。则平面上关于 l_i 的反射 τ_i, 把等边三角形变成与它自己重合的图形，$i = 1, 2, 3$; 平面上绕点 O 的转角分别为 $\frac{2}{3}\pi, \frac{4}{3}\pi$ 的旋转 σ_1, σ_2，以及恒等变换 I 也有这个性质。

平面上 (或空间中) 的正交 (点) 变换 (也称保距变换)，如果把平面 (或空间) 图形 Γ 变成与它自己重合的图形，则把这个正交 (点) 变换叫做图形　的对称 (性) 变换。

上面指出，等边三角形的对称 (性) 变换已经有 6 个。进一步可以证明，只有这 6 个。类似地，等腰三角形 (它的腰与底不相等) 的对称 (性) 变换有且只有两个。我们自然可以说: 等边三角形比等腰三角形更具有对称性。

我们把等边三角形的所有对称 (性) 变换组成一个集合:

$G = \{I, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\}$

我们知道，平面上两个正交 (点) 变换的乘积仍是正交 (点) 变换；并且如果它们都把等边三角形变成与它自己重合的图形，那么它们的乘积也有这个性质因此等边三角形的任意两个对称 (性) 变换的乘积仍是它的对称 (性) 变换。从而集合 G 对于映射的乘法封闭。因此映射的乘法是集合 G 上的一个 (二元) 代数运算。

由于映射的乘法适合结合律，因此上述集合 G 上的代数运算适合结合律。G 中有恒等变换 I，I 与 G 中任一元素的乘积 (左乘或右乘) 都等于该元素自己。容易看出：G 中每个变换都有逆变换。因此，G 就是一个群。

图形 Γ 的所有对称 (性) 变换组成的集合 G, 对于映射的乘法成为一个群，称 G 是图形的 Γ 对称 (性) 群。

2.6.2.1 点群

现实生活中, 常常用正方形或正六边形的砖铺地面，如图 7；也常常用具有对称性图案的纸贴墙壁，如图 8。

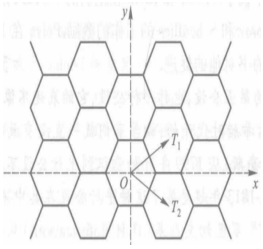


图 2.7

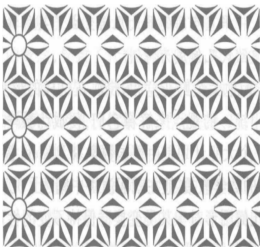


图 2.8

设想这些图案分别铺满了整个平面。如果铺满了图案的平面的对称 (性) 群不固定一个点，也不固定一条直线, 则称它为平面晶体群 (或者称为贴墙纸群)。R.Fricke 和 F.Klein(克莱因) 在他们关于自同构函数的第一本书 (1897) 中，对平面晶体群进行分类。G.Pólya(波利亚) 在 1924 年发表的一篇文章中，完成了对平面晶体群的分类: 共有 17 种不同的平面晶体群，并且给出了相应的装饰图案式样的例子。

自然界中有各种各样的晶体，每一种晶体的原子结构的模型可以看成是空间中的点阵。设想将这种点阵连续地、无限地填充整个空间。填充了点阵的空间的对称 (性) 群，如果既不固定一个点，也不固定一条直线，而且不固定一个平面，则称它为空间晶体群。对空间晶体群进行分类，就可以了解自然界中各种晶体的结构。在 1868 年，C.Jordan（若尔当) 借助 Bravais(1848)

对晶体结构分类的工作，研究空间晶体群的分类，虽然没有完全分类，但是这为 E.S.Fedorov(1890) 和 A.Schonflies (1891) 的工作铺平了道路。Fedorov 和 Schonflies 分别独立地证明了空间晶体群共有 230 个。这是历史上将群论直接用于自然科学的第一个例子。

到这里，我想我已经介绍了一些莫明奇妙的问题，前面所涉及到的知识不足以解答“染色问题”，它还需要一点群论和数论知识，另外我还想写一点环论，群表示论，晶体群与磁群，伽罗瓦理论等等，不过我没有太多时间去完善了，尽管还有许多格式问题与字体问题，还有一些过于僵硬的表达叙述，姑且维持现状吧。

n=11 时，对应的方案数为

$$S_{11}=\frac{11^{11}+11\times 11^{6}+10\times 11^{1}}{2\times 11}=12969598086$$

如果你有惊人的注意力的话，应该可以注意到以下公式（当时研究这玩意，写的草稿找不见了，不然我能写个比这复杂 100 倍的）

$$[(P_1-1)+(P_2-1)+(P_3-1)+(P_4-1)]+\{[(P_1P_2-1)+(P_1-1)+(P_2-1)]+[(P_1P_3-1)+(P_1-1)+(P_3-1)]+[(P_1P_4-1)+(P_1-1)+(P_4-1)]+[(P_2P_3-1)+(P_2-1)+(P_3-1)]+[(P_2P_4-1)+(P_2-1)+(P_4-1)]+[(P_3P_4-1)+(P_3-1)+(P_4-1)]\}+\{[(P_1P_2P_3-1)-\{[(P_1P_2-1)+(P_1-1)+(P_2-1)]+[(P_1P_3-1)+(P_1-1)+(P_3-1)]+[(P_2P_3-1)+(P_2-1)+(P_3-1)](P_1-1)+(P_2-1)+(P_3-1)\}\}+\{[(P_1P_2P_4-1)-\{[(P_1P_2-1)+(P_1-1)+(P_2-1)]+[(P_1P_4-1)+(P_1-1)+(P_4-1)]+[(P_2P_4-1)+(P_2-1)+(P_4-1)]-\{(P_1-1)+(P_2-1)+(P_4-1)\}\}+\{[(P_1P_3P_4-1)-\{[(P_1P_3-1)+(P_1-1)+(P_3-1)]+[(P_1P_4-1)+(P_1-1)+(P_4-1)]+[(P_3P_4-1)+(P_3-1)+(P_4-1)]-\{(P_1-1)+(P_3-1)+(P_4-1)\}\}+\{[(P_2P_3P_4-1)-\{[(P_2P_3-1)+(P_2-1)+(P_3-1)]+[(P_3P_4-1)+(P_3-1)+(P_4-1)]+[(P_2P_4-1)+(P_2-1)+(P_4-1)]-\{(P_2-1)+(P_3-1)+(P_4-1)\}\}=(P_1-1)(P_2-1)(P_3-1)(P_4-1)$$

图 2.9

这就是我在第一节提到的质因数分解及其等式关系（不完善的）。

2.7 从星期到模 m 剩余类环

2.8 模 m 剩余类环

2.8.1 模 m 剩余类

图 2.10

由 4.5 节中的例子，两个整数属于同一个子集当且仅当它们被 7 除后余数相同，此时称 a 与 b 模 7 同余，记作 $a \equiv b\ (mod\ 7)$，读作“a 同余 b 模 7”或“a 模 7 同余 b”两个整数任给两个整数 a 与 b，要么 a 与 b 模 7 同余，要么 a 与 b 模 7 不同余，二者必居其一旦只居其一。我们称它为模 7 同余关系，很自然地可以把模 7 同余称为整数集 Z 上的一个等价关系。

星期一，星期二，... 星期日就是 $\mathbb{Z}$ 在模 7 同余关系下的等价类：

$$\overline{1} = H_1, \overline{2} = H_2, \cdots, \overline{0} = H_0$$

与模 7 同余关系类似，给出了一个大于 1 的整数 m，可以在整个概 m 同余关系：

$$a \equiv b(\mathrm{mod} m) \iff a - b \text{ 是 m 的整数倍。}$$

显然, 这是 $\mathbf{Z}$ 上的一个等价关系, 具有 m 个等价类:

$$\overline{0} = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{m}\} = \{km \mid k \in \mathbb{Z}\},$$

$$\overline{1} = \{x \in \mathbf{Z} \mid x \equiv 1 \pmod{m}\} = \{km + 1 \mid k \in \mathbf{Z}\},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\overline{m-1} = \{x \in \mathbf{Z} \mid x \equiv m - 1 \mod m\} = \{km + (m-1) \mid k \in \mathbf{Z}\},$$

它们都称为模 m 剩余类（或模 m 同余类）。集合

$$(\overline{0}, \overline{1}, \cdots, \overline{m-1})$$

是 $\mathbf{Z}$ 的一个划分，把这个集合记做 $\mathbf{Z}_m$。

命题 2.8.1　命题 1 设 m 是大于 1 的整数. 如果

$$a \equiv b(\mathrm{mod} m), \quad \text{且} \quad c \equiv d(\mathrm{mod} m),$$

那么 $a + c \equiv b + d(\mathrm{mod} m)$，且 $ac \equiv bd(\mathrm{mod} m)$.

