商环和有限域

2023 年 12 月 16 日

目录

1 商环和有限域

代数基本定理指出：每个$C[x]$中的非常数多项式都是$C[x]$中的线性多项式乘积。不严谨的说，C包含着每个$C[x]$中多项式的根。于是，现在我们重新回到理想和同态以证明任意域k上的多项式和代数基本定理有局部相似性。

给定多项式$f(x) \in k[x]$，则有一些域K包含k上$f(x)$的所有根。在K的构造背后的主理想涉及到商环，这关系到我们之前学习的I_m构造的直接推广。我们来复习一下

给定Z和整数m，则一个Z上的同余关系被定义为：

$$a \equiv b \mod m \iff m \mid (a-b)$$

我们可以把该定义重写为$a \equiv b \mod m$当且仅当$a-b=km$对某些$k \in Z$成立，而这等价于$a-b \in (m)$，其中(m)是Z中由m生成的主理想。而同余是一种Z上的等价关系，它是被称为同余类的等价类$[a]$。而I_m则是包含所有这种同余类的集合。

现在我们来看一种新的构造，给定交换环R和理想I，定义同余关系$\mod I$或者R

$$a \equiv b \mod i \iff a-b \in I$$

1.1 引理

若R是交换环且I是在R中的理想，则同余 $\mod I$是R上的等价关系

证明： 首先我们来证明

自反： $a \in R$，则$a-a=0 \in I$，所以$a \equiv a \equiv I$

对称： $a \equiv b \mod I \Rightarrow a-b \in I$，因此$-1 \in R$有$b-a=(-1)(a-b) \in I$有$b \equiv a \in I$

传递： 若$a \equiv b \mod I$且$b \equiv c \mod I$，那么$a-c=(a-b)+(b-c) \in I$有$a \equiv b \mod I$

1.2　定义：同余类

若R是交换环且I是R上的理想，则$a \in R$的等价类是：

$$[a] = \{b \in R : b \equiv a \mod I\}$$

称为$a \mod I$的等价类

而所有 $\mod I$的同余类被记为R/I

加法和乘法在I_m中用如下方程定义：

$$[a] + [b] = [a + b],\ [a][b] = [ab]$$

这些公式也许能给出R/I上加和乘的运算。

1.3　引理

函数

$$\alpha : (R/I) \times (R/I) \to R/I\text{由函数}([a], [b]) \to [a + b]\text{定义}$$

和

$$\mu : (R/I) \times (R/I) \to R/I1([a], [b]) \to [ab]\text{定义}$$

都是R/I中定义良好的函数

证明： 若$\equiv$是集合X上的等价关系，那么$[a] = [a']$当且仅当$a - a' \in I$。若$[a] = [a']$和$[b] = [b']$，则$[a+b] = [a'+b']$，因此，若$a-a' \in I$和$b-b' \in I$，则$(a - a') + (b - b') = (a + b) - (a + b)' \in I$，因此$[a + b] = [a' + b']$证明完毕。

接着我们证明乘法的定义是良好的，

$$ab - a'b' = (ab - ab') + (ab' - a'b') = a(b - b') + (a - a')b \in I$$

由于主理想被元素乘积ri封闭，其中$r \in R, i \in I$，因此$[ab] = [ab']$

1.4　定理

若I是交换环中的理想，则R/I带上引理1.3的加法和乘法是交换环。

证明： 我们来检查交换环的定义

首先，由于$a+b=b+a\in R$，有

$$[a]+[b]=[a+b]=[b+a]=[b]+[a]$$

其次 $[a]+([b]+[c])=[a]+[b+c]=[a+(b+c)]=[a+b]+c=[(a+b)+c]$

第三条，定义$0=[0]$，其中0是R中的元素，$0+[a]=[0+a]=[a]$，因为$0+a=a\in R$

第四条，定义$[a]'=[-a]$，而$[-a]+[a]=[-a+a]=[0]=0$

第五条，$ab=ba\in R$，我们有$[a][b]=[ab]=[ba]=[b][a]$

第六条，$[a]([b][c])=[a][bc]=[a(bc)]$，而$([a][b])[c]=[ab][c]=[(ab)c]$。这个结果的合理性是继承自$a(bc)=(ab)c\in R$的

