〔法〕Simon J.AGOU 著
肖国镇 周炜 忻鼎稼 译
忻鼎稼 肖国镇 校

有限域

河南科学技术出版社

有 限 域

[法] Simon J. AGOU 著
肖国镇 周 炜 忻鼎稼 译
忻鼎稼 肖国镇 校

河南科学技术出版社

内 容 提 要

本书致力于有限域上多项式的介绍，并对下列主题进行了深入的研究：不可约性，因式分解，置换，本原性，互反律，线性可分等．书中不少结果为第一次公布．此外，书中也可找到有关 Gauss 和、Jacobi 和及特征标等经典结果，而次正规概念则是作者提出的并正在发展的新课题．本书可供数学、信息论及密码学有关专业的高年级大学生、研究生和科研人员学习参考．

有 限 域

[法] Simon J. AGOU 著

肖国镇 周 炜 忻鼎稼 译

忻鼎稼 肖国镇 校

责任编辑 王广照

河南科学技术出版社出版

郑州市农业路 73 号

邮政编码：450002 电话：(0371) 5721450

河南郑州中华印刷厂印刷

全国新华书店发行

开本：850×1168 1/32 印张：6.25 字数：142 千字

1997 年 12 月第 1 版 1997 年 12 月第 1 次印刷

印数：1—1 000

ISBN 7-5349-2138-4/G·588 定价：9.80 元

前　言

本专著用简洁的形式给出一些精辟的结果，目的是使学生和研究人员得以接触源于他们研究领域的许多问题.

本专著的内容自成体系，读者不必过多地参阅其他著作即可方便地学习和使用.

本专著的部分内容源于作者 1985～1986 年在法国里昂第一大学为博士研究生所开设的“数论与多项式”教程.

本专著主要论述次正规性的概念，即在一个次正规多项式的分解中存在一个多项式，它的次数除尽每一个因式的次数. 由作者引人的这一观点是一个能被广泛拓广的新的研究领域.

在一般情况下，由次正规性的概念可导出在有限域 GF（p^s）上分解次正规多项式 $F\left(\sum_{i=0}^{m} a_i x^{p^{r_i}}\right)$ 的一个次数最低的不可约多项式，并证明了当 $m \geqslant 3$ 时，该次正规多项式不是不可约的，进而在 $m \geqslant 1$，2 的情况下给出不可约性的判别准则.

本专著中所设的一些较为困难的习题只给出技巧性的结果，作者希望读者能更加深人地钻研有关内容.

本专著的全部内容以清晰的表达方式给出所期望的结果，使得在计算机上实现这些算法成为可能.

感谢西安电子科技大学的肖国镇教授，他最先倡导在中国出版此专著，他为本专著在河南科学技术出版社的出版做了大量的组织工作，包括主持了繁重的翻译和校阅任务.

感谢上海复旦大学的忻鼎稼教授，他为本专著的出版付出了辛勤的劳动.

我还感谢 Jouin 夫人，她承担了英文原稿的打印工作，这是最后完成本专著的重要一环.

Simon J. AGOU

译 者 序

本书作者，法国里昂大学及梅茵大学教授 Simon J. AGOU，是法国著名数学家，他在离散数学、数论以及计算机科学方面均有杰出的成就. 更为难能可贵的是，近年来他为中法两国科学家的学术交流做了大量的工作. 在他的不懈努力下，1994 年法国外交部与中国国家科委拟定了一项中法关于离散数学与计算机科学领域的交流计划（属于中法科技合作与交流混合委员会的合作项目之一）. 中国方面的组织者是复旦大学忻鼎稼教授，参加此项目者有中国科学院系统科学研究所（吴文俊教授）及西安电子科技大学信息保密研究所（肖国镇教授），本书的出版即为此项交流计划的一部分. AGOU 教授把本书的中文出版权无偿地转让给河南科学技术出版社，我们以能为本书的翻译工作出点力而感到十分荣幸. 参加本书翻译工作的还有博士生朱华飞、温巧燕和张建中.

我们愿以此书奉献给从事信息科学、计算机科学、离散数学、统计数学、密码学及编码学研究的学者、研究生和高年级大学生朋友，并恳请读者批评指正.

肖国镇

1996 年 11 月

本书常用符号

N, Z, Q, R, C 分别表示自然数集，整数集，有理数集，实数集及复数集.

N^*, Z^*, Q^*, R^*, C^* 分别表示与上述集合相对应的不包含 0 元素的集合.

目　录

第一章

代数的回顾

本章的目的在于准确地说明数学词汇、术语、符号并给出一些重要的证明.

1.1 群

定义

设 G 是一个非空集合,在其中满足结合律与封闭性,记为

$$G\times G\to G,$$

$$(x,y)\to x\cdot y.$$

若 G 中存在一个单位元 e,使得对于 G 中的任何元素 x,有 $e\cdot x=x\cdot e=x$,并且存在元素 $x'\in G$,使得 $x\cdot x'=x'\cdot x=e$(元素 x' 称为 x 的逆元),则称集合 G 为群.

我们把群记为 $(G,\cdot)$. 在不致引起混淆的情况下,也可用 G 表示.

