2026年3月9日 星期一 18:42

习题课1.

作业

1 设 $f=x^3+1$, $g=x^2+1$

(i) 设 $f,g\in\mathbb{Z}_2[x]$. 求 $\gcd(f,g)$

(ii) 设 $f,g\in\mathbb{Z}_3[x]$. 求 $\gcd(f,g)$

解：作带余除法， $x^3+1\equiv x(x^2+1)+1+x \pmod 2$ $r_1(x)=x+1$, $q_1(x)=x$

$x^2+1\equiv(x+1)(x+1)\pmod 2$ $q_2(x)=x+1$, $r_2(x)=0$

(i) 故在 $\mathbb{Z}_2[x]$ 中, $\gcd(f,g)=x+1$

(ii) 同(i)，在 $\mathbb{Z}_3[x]$ 中, $x^3+1\equiv x(x^2+1)+2x+1\pmod 3$ $q_1(x)=x$, $r_1(x)=2x+1$

$x^2+1\equiv(2x+2)(2x+1)+2\pmod 3$ $q_2(x)=2x+2$, $r_2(x)=2$

故在 $\mathbb{Z}_3[x]$ 中, $\gcd(f,g)=2$（或1）

2、设F是域， $A: F^n\to F^n$ 是线性映射且满足 $A^2=A$. 证明：

(i) $\dim(\ker(A))+\dim(\ker(A-\varepsilon))=n$，其中 ε 为恒同映射.

(ii) $\ker(A-\varepsilon)=\operatorname{im}(A)$.

证明：

(i) 设 $\forall\alpha\in F^n$, $\alpha=A\varepsilon+\varepsilon-A\varepsilon$，其中 $A\varepsilon\in\ker(A-\varepsilon)$ $\varepsilon-A\varepsilon\in\ker(A)$

故 $F^n=\ker A+\ker(A-\varepsilon)$

另一方面，设 $\forall\beta\in\ker A\cap\ker A-\varepsilon$，则 $A\beta=(A-\varepsilon)\beta=0$

$\Longrightarrow\beta=0$ 故 $F^n=\ker A+\ker(A-\varepsilon)=\ker A\oplus\ker(A-\varepsilon)$

由此 $\dim(\ker(A))+\dim(\ker(A-\varepsilon))=n$.

(ii) 由(i) $\dim(\ker(A-\varepsilon))=n-\dim\ker A=\dim\operatorname{Im}A$

现设 $\beta\in\operatorname{Im}A$，则存在 $\alpha\in F^n$, $\beta=A\alpha$，此时 $(A-\varepsilon)\beta=(A-\varepsilon)A\alpha=0$

故 $\beta\in\ker A-\varepsilon$，即 $\operatorname{Im}A\subseteq\ker(A-\varepsilon)$

这说明 $\operatorname{Im}A=\ker(A-\varepsilon)$ （第(i)问尽量掌握讲义证明）

3. 设F是域， $f=f_nx^n+\cdots+f_1x+f_0=f_n(x-\alpha_1)\cdots(x-\alpha_n)$，其中 $f_n,f_{n-1},\dots,f_0,\alpha_1,\dots,\alpha_n\in F$ 且 $f_n\neq0$. 证明：

$\alpha_1+\cdots+\alpha_n=-\frac{f_{n-1}}{f_n}$ 和 $\alpha_1\cdots\alpha_n=(-1)^n\frac{f_0}{f_n}$

证明：由条件 $f_nx^n+\cdots+f_1x+f_0=f_n(x-\alpha_1)\cdots(x-\alpha_n)$ ……(*)

在*中对比两边关于 x^{n-1} 系数 $\Longrightarrow -(\alpha_1+\cdots+\alpha_n)f_n=f_{n-1}$

在*中令 $x=0$ $\Longrightarrow(-1)^nf_n\alpha_1\cdots\alpha_n=f_0$

故 $\alpha_1+\cdots+\alpha_n=-\frac{f_{n-1}}{f_n}$, $\alpha_1\cdots\alpha_n=(-1)^n\frac{f_0}{f_n}$

