数与对称

左 康

2011年8月14日，于美茵茨读书会

Contents

1　引言－－传奇天才伽罗华

伽罗华

伽罗华生平

埃瓦里斯特·伽罗华(Évariste Galois, 1811-1832)，法国数学家，与尼尔斯·阿贝尔(Niels Henrik Abel)并称为现代群论的创始人。

从下面摘自维基百科的段落可以看出其传奇般的生平:

(http://zh-classical.wikipedia.org/wiki/%E4%BC%BD%E7%BE%85%E8%8F%AF)

> 埃瓦里斯特·伽罗华，1811年10月25日生于法兰西波格拉莱(Bourg La Reine)。
>
> 十六岁那年，伽罗华报考巴黎理工大学，落榜而归。

十八岁时，他证明了高次方程没有根式解，并将论文送交法国科学院，但审阅人柯西把论文弄丢了。不久其父亲因为在选举中被人恶意中伤而自尽。当年伽罗华再次报考巴黎理工大学，仍然落榜，于是就读于巴黎高等师范学院。

第二年，伽罗华将高次方程没有根式解的论文送给傅利叶审阅。可惜傅利叶病逝，论文再次丢失。

不久，七月革爆发，伽氏因政见不同而撰文抨击校长，被校长勒令退学。七月革命期间伽罗华因支持共和而两次被囚禁，且曾自杀未遂。

1832年3月，伽罗华爱上了一位医生的女儿，并因此和一军官进行决斗，不幸身亡，时年21岁。

其朋友齐瓦利尔(Chevalier)遵照遗嘱将伽罗华的数学论文寄给高斯(Gauss)、雅各比(Jacobi)审阅，皆石沉大海。十多年后，论文流传到了刘维尔(Liouville)手中，刘氏将论文刊登于《纯粹与应用数学杂志》上，伽罗华理论才从此闻名于世。

伽罗华虽然英年早逝，但其所开创的方法，独特而深邃，奠定了现代群论乃至代数学的基础。

那么，究竟是什么使得一个年仅十八岁的少年所开创的方法奠定了现代群论的基础呢?

伽罗瓦理论的关键在于引入**群**的概念，并由此来讨论**方程的可解性**的相关问题。

今天我们便来简单地看一下方程的解与群(对称)之间的关系。

2 数的发展

2.1 集合

集合就是一组元素的全体，比如

{在Mainz居住的华人}

{地球上身高高于 2 米的人}。

集合和其中的元素的从属关系用**属于**来表示，比如

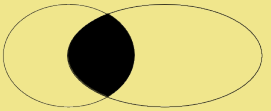
$$\text{姚明} \in \{\text{地球上身高高于 2 米的人}\}。$$

特别地，什么元素都没有的集合称为**空集**($\emptyset$)，比如

$$\{\text{地球上身高高于3米的人}\} = \emptyset。$$

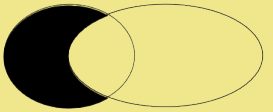
我们可以对集合进行运算: 交、并、差、对称差。

交

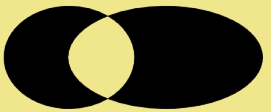


并

差



对称差



我们也可以考虑集合的大小。正是对集合大小的讨论导致了现代集合论的产生。

1873，在康托(Cantor)和戴德金(Dedekind)(高斯(Gauss)的学生)关于有理数集合大小的通信讨论中诞生了现代集合论。

对有限集合可以用其中元素的个数来表示该集合的大小，这个个数就是通常所用到的自然数。

2.2 自然数 $\mathbb{N}$ ——可以进行运算的集合

$$\begin{aligned}\mathbb{N} &:= \{\ |\ ,\ ||\ ,\ |||\ ,\ ||||\ ,\ \cdots\} \\ &\quad\ \downarrow \quad\ \downarrow \quad\ \downarrow \quad\ \downarrow \\ &= \{\ 1,\ 2,\ 3,\ 4,\ \cdots\}\end{aligned}$$

自然数的发现是从计数开始的，距今已经有两万年的历史。然而 0 的发现则是很久以后的事了。在罗马数字里面就没有专门的 0 这个符号。

在中学的时候我们就学过了:

加法 : $m+n$

$$\text{结合律} : (l+m)+n = l+(m+n), \qquad (3+5)+2 = 10 = 3+(5+2) \tag{1}$$

$$\text{零} : 0+m = m, \qquad 0+3 = 3 \tag{2}$$

$$\text{交换律} : m+n = n+m, \qquad 3+5 = 8 = 5+3 \tag{3}$$

乘法 : $m \bullet n$

结合律 : $(l \bullet m) \bullet n = l \bullet (m \bullet n)$, $(3 \bullet 5) \bullet 2 = 30 = 3 \bullet (5 \bullet 2)$ (4)

壹 : $l \bullet 1 = l$, $3 \bullet 1 = 3$ (5)

交换律 : $m \bullet n = n \bullet m$, $3 \bullet 5 = 15 = 5 \bullet 3$ (6)

分配律 : $l \bullet (m + n) = l \bullet m + l \bullet n$, $3 \bullet 5 = 3 \bullet (1 + 1 + 1 + 1 + 1)$ (7)

$= 3 \bullet 1 + 3 \bullet 1 + 3 \bullet 1 + 3 \bullet 1 + 3 \bullet 1$ (8)

$= 3 + 3 + 3 + 3 + 3$ (9)

其中分配律说明了加法($+$)和乘法($\bullet$)之间是**相容的**。

在自然数里我们可以自由地做加法和乘法，但是**减法**却不一定行得通，比如说:

$$3-5。$$

为了求解方程

$$x+5=3$$

我们需要知道

$$x=3-5=?$$

我们把类似于 $-2\ (=3-5)$ 的所有**负数**添加进来，这样我们就得到了整数:

$$\mathbb{Z}=\{\cdots,-4,-3,-2,-1,0,1,2,3,4,\cdots\}。$$

$\mathbb{Z}$ 和 3 种运算 $\{+, -, \bullet\}$ 一起构成了一个**环**。

类似地，为了解方程

$$7x = 2\ ,$$

我们必需引入**有理数** $\frac{2}{7}$ 。通过引入所有类似的有理数，我们得到:

$$\mathbb{Q} = \left\{ \cdots, -\frac{2}{3}, -\frac{1}{2}, -\frac{1}{3}, -\frac{2}{7}, 0, \frac{1}{7}, \frac{2}{7}, \frac{1}{2}, \frac{2}{3}, 1, \cdots \right\} 。$$

$\mathbb{Q}$ 和满足结合律、交换律、分配律的 4 种运算 $\{+, -, \bullet, /\}$ 一起构成了一个**有理数域**。

而且我们有如下关系：

$$\begin{array}{ccccc} \mathbb{N} & \subset & \mathbb{Z} & \subset & \mathbb{Q} \\ & & \uparrow & & \uparrow \\ & & \text{环} & & \text{域} \end{array}$$

在 $\mathbb{N}$ 上：加法、乘法； (10)

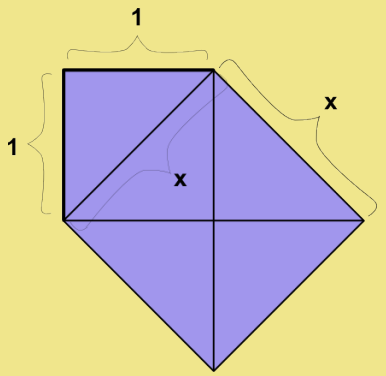
在 $\mathbb{Z}$ 上：加法、减法、乘法； (11)

在 $\mathbb{Q}$ 上：加法、减法、乘法、除法。 (12)

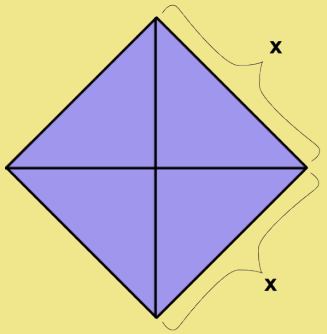
2.3 无理数的发现－－有理数域的扩张

从勾股定理我们知道，在边长为 1 的正方形中，其对角线长度满足方程：

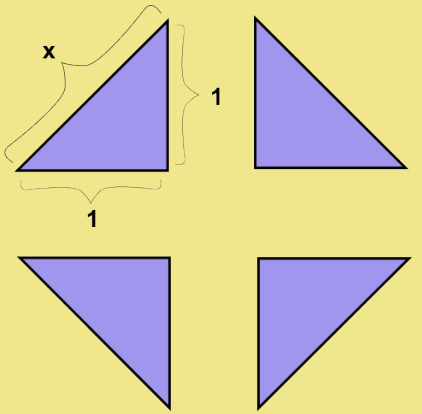
$$x^2 = 2 \ ,$$



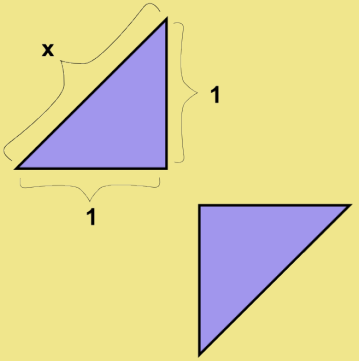
x^2 =



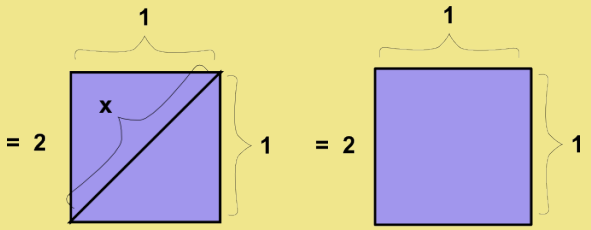
=



= 2 (



)



$$= 2 \bullet 1^2 = 2 \bullet 1 = 2$$

即对角线的长度是方程

$$x^2 = 2$$

的解，我们记作 $\sqrt{2}$ 。

但 $\sqrt{2}$ 并**不是有理数**，即是说，我们不能在 $\mathbb{Q}$ 中找到一个数使其满足方程

$$x^2 = 2。$$

所以为了求解这样一个方程，我们必须扩展我们的数域。

我们将

$$x^2 = 2$$

的解，即 $\sqrt{2}$ 看成是一个全新的数(符号)添加到有理数集 $\mathbb{Q}$ 中，并在这上面给出加法和乘法，从而我们得到数域

$$\mathbb{Q}(\sqrt{2}) = \left\{ m + n\sqrt{2} | m, n \in \mathbb{Q} \right\}。$$

比如说，

$$0 + 1 \bullet \sqrt{2} = \sqrt{2}$$

$$0 + 0 \bullet \sqrt{2} = 0$$

$$1 + 0 \bullet \sqrt{2} = 1$$

$$0 + (-1) \bullet \sqrt{2} = -\sqrt{2}$$

都是 $\mathbb{Q}(\sqrt{2})$ 中的数。

$$\frac{1}{3} + \frac{12}{7}\sqrt{2}$$

也是典型的 $\mathbb{Q}(\sqrt{2})$ 中数。

在数域 $\mathbb{Q}(\sqrt{2})$ 上我们同样地可以做 4 **种运算** $(+,-,\bullet,/)$。在这里，除了 $(\sqrt{2})^2 = 2$ 之外我们不需要知道更多关于 $\sqrt{2}$ 的信息:

$$(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2}$$

$$(a+b\sqrt{2}) \bullet (c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2}$$

$$\begin{aligned}\frac{a+b\sqrt{2}}{c+d\sqrt{2}} &= \frac{(c-d\sqrt{2})(a+b\sqrt{2})}{(c-d\sqrt{2})(c+d\sqrt{2})} \\ &= \frac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-d^2(\sqrt{2})^2} \\ &= \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2}\end{aligned}$$

$$(1+2\sqrt{2})+(3+5\sqrt{2})=(1+3)+(2+5)\sqrt{2}=4+7\sqrt{2}$$

$$(1+2\sqrt{2})\bullet(3+5\sqrt{2})=23+11\sqrt{2}$$

$$\frac{1+2\sqrt{2}}{3+5\sqrt{2}}=\frac{17}{41}-\frac{1}{41}\sqrt{2}\,.$$

扩展之后的数域 $\mathbb{Q}(\sqrt{2})$ 被称作“有理数域 $\mathbb{Q}$ 通过**添加**多项式方程 $x^2 = 2$ 的**解**得到的一个**扩域**”。

$\sqrt{2}$ 是有理数域 $\mathbb{Q}$ 之外的数。由于它是代数方程(即多项式方程)的根，我们称之为**代数数**。

有理系数多项式方程的解被称作代数数。比如如下方程的解：

$$x^2 - 2 = 0$$

$$x^3 + 7x^2 + 5x + 1 = 0$$

$$x^2 + 1 = 0。$$

2.4 $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$

那么 $\sqrt{2}$ 到底是什么，有多大?

