目　　录

第一章　瞎扯伽罗华群论思想

基本信息

1. 原文链接 https://www.douban.com/group/topic/95244972/.
2. 本文作者 wxmang.

1.1　序

先声明一句，这篇帖子为了使非数学专业的人能够阅读下去，对主要概念的来源和主要定理的证明进行了一些简化，可能导致不严谨。所以只能归类于瞎扯范畴。专业的数学工作者不要过于苛责。我为了简明扼要说清楚，不得不在严谨上做妥协，甚至有的地方可能是错的。

这篇帖子目的是介绍数学是如何从研究计算进化到研究结构的。

伽罗华是数学从计算转向结构的关键人物，或者说是数学从古代转向近代的关键人物。在伽罗华之前，数学本质是靠计算来解决问题，伽罗华以超凡的洞察力，构建了从数学结构来研究数学本质问题的框架。这时从具体到抽象的一步巨大跨越。

我想用一个具体例子说明人类是如何从具体事物进化到抽象概念的。

为了非数学系的人能够知道我说的内容，我用了大量描述性语言，所以不够严谨。在通俗和严谨之间，只能做此取舍。

人类第一个真正的抽象学科是抽象代数，抽象代数是从伽罗华群论发展起来。为了理解抽象代数，我们介绍一下伽罗华群论的来历，这样便于以后有兴趣看抽象代数，进入本质更快一点。

由于篇幅和豆瓣对符号的限制，一般抽象代数就无法介绍了，有兴趣的自己去看书。这里只做点科普。

我们已经在以前讨论数学基础的帖子里知道，现代数学主要研究从现实世界中抽象出的空间形式和数量关系，也即结构及结构之间的关系，而结构进入数学只有 100 年的历史，是由群的概念引进而开始的。群的概念的引入就是伽罗华，他也是第一位在有意识地以结构的研究代替计算的人。群论彻底解决了代数方程的根式求解问题此发展了一整套关于群和域的理论。

但是群的概念并不是伽罗华发明的，而是产生于拉格朗日研究代数方程的解过程中：拉格朗日已经意识到一元 n 次方程的根是一个置换群，而且也猜想一般五次以上方程无根式解，但是拉格朗日没能证明这个猜想，后来鲁菲力和阿贝尔都企图证明这个猜想，其中鲁菲力的论文有 560 多页，阿贝尔有几页，不过证明被验证后都是错的或逻辑不完备的。

而置换群的性质，柯西在 1815 年就已经发现了，可是柯西没能把其与一元 n 次方程的解结合起来，错过了这一数学史上最伟大的发现。

伽罗华的重大发现不是发明了群的概念，而是发现每个一元 n 次方程的解都与一个置换群对应，而置换群的群结构决定了解的特性。所以不需要计算解，只需要研究置换群的结构，就能了解解的性质。也即把数学计算改为研究数学结构。

抽象代数是研究数学结构的，代数结构＝集合上按照公理体系定义的运算规则（集合包括包括实数、复数、向量（vector）、矩阵（matrix）、变换（transformation）等集合，运算规则包括加法，乘法等等）。

按照教科书定义，抽象代数是研究各种抽象的公理化代数结构的学科，如群（group）、环（ring）、域（domain）等等。

下面先说说目前抽象代数对其研究的主要代数结构的抽象定义，不过这些定义不是我们的重点，看不看无所谓。只是想表明一下抽象的格式是什么，不是我想讲的。

1.2 基本定义

群的定义是：

定义 1.1: 群的定义

假设一个非空集合，上面有一个二元运算，如果满足以下条件：
(1) 封闭性：若 $a,b \in G$，则存在唯一确定的 $c \in G$，使得 $a \cdot b = c$；
(2) 结合律成立，即对 G 中任意元素都有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$；
(3) 单位元存在：存在 $e \in G$，对任意 a，满足 $a \cdot e = e \cdot a = a$。- e 称为单位元，也称幺元；
(4) 逆元存在：任意 $a \in G$，存在 b，$a \cdot b = b \cdot a = e$（$e$ 为单位元），则称 a 与 b 互为逆元素，简称逆元。记作 a^{-1}；
则称 G 对 $\cdot$ 构成一个群。

环的定义是：

定义 1.2: 环的定义

R 是一个非空集合，若定义了两种代数运算 $+$ 和 $\cdot$（不一定是我们常识的加与乘，是一种抽象运算规则），且满足：
(*1*)、集合 R 在 $+$ 运算下构成阿贝尔群 *(Abel group*，交换群，也即对任意的 $a,b \in G$, 有 $(a \cdot b) \cdot (a \cdot b) = (a \cdot a) \cdot (b \cdot b)$，并不是所有群都是阿贝尔群，比如矩阵的乘法不满足交换律，所以 n 阶可逆方阵关于乘法组成的群不是交换群)；
(*2*)、关于有结合律，即，
$\cdot R$ 对 $\cdot$ 构成一个半群；
(*3*)、分配律与结合律对成立，即，有:；
称代数系统是一个环 *(Ring)*。

域的定义有两种方式：

定义 1.3: 域的定义

第一种定义是 D 是一个有单位元 $e(\neq 0)$ 的交换环（即对于乘法运算可交换），如果 D 中每个非零元都可逆，称 D 是一个域。（比如有理数域，剩余类域，典型域，有理函数域，半纯函数域等等）。

定义 1.4: 域的定义

第二种定义，设 $< R, +, * >$ 是环，如果 $< R, + >$ 和 $< R-0, * >$ 都是交换群（0 为 $< R, + >$ 的幺元）且满足分配律，则称 $< R, +, * >$ 是域。比如 D 是一个含有非零数的数集，如果 D 对于数的四则运算都封闭，那么称代数系统 $(D, +, -, \times, \div)$ 为一个域。

有理数域 $(Q, +, *)$，实数域 $(R, +, *)$，复数域 $(C, +, *)$，连续函数域 $(R^R, +, \cdot)$ 都是域。但整数集 Z 不是域，因为 $\frac{1}{x}$ 不是整数。（整数集 Z 是一个环，是整环）。

线性代数就是域的一个特例。

抽象代数与数学其它分支相结合产生了代数几何、代数数论、代数拓扑、拓扑群等新的数学学科。抽象代数已经成了当代大部分数学的通用语言。

在抽象代数研究的代数结构中，最简单的是群（Group）。它只有一种符合结合率的可逆运算，通常叫“乘法”。如果这种运算也符合交换率，那么就叫阿贝尔群（Abelian Group）。

群论是伽罗华（Galois）在研究多项式方程根式求解过程中提出的，是抽象代数的起点。

所以想理解抽象代数，就得先理解群论，想理解群论，就得先理解伽罗华理论，想理解伽罗华理论，就得先了解拉格朗日的代数方程工作。

1.3　代数方程的历史

我们在初中就知道的一元一次和一元二次方程的求解方法其实在古巴比伦时代就存在了，但是一元三次方程解的公式直到十六世纪初才由意大利人塔塔

里亚发现。

三次方程被解出来后，一般的四次方程很快就被意大利人的费拉里解出。

先补充介绍一下一元一次方程到一元四次方程的解法，这个与后来的群的思想有关。

一次方程：$ax+b=0$，只要是学过初等代数的都会解：$x=-\frac{b}{a}$。

二次方程：$ax^2+bx+c=0$, 解是:$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$，这个用因式分解很容易。

在公元前巴比伦人已能解这种形式的方程。

三次方程：$ax^3+bx^2+cx+d=0$ 和四次方程 $ax^4+bx^3+cx^2+dx+e=0$ 的解法比解一次，二次的方程难得多了。

对一般三次方程 $ax^3+bx^2+cx+d=0$，先除掉 a，令 $b\div a=a$，$c\div a=b$，$d\div a=c$，原方程变成：

$x^3+ax^2+bx+c=0$，

令 $y=x+\frac{a}{3}$，得：$y^3+py+q=0$。（1）

其中 $p=b-\frac{a^2}{3}$，$q=\frac{2a^3}{27}-\frac{ab}{3}+c$，考虑等式 $(u+v)^3=u^3+v^3+3(u+v)uv$.

即 $(u+v)^3-3(u+v)uv-(u^3+v^3)=0$。（2）

比较（1）和（2），令 $y=u+v$，

则方程（2）变为：$(u+v)^3+p(u+v)+q=0$，其中 $p=-3uv$,$q=-(u^3+v^3)$。

即 $u^3v^3=-\frac{p^3}{27}$，$u^3+v^3=-q$。（3）

则得到 $v^6+qv^3-\frac{p^3}{27}=0$

把 v^3 当成 x, 则是一个二次函数，易解得，$u^3=-\frac{q}{2}+((\frac{q}{2})^2+\frac{p^3}{27})^{\frac{1}{2}}$，$v^3=-\frac{q}{2}-((\frac{q}{2})^2+\frac{p^3}{27})^{\frac{1}{2}}$;

由于 u,v 对称，所以也有 $v^3=-\frac{q}{2}+((\frac{q}{2})^2+\frac{p^3}{27})^{\frac{1}{2}}$，$u^3=-\frac{q}{2}-((\frac{q}{2})^2+\frac{p^3}{27})^{\frac{1}{2}}$ 同时成立;

所以可得到:

$y=(-(\frac{q}{2})+(\frac{p^3}{27}+\frac{q^2}{4})^{\frac{1}{2}})^{\frac{1}{3}}+(-(\frac{q}{2})-(\frac{p^3}{27}+\frac{q^2}{4})^{\frac{1}{2}})^{\frac{1}{3}}$，进而可得到原方程根 x 的值。

同理整理四次方程，对于 $x^4+ax^3+bx^2+cx+d=0$，令 $y=x+\frac{a}{4}$，则原方程可变为：

$y^4+py^2+qy+r=0$。（4）

其中 $p=b-6(\frac{a}{4})^2$，$q=c-(\frac{a}{c})b+(\frac{a}{2})^3$，$r=d-(\frac{a}{4})c+(\frac{a}{4})^2b-3(\frac{a}{4})^4$ （4）

移项，得：$y^4+py^2=-qy-r$。（5）

（5）等式左边配方，得：$(y^2+\frac{p}{2})^2=-qy-r+(\frac{p}{2})^2$

在左端括号内加 u 得：$(y^2+\frac{p}{2}+u)^2=-qy-r+(\frac{p}{2})^2+2uy^2+pu+u^2$。（6）

则右端应为完全平方数，故有：$\Delta=q^2-4\times 2u(\frac{p^2}{4}+pu+u^2-r)=0$。（二次方程可以分解为 $(x-\frac{(-b+(b^2-4ac)^{\frac{1}{2}})}{2a})(x-\frac{(-b-(b^2-4ac)^{\frac{1}{2}}}{2a})$，如果 Δ 不等于零，就无法满足右端完全平方数条件。（$\Delta=b^2-4ac$）。

即：$8u^3+8pu^2+(2p^2-8r)u-q^2=0$。（7）

（7）显然为可解的三次方程，解答该方程就可得到 u 的值。

而且（6）就变为 $(y^2+\frac{p}{2}+u)^2=((2uy)^{\frac{1}{2}}-(\frac{q}{2}(2u)^{\frac{1}{2}}))^2$。

因此有 $y^2+\frac{p}{2}+u=(2uy)^{\frac{1}{2}}-((\frac{q}{2})(2u)^{\frac{1}{2}})$

由于 u 已经解出（按照三次方程解法，有两组，每组三个值），p,q,r 都是已知的方程系数（见（4））所以这个二次方程很容易得到 y 的值，进而得到原方程的根 x 的值。

上面工作都是初等数学，学过初中一年级因式分解，理解毫无问题。

注意，数学家的大招马上就来，一步从初中跨入大学。当然后面内容也是检验一个人抽象思维能力的试金石，看不懂的话，也就没法从事数学工作了。

1.4　拉格朗日工作

在介绍拉格朗日工作前，我们先得介绍韦达定理。

定理 1.1: 韦达定理

设 $x_1, x_2, \cdots, x_n$ 是方程 $x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$ 的 n 个根，则：

$$x_1 + x_2 + \cdots + x_n = -a_1$$

$$x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n = a_2$$

$$\cdots$$

$$x_1x_2 \cdots x_n = (-1)^n a_n$$

韦达定理很容易用数学归纳法证明。

下面介绍一下简单置换的记号：

$x_1, x_2, x_3, \cdots x_n$, 如果进行置换，例如 x_1 置换成 x_2,x_2 置换成 x_3,$\cdots$ x_n 置换成 x_1, 记成 $(123\cdots n)$，置换不变，记为 1。显然 n 元素所有的置换是一个 $n!$ 元素的集合。

先介绍拉格朗日的发现，然后介绍其发现过程。

拉格朗日发现：

□ 解一元三次方程需要预解二次辅助方程，解一元四次方程需要预解三次辅助方程。

□ 要解高次方程主要是解它的辅助方程。

□ 辅助方程的次数必须小于原方程的次数，不然原方程一般不可解。（当然解三次方程时的辅助方程是六次的，是因为可按二次方程求，所以本质还是降阶了）

□ 由于辅助方程解的表达式可以任意交换其系数 a, b, c 的位置（因为对称），即 3 次方程的解的表达式有 $3! = 3 \times 2 = 6$ 个。（Lagrange 原话是：方程的解其实不依赖 a, b, c 的值，而是依赖辅助方程结构在原方程根下置换出的不同值的个数）。

