近世代数 (H) 第二周作业

涂嘉乐 PB23151786

2025 年 3 月 14 日

Exercise 1 设 $p \lhd R$，若 R/p 是整环，则 p 是素理想

Proof $\forall a, b \notin p$，则 $a+p, b+p \neq p = 0_{R/p}$，由 R/P 是整环知，$(a+p)(b+p) = (ab+p) \neq p = 0_{R/p}$，故 $ab \notin p$，因此 p 是素理想 $\square$

Exercise 2 求证：$2 \in \mathbb{Z}[\sqrt{-3}]$ 是不可约元，但不是素元

Proof 假设 $2 = (a+b\sqrt{-3})(c+d\sqrt{-3})$，两边同时取模得

$$2 = \sqrt{(a^2+3b^2)(c^2+3d^2)} \Rightarrow 4 = (a^2+3b^2)(c^2+3d^2)$$

所以 $a^2+3b^2 = 1, 2, 4$

①若 $a^2+3b^2=1$，则只能是 $a=\pm 1, b=0$，而 $\pm 1 \in U(\mathbb{Z}[\sqrt{-3}])$ 为平凡分解

②若 $a^2+3b^2=2$，因为 a^2, b^2 的取值为 $0,1,4$，a^2+3b^2 不可能为 2，矛盾！

③若 $a^2+3b^2=4$，此时 $c^2+3d^2=1$，故只能是 $c=\pm 1, d=0$，而 $\pm 1 \in U(\mathbb{Z}[\sqrt{-3}])$ 为平凡分解

综上，2 为不可约元

另一方面，我们有 $(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = 2 \times 2 \in (2)$，但实际上 $1+\sqrt{-3}, 1-\sqrt{-3} \notin (2)$，这是因为若 $1 \pm \sqrt{-3} \in (2)$，则 $\exists a+b\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}], \text{s.t. } 1 \pm \sqrt{-3} = 2(a+b\sqrt{-3})$，对比实部、虚部得

$$\begin{cases} 2a = 1 \\ 2b = \pm 1 \end{cases}$$

这与 $a, b \in \mathbb{Z}$ 矛盾！故 (2) 不是素理想，故 2 不是素元 $\square$

Exercise 3 设 R, S 是环，$\psi : R \to S$ 是环同态，$s \in S$，则 $\exists$ 环同态 $\tilde{\psi} : R[x] \to S, \text{s.t. } \tilde{\psi}|_R = \psi$，且 $\tilde{\psi}(x) = s$

Proof 即验证 $\tilde{\psi}$ 是环同态：首先，对 $\forall n \in \mathbb{N}^*, \tilde{\psi}(x^n) = \overbrace{\tilde{\psi}(x) \cdots \tilde{\psi}(x)}^{n\text{个}} = s^n$，所以

1. $\tilde{\psi}(1_{R[x]}) = \psi(1_R) = 1_R$

2. 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0, g(x) = b_m x^m + \cdots + b_1 x + b_0$，若 $n > m$，我们记 $b_k = 0_R, \forall m < k \leq n$，则 $g(x) = b_m x^m + \cdots + b_1 x + b_0 = b_n x^n + \cdots + b_1 x + b_0$，因此我们不妨设 $m = n$，则

$$\begin{aligned}
\tilde{\psi}(f(x)+g(x)) &= \tilde{\psi}((a_n+b_n)x^n + \cdots + (a_1+b_1)x + (a_0+b_0)) \\
&= \tilde{\psi}(a_n+b_n)\tilde{\psi(x^n)} + \cdots + \tilde{\psi}(a_1+b_1)\tilde{\psi(x)} + \tilde{\psi}(a_0+b_0) \\
&= \psi(a_n+b_n)s^n + \cdots + \psi(a_1+b_1)s + \psi(a_0+b_0) \\
&= [\psi(a_n)s^n + \cdots + \psi(a_1)s + \psi(a_0)] + [\psi(b_n)s^n + \cdots + \psi(b_1)s + \psi(b_0)] \\
&= \tilde{\psi}(a_n x^n + \cdots + a_1 x + a_0) + \tilde{\psi}(b_n x^n + \cdots + b_1 x + b_0) \\
&= \tilde{\psi}(f(x)) + \tilde{\psi}(g(x))
\end{aligned}$$

