群论和魔方（P1）

Original:Accela推箱子 Accela推箱子 5/28

从未有理论如此直击心灵，仿佛世间所有答案早已漂浮于空气中，只是从未被看见。

为什么是群论?

本文P1介绍群论，P2求解魔方。本文保证深入浅出（^_^）。群论是求解魔方的基础。P2实现了可运行的程序。

群论可以研究空间的结构。

求解魔方犹如在庞大的状态空间中寻找最短路径。与其熟记所有捷径，不如绘制空间结构的地图，将捷径的“巧”转化为地图搜索的“系统”。

几乎所有算法问题都可以转化为“空间结构”。可能的状态，在约束内自由滑动，张成空间。而问题的答案，即是空间中的特殊一点，也是空间结构本身；那便是“特殊”的含义。

空间结构的本质是对称。

是什么使空间结构各不相同？不同的约束，从完全自由杂乱的母板上，雕刻出不同的空间结构。而“约束”本身是恒定的等价性，即是对称。（所有的群都是自由群的商群，**链接表见文末**，下同）

群论也被称为研究对称的理论。对称有着更深刻的本质，动量守恒对应空间平移不变性，能量守恒对应时间平移不变性，而量子物理几乎离不开群论。（诺特定理）

对称一定是普遍的。

算法问题总有着少量的规则，大量的状态。犹如鸽笼原理，把大量状态塞进少量规则，一定会充满对称。而研究对称的群论，总有用武之地。

在时间和空间的主轴上，“对称”构建起人类的思维。“不变”是对称。时间中不变的相对空间，被识别为物体。万物中的不变，被识别为概念。概念间的不变，产生了层层抽象和思想。它们即是认知的本源，也是人类的囚笼。（物自体）

下面，让群论揭开现实的本质……

群论：基本概念

本文的定理和截图基本出自J.S. Milne Group Theory，推荐。本文讨论的群都是有限大小的群。

群（Group）的定义

我们希望“群”的定义足够普通，又能反映对称。看数学的选择：

群被定义为集合G上的二元运算；运算是封闭的，不会超出集合；运算可逆，拥有逆元；满足结合律，因而可以稳定地连接多次运算；但不一定满足交换律。

DEFINITION 1.1 A ***group*** is a set G together with a binary operation

$$(a,b) \mapsto a * b : G \times G \to G$$

satisfying the following conditions:

G1: (associativity) for all $a,b,c \in G$,

$$(a*b)*c = a*(b*c);$$

G2: (existence of a neutral element) there exists an element $e \in G$ such that

$$a*e = a = e*a \tag{1}$$

for all $a \in G$;

G3: (existence of inverses) for each $a \in G$, there exists an $a' \in G$ such that

$$a*a' = e = a'*a.$$

去除群定义中部分规则，数学概念依然存在，例如半群。而向群中加入第二种运算，则可构成域，例如有理数域。

子群（Subgroup）

群所在的集合G有子集S，如果S对群运算是封闭的，则S成为子群。“封闭”指，S中任意两个元素的运算结果，仍在S中。

正规（Normal）子群

若G的子群N，对共轭运算（gng^(-1)）封闭，那么N是正规子群。为什么需要“正规子群”这个概念呢，见下文的商群。

A subgroup N of G is ***normal***, denoted $N \lhd G$, if $gNg^{-1} = N$ for all $g \in G$.

陪集（Coset）

G有子集S和元素a，a可与S中所有元素相乘，得到新集合——aS称为左陪集，Sa称为右陪集。左右陪集通常对等，本文默认“陪集”用左陪集。

For a subset S of a group G and an element a of G, we let

$$aS = \{as \mid s \in S\}$$
$$Sa = \{sa \mid s \in S\}.$$

陪集看似抽象，实则直观，是触及群论本质的东西。它有近乎完美的性质：陪集间互不重叠，互相等大，完整覆盖群——陪集的集合构成群的**划分**。

PROPOSITION 1.25 *Let H be a subgroup of a group G.*

(a) An element a of G lies in a left coset C of H if and only if $C = aH$.

