D will denote a unique factorization domain throughout this problem set. For \( n \in \mathbb{N}, n \geq 2, \mathbb{Z}_n \) will denote the ring of integers modulo \( n \). We will denote the elements of \( \mathbb{Z}_n \) as \( 0, 1, \ldots, n - 1 \) instead of the more cumbersome \( \{0\}_n, \{1\}_n, \ldots, \{n - 1\}_n \).

1. Let \( f(x), g(x) \in D[x] \). Show that if \( f(x) \mid g(x) \) in \( D[x] \) and \( g(x) \) is primitive, then \( f(x) \) is primitive.

Solution. Let \( f(x) \) be a nonconstant divisor of the primitive polynomial \( g(x) \) in \( D[x] \). Suppose that \( g(x) = f(x)q(x) \) for some \( q(x) \in D[x] \). Because \( D \) is a UFD, we know that \( D[x] \) is a UFD also by Theorem V in the lectures. Factor \( g(x) \) into irreducibles by factoring each of \( f(x) \) and \( q(x) \) into irreducibles, and then taking the product of these factorizations. Each nonconstant factor appearing is an irreducible in \( D[x] \), and hence is a primitive polynomial. Because the product of primitive polynomials is primitive by Lemma Q in the lectures, we see that the content of \( f(x)q(x) \) is the product of the content of \( f(x) \) and the content of \( q(x) \), and must be the same (up to a unit factor) as the content of \( g(x) \) by uniqueness in Lemma P in the lectures. But up to a unit factor, \( g(x) \) has content 1 because it is primitive. Thus \( f(x) \) and \( q(x) \) both have content 1 up to a unit factor. Hence \( f(x) \) is a product of primitive polynomials, so it is primitive by Lemma Q.

2. Prove that the following polynomials are irreducible over \( \mathbb{Q}[x] \),

\[
\begin{align*}
e_1(x) &= x^4 - 22x^2 + 1, & e_2(x) &= x^4 + x^3 + x^2 + 6x + 1, \\
e_3(x) &= 16x^5 - 125x^4 + 50x^3 - 100x^2 + 75x + 25, & e_4(x) &= x^6 + 539x^5 - 511x + 847.
\end{align*}
\]

Solution. If \( e_1(x) \) is reducible in \( \mathbb{Z}[x] \), then it factors in \( \mathbb{Z}[x] \), and must therefore either have a linear factor in \( \mathbb{Z}[x] \) or factor into two quadratics in \( \mathbb{Z}[x] \). The only possibilities for a linear factor are \( x \pm 1 \), and clearly neither 1 nor \(-1\) is a zero of the polynomial, so a linear factor is impossible. Suppose

\[
x^4 - 22x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d).
\]

Equating coefficients of \( x^3, x^2, x^1, x^0 \), we get respectively

\[
0 = a + c, \quad -22 = ac + b + d, \quad 0 = bc + ad, \quad 1 = bd.
\]

From the last equation, either \( b = d = 1 \) or \( b = d = -1 \). Suppose \( b = d = 1 \). Then

\[
-22 = ac + 1 + 1
\]

and so \( ac = -24 \). Because \( a + c = 0 \), we have \( a = -c \), so \(-c^2 = -24\) which is impossible for an integer \( c \). Similarly, if \( b = d = -1 \), we deduce that \(-c^2 = -20\), which is also impossible. Hence \( e_1(x) \) has no quadratic factors either and is thus irreducible over \( \mathbb{Z}[x] \). Hence by Gauss Lemma, it is also irreducible over \( \mathbb{Q}[x] \).
• Let $x = y + 1$ and let $f(y) = e_2(y + 1)$. Then

$$e_2(x) = (x^4 + x^3 + x^2 + x + 1) + 5x$$

$$= \frac{x^5 - 1}{x - 1} + 5x,$$

$$f(y) = \frac{(y + 1)^5 - 1}{y} + 5y + 5$$

$$= y^4 + 5y^3 + 10y^2 + 15y + 10.$$

The coefficients of $y^3, y^2, y, 1$ of $f(y)$ are integers divisible by $5 \in \mathbb{P}$ and the constant term is $10$, which is not divisible by $5^2$. So $f(y)$ and thus $e_2(x)$ is irreducible over $\mathbb{Q}$ by the Eisenstein Criterion and Gauss Lemma.

