Abstract algebra Exam 2

Question 1

Let $f(x) = x^4 + 5x - 6$ and $g(x) = x^3 + 3x^2 - 4$.

- Find, with proof, the greatest common denominator (f, g) of f and g and write (f, g) in the form $af + bg$, for suitable polynomials a and b.
- Hence write f and g as products of irreducible polynomials in the rings $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ and $\mathbb{Z}_7[x]$.

We implement the Euclidean algorithm. We have:

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

$$f - xg + 3g = -3x^3 + 9x - 6 + 3(x^3 + 3x^2 - 4) = -3x^3 + 9x - 6 + 3x^3 + 9x^2 - 12$$

$$= 9x^2 + 9x - 18 = 9(x^2 + x - 2) = 9h,$$

$$h = x^2 + x - 2 = (x + 2)(x - 1),$$

$$f = (x - 3)g + 9h.$$

Next we have:

$$g - xh = x^3 + 3x^2 - 4 - x(x^2 + x - 2) = x^3 + 3x^2 - 4 - x^3 - x^2 + 2x = 2x^2 + 2x - 4 = 2(x^2 + x - 2) = 2h,$$

$$g = (x + 2)h + 0.$$

The last non-zero remainder gives the monic g.c.d., (f, g) of f and g as the polynomial:

$$(f, g) = h = x^2 + x - 2 = (x + 2)(x - 1).$$

We have the expression of h in terms of f and g as:

$$h = \frac{1}{9}(f - (x - 3)g) = af + bh,$$

$$a = \frac{1}{9}, \quad b = \frac{3 - x}{9}.$$

Next we have:

$$g = (x+2)h = (x+2)^2(x-1).$$

This factors g as a product of irreducibles in all the four rings: $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ and $\mathbb{Z}_7[x]$.

For the polynomial f, we have:

$$f = (x-3)g+9h = (x-3)(x+2)h+9h = (x^2-x-6+9)h = (x^2-x+3)h = (x+2)(x-1)(x^2-x+3).$$

The discriminant D of the quadratic $x^2 - x + 3$ is:

$$D = (-1)^2 - 4(1)(3) = -11 < 0.$$

So the quadratic $x^2 - x + 3$ is reducible over the reals.
The complex roots of the quadratic $x^2 - x + 3$ are:

$$x = \frac{-(-1) \pm \sqrt{D}}{2} = \frac{1 \pm i\sqrt{11}}{2}.$$

Since these roots are neither rational nor real, the factorization of f as product of irreducibles in the rings $\mathbb{Q}[x]$ and $\mathbb{R}[x]$ is:

$$f = (x+2)(x-1)(x^2 - x + 3).$$

Next the factorization of f as product of irreducibles in the ring $\mathbb{C}[x]$ is:

$$f = \frac{1}{4}(x+2)(x-1)\left(2x - 1 - i\sqrt{11}\right)\left(2x - 1 + i\sqrt{11}\right).$$

Finally modulo 7, we have $-11 = -11 + 14 = 3$.
The squares modulo 7 are $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$ and $(\pm 3)^2 = 9 = 2$.
Since 3 is not a square modulo 7, the quadratic $x^2 - x + 3$ is irreducible modulo 7 and the factorization of f in the ring $\mathbb{Z}_7[x]$ as a product of irreducibles is:

$$f = (x+2)(x-1)(x^2 - x + 3).$$

Alternatively, if we put $q(x) = x^2 - x + 3 \mod 7$, we have:

$$q(0) = 3, \quad q(1) = 3, \quad q(2) = 5, \quad q(3) = 9 = 2, \quad q(4) = 15 = 1, \quad q(5) = 23 = 2, \quad q(6) = 33 = 5.$$

Since the quadratic polynomial $q(x)$ has no roots, it is irreducible.

Question 2

Find all solutions of the following polynomial equations and hence factor the polynomials completely; if a polynomial is irreducible, say why.

- $f(x) = x^2 + x + 3 = 0 \bmod 11$.

  We use the quadratic formula.
  The discriminant is $(1)^2 - 4(1)(3) = 1 - 12 = -11 = 0 \mod 11$.
  So the only root is $x = -\frac{1}{2} = \frac{10}{2} = 5$ and the quadratic factorizes as a product of irreducibles as:

  $$x^2 + x + 3 = (x - 5)^2$$

  Check: we have:

  $$(x-5)^2-(x^2+x+3) = x^2-10x+25-x^2-x-3 = -11x+22 = 11(2-x) = 0 \mod 11.$$

  Also we have $f(5) = 5^2 + 5 + 3 = 25 + 5 + 3 = 33 = 0 \mod 11$ and $x = 5$ is the only root of $f(x)$.

