有限域

张远达

湖北教育出版社

有限域

张远达

*

湖北教育出版社出版　湖北省新华书店发行

湖北教育出版社印刷厂印刷

787×1092毫米32开本　2印张　1插页　42,000字

1985年5月第1版　1985年5月第1次印刷

印数：1—2.9000

统一书号：7306·63　　定价：0.55元

写在前面

代数学是数学中一个很重要的分支。近几十年的发展特别迅速，应用又非常广泛。于是人们要求学习代数学的愿望日渐增多且迫切，故写一本适宜广大搞应用科技工作者需要的代数读物确是刻不容缓。但代数的范围太广、内容又多，非短期所能如愿，于是考虑结果，乃选目前在应用上较广的《有限域》这个课题，着重谈《有限域》的几个极基本的问题，写的方法想尽量通俗一点，也就是希望一般有点高等数学基础常识的科技工作者以及中学教师甚至中学毕业同学都能看懂，藉以引起广大读者对学习代数的兴趣。由于个人学识浅，教学经验不够，虽然主观愿望是想做到上面的要求，恐实际情况并非如此。希望读者在实践过程中提出批评和指正，并希望今后有较好的且适宜于这方面的读者需要的书籍问世，这本小册子只是抛砖引玉。

武汉大学　张远达

目　录

凡学过一点高等代数的同志都知道群、环、体的意义。由于计算机科学的发展，有限多个元素所组成的体（简称有限体）的理论的重要性表现得非常显著，因此有必要将有限体中几个最基本的问题阐述透彻，以引起初学高等代数同志们的兴趣。

这本小册子解决五个问题。第一个问题是有限体必是可交换的，即对体中任二元 a，b 恒有 $ab=ba$ 之关系；因一般叫可换体为域，故要解决的第一个问题是有限体必为有限域。第二个问题是有限域 K 中所包含元素的个数一定等于某一个素数 p 的幂 p^n，这时就叫 K 的阶等于 p^n，记作 $|K|=p^n$（p 表某素数，$n\in N$ 表自然数的集合）。第三个问题是第二个问题的逆定理，也就是说对任意的素数 p 及任意的自然数 n，一定存在一个包含 p^n 个元素的体 K，因而 K 是有限体，也就是有限域(第一个问题)。第四个问题是第三个问题的延伸，也就是要解决的不仅是 p^n 阶域的存在性，如第三个问题所说的，而更着重解决 p^n 阶域的具体作法，即探索怎样实际地去作一个 p^n 阶域的方法。第五个问题要解决的是 p^n 阶域的唯一性，即以同构的意义言 p^n 阶域只有一个，也就是说凡 p^n 阶域都是同构的(同构的意义下面要解释的)。

1

体的意义及其简单性质

为了这本小册子的自给自足，还是将下面要用到的群、环的定义先介绍一下。

设有一个某类元素的集合G满足下列的四个条件：

1°. 在G内有一种运算法则（简记为“$\cdot$”，叫做“乘法”），使得对G中任二元a，b经过运算法则“$\cdot$”而结合的结果$a\cdot b$仍为G的元，即$a, b\in G\Longrightarrow a\cdot b\in G$；

2°. 结合律成立，即$a, b, c\in G\Longrightarrow(a\cdot b)\cdot c=a\cdot(b\cdot c)$；

3°. G中有单位元e，即对G的任何元x恒有$e\cdot x=x\cdot e=x$；

4°. G的每元x必有逆元x^{-1}，即对$\forall x\in G$恒有与x有牵连的G的元记作x^{-1}使得$x\cdot x^{-1}=x^{-1}\cdot x=e$，但$e$为3°中所说的$G$的单位元；

那末我们就叫集合G关于运算法则“$\cdot$”成群。

附注 1

运算法则“$\cdot$”简称“乘法”，是习惯的称呼，切不可把这习惯的称呼“乘法”误解为人们所熟知的普通的乘法。例如一切整数的集合Z关于加法运算“$+$”成群（这时，0（零）为单位元，$x\in Z$之逆元为$-x$），这里习惯的称呼乘法“$\cdot$”就是通常的加法，即以通常的加法“$+$”表示运算法则“$\cdot$”。同理，一切有理数的集合Q，一切实数的集合R，一切复数的集合

