关于最大公因数与最小公倍数概念的推广及其应用举例

周 泽 滋

提 要 本文运用通常最大公因数与最小公倍数的性质以引入非空整数组的最大公因数与最小公倍数的概念，并运用它引入群元素的特征数和环与域的特征数，此外论证了任意非空整数组必存在最大公因数和最小公倍数，且对于确定的非空整数组它们是唯一的

1. 问题的提出

最大公因数与最小公倍数已是人们非常熟悉的两个概念，但0，0的最大公因数是什么？它们有最小公倍数吗？任意多个不全为零的整数必有最大公因数，但它们有最小公倍数吗？在不少著作中的回答是："(0，0) 沒有定义"，[1],[2]当然 [0，0] 更沒有定义了，能否使它们有合理的意义呢？在近世代数中关于域的特征数（示性数）的定义其描述中有如下之说：如果域F的单位元的某质数p倍是零，则称F的特征数是p，否则称F的特征数是0，[3]、[4]、[5]（或无穷大）[6]、[7]。这里自然要问，否则称F的特征数是-1.（即不是0）行不行？为什么？再如对循环群的性质描述中，往往总是就群的阶是有限的或阶是无穷的情形分别描述，其统一描述的范围能否扩大一些呢……。后面我们将会看到这些问题与推广了的最大公因数和最小公倍数概念不是沒有关系的。在下面的讨论中，我们假定I表示全体自然数所成的集，Z表示全体整数所成的集。

关于在自然数范围内的这两个概念及其性质在一些数论的书中已讨论得比较详细了，我们只将其主要的列出如下：

1) 设$a, b \in I$，如果a能整除b，则称a是b的约数，称b是a的倍数，并记作$a \mid b$.

用S表示自然数的数组（元数可能是有限，也可能是无穷，且数组中的数可以是相同的），如果S至少含有一个数，则称S为非空自然数组*并记作

$$\phi \neq S \subseteq I.$$

2) 设$\phi \neq S \subseteq I$，如果$d \in I$对于任何$a \in S$总有$d \mid a$，则称d为S的公约数。

3) 设$\phi \neq S \subseteq I$，如果有$m \in I$对于任何$a \in S$总有$a \mid m$，则称S有公倍数，且称m为S的一个公倍数。

注意：任意非空自然数组必有公约数，但元数是无穷的非空自然数组不一定有公倍

* 如果把自然数换成整数，则称S为非空整数组，并记作$\phi \neq S \subseteq Z$.

本文1983年4月26日收到

数。

4) S的公约数中的最大者称为S的最大公约数。

自然数 a，b，…，l 的最大公约数用$(a,b,\cdots,l)$ 表示

5) S的任一公约数都是S的最大公约数的约数。

6) 如果非空自然数组S有公倍数，则其中最小者称为S的最小公倍数。

有限个自然数 a，b，…，l 的最小公倍数用$[a,b,\cdots,l]$ 表示。

7) 设m是S的公倍数，那末m是S的最小公倍数其充要条件是S的每个公倍数都是m的倍数。

8) 设 $\phi\neq S\subseteq I$，且S具有公倍数，记S的公倍数所成的集为M，则下面的关系式成立：

S的最小公倍数$=M$的最大公约数。

2. 两个概念在整数范围内的推广

定义 1 设 a，$b\in Z$，如果存在 $c\in Z$使得 $ac=b$，则称 a 为 b 的因数，称 b 为 a的倍数，也记作 $a\mid b$（以后记号 $a\mid b$ 都是指 a 是 b 的因数）。

根据定义，因数、倍数显然有以下性质：

1° $a\mid b$ 同时 $b\mid a\Longleftrightarrow\mid a\mid=\mid b\mid$,

2° $a\mid b\Longleftrightarrow a\mid\mid b\mid\Longleftrightarrow\mid a\mid\mid b\Longleftrightarrow\mid a\mid\mid\mid b\mid$,

3° 0 是任意整数的倍数，但不是任何非零整数的因素。

4° 任何整数都以 1，-1 及其自身为其因数，即它是 1，-1 及其自身的倍数。

定义 2 设 $\phi\neq S\subseteq Z$，如果 $d\in Z$ 对任何 $a\in S$ 总有 $d\mid a$，则称 d 为 S 的公因数。

关于公因数显然有：

1° 任意一个非空整数组 S 至少有两个公因数 1 及 -1.

