polynomial多项式·

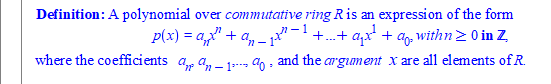
一个标准的polynomial function



是polynomial的coefficients 系数， x是变量variable(也叫argument)。 n的最大值叫做polynomial的degree。必须是一个非负数， 因为实数是commutative ring，因此多项式可以写成 //commutative ring满足交换律



对于polynomial的定义可以延伸到所有commutative ring R



一个基于commutative ring R的多项式可以表示成

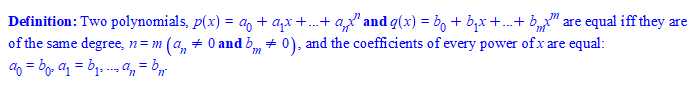


系数是an,...a0

argument x 可以是R的任意元素

因为commutative ring是closed，所以当X基于commutative ringR, 那么p(x)也在R的范围内

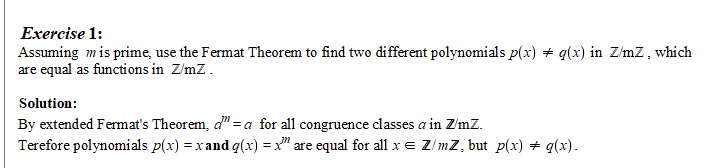




两个多项式相等当且仅当 他们degree相同既n=m, 且每一个系数一一相等

你把两个多项式看做函数，那么相等的多项式函数也相等，但是这句话反过来不对，函数相等并不代表多项式相等

例题：



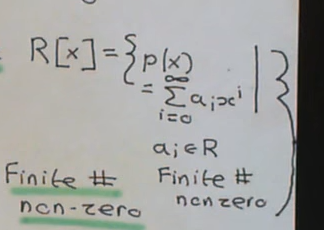
使用fermat Theorem



因此p(x)=x, q(x)=x^m ， 作为function相等（在这个Z/mZ中两者等价）， 但是作为多项式不相等，degree不同

Polynomial Ring R[x](ch.13B)

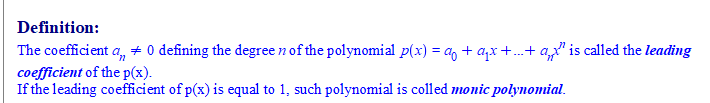
因为R是一个commutative ringm 那么R的所有element满足commutation, association与distribution。 基于R构建的Polynomial本身自己也是个commutative ring，记作R[x] x是variable x， R可以使任意commutative ring, 例如Q，Z/MZ。 绝大多数我们会考虑在R=Z/mZ上构建polynomial,



意思就是所有系数属于R的多项式组成的集合，

如果m为质数p，那么Z/pZ是一个field //任何element除了[0]都是unit。

我们用这个记号notation来表示基于Fp的polynomial



最大项数的系数an叫做**leading coefficient**

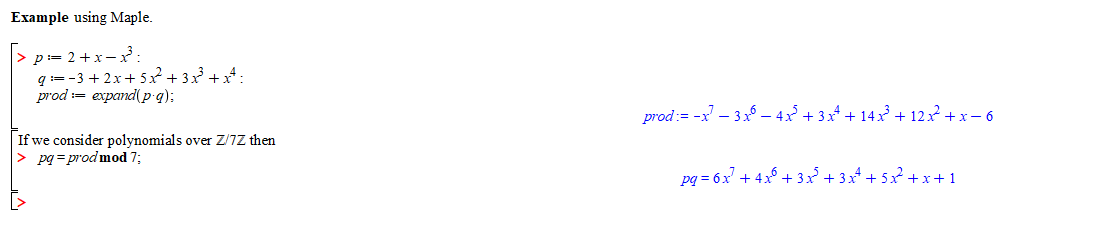
如果leading coefficient=1, 那么这个polynomial叫做monic polynomial