3. 同上，我们不妨设 $\deg f=\deg g$，注意到 $a_{n+1}=b_{n+1}=a_{n+2}=b_{n+2}=\cdots=a_{2n}=b_{2n}=0$，则

$$\begin{aligned}\tilde{\psi}(f(x)g(x))&=\tilde{\psi}\left(\sum_{k=0}^{2n}\left(\sum_{l=0}^{k}a_lb_{k-l}x^k\right)\right)\\&=\sum_{k=0}^{2n}\left(\sum_{l=0}^{k}\tilde{\psi}(a_lb_{k-l}x^k)\right)=\sum_{k=0}^{2n}\left(\sum_{l=0}^{k}\tilde{\psi}(a_lb_{k-l})\tilde{\psi}(x^k)\right)\\&=\sum_{k=0}^{2n}\left(\sum_{l=0}^{k}\psi(a_lb_{k-l})s^k\right)=\sum_{k=0}^{2n}\left(\sum_{l=0}^{k}\psi(a_l)\psi(b_{k-l})s^k\right)\\&=[\psi(a_n)s^n+\cdots+\psi(a_1)s+\psi(a_0)]\cdot[\psi(b_n)s^n+\cdots+\psi(b_1)s+\psi(b_0)]\\&=\tilde{\psi}(f(x))\tilde{\psi}(g(x))\end{aligned}$$

综上，$\tilde{\psi}$ 是环同态 □

Exercise 4 证明：$\mathrm{Ker}(\mathrm{ev}_a)=(x-a)$

Proof 因为

$$\mathrm{Ker}(\mathrm{ev}_a)=\{f(x)\in R[x]|\mathrm{ev}_a(f(x))=0_R\}=\{f(x)\in R[x]|f(a)=0_R\}$$

①.$(x-a)\subseteq\mathrm{Ker}(\mathrm{ev}_a)$：设 $g(x)\in(x-a)$，则 $\exists h(x)\in R[x],\text{s.t. } g(x)=h(x)(x-a)$，所以 $g(a)=h(a)(a-a)=0_R$，故 $g(x)\in\mathrm{Ker}(\mathrm{ev}_a)$，即 $(x-a)\subseteq\mathrm{Ker}(\mathrm{ev}_a)$

②.$\mathrm{Ker}(\mathrm{ev}_a)\subseteq(x-a)$：设 $m(x)\in\mathrm{Ker}(\mathrm{ev}_a)$，则 $m(a)=0$，由留数公式，$\exists q(x)\in R[x],\text{s.t. } m(x)=q(x)(x-a)+m(a)=q(x)(x-a)$，因此 $m(x)\in(x-a)$，即 $\mathrm{Ker}(\mathrm{ev}_a)\subseteq(x-a)$

综上，$\mathrm{Ker}(\mathrm{ev}_a)=(x-a)$ □

Exercise 5 设 X 是集合,R 是环,$\mathrm{Map}(X,R)=\{\theta|\theta:X\to R\}$,在 $\mathrm{Map}(X,R)$ 上定义加法、乘法:设 $\theta,\delta\in\mathrm{Map}(X,R)$

$$\begin{aligned}\theta+\delta:X&\longrightarrow R\\x&\longmapsto\theta(x)+\delta(x)\end{aligned}$$

$$\begin{aligned}\theta\cdot\delta:X&\longrightarrow R\\x&\longmapsto\theta(x)\cdot\delta(x)\end{aligned}$$

求证 $(\mathrm{Map}(X,R),+,\cdot)$ 为含幺交换环

Proof 由定义知加法、乘法满足封闭性，接下来验证八条公理以及交换性

(A1) 加法结合律：设 $\theta,\varphi,\psi\in\mathrm{Map}(X,R)$，则 $\forall x\in X$

$$\big((\theta+\varphi)+\psi\big)(x)=(\theta+\varphi)(x)+\psi(x)=\theta(x)+\varphi(x)+\psi(x)=\theta(x)+(\varphi+\psi)(x)=\big(\theta+(\varphi+\psi)\big)(x)$$

由 x 的任意性，$\big((\theta+\varphi)+\psi\big)=\big(\theta+(\varphi+\psi)\big)$

(A2) 加法交换律：设 $\psi,\varphi\in\mathrm{Map}(X,R)$，则由 R 是交换环知，$\forall x\in X$

$$(\psi+\varphi)(x)=\psi(x)+\varphi(x)=\varphi(x)+\psi(x)=(\varphi+\psi)(x)$$

由 x 的任意性，$\varphi+\psi=\psi+\varphi$

(A3) 零元存在性：考虑

$$\begin{aligned}\mathbf{0}:X&\longrightarrow R\\\forall x&\longmapsto 0_R\end{aligned}$$