2° 若 d 是 S 的公因数，则 $\mid d\mid$ 也是 S 的公因数，反之亦然。

3° 当且仅当 S 的元全为 0 时，0 是 S 的公因数。

以下总假定用 S^*表示 S 中的元都取绝对值所成的整数组，用 S_1 表示 S^* 中去掉零元所成的整数组。显然有

定理 1 d 是 S 的公因数其充要条件是 d 是 S^*的公因数。

定理 2 若 S_1 非空，那末 d 是 S^* 的公因数其充要条件为 d 是 S_1 的公因数。

证 必要性是显然的，只证充分性。

由于 d 是 S_1 的公因数，而 d 也是 0 的因数，故 d 是 S^* 的公因数。

系 2.1 如果 S_1 非空，则 d 是 S 的公因数其充要条件为 d 是 S_1 的公因数。

系 2.2 如果 S_1 非空，则 S 的公因数中有最大者，这最大者就是 S_1 的最大公约数 d，且 S 的任何公因数都是 d 的因数。

证：由于 S_1 非空，故 S_1 有最大公约数（指在自然数范围讨论的），记为 d（显然 $d\geqslant 1$）由系 2.1 知 d 是 S 的公因数，如果 S 有比 d 大的公因数，设为 d_1，则 $d_1>d\geqslant 1$

由系 2.1 知 d_1 是 S_1 的公约数，这与 d 是 S_1 的最大公约数矛盾。

今设 d' 是 S 的公因数，则 $|d'|$ 也是 S 的公因数，而 S_1 非空，故 $d'\neq 0$ 从而 $|d'|$ 是 S_1 的公约数，故 $|d'|$ 是 d 的约数，所以 d' 是 d 的因数。

显然如果 $S_1=\phi$，即 S 中的数全为 0，则 S 的一切公因数都是 S 的公因数 0 的因数。

定义 3 设 S 是一个非空整数组，如果整数 d 满足如下两条件：

1) d 是 S 的非负公因数，

2) S 的任何公因数都是 d 的因数。则称 d 是 S 的最大公因数。

根据定义知

全 0 的整数组 S 的最大公因数是 0.

由系 2.2 知不全为 0 的非空整数组 S 总存在最大公因数。

容易证明非空整数组的最大公因数是唯一的。从而有

定理 3 任意非空整数组的最大公因数必定存在且唯一。

定义 4 设 $\phi\neq S\subseteq Z$，如果 $m\in Z$ 对任何 $a\in S$ 总有 $a\mid m$，则称 m 为 S 的公倍数。

根据定义显然有

1° 0 是任意非空整数组的公倍数。

2° 如果整数组 S 含有数 0，则 S 只有唯一的一个公倍数 0。

3° 如果 m 是 S 的公倍数，则 $|m|$ 也是 S 的公倍数。

定义 5 设 S 是一非空整数组，如果整数 m 满足：

1) m 是 S 的非负公倍数。

2) S 的任何公倍数都是 m 的倍数。则称 m 为 S 的最小公倍数。

根据定义显然有

1° 如果 S 中含有数 0，则 S 的最小公倍数是 0.

2° 如果 S 是有限的非空自然数组，则此定义与自然数范围内最小公倍数的定义是等价的。

定理 4 设 S 是一非空整数组，则 S 的最小公倍数必存在且唯一。

证：分两种情况讨论：

1) 如果 S 中含有数 0，则 S 有唯一的公倍数 0，此时 S 有唯一的一个最小公倍数 0.