2.8.2 模 m 剩余类环

今天是星期五，过了 181 天是星期几？由于每经过 7 天又是星期五，$181 = 6 \pmod 7$，$5+6=4 \pmod 7$，因此，过了 181 天是星期四。

星期五是 $\mathbf{Z}$ 的一个子集 $\overline{5}$ 又有 $\overline{181}=\overline{6}$，我们大胆地尝试如下计算：

$$\overline{5}+\overline{181}=\overline{5}+\overline{6}:=\overline{5+6}=\overline{4}.$$

也得出，过了 181 天是星期四。

由此受到启发，我们规定模 m 剩余类的加法：

$$\overline{a}+\overline{b}:=\overline{a+b}.$$

这样的规定是否合理呢？由于 $\overline{a},\overline{b}$ 的代表不唯一，因此需要验证：若 $\overline{a}=\overline{c},\overline{b}=\overline{d}$, 是否有

$$\overline{a+b}=\overline{c+d}$$

由于 $\overline{a}=\overline{c},\overline{b}=\overline{d}$，因此据等价类的性质，得

$$a\equiv c \pmod m, \quad b\equiv d \pmod m.$$

据 10.1 的命题 1，得

$$a+c\equiv b+d(\mathrm{mod}m)$$

再利用等价类的第三条性质，得

$$\overline{a+b}=\overline{c+d}$$

因此用 $\overline{a}+\overline{b}:=\overline{a+b}$ 规定的模 m 剩余类的加法是合理的。同样我们也可以规定模 m 剩余类的乘法：$\overline{a}\cdot\overline{b}:=\overline{a\cdot b}$。类似可以证明：该个定义是合理的，即与代表的选择无关。

这样, 我们在模 m 剩余类组成的集合

$$Z_m=\left\{\overline{0},\overline{1},\overline{2},\cdots,\overline{m-1}\right\}$$

中, 规定了加法和乘法两种运算, 模 m 剩余类是 Z 的子集, 它们也能做出法和乘法, 这是数学上的一个创新点, 它拓宽了人们的视野, Z_n 中的加法和乘法满足哪些运算法则呢？由于模 m 剩余类的加法和乘法分别归结为它们的代表相加和相乘, 因此直觉判断 Z_n 的加法和乘法满足整数的加法和乘法的运算法则, 并且容易验证这一猜测是真的, 即 Z_n 的加法满足：交换律, 结合律, $\overline{0}$ 具有下述性质：

$$\overline{0+a}=\overline{a}+\overline{0}=\overline{a}, \quad \forall a\in Z_m,$$

$\overline{0}$ 称为 Z_m 的零元；对于 $\overline{a}\in Z_m$，由 $\overline{-a}\in Z_m$，使得

$$\overline{a}+\overline{-a}=\overline{-a}+\overline{a}=\overline{0}.$$

$\overline{-a}$ 称为 $\overline{a}$ 的负元。记作 $-\overline{a}$。

Z_m 的乘法满足交换律、结合律，以及（乘法）对于加法的分配律，并且

$$\overline{1}\overline{a}=\overline{a}\overline{1}=\overline{a}, \quad \forall a\in\mathbb{Z}_m,$$

$\overline{1}$ 称为 $\mathbf{Z}_m$ 的单位元。

$\boldsymbol{Z}_m$ 中还可以规定减法如下：

$$\overline{a}-\overline{b}:=\overline{a}+(-\overline{b}),$$

即减法通过加法来定义。

整数集 Z，模 m 剩余类组成的集合 Z_m，它们都有加法和乘法两种运算，并且满足上述运算法则。

所有偶数组成的集合记做 2Z，由于两个偶数的和、积仍是偶数，因此 2Z 也有加法和乘法两种运算。2Z 中不存在一个偶数具有性质：与任一偶数的乘积等于那个偶数自身。因此 2Z 中没有单位元。上述其他运算法则在 2Z 中都成立。

整数集 Z，模 m 剩余类集 Z_m，偶数集 2Z 有共同的特征：有加法和乘法两种运算，并且满足加法的 4 条运算法则，以及乘法的交换律、结合律，乘法对于加法的分配律。我们想由此抽象出现代数学的一个重要概念。

定义 2.8.1 设 R 是一个非空集合，如果 R 上定义了两个代数运算，一个叫做加法，另一个叫做乘法，并且满足下列 6 条运算法则：

1. $a+b=b+a, \forall a, b \in \mathbb{R}$(加法交换律)；
2. $(a+b)+c=a+(b+c), \forall a, b, c \in \mathbb{R}$(加法结合律)；
3. R 中有一个元素，记做 0，它具有下述性质：
$$a+0=0+a=a, \quad \forall a \in \mathbb{R},$$
称 0 是 R 的**零元**；
4. 任给 $a \in R$，都有 $b \in R$，使得
$$a+b=b+a=0,$$
把 b 称为 a 的**负元**，记做 $-a$；
5. $(ab)c=a(bc), \forall a, b, c \in R$ (乘法结合律)；
6. $a(b+c)=ab+ac, \forall a, b, c \in R$ (左分配律)，
$(b+c)a=ba+ca, \forall a, b, c \in R$ (右分配律)，

那么称 R 是一个**环**。

显然, $Z, Z_m, 2Z$ 都是环, 称 Z 是整数环, 称 Z_m 是模 m 剩余类环, 称 $2Z$ 是偶数环，环 R 中可以定义减法运算如下
$$a-b:=a+(-b).$$
如果环 R 的乘法满足交换律，那么称 R 是**交换环**。$Z, Z_m, 2Z$ 都是交换环。

如果环 R 中有一个元素 e 具有下述性质：
$$ea=ae=a, \quad \forall a \in R,$$
那么称 e 是 R 的**单位元**，此时称 R 是有单位元的环。

在环 R 中, $0a=a0=0, \forall a \in R$.

定义 2.8.2 设 R 是有单位元 $e(\neq 0)$ 的环，对于 $a \in R$，如果存在 $b \in R$，使得
$$ab=ba=e$$
那么称 a 是 R 的一个**可逆元** (或**单位**)，把 b 叫做 a 的逆元，记做 a^{-1}。（请注意单位和单位元的区别）

定义 2.8.3 设 R 是一个环, 对于 $a \in R$, 如果存在 $c \in R$, 且 $c \neq 0$, 使得 $ac=0$ (或 $ca=0$), 那么称 a 是 R 的一个**左零因子** (或**右零因子**)。左、右零因子统称为零因子。

命题 2.8.2 设 R 是有单位元 $e(\neq 0)$ 的环，则 R 的零因子不是可逆元。

命题 2.8.3　设 R 是有单位元 $e(\neq 0)$ 的环，则 R 的零因子不是可逆元。

命题 2.8.4　对于任意整数 $m > 1$，模 m 剩余类环 Z_m 中每一个元素或者是可逆元，或者是零因子，二者必居其一，且只居其一。

定义 2.8.4 设 F 是一个有单位元 $e(\neq 0)$ 的交换环, 如果 F 中每一个非零元都是可逆元, 那么称 F 是一个域 (field)。

定义 2.8.5 设 m 是大于 1 的整数, 如果 m 的正因数只有 1 和 m 自身, 那么称 m 是一个**素数** (或**质数**)；否则称 m 是合数。

若 p 是素数, 则 Z_p 是一个域, 称它为模 p 剩余类域。

命题 2.8.5　若 p 是素数，则 Z_p 是一个域, 称它为模 p 剩余类域。

2.9 从环出发的一点数论

2.9.1 整数环

定理 2.9.1 (带余除法)，任给 $a, b \in \mathbb{Z}$，且 $b \neq 0$，则存在唯一的一对整数 q, r，使得

$$a = qb + r, \quad 0 \leq r < |b|. \tag{1}$$

(1) 式中的 q 和 r 分别称为 a 被 b 除所得的商和余数。当 $r = 0$ 时，a 被 b 除得尽，由此引出整除的概念；

定义 2.9.1 对于整数 a, b，如果存在整数 c，使得

$$a = cb, \tag{2}$$

那么称 b **整除** a，记做 $b \mid a$；否则，称 b 不能整除 a，记做 $b \nmid a$ 的一个因数（或约数），a 称为 b 的一个倍数。

任给 $a \in \mathbf{Z}$，由于 $0 = 0a$，因此 $a \mid 0$。特别地，$0 \mid 0$。

命题 2.9.1　在 Z 中, 若 $b \mid a_i, i = 1, 2, \cdots, s$ 则对任意整数 $u_1, u_2, \cdots, u_i$, 有

$$b \mid u_1a_1 + u_2a_2 + \cdots + u_ia_i.$$

如果 $c \mid a$ 且 $c \mid b$, 那么称 c 是 a 与 b 的一个 **公因数** (或**公约数**)。

定义 2.9.2 整数 a 与 b 的一个公因数 d 如果具有下述性质；a 与 b 的任一公因数都能整除 d，那么称 d 是 a 与 b 的一个**最大公因数**（或**最大公约数**）。

任给 $a \in \mathbf{Z}$, 由于 $a \mid a$ 且 $a \mid 0$, 因此 a 是 a 与 0 的一个公因数, 任取 a 与 0 的一个公因数 c, 显然 $c \mid a$, 因此 a 是 a 与 0 的一个最大公因数. 特别地, 0 是 0 与 0 的最大公因数.

