抽象代数讲义

黎永锦 编著

科学出版社

抽象代数讲义

黎永锦　编著

科学出版社
北京

内 容 简 介

本书是根据作者近年来在中山大学数学系讲授抽象代数课程的讲义写成的. 全书共 7 章. 第 1 章群论, 第 2 章环和域, 第 3 章环上的多项式, 第 4 章向量空间, 第 5 章 Sylow 定理和可解群, 第 6 章域的扩张, 第 7 章群论在微分方程中的应用. 书中附有习题和部分解答. 本书的特点是加强了代数与分析的联系, 书中还介绍了代数的一些较新的结果.

本书可作为高等院校数学专业高年级本科生和研究生学习抽象代数的教材, 也可供相关专业教师阅读参考.

图书在版编目(CIP)数据

抽象代数讲义/黎永锦编著. —北京：科学出版社, 2012
ISBN 978-7-03-033935-5
Ⅰ. ①抽… Ⅱ. ①黎… Ⅲ. ①抽象代数－高等学校－教材 Ⅳ. ①O153

中国版本图书馆 CIP 数据核字(2012) 第 054850 号

责任编辑: 李 欣 赵彦超 / 责任校对: 李 影
责任印制: 钱玉芬 / 封面设计: 陈 敬

科学出版社 出版
北京东黄城根北街 16 号
邮政编码: 100717
http://www.sciencep.com

新科印刷有限公司 印刷

科学出版社发行 各地新华书店经销
*
2012 年 5 月第 一 版 开本: B5(720 × 1000)
2012 年 5 月第一次印刷 印张: 15 1/4
字数: 290 000

定价: 58.00 元

(如有印装质量问题, 我社负责调换)

前　言

抽象代数是现代数学中的重要分支之一, 它产生于 19 世纪, 是研究各种抽象的公理化代数系统的数学学科. 抽象代数包含群、环、域和伽罗瓦理论等许多分支, 并与数学其他分支相结合产生了代数几何、代数数论、代数拓扑、拓扑群等数学学科. 通过这一课程, 学生可了解抽象代数的基本思想、原理及在其他学科中的应用, 掌握抽象代数的基本概念和重要的定理, 学会用代数处理问题的方法, 还可以加深学生理解数学理论的基本思想, 提高抽象思维能力. 抽象代数为学习代数几何、代数数论、代数拓扑、Banach 代数、李群等课程打下基础. 另外, 抽象代数的主要内容群、环、域等与物理学、化学等有紧密的联系, 总之, 它不仅在数学的各个分支有广泛的应用, 而且在许多现代科学, 如量子力学、结晶学、理论物理、量子化学以及密码学、系统科学、数理经济等领域都有广泛的应用.

本书根据作者在中山大学数学系讲授抽象代数课程时的讲稿, 在多年的教学过程中不断修改而成. 书中尽可能地介绍抽象代数中一些概念和定理的来历, 让学生可以了解一些抽象代数的历史, 提高学习兴趣. 不需要具有点集拓扑学的知识, 只要有数学分析和高等代数中关于矩阵和多项式的基础, 阅读本书是不会有困难的. 本书刻意加强了抽象代数和数学分析的连接, 目的是使抽象代数更加接近数学分析. 本书内容共分 7 章. 第 1 章是群论, 为了加强与点集拓扑学的联系, 编写了拓扑群一节, 简单地对拓扑群作了介绍. 在第 2 章中环上的微分和拓扑环部分, 加强了环与分析和拓扑的连接. 第 3 章环上的多项式中的非交换环上的多项式这一节, 给出了多项式在环不交换的情况下的特殊性质. 考虑到较多的抽象代数教材讲述的内容与数学其他学科的交叉很少, 因此编写了第 7 章, 目的是让学生初步理解抽象的群论等在微分方程等其他数学分支有着广泛的应用. 在教学时, 拓扑群和拓扑环以及群论在微分方程中的应用可以不讲或选讲. 本书可作为抽象代数的一本入门教材, 书中选有一定的习题. 书中的习题参考了很多抽象代数习题解答的书, 如腾加俊的《近世代数辅导与习题精解》、冯克勤的《近世代数三百题》等, 有些习题修改后比较难说明其出处, 无法指出并一一致谢. 为了教学的方便, 双数序号的习题都有解答, 单数序号的习题一般不再给出答案.

