Math 332 HW 11 Solutions

1. (a) It is easy to check that $f(a_i) = b_i$ for $i = 1, \dots, n+1$ and that $\deg f = n$. If g is another polynomial with these properties then $f - g$ is a polynomial of degree n with at least $n+1$ zeros. Hence, $f - g = 0$. $\square$

(b) $$f(x) = 0 \cdot \frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} - 1 \cdot \frac{(x-1)(x-3)(x-4)}{(2-1)(2-3)(2-4)} + 0 \cdot \frac{(x-1)(x-2)(x-4)}{(3-1)(3-2)(3-4)} + 1 \cdot \frac{(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)}$$

$$= -\tfrac{1}{2}(x-1)(x-3)(x-4) + \tfrac{1}{6}(x-1)(x-2)(x-3) = -\tfrac{1}{3}x^3 + 3x^2 - \tfrac{23}{3}x + 5.$$

2. (a) By Fermat's little theorem, $x^{p-1} - 1 = 0$ for $x = 1, 2, \dots, p-1$ in $\mathbb{Z}_p$. Hence, $x - i$ is a factor of $x^{p-1} - 1$ for $i = 1, 2, \dots, p-1$ in $\mathbb{Z}_p[x]$. Therefore, $x^{p-1} - 1 = \alpha (x-1)(x-2)\cdots(x-(p-1))$ for some $\alpha \in \mathbb{Z}_p[x]$. Comparing the coefficient of x^{p-1} on both sides of this equation, we get $\alpha = 1$. $\square$

(b) Setting $x = 0$ in (a), we get $-1 = (p-1)! \bmod p$. But $p - 1 = -1 \bmod p$, so $-1 = (p-1)(p-2)! = -(p-2)! \bmod p \Rightarrow (p-2)! = 1 \bmod p$.

3 (a) $p \in R$ prime iff $(p) \subseteq R$ prime.

Pf/ ($\Rightarrow$) Suppose $p \in R$ is prim and let $ab \in (p)$ for some $a, b \in R$. Thus, $ab = cp$ for some $c \in R$. Hence, $p \mid ab$. Since p is prime, we may assume $p \mid a$. So $\exists d \in R$ s.t. $a = dp \in (p)$, as required.

($\Leftarrow$) Conversely, suppose $(p) \subseteq R$ is prim and suppose $p \mid ab$ for some $a, b \in R$. Thus, $\exists c \in R$ s.t. $ab = cp \in (p)$. Since (p) is prime, we may assume $a \in (p)$. So $\exists d \in R$ s.t. $a = dp$. Thus, $p \mid a$. $\square$

(b) a, b are associates iff $(a) = (b)$.

Pf/ ($\Rightarrow$) Suppose $a = bu$ for some unit $u \in R$. Thus, $a = bu \in (b) \Rightarrow (a) \subseteq (b)$. Conversely, since $b = au^{-1} \in (a)$, so $(b) \subseteq (a)$. Therefore, $(a) = (b)$.

($\Leftarrow$) Conversely, suppose $(a) = (b)$. Then $a \in (a) = (b) \Rightarrow \exists c \in R$ s.t. $a = cb$ and $b \in (b) = (a) \Rightarrow \exists d \in R$ s.t. $b = da$. As a special case, note that that $a = 0$ iff $b = 0$, and in this case a, b are trivially associates.

otherwise, $a = cb$ and $b = da \Rightarrow b = dcb \Rightarrow b(1-dc) = 0 \Rightarrow 1 - dc = 0$ (since $b \neq 0$ and R is a domain) $\Rightarrow dc = 1 \Rightarrow d$ and c are units $\Rightarrow a$ and b are associates. $\square$

4). Find all maximal ideals in $\mathbb{Z}_5[x]$ of the form $(x^2 + ax + b)$.

Solution/ In a PID, like $\mathbb{Z}_5[x]$, an ideal is maximal iff it's generated by a prime, hence irreducible element. So we are just looking for all $a, b \in \mathbb{Z}_5$ such that $x^2 + x + b$ is irreducible. If a quadratic factors, it's factors must be linear. Hence, a quadratic factors iff it has a zero. So we are looking for $a, b \in \mathbb{Z}_5$ s.t. $x^2 + ax + b$ has no zeros in $\mathbb{Z}_5$. The quadratic equation applies in $\mathbb{Z}_5$ (just complete the square as usual). So $x^2 + ax + b$ does not factor iff its discriminant, $a^2 - 4b$, which equals $a^2 + b$ in $\mathbb{Z}_5$, is not a perfect square mod 5. This means iff $a^2 + b \in \{2, 3\}$. Letting $a = 0, 1, 2, 3, 4$, in turn and solving for b gives the following possibilities: $x^2 + 2$, $x^2 + 3$, $x^2 + x + 1$, $x^2 + x + 2$, $x^2 + 2x + 3$, $x^2 + 2x + 4$, $x^2 + 3x + 3$, $x^2 + 3x + 4$, $x^2 + 4x + 1$, $x^2 + 4x + 2$.

