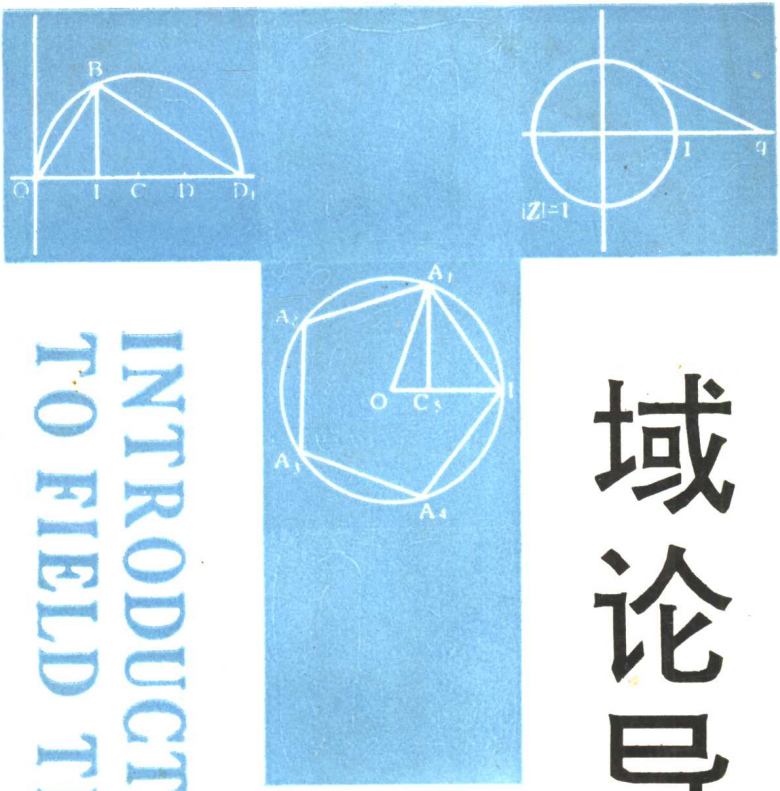

域论导引

INTRODUCTION TO FIELD THEORY

原著IAIN T.ADAMSON

张君达　胡先蕙 译

域 论 导 引

(INTRODUCTION TO FIELD THEORY)

亚当森
IAIN T. ADAMSON 原著

张君达 胡先蕙 译

北京师范学院出版社

京新登字208号

域论导引

(INTRODUCTION TO FIELD THEORY)

IAIN T. ADAMSON 原著

张君达 胡先蕙 译

北京师范学院出版社出版发行

(北京阜成门外花园村)

全国新华书店经销

三河科教印刷厂印刷

1992年1月北京第一版 1992年1月北京第一次印刷

开本:787×1092 1/32 印张:5.5 字数:116千

ISBN7-81014-573-8/O·9

印数:0,001—1500 定价:4.40元

前　言

域论是代数学的一个重要分支，我国各大学数学系都作为“近世代数”的后继课开设，迄今尚无一本适用教材。英国剑桥大学出版社出版的“域论导引”(Introduction to Field Theory)是Iain T. Adamson根据其多年的教学经验写成的一本内容恰当而且能深入浅出的教材，不仅适用于我国大学的教学，而且对广大中学教师也有重要的参考价值。张君达和胡先蕙两位同志的译稿，忠实于原著，不仅正确地表达了原文意义，而且译文流畅，我在北京师大讲授“域论”时曾以此译稿作为主要参考书，一学期每周四学时恰好能讲完全部内容，学生不仅巩固了近世代数课所学内容，而且为今后学习其它分支如代数数论，环论提供必需的基础知识，本书能够出版，是数学教育界的一大好事。

吴品三

1990年12月28日

序

在近世代数的现代潮流中，域论常常被忽视，近来出版的代数教科书，大多数是关于群论或向量空间的，但域论是代数中最富有吸引力的一个分支，有很多引人注目的应用．它的中心结果是Galois基本定理，这是一个按照任何标准来说都堪称是真正“重要”的数学定理．本书的目的旨在引导读者从基本定义的简述到重要结果的产生中领会抽象代数的精神实质及其某些处理技巧．本书予先只假定读者具有一点群论的基础知识，并诚望读者能准确地记忆各种定义以便能进行严密论证．

