典型群

华罗庚 万哲先 著

上海科学技术出版社

典 型 群

华罗庚 萬哲先 著

上海科学技术出版社

內 容 提 要

本书是典型群方面作者历年来工作的系統总結性論著，也包含了作者在体論和矩陣几何方面的工作．书中不仅列举了作者在这一領域中所获得的丰富而完整的結果，也充分体現了作者所創用的方法和技巧的特点．

全书共分十二章，前六章由第一作者执笔，初稿完成于1951年，后六章由第二作者根据他所体会的前六章的精神和方法續写．书末附有一些注釋．

典　型　群

华罗庚　萬哲先　著

上海科学技术出版社出版（上海瑞金二路450号）
上海市书刊出版业营业許可証出093号

上海新华印刷厂印刷　新华书店上海发行所发行

开本 787×1092 1/23　印張 23 5/23　插頁 4　排版字数 462,000
1963年7月第1版　1963年7月第1次印刷
印数 1—3,860（其中胶版紙本60册）

統一书号 13119·516　定价(十四) 3.75元

序

早在1949年，本书作者之一就有了写这样一本书的輪廓，希望根据这个輪廓組織一个討論班，和一批大学四年級及剛毕业的同学在一起，使他們边学习边搞研究，集体地較整套地来进行这一領域的研究工作，一来可以使他們在工作过程中逐步地扩充自己的知識領域，另一方面可以让他們习作一些研究，預計在計划完成之后，可以給典型群論，射影几何学，矩陣論及群表示論等数学分支以一个不同的面貌．1950年初，当他在北京清华大学执教时，組織了这样一个討論班．討論班进行到1951年暑假，在討論班里他完成了本书前六章的初稿．接着，在1951年下半年和1957年上半年，他又在中国科学院数学研究所代数討論班里两度报告了本书前六章的大部分章节，并进行了一些修改．随后，从1959年下半年起，本书后一作者又在数学研究所代数討論班里报告了前六章的部分章节，并根据他所体会的前六章的精神与方法續写了本书的后六章．这就是本书簡单的写作經过．

簡要地可以这样說，体上的矩陣是一个値得注意的对象，因为它是一个不太失去普遍性的抽象事物，但同时又和成果丰富的具体的域上的矩陣論距离不远．当然，結合环，李环和柔丹环中有趣的部分又都有矩陣形式，而綫性群，正交群，辛群，罗倫兹群也都是矩陣群；几何学中綫几何，圓几何，格拉斯曼几何都有矩陣的表示法．更如多复变函数論的典型域也离不开矩陣的表达形式．这些形成了我們的工作背景．

仅仅找到一个值得研究的对象，而没有处理的方法那也还是空話．本书中提供了一些方法，这些方法是初步的，犹待改进，补充和发展，只有在发展过程中才能把方法搞得更完备．

1950 年本书作者之一选擇这个主題的原因之一是为了易于訓練干部．預备知識需要得少，可以从簡单处着手，从具体处着手；发展前途不太小，通过这一系列的研究也可以熟悉代数学，几何学中不少分支，可以从寬广处着眼，从抽象处着眼．換言之，开始时不受基础的限制，終了时不致侷促于太仄狹的領域之中．

匆匆已經十年，这計划还只能說在第一阶段中完成了第一部分而已．更重要的工作还有待于今后的努力．这决不是一个完整的东西，而仅仅是一个开始．这是一个阶梯中的一級，讀者必須想想前面几級——实数域，复数域，有限域及四元数体上的情况，讀者更必須看看后面几級——体上矩陣的环和群的构造，不用連續性的群表示論等等，这样才不致于为本书引入歧途．長期局限于本书范圍內的工作将不是作者的本意，但我們認为搞清这些对象和方法对学好典型群論，射影几何学等都能有所帮助．

我們感謝王仰賢，应玫茜，徐誠浩等同志，在本书付印之前，他們分头閱讀了本书手稿的各部分，进行了核算，并提出了一系列宝貴的修改意見．

华罗庚　萬哲先

1962 年 8 月于北京

目　录

第一章

体論

§1 环与体

为了使本书尽可能地自給自足，我們先叙述一下环和体的基本性质，并且提供若干例子，通过这些例子来說明某些概念的具体涵义.

