1. (a) Find the greatest common divisor $(105, 133)$ of 105 and 133.

   Answer: We can use the Euclidean algorithm to find $(105, 133)$ as follows:

$$\begin{aligned} 133 &= 105 \cdot 1 + 28 & 0 \le 28 < 105 \\ 105 &= 28 \cdot 3 + 21 & 0 \le 21 < 28 \\ 28 &= 21 \cdot 1 + 7 & 0 \le 7 < 21 \\ 21 &= 7 \cdot 3 + 0 \end{aligned}$$

   Therefore $(105, 133) = 7$ by the Euclidean algorithm.

   (b) Find a pair of integers $u, v \in \mathbb{Z}$ for which $(105, 133) = 105u + 133v$.

   Answer: Using part (a), we can use backward substitution as follows:

$$7 = 28 - 1(105 - 3 \cdot 28) = 4 \cdot 28 - 105$$
$$7 = 4 \cdot (133 - 1 \cdot 105) - 105 = 4 \cdot 133 - 5 \cdot 105$$

   Therefore $u = -5$ and $v = 4$.

2. Compute the following remainders:

   (a) The remainder when 25^{125} is divided by 13 in $\mathbb{Z}$.

   Answer: Since $25 \equiv -1 \pmod{13}$, we have

$$25^{125} \equiv (-1)^{125} \equiv -1 \equiv 12 \pmod{13}$$

   by repeatedly applying Theorem 2.2. Therefore the remainder when 25^{125} is divided by 13 is 12.

   (b) The remainder when 642^{7531} is divided by 5 in $\mathbb{Z}$.

   Answer: By Fermat's Little Theorem (Homework 2 Q4), since $5 \nmid 642$, we have $642^{5-1} \equiv 1 \pmod{5}$. Then

$$642^{7531} \equiv 642^{4^{1882}} \cdot 4^3 \equiv 4^3 = 64 \pmod{5}.$$

   Therefore the remainder when 642^{7531} is divided by 5 is 64.

   (c) The remainder when $f(x) = x^{100} - 2x^{50} + 3x^{15} - 4x^2 + 5$ is divided by $g(x) = x^2 - x + 1$ in $\mathbb{Q}[x]$.

   Answer: Since $x^3 \equiv -1 \pmod{x^2 - x + 1}$, we have

$$\begin{aligned} f(x) &= x^{100} - 2x^{50} + 3x^{15} - 4x^2 + 5 \\ &= x \cdot x^{3^{33}} - 2x^2 \cdot x^{3^{16}} + 3x \cdot x^{3^5} - 4x^2 + 5 \\ &\equiv x \cdot (-1)^{33} - 2x^2 \cdot (-1)^{16} + 3x \cdot (-1)^5 - 4x^2 + 5 \\ &\equiv -x - 2x^2 - 3x - 4x^2 + 5 \\ &= -6x^2 - 4x + 5 \\ &\equiv -10x + 11 \pmod{x^2 - x + 1}. \end{aligned}$$

   Therefore the remainder when $f(x) = x^{100} - 2x^{50} + 3x^{15} - 4x^2 + 5$ is divided by $g(x) = x^2 - x + 1$

is $-11x+11$.

3. Let $R = \{0_R, a, b, c\}$ be a ring with 4 elements and additive identity 0_R. The addition and multiplication tables for R are given below, with some entries missing. Fill in the missing entries. All of the entries in the tables should be one of the symbols '0_R', 'a', 'b' or 'c'. Do not give unsimplified answers like '$b+c$'.

   Answer:

$+$	0_R	a	b	c
0_R	0_R	a	b	c
a	a	0_R	c	b
b	b	c	0_R	a
c	c	b	a	0_R

$\cdot$	0_R	a	b	c
0_R	0_R	0_R	0_R	0_R
a	0_R	0_R	a	a
b	0_R	0_R	b	b
c	0_R	0_R	c	c

4. In each part, determine whether or not the first ring is isomorphic to the second. Prove that your answer is correct:

   (a) $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ and $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2)$.

