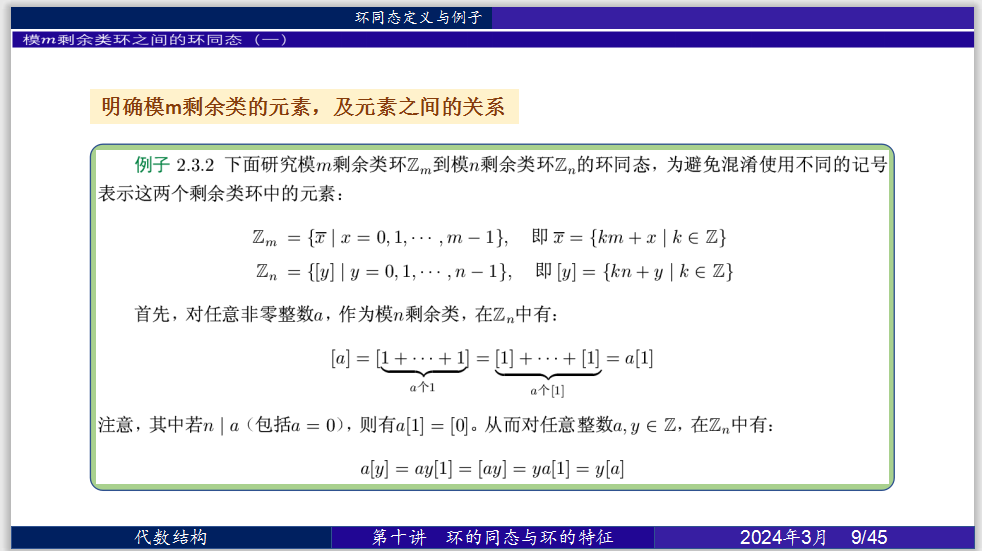
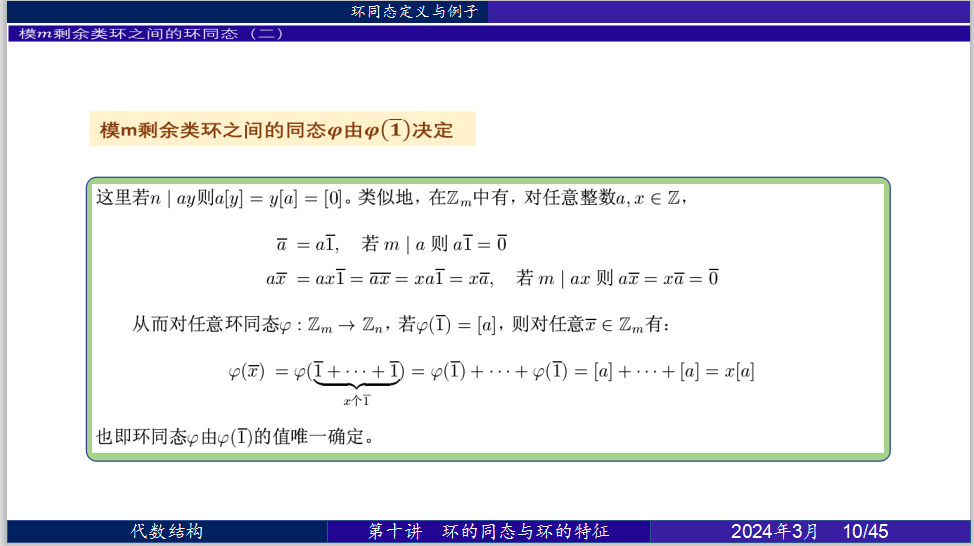