第六条，定义$1=[1]$，那么$1[a]=[1a]=[a]$，这是因为$1a=a\in R$

第七条，$[a]([b][c])=[a][b+c]=[a(b+c)]$，而$[a][b]+[a][c]=[ab]+[ac]=[a(b+c)]$

1.5 定义：商环

交换环R/I被称为R模 I的商环。

I_m中的同余类有另一种说明，即陪集：

$$[a]=\{b\in Z:b=a+km,k\in Z\}=a+(m)$$

1.6 定义：陪集

若R是交换环且I是理想，则陪集指的是R的形如

$$a+I=\{b\in R:b=a+i,i\in I\}$$

的子集。

我们同样可以证明陪集也是同余类。

1.7 引理

若R是交换环且I是理想，则对每个$a\in R$，R/I中的同余类是陪集

$$[a]=a+I$$

证明： 若$b \in [a]$，则$b-a \in I$有$b = a + (b-a) \in a + I$，那么$[a] \subseteq a + I$，对于反包含，若$c \in a + I$，则$c = a + i$对某个$i \in I$成立，那么$c - a \in I$，因此$c \equiv a \in I$有$c \in [a]$，因此$a + I \subseteq [a]$得到$[a] = a + I$

陪集的符号$a + I$是比较常用的，为此定义

$$R/I = \{a + I : a \in I\}$$

1.8 定义：自然映射

1. 令I是交换环R中的理想，则自然映射$\pi : R \to R/I$是满射同态，且ker是I
2. R的子集J是理想当且仅当J是R到某个交换环的同态的ker

证明1： 自然的，$\pi(1) = 1 + I$。现在由R/I中的加法给出：

$$\pi(a) + \pi(b) = (a + I) + (b + I) = a + b + I = \pi(a + b)$$

而乘法给出：

$$\pi(a)\pi(b) = (a + I)(b + I) = ab + I = \pi(ab)$$

所以$\pi : R \to R/I$是同态。

为了证明是满射，R/I的元素是陪集$a+I$，由于$a+I = \pi(a)$，若$a \in I$，则$\pi(a) = a + I = I$成立，因此$I \subseteq \ker \pi$，对于反包含，$a \in \ker \pi$，那么$\pi(a) = a + I = I$，则$a \in I$有$\ker \pi = I$

1.9 第一同构定理

若$\varphi : R \to S$是交换环的同态，则$\ker \varphi$是R中的理想，imφ是S的子环，则这里存在一个同构

$$\widetilde{\varphi} : R/\ker \varphi \to \mathrm{im}\varphi$$

由$\widetilde{\varphi} : a + \ker \varphi \to \varphi(a)$定义。

证明： 设$I = \ker \varphi$，我们引入如下定理：

> 若$f : A \to R$是环同态，其中R是非零环，则im$f$是R的子环且$\ker f$是满足下列条件的真子集：

1. $0 \in \ker f$

2. $x, y \in \ker f \Rightarrow x + y \in \ker f$

3. $x \in \ker f, a \in A \Rightarrow ax \in \ker f$

因此I就是R中的理想，且$\mathrm{im}\varphi$就是S的子环。且$\widetilde{\varphi}$是定义良好的

若$a+I=b+I$，则$a-b\in I=\ker\varphi$，因此$\varphi(a-b)=0$，但$\varphi(a-b)=\varphi(a)-\varphi(b)$，因此$\widetilde{\varphi}(a+I)=\varphi(a)=\varphi(b)=\widetilde{\varphi}(b+I)$，因此$\widetilde{\varphi}$是同态。

为了证明是同构，首先有$\widetilde{\varphi}(1+I)=\varphi(1)=1$

其次

$$\begin{aligned}\widetilde{\varphi}((a+I)+(b+I)) =&\widetilde{\varphi}(a+b+I)\\ =&\varphi(a+b)\\ =&\varphi(a)+\varphi(b)\\ =&\widetilde{\varphi}(a+I)+\widetilde{\varphi}(b+I)\end{aligned}$$

第三，对于乘法则有

$$\begin{aligned}\widetilde{\varphi}((a+I)(b+I)) =&\widetilde{\varphi}(ab+I)\\ =&\varphi(ab)\\ =&\varphi(a)\varphi(b)\\ =&\widetilde{\varphi}(a+I)\widetilde{\varphi}(b+I)\end{aligned}$$

$\widetilde{\varphi}$是满射的，为了证明这个，我们令$x\in\mathrm{im}\varphi$，则$x=\varphi(a)$对某个$a\in R$是成立的。因此$x=\widetilde{\varphi}(a+I)$

最后，我们来证明其是单射的，若$a+I\in\ker\widetilde{\varphi}$，则$\widetilde{\varphi}(a+I)=0$，但$\widetilde{\varphi}(a+I)=\varphi(a)$，因此$\varphi(a)=0$，$a\in\ker\varphi=I$，则$a+I=I=0+I$，所以$\ker\widetilde{\varphi}=\{0+I\}$且$\widetilde{\varphi}$是单射

1.10 引理

若k是域，则素域与Q或者对某个素数p的F_p同构

证明： 我们将k中的单位表示为ϵ，然后让我们考虑一个同态$\chi : Z \to k$由$\chi(n) = n\epsilon$定义。由于Z中的理想是主理想，则这里存在一些整数$m \geq 0$使得$\chi = (m)$，若$m = 0$，则χ是单射。并且，$\mathrm{im}\chi$是k的子环且同构于Z。而Q是Z的分式域，现在我们引入如下命题：

1. 若A和R是整环，且$\varphi : A \to R$是环同态，则$[a, b] \to [\varphi(a), \varphi(b)]$是环同构$Frac(A) \to Frac(R)$
2. 证明，若域k含有和Z同构的子环，则k含有和Q同构的子域。

则$Q = Frac(Z) \cong Frac(\mathrm{im}\chi)$，现在由于$Q$是包含$Z$作为子环的的最小域，现在我们再导入一个命题辅助证明：

设k是一个域，R是子环：

$$R = \{n \cdot 1 : n \in Z\} \subseteq k$$

证明：k的子域F是素域当且仅当它是k中包含R的最小子域。

[1]

由假设和上述命题可知k的素域同构于Q

[1] 设$f : Frac(A) \to Frac(R)$由函数$[a, b] \to [\varphi(a), \varphi(b)]$决定，首先$\varphi[1, 1] = [1, 1]$是绝对的。其次，对任意$a, b, a', b' \in A$有

$$f([a, b] + [a', b']) = f([a + a', b + b']) = [\varphi(a + a'), \varphi(b + b')]$$

但由于φ是同态，则得到

$$\begin{aligned}[\varphi(a + a'), \varphi(b + b')] =& [\varphi(a) + \varphi(a'), \varphi(b) + \varphi(b')] \\ =& [\varphi(a), \varphi(b)] + [\varphi(a'), \varphi(b')] \\ =& f([a, b]) + f([a', b'])\end{aligned}$$

是同态，对乘法如法炮制既可得到相同的结果，因此f是个环同态。然后我们证明其是双射的。首先，对任意$[\varphi(a), \varphi(b)] = f([a, b])$成立，所以是一个满射，其次，我们设存在$a = a', b = b' \in A$且$f([a, b]) \neq [\varphi(a'), \varphi(b')]$。由于$a = a', b = b'$，那么有$a - a' = b - b' = 0$有$f([a - a', b - b']) = [\varphi(a) - \varphi(a'), \varphi(b) - \varphi(b')] = 0$矛盾，因此$f$是单射得到$f$是一个同构。

对于第二个命题，我们设k中和Z同构的子环为A，而$Q = Frac(Z)$，则我们定义函数$f : A \to Z$是同构，利用第一个命题可知$Frac(A)$就是与Q同构的子域。

若$m\neq 0$，则第一同构定理给出$F_m=Z/(m)\cong \mathrm{im}\chi\subseteq k$，由于$k$是域。若$m$是素数，则$\mathrm{im}\chi$是整环。若$m=p$，则$\mathrm{im}\chi$记为$\mathrm{im}\chi=\{0,\epsilon,2\epsilon,\cdots,(p-1)\epsilon\}$是同构于$F_p$的子域，再利用刚才引入的命题可知$\mathrm{im}\chi$是素域。

1.11 定义：特征

若域k的素域同构于Q，则k有特征0，若同构于F_p，其中p是素数，则k的特征为p

域$Q,R,C,C(x)$都是特征为0，且后三个域的任何子域特征也是0。每个有限域以某个素数p作为特征，例如：F_p上所有有理函数构成的函数域$F_p(x)$的特征为素数p

