注意，以下F均表示一个给定的域。

命题

$$\text{给定} g \in F[x], \deg g \geq 1, I = \{qg : q \in F[x]\}, H = \{h \in F[x] : \deg h \leq \deg g - 1\}$$

则商环$F[x]/I$是交换环（继承了环的交换性），且有如下性质：

$$(1) F[x]/I = \{h + I : h \in H\}\text{，并且}\forall h_1, h_2 \in H, \text{有} h_1 + I = h_2 + I \text{蕴含} h_1 = h_2$$
$$(2)\text{加法性质：}\forall f, h \in F[x]\text{，有}(f + I) + (h + I) = (f + h) + I$$
$$(3)\text{乘法性质：}\forall f_1, f_2 \in F[x], f_1 f_2 \text{对} h \text{作带余除法} f_1 f_2 = qg + h\text{，则有}(f_1 + H)(f_2 + H) = h + H$$
$$(4)\text{商环的幺元：}1_F + I$$
$$(5)\text{若} g \text{在} F \text{上不可约，则} F[x]/I \text{是域}$$
$$(6)\text{若} g \text{在} F \text{上可约，则存在} F[x]/I \text{中的两个非零元素，它们的乘积为0.则} F[x]/I \text{不是域}$$
$$(7)\text{如下定义}\sigma : F \to F[x]/I\text{，}\sigma(a) := a + I, \forall a \in F.\text{则}\sigma\text{是单同态}$$

证明

（1）任取$f \in F[x]$, 希望证明

$$f + I \in \{h + I : h \in H\}$$

作带余除法$f = qg + h$, 则有$\deg h \leq \deg g - 1$，即$h \in H$，且有$f + I = h + I$. 命题成立。
$\forall h_1, h_2 \in H, h_1 + I = h_2 + I$，有$h_2 - h_1 \in I$，则有$g \mid (h_2 - h_1)$，假设$h_2 - h_1 \neq 0$，这推出$\deg(h_2 - h_1) \geq \deg g$. 但是又有

$$\deg h_2 \leq \deg g - 1, \deg h_1 \leq \deg g - 1$$

则有

$$\deg(h_2 - h_1) < \deg g$$

矛盾。
(2)(3)(4)都是自然的。
(5) 只需证明：$F[x]/I$中的任意非零元均有乘法逆元。
任取$f \in F[x]$，使得$f + I \neq I$. 希望找到$f + I$的乘法逆元。

回忆不可约多项式的一个重要性质：
若$g \in F[x]$不可约，则下面两个命题之一成立：

1. $g \mid f$
2. 存在$u, v \in F[x]$，使得$gu + fv = 1_F$.

回到原题，由$f+I\neq I$，有$f\notin I$.由g不可约，$g\nmid f$. 则存在$u,v\in F[x]$，使得$gu+fv=1_F$. 我们断言：$v+I$是$f+I$的乘法逆元。这是因为

$$(f+I)(v+I)=fv+I=(1_F-gu)+I=1_F+I$$

最后一个等号成立是因为$gu\in I$.
(6) 由g在F上可约，存在$h_1,h_2\in F[x]$，使得$g=h_1h_2$，其中$\deg h_1\geq 1,\deg h_2\geq 1$. 则有

$$1\leq \deg h_1,\deg h_2\leq \deg g-1$$

那么自然有$h_1,h_2\in H$. 由$h_1\neq 0,h_2\neq 0$，有$h_1+I,h_2+I\neq I$. 即h_1+I,h_2+I都是商环中的非零元。但是又有

$$(h_1+I)(h_2+I)=h_1h_2+I=g+I=I$$

最后一个等号成立是因为$g\in I$. 即h_1+I,h_2+I的乘积是商环中的零元。综上，此时商环不是域。

另一种理解商环的方式：不是将陪集作为商环的元素，而是从陪集中选取代表元组成商环。
考虑结构$(H,+,\otimes)$，其中H的定义同上，$+$为多项式加法，$\otimes$定义如下：
$\forall f_1,f_2\in H,\ f_1f_2$对$g$作带余除法

$$f_1f_2=qg+h,h\in H$$

则定义

$$f_1\otimes f_2:=h$$

我们容易验证这个结构的封闭性。事实上，$(H,+,\otimes)$是交换环，1_F是其幺元，$F\subset H$.
这在本质上也是商环。因为它和我们上面所说的“一般意义上的商环”是同构的，即

