群论的预备知识 [1]

leolinuxer

July 8, 2020

Contents

1 集合与映射

1.1 集合基本概念

- **并集**: $C = A \cup B$, 即 $x \in C \Leftrightarrow x \in A \quad or \quad x \in B$
- **交集**: $C = A \cap B$, 即 $x \in C \Leftrightarrow x \in A \quad \& \quad x \in B$
- **差集**: $C = A - B$, 即 $x \in C \Leftrightarrow x \in A \quad \& \quad x \notin B$
- **直积**: $C = A \times B = \{(a, b) | a \in A \& b \in B\}$

若映射 $f : A \to B$ 有如下不同情况, 可以区分出:

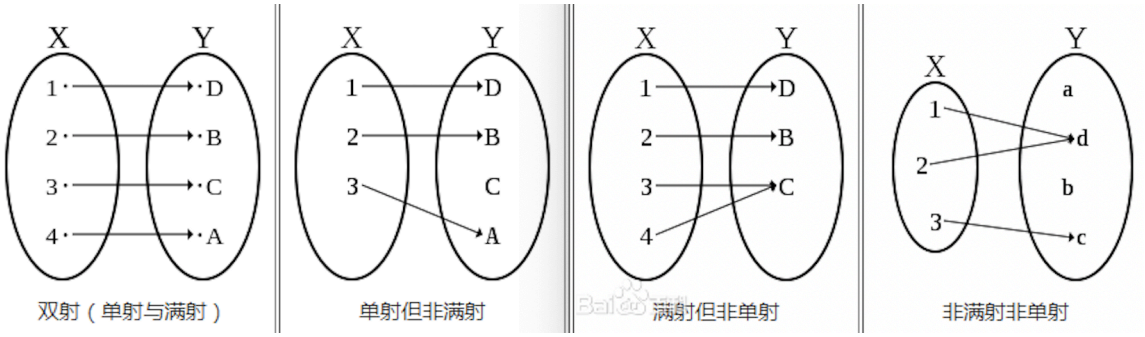
1) 若 $A \subset B$, 而 f 满足 $f(a) = a, \forall a \in A$, 则称 f 为**包含映射**, 记为 i; 若此时 $B = A$, 此时的 i 称为 A 的**恒等映射**, 记作 1_A。

2) 若 $f(A) = B$, 则称 f 为 A **到** B **的满射**

3) 若 $f(a) = f(a') \Rightarrow a = a', a, a \in A$, 则称 f 为**单射**。

4) 若 f 既是单射又是满射, 则称 f 为**双射**; 此时从 $f(a) = b$, 可记 $a = f^{-1}(b)$, 从而确定了映射 $f^{-1} : B \to A$, 称为 f 的**逆映射**。

5) 若 $C \subset A$, 则由于 $f(c) \in B$ 对应于 $c \in C$, 可定义 $f_c : C \to B$, 即把 f 的定义域缩小到 C 上, 则称 f_c 为 f 到 C 的**限制**。



如果 $f: A \to B$，且 $g: B \to C$，此时把 $a \in A$ 映为 $h(a) = g(f(a)) \in C$ 来定义映射 $h: A \to C$，则称 h 为 f 和 g 的**结合**，记作 $h = g \circ f$

如果 $f: A \to B$ 是双射，不难看出 $f^{-1}: B \to A$ 也是双射，且 $f^{-1} \circ f = 1_A, f \circ f^{-1} = 1_B$

对于 $f: A \to B, g: B \to C, h: C \to D$，有 $h \circ (g \circ f) = (h \circ g) \circ f$，即映射的结合运算满足结合律。

1.2 集合 A 中的变换

考虑 $f: A \to B$，且 $B = A$，即 f **是** A **到** A **自身的映射，把映射** f **称为** A **的一个变换**，即 f 将 $a \in A$ 变为 $f(a) \in A$。

A **的所有变换，构成集合** T**，称为** A **的变换全集**。

A **的所有双射构成** T **的一个重要子集，记作** G**，称为** A **的变换群**。集合 G 具有如下性质：

1) $1_A \in G$，即 G 中含有**恒等变换**。

2) $f \in G \Leftrightarrow f^{-1} \in G$

3) $f \in G, g \in G \Rightarrow g \circ f \in G$。因此 G 的元素对结合运算 $\circ$ 而言是**封闭的**。

4) 对于 $f, h, h \in G$，可知 $(h \circ g) \circ f = h \circ (g \circ f)$，即 G 的元素对 $\circ$ 满足结合律。

思考：T 包含 A 的**所有**变换，其中包括从 A 到 A 的双射（一一映射），也包括其它变换；而 A 的所有**双射**（一一映射）构成的 T 的子集 G，也就是 A 的变换群；

1.3 关系、等价关系与分类

1.3.1 关系

映射反应的是一个集合与另一个集合的外部联系；“关系”给出了集合内元素的内部联系。

集合上的一个**关系** $\sim$，指的是一种法则。由它可以判断任意 $a, b \in A$ 所构成的有序偶 (a, b) 是满足某种条件（此时称 a, b 有关系，记作 $a \sim b$），还是不满足这一条件（此时称 a, b 无关系，记作 $a \nsim b$）

例如大于 ($\geq$) 就给出了整数集合 Z 的一个关系；对于三角形的集合，三角形的全等和相似也分别给出了这个集合的一个关系。

1.3.2 等价关系

集合 A 上定义的关系 $\sim$，若满足如下条件，则称 $\sim$ 是一个等价关系：

1) 自反律：对 $\forall a \in A \Rightarrow a \sim a$

2) 对称率：对 $a \sim b \Rightarrow b \sim a$

3) 传递率：对 $a \sim b, b \sim c \Rightarrow a \sim c$

1.3.3 集合的分类

集合 A 的一个**分类**，指的是把 A 分成许多称为**类**的非空子集合 $A_a, A_b, \cdots$，而其中每两个不同类的交集为空集，它们全体的并集是 A。

设 $\sim$ 是集合 A 的一个等价关系，对于 $a \in A$，我们把 A 中所有与 a 等价的元都汇集在一起，而构造出 A 的子集合 A_a，如果此时存在 $b \in A$，且 $b \notin A_a$，则同样构造 A_b，显然这些 $A_a, A_b, \cdots$ 给出 A 的一个分类。

反过来，如果给定了 A 的一个分类，那么我们就可以如下的定义 A 的一个等价关系：$\sim$: $a \sim b$，当且仅当 a, b 属于同一类；$a \nsim b$，当且仅当 a, b 不属于同一类；

总结后有：集合 A 的一个分类可以确定它的一个等价关系；反之，集合 A 的一个等价关系可以确定它的一个分类。

因此，类也称为**等价类**。而 A_a 称为**由 a 确定的等价类**，a 是 A_a 的一个**代表**。当然，若 $a \sim b$，则 $A_a = A_b$，即一个等价类可以由其中的任一元做代表，因为有这种随意性，所以任何关于等价类的命题首先必须与**代表元的选取无关**。

全体奇数和全体偶数这两个集合构成了整数集合 Z 的一个分类。

理解：集合的分类是**不重不漏**的。

1.3.4 商集合

由 A 的等价关系 $\sim$，确定了 A 的各个类 $A_a, A_b, \cdots$，以这些类做为元素而得到的集合，称为由 A 按 $\sim$ 而确定的商集合，记作：

$$A/\sim = \{A_a, A_b, \cdots\}$$

此时，很自然的由 a 对应 A_a，可定义 $f : A \to A/\sim$，容易验证这是一个满射，称为 A 到商集合 $A/\sim$ 上的**自然映射**。

1.4 整数集合 Z 与同余关系

接下来，我们把上面的理论应用到整数集合 Z 上。取定 $n \in N^*$，定义关系 $\sim$: $a \sim b$，当且仅当 $a-b$ 能被 n 整除时（记作 $n|(a-b)$），称 a,b 对于**模 n 同余**，记作 $a \equiv b \mod(n)$。

可以证明，这是一个等价关系；这时的等价类称为模 n 的**同余类**；通常把以 a 为代表的同余类记作 $[a]_n$ 或简记为 $[a]$ 或 $\bar{a}$。而把此时的商集合记为 Z_n，称为**模 n 同余类集合**。于是：

$$\bar{a} = \{a + kn \mid k \in Z\}$$

$$Z_n = \{\bar{1}, \bar{2}, \cdots, \bar{n}\}$$

> 举例：
>
> 当 $n=2$ 时，模 2 同余的数分别为 $\{1,3,5,\cdots\}$ 和 $\{2,4,6,\cdots,\}$。因此 $Z_2 = \{\bar{1}, \bar{2}\}$；其中 $\bar{1}$ 为全体奇数，$\bar{2}$ 为全体偶数；
>
> 当 $n=7$ 时，$Z_7 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$；对于一年中的 365 天，这些同余类通常以周一、周二、……、周日来标记。同理，对于年份，可以按 $n=12$ 划分为以十二生肖为代表的 12 个同余类。

为了今后的应用，我们在 Z_n 中再划分出一个重要的子集 Z'_n 来。为此，对于 $l,m \in N^*$，我们以 (l,m) 来表示 l,m 的最大公因数。如果 l,m 互素，则 $(l,m)=1$。定义：

$$Z'_n = \{\bar{k} \in Z_n | 1 \le k \le n, (k,n) = 1\}$$

称为**模 n 同余类乘群**。

> 举例：当 $n=6$ 时，$Z_6 = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$，其中与 $n=6$ 互素的元素为 $\bar{1}, \bar{5}$，所以 $Z'_6 = \{\bar{1}, \bar{5}\}$；

当 p 是素数时，有 $Z_p = \{\bar{1}, \bar{2}, \cdots, \overline{p-1}, \bar{p}\}$，$Z'_p = \{\bar{1}, \bar{2}, \cdots, \overline{p-1}\}$