定义1 环 R 乃具有两种运算"+"及"×"的集合，即若 a, b 在 R 中，則 $a+b$ 及 $a\times b$ 也是 R 中唯一定义的元素；这两个运算有次之性质：

I. 对加运算"+"，R 成一交换群（或称为 Abel 群），即对 R 中的任意三元素 a, b, c 有次之关系：(i) $a+b=b+a$；(ii) $(a+b)+c=a+(b+c)$；(iii) R 有一元素 0，称为零元素，使对所有的 a，常有 $0+a=a$，及 (iv) 对 R 中任意元素 a，R 中一定有一个元素 b，使得 $a+b=0$；

II. 对乘运算"×"，适合結合律，即对 R 中的任意三元素 a,b,c,常有

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

III. 加乘之間适合分配律，即对 R 中的任意三元素 a, b, c，常有

$$a\times(b+c)=a\times b+a\times c,$$

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

以后为方便計，将"×"号略去. 通常习見的名詞"和"，"差"，"积"

等名詞，其义自明，不再定义。

〔例 1〕 所有的整数成一环；所有的偶数也成一环。

〔例 2〕 命 m 表一正整数，以 m 为模所得的同余类成一环．且看一个具体情形．命 $m=6$，任一整数可以唯一地归入下面六类之一：

$$\{0+6k\},\ \{1+6k\},\ \{2+6k\},\ \{3+6k\},\ \{4+6k\},\ \{5+6k\}.$$

分别以 $\Gamma_0, \cdots, \Gamma_5$ 表示上述的类．两类的加法定义为

$$\Gamma_i+\Gamma_j=\Gamma_k, \quad 若\ i+j\equiv k \pmod 6,$$

而 Γ_0 为加法群中的零元素；乘法定义为

$$\Gamma_i\Gamma_j=\Gamma_k, \quad 若\ ij\equiv k \pmod 6.$$

显然，这样定义出一个环。

〔例 3〕 所有带有理系数的单变数多項式成一环。

〔例 4〕 以一多项式为模，分上例中所述的多項式为同余类，这些类也成为一环。

〔例 5〕 形如 $a+bi$ $(i=\sqrt{-1})$ 的数，其中 a, b 为整数，也成一环。

〔例 6〕 所有在区間 (a, b) 内的連續函数成一环。

〔例 7〕 复变数函数論中所討論的全体整函数也成一环。

环 R 中的零元素 0 还有次之性质：由

$$0a=(0+0)a=0a+0a$$

可知

$$0a=0.$$

同样，可知 $a0=0$．即 0 左乘或右乘任一元素恒为 0．但从 $ab=0$ 并不能断定 a, b 中至少有一为 0；例如，在例 2 中，$\Gamma_2\Gamma_3=\Gamma_0$，但是 $\Gamma_2\neq\Gamma_0$，$\Gamma_3\neq\Gamma_0$．因而我們定义：环中如有二元素 $a\neq0$，$b\neq0$ 而 $ab=0$，則称 a 为左零因子，b 为右零因子。

显然，如果环中无左零因子，当然也无右零因子．这样的环謂之无零因子的环。

如果环 R 的一个子集合 S 对 R 的两个运算也成一环，那末，S 称为环 R 的子环．例 1 即說明子环是存在的。

定义 2　环 R 若再满足下面的条件則称为体：

II′. R中除0外,其他的元素对乘法成一群,即有一元素1,称为么元素,使$1\cdot a=a$,而且对R中任意元素$a\neq 0$,有一元素b存在,使$b\cdot a=1$.

若体中乘法满足交换律,即$ab=ba$,则体称为域.

〔例1〕 命p为一素数,以p为模所得的同余类成一域.

〔例2〕 所有的有理数成一域.

〔例3〕 所有的形如$a+bi$的数也成一域,此处a,b过所有的实数.

〔例4〕 所有的有理函数成一域.

〔例5〕 所有的半純函数也成一域.

以上列举的全是域的例子. 現在問:是否有非域之体?