第一章从头开始介绍关于环、域和向量空间的基本性质．第二章叙述域的扩张以及关于域的各种分类方法．在第三章中，我们阐明有限次正规可离扩域的Galois理论，基本上采用Artin方法．第四章提供Galois理论的各种应用，包括有限个元素的所有域的分类，圆规直尺作图以及证明次数大于4的一般多项式不可能有根号解．

我很幸运地请到我的同事Hamish Anderson博士阅读本书的初稿．由于他的仔细阅读和深刻的评论，使本书的很多瑕疵得以改正．我深深地感谢他的宝贵帮助。在着手出版本书时，我还得到Joan Aldous博士、William

Blacburn先生和Brian Kennedy先生的帮助，这里表示深切的谢意.我由衷地感谢D.E.Rutherford教授，由于他关于群论的讲授，第一次引起我对于代数的兴趣，同时在本书的全部编写过程中，他给予了不断的鼓励与帮助.最后，我还要感谢贝尔法斯特的女王大学及邓迪女王学院的几届优等生，她们细心地聆听了最终成为本书的连续讲授，并提出了意见．特别是她们中的一人主动热情地给我提供第四章的一个恰当的结尾．

IAIN T. ADAMSON

1964年8月于DUNDEE

目　录

第一章 基本概念

§1 环和域

以域论作为它的一个组成部分的近世代数，可以粗略地认为是研究带有合成法的集合的一个数学分支．为了进行详细阐述，我们作以下定义：集合E上的一个合成法是一种运算，它使得集合E中元素的任一有序对(a, b)与E中的一个确定的元素对应，这个元素可以表示为$a+b$，此时把它叫做a与b的和．这种运算叫做加法．或者可以表示为$a\times b$或$a\cdot b$，或简记作ab，此时把它叫做a与b的积，这种运算叫做乘法．显然，实数集R上普通的加法和乘法运算就是实数集R上的合成法．

当希望对合成法作一般性讨论时，我们采用“中性”记号，例如用$a\circ b$来表示对有序对(a, b)作用合成法所得到的结果。采用这个记号，我们作几个进一步的定义．集合E上的一个合成法叫做可结合的，如果对于E的任意三个元a、b、c，都有$a\circ(b\circ c)=(a\circ b)\circ c$．一个合成法叫做可交换的，如果对于$E$的任意两个元$a$、$b$，都有$a\circ b=b\circ a$．如果对于$E$中取定的两个元$c$、$d$，有$c\circ d=d\circ c$，则只说$c$和$d$是可换的．$E$的一个元$n$称为合成法的恒等元，如果对于$E$的每一元$a$都有$n\circ a=a=a\circ n$．这里，若采用的是加法记号，则恒等元也称为零元，而且通常用0来表示；若采用的是乘法记号，恒等元也称为单位元，通常用e或1来表示．如果a是E的一千

瓦n是E上合成法的一个恒等元；若E中的一个元a'满足$a\circ a'=n=a'\circ a$，则称它是a关于这个合成法的逆元．当采用的分别是加法或乘法记号时，就分别用$-a$或a^{-1}来代替a'．通常实数的加法和乘法既是可结合的，又是交可换的．实数0和1分别是加法和乘法的恒等元．每一个实数都有一个加法逆元．每一个非零实数都有一个乘法逆元．实数的加法和乘法还具有一个进一步的性质：对于任意三个实数a、b、c，都有

$$a(b+c)=ab+ac \text{ 和 } (b+c)a=ba+ca$$

此时称乘法对于加法是可分配的．

本书的读者需要适当熟悉群论的基础知识，正如任何一本实用的近世代数入门教材中所包含的内容．为此这里我们作一下简单地回顾．一个群是一个具有可结合的合成法的集合G且满足

（1）对于这个合成法，G中存在一个恒等元；

（2）对于这个合成法，G中的每一个元都有一个逆元．

某些作者在初等群论中所提到的封闭性，在这里无需另外陈述，因为它已蕴含在G上合成法的定义中，即对于G中的任意元素对，作用G上的合成法所得的结果仍是G中的一个元．如群的合成法是可交换的，则称这个群为阿贝耳群．