4. 设F是域

$$':\ F[x]\to F[x]$$

$$f=\sum_{i=0}^n f_ix^i\longrightarrow f'=\sum_{i=1}^n if_ix^{i-1},$$

其中 $f_i\in F$. 特别地，对 $\forall c\in F$, $c'=0$，称 c' 是 $F[x]$ 上的形式导数. 验证：对 $\forall f,g\in F$

(i) $f'+g'=(f+g)'$ (ii) $(fg)'=f'g+fg'$

证明：设 $f=\sum_{i=0}^n f_ix^i$, $g=\sum_{j=0}^m g_jx^j$，不妨设 $n\geq m$，则 $g=\sum_{j=0}^n g_jx^j$

其中 $g_{m+1}=\cdots=g_n=0$

(i) $(f+g)'=\left(\sum_{i=0}^n(f_i+g_i)x^i\right)'=\sum_{i=1}^n i(f_i+g_i)x^{i-1}=\sum_{i=1}^n if_ix^{i-1}+\sum_{i=1}^n ig_ix^{i-1}$

$=f'+g'$

(ii) $(fg)'=\left(\sum_{i=0}^{2n}\left(\sum_{j=0}^i f_jg_{i-j}\right)x^i\right)'$

$=\sum_{i=1}^{2n}\left(i\sum_{j=0}^i f_jg_{i-j}\right)x^{i-1}$

$f'g=\left(\sum_{i=1}^n if_ix^{i-1}\right)\cdot\left(\sum_{j=0}^n g_jx^j\right)=\sum_{i=1}^{2n}\left(\sum_{j=1}^i jf_jg_{i-j}\right)x^{i-1}$

同理 $fg'=\left(\sum_{i=0}^n f_ix^i\right)\left(\sum_{j=1}^n jg_jx^{j-1}\right)=\sum_{i=1}^{2n}\left(\sum_{j=1}^i jg_jf_{i-j}\right)x^{i-1}$

最后，只要证 $\sum_{j=1}^i jf_jg_{i-j}+\sum_{j=1}^i jg_jf_{i-j}=i\sum_{j=0}^i f_jg_{i-j}$ 对 $\forall\ 1\leq i\leq 2n$ 成立.

对 $\forall\ 0\leq j\leq i$，右边关于 f_jg_{i-j} 次数为 i，左边为 $j+i-j=i$

故命题成立.

5、设 $\operatorname{char}F=0$，$p\in F[x]$ 不可约.

(i) 证明 $\gcd(p,p')=1$

(ii) 设 $f=p^mq$, $m>0$ $q\in F[x]$ 且 $p\nmid q$. 证明 $p^{m-1}\mid f'$ 但 $p^m\nmid f'$

证明：(i) 若 $p\in F$，命题成立，否则设 $\deg p=n\geq1$

由 $\operatorname{char}F=0$，故 $\deg p'=n-1\geq0$

$\gcd(p,p')\mid p$ 但 p 不可约，故 $\gcd(p,p')\sim p$ 或者

$\gcd(p,p')=1$

但 $\deg\gcd(p,p')\leq\deg p'\leq n-1<\deg p$，故第一种情况不可能. $\Longrightarrow\gcd(p,p')=1$

(ii) $f=p^mq$. $m>0$ $p\nmid q$，则 $f'=mp^{m-1}p'q+p^mq'=p^{m-1}(mp'q+pq')$

故 $p^{m-1}\mid f'$

另一方面，若 $p^m\mid f$，则 $p^m\mid mp^{m-1}p'q\Longleftrightarrow p\mid mp'q$

这与(i)以及 $p\nmid q$ 矛盾

6. $\operatorname{Char}F=0$，则 f 无平方 $\Longleftrightarrow\gcd(f,f')=1$.

