抽象代数简明教程

李慧陵 周胜林 刘伟俊 编著

清华大学出版社

抽象代数
简明教程

李慧陵 周胜林 刘伟俊 编著

清华大学出版社
北京

内 容 简 介

本书第 1 章在复数域内讨论数域扩张理论，在数域的特殊情况下引出了 Galois 群的概念. 第 2、3 章建立了群、环、域的概念，介绍了群论和环论的基本理论. 第 4 章讨论一般的域扩张理论，以及 Galois 理论的基本内容. 第 5 章是模论，在其中用抽象代数的方法重新建立了矩阵的 Jordan 标准形理论. 本书编者长期从事代数学的教学工作，有丰富的教学经验. 在处理数学问题时力求直接了当，努力做到叙述清楚，务求语言精确并且流畅. 每章末附有习题供练习用.

本书可作为高等院校数学各专业抽象代数课程教材，也可供自学者和科技工作者阅读.

图书在版编目(CIP)数据

抽象代数简明教程/李慧陵，周胜林，刘伟俊编著. --北京：清华大学出版社，2014

ISBN 978-7-302-36335-4

Ⅰ. ①抽…　Ⅱ. ①李… ②周… ③刘…　Ⅲ. ①抽象代数－教材　Ⅳ. ①O153

中国版本图书馆 CIP 数据核字(2014)第 084714 号

责任编辑：汪　操
封面设计：傅瑞学
责任校对：赵丽敏
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京国马印刷厂
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　　张**：12　　**字　　数**：267 千字
版　　次：2014 年 7 月第 1 版　　**印　　次**：2014 年 7 月第1 次印刷
印　　数：1～2000
定　　价：26.00 元

产品编号：057127-01

前　言

抽象代数是数学系的一门重要专业课, 其任务是提供近代代数学的基础知识和基本训练, 但它也是一门比较难学、比较难教的课程. 由于代数学在处理问题的思路和方法上与其他数学分支有很大差异, 加之没有后续课程, 以及本身教学时数不多, 所以学生对这门课程往往掌握得不够好. 抽象代数的教学的不足会使学生在数学修养上有所欠缺.

抽象代数教学效果不尽如人意的原因除去学时少和没有后续课程外, 教学内容的选取也是重要因素. 在某些情况下, 由于受到学时的限制, 抽象代数只讲一些基本概念, 如群、环、域等以及它们的初等性质, 而没有讲授代数的进一步理论和应用, 这使学生对代数理论所包含的数学思想缺乏了解. 结果是学生们知道了一些概念, 但没有看到它们解决了什么问题, 也就不会对这门学问有多少印象了.

本书是作为大学本科数学系抽象代数课程的教材来编写的, 也是对这一课程教材建设的一个探索. 我们在本书写作时, 遵循下面几个做法:

一、本书以域论和多项式方程的 Galois 理论作为一个重点. 这当然是抽象代数教材的通常做法. 这样做的原因在于 Galois 理论在代数学发展史上的划时代的意义. 在古代, 代数学的研究内容是解方程, 而在 Galois 理论出现后, 代数学的研究对象就转向各种代数体系的构造. 正是伽罗华揭示了代数体系的性质是代数学里一些数学现象出现的最根本的原因. 在介绍这个理论时, 我们不追求讲法的新颖性、一般性甚至严密性, 我们要说清楚的是子域和子群的对应关系以及方程可解与 Galois 群可解的关系, 是包含在这个理论中的数学思想.

二、本书在讲法上也作了一些尝试. 我们在第 1 章专门讨论数域扩张问题, 从数域的单纯扩张、分裂域一直到多项式的 Galois 群, 把数域的扩张问题演习了一遍. 这和一般抽象代数教材从群的定义开始讲授有较大的不同. 数域是我们身边的数学对象, 学生们对它早已有所了解. 只不过没有从代数学的角度去思考过问题. 此时讲数域扩张实际上是从一个新的角度去思考熟悉的对象. 在这里, 由于代数基本定理, 单纯扩域和分裂域的存在是明显的, 本原元素定理不难证明, 所以数域扩张的这部分内容也较容易, 学生们理解起来也没有困难. 编者曾经按这个办法讲授过, 学生们对于相关内容都能理解并表现出很大的兴趣. 这一章, 还对包含三等分角在内的所谓“古希腊三大几何作图问题”用域扩张理论证明了不可能. 在引出 Galois 群之后, 我们转向群和环的公理化的讨论, 即第 2、3 两章的内容, 重点是同态的理论. 这一部分也不从群论和环论的角度追求完整和数学上的严密, 在一定程度上还承认直觉, 目的只是为一般的域扩张理论做环论的准备, 为 Galois 理论做群论方面的准备. 在第 4 章则讲授任意域的扩张理论. 此时我们借助环同态理论来建立任意域上单纯扩张的存在性和分裂域的存在性. 于是就把第 1 章中的理论从数域推广到任意域上, 然后证明 Galois 理论的基本定理和方程可解的判别法.

三、为了帮助学生掌握抽象代数的新概念, 我们不断地回顾高等代数的内容, 试图用新概念去说明高等代数中的一些问题. 例如在谈到群作用时我们会举出许多在高等代数中出现

的群作用、轨道、轨道代表元的例子. 这样做, 一方面帮助学生理解新概念, 另一方面又使学生对高等代数的内容有更深的理解, 我们确信这也是提高教学质量的一种手段. 本书内有大量的例子. 有些例子中包含不少的计算, 建议学生们自己动手做这种计算.

四、本书包含的内容有些可能超出教学的需要, 这其实也是正常的现象. 这样做的好处是使教师有了一定的选择余地. 对于内容和学时不匹配的矛盾, 使用本教材时可以通过下面举出的一种或多种方式加以解决. 其一, 整个第 5 章可以不讲; 其二, 第 2、3 两章中带*号的内容可以不讲或少讲; 其三, 在第 4 章 Galois 理论部分我们在写法上做了特别的安排: 首先用整个一节的篇幅对这个理论的要点做了较详细的介绍, 并用例子加以说明, 然后再用三节的篇幅对介绍中举出的主要结论一一证明. 于是在使用本教材时, 如果感到学时紧张, 可以只学习介绍理论要点的那一节, 而把后面三节作为阅读材料. 我们估计, 只要学生用心体会要点介绍的那一节的内容, 也可以对 Galois 理论有一定的理解.

本书只是抽象代数教材建设的一种探索, 对于如何编出好教材, 我们有一些想法, 但这些想法是否正确, 以及这些想法是否在本书中很好地体现, 都是需要在使用中加以检验的. 因编者水平有限, 如有错误或不当之处, 欢迎读者批评指正.

编 者

2014 年 1 月

目　录

第 1 章　数环和数域

抽象代数的研究对象是群、环、域等代数体系. 有些代数体系的元素来自我们熟悉的复数集合, 更多的则不是. 作为抽象代数的第 1 章, 我们从数环和数域 (即元素是复数的环和域) 这些具体的代数体系开始讨论.

本章的重点是介绍数域的扩张理论. 在交代了数环和数域等基本概念的定义之后, 我们首先引入代数元素和单纯扩域等概念, 然后研究代数扩域、分裂域的理论, 最后引入分裂域的 Galois 群的概念. 这样, 就可以说是在复数集合这一相对熟悉的具体的环境下, 把域扩张理论演习了一遍. 因为遇到的数学对象是数, 是读者相对熟悉的, 不同的只是讨论问题的角度, 所以读者不会感到抽象和难以理解. 在这里, 一个重要的事情是引出了群. 随之也就揭示了研究群的必要. 读者会感到后面的内容不是无的放矢的. 从第 2 章开始, 将遵循公理化的方法, 讨论群、环、域的有关理论. 那时, 我们面对的将不限于元素是复数的代数体系.

需要指出的是, 本章自始至终都要假设代数基本定理成立. 即承认正次数复系数多项式至少有一个复根, 并承认由此引申出的 n 次多项式有总共 n 个根的结论.

本章讨论了包括三等分角在内的平面几何不可作图的问题. 这是数学系学生应该了解的问题. 我们希望, 读者通过学习, 能够理解处理这些问题的独特的代数方法.

1.1　数环与数域

在高等代数里我们学过数域的概念.

定义 1.1.1　*一个由复数组成的集合 F, 如果其中至少包含两个复数, 并且对于加、减、乘、除四种运算封闭 (作除法时除数不为 0), 就称 F 为一个数域.*

按这个定义, 全体复数组成的集合 $\mathbb{C}$, 全体实数组成的集合 $\mathbb{R}$, 全体有理数组成的集合 $\mathbb{Q}$ 都是数域. 除此之外, 我们还知道下面的集合

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$$

也成为一个数域. 不难看出, 若把 2 改成任意素数 p, 则 $\mathbb{Q}(\sqrt{p})$ 也是数域.

设 F 为一个数域, 并且设 $a \neq b \in F$, 则 a, b 中有一个不为 0. 不妨设 $a \neq 0$. 于是 $a/a = 1 \in F$. 进一步, $1 + 1 = 2, 2 + 1 = 3, \cdots$, 等也在 F 内, 即全体正整数在 F 内. 由于 F 对减法封闭, 所以全体负整数和 0 也在 F 内. 由于 F 对除法封闭, 所以一切有理数都在 F 内. 于是我们知道 F 包含 $\mathbb{Q}$. 在这个意义上, $\mathbb{Q}$ 是最小的数域.

熟知数域满足下边的运算律. 设 F 为任一数域, 则下列各款成立:

加法　A1) 结合律: 对任意 $a, b, c \in F$, 有 $(a + b) + c = a + (b + c)$;

A2) 交换律: 对任意 $a, b \in F$, 有 $a + b = b + a$;

A3) 有零元素 0, 对于一切 $a \in F$, $0+a=a$;

A4) 对 F 中任意元素 a, 有 $b \in F$, 使 $a+b=0$.

乘法 M1) 结合律: 对任意 $a,b,c \in F$, 有 $(ab)c=a(bc)$;

M2) 交换律: 对任意 $a,b \in F$, 有 $ab=ba$;

M3) 有单位元素 1, 对于一切 $a \in F$, $1 \cdot a=a$;

M4) 非零元素有倒数, 即若 $a \in F$, $a \neq 0$, 则有 $b \in F$, 使 $ab=1$.

加乘分配律 D) 等式 $a(b+c)=ab+ac$, 对一切 $a,b,c \in F$ 成立.

在上面九条运算律中, A1), A2), M1), M2) 和 D) 是任何复数运算所遵循的规律. 而 A3), A4), M3), M4) 是 F 作为数域所必须满足的. 设 F 为数域, 因为对减法封闭, 所以 $0 \in F$, 即 A3) 成立. 同样因为对减法封闭, 所以每个元素 $a \in F$ 都有其负元素 $-a \in F$, 即 A4) 成立. 数域 F 对除法封闭导致 M3), M4) 在其中成立.