• Suppose $e_3(x)$ is reducible over $\mathbb{Z}[x]$. Then there exists $f(x), g(x) \in \mathbb{Z}[x]$ such that $e_3(x) = f(x)g(x)$. Let

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad g(x) = b_0 + b_1 x + \cdots + b_m x^m.$$

Then we can see that $a_0 b_0 = 25$, which can only happen in two ways, either $a_0 = 25, b_0 = 1$ or $a_0 = 5, b_0 = 5$.

Case I: $a_0 = 25, b_0 = 1$. Then

$$75 = a_0b_1 + a_1b_0 = 25b_1 + a_1,$$

so $25$ divides $a_1$. Hence

$$-100 = a_2b_0 + a_1b_1 + a_0b_2 = a_2 + a_1b_1 + 25b_2,$$

so $25$ divides $a_2$. Continuing in this way, we find that $25$ also divides $a_3$ and $a_4$. However $16$, the leading coefficient of $e_3(x)$, is given by

$$16 = a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 \quad (2.1)$$

(since $m < 5, n < 5$), and $25$ does not divide $16$. Therefore Case I is impossible.

Case II: $a_0 = 5, b_0 = 5$. Then

$$75 = 5a_1 + 5b_1$$

and so if either $a_1$ or $b_1$ is divisible by $5$ then both are divisible by $5$. But by

$$-100 = 5a_2 + a_1b_1 + 5b_2,$$

we see that $5$ divides $a_1b_1$. Hence $5$ divides both $a_1$ and $b_1$. Similarly, we have

$$50 = 5a_3 + a_2b_1 + a_1b_2 + 5b_3$$

and

$$-125 = 5a_4 + a_3b_1 + a_2b_2 + a_1b_3 + 5a_4.$$

Exactly the same reasoning as before shows that $5$ divides $a_2$ and $b_2$, again a contradiction with (2.1), since $5$ does not divide $16$.

• Note that $539 = 7^2 \cdot 11, 511 = 7 \cdot 23$, and $847 = 7 \cdot 11^2$. Thus all coefficients of $e_4(x)$ except the leading one are divisible by $7$, but the constant term is not divisible by $7^2$. Since $7$ is a prime, $e_4(x)$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein Criterion and thus in $\mathbb{Q}[x]$ by Gauss Lemma.

3. Consider the following polynomials in $\mathbb{Z}[x]$,

$$f_1(x) = x^2 + 8x - 2, \quad f_2(x) = 2x^2 + 12x + 24,$$

$$f_3(x) = x^3 + 3x^2 - 8, \quad f_4(x) = x^4 + 1.$$

Determine if $f_i(x)$ is irreducible in $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x]$, and $\mathbb{C}[x]$ or not.

SOLUTION.
• $f_1(x)$ satisfies the Eisenstein Criterion for irreducibility over $\mathbb{Z}$ with $p = 2$. So by Gauss Lemma, it is also irreducible over $\mathbb{Q}$. It is not irreducible over $\mathbb{R}$ because the quadratic formula shows that $f_1(x)$ has the real zeros $(-8 \pm \sqrt{72})/2$. Because of this, it is not irreducible over $\mathbb{C}$ also.
• $f_2(x) = 2(x^2 + 6x + 12)$ is a factorization into a product of two factors in $\mathbb{Z}[x]$, neither of which are units. Hence $f_2(x)$ is reducible over $\mathbb{Z}$. The polynomial $x^2 + 6x + 12$ is irreducible over $\mathbb{Z}$ by the Eisenstein Criterion with $p = 3$ and thus over $\mathbb{Q}$ by Gauss Lemma. Since 2 is a unit in $\mathbb{Q}$, $f_2(x)$ is irreducible in $\mathbb{Q}[x]$. It is also irreducible over $\mathbb{R}$ because the quadratic formula shows that its zeros are $(-6 \pm \sqrt{-12})/2$, which are not in $\mathbb{R}$. It is not irreducible over $\mathbb{C}$, because its zeros lie in $\mathbb{C}$.
• If $f_3(x)$ is reducible over $\mathbb{Q}$, then by Gauss Lemma, it factors in $\mathbb{Z}[x]$, and must therefore have a linear factor of the form $x - a$ in $\mathbb{Z}[x]$. Then $a \in \mathbb{Z}$ must be a zero of the polynomial and must divide $-8$, so the possibilities are $a = \pm 1, \pm 2, \pm 4, \pm 8$. Computing the polynomial at these eight values, we find none of them is a zero of the polynomial, which is therefore irreducible over $\mathbb{Q}$. Since $f_3$ defines a continuous function on $\mathbb{R}$, $\lim_{x \to -\infty} f_3(x) = -\infty$, and $\lim_{x \to +\infty} f_3(x) = +\infty$, the Intermediate Value Theorem implies that $f_3(x)$ must have at least one zero in $\mathbb{R}$. So $f_3(x)$ is not irreducible over $\mathbb{R}$ nor $\mathbb{C}$.
• Note that $f_4(x)$ factors as follows
  $$x^4 + 1 = (x^2 + 1)^2 - 2x^2 = (x^2 - \sqrt{2} + 1)(x^2 + \sqrt{2} + 1)$$
and so it is reducible over $\mathbb{R}$ and thus over $\mathbb{C}$ as well.

4. Consider the following polynomials in $\mathbb{Z}_5[x]$,

$$g_1(x) = x^3 + x + 1, \quad g_2(x) = x^3 + 2x + 3, \quad g_3(x) = 2x^3 + x^2 + 2x + 1,$$
$$g_4(x) = x^4 + 4, \quad g_5(x) = x^4 + x^3 + x + 3.$$

Determine if $g_i(x)$ is irreducible in $\mathbb{Z}_5[x]$ or not. If it is reducible, find a factorization into a product of irreducibles (you will need to prove that your factors are indeed irreducible).

**Solution.**

- We will let the representatives of $\mathbb{Z}_5$ be $0, \pm 1, \pm 2$ (you can of course use $0, 1, 2, 3, 4$ but that’s making life harder for yourself). Since
  $$g_1(0) = 1, \quad g_1(1) = -2, \quad g_1(-1) = -1, \quad g_1(2) = 1, \quad g_1(-2) = -1,$$
  $g_1(x)$ has no zeros in $\mathbb{Z}_5$. Because $g_1(x)$ is of degree 3, if it is reducible, it must have at least one zero. Hence $g_1(x)$ is irreducible over $\mathbb{Z}_5$.
- By inspection, $-1$ is a zero of $g_2(x)$ in $\mathbb{Z}_5[x]$, so the polynomial is not irreducible. We divide by $x + 1$, and use the division algorithm to get
  $$x^3 + 2x + 3 = (x + 1)(x^2 - x + 3).$$
  By inspection, $-1$ and 2 are zeros of $x^2 - x + 3$, so the factorization is
  $$x^3 + 2x + 3 = (x + 1)(x + 1)(x - 2).$$
- Since
  $$g_3(0) = 2, \quad g_3(1) = 2, \quad g_3(-1) = -1, \quad g_3(2) = 1, \quad g_3(-2) = 1,$$
  $g_3(x)$ has no zeros in $\mathbb{Z}_5$. Because $g_3(x)$ is of degree 3, if it is reducible, it must have at least one zero. Hence $g_3(x)$ is irreducible over $\mathbb{Z}_5$.
- In $\mathbb{Z}_5$, we have
  $$g_4(x) = x^4 + 4 = x^4 - 1 = (x^2 + 1)(x^2 - 1).$$
  Replacing 1 by $-4$ again, we continue to see that
  $$(x^2 - 4)(x^2 - 1) = (x - 2)(x + 2)(x - 1)(x + 1).$$
5. Consider the following polynomials in \( \mathbb{Z}_5 \):

\[
g_5(x) = (x^2 + ax + 1)(x^2 + bx + 3),
\]

then equating the coefficients of \( x \), we get

\[
a + b = 1, \quad 4 + ab = 0, \quad 3a + b = 1
\]

and it is straightforward to check that this system of equations has no solutions in \( \mathbb{Z}_5 \). If

\[
g_5(x) = (x^2 + ax + 2)(x^2 + bx + 4),
\]

then equating the coefficients of \( x \), we get

\[
a + b = 1, \quad 1 + ab = 0, \quad 4a + 2b = 1
\]

and it is again straightforward to check that this system of equations has no solutions in \( \mathbb{Z}_5 \). Hence \( g_5(x) \) has no quadratic factors either. Hence \( g_5(x) \) is irreducible in \( \mathbb{Z}_5[x] \).