至此，解代数方程必有置换的想法已正式形成（也即 n 次方程的 n 个根的排列顺序有 $n!$ 个，或者说这 $n!$ 个排列组合的根，都是方程的解，也即方程根时对称的）。

这是一个很重要的发现：也即方程解必须满足置换条件，这也就是伽罗华从研究求解转为研究代数方程结构的起点，他通过研究根组成的集合（置换群）的性质，证明了：大于五次的方程的根组成的置换群其性质导致其不可通过辅助方程降阶，也即不可以用有理运算和方根求解）。

□ 辅助方程的关键是找到根的表达式——预解式（为原方程根的函数），解方程只需要找到预解式。

所以解代数方程实际是要解辅助方程，因此要寻找一个预解式，此预解式在原方程根的置换下取不同值的个数即为辅助方程的次数，找到了合适的预解式就得到了辅助方程（辅助方程的系数可由原方程的系数表示），解答了辅助方程就可以顺利的得到原方程的根。

因为只要有了预解式，就很容易得到它在原方程根下置换出不同值的个数，那么辅助方程的次数就确定了。

下面介绍拉格朗日的工作过程。

先用二次方程来解释他的思考过程。

考虑二次方程 $x^2+px+q=0$，设 x_1,x_2 是其两个解，构造预解式 $r_1=x_1-x_2$，$r_2=x_2-x_1$，显然 r_1,r_2 在置换 S(2)（包括置换 1 和（12），其实 1 和（12）就是一个 2 阶置换群）下，有 $r_1\to r_1$，$r_2\to r_2$；$r_1\to r_2$，$r_2\to r_1$。

构造以 r_1,r_2 为根的辅助方程（也称预解方程）

$\Phi(X)=(X-r1)(X-r2)$，这个方程显然在 S（2）下不变，

根据韦达定理，$r_1+r_2=-p$,$r_1r_2=q$，能够得到 $\Phi(X)=X^2-(p^2-4q)$

对一般 n 次方程，由于 $\Phi(X)$ 是根组成的置换群，是对称的，可以按照高中代数学过的牛顿多项式定理，得到：$\Phi(X)=$ 原方程系数构成的初等多项式表达，也即 $\Phi(X)$ 可以用原来方程的系数表达出来。

显然 X 有两个解：r_1,r_2,$(p^2-4q)^{\frac{1}{2}}$ 和 $-(p^2-4q)^{\frac{1}{2}}$，（当然 r_1,r_2 具体取值，是一个 2! 的排列组合）

$r_1=x_1-x_2$,$r_2=x_2-x_1$，原方程满足 $x_1+x_2=-p$，那么原方程解得到：$x_1,x_2=\dfrac{-p\pm(p^2-4q)^{\frac{1}{2}}}{2}$，具体 x_1,x_2 取值，也是 2! 个组合。

对一般三次方程 $x^3+px+q=0$(参见前面介绍，任意三次方程总能整理成

这个模式），假设 x_1, x_2, x_3 是其根，引入预解式：

$r_1 = x_1 + wx_2 + w^2x_3$,（其中 $x^3 = 1$ 的三个根表达为 1，w，w^2）

$x^n = 1$ 的解可以这样考虑，令 $x = r(isin\theta + cos\theta)$, 由于 $x^n = 1$，所以 $r = 1$，$n\theta = 2\pi k, k = 1, 2, \cdots, n-1$，方程的 n 个解分别为 $1, w, w^2, w^3 \cdots w^{n-1}$，其中 $w = \mathrm{e}^{\mathrm{i}2\pi/n}, e$ 是欧拉常数。（这是大学微积分常识）

用 $S(3)$ 做置换计算得到（$S(3)$ 包括：$1, (132), (321), (213), (231), (312)$ 等六个置换，这是一个六阶置换群）

$1 = x_1 + wx2 + w^2x3$

$r_2 = wx_1 + w^2x_2 + x_3$

$r_3 = w^2x_1 + x_2 + wx_3$

$r_4 = x_1 + w^2x_2 + wx_3$

$r_5 = wx_1 + x_2 + w^2x_3$

$r_6 = w^2x_1 + wx_2 + x_3$

做这种置换，是要用韦达定理把根与系数的关系建立起来.

定义预解方程 $\Phi(X) = (X - r_1)(X - r_2)\cdots(X - r_6)$

显然 $1 + w + w^2 = 0$，$w^3 = 1$（w 是 $x^3 = 1$ 的三个根之一）。

得到：$\Phi(X) = (X^3 - r_1^3)(X^3 - r_2^3) = 0$

令 $r_1^3 = u$,$r_2^3 = v$,$x^3 = t$, 则转化为一个二次方程，也即形如 $x^3 + px + q = 0$ 的一元三次方程的求根公式的形式应该为 $x = A^{\frac{1}{3}} + B^{\frac{1}{3}}$ 型，即为两个开立方之和。

（1）将 $x = A^{\frac{1}{3}} + B^{\frac{1}{3}}$ 两边同时立方可以得到

（2）$x^3 = (A + B) + 3(AB)^{\frac{1}{3}}(A^{\frac{1}{3}} + B^{\frac{1}{3}})$

（3）由于 $x = A^{\frac{1}{3}} + B^{\frac{1}{3}}$，

所以（2）可化为 $x^3 = (A + B) + 3(AB)^{\frac{1}{3}}x$，

移项可得

（4）$x^3 - 3(AB)^{\frac{1}{3}}x - (A + B) = 0$，

和一元三次方程和特殊型 $x^3 + px + q = 0$ 作比较，可知

(5)$-3(AB)^{\frac{1}{3}} = p, -(A + B) = q$，化简得

（6）$A+B=-q$，$AB=-(\frac{p}{3})^3$

（7）这样其实就将一元三次方程的求根公式化为了一元二次方程的求根公式问题，因为 A 和 B 可以看作是一元二次方程的两个根，而 (6) 则是关于形如 $ay^2+by+c=0$ 的一元二次方程两个根的韦达定理，即

（8）$y_1+y_2=-\frac{b}{a}, y_1y_2=\frac{c}{a}$

(9) 对比（6）和（8），可令 $A=y_1, B=y_2, q=\frac{b}{a}, -(\frac{p}{3})^3=\frac{c}{a}$

(10) 由于型为 $ay^2+by+c=0$ 的一元二次方程求根公式为 $y_1=-\frac{(b+(b^2-4ac)^{\frac{1}{2}}}{2a}; y_2=-\frac{(b-(b^2-4ac)^{\frac{1}{2}}}{2a}$ 可化为

(11)$y_1=-\frac{b}{2a}-((\frac{b}{2a})^2-(\frac{c}{a}))^{\frac{1}{2}}, y_2=-\frac{b}{2a}+((\frac{b}{2a})^2-(\frac{c}{a}))^{\frac{1}{2}}$

将 (9) 中的 $A=y_1, B=y_2, q=b/a, -(\frac{p}{3})^3=c/a$ 代入（11）可得

(12)$A=-(\frac{q}{2})-((\frac{q}{2})^2+(\frac{p}{3})^3)^{\frac{1}{2}}, B=-(\frac{q}{2})-((\frac{q}{2})^2+(\frac{p}{3})^3)^{\frac{1}{2}}$

(13) 将 A，B 代入 $x=A^{1/3}+B^{1/3}$ 得

(14)$x=(-(\frac{q}{2})-((\frac{q}{2})^2+(\frac{p}{3})^3)^{\frac{1}{2}}))^{(\frac{1}{3})}+((-(\frac{q}{2})+((\frac{q}{2})^2+(\frac{p}{3})^3)^{\frac{1}{2}}))^{\frac{1}{3}}$ 式

(14) 只是一元三方程的一个实根解，按韦达定理一元三次方程应该有三个根，不过按韦达定理一元三次方程只要求出了其中一个根，另两个根就容易求出了。

对于一般一元四次方程，$ax^4+bx^3+cx^2+dx+e=0$，拉格朗日照样构造预解方程 $r_1=x_1+ix_2-x_3-ix_4$, 然后经 S（4）置换，出来 24 组，

然后构造 $\Phi(X)=(X-r_1)(X-r_2)\cdots(X-r_24)$

根据上面解三次方程方法，拉格朗日解决了四次方程求根办法（具体写起来太复杂，纯粹是力气活，没创意，省略）。

按照拉格朗日方法，一元四次求根公式这种方法来解一元四次方程，只需求解一个一元三次方程即可。

根据上述结果，拉格朗日认为：解三次方程方法，辅助方程为二次的，解四次方程，辅助方程为 3 次的，那么解 n 次方程，只要找到 n-1 辅助方程，就可以解。

为这个目标，Lagrange 利用 1 的任意 n 次单位根 $(x^n = 1)$, 引进了预解式 $1+x+x^2+x^3+\ldots+x^{n-1}$ 来试图找到 n 次方程解法，但是用这种方法，Lagrange 进行五次及五次以上方程的尝试都失败了。

因为按照他的方法，解一元五次方程需要预解二十四次的辅助方程（Tschirnaus、Bezut、Euler 也得到同样的结果）。由此，他开始怀疑五次以上方程是无根式解的。

1771 年，拉格朗日发表长篇论文《关于方程的代数解法的思考》提出了这个怀疑。（不过德国数学家高斯在 1801 年，他解决了分圆方程 $x^p - 1 = 0$（p 为质数）可用根式求解，这表明并非所有高次方程不能用根式求解。因此，可用根式求解的是所有高次方程还是部分高次方程的问题需进一步查明）。

根据拉格朗日的判断，鲁菲力（Ruffini）1813 年，从反面论证高于五次的方程可能没有一般代数解，不过他的证明不严谨。

1826 年，阿贝尔严格证明：如果一个方程可以根式求解，则出现在根的表达式中的每个根式都可表示成方程的根和某些单位根的有理数。并且利用这个定理又证明出了阿贝尔定理：

一般高于四次的方程不可能代数地求解，这些方程的根不能用方程的系数通过加、减、乘、除、乘方、开方这些代数运算表示出来。但是阿贝尔没有回答每一个具体的方程是否可以用代数方法求解的问题。

阿贝尔还在在高斯分圆方程可解性基础上，证明了：

任意次的一类特殊方程的可解充分必要条件是全部根都是其中一个根（假设为 x）的有理函数，并且任意两个根 $q1(x)$ 与 $q2(x)$ 满足 $q1q2(x) = q2q1(x)$，$q1, q2$ 为有理函数。（现在称这种方程为阿贝尔方程）。

其实这就是群，只是阿贝尔没能意识到，也没有明确地构造方程根的置换集合（因为若方程所有的根都用根 x_1 来表示成有理函数 $q_j(x_1), j = 1, 2, 3, \cdots, n$，当用另一个根 x_i 代替 x_1 时，其中 $i \leq n$，那么 $qj(xi)$ 是以不同顺序排列的原方程的根，$j = 1, 2, \cdots, n$。也即根 $x_i = q_1(x_i), q_2(x_i), \cdots q_n(x_i)$ 是根 $x1, x2, \cdots, xn$ 的一个置换），阿贝尔仅仅考虑了根的可交换性：$q1q2(x) = q2q1(x)$，并证明方程只要满足这种性质，便可简化为低次的辅助方程，辅助方程可依次用根式求解。

所以阿贝尔解决了构造任意次数的代数可解的方程的问题，却没能解决判定已知方程是否可用根式求解的问题。

1.5　伽罗华出场了

伽罗华的思想来自于拉格朗日用置换的思想进行代数方程求解。

（1）、伽罗华从拉格朗日方程根的置换思想入手

为了介绍伽罗华从拉格朗日工作飞跃，我们用一个简单例子来解释。

拉格朗日已经意识到，如果一元 n 次方程能够变成 $[x-x(1)][x-x(2)]\cdots[x-x(n)]$ 这样彻底地分解因式，那么方程的解就得到了。但往往不能，必须扩张系数的数域才行。例如：

$f(x)=x^2+1$

这个多项式在实数范围内是不能分解的，如果允许把虚数单位 i 作为系数的话，这个式子可以分解成：

$f(x)=(x+\mathrm{i})(x-\mathrm{i})$

也即：当域的范围越大，在这个域中进行的因式分解就越彻底，当一个 n 次多项式可以被分解为 n 个一次多项式的乘积时，方程的 n 个解就找出来了。这个域叫做 $f(x)$ 的分裂域。

通过一系列的扩域就能把多项式的系数域扩张到多项式的分裂域，方程就找到解了。可是这里有一个核心问题：系数域可扩张为分裂域的充分必要条件是什么，或者是不是分裂域都是存在的（也即等价于一元 n 次方程都是有解的）。

由于域定义了四种运算（例如四则运算），拉格朗日发现域是一种非常难以把握的集合。而且一元 n 次方程涉及的大部分域都是无限域（有无限多的元素，比如实数域，有理数域），要准确地给出系数域可以扩张为分裂域的充分必要条件是非常困难的。

（2）、伽罗华的工作

伽罗华首先是对一元 n 次多项式方程可解的定义进行改进：

简单说是指经过有限次加、减、乘、除、乘方和开方运算可以表示出方程的

根。（这个定义的严格表达是：如果一个集合包含方程的系数，且对加、减、乘、除、乘方和开方封闭，那么求根公式的存在性等价于根在这个集合中的存在性。这个结论是显然的，多想一下就明白）。