C 都是关于加法运算“+”成群。上面说的这些群都是把通常的加法“+”当做运算法则“·”。又如一切非零的有理数之集合 Q^* 关于通常的乘法“×”成群(这时，1 为单位元，$x\in Q^*$ 之逆元为 $\frac{1}{x}=x^{-1}$，即为 x 的倒数)；同理，一切非零的实数之集合 R^* 与一切非零的复数之集合 C^* 也都是关于通常的乘法“×”成群。但 Q^* 关于加法“+”不成群，Q 关于乘法“×”不成群(对 R，R^*，C，C^* 可类似地去处理)，这就说明了一集合 G 成群必定要伴随运算法则“·”而言。习惯上简称运算法则“·”为乘法并非人们所理解的一般乘法，它可以为一般的加法，也可以为一般的乘法，甚至可以为别的运算规则，这就要根据集合 G 的具体情况而言。

附注 2

今后恒以 Z，Q，R，C 分别表示一切整数，一切有理数，一切实数，一切复数的集合，它们关于加法“+”都成群，因而今后干脆叫它们为加群；同理叫 Q^*，R^*，C^* 都为乘群。

附注 3

集合 G 为群只是要求 a，$b\in G$ 时必有 $a\cdot b\in G$ 与 $b\cdot a\in G$，并不要求 $a\cdot b=b\cdot a$，这是应特别注意的一点。如果对 G 之任二元 x，y 恒有 $x\cdot y=y\cdot x$ 之关系，这时特地叫 G 为交换群，于是加群 Z，Q，R，C 及乘群 Q^*，R^*，C^* 均为交换群，但一切满秩 n 级矩阵(例如矩阵的元素为复数)的集合 G 关于矩阵的乘法也成群，它却是一个非交换群。凡是把群 G 的运算法则“·”写为加号“+”的群 G 统统叫加群；加群总是表示交换群，即恒有 $a+b=b+a$ 之关系，今后不再

申明了。运算法则写作乘法"×"或简写为"·"的群一般指非交换群，但并不排斥有为交换群的可能性，这些都应予以注意。

附注 4

设 G 为群(关于运算"·")，则 G 的单位元 e 仅有一个，又 G 的每元 x 的逆元 x^{-1} 也仅有一个。又据结合律 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$，易证一般的结合律成立，即若用递归公式 $\prod_{i=1}^{1} a_i=a_1$，$\prod_{i=1}^{n+1} a_i=\left(\prod_{i=1}^{n} a_i\right)\cdot a_{n+1}$ 定义多个元的结合积的意义，也不难证明 $\prod_{i=1}^{m} a_i\cdot\prod_{j=1}^{n} a_{m+j}=\prod_{k=1}^{m+n} a_k$，其实质意义是说两个结合积之积与它们所有因子在同一顺序下的结合积相等，例如 $(abc)(ef)=abcef$，于是 n 个元 a_1，a_2，…，a_n 所决定的一切结合积，只要这 n 个元之顺序不改变，不管在它们中间怎样添加括号或去掉括号，结果都一样，总是等于 $\prod_{i=1}^{n} a_i$。特当这些 a_i 都相等而为 a 时，则用幂 a^n 表示 $a_1a_2\cdots a_n=\underbrace{a\,a\cdots a}_{n\text{个}}$，叫 a^n 为 a 的 n 次幂。于是又易证 $a^na^m=a^ma^n=a^{m+n}$，$(a^n)^n=(a^n)^m=a^{mn}$。再定义 $a^0=e$，$a^{-n}=(a^{-1})^n$，$n\in N$，易知公式 $a^na^m=a^ma^n=a^{m+n}$ 及 $(a^m)^n=(a^n)^m=a^{mn}$ 对任意的 m，$n\in Z$ 皆成立，因而又有 $a^{-n}=(a^n)^{-1}$。又由逆元之唯一性可知 $(ab)^{-1}=b^{-1}a^{-1}$，且归纳地可知 $(a_1a_2\cdots a_n)^{-1}=a_n^{-1}\cdots a_2^{-1}a_1^{-1}$。特当 G 为交换群时，则知任 n 个元之结合积的结果只与这 n 个元自身有关，而与其先后次序无关，因而又有 $(ab)^n=a^nb^n$，$n\in Z$

