

Homework 3

①

P1)

a) $f = 1 \cdot f \approx f/f$

b) $f/g \Rightarrow g = f \cdot q$ ~~$g/h \Rightarrow h = g \cdot s$~~ $g/f \Rightarrow f = g \cdot s \approx g = f \cdot q = g \cdot s \cdot q \therefore \deg s + \deg q = 0$
 $\approx \deg s = \deg q = 0$ hence q and s are ^{monics} constants, moreover $q = \frac{1}{s}$ and $\approx f = g \cdot s$ since g and f are monic $\Rightarrow s = 1 \Rightarrow f = g$

c) $f/h \Rightarrow h = f q_1, h/g \Rightarrow g = h q_2 \approx g = f q_1 q_2 \therefore f/g$

$\exists f, g \in \mathbb{F}[x]$, not necessarily monic, then $f = g \cdot s$ with a $s = \text{const.}$ ~~can~~ doesn't imply $f = g$ necessarily and anti-symmetry property fails $\therefore (\mathbb{F}[x], |)$ is not a pre-order.

P2)

a) p has a rational root $r/s \Rightarrow \sum_{i=0}^m a_i \frac{r^i}{s^i} = 0$, multiply by s^m , we get

$$a_0 \cdot s^m = - (a_1 r \cdot s^{m-1} + a_2 r^2 s^{m-2} + \dots + a_{m-1} r^{m-1} s + a_m r^m)$$

$$= r \cdot (\dots) = r \cdot c \approx r \cdot \frac{a_0 s^m}{r} \in \mathbb{Z} \Rightarrow \frac{a_0 s^m}{r}$$

$\hookrightarrow \text{integer} = c$

since $\gcd(r, s) = 1$ then $r/a_0, r/a_0$

likewise one can show s/a_m ~~multiply by~~, ~~divide~~ multiply by $\frac{s^{m-1}}{r}$ then we get

~~$\frac{a_0}{r^m} + \frac{a_1}{r^{m-1}s} + \dots + \frac{a_m}{s^m} = 0$~~ $\frac{a_m r^m}{s} = - (\sum_{l=0}^{m-1} a_l s^{m-1-l} r^l) \in \mathbb{Z}$

again, since $\gcd(r, s) = 1$ we get s/a_m .

b) $\deg f \geq 1$, any f has a root in $\mathbb{Q}$, since call this root r/s , since f is monic $a_m = 1$, and $m \geq 1$ and $s/a_m = 1 \approx s = 1$

c) $a_0 = -4$ and $a_3 = 1$ $\approx$ if there is a rational root, is integer, the only possibilities are $r \in \mathbb{Z}$ s.t. $r/a_0 = -4 \approx r \in \{\pm 1, \pm 2, \pm 4\}$, then one just check one by one.

P3/

a) $f = qg + r$, call $h = \gcd(f, g)$ then $h|g$ and $h|f$ so $h|\overbrace{(f - qg)}^r$
 $\Leftrightarrow h|r$. So $\gcd(f, g)$ divides g and r . Suppose $\exists h'$ s.t. $h'|g$ and $h'|r$, then $h'|(f - qg) \therefore h'|f$ and if h' divides f and g then $h|h'$ because $h = \gcd(f, g) \therefore h = \gcd(g, r)$ as well.

b) Let $p = \gcd(f_1, \dots, f_s)$ then $p|f_i \quad i=1, \dots, s$ and if $p' \nmid f_i \quad \forall i=1, \dots, s$ then $h|p'$
 in particular $p|f_1$ and if $h = \gcd(f_2, \dots, f_s)$ then, since $p|f_j$ for $j=2, \dots, s$, then $h|p$, by transitivity of division (note, transitivity is valid over $F[x]$, not only $F_0[x]$)
 then $h|f_1$, so $h|f_i \quad i=1, \dots, s$ then since $p = \gcd(f_1, \dots, f_s)$, $p|h$ ($\because p = c \cdot h$)
 (constant)

So for, $p|f_1$ and $p|\gcd(f_2, \dots, f_s)$. ~~Suppose $h^p|f_1$ and $h^p|\gcd(f_2, \dots, f_s)$~~