一个环是一个具有两种合成法的集合R，这两种法则分别称为加法和乘法，并满足下面的条件：

$A1$　加法是可结合的，即对R的任意三个元a、b、c，都有$a+(b+c)=(a+b)+c$．

$A2$　加法是可交换的，即对R的任意一对元a、b，都有$a+b=b+a$．

$A3$　对于加法存在一个恒等元，又叫零元，通常用0表

示，使得对R的每一个元a，都有　　$a+0=0+a$。

$A4$　R中的每一个元a都有一个加法逆元，通常用$-a$表示，使得$a+(-a)=0=(-a)+a$。

$M1$　乘法是可结合的，即对于R的任意三个元a、b、c，都有　$a(bc)=(ab)c$。

AM　乘法对于加法是可分配的，即对于R中的任意三个元a、b、c，都有

$$a(b+c)=ab+ac \quad \text{和} \quad (b+c)a=ba+ca$$

一个环称为交换环，如果除了上述环的确定性质外还满足条件：

$M2$　乘法是可交换的，即对于R中每一对元a、b，都有$ab=ba$。

一个环R称为是有单位元的环，如果它满足性质$A1$，$A2$，$A3$，$A4$，$M1$，AM，而且还满足条件：

$M3$　对于乘法存在一个恒等元e，又叫单位元，使得对R的每一个元a，都有$ea=a=ae$。

最后，一个有单位元的交换环称为一个域，如果它至少含有两个元，且满足所有上述的条件以及下面的条件：

$M4$　R中的任一非零元a，都有一个乘法逆元a^{-1}，使得$aa^{-1}=e=a^{-1}a$。

通常依据域F的元的个数是有限的或无限的，称它为有限域或无限域。

例1　环的最熟悉的例子是普通整数集（正整数、负整数和零），它具有通常的加法和乘法运算，我们用Z表示这个环。它是一个有单位元的交换环（显然数1是它的单位元），但它不是一个域——事实上，在Z里有乘法逆元的整数仅有1和-1。

例2 有理数集合、实数集合和复数集合对于通常的加法和乘法运算，容易验证满足所有域的条件，我们分别用Q，R和C来表示这些数域.

例3 如果R是任一环，n是任一正整数，则以R中$n\times n$矩阵为元素的集合对于通常的矩阵加法和乘法作成一个环，我们用$M_n(R)$表示. 环$M_n(R)$一般是不可交换的，如果R是有单位元的环，则它也是有单位元的环.

例4 设m是任一大于1的正整数，对于整数a、b，如果$a-b$能被m整除，则称a与b关于模m同余，记作$a\equiv b \pmod{m}$. 一个整数a关于模m的剩余类是关于模m与a同余的所有整数的集合. 显然，恰有m个不同的剩余类. 因为每一个整数关于模m同余于$0, 1, 2, \cdots, m-1$这m个整数中的一个，我们用Z_m表示整数模m的剩余类的集合. 我们定义适当的加法和乘法运算，使它成为一个环. 设C_1和C_2是任意两个剩余类，从C_1中任取一整数a_1，从C_2中任取一整数a_2，定义C_1+C_2和C_1C_2分别为a_1+a_2和a_1a_2所在的剩余类. 初看起来，似乎C_1+C_2和C_1C_2依赖于a_1和a_2的选取，但是可以证明事实并非如此. 其实，如果b_1、b_2分别是剩余类C_1，C_2里的整数，则有$a_1\equiv b_1 \pmod{m}$和$a_2\equiv b_2 \pmod{m}$；因此存在整数k_1、k_2使得$a_1=b_1+k_1m$和$a_2=b_2+k_2m$，从而$a_1+a_2=b_1+b_2+(k_1+k_2)m$和$a_1a_2=b_1b_2+(k_1b_2+k_2b_1+k_1k_2m)m$，所以有$a_1+a_2\equiv b_1+b_2 \pmod{m}$和$a_1a_2\equiv b_1b_2 \pmod{m}$. 于是$a_1+a_2$和$b_1+b_2$属于模$m$的同一剩余类，$a_1a_2$和$b_1b_2$也属于模$m$的同一剩余类. 因此$C_1+C_2$和$C_1C_2$的定义仅依赖于$C_1$和$C_2$，并不依赖于$C_1$、$C_2$中的代表元的选取.

容易验证，对于这两个合成法，Z_m是一个有单位元的交换环，零元O和单位元E分别是包含整数0和1的剩余类.