证明：

充分性：若 $\gcd(f,f')=1$ 但 f 不是无平方的，设 $f=p^2q$

p 为 f 不可约因子，则 $f'=2pp'q+p^2q'\Longrightarrow p\mid f'$

这与 $\gcd(f,f')=1$ 矛盾

必要性：若 f 无平方，设 f 的一个不可约分解为 $f=p_1\cdots p_m$

$p_i\nsim p_j$ $(\forall i\neq j)$，则 $f'=\sum_{i=1}^m p_1\cdots\hat{p_i}\cdots p_m$

若 $\gcd(f,f')\neq1$，则 $\exists\ p_j\mid\gcd(f,f')\Longrightarrow p_j\mid f'$

$\Longrightarrow p_j\mid p_1\cdots\hat{p_j}\cdots p_m$ 这与假设矛盾. □

补充

*例1. 作业第一问启发我们：若 φ 为 $\mathbb{Z}[x]\to\mathbb{Z}_p[x]$ 环同态
$f\to f\pmod p$

（以下将 $\varphi(f)$ 记为 f_p），则 $(\gcd(f,g))_p\mid\gcd(f_p,g_p)$，何时它们相伴？（我们假定这里多项式均首1）.

先证 $\gcd(f,g)_p\mid\gcd(f_p,g_p)$. 设 $h=\gcd(f,g)$,

$f=hf_1$, $g=hg_1$，则 $f_p=h_pf_{1p}$, $g_p=h_pg_{1p}$.

故 $h_p\mid\gcd(f_p,g_p)$

现令 $f=a_nx^n+\cdots+a_1x+a_0$, $g=b_mx^m+\cdots+b_1x+b_0$,

定义 f 与 g 的留数

$$\operatorname{res}(f,g)=\begin{vmatrix} a_n & a_{n-1} & \cdots & a_1 & a_0 & & \\ & a_n & \cdots & & a_1 & a_0 & \\ & & \ddots & & & \ddots & \\ & & & a_n & \cdots & a_1 & a_0 \\ b_m & \cdots & b_1 & b_0 & & & \\ & \ddots & & & \ddots & & \\ & & b_m & \cdots & & b_1 & b_0 \end{vmatrix}\begin{matrix}\left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}m\\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\}n\end{matrix}$$

$(n+m)\times(n+m)$

定理：对首一多项式 f,g，$\gcd(f_p,g_p)\sim\gcd(f,g)_p$ 当且仅当 $p\nmid\operatorname{res}(f,g)$.

代入第一题

$$\operatorname{res}(f,g)=\begin{vmatrix}1&0&0&1&0\\0&1&0&0&1\\1&0&1&0&0\\0&1&0&1&0\\0&0&1&0&1\end{vmatrix}=2,\quad\gcd(f,g)=1$$

定理与计算得到的结果吻合.

例2：多项式无平方分解 $(\operatorname{char}F=0)$

多项式的无平方分解是将其分解成若干无平方因式方幂之积

$$f=p_1p_2^2\cdots p_k^k\quad(p_1\cdots p_k\ \text{无平方，两两互素，但未必不可约})$$

例：$f=(2x-1)(x-1)^3(x-2)^3$，则 $f=(2x-1)^1\cdot1^2\cdot((x-1)(x-2))^3$

$p_1=2x-1$, $p_2=1$, $p_3=(x-1)(x-2)$.