则 $\forall \varphi \in \mathrm{Map}(X,R), \forall x \in X$

$$(\varphi+\mathbf{0})(x)=\varphi(x)+\mathbf{0}(x)=\varphi(x)+0_R=\varphi(x)=0_R+\varphi(x)=\mathbf{0}(x)+\varphi(x)=(\mathbf{0}+\varphi)(x)$$

由 x 的任意性，$\varphi+\mathbf{0}=\varphi=\mathbf{0}+\varphi$，则上面定义的 $\mathbf{0}$ 即为零元

(A4) 负元存在性：对 $\forall \varphi \in \mathrm{Map}(X,R)$，定义

$$\begin{aligned}\psi : X &\longrightarrow R\\ x &\longmapsto -\varphi(x)\end{aligned}$$

则对 $\forall x \in X$

$$\begin{cases}(\varphi+\psi)(x)=\varphi(x)+\psi(x)=\varphi(x)-\varphi(x)=0_R=\mathbf{0}(x)\\(\psi+\varphi)(x)=\psi(x)+\varphi(x)=-\varphi(x)+\varphi(x)=0_R=\mathbf{0}(x)\end{cases}$$

由 x 的任意性，$\varphi+\psi=\mathbf{0}=\psi+\varphi$，故 ψ 为 φ 的负元

(M1) 乘法结合律：设 $\theta,\varphi,\psi \in \mathrm{Map}(X,R)$，则 $\forall x \in X$

$$\big((\theta\cdot\varphi)\cdot\psi\big)(x)=(\theta\cdot\varphi)(x)\cdot\psi(x)=(\theta(x)\cdot\varphi(x))\cdot\psi(x)=\theta(x)\cdot(\varphi(x)\cdot\psi(x))=\big(\theta\cdot(\varphi\cdot\psi)\big)(x)$$

由 x 的任意性，$\big((\theta\cdot\varphi)\cdot\psi\big)=\big(\theta\cdot(\varphi\cdot\psi)\big)$

(M2) 幺元存在性：考虑

$$\begin{aligned}\mathbf{1} : X &\longrightarrow R\\ \forall x &\longmapsto 1_R\end{aligned}$$

则 $\forall \varphi \in \mathrm{Map}(X,R), \forall x \in X$

$$(\varphi\cdot\mathbf{1})(x)=\varphi(x)\cdot\mathbf{1}(x)=\varphi(x)\cdot 1_R=\varphi(x)=1_R\cdot\varphi(x)=\mathbf{1}(x)\cdot\varphi(x)=(\mathbf{1}\cdot\varphi)(x)$$

由 x 的任意性，$\varphi\cdot\mathbf{1}=\varphi=\mathbf{1}\cdot\varphi$，上面定义的 $\mathbf{1}$ 即为幺元

(D1) 左分配律：对 $\forall \theta,\varphi,\psi \in \mathrm{Map}(X,R), \forall x \in X$

$$\big((\theta+\varphi)\cdot\psi\big)(x)=(\theta+\varphi)(x)\cdot\psi(x)=\big(\theta(x)+\varphi(x)\big)\cdot\psi(x)=\theta(x)\cdot\psi(x)+\varphi(x)\cdot\psi(x)=(\theta\cdot\psi)(x)+(\varphi\cdot\psi)(x)$$

由 x 的任意性，$(\theta+\varphi)\cdot\psi=\theta\cdot\psi+\varphi\cdot\psi$

(D2) 右分配律：对 $\forall \theta,\varphi,\psi \in \mathrm{Map}(X,R), \forall x \in X$

$$\big(\theta\cdot(\varphi+\psi)\big)(x)=\theta(x)\cdot(\varphi+\psi)(x)=\theta(x)\cdot\big(\varphi(x)+\psi(x)\big)=\theta(x)\cdot\varphi(x)+\theta(x)\cdot\psi(x)=(\theta\cdot\varphi)(x)+(\theta\cdot\psi)(x)$$

由 x 的任意性，$\theta\cdot(\varphi+\psi)=\theta\cdot\varphi+\theta\cdot\psi$

故 $\mathrm{Map}(X,R)$ 是含幺环，最后验证 $\mathrm{Map}(X,R)$ 是交换的：$\forall \varphi,\psi \in \mathrm{Map}(X,R), \forall x \in X$

$$(\varphi\cdot\psi)(x)=\varphi(x)\cdot\psi(x)=\psi(x)\cdot\varphi(x)=(\psi\cdot\varphi)(x)$$