书中数学家的头像等图片是作者自己用电脑制作的, Galois 的图像是我的学生

张余的作品. 我要向我的学生们表示衷心的感谢, 龙永彪、王俊涛、邹昆儒、黄栋超、庄跃鸿、王观发等对本书的改进和校对做了很多的工作. 刘佩、赵志红、和炳和顾朝晖等在校对时提出了很多很好的意见. 在多年来的教学过程中, 我从学生身上学到了很多东西, 本书正是在他们的帮助下不断修改完善的结果.

黎永锦

2011 年 8 月于中山大学

符　号　表

$\mathbf{Q}$	有理数域
$\mathbf{R}$	实数域
$\mathbf{C}$	复数域
$\mathbf{Z}$	整数集合, 正负整数, 包含 0
$\mathbf{N}$	自然数集
$a\|b$	a 整除 b
$a \equiv b(\mathrm{mod}m)$	a 与 b 模 m 同余
(a,b)	a 和 b 的最大公因子
$o(a)$	a 的阶
$\|G\|$	群 G 的阶
S_n	n 个字母的对称群
$\mathbf{Z}_n$	模 n 整数加法群或环
$\mathbf{Z}_p$	模 p 整数加法群或域 (p 为素数)
$\cong$	同构
$\mathrm{Ker}(f)$	同态 f 的核
$< H >$	由集合 H 生成的子群
$< a >$	由元素 a 生成的循环子群
$aH,\ Ha$	a 的左陪集和右陪集
$[G:H]$	子群 H 在群 G 中的指数
GH	$\{ab\|a \in G, b \in H\}$
$H \triangleleft G$	H 为 G 的正规子群
G/H	G 对 H 的商群
$\mathrm{sgn}\sigma$	置换 σ 的符号
A_n	n 个字母的交错群
$C_H(a)$	a 在 H 中的中心化子
$N_H(K)$	H 在 K 中的正规化子
$C(G)$	G 的中心
G'	G 的换位子群
$G^{(n)}$	G 的第 n 次导群

$\mathrm{char}R$	环 R 的特征
(H)	由集合 H 生成的理想
(a)	由元素 a 生成的主理想
$F[x]$	F 上的多项式环
$F[x_1, x_2, \cdots, x_n]$	F 上 n 个未定元的多项式环
$\deg f$	多项式 f 的次数
$\dim V$	线性空间 V 的维数
G_f	多项式 f 的伽罗瓦群
H^{-1}	$H^{-1} = \{a^{-1} \mid a \in H\}$
$R[a]$	由 R 和 a 生成的环, 包含 R 和 a 的最小环
$F(a)$	域 F 上的单扩张
$[K : F]$	域扩张 K/F 的次数

我们是孩子, 但我们精力充沛,

勇往直前…

——伽罗瓦(E. Galois, 1811—1832)

目　　录

前言
符号表
第 1 章　群论 ····· 1
1.1　群的定义 ····· 1
1.2　子群 ····· 5
1.3　置换群 ····· 10
1.4　陪集 ····· 16
1.5　正规子群 ····· 22
1.6　交错群 ····· 29
1.7　群的同态 ····· 31
1.8　群的直积 ····· 37
1.9　拓扑群 ····· 41
习题一 ····· 44
学习指导 ····· 47
第 2 章　环和域 ····· 52
2.1　基本概念 ····· 53
2.2　理想和商环 ····· 59
2.3　环的同态 ····· 65
2.4　域 ····· 69
2.5　环上的微分 ····· 75
2.6　拓扑环 ····· 77
习题二 ····· 80
学习指导 ····· 83
第 3 章　环上的多项式 ····· 88
3.1　多项式 ····· 88
3.2　带余除法 ····· 92
3.3　因式分解 ····· 100
3.4　本原多项式 ····· 108
3.5　唯一因子分解环上的多项式 ····· 111
3.6　非交换环上的多项式 ····· 113