1.11.1 例子

考虑由$f(x)\to f(i)$定义的同态$\varphi:R[x]\to C$，其中$i^2=-1$。那么$\varphi:\sum_k a_kx^l\to\sum_k a_ki^k$，让我们利用第一同构定理找到$\mathrm{im}\varphi$和$\ker\varphi$。

首先，φ是满射，若$a+bi\in C$，则$a+bi=\varphi(a+bx)\in\mathrm{im}\varphi$，其次

$$\ker\varphi=\{f(x)\in R[x]:f(i)=0\}$$

是所有以i为根的多项式集合。当然，$x^2+1\in\ker\varphi$，我们断言$\ker\varphi=(x^2+1)$，由于$R[x]$是PID，则理想$\ker\varphi$可以由首一的最低次多项式生成它。若x^2+1不能生成$\ker\varphi$，则x^2+1在$R[x]$中是可约的，意味着有实根，而第一同构定理告诉我们$R[x]/(x^2+1)\cong C$。

因此，我们从实数出发到复数来构造商环。当我们不知道什么是复数时，它可以被定义为$R[x]/(x^2+1)$。当我们用这种方法构造的好处就是不需要验证所有域公理。它会继承这些公理。

1.12 定理

若k是域且$I=(p(x))$，其中$p(x)\in k[x]$是非常数的，那么下面的话是等价的：

1. $k[x]/I$是域
2. $k[x]/I$是整环
3. $p(x)$在$k[x]$中不可约

证明： 首先，域都是整环。

其次，若$p(x)$是可约的，则存在因式分解$p(x) = g(x)h(x) \in k[x]$，其中$\deg(g) < \deg(p)$且$\deg(h) < \deg(p)$，若$g(x) \in I = (p)$，则$p(x) \mid g(x)$且$\deg(p) < \deg(g)$是一个矛盾，因此在$k[x]/I$中$g(x) + I \neq 0 + I$，类似的$h(x) + I \neq 0 \in k[x]/I$，但是

$$(g(x) + I)(h(x) + I) = p(x) + I = 0 + I$$

在商环中是零元，与$k[x]/I$是整环矛盾，因此$p(x)$不可约。

然后我们从3推1，由于$p(x)$不可约，所以$p(x)$不是单位得到理想$I = (p(x))$不包含1。因此$1 + I \neq 0 \in k[x]/I$，若$f(x) + I \in k[x]/I$是非零的，则$f(x) \neq I$。所以，$f(x)$不是$p(x)$的倍数，有$p \nmid f$，所以p, f互素存在一些多项式s, t使得$sf + tp = 1$有$sf - 1 \in I$，所以$1 + I = sf + I = (s + I)(f + I)$意味着每个$k[x]/I$的非零元素都存在逆，所以$k[x]/I$是域。

1.13 命题

1. 若k是域，令$p(x) \in k[x]$是不可约多项式和$I = (p(x))$，则$k[x]/(p(x)) = k[x]/I$是域且包含k和$p(x)$的一个根z
2. 若$g(x) \in k[x]$且z也是$g(x)$的一个根，有$p(x) \mid g(x)$

证明： 记商环$k[x]/I = K$是域。由定理1.12可知$p(x)$不可约。定义$\varphi : k \to K$由$\varphi(a) = a + I$定义，则φ是同态。且k是域[2]因此φ是单射，利用定义1.8可知，φ是一个从k到$k' = \{a + I : a \in k\} \subseteq K$的子域的同构。

而x是$k[x]$中的特殊元素，我们声称$z = x + I \in K$是$p(x)$的根，现在令

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n$$

，其中$a_i \in k$对所有i成立。在$k[x]/I$，我们有

$$\begin{aligned}
p(z) =& (a_0 + I) + (a_1 + I)z + \cdots + (a_n + I)z^n \\
=& (a_0 + I) + (a_1 + I)(x + I) + \cdots + (a_n + I)(x + I)^n \\
=& (a_0 + I) + (a_1 x + I) + \cdots + (a_n x^n + I) \\
=& a_0 + a_1 x + \cdots + a_n x^n + I \\
=& p(x) + I = I
\end{aligned}$$

[2]验证$\ker \varphi = \{0\}$即可

，因为$p(x) \in I = (p(x))$，但I是$k[x]/I$中的零元素，所以z是$p(x)$的根。

对于第二个命题,由于z是$g(x)$的根，则$g(x) \in \ker \pi$，其中$\pi : k[x] \to k[x]/(p(x))$是自然映射，那么综上所述$p(x) \mid g(x)$

1.14 定理

令k是域且$f(x) \in k[x]$是次数$n \geq 1$的非零多项式，令$I = (f(x))$，再令$K = k[x]/I$，则每个K中的元素都有唯一表示：

$$b_0 + b_1 z + \cdots + b_{n-1} z^{n-1}$$

其中$z = x + I$是$f(x)$的根且所有$b_i \in k$

证明： 每个K的元素形如$g(x) + I$，其中$g(x) \in k[x]$，由除法算式可得，存在一些多项式$q(x), r(x) \in k[x]$使得$g(x) = q(x)f(x) + r(x)$且$\deg(r(x)) < n = \deg(f)$或者$r(x) = 0$，由于$g - r = qf \in I$那么$g(x) + I = r(x) + I$，就像我们在定理1.13做的一样，我们也可以把$r(x) + I$重写为

$$r(z) = b_0 + b_1 z + \cdots + b_{n-1} z^{n-1}$$

其中$b_i \in k$

现在证明唯一性，设

$$r(z) = b_0 + b_1 z + \cdots + b_{n-1} z^{n-1} = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1}$$

其中所有$c_i \in k$。然后定义$h(x) \in k[x]$为$h(x) = \sum_{i=0}^{n-1}(b_i - c_i)x^i$。由于$z$是$h(x)$的根。则我们有$h(x) \in (f(x))$，因此$f(x) \mid h(x)$，若$h$是非零多项式，则$\deg(h) \geq n = \deg(f)$，但我们有$\deg(h) < n$。得到矛盾，所以$h(x) = 0$且对所有$i$都有$b_i = c_i$

1.15 定义：伴随(adjoining)

令K是域和k为子域，若$z \in K$，则我们定义$k(z)$是K中包含k和z的最小域。因此$k(z)$被称为从伴随着z的k中得到的域

例如：$C = R(i)$，复数是从实数伴随着i得到的。

1.16 命题

令k是域K的子域且设$z \in K$，则

1. 若z是某个非零多项式$f(x) \in k[x]$的根，且z也是不可约多项式$p(x) \in k[x]$的根，$p(x) \mid f(x)$

2. 对每个命题1中的$p(x)$，都存在一个同构

$$\varphi : k[x]/(p(x)) \to k(z)$$

   使得$\varphi(x + (p(x))) = z$且$\varphi(a) = a$对所有$a \in k$成立

3. 若z, z'是$p(x)$在K中的根，则有一个同构$\theta : k(z) \to k(z')$使得$\theta(z) = z'$且使得$\theta(a) = a$对每个$a \in k$成立

4. 每个$k(z)$的元素都有形如

$$b_0 + b_1 z + \cdots + b_{n-1} z^{n-1}$$

   的唯一表示。其中$b_i \in k$且$n = \deg(p)$

证明： 定义同态$\varphi : k[x] \to K$由$\varphi(x) = z$定义，那么对于多项式则有

$$\varphi : \sum b_i x^i \to \sum b_i z^i$$

注意$\varphi(a) = a$对所有$a \in k$固定。现在$f(x) \in \ker \varphi$，这是因为z是f的根。且$\ker \varphi$是$k[x]$中的非零理想。所以$\ker \varphi$形如$(p(x))$。这是因为$k[x]$是PID，所以结论是准确的，并且$\mathrm{im}\varphi$是K的子环，所以它是整环[3]，由定理1.12可知$p(x)$在$k[x]$中不可约。

现在我们同时考虑$p, f \in k[x]$和每个在$K[x]$中的乘积$(x-z)$。那么$\gcd(f, p) \in K[x]$不等于1，且不管在$k[x]$还是$K[x]$中计算都是不变的，所以$p(x)$不可约。综上所述$p \mid f \in k[x]$

证明2： 由于$p(x)$不可约，那么$k[x]/(p(x))$是一个域，由定理1.12得$\mathrm{im}\varphi$是域[4]。由于$k(z)$是包含k, z的最小域，不难得到$\mathrm{im}\varphi$包含$k(z)$，因此$k(z) \subseteq \mathrm{im}\varphi$。现在，对于另一方面，$\mathrm{im}\varphi$是形如$g(x) + I$的集合，其中$g \in k[x]$，

[3] 域的子环是整环

[4] 因为$\mathrm{im}\varphi$同构$k[x]/(p(x))$，所以其是域。

那么对于任意K中包含k, z的子域S来说，它是应该包含φ的，这是因为，当我们利用第一同构定理给出这些条件之后，我们是把$a + \ker\varphi$映射到$\varphi(a)$，因此题设的映射到的就是k，那么$\mathrm{im}\varphi \subseteq k(z)$，我们得到$\mathrm{im}\varphi = k(z)$

证明3： 我们只需要定义同构$\psi : k[x]/(p(x)) \to k(z')$且$\psi(a) = a, \psi(x + p(x)) = z'$即可，再复合$\theta = \psi \circ \varphi^{-1}$就是我们需要的函数了。

证明4： 利用定理1.14，每个$k[x]/I$中的元素，其中$I = (p(x))$都是有唯一表示为：$b_0 + b_1(x + I) + \cdots + b_{n-1}(x + I)^{n-1}$的。由于$k[x]/I \to k(z)$是同构，所以$x + I \to z$保证了表示的唯一。

1.17 推论

令k是域且$p(x) \in k[x]$是不可约多项式，若$K = k[x]/I$，其中$I = (p(x))$，若$\alpha \in K$，则存在唯一的首一不可约多项式$h(x) \in k[x]$以α为根。

证明： 由定理1.14，$\alpha = b_0 + b_1 z + \cdots + b_{n-1} z^{n-1}$，其中$z = x + I$，且对其中所有$b_i \in k$和$\deg(p) = n$。所以，若$\alpha$是$b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$的根。利用命题1.16的1，则存在一个以$\alpha$为根的不可约多项式。

为了证明$h(x)$唯一。我们设$g(x) \in k[x]$是另一个以α为根的不可约首一多项式。在$K[x]$中，$\gcd(h, g) \neq 1$，这是因为都被$x - \alpha$整除，由于h是不可约的，因此其唯一的公因子只有1和自身，那么我们有$(h, g) = h$，因此$h(x) \mid g(x)$，但g也是不可约的，因此$h = g$。

1.18 定理：克罗内克

若k是域且$f(x) \in k[x]$是非常数的，则存在一个域K，它包含k作为子域使得$f(x)$在$K[x]$中分裂，因此$f(x)$可以在$K[x]$中表示为一些线性多项式的乘积

当我们说$f(x)$可以在K中表示为线性多项式的乘积时，我们说它在$K[x]$中分裂

证明： 我们通过归纳$\deg(f)$来证明定理。若E是任意的包含k作为子域的域，则这里有一个域K使得$f(x)$在$K[x]$中表现为一些多项式的乘积，若$\deg(f) = 1$，则$f(x)$是线性的，可以直接选择$K = E$

现在，对于归纳步骤，考虑两个可能的例子，若$f(x)$是不可约的，则$f(x) = g(x)h(x) \in k[x]$。其中$\deg(g), \deg(h) < \deg(f)$，由归纳法，这里有一个包含$k$的域$E$使得$g(x)$在$E$中分裂。

归纳假设的第二个用途是：证明K包含E使得h在K中分裂。因此$f(x) = g(x)h(x)$在K上分裂。若$p(x)$是$k[x]$中的不可约多项式。则命题1.13的(1)证明了E包含k, z和一个$p(x)$的根z，因此$p(x) = (x - z)l(x) \in E[x]$。由归纳假设，我们就找到了一个被$K$包含的$E$中一个多项式$l(x)$，因此$f(x) = (x - z)l(x)$在$K[x]$上分裂

1.19 命题

若E是有限域，则$\mid E \mid = p^n$对某个p和$n \geq 1$成立。

证明： 由引理1.10我们知道，若k是E的素域，那么$k \cong Q$或者F_p对某个p成立，由于Q是无限多元的，所以 k有特征p，因此$pa = 0$对$a \in E$成立。也就是说，如果E作为加法阿贝尔群，则每个E中的非零元素都是阶为p的。若存在一些其他的素因子$q \mid\mid E \mid$，且$q \neq p$，则存在非零元素$b \in E$使得$qb = 0$矛盾，因此$\mid E \mid = p^n$对$n \geq 1$成立。