所以一个代数方程是否有解，要看我们对于解所加的限制条件而定，例如如果允许 x 可以是负数的话，$x+5=3$ 是可解的，但是如果限定 x 不能是负数，那么这个方程就无解了。

同样，假使 x 表示有理数，方程 $2x+3=10$ 是可解的。如果 x 表示整数，这方程就无解了，因为 x=3.5 在整数里面没有意义。

再例如，要三等分任意一角，若只准用直尺与圆规，这是不可能的，但是若许用别的仪器，就可能了。

所以关键的一个要点来了：一个多项式是可以因式分解的或不可因式分解的，要看在什么数域中分解而定。例如 x^2+1 在实数域中就是不可分解的，但是在复数域中却是可分解的，因为 $x^2+1=(x+\mathrm{i})(x-\mathrm{i}), \mathrm{i}=(-1)^{\frac{1}{2}}$。所以，单说一个多项式是不是可因式分解的，而不说出在什么数域内，这其实是废话。

同理，一个命题在什么范围中是对的，在什么范围中是错的，甚而至于在什么范围中是绝对没有意义的也是这个道理。

伽罗华要解决的问题是：一般高于四次的方程不能用根式解。

不能用根式解，就是说方程的根不能用方程的系数通过有限次的有理运算（加，减，乘，除）和开方得到（或者说等价于方程的根不能表达成方程系数通过有理运算形成的函数）。

例如一次方程 $ax+b=0$，方程的根是 $x=-\dfrac{b}{a}$，也即 x 的值可以用 a 除 b 而得，这是一个有理运算。

二次方程 $ax^2+bx+c=0$，两根是 $x=\dfrac{-b\pm(b^2-4ac)^{\frac{1}{2}}}{2a}$，这也可以由方程系数经过有限次的有理运算和开方而得。

同样，一般的三次，四次方程的根也表达成用有限次的有理运算和开方方程系数的函数。

显然乘方是乘法的特例（反复乘法）。开方显然不是四则运算（域中被定义的运算只有加减乘除四种），所以必须把开方通过扩域的方式被加入到求根公式

允许的运算方式中。

所以伽罗华发展出了第一个重要的概念：扩域。也即伽罗华发现了：从包含方程系数的最小的域出发，通过域的扩张逐渐添加元素，直到把方程的所有解包含在某个扩域中为止：如果我们能这样做到，方程就是有解的，否则，方程就没有一般的求根公式。

（3）、伽罗华定理

基于上述发现，伽罗华继续努力。

对有理系数的 n 次方程 $x^n + a_1x^n - 1 + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0$，

假设它的 n 个根是 $x_1, x_2, \ldots, x_n$，伽罗华证明：

每个方程对应一个域（由方程系数和全部根组成，这个域定义为伽罗华域），每一个域与一个伽罗华群对应。

这也就意味着，伽罗华发现了研究一元 n 次方程解结构问题，可以转为研究伽罗华群结构性质。

伽罗华群定义：某个数域上任意一个一元 n 次多项式方程, 它的根的置换群里面某些置换所构成的一个子群，满足如下条件就被定义作该方程的伽罗华群：

对任意一个取有理数值关于根的多项式函数，伽罗华群中的每一个置换都使函数的值不变。同时，如果伽罗华群中每一个置换都使根的一个多项式函数的值不变，则这个多项式函数的值是有理的。

伽罗华域定义：对有理系数的 n 次方程 $x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0$，假设它的 n 个根是 $x_1, x_2, \cdots, x_n$，方程系数生成的域是 F，E 是把 n 个根添加到 F 上生成的域，又叫伽罗华扩域或伽罗华扩张。

伽罗华定理：假定 G 为这个方程的伽罗华群，一元 n 次方程是否有根式解的充分必要条件是：假定 F 是含有这个方程的系数及 $x^n = 1$ 的各次方根的最小域，那么 F 是否可以经过有限次添加根式扩张，成为 E。

也即是否存在有限多个中间域 $Fi(i = 1, 2, \cdots, k)$, 使 $F < F_1 < F_2 < \cdots < F_k < E$，其中每个 F_i 都是由 F_{i-1} 添加 F_{i-1} 数的根式产生的扩域。F 是方程系数和 1 的 n 次方根组成的最小域。

那么如何把伽罗华域伽罗华群联系起来呢？

伽罗华定义了域上自同构群。域上的自同构群概念的引入，使域与群发生

了联系，即建立了伽罗华域的子域与伽罗华群的子群之间的一一对应关系：保持 F 元素不动的的每个自同构决定方程根的一个置换, 它属于伽罗瓦群 G, 反之,G 中每个置换引起的一个自同构, 它使 F 的元素不动。

这样就建立了 E 的自同构群和方程的伽罗瓦群之间的同构。由此建立 E 的子域 (包含 F) 和 G 的子群之间的一一对应：保持子域 F_i 不动的 G 中全部置换构成的一个子群 G_i, 让 G_i 与 F_i 对应, 而且反过来也可用 G_i 来刻划 F_i, 即 F_i 是 E 中被 G_i 的每个置换保持不动的元素全体。也即 F_i 和 G_i 存在一一对应关系。

这就是伽罗瓦基本定理。显然利用这种一一对应关系，就可由群的性质刻划域的性质, 反之亦然。因此, 伽罗华的理论是群与域这两种代数基本结构综合的结果。

那么怎么用伽罗华群性质证明方程是否可解呢？

伽罗华在拉格朗日方法基础上，认为解方程，必须从预解式开始，当他构造二项方程作为预解方程时，发现其相应的置换子群应是正规子群且指数为素数才行。利用正规子群概念可以区分合成群与单群的概念，利用它的性质就可以判别已知方程能否转化为低次方程的可解性问题。这是伽罗华的第二个重要发现。

伽罗华的的思想是：

首先定义正规子群的概念：群 G 的子群 N 是 G 的正规子群，是指对每个 $g \in G$，$g^{-1}Ng = N$；

其次是寻找极大正规子群列，确定极大正规子群列的一系列合成因子。

伽罗华证明：伽罗华域 F，如果每次所添加的根式均为素数次根，那么, 那么 F 可以经过有限次添加根式扩张，成为 E（也即方程有根式解）。这时中间域 Fi 的结构等价于使 F_{i-1} 保持不变的的 Fi 自同构置换群的结构。这样的自同构群是素数阶的循环群, 且阶数为 $(F_i : F_{i-1})$。

伽罗华因此定义：如果一个群所生成的全部合成因子都是素数，则称这个群为可解的。

这样就利用可解群的概念全面刻划了用根式解方程的特性，给出了一个方程可用根式解的判别准则是：一个方程可用根式解的充要条件是这个方程的伽罗华群是可解群。

这样伽罗华证明了：一元 n 次多项式方程能用根式求解的一个充分必要条件是该方程的伽罗华群为可解群。这时是 1832 年。

由于高于四次的一般方程的伽罗华群不是可解群，也就直接推论出高于四次的一般方程的不可解性。

也即伽罗华发现本质就是：域的无数种扩张方式其实就是有限阶的群。n 阶对称群对应着 n 次一元方程，而 5 阶和 5 阶以上的对称群不是可解群，也就是五次和五次以上的代数方程没有求根公式。

（4）、伽罗华的创造

□ 先不忙考虑求解方法，先证明解是不是存在，不然就是无用功，也即伽罗华把存在性证明与数的计算相分离，这是人类伟大的一步。

□ 通过研究根式扩张和根对称性得出代数方程是否可解。也即发现方程解的对称性和解的结构，决定是否可以根式解。

具体说就是伽罗华发现：一个多项式方程有根式解的话，各个根的对称性要满足一定关系：出现在根的表达式中的每个根式，一定可以表成方程诸根及某些单位根的有理函数。五次以上的方程这个关系不一定满足。

伽罗华的发现证明：计算不如结构重要。

伽罗华定义的群本质就是方程根形成的集合必须具有对称性质。

如果解集上定义某种两两映射（同构），如果能保持解集不变，解集就是对那个自同构对称的。

事实上，如果解集存在，保持解集不变的自同构一定是存在的（很容易证明）。因为至少有一个恒等自同构，即从自身映射到自身。再比如一元二次方程有两个根 x_1 和 x_2，那么 x_1 到 x_2 的映射也是一个自同构。

这就是说，如果某个扩张域是存在的，扩张所对应的自同构也一定存在，这两个存在性是等价的。所以扩域的研究自然而然地变成了对自同构的研究。

至此为止，我们把伽罗华的基本思想介绍完了。至于细节，我们在下面简单介绍一下，对不想麻烦的人，不看也可以。

附：五次以上方程不可解性的严格证明（给一个抽象代数教科书典型的证明定理的例子）

证：若 $S5$（五阶置换群）是可解的，则存在正规子群 N 使 $S5/N$ 可交换。

设 f 为 $S5$ 到 $S5/N$ 的自然同态，考察三项循环 $(a,b,c) \in S5$，再取另两元 d,e。令 $x=(d,b,a)$，$y=(a,e,c)$。$x^{-1}y^{-1}xy$ 的 f 像为 $x'^{-1}y'^{-1}x'y' \in S5/N$，由 $S5/N$ 可交换知 $x'^{-1}y'^{-1}x'y'=1$，即有 $x^{-1}y^{-1}xy=(a,b,c) \in N$。故 N 包含所有三轮换，同理其正规群列均包含三轮换，所以不可能结束于 1。这就是 5 次以上一元方程不可解的证明。

1.6 说点细节

其实伽罗华关键工作我们已经介绍完了。下面说点细节。

伽罗华定义的的群并不是现在抽象代数定义的群（最前面介绍的），伽罗华定义群是方程根的置换。从直觉来看，方程的解显然和它们的顺序无关，所以当置换作用于方程的解集合时，方程对这种变换而言是对称的。

伽罗华发现满足这些条件的集合（群）的结构是非常固定的。举个最简单的例子：包含三个元素的群的结构一定是 $(0,1,-1)$，其中 0 是恒等元，-1 是 1 的逆元。（但是 5 阶以上的对称群不一定是可解群，所以 5 次以上的代数方程没有一般的求根公式）。

在 1831 年的论文中，伽罗华首次提出了群这一术语，把具有封闭性的置换的集合称为群，首次定义了置换群的概念。他发现置换群是解方程的关键，方程的根是一个置换群。他从此开始把解方程问题转化为置换群结构问题 (其实群这个概念不是伽罗华原创，柯西在 1813 年就提出了，只是没能进一步发现：群的基本性质对称结构对一元 n 次多项式方程解的关系）。

（1）、群的定义

□（封闭性）集合中任意两个元素用规定的运算时，所得的结果还是系统中的一个元素。也即集合 G，任意 x,y 属于 G，集合 G 上定义的运算为 $*$，$x*y$ 也一定属于 G。（这个运算 * 的定义是广义的，既可以是加减乘除等运算，也可以是旋转，置换等等一切行为）。

例如：一个整数加到另一个整数上去的结果还是一个整数；两个有理数相乘的结果还是一个有理数；一个置换将 x_1 变成 x_2,x_2 变成 x_3,x_3 变成 x_1, 另外一

个置换是将 x_2 变成 x_1,x_3 变成 x_2,x_1 变成 x_3，那末这两个置换结合仍然是一个置换；平面一个 60 度的旋转（逆时针方向）之后跟着一个 120 度的旋转 (逆时针方向)，结果是一个 180 度的旋转 (逆时针方向)，仍然是一个旋转等等。

□ 结合律必须成立。也即任意 x, y, z 属于 G，$(x * y) * z = x * (y * z)$。

□ 集合中必须含有单位元，也即与集合中任意另一个元素运算的结果仍是那另一个元素。也即集合 G 存在单位元 e，任意一个 x 属于 G，$e * x = x$。

例如，在定义加法的整数中，单位元是 0，因为 0 与任何整数相加的结果还是那个整数；在定义乘法的有理数中，单位元是 1，因为任意一个有理数用 1 乘了之后的积还是那个有理数；在置换中，单位元就是那个将 x1 变成 x1，x2 变成 x2，x3 变成 x3 的置换，因为任意一个置换和这个置换结合的结果还是那个置换；在平面旋转中，单位元就是那个 360 度的旋转，因为集合中任意一个旋转和这个旋转结合的结果还是那个旋转等等。

□ 每个元素必须有一个逆元素：一个元素和他的逆元素用集合上定义的运算结合的结果是单位元。也即任意 x 属于 G，存在 x^-,$x^- * x = e$。

例如，在整数集合中，定义加法，3 的逆元素就是-3，因为 3 加上-3 的和是 0；在有理数集合中定义乘法，则 a/b 的逆元素是 b/a, 因为 a/b 和 b/a 相乘的积是 1；在置换中，将 x_1 变成 x_2,x_2 变成 x_3,x_3 变成 x_1 的置换的逆元素是那个将 x_2 变成 x_1,x_3 变成 x_2，x_1 变成 x_3 的置换，因为这两个置换结合的结果是那个将 x_2 变成 x_2,x_3 变成 x_3,x_1 变成 x_1 的置换；在平面旋转中，那个 60 度的旋转（逆时针方向）的逆元素是一个一个顺时针方向的 60 度的旋转，因为这两个旋转结合的结果和那个 360 度的旋转一样。