引理 1 在 $\mathbf{Z}$ 中如果有等式

$$a = qb + r$$

成立, 那么 d 是 a 与 b 的最大公因数当且仅当 d 是 b 与 r 的最大公因数.

定理 2.9.2 **定理 2** 任给两个整数 a, b, 都存在它们的一个最大公因数 d, 并且 d 可以表示成 a 与

b 的倍数和, 即存在整数 u, v, 使得

$$ua + vb = d.$$

定义 2.9.3 设 $a, b \in \mathbf{Z}$，如果 $(a, b) = 1$，那么称 a 与 b 互素。

由定义 10.8 立即得出，两个整数互素当且仅当它们的公因数只有 ± 1。

定理 2.9.3 两个整数 a 与 b 互素的充分必要条件是：存在整数 u, v，使得 $ua + vb = 1$。

利用定理 10.3 可以推导出互素的整数的一些重要性质。

1. 在 $\mathbf{Z}$ 中, 如果 $a \mid bc$, 且 $(a, b) = 1$, 那么 $a \mid c$.
2. 在 $\mathbf{Z}$ 中, 如果 $a \mid c, b \mid c$, 且 $(a, b) = 1$, 那么 $ab \mid c$.
3. 在 $\mathbf{Z}$ 中, 如果 $(a, c) = 1$, 且 $(b, c) = 1$, 那么 $(ab, c) = 1$.

素数在整数环的结构中起着基本建筑块的作用，下面分别从几个不同的角度来刻画素数的特征:

定理 2.9.4 设 p 是大于 1 的整数，则下列命题等价：

1. p 是素数；
2. 对任意整数 a，都有 $p \mid a$ 或 $(p, a) = 1$；
3. 对于整数 a, b，从 $p \mid ab$ 可以推出 $p \mid a$ 或 $p \mid b$；
4. p 不能分解成两个比 p 小的正整数的乘积。

定理 2.9.5 (**算术基本定理**)，任一大于 1 的整数 a 都能唯一地分解成有限多个系数时乘积，所谓唯一性是说，如果 a 有两个这样的分解式：

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_r,$$

那么一定有 $s = t$，并且适当排列因数的次序后，有

$$p_i = q_i, \quad i = 1, 2, \cdots, s.$$

算术基本定理刻画了整数环的结构；任一大于 1 的整数 a 能唯一地 (除了因数的排列次序外) 写成

$$a = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}, \tag{9}$$

其中 $p_1, p_2, \cdots, p_m$ 是两两不等的系数，r_i 是正整数，$i = 1, 2, \cdots, m$. (9) 式称为 a 的 **标准分解式**。

2.9.2 Z_m 的可逆元的判定，模 p 剩余类域，域的特征，费马小定理

定理 2.9.6 在模 m 剩余类环 Z_m 中, $\bar{a}$ 是可逆元当且仅当 a 与 m 互素。

定理 2.9.7 $\mathbf{Z}_m$ 的每一个元素或者是可逆元，或者是零因子，二者必居其一，且只居其一。

定理 2.9.8 设 p 是素数，则 Z_p 是域。

定理 2.9.9 设域 F 的单位元为 e，则或者对于任意正整数 n，都有 $ne \neq 0$；或者存在一个系数 p，使得 $pe = 0$，而对于 $0 < l < p$，有 $le \neq 0$。

定义 2.9.4 设域 F 的单位元为 e. 如果对于任意止整数 n, 都有 $ne \neq 0$, 那么称域 F 的**特征为0**; 如果存在一个常数 p, 使得 $pe = 0$, 而对于 $0 < l < p$, 有 $le \neq 0$, 那么称域 F 的**特征为p**。域 F 的特征记作 $charF$.

命题 2.9.2　设域 F 的特征为素数 p，则对于 F 中任一元素 a，都有 $pa = 0$。

命题 2.9.3　设域 F 的特征为素数 p，则对于任意 $a, b \in F$，有

$$(a+b)^b = a^b + b^b.$$

定理 2.9.10 (费马 (Fermat) 小定理) 设 p 是素数, 则对于任意整数 a, 都有

$$a^p \equiv a \pmod{p}.$$

2.9.3 Z_m 的可逆元的个数，欧拉函数

在本章 10.4 的定理 10.6 中，我们证明了下述结论：

定理 2.9.11 在模 m 剩余类环 Z_m 中, $\bar{a}$ 是可逆元当且仅当 a 与 m 互素。

把 Z_m 中所有可逆元组成的集合记做 Z_m。我们首先要问：Z_m^* 有多少个元素？

定义 2.9.5 把 Z_m 中可逆元的个数记做 $\varphi(m)$，称 $\varphi(m)$ 为**欧拉函数**。

由定理 1 立即得到：

命题 2.9.4　$\varphi(m)$ 等于集合 $\Omega_m = (1, 2, 3, \cdots, m)$ 中与 m 互素的整数的个数。

命题 2.9.5　若 p 是素数, 则 $\varphi(p) = p - 1$.

定理 2.9.12 设 p 是素数, 则对于任一正整数 r, 有

$$\mathbf{'(p^r) = p^{r-1}(p-1)}.$$

命题 2.9.6　$(\hat{a_1}, \widetilde{a_2})$ 是 $Z_{m_1} \oplus Z_{m_2}$ 的可逆元当且仅当 $\hat{a}_1, \widetilde{a}_2$ 分别是 Z_{m_1}, Z_{m_2} 的可逆元。

由上述命题立即得到：

推论 2 $\mathbf{Z}_{m_1} \oplus \mathbf{Z}_{m_2}$ 的可逆元的个数等于 $\varphi(m_1)\varphi(m_2)$。

定义 2.9.6 如果环 R 到环 R' 有一个双射 σ，且 σ 保持加法和乘法运算，那么称 σ 是环 R 到 R' 的一个同构映射，此时称环 R 与环 R' 是同构的，记做 $R \cong R'$。

定理 2.9.13 设 $m = m_1 m_2$，且 m_1 与 m_2 是互素的大于 1 的整数，则 $\sigma: \bar{x} \longmapsto (\hat{x}, \widetilde{x})$ 是环 Z_m 到 $Z_{m_1} \oplus Z_{m_2}$ 的一个同构映射，从而环 Z_m 与 $Z_{m_1} \oplus Z_{m_2}$ 同构。

定理 2.9.14 设 $m = m_1 m_2$, 且 m_1 与 m_2 是互素的大于 1 的整数, 则

$$\varphi(m) = \varphi(m_1)\varphi(m_2).$$

推论 2 设 $m = p_1^{r_1} p_2^{r_2} \cdots p_r^{r_r}$，其中 $\rho_1, \rho_2, \cdots, \rho_r$ 是两两不等的素数，则

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{r_1})\varphi(p_2^{r_2}) \cdots \varphi(p_r^{r_r}) \\ &= p_1^{r_1-1}(p_1-1)p_2^{r_2-1}(p_2-1) \cdots p^{r_r-1}(p_r-1).\end{aligned}$$

2.10 群

2.10.1 Z_m 的单位群 Z_m^*，欧拉定理，循环群及其判定

定义 2.10.1 设 G 是一个非空集合。如果在 G 上定义了一种代数运算 (即 $G \times G$ 到 G 的一个映射)，通常称为乘法，并且它满足下列条件：

1. $(ab)c = a(bc), \forall a, b, c \in G$ 结合律);
2. G 中有一个元素 e 使得 $ea = ae = a, \forall a \in G$, 称 e 是 G 的**单位元**;
3. 对于 $a \in G$, 存在 $b \in G$, 使得 $ab = ba = e$, 称 a 可逆, 此时称 b 是 a 的**逆元**, 记做 a^{-1}, 那么称 G 是一个**群** (group)。

群是认识现实世界中对称性的有力武器. 例如，一个平面图形 E 的对称性, 可以用平面上保持图形 E 不变的正交变换 (旋转、轴反射和它们的合成) 组成的集合对于映射的乘法形成的群来刻画, 这个群称为图形 E 的对称 (性) 群.

