代数和编码

万哲先 编著

科学出版社

代数和编码

万哲先 编著

科学出版社

1976

内 容 简 介

代数学是数学的重要基础分支．本世纪五十年代，抽象代数，特别是有限域理论在编码理论中找到了应用．

本书共分五章，前两章介绍了编码理论中用到的代数基础知识（有限域和线性代数）；次两章分别介绍了编码理论中的两类码，即伪随机码和纠错码；最后一章介绍了编码理论中出现的几个代数问题．

代 数 和 编 码

万 哲 先 编著

*

科 学 出 版 社 出 版

北京朝阳门内大街 137 号

中国科学院印刷厂印刷

新华书店北京发行所发行　各地新华书店经售

*

1976 年 3 月第 一 版　开本：787×1092　1/32

1976 年 3 月第一次印刷　印张：15 3/4

印数：0001—25,200　字数：361,000

统一书号：13031·356

本社书号：543·13—1

定价：1.45 元

序

代数学是数学的重要基础分支，有着上千年的悠久历史．近百年来，它的发展异常迅速，积累了丰富的内容，对数学的近代发展有显著的影响，同时在数学的其他分支及自然科学的许多部门里都有着重要的应用．但它对工程技术的应用则是比较间接的，最近二十年来，这种情况却有了显著的变化，代数学的一些成果被成功地直接应用到一些新的工程技术领域中去，而这些应用也给代数学带来了新的研究课题．四十年代末期出现了布尔（Boole）代数对开关电路的分析与综合以及对电子计算机逻辑设计的应用．五十年代则出现了抽象代数，特别是有限域的理论在编码理论中的应用．此外，代数学也是由于近代新技术的需要而诞生的时序电路和自动机理论、系统理论以及程序语言和数理语言学等新学科里的重要工具．

虽然人类在通信中采用种种明码和密码的历史相当久远，但编码理论可以认为是在电子技术飞速发展以后，针对当代数字通信和数字存储等的具体需要，于五十年代发展成为一门面目全新的应用数学，目前已有丰富的内容．

本书主要介绍编码理论所用的代数基础知识并在这一基础上阐述了编码理论中的某些课题，以利于有关工程技术人员与数学工作者掌握编码理论．全书共分五章，前两章介绍了编码理论所用到的最起码的一些代数基础知识，包括抽象代数，特别是有限域方面的知识和线性代数方面的知识；次两章分别就编码理论中的两类码，即伪随机码和纠错码作了导

引性的介绍，重点在于阐明基本概念；最后一章介绍了编码理论中出现的几个代数问题．另外，为不熟悉集合和映射这两个数学基本概念以及整数的分解的读者编写了两个附录附在书末，在前一附录里也介绍了本书采用的有关集合和映射的一些符号．

本书初稿是作者于1973年初在中国科学院数学研究所为一些单位的工程技术科研人员举办的代数和编码学习班上的讲稿．参加学习班的各单位的同志对本书初稿提了许多宝贵意见，作者根据这些意见对初稿进行了修改和补充，作者谨向这些同志表示感谢．

史无前例的无产阶级文化大革命使作者受到了深刻的教育，特别使作者认识到一定要遵循伟大领袖毛主席关于理论联系实际的教导，针对国家和人民的需要来发展我国的数学．在这一认识的基础上，作者才认真地学编码理论，才有机会和有关的工程技术科研人员接触并向他们学习，才有了编写这一本书的想法．而无产阶级文化大革命后的大好形势，特别是科技界和数学研究所的大好形势，数学研究所领导和一些同志的热情鼓励和支持，则是作者完成本书的重要条件．作者在此一并表示感谢．

编码理论的历史虽然很短，但内容却非常丰富．作者是编码理论的一个初学者，按本书的体系来介绍编码理论所用到的代数知识还是一个尝试，作者抱着虚心向国内有关同志学习的愿望，怀着抛砖引玉的心情，编写了这本书，希望得到读者的批评指正，也希望今后国内有更好的、更适宜于我国读者需要的这方面的书籍出版．