> 举例：当 $n=17$ 时，$Z'_{17} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \cdots, \overline{16}\}$；而数 3^m，对 $m=0,1,2,\cdots,15$ 所属的同余类分别为：
>
> - $m=0$ 时，$3^m=1$ 所属的同余类为 $\bar{1}$
> - $m=1$ 时，$3^m=3$ 所属的同余类为 $\bar{3}$
> - $m=2$ 时，$3^m=9$ 所属的同余类为 $\bar{9}$
> - $m=3$ 时，$3^m=27$ 所属的同余类为 $\overline{10}$
> - $\cdots$
>
> **即数 3^m，对 $m=0,1,2,\cdots,15$ 所属的同余类分别为：$\bar{1}, \bar{3}, \bar{9}, \overline{10}, \overline{13}, \bar{5}, \overline{11}, \overline{16}, \overline{14}, \bar{8}, \bar{7}, \bar{4}, \overline{12}, \bar{2}, \bar{6}$，它们是 $\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \cdots, \overline{16}$ 的另一种排列。**

1.5 算数基本定理与欧拉函数 $\varphi(n)$

欧拉函数 $\varphi(n)$ 的定义为 Z'_n 中元素的个数。即 $\varphi(x)$ 等于满足 $1 \le k \le n$，及 $(k,n)=1$ 的正整数 k 的个数。

根据定义，显然有：$\varphi(1)=\varphi(2)=1, \varphi(3)=\varphi(4)=\varphi(6)=2, \varphi(5)=4, \cdots$

证明如下：

$Z'_1=\{\bar{1}\}, Z'_2=\{\bar{1}\} \Rightarrow \varphi(1)=\varphi(2)=1$

$Z'_3=\{\bar{1},\bar{2}\}, Z'_4=\{\bar{1},\bar{2}\}, Z'_6=\{\bar{1},\bar{5}\} \Rightarrow \varphi(3)=\varphi(4)=\varphi(6)=2$

$Z'_5=\{\bar{1},\bar{2},\bar{3},\bar{4}\} \Rightarrow \varphi(5)=4$

为了推导 $\varphi(n)$ 的计算公式，我们先来叙述**算数基本定理**。因为任何大于 1 的整数 n 都或是合数或是素数。而如果 n 是合数，则 n 可以唯一地分解为一系列素数的乘积，这就是：

算数基本定理：对于大于 1 的自然数，一定可把它唯一地表达为 $n=p_1^{v_1}\cdot p_2^{v_2}\cdot\cdots\cdot p_k^{v_k}$，这里 $p_1,p_2,\cdots,p_k$ 是素数，且 $v_1,v_2,\cdots,v_k \in N^*$。

为了求得 $\varphi(n)$ 的表达式，先来讨论两个简单的情况，再把它们综合起来：

1) 首先求 $\varphi(p^n)$，这里 p 是素数。对于 $1 \le k \le p^n$ 的 k，要与 p^n 互素，其充要条件是 k 不能被 p 整除，即 $p \nmid k$。然而，在 1 到 p^n 之间，有 p^{n-1} 个数，即 $p, 2p, 3p, \cdots, (p^{n-1}p)$ 是能被 p 整除的，因此其中不能被 p 整除的数共有 p^n-p^{n-1} 个。于是有：

定理：设 p 是一个素数，则

$$\varphi(p^n)=p^n(1-\frac{1}{p})$$

特别的，当 $n=1$ 时，$\varphi(p)=p-1$。

2) 然后，我们设 $(l,m)=1$，来求 $\varphi(lm)$ 的计算公式。为此，我们以 $[k]_{lm}$ 映为 $([k]_l,[k]_m)$ 来定义对应：

$$\rho : Z'_{lm} \to Z'_l \times Z'_m$$

不难证明，这一对应是与同余类代表的选取无关的，因此，ρ 是一个映射。同样也不难证明，ρ 既是单射又是满射，即是双射。于是 Z'_{lm} 中元素的个数 $\varphi(lm)$ 等于 $Z'_l \times Z'_m$ 中元素的个数，即 Z'_l 中的元素个数 $\varphi(l)$ 与 Z'_m 中的元素个数 $\varphi(m)$ 的乘积，这就有：

定理：若 $(l,m)=1$，则 $\varphi(lm)=\varphi(l)\cdot\varphi(m)$

待加深理解：注意 $(l,m)=1$，即 l,m 是互素的。然后呢?

举个例子：$Z'_{15}=\{\overline{1},\overline{2},\overline{4},\overline{7},\overline{8},\overline{11},\overline{13},\overline{14}\}$ ，即 $\varphi(15)=8$

且 $15=3\times5$，$Z'_3=\{\overline{1},\overline{2}\},Z'_5=\{\overline{1},\overline{2},\overline{3},\overline{4}\}$，

所以 $\varphi(3)=2,\varphi(5)=4$，即 $\varphi(8)=\varphi(3)\cdot\varphi(5)=8$

综上两点，有如下定理：

定理：对于大于 1 的自然数 n，有：

$$\varphi(n)=\varphi(p_1^{v_1})\cdots\varphi(p_k^{v_k})=n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k})$$

其中 $p_1,p_2,\cdots,p_k$ 是 n 的各个素因数。

举个例子：$Z'_{15}=\{\overline{1},\overline{2},\overline{4},\overline{7},\overline{8},\overline{11},\overline{13},\overline{14}\}$ ，即 $\varphi(15)=8$

且 $15=3^1\times5^1$，所以 $\varphi(15)=\varphi(3^1)\varphi(5^1)=15(1-\frac{1}{3})(1-\frac{1}{5})=15\cdot\frac{2}{3}\cdot\frac{4}{5}=8$

2 群论基础

2.1 群的定义

首先给出下面两个例子：

例 1：给出集合 $A=\{1,-1\}$，并考虑其中元的通常乘法运算，不难看出集合 A 具有如下性质：

- A 的元在乘法下是封闭的，即对任意 $a,b\in A,a\cdot b\in A$
- 该乘法满足结合律，即对任意 $a,b,c\in A$，有 $a\cdot(b\cdot c)=(a\cdot b)\cdot c\in A$
- 有数 1，它对任意 $a\in A$，有 $1\cdot a=a\cdot1=a$
- 由 $1\cdot1=1,(-1)\cdot(-1)=1$，可知对于任意 $a\in A$，存在 $b\in A$，使得 $a\cdot b=b\cdot a=1$

例 2：给出整数集合 Z，并考虑其中元的通常加法运算，同样也有：

- Z 的元在加法下是封闭的，即对任意 $a,b\in Z,a+b\in Z$
- 该加法满足结合律，即对任意 $a,b,c\in Z$，有 $a+(b+c)=(a+b)+c\in Z$
- 有数 0，它对任意 $a\in Z$，有 $0+a=a+0=a$
- 对于任意 $a\in Z$，存在 $-a\in Z$，使得 $a+(-a)=(-a)+a=0$

尽管这两个例子中的集合不同，而且所考虑的运算也不同，但是它们具有共性：一个集合，一种封闭的运算，还有同样的一些运算性质。于是人们就从这些具体的原型中抽象出它们的共性，从而提出**抽象群**的概念，然后对抽象群进行研究。

理解：群论也是从变化中抽取出来的不变性（共性）。在其他领域中，有类似的思考过程。比如在线性空间中，不管坐标基如何变化，向量的”长度“不变；在欧式空间和闵氏空间中，两点间的”距离“不随坐标的变化而变化（虽然欧式空间和闵氏空间对于距离的定义不同）；比如拓扑学，也是研究在形状不断变化下，物体的拓扑结构具有什么样的不变形。

群的定义：在非空集合 $G=\{a,b,\cdots,\}$ 中规定元素间的一种运算，称为“乘法”，记作“$\cdot$”（在不会混淆时可以省略去 $\cdot$）。如果 G 对“$\cdot$”满足下列 4 条公理，则称 G 是一个群，记作 $(G,\cdot)$，或简单的用 G 来表示：

1. **封闭性：若 $a,b\in G$，则 $a\cdot b\in G$；**
2. **结合律：若 $a,b,c\in G$，则 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$**
3. **单位元：对任意 $a\in G$，存在 $e\in G$，满足 $e\cdot a=a\cdot e=a$，称 e 为 G 的单位元**
4. **逆元：对任意 $a\in G$，都有一个逆元，记作 a^{-1}，满足 $a^{-1}\cdot a=a\cdot a^{-1}=e$**

于是，$A=\{1,-1\}$ 在通常乘法下成群；Z 在通常加法下成群；集合 A 的双射全体，在映射的结合运算下成群，即 A 的变换群。

若对任意 $a,b\in G$，有 $ab=ba$，则称 G 为**可换群**；对于可换群常用”$+$“代替”$\cdot$“，且把此时的单位元称为**零元**，逆元称为**负元**。如果群 G 仅含 n 个元素，则称它为 n **阶群**，记作 $|G|=n$，这种群是**有限群**，否则是**无限群**。

对于上一节定义的 Z_n，可以如下地定义它的元素的乘法：$\overline{a}\cdot\overline{b}=\overline{ab}$，但是一般来说，$Z_n$ 不是群，因为 $\overline{n}$ 没有逆元；不难证明，$\overline{k}$ 有逆元的充要条件是 $(k,n)=1$，因此 Z_n' 是群，即**模 n 同余类乘群**，它是可交换群，且 $|Z_n'|=\varphi(n)$。

理解：对于 $Z_{15}=\{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6},\overline{7},\overline{8},\overline{9},\overline{10},\overline{11},\overline{12},\overline{13},\overline{14},\overline{15}\}$，根据乘法的定义：$\overline{a}\cdot\overline{b}=\overline{ab}$ 可知，它的单位元是 $\overline{1}$，并且有：

$$\overline{2}\cdot\overline{8}=\overline{16}\xrightarrow{\text{更换同余类}\overline{16}\text{的代表}}\overline{1}$$