〔同理，当 G 虽非交换群时，只要 $ab=ba$，也易证 $(ab)^n=a^nb^n$〕。注意加群恒表交换群，这时乃用符号 $\sum_{i=1}^{n} a_i$ 代替 $\prod_{i=1}^{n} a_i$，而用 na 表 a^n，由是就有 $ma+na=(m+n)a$，$m(na)=(mn)a$ 及 $n(a+b)=na+nb$。上述一切，在群论书里都载有证明，不难，我们都承认它，需要时则直接引用。

群的意义已明确，再来介绍环的概念。所谓一集合 R 为环，指的是它满足下列各条件：

1°. R 是一个加群〔于是 R 是交换的，即 $a, b\in R\Longrightarrow a+b=b+a(\in R)$，且 R 有零元 0 为加群 R 之单位元，并每 $x\in R$ 有唯一的元 $-x$ 使 $x+(-x)=0$〕；

2°. R 内还有乘法“$\cdot$”运算，且关于乘法的结合律成立，即 $a, b, c\in R\Longrightarrow a\cdot b\in R$ 并 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$；

3°. R 中加法与乘法间的分配律成立，即 $a, b, c\in R\Longrightarrow a\cdot(b+c)=a\cdot b+a\cdot c$ 与 $(b+c)\cdot a=b\cdot a+c\cdot a$。

附注 1

条件 2° 只是说 $a, b\in R\Longrightarrow a\cdot b\in R$ 与 $b\cdot a\in R$，并不要求有 $a\cdot b=b\cdot a$，也就是说环 R 一般不要求乘法的交换律成立，这是应注意的第一点，因此条件 3° 中分配律必需强调两个等式。当环 R 中任二元 a, b 恒有关系式 $a\cdot b=b\cdot a$ 时，就特地叫 R 为可换环（或交换环），这时分配律 3° 中只要求一个等式即可，因为据交换性易知 3° 中有一式成立，则另一式亦成立。又环 R 一般不要求它有元 e 使 $e\cdot x=x\cdot e=x$ 对任 $x\in R$ 是成立的，这是应注意的第二点；特当 R 有这样的元 e 时，就叫 e 为 R 的单位元，而叫 R 是具有单位元的环，且

易知单位元如存在则必唯一。

附注 2

$\forall x \in R$，有 $x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0$，故由加群 R 中零元的唯一性则不得不有 $x \cdot 0 = 0$，同理也有 $0 \cdot x = 0$。这说明了环 R 之零元 0 与 R 之任何元 x 不论左乘或右乘，其结果恒为 R 之零元 0。这是环中零元 0 的特性，是应注意的。但尤要注意的是：环 R 可能有元 a, b（均非零元），即 $a \neq 0$，$b \neq 0$，而 $a \cdot b = 0$ 的可能却是有的。

有了群、环的定义，下面可谈体的概念。

定义 1 设集合 K 至少包含两个元素，在 K 内又定义了两个运算规则“$+$”与“$\cdot$”分别叫加法与乘法，且满足下列的三个条件：

1°. K 为加群（因之有 $0 \in K$），

2°. K 中去掉元素 0 后之集合 K^* 关于乘法“$\cdot$”为乘群（因之有 $1 \in K$——今后恒用符号 1 表示乘群的单位元），

3°. “$+$”与“$\cdot$”间的分配律成立，即 $\forall a, b, c \in K$ 恒有 $a \cdot (b+c) = a \cdot b + a \cdot c$ 与 $(b+c) \cdot a = b \cdot a + c \cdot a$，

我们这时就叫集合 K 为体。特别当体 K 之任二元 a，b 恒有 $a \cdot b = b \cdot a$ 之关系时，就叫 K 为可换体，可换体简称域。

如同上面讲环之定义以后的附注 2 中所说利用分配律，可证体 K 中零元 0 不论用 K 中任何元 x 左、右乘之，其结果恒为零元 0。可是对体 K 言，其逆也成立，具体地说，有下面的