万哲先

目　录

第一章　抽象代数的基本概念和有限域的结构

抽象代数一般被认为是研究代数结构的性质的理论．在这一章里我们将介绍群、环、域这三个基本代数结构的定义，并详细地讨论有限域的结构．首先，我们从读者所熟悉的有理数域 $\mathbf{R}_0$，实数域 $\mathbf{R}$ 和复数域 $\mathbf{C}$ 出发归纳出域的概念．接着我们构造了对于编码理论来说是重要的有限域 $\mathbf{J}_p$ 和 $\mathbf{J}_p[x]_{p(x)}$ 作为例子．我们构造有限域的方法比较形式，这是因为我们想避免同余类环这一比较复杂的概念，因而直接在 $\mathbf{J}_p$ 中引进模 p 加法和模 p 乘法，同时直接在 $\mathbf{J}_p[x]_{p(x)}$ 中引进模 $p(x)$ 的加法和模 $p(x)$ 的乘法．对于熟悉模 2 加法的工程技术科研人员来说，也许这样做并不难接受，在 §7 中介绍了同余类环的概念以后，读者也就会更清楚在 $\mathbf{J}_p$ 和 $\mathbf{J}_p[x]_{p(x)}$ 中直接引入的加法运算和乘法运算的由来．在 §4 里我们从域的加法群和乘法群概括出交换群的概念，并证明了有限域的乘法群是循环群这一重要结果．§5 中关于有限域的结构定理，我们采用的是初等证明，显得比较复杂．读者可以从书后所附参考书目中的 [11]，[13]，[14] 或 [20] 里找到用较深工具的简单证明．为了能概括更广的一些代数结构，如整数环 $\mathbf{J}$，整数模 m 的环 $\mathbf{J}_m$（m 是个复合数）以及域上多项式环 $F[x]$，$F[x_1, x_2, \cdots, x_n]$ 等，我们引进了交换环的概念．对于了解编码理论的基础部分来说，一般的群（即它的运算不满足交换律的群）和一般的环（即它的乘法运算不满足交换律的环）并不十分必要，因此在本书中并没有讨论．对于一般的群

和环有兴趣的读者请参考书后所附参考书目中[11]或[12]. 为了引进同余类环,同时也为了以后讨论循环码的需要,我们还介绍了理想的概念. 在最后一节里我们介绍了我国古代数学的重要成就之一——孙子定理,并着重指出了它与近代环论中环的直和分解的关系.

§1 域的概念

我们从大家都熟悉的有理数开始讨论. 我们不是考察一个一个的有理数,而是考察有理数的全体所组成的集合. 我们用 $\mathbf{R}_0$ 来代表有理数的全体所组成的集合. 我们知道,在 $\mathbf{R}_0$ 中可以进行四则运算. 即任意给了两个有理数 a 和 b,可以对它们进行加法运算,得到它们的和 $a+b$ 也是个有理数;可以对它们进行减法运算,得到它们的差 $a-b$ 也是个有理数;可以对它们进行乘法运算,得到它们的积 $a\cdot b$ 也是个有理数;如果 $b\neq 0$ 的话,还可以用 b 做除数,用 a 做被除数进行除法运算,得到它们的商 $\frac{a}{b}$ 也是个有理数. 我们也知道,差可以表成和的形状,即如果用 $-b$ 表示 b 的相反数(适合条件 $b+(-b)=0$ 的数 $-b$),那么 $a-b=a+(-b)$,这样 a 减 b 所得的差就表成了 a 与 $-b$ 的和. 同样,商也可以表成积的形状,即当 $b\neq 0$ 时,如果用 b^{-1} 表示 b 的倒数(适合条件 $b\cdot b^{-1}=1$ 的数 b^{-1}),那么 $\frac{a}{b}=a\cdot b^{-1}$,这样 a 被 b 除所得的商就表成了 a 与 b^{-1} 的积. 因此在有理数的四则运算中,加法和乘法这两个运算是更为基本的.

我们也都知道,$\mathbf{R}_0$ 中的加法和乘法这两种运算满足以下这些运算规则:

I.1 对任意 $a, b\in\mathbf{R}_0$,有

$$a+b=b+a.\qquad(\text{加法交换律})$$

I.2 对任意 $a, b, c\in\mathbf{R}_0$，有

$$(a+b)+c=a+(b+c).\qquad(\text{加法结合律})$$

I.3 $\mathbf{R}_0$ 中有一个数，即 0，具有性质

$$a+0=0+a=a,\quad \text{对一切 } a\in\mathbf{R}_0.$$

I.4 对任意 $a\in\mathbf{R}_0$，$\mathbf{R}_0$ 中有一个与它相反的数，即 $-a$，具有性质

$$a+(-a)=(-a)+a=0.$$

II.1 对任意 $a, b\in\mathbf{R}_0$，有

$$ab=ba.\qquad(\text{乘法交换律})$$

II.2 对任意 $a, b, c\in\mathbf{R}_0$，有

$$(ab)c=a(bc).\qquad(\text{乘法结合律})$$

II.3 $\mathbf{R}_0$ 中有一个数，即 1，具有性质

$$a\cdot 1=1\cdot a=a,\quad \text{对一切 } a\in\mathbf{R}_0.$$

II.4 对任意 $a\in\mathbf{R}_0$ 而 $a\neq 0$，$\mathbf{R}_0$ 中有它的一个倒数，即 a^{-1}，具有性质

$$a\cdot a^{-1}=a^{-1}\cdot a=1.$$

III. 对任意 $a, b, c\in\mathbf{R}_0$，有

$$\begin{aligned}&a(b+c)=ab+ac,\\&(b+c)a=ba+ca.\end{aligned}\qquad(\text{分配律})$$

上面这些运算规则中，I 是关于加法的，II 是关于乘法的，I 和 II 完全是平行的，III 是说乘法对于加法来说是分配的.

我们再考察实数的全体所组成集合，我们把这个集合记作 $\mathbf{R}$. 我们知道，在 $\mathbf{R}$ 中也可以进行加法运算和乘法运算：任意给了两个实数 a 和 b，对它们进行加法运算，得到它们的和 $a+b$ 也是个实数；对它们进行乘法运算，得到它们的积 $a\cdot b$ 也是个实数. 而且 $\mathbf{R}$ 中加法运算和乘法运算也满足上面举出的运算规则 I, II, III，当然要把其中的 $\mathbf{R}_0$ 改成 $\mathbf{R}$.

我们再考察复数的全体所组成的集合，并把它记作 $\mathbf{C}$. 在 $\mathbf{C}$ 中也可以进行加法运算和乘法运算：对于任意 $a, b \in \mathbf{C}$，它们的和 $a+b$ 与积 $a \cdot b$ 也都是复数，而且 $\mathbf{C}$ 中的加法运算和乘法运算也满足上面举出的运算规则 I, II, III，当然要把其中的 $\mathbf{R}_0$ 改成 $\mathbf{C}$.

从上面这些例子，我们可以归纳出“域”的概念.

定义 1 设 F 是一个非空集合，F 的成员叫做元素. 假定在 F 中规定了加法和乘法这两种运算，即对于 F 中任意两个元素 a 和 b，可以对它们进行**加法运算**和**乘法运算**，把加法运算的结果记作 $a+b$，叫做它们的**和**，并把乘法运算的结果记作 $a \cdot b$，叫做它们的**积**. 我们还要求 F 中任意两个元素经加法运算和乘法运算的结果仍是 F 中的元素，即 F 中任意两个元素的和与积仍都是 F 中的元素（这个性质通常称为 F 对于加法运算和乘法运算是**自封的**）. 我们说 F 对于所规定的加法运算和乘法运算是一个**域**，如果以下运算规则都成立：

I.1 对任意 $a, b \in F$，有

$$a+b=b+a;$$

I.2 对任意 $a, b, c \in F$，有

$$(a+b)+c=a+(b+c);$$

I.3 F 中有一个元素，把它记作 0，具有性质

$$a+0=a, \text{对一切 } a \in F;$$

I.4 对任意 $a \in F$，F 中有一个元素，把它记作 $-a$，具有性质

$$a+(-a)=0;$$

II.1 对任意 $a, b \in F$，有

$$a \cdot b=b \cdot a;$$

II.2 对任意 $a, b, c \in F$，有

$$(a \cdot b) \cdot c=a \cdot (b \cdot c);$$

II.3　F 中有一个 $\neq 0$ 的元素，把它记作 e，具有性质

$$a \cdot e = a, \quad \text{对一切 } a \in F;$$

II.4　对任意 $a \in F$ 而 $a \neq 0$，F 中有一个元素，把它记作 a^{-1}，具有性质

$$a \cdot a^{-1} = e;$$

III　对任意 $a, b, c \in F$，有

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

值得注意的是，在这个定义里，因为假设了加法交换律 I.1 成立，所以在 I.3 中我们仅仅要求 $a + 0 = a$，而略去了 $0 + a = a$ 这一要求，这是由于从 I.1 和 $a + 0 = a$ 可以推出 $0 + a = a$；同理，我们在 I.4 中只要求 $a + (-a) = 0$，而略去了 $(-a) + a = 0$ 这一要求．因为我们在这个定义里假设了乘法交换律 II.1 成立，所以在 II.3 中只要求 $a \cdot e = a$，而略去了 $e \cdot a = a$ 这一要求；在 II.4 中只要求 $a \cdot a^{-1} = e$，而略去了 $a^{-1} \cdot a = e$ 这一要求；在 III 中也略去了 $(b + c) \cdot a = b \cdot a + c \cdot a$ 这一要求．

