离散数学

Discrete Mathematics

第11讲 群 Group

"As for everything else, so for a mathematical theory: beauty can be perceived but not explained."(Arthur Cayley)

"It is difficult to give an idea of the vast extent of modern mathematics. This word 'extent' is not the right one: I mean extent crowded with beautiful detail - not an extent of mere uniformity such as an objectless plain, but of a tract of beautiful country seen at first in the distance, but which will bear to be rambled through and studied in every detail of hillside and valley, stream, rock, wood and flower. But, as for everything else, so for a mathematical theory - beauty can be perceived but not explained."

— Arthur Cayley (1883)

鞠实儿先生在《简明逻辑学》序中的一段话：

“在我学习生涯刚开始时，父亲就对我说：“读书首先要细读序和跋，其中包含的知识会帮助你理解书的内容。”多少年过去了，现在轮到我来为书作序了，目的当然是为读者把握全书提供条件。

如何做到这一点呢？途径大致有二：

其一，微观法。通过对其组成部分及其相互关系的描述，揭示篇章间的前后关照，展现全书的结构，让人易于对书的内容入木三分。学人曰：慎思。

其二，宏观法。借助一个超越其内容的“宏大”叙事，烘托出全书背景，由此催发阅读心态在时空中扩张，让人易于自我感觉登高望远。学人曰：反思。”

“无论在什么地方，只要能应用群论，从一切纷乱混淆中立刻结晶出简洁与和谐，群的概念是近世科学思想的出色的新工具之一.”

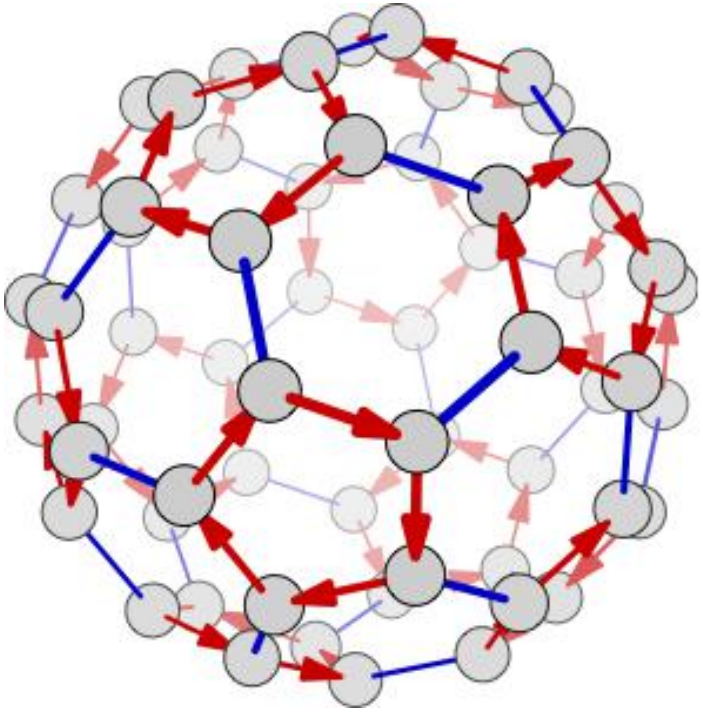
——E. T. Bell

Wherever groups disclosed themselves, or could be introduced, simplicity crystallized out of comparative chaos.

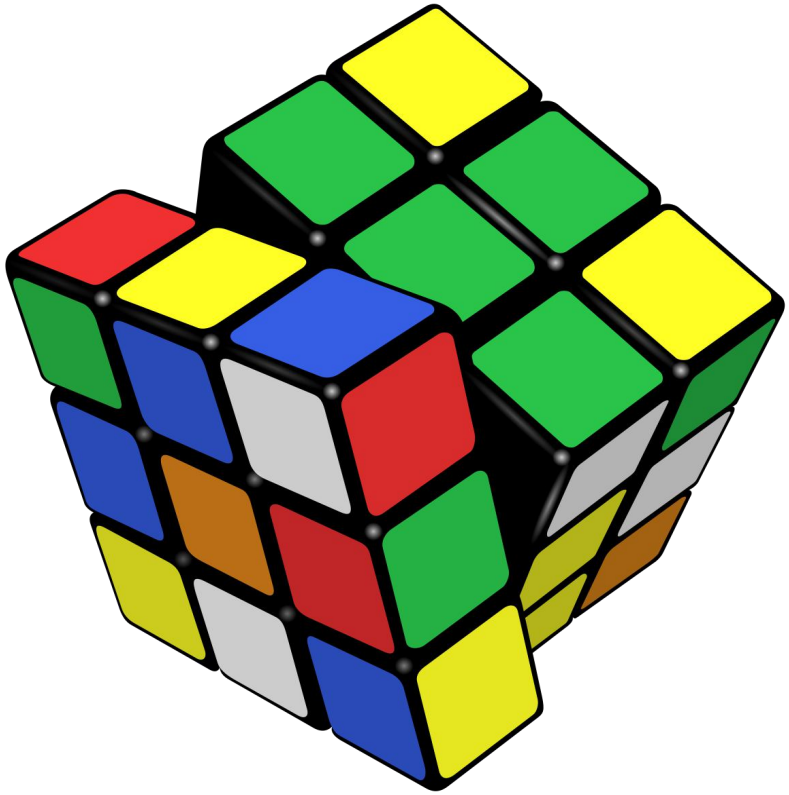
--Eric Temple Bell

Mathematics, Queen and Servant of Science, New York, 1951, p164.

群(Group)?



Alternative Group A_5



Rubik's Cube (Group)

四次方程？五次方程？

$$ax^4+bx^3+cx^2+dx+e=0,a\neq 0$$

$$x_1=-\frac{b}{4a}+\frac{1}{2}\sqrt{\frac{b^2}{4a^2}-\frac{2c}{3a}+\frac{\sqrt[3]{2}(c^2-3bd+12ae)}{3a\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+27b^2e-72ace)^2}}}+\frac{\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+27b^2e-72ace)^2}}}{3\sqrt[3]{2}a}}-\frac{1}{2}\sqrt{\frac{b^2}{2a^2}-\frac{4c}{3a}-\frac{\sqrt[3]{2}(c^2-3bd+12ae)}{3a\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+}}}}$$

$$x_2=-\frac{b}{4a}+\frac{1}{2}\sqrt{\frac{b^2}{4a^2}-\frac{2c}{3a}+\frac{\sqrt[3]{2}(c^2-3bd+12ae)}{3a\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+27b^2e-72ace)^2}}}+\frac{\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+27b^2e-72ace)^2}}}{3\sqrt[3]{2}a}}+\frac{1}{2}\sqrt{\frac{b^2}{2a^2}-\frac{4c}{3a}-\frac{\sqrt[3]{2}(c^2-3bd+12ae)}{3a\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+}}}}$$

$$x_3=-\frac{b}{4a}-\frac{1}{2}\sqrt{\frac{b^2}{4a^2}-\frac{2c}{3a}+\frac{\sqrt[3]{2}(c^2-3bd+12ae)}{3a\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+27b^2e-72ace)^2}}}+\frac{\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+27b^2e-72ace)^2}}}{3\sqrt[3]{2}a}}-\frac{1}{2}\sqrt{\frac{b^2}{2a^2}-\frac{4c}{3a}-\frac{\sqrt[3]{2}(c^2-3bd+12ae)}{3a\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+}}}}$$

$$x_4=-\frac{b}{4a}-\frac{1}{2}\sqrt{\frac{b^2}{4a^2}-\frac{2c}{3a}+\frac{\sqrt[3]{2}(c^2-3bd+12ae)}{3a\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+27b^2e-72ace)^2}}}+\frac{\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+27b^2e-72ace)^2}}}{3\sqrt[3]{2}a}}+\frac{1}{2}\sqrt{\frac{b^2}{2a^2}-\frac{4c}{3a}-\frac{\sqrt[3]{2}(c^2-3bd+12ae)}{3a\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+}}}}$$

$$\Delta=256a^3e^3-192a^2bde^2-128a^2c^2e^2+144a^2cd^2e-27a^2d^4+144ab^2ce^2-6ab^2d^2e-80abc^2de+18abcd^3+16ac^4e-4ac^3d^2-27b^4e^2+18b^3cde-4b^3d^3-4b^2c^3e+b^2c^2d^2$$

$$ax^4+bx^3+cx^2+dx+e=0,a\neq 0$$

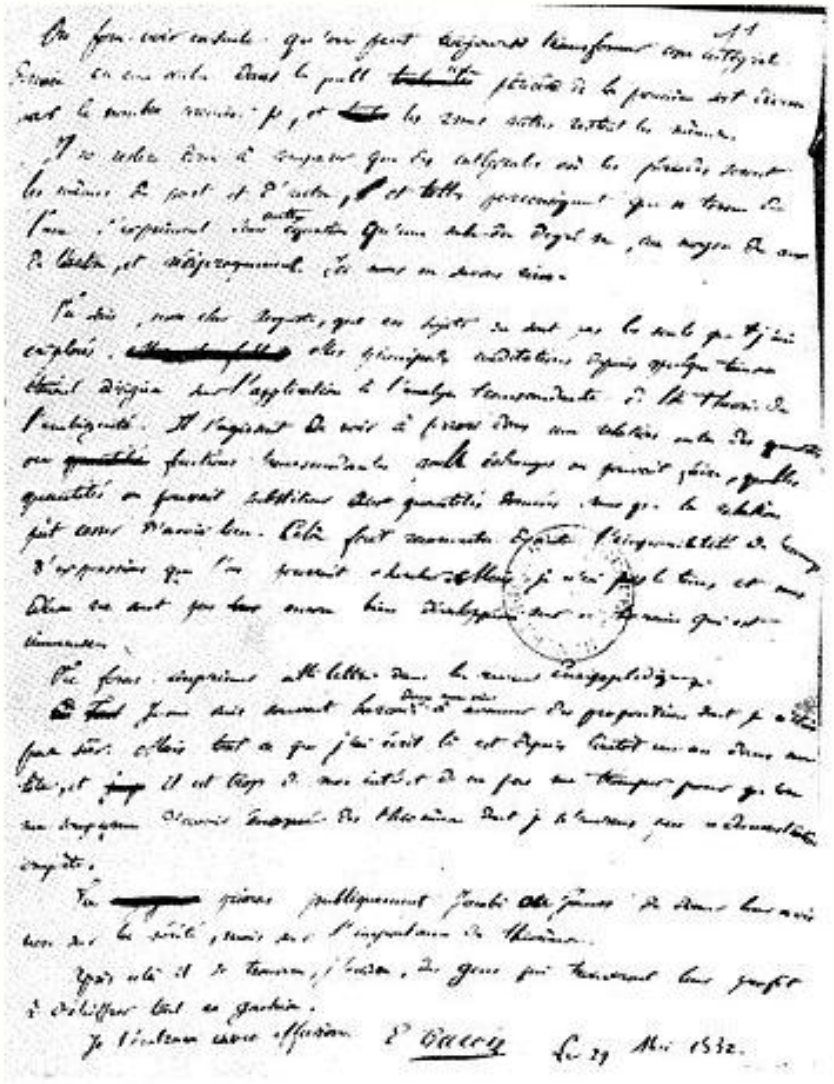
$$x_1=-\frac{b}{4a}+\frac{1}{2}\sqrt{\frac{b^2}{4a^2}-\frac{2c}{3a}+\frac{\sqrt[3]{2}(c^2-3bd+12ae)}{3a\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+27b^2e-72ace)^2}}}+\frac{\sqrt[3]{2c}}{}}$$

$$x_2=-\frac{b}{4a}+\frac{1}{2}\sqrt{\frac{b^2}{4a^2}-\frac{2c}{3a}+\frac{\sqrt[3]{2}(c^2-3bd+12ae)}{3a\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+27b^2e-72ace)^2}}}+\frac{\sqrt[3]{2c}}{}}$$

$$x_3=-\frac{b}{4a}-\frac{1}{2}\sqrt{\frac{b^2}{4a^2}-\frac{2c}{3a}+\frac{\sqrt[3]{2}(c^2-3bd+12ae)}{3a\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+27b^2e-72ace)^2}}}+\frac{\sqrt[3]{2c}}{}}$$

$$x_4=-\frac{b}{4a}-\frac{1}{2}\sqrt{\frac{b^2}{4a^2}-\frac{2c}{3a}+\frac{\sqrt[3]{2}(c^2-3bd+12ae)}{3a\sqrt[3]{2c^3-9bcd+27ad^2+27b^2e-72ace+\sqrt{-4(c^2-3bd+12ae)^3+(2c^3-9bcd+27ad^2+27b^2e-72ace)^2}}}+\frac{\sqrt[3]{2c}}{}}$$

$$\Delta=256a^3e^3-192a^2bde^2-128a^2c^2e^2+144a^2cd^2e-27a^2d^4+144ab^2ce^2-6ab^2d^2e-80abc^2de+18abcd^3+16ac^4e-4ac^3d^2-27b^4$$