〔例6〕 命F表一实域,就是具有下述性质的域:如果若干个元素的平方的和等于0,则这些元素全是0. 命i, j, k为三元素,与F中的元素皆可交换,且具有以下諸性质:

$$ij=-ji=k,\quad jk=-kj=i,\quad ki=-ik=j,$$
$$i^2=j^2=k^2=-1. \tag{1}$$

我們考虑全体形如

$$a_0+a_1i+a_2j+a_3k \qquad (a_0,\ a_1,\ a_2,\ a_3\in F)$$

的元素. 这种元素称为四元数,以Q表所有的四元数所成的集合,其中的加法定义为

$$(a_0+a_1i+a_2j+a_3k)+(b_0+b_1i+b_2j+b_3k)$$
$$=(a_0+b_0)+(a_1+b_1)i+(a_2+b_2)j+(a_3+b_3)k,$$

其乘法由(1)式及分配律予以确定. 讀者試自驗証,Q是一体,称为四元数体.

易見,在Q中与任一元素皆可交換的元素所成的集合,就是F. 这一性质引出以下概念:

一体R中的元素a,若对所有的$x\in R$常满足

$$ax=xa,$$

则a称为R的中心元素. 全体中心元素所成的集合,称为R的中心. 显然中心成一域.

一体的子集,如果对体的原有的两种运算仍成一体,这子集称为原体的子体,而称原体为子体的扩体. 例 6 中的 F 是 Q 的子体.

〔例 7〕 命 F 为一域, 系数在 F 中所有的 x 的多項式成一环, 以 $F[x]$ 記之. 設 $f(x)$ 为系数在 F 中的不可分解的多項式. 以 $f(x)$ 为模,分多项式为若干类,如此諸类成一域,証明如下:

对任一 $g(x)$, 如非 $f(x)$ 的倍数,由輾轉相除法可得二多項式 $a(x)$ 与 $b(x)$, 使

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

此处 $a(x)$, $b(x)$ 的系数也在 F 中. 由此立得

$$a(x)g(x)\equiv 1 \pmod{f(x)}.$$

即 $g(x)$ 所代表的同余类以 $a(x)$ 所代表的同余类为其逆. 显然可見, 此域以 F 为其子域.

假定 α 是方程式 $f(x)=0$ 的根, 且 α 与 F 中的元素都可交换, 则形如

$$a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1} \quad (a_0, \cdots, a_{n-1}\in F)$$

之元素成一域, 此处 n 为多項式 $f(x)$ 的次数. 只須重复上面的討論就可以証明这一性质. 如此所得的域称为 F 的单代数扩域, 且以符号 $F(\alpha)$ 記之.

§2 特征数及素域,由环建体

設 R 为一无零因子的环. 对 R 中某一元素 $a\neq 0$, 若有最小正整数 p 存在,使 $pa=0$, 即

$$\underbrace{a+a+\cdots+a}_{p\text{个}}=0,$$

則 p 称为此环的特征数. 若不存在这样的 p, 則称此环为特征数为零的环,或記之以 $p=0$. 特征数 p 有下述的性质:

I. p 与 a 的选擇无关;

II. p 为素数.

事实上,設 $a\neq 0$, $b\neq 0$ $(a, b\in R)$, 則由

$$(pa)b=a(pb)$$

可知由 $pa=0$ 推出 $pb=0$. 反之，由 $pb=0$ 推得 $pa=0$, 故得 I.

又若 p 不是素数而 $p=p_1p_2$ $(p_1>1,\ p_2>1)$, 則 $pa=p_1(p_2a)=0$, 若 $p_2a=0$, 此与 p 的假設不合；若 $p_2a\neq 0$, 此与 I 相矛盾，故得 II.

命 R 为有么元素的环，Σ 为 R 中包含么元素的最小子环. 若 R 为无零因子环而且 R 之特征数是 p, 則 Σ 就是：$0, 1, \cdots, p-1$ 所构成的集合. 若 R 之特征数为 0, 則 Σ 就是所有的整数.

命 F 为一体，若 F 的特征数是 p, 則 F 的最小子体就是由 $0, 1, \cdots, p-1$ 这些元素所构成的域. 若特征数是 0, 則 F 的最小子体就是由全体有理数所組成的域. 这最小子体称为体 F 的素域.

定义 1 在一环中，如 $a=bc$, 則 b 称为 a 的左因子，c 称为 a 的右因子；a 称为 b 的右倍数，c 的左倍数. 若有一元 m 具有性质

$$m=aa_1=bb_1,$$

則 m 称为 a 及 b 的右公倍数. 显然可以类似地定义任意多个元素的右公倍数.

本节之目的在于：从无零因子而任二元素有右公倍数的环出发，仿照由整数建立有理数的方法，来建立体.