性质 1 体 K 中二元之积等于 0 的充要条件是这二元中至少有一个为零元 0。

证明：要解决的问题是由 $x \cdot y = 0$ 必得 $x = 0$ 或 $y = 0$，

二者至少有一。

若 $x\neq 0$，则 $x\in K^*$，故存在 $x^{-1}\in K^*$ 使 $x^{-1}\cdot x=1$，因而从 $x\cdot y=0$ 得 $x^{-1}\cdot(x\cdot y)=x^{-1}\cdot 0=0$，于是再利用乘法的结合律得 $0=x^{-1}\cdot(x\cdot y)=(x^{-1}\cdot x)\cdot y=1\cdot y=y$。证毕。

由于 $0\cdot x=x\cdot 0=0$ 对任 $x\in K$ 成立，可知当 a，b，c 中有一为 0 时，易知 $(a\cdot b)\cdot c=0$ 及 $a\cdot(b\cdot c)=0$，故必 $a\cdot(b\cdot c)=(a\cdot b)\cdot c$。这说明了乘法的结合律在体 K 中是成立的，因而体 K 当然也为环，且乘群 K^* 之单位元 1 也是体 K 自身的单位元。即有

性质 2 体 K 是一个具有单位元的环。

下面介绍两个例子，它们是体之理论的基础。

例 1 一切有理数之集 Q 为可换体，即为域。

例 2 $z_p=\{0,\ 1,\ 2,\ \cdots,\ p-1\}\ (mod\ p)$ 也是域，即素数 p 的完全剩余系关于模 p 的加法与乘法而言是一个域。

例 1 由定义即可验证，再据数论知识也易验证例 2。

附注 1

在体的定义中之所以强调体 K 至少包含两个元素的原因是为了说明加群之单位元 0 与乘群之单位元 1 互异。

附注 2

有理数域 Q 之单位元 1 时任意的自然数 n 皆有 $1\cdot n\neq 0$，但域 z_p 之单位元 1 却有 $p\cdot 1=0$，即 $p\cdot 1\equiv 0(mod\ p)$。需注意的是：当 n 为合数时，模 n 之完全剩余系 $z_n=\{0,\ 1,\ \cdots,\ n-1\}$ 是一个有零因子的环〔因 $n=n_1n_2$，$1<n_i<n$，故 $n_i\neq 0\ (mod\ n)$，但 $n_1n_2\equiv 0(mod\ n)$；简表为 $n_1\neq 0$，$n_2\neq 0$，但 $n_1n_2=0$〕，故 z_n 非体。

附注 2 中域 Q 及 z_p 之单位元所具的性质对任意的体言

皆真，即有次

定理 1 设 K 为一体，其单位元表以 1，则下列二条必有一成立：

i) 不论 n 为任何自然数，恒有 $n1 \neq 0 (\in K)$，

ii) 有一素数 p 使 $p \cdot 1 = 0$。

证明：如对任 $n \in N$，皆有 $n1 \neq 0$，问题就解决了，即 i) 成立。若不然，即存在某 $n \in N$ 使得 $n1 = 0$，则在这样一些自然数 n 中必有一个最小的数设为 m，使得 $m1 = 0$，于是 $m > 1$；假若这 m 为合数，如 $m = m_1 m_2$，$1 < m_i < m$，则 $0 = m1 = m_1 m_2 1 = (m_1 1) \cdot (m_2 1)$，而据上述性质 1 可知或 $m_1 1 = 0$ 或 $m_2 1 = 0$，二者必至少有一，这都和 m 为最小之意义的假定相矛盾，不可。故 m 为素数。证完。

定理 1 说明了体之单位元的特点，故有

定义 2 设 K 为体，若有素数 p 使 $p1 = 0$，则叫体 K 的特征数为 p；如不然，即对任 $n \in N$ 恒有 $n1 \neq 0$，就叫 K 之特征数为 0（或 ∞）。前者记作 $\mathrm{char}\, K = p$，后者记作 $\mathrm{char} K = 0$ 或 ∞。