习题三 ····· 118
学习指导 ····· 120
第 4 章　向量空间 ····· 125
4.1　向量空间 ····· 125
4.2　内积空间 ····· 131
4.3　模 ····· 134
习题四 ····· 139
学习指导 ····· 141
第 5 章　Sylow 定理和可解群 ····· 144
5.1　群作用 ····· 144
5.2　Sylow 定理 ····· 151
5.3　可解群 ····· 156
习题五 ····· 163
学习指导 ····· 165
第 6 章　域的扩张 ····· 168
6.1　子域和扩域 ····· 168
6.2　代数扩张 ····· 173
6.3　Galois 域和分裂域 ····· 178
6.4　方程的根式解 ····· 189
习题六 ····· 196
学习指导 ····· 198
第 7 章　群论在微分方程中的应用 ····· 202
7.1　微分方程的不变群 ····· 202
7.2　一阶常微分方程的求解 ····· 207
7.3　常微分方程的降阶 ····· 210
习题七 ····· 211
学习指导 ····· 212
参考文献 ····· 214
部分习题解答 ····· 215
索引 ····· 231

第1章 群 论

最有价值的科学书籍是作者在书中明白地指出了他所不明白的东西的那些书, 遗憾地, 这还很少被人们所认识; 作者由于掩盖难点, 大多害了他的读者.

伽罗瓦 (1811—1832, 法国数学家)

群论起源于解高次方程, 它的思想可以追溯到 Lagrange. Lagrange 关于方程式根的对称函数的工作, 使人们注意到根的置换的性质, 从而导致置换群理论的产生. 18 世纪末, Lagrange, Vandermonde, Ruffini 等试图求出高次代数方程的代数解法, 由研究方程诸根之间的置换而注意到了群的概念, 挪威数学家 Abel 证明了 5 次以上的一般的代数方程没有根式解. 而置换群与代数方程之间的关系的完全描述是由伽罗瓦在 1830 年左右做出的, Jordan 在《置换和代数方程论》中对伽罗瓦理论作了很好的介绍. 很多数学家都对群论的发展做出了巨大贡献, 如 Möbius, Cayley, Klein 等. 群的概念已经被认为是数学及其应用中最基本的概念之一, 在几何学、代数拓扑学、泛函分析等学科中起着重要的作用, 并形成了拓扑群、李群、代数群等新学科. 同时, 群论在理论物理、量子化学以及编码学等都有重要的应用.

1.1 群的定义

群论对 19~20 世纪的数学整体发展影响深远, 群论的影响不仅深入数学领域的每个分支, 还在某种程度上促进了数学各个分支的统一.

1 二元运算

定义 1.1.1 设 S 和 G 都是集合, 则称所有有序对 (a,b) 构成的集合为它们的笛卡儿积, 其中 $a\in S$, $b\in G$, 记为 $S\times G$.

在算术中, 若 a,b 都是整数, 则 a 和 b 的加法运算将 a 和 b 从整数集 $\mathbf{Z}\times\mathbf{Z}$ 映

到 **Z**. 类似地, 在集合上, 可以定义二元运算.

定义 1.1.2　从 $S \times S$ 到 S 的一个映射 $\cdot$ 称为 S 上的一个二元运算.

也就是说, 对 S 中的任何一对元素 (a, b) 都有 S 中唯一确定的一个元素 $a \cdot b$ 与之对应.

例 1.1.1　取 S 为实数全体所构成的集合, 将映射 $\cdot$

$$\cdot : S \times S \to S$$

定义为

$$a \cdot b = a^2 + b^2,$$

则 $\cdot$ 就是一个二元运算.

例 1.1.2　设 $S = \{(a_1, a_2) | a_1, a_2$ 都是实数$\}$是二维欧氏空间, 则向量和 $u + v$, 矢量积 $u \times v$ 都是二元运算. 但内积的结果不再是向量, 而是一个数, 因此内积不是二元运算.

例 1.1.3　设 S 是 n 阶方阵全体所构成的集合, 则 $A + B$, AB, $AB - BA$ 是三种不同的二元运算.

2　群的定义和例子

伽罗瓦, Jordan 和 Klein 只用封闭性公理来定义群, 不过他们考虑的是置换或变换的有限群, 因此其他的公理都隐含在他们的论文里面. Cayley 在 1854 年的论文中才明确了群要有结合律和单位元. 1882 年 Dyck 和 Weber 都发表了完整的群的公理.