满足上述的四条性质，就是一个群。

如果在整数上定义加法，但是若把 0 去掉，就不成为群了，因为没有单位元；一切整数用乘法作集合中的运算不是群，例如 3 的逆元素 $\frac{1}{3}$ 不在整数集合中。

所以一个集合是否是群，不但与元素有关，也与运算有关。

前面已经说了，群的元素不必一定是数，可以是一种运动（如平面旋转），也可以是一种动作（例如置换）；运算不必一定要是加法或乘法，或寻常算术，抽象代数中所称为的运算，可以是任何定义，例如乘法可以是一个置换跟着另一

个置换，也可以说是一个置换乘另一个置换。这个乘法与普通算术或代数中乘法不是一个概念，千万不要蒙，而且群定义的广义的乘法的性质可以和普通乘法的性质大异，例如，在普通的乘法中，$2*3=3*2$（普通的乘法是适合交换律的），也即普通乘法中因子的次序可以交换，结果相同。可是，置换中的“乘法”，交换律就不成立了，例如将 x_1 变成 x_3，x_3 变成 x_1，x_2 变成 x_2 的置换和一个将 x_1 变成 x_2，x_2 变成 x_3，x_3 变成 x_1 的置换就没有交换律，如果先进行第一个置换然后进行第二个置换于式子 $x_1x_2+x_3$，那末，这式子先变成 $x_3x_2+x_1$，再变成 $x_1x_3+x_2$；如果将置换的次序交换一下，那末，原来的式子先变成 $x_2x_3+x_1$，再变成 $x_2x_1+x_3$，这个结果显与前面一个不同。所以群里面定义的“乘法”是不需要适合交换律的，因此，相乘时元素的次序很重要；两个元素用运算结合时当照一定的次序结合。

（2）、置换群

伽罗华用来解方程的是置换群 (SubstitutionGroup)，下面先介绍一下记号。

一个将 x_1 变成 x_2,x_2 变成 x_3,x_3 变成 x_1 的置换，可以用简单记号来表示：x 可以省去，只要用 1,2,3 来代表于是这个置换可以记作 (123)，这记号的意思是说：1 变作 2，2 变作 3，3 变作 1。也即：x_1 变作 x_2，x_2 变作 x_3，x_3 变作 x_1。（每个数变作他后一个数，而最后的一数则变成最先的一数，如此完成一个循环）

同样，一个将 x_2 变成 x_3,x_3 变成 x_1,x_1 变成 x_2 的置换可以记作 (231)；同样 (132) 表示一个将 x_1 变成 x_3,x_3 变成 x_2,x_2 变成 x_1 的置换；又如 (13)(2) 或 (13) 表示一个将 x_1 变成 x_3,x_3 变成 x_1,x_2 变成 x_2 的置换，所以前面讲乘法交换律时所说两个置换相乘的例子，若照第一种次序是 (13)(123)=(23)；若照第二种次序是 (123)(13)=(12)，由这两个式子就知道这种乘法是不适合交换律的，将一个元素右乘或左乘另一个元素，他的结果是完全不同的。

一个群的一部分元素构成一个群，这种群称为子群 (Subgroup)。例如整数集定义加法成为群，单拿偶数集，定义加法，也成一群：因为群的四个性质都能适合：

- 两个偶数的和还是偶数；
- 零是单位元；
- 一个正偶数的逆元素是一个负偶数，而一个负偶数的逆元素是正偶数；

□ 结合律成立。

所以单是偶数全体对于加法而言是一个群，这个群就是是那个由一切整数定义加法而成的群的子群。

再例如，一个置换群（即是以置换作元素的群）也可以有子群。

例如，$1,(12),(123),(132),(13),(23)$ 六个置换构成一个群（1 表示那个不动置换，即是将 x_1 变成 x_1,x_2 变成 x_2,x_3 变成 x_3 的置换)，因为群的四条性质都成立：这六个置换中每两个的积还是这六个中的一个置换，例如 (12)(123)=(13)，(123)(132)=1,(13)(23)=(123)，(123)(123)=(132)，等等）单位元是 1；每个元素的逆元素都在这六个元素之中，比如 (123) 的逆元素是 (132)，(12) 的逆元素是 (12) 等等；结合律成立。

现在从这六个置换中取出 1 和 (12) 两个来，这两个元素也成为一个群，这是原来那个群的子群。

很容易证明：子群的元数 (即集合中元素的个数) 是原来的群的元数的约数（拉格朗日定理）。

（3）、不变子群

最重要的子群是不变子群。

变换的直观定义：群中一个元素若以另一个元素右乘，再用这另一个元素的逆元素左乘，所得结果称为元素应用另一个元素的变换。

例如一个元素 (12), 我们用另一个元素 (123) 去右乘他，再用 (123) 的逆元素 (132) 去左乘他，结果是 (132)(12)(123)=(23)，(23) 就称为 (12) 应用 (123) 的变换。

定义：一个子群中任何元素应用原来的群中任何元素的变换，若仍是子群中的元素，这子群就称为原来那个群的不变子群。

对伽罗华理论来讲，不变子群是很重要的概念。

定义：设 H 是 G 的不变子群，假如 G 中没有包含 H 而且比 H 大的不变真子群存在时，H 就称为 G 的一个极大不变真子群。

定义：假设 G 是一个群，H 是 G 的一个极大不变真子群，K 是 H 的一个极大不变真子群..... 若将 G 的元数用 H 的元数去除，H 的元数用 K 的元数去除，..... 如此所得的系列数，就称为群 G 的组合因数，假设这些组合因数都是素数，就说 G 是一个可解群（可解的含义后面再介绍）。

在有些群中，群中的一切元素都是某一个元素 (不是单位元) 的乘幂，比如在群 1,(123),(132) 中，2(123)=(123)(123)=(132)3(123) =(123)(123)(123)=1，这群中的元素都是 (123) 的乘幂，像这种群，称为循环群。

在一个置换群中，如果每个元素都有一个而且只有一个置换将元素换成其他某一个元素 (这个元素也可以和原来那个元素相同)，那末，这个群就称为正置换群。

例如前面所说的群 1,(123),(132) 在 1 中 x_1 变成 x_1, 在 (123) 中 x_1 变成 x_2, 在 (132) 中 x_1 变成 x_3，..... 所以这是一个循环正置换群。这种群在方程的应用上很重要。

伽罗华证明：对于一个一定的数域，方程 $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ 的根都能构造一个置换群，群的阶数是 $n!$。

例如对三次方程：$ax^3 + bx^2 + cx + d = 0$，假定它的三个根 x1,x2,x3 是不同的，随便取一个这三个根的函数，例如 $x1x2 + x3$，在这函数中，我们若将这些 x 互相替换，那末，一共有多少种置换呢？

显然只有 1,(12),(13),(23),(123),(132) 六个置换（3!）。

(12) 置换，也即将 $x_1x_2 + x_3$ 变成 $x_2x_1 + x_3$；(13) 置换，就是将 $x_1x_2 + x_3$ 变成 $x_3x_2 + x_1$ 等等。

(123) 置换就是把原来的函数变成 $x_2x_3 + x_1$。而 1 就是不动置换了。所以对于这三个 x，一共有 3! 种可能的替换。

同理，对于四个 x 有 4！种可能的置换，一般的情形，n 个 x 就有 n! 可能的替换。

当然一个函数进行一个置换的时候，函数的值可以因此而变，也可以仍旧不变，例如若将 (12) 这个置换施行于函数 x1+x2，这函数的值不变，可是，若将 (12) 施行于函数 x1-x2，函数的值就由 x1-x2 一变而为 x2-x1 了。

计算一个已知 n 次方程的伽罗华群是很困难的，因此伽罗华认为目标不在于计算伽罗华群，而是证明：

对任意 n 次方程，其伽罗华群是方程根的最大置换群 $S(n)$，$S(n)$ 是由 n! 个元素集合构成的，S(n) 中的元素乘积实际上是指两个置换之积。现在把 S(n) 中的元素个数称为阶，S(n) 的阶是 n!。

伽罗华找出方程系数域中的伽罗华群 G 后，找到它的最大真子群 H_1，用有理运算来构造根的一个函数 $\Phi 1(x)$，$\Phi 1(x)$ 的系数属于方程的系数域 R，并且在 H_1 的置换下不改变值，但在 G 的所有别的置换下改变值。

再用上述方法，依次寻找 H_1 的最大子群 H_2，再找到一个函数 $\Phi 1(x)$，$\Phi 1(x)$ 的系数属于方程的系数域 $R1$;再找到 H_2 的最大子群 $H_3, \cdots$ 于是得到 $H_1, H_2, \cdots, H_m$，直到 H_m 里的元素恰好是恒等变换（即 H_m 为单位群 1）。

在得到一系列子群与逐次的预解式的同时，系数域 R 也随之一步步扩大为 $R_1, R_2, \cdots, R_m$，每个 R_i 对应于群 H_i。当 $H_m = 1$ 时，R_m 就是该方程的根域，其余的 $R_1, R_2, \cdots, R_{m-1}$ 是中间域。

我们从拉格朗日工作已经知道一个方程可否根式求解与根域的性质密切相关。

于是，伽罗华引出了根式求解原理，并且还引入了群论中的一个重要概念“正规子群”

（4）、正规子群

正规子群定义：设 H 是 G 的一个子群，如果对 G 中的每个 g 都有 $gH = Hg$，则称 H 为 G 的一个正规子群。

伽罗华证明：当作为约化方程的群 (如由 G 约化到 H_1) 的预解式是一个二项方程 $x^p = A$ (p 为素数) 时，则 H_1 是 G 的一个正规子群。反之，若 H_1 是 G 的正规子群，且指数为素数 p，则相应的预解式一定是 p 次二项方程。

极大正规子群：如果一个有限群有正规子群，则必有一个子群，其阶为这有限群中所有正规子群中的最大的，这个子群称为有限群的极大正规子群。

一个极大正规子群又有它自己的极大正规子群，这种序列可以逐次继续下去。因而任何一个群都可生成一个极大正规子群序列。

把一个群 G 生成的一个极大正规子群序列标记为 $G, H_1, H_2, H_3 \cdots$, 则可以确定一系列的极大正规子群的合成因子 $[G/H1], [H1/H2], [H2/H3] \cdots$。合成因子 [G/H]=G 的阶数/ H 的阶数。例如对上面的四次方程 $x^4 + px^2 + q = 0$，H_1 是 G 的极大正规子群，H_2 是 H1 的极大正规子群，H3 又是 H2 的极大正规子群，即对方程 $x^4 + px^2 + q = 0$ 的群 G 生成了一个极大正规子群的序列 G、H1、H2、H3。

伽罗华在此基础上定义可解群：如果它所生成的全部极大正规合成因子都是素数。也即伽罗华群生成的全部极大正规合成因子都是素数时，方程可用根式求解。若不全为素数，则不可用根式求解。

或者说：当且仅当一个方程系数域上的群是可解群时，该方程才可用根式求解。

可解性的性质在某一意义上是可继承的，如：

若 G 为可解的，且 H 为 G 的子群，则 H 也是可解的。

若 G 是可解的，且 H 为 G 的正规子群，则 G/H 也是可解的。

若 G 是可解的，且存在一 G 满射至 H 的同态，则 H 也是可解的。

若 H 及 G/H 为可解的，则 G 也是可解的。

若 G 及 H 为可解的，则其直积 $G \times H$ 也是可解的。

例如 $x^4 + px^2 + q = 0$，它的 [G/H1]=8/4=2，[H1/H2]=2/1=2，2 为素数，所以 $x^4 + px^2 + q = 0$ 是可用根式解的。

再看一般的 n 次方程，当 n=3 时，有两个二次预解式 $t^2 = A$ 和 $t^3 = B$，合成序列指数为 2 与 3，它们是素数，因此一般三次方程可根式解。同理对 $n = 4$，有四个二次预解式，合成序列指数为 2，3，2，2，于是一般四次方程也可根式求解。

（5）、5 次以上一元方程不可解

一般 n 次方程的伽罗华群是 s(n)，s(n) 的极大正规子群是 A(n) (A(n) 是由 s(n) 中的偶置换构成的一个子群。如果一个置换可表为偶数个这类置换之积，则叫偶置换。)，A(n) 的元素个数为 s(n) 中的一半，且 A(n) 的极大正规子群是单位群 1，因此 [s(n)/A(n)]=n!/(n!/2)=2，[A(n)/I]=(n!/2)/1=n!/2，2 是素数，但当 n ≥5 时，n！/2 不是素数，所以一般的高于四次的方程是不能用根式求解的。

例如，四次方程 $x^4 + px^2 + q = 0$，p 与 q 独立，系数域 R 是添加字母或未知数 p、q 到有理数中而得到的域，先计算出它的伽罗华群 G。

G 是 $S(4)$ 的一个 8 阶子群,$G = E, E1, E2, \cdots E7$，其中 $E = 1, E1 = (1234), E2 = (2134), E3 = (2143), E4 = (3412), E5 = (4312), E6 = (3421), E7 = (4321)$。

要把 R 扩充到 R1，需在 R 中构造一个预解式:$t^2 - (p^2 - 4q) = 0$，

则添加预解式的根 $((p^2-4q))^{\frac{1}{2}}$ 到 R 中得到一个新域 R1，于是可证明原方程 $x^4+px^2+q=0$ 关于域 $R1$ 的群是 $H1$，$H1=E,E1,E2,E3$，并发现预解式的次数等于子群 $H1$ 在母群 G 中的指数 $8\div 4=2$（即指母群的阶除以子群的阶）。