例 $(\mathbf{Z},+)$关于加法是群;$(\mathbf{R}^*,\cdot)$关于乘法是群.

如果群 $(G,\cdot)$ 中的运算满足交换律,则称 G 为交换群或阿贝尔群.

如果群 G 中的运算以乘号"·"标记,则 x 的逆元 x' 记为 x^{-1}.

如果群 G 中的运算以加号"+"标记,则我们称该群是阿贝尔群,并称 x' 为 x 的负元,记为 $-x$.

一个含 n 个有限元素的群，称为有限群或者 n 阶群.

1.2 元素的阶

定义和命题

设$(G,\cdot)$是含单位元 e 的 n 阶群，a 是 G 的任一元素，那么，一定存在一个最小整数 p，$p\geqslant 1$，使得 $a^p=e$. 整数 p 称为元素 a 的阶. 对任意整数 q，$q\geqslant 1$，若满足 $a^q=e$，则 q 必是 p 的倍数.

证明：设$(a^k)_{k\geqslant 1}$是$(G,\cdot)$的有限序列，则存在两个整数 k，l $(k<l)$，使得 $a^k=a^l$，即 $a^{l-k}=e$. 从而集合$\{q,q\in \mathbf{N}^*\mid a^q=e\}$非空. 设 p 是这个集合中的最小元素，我们有 $a^p=e$，设 q 满足$a^q=e$，利用 Euclidian 除法，q 除以 p 得到

$$q=pq'+r,0\leqslant r<p.$$

因此，

$$a^q=(a^p)^{q'}\cdot a^r=e\cdot a^r=e.$$

即

$$a^r=e.$$

由于 p 是最小整数，故 $r=0$.

1.3 循环群

定义

设$(G,\cdot)$是含单位元 e 的 n 阶群，如果存在元素 $g\in G$，使得 $G=\{g,g^2,\cdots,g^n\}$，则称 G 为循环群，g 为循环群$(G,\cdot)$的生成元.

注：(1)如果存在 $i,j,1\leqslant i\leqslant j\leqslant n$，满足 $g^i=g^j$，则 G 至多有 $j-i$ 个元素. 因此，满足 $g^q=e$ 的最小整数 q 就是 n，即 q 的阶为 n.

(2)显然，循环群是阿贝尔群.

1.4 子群

1.4.1 定义

设 H, K 是群 $(G, \cdot)$ 的两个非空子集，定义 $H^{-1}=\{x, x\in G \mid x^{-1}\in H\}$，$H\cdot K=\{x\cdot y\mid (x, y)\in H\times K\}$. 如果 $H\cdot H^{-1}=H$，则称 H 为 $(G, \cdot)$ 的子群.

例　G 是 $(G, \cdot)$ 的子群. 若 e 是 $(G, \cdot)$ 的单位元，则 $\{e\}$ 是 $(G, \cdot)$ 的子群.

1.4.2 命题

设 $(G, \cdot)$ 是含生成元 g 及单位元 e 的 n 阶循环群，对子 n 的每一个因子 d，相应地有且仅有一个含 d 个元素的 $(G, \cdot)$ 的子群 H. 这个子群为 $H=\{g^{n/d}, \cdots, (g^{n/d})^d\}$.

证明：g 的阶为 n，设 d 是 n 的一个因子，记 $H=\{g^{n/d}, \cdots, (g^{n/d})^d\}$.

若 $(g^{n/d})^i=(g^{n/d})^j$，$1\leqslant i<j\leqslant d$，则 $g^{\frac{n}{d}(j-i)}=e$. 因此，n 能整除 $n(j-i)/d$，这与 $0<(j-i)/d<1$ 相矛盾. 此即证明了 H 包含 d 个元素.

令 $((g^{h/d})^i, (g^{h/d})^j$ 是 H 中两个不同的元素，$1\leqslant i<j\leqslant d$，则 $(g^{n/d})^i\cdot(g^{n/d})^{d-j}\in H$. 此外，$e\in H$，$e\cdot e\in H$，若 $i=j<d$，则 $(g^{n/d})^{d-j}\cdot(g^{n/d})^i=e$，从而 $H\cdot H^{-1}=H$，即 H 是 $(G, \cdot)$ 的子群.

下证唯一性：设 K 是含 d 个元素的 $(G, \cdot)$ 的子群，记 $K=\{g^{n_1}, \cdots, g^{n_d}\}$，$1\leqslant a_1<\cdots<a_d\leqslant n$. 设 δ 是 $a_1, \cdots, a_d$ 的最大公约数，由 Bezout 恒等式知道，$\delta=u_1a_1+\cdots+u_da_d$，这里 $u_1, \cdots, u_d\in Z$，并且 $g^\delta\in K$. 设 g^δ 的阶为 p，则 $g^{\delta p}=e$. 由于 δ 整除 $a_1, \cdots, a_d$，因此可得 $K\subset\{g^\delta, \cdots, g^{\delta p}\}$. 显然，也有 $K\supset\{g^\delta, \cdots, g^{\delta p}\}$. 由此即得 $p=d$.