为了这个目的，我們将下面的集合分类：

$$\{(a, b);\ \ a, b\in R,\ \ b\neq 0\}.$$

設有 (a, b), (c, d). 若对于 d, b 的某一右公倍数 $m=bb_1=dd_1$, $ab_1=cd_1$ 成立，則称 (a, b) 与 (c, d) 属于同类，以 $(a, b)\sim(c, d)$ 表之.

首先証明，此定义与 m 的选择无关. 即若 m' 为另一右公倍数，$m'=bb_1'=dd_1'$, 則我們仍有 $ab_1'=cd_1'$. 事实上，由假定，m 与 m' 有一右公倍数 $M=mx=m'y$, 則有 $b_1x=b_1'y$ 及 $d_1x=d_1'y$. 再由 $ab_1=cd_1$ 立得 $ab_1'y=ab_1x=cd_1x=cd_1'y$, 即 $ab_1'=cd_1'$.

其次証明：关系"～"是一等价关系，即有以下的三种性质：

1. 反身性 $(a, b)\sim(a, b)$；

2. 对称性 若 $(a, b)\sim(c, d)$, 則 $(c, d)\sim(a, b)$；

3. 傳递性 若 $(a, b)\sim(c, d)$, $(c, d)\sim(e, f)$, 則 $(a, b)\sim(e, f)$.

1 及 2 是显然的事实．現在我們去証明傳递性．易見任何三元素 b, d, f，必有一右公倍数 m 使

$$m=bb_1=dd_1=ff_1,$$

由假定 $ab_1=cd_1$，$cd_1=ef_1$，故得 $ab_1=ef_1$，即 $(a, b)\sim(e, f)$．

所有的类成一集合，以 K 表之．今以 $\frac{a}{b}$ 表示 (a, b) 所属之类，(a, b) 称为此类的代表．今在 K 中定义加法和乘法．

对于加法，我們作如次的定义：

$$\frac{a}{b}+\frac{c}{d}=\frac{ab_1+cd_1}{m},$$

此处 m 是 b 及 d 的一个右公倍数，且 $m=bb_1=dd_1$．

首先指出这定义与 m 的选擇无关．盖設 $m'=bb_1'=dd_1'$ 及 $M=mx=m'y$，則 $b_1x=b_1'y$，$d_1x=d_1'y$，故得

$$\frac{a}{b}+\frac{c}{d}=\frac{ab_1+cd_1}{m}=\frac{ab_1x+cd_1x}{mx}$$
$$=\frac{ab_1'y+cd_1'y}{m'y}=\frac{ab_1'+cd_1'}{m'}.$$

其次指出，此定义与 $\frac{a}{b}$ 及 $\frac{c}{d}$ 的代表选擇无关．

設 $\frac{a}{b}=\frac{a'}{b'}$，$\frac{c}{d}=\frac{c'}{d'}$；則 $m=bb_1=b'b_1'=dd_1=d'd_1'$，由假定知 $ab_1=a'b_1'$，$cd_1=c'd_1'$，故得

$$\frac{a}{b}+\frac{c}{d}=\frac{ab_1+cd_1}{m}=\frac{a'b_1'+c'd_1'}{m}=\frac{a'}{b'}+\frac{c'}{d'}.$$

对于乘法定义如下：

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right)=\frac{ab_1}{dc_1},$$

此处 $m=bb_1=cc_1$，而 $c\neq 0$．

同样可証，此定义与 m 的选擇无关．設 $m'=bb_1'=cc_1'$，$mx=m'y$，則 $b_1x=b_1'y$，$c_1x=c_1'y$，故得

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right)=\frac{ab_1}{dc_1}=\frac{ab_1x}{dc_1x}=\frac{ab_1'y}{dc_1'y}=\frac{ab_1'}{dc_1'}.$$

再証明此定义与 $\frac{a}{b}$ 及 $\frac{c}{d}$ 的代表选择无关. 若 $\frac{a}{b}=\frac{a'}{b'}$, $\frac{c}{d}=\frac{c'}{d'}$, 由此可設

$$bb_1=b'b_1',\quad ab_1=a'b_1';\quad dd_1=d'd_1',\quad cd_1=c'd_1'.$$

取 $m=bb_1\alpha=b'b_1'\alpha=cd_1\beta=c'd_1'\beta$, 故

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}\right)=\frac{ab_1\alpha}{dd_1\beta},\quad \left(\frac{a'}{b'}\right)\left(\frac{c'}{d'}\right)=\frac{a'b_1'\alpha}{d'd_1'\beta}.$$

