我们考虑一般域上多项式的性质。

- 多项式的次数
- 带余除法与整除
- 最大公因式
- 不可约多项式
  这些性质，与$\mathbb{Z}$上的数论性质几乎可以一一对应。读者可以注意这种关联性。

定义——多项式的次数

1. 0多项式的次数为$-\infty$.
2. 对

$$f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n, \text{其中} a_n \neq 0$$

   定义其次数为n. 记为$\deg f = n$.

多项式次数的基本性质

设f,$g \in F[x]$是域F上的多项式，则有：

$$\deg(f+g) \leq \max\{\deg f, \deg g\}$$

$$\forall a \in F, a \neq 0, \deg(af) = \deg f$$

$$\deg(fg) = \deg f + \deg g$$

推论：两个非零多项式之积非零。
对于第一条性质，等号**不成立**的情况是$\deg f = \deg g$并且相加时最高项次数恰好抵消；当$\deg f \neq \deg g$时，等号**一定成立**。

证明：

(1) 记$n = \max\{\deg f, \deg g\}$, $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{n} b_i x^i$.
则有

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

所以当然有$\deg(f+g) \leq n$. 上述等号成立与不成立情形的讨论，也容易从这个证明中看出。

(2) 证明类似(1), 这是显然的。并且，这条性质也可视为第三条性质的特殊情况（其中一个多项式是0次）

但是需要注意的是，这里用到域上的一个结果：

$$对u, v \in F, u, v \neq 0, 则有uv \neq 0$$

这是因为，假设$uv = 0$，则有

$$(uv)v^{-1} = 0v^{-1} = 0$$

并且

$$(uv)v^{-1} = u(vv^{-1}) = u1_F = u$$

于是$u = 0$. 矛盾！值得指出，对于一般的域，我们不应当将这个结果视为显然的，而应该给出这样的一个证明。

(3) 注意我们规定了$\deg 0 = -\infty$，因此命题对于有0多项式的情形成立。下面考虑$f, g \neq 0$的情形。
记$m = \deg f, n = \deg g$. 并记

$$f = \sum_{i=0}^{m} a_i x^i, g = \sum_{i=0}^{n} b_i x^i$$

注意这里有$a_m, b_n \neq 0$
则有

$$fg = \sum_{k=0}^{m+n} (\sum_{i+j=k} a_i b_j) x^k$$

注意当$k = m + n$时，求和式$\sum_{i+j=k} a_i b_j = a_m b_n \neq 0$, 因此有

$$\deg(f + g) = m + n = \deg f + \deg g$$

域上多项式的带余除法

定理

设$f, g \in F[x], g \neq 0$. 则存在唯一的$q, r \in F[x]$, 使得

$$f = qg + r$$

并且$\deg r < \deg g$.
这种带余除法的具体做法，我们已经在Week11展示过.

回顾：$\mathbb{Z}$上的带余除法
对$b \in \mathbb{Z}, a \in \mathbb{Z}^+$, 则存在唯一的$q, r \in \mathbb{Z}$，使得

$$b = aq + r$$

并且$0 \leq r < a$.

域上多项式带余除法定理的证明

唯一性的证明

设有

$$f = q_1 g + r_1 = q_2 g + r_2$$

其中

$$\deg r_1, \deg r_2 < \deg g$$

则有

$$r_2 - r_1 = q_1 g - q_2 g = (q_1 - q_2) g$$

从而

$$\deg(r_2 - r_1) \leq \max\{\deg r_2, \deg r_1\} < \deg g$$

此时，假设$q_1 - q_2 \neq 0$, 则有

$$\deg(r_2 - r_1) = \deg((q_1 - q_2)g) = \deg(q_1 - q_2) + \deg g \geq \deg g > \deg(r_2 - r_1)$$

矛盾！故$q_1 - q_2 = 0$. 从而$r_2 - r_1 = 0$，即唯一性成立。
（还记得Week2对$\mathbb{Z}$上的带余除法的唯一性证明的读者，应当可以发现那个证明和该证明是异曲同工的）

存在性的证明

以下构造性的证明方法即求带余除法的过程。我们对$\deg f$做归纳（注意，我们此时将g视为固定的）。
记$m = \deg g$，以及

$$g = \sum_{i=0}^{m} b_i x^i, b_m \neq 0$$

若$\deg f < \deg g$， 则令$q = 0, r = f$即可，命题成立。
若$\deg f \geq \deg g$，记$n = \deg f$，以及

$$f = \sum_{i=0}^{n} a_i x^i, a_n \neq 0, n \geq m$$

记

$$h = a_n b_m^{-1} x^{n-m}$$

$$\begin{aligned}\phi &= f - hg \\ &= \sum_{i=0}^{n} a_i x^i - a_n b_m^{-1} x^{n-m} \sum_{i=0}^{m} b_i x^i \\ &= \sum_{i=0}^{n} a_i x^i - \sum_{i=0}^{m} a_n b_m^{-1} b_i x^{n-m+i}\end{aligned}$$

注意第二个求和中，最高项的次数为n, 且该项的系数为$a_n b_m^{-1} b_m = a_n$，与第一个求和的最高次项抵消. 故ϕ中x^n的系数为0.

则有

$$\deg \phi \le n - 1$$

那么有由归纳假设，我们就可以对ϕ作带余除法，于是存在唯一的$q_1, r \in F[x]$使得

$$\phi = q_1 g + r，\text{并且} \deg r < \deg g$$

从而令

$$q = h + q_1 = a_n b_m^{-1} x^{n-m} + q_1$$

则有

$$f = \phi + hg = q_1 g + r + hg = (q_1 + h)g + r = qg + r$$

即有

$$f = qg + r，\text{并且有} \deg r < \deg g$$

于是存在性成立.

域上多项式的整除关系

设$f, g \in F[x]$, 记$g | f$，若存在$q \in F[x]$使得$f = qg$.

若要判断两个多项式是否是整除的，只需对它们做带余除法，并检查余式是否为0. 若余式为0，则整除。

域上多项式的最大公因式

回顾：整数的最大公因数

对$a, b \in \mathbb{Z}$，存在$x, y \in \mathbb{Z}$使得

$$(ax + by) \mid a, (ax + by) \mid b, ax + by > 0$$

$d = ax + by$即为a和b的最大公因数。之所以说是最大，是因为

$$\forall c \in \mathbb{Z}, c \mid a, c \mid b，\text{都有} c \mid d.$$

这里的“最大”本质上是就整除关系而言的。一般我们把最大公因式规定为正的d.

回到域上的多项式

我们首先证明一个和上述$\mathbb{Z}$上的结论完全类比的结论:
设$f, g \in F[x]$，则存在$u, v \in F[x]$，使得

$$(uf+vg) \mid f, (uf+vg) \mid g$$

证明

我们对$\deg f + \deg g$进行归纳。
若$g=0$，则令$u=1_f, v=0$即有命题成立。（注意零多项式被任何一个多项式都整除）进一步地，f, g中若有任意一个是零多项式，则命题成立。
若$\deg f + \deg g = 0$, 则该命题就是$\mathbb{Z}$上最大公因式的对应命题，当然成立。
下面假设$\deg f + \deg g > 0$. 不妨设

$$\deg f \geq \deg g$$

作带余除法

$$f = qg + r$$

其中$q, r \in F[x]$并且$\deg r < \deg g$.
对(g, r)，由于$\deg r < \deg g \leq \deg f$，即$\deg g + \deg r < \deg f + \deg g$及归纳假设，一定有

$$\text{存在} u_1, v_1 \in F[x], \text{使得} (u_1 g + v_1 r) \mid g, (u_1 g + v_1 r) \mid r$$

又注意

$$u_1 g + v_1 r = u_1 g + v_1 (f - qg) = v_1 f + (u_1 - q v_1) g$$

从而令

$$u = v_1, v = u_1 - q v_1$$

则有

$$(uf+vg) \mid g, (uf+vg) \mid r$$

又有$f = qg + r$，因此

$$(uf+vg) \mid f, (uf+vg) \mid g$$

故原命题成立。

最大公因式的定义

设$f, g \in F[x]$.

1. 设有$h \in F[x], h \mid f, h \mid g$，则称$h$是$g$和$f$的公因式。
2. 若$f=g=0$，则规定0是f和g的最大公因式。

3. 若f, g不全为0, 则存在唯一的$d \in F[x]$使得：
    - d是f, g的公因式
    - 对任意$h \in F[x]$, h是f, g的公因式，总有$h \mid d$
    - d的首项系数为1_F.

    则称d为f, g的最大公因式. 记作$d = \gcd(f, g)$.