打开计算器我们就知道

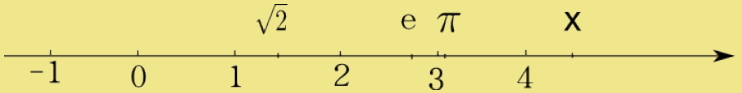
$$\sqrt{2} = 1.41421356237309504880168872420969807856967187537694807317 67\cdots$$

$$e = 2.71828182845904523536028747135266249775724709369995957496 70\cdots$$

$$\pi = 3.14159265358979323846264338327950288419716939937510582097 49\cdots$$

这些都被称之为**实数**。

中学里我们便知道，实数可以画在整个**数轴**上：



，其中 x 具有如下十进制展开的形式：

$$x = \underbrace{a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_0 10^0}_{\text{整数部分}} + \underbrace{\frac{a_{-1}}{10^1} + \frac{a_{-2}}{10^2} + \cdots + \frac{a_{-(m-1)}}{10^{(m-1)}} + \frac{a_{-m}}{10^m} + \cdots}_{\text{小数部分}},\ 0 \le a_i \le 9$$

比如：

$$\frac{2}{7} = 0.285714285714285714285714285714285714285714285714285714\cdots$$

$$= 0 \bullet 10^0 +$$

$$(\tfrac{2}{10^1} + \tfrac{8}{10^2} + \tfrac{5}{10^3} + \tfrac{7}{10^4} + \tfrac{1}{10^5} + \tfrac{4}{10^6}) +$$

$$(\tfrac{2}{10^7} + \tfrac{8}{10^8} + \tfrac{5}{10^9} + \tfrac{7}{10^{10}} + \tfrac{1}{10^{11}} + \tfrac{4}{10^{12}}) +$$

$$(\tfrac{2}{10^{13}} + \tfrac{8}{10^{14}} + \tfrac{5}{10^{15}} + \tfrac{7}{10^{16}} + \tfrac{1}{10^{17}} + \tfrac{4}{10^{18}}) +$$

$$(\tfrac{2}{10^{19}} + \tfrac{8}{10^{20}} + \tfrac{5}{10^{21}} + \tfrac{7}{10^{22}} + \tfrac{1}{10^{23}} + \tfrac{4}{10^{24}}) +$$

$$(\tfrac{2}{10^{25}} + \tfrac{8}{10^{26}} + \tfrac{5}{10^{27}} + \tfrac{7}{10^{28}} + \tfrac{1}{10^{29}} + \tfrac{4}{10^{30}}) +$$

$$(\tfrac{2}{10^{49}} + \tfrac{8}{10^{50}} + \tfrac{5}{10^{51}} + \tfrac{7}{10^{52}} + \tfrac{1}{10^{53}} + \tfrac{4}{10^{54}}) + \cdots$$

$$\sqrt{2} = 1.41421356237309504880168872420969807856967187537694807317 67\cdots$$

$$= 1\bullet 10^{0}+\frac{4}{10^{1}}+\frac{1}{10^{2}}+\frac{4}{10^{3}}+\frac{2}{10^{4}}+\frac{1}{10^{5}}+\frac{3}{10^{6}}+\frac{5}{10^{7}}+\frac{6}{10^{8}}+\frac{2}{10^{9}}+\frac{3}{10^{10}}+\frac{7}{10^{11}}+$$

$$\frac{3}{10^{12}}+\frac{0}{10^{13}}+\frac{9}{10^{14}}+\frac{5}{10^{15}}+\frac{0}{10^{16}}+\frac{4}{10^{17}}+\frac{8}{10^{18}}+\frac{8}{10^{19}}+\frac{0}{10^{20}}+\frac{1}{10^{21}}+\frac{6}{10^{22}}+\frac{8}{10^{23}}+$$

$$\frac{8}{10^{24}}+\frac{7}{10^{25}}+\frac{2}{10^{26}}+\frac{4}{10^{27}}+\frac{2}{10^{28}}+\frac{0}{10^{29}}+\frac{9}{10^{30}}+\frac{6}{10^{31}}+\frac{9}{10^{32}}+\frac{8}{10^{33}}+\frac{0}{10^{34}}+\frac{7}{10^{35}}+$$

$$\frac{8}{10^{36}}+\frac{5}{10^{37}}+\frac{6}{10^{38}}+\frac{9}{10^{39}}+\frac{6}{10^{40}}+\frac{7}{10^{41}}+\frac{1}{10^{42}}+\frac{8}{10^{43}}+\frac{7}{10^{44}}+\frac{5}{10^{45}}+\frac{3}{10^{46}}+\frac{7}{10^{47}}+$$

$$\frac{6}{10^{48}}+\frac{9}{10^{49}}+\frac{4}{10^{50}}+\frac{8}{10^{51}}+\frac{0}{10^{52}}+\frac{7}{10^{53}}+\frac{3}{10^{54}}+\frac{1}{10^{55}}+\frac{7}{10^{56}}+\frac{6}{10^{57}}+\frac{7}{10^{58}}+\cdots$$

$$
\begin{aligned}
e &= 2.71828182845904523536028747135266249775724709369995957496 70\cdots \\
&= 2\bullet 10^{0}+\tfrac{7}{10^{1}}+\tfrac{1}{10^{2}}+\tfrac{8}{10^{3}}+\tfrac{2}{10^{4}}+\tfrac{8}{10^{5}}+\tfrac{1}{10^{6}}+\tfrac{8}{10^{7}}+\tfrac{2}{10^{8}}+\tfrac{8}{10^{9}}+\tfrac{4}{10^{10}}+\tfrac{5}{10^{11}}+ \\
&\quad \tfrac{9}{10^{12}}+\tfrac{0}{10^{13}}+\tfrac{4}{10^{14}}+\tfrac{5}{10^{15}}+\tfrac{2}{10^{16}}+\tfrac{3}{10^{17}}+\tfrac{5}{10^{18}}+\tfrac{3}{10^{19}}+\tfrac{6}{10^{20}}+\tfrac{0}{10^{21}}+\tfrac{2}{10^{22}}+\tfrac{8}{10^{23}}+ \\
&\quad \tfrac{7}{10^{24}}+\tfrac{4}{10^{25}}+\tfrac{7}{10^{26}}+\tfrac{1}{10^{27}}+\tfrac{3}{10^{28}}+\tfrac{5}{10^{29}}+\tfrac{2}{10^{30}}+\tfrac{6}{10^{31}}+\tfrac{6}{10^{32}}+\tfrac{2}{10^{33}}+\tfrac{4}{10^{34}}+\tfrac{9}{10^{35}}+ \\
&\quad \tfrac{7}{10^{36}}+\tfrac{7}{10^{37}}+\tfrac{5}{10^{38}}+\tfrac{7}{10^{39}}+\tfrac{2}{10^{40}}+\tfrac{4}{10^{41}}+\tfrac{7}{10^{42}}+\tfrac{0}{10^{43}}+\tfrac{9}{10^{44}}+\tfrac{3}{10^{45}}+\tfrac{6}{10^{46}}+\tfrac{9}{10^{47}}+ \\
&\quad \tfrac{9}{10^{48}}+\tfrac{9}{10^{49}}+\tfrac{5}{10^{50}}+\tfrac{9}{10^{51}}+\tfrac{5}{10^{52}}+\tfrac{7}{10^{53}}+\tfrac{4}{10^{54}}+\tfrac{9}{10^{55}}+\tfrac{6}{10^{56}}+\tfrac{7}{10^{57}}+\tfrac{0}{10^{58}}+\cdots
\end{aligned}
$$

$$\pi = 3.14159265358979323846264338327950288419716939937510582097494\cdots$$

$$= 3\bullet 10^{0}+\frac{1}{10^{1}}+\frac{4}{10^{2}}+\frac{1}{10^{3}}+\frac{5}{10^{4}}+\frac{9}{10^{5}}+\frac{2}{10^{6}}+\frac{6}{10^{7}}+\frac{5}{10^{8}}+\frac{3}{10^{9}}+\frac{5}{10^{10}}+\frac{8}{10^{11}}+$$

$$\frac{9}{10^{12}}+\frac{7}{10^{13}}+\frac{9}{10^{14}}+\frac{3}{10^{15}}+\frac{2}{10^{16}}+\frac{3}{10^{17}}+\frac{8}{10^{18}}+\frac{4}{10^{19}}+\frac{6}{10^{20}}+\frac{2}{10^{21}}+\frac{6}{10^{22}}+\frac{4}{10^{23}}+$$

$$\frac{3}{10^{24}}+\frac{3}{10^{25}}+\frac{8}{10^{26}}+\frac{3}{10^{27}}+\frac{2}{10^{28}}+\frac{7}{10^{29}}+\frac{9}{10^{30}}+\frac{5}{10^{31}}+\frac{0}{10^{32}}+\frac{2}{10^{33}}+\frac{8}{10^{34}}+\frac{8}{10^{35}}+$$

$$\frac{4}{10^{36}}+\frac{1}{10^{37}}+\frac{9}{10^{38}}+\frac{7}{10^{39}}+\frac{1}{10^{40}}+\frac{6}{10^{41}}+\frac{9}{10^{42}}+\frac{3}{10^{43}}+\frac{9}{10^{44}}+\frac{9}{10^{45}}+\frac{3}{10^{46}}+\frac{7}{10^{47}}+$$

$$\frac{5}{10^{48}}+\frac{1}{10^{49}}+\frac{0}{10^{50}}+\frac{5}{10^{51}}+\frac{8}{10^{52}}+\frac{2}{10^{53}}+\frac{0}{10^{54}}+\frac{9}{10^{55}}+\frac{7}{10^{56}}+\frac{4}{10^{57}}+\frac{9}{10^{58}+\cdots}$$

我们也可以通过一个无穷次的四则运算序列将 e 和 π 定义出来:

$$e = 1 + \frac{1}{1} + \frac{1}{1 \bullet 2} + \frac{1}{1 \bullet 2 \bullet 3} + \frac{1}{1 \bullet 2 \bullet 3 \bullet 4} + \cdots + \frac{1}{1 \bullet 2 \bullet 3 \bullet \cdots \bullet n} + \cdots$$

$$\pi = 2\left(\frac{4 \bullet 1^2}{4 \bullet 1^2 - 1} \bullet \frac{4 \bullet 2^2}{4 \bullet 2^2 - 1} \bullet \frac{4 \bullet 3^2}{4 \bullet 3^2 - 1} \bullet \cdots \bullet \frac{4 \bullet n^2}{4 \bullet n^2 - 1} \bullet \cdots\right)$$

那么 $1, \sqrt{2}, e, \pi$ 这些实数之间有没有区别呢?