如果群 G 的运算还满足交换律. 那么称 G 是 **交换群** (阿贝尔 (Abel) 群)，

如果群 G 只含有限多个元素, 那么称 G 是有限群；否则称 G 是 **无限群**。有限群 G 所含元素的个数称为 G 的阶, 记做 $|G|$。

$\mathbf{Z}_m$ 的可逆元组成的集合 $\mathbf{Z}_m^*$ 是有限交换群，称它为 Z_m 的单位群.$\mathbf{Z}_m^*$ 的阶为 $\varphi(m)$

命题 2.10.1　设 G 是 n 阶交换群，则对于任意 $a \in G$，有

$$a^n = e,$$

其中 e 是 G 的单位元。

2.10.2 欧拉定理

定理 2.10.1 (欧拉定理) 设 m 是大于 1 的正整数, 如果整数 a 与 m 互素, 那么

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

2.10.3 群的元素的阶

定义 2.10.2 设 G 是一个群，对于 $a \in G$，如果存在正整数 n 使得 $a^n = e$，那么称 a 是有限阶元素，使 $a^n = e$ 成立的最小正整数 n 称为 a 的阶，记做 $|a|$；如果对于任意正整数 n 都有 $a^n \neq e$，那么称 a 是无限阶元素，

命题 2.10.2　群 G 中，如果元素 a 的阶为 n，那么

$$a^m = e \iff n \mid m.$$

命题 2.10.3　群 G 中, 如果元素 a 的阶为 n, 那么对于任意整数 k, 有

$$|a^k| = \frac{n}{(n,k)}.$$

命题 2.10.4　群 G 中，设 a, b 的阶分别为 n, m，如果 $ab = ba$，且 $(n, m) = 1$，那么 ab 的阶等于 nm。

命题 2.10.5　设 G 为有限交换群, 则 G 中有一个元素的阶是其他元素的阶的倍数.

2.10.4 循环群及其判定

定义 2.10.3 如果群 G 中有一个元素 a，使得 G 的每一个元素都能写成 a 的方幂的形式，那么称 G 是 **循环群**，把 a 叫做 G 的一个生成元，此时可以把 G 记成 $\langle a \rangle$。

从定义 12.3 立即得到下述结论：

1. 设 G 是有限群, 如果 G 中有一个元素 a, 使得 a 的阶等于 $|G|$, 那么 G 是循环群, a 是 G 的一个生成元；
2. 设 G 是有限循环群, 则 a 是 G 的生成元当且仅当 a 的阶等于 $|G|$。

$\mathbf{Z}_9^*$ 是循环群,$\overline{2}$ 是它的一个生成元,$\overline{5}$ 也是它的一个生成元。

当交换群 G 的运算记成加法时，如果 G 中有一个元素 a ，使得 G 的每一个元素都能写成 a 的整数倍的形式，那么 G 是循环群 a 是 G 的一个生成元。

$\mathbf{Z}_m$ 对于加法成的交换群, 由于 $\overline{l}=l\overline{1}, 1 \leq l \leq m$，因此加法群 Z_m 是循环群，$\overline{1}$ 是它的一个生成元。

Z 对于加法成的交换群, 由于 $l = l1, \forall l \in Z$, 因此加法群 Z 是循环群, 1 是它的一个生成元. 加法群 Z 是无限循环群.

定理 2.10.2 设 G 为有限交换群, 如果对于任意正整数 m, 方程 $x^n = e$ 在 G 中的解的个数不超过 m, 那么 G 是循环群.

定理 2.10.3 设 F 是有限域，则 F 的所有非零元组成的集合 F^* 对于乘法成为一个循环群。

推论 1 设 p 是素数，则 $Z_p{}^*$ 是循环群。

设 p 是奇素数，则 $Z_{p^r}^*, Z_{2p^r}^* \ (r \in N^*)$ 都是循环群。

引理设 p 是奇常数 $\overline{a}$ 是 $\mathbf{Z}_p^*$ 的一个生成元。如果在 $\mathbf{Z}_{p^2}^*$ 中 $\overline{a}^{p-1} \neq 1$ ，那么在 $\mathbf{Z}_p^*$ ($r \geq 2$) 中 $\overline{a}^{\varphi(p^{r-1})} \neq \overline{1}$。

定理 2.10.4 设 $m > 1$, 如果 Z_m 是循环群, 那么 m 必为下列情形之一：2，4，p^r，$2p^r$ （p 是奇素数, $r \in N^*$ ）。

定理 2.10.5 如果 Z_m^* 是循环群, a 是它的一个生成元，那么 $\overline{a}^k (1 \leq k \leq \varphi(m))$ 是 Z_n^* 的生成元当且仅当 $(k, \varphi(m)) = 1$. 从而 Z_n^* 的生成元的个数等于 $\varphi(\varphi(m))$。

2.11 半群与群

2.11.1 群

2.11.1 集合 G 中定义运算“$\circ$”, 且“$\circ$”满足以下规律, 则称 G 关于“$\circ$”为群, 记为 $\{G; \circ\}$; 当“$\circ$”还满足交换律时, 称 G 为交换群或 Able 群.

1. $\forall a, b \in G, a \circ b \in G$
2. $a, b, c \in G \quad (a \circ b) \circ = a \circ (b \circ c)$
3. $\exists e \in G$, 使 $e \circ a = a \circ e = a \quad \forall a \in G$
4. $\forall a \in G, \exists B \in G$, 使 $b \circ a = a \circ b = e$

例:①Z, Q, R, C 对于“+”构成群 $\{N; +\}, \{R; \cdot\}$ 不是群. ②$\{R^*; \cdot\}$ 是群. ③S_A(集合 A 上所有可逆映射),$\{S_A; \cdot\}$ 是群, 称为 A 的全变换群.④$\{\{1, -1\}; \cdot\}$ 是群.

2.11.2 半群；幺半群

2.11.2 集合 A 有运算“$\circ$”, 满足结合律, 则称 $\{A;\circ\}$ 为半群, 若还有 $e \in A$. 使

$$e \circ a = a \circ e = a, \forall a \in A$$

则称 $\{A;\circ\}$ 为幺半群,e 为幺元.

例:①$\{N;+\}$ 是半群, $\{N;\cdot\}$ 是幺半群. ②集合 A 的幂集 $\{\{P(A)\};\cap\},\{\{P(A)\};\cup\}$ 是幺半群.

幺半群中幺元的唯一性

$$e' = e'e = e$$

群一定是幺半群, 因此群中的幺元唯一.

2.11.3 群的基本性质

1. 消 (左, 右) 去律　群 G 中,$\forall a,b,c \in G$　$ab = ac(ba = ca) \Rightarrow b = c$
2. 群中的逆元是唯一的.

   证: 若 b 与 b' 均是 a 的逆元, 即 $ba = b'a \Rightarrow b = b'$
3. 群的定义方面的性质
   ① 在群 G 中,$\forall a,b \in G$, 方程 $ax = b$ 及 $xa = b$ 的解存在且唯一.
   ② 命题 2.11.1　若半群 G 满足:$\forall a,b \in G$, 方程 $ax_1 = b, x_2a = b$, 均有解, 则 G 是群.
   ③ 定理 2.11.1 有限半群 G, 若满足左, 右消去律, 则 G 是群.
4. 群中元素的整数次幂 (倍)

$$a^n \equiv a \ldots a(n \text{ 个 } a) \qquad a^0 \equiv e(1) \qquad a^{-n} = \left(a^{-1}\right)^n$$

$$na = a + \ldots + a \qquad 0a = 0 \qquad -na = n(-a)$$

5. 置换, 置换群

   当 $|A|= n$ 时, 全变换群 S_A 称为置换群, 记为 S_n, S_n 中的元素称为 n 元置换, 记为

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

   (a). 轮换 $(21538) \equiv \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 8 & 4 & 3 & 6 & 7 & 2 \end{pmatrix}$

   (b). 任一置换都可以表为有限个不相交轮换的乘积, 且不计乘积次序时, 表法是唯一的.
6. 群的阶; 有限群和无限群

   (a). 2.11.3 群 G 中元素的个数称为群的阶. 记为 $|G|$

$$|G| \begin{cases} < +\infty & \text{有限群} \\ = +\infty & \text{无限群} \end{cases}$$

   (b). 例:$\{R^*;\cdot\}$ 无限群,$\{\{1,-1\};\cdot\}$ 有限群.

   (c). 群表

·	1	-1
1	1	-1
-1	-1	1

(有限群, 内涵, 元素表达, 运算)

2.11.4 群中元素的阶

1. 2.11.4 设 G 是群, 运算记为乘法 (加法)，a 是 G 中一个元素, 如果 $\forall k \in N, a^k \neq e\ (ka \neq 0)$ 则称元素 a 的阶为无穷. 如果 $\exists k \in N, a^N = e\ (ka \neq 0)$ 则称 $\min\{k \in N |\ a^k = e\ (ka = 0)\}$ 为 a 的阶.
   (a). 只有幺元的阶是 1.
   (b). a 与 a^{-1} 有相同的阶.$(\forall k \in N, a^k = e \Longleftrightarrow \left(a^{-1}\right)^k = e)$
2. 性质
   (a). 命题 2.11.2　设 $a \in G$, 则 a 的阶是无穷 $\Longleftrightarrow \forall m \neq n, m, n \in Z$ 有 $a^m \neq a^n$
   (b). 命题 2.11.3　设 $a \in G$, 则 a 的阶为 d, 则
      I. $\forall k \in Z \quad a^h = e \Longleftrightarrow d|h$
      II. $\forall m, n \in Z \quad a^m = a^n \Longleftrightarrow d|(m-n)$
   (c). 命题 2.11.4　设 $a \in G$, 则 a 的阶为 d,$k \in N$ 则
      I. $a^k = \frac{d}{(d,k)}$
      II. $a^k = d \Longleftrightarrow (d, k) = 1$
   (d). 命题 2.11.5　设 $a, b \in G$,a 的阶为 m,b 的阶为 n,$ab = ba$,$(m, n) = 1$, 则 ab 的阶为 mn.