   Answer: Let $f : (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \to (\mathbb{Z}/2\mathbb{Z})[x]/(x^2)$ be defined as $f((a,b)) = [ax+b]$. Note that we can also have $f^{-1}([ax+b]) = (a,b)$, so f is bijective. Now we have

$$\begin{aligned} f((a,b)+(c,d)) &= f((a+c,b+d)) \\ &= [(a+c)x+(b+d)] \\ &= [ax+b]+[cx+d] \\ &= f((a,b))+f((c,d)) \end{aligned}$$

   and

$$\begin{aligned} f((a,b)(c,d)) &= f((ac,bd)) \\ &= [(ac)x+(bd)] \\ &\neq [ax+b][cx+d] \\ &= f((a,b))f((c,d)) \end{aligned}$$

   Therefore $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is not isomorphic to $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2)$.

   (b) $\mathbb{Q}[x]/(x^2+1)$ and $\mathbb{Q}[x]/(x^2+4)$.

   Answer: Let $f : \mathbb{Q}[x]/(x^2+1) \to \mathbb{Q}[x]/(x^2+4)$ be defined as $f([ax+b]) = [ax+b] \in \mathbb{Q}[x]/(x^2+4)$. Note that we can also have $f^{-1}([ax+b]) = [ax+b] \in \mathbb{Q}[x]/(x^2+1)$, so f is bijective. Now we have

$$\begin{aligned} f([ax+b]+[cx+d]) &= f([(a+c)x+(b+d)]) \\ &= [(a+c)x+(b+d)] \\ &= [ax+b]+[cx+d] \\ &= f([ax+b])+([cx+d]) \end{aligned}$$

and

$$\begin{aligned} f([ax+b][cx+d]) &= f([(ad+bc)x+bd]) \\ &= [(ad+bc)x+bd] \\ &= [ax+b][cx+d] \\ &= f([ax+b])([cx+d]) \end{aligned}$$

Therefore $\mathbb{Q}[x]/(x^2+1)$ is isomorphic to $\mathbb{Q}[x]/(x^2+4)$.

5. Which of the following polynomials are irreducible in the given polynomial rings? Prove that your answer is correct.

(a) $f(x) = x^{10} + \pi x^8 + 3x^3 + 2x^2 + \sqrt{110}$ in $\mathbb{R}[x]$.
Answer: $f(x)$ is not irreducible in $\mathbb{R}[x]$ by Theorem 4.30.

(b) $f(x) = x^5 + x^4 + 1$ in $(\mathbb{Z}/2\mathbb{Z})[x]$.
Answer: Neither 0 nor 1 is a root of $f(x)$, so $f(x)$ can only factor into the product of a quadratic polynomial and a cubic polynomial. Therefore one of $x^2, x^2+1, x^2+x, x^2+x+1$ must be a factor.

$g(x)$	is factor?	$f(x)/g(x)$
x^2	no	-
x^2+1	no	-
x^2+x	no	-
x^2+x+1	yes	x^3+x+1

Therefore $x^5 + x^4 + 1 = (x^2+x+1)(x^3+x+1)$ so $f(x)$ is not irreducible.

(c) $f(x) = x^4 + 3x^3 + 5x + 1$ in $\mathbb{Q}[x]$.
Answer: $f(x)$ is irreducible; by contradiction: suppose $f(x)$ is reducible, then it can be factored as the product of two nonconstant polynomials in $\mathbb{Q}[x]$. If either of those factors has degree 1, then $f(x)$ has a root in $\mathbb{Q}$. But the Rational Root Test shows that $f(x)$ has no roots in $\mathbb{Q}$ (the only possibilities are ± 1 and neither is a root). Thus if $f(x)$ is reducible, the only possible factorization is as a product of two quadratics, by Theorem 4.2. In this case Theorem 4.23 shows that there is such a factorization in $\mathbb{Z}[x]$. Furthermore, there is a factorization as a product of monic quadratics in $\mathbb{Z}[x]$, i.e.

$$(x^2+ax+b)(x^2+cx+d) = x^4 + 3x^3 + 5x + 1,$$

with $a, b, c, d \in \mathbb{Z}$. Multiplying out the left-hand side, we have

$$x^4 + (a+c)x^3 + (ac+b+d)x^2 + (ad+bc)x + bd = x^4 + 3x^3 + 0x^2 + 5x + 1.$$

Equal polynomials have equal coefficients; hence,

$$a + c = 3, ac + b + d = 0, ad + bc = 5, bd = 1.$$

Since $bd = 1 \in \mathbb{Z}$ implies that $b = d = 1$ or $b = d = -1$, using the third equation we have two possibilities: $ad + bc = 5 \implies a + c = \pm 5$. But this contradicts with the first equation, so a factorization of $f(x)$ as a product of quadratics in $\mathbb{Z}[x]$, and, hence in $\mathbb{Q}[x]$, is impossible. Therefore, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

6. Give an example of a field of order 125 (that is, a finite field containing *exactly* 125 elements). Note that $125 = 5^3$.