The last page of Galois' letter to a friend on the eve of the duel

伽罗瓦理论的核心思想

伽罗瓦将每个方程对应于一个域，即含有方程全部根的域(现在称之为方程的伽罗瓦域)，这个域又对应一个群，即这个方程的伽罗瓦群．这样，他就把代数方程可解性问题转化为与方程相关的置换群及其子群性质的分析问题．这是伽罗瓦工作的重大突破．

伽罗瓦非常彻底地把全部代数方程可解性问题，转化或归结为置换群及其子群结构分析的问题

伽罗瓦群理论被公认为十九世纪最杰出的数学成就之一。

最重要的是，群论开辟了全新的研究领域，以结构研究代替计算，把从偏重计算研究的思维方式转变为用结构观念研究的思维方式，并把数学运算归类，使群论迅速发展成为一门崭新的数学分支，对近世代数的形成和发展产生了巨大影响。同时这种理论对于物理学、化学的发展，甚至对于二十世纪结构主义哲学的产生和发展都发生了巨大的影响。

群的应用

→物理、化学、计算机科学（逻辑/语义、密码学、通信编码、数据表示、计数）

确定Ramsey数是著名的组合数学难题之一，不仅具有重大的理论意义，而且在计算机科学，通信、管理决策等许多领域有实际应用。

著名数学家G. C. Rota曾说过：如果别人问我们，组合数学中最精彩的东西是什么？那么大多数组合数学家都会说是Ramsey数问题。

应用数论、群论、组合数学、图论中的一系列概念和方法，创新算法，优化程序设计，通过计算机的大量计算寻找更好的结果：

具体应用了数论中的同余与同余方程求解、剩余系的构造、原根、指数与标数、勒让德符号、高斯二次互反律、有限域等方法，应用了群论中的循环群、陪集和商群、同构与自同构、线性变换与等价类、群的可迁性与本原性等方法，组合数学中的集合的分拆、组合计数、容斥原理等方法，图论中的图的同构、完全图的分拆、边的着色、导出子图、独立集、团数与独立数、顶点的度、顶点可迁与边可迁、图的连通性、路、链等方法。

——罗海鹏等，Ramsey数研究又获新成果

Aliens invade the earth and threaten to obliterate it in a year's time unless human beings can find the Ramsey number for red five and blue five. We could marshal the world's best minds and fastest computers, and within a year we could probably calculate the value. If the aliens demanded the Ramsey number for red six and blue six, however, we would have no choice but to launch a preemptive attack.

——Paul Erdős

群的应用

→物理、化学、计算机科学（逻辑/语义、密码学、通信编码、数据表示、计数）

Elliptic curve cryptography

From Wikipedia, the free encyclopedia

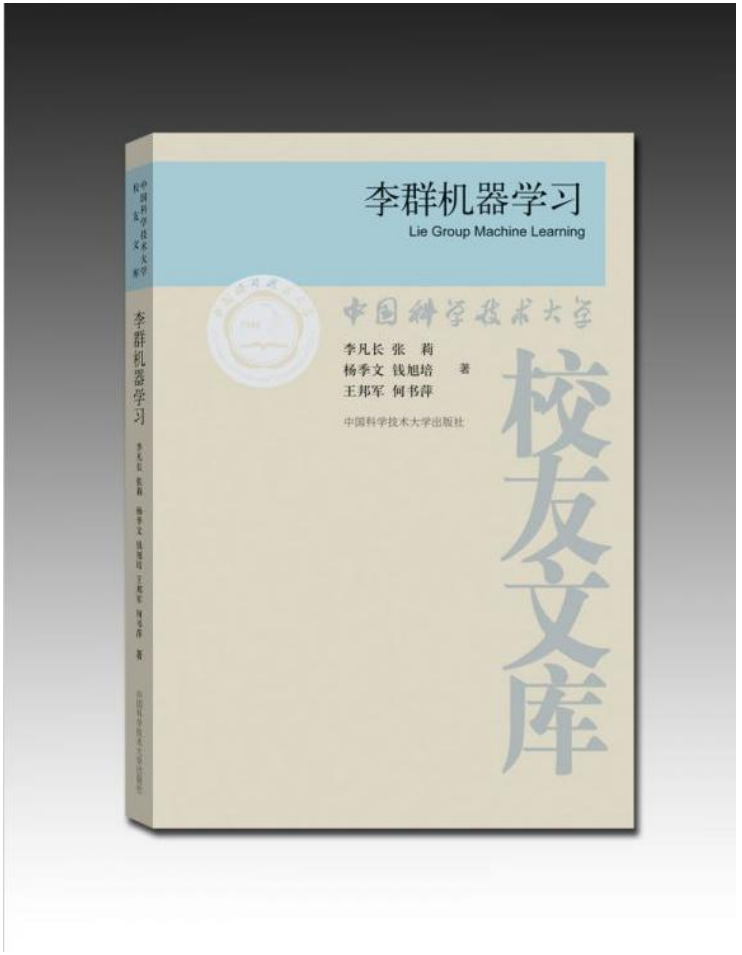
Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization.

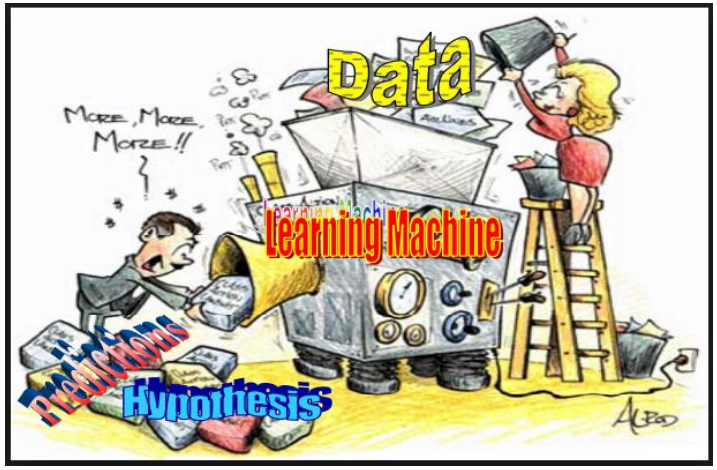
The use of elliptic curves in cryptography was suggested independently by Neal Koblitz[1] and Victor S. Miller[2] in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005.

当今计算机科学界的最权威人士很多都是研究组合数学出身的。美国最重要的计算机科学系（MIT，Princeton，Stanford，Harvard，Yale，....）都有第一流的组合数学家。计算机科学通过对软件产业的促进，带来了巨大的效益，这已是不争之事实。组合数学在国外早已成为十分重要的学科，甚至可以说是计算机科学的基础。一些大公司，如IBM，AT&T都有全世界最强的组合研究中心。Microsoft 的Bill Gates近来也在提倡和支持计算机科学的基础研究。例如，Bell实验室的有关线性规划算法的实现，以及有关计算机网络的算法，由于有明显的商业价值，显然是没有对外公开的。美国已经有一种趋势，就是与新的算法有关的软件是可以申请专利的。如果照这种趋势发展，世界各国对组合数学和计算机算法的投入和竞争必然日趋激烈。美国政府也成立了离散数学及理论计算机科学中心DIMACS（与Princeton大学，Rutgers大学，AT&T 联合创办的，设在Rutgers大学），该中心已是组合数学理论计算机科学的重要研究阵地。美国国家数学科学研究所（Mathematical Sciences Research Institute，由陈省身先生创立）在1997年选择了组合数学作为研究专题，组织了为期一年的研究活动。日本的NEC公司还在美国的设立了研究中心，理论计算机科学和组合数学已是他们重要的研究课题，该中心主任R. Tarjan即是组合数学的权威。美国重要的国家实际室（Los Alamos国家实验室，以造出第一颗原子弹著称于世），从曼哈顿计划以来一直重视应用数学的研究，包括组合数学的研究。所接触到的有关组合数学的计算机模拟项目经费达三千万美元。不仅如此，该实验室最近还在积极充实组合数学方面的研究实力。美国另外一个重要的国家实验室Sandia国家实验室有一个专门研究组合数学和计算机科学的机构，主要从事组合编码理论和密码学的研究，在美国政府以及国际学术界都具有很高的地位。由于生物学中的DNA的结构和生物现象与组合数学有密切的联系，各国对生物信息学的研究都很重视，这也是组合数学可以发挥作用的一个重要领域。前不久召开的北京香山会议就体现了国家对生物信息学的高度重视。

美国的大学，国家研究机构，工业界，军方和情报部门都有许多组合数学的研究中心，在研究上投入了大量的经费。但他们得到的收益远远超过了他们的投入，更主要的是他们还聚集了组合数学领域全世界最优秀的人才。高层次的软件产品处处用到组合数学，更确切地说就是组合算法。


Machine Learning


李群机器学习
Lie Group Machine Learning
中国科学技术大学
李凡长 张 莉
杨季文 钱旭培 著
王邦军 何书萍
中国科学技术大学出版社
校友文库


Data
More, More, More!!
Learning Machine
Predictions
Hypothesis

群与组合计数

→物理

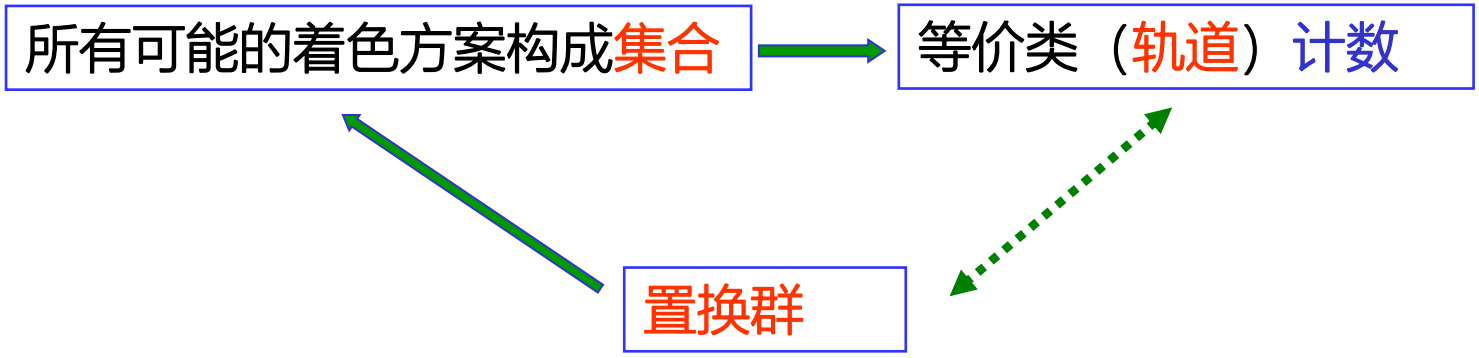
→化学

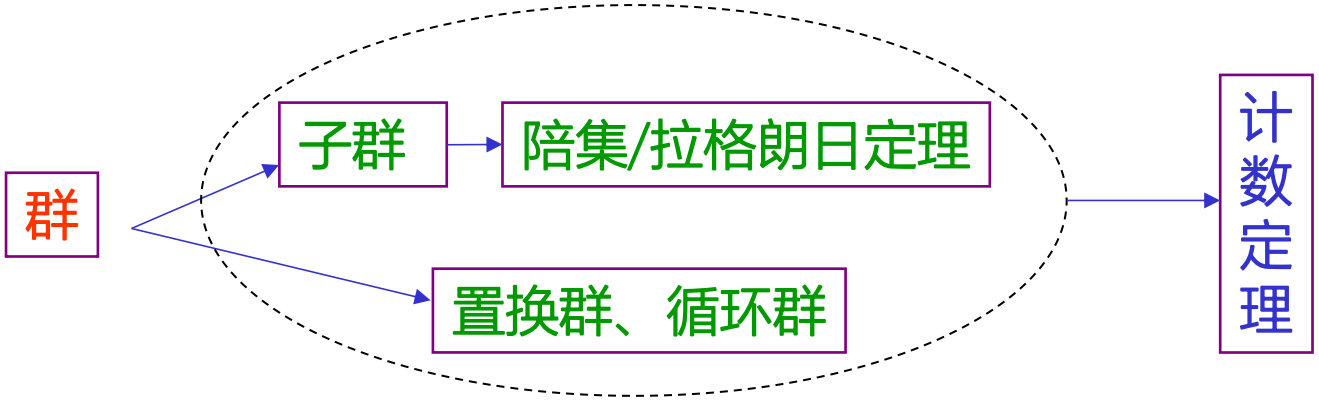
→计算机科学（逻辑/语义、密码学、通信编码、数据表示、计数）

以人造卫星仪器舱布局为例，如何求解全局最优的一种布局方案?

可以应用图论、群对集合的作用、轨道与等价关系等刻划各种布局方案的同构、等价类等内在性质，从而在此基础上找出一种全局优化算法。

→简化为着色问题


所有可能的着色方案构成集合
等价类（轨道）计数
置换群


群
子群
陪集/拉格朗日定理
置换群、循环群
计数定理

主要内容

1 群（群性质、子群、置换群、拉格朗日定理）

2 群同态定理（正规子群、商群）

2.1 群及其基本性质

2.2 群的元素阶

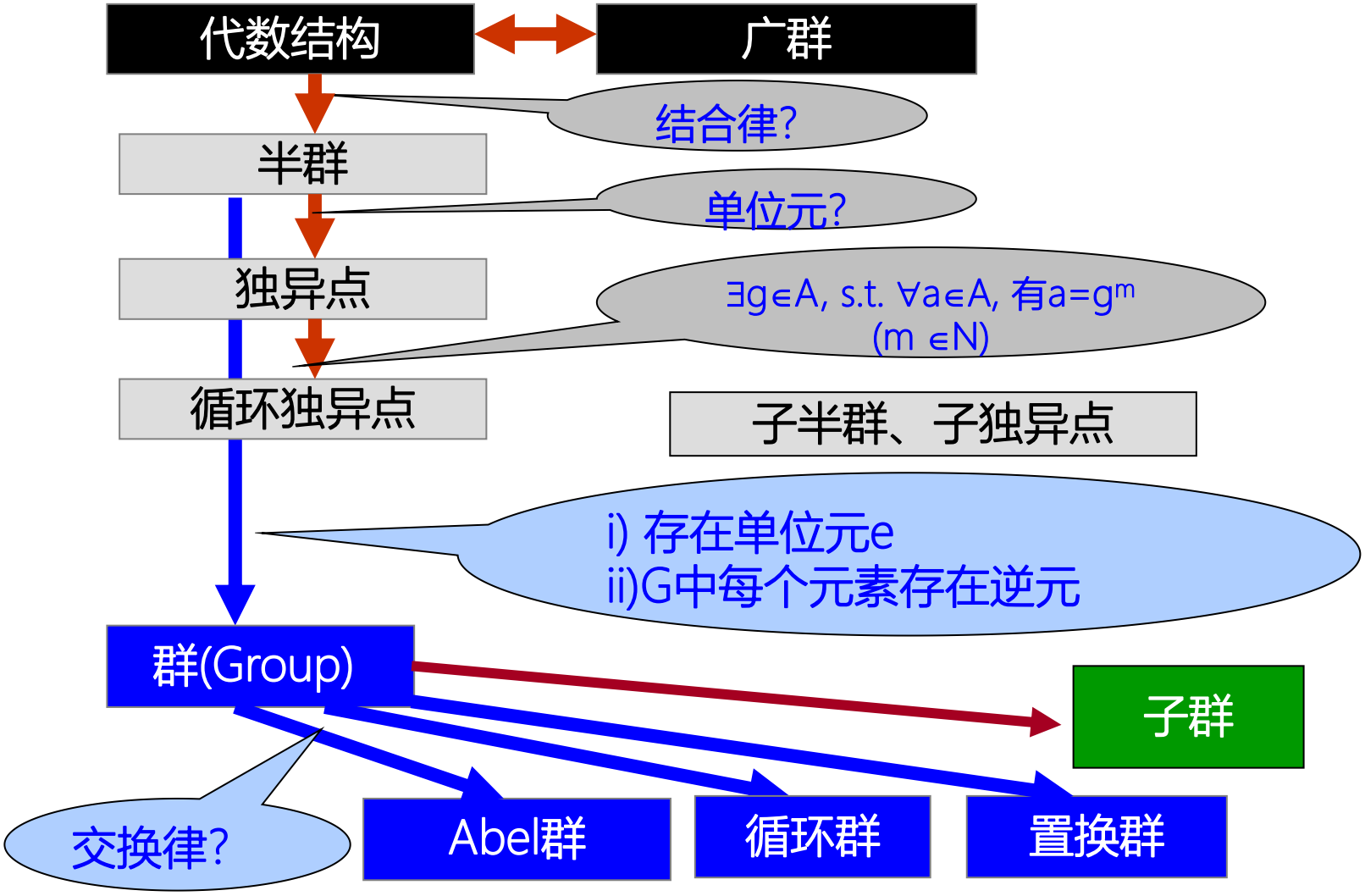
2.3 子群

2.4 置换群

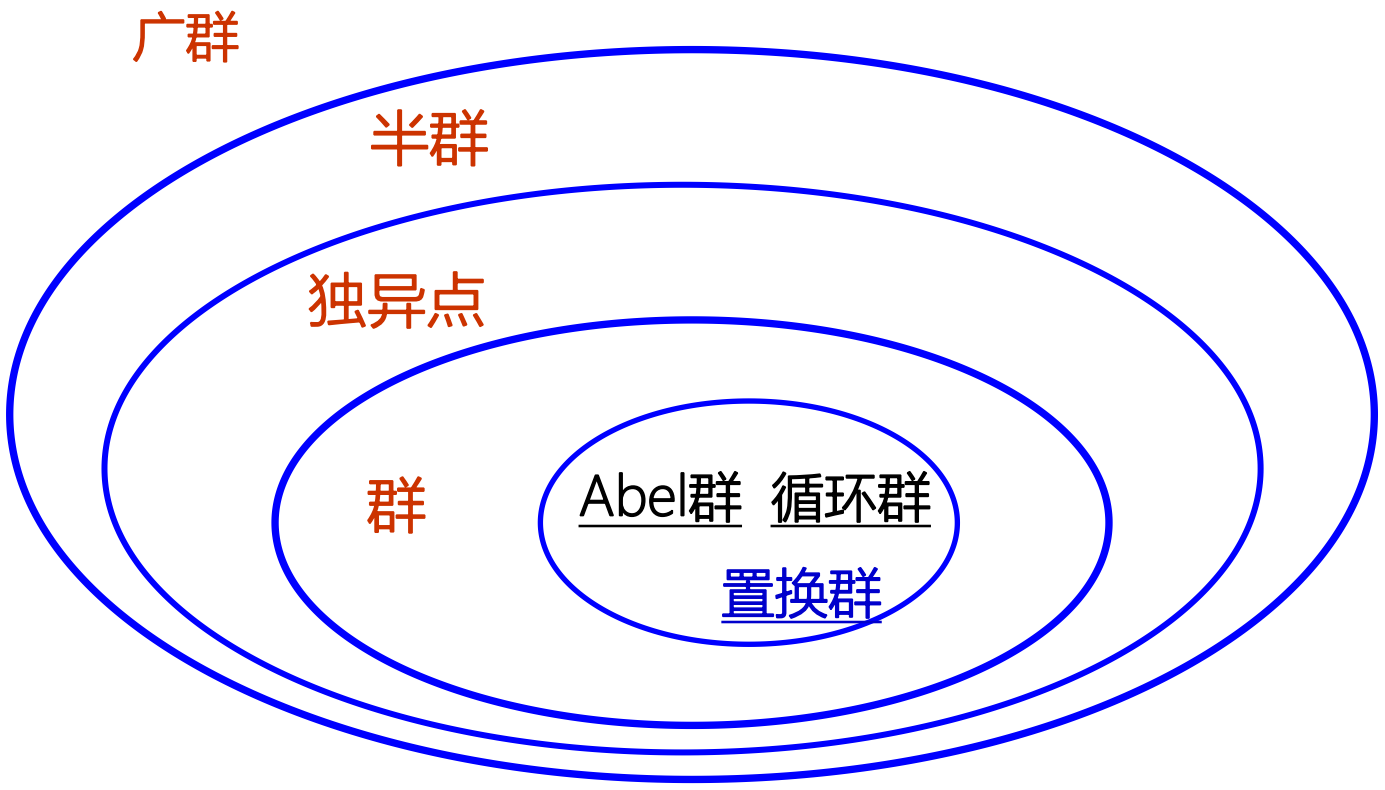
2.5 循环群

2.4 陪集与拉格朗日定理

2.5 正规子群与群同态基本定理


代数结构
广群
结合律?
半群
单位元?
独异点
∃g∈A, s.t. ∀a∈A, 有a=g^m
(m ∈N)
循环独异点
子半群、子独异点
i) 存在单位元e
ii)G中每个元素存在逆元
群(Group)
子群
交换律?
Abel群
循环群
置换群

上述代数结构之间的关系



请思考

1 群有无零元？独异点中的幂等元唯一吗？群中呢？

2 设A是非空集合，所有A上的双射所构成的集合在函数的复合运算下是否构成群？

示例

某通讯编码由4个数据位x1、x2、x3、x4和3位校验位x5、x7、x8构成，它们的关系如下：

$x5=x1\oplus x2\oplus x3$

$x6=x1\oplus x2\oplus x4$

$x7=x1\oplus x3\oplus x4$

其中，$\oplus$为异或运算。若S为满足上述关系的码字的集合，且当$x,y \in S$时有$x\oplus y=(x1\oplus y1,\ldots,x7\oplus y7)$。