5. Factor $f = x^3+x^2+x+1$ over $\mathbb{Z}_5$, $\mathbb{Q}$, and $\mathbb{C}$.

Solution / $\mathbb{Z}_5$ Look for zeros: $f(0)=1$, $f(1)=4$, $f(2)=0$, $f(3)=0$, $f(4)=0$.

Hence, $f = (x-2)(x-3)(x-4)$.

$\mathbb{Q}$ $f(-1) = 0 \Rightarrow x+1$ is a factor:

$$\begin{array}{r|l} & x^2+1 \\ \hline x+1 & x^3+x^2+x+1 \\ & \underline{x^3+x^2} \\ & \quad x+1 \\ & \underline{x+1} \\ & \quad 0 \end{array}$$

So $f = (x+1)(x^2+1)$, and

x^2+1 is irreducible over $\mathbb{Q}$ since $f(q) > 0 \ \forall q \in \mathbb{Q}$.

$\mathbb{C}$ $f = \frac{x^4-1}{x-1}$. Hence, the zeros of f are the 4^{th} roots of 1, besides 1 itself.

$f = (x+1)(x+i)(x-i)$, (which is also clear from the factorization over $\mathbb{Q}$).

6 (a) irreducible by Eisenstein's criterion with $p=3$.

(b) $f = \Phi_7$, the 7^{th} cyclotomic polynomial, which we showed was irreducible in class via Eisenstein's criterion applied to $f(x+1)$.

(c) Reduce mod 2 to get x^4+x+1. This polynomial has no zeros in $\mathbb{Z}_2$, hence, no linear factors. If $x^4+x+1 = (x^2+ax+b)(x^2+cx+d)$, multiplying out and comparing coefficients gives

$$x^4+x+1 = x^4+(a+c)x^3+(b+d+ac)x^2+(bc+ad)x+bd \in \mathbb{Z}_2[x].$$

So $bd=1 \Rightarrow b=d=1$ in $\mathbb{Z}_2$.

Then $1 = bc+ad = c+a$ (the x-term)

$0 = b+d+ac = 1+1+ac = ac \Rightarrow a=c=1$ (the x^2-term)

So $1=c+a=1+1=0$, a contradiction. So x^4+x+1 has no quadratic factors either. Hence, it is irreducible over $\mathbb{Z}_2$ and the original polynomial is irreducible over $\mathbb{Q}$.

(d) $f(x+2) = x^6+12x^5+60x^4+162x^3+249x^2+204x+69$, which is irreducible via Eisenstein's criterion with $p=3$. Hence, f is irreducibility.

7. (a) x^4+1 is irreducible over $\mathbb{Q}$.

Solution / Let $f = x^4+1$. Then $f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$, which is irreducible via Eisenstein's criterion with $p=2$. Hence, f is irreducible.

(b) For each prime p, we have that $-1, 2$, or -2 is a perfect square.

Solution / Fix a prime p and consider the multiplicative group $\mathbb{Z}_p^*$. Let $(\mathbb{Z}_p^*)^2$ be the subgroup of perfect squares. Then $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2$ is a group of order 2 (since $x^2 - a = 0$ has either no zeros or 2 zeros for each $a \in \mathbb{Z}_p^*$). If -1 and 2 are not perfect squares, then $-1 = 2$ in $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2$. Hence, $-2 = (-1)(2) = (-1)^2 = 1$ in $\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2$, i.e. $-2 \in (\mathbb{Z}_p^*)^2$. □

(c) Show $f = x^4+1$ is reducible modulo each prime p.

Solution / $(x^2+ax+b)(x^2+cx+d) = x^4 + (a+c)x^3 + (b+ac+d)x^2 + (bc+ad)x + bd$

$= x^4 + 1$

$\iff a+c=0,\ b+ac+d=0,\ bc+ad=0,\ bd=1$

$\iff c=-a,\ b-a^2+d=0,\ a(d-b)=0,\ bd=1.$

From $a(d-b)=0$, we need for $a=0$ or $d=b$.

If $a=0$, then $c=0$, $b+d=0$, and $bd=1 \Leftrightarrow a=c=0$, $d=-b$, $b^2=-1$.

Thus, we are ok if -1 has a square root in $\mathbb{Z}_p$.

Otherwise, $d=b$, $c=-a$, $2b=a^2$, $b^2=1 \Leftrightarrow b=\pm 1$, $d=b$, $c=-a$, $\pm 2 = a^2$.

So we are OK if we can solve $a^2=2$ or $a^2=-2$.