$$(H,+,\otimes)\cong F[x]/I$$

并且很容易给出一个同构映射

$$\phi:H\to F[x]/I,\phi(h)=h+I,\forall h\in H$$

例子：扩域

$\mathbb{R}\to\mathbb{C}$

考虑$\mathbb{R}[x]$上的多项式$g=x^2+1$. $H=\{a+bx:a,b\in\mathbb{R}\}$为次数小于$g$的多项式全体.
$I=\{(x^2+1)q:q\in\mathbb{R}[x]\}$,$\mathbb{R}[x]/I=\{a+gx+I:a,b\in\mathbb{R}\}$. 注意

$$(x+I)(x+I)=x^2+I=(-1+x^2+1)+I=-1+I$$

亦即

$$(x+I)^2=-1+I$$

这就似乎是一个很像**虚数单位**的元素了。
还有：

$$(a+bx)+I+(c+dx)+I=(a+c)+(b+d)x+I$$

$$\begin{aligned}&(a+bx+I)(c+dx+I)\\=&(ac+(bc+ad)x+bdx^2)+I\\=&(ac+(bc+ad)x+bd(x^2+1)-bd)+I\\=&((ac-bd)+(bc+ad)x)+I\end{aligned}$$

我们可以看到这和复数的加法和乘法运算是等价的。事实上，我们和容易给出从$\mathbb{C}$到$\mathbb{R}[x]/I$的同构ϕ

$$\phi(a+bi)=a+bx+I$$

特别地，$\phi(i)=x+I$.
这就从商环的角度从$\mathbb{R}$构造出了$\mathbb{C}$.

直接从H也能构造出复数。考虑$(H,+,\otimes)$上的加法和乘法：

$$(a+bx)+(c+dx)=(a+c)+(b+d)x$$

$$(a+bx)(c+dx)=ac+(ad+bc)x+bdx^2=bd(x^2+1)+(ac-bd)+(ad+bc)x$$

对它作带余除法，就得到

$$(a+bx)\otimes(c+dx)=(ac-bd)+(ad+bc)x$$

可以看到，通过映射

$$\phi:\mathbb{C}\to H,\phi(a+bi):=a+bx$$

有$\mathbb{C}\cong(H,+,\otimes)$.

F_2的扩张

考虑$F_2=(\{0,1\},\oplus,\otimes)$. 其中加法和乘法都是模2的运算，以及$F_2[x]$（加法和乘法继承$F_2$的加法和乘法）
考虑$F_2[x]$上的多项式x^2+x+1. 它在F_2上不可约。则F_2上所有次数小于2的多项式

$$H=\{0,1,x,1+x\}$$

构成的结构$(H,+,\otimes)$为域。其中$\otimes$是模(x^2+x+1)的乘法。这里我们就得到了一个更大的域。F_2中只有两个元素，但是H中有4个。我们看看它上面的乘法：

$$x\otimes(x+1)=x^2+x=(x^2+x+1)+1=1$$

$$x\otimes x=x^2=(x^2+x+1)+(x+1)=x+1$$

$$(x+1)\otimes(x+1)=x^2+2x+1=(x^2+x+1)+x=x$$

类似地，我们还可以得到等大的域，通过其他的多项式。我们可以断言x^3+x+1在F_2上不可约。

$$\begin{aligned}H&=\{h:h\in F_2[x],\deg h\leq 2\}\\&=\{0,1,x,1+x,x^2,x^2+1,x^2+x,x^2+x+1\}\end{aligned}$$

由于不可约性，有$(H,+,\otimes)$是域，其中$\otimes$是模x^3+x+1乘法。这就得到一个8元素有限域。

> 注意：通过模不可约多项式构造更大的有限域，在考试中很可能涉及。

一个结论是，两个元素个数相同的有限域总是同构的。因此，我们可以将所有的有限域都视为某种形式具体的多项式。

考虑有乘法幺元的交换环R及其上的多项式全体，我们有如下结论：

命题

设$u\in R$，则有$\forall f,g\in R[x]$，成立

$$(f+g)(u)=f(u)+g(u),(fg)(u)=f(u)g(u)$$

（左边的运算是多项式之间的运算，右边的是环上的运算）

证明

- 加法：
  记
  $$f=a_0+a_1x+a_2x^2+...+a_nx^n$$
  $$g=b_0+b_1x+b_2x^2+...+b_nx^n$$
  之所以可以假设它们有相同数量的项，是因为缺少的项可以用系数0补齐。
  则有
  $$f(u)+g(u)=\sum_{i=0}^{n}a_iu^i+\sum_{i=0}^{n}b_iu^i=\sum_{i=0}^{n}(a_i+b_i)u^i$$
  又有
  $$f+g=\sum_{i=0}^{n}(a_i+b_i)x^i$$