反过来, 若一个复数组成的集合 F 至少包含两个复数, 并且对加法和乘法封闭, 那么在 F 内 A1)-A2), M1)-M2) 和 D) 自然成立. 如果 F 还满足 A3)-A4) 和 M3)-M4), 那么它一定是一个数域 (这一点留作习题). 借助上面的运算律我们建立了一般的域的概念.

定义 1.1.2 *设 F 是至少包含两个元素的集合, 设在 F 中定义了加法和乘法两种运算. 如果运算律 A1)-A4), M1)-M4) 和 D) 成立, 则 F 称为一个域.*

由这个定义看出, 数域也是域. 它们是包含在复数集合里的域, 而且它们作为域的运算就是通常复数的加法和乘法运算. 在一般情况下, 域 F 中的元素不一定是数, 因而它与数字 0,1 可能毫无联系. 此时我们把 A3) 理解成: 在 F 内有一个元素, 它加上任何元素 a 都等于元素 a 本身. 我们把它称为 *零元素* 并借用数字 0 作为它的符号. 对 M3) 也同样理解, 那里借用 "1" 作为 *单位元素* 的符号. 对一般的域, A4) 中的 b 称为 a 的 *负元素*, M4) 中的 b 称为 a 的 *逆元素*.

例 1.1.1 设 F 是一个二元集, 它的两个元素分别用 0,1 表示. 在 F 中按下面的规则可进行加法和乘法运算:

$$0+0=1+1=0, \quad 0+1=1+0=1;$$

$$0 \cdot 0=0 \cdot 1=1 \cdot 0=0, \quad 1 \cdot 1=1,$$

则 F 是一个域 (请读者自行验证). 它称为二元域, 是包含元素个数最少的域.

例 1.1.2 设 p 是一个素数. 对于 $i, 0 \leqslant i<p$, 用 $\overline{i}$ 表示被 p 除余数为 i 的那些整数组成的集合, 这种集合称为模 p 的同余类. 于是整数集合可以表示成所有同余类 $\overline{0}, \overline{1}, \cdots, \overline{p-1}$ 的无交并. 把集合 $\{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$ 记做 F. 在 F 内我们规定加法和乘法两种运算:

$$\overline{i}+\overline{j}=\overline{k}, \quad \overline{i} \cdot \overline{j}=\overline{l},$$

这里 $0 \leqslant i,j,k,l<p$, 而 $i+j \equiv k \pmod{p}$, $i \cdot j \equiv l \pmod{p}$ (需要注意, 虽然在条件 $i \cdot j \equiv l \pmod{p}$ 成立时, 我们规定 $\overline{i} \cdot \overline{j}=\overline{l}$, 但这不意味着 $\overline{l}$ 中任何元素都可以表示成 $\overline{i}$ 中一个元

素和 $\overline{j}$ 中一个元素的乘积. 例如, 在 $p=5$ 时, 虽然 $\overline{2}$ 中任何整数和 $\overline{3}$ 中任何整数的乘积都在 $\overline{1}$ 内, 但这个积不会是 1, 尽管 1 是 $\overline{1}$ 中元素). 此时 F 为一个域, 其中 $\overline{0}$ 为零元素,$\overline{1}$ 为单位元素. 要证明这一点只要验证定义 1.1.2 中各款就行了. 这里我们只验证 M4), 其余的留给读者. 设 $\overline{i}\neq\overline{0}$, 则 i 与 p 互素, 于是有整数 u,v 使得 $ui+vp=1$ 成立. 这里我们还可要求 $u<p$. 于是 $\overline{u}\cdot\overline{i}=\overline{1}$. 这意味着 $\overline{u}$ 是 $\overline{i}$ 的逆元素. M4) 成立.

例 1.1.3 设 F 为一个数域, x 为未定元. 于是我们有多项式环 $F[x]$.

形如

$$\frac{f(x)}{g(x)}$$

的表达式称为 F 上的 **有理分式**, 其中 $f(x),g(x)$ 为 $F[x]$ 中的多项式并且 $g(x)$ 不是零多项式. 两个有理分式 $\frac{f_1(x)}{g_1(x)}$ 和 $\frac{f_2(x)}{g_2(x)}$ 称为相等的, 如果 $f_1(x)g_2(x)=f_2(x)g_1(x)$. 特别地, $\frac{f(x)}{g(x)}=0$ 当且仅当 $f(x)$ 是零多项式. 也把 $\frac{f(x)}{1}$ 写做 $f(x)$. 于是多项式也可视为有理分式. 另外, 作为零次多项式, F 中的元素也是有理分式.

把 F 上的全体有理分式组成的集合记做 $F(x)$. 在 $F(x)$ 内按下面的方法做加法和乘法:

$$\frac{f_1(x)}{g_1(x)}+\frac{f_2(x)}{g_2(x)}=\frac{f_1(x)g_2(x)+f_2(x)g_1(x)}{g_1(x)g_2(x)};$$

$$\frac{f_1(x)}{g_1(x)}\times\frac{f_2(x)}{g_2(x)}=\frac{f_1(x)f_2(x)}{g_1(x)g_2(x)},$$

则 $F(x)$ 满足运算律 A1)-A4), M1)-M3) 和 D), F 中的 0 和 1 分别是 A3) 中的零元素和 M3) 中的单位元. 在 $F(x)$ 内元素 $\frac{f(x)}{g(x)}$ 不为 0 当且仅当 $f(x)$ 不为零多项式. 此时 $\frac{g(x)}{f(x)}$ 也是有理分式, 而且 $\frac{f(x)}{g(x)}\times\frac{g(x)}{f(x)}=1$. 这说明在 $F(x)$ 内 M4) 也成立. 因此 $F(x)$ 为一个域, 称为**有理分式域**.