~~then $h^p|h$~~ $\therefore$ if $h^p = \gcd(f_1, \gcd(f_2, \dots, f_s))$ then $h^p|p$

but also, ~~we just show if $h^p|f_1$~~ $h^p|f_i \quad i=1, \dots, s$ (by definition) so

$p|h^p \therefore p = c \cdot h^p$
 (constant)

c) g_1, g_2 are $\gcd(f_1, \dots, f_s)$ then by b) g_1, g_2 are $\gcd(f_1, \gcd(f_2, \dots, f_s)) = \gcd(f_1, p)$
 so $g_1 = c \cdot g_2$.

d) Euclidean algorithm to compute $\gcd(f, g)$ WLOG $\deg f \leq \deg g$, then
 $g = f \cdot q_0 + r_0$ $\deg r_0 < \deg f$ so $f = q_1 r_0 + r_1$
 so $\gcd(f, g) \stackrel{\text{part a)}}{=} \gcd(f, r_0) \stackrel{\text{part a)}}{=} \gcd(r_1, r_0) \stackrel{\text{part a)}}{=} \gcd(r_2, r_1)$
 $= \dots = \gcd(r_m, r_{m+1})$ $\deg r_1 < \deg r_0$
 so $r_0 = q_2 r_1 + r_2$

since $\deg r_m < \deg r_{m-1}$, eventually $r_m = 0$, so

$\gcd(f, g) = \gcd(r_{m-1}, r_{m-2}) = \gcd(r_m=0, r_{m-1}) = r_{m-1}$ ✓

e) $\underline{s=2}$, $h = \gcd(f_1, f_2)$, then by what we learn in ^{lecture} ~~class~~, this base case is ~~is~~ already (2)

~~So~~ Assume for s , let's prove it for $s+1$

$$h = \gcd(f_1, \dots, f_{s+1}) = \gcd(f_1, \underbrace{\gcd(f_2, \dots, f_{s+1})}_{\substack{|| \\ h'}})$$

we know then that $\exists \alpha_1, \alpha_2 \in \mathbb{C}[x]$ s.t. $h = \alpha_1 f_1 + \alpha_2 h'$, by inductive hyp. we know $\exists \alpha'_2, \dots, \alpha'_{s+1} \in \mathbb{C}[x]$ s.t. $h' = \sum_{l=2}^{s+1} \alpha'_l f_l(x)$, define $\alpha_l = \alpha_2 \alpha'_l$ for $l=2, \dots, s+1$ and we have the desired result.

f) $\Rightarrow$ ~~suppose~~ $f_1, \dots, f_s$ ~~have no common root~~ ^{with no common root} $\in \mathbb{C}[x]$ ~~then~~ consider $h = \gcd(f_1, \dots, f_s)$, ~~then~~ $\exists \alpha_i$ s.t.

~~$h = \sum \alpha_i f_i \in \mathbb{C}[x]$, if $\deg h \geq 1$, by FTA it has a root~~

~~take λ root of h , then $h(\lambda) = 0 = \sum_{i=1}^s \alpha_i(\lambda) f_i(\lambda)$~~

~~then $(x-\lambda) \mid h = \sum \alpha_i f_i$~~

Suppose $\deg h \geq 1$ then $f_i = h \cdot g_i$ but since $h \in \mathbb{C}[x]$ by FTA

h has a root and so f_i 's have a common root $\therefore h = \text{const.} \neq 0$

and by e) $\exists \alpha_1, \dots, \alpha_s$ s.t. $\sum_{i=1}^s \alpha_i f_i = 1$

$\Leftarrow$ Suppose $1 = \sum \alpha_i f_i$ if f_i 's have a common root λ , $\sum \alpha_i(\lambda) f_i(\lambda) = 0 \neq 1$

124/

a) This was sketched in class: (no is essentially a gift!)