则，$<S;\oplus>$是群，试证明之。

性质1 可约性

群<G;*>适合消去律,即对于任意a,b,c∈G，则有：

(1) 若a*b=a*c 则b=c;

(2) 若b*a=c*a 则b=c。

性质2

设<G;*>是一个群,对于任意的a,b∈G. 有：

(1) 存在唯一元素 x∈G，使得a*x=b;

(2) 存在唯一元素 y∈G，使得y*a=b。

性质3

如果〈G；*〉是一个群，对于任意的a，b∈G. 则有

$(a*b)^{-1}=b^{-1}*a^{-1}$

思考1 单位元是群中唯一的幂等元

思考2 试证明如下命题

群〈G; *〉的运算表中的每一行或每一列是G中元素的置换。

(有限集合s到s的一个双射，称为s的一个置换)

思考3 “不存在有零元的群”

思考4

① 一阶群仅有1个

② 二阶群仅有1个

③ 三阶群仅有1个

④ 四阶群仅有2个

*	e
e	e

*	e	a
e	e	a
a	a	e

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

示例

设〈G；*〉是一个群，则〈G；*〉是阿贝尔(Abel)群的充要条件为：

$$\forall a,b\in G,\text{有}(a*b)*(a*b)=(a*a)*(b*b)$$

示例

1 设<M;o>是半群，若∀ a,b∈ M，方程aox=b，yoa=b有解，则称<M;o>是可解的，请证明：此可解半群是群。

2 证明：有限半群G是群的充要条件是，G中消去律成立。

3 证明： 半群<G;o>是群的充要条件是满足如下两个条件：

1) G中有左单位元e_L;

2) 对∀a∈G,有元素a'∈G,使得a'oa=e_L.

群中元素的周期(阶,Order)? $|a|$

——有限阶、无限阶。

示例

(1) 群的单位元e的阶为1,

(2) <I; +>中除0外,其余元素的阶为无限阶

性质

设a是群〈G；*〉中的一个周期为r的元素，k是一个整数，则有

(1) $a^k=e$当且仅当k为r的倍数。

(2) a与a^{-1}的周期相同。

(3) r小于或等于群〈G；*〉中元素的个数。

请你思考

在有限群<G,*>中,每一元素具有有限阶,且阶数至多为|G|.

证:

$\forall a \in G$,则在序列$a, a^2, a^3, \ldots, a^{|G|+1}$中至少有两个元素相同,不妨设$a^r = a^s$ $(1 \le s < r \le |G|+1)$

于是，$a^{r-s} = e$

所以，元素a的阶数至多为$r-s \le |G|$。

若元素$a \in G$，$|a|=|G|$，则G中元素可否列举出来?

示例

证明：若群G中元素a的阶是n，则H ={a^0,a^1,a^2,...,a^{n-1}}为群。

示例

若群G中元素a，b的阶分别是n，m，则

1)对任意正整数k，$|a^k|=n/(n, k)$，(n, k)为n, k的最大公因数。

2)若ab=ba，且(n, m)=1，则|ab|=nm。

1 什么是子群(Subgroup)？真子群、平凡子群

2 关于子群元素

(1)子群的单位元　(2)子群元素的逆元

示例

a)<{3n|n∈I},+>是<I; +>的子群,I为整数集

b)<N; +>不是<I,+>的子群, N是自然数集

c)<{0,3}; $+_6$>是<N_6; $+_6$>的子群

d)一个群能同构于其真子群吗?

3 子群判定

判定定理

1 群G的非空子集H是G的子群的充要条件是：

$$\forall a,b\in H，有 ab^{-1}\in H.$$

2 群G的非空有限子集H是G的子群的充要条件是：

$$\forall a,b\in H，有 ab\in H.$$

分析：显然，封闭性、结合律是成立的，需要证明逆元存在性、单位元存在性：

设<G;*>的单位元为e.对$\forall a \in H$,

i)若a=e，即$a=e \in H$，此a的逆元为$a \in H$.

ii)若$a \neq e$,由题设有$a, a^2, \ldots, a^n, a^{n+1}, \ldots \in H$，

而H有限，故必$\exists i,j \in Z^+$，$j>i$,有 $a^i=a^j$,

于是可以进一步得到：$a^{j-i}=e$,即$a^* a^{j-i-1}=e$

显然，$j-i>1$（否则，若$j-i=1$,则$a^{j-i}=a=e$，矛盾）。

则(1) $a^{j-i} \in H$，即$e \in H$;(2)$a^{j-i-1} \in H$,即为a的逆元；

于是，综合i)、ii)可知，H中存在单位元，且对$\forall a \in H$,其逆元存在且在H中.

所以，<H,*>是<G,*>的子群

思考与练习

1 <G,*>是群,有G之非空子集T,若$\forall a,b\in T$,有$a*b\in T, a^{-1}\in T$, 则<T,*>是<G,*>的子群.

证:下面按照定义进行证明

a) 运算封闭：$\forall a,b\in T$，由前提，$a*b\in T$

b) 结合律：继承成立

c) 单位元：$\forall a\in T, a^{-1}\in T$,于是$a*a^{-1}\in T$，即$e\in T$

d) 逆元存在：$\forall a\in T$，有$a^{-1}\in T$

所以，<T,*>是群,

从而 <T,*>是<G,*>的子群

2 <G;*>是Abel群,<A;*>、<B;*>是其子群, 设AB={a*b|a∈A,b∈B}, 则:<AB;*>亦为<G;*>之子群.

3 设H={a+b*$2^{1/2}$|a,b∈Q,但a,b不同时为0},试证:<H,×>是<R-{0}, ×>的子群.

4 设<G，*>是群，若H⊆G,∀a,b∈H⇒a^{-1}*b∈H,则<H,*>是<G,*>的子群.

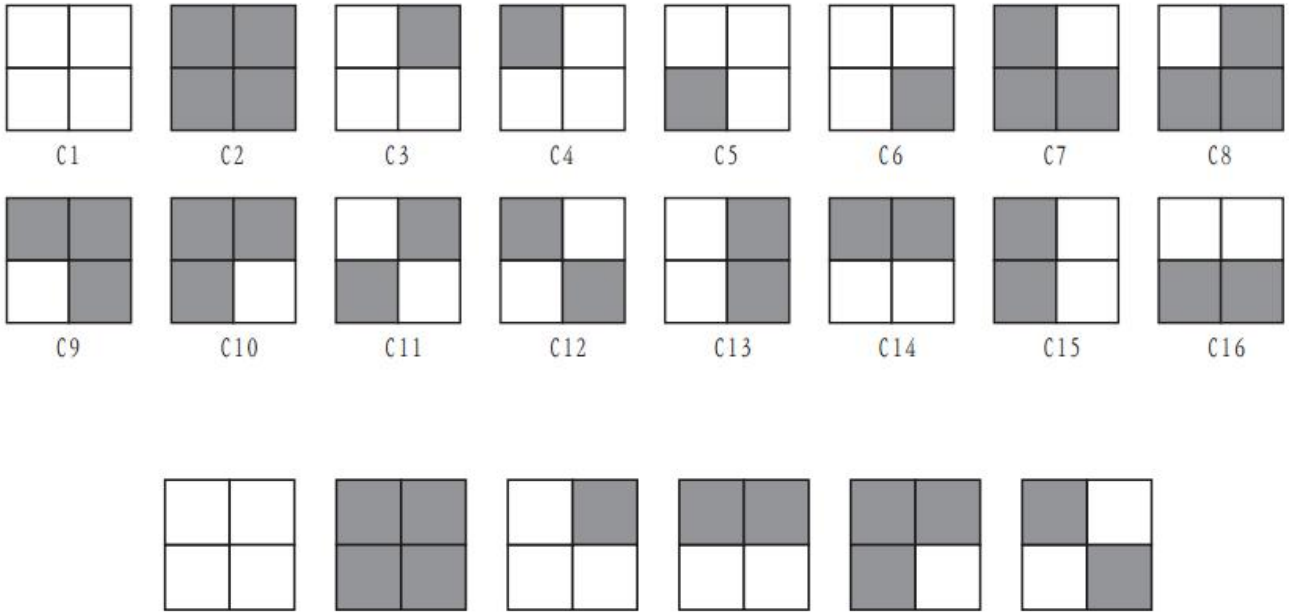
5 设f、g是从群<A;*>到群<B;o>的同态，C={x|x∈A且f(x)=g(x)},请证明：<C;*>是<A;*>的子群.

6 有限群G的非空子集H是G的子群的充要条件是：∀a,b∈H，有ab∈H.

7 阅读教材例题8.8，8.9

图着色计数问题

对2 × 2的方阵用黑白两种颜色涂色， 问能得到多少种不同的图像？ 经过顺时针旋转使之吻合的两种方案， 算是同一种方案。



着色方案计数问题

给出一个有p个元素的集合S， 用k种颜色给这些元素染色， 求本质不同的方案个数。 为了定义 “本质不同” 的含义， 需要给出一个关于这p个元素的置换群G， 对于G中的任意置换f ， 每个方案a和它在f 作用下的结果被看成是本质相同的。

“本质相同”关系是一个等价关系， 因此该关系把着色方案分成了若干个等价类， 目的就是要计算出等价类的数目。

图着色计数问题

变换

→满射、单射、双射变换

→变换群(Transformation Group)

有限集合上的双射变换?

$$\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ \varphi(1) & \varphi(2) & \dots & \varphi(n) \end{pmatrix}$$

置换

→n次置换

对称群，n次对称群，置换群(Permutation Group)

示例 置换及置换乘法

集合X={1，2，3, 4}，共有4！=24个4次置换

$$P_1=\begin{pmatrix}1234\\4123\end{pmatrix},\ P_2=\begin{pmatrix}1234\\3412\end{pmatrix},\ P_3=\begin{pmatrix}1234\\2143\end{pmatrix}$$

$$P_1^2=\begin{pmatrix}1234\\4123\end{pmatrix}\begin{pmatrix}1234\\4123\end{pmatrix}=P_2,$$

$$P_1P_3=\begin{pmatrix}1234\\4123\end{pmatrix}\begin{pmatrix}1234\\2143\end{pmatrix}=\begin{pmatrix}1234\\1432\end{pmatrix}$$

示例 轮换

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{m-1} & a_m & a_{m+1} & \cdots & a_n \\ a_2 & a_3 & \cdots & a_m & a_1 & a_{m+1} & \cdots & a_n \end{pmatrix}$$

$$P_1=\begin{pmatrix}1234\\4123\end{pmatrix},\ P_2=\begin{pmatrix}1234\\3412\end{pmatrix},\ P_3=\begin{pmatrix}1234\\2143\end{pmatrix}\qquad P_1P_3=\begin{pmatrix}1234\\1432\end{pmatrix}$$

P_1 =(2143), P_2 =(13)(24), P_3 =(12)(34), P_1P_3=(1)(24)(3)

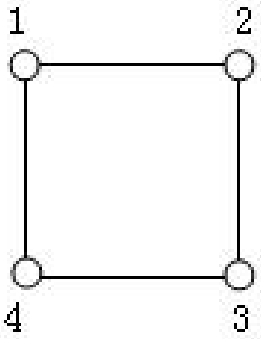
对称群、置换群

对称群：非空集合X上的全体双射变换构成的集合S(X)关于双射变换的乘法构成一个群.