基于这个定义并根据前面的分析，我们可以说，所有有理数组成的集合 $\mathbf{R}_0$ 对于有理数的加法和乘法运算来说是一个域，叫做*有理数域*；所有实数组成的集合 $\mathbf{R}$ 对于实数的加法和乘法运算来说是一个域，叫做*实数域*；所有复数组成的集合 $\mathbf{C}$ 对于复数的加法和乘法运算来说也是一个域，叫做*复数域*．我们也知道 $\mathbf{R}$ 是 $\mathbf{C}$ 的子集，而 $\mathbf{R}$ 中的加法运算和乘法运算即是把 $\mathbf{R}$ 中的元素看作 $\mathbf{C}$ 中元素所作的加法运算和乘法运算．这时我们说 $\mathbf{R}$ 是 $\mathbf{C}$ 的*子域*．一般地，我们有下面这个定义．

定义 2　设 F 是一个域，而 F_0 是 F 的一个非空子集．如果 F_0 对于 F 中的加法运算和乘法运算来说是一个域，这就是说，对 F_0 中任意两个元素按 F 中加法运算和乘法运算进行运算所得的和与积仍是 F_0 中的元素，而且 F 中的加法运算和乘

法运算对于 F_0 来说也满足定义 1 中的运算规则 I, II, III, 我们就说 F_0 是 F 的子域.

值得注意的是，设 F 是域，而 F_0 是 F 的一个非空子集，如果 F_0 对于 F 中的加法运算和乘法运算自封，那么要验证 F_0 是 F 的子域，只要验证 I.3, I.4, II.3, II.4 在 F_0 中成立就行了，因为这时 I.1, I.2, II.1, II.2, III 在 F_0 中自然成立.

根据定义2，我们可以说 $\mathbf{R}$ 是 $\mathbf{C}$ 的子域，$\mathbf{R}_0$ 也是 $\mathbf{C}$ 的子域，$\mathbf{R}_0$ 还是 $\mathbf{R}$ 的子域.

为了搞清楚域的概念，下面我们再举几个例子.

例 1 考察所有形状

$$a + b\sqrt{2}, \quad a, b \in \mathbf{R}_0$$

的实数的全体所组成的集合，把这个集合记作 $\mathbf{R}_0[\sqrt{2}]$. 我们规定 $\mathbf{R}_0[\sqrt{2}]$ 中两个元素的和与积分别是它们作为实数的和与积. 我们来验证 $\mathbf{R}_0[\sqrt{2}]$ 对于实数的加法运算和乘法运算是一个域，因而是 $\mathbf{R}$ 的子域. 首先，设 $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbf{R}_0$, 那么

$$\begin{aligned}&(a + b\sqrt{2}) + (c + d\sqrt{2})\\&\quad = (a + c) + (b + d)\sqrt{2},\\&(a + b\sqrt{2}) \cdot (c + d\sqrt{2})\\&\quad = (ac + 2bd) + (ad + bc)\sqrt{2}.\end{aligned}$$

显然 $a + c, b + d, ac + 2bd, ad + bc \in \mathbf{R}_0$. 因此 $\mathbf{R}_0[\sqrt{2}]$ 对于加法运算和乘法运算是自封的，其次，还要验证 $\mathbf{R}_0[\sqrt{2}]$ 中的加法运算和乘法运算满足运算规则 I.3, I.4, II.3, II.4.

显然 $0 = 0 + 0\sqrt{2} \in \mathbf{R}_0$, 而

对一切 $a + b\sqrt{2} \in \mathbf{R}_0[\sqrt{2}]$, 有 $(a + b\sqrt{2}) + 0 = a + b\sqrt{2}$. 因此 I.3 成立. 其次，对任意 $a + b\sqrt{2} \in \mathbf{R}_0[\sqrt{2}]$, 有 $-a + (-b)\sqrt{2} \in \mathbf{R}_0[\sqrt{2}]$, 而

$$(a + b\sqrt{2}) + [-a + (-b)\sqrt{2}] = 0,$$

因此 I.4 也成立.