可知，$\overline{2},\overline{8}$ 互为逆元。但是对于 $\overline{15}$，它和任意元素的乘法都是：

$$\overline{15}\cdot\overline{x}=\overline{15x}\xrightarrow{\text{更换同余类的代表}}\overline{15}$$

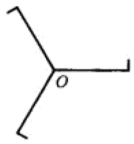
即 $\overline{15}$ 没有逆元。也就是说对于 Z_n，它的 $\overline{n}$ 没有逆元，因此 Z_n 不是群。

同理，对于 Z_{15}，可知 $\overline{3},\overline{5},\overline{6},\overline{9},\overline{10},\overline{12}$ 也都没有逆元，印证了 $\overline{k}$ 有逆元的充要条件是 $(k,n)=1$。

但是，基于上述逻辑容易证明，Z_n' 是群。

2.2 群与对称性

举个旋转的例子来描述群的对称性。给定下图，



我们用绕 O 点逆时针转动来描述该图形所具有的对称性：转动 0° 或 360° 记为 g_1，转动 120° 记作 g_2，转动 240° 记作 g_3；对于 $g_i, g_i \in G = \{g_1, g_2, g_3\}$，定义 $g_j \cdot g_i$ 表示先进行 g_i 再进行 g_j，于是 G 是群。

给出对称群的乘法运算如下：

$$\begin{cases} g_1 \cdot g_1 = g_1, & g_1 \cdot g_2 = g_2, & g_1 \cdot g_3 = g_3 \\ g_2 \cdot g_1 = g_2, & g_2 \cdot g_2 = g_3, & g_2 \cdot g_3 = g_1 \\ g_3 \cdot g_1 = g_3, & g_3 \cdot g_2 = g_1, & g_3 \cdot g_3 = g_2 \end{cases}$$

于是得到 G 的乘法表如下，表中第 i 行 j 列的元素是 $g_j \cdot g_i$：

Table 1: standard table

	g_1	g_2	g_3
g_1	g_1	g_2	g_3
g_2	g_2	g_3	g_1
g_3	g_3	g_1	g_2

从表中可以得到一个规律：表中的每一行和每一列都是这三个群元的一个排列。

重新排列定理：设 $g \in G = \{g_1, g_2, \cdots, g_n\}$，则当 i 取遍 $, 2, \cdots, n$，gg_i 或 g_ig 就取遍 G。

2.3 对称群

类似于 S_2, S_3, S_4, S_5，我们把 S_n 定义成 $1, 2, \cdots, n$ 这 n 个数字的置换的全体。接下来定义元素的乘法，使 S_n 成群。为简明起见，以 S_3 为例，对于

$$g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad g_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

有

$$g_2 \cdot g_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

即

$$1 \xrightarrow{g_5} 2 \xrightarrow{g_2} 3$$
$$2 \xrightarrow{g_5} 3 \xrightarrow{g_2} 2$$
$$3 \xrightarrow{g_5} 1 \xrightarrow{g_2} 1$$

所以

$$g_2 \cdot g_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = g_3$$

不难证明 S_3 在置换的乘法下是群。同样 n 个数字 $1, 2, \cdots, n$ 的全部置换 S_n，在上述乘法下构成 $n!$ 的**对称群** S_n。

2.4 子群 (subgroup)

集合有子集合，相应的，群也有子群的概念。

定义：群 G 的非空子集合 H 称为 G 的一个子群，记作 $H \trianglelefteq G$，或 $G \trianglerighteq H$（原书符号无法打出，类似这样），如果在 G 所定义的乘法运算下，H 本身构成构成一个群。

显然，$\{e\}$ 和 G 本身都是 G 的子群，它们是 G 的**平凡子群**。G 的其它子群则是 G 的**真子群**。

例如：对于前文给出的 S_3：

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$
$$= \{g_1, g_2, g_3, g_4, g_5, g_6\}$$

$H_1 = \{g_1, g_2\}$ 是一个真子群，$H_2 = \{g_1, g_5, g_6\}$ 也是一个真子群。

设 H 是 G 的一个子群，不难证明 H 的单位元就是 G 的单位元 e，而且任意 $a \in H$ 在 H 中的逆元就是 a 在 G 中的逆元 a^{-1}。另外，若要验证 G 的子集 H 对 G 的乘法运算是否成群，就需要判断此时 H 能否满足群的 4 条公理。不过 G 满足结合律，所以它的子集 H 也满足结合律。因此，只需要验证公理 (1)(3)(4)(封闭性、单位元、逆元)。

子群的判断定理：设 $H \subseteq G$，H 是 G 的子群的充要条件是对任意 $a, b \in H$，有 $ab^{-1} \in H$

理解：H 若想成为 G 的子群，需要满足的条件，是对于任意 $a, b \in H$，有 $ab^{-1} \in H$，即 a “乘法运算” b 的逆得到的元，仍然在 H 中。

子群的概念是重要的，伽罗瓦正式成功地揭示了每一个 n 次多项式都有一个与 S_n 有关的子群——**该方程的伽罗瓦群**相关联，从而把方程是否根式可解归结为该子群的性质——可解性的研究。在这个意义上，该子群是该方程的 “遗传密码”。

2.5 陪集 (cosets)

现在我们用 G 的真子群 H 来给出 G 的一个**分类**。由 $H \subset G$，可知存在 $a_2 \in G - H$（G 和 H 的差集），于是构造：

$$a_2H = \{a_2h | h \in H\}$$

容易证明，$H \cap a_2H = \varnothing$。如果存在 $a_3 \in G$，且 $a_3 \notin H \cup a_2H$，则同样再构造 a_3H，也有 $a_3H \cap (H \cup a_2H) = \varnothing$。类似地，可得到 $a_4H, a_5H, \cdots$，于是当群 G 是有限群时，就有：

$$G = H \cup a_2H \cup a_3H \cup \cdots a_lH$$

我们把 G 的具有 aH 形式的子集，称为 G 的关于子群 H 的由元素 a 给出的**左陪集**。令 $a_1 = e$，由 $H = eH = a_1H$ 可知，H 也是 G 的一个左陪集。于是上式 $G = H \cup a_2H \cup a_3H \cup \cdots a_lH$ 称为 G 的一个**左陪集分解**。若 $|G| = n, |H| = m$，并且把左陪集的个数，称为 H 在 G 中的**指数**，记为 $(G : H) = l$，于是考虑到**每一个左陪集中元素的个数都是** m，即有：

拉格朗日定理：设 H 是有限群 G 的子群，则 $|G| = (G : H) \cdot |H|$

由上可知，子群 H 的阶 m 是群 G 的阶 n 的一个因子。例如 $|S_3| = 6$，所以如果它有子群的话，它只可能有 2 阶，3 阶的真子群，而不可能有 4 阶，5 阶的真子群。

类似的，我们也有**右陪集**的概念，这指的是具有：

$$Ha = \{ha | h \in H\}$$

形式的集合。

关于陪集的定义：设 $(H,\cdot)$ 是群 $(G,\cdot)$ 的一个子集，$a\in G$，则集合 $aH(Ha)$ 称为由 a 所确定的 H 在 G 中的左陪集（右陪集），简称为 H 关于 a 的左陪集（右陪集），记为 $aH(Ha)$。元素 a 称为陪集 $aH(Ha)$ 的代表元素。

（理解，这里的陪集还是属于“子集”的概念，没有要求是“子群”，虽然 H 是 G 的子群，但是 aH 未必要求成群）

关于陪集的定理：设 H 是 G 的子群，对于任意 $a,b\in G$，有：

(1) $aH=bH$ 或者 $aH\cap bH=\varnothing$

(2) $Ha=Hb$ 或者 $Ha\cap Hb=\varnothing$

(来源于：https://www.voicenews.cn/21660.html)

对 a 来说的左陪集 aH，其实就是 a 在 G 上的一个等价类。

(来源于知乎：https://zhuanlan.zhihu.com/p/23886266)

理解：假如有实数加群 $<R,+>$，和一个整数加群 $<Z,+>$，则后者一定是前者的子群：

$$Z=\{\cdots,-n,\cdots,-2,-1,0,1,2,\cdots,n,\cdots\}$$

我们在实数加群里面随便选取一个 $a=2.5$, 得到 a 确定 G 在 H 上的左陪集是 (即 **2.5 确定的 $\langle R,+\rangle$ 中的整数的左陪集**)。)

$$aH=\{\cdots,2.5-n,\cdots,2.5-2,2.5-1,2.5,2.5+1,2.5+2,\cdots,2.5+n,\cdots\}$$

即

$$aH=\{a+x|x\in Z,a\in R\}$$

(来源于知乎：https://zhuanlan.zhihu.com/p/23886266)

2.6 正规子群与商群

根据 $G=H\cup a_2H\cup a_3H\cup\cdots a_lH$，我们定义**商集合**：

$$G/H=\{H,a_1H,a_2H,\cdots,a_lH\}$$

我们希望在 G/H 中引入乘法运算，即**两个陪集的乘法**，使 G/H 成群（理解：G/H 是“群的群”，因为 G/H 的每个元都是一个子群）。当然，这一乘法应该与 G 的乘法有关联，一个很自然的想法是令：

$$a_iH\cdot a_jH=(a_i\cdot a_j)H$$

不过，若 $h_i, h_j \in H$，则 $a_iH = a_ih_iH, a_jH = a_jh_jH$，即 a_i 与 a_ih_i 都是 a_iH 的代表，a_j 与 a_jh_j 都是 a_jH 的代表，因此如果上式成立，它应该与代表的选择无关，于是必须有：

$$a_iH \cdot a_jH = a_ih_iH \cdot a_jh_jH = a_ih_ia_jh_jH$$

因此应有：

$$(a_ia_j)H = (a_ih_ia_jh_j)H$$

然而，对 G 的任意子群 H 来说，这一条件一般是不能满足的。为此，伽罗瓦引入了**正规子群**这一重要的概念。

正规子群的定义：如果 G 的子群 H，对任意 $a \in G$，满足 $aH = Ha$，即此时不必区分左右陪集，则称 H 为 G 的一个正规子群，记作 $G \rhd H$ 或 $H \lhd G$。