2.12 子群与商群

2.12.1 子群

1. 2.12.1 设 H 是群 G 的一个非空子集, 如果 H 对于 G 的运算也构成群, 则称 H 为 G 的一个子群, 记作 $H < G$.(对任一群 G,$H = e$ 与 $H = G$ 都是 G 的子群, 它们称为 G 的平凡子群,G 的其他子群称为非平凡子群)
2. 例 1 $\{\mathbb{R}_+; \cdot\} < \{\mathbb{R}^*; \cdot\}$, 这里 $\mathbb{R}_+$, 表示全体正实数.
   $\{\{1, -1\}; \cdot\} < \{\mathbb{R}^*; \cdot\}$.
   例 2 设 V 是数域 P 上的 n 维线性空间, S_V, 为 V 上的全体可逆变换由 S_V ,$\{S_V\}$；是群. 现再以 $GL(V)$ 表示 V 上全体可逆线性变换的集合. 以 $SL(V)$ 表示 V 上全体行列式为 1 的线性变换的集合则 $GL(V) < S_V$. $SL(V) < S_V$, $SL(V) < GI(V)$
   我们称 $GL(V)$ 为 V 的一般线性群, 称 $SL(V)$ 为 V 的特殊线性群. 由于在 n 维线性空间中取定一组基后，V 上的线性变换与 P 上的 n 阶方阵之间就建立了一一对应的关系，所以，也常用 $GL_n(R)$ 表示 n 阶实可逆方阵的集合关于矩阵乘法构成的群称为一般实线性群用 $SL_n(R$ 戒示行列式为 1 的 n 阶实方阵关于矩阵乘法构成的群称为特殊实线性群。于是也有 $SL_n(R) < GL_n(R)$.
   例 3 设 $m \in Z$, 则 $mZ = \{mn \mid n \in Z\}$ 是整数加群 Z 的子群.
3. 等价条件
   定理 2.12.1 设 H 是群 G 的非空子集则下面的条件是等价的：

(a). H < G:
(b). $a, b \in H \implies ab \in H, a^{-1} \in H$:
(c). $a, b \in H \implies ab^{-1} \in H$.

命题 2.12.1 设 H 为群 G 的非空有限子集则

$$H < G \iff H \text{ 对 } G \text{ 中的运算封闭.}$$

4. 子群的交也是子群

命题 2.12.2 若 H_1, H_2 均是群 G 的子群则 $H_1 \cap H_2 < G$.

2.12.2 左陪集与右陪集

1. 2.12.2 设 H 是群 G 的一个子群 $a \in G$ 则$aH = \{ah \mid h \in H\}, Ha = \{ha \mid h \in H\}$分别称为以 a 为代表的 H 的左陪集 **右陪集**。
2. 定理 2.12.2 设 H 是群 G 的子群则由所确定的 G 中的关系 R 是一个等价关系且 a 所在的等价类 $\overline{a}$ 恰为以 a 为代表的 H 的左陪集 aH。故 H 的全体左陪集 (重复的只取一个) 集合 $\{aH\}$ 是 G 的一个分类。
3. 推论

设 H 是群 G 的子群 $a, b \in G$, 则 $aH = bH :\iff a^{-1}b \in H$.

4. 左陪集空间, 子群的指数
   (a). 2.12.3 设 H 为群 G 的子群 G 关于等价关系 $aRb \longleftrightarrow a^{-1}b \in H$ 的商集合 G/R 称为 G 对 H 的左商集, 也称为 G 对 H 的左陪集空间, 也记为 G/H.

   G/H 的基数 $|G/H|$ 称为 H 在 G 中的指数记为 $[G : H]$.

   如果群 G 中的运算记作加法 $a^{-1}b$ 记为 $b - a$, $a + H = \{a + h \mid h \in H\}$

   (b). 定理 2.12.3 Lagrange 定理

   设 G 是有限群 $H < G$ 则有

   $$|G| = [G : H] \mid H \mid .$$

   从而子群 H 的阶是群 G 的阶的因子。

   (c). 推论

   设 G 是有限群 $K < G$. $H < K$ 则有

   $$[G : H] = [G : K]\,[K : H]$$

2.12.3 正规子群

1. 2.12.4 设 G 是群 $H < G$ 如果有

   $$ghg^{-1} \in H, \forall\, g \in G, \forall\, h \in H,$$

   则称 H 为 G 的一个正规子群 **记为** $H \triangleleft G$.
2. 定理 2.12.4 设 G 是群 $H < G$ 则下边的条件是等价的:
   (a). $H \triangleleft G$
   (b). $gH = Hg, \forall\, g \in G$
   (c). $g_1 H g_2 H = g_1 g_2 H, \forall g_1\, g_2 \in G$.

这里 $g_1H \cdot g_2H = \{g_1h_1g_2h_2 \,|h_1, h_2 \in H\}$.

一般地, 子群 H 的两个左陪集的乘积不一定仍是在陪集, 但当 H 是 G 的正规子群时, 两个左陪集的乘积一定是在陪集, 并且乘积的代表元就是原来两个左陪集代表元的乘积.

2.12.4 商群

1. 定理 2.12.5

   设 G 是群 $H < G$.R 是 G 中由 $aRb \Longleftrightarrow a^{-1}b \in H$" 定义的关系则

   $$R \text{ 是 G 中的同余关系} \Longleftrightarrow H < G.$$

   此时商集合 G/R 对同余关系 R 导出的运算也构成一个群称为 G 对 H 的商群记为 G/H. 要注意的是, 只有对 G 中的正规子群 H 才能谈论商群, 对一般的子群是不能谈商群而只能谈左陪集空间 (左商集).

2.13 群的同态与同构

2.13.1 群的同态与同构

1. 2.13.1 设 $\{G_1;\cdot\}$ 与 $\{G_2;\circ$ 是两个群 f 是 G_1 到 G_2 的一个映射如果
$$f(a\cdot b)=f(a)\circ f(b),\quad \forall\, a,b\in G_1.$$
则称 f 是 G_1 到 G_2 的一个同态映射, 简称同态. 若 G_1 与 G_2 是同一个群则称 f 是自同态. 若同态 f 还是单射则称 f 是单同态; 若同态 f 还是满射则称 f 是满同态. 当 f 是满同态时, 称 G_1 与 G_2 是同态的. 若同态 f 还是双射 (双射即可逆映射, 也即既是单射又是满射) 则称 f 是 G_1 到 G_2 的一个同构映射, 简称同构. 此时称群 G_1 与 G_2 是同构的 $G_2\simeq G_2$.
2. 性质

命题 2.13.1　若 f 是群 G_1 到群 G_2 的同态，G_2 是群 G_2 到群 G_3 的同态，则 gf 是 G_1 到 G_3 的同态。若 g,f 都是满（单）同态，则 gf 也是满（单）同态。若 g,f 都是同构, 则 f^{-1} 也是同构.

命题 2.13.2　设 f 是群 G_1 到群 G_2 的同态,e_1,e_2 分别为 G_1 G_2 的幺元则有 $f(e_1)=e_2$ 及 $\forall\, a\in G.f(a^{-1})=f(a)^{-1}$.

命题 2.13.3　设 f 是群 G_1 到群 G_2 的同态 $H<G_1$, 则 H 的象集合 $f(H)$ 也是 G_2 的子群, 特别，$f(G_1)<G_2$.