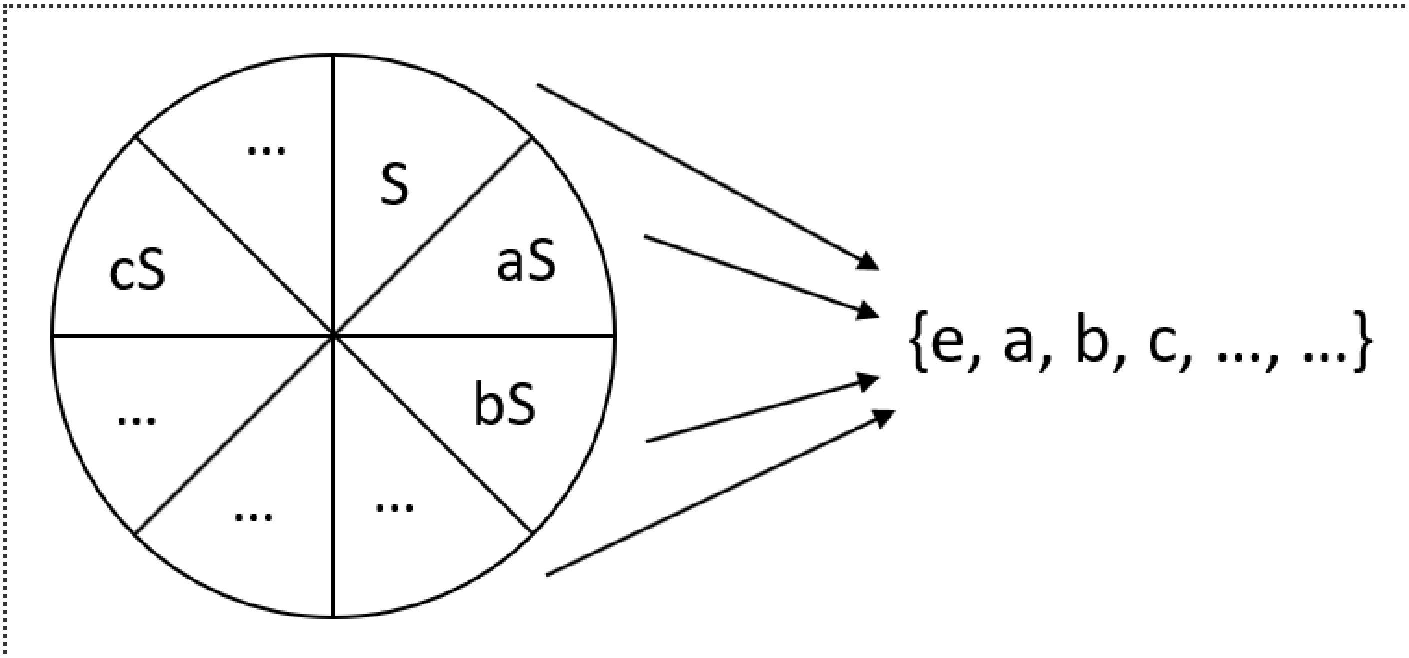
(b) Two left cosets are either disjoint or equal.

(c) $aH = bH$ if and only if $a^{-1}b \in H$.

(d) Any two left cosets have the same number of elements (possibly infinite).

商（Quotient）群

S的所有陪集的集合，记为G/S，称为**“商”**；它们是群G的划分。为方便，常从陪集中任取一个元素代表它，称为**代表元（Coset Representative）**。



G/S是群吗？当S是正规子群时，是，称作“商群”。群的二元运算定义为(aS)*(bS)=(a*b)S；正规子群便是为了等式成立。

等价类划分，和商群异曲同工。还有从整数Z构造分数Z×Z，用分数约分构造等价类，而商则是有理数。

群作用（Group Action）

为描述魔方，基本的群定义不太合适。因为其元素既表示魔方状态，又是参与运算的魔方操作。

我们将其分开，魔方操作构成群G，色彩方块构成集合X。二者一起被称为群作用**G-set**。

DEFINITION 4.1 Let X be a set and let G be a group. A ***left action*** of G on X is a mapping $(g,x) \mapsto gx: G \times X \to X$ such that

(a) $1x = x$, for all $x \in X$;
(b) $(g_1 g_2)x = g_1(g_2 x)$, all $g_1, g_2 \in G$, $x \in X$.