Zero polynomial:任意系数都是0，例如p(x)=0,zero polynomial的degree

注意 ring R自己就代表着polynomial ring R[x]的子集，

//R是R[x]的一部分

然后下面一长串就是在说两个属于R[x]的多项式相加，相乘必然还是属于R[x]



例如这个，

第一个例子我们基于commutative R实数,我们可以看到系数还是实数，因此是R【x】

第二个例子基于commutative ring Z/7Z, 我们可以看到系数还是Z/7[Z]的，6其实是[6]，因此仍然是R【x】

Proposition 1: Let R be a commutative ring. For every pair of non-zero polynomials p and q in R[x], if the leading coefficient of p or q is not a zero divisor in R then deg(p q)=deg(p) + deg(q).

理论，让R是一个commutative ring，对于每一组非0多项式p与q， 如果 p与q的leading coefficient不是R的zero divisor，那么deg(p\*q)=deg(p)+deg(q)

证明：

假设deg(p)=n,deg(q)=m,那么deg(p\*q)=应该是[anbm]x^n+m, 然后因为an,bm不是zero divisor，因此an\* bm不可能等于0，所以最高系数就是n+m

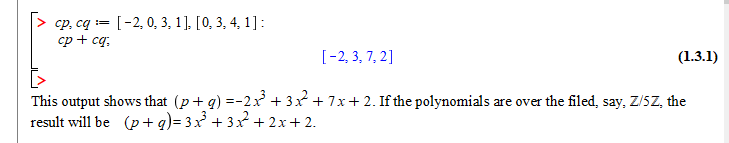
在接下来的课程中，我们的多数考虑的多项式，系数全都是基于ring 的，

原来有xy的多个variable的polynomial 写成POLYNOMIAL RING的形式就是

Detaching分离 the coefficients of p(x)

多项式可以轻松的表示成 类似坐标的tupel形式

表示为 

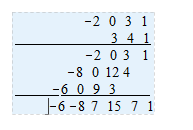


.这样就方便了很多

因为是z/5z还能转换一次

这样是加法

乘法是像运算一样



区别在于不要进1，

例如这里有个15，就留在那里

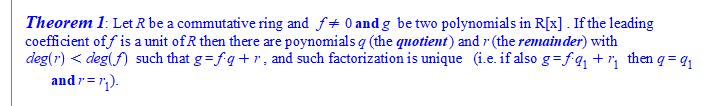


Polynomial Factorization

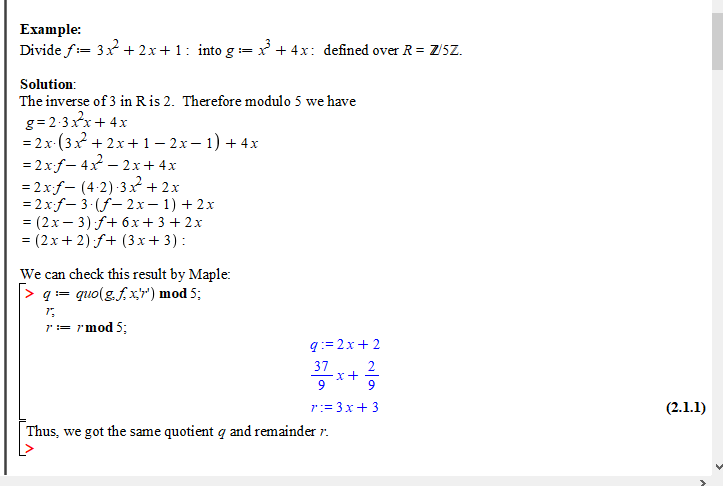
Division theorem,

Theorem1

如果R是一个commutative ring，而且 f≠0,与g 是R【x】中的两个polynomial。 如果f的最大系数是R的unit，那么必然存在polynomial q (商)，以及polynomial r(余数)， deg(r)<deg(f), 让g=fq+r, 且解是唯一的



怎么因式分解



例如我们要从g中分出个f

首先巧算一下

g=6x^3+4x //因为是Z/5Z

g=2x(3x^2+2x+1-2x-1)+4x

=2xf-4x^2-2x+4x

=2xf+x^2+2x //z/5z

=2xf+6x^2+2x //z/5z

=2xf+2f-2x-2

=(2x+2)f+(3x+3)

Collary2:

如果F是一个field，那么Division theorem对任意f≠0与g都有效

定义，polynomial f divides g如果g=fq， for some polynomial q in F(x)



Remainder theorem:如果f(x)是F[x]中的一个polynomial，且a属于F那么当r是f(x) divide (x-a)的余数

f(a)=r

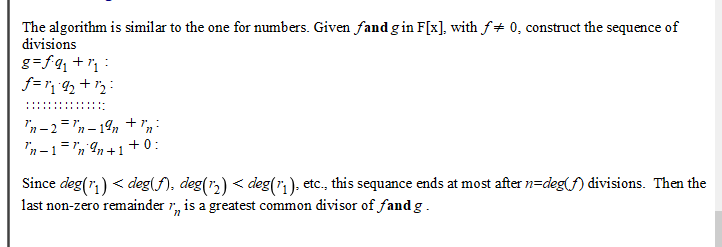
还有一大堆理论

Greatest common devisor

让f与g是两个F（x）中的polynomial， 那么polynomial d 是greatest common devisor of f and g, 如果d divides f且d divides g， 且与其他同时divide fg的polynomial比，他的degree是最大的

我们找到greatest common divisor可以通过重复使用division theorem

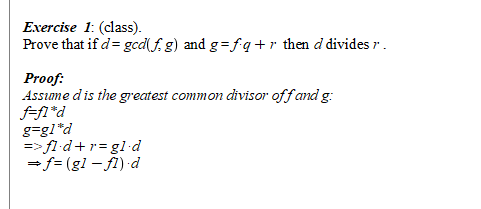
这个过程叫做Euclid's algorithm for polynomial



g=fq1+r1

f=r1q2+r2...

一直到最后r变成0



证明 如果d =gcd(f,g)且g=fq+r, 那么d divides r

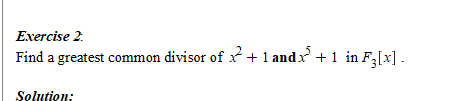
因为d是gcd

因此f=f1d

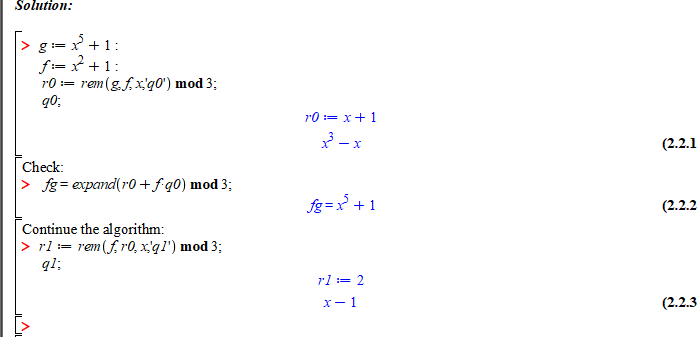
g=g1d

f1d+r=g1d

f=(g1-f1)d



找到common divisor



r0是 remainder

下一步是验证

然后继续算法

r1是余数

q1是商





常数项还是不是0

但是余数已经是常数了

下一步就成功了

事实上我们还可以巧算

(x+1)在Z/3Z中可以转换成4(x+1)

2(2x+2)(x-1)+2

2(2x^2-1)

4x^2-2=x^2+1=.....

注意如果F中有多个Unit，那么就有多个GCD



但是，有且只有一个monic greates divisor//通过 inverse转化而来



定义：

两个non-zero polynomial d 与 e被称作是associates,如果他们互相是对方的scalar倍数//scalar可以是小数

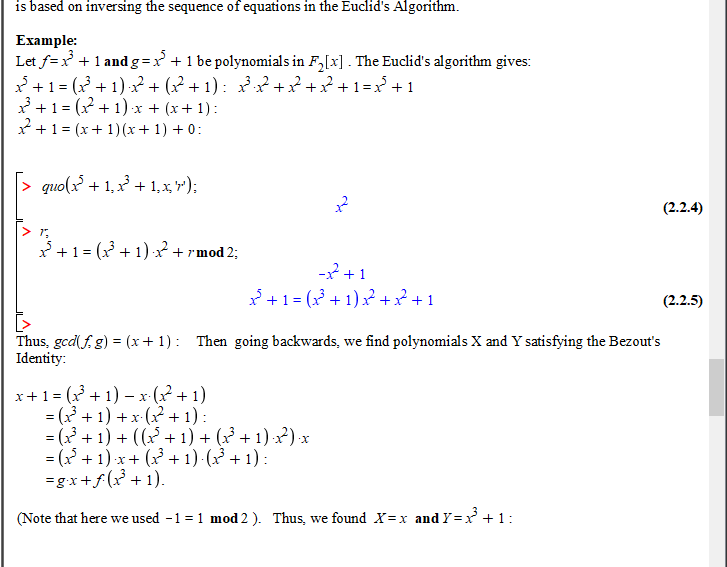


例如X^2+2与3X^2+6

Theorem8：Benzout's Identity,

对于任意F[x]内的d=gcd(f,g),inF(x),都可以写成d=Xf+Yg,对于F[x]中的某一个X,Y



例子：

先用Euclid algorithm求出gcd

Irreducible polynomial  
定义：irreducible 不可约的，不能再消减degree的：一个polynomial p in F[x] 被称作irreducible如果p已经不再是F[x]中的unit了，如果P=f\*g，那么f与g之间必定有一个是unit//换句话说，当p=f\*g,f与g中必然有一个是非零整数，这时p叫做irreducible

定义Unit: 如果F是一个field,那么对于polynomial p来说，存在q，让pq=1,那么p就是q的unit //换句话说，只有非零整数才能算unit

如果p是unit,那么必然存在另一个Unitq,让pq=1，那么在F【x】中，我们一直deg(p)+deg(q)=0,唯一满足的可能就是deg(p)=deg(q)=0,

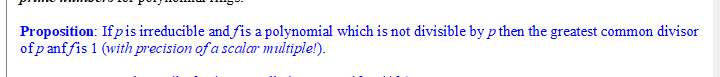
网课

irreducible polynomial相当于常数中的prime number的位置，已经不能再约分了（整数意义上）

x^2-3无法继续约分（实际上考虑根号3可以继续约分）

7无法继续factor（实际上考虑根号7可以继续factor）

Proposition:如果 p是irreducible且f是无法整除p的polynomial，，那么p与f之间的gcd是1



Definition:，两个polynomial被称作coprime如果gcd(f,g)=1



Irreducible polynomial的例子

p=x+a在任意F[x]里都是irreducible， 因为p=fg,那么deg(f)+deg(g)=1,那么g与f中任意一个deg必须是0

x^2+1在Z/3Z中是irreducible但是在Z/5Z中不是

为啥在Z/5Z中不是

x^2+1=x^2-4=(x-2)(x+2)

理论（factorization）：任意degree>=1的polynomial在F[x]中，要么是irreducible，要么可以积分乘irreducible polynomials的乘积

Theorem(Unique Factorization):在F[x]中，如果f=p1p2...ps =q1q2...qt， 是monic polynomial f(最大系数为1)的两种monic irreducible polynomial积分， 那么t必然等于s，且{p1...ps}与{q1,,,qs}必然相等