   Answer: $(\mathbb{Z}/5\mathbb{Z}[x])/(x^3 + x^2 + 1)$ contains exactly 125 elements. Take $x^3 + x^2 + 1$ in $\mathbb{Z}/5\mathbb{Z}[x]$, it is irreducible since the only possible roots are ± 1 and neither is a root. So the possible remainders on division by $x^3 + x^2 + 1$ in $\mathbb{Z}/5\mathbb{Z}[x]$ are the polynomials of the form $a_0 + a_1x + a_2^2$, with $a_k \in \mathbb{Z}/5\mathbb{Z}$. There are 5 possibilities for each of the 3 coefficients, so there are 5^3 different polynomials of this form. Consequently, by Corollary 5.5, there are exactly $5^3 = 125$ distinct congruence classes in $(\mathbb{Z}/5\mathbb{Z}[x])/(x^3 + x^2 + 1)$.

7. Let $I = \left\{ a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x] \middle| 5|a_0, 5|a_1 \right\} \subseteq \mathbb{Z}[x]$ be the set of all polynomials with integer coefficients with constant *and* linear terms divisible by 5.

   (a) Prove that I is an ideal in $\mathbb{Z}[x]$.

   Answer: Take $p(x) = a_0 + a_1x + \cdots + a_nx^n \in I$ and $q(x) = b_0 + b_1x + \cdots + b_nx^n \in I$ where $5|a_0, 5|a_1, 5|b_0, 5|b_1$. Then by definition of divisibility there must exist m_0, m_1 and n_0, n_1 such that $a_0 = 5m_0, a_1 = 5m_1, b_0 = 5n_0, b_1 = 5n_1$. Then

$$\begin{aligned} p(x) - q(x) &= a_0 + a_1x + \cdots + a_nx^n - b_0 - b_1x - \cdots - b_nx^n \\ &= 5m_0 + 5m_1x + \cdots + a_nx^n - 5n_0 - 5n_1x - \cdots - b_nx^n \\ &= 5(m_0 - n_0) + 5(m_1 - n_1)x + \cdots + (a_n - b_n)x^n. \end{aligned}$$

   Since $5(m_0 - n_0)$ and $5(m_1 - n_1)$ are clearly divisible by 5, $p(x) - q(x) \in I$. Now take any $r(x) = r_0 + r_1x + \cdots + r_nx^n \in \mathbb{Z}[x]$, we have

$$\begin{aligned} p(x)r(x) &= a_0r_0 + (a_0r_1 + a_1r_0)x + \cdots \\ &= 5m_0r_0 + (5m_0r_1 + 5m_1r_0)x + \cdots \\ &= 5m_0r_0 + 5(m_0r_1 + m_1r_0)x + \cdots \end{aligned}$$

and

$$\begin{aligned} r(x)p(x) &= r_0a_0 + (r_1a_0 + r_0a_1)x + \cdots \\ &= 5r_0m_0 + (5r_1m_0 + 5r_0m_1)x + \cdots \\ &= 5m_0r_0 + 5(m_0r_1 + m_1r_0)x + \cdots . \end{aligned}$$

Since $5m_0r_0$ and $5(m_0r_1 + m_1r_0)$ are divisible by 5, we have $p(x)r(x) \in I$ and $r(x)p(x) \in I$. Therefore I is an ideal in $\mathbb{Z}[x]$ by Theorem 6.1.

(b) Find two polynomials $f(x), g(x) \in \mathbb{Z}$ which generate I (i.e. $I = (f(x), g(x))$). Prove that they generate I.

Answer: Let $f(x) = 5$ and $g(x) = x^2$, we will show that $I = (f(x), g(x))$. Since $5|a_0$ and $5|a_1$, we can take $m_0, m_1 \in \mathbb{Z}$ such that $a_0 = 5m_0$ and $a_1 = 5m_1$. Then we have

$$\begin{aligned} a_0 + a_1x + \cdots + a_nx^n &= 5(m_0 + m_1x) + x^2(a_2 + a_3x + \cdots + a_nx^{n-2}) \\ &= f(x)(m_0 + m_1x) + g(x)(a_2 + a_3x + \cdots + a_nx^{n-2}) \in I \end{aligned}$$

by Theorem 6.1 since $m_0 + m_1x$ and $a_2 + a_3x + \cdots + a_nx^{n-2}$ are both in $\mathbb{Z}[x]$, so $I = (f(x), g(x))$.