可以平行地证明 II.3 和 II.4 也成立，只要注意 $1 = 1 + 0\sqrt{2} \in \mathbf{R}_0[\sqrt{2}]$；而当 $a + b\sqrt{2} \in \mathbf{R}_0[\sqrt{2}]$，$a + b\sqrt{2} \neq 0$ 时，$a^2 - 2b^2 \neq 0$，因此

$$\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbf{R}_0[\sqrt{2}],$$

而且

$$(a + b\sqrt{2}) \cdot \left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\right) = 1.$$

这证明了 $\mathbf{R}_0[\sqrt{2}]$ 是 $\mathbf{R}$ 的子域.

例 2 考察所有形状

$$a + b\sqrt[3]{2}, \quad a, b \in \mathbf{R}_0$$

的实数的全体所组成的集合，并把这个集合记作 S. 如果规定 S 中两个元素的和与积分别是它们作为实数的和与积，这时 S 不是域，这是因为 S 对于乘法运算不是自封的. 例如

$$\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$$

就不是形状 $a + b\sqrt[3]{2}$ $(a, b \in \mathbf{R}_0)$ 的数.

但是，如果考察所有形状

$$a + b\sqrt[3]{2} + c\sqrt[3]{4}, \quad a, b, c \in \mathbf{R}_0$$

的实数的集合，把这个集合记作 $\mathbf{R}_0[\sqrt[3]{2}]$，并规定 $\mathbf{R}_0[\sqrt[3]{2}]$ 中两个元素的和与积分别是它们作为实数的和与积，可以验证 $\mathbf{R}_0[\sqrt[3]{2}]$ 是域. 请读者自己验证一下.

例 3 考察全体整数(正、负整数和 0)的集合，并把这个集合记作 $\mathbf{J}$. 固然 $\mathbf{J}$ 对于整数的加法运算和乘法运算是自封的，而且 $\mathbf{J}$ 中加法运算和乘法运算满足运算规则 I.1, I.2, I.3, I.4, II.1, II.2, II.3 和 III，但是在 $\mathbf{J}$ 中II.4，却不成立. 譬如，2 和任意整数之积都不能等于 1. 因此 $\mathbf{J}$ 不是域.

下面我们经常要用到关于整数分解的一些性质. 不熟悉

这部分内容的读者请先阅读本书的附录二.

无论是 $\mathbf{C}$, $\mathbf{R}$, $\mathbf{R}_0$ 或是 $\mathbf{R}_0[\sqrt{2}]$, $\mathbf{R}_0[\sqrt[3]{2}]$, 它们的元素个数都是无限的. 但在编码里用的却是元素个数有限的域. 我们有

定义 3 设 F 是域. 如果 F 的元素个数无限, F 就叫无限域. 如果 F 的元素个数有限, F 就叫有限域也叫伽罗瓦(Galois)域.

我们举一个有限域的例子.

例 4 设 p 是一个给定的素数. 令 $\mathbf{J}_p$ 表示所有 $<p$ 的非负整数所组成的集合

$$\mathbf{J}_p = \{0, 1, 2, \cdots, p-1\}.$$

显然按照通常的整数加法运算和乘法运算, $\mathbf{J}_p$ 不是域, 因为 $\mathbf{J}_p$ 对于通常的整数加法运算和乘法运算都不自封. 下面我们将用另外的方法来规定 $\mathbf{J}_p$ 中的加法和乘法运算使 $\mathbf{J}_p$ 成域.

我们先引进一个记号, 这个记号今后经常要用到. 设 a 和 b 是两个整数, 而 $b \neq 0$. 再设用 b 去除 a 所得的商是 q 而余数是 r, 即

$$a = qb + r, \quad 0 \leqslant r < |b|.$$

我们知道, q 和 r 由 a 和 b 唯一确定. 引进记号

$$r = (a)_b$$

来表示用 b 去除 a 所得的余数.

现在设 $a, b \in \mathbf{J}_p$. 我们按下式来规定 a 与 b 的和(把它记作 $a \oplus b$)与积(把它记作 $a \odot b$):

$$a \oplus b = (a+b)_p,$$

$$a \odot b = (a \cdot b)_p.$$

我们也常把 $\mathbf{J}_p$ 中的加法$\oplus$叫做模 p 加法, 而把 $\mathbf{J}_p$ 中的乘法$\odot$叫做模 p 乘法. 我们来验证 $\mathbf{J}_p$ 对于如上规定的加法和乘

法运算是域.

首先,显然有

$$0 \leqslant (a+b)_p < p, \quad 0 \leqslant (a \cdot b)_p < p.$$

因此 $\mathbf{J}_p$ 对于模 p 加法和模 p 乘法是自封的.

其次要验证如上规定的 $\mathbf{J}_p$ 中的模 p 加法和模 p 乘法满足运算规则 I, II, III.

先证 I.1 和 II.1 成立. 对任意 $a, b \in \mathbf{J}_p$, 我们有

$$a+b=b+a, \quad ab=ba.$$

因此

$$(a+b)_p=(b+a)_p, \quad (a \cdot b)_p=(b \cdot a)_p.$$

这就是说

$$a \oplus b = b \oplus a, \quad a \odot b = b \odot a.$$

在验证 I.2 和 II.2 之前,我们先证明下面这个引理.

引理 1 设 a_1, a_2, b 都是整数,而 $b \neq 0$. 那么 $(a_1)_b = (a_2)_b$, 当且仅当 $b \mid a_1 - a_2$*.

证 "$(a_1)_b = (a_2)_b$, 当且仅当 $b \mid a_1 - a_2$" 这个命题的涵意是说"当 $b \mid a_1 - a_2$ 时, $(a_1)_b = (a_2)_b$" 及"当 $(a_1)_b = (a_2)_b$ 时, $b \mid a_1 - a_2$". 这两个命题同时成立.

根据带余除法,可以设

$$a_1 = q_1 b + (a_1)_b, \quad 0 \leqslant (a_1)_b < |b|.$$

$$a_2 = q_2 b + (a_2)_b, \quad 0 \leqslant (a_2)_b < |b|.$$

那么

$$a_1 - a_2 = (q_1 - q_2)b + (a_1)_b - (a_2)_b. \quad (1)$$

当 $b \mid a_1 - a_2$ 时,由 (1) 式可推出 $b \mid (a_1)_b - (a_2)_b$. 但因 $0 \leqslant (a_1)_b, (a_2)_b < |b|$, 故 $0 \leqslant |(a_1)_b - (a_2)_b| < |b|$. 因此一定有 $(a_1)_b = (a_2)_b$. 反过来,当 $(a_1)_b = (a_2)_b$ 时,由(1)式显

---

* $b \mid a$ 表示 a 能被 b 整除.

然有 $b \mid a_1 - a_2$. 这就证明了引理 1.

从引理 1 可以推出关于符号 $(a)_b$ 的运算规则, 即

引理 2 设 a_1, a_2, b 都是整数, 而 $b \neq 0$, 那么

$$(a_1 \pm a_2)_b = ((a_1)_b \pm (a_2)_b)_b, \tag{2}$$

$$(a_1 a_2)_b = ((a_1)_b \cdot (a_2)_b)_b. \tag{3}$$

((2)式实际是两个式子, 等号双方取'+'号得到一个式子, 等号双方取'−'号又得到一个式子. 以后出现符号'±'时, 也作此了解, 而不一一说明.)

证 首先注意, 对于任意整数 a, 根据带余除法, 可以写

$$a = qb + (a)_b, \quad 0 \leqslant (a)_b < |b|.$$

因此

$$b \mid a - (a)_b.$$

特别, 因

$$(a_1 \pm a_2) - ((a_1)_b \pm (a_2)_b) = (a_1 - (a_1)_b) \pm (a_2 - (a_2)_b)$$

和

$$a_1 a_2 - (a_1)_b (a_2)_b = a_1 (a_2 - (a_2)_b) + (a_1 - (a_1)_b)(a_2)_b$$

都是 b 的倍数, 所以根据引理 1 就推出 (2), (3) 两式.

显然, 可以将引理 2 推广到 n 个整数 $a_i (i = 1, 2, \cdots, n)$ 的和与积的情形, 即

$$(a_1 + a_2 + \cdots + a_n)_b = ((a_1)_b + (a_2)_b + \cdots + (a_n)_b)_b,$$

$$(a_1 a_2 \cdots a_n)_b = ((a_1)_b \cdot (a_2)_b \cdot \cdots \cdot (a_n)_b)_b.$$

请读者自己把证明补出.

现在来验证在 $\mathbf{J}_p$ 中 I.2 和 II.2 成立. 由 $\mathbf{J}_p$ 中加法运算和乘法运算的定义可知, 对任意 a, b, $c \in \mathbf{J}_p$, 有

$$(a \oplus b) \oplus c = ((a + b)_p + c)_p,$$

$$(a \odot b) \odot c = ((ab)_p \cdot c)_p.$$

因 $c \in \mathbf{J}_p$, 所以 $(c)_p = c$. 因此由引理 2 推出