3. 在$\mathbb{Z}_2$上的最大公因子 $x^3+x^2+x+1=(x-1)^3$

在$\mathbb{Z}_5$上的最大公因子 $4x^2+4x+2=-x^2-x+2=-(x^2+x-2)=-(x+2)(x-1)$

由于在$\mathbb{Z}_5$上最大公因子是2次多项式，∴在$\mathbb{Z}$中最大公因子次数小于等于2.

且若在$\mathbb{Z}$上，f和g有公因子$ax+b$，其中$|a|$、$|b|$都$\leqslant 2$时 则 在$\mathbb{Z}_2$上也有公因子$ax+b$.

若在$\mathbb{Z}$上，f和g有公因子$a'x+b'$，其中$|a'|$、$|b'|$都$\leqslant 5$时，则在$\mathbb{Z}_5$上也有公因子$a'x+b'$

∴~~最检查~~ 若$\mathbb{Z}$中有公因子$x+2$ 则在$\mathbb{Z}_2$中有公因子x，矛盾

若$\mathbb{Z}$中有公因子$x+1$ 则在$\mathbb{Z}_5$中有公因子$x+1$，矛盾

故只须检验在$\mathbb{Z}$中是否有公因子$x+1$和$x-3$. $f(1)=f(3)=g(1)=g(3)=0$ ∴在$\mathbb{Z}$中有公因子$(x+1)(x-3)$

(若在$\mathbb{Z}$中没有公因子$(x-1)(x-3)$，不能说明任何问题)(即也可能有次更大的a,b使$ax+b$是在$\mathbb{Z}$中的因子)

补充：∵$\varphi:\mathbb{Z}\to\mathbb{Z}_5$是同态

∴$\varphi^*:\mathbb{Z}[x]\to\mathbb{Z}_5[x]$~~是满射~~

~~且是同态~~

∴若$g(x)\mid f(x)\in\mathbb{Z}[x]$

则$\varphi(g(x))\mid\varphi(f(x))\in\mathbb{Z}_5[x]$

4. 证明：已知由定理知，$\exists u,v\in\mathbb{F}[x]$ s.t. $u(x)f(x)+v(x)g(x)=\gcd(f(x),g(x))$

∴显然$\forall n(x)\in\mathbb{F}[x]$，令$p(x)=n(x)u(x)$，$q(x)=n(x)v(x)$，则$n(x)\gcd(f,g)=pf+qg$.

∴右$\subseteq$左

令$\gcd(f,g)=d(x)$，则$f(x)=f^*(x)d(x)$ $g(x)=g^*(x)d(x)$

$\forall p,q\in\mathbb{F}[x]$ $p(x)f(x)+q(x)g(x)=(p(x)f^*(x)+q(x)g^*(x))d(x)$ ∴左$\subseteq$右

综上左=右.

5. (1) 证明：按字典序，若f_i的首项是$C_{f_{i1}}x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$，则$f_i$中所有其它的项$C_{f_{i2}}x_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n}$都有 $\begin{cases}\alpha_i=\beta_i & \text{when } i<j\\ \alpha_i>\beta_i & \text{when } i=j\end{cases}$

其中$j\in\{1,2,\cdots n\}$. 对于$\forall f\in\mathbb{F}[x]$，设$f=c_1x_1^{r_{11}}x_2^{r_{12}}\cdots x_n^{r_{1n}}+c_2x_1^{r_{21}}x_2^{r_{22}}\cdots x_n^{r_{2n}}+\cdots+c_nx_1^{r_{n1}}x_2^{r_{n2}}\cdots x_n^{r_{nn}}$

~~简为~~ $f=c_1X^{r_1}+c_2X^{r_2}+\cdots+c_nX^{r_n}$（其中$r_1=(r_{11},r_{12},\cdots r_{1n})$，…，$r_n=(r_{n1},r_{n2},\cdots,r_{nn})$）按字典序$X^{r_i}>X^{r_{i+1}}$

对于$c_1X^{r_1}$若~~是~~f的首项的倍式，则对$\forall i\in\{1,\cdots n\}$，$r_{1i}\geq\alpha_i$，∴可能式$\frac{c_1}{C_{f_{11}}}x_1^{r_{11}-\alpha_1}x_2^{r_{12}-\alpha_2}\cdots x_n^{r_{1n}-\alpha_n}\cdot\frac{1}{C_{f_{11}}}X^{r_1-\alpha}$

$(\alpha=(\alpha_1,\cdots,\alpha_n))$ 乘$\frac{c_1}{C_{f_{11}}}X^{r_1-\alpha}\cdot C_{f_{11}}X^{\alpha}=c_1X^{r_1}$ ∴ $f-\frac{c_1}{C_{f_{11}}}X^{r_1-\alpha}\cdot f_1=c_2X^{r_2}+\cdots+c_nX^{r_n}-\frac{c_1}{C_{f_{11}}}X^{r_1-\alpha}\cdot(f-C_{f_{11}}X^{\alpha})$

∵$f-C_{f_{11}}X^{\alpha}<_{lex}C_{f_{11}}X^{\alpha}$ ∴$\frac{c_1}{C_{f_{11}}}X^{r_1-\alpha}(f-C_{f_{11}}X^{\alpha})<_{lex}c_1X^{r_1}$ 又∵$c_2X^{r_2},\cdots,c_nX^{r_n}<_{lex}c_1X^{r_1}$

∴ $f-\frac{c_1}{C_{f_{11}}}X^{r_1-\alpha}f_1<_{lex}f$，依此进行下去直至$f$中不存在$f-gf_1$（其中$g_i\in\mathbb{F}[x]$）中不存在$f_1$的首项的倍式，~~且若$f$的首项不是$f_1$的首项的倍式，则$f$中所有的项都不是$f_1$的首项的倍式.~~

令$r_1=f-gf_1$，同理对于r_1中的单项若存在f_2的首项的倍式，用上述方法可求得$r_1-g_2f_2$中不存在f_2的首项的倍式，∴$\exists g_1,\cdots g_n\in\mathbb{F}[x]$，s.t. $r=f-\sum_{i=1}^{n}g_if_i$ 中不存在任何f_i的首项的倍式.

(2). 证明：对于无限集$\{lt(a)\mid a\in I\}$. 由Dickson引理，存在有限集X使对$\forall m\in\{lt(a)\mid a\in I\}$，$\exists n\in X$，

满足m是n的倍式.

1) 证明：取 $G=\{g\in I \mid \mathrm{lt}(g)\in X\}$（其中的X为上述的有限子集）$\subset I$，且 $\{\mathrm{lt}(g)\mid g\in G\}=X$，∵X有限，∴G有限，设为 $G=\{g_1,g_2,\cdots g_m\}$

现证 $\langle G\rangle=I$，显然 $\langle G\rangle\subset I$. 对 $\forall f\in I$. $\exists q_1,q_2,\cdots q_n, r\in F[x_1,\cdots x_n]$. s.t.

$$f=\sum_{i=1}^{n} q_i g_i + r$$

且r中所有的项都不是 g_i 的首项的倍式，若 $r\neq 0$ ∵ $f_i\in I$, $f\in I$ ∴ $r\in I$ ∴ r的首项一定是G中多项式的首项的倍式，∴矛盾 ∴ $r=0$ ∴ $f=\sum_{i=1}^{n} q_i g_i$ ∴ $I\subset\langle G\rangle$ ∴ $I=\langle G\rangle$

2. 法二：赋值同态：$f_1(A)=(A-E)(A-2E)=\begin{pmatrix}0&1&0\\0&0&0\\0&0&1\end{pmatrix}\begin{pmatrix}-1&1&0\\0&-1&0\\0&0&0\end{pmatrix}=\begin{pmatrix}0&-1&0\\0&0&0\\0&0&0\end{pmatrix}$

赋值同态定理：（环上由一个元素生成的环总是多项式环的同态象）设 σ 为环R到环S的同态，且 $\sigma(1)=1'$，$1\in R$, $1'\in S$，则对 $\forall u\in S$，σ 恒可唯一地扩充成R上未定元x的多项式环R[x]到S的同态 σ_u，使得 $\sigma_u(x)=u$.　　若 $f_1(x)=f_2(x)\in R[x]$

证明：1. 映射：$\sigma_u(f_1(x))=\sigma_u(a_n x^n+a_{n-1}x^{n-1}+\cdots+a_0)=\sigma_u(a_n)\cdot u^n+\sigma_u(a_{n-1})\cdot u^{n-1}+\cdots+\sigma_u(a_0)$

$$=\sigma(a_n)u^n+\sigma(a_{n-1})u^{n-1}+\cdots+\sigma(a_0)=\sigma_u(f_2(x))$$

2. 同态：①保持加法，设 $f_1=a_n x^n+\cdots+a_0$ 且 $f_2=b_m x^m+\cdots+b_0$ 且 $n\geq m$

$$\sigma_u(f_1+f_2)=\sigma_u(a_n x^n+\cdots+a_{m+1}x^{m+1}+(a_m+b_m)x^m+\cdots+(a_0+b_0))$$

$$=\sigma(a_n)u^n+\cdots+\sigma(a_{m+1})u^{m+1}+\sigma(a_m+b_m)u^m+\cdots+\sigma(a_0+b_0)$$

$$=\sigma(a_n)u^n+\cdots+\sigma(a_{m+1})u^{m+1}+\sigma(a_m)u^m+\cdots+\sigma(a_0)+\sigma(b_m)u^m+\cdots+\sigma(b_0)$$

