答疑

1. $R=\mathbb{Z}[x]$，$I=(p, f(x))$，p素数，$f(x)$首项系数与p互素

$\deg f(x)>0$，则（设 $\mathbb{Z}[x]\xrightarrow{\tilde{\varphi}}\mathbb{Z}_p[x]$）

$$R/I \cong \frac{R/(p)}{\frac{(p,f(x))}{(p)}} \qquad R/(p) = \frac{\mathbb{Z}[x]}{(p)} \overset{\phi}{\cong} \mathbb{Z}_p[\bar{x}] \qquad \bar{x}=x+(p)$$

$$I/(p) = \frac{(p,f(x))}{(p)} = \frac{(p)+(f(x))}{(p)} \xrightarrow[\cong]{\phi} (\bar{f}(\bar{x}))$$

（若 $f(x)=\sum a_i x^i$ $\qquad \bar{f}(\bar{x}) = \sum \bar{a}_i \bar{x}^i$

因此 $R/I \cong \dfrac{\mathbb{Z}_p[\bar{x}]}{(\bar{f}(\bar{x}))}$，使用图示

$$\begin{tikzcd}
I=(p,f(x)) \arrow[r, "\tilde{\varphi}"] \arrow[d] & \mathrm{Im}\tilde{\varphi}=(\bar{f}(\bar{x})) \arrow[d] \\
\mathbb{Z}[x] \arrow[r, "\tilde{\varphi}"] & \mathbb{Z}_p[\bar{x}] \\
f(x) \arrow[r, mapsto] \arrow[d] & \bar{f}(\bar{x}) \arrow[d] \\
\frac{\mathbb{Z}[x]}{I} \arrow[r, "\sim"] & \frac{\mathbb{Z}_p[\bar{x}]}{\mathrm{Im}\tilde{\varphi}}
\end{tikzcd}$$

一般地，R整区，I,J是R的理想，考虑 $\pi: R\to R/J$.

$$\begin{tikzcd}
I+J \arrow[r, "\pi"] \arrow[d] & \pi(I)=\frac{I+J}{J} \arrow[d] \\
R \arrow[r] \arrow[d] & R/J \arrow[d] \\
R/(I+J) \arrow[r] & (R/J)/\pi(I)
\end{tikzcd}$$

令 $\bar{R}=R/J$，π 满同态，$\pi(I)$ 是 $\bar{R}$ 的理想

$$R/_{I+J} \xrightarrow{\sim} \bar{R}/_{\pi(I)}$$

对于 $R=\mathbb{Z}[x]$，$I=(p,f(x))$，也可以如下刻划 R/I，考虑

$$\mathbb{Z}[x] \xrightarrow{\pi} \frac{\mathbb{Z}[x]}{(f(x))} = \{c_0+c_1\bar{x}+\cdots+c_{n-1}\bar{x}^{n-1} \mid c_i\in\mathbb{Z}\}$$

（设 $f(x)=\sum_{i=0}^{n} a_i x^i$）

$\forall g(x)\in\mathbb{Z}[x]$，$g(x)=q(x)f(x)+r(x)$　$\deg r(x)<\deg f(x)$

$\pi(g(x))=\bar{r}(\bar{x})$

(p) 在 π 下像为 $\{pc_0+pc_1\bar{x}+\cdots+pc_{n-1}\bar{x}^{n-1} \mid c_i\in\mathbb{Z}\}=p$ 在 $\frac{\mathbb{Z}[x]}{(f(x))}$ 中生成的理想.

2. 设 $\mathbb{F}$ 是一个域，$p(x)\in\mathbb{F}[x]$ 不可约，$\deg p(x)>0$. 则存在 $\mathbb{F}$ 的扩域 $\mathbb{E}=\frac{\mathbb{F}[x]}{(p(x))}$ 包含 $p(x)$ 的一个根. 这里我们使用了将 $\mathbb{F}$ 等同于 $\mathbb{E}$ 的子域 $\{a+(p(x)) \mid a\in\mathbb{F}\}$. 若希望构造 $\mathbb{F}$ 的真扩域，只需作 $\mathbb{F}$ 上一个空间 $\mathbb{F}^n$，$n=\deg p(x)$.

考虑 $\mathbb{F}^n \xrightarrow{\Phi} \mathbb{E}=\frac{\mathbb{F}[x]}{(p(x))}=\{\bar{c}_0+\bar{c}_1\bar{x}+\cdots+\bar{c}_{n-1}\bar{x}^{n-1} \mid c_i\in\mathbb{F}\}$

$$e_i=\begin{pmatrix}0\\ \vdots\\ 1\\ 0\\ \vdots\\ 0\end{pmatrix} \longmapsto \bar{x}^{i-1}$$

第i位置

Φ是一个向量空间同构. 因为$\mathbb{E}$是一个域, 可以赋予$\mathbb{F}^n$上乘法结构.

$$e_i * e_j \overset{\text{定义}}{=\!=\!=} \Phi^{-1}(x^{i-1} \cdot x^{j-1}) = e_{i+j-1}$$

$\forall\ v \in \mathbb{F}^n \quad w \in \mathbb{F}^n$, $\quad v = a_1e_1 + \cdots + a_ne_n,\ w = b_1e_1 + \cdots + b_ne_n$

$$v * w = \left(\sum a_ie_i\right) * \left(\sum b_je_j\right) = \sum_{k=2}^{n+1} \cancel{a}\left(\sum_{i+j=k} a_ib_j\right) e_{k-1}$$

这使得Φ成为一个域同构.

$$\begin{aligned} \mathbb{F} &\longrightarrow \mathbb{F}^n \\ a &\longmapsto \begin{pmatrix} a \\ 0 \\ \vdots \\ 0 \end{pmatrix} \end{aligned}$$

是一个域嵌入. (这里我们又使用了a和ae_1的等同)

如果不认同以上两种等同, 凭空造出$\mathbb{F}$的一个扩域是(可能)无法做到的. 例如 $\mathbb{R} \longrightarrow \mathbb{C} = \{a+bi \mid a, b \in \mathbb{R}\}$ 使得$\mathbb{R}$成为一个$\mathbb{C}$的子域. $\xrightarrow{\text{推广}}$ $\mathbb{F} \longrightarrow \mathbb{F}(s) = \{c_0 + c_1s + \cdots + c_1s^{n-1} \mid c_i \in \mathbb{F}\}$ 其中s是$p(x)=0$的根. 这里说"s是$p(x)=0$的根"很含糊, 必须要给一个更大的结构包含s. 所以使用 $\mathbb{E} = \frac{\mathbb{F}[x]}{(p(x))}$ 给出这个更大结构, 代价是需要$\mathbb{F}$等同于$\mathbb{E}$的子域.