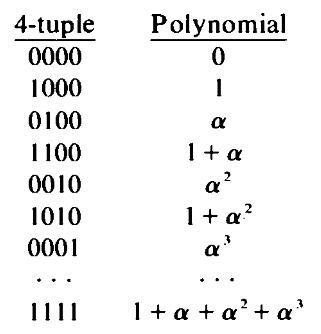
1. 域：域是一个元素的集合。
2. 集合中的元素之间有定义一套完整的加/减/乘/除规则（除0没有意义）；
3. 加法和乘法要满足交换律、结合律和分配律；
4. 存在元素0和1
5. 对于任意元素, 都存在 .
6. 有限域：有限域中包含有限个元素 [假设有n个元素，则称该域的序 (order) 为n]，有限域又称为伽罗瓦域（Galois fields）。
7. 构造一个GF(16)——16个元素的伽罗瓦域

将域中的16个元素各用一个不同的0/1四元组来表示，再将这16个四元组与多项式联系起来：



1. 加/减

首先，在伽罗瓦域中减法等同于加法，它们本质上都是元素之间的逐位异或，即

特别的，有

1. 乘法

将元素之间的乘法看成是元素所对应的多项式之间的乘法，例如：

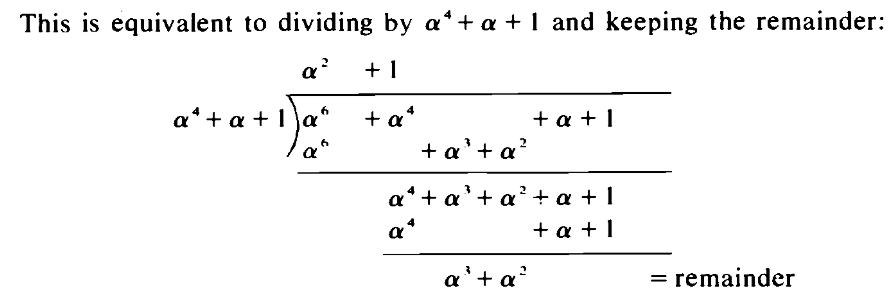
在得到的结果多项式中出现了，但是用0/1四元组是无法表示指数大于3的项的。为了整个体系的自洽，我们必须引入一个度为4的等式，比如：

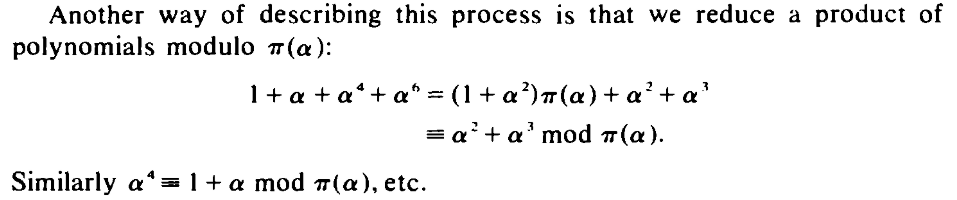
则有：

由此我们又可以推出：

则:

