

群论导引

离散数学 – 代数结构

南京大学计算机学院

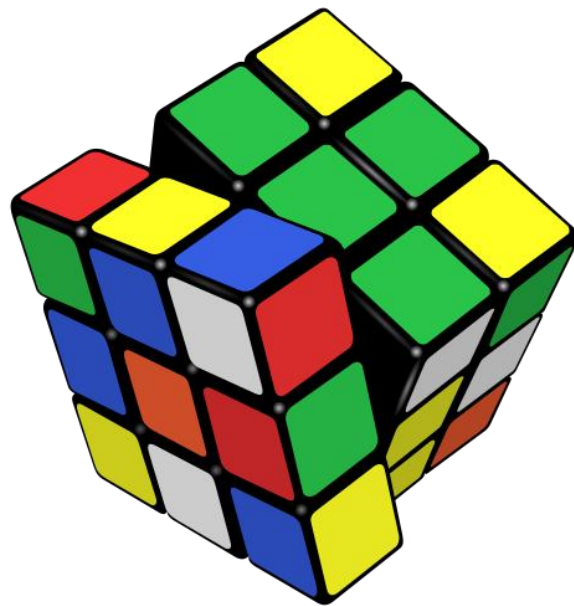
回 顾

- 运算及其封闭性
- 运算的性质
- 运算表
- 代数系统
- 代数系统的性质
 - 结合性、交换性、分配性
 - 单位元、零元、逆元
- 代数系统的同构与同态



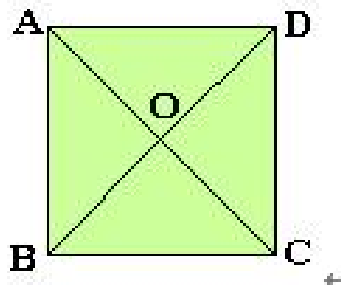
内容提要

- 引言
- 半群
- 么半群
- 群
- 群的性质
- 群的术语
- 群方程*

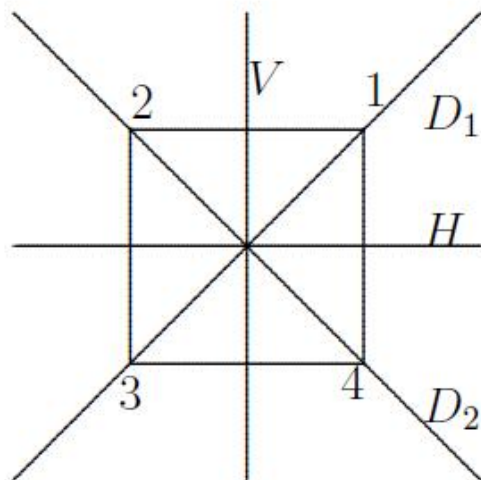


引言：对称变换

- 正方形的**刚体运动**是从四个顶点集到它本身的一一对应（变换），保持相邻点之间**距离不变**



引言：对称变换（续）



设正方形的4个顶点为1、2、3、4；重心为O，对角线为 D_1 和 D_2 ，水平中线为 H ，垂直中线为 V 。以下将从 $\{1, 2, 3, 4\}$ 到 $\{1, 2, 3, 4\}$ 的一一对应记成
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}.$$

我们现在找出正方形所有的对称

引言：对称变换 (续)