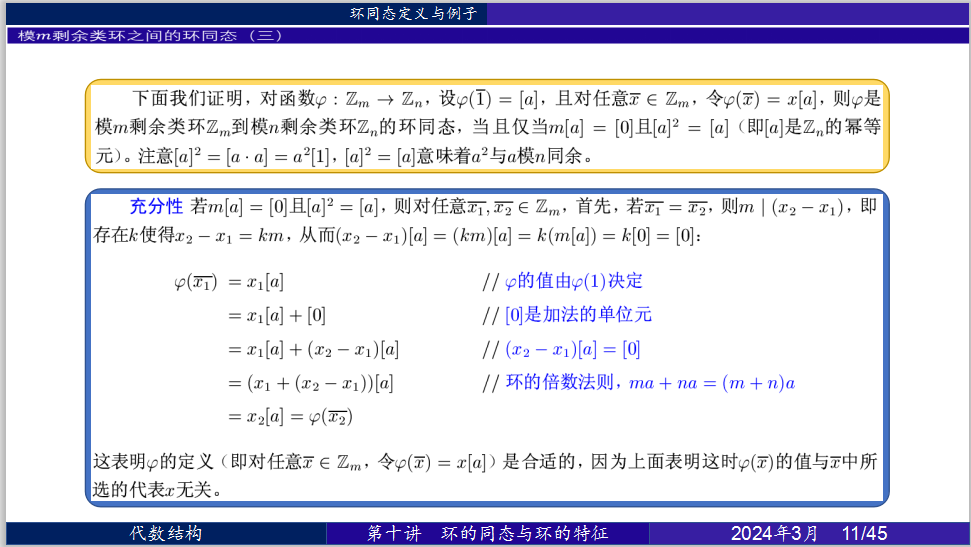
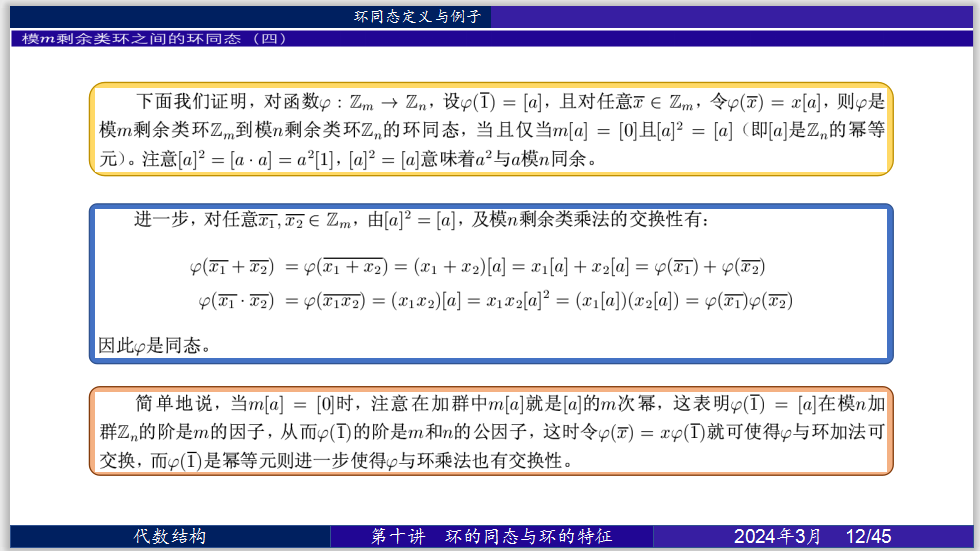
**关于剩余类环间同态的充要条件的辨析**