由 x 的任意性知 $\varphi\cdot\psi=\psi\cdot\varphi$，故它是交换环 □

Exercise 6 验证环同态

$$\begin{aligned}\mathrm{ev} : R[x] &\longrightarrow \mathrm{Map}(R,R)\\ g(x) &\longmapsto \text{多项式函数}g\end{aligned}$$

Proof

①. 因为 $1_{R[x]}$ 为常值多项式 $\mathcal{I}(x)=1_R$，它对应的多项式函数为

$$\begin{aligned}\mathcal{I}: R &\longrightarrow R\\ r &\longmapsto \mathcal{I}(r)=1_R\end{aligned}$$

故对 $\forall r\in R$ 都有 $\mathcal{I}(r)=1_R$，即 $\mathrm{ev}(\mathcal{I}(x))=\mathbf{1}$，其中 $\mathbf{1}$ 为 *Exercise 5* 中定义的幺元，故 $\mathrm{ev}(1_{R[x]})=1_{\mathrm{Map}(R,R)}$

②. 对 $\forall f(x),g(x)\in R[x],\forall r\in R$

$$\mathrm{ev}(f(x)+g(x))(r)=(f+g)(r)=f(r)+g(r)=\mathrm{ev}(f(x))(r)+\mathrm{ev}(g(x))(r)$$

由 $r\in R$ 的任意性知 $\mathrm{ev}(f(x)+g(x))=\mathrm{ev}(f(x))+\mathrm{ev}(g(x))$

③. 对 $\forall f(x),g(x)\in R[x],\forall r\in R$

$$\mathrm{ev}(f(x)g(x))(r)=(f\cdot g)(r)=f(r)\cdot g(r)=\mathrm{ev}(f(x))(r)\cdot\mathrm{ev}(g(x))(r)$$

由 $r\in R$ 的任意性知 $\mathrm{ev}(f(x)g(x))=\mathrm{ev}(f(x))\mathrm{ev}(g(x))$

因此 ev 是环同态 □

Exercise 7 考虑

$$\begin{aligned}\mathrm{ev}:\mathbb{F}_2[x]&\longrightarrow \mathrm{Map}(\mathbb{F}_2,\mathbb{F}_2)\\ f(x)&\longmapsto f\end{aligned}$$

验证：

(1) ev 为满射

(2) $\mathrm{Ker}(\mathrm{ev})=(x^2+x)$

(3) $\mathrm{Map}(\mathbb{F}_2,\mathbb{F}_2)$ 不是整环

Proof 因为 $\mathbb{F}_2=\{\overline{0},\overline{1}\}$，所以

$$\mathrm{Map}(\mathbb{F}_2,\mathbb{F}_2)=\{\mathrm{Id}_{\mathbb{F}_2},\mathbf{0}_{\mathbb{F}_2},\mathbf{1}_{\mathbb{F}_2},\theta\}$$

其中 $\mathrm{Id}_{\mathbb{F}_2}$ 为恒等映射；$\mathbf{0}_{\mathbb{F}_2}(\overline{1})=\mathbf{0}_{\mathbb{F}_2}(\overline{0})=\overline{0}$；$\mathbf{1}_{\mathbb{F}_2}(\overline{1})=\mathbf{1}(\overline{0})=\overline{1}$；$\theta(\overline{0})=\overline{1},\theta(\overline{1})=\overline{0}$

(1) 考虑 $f_1(x)=x$，则 $\mathrm{ev}(f_1)(x)=f_1,f_1(\overline{1})=\overline{1},f_1(\overline{0})=\overline{0}$，所以 $\mathrm{ev}(f_1(x))=\mathrm{Id}_{\mathbb{F}_2}$

考虑 $f_2(x)=x^2+x$，则 $\mathrm{ev}(f_2)(x)=f_2,f_2(\overline{1})=f_2(\overline{0})=\overline{0}$，所以 $\mathrm{ev}(f_2(x))=\mathbf{0}_{\mathbb{F}_2}$

考虑 $f_3(x)=x+\overline{1}$，则 $\mathrm{ev}(f_3)(x)=f_3,f_3(\overline{1})=\overline{0},f_3(\overline{0})=\overline{1}$，所以 $\mathrm{ev}(f_3(x))=\theta$