→ X上的n次对称群(Symmetric group), n=|X|, S_n).

→ S_n的任意一个子群，称为一个X上的n次置换群，简称X上的置换群(Permutation group).

示例 小球着色问题中，设每一个填置到正方形的顶点上的小球都着不同的颜色（不妨分别标记为1,2,3,4），试求出其旋转构成的置换群。



小球着色

旋转变换

	1	2	3	4
e	1	2	3	4
r	2	3	4	1
r^2	3	4	1	2
r^3	4	1	2	3
h	4	3	2	1
v	2	1	4	3
d	1	4	3	2
f	3	2	1	4

运算表

o	e	r	r^2	r^3	h	v	d	f
e	e	r	r^2	r^3	h	v	d	f
r	r	r^2	r^3	e	f	d	h	v
r^2	r^2	r^3	e	r	v	h	f	d
r^3	r^3	e	r	r^2	d	f	v	h
h	h	d	v	f	e	r^2	r^3	r
v	v	f	h	d	r^3	e	r	r^2
d	d	v	f	h	r	r^3	e	r^2
f	f	h	d	v	r^3	r	r^2	e

(Cayley定理) 任意一个群都同一个双射变换群同构。

群 ⟷ 置换群

证明 设G是任意一个给定的群，任取$a\in G$，对$\forall x\in G$令

$$f_a(x)=ax,$$

则易知f_a是G的一个双射变换。

$S(G)$为G的对称群，令$G'=\{f_a|a\in G\}\subseteq S(G)$ 。

现任取$f_a, f_b\in G'$,则

$$f_af_b(x)=fa(bx)=a(bx)=abx=f_{ab}(x),$$

$\forall x\in G$, $f_b^{-1}(x)=b^{-1}x=f_{b^{-1}}(x)$,

即有$f_af_b=f_{ab}\in G'$, $f_b^{-1}=f_{b^{-1}}\in G'$,

从而$f_a f_b^{-1}=f_a f_{b^{-1}}=f_{ab^{-1}}\in G'$，从而$G'$是$S(G)$的子群，是一个双射变换群。

又令$\varphi: G\to G'$，使对$\forall a\in G$，有$\varphi(a)=f_a$。

显然，φ是一个双射。 且对$\forall a, b\in G$,

$$\varphi(ab)=f_{ab}=f_af_b=\varphi(a)\varphi(b),$$

即映射满足保运算性。

故群G与一个双射变换群G'同构。

每一个有限群均与一个置换群同构。

置换群G作用在集合X上

→ **等价划分**： G可以诱导出X上的一个等价关系R:

$\forall x \forall y(xRy \leftrightarrow \exists g(g \in G, g(x)=y))$

→ X在G作用下的一个**轨道**(Orbit)：$[x]_R=\{g(x)|g \in G\}$, 记为：$\Omega(x)$

→a为g的一个**不动点**(Fixed Element): 设$g \in G$，$a \in X$，若$g(a) = a$.

$Fix_X(g)=\{a|a \in X, g(a)=a\}$ ？

即在g作用下所有的不动点集合。

→ G中使x保持不动的**不动置换类**: 以x为不动点的群G的所有元素的集合，即$\{g|g \in G, g(x)=x\}$，简记为$Fix_G(x)$。

不动点定理 [编辑]

维基百科，自由的百科全书

在数学中，**不动点定理**是一个结果表示函数*f*在某种特定情况下，至少有一个不动点存在，即至少有一个点*x*能令函数$F(x) = x$。

在数学中有很多定理能保证函数在一定的条件下必定有一个或更多的不动点，而在这些最基本的定性结果当中存在不动点及其定理被应用的结果具有非常普遍的价值。

目录 [隐藏]

分析领域 [编辑]

在巴拿赫不动点定理中给出了一般准则：如果满足该准则，保证迭代函数程序可以产生一个固定点。

布劳尔不动点定理的结果说：任何封闭单位球的连续函数在n维欧几里德空间本身必须有一个不动点，但它并没有说明如何找到不动点（见：斯苯纳引理）。

例如，余弦函数在[−1, 1]区间连续和画入[−1, 1]区间，故须一个不动点。描绘余弦函数图时这是清楚的；该不动点发生在余弦曲线 $y = \cos(x)$ 与直线 $y = x$ 交点上。在数值上，不动点是 $x = 0.73908513321516$。

代数拓扑的莱夫谢茨不动点定理（和尼尔森不动点定理）值得注意，它在某种意义上给出了一种计算不动点的方法。存在对博拉奇空间的概括和一般化，适用于偏微分方程理论。见：无限维空间的不动点定理。

分形压缩的拼贴定理证明，对许多图像存在一个相对较小函数的描述，当迭代适用于任何起始分形可迅速收敛在理想分形上。

离散数学和理论计算机科学领域 [编辑]

克纳斯特－塔斯基定理某种程度上从分析移除，而且不涉及连续函数。它指出在完全格上的任何次序保持函数都有一个不动点，甚至是一个最小不动点。见布尔巴基－维特定理。

λ演算的共同主题是找到给出λ表达式的不动点。每个λ表达式都有一个不动点，不动点组合子是一个“函数”，即输入一个λ表达式并输出该表达式的一个不动点。一个重要的不动点组合是Y组合子，它使用递归定义。

在程序语言的指称语义，一个克纳斯特－塔斯基定理的特例用于建立递归定义的语义。不动点定理虽然适用于“相同”函数（从逻辑的角度来看），但其理论发展完全不同。

递归函数的相同定义可用克莱尼递归定理在可计算性理论中给出。这些结果并不是等价的定理，克拉斯特尔－塔斯基定理是个比那用于指称语义的更强的结果。[1]然而，它却与丘奇－图灵论题的直观含义相同：一个递归函数可描述为特定泛函的最小不动点，将函数映射至函数。

迭代函数找不动点的技术还可用在集理论；正常函数的定点引理指出任何严格递增的函数从序到序有一个（甚至有许多）不动点。

在偏序集上的每个闭包算子都有许多不动点；存在关于闭包算子的“封闭要素”，它们是闭包算子首先被定义的主要理由。

In algebra and discrete mathematics [edit]

The Knaster–Tarski theorem states that any order-preserving function on a complete lattice has a fixed point, and indeed a *smallest* fixed point. See also Bourbaki–Witt theorem.

The theorem has applications in abstract interpretation, a form of static program analysis.

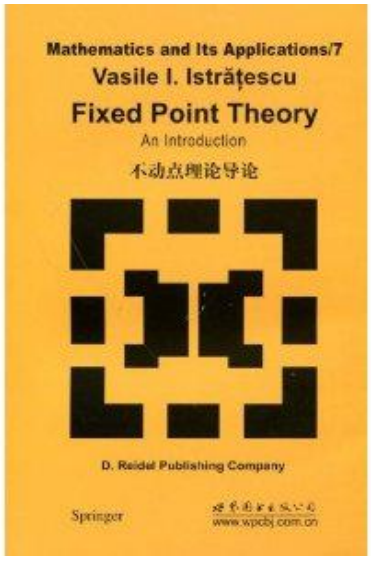
A common theme in lambda calculus is to find fixed points of given lambda expressions. Every lambda expression has a fixed point, and a fixed-point combinator is a "function" which takes as input a lambda expression and produces as output a fixed point of that expression. An important fixed-point combinator is the Y combinator used to give recursive definitions.

In denotational semantics of programming languages, a special case of the Knaster–Tarski theorem is used to establish the semantics of recursive definitions. While the fixed-point theorem is applied to the "same" function (from a logical point of view), the development of the theory is quite different.

The same definition of recursive function can be given, in computability theory, by applying Kleene's recursion theorem. These results are not equivalent theorems; the Knaster–Tarski theorem is a much stronger result than what is used in denotational semantics.[1] However, in light of the Church–Turing thesis their intuitive meaning is the same: a recursive function can be described as the least fixed point of a certain functional, mapping functions to functions.

The above technique of iterating a function to find a fixed point can also be used in set theory; the fixed-point lemma for normal functions states that any continuous strictly increasing function from ordinals to ordinals has one (and indeed many) fixed points.

Every closure operator on a poset has many fixed points; these are the "closed elements" with respect to the closure operator, and they are the main reason the closure operator was defined in the first place.



2 在经济中的应用

在经济中的应用

一般经济均衡理论是数理经济学的中心论题，其问题的提出可追溯到Adam Smith[1]于1776年在他的名著《国富论》中写下的那段名言：

“每人都在力图应用他的资本，来使其生产品能得到最大的价值。一般地说，他并不企图增进公共福利，也不知道他所增进的公共福利为多少。他所追求的仅仅是他个人的安乐，仅仅是他个人的利益。在这样做时，有一只看不见的手引导他去促进一种目标，而这种目标决不是他所追求的东西。由于追求他自己的利益，他经常促进了社会利益，其效果要比他真正想促进社会利益时所得到的效果为大。”

Adam Smith在这里提出一个意义十分深远的问题：假设有一个包含许许多多小系统的大系统，大系统有其总目标，小系统也各有各的小目标。那么，是否可能存在一只“看不见的手”来对各小系统进行引导，使得每个小系统都只需追求各自的小目标最优，就能使大系统的总目标达到最优。

很明显，这样的问题在社会科学与自然科学的许多地方都会遇到。但是，Adam Smith本人并未对问题作这样的理解，更没有把问题表达成一种数学的形式。

直到1954年, Arrow和Debreu[2,3]在一些具有明确经济学意义的假设条件下, 用数学公理化方法深刻表述该问题, 利用Brouwer不动点定理和Kakutani不动点定理, 严格证明了Walras经济的一般均衡的存在性和最优性, 使得那只"看不见的手"成为缜密的科学体系, 使得经济学形成了一个统一的方法论和分析框架. 他们分别于1972年和1983年获得了经济学Nobel奖.

经济中的应用

近些年来, 经济形势发生了深刻的变化, 生产规模扩大, 垄断势力增强, 人们要谈判、合作、讨价还价, 但所有这一切都建立在个人理性的基础之上, 建立在竞争的基础之上. 随着这种竞争的日益加剧, 各种策略和利益的对抗、依存和制约, 使博弈论(主要是非合作博弈, 而非合作博弈理论中最重要、最核心的概念是Nash均衡)达到了全盛时期, 由它的概念、内容思想和方法出发, 已经并将继续几乎全面地改写经济学, 也并将得到更加广泛的应用.

Von Neumann[4]就零和(所有局中人的收支和为零)的情况证明了非合作博弈均衡点的存在, 在1944年宣告了博弈论的诞生.

1950年, Nash考虑了 人非零和的情况, 他研究了 人有限非合作对策(每个局中人的纯策略均为有限个, 均考虑混合策略), 分别应用Brouwer不动点定理和Kakutani不动点定理证明了Nash均衡的存在性[5,6].这一模型实际上假定：

(1)对每个局中人来说, 所有信息都是公共的、完全的、对称的；

(2)每个局中人都是完全理性的, 都能在各自策略集中选择对自己最有利的策略.

对应用来说, 以上两个假设太理想了, 也太苛刻了, 因为它要求每个局中人都是神——无所不知且无所不能. 因此, 相当一段时间以来, 关于博弈论的研究就主要是数学家们的"专利", 大量的论文也主要发表在数学杂志上, 经济学家们并没有表现出很大的兴趣和很高的热情, 而数学家们则总在日夜辛劳, 不断地改进和推广着各种定理.