定义 1.1.3　设 G 是一个非空集合, 若在 G 上定义一个二元运算 $\cdot$, 满足

(1) 结合律: 对任何 $a, b, c \in G$, 有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, 则称 G 是一个半群 (semigroup), 记作 $(G, \cdot)$. 若 $(G, \cdot)$ 还满足

(2) 存在单位元 $e \in G$, 使对任何 $a \in G$ 有 $e \cdot a = a \cdot e = a$.

(3) 对任何 $a \in G$, 有 $a^{-1} \in G$, 使得 $a^{-1} \cdot a = a \cdot a^{-1} = e$, 则称 $(G, \cdot)$ 是一个群 (group).

如果半群中也有单位元, 则称为幺半群 (monoid).

幺半群不一定是群, 如整数集 **Z** 对于乘法是一个幺半群, 但它不是群.

如果群 $(G,\cdot)$ 适合交换律: 对任何 $a,b\in G$ 有 $a\cdot b=b\cdot a$, 则称 G 为交换群或 Abel 群.

Abel 于 1827 年发现, 如果多项式方程的根的伽罗瓦群是交换的, 那么该多项式方程一定可以用公式求解, Abel 群这一术语是 Jordan 在 1872 年引入来纪念数学家 Abel 的. 对于 Abel 群, 群运算常常称为加法, 记为 $a+b$. 这时单位元称为零元, 记作 0, 元素 a 的逆元记作 $-a$. 对任意自然数 n, 元素 a 的 n 倍 na 定义为 n 个 a 相加.

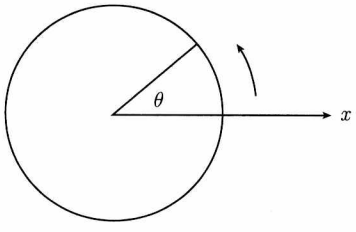
Niels Henrik Abel(1802—1829)

群中的乘法运算一般简记为 ab. 如果 $ab=ba=e$, 那么就称 a 为一个可逆元 (invertible element) 并称 b 为 a 的逆元 (inverse element). 可逆元 a 的逆元通常记作 a^{-1}. 容易知道可逆元的逆元是唯一的.

例 1.1.4 整数集 $\mathbf{Z}$ 对普通加法构成 Abel 群.

例 1.1.5 实数集 $\mathbf{R}$ 对普通加法构成 Abel 群, 但在乘法下不是群.

例 1.1.6 $[0,1]$ 上的所有实连续函数 $C[0,1]$ 全体加法构成 Abel 群, 但在函数相乘的乘法下不是群.



例 1.1.7 所有 2×2 可逆矩阵 $GL(2,\mathbf{R})$ 全体在矩阵的相乘的乘法下构成非交换群, 其单位元就是单位矩阵.

例 1.1.8 对于 $0\leqslant\theta<2\pi$, 所有形如

$$\begin{bmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{bmatrix}$$

的矩阵, 在矩阵乘法下是一个群. 容易知道这是平面上的旋转.

例 1.1.9 设 $K_4=\{e,a,b,c\}$, 乘法表为

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

则 K_4 是一个交换群, 称为**克莱因四元群**(Klein four-group), 记作 $\{e,a,b,ab\}$, 它是 Klein 在 1884 年给出的.

上面例子中的表一般称为**群的乘法表**(multiplication table), 也称为**群表**(group table) 或**凯莱表**(Cayley table). 乘法表常用来表示有限群的运算. 群表是凯莱在 1854 年的论文 *On the theory of groups, as depending on the symbolic equation* $\theta^n=1$ 中首次提出的. 通过群表, 可以直观地了解该群的单位元及是否交换等.

3　群的性质

性质 1.1.1(消去律)　*设群 G 中的元素 a, b, c 满足 $ab=ac$ 或 $ba=ca$, 则 $b=c$.*

Felix Christian Klein(1849—1925)

证明　若 $ab=ac$, 则在等式两边同时左乘 a^{-1}, $a^{-1}(ab)=a^{-1}(ac)$, 由结合律可知

$$(a^{-1}a)b=(a^{-1}a)c,\ \text{故}\ eb=ec,\ \text{所以}\ b=c.$$

同理, $ba=ca$ 时, 有 $b=c$. ■

容易知道, 设 G 是群, 则对任意的 $a,b\in G$, 方程 $ax=b$ 和 $ya=b$ 在 G 中都有唯一解. 不难验证, 群还具有下面的一些简单性质.

性质 1.1.2　*设 a, b 是群 G 中的两个元素.*

(1) *若 $ab=a$ 或 $ba=a$, 则 $b=e$;*

(2) *若 $ab=e$ 或 $ba=e$, 则 $b=a^{-1}$;*

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

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

4　元素的阶

Cayley 在 1815 年定义了群的元素的阶.

定义 1.1.4　*由有限多个元素构成的群 G 称为有限群* (finite group), *其中元素的个数记作 $|G|$, 称为 G 的阶* (order). *用 $|G|=\infty$ 表示 G 是无限群.*

定义 1.1.5　若 a 是群 G 的一个元, 则使得 $a^n = e$ 的最小的正整数 n 称为 a 的阶或周期, 记为 $o(a)$. 若这样的正整数 n 不存在, 则称 a 的阶为无穷.

例 1.1.10　2×2 可逆矩阵 $GL(2, \mathbf{R})$ 群中, 由于矩阵

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad A^n = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix},$$

故 A 的阶是无穷.

定理 1.1.1　若 a 的阶为 m, 则 $a^n = e$ 当且仅当 m 整除 n.

证明　设 m 整除 n, 则存在整数 k, 使得 $n = mk$. 故

$$a^n = a^{mk} = e.$$

反过来, 若 $a^n = e$, 但 m 不整除 n, 则 $n = mk + r$, $1 \leqslant r < m$. 于是 $a^r = a^{mk+r} = a^n = e$, 但这与 m 是 a 的阶矛盾. ■

思考题 1.1.1　是否存在一个群, 除了单位元外, 所有的元的阶都是无穷?

例 1.1.11　所有非零正实数 G 在乘法下是一个群, 容易看出该群除了单位元外, 所有的元的阶都是无穷.

思考题 1.1.2　对任意自然数 n, 是否存在一个群 G, G 的阶就是 n?

例 1.1.12　设 C 为复数, 则所有 n 次单位根构成的集合

$$\begin{aligned} G &= \{a \in C | a^n = 1\} \\ &= \left\{ \cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n} | k = 0, 1, 2, 3, \cdots, n-1 \right\} \end{aligned}$$

在乘法下, 就是一个 n 阶的 Abel 群.

1.2 子　群

如果群 G 的子集 H 对 G 的运算构成群, 那么称它是 G 的子群. 通过研究子群 H 的性质, 可以了解群 G 的一些整体性质.

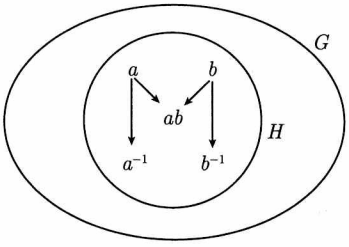
1 子群的定义

定义 1.2.1　设 H 是群 G 的满足下面两个条件的一个非空子集:

(1) (乘法封闭) 对 H 中的任意元 a 和 b 都有 $ab \in H$;

(2) (求逆封闭) 对 H 中的任意元 a 都有逆元 $a^{-1} \in H$.

则称 H 为 G 的一个子群.



根据乘法封闭性, H 中的乘法运算是有意义的. 乘法结合律自然成立. 由于 H 非空, 存在 $a \in H$. 于是 $a^{-1} \in H$, $e = a^{-1}a$. 因此 H 含有单位元. 所以 H 在乘法下构成一个群, 这就是 "子群" 这个名词的意义.

容易看出, Abel 群的子群仍然是 Abel 群.

例 1.2.1　每个群 G 一定有两个子群 $\{e\}$ 和 G, 称为 G 的平凡子群.

例 1.2.2　设 n 是一个自然数, 令 $n\mathbf{Z}$ 为所有被 n 整除的整数所构成的集合, 它是整数加法群 $\mathbf{Z}$ 的子群.