考虑 $f_4(x)=x^2+x+\overline{1}$，则 $\mathrm{ev}(f_4(x))=f_4,f_4(\overline{0})=f_4(\overline{1})=\overline{1}$，所以 $\mathrm{ev}(f_4(x))=\mathbf{1}_{\mathbb{F}_2}$

综上，ev 是满射

(2) 因为

$$\mathrm{Ker}(\mathrm{ev})=\{f(x)|\mathrm{ev}(f(x))=\mathbf{0}_{\mathbb{F}_2}\}=\{f(x)|f(\overline{0})=f(\overline{1})=\overline{0}\}$$

设 $f(x)\in\mathrm{Ker}(\mathrm{ev})$，则 $f(\overline{0})=f(\overline{1})=\overline{0}$，由留数定理，存在 $q_1(x),q_2(x)\in\mathbb{F}_2[x]$, s.t.

$$\begin{cases}f(x)=q_1(x)(x-\overline{0})+f(\overline{0})=q_1(x)x\\ f(x)=q_2(x)(x-\overline{1})+f(\overline{1})=q_2(x)(x-\overline{1})\end{cases}$$

所以 $x-\overline{1}\mid f(x),x\mid f(x)$，因为 $\gcd(x-\overline{1},x)=\overline{1}$，所以 $(x-\overline{1})x\mid f(x)$，即 $\exists h(x)\in\mathbb{F}_2[x]$, s.t.

$$f(x)=h(x)(x-\overline{1})x=h(x)(x^2-x)=h(x)(x^2+x)$$

所以 $f(x)\in(x^2+x)$，故 $\mathrm{Ker(ev)}\subseteq(x^2+x)$

反之，设 $a(x)\in(x^2+x)$，则 $\exists b(x)\in\mathbb{F}_2[x],\text{s.t.}\ a(x)=b(x)(x^2+x)$，所以

$$a(\overline{0})=b(\overline{0})\cdot\overline{0}=\overline{0},\quad a(\overline{1})=b(\overline{1})\cdot\overline{0}=\overline{0}$$

所以 $a(x)\in\mathrm{Ker(ev)}$，故 $(x^2+x)\subseteq\mathrm{Ker(ev)}$

综上，$\mathrm{Ker(ev)}=(x^2+x)$

(3) 通过比较次数可以看出，$x,x+\overline{1}\notin(x^2+x)$，故它们不是零映射，但 $x(x+\overline{1})=x^2+x$ 为零映射，所以 $\mathrm{Map}(\mathbb{F}_2,\mathbb{F}_2)$ 不是整环 □

Exercise 8 设 $R=\mathbb{Z}[\sqrt{-3}]$，$a=4,b=(1-\sqrt{-3})^2$，讨论 $\gcd(a,b)$ 是否存在

Solution 显然 $\forall u\in U(R)$ 为 a,b 的公因子；假设 $x+y\sqrt{-3}\notin U(R)$ 是 a,b 的公因子，则 $x+y\sqrt{-3}\mid a,x+y\sqrt{-3}\mid b$，故 $\exists m,n,p,q\in\mathbb{Z},\text{s.t.}$

$$\begin{cases}(x+y\sqrt{-3})(m+n\sqrt{-3})=4\\(x+y\sqrt{-3})(p+q\sqrt{-3})=(1-\sqrt{-3})^2\end{cases}$$

对第一式比较模长得

$$(x^2+3y^2)(m^2+3n^2)=16$$

由于满足上述条件的 x^2+3y^2,m^2+3n^2 为正整数，且为 16 的因数，接下来考虑 m^2,n^2 可取何值，因为 $m^2\leq 16,3n^2\leq 16$，所以 $m^2=0,1,4,9,16,n^2=0,1,4$

(1). $m^2+3n^2=1$，则 $m^2=1,n^2=0$，故 $m+n\sqrt{-3}=\pm1$，所以 $x+y\sqrt{-3}=\pm4$，进而

$$p+q\sqrt{-3}=\frac{(1-\sqrt{-3})^2}{\pm4}=\frac{1-\sqrt{-3}}{\pm2}\notin\mathbb{Z}[\sqrt{-3}]$$