$f(x_i) = w_i$ $i=0, \dots, m$, write $f(x) = \sum_{i=0}^m a_i x^i$

$$\Rightarrow \underbrace{\begin{bmatrix} 1 & x_0 & \dots & x_0^m \\ 1 & x_1 & \dots & x_1^m \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_m & \dots & x_m^m \end{bmatrix}}_{A \in M_{m+1, m+1}(\mathbb{C})} \begin{bmatrix} a_0 \\ \vdots \\ a_m \end{bmatrix} = \begin{bmatrix} w_0 \\ \vdots \\ w_m \end{bmatrix}$$

$\det A = \prod_{0 \leq i < j \leq m} (x_i - x_j)$ since all x 's are distinct, then $\det A \neq 0$ hence A is invertible, so $\vec{a} = A^{-1} \vec{w}$ is unique.

b)

$$\begin{aligned}
 & T(c_1 P_1 + c_2 P_2) = (c_1 P_1(x_0) + c_2 P_2(x_0), \dots, c_1 P_1(x_m) + c_2 P_2(x_m)) \\
 & = c_1 (P_1(x_0), \dots, P_1(x_m)) + c_2 (P_2(x_0), \dots, P_2(x_m)) \\
 & = c_1 T(P_1) + c_2 T(P_2)
 \end{aligned}$$

2) a basis is given by $1, x, x^2, \dots, x^m$ hence $\dim(\mathbb{C}_m[x]) = m+1$

3) $T: \mathbb{C}_m[x] \rightarrow \mathbb{C}^{m+1}$ 1st injectivity $\text{Ker } T = ?$

~~rank-nullity thm~~ $\Rightarrow$

$$T(f(x)) = (f(x_0), \dots, f(x_{m+1})) = (0, \dots, 0)$$

must be
 f a polynomial of degree $\leq m$, with $m+1$ roots $(x_0, \dots, x_{m+1}) \therefore f = 0$

so $\text{Ker } T = \{0\}$ means T is injective

now, rank-nullity thm

$$\dim(\text{Ker } T) - \dim V = -\dim \text{Image } T = 0 - (m+1)$$

$$\Rightarrow \dim(\text{Image } T) = m+1 \therefore T \text{ is } \underline{\text{surjective}}$$

hence T is invertible and so $\exists!$ sol to $T(p) = (w_0, \dots, w_m) \in \mathbb{C}^{m+1}$

c) P_k satisfies $P_k(x_k) \in \mathbb{C} \setminus \{0\}$ (because all x 's are distinct) and $P_k(x_j) = 0$ for $j \neq k$

$$\text{so } y_k = \frac{P_k(x)}{P_k(x_k)} \cdot w_k \text{ satisfies } y_k(x_k) = w_k \quad y_k(x_j) = 0 \text{ for } j \neq k \text{ hence a sol. is}$$

$$f = \sum_{i=0}^m \frac{P_i(x)}{P_i(x_i)} \cdot w_i$$

(I forgot to explicitly ask for uniqueness, but it comes just from considering f' being another sol. and looking at zeroes of $f - f'$)

P5

3

a) $T(C_1 P_1(x) + C_2 P_2(x)) = C_1 P_1(x^2) + C_2 P_2(x^2) = C_1 T(P_1) + C_2 T(P_2)$

b) $\{1, \dots, x^5\}$ is a basis of $\mathbb{R}_5[x]$, then applying T to it, we get

$\{1, x^2, x^4, x^6, x^8, x^{10}\}$ ~~this is a basis~~ since all ~~these~~ these elements are L.I., thus is
a basis of $\text{Image}(T)$

another way is to show by direct computation $\text{Image}(T) \subseteq \langle 1, x^2, x^4, x^6, x^8, x^{10} \rangle$

and $\langle 1, x^2, \dots \rangle \subseteq \text{Image } T \Rightarrow \text{Image}(T) = \langle 1, x^2, \dots, x^{10} \rangle$

c) we need to prove $\text{Ker } T = \{0\}$

~~$T(p) = 0 \Rightarrow$~~ $T\left(\sum_{i=0}^m a_i x^i\right) = \sum_{i=0}^m a_i x^{2i} = 0 \Rightarrow a_i = 0 \forall i$