A set together with a (left) action of G is called a (left) ***G-set***. An action is ***trivial*** if $gx = x$ for all $g \in G$.

稳定（Stabilizer）子群

有了群作用G-set，我们希望为它的特别之处建立概念。G中哪些元素g操作X的子集S后，可以不改变S呢？可证明这些g组成的集合是群，称之为S的稳定子群Stab(S)。

For a subset S of X, we define the ***stabilizer*** of S to be

$$\mathrm{Stab}(S) = \{g \in G \mid gS = S\}.$$

Stab(S)和函数不动点异曲同工，内涵深刻；对应能把魔方转回原位的操作。试想Stab(S)的陪集、商是什么呢？后文有更多讲解。

轨道（Orbit）

与稳定子群相反，不稳定的话会怎样呢？取X中元素x0，用G不断变换它；x0走过的全部，称为x0的轨道Gx0，也记Orbit(x0)，是X的子集。

By definition, the G-orbit containing x_0 is

$$Gx_0 = \{gx_0 \mid g \in G\}.$$

It is the smallest G-stable subset of X containing x_0.

不同x0有不同轨道，神奇的是，**轨道的集合是X的划分**；即轨道间互不重叠，完整覆盖。本质上，是因为群中元素可互相“传递”，形成了等价类。

Write $x \sim_G y$ if $y = gx$, some $g \in G$. This relation is reflexive because $x = 1x$, symmetric because

$$y = gx \implies x = g^{-1}y$$

(multiply by g^{-1} on the left and use the axioms), and transitive because

$$y = gx, \quad z = g'y \implies z = g'(gx) = (g'g)x.$$

It is therefore an equivalence relation. The equivalence classes are called G-***orbits***. Thus the G-orbits partition X. Write $G\backslash X$ for the set of orbits.

对于魔方，试想我们仅允许部分旋转操作，色彩方块所能达到的全部状态就是轨道。

同态映射（Homomorphism）

如何表达两个群拥有相同的结构？同态映射要求群G的二元运算，在群G′上仍保持。G和G′大小可以不等。

DEFINITION 1.20 A ***homomorphism*** from a group G to a second G' is a map $\alpha: G \to G'$ such that $\alpha(ab) = \alpha(a)\alpha(b)$ for all $a, b \in G$. An ***isomorphism*** is a bijective homomorphism.

G和G′的元素，到底有何种对应关系？同态映射背后有着近乎“疯狂”的定理。

同构（Isomorphism）

同态映射，如果是一一映射（Bijective），则G和G′相等（大小相等，元素一一对应），称为同构（Isomorphism）。

核（Kernel）

同态映射f中（贴图中符号是“α”），核Ker(f)是被映射成单位元的元素的集合（单位元的原像）。核就是“1”（乘法表示），核就是“零”（加法表示）。

The ***kernel*** of a homomorphism $\alpha: G \to G'$ is

$$\mathrm{Ker}(\alpha) = \{g \in G \mid \alpha(g) = e\}.$$

可以发现，核与稳定子群概念一致。那么，核的商是什么呢？后文有更多讲述。

另外，**核一定是正规子群**。因为：∀g∈G, ∀a∈Ker(f), f(gag^(-1)) = f(g)f(a)f(g^(-1)) =f(e)=e′ => gag^(-1)∈Ker(f)。

群论：作为背景的定理

群论最激动人心之处，在于许多极其强大却又无比普适的定理；如同包容一切复杂度的边界，真相如此朴实，却又从未被察觉。

所有的群都是置换群（Permutation Group）的子群

群可以写成乘法表的形式。可证明，每一行无重复元素，是集合元素的置换。**“置换”**是一个从集合S到S的双射函数，即把S中的元素重新排列了顺序。

	e	a	b	c	$\dots$
e	ee	ea	eb	ec	$\dots$
a	ae	a^2	ab	ac	$\dots$
b	be	ba	b^2	bc	$\dots$
c	ce	ca	cb	c^2	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

