6.1 代数元素 2021年8月10日11点12分

6.1.1定义. 令是的扩展域,令.如果存在非零多项式使得,则称**满足**多项式并且是的**代数**.如果不满足中的任何非零多项式,则称在上是**超越的[transcendental]**.

6.1.2命题. 令为的扩展域,令是上的代数.则存在唯一的一元不可约多项式使得.它的特征是最小次的一元多项式,是它的根.此外,如果是中的任何多项式且满足,则.

6.1.3定义. 令为的扩展域,令为的代数元素.中最小次数的单调多项式使得 称为在上的**最小多项式**.在上的最小多项式的次数称为在K上的**次数**.

6.1.4定义. 令F为K的扩展域,令.包含和的F的最小子域将由 表示.称为**生成的的扩展域**.或者,被称为通过将与K**相邻而定义的K的扩展域**.如果对于单个元素,则称F是K的**简单扩展**.

6.1.5命题. 令F是K的扩展域,令.

如果u是K上的代数,则,其中是u在K上的最小多项式.

如果u在K上是超越,则,其中是积分域的商域.

4.3.8定理(克罗内克). 令K是一个域,并且令f(x)是K[x]中的任意非常数多项式.则K存在一个扩展域F和一个元素使得.

6.2 有限和代数扩展 2021年8月10日14点24分

6.2.1命题. 如果F是K的扩展域,则F是K上的向量空间.

6.2.2命题. 令F是K的扩展域,令是K上的一个元素代数.如果u在K上的最小多项式的阶数为n,则是K上的一个n维向量空间.

6.2.3定义. 设F是K的一个扩展域.如果F作为K上的向量空间的维数是有限的,则称F是K的有限扩展.F作为K上的向量空间的维数称为F在K上的次数,用表示.

6.2.4命题. 令F是K的一个扩展域,令.下列条件等价:

在K上是一个代数;

是K的有限扩展;

属于K的一个有限扩展.

6.2.5定理. 令是的有限扩展,令是的有限扩展.那么是的有限扩展,并且

6.2.6推论. 令F是K的有限扩展.如果,则在K上的此数是的除数.

6.2.7推论. 令F是K的扩展域,其中代数元素

在在K的次数至多是在K上次数的乘积,.

6.2.8推论. 令F是K的扩展域.F中所有对K代数的元素的集合形成F的子域.

6.2.9定义. 如果F的每个元素都是K上的代数,则称K的扩展域F是K上的**代数**.

6.2.10命题. 每一个有限扩展都是代数扩展.

6.2.11命题. 设F是E的代数扩展,E是K的代数扩展.那么F是K的代数扩展.

6.3 几何构造 2021年8月10日17点10分

6.3.1定义. 如果仅使用直尺和圆规就可以构造长度为的线段,则称实数是**可构造数**.

6.3.2命题. 所有可构造实数的集合是所有实数域的一个子域.

6.3.3定义. 令F是的一个子域.

对于元素,具有方程形式的直线,被称为**上的一条线**.

对于元素,具有方程形式的任意圆,被称为**上的圆**.

6.3.4引理. 令F是的一个子域.

任何连接坐标属于F的两点的直线都是F上的一条线.

任何半径和中心坐标都属于F的圆是F上的圆.

6.3.5引理. 设F是的一个子域.上的线和上的圆的交点属于域,其中是某个值.

6.3.6定理. 实数是可构造的当且仅当存在实数的有限集使得

,

,其中,

.

6.3.7推论. 如果是可构造的实数,则是Q上的代数,并且其最小多项式在Q上的次数是2的幂.

6.3.8引理. 对于任意角度,下列三角等式恒成立.

,

.

6.3.9 定理. 不可能找到三等分角,复制立方体或平方圆的一般构造.

6.4分割域 2021年8月11日10点53分

6.4.1定义. 令K是一个域,令是中次数为的多项式.令F是K的一个扩展域,如果存在元素使得

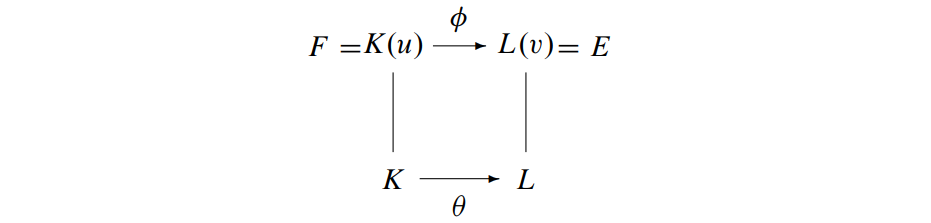
且

.