也可以从模运算的角度来理解这个结果：

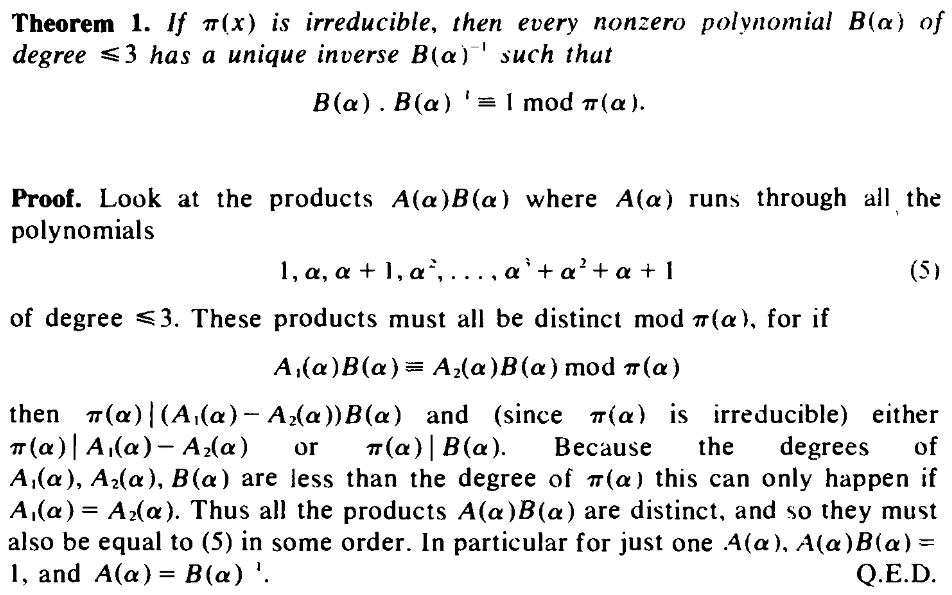




综上，有：

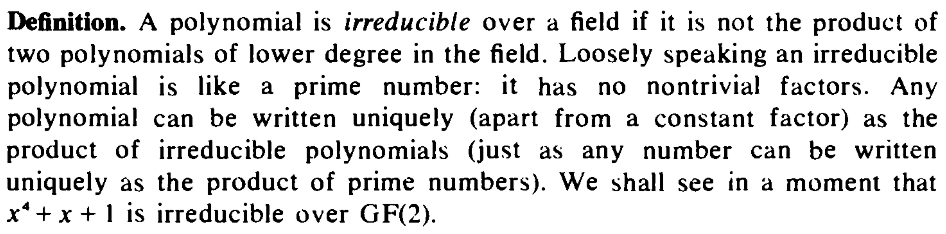
1. 逆

逆存在性定理：

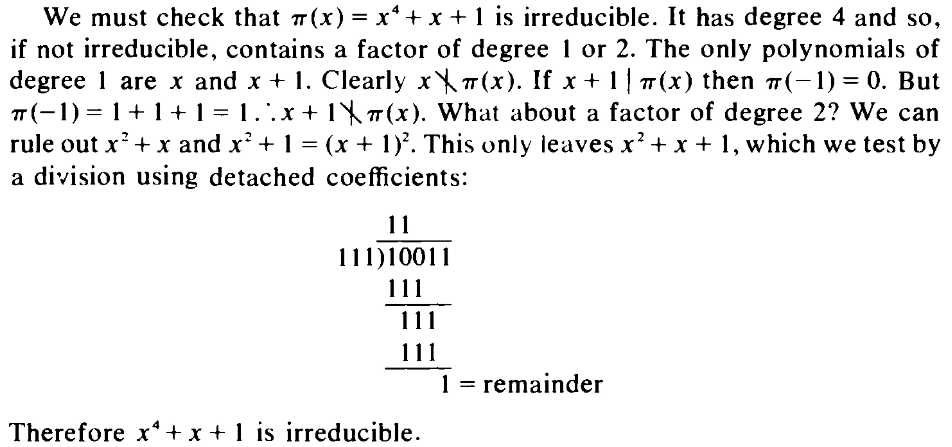


何为irreducible(不可约)？

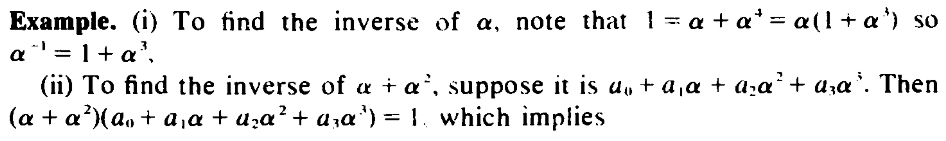
答：在一个域中，对于一个多项式A，如果不存在另外的两个多项式B,C，满足，则称多项式A不可约。

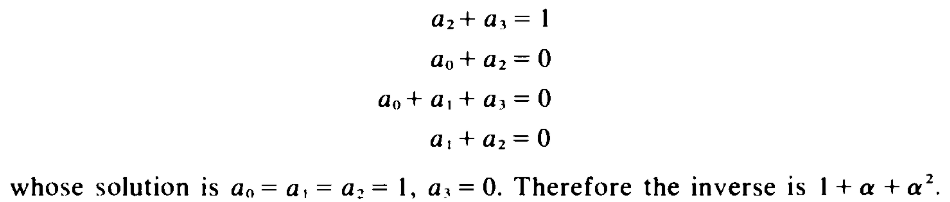


如何证明 不可约？



如何求逆？





1. 除法

求，等价于求，利用上一节讲的求逆操作即可。

1. 123
2. 123