如果把所有可能的置换凑齐，就有了**置换群Sn**。置换群的二元运算定义为置换的复合函数（还是置换）。Sn大小是|S|!。

直觉上可以看到，S上的群，都是其完整版——置换群Sn——的子群。S的元素可以看作Sn中的置换函数，置换规则就是乘法表中的对应行。而“看作”的本质则是同态映射（Homomorphism）。

THEOREM 1.22 (CAYLEY) *There is a canonical injective homomorphism*

$$\alpha: G \to \mathrm{Sym}(G).$$

PROOF. For $a \in G$, define $a_L: G \to G$ to be the map $x \mapsto ax$ (left multiplication by a). For $x \in G$,

$$(a_L \circ b_L)(x) = a_L(b_L(x)) = a_L(bx) = abx = (ab)_L(x),$$

and so $(ab)_L = a_L \circ b_L$. As $e_L = \mathrm{id}$, this implies that

$$a_L \circ (a^{-1})_L = \mathrm{id} = (a^{-1})_L \circ a_L,$$

and so a_L is a bijection, i.e., $a_L \in \mathrm{Sym}(G)$. Hence $a \mapsto a_L$ is a homomorphism $G \to \mathrm{Sym}(G)$, and it is injective because of the cancellation law. □

COROLLARY 1.23 *A finite group of order n can be realized as a subgroup of S_n.*

PROOF. List the elements of the group as $a_1, \dots, a_n$. □

魔方的旋转操作是对色彩方块集合的置换。而魔方操作并不能抵达色彩方块的任意组合，魔方群是置换群的子群。

找到作为完整版的置换群，便让被研究的群有了边界——它们都是更小的子群而已，无论多么复杂。而“置换”的普适，则使得程序可以使用映射数组，来实现群的快速运算。

所有的群都是自由群（Free Group）的商群

将集合X中元素任意组合连接，不限长度，生成自由群FX。FX除遵守群定义外，无任何约束。

{a,b,c} => {a,b,c, aab, abb, abac, aaab^(-1)c, abbc^(-1), ...}

下一步，加入约束。如何表示约束呢？用“对称”：a=b。换个形式，即ab^(-1)=e。也即是说，约束就是元素的乘积，ab^(-1)；群论中称为**关系（Relation）**。关系的集合记为R。

那么，R有多大？如果h属于R，那么gh=g，即ghg^(-1)=e，所以共轭运算ghg^(-1)也是关系，属于R。把FX中所有g试遍，我们发现**R是正规子群**。

于是，有了商群FX/R，记为G。G就是向自由无结构的FX中，逐步加入约束/关系（本质是“对称”），所得到的有结构的空间。（Quora有易懂的解释）

所有的群G，都可以如此得到；它们都是自由群的商群。

COROLLARY 2.5 *Every group is a quotient of a free group.*

PROOF. Choose a set X of generators for G (e.g., $X = G$), and let F be the free group generated by X. According to (2.3), the map $a \mapsto a\colon X \to G$ extends to a homomorphism $F \to G$, and the image, being a subgroup containing X, must equal G. □

自由群就像世界的母板，“对称”雕刻出的一切空间结构，都有精确的数学解释。而自由组合词语的语言，是否与自由群有更本质的关系呢？而语言的结构，便是世界的结构。（语言哲学）