1 是**自然数**、**有理数**;

$\sqrt{2}, e, \pi$ 都不是有理数。

$\sqrt{2}$ 是**代数数**(有理系数的多项式方程的解);

但 e, π 则不是(这个结论本身是个深刻的定理)。

绝大多数实数都不是代数数。但要显式地找出他们却不是一件容易的事。

另一方面，并不是所有的代数数都是实数。比如说方程

$$x^2 + 1 = 0$$

的解就不是实数。

因为我们在学校学过，一个实数的平方不可能是负数。比如

$$1 \bullet 1 = 1 \geq 0$$

$$(-1) \bullet (-1) = 1 \geq 0。$$

因此假设 i 是方程

$$x^2 + 1 = 0$$

的解，那么

$$i^2 + 1 = 0 \ ,$$

即

$$i^2 = -1 \ ,$$

这就说明 i 不可能是实数。

如果我们将所有的代数数，比如,

$$\sqrt{2},\ \sqrt{-1},\ \sqrt{3},\ \sqrt[3]{2},\cdots$$

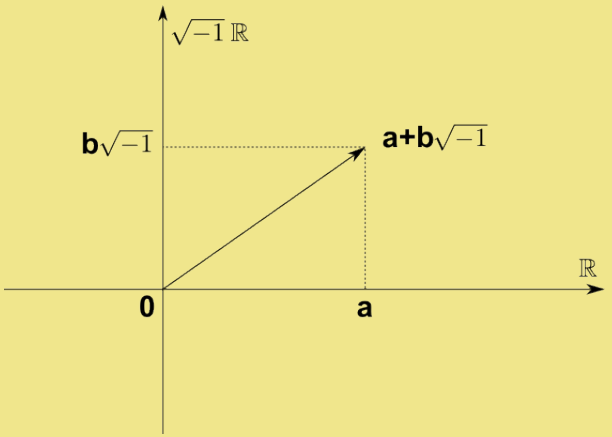
加入到有理数集 $\mathbb{Q}$ 中，我们便得到了所谓的**代数闭域**

$$\overline{\mathbb{Q}} = \mathbb{Q}(\sqrt{2}, \sqrt{-1}, \sqrt{3}, \sqrt[3]{2}, \cdots) \supset \mathbb{Q}。$$

这意味着，所有的以 $\overline{\mathbb{Q}}$ 中的数为系数的多项式方程都可以在 $\overline{\mathbb{Q}}$ 中求解。

如果将 $(\sqrt{-1})$ 加入实数域 $\mathbb{R}$ ， 我们就得到了**复数域**:

$$\mathbb{C} = \{a + b \bullet (\sqrt{-1}) | a, b \in \mathbb{R}\}$$



比如

$$1+0\bullet(\sqrt{-1})\ \ (=1), \sqrt{2}+\pi\bullet(\sqrt{-1})\in\mathbb{C}$$

$$\text{加法}: (a+b(\sqrt{-1}))+(c+d(\sqrt{-1}))=(a+c)+(b+d)(\sqrt{-1})$$

$$\text{乘法}: (a+b(\sqrt{-1}))\bullet(c+d(\sqrt{-1}))=(ac-bd)+(ad+bc)(\sqrt{-1})$$

$$\text{除法}: \frac{a+b(\sqrt{-1})}{c+d(\sqrt{-1})}=\frac{(c-d(\sqrt{-1}))(a+b(\sqrt{-1}))}{(c-d(\sqrt{-1}))(c+d(\sqrt{-1}))} \tag{13}$$

$$=\frac{(ac+bd)+(bc-ad)(\sqrt{-1})}{c^2-d^2((\sqrt{-1}))^2} \tag{14}$$

$$=\frac{ac+bd}{c^2+d^2}+\frac{bc-ad}{c^2+d^2}(\sqrt{-1})。 \tag{15}$$

定理:(高斯) 每个次数不低于 1 的复系数($\in \mathbb{C}$)多项式方程都有一个复数解($\in \mathbb{C}$)。

高斯

高斯生平：

约翰·卡尔·弗里德里希·高斯(Johann Karl Friedrich Gauß)(1777–1855)，

生于布伦瑞克(Braunschweig)，卒于哥廷根(Göttingen)，

德国著名数学家、物理学家、天文学家、几何学家，大地测量学家。

高斯在数学各个方面都有很多贡献。比如数论、统计、分析、微分几何等。

高斯因此被认为是最重要的数学家，并享有“数学王子”的美誉。

著名典故：$1+2+3+\cdots+99+100$ 的计算。

他有很多学生都成为了著名的数学家，如后来闻名于世的戴德金和黎曼。

线性方程

在中学里我们学过如何解线性方程

$$ax + b = 0$$

我们知道其解是

$$x = -\frac{b}{a}。$$

2 次方程

2 次方程

$$x^2 + px + q = 0$$

则有两个解

$$x_{1,2} = \frac{-p \pm \sqrt{p^2 - 4q}}{2}。$$

3 次方程

但是如何解 3 次方程?

我们先考虑最简单的 3 次方程

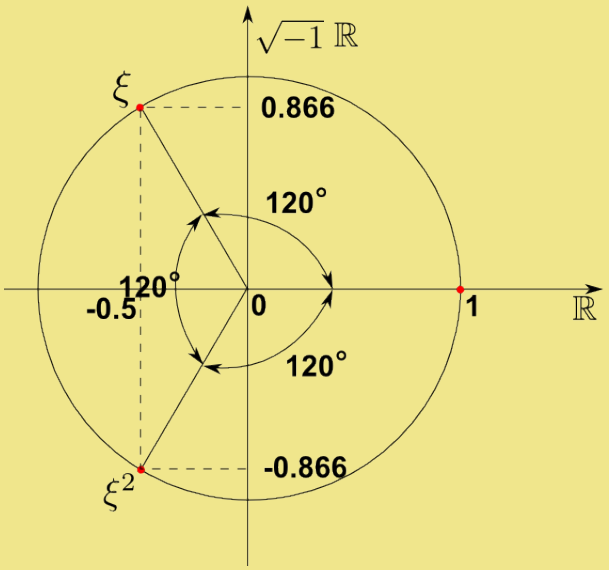
$$x^3 = 1。$$

这个方程的解是

$$\sqrt[3]{1} = \{1, \xi, \xi^2\}。$$

这三个解就是 1 开三次方的值。

它们均匀地分布在单位圆周上，因此也称作 3 次单位根。



$$\xi = \cos(120°) + \sin(120°)\sqrt{-1}$$
$$\approx 0.5 + 0.866\sqrt{-1}$$

$$\xi^2 = \cos(240°) + \sin(240°)\sqrt{-1}$$
$$\approx 0.5 - 0.866\sqrt{-1}$$

下面我们再来看一个普通的 3 次方程:

$$y^3 + ay^2 + by + c = 0$$

这个方程可以转化为一个特殊类型的3次方程

$$x^3 = px + q \ ,$$

$$p = -b + \frac{a^2}{3},\ q = \frac{1}{3}ab - c - \frac{2}{27}a^3 。$$

这个方程也有 3 个解

$$x_1 = \sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}} + \frac{p}{3\sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}}}$$

$$x_2 = (\sqrt[3]{1})\sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}} + \frac{p}{3(\sqrt[3]{1})\sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}}}$$

$$x_3 = (\sqrt[3]{1})^2\sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}} + \frac{p}{3(\sqrt[3]{1})^2\sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}}}。$$

这说明，对于任意 3 次方程，我们都可以通过开根号来进行求解。

4 次方程

在进行更复杂些的计算之后我们可以求得 4 次多项式方程的类似的求解公式(也称求根公式)。

根据以上讨论，我们已经知道，所有 4 次及 4 次以下的方程我们都可以将其解用仅含有加、减、乘、除和开方的公式来表示。这些解都被称作 **根式解**。

高次方程

那么对于**次数更高**的多项式方程我们是否也有根式解呢?

定理 :(伽罗华、阿贝尔) “大多数” 5 次和 5 次以上的多项式方程没有根式解。

比如，方程

$$x^5 - 4x + 2 = 0$$

就没有根式解(见下文)。

3　群与对称

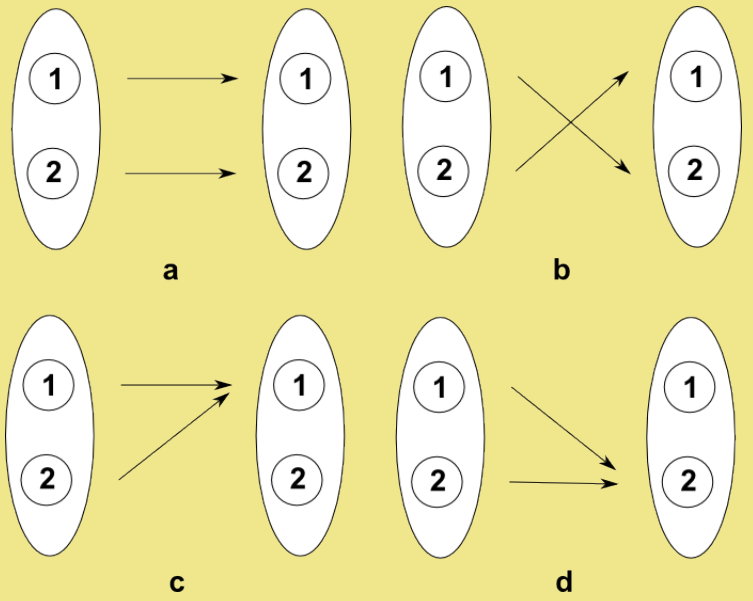
3.1　群——可以做乘除运算的集合

2 元集合的对称群

考虑集合

$$\{1,2\}。$$

中元素的置换。



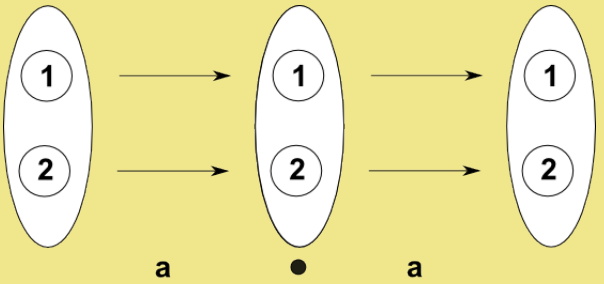
a, b 都是集合 $\{1,2\}$ 的置换，其中 a 是恒同变换，即什么都不变；

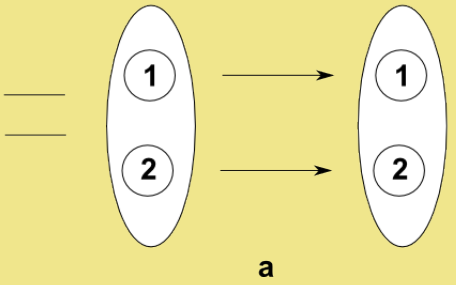
c, d 则不是集合 $\{1,2\}$ 的置换。

特别地，$\{a,b\}$ 是 $\{1,2\}$ 上全体置换的集合。

群上的运算－－乘法

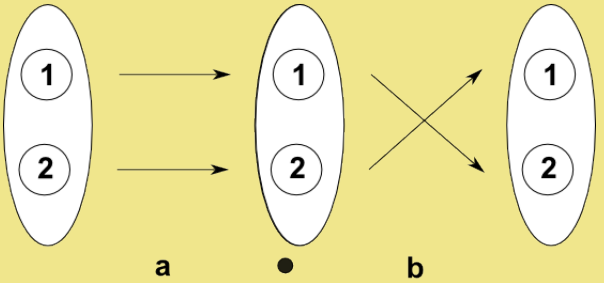
a●a=?