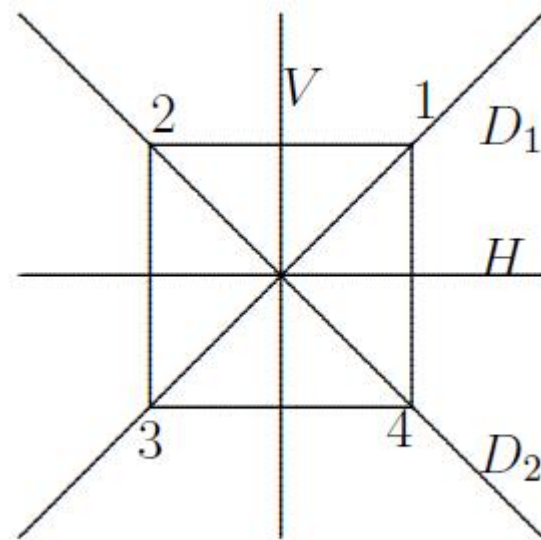
旋转对称：由以下刚体运动完成

$$R_1: \text{绕} O \text{顺时针转} 90^\circ, \text{易见} R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$R_2: \text{绕} O \text{顺时针转} 180^\circ, \text{易见} R_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$R_3: \text{绕} O \text{顺时针转} 270^\circ, \text{易见} R_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$R_0: \text{绕} O \text{顺时针转} 360^\circ, \text{易见} R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

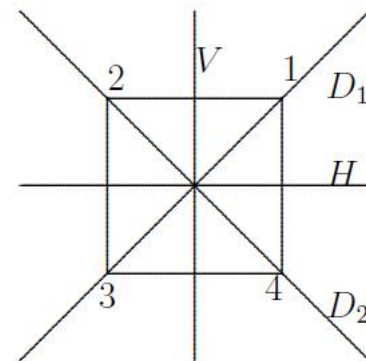


引言：对称变换（续）

反射对称：由以下刚体运动完成

H: 对于水平中线H的反射。 D_1 : 对于对角线 D_1 的反射。

V: 对于垂直中线V的反射。 D_2 : 对于对角线 D_2 的反射。

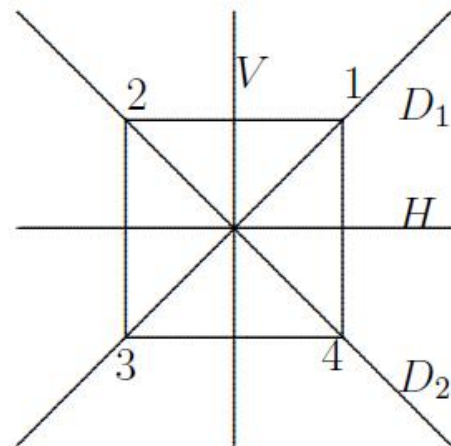


$$H = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \quad V = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad D_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \quad D_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

引言：对称变换（续）

- 两个对称变换的连续作用依然是对称变换

- 例如： $R_1 * H$ 指先右转 90° ，后做水平反射，结果得 D_1 ，故 $R_1 * H = D_1$ ；而 $H * R_1 = D_2$ ；由此可以看出 $R_1 * H \neq H * R_1$



引言：对称变换（续）

Cayley Table

.	R_0	R_{90}	R_{180}	R_{270}	V	H	D_1	D_2
R_0	R_0	R_{90}	R_{180}	R_{270}	V	H	D_1	D_2
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D_2	D_1	V	H
R_{180}	R_{180}	R_{270}	R_0	R_{90}	H	V	D_2	D_1
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D_1	D_2	H	V
V	V	D_1	H	D_2	R_0	R_{180}	R_{90}	R_{270}
H	H	D_2	V	D_1	R_{180}	R_0	R_{270}	R_{90}
D_1	D_1	H	D_2	V	R_{270}	R_{90}	R_0	R_{180}
D_2	D_2	V	D_1	H	R_{90}	R_{270}	R_{180}	R_0