Harsanyi[7]和Selten[8]的工作分别在这两个方面提出了新的思想, 大大扩展了博弈论的应用(他们二位都是有数学背景的经济学家), 正因为如此, 他们才与Nash一起, 获得了1994年的经济学Nobel奖.

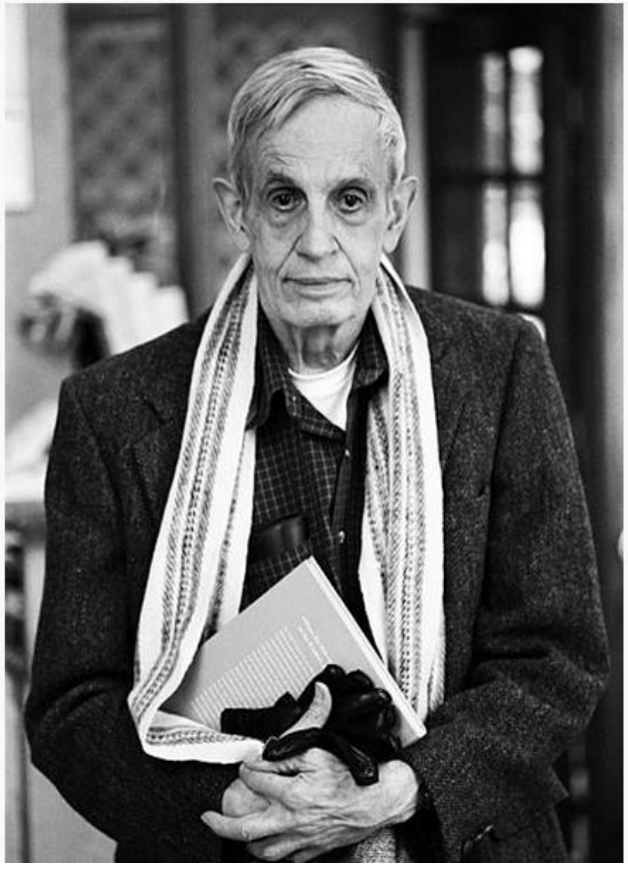
John Forbes Nash, Jr.

From Wikipedia, the free encyclopedia

John Forbes Nash, Jr. (born June 13, 1928) is an American mathematician whose works in game theory, differential geometry, and partial differential equations have provided insight into the forces that govern chance and events inside complex systems in daily life. His theories are used in market economics, computing, evolutionary biology, artificial intelligence, accounting, politics and military theory. Serving as a Senior Research Mathematician at Princeton University during the latter part of his life, he shared the 1994 Nobel Memorial Prize in Economic Sciences with game theorists Reinhard Selten and John Harsanyi.

Nash is the subject of the Hollywood movie *A Beautiful Mind*. The film, loosely based on the biography of the same name, focuses on Nash's mathematical genius and also his schizophrenia.[1][2][3]

John Forbes Nash, Jr.



Contents [hide]

As of 2011 Nash's recent work involves ventures in advanced game theory, including partial agency, which show that, as in his early career, he prefers to select his own path and problems. Between 1945 and 1996, he published 23 scientific studies.

Nash has suggested hypotheses on mental illness. He has compared not thinking in an acceptable manner, or being "insane" and not fitting into a usual social function, to being "on strike" from an economic point of view. He has advanced evolutionary psychology views about the value of human diversity and the potential benefits of apparently nonstandard behaviors or roles.[33]

Nash has developed work on the role of money in society. Within the framing theorem that people can be so controlled and motivated by money that they may not be able to reason rationally about it, he has criticized interest groups that promote quasi-doctrines based on Keynesian economics that permit manipulative short-term inflation and debt tactics that ultimately undermine currencies. He has suggested a global "industrial consumption price index" system that would support the development of more "ideal money" that people could trust rather than more unstable "bad money". He notes that some of his thinking parallels economist and political philosopher Friedrich Hayek's thinking regarding money and a nontypical viewpoint of the function of the authorities.[34][35]

Nash received an honorary degree, Doctor of Science and Technology, from Carnegie Mellon University in 1999, an honorary degree in economics from the University of Naples Federico II on March 19, 2003,[36] an honorary doctorate in economics from the University of Antwerp in April 2007, and was keynote speaker at a conference on Game Theory. He has also been a prolific guest speaker at a number of world-class events, such as the Warwick Economics Summit in 2005 held at the University of Warwick. In 2012 he became a fellow of the American Mathematical Society.[37]

A Beautiful Mind (film)

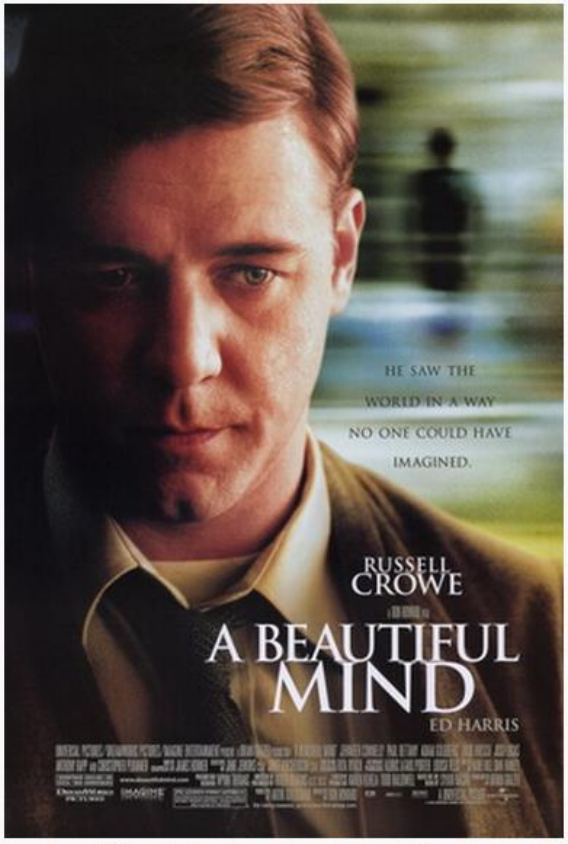
From Wikipedia, the free encyclopedia

A Beautiful Mind is a 2001 American biographical drama film based on the life of John Nash, a Nobel Laureate in Economics. The film was directed by Ron Howard, from a screenplay written by Akiva Goldsman. It was inspired by a bestselling, Pulitzer Prize-nominated 1998 book of the same name by Sylvia Nasar. The film stars Russell Crowe, along with Ed Harris, Jennifer Connelly, Paul Bettany, Adam Goldberg, Judd Hirsch, Josh Lucas, Anthony Rapp, and Christopher Plummer in supporting roles. The story begins in the early years of a young prodigy named John Nash. Early in the film, Nash begins to develop paranoid schizophrenia and endures delusional episodes while painfully watching the loss and burden his condition brings on his wife and friends.

The film opened in the United States cinemas on December 21, 2001. It went to gross over $313 million worldwide and to win four Academy Awards, for Best Picture, Best Director, Best Adapted Screenplay and Best Supporting Actress. It was also nominated for Best Actor, Best Film Editing, Best Makeup, and Best Original Score.

It was well received by critics, but has been criticized for its inaccurate portrayal of some aspects of Nash's life, especially his other family and a son born out of wedlock. However, the filmmakers have stated that the film

A Beautiful Mind



Theatrical release poster

示例 X={a,b,c,d}, G={I_s,P_1,P_2,P_3}.

$$I_s=\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix},\quad P_1=\begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix},$$

$$P_2=\begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix},\quad P_3=\begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix},$$

1) G为X上的置换群?

2) G在X上诱导出的等价关系R?

3) X在G作用下的轨道?

4) 保持X中元素不动的不动置换类?

观察

$|G|$、$|\Omega(x)|$与$|Fix_G(x)|$之间关系?

→$|G|=|\Omega(x)||Fix_G(x)|$

(群论中的Lagrange 定理)

Burnside定理

*G*是作用在有限集合X上的一个有限群，X在*G*作用下的轨道数为

$$\frac{1}{|G|}\sum_{g\in G}|Fix_X(g)|$$

证明 令 $S=\{(g,x)\mid g\in G,x\in X,且\ g(x)=x\}$。 则分别针对 $g\in G$，$x\in X$ 计数，可得

$$|S|=\sum_{g\in G}|Fix_I(g)|=\sum_{x\in I}|Fix_G(x)|,$$

进而由 $|G|=|\Omega(x)||Fix_G(x)|$ 可得，

$$|S|=\sum_{x\in I}|Fix_G(x)|=\sum_{x\in I}\frac{|G|}{|\Omega(x)|}=|G|\sum_{x\in I}\frac{1}{|\Omega(x)|},$$

又设 X 在 G 作用下有 m 条轨道，于是 $X=\Omega(x_1)\cup\Omega(x_2)\cup\cdots\cup\Omega(x_m)$，其中，$\Omega(x_i)(1\le i\le m)$ 为 x_i 所在的轨道。

$$\sum_{x\in I}\frac{1}{|\Omega(x)|}=\sum_{x_1\in\Omega(x_1)}\frac{1}{|\Omega(x_1)|}+\sum_{x_2\in\Omega(x_2)}\frac{1}{|\Omega(x_2)|}+\cdots+\sum_{x_m\in\Omega(x_m)}\frac{1}{|\Omega(x_m)|}$$

$$=1+1+\cdots+1=m$$

于是，$|S|=\sum_{g\in G}|Fix_I(g)|=\sum_{x\in I}|Fix_G(x)|=|G|\sum_{x\in I}\frac{1}{|\Omega(x)|}=|G|m,$

所以，X 在 G 作用下的轨道数 $m=\frac{1}{|G|}\sum_{g\in G}|Fix_I(g)|$。

■

显然，公式中，$\sum_{g\in G}|Fix_I(g)|$ 是比较容易求解的。

Pĺya计数原理

G是作用在集合X上的一个有限群，如果用k种颜色对X中元素着色，则本质不同的着色数为

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

其中，m(g)为<g>作用在X上的轨道数量，<g>称为循环群。

乔治·波利亚 [编辑]

乔治·波利亚（有时译作**波里亚**，名字常缩写作G. Pòlya，英语：**George Pòlya**，匈牙利语：**Pòlya György**）（1887年12月13日－1985年9月7日），犹太人，著名匈牙利裔美国数学家和数学教育家。生于匈牙利布达佩斯。1940年移居美国，历任布朗大学和斯坦福大学教授。

他在大量的数学范畴工作，包括级数、数论、组合数学和机率。1937年提出的波利亚计数定理是组合数学的重要工具。 同时，他长期从事数学教学，对数学思维的一般规律有深入的研究。

著作 [编辑]

有关解题的著作：

- 《怎样解题》(*How to Solve It*)
- 《数学与猜想》(*Mathematics and plausible reasoning*)
- 《数学发现》(*Mathematical discovery*)

其他：

- 《数学分析中的问题和定理》 (*Problems and theorems in analysis*)
- 《复变函数》 (*Complex variables*, 与Gordon Latta合写)

由于他在数学教育上的杰出工作，1980年被邀请担任第四届国际数学教育大会的名誉主席，并发表了题为「数学增进智力」的书面致词.