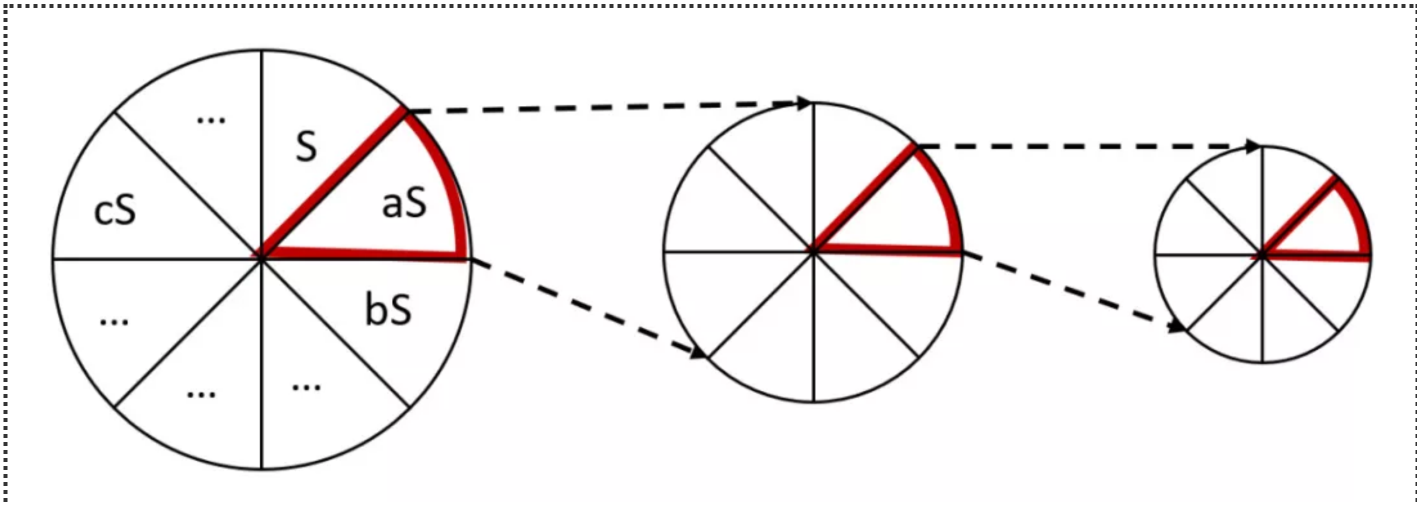
群论：空间的结构

如何研究空间结构？这是最震撼人心的地方，表象背后的一致浮出水面，现实从未如此清晰。“分而治之”仍然质朴有力。

陪集划分

前文讲过，陪集的集合G/S构成群G的划分。而陪集间不仅大小相等，还具有相同结构；例如用*a，将S中元素一一映射到aS。

这构成了“分而治之”的完美适用。选取子群，层层分解，而层内陪集间结构都相同。更妙的是，子群可以任意选取。



对于魔方群，我们可以层层分解，构造出链条。如何选取子群呢？P2中我们将讲到稳定链（Stabilizer Chain）。

稳定子群的商与轨道同构

如何理解呢？从魔方开始。选取魔方色彩方块的子集S。Stab(S)中的操作，无法转动S。

下面来看Stab(S)的陪集；设其代表元为g，陪集为gStab(S)。gStab(S)中任意元素，可由g*x∈Stab(S)得到。可以发现，因Stab(S)没有转动作用，所以g*x都将S旋转到相同位置，即g的位置。

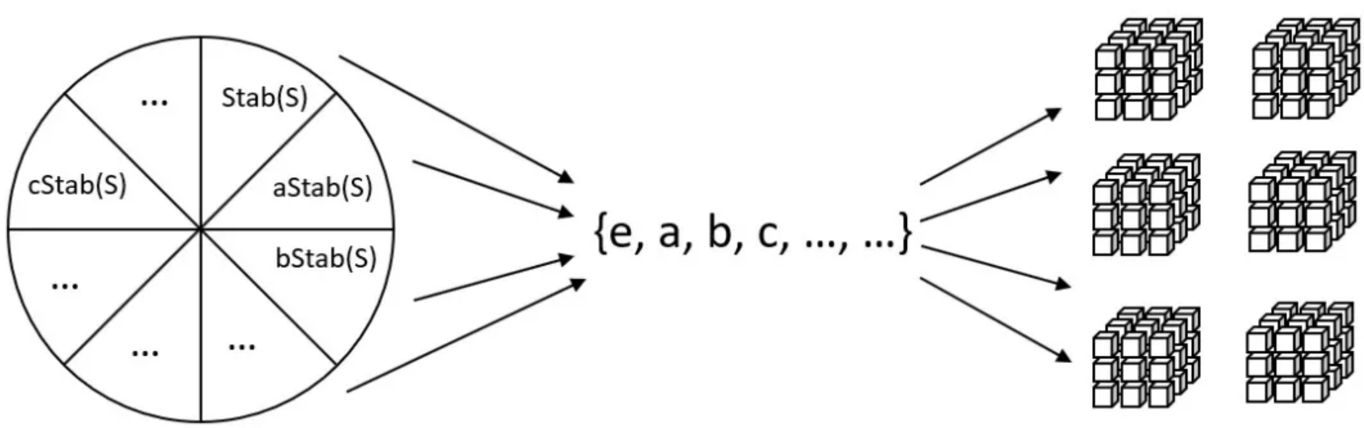
也就是说，Stab(S)的陪集，与S能被旋转到位置，是一一对应的。而陪集完整覆盖魔方群G。所以，陪集的集合、即Stab(S)的商，与S能到达的所有位置、即S的轨道，同构：**G/Stab(S)<-> Orbit(S)**。