性质 3 设 $\mathrm{char}\, K = p$，则 $n1 = 0$ 的充要条件是 $p \mid n$。

证明：因有唯一组 q，$r \in Z$ 使 $n = qp + r$ 且 $0 \leqslant r < p$，故 $n1 = qp1 + r1 = q(p1) + r1 = 0 + r1 = r1$，于是 $n1 = 0 \Longleftrightarrow r1 = 0$；但 $0 \leqslant r < p$，故由 $\mathrm{char}\, K = p$ 之意义即知 $r1 = 0 \Longleftrightarrow r = 0$，因而 $n1 = 0 \Longleftrightarrow r = 0$ 即 $p \mid n$。证完。

性质 4 设 $\mathrm{char}\, K = p$，则对任 $x \in K$ 恒有 $px = 0$。

证明：$px = \underbrace{x + x + \cdots + x}_{p\text{个}} = \underbrace{1 \cdot x + 1 \cdot x + \cdots + 1 \cdot x}_{p\text{个}} =$

$= \underbrace{(1+1+\cdots+1)}_{p\text{个}} \cdot x = (p1) \cdot x = 0 \cdot x = 0$。证毕。

下面再介绍子群、子环及子体与同构的概念。

定义 3 设群 G 的子集合 H 关于群 G 的运算法则仍成群时，就叫 H 为 G 的子群。同样，环（或体）的子集 R' 关于 R 中的加法与乘法而言仍成环（或体）时，就叫 R' 为 R 的子环（或子体）。

例如 Z 为 Q 的子群（以加群而言）；Q^* 显然为 Q 的子集，但不为 Q 的子群（因 Q 为加群，Q^* 非加群而只为乘群）；又 $z_p=\{0, 1, 2, \cdots, p-1\}$ 虽为域，但非 Q 的子域（尽管 z_p 为 Q 的子集）；可是 Q 为 R 的子域，等等。这些概念必需弄清。

定义 4 设 K 与 K' 是两个体。K 的元素为 a, b, c, $\cdots$, x, y, $\cdots$，而 K' 的元记为 a', b', c', $\cdots$, x', y', $\cdots$。如果找得着一种方法（叫对应方法）使 K 的每元 a 有唯一的一元 $a'\in K'$ 相对应（叫 a' 为 a 的像，而叫 a 为 a' 的原像），且 K' 的每元也有唯一的原像（简记这关系为 $a\rightleftarrows a'$），并满足下列的二个条件：

1°. $a\rightleftarrows a'$, $b\rightleftarrows b' \Longrightarrow a+b\rightleftarrows a'+b'$,

2°. $a\rightleftarrows a'$, $b\rightleftarrows b' \Longrightarrow a\cdot b\rightleftarrows a'\cdot b'$,

我们就说 K 与 K' 同构，表写为 $K\cong K'$。

同样，对群或环也可类似地定义同构的概念。例如 R 为加群，R^+为一切正实数所组成的乘群；若 $a\in R^+$，取 a 之对数 $\log a=a'\in R$，我们已知每个 $a\in R^+$ 必可唯一地决定一个 $a'=\log a\in R$，且对于每个 $x'\in R$ 又必有唯一个 $x\in R^+$ 使 $x'=\log x$（令 $x=10^{x'}$）。现在所谓的对应方法如令为“取对数”，

则有 $a \rightleftarrows a'$；由于 $a \rightleftarrows a'$ 及 $b \rightleftarrows b'$（即 $a' = \log a$，$b' = \log b$），马上可知 $a' + b' = \log a + \log b = \log ab$，即 $ab \rightleftarrows a' + b'$，这说明了 $R^+ \cong R$。

由体的同构意义，可知当两个体同构时，它们没有实质性的差异，如果硬要说他们有差异，那不过是各个的元素所采用的符号不同而已，但运算的结果完全类似。因此，往往把同构的体视为同一体。对群、环的同构亦可这样看待，据上段已得知的 $R^+ \cong R$，可知一切正实数之集 R^+ 与一切实数之集 R 是一回事，只要在 R^+ 内把乘法视为运算法则，而在 R 内把加法当作运算方法。

再来解决体理论中极基本的结果。

定理 2 任何体 K 一定包含一个子域，当 $\mathrm{char}\, K = 0$ 时，与 Q 同构；当 $\mathrm{char}\, K = p$ 时与 z_p 同构。