2.13.2 同态基本定理

1. 同态核
   (a). 2.13.2 设 f 是群 G_1 到群 G_2 的同态则 G_2 的幺元 e_2 的完全原象 $\{a\in G_1\mid f(a)=e_2\}$ 称为同态映射 f 的核, 记为 $\ker f$.
   (b). 命题 2.13.4　设 f 是群 G_1 到群 G_2 的同态则 $\ker f\lhd G_1$.
   (c). 命题 2.13.5　设 f 是群 G_1 到群 G_2 的同态, 则 f 是单同态 $\Longleftrightarrow \ker f=\{e_1\}$. 这里 e_1 是 G_1 的幺元.
2. 群的同态基本定理

   定理 2.13.1 设 f 是群 G_1 到群 G_2 的满同态映射则 $G_1/\ker f\simeq G_2$.
3. 推论

   设 G 为一群, f 是 G 到另一群的同态映射, 则 G 的同态象 G 必同构于 G 的商群 $G/\ker f$; 反之, G 的任一商群都可看作 G 的同态象。

2.13.3 群的同态定理

1. 定理 2.13.2 设 f 是群 G_1 到群 G_2 的满同态 $N=\ker f$ 则
   (a). f 建立了 G_1 中包含 N 的子群与 G_2 中子群间的双射；
   (b). 上述双射把正规子群对应到正规子群；

(c). 若 $H \lhd G_1, N \subseteq H$ 则 $G_1/H \simeq G_2/f(H)$.

2. 推论

设 G 是群,$N \lhd G, \pi$ 是 G 到 G/N 的自然同态，则 π 建立了 G 中包含 N 的子群与 G/N 的子群间的双射，而且把正规子群对应到正规子群. 又若 $H \lhd G$，$N \subseteq H$，则 $G/H \simeq (G/N)/(H/N)$.

3. 定理 2.13.3 设 G 是群，$N < G$，π 是 G 到 G/N 的自然同态，$H < G$ 则

(a). HN 是 G 中包含 N 的子群且

$$HN = \pi^{-1}(\pi(H)).$$

即 HN 是 H 在 π 映射下的象集合 $\pi(H$ 的完全原象 $\pi^{-1}(\pi(H))$.

(b). $(H \cap N) \lhd H$ 且 $ker(\pi|_H) = H \cap N$.

(c). $HN/N \simeq H/(H \cap N)$.

2.14 循环群

2.14.1 循环群

1. 2.14.1 由一个元素 a 反复运算生成的群

$$G = \{a^n \mid n \in Z\}$$

称为循环群记为 (a) μ 称为这个循环群的生成元。

2. 定理 2.14.1 循环群都是交换群，循环群的子群也是循环群。
3. 推论

整数加群 Z 的子群必形如 mZ,m, $N \cup \{0\}$.

2.14.2 循环群的分类

定理 2.14.2 设群 $G =< a >$。若 G 是无限阶的, 则 G 与 $\{\mathbf{Z}; +\}$ 同构若 G 是有限阶 m 阶的则 G 与 $\{\mathbf{Z}_m; +\}$ **同构**. 所以两个循环群同构的充要条件是它们有相同的阶.

2.14.3 循环群的子群

定理 2.14.3 设 G 是 m 阶循环群，m_1 是 m 的一个正整数因子则存在 G 的唯一的 m_1 阶子群.
定理 2.14.4 设 G 是 m 阶群则 G 是循环群的充要条件是，对 m 的每个正整数因子 m_1，都存在 G 的惟一的 m_1 阶子群。
命题 2.14.1　有限群 G 的任一元素 a 的阶是有限的, 且是 G 的阶的因子。

2.14.4 生成的子群

1. 2.14.2 设 S 是群 G 中一个非空子集. 记 $S^{-1} = \left\{a^{-1} | a \in S\right\}$ 则

$$\{x_1, \ldots x_m | x_1, \ldots, x_m \in SUS^{-1}\}.$$

是 G 的一个子群称为 S 生成的子群记为 $< S >$.

2. 等价说法
   (a). $< S >$ 是 G 中包含 S 的最小群
   (b). $< S >$ 是 G 中所有包含 S 的子群的交

2.15 变换群与置换群

2.15.1 变换群

1. 2.15.1 设 A 是非空集合 A 的所有可逆变换关于映射的乘法构成的群称为 A 的全变换群. 记为 $\{S_A;\cdot\}$. 简记为 S_A . S_A 的一个子群称为 A 的一个变换群. 当 A 为含有 n 个元素的有限集时 S_A 也叫作 n 元对称群, 也记作 S_n . S_n 中的一个元素称为一个 n 元素换 S_A 的一个子群称为一个 n 元置换群.
2. 定理 2.15.1 (凯莱 (Cayley) 定理) 任何一个群都与一个变换群同构.
   任一有限群都与一个量换群同构。
3. 命题 2.15.1　任一有限群都与一个量换群同构。
   定义 1.6.2 设集合 $\{i_1, i_2, \ldots, i\}$ 为集合 $\{1, 2, \ldots, n\}$ 的一个子集. 若 $\sigma \in S_n$ 满足
   $$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1,$$
   及
   $$\sigma(k) = k. \forall k \in \{1, 2, \ldots, n\} \setminus \{i_1, i_2, \ldots, i_r\},$$
   则称 σ 为 S_n 中的一个 r —轮换. 或称 r —循环置换，记为 $\sigma = (i_1 i_2 \cdot i_n). i_1 i_2, \ldots, i_r$ 均为轮换 σ 中的文字, r 称为轮换 σ 的长.
   特别 2 —轮换 ij 称为对换. 恒等量换可记为 1—轮换.

2.15.2 置换群

若 $\sigma \in S_n$, 则 σ 称为一个 n **元置换**通常表示为
$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}.$$
它的含义是 $\sigma(1) = i_1, \sigma(2) = i_2, \cdots \sigma(n) = i_n$. 由于 σ 是双射所以 $i_1 i_2, \cdots, i_n$ 是 1 2 $\cdots$ n 的一个排列. 并且不同的排列得到的置换 σ 也不同. 因此 n 元置换的个数 就是 $1 \geq n$, n 的所有排列的个数。于是有:n 元对称群 S_n 的阶是 $n!$

命题 2.15.2　任一 n 元置换都可以表为一些对换的乘积。

2.15.3 自同构群；内自同构群

2.15.2 群 G 到自身的同构映射称为 G 的一个自同构群 G 的全体自同构的集合记为 Aut G.

命题 2.15.3　设 G 是群则 Aut $G < S_G$ 称 Aut G 为群 G 的自同构群。

命题 2.15.4　设 G 是群则 Aut $G < S_G$ 称 Aut G 为群 G 的自同构群。

命题 2.15.5　命题 1.6.13 设 G 为群 $a \in G$ 定义映射 $\sigma_a : G \to G$ 为
$$\sigma_a(g) = aga^{-1}. \forall g \in G,$$
则 $\sigma_a \in \mathrm{Aut}G$ 称为由 a 决定的内自同构. 记
$$InnG = \{\sigma_a \mid a \in G\}$$
则 $InnG \lhd AutG$ 称 $InnG$ 为 G 的内自同构群.

2.16 群在集合上的作用

2.16.1 群在集合上的作用

2.16.1 设 G 是一个群，Ω 是一个非空集合。如果 $G\times\Omega$ 到 Ω 有一个映射：$(a,x)\mapsto a\circ x$，满足

$$(ab)\circ x = a\circ(b\circ x), \forall a,b\in G, \forall x\in\Omega;$$

$$e\circ x = x, \forall x\in\Omega$$

则称群 G 在集合 Ω 上有一个作用 (action).

命题 2.16.1　设群 G 在集合 Ω 上有一个作用. 任意给定 $a\in G$，令

$$\psi(a)\,x \xlongequal{def} a\circ x \quad \forall x\in\Omega, \tag{2.2}$$

则 ψ 是群 G 到 Ω 的全变换群 S_Ω 的一个同态.

命题 18.1 的逆命题也成立, 即, 如果群 G 到非空集合 Ω 的全变换群 S_Ω 有一个同态 ψ, 令

$$a\circ x \xlongequal{def} \psi(a)x, \quad \forall a\in G, \quad \forall x\in\Omega, \tag{2.3}$$

则群 G 在集合 Ω 上有一个作用; $(a,x)\mapsto a\circ x$.

设群 G 在集合 Ω 上有一个作用，据命题 18.1，它引起了群 G 到 S_Ω 的一个同态 ψ. 我们把同态 ψ 的核 $\ker\psi$ 称为这个作用的核。显然群 G 中元素 a 属于作用的核当且仅当 $a\circ x = x$，$\forall x\in\Omega$ 如果作用的核仅由单位元 e 组成，则称这个作用是**忠实的** (faithful)，此时 ψ 是群 G 到 S_Ω 的单同态.

群 G 在集合 G 上的左平移设 G 是一个群，令

$$G\times G \longrightarrow G$$

$$(a,x) \longrightarrow ax.$$

显然有 $(ab)x = a(bx)$，$ex = x$，$\forall x\in G$，$\forall a,b\in G$. 因此上式给出了群 G 在集合 G 上的一个作用，称这个作用为群 G 在集合 G 上的左平移（left translation）.