当代数学家N．G、德布鲁因（de Bruijn）这样评价他："波利亚是对我的数学活动影响最大的数学家．他的所有研究都体现出使人愉快的个性、令人惊奇的鉴赏力、水晶般清晰的方法论、简捷的手段、有力的结果．如果有人问我，想成为什么样的数学家，我会毫不迟疑地回答：波利亚。"

循环群的存在性问题、构造问题、数量问题以及子循环群问题等都已完全研究清楚

什么是循环群？

如果群G可以由一个元素a生成，即$G=\{a^k|k\in Z\}$或$\{ka|k\in Z\}$,则称G为由a生成的一个循环群(Cyclic Group)，记为$G=\langle a\rangle$，称a称为G的一个生成元（Generator）。

生成集合

在抽象代数中，群 G 的生成集合是子集 S 使得所有 G 的所有元素都可以表达为 S 的元素和它们的逆元中的有限多个元素的乘积。

示例

1）容易证明循环群是Abel群。

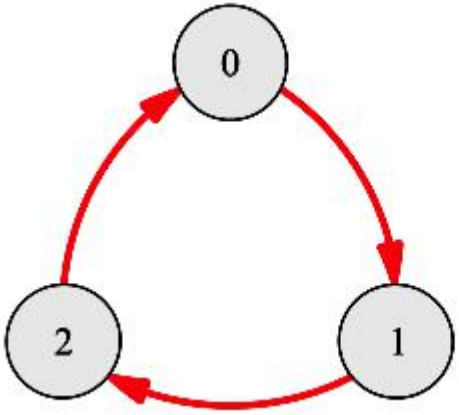
2）整数加群Z是无限阶循环群，<12>为其循环子群。

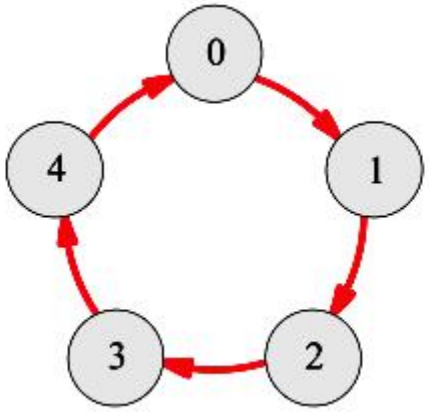
3）n次单位根群$U_n=\{e^{\frac{2k\pi}{n}i}|k=0，1，…,n-1\}$是n阶循环群，其生成元

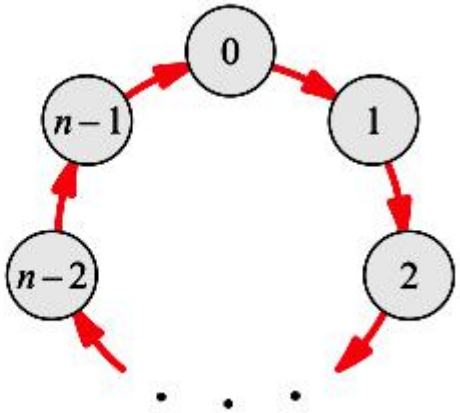
$\varepsilon=e^{\frac{2\pi}{n}i}$，即$U_n=<\varepsilon>$。

示例

循环群C_3，C_5，C_n的Cayley图







几个结论

1) 设群$G=\langle a\rangle$，若$|a|=\infty$，则$\langle a\rangle=\{\ldots, a^{-2},a^{-1},e,a^{1},a^{2},\ldots\}$.

2) 设群$G=\langle a\rangle$，若$|a|=n$，则$\langle a\rangle$为n阶群，$\langle a\rangle=\{a^{0},a^{1},a^{2},\ldots,a^{n-1}\}$.

可以看出，循环群的阶与其生成元的阶是相同的 .

n阶群G是循环群当且仅当G有n阶元素?

3) 无限循环群$\langle a\rangle$有两个生成元，即a与a^{-1}；n阶循环群有$\varphi(n)$个生成元．如4、5、6阶循环群分别有 2、4、2个生成元.

4) 设$\langle a\rangle$是任意一个循环群，若$|a|=\infty$，则$\langle a\rangle$与整数加群Z同构；若$|a|=n$，则$\langle a\rangle$与n次单位根群$U_n=\langle \varepsilon\rangle$($\varepsilon$为n次单位根)同构.

5) 无限循环群有无限多个子群:$\langle e\rangle,\langle a^{1}\rangle,\langle a^{2}\rangle$，…,都是全部互异的的子群

6) 当$\langle a\rangle$为n阶循环群时，对n的每个正因数k，$\langle a\rangle$有且仅有一个k阶子群，此时$\langle a\rangle$所有的循环子群为$H_k=\langle a^{\frac{n}{k}}\rangle$（其中k|n）.

7) 循环群的子群也是循环群.

1 左陪集、右陪集(coset)

利用一个整数n可以把全体整数Z分成剩余类，
即利用等价关系

$R=\{(a,b)|a \equiv b(\mathrm{mod}\ n), n\in Z+\}$

令n=3，则可以将Z分为如下3个等价类：

[0]={…,-6，-3，0，3，6，…}

[1]={…,-5, -2，1，4，7，…}

[2]={…,-4, -1, 2, 5, 8, …}

于是

aRb当且仅当n | a-b

如果把包含所有n的倍数的集合记为H，即有

H={hn|h=…，-2，-1，0，1，2，…}

则有

aRb当且仅当a-b∈H。

代数的观点

易验证<H; +>为<Z; +>的子群(+为一般加法).

推广之，H为G的子群，等价关系R：

对于∀a,b∈G，aRb当且仅当$ab^{-1}\in H$.

于是，等价类[a]=

$\{x|x\in G,xRa\}$

$=\{x|x\in G,xa^{-1}\in H\}$

$=\{x|x\in G,xa^{-1}=h,h\in H\}$

$=\{x|x\in G,x=ha,h\in H\}$

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

$=Ha$

1 左陪集、右陪集(coset)

示例

求出<Z_6; $+_6$>关于子群<{0,3}; $+_6$>的所有左陪集,右陪集

令H={0,3},

则左陪集: 右陪集:

0H={0,3}=3H H0={0,3}=H3

1H={1,4}=4H H1={1,4}=H4

2H={2,5}=5H H2={2,5}=H5

从中可以看出：{0H,1H,2H}是由G的子群得到的G的一个划分

陪集性质1： $a\sim b\Leftrightarrow Ha=Hb$

由陪集诱导出的等价关系：

设<H,*>是群<G,*>的子群,则H的右陪集所构成的集合是G的一个划分,由此划分导出的等价关系称为H的右陪集等价关系,右陪集等价关系记为~

$a\sim b\Leftrightarrow Ha=Hb$

$a\sim b\Leftrightarrow ab^{-1}\in H$

陪集性质2

设<H,*>是<G,*>的子群,$\forall a,b\in G$，则Ha=Hb或$Ha\cap Hb=\Phi$

证:

若$Ha\cap Hb\neq\Phi$,设$\exists x\in Ha\cap Hb$

于是，$\exists h_1$，$h_2\in H$，使$x=h_1*a=h_2*b$

从而，$a=h_1^{-1}*h_2*b\in Hb$

对于$\forall x\in Ha$,

$\exists h_3\in H$,使得$x=h_3*a=h_3*h_1^{-1}*h_2*b\in Hb$

故$Ha\subseteq Hb$.

同理$Hb\subseteq Ha$.

所以 Ha=Hb.

综上，命题得证。

陪集性质3

设G是一个有限群，H是G的子群，则G可以分解为两两不同的H的陪集的并，即存在一个正整数n，使得：

$G=Ha_1 \cup Ha_2 \cup \ldots \cup Ha_n$

其中：$Ha_i \cap Ha_j=\Phi(i\neq j,i,j=1,2,\ldots,n)$

2 拉格朗日定理

H为有限群G的子群，则$|G|=|H|[G:H]$

从而有$|H| \mid |G|$

请思考：

1.有限群<G,*>中的任何元素a的阶可整除|G|.

2.质数阶的群没有非平凡子群，且为循环群.

3.试证奇数阶群所有元素之积可以等于单位元.

证:设<G,*>是一个群,e为单位元,则

$\forall a \in G$，若$a \neq e$，则$a \neq a^{-1}$ ，

若$a=a^{-1}$ 则$a^2=e$，于是<{a,e},*>是<G,*>的2阶的子群

由拉格朗日定理:2 ｜ |G|，即群G阶数为偶数，矛盾.

所以，$\forall a \in G$，若$a \neq e$,a、a^{-1}总是成对出现，

于是,G可以表示为：$\{e, a_1, a_1^{-1}, a_2, a_2^{-1}, \ldots, a_n, a_n^{-1}\}$，其中$a_i \neq a_i^{-1}$

故 $e*a_1*a_1^{-1}*\ldots*a_n*a_n^{-1}=e*e*\ldots*e=e$.

1 正规子群:从陪集到正规子群

（Normal Subgroup)

2 正规子群的判定

群G的一个子群H是G的正规子群当且仅当对任意$a\in G$，$h\in H$，皆有$aha^{-1}\in H$。

示例

设$\langle G_1;*\rangle$,$\langle G_2;*\rangle$是群$\langle G;*\rangle$之二正规子群，则$\langle G_1G_2;*\rangle$亦是$\langle G;*\rangle$之正规子群. 这里,$G_1G_1=\{g_1g_2|g_1\in G_1,g_2\in G_2\}$.

3 商群(Quotient Group)

$<G/H;*>, *: Ha, Hb \in G/H, Ha*Hb=\{h_1 a h_2 b \mid h_1, h_2 \in H\}$

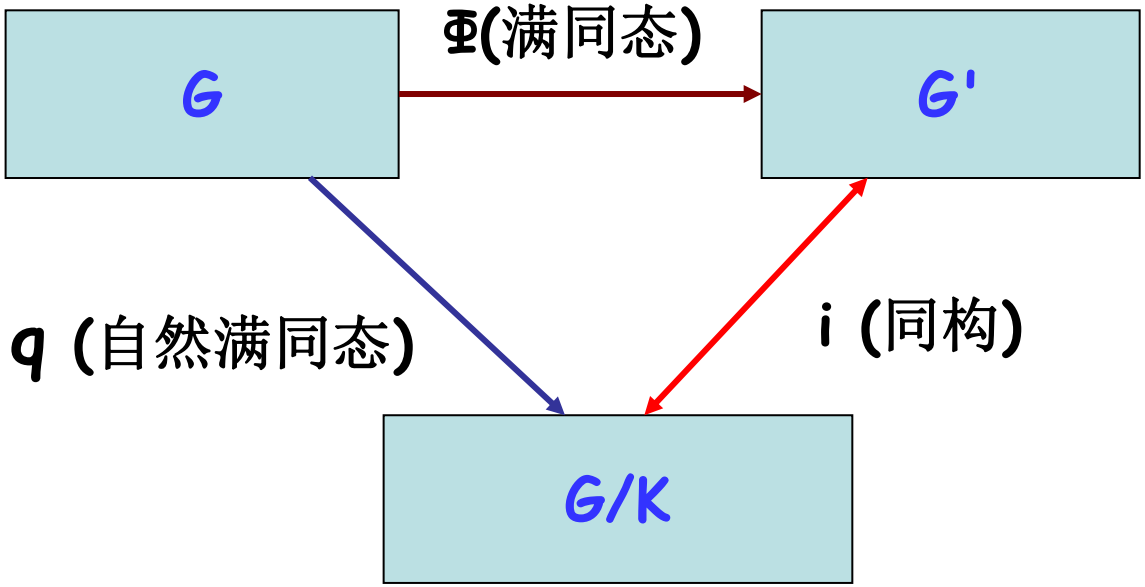
1) *在G/H上满足封闭性

2) *在G/H上满足结合性

3) G/H存在单位元

4) G/H的每一个元素存在逆元

4 群同态三角形



1) 由Φ得到的同态核K为G之正规子群

2) G与G/K同态[群<G;*>与其每一个商群<G/H;*>同态]