设 $G \rhd H$，由群的乘法定义满足结合律和“重新排列定理”可知，$(a_ih_ia_jh_j)H = (a_ih_ia_j)H = (a_ih_i)Ha_j = (a_i)h_iHa_j = a_iHa_j = a_ia_jH$，从而推出了 $(a_ia_j)H = (a_ih_ia_jh_j)H$。此时利用 G/H 中的这一乘法，不难证明：

定理：设 $G \rhd H$，并按照 $a_iH \cdot a_jH = (a_i \cdot a_j)H$ 定义的元素的乘法，则 G/H 构成群，这个群称为 G 关于正规子群 H 的商群。

例：**可换群 G 的任意子群都是它的正规子群。**

例：若 H 是 G 的指数为 2 的子群，则 $G = H \cup aH = H \cup Ha$，从而有 $aH = Ha$，因此 $G \rhd H$。（理解，**也就是说，如果 H 是 G 的子群，且 H 的指数为 2，则 H 就是 G 的正规子群**）

例：对任意群 G 而言，群 G 本真与 $\{e\}$ 都是 G 的正规子群，称这两个群为 G 的**平凡正规子群**。

例：设 $G \rhd H$，则 $|G/H| = |G|/|H|$。

理解 1：把群 G 当成一个高中，里面的元素就是学生。这个高中有三个年级，每个年级 5 个班，每个班 40 个学生。

下面来谈谈商的本质，其实**商就是把有等价关系的两个元素在新的群中看成同一个，而等价关系的给出，就是由被商掉的那个群决定的**。

回到之前的例子，我现在把一个班级看成一个子群，就取高一一班好了，这里的等价关系就是同一个班级的学生是彼此等价的，显然互反性，传递性，对称性满足，这确实是个等价关系。那么**做商以后得到的集合是什么呢，这个集合就是这个高中班级的集合**，里面有十五个元素：高一一班一直到高三五班。每个元素都是一个集合，里面的元素是这个班级的学生，**这样在这个商关系之下，班级也就是所谓的陪集**。

现在我们换一下，把年级看成等价关系，被商的子群就是一个年级，就取高一年级，这样得到的商群中的元素就是三个年级。

那么什么是正规子群呢，你可以把正规子群理解为一类特殊的子群，特殊在于，**商掉正规子群得到的商群有自然的群结构**。在上面的例子中，可以非常不严格的把班级和年级看成正规子群，因为它们是特殊的，因为生活中我们常以班级年级作为统一的单位。

在上面的例子中，还有什么可以当子群呢，你不妨把学号为 1 的学生全体当一个子群，此时的等价关系就是相同的学号。这样得到的商群就是 40 个，为什么我要把它当子群，因为在生活中你基本遇不到学校以学号来划分全体学生…在正规子群这里，类比是很不贴切的，我主要想告诉你的是正规子群是极其特殊的子群。

来源于知乎：https://www.zhihu.com/question/63046350/answer/204840915

理解 2：一个群可以看作正规子群和商群“组合”起来的（在特殊情况下就是直积），这样就把复杂的群化解成了简单的群，得到一个群的合成因子。

来源于知乎：https://www.zhihu.com/question/21561484/answer/92539982

理解 3：回忆，**商集合**是由集合 A 的各个类作元素得到的集合，其中的每个类都是一个等价类（即类内元素等价）；而**商群**是由正规子群构成的群。

理解 4：再加深一下对“商”的理解，比如有 6 个桔子，按照每行 2 个排列成 3 行，那么对于每一行的 2 个桔子，可以看成这一行内的桔子是等价的，并且一共有 3 “类”。

理解 5：构造商集的主要目的就是把“多对一”的映射变成“一对一”的映射。在代数里面称为同构。它的基本想法是把原像集里面对应于像集中同一个原素的所有元素看成是一个元素（等价类）。原像集中的两个元素如果具有相同的像，则称这两个元素等价，所有等价的元素放在一起称为等价类，可以看成是一个元素，每一个等价类可以用一个代表元（可在等价类中任意选取，不唯一）来表示。可以证明，这种等价关系给出了原像集的一个划分。这个划分后的集合称为原像集的商集。商集中的元素与像集是一一对应的。这样“多对一”映射就变成了“一对一”映射。这个看法很简单，但是很重要。

来源于：https://www.zhihu.com/question/52574116/answer/131797911

2.7 循环群 (cycle group) 与 n 次本原根

设 G 是一个群，而 e 是它的单位元。我们对于 $0 \in N, n \in N^*$，规定 $a^0 = e, a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n个}$，$a^{-n} = (a^{-1})^n$，则显然有 $a^m \cdot a^n = a^{m+n}, (a^n)^m = a^{nm}, \forall m, n \in \mathbf{Z}$。

因此，我们引入**循环群**的定义：

循环群的定义：对于 n 阶群 G，如果存在 $a \in G$，使得 $G = \{a^0, a, a^2, \cdots, a^{n-1}\}$，则称 G 为由 a 生成的（有限）循环群，记作 $G = \langle a \rangle$，a 是 G 的一个生成元。

对于有限群 G，取任意 $a \in G$，$a \neq e$，构造 $H = \langle a \rangle$，不难证明 H 是 G 的一个循环子群。**如果 G 是素数阶的，则由拉格朗日定理可知，G 不含任何真子群，因此 $G = H = \langle a \rangle$，即 G 是循环群，当然也是可换群，并且它的每一个非单位元都是生成元。**

例：根据前文定义的模 n 同余类集合 Z_n 和同余类乘群 Z_n'，即：

$$\bar{a} = \{a + kn \mid k \in Z\}$$

$$Z_n = \{\bar{1}, \bar{2}, \cdots, \bar{n}\}$$

$$Z_n' = \{\bar{k} \in Z_n | 1 \le k \le n, (k, n) = 1\}$$

有：$Z_3' = \{\bar{1}, \bar{2}\} = \langle\bar{2}\rangle$；同理，$Z_5' = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \langle\bar{2}\rangle$；$Z_7' = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} = \langle\bar{3}\rangle$。

理解：根据前文，我们知道 Z_n 和 Z_n' 上定义的乘法运算是 $\bar{a} \cdot \bar{b} = \overline{ab}$，并且知道 Z_n 不是群（因为它的元 $\bar{n}$ 没有逆元），并且 Z_n' 是群。

因此我们知道，对于群 Z_n' 来说，$\bar{1}$ 是它的单位元。那么对于任意元素 $a \in G, a \neq e$，并且如果 Z_n' 是素数阶的，那么 Z_n' 的每一个非单位元都是生成元。

理解：注意，Z_n' 是素数阶的，不等价于 n 是素数；比如 $Z_5' = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$，5 是素数，但是 $|Z_5'| = 4$ 不是素数，因此不能推导出来 Z_5' 的任意非单位元 $\bar{2}, \bar{3}, \bar{4}$ 都是它的生成元，实际上，$\bar{4}$ 就不是 Z_5' 的生成元（$\bar{4}$ 只能循环生成 $\bar{1}$ 和 $\bar{4}$）。

一般地，当 p 是素数时，可以证明 $Z_p' = \{\bar{1}, \bar{2}, \cdots, \overline{p-1}\}$ 是循环群。

理解：以模 6 加法群 $\langle Z6, +\rangle$ 入手，来认识循环群的特点。

首先，循环群，顾名思义，cycle group 即带有循环的意思。怎么个循环法呢?

我们看 $\langle Z6, +\rangle$ 中的元素 $\{0, 1, 2, 3, 4, 5\}$。取其中的元素 1，不停地对自身进行模 6 加法，即对本身进行幂运算。可得：

$$1^1 = 1$$

$$1^2 = 1 + 1 = 2$$

$$1^3 = 1 + 1 + 1 = 3$$

$$1^4 = 1 + 1 + 1 + 1 = 4$$

$$1^5 = 1 + 1 + 1 + 1 + 1 = 5$$

$$1^6 = 1 + 1 + 1 + 1 + 1 + 1 = 0\text{(模 6 加法意义下)}$$

$$1^7 = 1 + 1 + 1 + 1 + 1 + 1 + 1 = 1\text{(模 6 加法意义下)}$$

$$\cdots$$

如上对 1 不断幂运算，可见两个现象：

1、可以遍历所有的元素，也可以说，我们仅用元素 1 就能生成所有的元素，这就是循环群里的生成元的

概念。

2、幂运算的结果就是 123450123450123450 这样不断的循环，这就是循环群名字由来。

现在，我们继续思考，如果对其它元素进行不断的幂运算呢，会出现什么结果?