(c) Prove that I is not a principal ideal in $\mathbb{Z}[x]$ (i.e. I cannot be written in the form $I = (h(x))$ for any polynomial $h(x) \in \mathbb{Z}[x]$).

Answer: By contradiction. Suppose that there is an $h(x)$ such that $I = (h(x))$, then $h(x)$ must be a constant or else it won't be able to generate the constant term in polynomials in I with a nonzero constant coefficient, i.e. we must have $h(x) = h_0$ for some $h_0 \in \mathbb{Z}$. Since $h(x) \in I$, we must also have $5|h_0$ as h_0 is a constant coefficient. However now we cannot generate polynomials where the x^2 or higher terms have coefficients that are not divisible by 5 (e.g. we cannot generate x^2 which should be in I). Therefore there is no such $h(x)$ and I is not a principal ideal in $\mathbb{Z}$.

8. Let R and S be rings. If $I \subseteq R$ and $J \subseteq S$ are ideals in R and S, respectively, let

$$I \times J = \{(x, y) \mid x \in I, y \in J\} \subseteq R \times S$$

(a) If I and J are any ideals in R and S, prove that $I \times J$ is an ideal in $R \times S$ and

$$(R \times S)/(I \times J) \cong (R/I) \times (S/J).$$

Answer: Take $(x_1, y_1), (x_2, y_2) \in I \times J$, then

$$(x_1, y_1) - (x_2, y_2) = (x_1 - x_2, y_1 - y_2) \in I \times J$$

since $x_1 - x_2 \in I$ and $y_1 - y_2 \in J$ by Theorem 6.1 as $x_1, x_2 \in I$ and $y_1, y_2 \in J$. Now take $(r, s) \in R \times S$, we have

$$(r, s)(x, y) = (rx, sy)$$

and

$$(x, y)(r, s) = (xr, ys).$$

Note that since $x \in I$, by Theorem 6.1 rx and xr are also in I. Similarly, since $y \in J$, sy and ys are also in J. Therefore both (rx, sy) and (xr, ys) are in $I \times J$, so $I \times J$ is an ideal by Theorem 6.1.

(b) Now assume that R and S have (multiplicative) identities 1_R and 1_S. If $K \subseteq R \times S$ is any ideal of $R \times S$, prove that there are ideals $I \subseteq R$ and $J \subseteq S$ for which $K = I \times J$.

Answer: Take $I = \{r \in R \mid (r, 0_R) \in K\}$ and $J = \{s \in S \mid (0_R, s) \in K\}$, clearly we have $I \subseteq R$ and $J \subseteq S$ by definition of $K \subseteq R \times S$, as well as $I \times J \subseteq K$. Now take $r \in I$ and $s \in J$; since R and S have multiplicative identities 1_R and 1_S, we have

$$r(1_R, 0_S) + s(0_R, 1_S) = (r, 0_S) + (0_R, s) = (r, s)$$

for every $(r, s) \in K$, so $K \subseteq I \times J$. Therefore $K = I \times J$.

Now we will show that I and J are ideals; take $(r_1, 0_S), (r_2, 0_S) \in K$, by Theorem 6.1 we have

$$(r_1, 0_R) - (r_2, 0_R) = (r_1 - r_2, 0_R) \in K,$$

so $r_1 - r_2 \in I$. Similarly for $(0_R, s_1), (0_R, s_2) \in K$ we have $s_1 - s_2 \in J$. In addition, by Theorem 6.1 we also have

$$(r, s)(r_1, 0_S) = (rr_1, 0_S) \in K$$

and

$$(r_1, 0_S)(r, s) = (r_1 r, 0_S) \in K$$

for $(r, s) \in R \times S$, so $rr_1, r_1 r \in I$ and similarly $ss_1, s_1 s \in J$. Therefore I, J are both ideals by Theorem 6.1.

I assert, on my honor, that I have not received assistance of any kind from any other person, or given assistance to any other person, while working on the midterm.

Signature: