3.3 多项式环

定义(多元多项式环) R 是一个任意的非零环，$X, Y, \cdots$ 是任意一族变元，则多元多项式环 ~~$R[X,Y,\cdots]$~~

$$R[X,Y,\ldots]=\left\{\sum_{a,b,\ldots} c_{ab\ldots} X^a Y^b \cdots \;\middle|\; c_{ab\ldots}\in R\right\}$$

形如 $X^aY^b\cdots$ 的项称为单项式.

Remark: ① $f=\sum_{a,b,\ldots} c_{a,b,\ldots} X^a Y^b\cdots$ 要求是有限和

每个 $f\in R[X,Y,\cdots]$ 都只涉及有限多个变元

② 对于可数个变元的情形，对应的多项式环遂表达为子环的渐增并

$$R[X,Y,Z,\ldots]=R[X]\cup R[X,Y]\cup R[X,Y,Z]\cup\cdots$$

$$R[X]\subseteq R[X,Y]\subseteq R[X,Y,Z]\subseteq\cdots$$

定义($N\in\mathbb{Z}_{\geq 0}$ 次齐次多项式) 设 $f=\sum_{a_1,\cdots,a_n\geq 0} c_{a_1,\cdots,a_n} X_1^{a_1}\cdots X_n^{a_n}$ 是 $R[X_1,\cdots,X_n]$ 的元素. 若有 $N\in\mathbb{Z}_{\geq 0}$ 使得仅当 $a_1+\cdots+a_n=N$ 时才可能有 $c_{a_1,\cdots,a_n}\neq 0$，则称 f 是 N 次齐次的.

定义(多项式的求值) R 是交换环，对 $\forall x,y,\ldots\in R$，可以将 $X=x$，$Y=y$ 等代入 $f\in R[X,Y,\cdots]$ 进行求值，给出

$$f=\sum_{a,b,\cdots} c_{ab\ldots} X^a Y^b\cdots \longmapsto \sum_{a,b,\cdots} c_{ab\ldots} x^a y^b\cdots =: f(x,y,\cdots)$$

Lemma：对$\forall f, g \in R[X, Y, \cdots]$，$\forall x, y, \cdots \in R$，有：

$$(f+g)(x, y, \cdots) = f(x, y, \cdots) + g(x, y, \cdots)$$

$$(fg)(x, y, \cdots) = f(x, y, \cdots) g(x, y, \cdots)$$

对$\forall$常数多项式 $c \in R[X, Y, \cdots]$，$\forall x, y, \cdots \in R$，有：

$$(\text{常数多项式}\, c)(x, y, \cdots) = c$$

Proof：~~设 $f = \sum_{a,b,\cdots} c_{ab\cdots} X^a Y^b \cdots$，$g = \sum_{a,b,\cdots} d$~~

设 $f = \sum_{a,b,\cdots} \alpha_{ab\cdots} X^a Y^b \cdots$，$g = \sum_{a,b,\cdots} \beta_{ab\cdots} X^a Y^b \cdots$

则有：$f+g = \sum_{a,b,\cdots} (\alpha_{ab\cdots} + \beta_{ab\cdots}) X^a Y^b \cdots$

$$\therefore (f+g)(x, y, \cdots) = \sum_{a,b,\cdots} (\alpha_{ab\cdots} + \beta_{ab\cdots}) x^a y^b \cdots$$

$$= \sum_{a,b,\cdots} (\alpha_{ab\cdots} x^a y^b \cdots + \beta_{ab\cdots} x^a y^b \cdots)$$

这是有限求和

$$= \sum_{a,b,\cdots} \alpha_{ab\cdots} x^a y^b \cdots + \sum_{a,b,\cdots} \beta_{ab\cdots} x^a y^b \cdots$$

$$= f(x, y, \cdots) + g(x, y, \cdots)$$

设 $f = \sum_{a,b,\cdots} \alpha_{ab\cdots} X^a Y^b \cdots$，$g = \sum_{a',b',\cdots} \beta_{a',b',\cdots} X^{a'} Y^{b'} \cdots$