当 $c=0$ 时，我們定义

$$\left(\frac{a}{b}\right)\left(\frac{0}{d}\right)=\left(\frac{0}{d}\right).$$

集合 K 經过这样定义加法和乘法之后成为一体，称为 R 的商体. 今往証明其适合体之諸条件:

I. 对加法运算成一 Abel 群. 易見 $\frac{0}{d}$ 相当于 0 元素，而 $-\frac{a}{b}$ 相当于 $\frac{a}{b}$ 的逆元素. 証明甚易，讀者自証之.

II. 非零元素对乘法成一群. 这一証明也略去. 其中 $\frac{d}{d}$ 相当于么元素，而 $\frac{b}{a}$ 相当于 $\frac{a}{b}$ 的逆元素.

III. 分配律成立. 首先我們来証明左分配律:

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}+\frac{e}{f}\right)=\left(\frac{a}{b}\right)\left(\frac{c}{d}\right)+\left(\frac{a}{b}\right)\left(\frac{e}{f}\right).$$

設 $bb_1=cc_1$, $dc_1d_1=fc_1f_1=m$, 則

$$\left(\frac{a}{b}\right)\left(\frac{c}{d}+\frac{e}{f}\right)=\left(\frac{ab_1d_1}{bb_1d_1}\right)\left(\frac{cc_1d_1+ec_1f_1}{m}\right)$$
$$=\left(\frac{ab_1d_1}{bb_1d_1}\right)\left(\frac{bb_1d_1}{m}+\frac{ec_1f_1}{m}\right),$$

故在証明中不妨假定 $d=f$, $c=b$, 即只須証明

$$\left(\frac{a}{b}\right)\left(\frac{b+e}{d}\right)=\frac{a}{d}+\left(\frac{a}{b}\right)\left(\frac{e}{d}\right)$$

即足.

設 $n=bb_1=ee_1$, 此式的右边等于

$$\frac{a}{d}+\frac{ab_1}{de_1}=\frac{ae_1+ab_1}{de_1},$$

而左边等于

$$\left(\frac{a}{b}\right)\left(\frac{(b+e)e_1}{de_1}\right)=\left(\frac{a}{b}\right)\left(\frac{b(e_1+b_1)}{de_1}\right),$$

于是左右两边完全符合.

右分配律的証明比較容易. 由于在証明

$$\left(\frac{a}{b}+\frac{c}{d}\right)\left(\frac{e}{f}\right)=\left(\frac{a}{b}\right)\left(\frac{e}{f}\right)+\left(\frac{c}{d}\right)\left(\frac{e}{f}\right)$$

时,不妨假定 $b=d=e$.

如逕写 $\frac{ac}{c}=a$, $\frac{c}{bc}=b^{-1}$, 則 $\frac{a}{b}=ab^{-1}$. 如欲$(ab^{-1})(cd^{-1})=ef^{-1}$, 一个自然条件是存在两元素 b_1, c_1, 使 $b^{-1}c=b_1c_1^{-1}$, 即 $bb_1=cc_1$, 也即 b, c 有右公倍数. 由此可見,从环建体,有右公倍数这一条件是自然的.

在 $\frac{ac}{c}=a$ 的了解下,体 K 包有 R 作为其自己的子环,而在 $\frac{c}{bc}=b^{-1}$ 的了解下, 体 K 是包有 R 的最小体.

在交换环中, 任二元素显然有公倍数, 故在无零因子的情况下,就可以利用上述的理論,从环来建体. 最具体的例子是:从整数环到有理数域,从多項式环到有理函数域,从整函数环到半純函数域等等. 但是除了交换环是有右公倍数的以外, 是否还存在着有右公倍数的非交换环,下一节我們将回答这个問題.

§3 多項式环

命 K 为一体. 形如

$$f(x)=\sum_{i=0}^{n}a_ix^i \quad (a_0, a_1, \cdots, a_n\in K)$$

的式子称为不定子 x 的多項式. 若 $a_n\neq 0$, 則 n 称为这多項式的次数,記作 $\partial^0 f$.

設

$$g(x)=\sum_{i=0}^{m}b_ix^i.$$

我們可以定义两多項式的加和乘: