Introduction to Analysis – MA 542 – Fall 2019 – R. Pollack
HW #3 Solutions

Section 22:
17) Clearly 0 is a root of this polynomial. Then for $a \not\equiv 0 \pmod 5$, by Fermat's little theorem, we know that $a^4 \equiv 1 \pmod 5$. Thus, for any $a \in (\mathbb{Z}_5)^\times$ we have

$$2a^{219} + 3a^{74} + 2a^{57} + 3a^{44} \equiv 2a^3 + 3a^2 + 2a^1 + 3a^0 \equiv 2a^3 + 3a^2 + 2a^1 + 3 \pmod 5.$$

Directly computing, we see that $a = 1, 2, 3$ satisfy $2a^3 + 3a^2 + 2a^1 + 3 \equiv 0 \pmod 5$. Thus the zeroes of this polynomial in $\mathbb{Z}_5$ are $0, 1, 2, 3$.

23)

a. True.

b. True.

c. True.

d. True.

e. False.

f. False. For instance, $f(x) = 2x^3$ and $g(x) = 2x^4$ in $\mathbb{Z}_4[x]$.

g. True.

h. True.

i. True.

j. False.

25) (a) The units of $D[x]$ are simply the units of D when D is an integral domain. It's clear that the units of D are units in $D[x]$. For the reverse inclusion, let $f \in D[x]^\times$. Then there exists $g \in D[x]$ such that $fg = 1$. Then since over an integral domain, we have $\deg(fg) = \deg(f) + \deg(g)$, we have $\deg(f) + \deg(g) = \deg(1) = 0$. In particular, $\deg(f) = \deg(g) = 0$ and both f and g are constants in D. Since $fg = 1$, we see that f and g are units in D as desired.

(b) By part (a), $(\mathbb{Z}[x])^\times = \mathbb{Z}^\times = \{\pm 1\}$ since $\mathbb{Z}$ is an integral domain.

(c) By part (a), $(\mathbb{Z}_7[x])^\times = \mathbb{Z}_7^\times = \mathbb{Z}_7 - \{0\}$ since $\mathbb{Z}_7$ is a field.

Section 23:
2) $q(x) = 5x^4 + 5x^2 + 6x$ and $r(x) = x + 2$.

6) The generators of $\mathbb{Z}_7$ are 3 and 5.

7) First note (by direct computation) that 3 is a generator of $\mathbb{Z}_{17}$. Then all generators of $\mathbb{Z}_{17}$ are given by 3^a where $\gcd(a, 16) = 1$. This list is $\{3, 5, 6, 7, 10, 11, 12, 14\}$.

9) $x^4 + 4 \equiv x^4 - 1 = (x-1)(x-2)(x-3)(x-4) \pmod 5$ by Fermat's little theorem.

12) We have $x^3 + 2x + 3 = (x+3)(x+1)^2$ in $\mathbb{Z}_5[x]$ and is thus not irreducible.

14) We have that $f(x) = x^2 + 8x - 2$ is irreducible over $\mathbb{Q}$ iff it has no roots in $\mathbb{Q}$. To see if it has any roots, we use the quadratic formula which gives that any root if of the form

$$\frac{-8 \pm \sqrt{64+8}}{2} = \frac{-8 \pm \sqrt{72}}{2} = \frac{-8 \pm 6\sqrt{2}}{2} = -4 \pm 3\sqrt{2}.$$

As $\sqrt{2}$ is irrational, so is $-4 \pm 3\sqrt{2}$ and thus $f(x)$ has no roots in $\mathbb{Q}$ and is irreducible over $\mathbb{Q}$. However, $f(x)$ is reducible over $\mathbb{R}$ or $\mathbb{C}$ as it has real (and thus complex) roots.

16) By the rational root theorem, if $f(x) = x^3 + 3x^2 - 8$ has a root in $\mathbb{Q}$, then the root is in the set $\{\pm 1, \pm 2, \pm 4\}$. By direct computation, none of these elements are roots and thus $f(x)$ has no roots in $\mathbb{Q}$. Since $f(x)$ is a cubic, this means that $f(x)$ is irreducible over $\mathbb{Q}$.

18) $x^2 - 12$ is an Eisenstein polynomial for $p = 3$ and is thus irreducible over $\mathbb{Q}$.

20) $4x^{10} - 9x^3 + 24x - 18$ is not Eisenstein for any prime p. Indeed, because of the cubic term $-9x^3$ the only possible prime to use is $p = 3$. However, 9 divides the constant term which is -18.

25)

a. True.

b. True.

c. True.

d. False. $x = 2$ is a zero.

e. True.

f. False. Every non-zero element is a unit.

g. True (unless you want to say that 0 is a counter-example).

h. True (unless you want to say that 0 is a counter-example).

i. True.

j. False. The 0 polynomial can have infinitely many zeroes.

26) We have $f(x) = x^4 + x^3 + x^2 - x + 1$ has $x + 2$ as a factor iff $f(x)$ has -2 as root. This is the case if $f(-2) \equiv 0 \pmod p$. Since $f(-2) = (-2)^4 + (-2)^3 + (-2)^2 - (-2) + 1 = 15$ we have that this holds iff $p = 3$ or $p = 5$.

28) The only polynomials of degree 3 in $\mathbb{Z}_2[x]$ are:

$$x^3, x^3+1, x^3+x, x^3+x+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1.$$

The irreducible ones in this list are the ones with no roots in $\mathbb{Z}_2$. First eliminating the ones with 0 as a root gives:

$$x^3+1, x^3+x+1, x^3+x^2+1, x^3+x^2+x+1.$$

Then eliminating the ones with 1 as a root gives

$$x^3+x+1, x^3+x^2+1.$$

30) Now there are a lot of polynomials to consider. Let's not list them all. Rather any such polynomial will be of the form ax^3+bx^2+cx+d with $a \neq 0$. In fact, let's scale so that $a=1$. Then if such a polynomial is irreducible then 0, 1 and 2 are not zeroes. Since 0 is not a zero, we know that $d \neq 0$. Since 1 is not a root, we know that $1+b+c+d \neq 0$. Since 2 is not a root, we know that $2+b+2c+d \neq 0$.

The complete list of such polynomials is:

$$x^3+2x+1, x^3+2x+2, x^3+x^2+2, x^3+x^2+x+2, x^3+x^2+2x+1, x^3+2x^2+1, x^3+2x^2+x+1, x^3+2x^2+2x+2.$$

These are just the monic irreducibles. There are also the polynomials whose leading coefficient is 2 (which is obtained by simply scaling each polynomial in the above list by 2):

$$2x^3+x+1, 2x^3+x+2, 2x^3+x^2+2, 2x^3+x^2+x+1, 2x^3+x^2+2x+2, 2x^3+2x^2+1, 2x^3+2x^2+x+2, 2x^3+2x^2+2x+1.$$

34) To show that $f(x) = x^p + a$ is never irreducible over $\mathbb{Z}_p$, we will exhibit a root of this polynomial. Namely,

$$f(-a) = (-a)^p + a = -a + a = 0$$

as by Fermat's little theorem $b^p = b$ for any b in $\mathbb{Z}_p$.

37c) The mod 5 reduction of f is x^3+2x+1 which is irreducible as it has no roots in $\mathbb{Z}_5$. Thus, f is irreducible over $\mathbb{Q}$.