然后构造第二个预解式 $t^2-2(-p-(p^2-4q)^{\frac{1}{2}})$，

解出根 $(2(-p-(p^2-4q)^{\frac{1}{2}}))^{\frac{1}{2}}$ 在域 R1 中添加得到域 R2，同样找出方程 $x^4+px^2+q=0$ 在 R2 中的群 H2，$H2=E,E1.$

此时第二个预解式的次数也等于群 $H2$ 在 $H1$ 中的指数 $4\div 2=2$。

再然后构造第三个预解式 $t^2-2(-p+(p^2-4q)^{\frac{1}{2}})$，得它的根 $2(-p+(p^2-4q)^{\frac{1}{2}}))^{\frac{1}{2}}$，把添加到 $R2$ 中得扩域 $R3$，此时方程 $x^4+px^2+q=0$ 在 R3 中的群为 $H3\square H3=E$，即 H3=1，则 R3 是方程 $x^4+px^2+q=0$ 的根域，且该预解式的次数仍等于群 H3 在 H2 中的指数 $2\div 1=2$。

在这个四次方程中，系数域到根域的扩域过程中每次添加的都是根式，则方程可用根式解。

这种可解理论对于一般的高次方程也同样适用，只要满足系数域到根域的扩域过程中每次都是添加根式，那么一般的高次方程也能用根式求解。

现仍以四次方程 $x^4+px^2+q=0$ 为例，伽罗华从中发现了这些预解式实质上是一个二次的二项方程，既然可解原理对高次方程也适用，那么对于能用根式求解的一般高次方程，它的预解式方程组必定存在，并且所有的预解式都应是一个素数次 p 的二项方程 $x^p=A$。由于高斯早已证明二项方程是可用根式求解的。因此很容易得到：如果任一高次方程所有的逐次预解式都是二项方程，则能用根式求解原方程。

至此，伽罗华完全解决了方程的可解性问题。

（6）、用直尺与圆规的作图

伽罗华解决了用直尺与圆规的作图难题。

伽罗华发现了判别方程能否用根式解的方法后，他还解决了如何求一个能用根式解的方程的根的方法，这方法是利用一组辅助方程，这些辅助方程的次数恰是原来那个方程的群的组合因数。

基本流程如下：先把第一个辅助方程的根加入数域 F 中，将数域扩大了可

以增加 $P(y)$ 分解因数的可能性，也能将 $P(y)$ 的不可约部分减少，因此能将方程的群变小，当然，必须数域扩大了之后的确能继续分解 $P(y)$ 的因数，才会成立。

现在假设数域经第一个辅助方程的根加入而扩大了，而且使分解因数的工作因之可以再继续下去，结果使方程在这扩大了的数域 $F1$ 中的群是 H。

再将第二个辅助方程的根加入 $F1$ 中，使方程的群变为 K，如此持续，直到后来，方程在那个最后扩大成的数域 Fm 中的群是 1。函数 $x1$ 显然不能被群 1 中的置换变更他的值，所以 $x1$ 必在数域 Fm 中。仿此，其余的根也都在 Fm 中。

这样先决定了方程的群和此群的组合因数，才知道辅助方程的次数。由此我们可以知道什么样的数应该加入原来的数域里去，而把方程的群变为 1。于是可以决定方程的根存在于怎样一个数域中。

现在用方程 $x^3-3x+1=0$ 为例,这个方程在有理数域中的群是由 1,(123),(132) 三个置换构成的，其唯一极大不变真子群是 1，所以组合因数是 3, 所以有一个次数是 3 的辅助方程，而这个辅助方程的根含有一个立方根，所以这个立方根必须加入数域中，才能使方程的群变为 1，这样原来的方程的根可以从有理数域中的数及这个立方根用有理数运算得出。

直尺与圆规作图等价于直线和圆作交点图。也即求一次和二次方程的交点，只要解一个二次方程就可以把交点的坐标用有理运算和平方根表作系数的函数。所以凡是能用直尺与圆规作出的图都可以有限次的加，减，乘，除和平方根表出，而且假使给了两线段 a,b 和单位长度，我们可以用直尺与圆规作出他们的和 $a+b$, 差 $a-b$, 积 ab, 商 $\frac{a}{b}$, 以及这些量的平方根如 $(ab)^{\frac{1}{2}}$,$b^{\frac{1}{2}}$ 之类，这种运算当然可以重复应用于一切已经作出的线段。

一个作图单用直尺，圆规是否可能时，必须作出一个表示这作图的代数方程：假使这方程在数域中可以分解成单是一次和二次的代数式，那么，一切实数根当然都能用直尺与圆规作出。即使方程不能分解成上述的样子，只要方程的实数根能用有限次的有理运算与平方根作已知的几何量的函数，那末这作图单用直尺，圆规还是可能的，否则这作图就不可能了。

也即立方根是无法靠直尺和圆规作出的。

如果能够找到一个三等分角的方程是不能用直尺与圆规三等分，那末用直

尺和圆规三等分任意角的作图就不可能了。

取 120 度角来三等分。假定这角位于一个半径是单位长的圆中心。假使能作出 $cos40$ 度来，那末，只要取 $OA = cos40$, 于是 a 就是一只 40 度的角，而三等分 120 度的作图就完成了。

应用三角恒等式 $2cos(3\alpha) = 8cos(\alpha^3) - 6cos(\alpha)$，令 $x = 2cos\alpha$, 证明：

$$
\begin{aligned}
cos3\alpha &= cos(2\alpha + \alpha) \\
&= cos2\alpha cos\alpha - sin2\alpha sin\alpha \\
&= (2cos^2(\alpha) - 1)cos\alpha - (2sin\alpha cos\alpha)sin\alpha \\
&= 2cos^3(\alpha) - cos(\alpha) - 2sin^2(\alpha)cos\alpha \\
&= 2cos^3(\alpha) - cos\alpha - 2(1 - cos^2(\alpha))cos\alpha \\
&= 2cos^3(\alpha) - cos\alpha - 2cos\alpha + 2cos^3(\alpha) \\
&= 4cos^3(\alpha) - 3cos(\alpha)
\end{aligned}
$$

则有：$2cos3\alpha = x^3 - 3x$

因为 $3\alpha = 120$ 度，$cos3\alpha = -1/2$，所以上面的方程可以写作 $x^3 - 3x + 1 = 0$

这正是以前讨论过的方程。

现在作一个半径是单位长的圆，而且可以作 $OB = 1/2$，于是角 $AOC = 120$ 度。因为所给的只有单位长，所以数域限定在有理数域。

所以要解这个方程，必须将一个立方根加入于有理数域中，然而一个立方根是不能用直尺与圆规作出的，这样，我们可以知道：用直尺与圆规三等分任意角是不可能的。

以相似的方法，不难证明用直尺，圆规解决立方倍积问题也是不可能的，对于这个问题，方程是 $x^3 = 2$

数域是有理数域，这方程在这个数域中的群含有六个置换。可以当证明须加入一个平方根和一个立方根于有理数域中，方程的群才会变成 1。又因一个立方根是不能用直尺，圆规作出的，所以我们这个立方倍积问题是不可能的。

类似的，也可以可以应用群论去探讨正多边形作图的问题。

附：伽罗华的关键定理的思想脉络：

问题：要证明一个方程若有一个伽罗华可解群，这方程就可用根式解。

伽罗华的思想脉络如下：在二次方程 $x^2+bx+c=0$ 的两个根 $x1,x2$ 中，用韦达定理有 $x_1+x_2=-b$ 与 $x_1x_2=c$ 的关系，那么为什么不从这两个方程中去解 x_1,x_2 呢？因为这条路是走不通的，因为经过计算的结果是与原来的二次方程丝毫也没分别。

但是，如果能得到一对都是一次的方程，x_1 和 x_2 就可以求得了。

假设方程 $f(x)=0$ 有 n 个相异的根，而且由方程的系数及 $x^n=1$ 的 n 次根决定的数域中，此方程的群是一个元数为素数的循环正置换群。

为什么伽罗华要先引进这个 1 的 n 个 n 次根呢？

先看看 1 有三个立方根：$1,-\frac{1}{2}+\frac{1}{2}(-3)^{\frac{1}{2}},-\frac{1}{2}-\frac{1}{2}(-3)^{\frac{1}{2}}$,(通常都记作 1，$\omega$，$\omega^2$)（在一般的情形，1 有 n 个 n 次根，这 n 个 n 次根记作 $1,\rho,\rho^2,\cdots,\rho^{n-1}$）

1 的三个立方根只包含有理数和有理数的根数，同样 1 的 n 个 n 次根也只包含有理数和有理数的根数，所以这种数加入数域中去时并不影响到方程是能用根式解的命题。

因为前面假定这个方程的群是一个元数为素数的循环正置换群，群中元素都是置换群，群中的元素都是置换 $(123\cdots n)$ 的乘幂，这个置换的 n 次乘幂就是不动置换。

现在构造一组一次方程（n 个）：

$x_1+(\rho^k)x_2+(\rho^{2k})x_3+.....+(\rho^{(n-1)k})x_n=\gamma k$

此处 k 的值为 0 与 $n-1$ 间之任何整数。

例如当 $k=0$ 时，上式就成为：

$x_1+x_2+x_3+.....+x_n=\gamma 0$

当 $k=1$ 时，上式就成为：

$x_1+\rho x_2+\rho^2x_3+.....+\rho^{n-1}x_n=\gamma 1$ 等等。

因为一个方程的最高次项系数是 1，则诸根之和等于方程中第二项的系数的负值，所以 $\gamma 0$ 之值可以直接从方程的系数中求得。

现在要将置换 $(123\cdots n)$ 作用于上面方程组的左端，左端就成为：

$x_2+(\rho^k)x_3+(\rho^{2k})x_4+.....+(\rho^{(n-1)k})x_1$ 等等，

若将左端用 $\rho^(-k)$ 一乘，也可得出同样的结果，这是因为 $\rho^n=1$ 的缘故。所以置换 (1234.....n) 将 γk 之值变为 $\rho^{-k}\gamma k$。

又因 $\rho^n = 1$，所以 $\gamma k^n = (\rho^{-k}\gamma k)^n$

所以置换 (1234.....n) 不变更 γk^n 的值。同样，群中其他的置换也不变 γk^n。

这样群中一切置换都不变更 γk^n 之值，γk^n 之值必在数域中。因此，γk^n 是数域中某一个数的 n 次根，这就是说：所有 γ 的值都可由根式得到（对于定义的数域而言）。而上面方程组中可以将 x 用 ρ 与 γ 表出，于是这组方程是可以用根式解的。这些 x 就是方程 $f(x) = 0$ 根。

所以已经证明：如果方程在一数域中的群是元数为素数的循环正置换群，则此方程必可用根式解。

举例来说：方程 $x^3 - 3x + 1 = 0$ 在有理数域中的群是 1，(123),(132)；这是一个元数为素数的循环正置换群，所以可以从

$$x1 + x2 + x3 = 0$$

$$x1 + \omega x2 + \omega^2 x3 = \gamma 1$$

$$x1 + \omega^2 x2 + \omega x3 = \gamma 2$$

这三个一次方程求解。此处 ω 表示 1 的一个虚立方根，$\gamma 1$ 与 $\gamma 2$ 可以由数域中的数的根数而得。换句话说，如果把根加入到数域中去，则 x 都存在于扩大的数域中。

假使方程的群是一个可解群时，由于组合因数都是素数，这方程还是能用根式解的，因为这时候每个辅助方程在那个用前几个辅助方程的根扩大成的数域中的群是一个元数为素数的循环正置换群，这些辅助方程都能用根式解。因为这些加入原来的数域去的辅助方程的根，都只不过是原来的数域中的数的根数而已。所以只要方程的群是可解群，方程就是能用根式解的。

在一般的情形，取：

$y^2 = (x(1) - x(2))^2(x(1) - x(3))^2 \cdots (x(n-1) - x(n))^2$ 作第一个辅助方程，此式右端是所有每两个根之差的平方之积。假若方程的第一项系数是 1 的话，则上式的右端正是方程的判别式，例如二次方程 $x^2 + bx + c = 0$ 的两个根 x_1,x_2 之差之平方是 $(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = b^2 - 4c$，这恰是方程的判别式。同样，高次方程的判别式也可从系数求得。现在第一个辅助方程的两个根就是这判别式的两个平方根，将这两个平方根加入数域中，方程式在这新的数域 F1 中的群是 H，再照同样方法用其余的辅助方程进行下去。

设若所要解的方程是一个一般的三次方程，将第一个辅助方程的根加入原来的数域之后，方程的群变为 H，在这情形，H 是一个元数为素数的循环正置换群，所以我们可以利用

$x_1 + x_2 + x_3 = 0$

$x_1 + \omega_2^x + \omega^2 x_3 = \gamma 1$

$x_1 + \omega^2 x_2 + \omega_3^x = \gamma 2$

这三个一次方程来解原来的三次方程，此中的 $\gamma 1$，$\gamma 2$ 可由数域 (由三次方程的系数以及第一个辅助方程式的根决定）中的数的根数求得。换句话说，假使把 $\gamma 1$，$\gamma 2$ 的值也加入数域中，则方程的群变为 1，这也就是说，x1,x2,x3 存在于这个最后经 $\gamma 1$，$\gamma 2$ 之加入而扩大成的数域中。