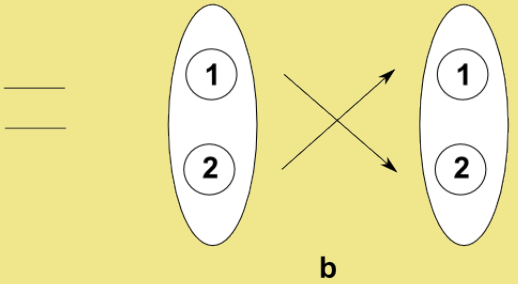




$$a \bullet a = a$$

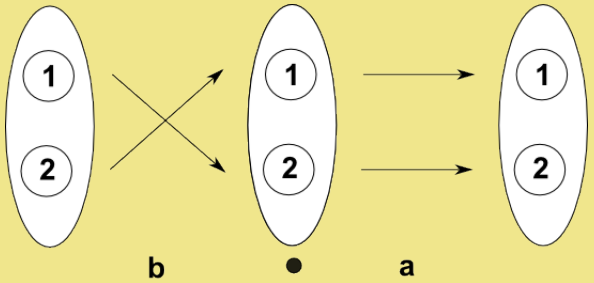
$$a \bullet b = ?$$

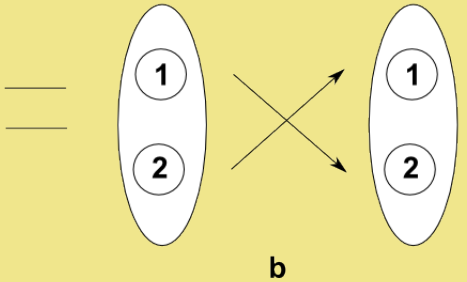




$$a \bullet b = b$$

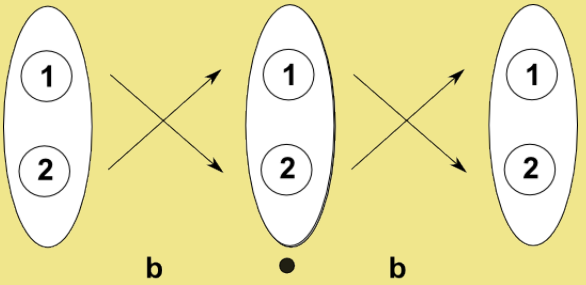
$$b \bullet a = ?$$

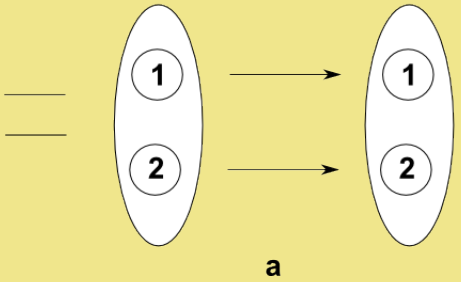




$$b \bullet a = b$$

$$b \bullet b = ?$$





$$b \bullet b = a$$

集合 $\{1,2\}$ 的(所有)置换 $\{a,b\}$ 构成了一个二元 群

$$S_2 := (\{a,b\}, \bullet) ,$$

其乘法表为

$\circ$	a	b
a	a	b
b	b	a

我们可以发现，任何 S_2 中的元素和 a 相乘总是等于该元素自身。因此 a 被称做 S_2 中的**单位元**，它和有理数 $\mathbb{Q}$ 中的 1 作用相似，因此也称作**幺(1)元**。单位元常被记作 e 。

因为 $a \bullet a = e$ ，所以 $a = \frac{e}{a} = a^{-1}$ (我们称为 a 的逆元) 。

S_2 中元素的乘积都可以交换，比如

$$a \bullet b = b = b \bullet a。$$

因此 S_2 被称作是一个**交换群**(也称**阿贝尔群**)。

阿贝尔

阿贝尔生平

尼 尔 斯 • 亨 利 克 • 阿 贝 尔 （Niels Henrik Abel，1802年8月5日－1829年4月6日），挪威数学家。

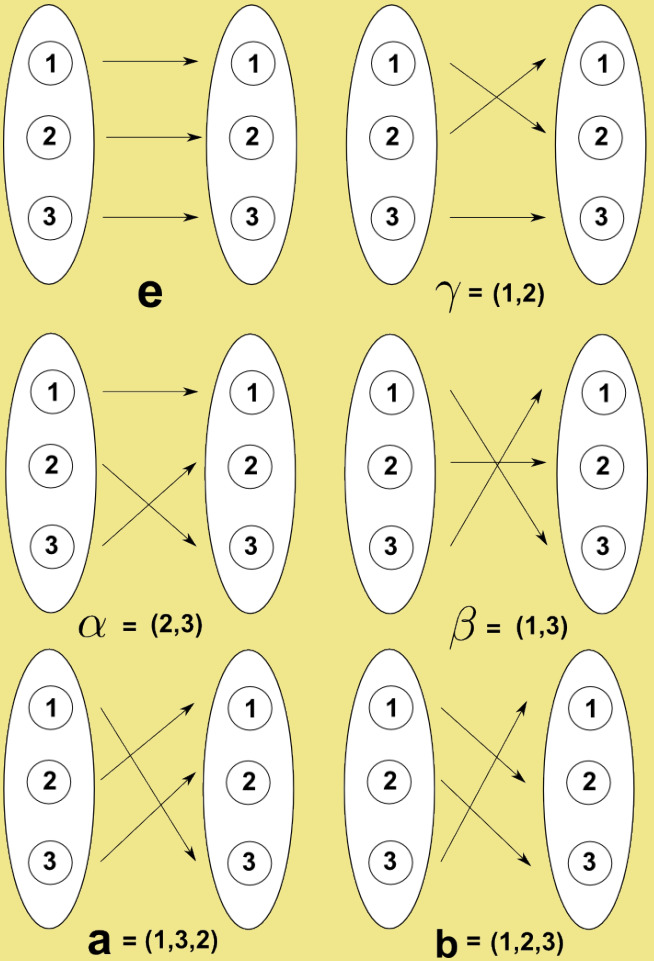
阿贝尔以证明五次方程没有根式解和对椭圆函数论的研究而闻名。

阿贝尔1825年得到政府资助，游学柏林和巴黎。但一直不得志，无法获得教席以专心从事研究，最后因肺结核在挪威的弗鲁兰逝世，时年27岁。

阿贝尔和同样英年早逝的伽罗华一同被奉为群论的先驱。

以他名字命名的阿贝尔奖是数学界中和诺贝尔奖齐名的三大奖项之一。

3 元集的对称群



乗法表

$\circ$	e	a	b	α	β	γ
e	e	a	b	α	β	γ
a	a	b	e	γ	α	β
b	b	e	a	β	γ	α
α	α	β	γ	e	a	b
β	β	γ	α	b	e	a
γ	γ	α	β	a	b	e

S_3 里的每个元素都有逆元，比如：

$$a \bullet b = e = b \bullet a \ ,$$

所以

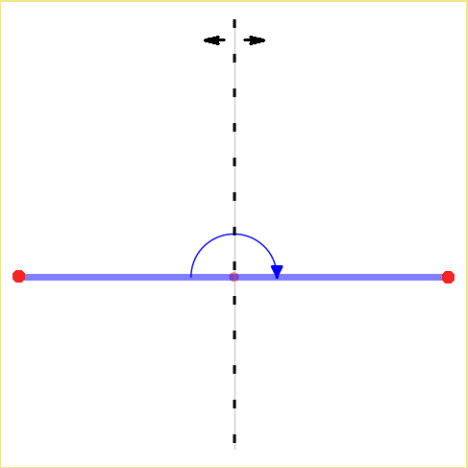
$$a^{-1} = b, \quad b^{-1} = a$$

S_3 不是阿贝尔群。比如

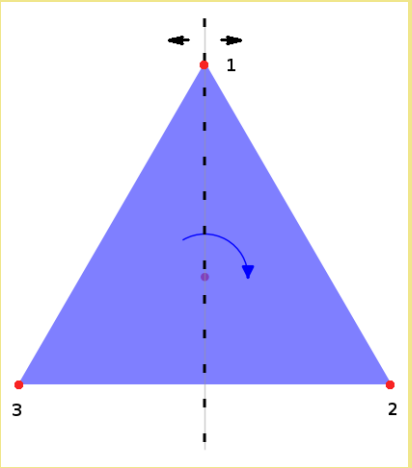
$$\alpha \bullet \beta = a \neq b = \beta \bullet \alpha 。$$

但他是一个**可解群**，即是说它是由一系列阿贝尔群合成的。(参见3.2)

正 n-边形的对称群

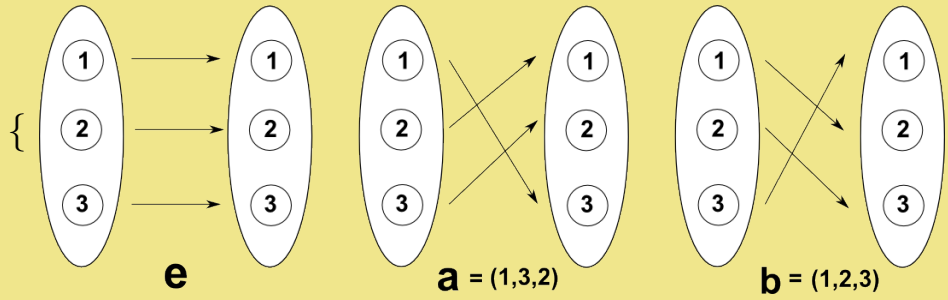


正 2 边形



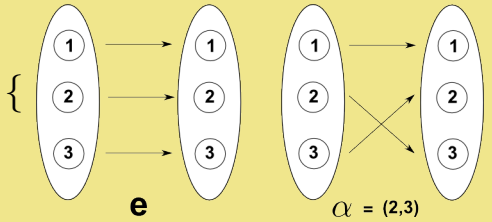
正 3 边形(正三角形)

正三角形的对称群由旋转



$\} = \mathbb{Z}_3$ (3 阶循环群)