$$=\sigma_u(f_1)+\sigma_u(f_2)$$

②保持乘法，

$$\sigma_u(f_1\cdot f_2)=\sum_{i=1}^{m+n}\left(\sum_{j=1}^{i}a_j b_{i-j}\right)x^i=\sum_{i=1}^{m+n}\sum_{j=1}^{i}\sigma_u(a_j)\sigma_u(b_{i-j})x^i$$

$$=\sigma_u$$

$$=\sum_{i=1}^{m+n}\sum_{j=1}^{i}\sigma(a_j)\sigma(b_{i-j})x^i=(\sigma(a_n)x^n+\cdots+\sigma(a_0))(\sigma(b_m)x^m+\cdots+\sigma(b_0))$$

$$=\sigma_u(f_1)\sigma_u(f_2)$$

3. 唯一：若已知 σ，且已知 $\sigma(x)=u$ 则 σ_u 可唯一确定.

一. 设域$\mathbb{F}$, $a,b\in\mathbb{F}$, 且$a\neq 0$, 定义映射 $\varphi_{ab}: \mathbb{F}[x]\to\mathbb{F}[x]$: $f(x)\mapsto f(ax+b)$

且 $(\varphi_{ab})|_{\mathbb{F}}=id_{\mathbb{F}}$ 证明: φ_{ab}是自同构.

证明: 设 $\varphi:\mathbb{F}\to\mathbb{F}[x]: a\mapsto a$ 即 φ是一个嵌入同态. $ax+b$是φ的值域的一个元素 $ax+b\in\mathbb{F}[x]$

由赋值同态定理, φ可扩充成 $\varphi_{ax+b}:\mathbb{F}[x]\mapsto\mathbb{F}[x]$: $\varphi_{ax+b}(x)=ax+b$.

由唯一性知 $\varphi_{ax+b}=\varphi_{ab}: f(x)\mapsto f(ax+b)$, 且是一个同态. 现证同构, 即单射.

设 $f_1(x)\in\mathbb{F}[x]$. 将 $f_1(x)$关于$ax+b$做带余除法.

$$f_1(x)=g_1(x)(ax+b)+c_1 \quad (c_1\in\mathbb{F})$$

再将$g_1(x)$关于$(ax+b)$做带余法:

$$f_1(x)=(g_2(x)(ax+b)+c_2)(ax+b)+c_1=g_2(x)(ax+b)^2+c_2(ax+b)+c_1$$

以此类推 有 $f_1(x)=c_{n+1}(ax+b)^n+\cdots+c_2(ax+b)+c_1$

则令 $f_1^*=c_{n+1}x^n+\cdots+c_2x+c_1$ 有 $\varphi_{ab}(f_1^*)=f_1$

若 $f_1^*(x)\in\ker(\varphi_{ab})$ 即 $f_1(x)=0$ $\therefore$ 有 $c_{n+1}a^n=0\Rightarrow c_{n+1}=0\Rightarrow c_n=0\Rightarrow\cdots\Rightarrow f_1^*(x)=0$

$\therefore \ker(\varphi_{ab})=\{0\}$ $\therefore\varphi_{ab}$是单射.

二. 矩阵 $A,B\in M_n(\mathbb{R})$, 求证: $(AB)^V=B^VA^V$

证明: 利用赋值同态.

对$\forall A\in M_n(\mathbb{R})$, 引入未定元$t$, 考虑矩阵 $A+tE\in M_n(\mathbb{R}(t))$, 其中$\mathbb{R}(t)$为关于$t$的有理函数域(等价于$\mathbb{R}[t]$的分式域). $\mathbb{R}(t)=\left\{\frac{a(t)}{b(t)}\mid \forall a(t),b(t)\in\mathbb{R}[t]\right\}$ 其中$b(t)\neq 0$

令 $C=A+tE=(c_{ij})_{n\times n}$ 则 $|C|=\sum_{\tau\in S_n}\varepsilon_\tau\cdot c_{\tau(1),1}\cdots c_{\tau(n),n}$ 是一个关于t的n次多项式且除t对角线上的元素相乘后含有t的n次幂, 其余的都没有, 而对角线的t^n的系数为1. $\therefore |C|$是首1的n次多项式 $\therefore |C|\neq 0$ $\therefore C$可逆 $\therefore B+tE$也可逆

$\therefore (A+tE)(B+tE)$可逆 $\therefore$ $((A+tE)(B+tE))^V=|A+tE||B+tE|((A+tE)(B+tE))^{-1}$

$$=|B+tE|(B+tE)^{-1}|A+tE|(A+tE)^{-1}$$
$$=(B+tE)^V(A+tE)^V$$

$\because$ 赋值同态 $\varphi_0:\mathbb{R}[t]\to\mathbb{R}: t\mapsto 0$

$$\therefore \varphi_0((A+tE)(B+tE))^V=\varphi_0((B+tE)^V)\varphi_0((A+tE)^V)$$

即 $(AB)^V=B^VA^V$