故此时 $x+y\sqrt{-3}\nmid b$，矛盾！

(2). $m^2+3n^2=2$，这是不可能的

(3). $m^2+3n^2=4$，则 $x^2+3y^2=4\Rightarrow x^2=y^2=1$ 或 $x^2=4,y^2=0$

(3.1) $x^2=y^2=1$ 时在相伴意义下（差一个 -1），可设 $x+y\sqrt{-3}=1+\sqrt{-3}$ 或 $1-\sqrt{-3}$，因为

$$\begin{cases}(1-\sqrt{-3})(1+\sqrt{-3})=4\\(1-\sqrt{-3})(1-\sqrt{-3})=(1-\sqrt{-3})^2\end{cases}\qquad\begin{cases}(1+\sqrt{-3})(1-\sqrt{-3})=4\\(1+\sqrt{-3})(-2)=(1-\sqrt{-3})^2\end{cases}$$

所以 $1+\sqrt{-3},1-\sqrt{-3}$ 为 a,b 的公因数

(3.2) $x^2=4,y^2=0$，在相伴意义下，可设 $x+y\sqrt{-3}=2$，因为

$$\begin{cases}2\times2=4\\2(-1-\sqrt{-3})=(1-\sqrt{-3})^2\end{cases}$$

所以 2 为 a,b 的公因数

(4). $m^2+3n^2=8$，这是不可能的

(5). $m^2+3n^2=16$，此时 $x^2+3y^2=1$，故 $x+y\sqrt{-3}=\pm1\in U(R)$ 为平凡分解

综上，a,b 的非平凡公因数为 $2,1+\sqrt{-3},1-\sqrt{-3}$，但从这三者中任取二者，它们没有整除关系，所以 $\gcd(a,b)$ 不存在 □

Exercise 9 设 k 是域，$0\neq f(x)\in k[x]$，求证：$|\mathrm{Root}_k(f)|\leq\deg(f(x))$

Proof 对 $\deg(f(x))$ 作归纳：

若 $\deg(f(x))=0$，则 $f(x)=a_0, a_0\in k\backslash\{0_k\}$，所以 $\forall y\in k, f(y)=a_0\neq 0_k$，故 $\mathrm{Root}_k(f)=\varnothing\Rightarrow 0=|\mathrm{Root}_k(f)|\leq\deg(f(x))=0$

若 $\deg(f(x))=1$，则 $\exists a_1\in k\backslash\{0_k\}, a_2\in k, \text{s.t. } f(x)=a_1x+a_0$，由 $a_1\neq 0_k$ 知，$f(-a_1^{-1}a_0)=0$，且 $\forall y\in k$，若 $y\neq -a_1^{-1}a_0$，则 $f(y)\neq 0$（否则 $a_1y+a_0=0\Rightarrow y=-a_1^{-1}a_0$），因此 $\mathrm{Root}_k(f)=\{-a_1^{-1}a_0\}, 1=|\mathrm{Root}_k(f)|\leq\deg(f(x))=1$

假设 $\deg(f(x))=k-1$ 时命题成立，下证 $\deg(f(x))=k$ 时，命题也成立

若 $|\mathrm{Root}_k(f)|=0$，则命题显然成立；若 $|\mathrm{Root}_k(f)|\neq 0$，设 $\alpha\in\mathrm{Root}_k(f)$，则 $f(\alpha)=0$，由留数公式，$\exists q(x)\in k[x], \text{s.t.}$

$$f(x)=q(x)(x-\alpha)+f(\alpha)=q(x)(x-\alpha)$$

且 $\deg(q(x))=\deg(f(x))-1=k-1$，故 $|\mathrm{Root}_k(q)|\leq k-1$，若 $\exists y\in k, \text{s.t. } f(y)=0$，则 $q(y)(y-\alpha)=0$，则 $y\neq\alpha$ 时，$q(y)=0$，因此 $\mathrm{Root}_k(f)\subseteq\mathrm{Root}_k(q)\cup\{\alpha\}$，即

$$|\mathrm{Root}_k(f)|\leq|\mathrm{Root}_k(q)|+1\leq k-1+1=k$$

由数学归纳法知，命题对 $\deg(f(x))=n, \forall n\in\mathbb{N}^*$ 均成立 $\square$

Exercise 10

(1) 设 $k\overset{\text{子域}}{\subseteq}K, f(x), g(x)\in k[x]\subseteq K[x]$，求证 $\gcd_{k[x]}(f,g)=\gcd_{K[x]}(f,g)$