例 1.2.3　令 $SL_n(K)$ 为数域 K 上行列式等于 1 的 n 阶方阵全体所构成的集合, 它是 n 阶可逆矩阵群 $GL_n(K)$ 的子群, 称为**特殊线性群**(special linear group).

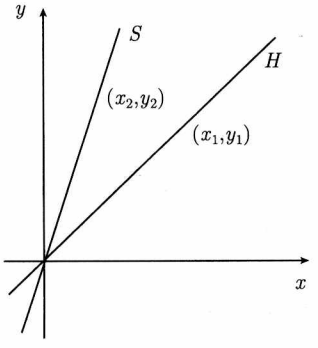
例 1.2.4　设 l_∞ 为所有有界实数列全体, 则在加法下它是一个群, 若 c_0 为所有收敛到零的实数列全体, 则在加法下 c_0 是 l_∞ 的一个子群.

在 $\mathbf{R}^2$ 按坐标的加法所构成的加法群中, 容易看出过点 (x_1, y_1) 的子群 H 在过点 (x_1, y_1) 和 $(0,0)$ 的直线内. 但经过点 (x_1, y_1) 的子群不是唯一的, 如

$$H_1 = \{(nx_1, ny_1) | n \text{ 为整数}\},$$

$$H_2 = \{(qx_1, qy_1) | q \text{ 为有理数}\}$$

都是 $\mathbf{R}^2$ 经过点 (x_1, y_1) 的子群. 另外, 经过点 (x_2, y_2) 和 $(0,0)$ 的直线一定是 $\mathbf{R}^2$ 的一个子群, 如右图中的 S 和 H 都是 $\mathbf{R}^2$ 的子群.



2 子群的性质

命题 1.2.1(子群判别法)　设 H 是群 G 的一个非空子集, 若 $ab^{-1} \in H$ 对任意 $a, b \in H$ 成立, 则 H 是 G 的一个子群.

证明　任取 $c \in H$, 则 $e = cc^{-1} \in H$. 对任意的 $a \in H$, 有 $a^{-1} = ea^{-1} \in H$, 因此 H 对求逆封闭. 对任意 $a, b \in H$ 都有 $ab = a(b^{-1})^{-1} \in H$, 故 H 对乘法封闭. 所以 H 是 G 的一个子群. ■

性质 1.2.1　设 $\{H_\alpha\}_{\alpha \in I}$ 是群 G 的任意多个子群, 则 $H = \cap_{\alpha \in I} H_\alpha$ 是 G 的一个子群.

证明　由于 $e \in \cap_{\alpha \in I} H_\alpha$, 故 H 非空. 设 $a, b \in H$, 则 $ab^{-1} \in H_\alpha$ 对每个 $\alpha \in I$ 成立, 故 $ab^{-1} \in H$, 所以 H 是 G 的一个子群. ■

3 中心化子

定义 1.2.2　设 g 是群 G 的一个元素, 则集合 $C(g) = \{a \in G | ag = ga\}$ 称为 g 在 G 中的中心化子 (centralizer), 设 $S \subseteq G$, 则集合 $C(S) = \{a \in G | ag = ga$ 对所有 $g \in S\}$ 称为 S 在 G 中的中心化子. $C(G)$ 称为 G 的中心 (center).

例 1.2.5　所有对角线上都是 1 的 3×3 实上三角矩阵 G 全体在矩阵的相乘的乘法下构成非交换群, G 的中心 $C(G)$ 就是形如:

$$\begin{bmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

的实矩阵全体构成的子群.

明显地, $C(g)$ 和 $C(S) = \cap_{g \in S} C(g)$ 都是 G 的子群. 容易看出, 下面性质成立.

性质 1.2.2　(1) G 的中心 $C(G)$ 是 Abel 群.

(2) G 是 Abel 群当且仅当 G 的中心 $C(G)$ 就是 G.

性质 1.2.3　设 H_1 和 H_2 是群 G 的子集, $H_1 \subseteq H_2$, 则

(1) $C(H_1) \supseteq C(H_2)$;

(2) $H_1 \subseteq C(C(H_1))$;

(3) $C(H_1) = C(C(C(H_1)))$.