引言：对称变换（续）

令 $S = \{R_0, R_1, R_2, R_3, V, H, D_1, D_2\}$

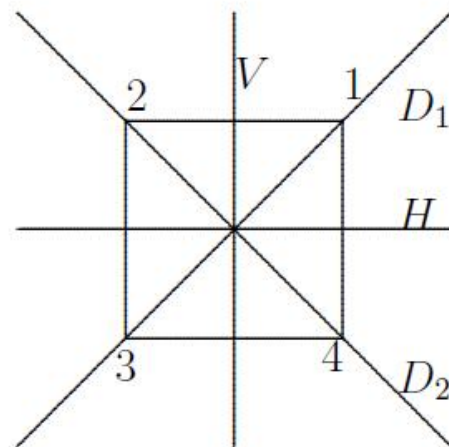
$*$ 为 S 上的两元运算

事实上可通过函数的复合来计算积。例如

$$R_1 * H = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = D_1$$

通过运算可知

- (1) $*$ 对于 S 是封闭的，即 $(\forall x, y \in S)(x * y \in S)$
- (2) $(\forall x, y, z \in S)(x * (y * z) = (x * y) * z)$
- (3) $(\forall x \in S)(R_0 * x = x * R_0 = x)$
- (4) $(\forall x \in S)(\exists y \in S)(x * y = y * x = R_0)$



群论



Je n'ai pas le
temps.



—Evariste Galois

半群

定义 设 $(S, *)$ 为代数系统, $(S, *)$ 为半群 (Semigroup) 指

$$(1) (\forall x, y \in S)(x * y \in S)$$

$$(2) (\forall x, y, z \in S)((x * y) * z = x * (y * z))$$

若 $(\forall x, y \in S)(x * y = y * x)$ 则称 $(S, *)$ 为交换半群 (abelian 半群)

■ “代数系统” + “结合性” = “半群”

■ 例: 代数系统 $\langle \{1,2\}, * \rangle$ 为半群, 其中 $*$ 定义为

$$\forall x, y \in \{1,2\}, x * y = y$$

么半群 (Monoid)

定义 设 $(S, *)$ 为代数系统, $(S, *)$ 为 Monoid (Semigroup with unit) 指

$$(1) (\forall x, y \in S)(x * y \in S)$$

$$(2) (\forall x, y, z \in S)((x * y) * z = x * (y * z))$$

$$(3) (\exists e \in S)(\forall x \in S)(e * x = x * e = x)$$

■ “半群” + “单位元” = “Monoid”

■ 注意: 代数系统中左右单位元若存在则必相等且唯一

么半群 (续)

■ 例1: $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$, $T = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \right\}$

则集合 S 与 T 关于矩阵的乘法皆构成Monoid

■ 例2: $\langle \mathbb{Z}^+, + \rangle$ 为半群, 但非Monoid

■ 例3: $\langle \mathbb{Z}_n, \oplus_n \rangle$ 为Monoid, \oplus_n 是模 n 加法

■ 例4: $\langle A^A, \circ \rangle$ 为Monoid, \circ 是函数复合运算

■ 例5: $\langle \mathcal{P}(B), \oplus \rangle$ 为Monoid, \oplus 为对称差运算

群 (Group)

- $(G, *)$ 为群 **当且仅当** 有 $e \in G$ 和 G 上的一元运算⁻¹使

(0) $G \neq \emptyset$

(1) $(\forall x, y \in G)(x * y \in G)$ 代数系统

(2) $(\forall x, y, z \in G)(x * (y * z) = (x * y) * z)$...半群

(3) $(\forall x \in G)(x * e = e * x = x)$ 么半群

(4) $(\forall x \in G)(x * x^{-1} = x^{-1} * x = e)$ 群

(1) ~ (4) 有时被称为群论公理

群 (续)

- 群的等价描述:

- 设 G 为非空集合, $*$ 为 G 上的二元运算, $\langle G, * \rangle$ 为群指 $\langle G, * \rangle$ 为Monoid, 其单位元为 e , 且满足:

$$(\forall x \in G)(\exists y \in G)(x * y = y * x = e)$$

- 注意: 可结合的代数系统中逆元若存在则唯一

群 (续)

命题 设 $\langle G, *, e \rangle$ 为群, 任何元素之逆是唯一的。

证: 设 y, z 为 x 之逆, 从而

$$x * y = y * x = e = x * z = z * x$$

$$\therefore x * y = e \rightarrow z * (x * y) = z * e$$

$$\rightarrow (z * x) * y = z$$

$$\rightarrow e * y = z$$

$$\rightarrow y = z$$

$$\therefore y = z \quad \square$$

群 (续)