群 G 在集合 G 上的共轭作用

$$G\times G \to G$$

$$(a,x) \longmapsto axa^{-1}.$$

对于任意 $a,b\in G$, 任意 $x\in G$, 有

$$\begin{aligned}(ab)\circ x = (ab)x(ab)^{-1} &= a(bxb^{-1})a^{-1}\\ &= a(b\circ x)a^{-1} = a\circ(b\circ x),\\ e\circ x = exe^{-1} &= x,\end{aligned}$$

因此式给出了群 G 在集合 G 上的一个作用, 称它为群 G 在集合 G 上的共轭作用 (conjugation action).

群 G 在集合 G 上的共轭作用的核是群 G 的中心.

定理 2.16.1 群 G 的内自同构群 $\mathrm{Inn}(G)$ 同构于群 G 对于中心 $Z(G)$ 的商群 $G/Z(G)$.

2.16.2 轨道

2.16.2 设群 G 在集合 Ω 上有一个作用，对于 $x \in \Omega$，令

$$G(x) \overset{def}{=} \{g \circ x | g \in G\},$$

称 $G(x)$ 是 x 的 G–轨道 (orbit).

在集合 Ω 中规定一个二元关系如下：

$$x \sim y \iff \text{存在} g \in G, \text{使得} y = g \circ x$$

容易验证 $\sim$ 是等价关系. 由 x 确定的等价类 $\overline{x}$ 为

$$\begin{aligned}\overline{x} &= \{y \in \Omega \mid x \sim y\} \\ &= \left\{y \in \Omega \text{存在} g \in G, \text{使得} y = g \circ x\right\}, \\ &= \{g \circ x \mid g \in G\} \\ &= G(x).\end{aligned}$$

因此所有轨道 (即等价类) 组成的集合给出了 Ω 的一个划分. 由于轨道就是等价类，因此任意两条轨道或者相等，或者不相交. 于是有

$$\Omega = \bigcup_{i=1}^{r} G(x_i),$$

其中 $G(x_i) \cap G(x_j) = \varnothing$，当 $i \neq j$ 我们把集合 $\{x_i \mid i \in I\}$ 称为 Ω 的 G-轨道的完全代表系。

如果群 G 在集合 Ω 上的作用只有一条轨道，即对于任意 $x, y \in \Omega$, 存在 $g \in G$ 使得 $y = g \circ x$, 则称 G 在 Ω 上的这个作用是传递的 (transitive)。此时称 Ω 是群 G 的一个 **齐性空间** (homogeneous space).

例如，群 G 在左商集 (G/H), 上的左平移是传递的, 这是因为对于任意 $xH, yH \in (G/H)$, 有

$$(yx^{-1}) \circ xH = yx^{-1}xH = yH,$$

从而左商集 (G/H), 就是群 G 的一个齐性空间。

考虑群 G 在集合 G 上的共轭作用，x 的轨道为

$$G(x) = \left\{gxg^{-1} | \ g \in G\right\}.$$

我们把上式右端的集合称为 x 的共轭类 (conjugacy class). 从式看出，x 的共轭类就是群 G 在集合 G 上的共轭作用下 x 的轨道. 从而群 G 的任意两个共轭类或者相等，或者不相交. 从共轭类的定义看出，x 的共轭类只含一个元素当且仅当 $x \in Z(G)$. 于是当 G 是有限群时，可得出

$$|G| = |\ Z(G)| \ | + \sum_{j=1}^{r} | \ G(x_j)|$$

其中 $G(x_j)$ 是 x_j 的共轭类，$x_1, \cdots, x_r$ 是 G 中非中心元素的共轭类的完全代表系，我们把上式称为有限群 G 的类方程 (class equation). 给定 $x \in G$，任取 $g \in G$，gxg^{-1} 称为 x 的共轭元 (conjugate elements).

2.16.3 轨道稳定子定理

2.16.3 设群 G 在集合 D 上有一个作用. 给定 $x \in \Omega$，令

$$G_x \overset{\text{def}}{=} \{g \in G \mid g \circ x = x\},$$

称 G_x 是 x 的 **稳定子** (stabilizer). 容易验证，G_x 是 G 的一个子群。因此也称 G_x 是 x 的 **稳定子群**。

我们把 (23) 式右端的集合称为 x 在 G 里的 **中心化子** (centralizer)，记作 $C_G(x)$，它就是在群 G 的共轭作用下 x 的稳定子群.

定理 2.16.2 (轨道一稳定子定理) 设群 G 在集合 Ω 上有一个作用, 则对于任意给定的 $x \in \Omega$, 有

$$|G(x)| = [G : G_x]$$

即, x 的轨道的基数等于 x 的稳定子在 G 中的指数.

推论 如果有限群 G 在集合 Ω 上有一个作用, 则每一条轨道的长 (即轨道的基数) 是 G 的阶的因子, 即

$$|G| = |G_x||\ G(x)\ |\ .$$

命题 2.16.2　设群 G 在集合 Ω 上有一个作用，则同一条轨道上的点，它们的稳定子群彼此共轭，从而这些稳定子群的基数相同.

定理 2.16.3 (Burnside 引理) 设有限群 G 在有限集合 Ω 上有一个作用, 用 $F(g)$ 表示 g 的不动点集, 即

$$F(g) \overset{def}{=} |x \in \Omega \mid g \circ x = x|.$$

则轨道条数 r 为次

$$r = \frac{1}{|\ G\ |} \sum_{g \in G} |\ F(G)\ |\ .$$

即, 轨道条数等于平均被 G 的一个元素保持不动的点的数目.

定理 2.16.4 (Polya 定理) 设有限取 G 作用在 n 个对象组成的集合 W 上 G 中元素 $\tilde{g}$ 在 W 上的置换表示记作 $\tilde{g}$, 用 m 种颜色给 W 里的 n 个对象染色, 则真正不同的染色方案的个数 r 为

$$r = \frac{1}{|G|} \sum_{g \in G} m^{r(\tilde{g})}$$

其中 $r(\tilde{g})$ 是 $\tilde{g}$ 的轮换表示中轮换的个数 (包括 1-轮换).

群 G 在集合 G 上的共轭作用的核是群 G 的中心.

定理 2.16.5 群 G 的内自同构群 $\mathrm{Inn}(G)$ 同构于群 G 对于中心 $Z(G)$ 的商群 $G/Z(G)$.

2.16.4 轨道

2.16.4 设群 G 在集合 Ω 上有一个作用，对于 $x \in \Omega$，令

$$G(x) \overset{def}{=} \{g \circ x | g \in G\},$$

称 $G(x)$ 是 x 的 G–轨道 (orbit).

在集合 Ω 中规定一个二元关系如下：

$$x \sim y \iff \text{存在} g \in G, \text{使得} y = g \circ x$$

容易验证 $\sim$ 是等价关系. 由 x 确定的等价类 $\overline{x}$ 为

$$\begin{aligned}\overline{x} &= \{y \in \Omega \mid x \sim y\} \\ &= \left\{y \in \Omega \text{存在} g \in G, \text{使得} y = g \circ x\right\}, \\ &= \{g \circ x \mid g \in G\} \\ &= G(x).\end{aligned}$$

因此所有轨道 (即等价类) 组成的集合给出了 Ω 的一个划分. 由于轨道就是等价类，因此任意两条轨道或者相等，或者不相交. 于是有

$$\Omega = \bigcup_{i=1}^{r} G(x_i),$$

其中 $G(x_i) \cap G(x_j) = \varnothing$，当 $i \neq j$ 我们把集合 $\{x_i \mid i \in I\}$ 称为 Ω 的 G-轨道的完全代表系。

如果群 G 在集合 Ω 上的作用只有一条轨道，即对于任意 $x, y \in \Omega$, 存在 $g \in G$ 使得 $y = g \circ x$, 则称 G 在 Ω 上的这个作用是传递的 (transitive)。此时称 Ω 是群 G 的一个 **齐性空间** (homogeneous space).

例如，群 G 在左商集 (G/H), 上的左平移是传递的, 这是因为对于任意 $xH, yH \in (G/H)$, 有

$$(yx^{-1}) \circ xH = yx^{-1}xH = yH,$$

从而左商集 (G/H), 就是群 G 的一个齐性空间。

考虑群 G 在集合 G 上的共轭作用，x 的轨道为

$$G(x) = \left\{gxg^{-1} \mid g \in G\right\}.$$

我们把上式右端的集合称为 x 的共轭类 (conjugacy class). 从式看出，x 的共轭类就是群 G 在集合 G 上的共轭作用下 x 的轨道. 从而群 G 的任意两个共轭类或者相等，或者不相交. 从共轭类的定义看出，x 的共轭类只含一个元素当且仅当 $x \in Z(G)$. 于是当 G 是有限群时，可得出

$$|G| = |Z(G)| + \sum_{j=1}^{r} |G(x_j)|$$

其中 $G(x_j)$ 是 x_j 的共轭类，$x_1, \cdots, x_r$ 是 G 中非中心元素的共轭类的完全代表系，我们把上式称为有限群 G 的类方程 (class equation). 给定 $x \in G$，任取 $g \in G$，gxg^{-1} 称为 x 的共轭元 (conjugate elements).