经过不断的幂运算，我们发现：元素 0 形成的结果只有 0，结果集合为 {0}；元素 2、4 形成的结果是一样的，结果集合为 {0,2,4}；元素 3 形成的结果集合为 {0,3}；元素 1、5 形成的结果为 {0,1,2,3,4,5}；可见，不同的元素，有的形成的结果不同，有的却相同。我们可以按照他们生成的结果来将他们划分为不同的群体。

对于元素 1、5，他们都能生成所有元素，所以他们两个元素不仅证明了这个群是循环群，还说明他们都是循环群的生成元。他们生成了 {0,1,2,3,4,5} 这个子群（或者说群本身，也叫平凡子群）并且他们都是 6 阶元素，所谓 6 阶，就是 $a^6 = e = 0$(幺元，或称单位元，这个群的单位元是 0)。6 阶也是这个群的阶数。

对于元素 2、4，他们生成了子群 {0,2,4}，他们都是 3 阶元素。

对于元素 3，生成了子群 {0,3}，他是 2 阶元素。

对于元素 0，生成了子群 {0}，他是 1 阶元素。

通过对上面的观察，我们又看出一些规律，就是：

(1). n 阶元素生成的子群中具有 n 个元素

(2). 一个 n 阶群，他具有 p 个不同类型的生成子群，p 是 n 的正因子个数，比如本例中 6 的正因子有 1,2,3,6 共四个。

(3). 一个 n 阶群，他的生成元个数是小于 n 且与 n 互为素数的个数。本例中，小于 6 且与 6 互素的数是 1、5，共两个，所以这个群的生成元就正好 2 个。

（来源：https://blog.csdn.net/u013709443/article/details/82823678）

在之前的章节中，我们研究过 $x^n - 1 = 0$ 的解集合为：

$$1, \zeta = e^{i2\pi/n}, \zeta^2 = e^{i4\pi/n}, \cdots, \zeta^{n-1} = e^{i2\pi(n-1)/n}$$

（在复平面中，这 n 个根 $1, \zeta, \zeta^2, \cdots, \zeta^{n-1}$ 均匀地分布在圆心为点 O，半径为 1 的一个圆上）

即方程 $x^n - 1 = 0$ 的解集合 $G_n = \{1, \zeta, \cdots, \zeta^{n-1}\}$，其中 $\zeta = e^{i2\pi/n}$。对于集合 G_n，以数的乘法为 G 中元素的乘法，显然 G_n 是一个 n 阶循环群，且 ζ 是它的一个生成元。

由其中的元的性质可知，$G_1 = \{1\} = \langle 1 \rangle$，$G_2 = \{1, -1\} = \langle -1 \rangle$，$G_3 = \{1, \omega, \omega^2\} = \langle \omega \rangle = \langle \omega^2 \rangle$，$G_6 = \{1, \zeta, \omega, -1, \omega^2, \zeta^5\} = \langle \zeta \rangle = \langle \zeta^5 \rangle$。由此看见，$x^6 - 1 = 0$ 的 6 个根中，只有 ζ, ζ^5 是 G_6 的生成元，而其它的 4 个根都不是 G_6 的生成元。

因为 $1, -1, \omega, \omega^2$ 满足的 $x^n - 1 = 0$ 型的方程的最低次数分别为：$n = 1, 2, 3$，它们只能分别是 G_1, G_2, G_3 的生成元。因此，我们把 $1, -1, \omega, \omega^2$ 分别称为 1 次，2 次和 3 次**本原根**，即是这些方程所“固有的”根。按照这种说法，ω, ω^5 就是 6 次本原根了。

上面从是否是 G_6 的生成元的角度，把 $x^6 - 1 = 0$ 的根分成了两类：非本原根和本原根。注意到 $\zeta^6 = 1, \zeta^2, \zeta^3, \zeta^4$ 这 4 个非本原根中的指数 6，2，3，4 与 $n = 6$ 都不是互素的，因此不难得出本原根的另一种刻画：ζ^k 是 $x^6 - 1 = 0$ 的一个本原根，当且仅当 $(k, 6) = 1$。

在一般情况下，$x^n-1=0$ 的解 $1,\zeta,\cdots,\zeta^{n-1}$ 中，凡满足 $(k,n)=1$ 的 k 所确定的根 ζ^k 是 G_n 的生成元，是 $x^n-1=0$ 的本原根，称为 n **次本原根**。因此，$x^n-1=0$ 的本原根共有 $\varphi(n)$ 个。当 $n=$ 素数 p 时，$\varphi(p)=p-1$，即 $\zeta,\cdots,\zeta^{p-1}$ 都是本原根。

于是在 $x^6-1=0$ 的 6 个根中：

- 1 次本原根有 $\varphi(1)=1$ 个：1；
- 2 次本原根有 $\varphi(2)=1$ 个：-1；
- 3 次本原根有 $\varphi(3)=2$ 个：ω,ω^2；
- 6 次本原根有 $\varphi(6)=2$ 个：ζ,ζ^5；

因此，$6=\varphi(1)+\varphi(2)+\varphi(3)+\varphi(6)=\sum_{d|6}\varphi(d)$，其中 $\sum$ 是求和符号，下标 $d|6$ 表示，对 $\varphi(d)$ 的求和时，d 取遍 6 的所有因子，即 $d=1,2,3,6$。而在一般情况下，有：

$$\sum_{d|n}\varphi(d)=n$$

2.8 单群

单群的定义：如果群 G 除了 G 本身和 $\{e\}$ 这两个平凡的正规子群外，不含任何其他的正规子群，则称 G 为（简）单群。

素数阶群必是可换群，又因为它没有任何真子群，所以它又是可换单群；反过来，设 G 是 n 阶可换单群，因此 G 就没有任何真子群，任取 $a\in G$，且 $a\neq e$，构造 $\langle a\rangle$，那么 $\langle a\rangle=G$，于是 $G=\{a^0=e,a,a^2,\cdots,a^{n-1}\}$；若 n 是合数，则从 $n=l\cdot m,1<l<n,1<m<n$ 可推知 $\langle a^l\rangle$ 是 G 的一个真子群，这就矛盾了，因此 n 比是素数。所以**有限可换单群**一定是素数阶群。

2.9 群的同态映射与同构映射

给定两个群 $(G,\cdot)$ 和 $(G',\times)$，要把这两个群联系起来的话，需要讨论 G 到 G' 的映射。但是这时的 G 和 G' 除了是集合外，还是群，所以所考虑的映射还要与它们的乘法运算联系起来。

同态映射的定义：映射 $f:(G,\cdot)\to(G',\times)$ 称为一个同态映射，如果对任意 $a,b\in G$，都有：

$$f(a\cdot b)=f(a)\times f(b)$$

即 a 和 b 的乘积 $a\cdot b$（按照 G 中的 $\cdot$ 进行），对应于它们在 G' 中的像 $f(a)$ 和 $f(b)$ 的乘积 $f(a)\times f(b)$（按照 G' 中的 $\times$ 进行）。

这一条件也可以简单说为 “f **保持群的运算**”。在上式中，令 $a=e$，则有：$f(b)=f(e)\times f(b)$，由此可推知 $f(e)$ 是 G' 的单位元 e'。因此 f 将 “单位元映为单位元”。再令 $b=a^{-1}$，有 $f(e)=f(a)\times f(a^{-1})$，由此可推知 $f(a^{-1})=(f(a)^{-1})$，即 f 将 “逆元映为逆元”。在不至于混淆的情况下，我们就省略 “$\cdot$ $\times$” 这些符号。

理解：f 是 G 到 G' 的映射，也就是说给定元 $a\in G, b\in G$，有 $f(a)\in G', f(b)\in G'$；并且 $a\cdot b\in G, f(a\cdot b)\in G', f(a)\times f(b)\in G'$。

同构映射的定义：映射 $f:G\to G'$ 如果是同态映射，又是双射，则称为同构映射。此时称 G 和 G' 同构，记作 $G\approx G'$。

$$f(a\cdot b)=f(a)\times f(b)$$

很明显，两个同构的群，在抽象意义上来看是完全一样的，两者只有符号上的差别。

前文所讨论的对称性群 $G_3=\{g_1,g_2,g_3\}$（旋转 $0°,120°,240°$）与 $x^3-1=0$ 的三个根构成的循环群 $\{1,\omega,\omega^2\}$ 显然是同构的：$0°,120°,240°$ 的转动分别对应 $1,\omega,\omega^2$。事实上，**任意 n 阶循环群都是同构的**。

理解同态映射和同构映射：

你可以定义一个二进制自然数到十进制自然数的映射，叫做 “把一个数映到它自己”；然后这个映射是个（半环）同构，它保持加法保持乘法——意思是两个数在二进制下怎么加，在十进制下还是怎么加，加出来的结果还是能相互对应；还是个双射。然后你就相信了，二进制自然数和十进制自然数其实是同一个东西，这个世界上只有一种自然数，进制的不同并不会改变自然数半环本身的加法乘法结构以及序结构等等；但是一个小学生可能很难理解，他会觉得，二进制和十进制看起来如此不同，怎么能把他们看成同一个对象？

所以同构起到的就是这么个作用，它抓取一个数学对象最本质的信息（比如上面例子里的加法和乘法结构），而忽略其他没那么重要的信息（比如进制），然后把具有相同 “本质信息” 的对象视为一体。“同构” 或者更一般地，“取等价类” 这种思想观念其实在你学抽象代数之前早就有了。比如 “三个苹果” 和 “三个香蕉” 在只考虑数目的情况下 “同构”，他们帮助你给出了 3 这个抽象的数学概念。再比如两个全等的三角形可以被视为一体，但是他们被摆放的位置明明不同，但是你知道，在很多情况下，位置的信息并不重要，重要的是三角形本身的几何信息，比如边长、内角等等。

至于同态，那比同构的含义更广一些。它是在两个本质不一定相同的数学对象之间建立联系；比如自然数半环包含进实数域的那个包含映射，就是一个（单的）半环同态，它告诉你自然数可以视为实数这个更大的结构的一部分——而不是说自然数和实数是一回事。所以同态相当于是两个数学对象之间的 “纽带”。