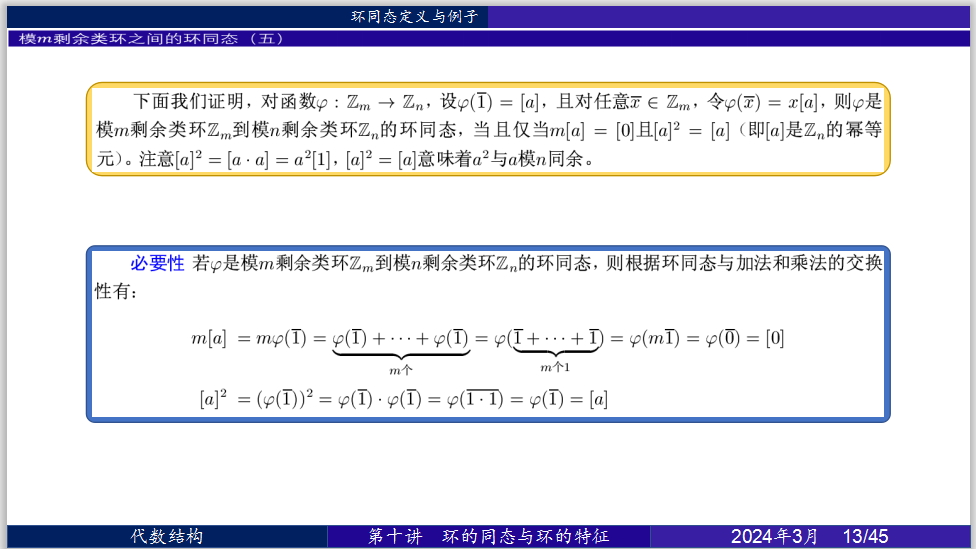
**以下讲义及教材答案的写法，可能会引起理解不当，辨析如后。**

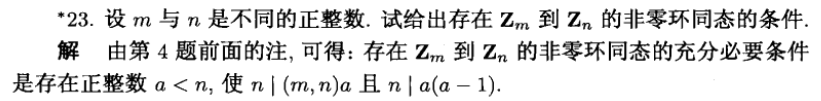
****

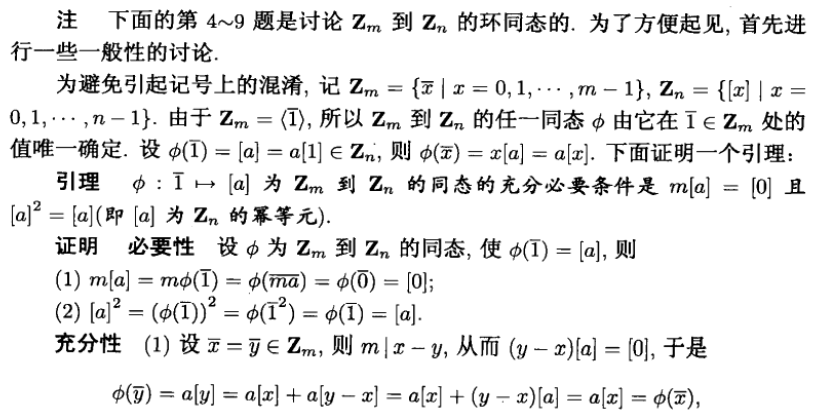
****

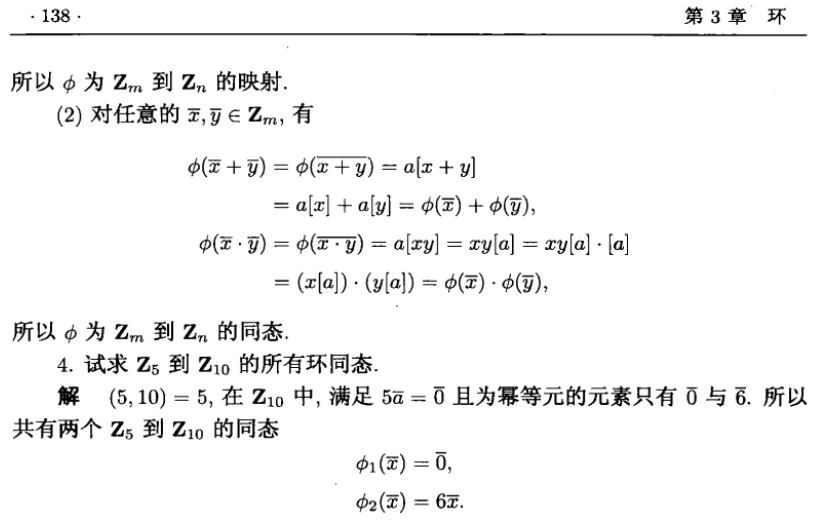
****

****

****

****

****

****

**以上讨论环Zm到Zn的映射为同态映射的充要条件。**

**后面我们采用Zm={0,1,2…,m-1}做模m加和模m乘，以及Zn={0,1,2…,n-1}做模n加和模n乘的简洁形式。**

**通常，我们初读容易理解成了：“m和n满足什么样的条件”，这样的条件成为“环Zm到Zn的映射是同态映射”的充要条件”。**

**其实，以上讨论的是：首先（大前提），从环Zm到Zn构造好映射类型，\phi( x mod m)=xa mod n这样类型映射(特别写出mod m和mod n是在强调映射前后的运算是不同的，后续证明也利用到这点不同)。然后，才要确定，“m和n满足什么样的条件”，才能成为“环Zm到Zn的特殊类型的映射\phi(.)是同态映射”的充要条件”。**

**注意，不加限制的话，仅从映射的概念出发，可以知道，Zm到Zn的映射的总个数为n^m，数量是指数形式的，非常多。而特殊类型的映射\phi(.)只有n个（就是取a=0,1,…,n-1这n种）。这n种映射可并不都是同态映射，有个充要条件来判定。**

**当然，既然是考虑充分必要条件，在必要条件的时候，已经有同态的映射必然满足“\phi( x mod m)=xa mod n这种形式”，所以，充要条件的论述就限制到这种特殊映射的大前提下了。包括教材习题第23提中提及的“存在”其实也蕴含着是针对这种特殊类型的映射的——因为这种类型之外的映射肯定不是同态映射（同态必要性的逆否命题）。**

**所以，完整论断应该是这样：给定正整数m和n，对环(Zm={0,1, 2,…,m-1},+m,xm )到环(Zn={0,1,2,…,n-1},+n,xn )的映射\phi(x mod m)= ( (x mod m) x mod n )，其为同态映射的充要条件是，n|(m,n)a且n|a(a-1)，其中a为元素1\in Zm在映射\phi下的像点，即\phi(1)=a \in Zn。**

**理解前一段的基础上，就可以简化掉特殊类型的映射了（讲义和教材答案就是这样做的，但未做解释，无法正确而准确地理解）。**

**必要性：已知\phi(.)是同态映射，对m个1 \in Zm，利用加法同态性质有 \phi(1+1+ …+1 mod m)= \phi(1)+ \phi(1)+…+\phi(1) mod n = ( ma mod n )，此式同时也等于\phi(0)=0 mod n（因为1+1+ …+1 mod m =0 mod m，且同态下第一个环的加法单位元一定会被映射成第二个环的加法单位元），即 ma=0 mod n，进而 n|ma。另外，n|na，即n是ma和na的公因子，进而是最大公因子(ma,na)=(m,n)a的因子，即n|(m,n)a。**

**对1 \in Zm，利用乘法同态有\phi(1\*1 mod m)=\phi(1)\*\phi(1) mod n=a2 mod n，此式同时也等于\phi(1)（因为1\*1 mod m=1 mod m），即 a2=a mod n，进而n|a(a-1)。**

**至此，必要性证毕。**

**充分性：考虑环Zm到环Zn的映射\phi(x mod m)= ( (x mod m) x mod n )，其中，\phi(1)=a，a为Zn中元素，0 =< a <n。对任意x,y \in Zm，根据\phi 的定义及严格意义上的数值相等x+y mod m= x+y+km（k为0或-1），有\phi( x+y mod m) = ( x+y mod m)a mod n = ( x mod m) a + ( y mod m) a + (km)a mod n = ( ( x mod m) a mod n) + ( ( y mod m) a mod n) + ( (km)a mod n) mod n =\phi(x) + \phi(y) + ( (km)a mod n) mod n。根据充分性的条件n|(m,n)a及m=m’(m,n)有 (km)a mod n = k m’(m,n)a =km’\*0 mod n = 0 mod n，从而前一式子可以简化为 \phi( x+y mod m) = \phi(x) + \phi(y) mod n，即为加法同态。**

**对任意x,y \in Zm，根据\phi 的定义及充分性的条件n|a(a-1)（等价于a2=a mod n），\phi(xy mod m)= (xy mod m)a mod n = (xy mod m)a2 mod n = ((x mod m)a mod n)\* ((y mod m)a mod n) mod n = \phi(x) \* \phi(y) mod n，即为乘法同态。**

**至此，充分性证毕。充要条件论断证毕。**