2) 如果 S 不含数 0，则 $\phi\neq S^*=S_1\subseteq I$ 由于在整数范围内有

m 是 S 的公倍数$\Longleftrightarrow|m|$ 是 S 的公倍数$\Longleftrightarrow|m|$ 是 S^* 的公倍数。

故 S 有非 0 的公倍数$\Longleftrightarrow S^*$ 在自然数范围内有公倍数，

故若 S^* 在自然数范围内没有公倍数，则 S 在整数范围内只有唯一的一个公倍数 0，从而此时 S 有唯一的一个最小公倍数 0，否则 S^* 在自然数范围内有公倍数，则 S^* 在自然数范围内有最小公倍数，设为 $m(\geqslant 1)$，据因数的性质 2° 知 m 是 S 的公倍数，今设 m' 是 S 的任意一个公倍数，如果 $m'=0$，则 $m\mid m'$，如果 $m'\neq 0$，则 $|m'|$ 也是 S^* 的公倍数，今 m 是 S^* 在自然数范围内的最小公倍数，故 $m\mid|m'|$，从而 $m\mid m'$，故 m 是 S 的最小公倍数，此时其唯一性是明显的。 证毕

据最小公倍数和最大公因数定义显然有

定理 5 设 $\phi \neq S \subseteq Z$，S 的所有公倍数所成的集记为 M，S 的所有公因数所成的集记为 D，则

S 的最小公倍数 $=M$ 的最大公因数。

S 的最大公因数 $=D$ 的最小公倍数。

如果 $a, b, \cdots, l \in Z$，

用 $(a,b,\cdots,l)$ 表示 $a,b,\cdots,l$ 的最大公因数。

用 $[a,b,\cdots,l]$ 表示 $a,b,\cdots,l$ 的最小公倍数。

3. 应用举例

1. 群的元素的特征数

定义 设 $<G,\cdot>$ 为一群，$a\in G$，记

$$S=\{m \mid a^m=e,\ m\in Z\}^*.$$

则称 S 的最大公因数 d 为 a 的特征数，其中 e 是 $<G,\cdot>$ 的单位元。

定理 1 设 $<G,.>$ 为一群，$a\in G$，如果 a 的特征数为 n，则 $a^n=e$，且当 $n=0$ 时，(a) 为无穷群；当 $n\neq 0$ 时，则 n 是使 $a^m=e$ 的 m 中的最小正整数，且 (a) 的元数是 n。

证：记 $S=\{m \mid a^m=e,\ m\in Z\}$。

当 $n=0$ 时，显然 $a^n=e$，此时 S 只含有一个数 0，即对任何非 0 整数 m，$a^m\neq 0$，从而当 $i\neq j$ 时，$a^i\neq a^j$，故此时 (a) 为无穷群。

当 $n\neq 0$ 时，则 S 中必含有非零整数，记 S 中最小正整数为 m_0。则对任意 $m\in S$，存在 $p,q\in Z$ 使得

$$(m_0,m)=pm_0+qm,$$

从而
$$a^{(m_0,m)}=a^{(pm_0+qm)}=(a^{m_0})^p(a^m)^q=e,$$

故
$$(m_0,m)\in S.$$

因 m_0 是 S 中的最小正整数，故 $m_0\leqslant(m_0,m)$ 但 $0<(m_0,m)\leqslant m_0$，故 $n=m_0$，从而 $a^n=e$。显然此时 (a) 的元数是 n。 证毕

定理 2 设循环群 (a) 中 a 的特征数为 n，则 $(a^t)=(a^{(t,n)})$，又 $a^m\in(a^t)$ 其充要条件为 $(t,n)\mid m$。

证：由于 $(t,n)\mid t$，故 $a^t\in(a^{(t,n)})$ 从而 $(a^t)\subseteq(a^{(t,n)})$。

另一方面，由于 a 的特征数为 n，则 $a^n=e\in(a^t)$ 对于 t，n 必有 p，$q\in Z$ 使得

$$(t,n)=pt+qn$$

故
$$a^{(t,n)}=a^{(pt+qn)}=(a^t)^p(a^n)^q\in(a^t)$$

从而
$$(a^{(t,n)})\subseteq(a^t)$$

所以
$$(a^t)=(a^{(t,n)}).$$

* 显见 $0\in S$，从而 S 非空，且当 $a^m=e$ 时有 $a^{|m|}=e$。对于加群 $<G,+>$，则 $S=\{m \mid ma=0,\ m\in Z\}$ 其中 0 是 G 的零元素。

后半部份其充分性是显然的，只证必要性，

由于 $a^m\in(a^t)$，故存在整数 p 使得

$pt\equiv m(mod\ \ n)$*，从而存在整数 q 使得

$$pt+qn=m.$$

今 $(t,n)\mid t$，$(t,n)\mid n$，从而 $(t,n)\mid m$.