2.16.5 轨道稳定子定理

2.16.5 设群 G 在集合 D 上有一个作用. 给定 $x \in \Omega$，令

$$G_x \overset{\text{def}}{=} \{g \in G \mid g \circ x = x\},$$

称 G_x 是 x 的 **稳定子** (stabilizer). 容易验证，G_x 是 G 的一个子群。因此也称 G_x 是 x 的 **稳定子**

群。

我们把 (23) 式右端的集合称为 x 在 G 里的 **中心化子** (centralizer)，记作 $C_G(x)$，它就是在群 G 的共轭作用下 x 的稳定子群.

定理 2.16.6 (轨道一稳定子定理) 设群 G 在集合 Ω 上有一个作用, 则对于任意给定的 $x \in \Omega$, 有

$$|G(x)| = [G : G_x]$$

即, x 的轨道的基数等于 x 的稳定子在 G 中的指数.

推论 如果有限群 G 在集合 Ω 上有一个作用, 则每一条轨道的长 (即轨道的基数) 是 G 的阶的因子, 即

$$|G| = |G_x||\ G(x)\ | .$$

命题 2.16.3　设群 G 在集合 Ω 上有一个作用，则同一条轨道上的点，它们的稳定子群彼此共轭，从而这些稳定子群的基数相同.

定理 2.16.7 (Burnside 引理) 设有限群 G 在有限集合 Ω 上有一个作用, 用 $F(g)$ 表示 g 的不动点集, 即

$$F(g) \overset{def}{=} |x \in \Omega \mid g \circ x = x|.$$

则轨道条数 r 为次

$$r = \frac{1}{|\ G\ |} \sum_{g \in G} |\ F(G)\ | .$$

即, 轨道条数等于平均被 G 的一个元素保持不动的点的数目.

定理 2.16.8 (Polya 定理) 设有限取 G 作用在 n 个对象组成的集合 W 上 G 中元素 $\tilde{g}$ 在 W 上的置换表示记作 $\tilde{g}$, 用 m 种颜色给 W 里的 n 个对象染色, 则真正不同的染色方案的个数 r 为

$$r = \frac{1}{|G|} \sum_{g \in G} m^{r(\tilde{g})}$$

其中 $r(\tilde{g})$ 是 $\tilde{g}$ 的轮换表示中轮换的个数 (包括 1-轮换).

2.17 染色问题

现在让我们回到染色问题上，首先让我重复一下这个问题：
使用 n 种不同的颜色对正 n 边形的顶点进行染色，每种颜色可以使用多次（对顶点染色），也可以一次都不用，正 n 边形的每个顶点都要进行染色，如果正 n 边形经过刚体运动，使得两种不同状态最后看起来是一样的（重合），那么称这两种状态是一个方案。（当然，需要保证每个三角形都是一样的边长）

问题是：对于一个确定的 n，由 n 确定的方案总数 S 是多少；对于 n 来说，S 有通项公式吗？

首先让我们考虑正 n 边形的刚体运动能和原本重合对应的群：

(1) 不做任何运动，它对应于恒等变换，记作 I。

(2) 考虑通过几何中心的轴为旋转轴，旋转 180° 后，能与原本位置重合的几何变换。当 n 是偶数时，一种是经过顶点的，有 $\frac{n}{2}$ 个，记作 σ_1, 另一种是不经过顶点的记作 σ_2，也有 $\frac{n}{2}$ 个，共有 n 个；当 n 是奇数时，都经过顶点，这样的变换有 n 个，记作 σ。

(3) 想象正 n 边形所在的平面与其几何中心，正 n 边形有 n 个顶点，考虑绕几何中心的旋转，那些能与原本位置重合的旋转是 $\frac{360^\circ}{n_i}$，其中 n_i 取值范围是整数 2 到 n，这样的几何变换共有 $n-1$ 个。这样的变换记作 τ_{n_i}

上述的三种变换，构成了一个群，我们称之为二面体群，显然二面体群里的元素有 $2n$ 个。

如果把把正 n 边形的每个顶点看作是不同的对象，上述变换把正 n 边形的每个顶点变换到另外的一些顶点，在这些变换中有些点对应，有些点不对应。

如果对应的点染相同的颜色，非对应的点染不同颜色那么相应的不对应点的组数为：

(1) 对于恒等变换为 n

(2) 当 n 是偶数时 $\sigma_1 = \frac{n}{2} + 1$，$\sigma_2 = \frac{n}{2}$，当 n 是奇数时 $\sigma = \frac{n-1}{2} + 1 = \frac{n+1}{2}$

(3) 当 n 与 n_i 的最大公因式是 1 时，n; 当 n 与 n_i 的最大公因式是 k 时，$\frac{n}{k}$

然后考虑每组对应点包含多少点

(1) 对于恒等变换为 n

(2) 当 n 是偶数时 σ_1：2 个单独的对应点组，这两组之中只有一个单独的点它们不与其他任何点对应；还有 $\frac{n}{2} - 1$ 个对应组，它们中有 2 个对应点。σ_2，有 $\frac{n}{2}$ 个对应组，它们中有 2 个对应点。当 n 是奇数时 σ，1 个单独的对应点组，中只有一个单独的点它不与其他任何点对应，有 $\frac{n-1}{2}$ 个对应组，它们中有 2 个对应点。

(3) 当 n 与 n_i 的最大公因式是 1 时，n; 当 n 与 n_i 的最大公因式是 k 时，有 $\frac{n}{k}$ 个对应组，每组有 k 个对应点。

最后一步，让我们进行如下的计算：对于上述的每种变换的每个对应组：点数做底数，组数做幂，然后把他们加起来，最后再除以相应的二面体群的基数，最后的最后计算这个式子的值。

举个例子：对于 D3

$$\frac{3^3+3\times3^2+2\times3^1}{2\times3}=10$$

对于 D4

$$\frac{4^4+2\times4^3+2\times4^2+2\times4^1+1\times4^2}{2\times4}=55$$

如果你有惊人的注意力的话那么：n 为 3，4 时的方案数为 10，55。上述的步骤大概讲述了得到答案的整个过程，当然这省去了大部分的步骤，其中最为主要的就是群论。

当然，我更想说的是在上面讨论的“考虑每组对应点包含多少点”中的 (3) 如果你能详细考虑这一点的话对比 (1)(2)，他没有那么的公式化。。(3) 比较过程化，其公式化过程较为繁琐，其公式化结果也不那么“公式化”。对于 D210 的公式化，我想我可以这幅图来描述。（这相当繁琐）

$$[(P_1-1)+(P_2-1)+(P_3-1)+(P_4-1)]+\{[(P_1P_2-1)+(P_1-1)+(P_2-1)]+[(P_1P_3-1)+(P_1-1)+(P_3-1)]+[(P_1P_4-1)+(P_1-1)+(P_4-1)]+[(P_2P_3-1)+(P_2-1)+(P_3-1)]+[(P_2P_4-1)+(P_2-1)+(P_4-1)]+[(P_3P_4-1)+(P_3-1)+(P_4-1)]\}+\{[(P_1P_2P_3-1)-\{[(P_1P_2-1)+(P_1-1)+(P_2-1)]+[(P_1P_3-1)+(P_1-1)+(P_3-1)]+[(P_2P_3-1)+(P_2-1)+(P_3-1)](P_1-1)+(P_2-1)+(P_3-1)\}\}+\{[(P_1P_2P_4-1)-\{[(P_1P_2-1)+(P_1-1)+(P_2-1)]+[(P_1P_4-1)+(P_1-1)+(P_4-1)]+[(P_2P_4-1)+(P_2-1)+(P_4-1)]-\{(P_1-1)+(P_2-1)+(P_4-1)\}\}+\{[(P_1P_3P_4-1)-\{[(P_1P_3-1)+(P_1-1)+(P_3-1)]+[(P_1P_4-1)+(P_1-1)+(P_4-1)]+[(P_3P_4-1)+(P_3-1)+(P_4-1)]-\{(P_1-1)+(P_3-1)+(P_4-1)\}\}+\{[(P_2P_3P_4-1)-\{[(P_2P_3-1)+(P_2-1)+(P_3-1)]+[(P_3P_4-1)+(P_3-1)+(P_4-1)]+[(P_2P_4-1)+(P_2-1)+(P_4-1)]-\{(P_2-1)+(P_3-1)+(P_4-1)\}\}=(P_1-1)(P_2-1)(P_3-1)(P_4-1)$$

图 2.11

在我的视角里这已经和数论中的难题“黎曼猜想”联系了起来（我是没能力搞这个.....）。

到这里，一部分内容我已经介绍了，但还有很多东西没有提及。原本的计划是多种内容相互交叉，但由于多种因素的影响，这些内容只能以模块化的形式出现了，但愿在后边我能把所有想写的全部写在这里。