PROPOSITION 4.7 *If G acts transitively on X, then for any $x_0 \in X$, the map*

$$g\,\mathrm{Stab}(x_0) \mapsto g x_0 : G/\mathrm{Stab}(x_0) \to X$$

is an isomorphism of G-sets.

这条定理是我们绘制魔方状态地图的基础。稳定子群像不动点，而陪集像切换“视角”，把S的状态从e切换到某g。商则从（不动）“点”构造出全局（“面”）的划分。



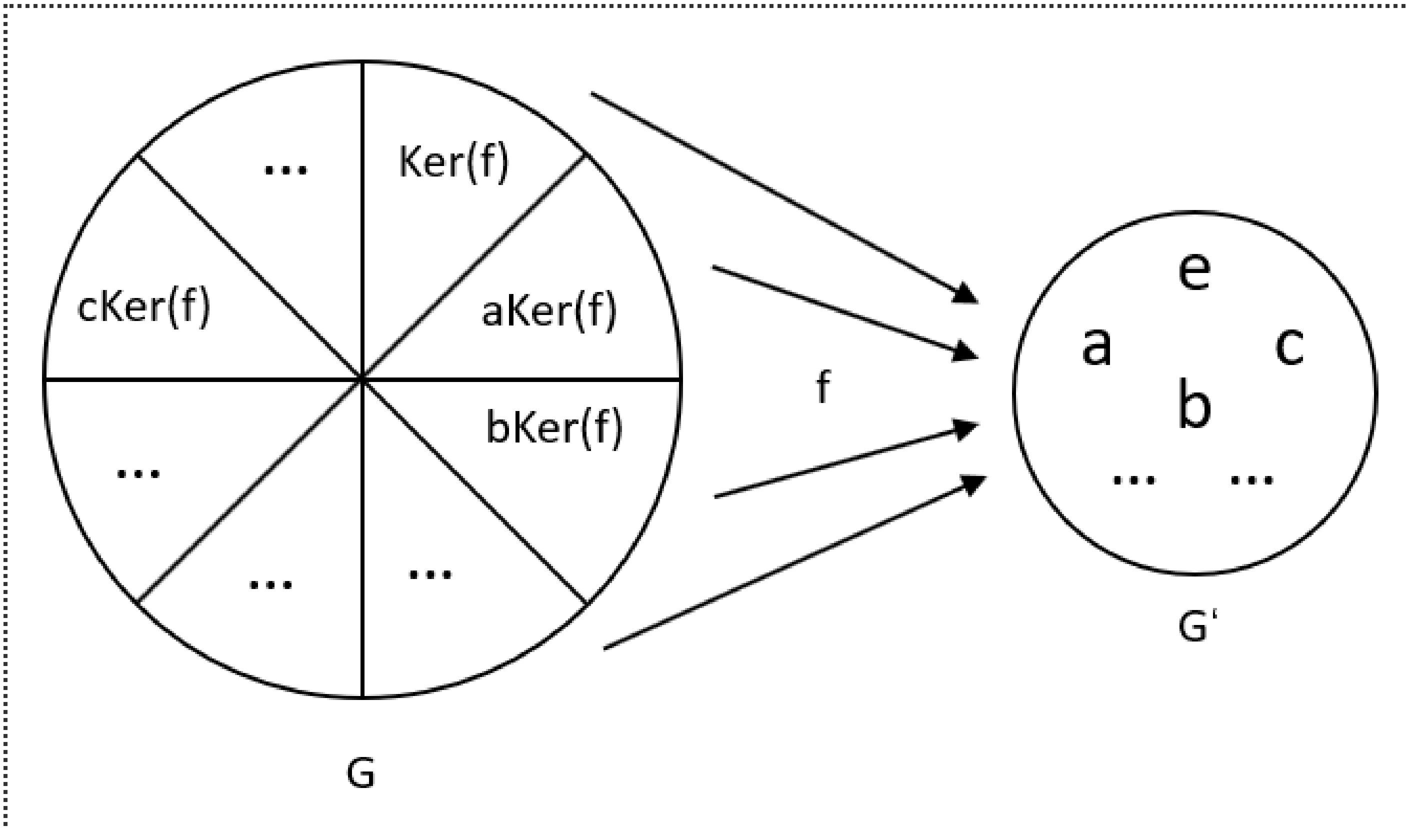
“点”蕴含了所处的“面”，正如答案反而蕴含了问题本身。人们常问“答案”，但若已在眼前，如何判断它就是呢？“判断”、“答案”、“问题”，内在便是一致的空间结构。与其寻找答案，不如明晰问题的结构本身。