另外，含有a的剩余类的加法逆元是含有$-a$的剩余类。

我们说一个整数与m互素，如果它同m没有1和-1以外的公因子。显然，如果一个模m的剩余类C里的一个整数与m互素，则C里的所有整数都与m互素。在这种情况下，我们说C是一个与m互素的剩余类。设R_m是与m互素的剩余类的集合。我们来证明模m的一个剩余类在Z_m中有乘法逆元的充要条件是它属于R_m。

首先假定Z_m里的剩余类C有一个乘法逆元C'，则$CC'=E$。因此，如果a和a'分别是C和C'里的整数，就有$aa'\equiv 1(\mathrm{mod}\,m)$，于是存在一个整数$k$使得$aa'+km=1$。由此可见，如果$r$是$a$和$m$的一个公因子，则$r$是$aa'+km=1$的一个因子，因此$r$只能是1或$-1$。所以，若$C$在$Z_m$中有乘法逆元，则$C$属于$R_m$。顺便指出，因为$C'$在$Z_m$中也有逆元（$C$为$C'$的逆元），所以$C'$也属于$R_m$。

反之，假定C属于R_m，我们来证明C在Z_m中有一个乘法逆元。为了得到这个结果，从C里任选一个整数a，则a与m互素。现在考虑可以表为$xa+ym$这种形式的正整数集合，这里x、y是整数。这个集合显然是非空的，因此包含一个最小的正整数，不妨是$d=x_0a+y_0m$。用d去除a，可得整数q、r，使得$a=qd+r$，$0\leqslant r<d$，由此可推出

$$r=a-q(x_0a+y_0m)=(1-qx_0)a+(-qy_0)m.$$

如果r不是零，就与d是形如$xa+ym$的数中的最小正整数相矛盾。所以$r=0$，且d是a的因子。完全类似地可以证明d是m的因子，从而d是a和m的公因子，所以$d=1$。这就证明了存在整数x_0、y_0，使得$x_0a+y_0m=1$，所以$x_0a\equiv 1(\mathrm{mod}\,m)$。从而，如果$C'$是$x_0$关于模$m$所在的剩余类，就有$CC'=E$，即$C'$是$C$的逆元。

因为两个与m互素的整数的乘积仍然与m互素，因此R_m中两个剩余类的乘积仍然在R_m中．所以Z_m中的乘法在R_m上是可结合的．又单位同余类E属于R_m．上述讨论表明R_m中的每一个剩余类在R_m中都有乘法逆元，此即R_m对于Z_m的乘法运算作成一个阿贝耳群．

例5 设p是一个素数，按照例4所叙述的步骤，Z_p构成一个环．现在再证明Z_p是一个域．既然我们已证明了Z_p是一个有单位元的交换环，现在仅需确定它满足性质$M4$．然而，这一点立即可由例4的讨论中得到，因为每一个模p的非零剩余类都是与p互素的．

§2 基本性质

我们注意到环R中的元对于加法运算满足条件$A1$到$A4$，即构成一个阿贝耳群．这个群称为环R的加群，记作R^+．

容易证明R的零元0和R的每一元a的加法逆元$-a$是唯一的．首先，假定0和$0'$都是R的零元，则$0+0'=0$（因为$0'$是零元），并且$0+0'=0'$（因为0是零元），因此$0=0'$．其次假设$-a$和a'都是a的加法逆元，则有$(a'+a)+(-a)=0+(-a)=-a$（因为a'是一个逆元），并且$(a'+a)+(-a)=a'+(a+(-a))=a'+0=a'$（因为加法是可结合的，且$-a$是一个逆元），因此$a'=-a$．从而立即可得：对$R$的任一元$a$，有$-(-a)=a$，这是因为$a$和$-(-a)$两个元都是$-a$的加法逆元．

一个环中每一个元都存在加法逆元表明在环里减法总是可以进行的．对于一个元a减去另一个元b的问题可以转变为

寻找一个元x，使得$a = x + b$成立．显然$x = a + (-b)$满足要求，因为$(a + (-b)) + b = a + ((-b) + b) = a + 0 = a$．我们通常把$a + (-b)$简写成为$a - b$．因为环里的加法运算是可交换的，所以有$a - b = (-b) + a$．

虽然环的零元是由于其加法性质而被单独提出加以注意的，但是分配律AM使得它也具有我们熟悉的和实数0相联系的乘法性质．此即如果在一个乘积里有一个因子为零，则这个乘积是零．因此，设a是R的任一元，可以证明$a0 = 0$．因为0是加法的恒等元，因此有$0 + 0 = 0$，所以$a(0 + 0) = a0$．利用AM可推出$a0 + a0 = a0$，再由$A4$，$a0$有一个加法逆元$-(a0)$．上式两边加上$-(a0)$，就得到

$$-(a0) + (a0 + a0) = -(a0) + a0 = 0$$

在左边应用结合律$A1$，有$(-(a0) + a0) + a0 = 0$，从而$0 + a0 = 0$，即$a0 = 0$，此即所要证明的．类似地，可以证明对于R的每一个元a，$0a = 0$．进而可知，在域里零元0和单位元e是截然不同的，因为如果a是一个非零元，就有$a0 = 0$，但$ae = a$．