证明：先设 $\mathrm{char}\, K = 0$，于是 $n \in Z$ 且 $n \neq 0$ 时就有 $ne \neq 0$（暂采用 e 表示体 K 的单位元，便于下面论证时容易区别）。$\forall m \in Z$，易知 $(me) \cdot (ne) = (mn)e = (nm)e = (ne) \cdot (me)$，故从 $ne \neq 0$ 知 $(ne)^{-1} \in K$，而又有

$$(ne)^{-1} \cdot (me) \cdot (ne) \cdot (ne)^{-1} = (ne)^{-1} \cdot (ne) \cdot (me) \cdot (ne)^{-1},$$

即 $(ne)^{-1} \cdot (me) = (me) \cdot (ne)^{-1}$。这说明了当 $n \neq 0$ 时 $(ne)^{-1} \cdot (me) = (me) \cdot (ne)^{-1}$，故干脆记为 $\frac{me}{ne} = (ne)^{-1} \cdot (me) = (me) \cdot (ne)^{-1}$，即符号 $\frac{me}{ne}$ 的意义明确。今作 K 的一子集 $\overline{Q} = \left\{ \frac{me}{ne} \middle| m,\ n \in Z \text{ 且 } n \neq 0 \right\}$，由于 $\frac{me}{ne} = \frac{m'e}{n'e}$（$n$，$n'$，$m$，$m' \in Z$ 且 $nn' \neq 0$）的充要条件是 $(ne)^{-1} \cdot (me) = (n'e)^{-1} \cdot (m'e)$，故为 $(n'e) \cdot (me) = (ne) \cdot (m'e)$，即 $(n'm)e = (nm')e$，就知道

当令 Q 中 $\frac{m}{n}$ $(m,\ n\in Z,\ n\neq 0)$ 对应于 $\overline{Q}$ 的元 $\frac{me}{ne}$ 时，那末这种对应的方法就建立了 Q 与 $\overline{Q}$ 间的一一对应关系，也就是说在上述对应方法之下，得知 Q 中有理数 $\frac{m}{n}$ 在 $\overline{Q}$ 内有唯一个象元 $\frac{me}{ne}$，且 $\overline{Q}$ 中每元 $\frac{me}{ne}$ 又只有唯一个原像 $\frac{m}{n}$。

其次，从 $\frac{m}{n}\rightarrow\frac{me}{ne}$，$\frac{m'}{n'}\rightarrow\frac{m'e}{n'e}$，又得 $\frac{m}{n}+\frac{m'}{n'}=\frac{mn'+m'n}{nn'}\rightarrow\frac{(mn'+m'n)e}{(nn')e}=((nn')e)^{-1}\cdot(mn'+m'n)e=(ne)^{-1}\cdot(n'e)^{-1}\cdot(mn'+m'n)e=(ne)^{-1}\cdot(n'e)^{-1}\cdot[(me)\cdot(n'e)+(m'e)\cdot(ne)]=(ne)^{-1}\cdot(me)+(n'e)^{-1}\cdot(m'e)=\frac{me}{ne}+\frac{m'e}{n'e}$，以及

$$\frac{m}{n}\cdot\frac{m'}{n'}=\frac{mm'}{nn'}\rightarrow\frac{(mm')e}{(nn')e}=((nn')e)^{-1}\cdot((mm')e)$$
$$=(ne)^{-1}\cdot(n'e)^{-1}\cdot(me)\cdot(m'e)=(ne)^{-1}\cdot(me)\cdot(n'e)^{-1}(m'e)$$
$$=\frac{me}{ne}\cdot\frac{m'e}{n'e}。$$

于是 $\overline{Q}$ 与 Q 的差别只是把 Q 的元 $\frac{m}{n}$ 的分子 m 分母 n 分别改为 me 与 ne，且 $\frac{me}{ne}$ 间的加法与乘法运算可以认为先去掉一切 e 而只作为 Q 中的加法和乘法运算，但将算出的结果 $\frac{l}{k}\in Q$ 再改为 $\frac{le}{ke}$ 即可。由 Q 为域可知 $\overline{Q}$ 亦必为域，且有 $Q\cong\overline{Q}$，即证明了特征数 0 的体 K 必定包含一个与有理数域 Q 成同构的子域 $\overline{Q}$。