来源于：https://www.zhihu.com/question/293890350/answer/487914082

如果群 G 和群 H 之间若建立了同构映射，那么不仅群 G 中的每个元素在群 G' 中都有一一对应（元素 $g_i \in G$ 对应 $f(g_i) \in G'$），而且对于群 G 中的两个元素 g_1, g_2，在群运算 $\cdot$ 下得到的元素 $g_1 \cdot g_2 \in G$ 也在这个映射下保持一一对应（对应 $f(g_1 \cdot g_2) = f(g_1) \times f(g_2) \in G'$）

像和核的定义：设 $f : G \to G'$ 是一个同态映射，定义：

$$\mathbf{Im}f = \{f(a)|a \in G\}, \quad \mathbf{Ker}f = \{a \in G|f(a) = e'\}$$

$\mathbf{Im}f$ 称为同态 f 的像 (Image)，$\mathbf{Ker}f$ 称为同态 f 的核 (Kernel)。

$\mathbf{Im}f$ 显然就是 f 的值域，即 $\mathbf{Im}f = f(G)$，当然 $\mathbf{Im}f \subset G'$，且 f 是满射的充要条件是 $\mathbf{Im}f = G'$；

$\mathbf{Ker}f$ 是 e' 的原像的全体，即 $\mathbf{Im}f$ 表示的是 G 中的所有像是 e' 的那些元所构成的集合，当然 $\mathbf{Ker}f \subset G$，且 f 是单射的充要条件是 $\mathbf{Ker}f = \{e\}$。

还可以证明 $\mathbf{Im}f \trianglelefteq G'$，以及 $G \triangleright \mathbf{Ker}f$，也就是说，$\mathbf{Im}f$ 是 G' 的子群，$\mathbf{Ker}f$ 是 G 的正规子群。

由 G 和它的正规子群 $\mathrm{Ker}f$，我们有商群 $G/\mathrm{Ker}f$，它的元是 $a\mathrm{Ker}f$ 形式的陪集。因此由 $a\mathrm{Ker}f$ 映射为 $f(a)$，可定义：$g : G/\mathrm{Ker}f \to \mathrm{Im}f$，不难证明这个 g 是一个同构映射。因此有：

同态基本定理：如果 $f : G \to G'$ 是一个同态映射，则：

$$G/\mathrm{Ker}f \approx \mathrm{Im}f$$

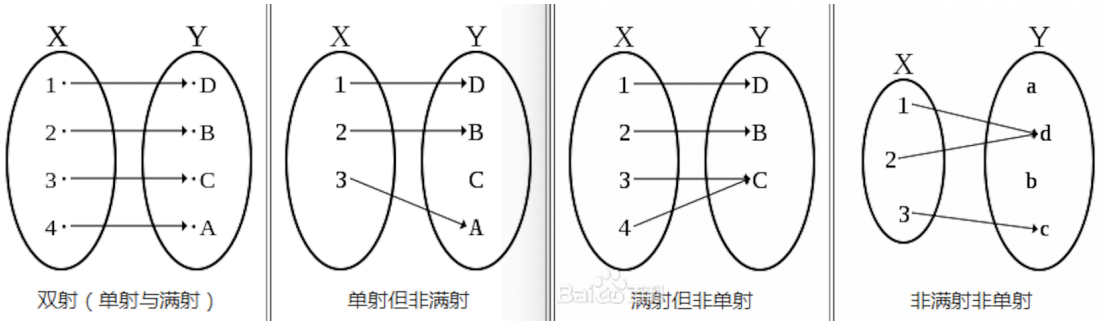
如果 f 还是一个满射，那么 $\mathbf{Im}f = G'$，从而：

$$G/\mathrm{Ker}f \approx G'$$

有了群的概念后，我们就能更详细地描述以前提到过的数集合 **N, Z, Q, R, C**。

加深对同态基本定理的理解：

同态不是同构的原因主要体现在：相应的映射不是双射，即不是单射或不是满射。当然也可能既不是单射也不是满射：



(1) 当映射不是满射时，我们只需考虑映射的像集，这个像集是原来代数结构的子结构。比如，对群的情形，同态的像集是一个子群。用子结构替换原来的代数结构，原来的映射变成了满射!

(2) 当映射不是单射时，不同的元素被映到相同的元素。这时，可以把映到同一个元素的元素看成是一样的，或者说它们是等价的。这样我们将得到一个等价关系，做商集。在这个商集上诱导的映射就是一个单射了。这就是同态基本定理的主要想法。在这个商集上可以定义类似的代数结构，使得前面提到的映射是同态。从这个商代数到上述提到的子代数诱导的映射就是一个同构映射了。

来源于：https://www.zhihu.com/question/301173742/answer/526247988

3 数与代数系

3.1 自然数集 N 作为可换半群及其可数性

自然数集 $\mathbf{N}=\{0,1,2,\cdots\}$ 对加法运算满足：(1) 封闭性 (2) 结合律（不满足逆元条件）。数学家把满足条件 (1)(2) 的代数系称为**半群**。在 $\mathbf{N}$ 这个半群中，它还有加法的零元，以及加法运算是可交换的，因此 $(\mathbf{N},+)$ 是一个**有零元的可换半群**。

虽然 $\mathbf{N}$ 有无限多个元素，但是这个无限有一个特性：任意一个 $n\in\mathbf{N}$，只要 0，1，2，……这样数下去，总可以数到，所以我们称 $\mathbf{N}$ 是（无限）**可数**的。

3.2 整数集合 Z 与整环

对于自然数集 $\mathbf{N}$ 来说，$3\in\mathbf{N}$，但是它的加法负元 $-3\notin\mathbf{N}$，因此 $\mathbf{N}$ 还不是群，所以必须扩展 $\mathbf{N}$，让它把负整数添加进去，这就有了整数集合 $\mathbf{Z}=\{0,\pm1,\pm2,\cdots\}$，此时 $(\mathbf{Z},+)$ 是一个可换群。

$\mathbf{Z}$ 中还有通常的乘法运算 “$\cdot$”，容易知道 $(\mathbf{Z},\cdot)$ **是一个具有单位元 1 的可换半群**。如果我们在 $\mathbf{Z}$ 中同时考虑 “$+$” 和 “$\cdot$” 这两种运算，那么 $(\mathbf{Z},+,\cdot)$ 还分别满足左分配律 $a\cdot(b+c)=a\cdot b+a\cdot c$ 和右分配律 $(b+c)\cdot a=b\cdot a+c\cdot a$，因此我们引入**环**的概念。

环的定义：集合 K 有 “$+$” 和 “$\cdot$” 运算，并满足：(1)$(K,+)$ 构成可换群；(2)$(K,\cdot)$ 构成半群；

(3)$(K,+,\cdot)$ 有左、右分配率，则称 $(K,+,\cdot)$ 构成一个环；如果 $(K,\cdot)$ 还满足 (4) 交换律，则称 $(K,+,\cdot)$ 是一个可换环。

于是，$(K,+,\cdot)$ 是一个有乘法单位元 1 的可转环。同时 $(K,\cdot)$ 还满足**消去律**，即对任意 $c\neq 0$，由 $c\cdot a=c\cdot b$，可推出 $a=b$，这是一个很重要的性质，为此我们引入：

整环的定义：有乘法单位元的可换环，若满足消去律，则称为整环。

4 域与有理数域 Q

对于整环 $(K,+,\cdot)$ 而言，$(K,\cdot)$ 一定不是群。这是因为 K 中的加法零元，是一定没有乘法的逆元的。这一点可以用反证法来证明。设 0 的乘法逆元为 a，于是 $0\cdot a=1$（这里 1 是乘法元，因此我们假定了 K 中至少存在 0，1 两个元素），然而由分配率可知，$0\cdot a=(1-1)\cdot a=a-a=0$，即 $0=1$，这就矛盾了，因此我们只能要求 $K^*=K-\{0\}$ 成群，从而有：

域的定义：如果整环 $(F,+,\cdot)$ 至少有 2 个元，且对 F 中的每一个非零元素都有逆元，则称 F 是一个域。

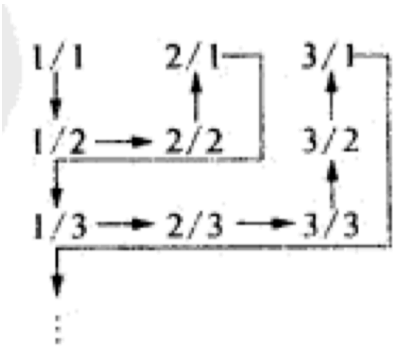
由此可见，域对加法是加群，而 $F^*=F-\{0\}$ 对乘法是可换群，且对乘法和加法有分配率。在域 F 中，按 $a\div b=a\cdot b^{-1}$ $a,b\in F,b\neq 0$，可引入除法。这样，域是一种具有良好运算的数学对象。在其中，**域运算**，即四则运算（加减乘除）能**如常地进行**。在方程的根式求解中，我们对数字要进行域运算及开放运算，对域运算而言，由数字构成的域——**数域**就十分重要了。设 $a\in F$，则一般来说 $\sqrt[n]{a},n\in N^*$ 不一定属于 F，所以对开方运算来说，**扩域**就十分重要了。

例：当 $n=$ 素数 p 时，$\mathbf{Z}_p=\{\overline{1},\overline{2},\cdots,\overline{p}\}$，定义 $\overline{a}+\overline{b}=\overline{a+b},\overline{a}\cdot\overline{b}=\overline{a\cdot b}$，而：

$$\mathbf{Z}_p-\{\overline{0}\}=\mathbf{Z}_p'=\{\overline{1},\overline{2},\cdots,\overline{p-1}\}$$