与此类似的论证可用来证明下面的结果：如果a和b是环R中任意两个元，那么

$$a(-b) = -(ab), (-a)b = -(ab) \text{和} (-a)(-b) = ab.$$

例如要证明第一个式子，注意到$b + (-b) = 0$，因此$a(b + (-b)) = a0$．这样，由AM和我们刚证过的式子，有$ab + a(-b) = 0$，所以$a(-b)$是ab的一个加法逆元．由于$-(ab)$是ab唯一的加法逆元，因此$a(-b) = -(ab)$．类似可证其余的结果．

我们曾指出：对于任一环R，如果它的元素的乘积里有一个因子是0，则乘积为0．一般，这一结论的逆命题不成

立．例如在复数域C上的二阶矩阵环$M_2(C)$中，就有

$$\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

然而，对于域来说这一逆命题永远成立．因为假设a和b是域F的元，且$ab=0$，可以证明或者$a=0$，或者$b=0$．换句话说，如果a是非零元，则$b=0$．因为如果a是非零元，则它有乘法逆元a^{-1}，用a^{-1}去乘上式，可得$a^{-1}(ab)=a^{-1}0$，所以由$M1$，有

$$b=eb=(a^{-1}a)b=a^{-1}(ab)=a^{-1}0=0$$

这个讨论表明，域的两个非零元的乘积是非零元．因此域里的乘法是非零元集合上的一个合成法，这样域F的非零元的集合对于乘法运算满足条件$M1$，$M2$，$M3$和$M4$，即作成一个阿贝耳群．我们称它为域F的乘群，用F^*表示．

类似于在加群里的论证方法，容易验证域F的单位元e和域F的非零元的乘法逆元是唯一的，并且对于域F的任一非零元a，有$(a^{-1})^{-1}=a$．

最后，在一个域F里(除去零元)，除法运算总是可以进行的．用一个非零元b去除一个元a，只须找到一个元x，使得$a=xb$，显然$x=ab^{-1}$满足要求．由于在域F中，乘法是可交换的，所以有$ab^{-1}=b^{-1}a$．我们经常用记号a/b代替ab^{-1}．

设F是一个域，现在定义一个运算，对每个整数n和F的每个元a，令F中的元na与之对应，并归纳地定义：

(i) $0a=0$；

(ii) $(k+1)a=ka+a$，对所有的整数$k\geqslant 0$；

(iii) $(-k)a=-(ka)$，对所有的整数$k>0$．

我们称na是a的整倍元．用数学归纳法可以证明：对所有的F中的元a、b和所有的整数m、n，有

$$(m+n)a=ma+na,\quad m(a+b)=ma+mb,$$

$$(mn)a=m(na),\quad (ma)(nb)=(mn)(ab).$$

现在考虑一个域F的单位元e的整倍元，特别考察使得$ne=0$的整数n的集合A，A称为e的零化子．存在如下的两种情形：

情形1　零化子只含单独一个整数0．这时我们称域F的特征为零．注意：如果n是一个非零整数且a是F的非零元，那么$na=n(ea)=(ne)(1a)$不为零．

情形2　零化子A至少含有一个非零整数．从而立即得A至少含有一个正整数．因为如果a属于A，那么$ae=0$，从而$(-a)e=-(ae)=0$，即有$-a$也属于A．并且如果a是非零的，则整数a和$-a$中有一个是正的．设p是A中的最小正整数，可以证明p是一个素数，且A恰由p的倍数组成．

首先，假设p不是素数，则p能分解为$p=ab$的形式，这里$1<a,b<p$，则有$0=pe=(ab)e=(ae)(be)$．从而不是$ae=0$，就是$be=0$，但这与p是A中选取的最小正整数相矛盾．

其次，显然p的所有倍数都属于A，因为对任一整数n，有$(np)e=n(pe)=n0=0$反之，假设k属于A，用p除k所得的商是q，余数是r，则有$k=qp+r$，且$0\leqslant r<p$，因此

$$0=ke=(qp+r)e=(qp)e+re=re$$

所以r属于A．如果r不为零，又与p是A中选取的最小正整数相矛盾．因此$r=0$，即k是p的倍数．

这种情形，我们称域F有特征p．注意：如果k是p的任