由于 $e=g^{\delta d}$，因此 $\delta d \mid n$，$\delta \mid n/d$，从而 $g^{\delta} \in H$. 即 $H \supset K$.

由于 H, K 均是含 d 个元素的群，从而 $H=K$.

注：由上述命题可知：循环群的子群是循环群.

1.4.3 **命题**

设 $(G, \cdot)$ 是含单位元 e 及生成元 g 的 n 阶循环群，那么，对于任意 $k, 1 \leqslant k \leqslant n$，$g^k$ 是 $(G, \cdot)$ 的含 $n/\gcd(n,k)$ 个元素的子群 H 的生成元.

证明：设 g^k 的阶为 p，则 $(g^k)^p = e$. 因此，$n \mid pk$ 并且 $n/\gcd(n,k) \mid p$. 显然，$(g^k)^{n/p \cdot \gcd(n,k)} = e$. 由 p 的最小性可知 $p = n/\gcd(n,k)$，记 $H = \{g^k, \cdots, (g^k)^p\}$. 由 1.4.2 节所述的同样理由可知 H 是含 p 个元素的循环群 $(G, \cdot)$ 的子群.

1.5 环

1.5.1 **定义**

非空集合 A 称为环，如果存在两个封闭的运算：

$$+ : A \times A \to A, \quad \cdot : A \times A \to A,$$

使得 $(A, +)$ 是个阿贝尔群，在此集合上“$\cdot$”满足结合律，存在单位元，并且对于任何 $x, y, z \in A$，两个乘法关于加法的分配律成立，即

$$x \cdot (y+z) = x \cdot y + x \cdot z,$$

$$(y+z) \cdot x = y \cdot x + z \cdot x.$$

在不致引起混淆时，我们用 $(A, +, \cdot)$ 或者 A 表示环.

当 $\cdot$ 满足交换律时，称此环为交换环.

例 $(\mathbf{Z}, +, \cdot)$，$(\mathbf{R}, +, \cdot)$ 是交换环.

群 $(A, +)$ 的单位元记为 0_A；“$\cdot$”的单位元记为 1_A.

1.5.2 **定义**

设 $(A, +, \cdot)$ 是环，U, V 是两个非空集合，定义 U, V 之间的

"+","·"两种运算如下:

$$U+V=\{x+y\mid(x,y)\in U\times V\},$$

$$U\cdot V=\{x\cdot y\mid(x,y)\in U\times V\}.$$

1.6 理想

定义

设$(A,+,\cdot)$是交换环,非空集合$I\subset A$,如果

$$I+I=I,$$

$$A\cdot I=I,$$

则称集合I为环$(A,+,\cdot)$的一个理想.

例 $\{2\}\cdot Z,\{1994\}\cdot Z$是环$(Z,+,\cdot)$的两个理想.

1.7 极大理想

定义

设$(A,+,\cdot)$是交换环,I是理想,如果$I\neq A$且对任意理想$J\subset A$,式

$$(J\supseteq I)\Rightarrow(J=I\text{ 或者 }J=A)$$

恒成立,则称I为环$(A,+,\cdot)$的极大理想.

例 当且仅当p是素数时,$\{p\}\cdot Z$是环$(Z,+,\cdot)$的极大理想.

1.8 商环

1.8.1 定义和命题

设$(A,+,\cdot)$是交换环,I为理想.对于任意的$x\in A$,记

$$\bar{x}=\{x\}+I=\{x+i,i\in I\}.$$

在子集$\bar{x}$中,我们定义两种运算"+"和"·"为

$$\bar{x}+\bar{y}=\{x+y\}+I;$$

$$\bar{x}\cdot\bar{y}=\overline{|xy|}+I.$$

易知$(\{\bar{x}, x\in A\}, +, \cdot)$是交换环，称此环为由 I 导出的 A 的商环，记为$\frac{A}{I}$.

例　设 Z 是整数环，$n\in N$. 由理想$\{n\}\cdot Z$ 导出的 Z 的商环记为$\frac{Z}{nZ}$，称此环为模 n 的剩余类环.

注：(1)若 $n=0$，则$\frac{Z}{0Z}=Z$，它是由恒等映射 $\bar{x}$到 x，对任意 $x\in Z$导出的.

(2)若 $n=4$，则$\frac{Z}{4Z}$包含四个元素：$\bar{0}, \bar{1}, \bar{2}, \bar{3}$. 可列成下表形式：

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

1.8.2　定理

当$\geqslant 2$ 时，$A=\frac{Z}{nZ}$中可逆元素作成的乘法群由这样的元素 $\bar{x}$ 构成，当 $0\leqslant x\leqslant n-1$ 时，$(x, n)=1$.

证明：由 Bezout 恒等式知，当且仅当存在 $u, v\in Z$，使得 $ux+vn=1$ 时，$(x, n)=1$. 由此可知，当且仅当$(x, n)=1$，$\bar{x}$在 A 中可逆.

至于 A 中的所有可逆元素作成群则是明显的.

注：我们用 $\varphi(n)$表示$\frac{Z}{nZ}$乘法群的元素个数.