(2) 推广到一般情形 $\theta: k\hookrightarrow K$？

Proof

(1). 记 $d(x)=\gcd_{k[x]}(f(x),g(x)), d'(x)=\gcd_{K[x]}(f(x),g(x))$

Case 1. $d(x)=1$，则由 *Bezout* 等式知，$\exists u(x), v(x)\in k[x], \text{s.t. } u(x)f(x)+v(x)g(x)=1$，因为 k 是 K 的子域，所以在 k 中也有 $u(x)f(x)+v(x)g(x)=1$，由 *Bezout* 定理知 $\gcd_{K[x]}(f(x),g(x))=1$，故 $d'(x)=d(x)=1$

Case 2. $\deg(d(x))\geq 1$，则可设 $d(x)a(x)=f(x), d(x)b(x)=g(x)$，则由 *Case 1* 知

$$\gcd_{k[x]}(a(x),b(x))=\gcd_{K[x]}(a(x),b(x))=1$$

因为在 $K[x]$ 中，也有 $d(x)\mid f(x), d(x)\mid g(x)$，所以 $d(x)\mid\gcd_{K[x]}(f,g)=d'(x)$，只需证明 $d'(x)\mid d(x)$ 即可证明二者相等，因为 $\gcd_{k[x]}(a(x),b(x))=1$，由 *Bezout* 定理知，$\exists u(x), v(x)\in k[x], \text{s.t. } u(x)a(x)+v(x)b(x)=1$，这在 K 中也成立，因此在 K 中我们有

$$u(x)a(x)d(x)+v(x)b(x)d(x)=d(x)\Rightarrow u(x)f(x)+v(x)g(x)=d(x)$$

由 *Bezout* 定理的逆定理知，$d'(x)\mid d(x)$，因此二者相等

(2). **命题：**考虑环同构

$$\begin{aligned}\tilde\theta: k[x]&\longrightarrow \mathrm{Im}\theta[x]\\ a&\longmapsto\theta(a)\\ x&\longmapsto x\end{aligned}$$

设 $f(x)=a_nx^n+\cdots+a_1x+a_0$，则 $\tilde\theta(f(x))=\theta(a_n)x^n+\cdots+\theta(a_1)x+\theta(a_0)$ ，则我们有

$$\tilde\theta\left(\gcd_{k[x]}(f,g)\right)=\gcd_{\mathrm{Im}\theta[x]}(\tilde\theta(f),\tilde\theta(g))=\gcd_{K[x]}(\tilde\theta(f),\tilde\theta(g))$$

证明： 由于 $\mathrm{Im}\theta \overset{\text{子域}}{\subseteq} K$，由 (1) 知 $\gcd_{\mathrm{Im}\theta[x]}(\tilde{\theta}(f),\tilde{\theta}(g)) = \gcd_{K[x]}(\tilde{\theta}(f),\tilde{\theta}(g))$，因此只需证明

$$\tilde{\theta}\left(\gcd_{k[x]}(f,g)\right) = \gcd_{\mathrm{Im}\theta[x]}(\tilde{\theta}(f),\tilde{\theta}(g))$$

我们记

$$d(x) = \gcd_{k[x]}(f,g), d'(x) = \gcd_{\mathrm{Im}\theta[x]}(\tilde{\theta}(f),\tilde{\theta}(g))$$

因为 $d(x) \mid f(x), d(x) \mid g(x)$，所以 $\exists a(x), b(x) \in k[x], \text{s.t. } f(x) = a(x)d(x), g(x) = b(x)d(x)$，同时作用 $\tilde{\theta}$ 得

$$\tilde{\theta}(f(x)) = \tilde{\theta}(a(x))\tilde{\theta}(d(x)), \quad \tilde{\theta}(f(x)) = \tilde{\theta}(b(x))\tilde{\theta}(d(x))$$

所以 $\tilde{\theta}(d(x)) \mid d'(x)$

又因为 $\tilde{\theta}^{-1}$ 也为环同构，所以同理我们有

$$\tilde{\theta}^{-1}(d'(x)) \mid d(x)$$

即 $\exists u(x) \in k[x], \text{s.t. } \tilde{\theta}^{-1}(d'(x))u(x) = d(x)$，两边同时作用 $\tilde{\theta}$ 得 $d'(x)\tilde{\theta}(u(x)) = \tilde{\theta}(d(x))$，故 $d'(x) \mid \tilde{\theta}(d(x))$，所以它们相互整除，故 $d'(x) = \tilde{\theta}(d(x))$ □