则F被称为在K上的**分割域**.

6.4.2定理. 令是一个次数为的多项式.则存在一个在K上的分割域F,使得.

6.4.3引理. 令是一个域同构.令F是K的扩展域使得,其中是一个代数元素.令是在K中的极小多项式.令是在下的图像.如果是在L扩展域的的任意根,,则存在一个唯一的方法将扩展到同构使得和对有成立.



6.4.4引理. 令F是上的分割域.如果是一个域同构,将映射到,E是在L上的分割域,则存在一个同构使得对有成立.

6.4.5定理. 设是域K上的正次数多项式.如果E和F是在K上的分割域,则存在同构使得对有成立.

6.5 有限域 2021年8月11日12点42分

6.5.1命题. 令F为特征p的有限域.那么F有个元素,对于某个正整数.

如果F是任何域,则F中包含单位元素1的最小子域称为F的素子域[prime subfield].如命题6.5.1的证明所述,如果F是有限域,则其素子域与同构,其中.

6.5.2定理. 令F是具有个元素的有限域.则是多项式在的质数子域上的分割域.

6.5.3推论. 两个有限域是同构的当且仅当它们具有相同数量的元素.

6.5.4引理. 令F是特征为p的素数域,令.

对所有成立.

是F的一个子域.

6.5.5命题. 令F是一个包含个元素的域.F的每个子域都有个元素,对于n的某个除数m.相反,对于n的每个正除数m,存在F的唯一子域,其中包含元素.

6.5.6引理. 设F是一个特征为的域.如果是不能被整除的正整数,则多项式在F的任何扩展域中都没有重复根.

6.5.7定理 对于每个素数p和每个正整数n,都存在一个包含个元素的域.

6.5.8定义 令为素数,令.含有个元素的域称为阶**伽罗瓦域**,记为.

6.5.9引理 令G为有限阿贝尔群.如果是G中最大阶的元素,则G的每个元素的阶都是的阶的约数.

6.5.10定理. 域的乘法群的任何有限子群都是循环的.

6.5.11定理. 任何有限域都是其素子域的简单扩展.

6.5.12推论 对于每个正整数n,在上存在n次不可约多项式.

6.6 有限域上的不可约多项式 2021年8月11日15点50分

6.6.1定理. 令,其中.中的一元不可约因子正是中的一元不可约多项式,其次数是m的除数.

6.6.2推论. 令K为有限域,令为不可约多项式.如果F是K的扩展域,并且包含一个根u,则是在K上的分割域.

6.6.3定义. 如果d是一个正整数,我们定义莫比乌斯函数如下:

;

仅当d有偶数个质因子(每个仅出现一次);

仅当d有奇数个质因子(每个仅出现一次);

仅当d可以被质数的平方整除.

6.6.4命题. 如果且,则.

6.6.5命题. 令R是一个交换环,令是一个乘法函数.如果函数被定义为

则F是一个乘法函数.

6.6.6命题. 对于任意正整数n,

6.6.7定理(莫比乌斯逆公式). 令R是一个交换环,令是任意函数,如果函数被定义为

则

6.6.8定理(莫比乌斯逆公式(2)). 令R是一个交换环,令是任意函数,如果函数被定义为

则

6.6.9推论. 对于任意正整数n,.

6.6.10定义. 在有限域上的m次不可约多项式的数量,将用表示,其中是素数幂.

6.6.11定理. 对于任意质数幂和任意正整数,

6.6.12推论. 对于所有正整数和所有素数幂我们有.

6.7 二次互反 2021年8月11日17点14分

6.7.1定义. 令n是一个正整数,令a是一个整数使得.如果同余

是有解的,则被称为**二次剩余模[quadratic residue modulo]**,否则是**二次非剩余[quadratic nonresidue]**.当是素数时,如果是二次剩余模,我们写;如果是二次非剩余模,我们写.符号被称为**勒让德符号[Legendre symbol]**.

6.7.2命题(欧拉判别式). 如果是一个奇素数,且,,则

6.7.3定理(二次互反). 令是不同的奇素数.则

6.7.4定理. 令p是一个奇素数.则

;

,其中.