■ 示例

- $\langle \mathbb{R}, + \rangle, \langle \mathbb{Z}, + \rangle$ 为群, 但 $\langle \mathbb{N}, + \rangle$ 不为群 (1 无逆)
- $\langle \mathbb{R} - \{0\}, * \rangle$, 非零实数乘法群; a 的逆元素为 $1/a$
- $\langle \mathbb{Z}_n, \oplus_n \rangle$ 为群, i 之逆为 $n - i$
- 正方形的对称变换集与乘积构成群
- $T_A = \{f: A \rightarrow A \mid f \text{ 为双射} \}$, 单位元 I_A , f 的逆元 f^{-1}
- $A = \{f: \mathbb{R} \rightarrow \mathbb{R} \mid \text{呈形 } f(x) = ax + b\}$, $\langle A, \circ \rangle$ 是群?

群 (续)

设 $f(x) = ax + b$ ($a, b \in \mathbb{R}$) $f \in A$ f 有逆吗?

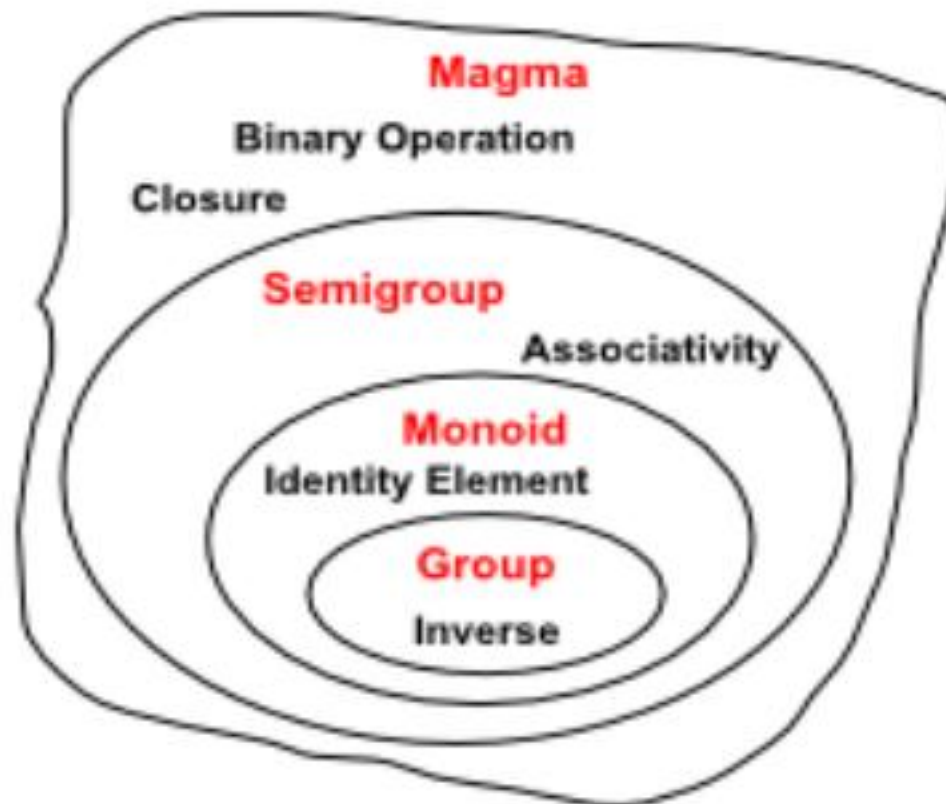
设 $g(x) = cx + d$ ($c, d \in \mathbb{R}$) 为 f 之逆, 从而 $f(g(x)) = g(f(x)) = x$ 。

因此, $a(cx + d) + b = x$, $c(ax + b) + d = x$; $acx + ad + b = x$, $acx + cb + d = x$; $ac = 1$, $ad + b = cb + d = 0$; $c = 1/a$, $d = -b/a$ 。

故当 $a = 0$ 时 f 无逆, 当 $a \neq 0$ 时 f 的逆为 $g(x) = x/a - b/a$ 。

然而令 $A' = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ 呈形 } f(x) = ax + b \text{ 且 } a \neq 0\}$, (A', \circ) 为群。