5. Consider the following polynomials in \( \mathbb{Q}[x, y] \),

\[
h_1(x, y) = x^3 - y^3, \quad h_2(x) = x^2 + y^2 - 1.
\]

Determine if \( h_1(x, y) \) is irreducible in \( \mathbb{Q}[x, y] \) or not. If it is reducible, find a factorization into a product of irreducibles (you will need to prove that your factors are indeed irreducible). Hence or otherwise, determine if the following quotient rings are integral domains

\[
\mathbb{Q}[x, y]/(x^3 - y^3), \quad \mathbb{Q}[x, y]/(x^2 + y^2 - 1).
\]

**Solution.**

- We have

\[
h_1(x, y) = x^3 - y^3 = (x - y)(x^2 + xy + y^2).
\]

Of course \( x - y \) is irreducible. We claim that \( x^2 + xy + y^2 \) is irreducible in \( \mathbb{Q}[x, y] \). Suppose that \( x^2 + xy + y^2 \) factors into a product of two polynomials that are not units in \( \mathbb{Q}[x, y] \). Such a factorization would have to be of the form

\[
x^2 + xy + y^2 = (ax + by)(cx + dy)
\]

with \( a, b, c, d \) all nonzero elements of \( \mathbb{Q} \). Consider the evaluation homomorphism

\[
\varphi : (\mathbb{Q}[x])[y] \to \mathbb{Q}[x]
\]

such that \( \varphi(y) = 1 \). Applying \( \varphi \) to both sides of such a factorization would yield

\[
x^2 + x + 1 = (ax + b)(cx + d).
\]

But \( x^2 + x + 1 \) is irreducible in \( \mathbb{Q}[x] \) because its zeros are complex, so no such factorization exists. This shows that \( x^2 + xy + y^2 \) is irreducible in \( (\mathbb{Q}[x])[y] \) which isomorphic to \( \mathbb{Q}[x, y] \) under an isomorphism that identifies \( (y^2) + (y)x + x^2 \) (univariate polynomial in \( x \) with coefficients in \( \mathbb{Q}[y] \)) and \( x^2 + xy + y^2 \) (bivariate polynomial in \( x, y \)). Since \( h_1(x, y) \) is reducible, the principal ideal \( \langle h_1(x, y) \rangle \) is not prime and so \( \mathbb{Q}[x, y]/(x^3 - y^3) \) is not an integral domain.

- The degree-2 polynomial \( x^2 + y^2 - 1 \) does not factor into the product of two linear ones. This implies that it is irreducible and so the principal ideal \( \langle x^2 + y^2 - 1 \rangle \) is prime and thus \( \mathbb{Q}[x, y]/(x^2 + y^2 - 1) \) is an integral domain.
6. Let \( p \in \mathbb{P} \). Find the number of irreducible quadratic polynomials in \( \mathbb{Z}_p[x] \).

SOLUTION. Each reducible quadratic that is of the form \( x^2 + ax + b \) is a product \((x + c)(x + d)\) for \( c, d \in \mathbb{Z}_p \). There are \( \binom{p^2}{2} = p(p - 1)/2 \) such products (neglecting order of factors) where \( c \neq d \). There are \( p \) such products where \( c = d \). Thus there are \( p(p - 1)/2 + p = p^2/2 + p/2 = p(p + 1)/2 \) reducible quadratics with leading coefficient 1. Because the leading coefficient (upon multiplication) can be any one of \( p - 1 \) nonzero elements, there are \( (p - 1)p(p + 1)/2 \) reducible quadratics altogether. The total number of quadratic polynomials in \( \mathbb{Z}_p[x] \) is \( (p - 1)p^2 \). Thus the number of irreducible quadratics is

\[
(p - 1)p^2 - \frac{(p - 1)p(p + 1)}{2} = p(p - 1) \left[ \frac{p - (p + 1)}{2} \right] = \frac{p(p - 1)^2}{2}.
\]