证毕

定题 3 设循环群(a)中 a 的特征数为 n，则

$(a^t)=(a^r)$ 的充分必要条件是 $(t,n)=(r,n)$.

证：充分性，若 $(t,n)=(r,n)$，由定理 2 有$(a^t)=(a^{(t,n)})=(a^{(r,n)})=(a^r)$.

必要性，由于$(a^t)=(a^{(t,n)})$，$(a^r)=(a^{(r,n)})$，若$(a^t)=(a^r)$，则 $(a^{(t,n)})=(a^t)=(a^r)=(a^{(r,n)})$ 从而 $a^{(t,n)}\in(a^r)$

由定理 2 知 $(r,n)\mid(t,n)$

同理由于 $a^{(n,n)}\in(a^t)$ 知 $(t,n)\mid(r,n)$，

故必有 $(t,n)=(r,n)$. 证毕，

2. 环和域的特征数（示性数）

定义 1 设$<G,+,\cdot>$为一环，关于加群$<R,+>$的元素 a 的特征数记为d_a，则称 $S=\{d_a\mid a\in R\}$ 的最小公倍数 m 为环$<R,+,\cdot>$的特征数（示性数）。

定义 2 设 e 是域 F 的单位元，则称$<F,+>$中 e 的特征数为域 F 的特征数（示性数）。

容易证明这样定义环和域的特征数与习惯的定义法其效果是一致的，由于示性数应为揭示其特征的数，故应由环和域所具有的特征所确定，因此这样定义避免了示性数 0 的硬性规定。

3. 一个完全格的例子

我们知道自然数集 I 如果偏序关系 $a\leqslant b$ 为 a 是 b 的约数并记作 $a\mid b$，则$<I,\mid>$是一个格，但不是定全格。

今对非负整数全体的集 Z_1 规定偏序关系 $a\leqslant b$ 是指 a 是 b 的因数，也记作 $a\mid b$，则$<Z_1,\mid>$为一格，且是完全格，其全元素是 0（而不是 1），其零元素是 1（而不是 0）。

4. 结束语

1° 由于因数与约数之别仅在于 0 可作因数，但不能作约数，从而公约数可作除数，而公因数就不一定能作除数了。

2° 对最大公因数与最小公倍数的这种定义法在一些著作[6],[7]中也能找到但那里的定义只限于两个整数的，而不是一个非空整数组的，本文还论证了任意非空整数组的最大公因数与最小公倍数是存在的且是唯一的。

3° 完全格的例子$<Z_1,\mid>$揭示了 0 的特殊性，在通常的大小次序下，0 在 Z_1 中

* $a=b(mod\,n)$ 是指 n 是 $a-b$ 的因数

是“最小的”数，但在偏序关系“|”下，0则是Z_1中“最大的”数，因此在群论中用a的特征数代替a的阶是合理的，它更能揭示a的特征。

4° 全文对两个概念的引入及结论的证明所采用的都是一些初等的方法，因此用以定义域的特征数是可行的。

本文承汪浩教授给予审阅，对于他的鼓励与支持，在此谨致谢意。

参 考 文 献

[1] U. Dudley [周仲良译]《基础数论》 上海科技出版社 1980年

[2] 維诺格拉陀夫[裘光明译]《数论基础》 北京高等教育出版社 1956年

[3] Marvin Marcus: Introduction to modern algebra New york Dekker 1978

[4] 熊全淹：《近世代数》 上海科技出版社 1978年

[5] 谢邦杰《抽象代数》 上海科技出版社 1982年

[6] N. Jacobson[黄缘芳译]《抽象代数学》卷 1 科学出版社 1960年

[7] G. 伯克霍夫 S. 麦克莱恩 [王連祥 徐广善译]《近世代数概论》 人民教育出版社 1979年

A Generalized Concept of Greatest Common Factor and Least Common Multiple with Applied Examples

Zhou Ze-Zi

Abstract

In this paper, we have given a concept of greatest common factor and least common multiple in the nonempty set of integers with the nature of usual greatest common factor and least common multiple. Applying this concept, we incorpoate the characteristic number of a group's element and the characteristic numbers of a ring and field. Besides, we have proved that the greatest common factor and the least common muliple are existential for every nonempty set of integers and unique for definite nonempty set of integers.