MAT 312/AMS 351: Applied Algebra
Solutions to Problem Set 10 (13pts)

Problem F (6pts)

Factor the following polynomials into irreducible ones (and show that the factors are indeed irreducible).
(a) x^3+x+1 *in* $\mathbb{Z}_2[x]$ *(b)* x^2-3x-3 *in* $\mathbb{Z}_5[x]$ *(c)* x^2+1 *in* $\mathbb{Z}_7[x]$

(a) Since x^3+x+1 does not vanish at $x=0,1\in\mathbb{Z}_2$, this cubic polynomial has no linear factor and is thus irreducible in $\mathbb{Z}_2[x]$.

(b) This polynomial vanishes at $x=1,2$. Thus, it splits as $(x-1)(x-2)$ in $\mathbb{Z}_5[x]$.

(c) Since x^2+1 does not vanish at $x=0,\pm1,\pm2,\pm3\in\mathbb{Z}_7$, this quadratic polynomial has no linear factor and is thus irreducible in $\mathbb{Z}_7[x]$.

Note. The *reason* for the irreducibility of x^2+1 in $\mathbb{Z}_7[x]$ is *not* that the only roots of x^2+1 in $\mathbb{C}$ are $\pm\mathfrak{i}$ and these are not real numbers. Since x^2+1 has at most two roots over any field and its only roots in $\mathbb{C}$ are $\pm\mathfrak{i}$, x^2+1 has no other roots in any ring *contained* in $\mathbb{C}$. In particular, x^2+1 has no roots in any ring R *contained* in $\mathbb{R}$ (such as $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}$) and is thus irreducible over any ring R *contained* in $\mathbb{R}$. However, $\mathbb{Z}_7$ is *not* contained in $\mathbb{R}$ (or $\mathbb{C}$). Thus, x^2+1 not having roots in $\mathbb{R}$ says nothing about it not having roots in $\mathbb{Z}_7$. For example, x^2+1 *does* have roots in $\mathbb{Z}_5$, $x=\pm2$, and factors as $(x+2)(x-2)$ in $\mathbb{Z}_5[x]$.

Problem H (3pts)

Let F be a field (possibly finite). Show that there are infinitely many irreducible monic polynomials in $F[x]$ (monic means that the coefficient of the highest power of x is 1).
Hint: How was a similar result proved for $\mathbb{Z}$?

The proof is almost identical to the proof of Corollary 1.3.4. Suppose $p_1,\ldots,p_n$ are all the irreducible monic polynomials in $F[x]$. Let

$$a = p_1p_2\ldots p_n+\mathbf{1} \in F[x].$$

Since the remainder of the division of a by p_i is the constant polynomial $\mathbf{1}$, none of the p_i's divides a. Since x is a monic irreducible polynomial, the degree of a is at least 1. By the "Unique" Factorization Theorem for $F[x]$, some irreducible polynomial $p\in F[x]$ divides a. Since F is field, p can be taken to be monic (just divide the initial p by the inverse of the coefficient of the highest power of x). Since none of the p_i's divides a, $p\neq p_i$ for all $i=1,2,\ldots,n$. Since $p\in F[x]$ is an irreducible monic polynomial, this contradicts the assumption that $p_1,\ldots,p_n$ are all the irreducible monic polynomials in $F[x]$. Thus, there are infinitely many irreducible monic polynomials in $F[x]$.

Problem G (4pts)

Find a greatest common divisor of x^3-6x^2+x+4 *and* x^5-6x+1 *in* $\mathbb{R}[x]$.

$$\begin{aligned}
x^5-6x+1 &= x^2(x^3-6x^2+x+4) + (6x^4-x^3-4x^2-6x+1)\\
&= (x^2+6x)(x^3-6x^2+x+4)+(35x^3-10x^2-30x+1)\\
&= (x^2+6x+35)(x^3-6x^2+x+4)+(200x^2-65x-139)\\
x^3-6x^2+x+4 &= \frac{x}{200}\big(200x^2-65x-139\big) - \frac{1}{200}\big(1135x^2-339x-800\big)\\
&= \frac{1}{200}\big(x-\frac{227}{40}\big)\big(200x^2-65x-139\big) - \frac{1}{8000}(1195x-447)\\
200x^2-65x-141 &= \frac{40x}{239}(1195x-447) + \frac{1}{239}(2345x-33699)\\
&= \frac{1}{239}\big(40x+\frac{469}{239}\big)(1195x-447) - \frac{7844418}{239^2}
\end{aligned}$$

Thus, a gcd of x^3-6x^2+x+4 and x^5-6x+1 in $\mathbb{R}[x]$ is the constant polynomial $7844418/239^2$ or equivalently **1**, i.e. these two polynomials have no common polynomial factor in $\mathbb{R}[x]$.

Alternatively, $x=1$ is a root of x^3-6x^2+x+4 and so $(x-1)$ divides x^3-6x^2+x+4 even in $\mathbb{Z}[x]$. Using polynomial division, we obtain

$$x^3-6x^2+x+4 = (x-1)(x^2-5x-4).$$

Since x is not a root of x^5-6x+1, $(x-1)$ does not divide x^5-6x+1 and

$$\gcd\big(x^3-6x^2+x+4, x^5-6x+1\big) = \gcd\big(x^2-5x-4, x^5-6x+1\big).$$

The polynomial x^2-5x-4 has no rational roots (any such root would be an integer dividing 4, i.e. $\pm 1, 2$, none of which is a root). Thus, x^2-5x-4 is therefore irreducible in $\mathbb{Q}[x]$. Since x^2-5x-4 and x^5-6x+1 lie in $\mathbb{Q}[x]$, their gcd in $\mathbb{Q}[x]$ is also their gcd in $\mathbb{R}[x]$. Since x^2-5x-4 is irreducible in $\mathbb{Q}[x]$, it is thus enough to check whether x^2-5x-4 divides x^5-6x+1:

$$\begin{aligned}
x^5-6x+1 &= x^3(x^2-5x-4)+(5x^4+4x^3-6x+1)\\
&= (x^3+5x^2)(x^2-5x-4)+(29x^3+20x^2-6x+1)\\
&= (x^3+5x^2+29x)(x^2-5x-4)+(165x^2+110x+1)\\
&= (x^3+5x^2+29x+165)(x^2-5x-4)+(935x+661).
\end{aligned}$$

Since x^2-5x-4 is irreducible and does not divide x^5-6x+1, it follows that a gcd of x^2-5x-4 and x^5-6x+1 is the constant polynomial **1** (or any nonzero constant multiple of it).

Note: the above computations of remainders are essentially long divisions of polynomials written in a more compact form.