可知 $\mathbf{Z}_p$ 构成域，称为**素域**。

不难知道，作为整数 $\mathbf{Z}$ 的扩张，有理数集合 $(\mathbf{Q},+,\cdot)$ 是一个数域，称为**有理数域**。而且 $\mathbf{Q}$ 也是可数的，下图给出了正有理数 $\mathbf{Q}^+$ 的一种数数的方法（跳过重复出现的数字），那么负有理数 $\mathbf{Q}^-$ 也是可数的，再由 $\mathbf{Q}=\{0\}\cup\mathbf{Q}^+\cup\mathbf{Q}^-$ 可知 $\mathbf{Q}$ 也是可数的。



4.1 实数域 R 的不可数性

对于实数集合 $\mathbf{R}$ 及其中的运算“+”和“·”而言，可以验证 $\mathbf{R}$ 构成**实数域**。$\mathbf{R}$ 中除了有理数，还包括无理数，这使得 $\mathbf{R}$ 不可数了。下面用反证法证明：

证明：$\mathbf{R}$ 是不可数的。

思路：通过满足 $0 < r < 1$ 的全体实数 $\bar{r}$ 是不可数的，从而证明 $\mathbf{R}$ 是不可数的。

假定 $\bar{r}$ 是可数的，因而存在双射 $f : N \to \bar{r}$，有：

$$
\begin{aligned}
f(0) &= 0.a_{00}a_{01}a_{02}\cdots, \\
f(1) &= 0.a_{10}a_{11}a_{12}\cdots, \\
f(2) &= 0.a_{20}a_{21}a_{22}\cdots, \\
&\cdots
\end{aligned}
$$

现构造：

$$
b = 0.b_0b_1b_2\cdots, \quad \text{其中} b_n = \begin{cases} a_{nn} - 1, & \text{若} a_{nn} \neq 0, \\ 1, & \text{若} a_{nn} = 0, \end{cases} \qquad n = 0, 1, 2, \cdots
$$

即 b 的第 0 位 $b_0 = a_{00}$，第 1 位 $b_1 = a_{11}$，第 2 位 $b_2 = a_{22}$，……

因为 $0 < b < 1$，由此可推出 $b \in \bar{r}$，但 $b_n \neq a_{nn}, n = 0, 1, 2, \cdots$，因此 b 不会出现在上述排列之中，这就与 f 是双射矛盾了，所以 $\mathbf{R}$ 是不可数的。

4.2 复数域 C 与子域

不难验证复数集合 $\mathbf{C}$，对通常的“+”和“·”运算而言，满足域的定义，因此有**复数域**。作为集合，显然有 $\mathbf{C} \supset \mathbf{R} \supset \mathbf{Q}$，那么它们之间是否有进一层的关系呢？为此我们引入

子域和扩域的定义：若域 $E \supseteq F, F \neq \varnothing$，$F$ 对于 E 中的“+”和“·”构成一个域，则称 F 为 E 的一个子域，而 E 为 F 的一个扩域，记作 E/F。

从域的定义以及子群的判断定理（设 $H \subseteq G$，H 是 G 的子群的充要条件是对任意 $a, b \in H$，有 $ab^{-1} \in H$），有：

子域的判断定理：设 $F \subseteq E$，E 是域，而 $F \neq \varnothing$，则 F 是 E 的子域的充要条件为：

(1) $\forall a, b \in F$，有 $b - a \in F$；

(2) $\forall a, b \in F$，$b \neq 0$，有 $ab^{-1} \in F$；

换言之，F 在“+”，“-”，“×”，“÷”运算下是封闭的。于是不难验证 $\mathbf{C}/\mathbf{R}$，$\mathbf{C}/\mathbf{Q}$，$\mathbf{R}/\mathbf{Q}$ 等。我们把 $\mathbf{C}$ 以及它的任意子域都称为**数域**。

数域的定义：数域 P 是复数域 $\mathbf{C}$ 的子集，它至少包含数 1 与 -1，并且它对复数的加法、乘法以及非零数的取逆运算封闭。

来源：https://zhuanlan.zhihu.com/p/36202766

数域的常见例子：

全体有理数构成数域，称为有理数域，记为 $\mathbf{Q}$；全体实数构成数域，称为实数域，记为 $\mathbf{R}$；**有理数域是最小的数域；复数域是最大的数域；在实数域与复数域之间没有其它的数域**（因为复数域作为实数域上的向量空间是 2 维的）。

设 F 是一个数域，因为 $1 \in F$，由此能推出 $1 - 1 = 0, 1 + 1 = 2, \cdots$ 都属于 F，即 $\mathbf{N} \subset F$，再由加法运算的负元都属于 F，能推出 $Z \subset F$。最后由除法运算的封闭性（0 不做除数）能推出 $Q \subseteq F$，即：

定理：对任意数域 F 都有 F/Q，即 Q 是任意数域的子域。

理解：有理数域 $\mathbf{Q}$ 是任意数域的子域 $\Leftrightarrow$ 有理数域 $\mathbf{Q}$ 是最小的数域；

定理：设 E 为一个域，则 E 的所有子域的交集 F 是 E 的一个子域。

除了上面的 $\mathbf{C}$，$\mathbf{R}$，$\mathbf{Q}$ 外，还有许多其他的数域。例如，由 $\mathbf{Q}$ 可构成：

$$\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in Q\}$$

对于任意 $a_i + b_i\sqrt{2} \in Q(\sqrt{2}), i = 1, 2$，有：

$$(a_1 + b_1\sqrt{2}) \pm (a_2 + b_2\sqrt{2}) = (a_1 \pm a_2) + (b_1 \pm b_2)\sqrt{2}$$

$$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})=(a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}$$

$$\frac{1}{a+b\sqrt{2}}=\frac{a}{a^2+2b^2}-\frac{b}{a^2+2b^2}\sqrt{2},\quad (a,b\neq 0)\quad \text{即通常的“分母有理化”}$$

从上可知，$\mathbf{Q}(\sqrt{2})$ 是一个域，称为 **Q 添加** $\sqrt{2}$ 而构成的域。有了域的概念，接下来就能讨论域上的向量空间了。（有理数域 $\mathbf{Q}$ 中只包含有理数，不包含 $\sqrt{2}$，而 $\mathbf{Q}(\sqrt{2})$ 添加了元 $\sqrt{2}$。）

理解群、环、域：

半群：定义了“乘法”一种运算，并且该运算满足 (1) 封闭性；(2) 结合律；

群：定义了“乘法”一种运算，并且该运算满足 (1) 封闭性；(2) 结合律；(3) 单位元；(4) 逆元；?? 群也是一种特殊的环??。

环：定义了“加法”和“乘法”两种运算，其中“加法”运算满足可换群的条件，“乘法”运算满足半群的条件，“乘法”对“加法”满足分配率。

可换环：“乘法”运算还满足交换律的环。

整环：三个条件：(1) 有乘法单位元，(2) 是可换环，(3) 满足消去律；是一种特殊的环。

域：满足逆元的整环，是一种特殊的环。

因此，环是基础，群、域都是特殊的环。

5 域上的向量空间

5.1 向量空间的定义

向量和向量空间的定义：集合 V 称为数域 F 上的向量空间，V 中的元素称为向量，如果有：

(1) 集合 V 中定义了“+”运算，使 $(V,+)$ 构成可换群，此时的零元是**零向量**，记为 0，而 $v\in V$ 的负元记为 $-v$；

(2) 对于 $a\in F, v\in V$ 定义了它们的数乘运算，即 $av\in V$，而对 $v_1,v_2,v\in V, a,b\in F$，有：

$$a(v_1+v_2)=av_1+av_2, (a+b)v=av+bv, (ab)v=a(bv), 1\cdot v=v$$

其中 1 是域 F 的乘法单位元，即数字 1。

据此，不难得出平面中的所有向量构成 $\mathbf{R}$ 上的向量空间 V_2。类似地，域 F 上的一元多项式全体，即

$$F[x]=\{a_nx^n+\cdots+a_1x+a_0=\sum_{i=0}^{n}a_ix^i | a_i\in F, n\in N\}$$

以多项式的加法定义 $F[x]$ 中元素的加法，以数与多项式的乘法定义 $F[x]$ 中元素的数乘，则 $F[x]$ 就是 F 上的一个向量空间。

5.2 向量空间的一些基础理论

我们知道，在 V_2 中还存在着向量 $\mathbf{i}$ 和 $\mathbf{j}$，它们有以下性质：(1) 任意的向量 $v\in V_2$，都可以唯一地表示为 $v=a\mathbf{i}+b\mathbf{j}, a,b\in\mathbf{R}$；(2) 若 $a\mathbf{i}+b\mathbf{j}=\mathbf{0}$，则必有 $a=b=0$。这里前面的一个 $\mathbf{0}$ 是零向量，后面的 0 是 $\mathbf{R}$ 中的数字 0，但一般不会混淆，后文不加区分。在一般情况下，有：

基和维度的定义：设 $v_1,v_2,\cdots,v_s\in V$，称它们是线性无关的，如果 $a_1v_1+a_2v_2+\cdots+a_sv_s=0, a_1,a_2,\cdots,a_s\in F$，能推出 $a_1=a_2=\cdots=a_s=0$，否则则是线性相关的。若 V 中存在 n 个线性无关的向量 $u_1,u_2,\cdots,u_n$，且对任意 $v\in V$，都可表示为 $v=a_1u_1+a_2u_2+\cdots+a_nv_n$，其中 $a_1,a_2,\cdots,a_n\in F$，则称 $\{u_1,u_2,\cdots,u_n\}$ 是 V 在 F 上的一个基，且 V 是 n 维的。

因此，上述 $\mathbf{i}$ 和 $\mathbf{j}$ 是线性无关的，它们是 V_2 的一个基，且 V_2 是 2 维的，而 $F[x]$ 中的 $1,x,x^2,\cdots$ 是线性无关的，且 $F[x]$ 不是有限维的。(?? 为什么 $F[x]$ 不是有限维的??)