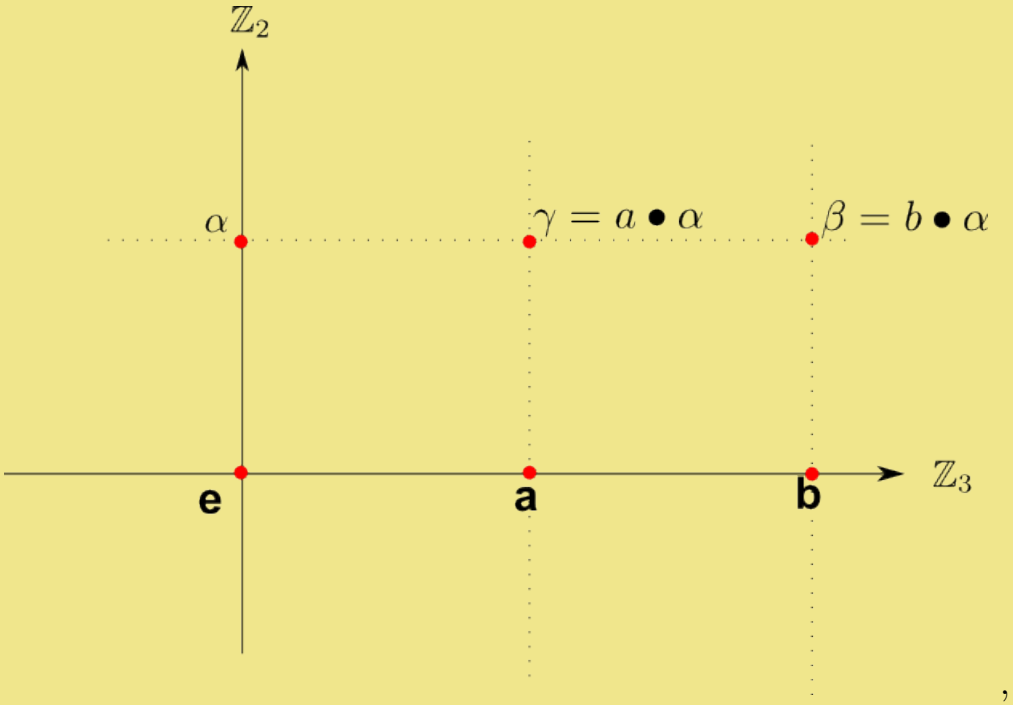
和反射



$\} = \mathbb{Z}_2$ (2 阶循环群)

合成，

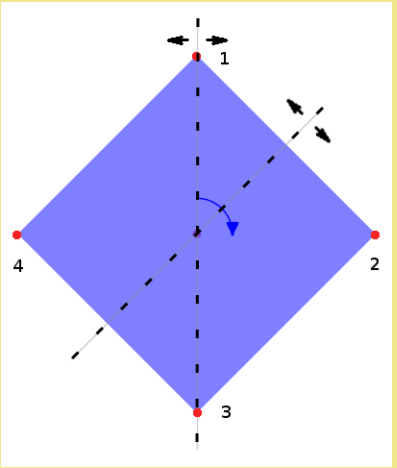
$$S(\triangle) = \mathbb{Z}_3 \ltimes \mathbb{Z}_2$$



，

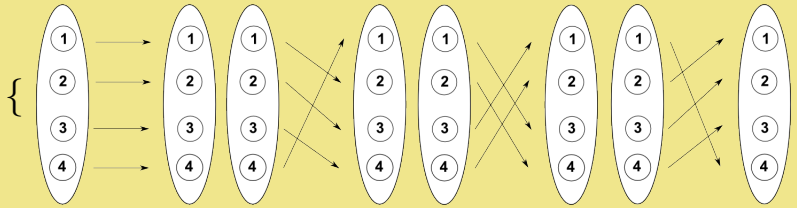
并且恰好就是 3 元集的对称群 S_3 ， 共有 $3 \bullet 2 = 6$ 个元素。因此 S_3 是由 $\mathbb{Z}_3$ 和 $\mathbb{Z}_2$ 合

成的。

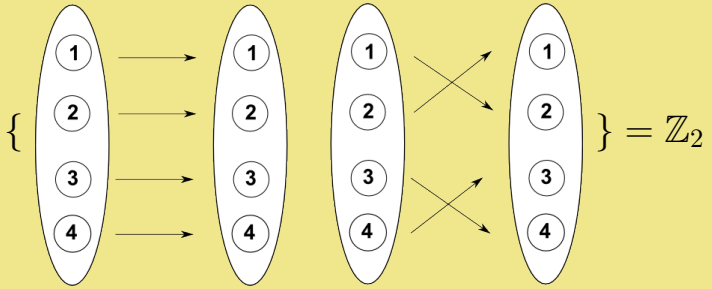


正4边形(正方形)

正方形的对称群同样是由旋转



和对称



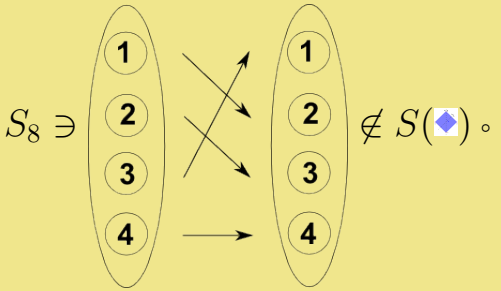
合成,

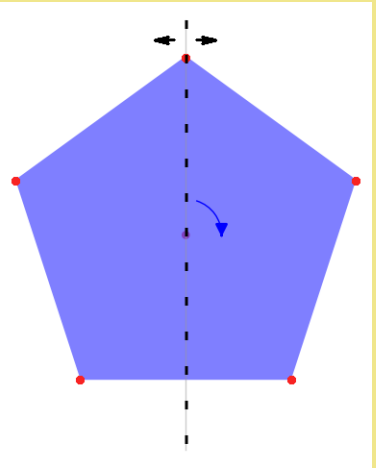
$$S(\diamond) = \mathbb{Z}_4 \ltimes Z_2 \nsubseteq S_8 \circ$$

$S(\diamondsuit)$ 共有 $4 \bullet 2 = 8$ 个元素。

$$S(\diamondsuit) \subsetneqq S_8 \ ,$$

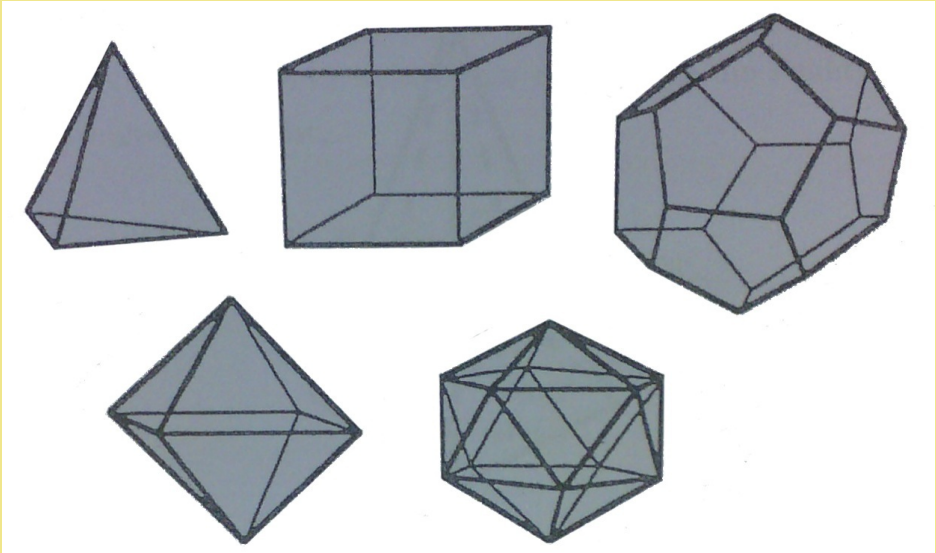
比如



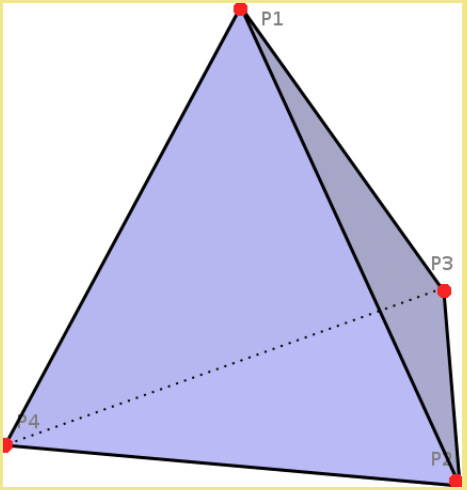


正 5 边形

3.3　5 种正多面体

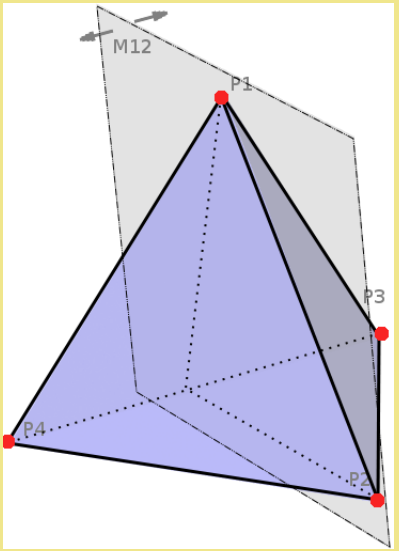


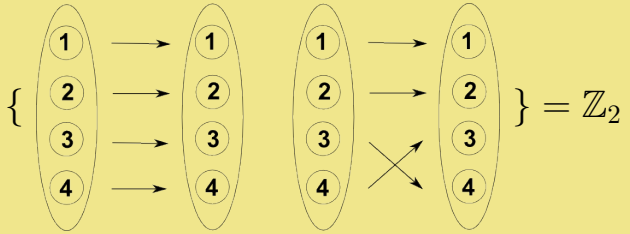
名称	元素、特性	顶点数	边数	面数
正4面体	火、热	4个顶点	6条边	4个面(正三角形)
正6面体	土、致密	8个顶点	12条边	6个面(正方形)
正8面体	气、飘渺	6个顶点	12条边	8个面(正三角形)
正12面体	宇宙、超俗的	20个顶点	30条边	12个面(正5边形)
正20面体	水、流动的	12个顶点	30条边	20个面(正三角形)



正4面体

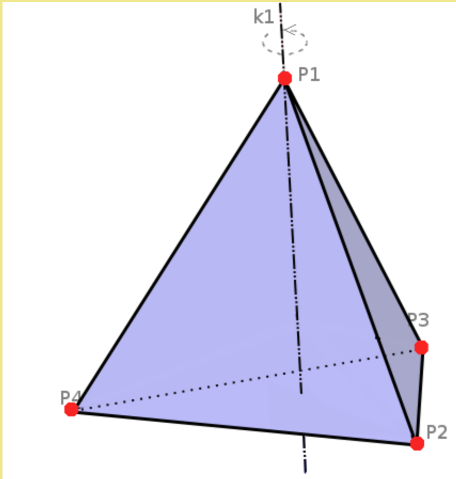
关于平面 M_{12} (经过 P_1, P_2 两个顶点垂直于对边的平面)的反射对称:

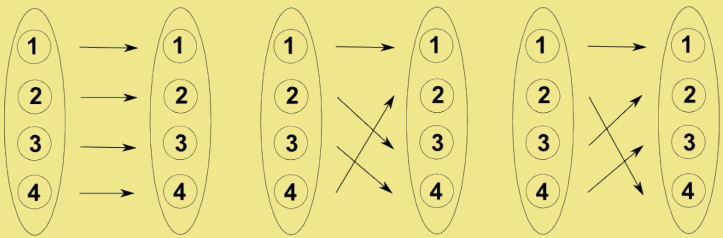




$$\{\ \} = \mathbb{Z}_2$$

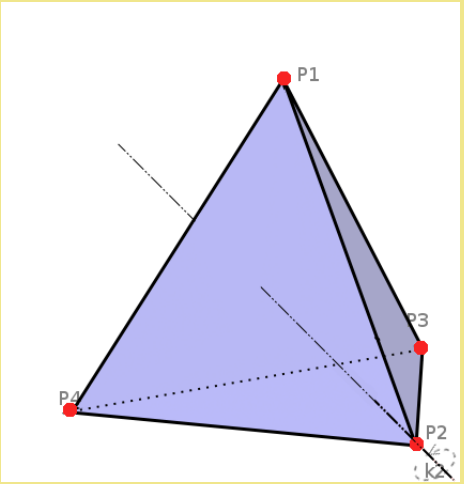
关于轴 k_1 (经过顶点 P_1 垂直于底面的直线，经过底面中心 P_{234})的旋转对称:



