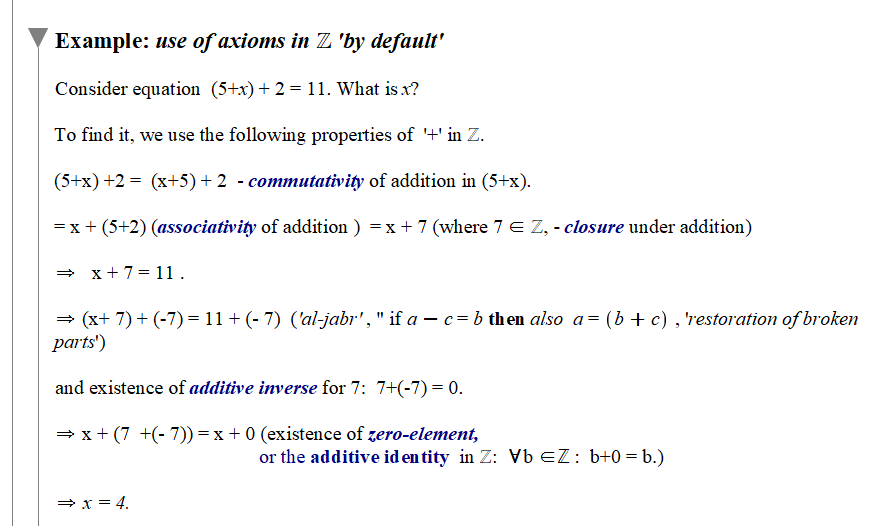
Definition



解决这个方程，我们实际上需要

五个properties:   
communtativity:交换律

Associativity: 结合律

Additive inverse: 加法逆运算

Additive identity:加法性质

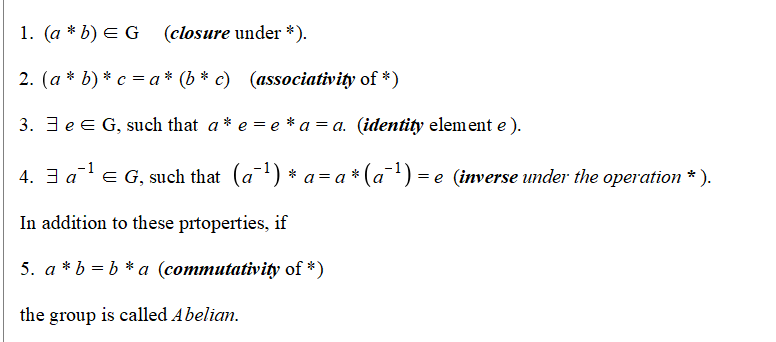
Zero-element:零元素

这五个Property对应了描述abelian group阿贝尔群的 axiom公理

阿贝尔群指的是一组元素

Definition:

一个set G 和一个运算符号operation 组成一个 group， 如果G里任意三个数满足以下axiom公理



1.a经过这个operation仍然在G里 //closure闭环

2. 结合律 associativity

3. identity element e恒等元素e， g里一定要存在一个e

让a\*e=e\*a=a例如加法里的0

4. inverse在G中必然存在一个数b，让b\*a=a\*b=e，(注意这里的a^-1是不是倒数的意思，是Inverse的意思)

5.如果a\*b=b\*a commutativity

那么这个group叫做abelian

例如，加法符号配上set Z， 就是一个标准的abelian group

性质1：

一个group有且只有一个identity element e

那么e\*g=g, e\*g=e,那么 e=g

这个也解释了为什么1不是乘法中的identity element，因为1\*0=0，不等于1

性质2：

在一个group中，任意一个元素有且只有一个inverse

假设b与c是a的inverse,那么a\*b=b\*a=e=a\*c

B\*e=b\*e

B\*a\*b=b\*a\*c

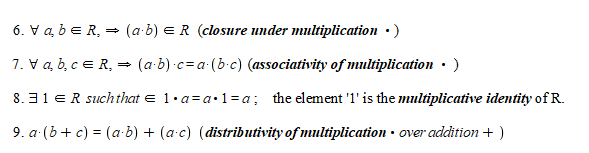
交换律

B=c

定义：一个set R 伴随着加号+乘号\*, 以及连个特殊element 0 与1 可以被称作ring(with identity)如果他么满足以下性质

对于+号，只要满足axiom 1到5， addictive identity是0，叫做zero elemeng，  b代表着additive inverse of a ,b+a =a+b=0,叫做negative of a

对于乘号，要满足以下四个性质



closure：任意a,b属于set，a\*b仍然属于set,

associativity:(a\*b)\*c=a\*(b\*c)

multiplicative identity: 1, 让1\*a=a\*1=a

distributivity: a(b+c)=ab+ac

 满足以上四条称作普通乘法ring

如果满足communication law a\*b=b\*a

叫做commutative ring

理论：

C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\FFE9B905.tmp

Z/mZ是 commutative ring

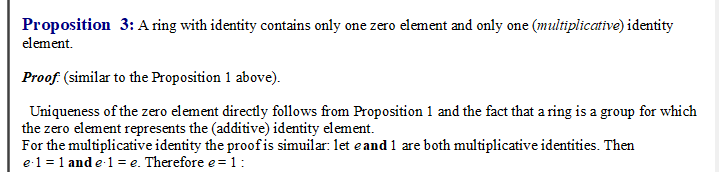
10条性质都满足

[0]是additive identity

[1]是multiplicative identity

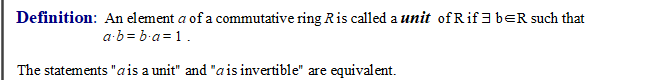
addictive inverse [2] 为[-2]= [m-2]

Proposition 3: 一个ring只有一个addictive identity: zero element 以及一个Multiplicative identity

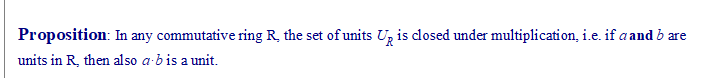


Definition: 在commutative ring内，一个元素被称作Unit，如果a\*b=b\*a=1

a is a unit等价于a is invertible



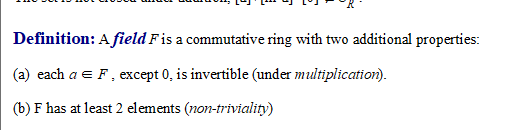
PROPOSITION, 在任意commutative ring中， Unit集合 UR是乘法close(任意两个数相乘仍然在集合中)



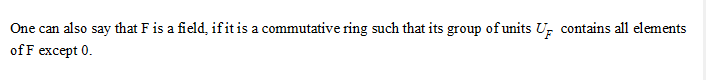
定义:Field:在commutative ring的基础上额外加上两条性质

（a）在乘法中，任意一个数除了0都是invertible(任意a存在b让a\*b=b\*a)

（b）F至少有两个元素



还有一种说法



Zero divisor：

在整数里，如果a\*b=0,那么要么a=0,要么b=0

在许多ring中不是这样，例如

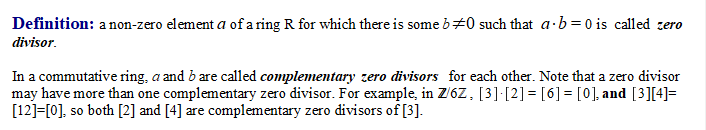
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2A0E4999.tmp

定义：

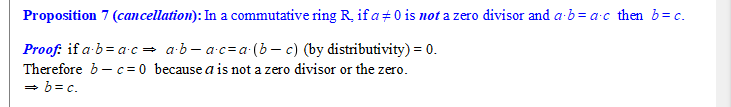
如果有一个非零数a，在ring中存在一个非零数b，让a\*b=0, 那么这个数a叫做zero divisor

ring a\*b不一定等于b\*a， 看communitative

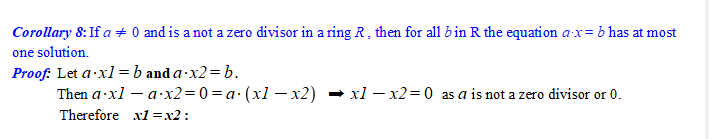
在commutative ring中，a与b叫做complementary zero divisors互补zero devisor



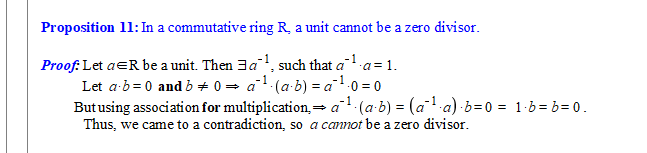
proposition:在一个commutative ring R中，如果a≠0不是一个zero divisor，且a\*b=a\*c，那么b=c



Collary：如果a不等于0且不是一个zero divisor在ring R中，那么无论b取什么值，a\*x=b最多一个解

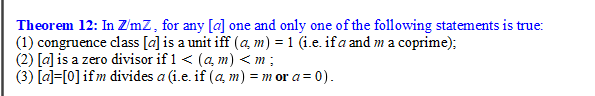


**Proposition:****在一个·commutative ring R中，unit 不可能是zero divisor**



Collary:一个field没有zero divisor， 因为除了0以外都是Unit

C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\AB4DA347.tmp



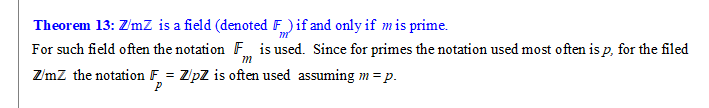
在Z/mZ中，任意【a】只能是以下三种情况的一种

(1)[a]是Unit当且仅当（a,m）=1

(2)[a]是zero divisor，如果1<（a,m）<m

(3)[a]=[0]如果(a,m)=m or a=0

理论13：Z/MZ是一个field当且仅当m是Prime的时候



理论14：如果R是一个有限commutative ring，而a是R里任意非零element，那么a要么是·Unit，要么是zero divisor

C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\85F9189.tmp