By part (b), we are done.

(d) Factor x^4+1 completely over $\mathbb{Z}_2$ and $\mathbb{Z}_3$

Solution / $\mathbb{Z}_2$ $f(1)=0 \Rightarrow x+1$ is a factor. One could use long division and recurse, but a lucky guess at this point gives $x^4+1=(x+1)^4$.

$\mathbb{Z}_3$ $f(0)=1$, $f(1)=2$, $f(2)=2$. So there are no linear factors.

Using our solution to (c), note that $-2=1$ is a perfect square mod 3.

Using notation from above: $d=b$, $c=-a$, $b=-1$, $a=1$, which gives

$$x^4+1=(x^2+x-1)(x^2-x-1).$$

(e) Why don't (a) & (c) contradict Thm. 35.8.

Solution / Theorem 35.8 says that f reducible $\Rightarrow \bar{f}$ reducible, not conversely. □

8 (a) $a_1, \dots, a_n \in R$, R a PID. Show $(a_1, \dots, a_n) = (\gcd(a_1, \dots, a_n))$

Pf/ Let $d = \gcd(a_1, \dots, a_n)$. Since $d \mid a_i \ \forall i$, we have $a_i = e_i d_i$ for some $e_i \in R \ \forall i$. Hence, $a_i \in (d) \ \forall i$ and $(a_1, \dots, a_n) \subseteq (d)$. Conversely, since R is a PID, $\exists c \in R$ s.t. $(c) = (a_1, \dots, a_n)$. Therefore, $a_i \in (c) \ \forall i$, which implies $\exists b_i \in R$ s.t. $a_i = b_i c \ \forall i$. Thus, $c \mid a_i \ \forall i$. By definition of the gcd, we get that $c \mid d$. So $\exists u \in R$ s.t. $d = cu$. Hence, $d \in (c)$, which shows $(d) \subseteq (c) = (a_1, \dots, a_n)$.

(b) $f = x^4 + 5x^3 + 5x^2 - 5x - 6$, $g(x) = x^3 + 4x^2 - 9x - 36$

(i) Compute $\gcd(f, g)$.

Solution/
$$\left.\begin{aligned} f - xg &= x^3 + 14x^2 + 31x - 6 \\ f - xg - g &= 10x^2 + 40x + 30 \end{aligned}\right\} \Rightarrow (f,g) = (g, \underbrace{x^2 + 4x + 3}_{\frac{1}{10}h})$$
$$\left.\begin{aligned} g - x\left(\tfrac{1}{10}h\right) &= -12x - 36 =: \ell \end{aligned}\right\} = (f,g) = (\underbrace{x+3}_{-\frac{1}{12}\ell}, \tfrac{1}{10}h)$$
$$\left.\begin{aligned} \tfrac{1}{10}h - x\left(-\tfrac{1}{12}\ell\right) &= x + 3 \\ \tfrac{1}{10}h - x\left(-\tfrac{1}{12}\ell\right) - \left(-\tfrac{1}{12}\ell\right) &= \underline{0} \end{aligned}\right\} \Rightarrow (f,g) = (x+3).$$

Hence, $\gcd(f,g) = (x+3)$.

(ii) Write $\gcd(f,g)$ as a linear combination of f and g.

Solution / Retracing our steps in (i):

$$x+3 = \tfrac{1}{10}h - x\left(-\tfrac{1}{12}l\right)$$

$$= \tfrac{1}{10}h + \tfrac{1}{12}xl$$

$$= \tfrac{1}{10}h + \tfrac{1}{12}x\left[g - x\left(\tfrac{1}{10}h\right)\right]$$

$$= \tfrac{1}{12}xg + \left(1 - \tfrac{1}{12}x^2\right)\tfrac{1}{10}h$$

$$= \tfrac{1}{12}xg + \left(1-\tfrac{1}{12}x^2\right)\left(\tfrac{1}{10}\right)(f - xg - g)$$

$$= \tfrac{1}{10}\left(1-\tfrac{1}{12}x^2\right)f + \tfrac{1}{12}xg + \left(1-\tfrac{1}{12}x^2\right)(-x-1)\left(\tfrac{1}{10}\right)g$$

$$= \tfrac{1}{10}\left(1-\tfrac{1}{12}x^2\right)f + \left(\tfrac{1}{12}x + \tfrac{1}{10}\left(\tfrac{1}{12}x^2-1\right)(x+1)\right)g$$

$$= \left(-\tfrac{1}{120}x^2 + \tfrac{1}{10}\right)f + \left(\tfrac{1}{120}x^3 + \tfrac{1}{120}x^2 - \tfrac{1}{60}x - \tfrac{1}{10}\right)g.$$

$l = g - x\left(\tfrac{1}{10}h\right)$

$h = f - xg - g$