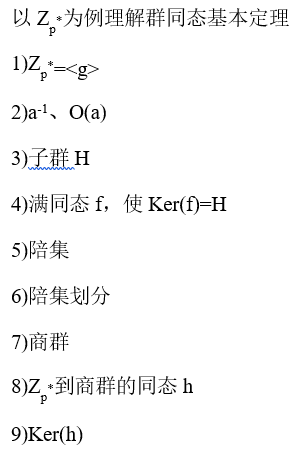
群同态基本定理：

设f是<G; \* >到<H; Δ>群同态，令K=Ker(f)。则

1. 对于任意的a∈G，有f(aK)={f(a)}
2. G/K与f(G)同构

同态基本定理：

设f是<A; \* >到<B; Δ>的一个满同态，Ef是由同态f诱导的同余关系，<A/Ef; ☆>是<A; \* >关于Ef的商代数，则<B; Δ>≌<A/Ef; ☆>



以<Z17\*；×17>为例理解群同态基本定理

1. 循环群：

设< G ; \* >是群，若存在g∈G使得对于G中的一切元素a皆可表示成a=gi,其中i∈Z，则称< G ; \* >是一个以g为生成元的循环群，常用G=<g>表示。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 2i | 1 | 2 | 4 | 8 | 16 | 15 | 13 | 9 | 1 |  |  |  |  |  |  |  |  |
| a=3i | 1 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |

求Z17\*的循环群表示：17=2\*8+1,所以（17-1）/2=8

则Z17\*=<3>;

1. 逆元&元素的周期：

a-1a=a-1a=e;

设e是群< G ; \* >的单位元，a∈G，若存在n∈N+使得an=e,则称使之成立的最小n值为元素a的阶（Order，或周期），否则便称元素a的周期为无限，即O(a)=min{n|n∈N+且an=e}。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| a=3i | 1 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| i |  | 16 | 14 | 1 | 12 | 5 | 15 | 11 | 10 | 2 | 3 | 7 | 13 | 4 | 9 | 6 | 8 |
| a |  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| a-1 |  | 1 | 9 | 6 | 13 | 7 | 3 | 5 | 15 | 2 | 12 | 14 | 10 | 4 | 11 | 8 | 16 |
| O(a) |  | 1 | 8 | 16 | 4 | 16 | 16 | 16 | 8 | 8 | 16 | 16 | 16 | 4 | 16 | 8 | 2 |

·周期O(a)可能的值只能是p-1=17-1的因子。

·利用数论验证：以N为周期的元素个数=ψ(N)；

16的因子1，2，4，8，16；

ψ(1)=1；ψ(2)=1；ψ(4)=ψ(22)=22-22-1=4-2=2；

ψ(8)=ψ(23)=23-23-1=8-4=4；

ψ(16)=ψ(24)=24-24-1=16-8=8；

·3是生成元，与O(3)周期相同的都是生成元。

1. 子群H：

设< G ; \* >是群，H⊆G，H≠Ф。若< H ; \* >是群，则称它是< G ; \* >的子群，用H<G表示。

循环群的子群一定是循环群。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| a=3i | 1 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |

a=3i按i从小到大排序，等距取，即可形成各阶的子群，例如划成2阶子集

则间隔16/2=8取子群H={3,14}（或H={9,8},H={10,7}......）

1. 满同态f，Ker(f)=H

满同态：

设g是< A ; \* >到<B; Δ>的一个同态；若g是A到B的满射，则称g为满同态。

满射：如果f(X)=Y,即对于每一个y∈Y，均存在x∈X，使得f(x)=y,那么f是满射。

同态的核Ker(f)：

设f是G到H的群同态，则称集合{a|a∈G且f(a)=eH}为f的核(Kernel)，记为Ker(f)，其中eH是群H的单位元。

G是30阶的，子集H是2阶，则<Z17\*; ×17>≌<Z8; +8>

f是<Z17\*; ×17>到<Z8; +8>的满同态，Ker(f)={3,14}

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a=3i | 1 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |
| f(a) |  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