同态映射的结构

如何理解呢？设同态映射f将群G映射到群G′。先从“不动点”核Ker(f)入手。因Ker(f)是正规子群，故G/Ker(f)构成商群，元素是Ker(f)的陪集。

Ker(f)的陪集有何性质？任取g∈aKer(f)，则g=a*p而p∈Ker(f)，故f(g)=f(a)f(p)=f(a)。即，同一陪集中的元素总映射到G′中同一点。

可以发现，此定理与“稳定子群的商与轨道同构”是一样的：**G/Ker(f)与G′同构，由f映射**。准确说，G/Ker(f)是与f在G′中的像，记为I.（Image，即f在G′中能达到的所有元素的集合），同构。



反过来，能够**从任意核Ker(f)，构造出同态映射f**吗？是的。任取正规子群N，把它当作Ker(f)，而令f把g∈G映射到其陪集∈G/N，G′就是商群G/N。

THEOREM 1.45 (HOMOMORPHISM THEOREM) *For any homomorphism $\alpha: G \to G'$ of groups, the kernel N of α is a normal subgroup of G, the image I of α is a subgroup of G', and α factors in a natural way into the composite of a surjection, an isomorphism, and an injection:*

$$\begin{tikzcd} G \arrow[r, "\alpha"] \arrow[d, "\text{surjective}"', "g\mapsto gN"] & G' \\ G/N \arrow[r, "gN\mapsto\alpha(g)", "\text{isomorphism}"'] & I. \arrow[u, "\text{injective}"'] \end{tikzcd}$$

可以看到，**同态映射、正规子群、商群，本质是一样的**。它们与稳定子群、轨道，本质也是一样的。同态映射就是正规子群，正规子群就是同态映射。商群G/N是同态映射约减后的G。“约减”是等价类划分。

同态映射，是如同函数般普遍的概念。而在群论中，却给出了无比本质，无比普适的强大定理。群的空间结构由此层层剖析。

群的分解

由上节，我们有了分解群G的方法。选取正规子群N，构造的商群G/N比G更小，而且保持了与G一致的结构，由以N为核的同态映射f维持。

G被分解成了G/N；G是N与G/N的**半直积（Semidirect Product）**。将G层层分解，从复杂到简单，便有了研究群结构的方法。

DEFINITION 3.8 A group G is a ***semidirect product*** of its subgroups N and Q if N is normal and the homomorphism $G \to G/N$ induces an isomorphism $Q \to G/N$.