5.3 数域作为向量空间

以有理数域 $\mathbf{Q}$ 为例来说明，$\mathbf{Q}$ 作为域，已有元素间的加法和乘法。现在把向量空间定义中的 V 取为 $\mathbf{Q}$，F 也取为 $\mathbf{Q}$，则由 $\mathbf{Q}$ 是域不难看出，此时 $\mathbf{Q}$ 是 $\mathbf{Q}$ 自己身上的向量空间，而且此时 $\mathbf{Q}$ 是 1 维的。类似地，$\mathbf{R}$ 和 $\mathbf{C}$ 都分别是其自身上的向量空间。

如果我们取 $\mathbf{V}=\mathbf{C},\mathbf{F}=\mathbf{R}$，即这时的数乘是用实数去乘，则 $\mathbf{C}$ 也是 $\mathbf{R}$ 上的向量空间，我们把 $c=a+bi,a,b\in\mathbf{R}$，把 $\mathbf{C}$ 看成是 $\mathbf{R}$ 上的向量空间，则 $\mathbf{C}$ 有一个由 $\{1,i\}$ 构成的基，所以 $\mathbf{C}$ 作为 $\mathbf{R}$ 上的向量空间是 2 维的。

同样，上面给出的 $\mathbf{Q}(\sqrt{2})$ 是自身上的 1 维向量空间，而作为 $\mathbf{Q}$ 上的向量空间时，它有基 $\{1,\sqrt{2}\}$，所以是 2 维的；然而，当我们取 $\mathbf{Q}=\mathbf{R},\mathbf{F}=\mathbf{Q}$ 时，则 $\mathbf{R}$ 是 $\mathbf{Q}$ 上的向量空间，不过诸如基和维数之类的问题就不那么简单了。后文再进一步分析讨论。

6 域上的多项式

6.1 一些基本事项

一元多项式 $f(x)=\sum_{i=0}^{n}a_ix^i,a_i\in F,n\in N$ 应是 $F[x]$ 中的元。若最高项系数 $a_n\neq 0,n>0$，则称 $f(n)$ 是 **n 次的**；若 $n=0$，而 $a_0\neq 0$，则 $f(x)=a_0$ 是 **0 次的**，即 F 中的非零元是 0 次多项式；若所有的 a_i 都为 0，则 $f(x)=0$ 是零多项式，它是 F 中的零元，我们不定义它的次数。$f(x)$ 的次数用 $\deg f$ 来表示。

对于 $F[x]$ 中多项式的加法和多项式的数乘，$F[x]$ 是 F 上的一个向量空间，而 $F[x]$ 中还有多项式的乘法，不难得出 $F[x]$ 是一个整环。

6.2 多项式的可约性与艾森斯坦定理

可约的定义：对于 $p(x)\in F[x],\deg\ p\geq 1$，如果不存在分别满足：

$$\deg\ p>\deg\ f\geq 1 \text{ 和 } \deg\ p>\deg\ g\geq 1$$

的 $f(x),g(x)\in F[x]$，使得 $p(x)=f(x)\cdot g(x)$，则称 $p(x)$ 在 $F[x]$ 中（或 F 上）是不可约的，否则是可约的。

利用因式分解，可将可约的多项式分解成一些次数更低的多项式。不过**多项式能否因式分解是与所考虑的域有关的**。例如 $x^2-2=0$ 在 $\mathbf{Q}$ 上是不可约的，但在 $\mathbf{R}$ 上，$x^2-2=(x-\sqrt{2})(x+\sqrt{2})$，又如 x^4-x^2-2 分别作为 $\mathrm{Q}[x],\mathrm{R}[x],\mathrm{C}[x]$ 中的多项式就分别有：$(x^2-2)(x^2+1),(x-\sqrt{2})(x+\sqrt{2})(x^2+1),(x-\sqrt{2})(x+\sqrt{2})(x-i)(x+i)$

为了今后的应用，我们给出艾森斯坦证明过的如下判据：

艾森斯坦不可约判据：设 $f(x)=\sum_{i=1}^{n}a_ix^i\in Z[x]$，即 $a_i\in Z,i=0,1,2,\cdots,n$，若存在一个素数 p，它能整除 a_n 外的所有系数，且 p^2 不能整除 a_0，那么 $f(x)$ 在Q 上是不可约的。

例：$f(x)=2x^5-10x+5$ 在 Q 上是不可约的，因为存在 $p=5$，满足上述条件（$p=5$ 能整除除 $a_n=2$ 之外的所有系数 $a_4=0,a_3=0,a_2=0,a_1=10,a_0=5$，并且 $p^2=25$ 不能整除 $a_0=5$）

例：多项式 $x^n-1=(x-1)(x^{n-1}+\cdots+x+1)=(x-1)f(x)$，因此它在Q上是可约的；当 n 是偶数时，因为 $f(x)=x^{n-1}+x^{n-2}+\cdots+x+1=(x+1)(x^{n-2}+x^{n-4}+\cdots+x^2+1)$，所以 $f(x)$ 仍是可约的；当 n 是奇数时，尽管 $f(x)$ 的根都是复数，但是它可能在 $\mathbf{Q}$ 上仍是可约的。例如，当 $n=9$ 时，$f(x)=x^8+x^7+\cdots+x+1=(x^2+x+1)(x^6+x^3+1)$；但当 $n=p$(素数) 时，$f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ 在 $\mathbf{Q}$ 上不可约。要直接运用艾森斯坦不可约判据来证明此时 $f(x)$ 在 $\mathbf{Q}$ 上不可约是行不通的。为此，我们利用 $f(x)$ 在 $\mathbf{Q}$ 上的不可约性等价于 $f(x+1)$ 在 $\mathbf{Q}$ 上的不可约性这一点，于是由 $x^p-1=(x-1)\cdot f(x)$，即

$$f(x)=\frac{x^p-1}{x-1}$$

$$\begin{aligned}f(x+1)&=\frac{(x+1)^p-1}{(x+1)-1}\\&=\frac{x^p+px^{p-1}+\cdots+px}{x}\\&=x^{p-1}+px^{p-2}+\frac{p(p-1)}{2}x^{p-3}+\cdots+p\end{aligned}$$

其中在 $(x+1)^p$ 展开时用到了牛顿二项式公式。所以存在素数 p 满足艾森斯坦不可约判据条件，即 $f(x+1)$ 在 $\mathbf{Q}$ 上是不可约的，所以 $f(x)$ 在 $\mathbf{Q}$ 上是不可约的。

n 是偶数时候的证明：$x^{n-1}+x^{n-2}+x^{n-3}+x^{n-4}+\cdots+x+1=(x^{n-1}+x^{n-2})+(x^{n-3}+x^{n-4})+\cdots+(x+1)=(x+1)x^{n-2}+(x+1)x^{n-4}+\cdots+(x+1)=(x+1)(x^{n-2}+x^{n-4}+\cdots+x^2+1)$

理解：证明 $f(x)$ 在 $\mathbf{Q}$ 上的不可约性等价于 $f(x+1)$ 在 $\mathbf{Q}$ 上的不可约性。

$f(x)=\sum_{i=1}^n a_ix^i, f(x+1)=\sum_{i=1}^n a_i(x+1)^i=\sum_{i=1}^n b_ix^i$，所以二者的不可约性等价。

6.3 关于三次方程根的一些定理

对于 $f(x)\in F[x], F\subset\mathbf{C}$，若存在 $a\in\mathbf{C}$ 使得 $f(a)=0$，则称 a 是**多项式 $f(x)$ 的一个根，或多项式方程 $f(x)=0$ 的一个根**。为了以后的应用，我们考虑域 F 上的一般三次方程：

$$ax^3+bx^2+cx+d=0, a,b,c,d\in F, a\neq 0$$

给出下面的三个定理：

三次方程根相关的三个定理：

定理 1：设上述三次方程的根为 a_1, a_2, a_3，则 $a_1 + a_2 + a_3 = -\frac{b}{a} \in F$

定理 2：如果 $p + q\sqrt{r}$ 是上述三次方程的一个根，其中 $p, q, r \in F, r > 0$，且 $\sqrt{r} \notin F$，则 $p - q\sqrt{r}$ 也是方程的一个根

定理 3：如果上述三次方程是整系数方程，即 $a, b, c, d \in \mathbf{Z}$，且它有有理根 $p/q, p, q \in \mathbf{Z}$，且 $(p, q) = 1$，那么分子 p 应是 d 的一个因数，而分母应是 a 的一个因数。

三个定理的解读:

定理 1 就是韦达定理的根和系数的关系。

定理 2 可以类比共轭的复数根。正如我们所熟知的，实系数多项式方程，如果有复根 $a+bi, b \neq 0$，则它一定有共轭根 $a-bi$，即互为共轭的复根是成对出现的。例如 $x^3 - 5x^2 + 5x - 1 = (x-1)(x-2-\sqrt{3})(x-2+\sqrt{3})$，根 $x+\sqrt{3}$ 与根 $x-\sqrt{3}$ 是成对出现的。

定理 3 也是熟知的。例如，$12x^3 - 8x^2 - 3x + 2 = 0$，$d = 2, a = 12$，$d$ 的因子为 $\{1, 2\}$, a 的因子为 $\{1, 2, 3, 4, 6, 12\}$, , 所以方程的有理根应为 $\pm 1, \pm 2, \pm 1/2, \pm 1/3, \pm 2/3, \pm 1/4, \pm 1/6, \pm 1/12$，验证后可知 $1/2, -1/2, 2/3$ 是根。

同样，容易验证整系数方程 $8x^3 - 6x^2 - 1 = 0$ 没有有理根。

在群论中，常感兴趣的是如何决定给一个群 G 的子群；在域论中，感兴趣的是给定一个域后，如何去做出它的扩域。

References

[1] 冯承天, 从一元一次方程到伽罗瓦理论.