群 (续)



群的性质

定理 设 $(G, *, e, ^{-1})$ 为群

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

$$(2) (ab)^{-1} = b^{-1}a^{-1}$$

$$(3) ab = ac \rightarrow b = c \text{ (左消去律)}$$

$$(4) ba = ca \rightarrow b = c \text{ (右消去律)}$$

$$(5) \text{方程 } ax = b \text{ 和 } ya = b \text{ 在 } G \text{ 中对 } x, y \text{ 有唯一解}$$

有限群的运算表中每行（列）均为群中所有元素的一种排列，不同行（列）也不可能出现同样的排列。

群的术语：群的阶

- (1) 若 G 为有穷集，则称 $(G, *)$ 为有限群。当 $|G| = n$ 时称 $(G, *)$ 之阶为 n 且称 G 为 n 阶群
- (2) 若 G 为无穷集，则称 $(G, *)$ 为无限群
- (3) 若群 $(G, *)$ 满足 $(\forall x, y \in G)(xy = yx)$ ，则称 G 为交换群(abelian群)

下面我们给出1, 2, 3, 4阶全部不同构的群

- (1) 若 $(G, *)$ 为1阶群，从而设 $G = \{e\}$ 有 $ee = e$ 。故1阶群在同构意义下只有一个。
- (2) 若 $(G, *)$ 为2阶群，从而设 $G = \{e, a\}(a \neq e)$ ，易见 $ea = ae = a$ ， $ee = e$ 但 aa 呢？若 $aa = a$ 则 $a = e$ 矛盾，故 $aa = e$ 。故2阶群在同构意义下只有一个。

乘法表见下：

$*$	e	a
e	e	a
a	a	e

有关群的术语 (续)

(3) 若 $\langle G, * \rangle$ 为 3 阶群，从而可设 $G = \{e, a, b\}$ ， e, a, b 互异。若 $a * a = e$ ，则 $a * b = b$ ，矛盾，故 $a * a = b$ 。运算表唯一。因此，3 阶群在同构意义下只有一个。

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

有关群的术语 (续)

■ 证明：四阶群皆为Abel群

证：设 $G = \{e, a, b, c\}$, e 为幺。现证 $ab = ba$

情况1. $ab = e$ 从而 ba 只能为 e 或 c , 若 $ba = c$ 则 $aba = ac$, 从而 $ea = ac$, 从而 $c = e$ 矛盾, 故 $ba = e$ 。

情况2. $ab = c$, 同理 $ba = c$

同理 $bc = cb$, $ac = ca$ 。 \square

■ 证明：四阶群中元素的阶为1、2或者4（不为3）。

假设有个元素 a 的阶为3, $\{e, a, a^2, b\}$, $ab=?$ (矛盾)

有关群的术语 (续)

(4) 只有两种四阶群

- 有个元素的阶为4:

$$\{e, a, a^2, a^3\}$$

与 $\langle \mathbb{Z}_4, \oplus_4 \rangle$ 同构

- 元素的阶均不为4:

Klein四元群

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

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

群的方程定义*

- 群有以下二种等价的定义：
- (1) 若 $\langle G, * \rangle$ 为半群且方程 $ax = b$ 与 $ya = b$ 有唯一解，则称 $\langle G, * \rangle$ 为群
- (2) 若 $\langle G, * \rangle$ 为半群，存在左单位元，且每个元素都具有左逆元，则 $\langle G, * \rangle$ 称为群