Equivalently, G is a semidirect product of subgroup N and Q if

$$N \lhd G; \qquad NQ = G; \qquad N \cap Q = \{1\}. \tag{15}$$

如果将G分解到底会怎样？犹如整数分解为质数，最终产物称作**单群**（Simple Group），即不含更小的正规子群（Non-trivial）的群。

Jordan–Hölder定理指出，G的分解链条（Composition Series）是唯一的：长度相等，单群相同，只有顺序可变。

$$1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = G,$$

如何从单群构造原来的群G呢？这一过程称为**Group Extension**，结果并不唯一（Quora）。半直积是典型方式。

A sequence of groups and homomorphisms

$$1 \to N \xrightarrow{\iota} G \xrightarrow{\pi} Q \to 1 \tag{16}$$

is ***exact*** if ι is injective, π is surjective, and $\mathrm{Ker}(\pi) = \mathrm{Im}(\iota)$. Thus $\iota(N)$ is a normal subgroup of G (isomorphic by ι to N) and $G/\iota(N) \xrightarrow{\simeq} Q$. We often identify N with the subgroup $\iota(N)$ of G and Q with the quotient G/N.

An exact sequence (16) is also called an ***extension of*** Q ***by*** N.[1] An extension is ***central*** if $\iota(N) \subset Z(G)$. For example, a semidirect product $N \rtimes_\theta Q$ gives rise to an extension of Q by N,

$$1 \to N \to N \rtimes_\theta Q \to Q \to 1,$$

which is central if and only if θ is the trivial homomorphism.

揭晓答案的时刻：**单群已被完全分类**。出乎意料，只有如下4种。这便是构成一切群的“质数”，群的结构可如此洞悉。

A. The classification of finite simple groups

There is a complete list of finite simple groups. They are

(a) the cyclic groups of prime order,
(b) the alternating groups A_n for $n \geq 5$ (see the next chapter),
(c) certain infinite families of matrix groups, and
(d) the 26 “sporadic groups”.

无论空间结构多么复杂，砖块皆如此。这便是世间为何总有许多“似曾相识”。由“对称”雕刻的无限现实，本源却如此寥寥；真相是祝福，亦或牢笼？

结语

现在回看开头，是否更有感触？空间结构中，“对称”如此普遍，群论能将其“质数”分解；构筑现实的砖块，内在却是出奇一致地简单。最震撼人心的理论，如空气般朴实却又难以察觉。

一切只是开始。P2中，我们将求解魔方的谜团。看似简单的3*3*3魔方，拥有43百万兆的组合。而我们将从4*4*4魔方入手……

$$8! \times 3^7 \times (12!/2) \times 2^{11} = 43,252,003,274,489,856,000$$

附录：链接表

微信文章禁止外链，故将资料链接存放此处。

所有的群都是自由群的商群：https://math.stackexchange.com/questions/9446/every-group-is-the-quotient-of-a-free-group-by-a-normal-subgroup

诺特定理：https://zhuanlan.zhihu.com/p/51330777

物自体：http://www.lunwenstudy.com/wgzhexue/65123.html

J.S. Milne Group Theory：https://www.jmilne.org/math/CourseNotes/GT310.pdf

半群：https://zh.wikipedia.org/wiki/%E5%8D%8A%E7%BE%A4

域：https://zh.wikipedia.org/wiki/%E5%9F%9F_(%E6%95%B8%E5%AD%B8)

自由群的商群 Quora有易懂的解释：
https://math.stackexchange.com/questions/9446/every-group-is-the-quotient-of-a-free-group-by-a-normal-subgroup

语言哲学：
https://zh.wikipedia.org/wiki/%E8%AF%AD%E8%A8%80%E5%93%B2%E5%AD%A6

Simple Group：https://en.wikipedia.org/wiki/Simple_group

Jordan–Hölder定理：https://en.wikipedia.org/wiki/Composition_series

Group Extension Quora：https://math.stackexchange.com/questions/25315/how-is-a-group-made-up-of-simple-groups

单群已被完全分类：
https://en.wikipedia.org/wiki/Classification_of_finite_simple_groups

3*3*3魔方：https://en.wikipedia.org/wiki/Rubik%27s_Cube