从而

$$(f+g)(x)=\sum_{i=0}^{n}(a_i+b_i)u^i$$

即上述加法性质是成立的。

- 乘法

  记

$$f=a_0+a_1x+a_2x^2+\ldots+a_mx^m$$

$$g=b_0+b_1x+b_2x^2+\ldots+b_nx^n$$

则有

$$fg=\sum_{k=0}^{m+n}(\sum_{i=0}^{m}a_ib_{k-i})x^k$$

这里需要注意：右式就是**多项式乘法的定义**。这里并没有所谓交换律分配律之类性质。（当然，给出这样的定义，是为了确保多项式的运算在形式上满足这些性质）

$$(fg)(u)=\sum_{k=0}^{m+n}(\sum_{i=0}^{m}a_ib_{k-i})u^k$$

又有

$$f(u)=\sum_{i=0}^{m}a_iu^i$$

$$g(u)=\sum_{i=0}^{n}b_iu^i$$

从而

$$\begin{aligned}f(u)g(u)&=(\sum_{i=0}^{m}a_iu^i)(\sum_{i=0}^{n}b_iu^i)\\&=\sum_{i=0}^{m}\sum_{j=0}^{n}a_iu^ib_ju^j\\&=\sum_{i=0}^{m}\sum_{j=0}^{n}a_ib_ju^{i+j}\\&=\sum_{k=0}^{m+n}(\sum_{i=0}^{m}a_ib_{k-i})u^k\end{aligned}$$

即上述乘法性质也是成立的。需要注意的是，第三个等号成立用到了环上**乘法的交换性**。如果R不是交换环，那么这步就未必成立。也就是说，多项式的赋值和乘法的可交换性，需要它的环上的乘法的可交换性。

从这里的赋值性质出发，在我们熟知的交换环$\mathbb{R}$上，有如下性质：

$$\forall u \in \mathbb{R}, f(u) = g(u) \implies \forall u \in \mathbb{R}, (f-g)(u) = 0 \implies g - f = 0 \implies g = f$$

第二步$\implies$由代数基本定理保证。然而，这一性质未必对所有的交换环R都成立。即，对任意的交换环R（注意区分$\mathbb{R}$和R（）），未必有

$$\forall u \in R, f(u) = g(u) \implies g = f$$

一个例子是之前提过的F_2. 例如：

$$f = x + 1, g = x^2 + 1$$

则有

$$f(0) = g(0), f(1) = g(1)$$

但是显然没有$f = g$. 可以看到会出现这种情况的原因是，$x = x^2$在F_2上总是成立。同样地，因为$x = x^4$在F_4上总是成立，$f = x + 1$和$g = x^4 + 1$也给出一个例子。$x = x^4, \forall x \in F_4$的证明：
当$x = 0$时，命题显然成立；当$x \neq 0$时，$x^3 = 1$. 注意$(F_4 - \{0\}, \cdot)$是三阶群，故它的元素的三次方必然都为1，于是命题也成立。

我们接下来回到域上的多项式。

余式定理

给定$f \in F[x], a \in F$. 则存在$q \in F[x]$，使得

$$f = q(x-a) + f(a)$$

特别地，有

$$(x-a) \mid f \iff f(a) = 0$$

证明

f对$x - a$作带余除法，则存在$q, r \in F[x]$，使得

$$f = q(x-a) + r$$

又有

$$\deg r \leq \deg(x-a) - 1 = 0$$

故r是常数。我们对上述等式赋值a，有

$$f(a) = q(a-a) + r$$

从而

$$r = f(a)$$

推论

给定$f \in F[x]$是次数不小于2的不可约多项式。则有

$$\forall u \in F，有 f(u) \neq 0$$

证明是简单的。若否，则存在$u \in F$使得$f(u) = 0$，则有$(x-u) \mid f$. 但$\deg f \geq 2$，矛盾!