群 方 程*

定理 若代数系统 $(G, *)$ 为半群且在 G 中方程 $ax = b$ 与 $ya = b$ 有唯一解, 则 $(G, *)$ 为群

证: 第一步 证明有左幺 $e_l \in G$ 使 $(\forall a \in G)(e_l a = a)$

取定 $b \in G$, $xb = b$ 有唯一解, 设为 e_l 。对任何 $a \in G$ 下证 $e_l a = a$ 。

$\because bx = a$ 有解 c , $\therefore e_l a = e_l(bc) = (e_l b)c = bc = a$

第二步 证明 $(\forall a \in G)(\exists a^{-1} \in G)(a^{-1}a = e_l)$ 即左逆存在

令 a^{-1} 为 $ya = e_l$ 的唯一解即可

第三步 证明 $aa^{-1} = e_l$ 即左逆=右逆

$\because a^{-1} \in G \therefore ya^{-1} = e_l$ 有唯一解 a' , 从而 $a'a^{-1} = e_l$ 从而

$$aa^{-1} = e_l(aa^{-1}) = (a'a^{-1})(aa^{-1}) = a'(a^{-1}a)a^{-1} = a'e_la^{-1} = a'a^{-1} = e_l$$

第四步 $(\forall a \in G)(ae_l = a)$ 即左幺=右幺

$$\because ae_l = a(a^{-1}a) = (aa^{-1})a = e_la = a \therefore ae_l = a$$

因此 $(G, *, e, ^{-1})$ 为群 \square

群的方程定义* (续)

对于半群 $\langle G, * \rangle$, 设 e_l 为其左幺元 (题设), 对任意 $a \in G$, a_l 为其左逆元 (题设), 故 $a * a_l = e_l$, 因为 $a_l \in G$, 故对于 a_l , $\exists a^{-1} \in G$, 使得 $a^{-1} * a_l = e_l$, 则立即有: $a * a_l = e_l * (a * a_l) = (a^{-1} * a_l) * (a * a_l) = a^{-1} * (a_l * a) * a_l = a^{-1} e_l a_l = a^{-1} a_l = e_l$. 故左逆元 = 右逆元;

下证 e_l 即为右幺: $\forall a \in G$, $a * e_l = a * (a_l * a) = (a * a_l) * a = e_l * a = a$, 故 e_l 即为系统的幺元, $\forall a \in G$, a_l 为 a 之逆. 综上, $\langle G, * \rangle$ 即为群.

群的方程定义* (续)

推论 设 $(G, *)$ 为半群且 $|G|$ 有穷, 若 $(G, *)$ 满足消去律, 则 $(G, *)$ 为群

证: 设 $G = \{a_1, \dots, a_n\}$, $\forall a, b \in G$ 下证明方程 $ax = b$ 有唯一解, 令 $aG = \{aa_i | i = 1, 2, \dots, n\}$

\because 左消去律 $\therefore |aG| = n$ 从而 $aG = G$ 而 $b \in G$ 故有 $a_i \in G$ 使 $aa_i = b$ 从而 $ax = b$ 有解,
又 \because 左消去律 \therefore 解唯一。同理可证 $ya = b$ 有唯一解。因此 $(G, *)$ 为群。 \square

有穷代数系统若满足结合律和消去律, 则必为**群**。

$\langle \mathbb{Z}^+, * \rangle$ (普通乘法) 满足结合律和消去律, 但**不是**群

作业

- 教材内容：[屈婉玲] 10.1 节
- 课后习题：见课程主页

Niels Abel (1802-1829): 天才与贫困



阿贝尔的第一个抱负不凡的冒险，是试图解决一般的五次方程。…失败给了他一个非常有益的打击；它把他推上了正确的途径，使他怀疑一个代数解是否是可能的。他**证明了不可解**。那时他大约十九岁。

阿贝尔的《关于非常广泛的一类超越函数的一般性质的论文》呈交给巴黎科学院。这就是勒让德后来用贺拉斯的话描述为“永恒的纪念碑”的工作，埃尔米特说：“**他给数学家们留下了够他们忙上五百年的东西。**”它是现代数学的一项登峰造极的成就。(摘自贝尔：《数学精英》)

这篇论文的一个评阅人勒让德74岁，发现这篇论文很难辨认，而另一位评阅人，39岁的柯西正处于自我中心的顶峰，把论文带回家，不知放在何处，完全忘了。4年后，当柯西终于将它翻出来时，阿贝尔已经不在人世。作为补偿，科学院让阿贝尔和雅可比一起获得1830年的数学大奖。