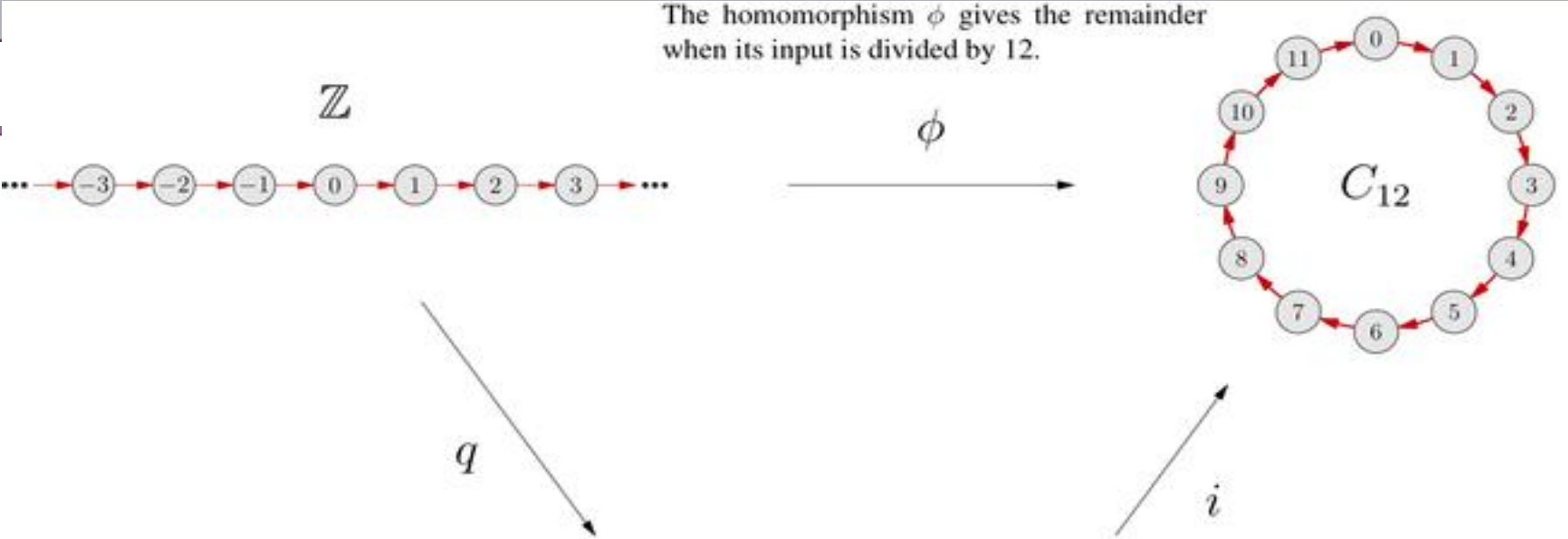
3) G/K与G'同构

An example: triangle of homomorphisms

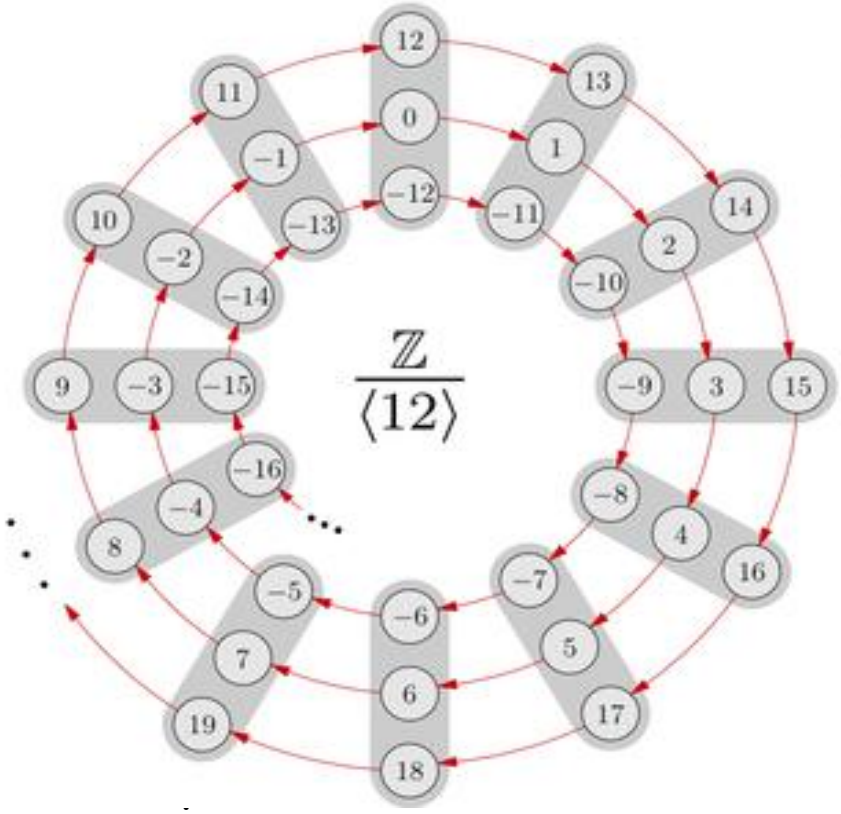
The quotient process can also be performed on infinite groups. In this diagram, the group of integers Z is divided by the subgroup <12> to create a structure in which arithmetic takes place mod 12. That structure is then shown to be isomorphic to the group C_{12}, using a triangle of homomorphisms as given by the Fundamental Homomorphism Theorem.

——from Nathan Carter: *Visual Group Theory*

The homomorphism ϕ gives the remainder when its input is divided by 12.



The quotient map q corresponds to the quotient process described in the text, whose rearranged Cayley diagram is shown here.



The isomorphism i renames the cosets to the single nodes of C_{12}, showing that the structures are identical.

Another example: triangle of homomorphisms

——from Nathan Carter: *Visual Group Theory*

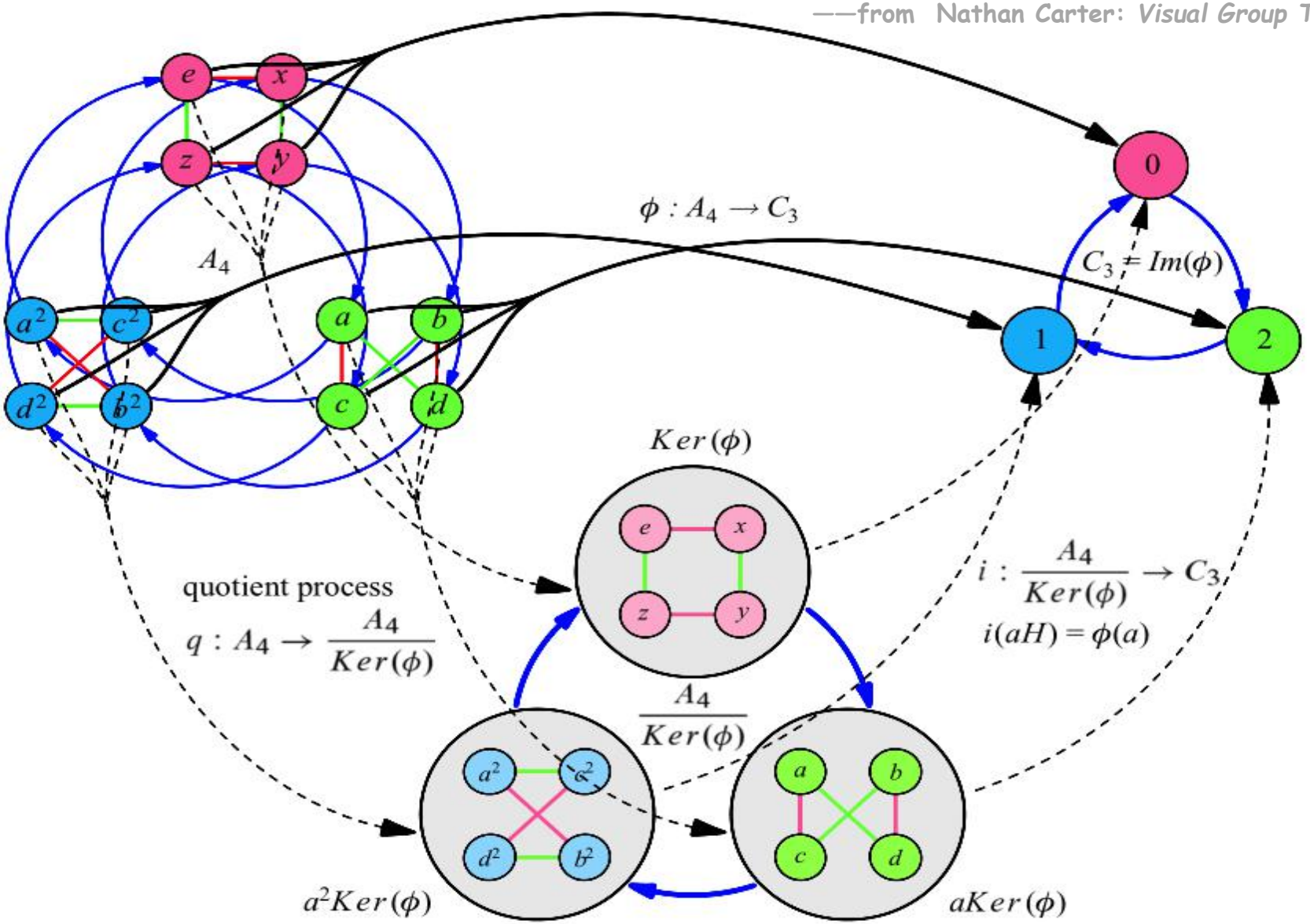


Figure 8.14. The Fundamental Homomorphism Theorem (Theorem 8.5) exemplified using the group A_4 and the quotient map ϕ whose kernel is the subgroup $\{e, x, y, z\}$ of A_4

补充例题

1 设<G; *>是n阶有限群，e为单位元，$a_1,a_2,\ldots,a_n$是G的任意n个元素（不一定两两不同）。试证明：存在整数p,q，$1\le p\le q\le n$，使得$a_p*a_{p+1}*\ldots*a_q=e$.

2 ‹G；*›是群，H，K为其子群，在G上定义二元关系R：

任意a,b∈G,aRb⇔存在h∈H,k∈K,使得b=h*a*k.

证明: R是G上的等价关系.

3 设R为实数集合，G={(a,b)|a,b∈R,a≠0}. 定义G上的运算*：对任意

$(a_1,b_1),(a_2,b_2)\in G$，$(a_1,b_1)*(a_2,b_2)=(a_1\times a_2,b_1\times a_2+b_2)$,

其中+、×分别是一般的加法、乘法，证明：

1) <G;*>是群.

2）设S={(1,b)|b∈R},则<S; *>是<G; *>的子群.

4 G为群，x,y∈G, 且$yxy^{-1}=x^2$，其中$x\neq e$，$|y|=2$，这里e是单位元。求x的阶.

小结

1）群的概念；

2）元素的周期；

3）置换群的概念与性质；

4）循环群的性质；

5）子群、正规子群；

6）陪集与拉格朗日定理；

7）商群与群的同态基本定理。

其中，子群、陪集与拉格朗日定理是重点，置换群及其在Burnside定理与Plóya计数原理,正规子群、商群与群同态基本定理是难点。