再考虑 $\mathrm{char}\,K=p$。这时作 K 的子集

$$\bar{z}_p=\{e,\ 2e,\ \cdots,\ (p-1)e,\ pe=0\},$$

并作 z_p 到 $\bar{z}_p$ 的映射 τ：$i\to i^\tau=ie(i=0,\ 1,\ 2,\ \cdots,\ p-1)$。若 $i,\ j\in Z_p$，且 $i^\tau=j^\tau$，则因 $i^\tau=ie,\ j^\tau=je$，故 $i^\tau=j^\tau$ 的充要条件是 $ie=je$，即 $(i-j)e=0$，因而据性质 3 得知等价的条件为 $p\mid(i-j)$，于是再从 $i,\ j\in Z_p$ 可知不得不有 $i=j$，这说明了映射 τ 是一一的且为可逆的，即 Z_p 的每个元经映射 τ 有唯一个象元在 $\bar{z}_p$ 内，且 $\bar{z}_p$ 的每个元又只有一个原像属于 z_p。

其次，$i,\ j\in z_p\Longrightarrow i+j\equiv k(\mathrm{mod}\ p)$，$i\cdot j\equiv l(\mathrm{mod}\ p)$，而有 $k,\ l\in z_p$，于是 $i+j=qp+k$，$i\cdot j=q'p+l$，$q,\ q'\in Z$，故 $(i+j)e=(qp+k)e=q(pe)+ke=ke$，同理 $(ij)e=le$，这说明了 $(i+j)^\tau=k^\tau=ke=(i+j)e=ie+je=i^\tau+j^\tau$，$(ij)^\tau=l^\tau=le=(ij)e=(ie)\cdot(je)=i^\tau\cdot j^\tau$，故 $z_p\cong\bar{z}_p$，因 $\bar{z}_p$ 为 K 的子域，即得特征数为 p 的体 K 一定包含一个与 z_p 成同构的子域 $\bar{z}_p$。证完。

这定理 2 当然同时也说明了这样一个问题，即若把同构的体视为同一体时，可知 Q 是特征数为 0 的最小的体，即特征数为 0 的任何体一定包含 Q，因此叫 Q 为特征数是 0 的素体（实际是素域）；同样可知 z_p 是特征数为 p 的最小的体，即特征数 p 的体一定包含 z_p 为子体且还是子域，因而叫 z_p 为特征数是 p 的素域。

2

分圆多项式的特性

已知 $x^n=1$ 有 n 个根 $\omega^k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$ $(k=0,\ 1,\ 2,\ \cdots,\ n-1)$，式中 $\omega=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$。又易知 ω 具有下面二个性质：

(i) $\omega^n=1$，

(ii) $\omega^s\neq 1$ 在 $0<s<n$ 时。

于是已知 $x^n=1$ 的根中确有一根 $\omega=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$ 具有性质(i)与(ii)。当然，方程 $x^n=1$ 可能还有别的根 $\omega^k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$ 具有性质 (i) $(\omega^k)^n=1$ 及(ii) $(\omega^k)^s\neq 1$ 在 $0<s<n$ 时。$x^n-1=0$ 之 n 个根中凡具性质(i) $(\omega^k)^n=1$ 及(ii) $(\omega^k)^s\neq 1$，在 $0<s<n$ 时，根 ω^k 统统叫做 1 的 **n 次本原根**。

下面来探索 $x^n-1=0$ 的 n 个根 $\omega^k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$ $(k=0,\ 1,\ 2,\ \cdots,\ n-1)$ 中哪些为本原根。

由于 1 的任一个 n 次根为 ω^k，今令 $(k,\ n)=d$，则有 $(\omega^k)^{\frac{n}{d}}=(\omega^n)^{\frac{k}{d}}=1$，故当 $d>1$ 时就说明了 ω^k 不是 1 的 n 次本原根，于是若 ω^k 为 1 的 n 次本原根就不得不有 $(k,\ n)=1$。反之，当 $(k,\ n)=1$ 时，则从 $1=(\omega^k)^s$ 得 $1=\omega^{ks}=$