数域是一个代数体系. 与数域有密切联系的代数体系是数环.

定义 1.1.3 *一个由复数组成的非空集合 R, 如果对加法、减法、乘法封闭, 则 R 称为一个数环.*

下面来看一些例子:

例 1.1.4 只由数字 0 组成的集合 $\{0\}$ 是一个数环.

例 1.1.5 全体整数组成的集合 $\mathbb{Z}$ 是一个数环, 称为整数环.

例 1.1.6 全体偶数组成的集合（记做 $2\mathbb{Z}$）是一个数环. 同样, $3\mathbb{Z}$, $4\mathbb{Z}$ 等都是数环.

这些例子说明, 整数环不是最小的数环.

例 1.1.7 用 i 表示虚数单位, 即 $\mathrm{i}=\sqrt{-1}$. 考虑集合

$$\mathbb{Z}[\mathrm{i}]=\{a+b\mathrm{i}|a,b\in\mathbb{Z}\},$$

于是 $\mathbb{Z}[i]$ 由实部是整数而虚部是 i 的整数倍的复数组成. 这种数称为 Gauss 整数. 容易证明 $\mathbb{Z}[i]$ 是一个数环, 称为 Gauss 整数环.

例 1.1.8 取定一个素数 p, 令

$$R=\left\{\frac{a}{p^i}|a\in\mathbb{Z},i=0,1,2,\cdots\right\},$$

则 R 为 $\mathbb{Q}$ 的子集合, R 中元素写成分数 $\frac{a}{b},a,b\in\mathbb{Z},(a,b)=1$ 时, 分母 b 是素数 p 的方幂. 不难验证 R 是一个数环.

例 1.1.9 取定素数 p, 令

$$R=\left\{\frac{a}{b}|a,b\in\mathbb{Z},(p,b)=1\right\},$$

则 $R\subseteq\mathbb{Q}$. 容易验证 R 也是数环.

根据定义 1.1.3, 数环是 $\mathbb{C}$ 的一个非空集合, 它满足运算律 A1)-A4), M1)-M2) 和 D). 反过来一个由数组成的非空集合 R, 如果它对加法和乘法封闭, 并且 A3) 和 A4) 成立, 则 R 是一个数环. 和域的情形一样, 我们有一般的环的概念.

定义 1.1.4 *设 R 是一个非空集合, 在其中定义了加法和乘法, 并且满足 A1)-A4), M1) 和 D), 则 R 称为一个环. 如果环 R 还满足 M2), 则 R 称为交换环. 如果环 R 还满足 M3), 则 R 称为有单位元素的环.*

于是, 由上述定义所给出的环, 不一定满足乘法交换律 M2), 也不一定有单位元, 即不一定满足 M3).

作为一般的环的例子, 我们举出域上的一元多项式环 $F[x]$ 和下面的全矩阵环.

例 1.1.10 设 F 是一个数域, n 为一个大于 1 的整数. 把 F 上的全体 $n\times n$ 矩阵组成的集合记做 $\boldsymbol{M}_n(F)$. 根据线性代数的理论, $\boldsymbol{M}_n(F)$ 在矩阵的加法和乘法下成为一个环. 称为全矩阵环.

在 $\boldsymbol{M}_n(F)$ 里乘法交换律不成立. 但单位矩阵是 $\boldsymbol{M}_n(F)$ 的单位元, 即 M3) 成立. 而 M4) 不成立.

定义 1.1.5 *设 R_1 是一个环, R_2 是 R_1 的非空子集合. 如果对于 R_1 的加法和乘法两种运算, R_2 也成为一个环, 则称 R_2 为 R_1 的子环, R_1 称为 R_2 的扩环. 此时, 若 R_2 还是域, 就称之为 R_1 的子域, R_1 为域时, R_1 称为 R_2 的扩域.*

于是, 当 R_1,R_2 都是数环时, 只要 $R_2\subseteq R_1$ 成立, R_2 就是 R_1 的子环.

设 R_1,R_2 都是某个 R 的子环, 则它们的集合交 $R_1\bigcap R_2$ 也是一个环. 若 R_1, R_2 都是域, 则 $R_1\bigcap R_2$ 也是一个域. 同样, 任意多个子环 (子域) 的交仍是子环 (子域).

今设 R 为一个数环, S 为一个复数集合, 则存在包含 R 又包含 S 的数环, 即 R 的包含 S 的扩环. 所有这些扩环的交也是 R 的一个包含 S 的扩环, 称为在 R 上添加 S 所得的扩环,

记做 $R[S]$. 若 R 为一个数域, 所有包含 S 的 R 的扩域的交也是一个数域, 称为 R 上添加 S 所得的数域, 记做 $R(S)$.

考虑 S 为有限集合 $\{s_1,\cdots,s_t\}$ 的情形, 此时 $R[S]$ 也记做 $R[s_1,\cdots,s_t]$. 因为 $R[S]$ 为环, 所以在它包含 S 中元素的同时, 还要包含这些元素的方幂, 以及 S 中元素 $s_1, s_2, \cdots, s_t$ 所构成的单项式 $as_1^{n_1}s_2^{n_2}\cdots s_t^{n_t}$, 这里 $a\in R$, 而 $n_1,\cdots,n_t$ 为非负整数, 进而包含 $s_1,\cdots,s_t$ 的以 R 中元素为系数的 "多项式" $f(s_1,s_2,\cdots,s_t)$. 反过来, 所有这类多项式对加法封闭, 对乘法封闭, 因而构成一个数环. 显然它是包含 R 和 S 的数环而且是一切包含 R 和 S 的数环的子环. 所以所有这些多项式组成了数环 $R[S]$. 容易看出, $R[S]$ 可以通过在 R 上逐步添加 $s_1,s_2,\cdots,s_t$ 而得到, 并且与添加的顺序无关. 例如 $R[s_1,s_2]=R[s_1][s_2]=R[s_2][s_1]$. 同样, 当 R 为一个数域且 S 为有限集合 $\{s_1,\cdots,s_t\}$ 时, $R(S)$ 也记做 $R(s_1,\cdots,s_t)$.

说明 这里 "多项式" 一词的用法与我们通常的用法有所不同. 通常, x_1, x_2, $\cdots$, x_n 为不定元, $R[x_1,\cdots,x_t]$ 中多项式是由 $x_1,\cdots,x_t$ 和 R 中元素构成的形式表达式

$$\sum a_{n_1n_2\cdots n_t}x_1^{n_1}\cdots x_t^{n_t},$$

其中作为指数的 $n_1,n_2,\cdots,n_t$ 为非负整数. 在 $R[x_1,\cdots,x_t]$ 中形式上不同的表达式是不相同的多项式. 而我们上面的 "多项式" 中 $s_1,\cdots,s_t$ 为复数, 可能形式上不同的两个表达式 $\sum a_{n_1n_2\cdots n_t}s_1^{n_1}\cdots s_t^{n_t}$ 和 $\sum b_{n_1n_2\cdots n_t}s_1^{n_1}\cdots s_t^{n_t}$ 给出同一个复数. 以后在上述两种情况下, 我们都使用多项式这个词.

再设 R 为一个数环, 但 $R\neq\{0\}$. 定义集合

$$F=\left\{\frac{a}{b}|a,b\in R,b\neq 0\right\},$$

即 F 为由分子、分母都来自 R 的分数 (分母不为 0) 组成. 容易验证 F 是数域, 并且是包含 R 的最小的数域, 它称为 R 的 **分式域**. 常常见到这样的情况: R_1,R_2 是两个不同的数环, 但它们拥有相同的分式域, 例如, 包含在有理数域内的任意数环 R, 只要 $R\neq\{0\}$, 都以有理数域为分式域.

在本节最后建立环 (以及域) 的同构和自同构的概念.

定义 1.1.6 设 R_1,R_2 都是环, 如果有一个由 R_1 到 R_2 的双射 σ 使

$$\begin{aligned}\sigma(a+b)&=\sigma(a)+\sigma(b),\\ \sigma(a\cdot b)&=\sigma(a)\cdot\sigma(b)\end{aligned}$$

对一切 $a,b\in R$ 成立, 则称 σ 为 R_1 到 R_2 的同构映射. 若环 R_1 到 R_2 有同构映射, 则 R_1,R_2 称为同构的. 环 R 到自身的同构映射称为自同构.

若定义中的 R_1,R_2 本身还是域, 则把 σ 称为域 R_1 到 R_2 的同构.

例 1.1.11 复数域 $\mathbb{C}$ 的共轭映射

$$\sigma: a+b\mathrm{i}\to a-b\mathrm{i}$$

是 $\mathbb{C}$ 的自同构.

例 1.1.12 令

$$R_1 = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} | a, b, c \in \mathbb{Q}\},$$

$$R_2 = \mathbb{Q}(\sqrt[3]{2}\omega) = \{a + b\sqrt[3]{2}\omega + c\sqrt[3]{4}\omega^2 | a, b, c \in \mathbb{Q}\},$$

其中 $\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$, 则 R_1, R_2 都是数域. 映射 $\sigma : a + b\sqrt[3]{2} + c\sqrt[3]{4} \to a + b\sqrt[3]{2}\omega + c\sqrt[3]{4}\omega^2$ 是 R_1 到 R_2 的同构映射. 注意这里 R_1 作为集合而言是实数域的子集合, 而 R_2 中既有实数也有非实的复数.

例 1.1.13 对于上面的 ω, 令

$$R = \mathbb{Q}(\omega) = \{a + b\omega + c\omega^2 | a, b, c \in \mathbb{Q}\},$$

则 R 为一个数域,

$$\sigma : \omega \to \omega^2$$

是 R 的一个自同构.

因为 $\omega = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$, 所以 $\omega^2 = -\frac{1}{2} - \frac{\sqrt{-3}}{2}$, 所以

$$a + b\omega + c\omega^2 = a - \frac{b+c}{2} + \frac{b-c}{2}\sqrt{-3},$$

因此 R 由形如 $a + b\sqrt{-3}, a, b \in \mathbb{Q}$ 的复数组成. R 可以表示成

$$\mathbb{Q}(\sqrt{-3}) = \{a + b\sqrt{-3} | a, b \in \mathbb{Q}\},$$

此时 σ 对一切有理数不变, 而把 $\sqrt{-3}$ 变成 $-\sqrt{-3}$, 它实际上是例 1.1.11 中的共轭映射在 $\mathbb{Q}(\sqrt{-3})$ 上的限制.

环与环同构是环之间的一种关系, 这种关系具有反身性、对称性和传递性, 同构的环或域在代数上认为是一样的.

设 σ 为数环的同构, 则 $\sigma(0) = 0, \sigma(-a) = -\sigma(a)$. 如果 $1 \in R$, 则 $\sigma(1) = 1$. 如果 σ 是数域 F_1 到 F_2 的同构, 那么由 $\sigma(1) = 1$, 进一步推出 $\sigma(2) = 2, \sigma(3) = 3, \cdots$. 对一切整数 n (也可能是负整数) 均有 $\sigma(n) = n$, 进而对任意有理数 a, $\sigma(a) = a$.

定义 1.1.7 *设 K_1 和 K_2 都是数域 F 的扩域. 若 $\phi : K_1 \to K_2$ 为 K_1 到 K_2 的同构 (即同构映射, 以下常把同构映射简称同构), 并且对一切 $a \in F$ 有 $\phi(a) = a$, 则称 ϕ 为 K_1 到 K_2 的 F-同构, 或关于 F 的相对同构. 当 $K_1 = K_2$ 时, 则 ϕ 称为 K_1 的 F-自同构或关于 F 的相对自同构.*

我们还常常使用由数域 K 到数域 L 内的 F-同构的说法, 这是指从 K 到 L 内的一个单射 ϕ, 它对一切 $a, b \in K$, 满足

$$\phi(a + b) = \phi(a) + \phi(b), \quad \phi(a \cdot b) = \phi(a) \cdot \phi(b),$$

并且对一切 $a \in F$ 有 $\phi(a) = a$, 这里 F 是 K 和 L 的共同子域. 显然此时 K 的像 $\phi(K)$ 是 L 的子域, 而 ϕ 实际上是 K 到 L 的子域 $\phi(K)$ 的 F-同构.

1.2 域的单纯扩张

以下各节中, 我们讨论数域的理论.

设 F 为一个数域, S 为有限集合, 考虑扩域 $F(S)$ 的结构. 为此我们从 $S = \{c\}$ 为单独一个元素的情形开始, 此时 $F(c)$ 称为 单纯扩张.

先建立一个概念.

定义 1.2.1 设 F 为数域, c 为复数. 如果 c 是一个系数在 F 内的非零多项式的零点(或根), 则 c 称为 F 上的代数元素. 如果 c 不是任何一个系数在 F 内的非零多项式的零点(或根), 则 c 称为 F 上的超越元素. 一个复数 c, 如果它在有理数域上是代数元素, 则称为代数数, 否则称为超越数.

于是 $\sqrt{2}, \sqrt[3]{3}, \mathrm{i}, \omega\left(=-\frac{1}{2}+\frac{\sqrt{-3}}{2}\right)$ 等都是代数数, 它们分别是有理数域上的多项式 $x^2-2, x^3-3, x^2+1, x^2+x+1$ 的零点. 最著名的超越数有 e, π 等. 要证明它们是超越数不是一件容易的事情, 我们将证明省略. 注意, F 内的任何元素 a 都是 F 上的代数元素, 因为它是多项式 $x-a$ 的零点.

按照 c 是 F 上的代数元素还是超越元素, 单纯扩张 $F(c)$ 有代数扩张和超越扩张两种情形.

1.2.1 单纯代数扩张

先设 c 为 F 上的代数元素, 此时 $F(c)$ 称为 单纯代数扩张. 因为当 c 为 $f(x)$ 的零点时, c 也是 $f(x)$ 的一切倍式的零点, 所以以 c 为零点的 F 上的非零多项式不只一个. 在所有这些多项式中, 有一个次数最低的、首项系数为 1 的多项式, 它称为 c 在 F 上的 最小多项式. 于是若 c 在 F 上的最小多项式就是 $f(x)$, 则以下三个事实成立:

(1) $f(x)$ 是被 c 唯一确定的;

(2) $f(x)$ 为 $F[x]$ 中的不可约多项式;

(3) 若 $g(x) \in F[x]$ 以 c 为零点, 则 $g(x)$ 是 $f(x)$ 的倍式.

这些事实的证明都很容易, 我们留给读者.

设 c 在 F 上的最小多项式

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

为 n 次的, 其中 $a_i \in F$. 我们先来考查扩环 $F[c]$ 的结构.

$F[c]$ 中的每个元素 u 都可以表示成 c 的多项式. 换句话说, 有 $F[x]$ 中的多项式 $g(x)$, 使 $u = g(c)$. 按照带余除法, 有 $q(x), r(x) \in F[x]$, 使

$$g(x) = q(x)f(x) + r(x),$$

其中 $r(x) = 0$ 或 $r(x)$ 非零但次数低于 n. 把 c 代入上式得

$$g(c) = q(c)f(c) + r(c) = r(c).$$

所以 $F[c]$ 中一切元素都可以表示成

$$r(c) = b_0 + b_1c + b_2c^2 + \cdots + b_{n-1}c^{n-1}$$

的形状, 其中 $b_0, b_1, \cdots, b_{n-1} \in F$. 容易看出这里多项式 $r(x)$ 由 u 唯一确定 (证明请读者给出). 反过来, 对于 $F[x]$ 中的每个次数小于 n 的多项式 $g(x)$(包括零多项式), $g(c)$ 是 $F[c]$ 中的元素. 因此如果我们把零多项式也看成是次数小于 n 的多项式, 则映射 $g(x) \to g(c)$ 是集合

$$\{g(x) | g(x) \in F[x], \deg g(x) < n\}$$

到集合 $F[c]$ 的双射.

当把 $F(c)$ 中元素表示成 $g(c), \deg g(x) < n$ 的形状时, 它们的运算按怎样的规则进行呢? 设 $u_1 = g_1(c), u_2 = g_2(c)$, 其中 $g_1(x), g_2(x)$ 都是 $F[x]$ 中次数小于 n 的多项式. 那么明显地, 和 $u_1 + u_2 = g_3(c)$, 这里 $g_3(x) = g_1(x) + g_2(x)$ 是次数小于 n 的多项式. 再来看积 u_1u_2, 此时应有 $u_1u_2 = g_1(c)g_2(c)$. 但多项式 $g_1(x)g_2(x)$ 的次数可能大于 n. 用 $f(x)$ 做除式去除 $g_1(x)g_2(x)$, 得 $g_1(x)g_2(x) = q(x)f(x) + g_4(x)$, 这里余式 $g_4(x)$ 为零或是次数小于 n 的多项式. 于是有 $u_1u_2 = g_4(c)$.

下面我们断言, $F[c]$ 还是一个数域, 因而有 $F[c] = F(c)$. 明显地, $F[c]$ 有单位元 1, 即满足运算律 M3), 我们再证它满足 M4). 实际上, 若有一个元素 $u = g(c) \neq 0$, 而

$$g(c) = d_0 + d_1c + \cdots + d_{n-1}c^{n-1},$$

其中各系数 $d_i \in F$. 令 $g(x) = d_0 + d_1x + \cdots + d_{n-1}x^{n-1}$, 则 $g(x) \in F[x]$ 为次数 $< n$ 的非零多项式. 它显然与不可约多项式 $f(x)$ 互素. 于是有多项式 $a(x), b(x) \in F[x]$, 使得

$$a(x)g(x) + b(x)f(x) = 1$$

成立. 因为 $f(c) = 0$, 把上式中的 x 换成 c, 得 $a(c)g(c) = 1$, 这说明 $a(c) \in F[c]$ 是 u 的倒数. 于是在 $F[c]$ 中 M4) 成立, $F[c]$ 为数域. 断言 $F[c] = F(c)$ 成立. 当然, 满足条件 $a(x)g(x) + b(x)f(x) = 1$ 的多项式 $a(x), b(x)$ 是不唯一的. 但给出的倒数 $a(c)$ 是被 u 唯一确定的.

例 1.2.1 取复数

$$c = \cos\frac{2\pi}{5} + \mathrm{i}\sin\frac{2\pi}{5}.$$

不难看出, c 满足 $c^5 = 1$, 是 5 次单位根. 我们在单纯代数扩域 $F = \mathbb{Q}(c)$ 内考虑问题.

因为 $x^5-1=(x-1)(x^4+x^3+x^2+x+1)$, 而 $x^4+x^3+x^2+x+1$ 是 $\mathbb{Q}$ 上不可约多项式, 所以 c 的最小多项式为 $x^4+x^3+x^2+x+1$.

于是 F 由形如 $b_0+b_1c+b_2c^2+b_3c^3, b_i\in\mathbb{Q}$ 的复数组成, 并且 F 中每个元素只有一种方法表示成上述形状. 显然, 有 $c^4=-1-c-c^2-c^3, c^5=1, c^6=c$. 由这些等式, 再使用分配律可以计算任何两个元素的乘积. 现在设

$$u=1+c+c^3,\quad v=1+c+c^2,$$

求 uv 和 uv^{-1}. 容易算出

$$uv=1+2c+2c^2+2c^3+c^4+c^5=1+c+c^2+c^3.$$

再求 v^{-1}. 因为

$$1=(1+x+x^2)(1+x^3)-x(1+x+x^2+x^3+x^4),$$

所以, $v^{-1}=1+c^3$. 于是

$$uv^{-1}=(1+c+c^3)(1+c^3)=1+c+c^3+c^3+c^4+c^6$$

$$=1+2c+2c^3+c^4=c-c^2+c^3.$$

最后讨论单纯代数扩域的同构问题. 设 $F(c)$ 和 $F(d)$ 都是 F 上的单纯代数扩域, 这里 c,d 在 F 上的最小多项式分别为 $f(x)$ 和 $g(x)$. 设有一个 $F(c)$ 到 $F(d)$ 的 F-同构 σ, 并且 $\sigma: c\to d$. 因为 c 的最小多项式为 $f(x)$, 有 $f(c)=0$. 在上式两端用 σ 作用得到 $f(d)=0$. 这说明 $f(x)$ 是 $g(x)$ 的倍式. 同样我们知 $g(c)=0$, 因而 $g(x)$ 是 $f(x)$ 的倍式. 于是我们知 $f(x)=g(x)$. 就是说 c 和 d 有相同的最小多项式.

现在设 $F(c)$ 和 $F(d)$ 都是 F 上的单纯代数扩域, 并且 c 和 d 在 F 上有相同的最小多项式 $f(x)$, 其次数为 n. 根据前面的讨论, 知映射 $\sigma_1: g(x)\to g(c)$ 和 $\sigma_2: g(x)\to g(d)$ 分别是集合 $\{g(x)|g(x)\in F[x], \deg(g(x))<n\}$ 到 $F(c)$ 和 $F(d)$ 的双射. 这样一来, 映射 $\tau=\sigma_2\sigma_1^{-1}$ 把 $F(c)$ 中元素 $g(c)$(其中 $g(x)$ 的次数小于 n), 映成 $g(d)$, 它也是 $F(c)$ 到 $F(d)$ 的双射. 不难看出映射 τ 满足 $\tau(u+v)=\tau(u)+\tau(v)$ 其中 $u,v\in F(c)$. 而且, 如果 $\deg g_1(x), \deg g_2(x), \deg g_3(x)<n$ 并且 $g_1(x)g_2(x)\equiv g_3(x)\pmod{f(x)}$, 则同时有 $g_1(c)g_2(c)=g_3(c)$ 和 $g_1(d)g_2(d)=g_3(d)$. 由此立知 $\tau(uv)=\tau(u)\tau(v), u,v\in F(c)$. 因此 τ 是扩域 $F(c)$ 到扩域 $F(d)$ 的同构. 无论是 σ_1 还是 σ_2 都保持 F 中每个元素不变, 所以其乘积 τ 保持 F 中每个元素不变. 于是 τ 是一个 F-同构.

把上面的讨论略加引申, 得到定理:

定理 1.2.1 设 $f(x)$ 为 F 上的 n 次不可约多项式, $c=c_1,c_2,\cdots,c_n$ 为 $f(x)$ 在 $\mathbb{C}$ 内的根. 定义 $F(c)$ 到 $F(c_i)$ 内的映射

$$\tau_i: b_0+b_1c+\cdots+b_{n-1}c^{n-1}\to b_0+b_1c_i+\cdots+b_{n-1}c_i^{n-1},$$

其中 $b_0, b_1, \cdots, b_{n-1} \in F$, 则 $\tau_1, \tau_2, \cdots, \tau_n$ 是 $F(c)$ 到复数域内的全部 F-同构, 并且 $F(c_1)$, $F(c_2), \cdots, F(c_n)$ 是 F 上与 $F(c)$ 同构的全部单纯代数扩域.

注意, 有可能出现元素 $c_i \neq c_j$ 而数域 $F(c_i) = F(c_j)$ 的情况. 这种情况出现当且仅当 $c_i \in F(c_j)$, 或等价地, $c_j \in F(c_i)$. 此时虽然 $F(c)$ 在 τ_i 和 τ_j 下有相同的像, 但映射 τ_i, τ_j 本身是不同的. 特别地, 若有某个 $i, i \neq 1$, 而 $c_i \in F(c)$, 就出现 $F(c_1) = F(c_i)$ 的情况. 此时 τ_i 就成为 $F(c)$ 的自同构, 而 τ_1 是 $F(c)$ 的恒等自同构.

例 1.2.2 仍设 F 为例 1.2.1 中的代数扩张. 多项式 $1 + x + x^2 + x^3 + x^4$ 有四个根: c, c^2, c^3, c^4. 它们都是 $F = \mathbb{Q}[c]$ 中的元素. 所以上面定义的 τ_i 都是 F 的自同构. 例如

$$\begin{aligned} \tau_2 : b_0 + b_1 c + b_2 c^2 + b_3 c^3 &\to b_0 + b_1 c^2 + b_2 c^4 + b_3 c^6 \\ &= (b_0 - b_2) + (b_3 - b_2)c + (b_1 - b_2)c^2 - b_2 c^3. \end{aligned}$$

1.2.2 单纯超越扩张

下面再设 c 为 F 上的超越元素, 和上面一样, 对于 $F[x]$ 上的每个多项式 $f(x)$, $f(c) \in F[c]$. 设 $f(x), g(x) \in F[x]$ 是不相等的多项式, 那么 $f(c) \neq g(c)$. 否则 $h(x) = f(x) - g(x)$ 是非零多项式, 而 $h(c) = 0$, 与 c 为 F 上的超越元素的事实矛盾. 这样一来映射

$$\sigma : f(x) \to f(c)$$

是由 $F[x]$ 到 $F[c]$ 的一个单射. 和单纯代数扩张的情形一样这还是一个满射, 因而是双射. 即 $F[c]$ 与多项式环 $F[x]$ 之间可建立一一对应. 同样, 映射 σ 保持加法和乘法, 即

$$\sigma(f(x) + g(x)) = \sigma(f(x)) + \sigma(g(x)), \quad \sigma(f(x)g(x)) = \sigma(f(x))\sigma(g(x)).$$

所以 σ 是环 $F[x]$ 到数环 $F[c]$ 的同构.

数环 $F[c]$ 不是数域. 当 $f(x) \in F[x]$ 是次数大于 0 的多项式时, 不存在 $g(x) \in F[x]$ 使 $f(x)g(x) = 1$. 由此推知 $f(c)$ 在 $F[c]$ 内没有倒数. 此时数域 $F(c)$ 是数环 $F[c]$ 的分式域.

有理函数域 $F(x)$ 中每个元素都可表示成两个多项式的商. 借助映射 σ 可以定义 $F(x)$ 到 $F(c)$ 上的映射

$$\sigma : \frac{f(x)}{g(x)} \to \frac{f(c)}{g(c)}.$$

(注意这里有一个问题: σ 是否把相等的有理分式映成 $F(c)$ 中的同一复数? 当这点成立后, 我们才能说 σ 是 $F(x)$ 到 $F(c)$ 内的映射, 才能进一步谈论 σ 是否是满射和双射.) 不难看出这还是一个同构. 于是 $F(c)$ 与有理分式域同构. 我们有下面的定理:

定理 1.2.2 设 $F(c)$ 和 $F(d)$ 是 F 上的单纯超越扩域, 则有一个 $F(c)$ 到 $F(d)$ 的 F-同构 σ, 它把 c 映到 d. 因此, F 上的一切单纯超越扩域都是相互同构的.

F 上的任何单纯代数扩域和 F 上的任何一个单纯超越扩域都不是 F-同构的.