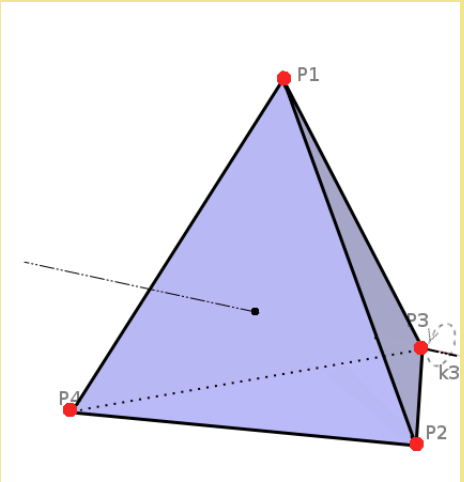
$\{$  $\} = \mathbb{Z}_3$

类似地

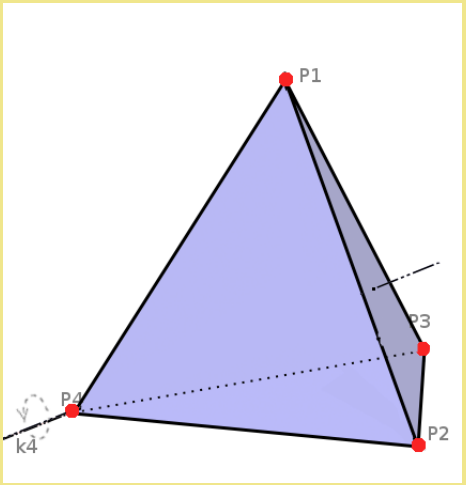
关于轴 k_2 (经过顶点 P_2 垂直于底面的直线)的旋转对称 $= \mathbb{Z}_3$



关于轴 k_3 (经过顶点 P_3 垂直于底面的直线)的旋转对称 $= \mathbb{Z}_3$



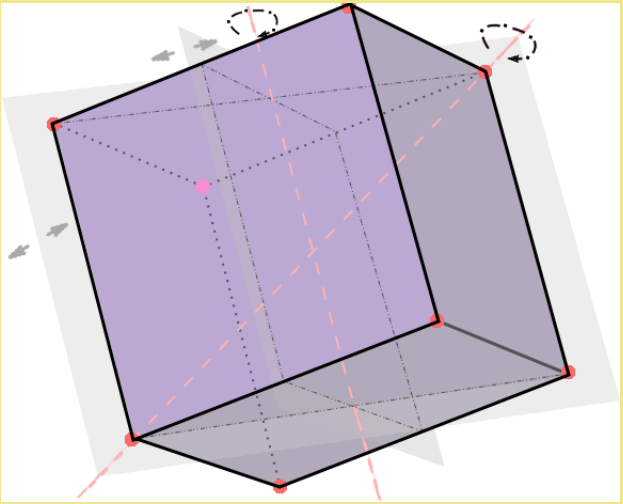
关于轴 k_4 (经过顶点 P_4 垂直于底面的直线)的旋转对称 $= \mathbb{Z}_3$



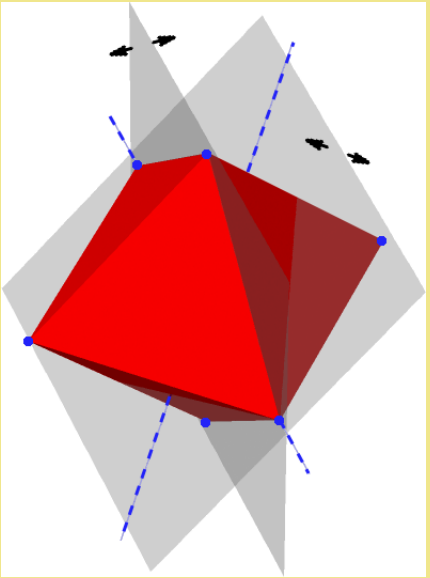
正 4 面体的对称群S(△)便是由这样的反射 $\mathbb{Z}_2$ 和 4 种旋转 $\mathbb{Z}_3$ 生成的。

$$S(\triangle) \subset S_4$$

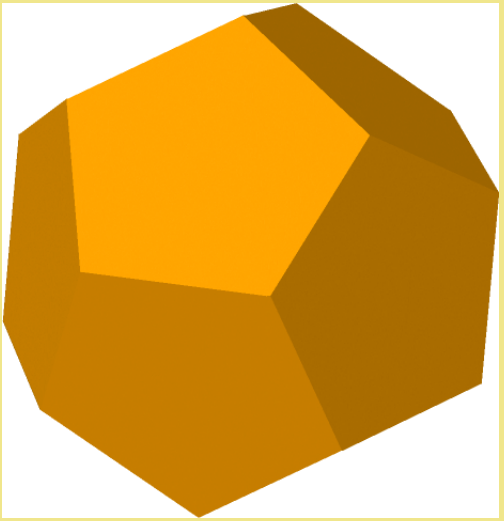
事实上S(△)$= S_4$, 因而是可解的.



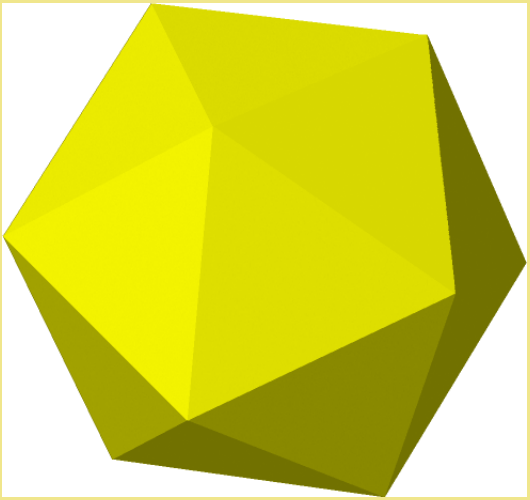
正 6 面体



正 8 面体



正 12 面体



正 20 面体

正 X 面体?

No! 没有更多的正多面体了。

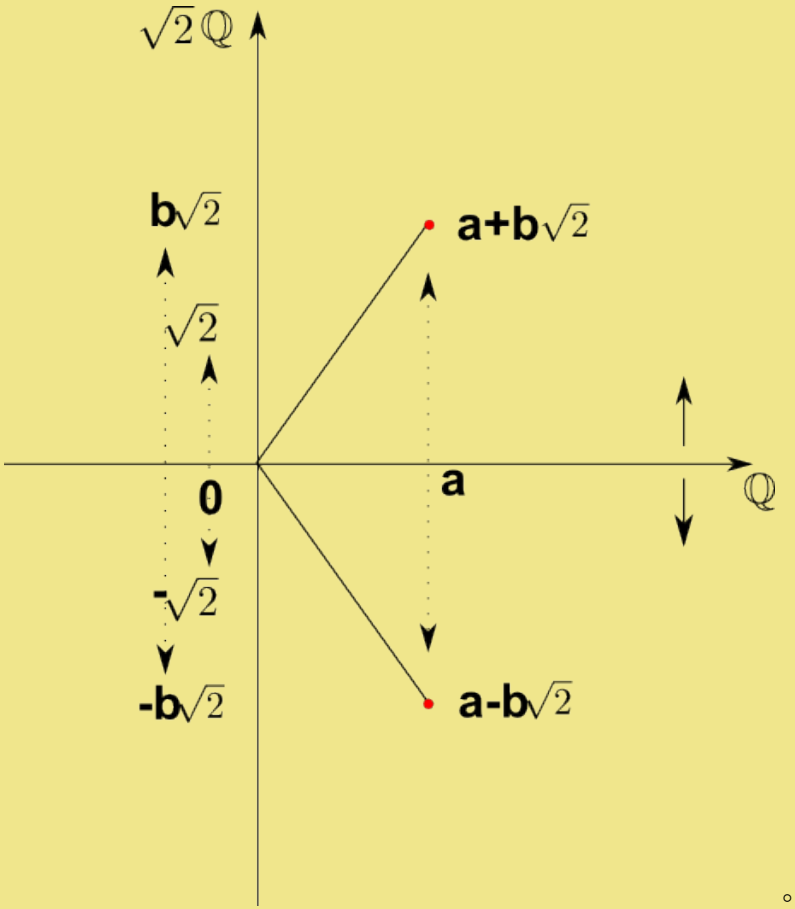
由于时间关系，这里只是简单提一下以下结论:

正 12 面体和正 20 面体的对称群(抽象地来说)是一样的。它们是 S_5 的一个子群 $A_5 \subset S_5$.

注意: S_2, S_3, S_4 都可以由 $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_5, \cdots$ 等循环群合成，但 A_5 和 S_5 不能。

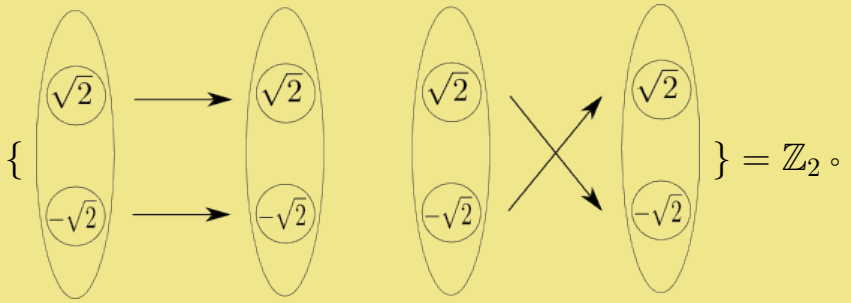
3.4 域的扩张的对称－－伽罗华群

域的扩张 $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\} \supset \mathbb{Q}$ 的对称看起来如下图:



。

这个对称由方程 $x^2-2=0$ 的两个解 $\pm\sqrt{2}$ 的置换决定。



$\}=\mathbb{Z}_2$。

这个二元置换群就是扩张 $\mathbb{Q}(\sqrt{2})\supset\mathbb{Q}$ 的对称群，也称作扩张 $\mathbb{Q}(\sqrt{2})\supset\mathbb{Q}$ 的

伽罗华群，

记作 $Gal(\mathbb{Q}(\sqrt{2})\supset\mathbb{Q})$ 。

它在 $\mathbb{Q}(\sqrt{2})$ 上的置换保持 $\mathbb{Q}$ 不动，并且和四则运算 $(+,-,\bullet,/)$ 相容，即先做四则运算再做置换与先做置换再做四则运算得到的结果是一样的。