请注意，反过来未必成立，即没有根未必可以推出不可约。

又一个推论

给定$f \in F[x], \deg f = n \geq 0$. 则$f$在$F$上至多有$n$个根。
证明：对次数归纳即可。
若$n = 0$, 即$f = a \in F - \{0\}$，则有$\forall u \in F，f(u) = a \neq 0$.
若$n \geq 1$，若f没有根，则命题显然成立；下设存在$v \in F$，使得$f(v) = 0$. 于是存在$q \in F[x]$，使得$f = q(x-v)$.
于是，对f的任意根$u \neq v$，有$q(u) = 0$（注意，这个断言用到了**域**的性质。对于域上的两个元素$ab = 0$，有$a = 0$或$b = 0$，若非域上，这个性质未必成立）. 又由归纳假设，q在F上至多有$(n-1)$个根，从而f在F上至多有n个根。

可以看到证明过程中用到了域的性质。事实上，该结论若不在域上，确实未必成立。我们接下来给出一个反例。
设R, S都是环。考虑$(R \times S, +, *)$. $\forall (a,b), (c,d) \in R \times S$，定义：

$$(a,b) + (c,d) := (a+c, b+d)$$
$$(a,b) * (c,d) := (ac, bd)$$

显然上述结构有加法幺元$(0_R, 0_S)$. 若R, S都有加法幺元，则上述结构也有乘法幺元$(1_R, 1_S)$. 事实上，我们很容易验证$(R \times S, +, *)$是一个环。这种通过笛卡尔积产生新环的操作是常见的，考试可能会考。
考虑交换环$R = \mathbb{Z}_4 \times \mathbb{Z}_4$. $\mathbb{Z}$中满足$u^2 = 0$的元素有$u = 0$和$u = 2$. 于是R上$u^2 = 0$的解有如下四个:

$$(0,0), (0,2), (2,0), (2,2)$$

而非我们预期中的“至多2个”。

设$g \in F[x]$是F上的不可约多项式。我们知道，$F[x]/I$是一个域。其中I是F上所有g的倍式的集合。这是得到更大的域的过程，现在我们也可以反其道而行。

以下是一个常见的操作：
任取$\alpha \in \mathbb{C}$，将α添加到$\mathbb{Q}$中得到包含$\mathbb{Q}$和α的最小子域$\mathbb{Q}[\alpha]$.
例如，$\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$，其中$i$为虚数单位。我们容易验证$\mathbb{Q}[i]$对于加法、乘法、求逆都封闭。
又例如，$\mathbb{Q}[e] = \{a + be : a, b \in \mathbb{Q}\}$，其中$e$为自然对数的底。我们可以验证它对乘法不封闭（会引入e^2.）然而，即使加入了e^2，这个结构对于乘法仍然不封闭，因为又会引入e^3，以此类推. 最终，如果需要确保乘法封闭性，这个结构最小是

$$\{a_0 + a_1 e + a_2 e^2 + \ldots + a_n e^n : n \in \mathbb{N}, a_i \in \mathbb{Q}\}$$

或者写成

$$\{f(e) : f \in \mathbb{Q}[x]\}$$

然而这还是不够，因为这个结构对求逆尚不封闭。为了使它对求逆也封闭，这个结构最小是

$$\{\frac{f(e)}{g(e)} : f, g \in \mathbb{Q}[x], g(e) \neq 0\}$$

这两个例子相当不同，一个原因是，前者加入的数是$\mathbb{Q}$上代数方程的根，而后者不是。

接下来给出严格的定义。

子域的定义

给定域$(K, +, \cdot)$. $F \subset K$, 若$(F, +, \cdot)$是域，则称F是$(K, +, \cdot)$的子域。

容易证明：F是$(K, +, \cdot)$的子域当且仅当以下条件满足：

1. $0 \in F, 1_K \in F$.
2. $\forall a, b \in F, a + b \in F, -a \in F, ab \in F$.
3. $\forall a \in F, a \neq 0, a^{-1} \in F$.
   （主要是确保运算的封闭性和幺元的存在性）

代数元/超越元的定义

给定域K及其子域F，任取$\alpha \in K$，若存在$f \in F[x], f \neq 0$，使得$f(\alpha) = 0$，则称α是F上的代数元。若不存在上述f，则称α是F上的超越元。

取$K = \mathbb{C}, F = \mathbb{Q}$，则这就是代数数和超越数的定义。
上一行环视$KF\mathbb{C}$了，谁来V我50啊（）