如此就已经证明：方程在一个由其系数与 1 之 n 个 n 次根而决定的数域中的群若是一个可解群，则此方程是可以用根式解的。

当然，如果方程在一个含有其系数的数域中的群是可解群，则对于这数域而言，此方程是可以解的。

至此伽罗华解决了为何五次以上之方程式没有公式解，而四次以下有公式解。

他也解决了古代三大作图问题中的两个：“不能任意三等分角”，“倍立方不可能”。

对上述思想再举一个简单例子：

二次方程 $x^2 + 3x + 1 = 0$, 有两个根 x_1, x_2, 因为只有两个根，所以可能的置换只有 1 和 (12) 两种（也即是 $S(2)$ 置换群），所以这方程的伽罗华群或者含有这两个置换，或者只有 1 一个，至于是什么，这就要凭在什么数域中而决定了。

现在取函数 $x_1 - x_2$，从韦达定理中我们知道：二次方程 $x^2 + bx + c = 0$ 的两个根之差是 $x_1 - x_2 = (b^2 - 4c)^{\frac{1}{2}}$，$b = 3, c = 1$, 所以 $x_1 - x_2 = 5^{\frac{1}{2}}$ ，如果所讨论的数域是有理数域，这个函数的值不在数域中，所以群中必有一个置换，他能变更这函数的值。而 1 和 (12) 两个置换中只有 (12) 变更函数 x1-x2 的值。所以伽罗华群中必含有 (12), 因此，这方程在有理数域中的伽罗华群是由 1,(12) 两个置换构成的。

如果所讨论的数域是实数域，显然 $5^{\frac{1}{2}}$ 在其中，所以 S（2）群中一切置换都

不改变函数 $x_1 - x_2$ 的值。所以 (12) 不能在伽罗华群中，这方程在实数域中的伽罗华群是由 1 一个置换构成的。

再以方程 $x^3 - 3x + 1 = 0$ 为例，假设三个根为 x_1, x_2, x_3，所以至多有六种可能的置换，即是 1,(12),(13),(23),(123),(132)（即 $S(3)$ 置换群）。

求这方程在有理数域中的伽罗华群，我们应用 $(x_1-x_2)(x_1-x_3)(x_2-x_3)$ 这个函数，根据韦达定理，$(x_1-x_2)(x_1-x_3)(x_2-x_3)$ 之值是 $\pm(-4c^3-27d^2)^{\frac{1}{2}}$。现在 $c=-3, d=1$, 所以 $(x_1-x_2)(x_1-x_3)(x_2-x_3) = \pm 9$，$\pm 9$ 是有理数，在有理数域中，伽罗华群中一切置换都不能变更函函数的值。但在上列六个置换中，只有 1,(123),(132) 不变更这数的值，所以这个三次方程在有理数域中的伽罗华群的元素或者就是这三个置换，或者只是 1 一个，所以单利用函数 $(x_1-x_2)(x_1-x_3)(x_2-x_3)$ 还不能决定这个方程在有理数域中的伽罗华群。我们再应用另外一个函数 x1，如果群中只有 1 一个元素，那么，1 不会变更函数 x_1 的值，所以 x_1，必在有理数域中，换句话说，这个三次方程的根 x_1 必须是有理数，同样的道理，x_2, x_3 也须是有理数，但是，这个三次方程没有一个根是有理数，所以，他在有理数域中的伽罗华群不能单含 1 一个元素，个伽罗华群必定是由 1,(123),(132) 三个元素构成的。

如此，我们利用 $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ 和 x_1 两个函数而决定了这个方程在有理数域中的伽罗华群。

上面讨论的这个三次方程也是讨论直尺圆规三等分任意角问题的基本方程。

至此，我们已经知道什么叫做一个方程在一个数域中的伽罗华群，而且知道如何去求。

根据前面介绍的伽罗华定理，我们知道一个方程在一个含有他的系数的数域中的群若是可解群，则此方程就能用根式求解，而且仅满足这个条件的方程才能用根式解。

例如对一般的二次方程:$ax^2 + bx + c = 0$，设两个根是 x_1, x_2, 在一个含有他的系数的数域中的置换群的元素是 1 和 (12), 这个置换群的唯一的极大不变真子群是 1，所以此群的组合因数是 2/1=2 是一个素数，因此，根据伽罗华定理，二次方程都可用根式解。

再例如，一般的三次方程 $ax^3 + bx^2 + cx + d = 0$，三个根 x_1, x_2, x_3，在一个

含有他的系数的数域中，他的群含有 1,(12),(13),(23),(123),(132) 六个置换，此群的唯一极大不变真子群 H 含有 1,(123),(132) 三个置换，而 H 的唯一极大不变真子群是 1，所以组合因数是 6/3=2, 与/1=3, 两个都是素数，所以三次方程都是可用根式求解。

再例如四次方程 $ax^4+bx^3+cx^2+dx+e=0$，在一个含有其系数的数域中的群的元数是 $4!=24$, 按照前面计算，能够得到这个群的组合因数是 2,3,2,2, 这些都是素数，所以四次方程也都可以用根式解。

对于一般的五次方程，G 含有 5! 个置换，G 的极大不变真子群 H 含有 5!/2 个置换，而 H 的唯一极大不变真子群是 1，所以组合因数是 2 与 5!/2，5!/2 当然不是素数，所以一般的五次方程是不能用根式解的。

其实，对于一般的 n 次方程，n 若是大于 4，组合因数便是 2 与 $n!/2$ 而后者当然不是素数。

这样就得到了用方程结构来决定一个方程是否能用根式求解。

但是如果方程的群是一个元数为素数的循环正置换群，这方程的确可以通过辅助方程降阶简化，也即可以根式解。

1.7 感想

一般说来，一个抽象的集合不过是一组元素而已，无所谓结构，没有结构的集合，是没有意义的。数学研究的集合是定义了运算或者变换的（系统科学研究的集合，上面定义的可能是正反馈，负反馈，延迟，发散，收敛等等），这些运算或变换，就形成了集合的结构，也即定义了集合中元素的关系。伽罗华群结构思想是人类第一次将对象按照结构进行研究，并不管研究对象和运算具体是什么（群上面定义的运算，可以是加法，也可以是变换等等）。

伽罗华思想的价值是开启了现代数学的大门，使数学从运算转向研究运算性质，也即集合的结构。所以伽罗华思想是开启后来法国布尔巴基学派以数学结构观念统一数学的先导（布尔巴基学派简介在上一篇介绍数学基础时介绍过），布尔巴基实现了伽罗华没有实现的理想，他们把康托尔的集合论及希尔伯特的

公理化方法作为统一数学的基础，从抽象群的公理理论出发，通过分析抽象群结构，搞清楚了人类的抽象结构概念是如何产生的，例如他们通过群就是在某一集合中定义有结合性，么元和逆元的一个运算（这三个性质叫群结构公理），就抽象出结构概念的一般特点是：满足一定条件公理的关系集合。所以布尔巴基认为集合上的关系是数学至关重要的概念，因为关系是各种运算的抽象，是构成一个结构的基础，不同的关系可以构成不同的结构。布尔巴基学派就从结构观点出发，选出三种基本结构：代数结构、序结构、拓扑结构，作为元结构，通过从简单到复杂，从一般到特殊的层次概念，构造出各种不同的结构，如复合结构、多重结构、混合结构，建立了各种公理理论，在此基础上，统一了人类目前所有的数学学科。这其实是伽罗华思想的进一步发展：数学本质就是研究结构的。布尔巴基所做的只是把伽罗华已经确定的观念推广而已。

群的抽象定义是凯莱提出的，到 20 世纪初，已经成为数学的核心概念，几乎所有大数学家都认为其是数学的中心概念和统一数学的基础概念。如外尔就说过：没有群就不可能理解近代数学。庞加莱也曾说过：可以说群论就是那摒弃其内容化为纯粹形式的整个数学。

总之，群论是十九世纪最杰出的数学成就，是人类摆脱幼年思维的标志，也即从此摆脱了依赖直观 + 计算来理解世界。群论以结构研究代替计算，把人类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，是物理学和化学发展的重要推动。

抽象的力量是巨大的，Feynman 认为用代数角度而不是偏微分方程来理解量子力学要容易得多，因为代数的抽象恰好可以避免望文生义和误入歧途。而且偏重计算的偏微分方程会导致学生舍本求末，陷入细节而难以抓住本质。

代数虽然没几何直观，但是面对 N 维空间时，其实几何直观优势已经荡然无存（所以克莱因才要用抽象代数统一几何）。面对直观以外的世界，我们唯一可以依靠的只有抽象 + 逻辑。

几何与代数的特点很像以现象研究为对象的初等物理和以本质研究（不变量研究）为主的理论物理。

代数通过不断的抽象来提炼更加基本的概念，例如两个群，不论它们的元素真实背景是什么（这些元素不管描述的是膨胀、收缩、转动、反演、振动、声

音、流体、电磁波等等)，只要运算性质相同，彼此就是同构的，并且可以因此认为是相同的代数结构而不加区别。

代数的每一次抽象都是学科升级的过程。

例如克莱因用群论来把几何中的许多互不相干的分支之间建立了内在的联系。

克莱因对几何学的定义：几何学是当集合 S 的元素经受某变换群 T 中所包含的变换时集合 S 保持不变的那些性质的研究，为方便起见, 这种几何学以符号 G(S,T) 表示。

也即任何一种几何学可以用公理化方法来构建，也可以把变换群和几何学联系起来。

例如集合 S 叫做空间，S 的元素叫做点，S 的子集 A 和 B 叫做图形，凡是等价的图形都属于同一类（图形等价类）。

同一类里的一切图形所具有的几何性质必是变换群 G 下的不变量，因而可用变换群来研究几何学（Erlangen 纲领），例如在正交变换群下保持几何性质不变的便是欧式几何，在仿射变换群下保持不变的便是仿射几何，在射影变换群下保持不变的便是射影几何，在微分同胚群下保持不变的便是微分几何。

稍微具体一点，平面欧几里得度量几何为设 S 为通常平面上所有点的集合, 考虑由平移、旋转和线上的反射组成的所有 S 的变换的集合 T。因为任何两个这样的变换的乘积和任何这样的变换的逆变换还是这样的变换, 所以,T 是一个变换群。长度、面积、全等、平行、垂直、图形的相似性, 点的共线性和线的共点性这样的一些性质在群 T 下是不变的, 而这些性质正是平面欧几里得度量几何所研究的。

仿射几何就是把平面欧几里得度量几何的变换群 T 扩大, 除了平移、旋转和线上的反射外, 再加上仿射变换（换句话说，就是从欧几里得空间的距离概念抽象化出单比的概念，就从欧式几何中舍弃距离不变而保留更普遍的单比不变，就从欧氏几何升级到仿射几何）。在此扩大的群下, 像长度面积和全等这类性质不再保持不变, 因而不再作为研究的课题。但平行垂直图形的相似性, 点的共线性, 线的共点性仍然是不变的性质, 因而仍然是这种几何中要研究的课题.

射影几何所研究的是平面上的点经受所谓射影变换时仍然保持不变的性质

从单比抽象到交比概念（换句话说，从仿射几何中舍弃单比不变而保留更普遍的交比不变，升级射影几何）。在前面讲的那些性质中, 点的共线性和线的共点性仍然保持不变, 因而是这种几何所要研究的课题

在上述的几何中, 使某变换群的变换起作用的基本元素是点, 因此, 上述几何均为点几何的例子。还有线几何, 圆几何, 球几何和其他几何的例子。

在建立一种几何时, 人们首先是不受拘束地选择几何的基本元素，其次是自由选择这些元素的空间或流形，自由选择作用于这些基本元素的变换群, 这样, 新几何的建立就成为相当简单的事了。也即从欧式空间（长度，夹角）到内积空间（模，不严格的夹角）再到赋范空间（范，完全抛弃夹角），不断的抽象，最后甚至连范数（最不愿抛弃的度量或度规）也抛弃了，从不严格的距离发展到不确定的距离，也即由欧式空间的连续函数抽象出度量空间的连续映射，一直到抽象出拓扑空间中的同胚映射，最后得到了拓扑空间的概念，这是人类目前为止在抽象上最深刻的极限。可以说克莱因用群论来研究几何学是人类思想的突破。

总之，群是数学中最有影响的概念，不了解群，就不可能了解现代数学。群论直接推动了代数数论、代数几何、函数论、微分方程与特殊函数论和代数拓扑的产生和发展，甚至很多经典数学领域，因为群论的引入而现代化。

其实数学上这种抽象过程，也推动了理论物理学的发展，例如狭义相对论发展就是要摆脱坐标而直接度量时空的过程，而广义相对论发展就是摆脱时空度量概念，走向空间同胚概念的过程。

目前群论已经是现代物理的主要工具。群论广泛用于基本粒子、核结构、原子结构和晶体结构等，因为对称性是物质世界最普遍的性质，例如各种物体（分子、晶体或图形）都可以用特定的对称性群来描述其结构（晶体的空间对称性可以用点群描述，其实晶体 X 射线衍射的图案直接与其点群相关）；再例如时空存在对称性，可以用彭加莱群描述不同表示对应不同自旋的粒子，例如标量粒子、旋量粒子、矢量粒子；再例如量子力学里的全同粒子就是对称性的（基本粒子的规范对称性可以由李群描述，其实李群的结构常数直接决定了规范玻色子，比如胶子、W、Z 玻色子的自相互作用）。