通过添加方程

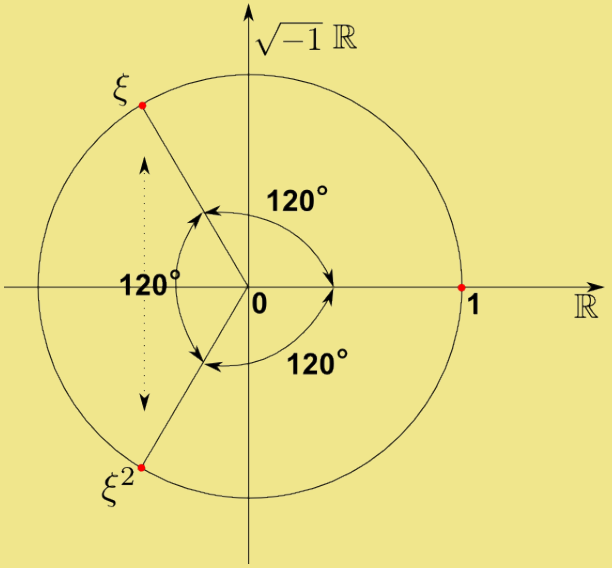
$$x^3 - 1 = 0$$

的所有解

$$\sqrt[3]{1} = \{1, \xi, \xi^2\} \ ,$$

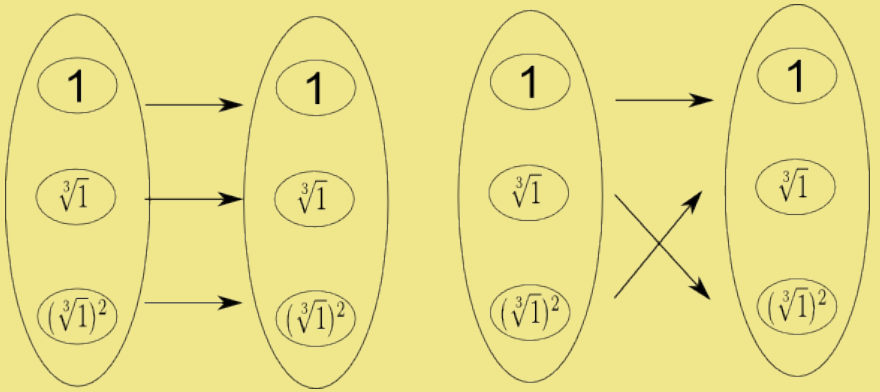
我们可以得到域的扩张

$$\mathbb{Q}(\xi) \supset \mathbb{Q}。$$



$Gal(\mathbb{Q}(\xi) \supset \mathbb{Q})$ 对这三个解 $(1, \xi, (\xi)^2)$ 进行置换。 $1 \in \mathbb{Q}$ ， 所以应该被固定住。

因此我们有

$$Gal(\mathbb{Q}(\xi) \supset \mathbb{Q}) = \{$$  $$\} = \mathbb{Z}_2 。$$

下面考虑方程

$$x^3 - 2 = 0\,。$$

通过求根公式可知，该方程有三个根式解

$$\{\sqrt[3]{2},\quad \xi\sqrt[3]{2},\quad (\xi)^2\sqrt[3]{2}\}\,。$$

$$(\sqrt[3]{2})^3 = 2$$

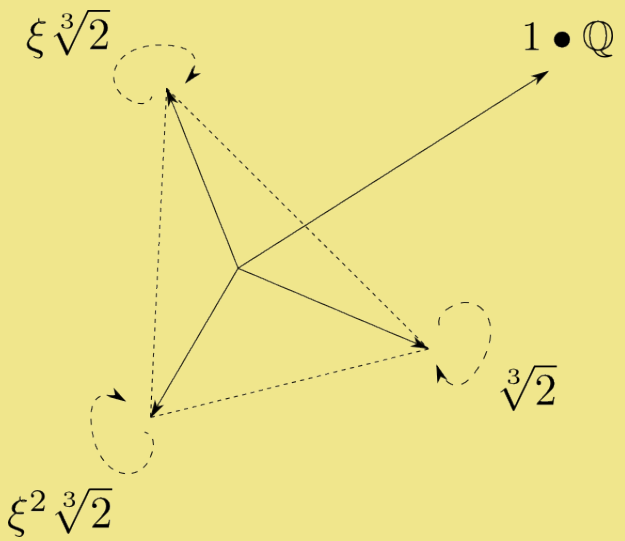
$$(\xi\sqrt[3]{2})^3 = (\xi)^3(\sqrt[3]{2})^3 = 1 \bullet 2 = 2$$

$$((\xi)^2\sqrt[3]{2})^3 = (\xi^3)^2(\sqrt[3]{2})^3 = 1^2 \bullet 2 = 2$$

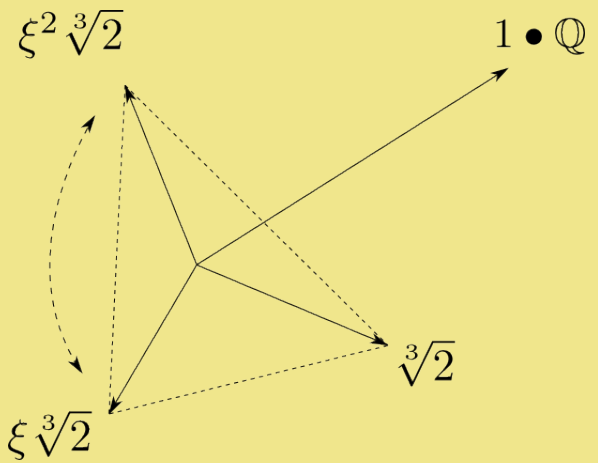
将这些解添加到 $\mathbb{Q}$ 我们得到了域的扩张 $K \supset \mathbb{Q}$。在这里，$Gal(K \supset \mathbb{Q})$ 对 $\{\sqrt[3]{2}, \xi\sqrt[3]{2}, (\xi)^2\sqrt[3]{2}\}$ 进行置换。由于这些解都不再 $\mathbb{Q}$ 中，所以没有特别的限制，因此：

$$Gal(K \supset \mathbb{Q}) = S_3 = Sym(\text{  })。$$

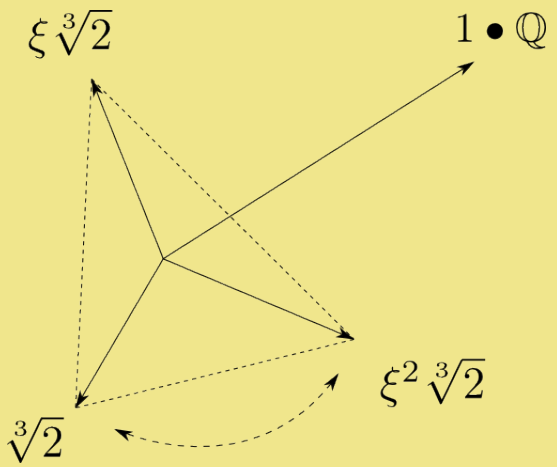
我们可以看一下 $Gal(K \supset \mathbb{Q})$ 在这些根上的作用。这些作用和正三角形的对称变换对应：



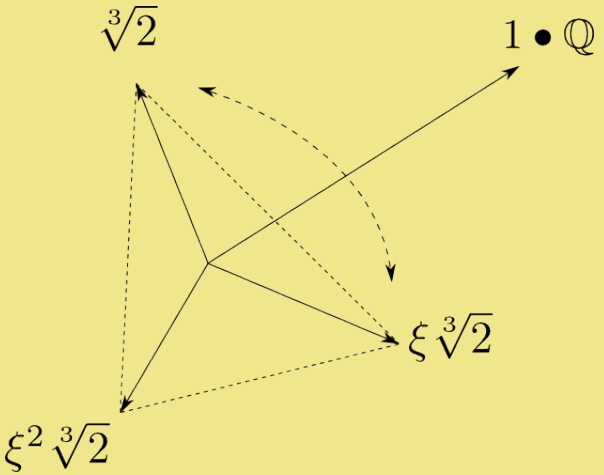
e



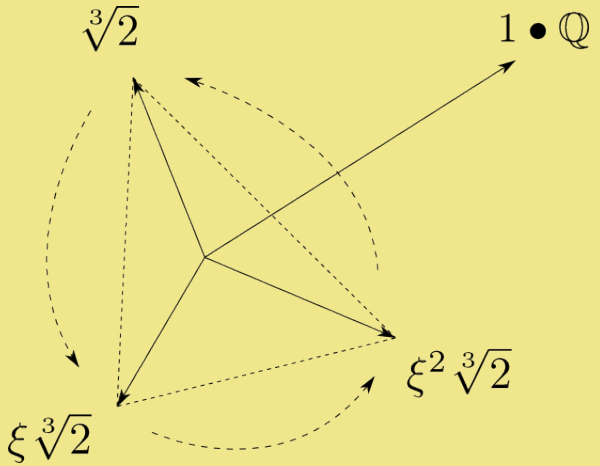
(23)



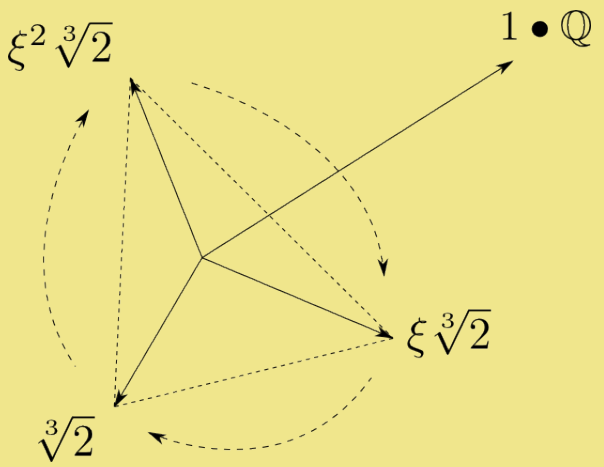
(13)



(12)

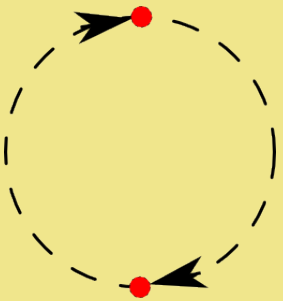


(132)

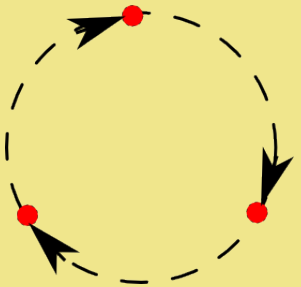


(123)

前面的例子暗示我们那些通过添加多项式方程**根式解**得到的域的扩张的伽罗华群应该是**可解的**，也就是说它们都是由循环群 $\mathbb{Z}_2, \mathbb{Z}_3, \cdots$ 等合成的。



$\mathbb{Z}_2$



$\mathbb{Z}_3$

定理：通过添加方程 $x^n - a = 0, a \in \mathbb{Q}$ 的根式解 $\sqrt[n]{a}$ 得到的域的扩张的伽罗华群 $Gal(\mathbb{Q}(\sqrt[n]{a}) \supset \mathbb{Q})$ 总是可解群。

我们在前面已经看到过一个典型的例子：

$$x^3 = px + q$$

其解为

$$x_1 = \sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}} + \frac{p}{3\sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}}}$$

$$x_2 = \xi\sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}} + \frac{p}{3\xi\sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}}}$$