则有：$fg = \sum_{\substack{a,b,\cdots \\ a',b',\cdots}} \alpha_{ab\cdots} \beta_{a'b'\cdots} X^{a+a'} Y^{b+b'} \cdots$

$$\therefore f(x,y,\cdots)g(x,y,\cdots)=\left(\sum_{a,b,\cdots}\alpha_{ab\cdots}x^a y^b\cdots\right)\left(\sum_{a',b',\cdots}\beta_{a'b'\cdots}x^{a'}y^{b'}\cdots\right)$$

$$=\sum_{\substack{a,b,\cdots\\a',b',\cdots}}(\alpha_{ab\cdots}x^a y^b\cdots)(\beta_{a'b'\cdots}x^{a'}y^{b'}\cdots) \underset{\text{用到}R\text{是交换环}}{=} \sum_{\substack{a,b,\cdots\\a',b',\cdots}}\alpha_{ab\cdots}\beta_{a'b'\cdots}x^{a+a'}y^{b+b'}\cdots$$

$$=(fg)(x,y,\cdots)$$

$$(\text{常数多项式 }c)(x,y,\cdots)=c+\sum_{a,b,\cdots}0x^a y^b\cdots=c \qquad \square$$

Remark：每个多项式 $f\in R[X,Y,\cdots]$ 都确定从 $R\times R\times\cdots$（乘积项数 $=$ 变元个数）到 R 的映射，这是多项式 f 所确定的多项式函数.

Recall Lemma：对 $\forall N\in\mathbb{Z}_{\geq 1}$，有：$\mathbb{Z}/N\mathbb{Z}$ 是域 $\Leftrightarrow$ N 是素数

定义（域 $\mathbb{F}_p$）对 $\forall$ 素数 p，$\mathbb{Z}/p\mathbb{Z}$ 是域，记作：

$$\mathbb{F}_p:=\mathbb{Z}/p\mathbb{Z}$$

Remark：$\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}=\{[x]_p \mid x\in\mathbb{Z}\}=\{[0]_p,[1]_p,[2]_p,\cdots,[p-1]_p\}$

例（非零多项式可以给出零函数）考虑 $\mathbb{F}_p[X]$ 中的多项式：（p是素数）

$$f(X)=X^p-X\in\mathbb{F}_p[X]$$

对 $\mathbb{F}_p$ 中的任一元：$[x]_p$ （$x\in\mathbb{Z}$），

$$\cancel{f([x]_p)}\quad f([x]_p)=[x]_p^p-[x]_p=[1]_p\cdot[x]_p^p+(-[1]_p)\cdot[x]_p$$

$$=[1\cdot x^p]_p+[-1]_p\cdot[x]_p=[x^p]_p+[-x]_p=[x^p-x]_p=[0]_p$$

$\therefore f(X)=X^p-X\in\mathbb{F}_p[X]$ 作为多项式函数给出 $\mathbb{F}_p\longrightarrow\mathbb{F}_p$ （零函数）

$[x]_p\longmapsto[0]_p$

例（有限域F上的非零多项式给出零函数）F是一个任意的有限域，

设 $F=\{a_1,a_2,\cdots,a_n\}$ 则有：

$$f(X)=(X-a_1)(X-a_2)\cdots(X-a_n)\in F[X]$$

$\because f(X)$ 的 n 次项为 X^n，n 次项系数为 $1_F\neq0_F$ $\therefore f(X)$ 不是零多项式

对 $\forall a_i\in F$，$f(a_i)=(a_i-a_1)\cdots(a_i-a_i)\cdots(a_i-a_n)=0_F\cdot(a_i-a_1)\cdots(a_i-a_n)$

$$=0_F$$

$\therefore f(X)=\prod_{i=1}^{n}(X-a_i)\in F[X]$ 作为非零多项式给出 $F\longrightarrow F$ （零函数）

$a_i\longmapsto0_F$