现代化学也离不开群论。例如化学中分子的性质受到分子对称性的影响（因

为分子的对称性反映出分子中原子核和电子云的分布情况），所以可以根据分子对称性判断该分子的一些基本性质，例如判断是否具有旋光性（判别分子是否具有旋光性的常用的方法是比较实物和它的镜像，看它们能否完全重合，凡不能和镜像重合的分子都具有旋光性；反之，如果两者能够重合，则分子就没有旋光性），所以可以用分子的对称元素和所属对称群来判断其是否具有旋光性。

同样，根据分子的对称性，也可以判断分子有无偶极距。分子偶极距大小决定于分子正负电重心间的距离与电荷量，其方向规定为从正至负。因为分子所具有的对称性是分子中原子核和电子云对称分布的反映，分子正负电重心一定处于分子的对称元素上。所以分子的永久偶极矩是分子的静态性质，静态性质的特点就是它在分子所属点群每一对称操作下必须保持不变，为此 μ 向量必须落在每一元素上，因此可以根据“分子对称元素是否只交于一点”来预测分子有无永久 μ。如果分子有对重心落在同一点上，因而无偶极距。若不存在上述的对称元素时，则分子的正负电重心不落在同一点上，就有偶极矩。

如果分子具有对称中心，那么分子的所有对称元素都交于此点，此点亦即分子正负电荷的重心。因此，具有对称中心的分子没有偶极矩。如果分子有两个对称元素交于一点，比如有一个对称面和垂直于此面的对称轴，或者有两个以上不相重合的对称轴，那么分子的正负电荷中心必重合于此交点，因而也没有偶极矩。分支虽有对称面和对称轴，但他们若不相较于一点，而且对称轴为对称面所包含，则他们具有偶极矩。

按照这一判据，可将分子所属点群和它是否具有偶极矩的关系总结为：对于具有偶极矩的分子可以进一步推断：当分子有 C2 轴时，偶极矩必沿着此轴；当分子有对称面时，偶极矩必位于此面上；当分子有几个对称面时则偶极矩必沿着他们的交线。

再例如化学位移等价性的判别质子或其他的原子核，在一定的交变磁场的作用下，由于分子中所处的化学环境不同，从而将在不同的共振磁场下显示吸收峰。这一现象就叫做化学位移。化学位移是核磁共振波普中反映化合物结构特征最重要的信息之一。

氢气 (H1) 谱亦即质子谱，在核磁共振波普中应用最为广泛。氢谱中的各个峰与分子中的不同环境的质子相对应。这样便可根据分子对称性识别等价院子

或基团，进而可以判别氢谱中化学位移的等价性。全同质子（通过旋转操作课互换的质子）在任何化学环境中都是化学位移等价的。对映异位质子（存在对称操作使分子中两个质子互换的质子）在非手性溶剂中具有相同的化学性质，也是化学位移等价的，但在光学活性或酶产生的手性环境中就不再是化学等价的，在核磁共振波普中可以显示偶合现象。此外，非对映异位质子（不能通过操作达到互换的质子）在任何化学环境中都是化学位移不等价的。分子中化学位移等价的核构成一个核组，相互作用的许多核组构成一个自旋系统。考虑分子的对称性，有利于对它们进行分类，因而群论就是最基础的。

群论也广泛用于分子结构判断，因为分子外形的对称性通过分子波函数与分子结构联系，而分子波函数可以作为分子所属点群的不可约表示的基。

杂化轨道理论主要是研究分子的几何构型，而构型和杂化的原子轨道在空间的分布和方向有密切的联系。由于在微观世界中，分子都具有一定的对称性，而对称性不同时，则其分子构型也必然不同，因此分子对称性就与其杂化轨道有内在的联系。群论的方法可以告诉我们：在具有一定形状的分子的化学成键中，中心原子可能采用什么样的杂化方式。运用群论的知识还可以知道中心原子提供哪些原子轨道去构成合乎对称性要求的杂化轨道，而且还可以进一步求出杂化轨道的数学表达式。

当然群论还有实际工程应用，例如先进陶瓷材料研发。我们都知道，先进陶瓷材料现在用途极为广泛，例如涡扇发动机用的陶瓷涂层材料，或陶瓷基复合叶片，甚至在尾喷管，燃烧室等等都开始使用陶瓷复合材料，以及在导弹某些关键部位的应用。

而大家不知道的是：群论在先进（陶瓷）材料的结构筛选中是基本工具。

因为晶粒对陶瓷的性能起着关键性的作用，所以研究晶粒是获得新材料性能的关键，例如由晶体的各向异性性，可以通过控制外界工艺条件使晶粒在某个晶向优先生长，从而可能具有某些前所未有的性能，在力学上使结构陶瓷得到更好的晶须增韧效果，在物理性能上或者在力学性质上增强，使功能陶瓷获得更好的韧性，刚性，抗切变性，或者是在电学性能上增强，例如获得更好的压电性能、热释电性、倍频效应，或者使人工晶体获得更好的旋光性等光学性能等等。

目前通常做法是通过对这些具有一定力学性能、物理性能的材料的微观本质的分析，可以利用对称群分析计算，筛选出掺杂物质和优化结构构造方式等等，来改变晶体的晶格，以获得性能更佳，物理效应更显著的晶体。

用对称群为工具也可以研究非晶态材料和非平衡态材料结构。非晶体与晶体相比有着大量的缺陷，原子或离子间的结合也不如晶体那般整齐有序，所以比同类晶体具有更大的内能，因此当非晶态向晶态转变或者反过来晶态向非晶态转变时将吸收或放出大量的能量，选择适当的材料显然在某些场合可以考虑由此而用来存储能量。

1.8 小结

本篇帖子由于豆瓣不能上数学公式，所以用一直奇特的模式写，痛苦不堪，可能错误比较多，发现错误请指出来。

再顺便感概一下，现在大学老师基本都是照本宣科，把教科书在课堂朗读一遍拉倒，纯粹是误人子弟。

我在中国科大数学系上学时，任意一门数学课的老师教课都是这个模式：任何一个重要概念的实际背景（包括但不限于工程，物理，军事等等问题），来龙去脉，要解决什么问题，结果解决什么问题，这些抽象概念的基本思想和原型是什么等等，都要让学生知其然，也知其所以然。

一个蒙查查的老师，一般不太可能教出什么明白学生。大学之间的水平差距，其实在老师之间的差距。上大学，如果不想被教成蒙查查，最好上最好的大学，不然人家勇猛奋进的四年光景，你不过是混日子的四年。

第二章　瞎扯贝叶斯理论的基本思想

基本信息

1. 原文链接 https://www.douban.com/group/topic/82509566/.
2. 本文作者 wxmang.

2.1　序

既然是瞎扯，就不是很严谨的，因为要简单明了，可能有的地方细节删除过多了，导致说不通。所以只能大概齐。真的要弄懂，还是请看教科书为好。写这种文章，华罗庚先生写得最好。

2.2　倒向问题

自从人类有自我意识，可能就在讨论一个至今没有结论的问题：机遇（或者运气，或者机会）到底是什么？怎么把握，怎么预测，怎么估计或计算大小等等。这是人类的一个核心问题。其实这也是一个典型的倒向问题。

人类思考问题有两个方向，一个是正向，也即知道结果找原因（例如现在我们经常讨论的明朝灭亡的原因）；一个是倒向，也即根据一些现象判断结果（例如如果我们事先并不知道黑箱里面黑白球的比例，而是闭着眼睛摸出一个或好

几个球，观察这些取出来的球的颜色之后，就此对黑箱里面的黑白球的比例进行推测。现实需要大量的倒向计算，例如现在某些现象出现，企业会不会破产，现在应该怎么办等等）。

用正向思维方式研究问题的，我们叫他们事后诸葛亮，历史学家便是。这种研究只能用于经验总结和知识储备上。

用倒向思维方式研究问题的，我们叫他们预测大师，见微知著的真人，管蠡窥测或以蠡测海的超人等等。实际上有价值的问题多数都是倒向问题，例如：股市上，通过那几点征兆就能判断是一次多或空的机会；医院中，通过那几个症状就能判断是什么病；科学研究上，通过几个实验数据，就能构造什么理论解释模型等等。一般说来，数学家，物理学家等等都是研究倒向问题的，或者说，他们不能通过很少征兆或现象来预测或判断结果，就没存在价值（顺便说一句，不知道倒向问题思维方式的人，没法再金融市场或股市搏击，目前投机市场最前沿的研究几乎就是倒向随机过程和鞅论为主，中国的彭实戈院士是倒向随机过程领域的其中一个领军人物）。

如何用倒向思维方式研究机遇？也即如何从一些征兆或现象，判断机遇，或者把问题进行等价推广：如何用一些已知的信息或经验，判断或预测未知。

1763 年，英国的长老会牧师贝叶斯发表了一篇论文“论有关机遇问题的求解”，提出了解决的框架：那就是用不断增加的信息和经验，可以逐步逼近未知的真相或理解未知。并给出了算法（其实贝叶斯由于是一个牧师，他关心的原始问题本来的表述是：人能不能根据凡人世界的经验和现实世界的证据，证明上帝的存在，因为宗教人士的逻辑是机遇就是上帝存在的主要证据，能够认识机遇的规律，几乎等同于证明上帝存在）。

后来经拉格朗日等数学家进一步努力，获得了大突破，贝叶斯理论成为现代统计学两大支柱之一。

由于我们不讨论数学，所以不进一步讨论贝叶斯思想的各种复杂数学表达，我们只讨论其基本思想。

2.3　贝叶斯基本思想

下面我们用一个例子来介绍贝叶斯思想。

假定甲乙两人做一个游戏：甲蒙上眼睛，乙随手在一张纸上画一条线段，两个端点分别 A 点和 B 点，再随机在线段上画一点 C，现在游戏是：通过一些信息，让甲判断 C 点位置。

信息 1：乙随机在线段上划点，并告诉每一个点是离 A 端点近还是离 B 端点近；

信息 2：乙必须告诉每一个点是位于 AC 之间还是 CB 之间。

显然只需要有限次划点，甲就能基本确定 C 的大致位置。

为简单说明，我们假设乙划点总是在中位点，也即第一个点是 A+B 的中点，根据上面游戏规则，必须告诉甲的两个信息，甲这样就能判断 C 靠 A 点近还是 B 点近；如果 C 靠 A 点近，那么第二个点划在 $A+C$ 的中点，同样重复上述步骤，甲就能判断 C 点是靠 A 点近还是 $\frac{(A+C)}{2}$ 近，继续循环。我们知道中位点划分会形成一个 $\frac{1}{2^N}$ 的收敛级数，可以在有限的 N 次内，就能获得 C 点位置范围，误差不大于 $\frac{1}{2^N}$。

这就是用逐步增加的信息确定未知的例子。这也就是贝叶斯思想的基本模型。

当然贝叶斯考虑的逐步增加信息是人的经验和知识构成的先验信息，而先验信息会因为个人的经验偏见，视野局限，测量误差，外部环境变化，数据丢失等等导致一定的不准确，也即只有概率意义上的正确。所以他能够得到的对未知的判断也只能是概率意义上的。

简单总结一下贝叶斯的基本观点是：

（1）、由于经验或知识是否正确带有不确定性因素，所以基于以前经验和知识（也即先验），根据一些随机出现或观察到的现象来判断事物真相，原因或未知，就有一定的不确定性。（其实这个观点有一个强大的前提假设：未知世界本质是随机的，所以任何未知都具有不确定性，这是现代量子力学和复杂系统证明了的假设）。

（2）、由于我们依靠已知的经验或知识, 来分析观察到的现象，以此推测或断未知，所以任何未知的判断或推测都是是不确定的，能用一个概率分布去描述，也即未知的不确定性程度由先验概率分布和现象出现的概率分布决定。

上面这句话的本质意思是：是不是能够通过一些现象正确判断或推测未知，取决于我们经验多少和掌握的现象多少。例如，医生能否通过症状判断疾病，取决于医生知识（这也是一种经验，是从前人身上学习的）和经验积累，也取决于掌握的症状多少（掌握症状一般通过各种检查实现，例如为了掌握症状而进行的量体温，照 X 光，核磁共振，CT 检查，超声波检查等等）。

但是光掌握症状并不能完全判断病症（否则就不需要医生，只需要检测工程师了），还需要医生知识和经验。

因为任何检查都不可能完备，再加上任何医生的经验和知识也是不完备的（例如对一种新疾病原有的经验和知识就无能为力），所以任何判断都有一定的对错概率。

（3）、由于基于 N 个现象（或症状）和个人主观经验来判断未知带有一定不确定，我们往往需要做多次检测和由具有不同个人主观经验的人来判断，然后按照极大似然原则选择结果（例如医院诊断重大疾病往往要请不同医生会诊，也要进行不同系列，不同类型的医疗检查）。

（4）、先验信息可以通过的收集、挖掘和加工而数量化，形成先验分布（也即所谓专家知识库可以提高判断精度）。

上面这些观点，综合起来就是：

现实世界本身是不确定的，人类的观察能力是有局限性的（例如如果人类能够直接观察到电子的运行，还需要假设什么模型），人类所观察到的只是事物表面上的结果（若干症状或现象），例如往往只能知道从黑箱里面取出来的球是什么颜色，而并不能直接看到黑箱里面实际的情况。

贝叶斯思想给我们提供了一个猜测黑箱里面情况的方法。当然这种方法得到的结果是不确定的（因为世界本质就是不确定的，而且这种方法依赖于人的主观经验，本身是否正确也是不确定的）。

贝叶斯的方法其实是一个算法：第一步，算出各种不同猜测的可能性大小；第二步算出最可能的猜测是什么。

第一步就是计算特定猜测的后验概率（对于连续的猜测空间就是计算猜测的概率密度函数），第二步则是极大似然方法。

定义 2.1: 极大似然的定义是

事件 A 与参数 $\theta \in \Theta$ 有关，θ 取值不同，则 $P(A)$ 也不同，若 A 发生了，则认为此时的 θ 值就是 Θ 的估计值。这就是极大似然。

例如两人一起打猎，只响一枪，就打中一猎物，那么按正常逻辑，一枪命中，肯定是枪法好的那个，这个推断就体现了极大似然法的基本思想。

再例如，袋中装有许多黑、白球，不同颜色球的数量比为 3:1，试设计一种方法，估计任取一球为黑球的概率 P。

显然 P 的值无非是 $\frac{1}{4}$ 或 $\frac{3}{4}$，需要通过抽样来决定分布中参数究竟是 $\frac{1}{4}$ 还是 $\frac{3}{4}$。现从袋中有放回地任取 3 只球，显然白球出现次数多的话，P 就是 $\frac{1}{4}$，黑球出现次数多的话，P 就是 $\frac{3}{4}$)。

也即贝叶斯思想就是：对于给定观测数据，一个猜测是否正确，取决于这个猜测本身独立的可能性大小（先验概率）和这个猜测生成我们观测到的数据的可能性大小（似然）的乘积。（也即最可能的猜测 = 先验概率 * 似然最大的这个值）。

2.4 贝叶斯公式

先用一个 wikipedia 上的例子介绍贝叶斯公式的原理。

假设一所学校里面有 60% 的男生，40% 的女生。男生总是穿长裤，女生则一半穿长裤一半穿裙子。问题：随机在校园乱走，看到在校园里穿长裤的人里面有多少女生的概率？

假设学校里面人的总数是 N 个。60% 的男生都穿长裤，于是我们得到了 $N \cdot P(\text{Boy})P(\text{Pants}|\text{Boy})$ 个穿长裤的（男生）（其中 $P(\text{Boy})$是男生的概率 $= 60\%$，这里可以简单的理解为男生的比例；$P(\text{Pants}|\text{Boy})$ 是条件概率，即在 Boy 这个条件下穿长裤的概率是多大，这里是 100%，因为所有男生都穿长裤）。40% 的女生

里面又有一半（50%）是穿长裤的，于是我们又得到了 $N \cdot P(\text{Girl})P(\text{Pants}|\text{Girl})$ 个穿长裤的（女生）。加起来一共是 $N \cdot P(\text{Boy})P(\text{Pants}|\text{Boy}) + N \cdot P(\text{Girl})P(\text{Pants}|\text{Girl})$ 个穿长裤的。

整理一下：

$$P(\text{Girl}|\text{Pants})(\text{穿长裤的人里面有多少女生的概率}) = \frac{N \cdot P(\text{Girl})P(\text{Pants}|\text{Girl})}{[N \cdot P(\text{Boy})P(\text{Pants}|\text{Boy}) + N \cdot P(\text{Girl})P(\text{Pants}|\text{Girl})]}$$

很容易发现公式与校园内人的总数是无关的，可以消去。于是得到

$$P(\text{Girl}|\text{Pants}) = \frac{P(\text{Girl})P(\text{Pants}|\text{Girl})}{[P(\text{Boy})P(\text{Pants}|\text{Boy}) + P(\text{Girl})P(\text{Pants}|\text{Girl})]}$$

上式中的 Pants 和 Boy/Girl 可以指代一切东西，所以其一般形式就是：

$$P(B|A) = \frac{P(A|B)P(B)}{P(A|B)P(B) + P(A|\ B)P(\ B)}$$

即已知 $P(A|B)$、$P(A)$ 和 $P(B)$，可以计算出 $P(B|A)$。

这就是著名的贝叶斯公式。所以拉普拉斯说概率论只是把常识用数学公式表达了出来。

2.5 贝叶斯思想在决策中

当然贝叶斯思想用的最多的领域是决策。贝叶斯决策就是在不完全情报下，对部分未知的状态用主观概率估计，然后用贝叶斯公式对发生概率进行修正，最后再利用期望值和修正概率做出最优决策。

贝叶斯决策属于风险型决策，决策者虽不能控制客观因素的变化，但却掌握其变化的可能状况及各状况的分布概率，并利用期望值即未来可能出现的平均状况作为决策准则。

贝叶斯思想能够用于决策的原因是：除样本（例如决策调查获得的一些事件或资料）提供的基础信息外，人类的经验的先验信息也是决策判断的重要依据。

例如以对神童出现的概率 p 的估计为例。按经典统计的做法，完全由样本提供的信息 (即基础抽样信息) 来估计，认为参数 p 是一个“值”。而人类经验其实对 p 已经有了一个了解，如 p 可能取 p_l 与 p_2，且取 p_1 的机会很大，取 p_2 机会很小。

先验信息关于参数 p 的信息是一个“分布”，如 $P(p=p_1)=0.9, P(p=p_2)=0.1$，即在抽样之前已知道 (先验的)$p$ 取 p_1 的可能性为 0.9。若不去抽样便要作出推断，自然会取 $p=p_1$。但若抽样后，除非采样信息 (即样本提供的信息) 包含十分有利于“$p=p_2$”的支持论据，否则采纳先验的看法“$p=p_1$”。

下面用一个例子解释这种决策。

假设患者有肺炎为事件 B，$P(B)$ 是医生在检测前，基于经验对当时当地的肺炎肺病率的概率判断，例如 1%，也即如果没有任何检查，医生基于经验，会判断得肺炎概率很小，$P(\ B)$ 是不是肺炎的概率，例如是 99%；

$P(A)$ 是全体人群（包括肺炎和不是肺炎人群）检查出现各种指标异常的概率，这可以是一个函数曲线，自变量是各种检测指标，总和等于 1（可以经过规范整理得到）；

$P(A|B)$ 是当病人是肺炎时，各种检测指标出现异常的概率，是医院经过大量临床试验和检测数据分析得到的；

$P(A|\ B)$ 是当病人不是肺炎时，各种检测指标出现异常的概率，是医院经过大量临床试验和检测数据分析得到的；

那么根据贝叶斯公式，就可以计算出 $P(B|A)$，也即当某一个异常指标出现时，确诊是肺炎的概率。

例如假设我们知道检测肺炎有 12 个指标，根据多年来的经验和大量临床数据，如果是肺炎，可以得到这 12 个检测指标的出现异常的概率分布情况，也即知道 $P(A_i|B)$；对不是肺炎的，这 12 个指标的异常概率分布情况我们也知道，也即 $P(A_i|\ B)$。

在疹疗过程中，医生要根据临床经验对各种病症状 Ai 进行权衡。当然由于经验数据误差和知识不完备，存在误诊概率。

举个例子来说明，假设有一台肺炎诊断仪，通过对它以往的诊断记录的分析，如果患者确实患有肺炎它的确诊率为 90%，若果患者没有癌肺炎，被诊断成肺炎的概率为 10%。

那么如果一个人被这台诊断仪确诊成肺炎（这是现象），这个人患有肺炎的概率是多少（这是判断）?

设 A：肺炎诊断仪给出肺炎诊断。B1：病人是肺炎患者。B2 病人不是肺炎

患者。

根据贝叶斯公式：$P(A|B1) = 90\%$；$P(A) = 90\% \cdot P(B1) + 10\% \cdot P(B2)$；则 $P(B1|A) = P(B1) \cdot 90\%/(90\% \cdot P(B1) + 10\% \cdot P(B2))$；

我们知道当时当地人群中肺炎患者的比重很小，假设为 1%（这就是经验，有一定的主观性），则 $P(B1) = 1\%$；$P(B2) = 99\%$；

可以算出：$P(B1|A) = 8\%$，也即一个人被这台诊断仪确诊成肺炎，而这个人真正患有肺炎的概率只有 8%。显然这是一个不能饶恕的结果。

但是实际上医生经常这么做，只是他们不是用肺炎诊断仪，而是用一些简单诊断手段就随便下结论了。

所以医院需要加入更多的检查项目，增加更多的检测设备，加入更多医生判断的判断，通过极大似然原则，筛选最可能的结果，逐步逼近真相，解决掉判断的错误风险。

2.6 先验和后验

先验就是指在抽样前就有的经验信息的概率表述，先验不必有客观的依据，它可以部分地或完全地基于主观信念。

再以肺炎为例子，某人认为自己得肺炎，去看病，医生在没有检测之前，基于经验，认为本地在此时此地，得肺炎情况很小，认为他极可能只是感冒，这就是先验。

当然医生不会完全相信自己先验，必然会给某人进行完整的检查，例如测体温，量血压，甚至照 X 光等等，这些检测结果数据就构成检测样本 X。

医生诊断时, 必然不会只使用 X（检测数据）提供的信息进行诊断，而必须先验（否则就不需要医生，只需要工程师就能治病了）。

假定 $\theta = 0$ 是没病，$\theta = 1$ 是有病，贝叶斯理论认为 X 的分布取决于 θ 是 θ 还是 1, 同时根据贝叶斯公式，我们知道了 X，就有助于推断 θ 是否为 1。

通过使用贝叶斯公式计算后验分布，也即根据抽样样本（检测数据）X 的分布 p（x）及 θ 的先验分布 p(θ)（当时当地某种疾病的分布的先验概率，由医

生经验和知识积累决定），用贝叶斯公式就可计算出在已知 X=x 的条件下,θ 的条件分布 p(θ|x)（这就是后验概率，也即经取样和先验概率计算后的出来的）。

显然这个分布综合了样本 X（检测数据）及先验分布 p(θ)(医生经验）所提供的有关的信息。假定设 p(θ=1)=0.001, 经计算，p(θ=1|x)=0.86, 则含义为：在某人的检测指标量出之前, 根据医生经验（p(θ=1)），他患病的可能性定为 0.001，而在得到 X 后, 认识发生了变化：其患病的可能性提高为 0.86。这一判断既与 X 有关，但也也离不开先验分布。也即若当时当地肺炎的发病率很小, 医生将倾向于只有在样本 X 显示出很强的证据时, 才诊断某人有肺炎，这样就可以避免误诊。

2.7　奥卡姆剃刀对决策的筛选

贝叶斯思想本质上是一个经验归纳推理的计算公式，解决了逐步逼近真实的过程，但是显然，这种逼近有不确定性，因为即便一个判断与经验数据非常符合，也并不代表这个判断就是正确的判断，因为经验数据总是会有各种各样的误差，比如观测误差，记忆误差等等，再加上有时无法分别背景噪音，把背景噪声纳入经验数据，来加以判断（背景噪声可以看成与事件完全无关的因素）。

这时，我们就必须应用奥卡姆剃刀：如果两个理论具有相似的解释力度，那么优先选择那个更简单的（往往也正是更平凡的，更少繁复的，更常见的）。

所以现实中，我们建立解释问题的模型往往只提取出几个与结果相关度很高，很重要的因素，而不会面面俱到，太复杂的模型不但成本高，而且会因为无法辨别背景噪声因素，导致失真。

例如我们知道现在各种计算健康体重的模型都是用身高和体重近似于一个二阶多项式的关系（对人群随机抽取了 N 个样本，用最小二乘法拟合出一个二阶多项式），但大家都知道并不是只有身高才会对体重产生影响。但是总体上来说，绝大多数人的身高与体重有关，成正态分布，这个分布就保证了身高体重相关模型能够在大多数情况下做出靠谱的预测。当然人有胖瘦，密度也有大小，所以完美符合身高体重的二阶多项式关系的人是不存在的，只是近似。这就是人类对事物理解的模式。

2.8 简单总结

根据上述描述，我们可以得出几个结论：

（1）、当假定世界本质是随机的，那么我们认识世界的结论也是不确定的，只能通过不断累积的经验去逼近；

（2）、所以我们认识世界本质基于经验积累；

（3）、我们判断事物是什么的准确概率，往往基于经验积累程度多少。或者说，我们经验积累，能够使我们逐步减少判断事件错误的概率。

所以贝叶斯对先验概率的指定既是主观的，又是理性的，而且随经验积累逐渐优化。

从哲学角度看，贝叶斯思想是一种逻辑 + 历史的方法，是归纳推理方法的一次革命（归纳推理就是根据过去的经验预测未来的推理），把经验数据量化，并直接带入预测判断。解决了休谟对归纳推理的合理性提出的质疑。

现在贝叶斯的思想已经成为归纳逻辑的核心, 并且逐步发展为一套一般性的科学推理理论和方法。贝叶斯思想现在是机器学习[1]的核心方法之一。

不用数学公式介绍数学思想，真的很费力，也不知道讲清楚没有。

[1]比较好的书籍参见, 周志华著. 机器学习, 北京: 清华大学出版社,2016. 南京大学周志华研究组链接 http://cs.nju.edu.cn/zhouzh/