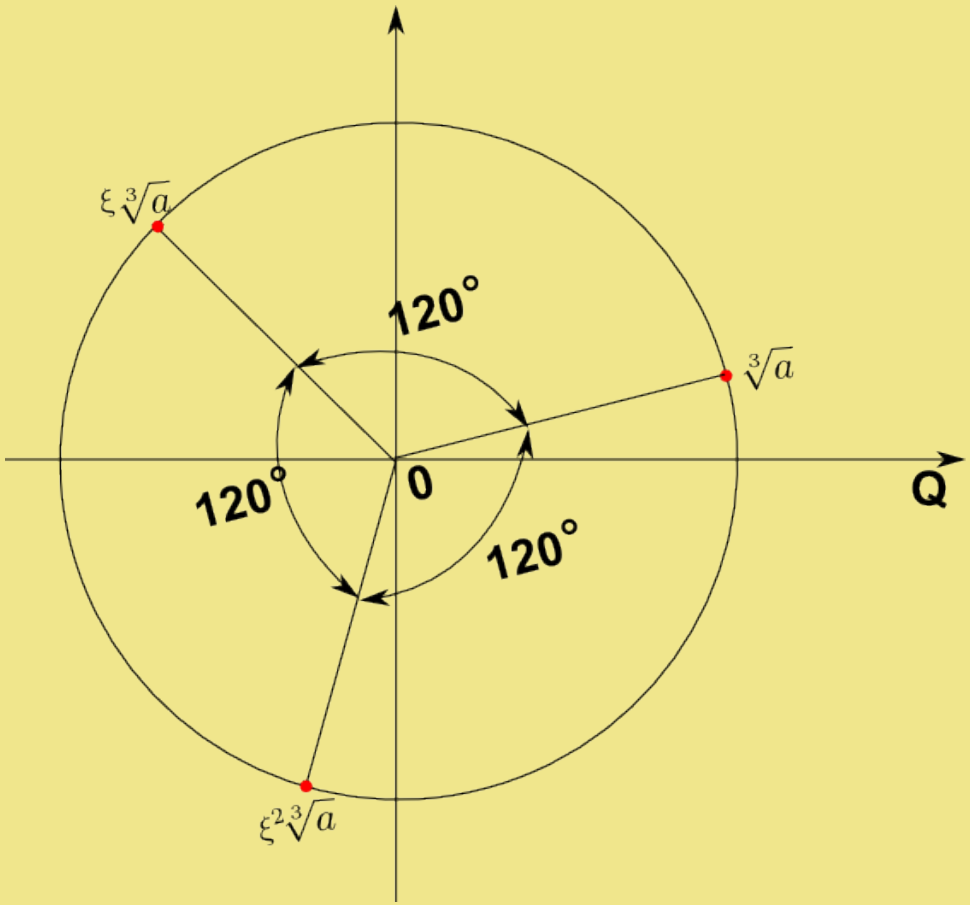
$$x_3 = \xi^2\sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}} + \frac{p}{3\xi^2\sqrt[3]{\frac{q}{2} + \sqrt{(\frac{q}{2})^2 - (\frac{p}{3})^3}}}。$$

这里涉及到了五种运算 $(+, -, \bullet, /, \sqrt[3]{\ }, \sqrt[2]{\ })$。然而只有 $(\sqrt[3]{\ }, \sqrt[2]{\ })$ 被

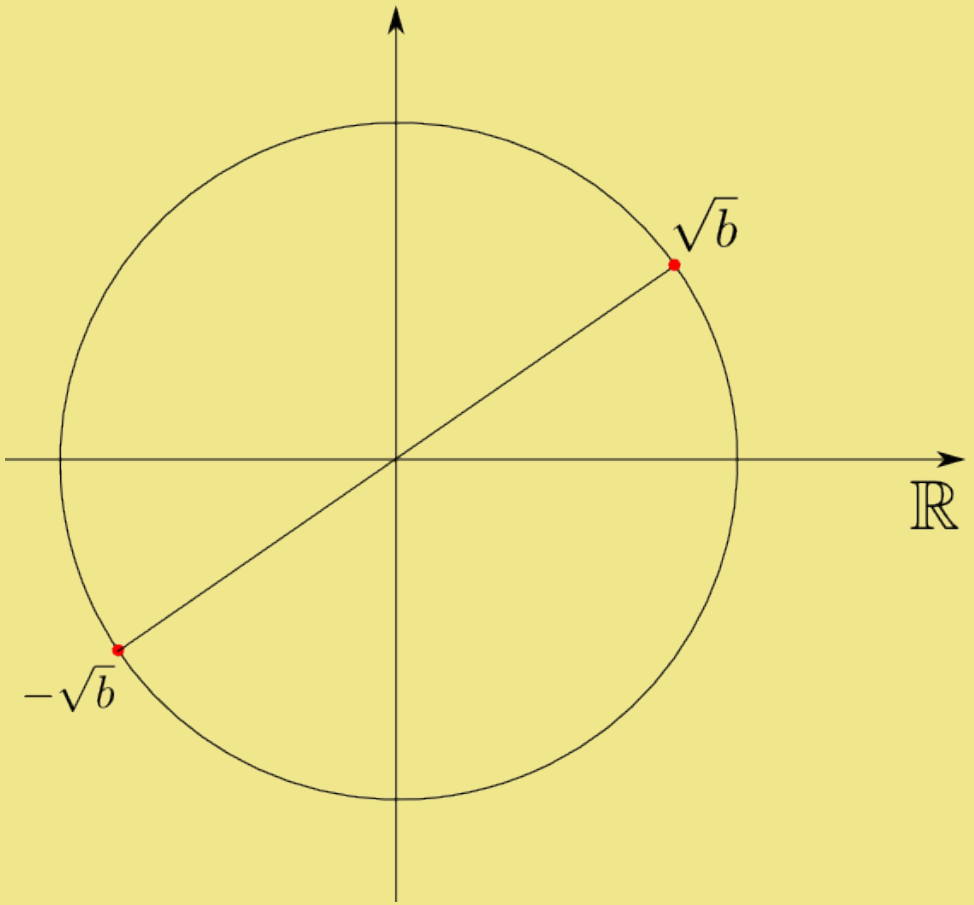
$$Gal(Q(x_1, x_2, x_3) \supset \mathbb{Q}) \subset S_3$$

所识别。

我们可以这样来理解:



$$\sqrt[3]{a} \leftrightsquigarrow S_3 \subset Gal(Q(x_1, x_2, x_3) \supset \mathbb{Q})$$



$$\sqrt{b} \leftrightsquigarrow \mathbb{Z}_2 \subset Gal(Q(x_1, x_2, x_3) \supset \mathbb{Q})$$

在这里， $Gal(Q(x_1, x_2, x_3) \supset \mathbb{Q})$ 并没有看到四则运算。

我们可以认为，如果一个 n 次多项式能通过运算 $(+,-,\bullet,/,\sqrt[n]{\ },\sqrt[n-1]{\ },\cdots,\sqrt[2]{\ })$ 得到根，那么

$$\sqrt[n]{\ } \leftrightsquigarrow \text{可解群}_n \subset Gal(\mathbb{Q}(\text{所有解}) \supset \mathbb{Q})$$

$$\sqrt[n-1]{\ } \leftrightsquigarrow \text{可解群}_{n-1} \subset Gal(\mathbb{Q}(\text{所有解}) \supset \mathbb{Q})$$

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

因此 $Gal(\mathbb{Q}(\text{所有解}) \supset \mathbb{Q})$ 是由那些 $\{\sqrt[n]{\ },\sqrt[n-1]{\ },\cdots\}$ 所对应的可解群（ 可解群$_n$ ，可解群$_{n-1}$ ， $\cdots$ ， 可解群$_1$ ）所合成。这从而说明 $Gal(\mathbb{Q}(\text{所有解}) \supset \mathbb{Q})$ 依然是可解群。

因此我们得到了如下对应

$$\text{一个有根式解的多项式 } f \ \leftrightarrow Gal(\mathbb{Q}(f \text{ 的所有解}) \supset \mathbb{Q}) \text{ 是可解群 ,}$$

这里 $\mathbb{Q}(f$ 的所有解$) \supset \mathbb{Q}$ 是通过添加 f 的解得到的域的扩张。

注释：可解群是除单位群之外最简单的群，而可解群与根式运算对应，因此，在这个意义下我们可以认为根式解是继四则运算解之后最简单的解的形式。

人们会问，如果我们不知道 f 的显式解，我们能否确定 $Gal(\mathbb{Q}(f \text{ 的所有解}) \supset \mathbb{Q})$?

答案是肯定的。即是说，在稍微弱一些的条件下，不需要通过 f 的显式解我们也能确定 $Gal(\mathbb{Q}(f \text{ 的所有解}) \supset \mathbb{Q})$.

定理：设

$$f = a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x^1 + a_5 \ ,$$

$$a_0,\ a_1,\ a_2,\ a_3,\ a_4,\ a_5 \in \mathbb{Q} \ ,$$

且 f 不可约，即 f 不能写成 $g \bullet h, g, h \in \mathbb{Q}[x]$ 的形式。若 f 有 3 个实数解，那么 $Gal(\mathbb{Q}(f \text{ 的所有解}) \supset \mathbb{Q}) = S_5$ ，从而是不可解群。

比如，我们取

$$g = x^5 - 4x \tag{16}$$

$$= x(x^4 - 4) \tag{17}$$

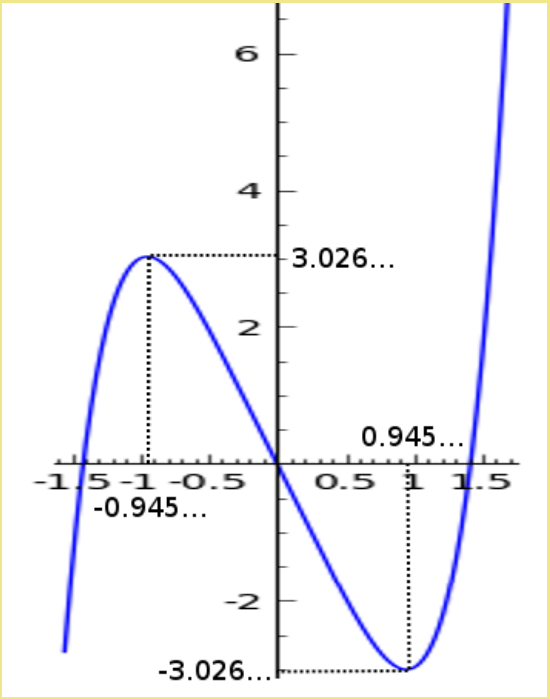
$$= x(x^2 - 2)(x^2 + 2) \tag{18}$$

$$= x(x - \sqrt{2})(x + \sqrt{2})(x^2 + 2)。 \tag{19}$$

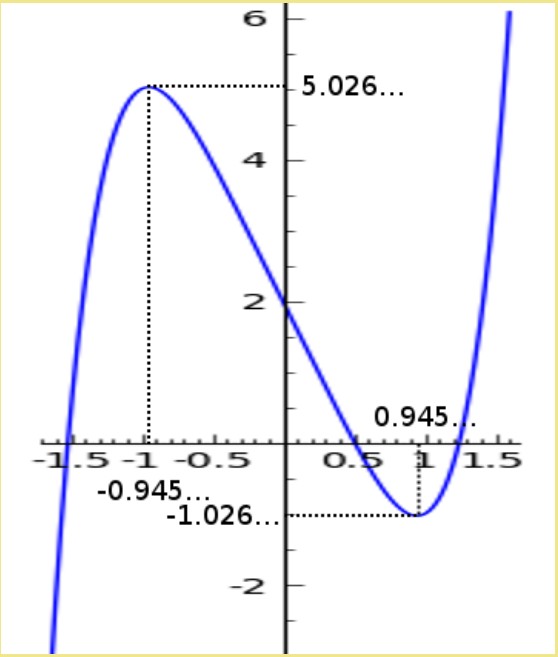
所以 g 有 3 个实数解 $0, \sqrt{2}, -\sqrt{2} \in \mathbb{R}$ 。

不过 g 是可约的。所以我们对 g 稍做修改，即取

$$f = g + 2 = x^5 - 4x + 2$$



$g = x^5 - 4x$



$f = g + 2 = x^5 - 4x + 2$

我们可以证明 $f = x^5 - 4x + 2$ 是不可约的。同时由上图可以看出， f 仍然有 3 个实数解。因此 $Gal(\mathbb{Q}(f \text{ 的所有解}) \supset \mathbb{Q}) = S_5$ ，是不可解群。

对应地，作为结论，我们知道

多项式方程 $f = x^5 - 4x + 2 = 0$ 没有根式解。

谢谢！