1.20 引理

若E是有限域，再令k是素域

1. 则有一些素数p使得$k \cong F_p$
2. 存在一些整数$M > 0$使得每个$z \in E$的非零元都是$x^M - 1$的根。
3. 若S是E的子域且$z \in E$，则$\mid S(z) \mid = \mid S \mid^m$对一些$m \geq 1$成立。

证明1： 由于E是有限的，所以不可能同构Q，只能是同构F_p

证明2： 令$z \in E$是非零的，由于E是有限的，则列表中存在一些重复项$1, z, z^2, \cdots$，设阶为m，则$1, z, z^2, \cdots, z^{m-1}$是互异的元，当$z^m \in \{1, z, z^2, \cdots, z^{m-1}\}$时，若$z^m \neq 1$，则$z^m = z^i$，$i < m$成立。如果$z^{m-i} = 1$，但这会引发矛盾，因为$m - i \geq m - 1$得到和$1, z, z^2. \cdots, z^{m-1}$是互异的矛盾，因此$z^m = 1$对每个$z \in E$成立。我们就找到了一个整数$m = m(z)$使得$z^{m(z)} = 1$，由

于E是有限的，我们可以定义$M = \Pi_{z\in E^\times} m(z)$，那么就对每个$z \in E^\times$都存在$z^M = 1$，因此每个非零$z \in E$都是$x^M - 1$的根。

证明3： 我们设$q(x) \in k[x]$是以z为根的不可约多项式。若$z = 0$，取$q(x) = x$，若$z \neq 0$，则命题的2部分告诉了我们$x^M - 1$有以z为根在某个域$S[x]$上成立。令$X = S \times \cdots \times S$为$d$个笛卡尔积。其中$d = \deg(q)$。由命题1.16，通过函数

$$\beta : b_0 + b_1 z + \cdots + b_{d-1} z^{d-1} \to (b_0, b_1, \cdots, b_{d-1})$$

定义映射$\beta : S(z) \to X$是一个双射，因此$\mid S(z) \mid = \mid X \mid = \mid S \mid^d$

1.21 定义：本原元素

若E是有限域，其中每个$a \in E$都等于$\pi \in E$的某个幂次，则π被称为E中的本原元素。

1.22 定理

1. 若k是域且G是乘法群$k^\times$的有限群，则G是循环群，特别的，若k自身有限，则$k^\times$也是循环的。
2. 对每个正整数m，存在一个本原单位m次根$z \in k$，因此，每个k中的m次单位根是z的幂次。

证明： 令$d \mid\mid G \mid$是一个因子，则这里存在两个G的子群且阶为d。设为S, T，则$\mid S \cup T \mid > d$。但对每个$a \in S \cup T$应该满足$a^d = 1$，因此这里有一些$x^d - 1$的根存在，但这和代数基本定理矛盾，$S \cup T$中有太多$x^d - 1$在k中的根了。因此G是循环的。

证明2： 集合$\Gamma_m = \{$k中所有m次单位根$\}$是$k^\times$的子群，因此它是一个k的循环群，Γ_m由单位的m次本原根生成。

1.23 定理：伽罗瓦

若p是素数且n是一个正整数，则这里存在一个恰好有p^n个元素的域。

证明： 记$q=p^n$，然后我们考虑多项式

$$g(x)=x^q-x\in F_p[x]$$

由克罗内克定理，则这里存在一个域E包含F_p使得其在$E[x]$中分裂，定义

$$F=\{\alpha\in E:g(\alpha)=0\}$$

因此，F是g的所有根的集合。由于$g'(x)=qx^{q-1}-1=p^nx^{q-1}-1=-1$有$(g,g')=1$，所以$g(x)$的根都是互异的。因此，$F$有$q=p^n$个元素。

如果F是E的子域，那么证明完毕。若$a,b\in F$。若$a,b\in F$，则有$a^q=a$和$b^q=b$。因此$(ab)^q=a^qb^q=ab$有$ab\in F$成立。对于$a-b$，由于$a^p=a,b^p=b$，所以$a^p-b^p=a-b$。再利用利用费马小定理，则$(a-b)^p\equiv a-b \mod p$成立，所以$(a-b)^p=a^p-b^p=a-b\in F$。最后，若$a\neq 0$，则消去律用在$a^q=a$上会得到$a^{q-1}=1$，因此a的逆就是a^{q-2}