1. 陪集：

设< G ; \* >是一个群，且H<G，a∈G，分别称

aH={x|x∈G且存在h∈H使得x=a\*h}={a\*h|h∈H}

Ha={x|x∈G且存在h∈H使得x=h\*a}={h\*a|h∈H}

为H在G中以a为代表的左陪集和右陪集，a称为陪集代表。

H={3,14}

3H=14H={3,14} 9H=8H={8,9} 10H=7H={7,10} 13H=4H={4,13}

5H=12H={5,12} 15H=2H={2,15} 11H=6H={6,11} 16H=1H={1,16}

1. 陪集划分：

设< G ; \* >是群，H<G，令π={aH|a∈G}，那么π是G的一个划分。

π={aH|a∈G}={{3,14},{8,9},{7,10},{4,13},{5,12},{2,15},{6,11},{1,16}}

π的秩为8。

1. 商群：

设H是< G ; \* >的正规子群，则G关于H的陪集关系≡H的商代数是群，习惯上用G/H表示，并称之为关于H的商群。

正规子群：设< G ; \* >是群，H<G，若对任意a∈G，总有aH=Ha。则称H是G的正规子群。（任意元素自身的左右陪集相等）

陪集关系：设< G ; \* >是群，H<G，称由G关于H的左陪集划分所诱导的等价关系为G关于H的左陪集关系。

商代数：设<A; \* >是一个代数，R是A上关于\*的同余关系。B=A/R是A关于R的商集合。g=A—>B:任意a∈A，g(a)=[a]R,称g为“与同余关系相关联的自然同态”，常用gR表示，而代数<B; ☆ >则被称作<A; \* >关于R的商代数。

同余关系：设<A; \* >是一个代数，R是A上的等价关系。若R关于\*满足代换条件，a1Ra2∧b1Rb2=>a1\*b1Ra2\*b2则称R是A上关于运算\*的同余关系。

Z17\*/π如下：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ☆ | 3H | 8H | 7H | 4H | 6H | 2H | 5H | 1H |
| 3H | 3H | 8H | 7H | 4H | 6H | 2H | 5H | 1H |
| 8H | 8H | 7H | 4H | 6H | 2H | 5H | 1H | 3H |
| 7H | 7H | 4H | 6H | 2H | 5H | 1H | 3H | 8H |
| 4H | 4H | 6H | 2H | 5H | 1H | 3H | 8H | 7H |
| 6H | 6H | 2H | 5H | 1H | 3H | 8H | 7H | 4H |
| 2H | 2H | 5H | 1H | 3H | 8H | 7H | 4H | 6H |
| 5H | 5H | 1H | 3H | 8H | 7H | 4H | 6H | 2H |
| 1H | 1H | 3H | 8H | 7H | 4H | 6H | 2H | 5H |

1. Z17\*到商群的自然同态：

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a=3i | 1 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |
| h(a) |  | 3H | 8H | 7H | 4H | 5H | 2H | 6H | 1H | 3H | 8H | 7H | 4H | 5H | 2H | 6H | 1H |

1. Ker(h)={a|a∈G且h(a)=eH}=3H={3,14}

总结：

f：群<Z17\*；×17>–> <Z8; +8>是一个满同态

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a=3i | 1 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |
| f(a) |  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 |

令K=Ker(f)={3,14},对于任意的a∈Z17\*，有f(aK)={f(a)}

陪集划分所诱导的等价关系π={aH|a∈G}={{3,14},{8,9},{7,10},{4,13},{5,12},{2,15},{6,11},{1,16}}

h=<Z17\*；×17> —> <B; ☆ >:任意a∈<Z17\*；×17>，h(a)=[a]π。<B; ☆ >则被称作<Z17\*；×17>关于π的商代数。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| a=3i | 1 | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |
| h(a) |  | 3H | 8H | 7H | 4H | 5H | 2H | 6H | 1H | 3H | 8H | 7H | 4H | 5H | 2H | 6H | 1H |

G/K=<B; ☆ >与<Z8; +8>同构

即

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ☆ | 3H | 8H | 7H | 4H | 6H | 2H | 5H | 1H |
| 3H | 3H | 8H | 7H | 4H | 6H | 2H | 5H | 1H |
| 8H | 8H | 7H | 4H | 6H | 2H | 5H | 1H | 3H |
| 7H | 7H | 4H | 6H | 2H | 5H | 1H | 3H | 8H |
| 4H | 4H | 6H | 2H | 5H | 1H | 3H | 8H | 7H |
| 6H | 6H | 2H | 5H | 1H | 3H | 8H | 7H | 4H |
| 2H | 2H | 5H | 1H | 3H | 8H | 7H | 4H | 6H |
| 5H | 5H | 1H | 3H | 8H | 7H | 4H | 6H | 2H |
| 1H | 1H | 3H | 8H | 7H | 4H | 6H | 2H | 5H |

同构<Z8; +8>