下面以 $k=4$ 为例（$f=p_1p_2^2p_3^3p_4^4$），给出一个 f 的无平方算法

① $f=p_1p_2^2p_3^3p_4^4$. $f'=p_2p_3^2p_4^3(4p_1p_2p_3p_4'+3p_1p_2p_4p_3'+2p_1p_3p_4p_2'+p_1'p_2p_3p_4)$

$\Longrightarrow\gcd(f,f')=p_2p_3^2p_4^3$, $\frac{f}{\gcd(f,f')}=p_1p_2p_3p_4$，记为 h_1

② 令 $f_1=\gcd(f,f')=p_2p_3^2p_4^3$，则 $\frac{f_1}{\gcd(f_1,f_1')}=p_2p_3p_4$ …… h_2

③ 令 $f_2=\gcd(f_1,f_1')$ 则 $\frac{f_2}{\gcd(f_2,f_2')}=p_3p_4$ …… h_3

④ 令 $f_3=\gcd(f_2,f_2')$ 则 $\frac{f_3}{\gcd(f_3,f_3')}=p_4$ …… h_4，此时 $f_3=p_4$.

则 $p_i=\frac{h_i}{h_{i+1}}$ $(i=1,2,3)$ $p_4=h_4$

由以上过程，我们给出一般的无平方算法

输入：$f\in k[x]$.

输出：$p_1,\dots,p_k$，无平方，两两互素

```
$g_1 := \gcd(f,f')$
$h_1 := f/g_1$ ;  $i:=1$
while $g_i\neq1$ do
    $g_{i+1} := \gcd(g_i,g_i')$   $h_{i+1} := g_i/g_{i+1}$ , $p_i := h_i/h_{i+1}$   $i=i+1$
end{while}
$k:=i$   $p_k:=h_k$ ;
return $p_1,\dots,p_k$
```

（$g_i=1$ 时循环终止，由作业题6，此时已无平方因子）

注：以上算法要求 $\operatorname{char}F=0$，下面是一个反例

$f\in\mathbb{Z}_3[x]$, $f=(2x-1)(x-1)^3$，则 $f'=2(x-1)^3$

$\gcd(f,f')=(x-1)^3$ $f/\gcd(f,f')=2x-1$

令 $g_1=(x-1)^3$, $\gcd(g_1,g_1')=\gcd(g_1,0)=g_1$, $g_1/\gcd(g_1,g_1')=1$

陷入死循环. 问题在于 $\deg(g_1)>0$ 但 $g_1'=0$

例3. 设 $\varphi_1\cdots\varphi_m$ 是n维线性空间V上的线性变换，且适合条件：

$\varphi_i^2=\varphi_i$, $\varphi_i\varphi_j=0$ $(i\neq j)$, $\ker\varphi_1\cap\cdots\cap\ker\varphi_m=0$

求证 $V=\operatorname{Im}\varphi_1\oplus\cdots\oplus\operatorname{Im}\varphi_m$.

证明

① 直和，设 $\alpha\in\operatorname{Im}\varphi_1\cap(\operatorname{Im}\varphi_2+\cdots+\operatorname{Im}\varphi_m)$

则 $\exists\ \alpha_1,\alpha_2\cdots\alpha_n\in V$

$\alpha=\varphi_1(\alpha_1)=\varphi_2(\alpha_2)+\cdots+\varphi_m(\alpha_m)$

则 $\varphi_1^2(\alpha_1)=\varphi_1\varphi_2(\alpha_2)+\cdots+\varphi_1\varphi_m(\alpha_m)=0$

故 $\alpha=\varphi_1(\alpha_1)=\varphi_1^2(\alpha_1)=0$

② $V=\operatorname{Im}\varphi_1+\cdots+\operatorname{Im}\varphi_m$

设 $\forall\alpha\in V$ $\alpha=(\alpha-\varphi_1\alpha-\cdots-\varphi_m\alpha)+\varphi_1\alpha+\cdots+\varphi_m\alpha$

$\alpha-\varphi_1\alpha-\cdots-\varphi_m\alpha\in\ker\varphi_1\cap\cdots\cap\ker\varphi_m$.

故 $\alpha=\varphi_1\alpha+\cdots+\varphi_m\alpha\in\operatorname{Im}\varphi_1+\cdots+\operatorname{Im}\varphi_m$.

综上 $V=\operatorname{Im}\varphi_1\oplus\cdots\oplus\operatorname{Im}\varphi_m$