- $g(x) = x^3 + x + 4 = 0 \bmod 17$.

  We have:

  $$g(1) = 1+1+4 = 6 \neq 0, \quad g(2) = 8+2+4 = 14 \neq 0, \quad g(3) = 27+3+4 = 34 = 2(17) = 0.$$

  So $g(x)$ has a factor of $x - 3$.
  Factoring we get:

  $$g(x) = x^3+x+4 = (x-3)(x^2+ax+b) = x^3+ax^2+bx-3x^2-3ax-3b$$

  $$= x^3 + (a-3)x^2 + (b-3a)x - 3x^2 - 3b$$

  Comparing coefficients, we get $0 = a - 3$, $1 = b - 3a$ and $4 = -3b$.
  So $a = 3$, $b = 1 + 3a = 1 + 9 = 10$.
  Check $4 + 3b = 4 + 30 = 34 = 0 \mod 17$.
  So the factorization is:

  $$g(x) = (x - 3)(x^2 + 3x + 10).$$

The discriminant of the quadratic $x^2 + 3x + 10$ is:

$$3^2 - 4(1)(10) = 9 - 40 = -31 = 3 \mod 17.$$

The squares modulo 17 are:

$$0^2 = 0, \quad (\pm 1)^2 = 1, \quad (\pm 2)^2 = 4, \quad (\pm 3)^2 = 9, \quad (\pm 4)^2 = 16, \quad (\pm 5)^2 = 25 = 8,$$
$$(\pm 6)^2 = 36 = 2, \quad (\pm 7)^2 = 49 = 15, \quad (\pm 8)^2 = 64 = 13.$$

Since 3 is not a square modulo 17, the quadratic $x^2 + 3x + 10$ is irreducible and $g(x)$ factorizes as a product of irreducibles as:

$$x^3 + x + 4 = (x - 3)(x^2 + 3x + 10).$$

Also $x = 3$ is the only root of $g(x)$.

- $h(x) = x^4 - 8x^2 - 20 = 0$ in $\mathbb{R}[x]$ and in $\mathbb{C}[x]$.

  We have in $\mathbb{R}[x]$:

  $$h(x) = x^4 - 8x^2 - 20 = (x^2 - 10)(x^2 + 2) = \left(x - \sqrt{10}\right)\left(x + \sqrt{10}\right)(x^2 + 2).$$

  The quadratic $x^2 + 2$ has discriminant $0 - 4(1)(2) = -8 < 0$, so is irreducible over the reals.
  So $h(x)$ factors as a product of irreducibles in $\mathbb{R}[x]$ as:

  $$h(x) = \left(x - \sqrt{10}\right)\left(x + \sqrt{10}\right)(x^2 + 2).$$

  Also the only real roots are $x = \pm\sqrt{10}$.
  Finally over $\mathbb{C}[x]$ we have $x^2 + 2 = \left(x + i\sqrt{2}\right)\left(x - i\sqrt{2}\right)$, so we have that $h(x)$ factors as a product of irreducibles in $\mathbb{C}[x]$ as:

  $$h(x) = \left(x - \sqrt{10}\right)\left(x + \sqrt{10}\right)\left(x + i\sqrt{2}\right)\left(x - i\sqrt{2}\right).$$

  Also the complex roots are $x = \pm\sqrt{10}$ and $x = \pm i\sqrt{2}$.

Question 3

Let $p(x) = x^4 + 3x^2 + 4$.
Write, with proof, $p(x)$ as a product of irreducibles in:

- $\mathbb{Z}_7[x]$

  We have, working modulo 7:

  $p(x) = x^4+3x^2+4 = x^4-4x^2+4 = (x^2-2)^2 = (x^2-9)^2 = (x-3)^2(x+3)^2$.

  Check $p(\pm 3) = 81 + 27 + 4 = 112 = 7(16) = 0 \mod 7$.

- $\mathbb{Z}[x]$

  By the rational root test, the only possible rational roots are ± 1, ± 2 and ± 4.
  We have:

  $p(\pm 1) = 1+3+4 = 8 \neq 0, \quad p(\pm 2) = 16+12+4 = 32 \neq 0, \quad p(\pm 4) = 256+48+4 = 308 \neq 0.$

  So there are no rational roots.

  We look for factorization into a pair of integer quadratics:

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

  $$a + c = 0, \quad ac + b + d = 3, \quad ad + bc = 0, \quad bd = 4.$$

  So $c = -a$ and $a(d - b) = 0$, so $a = c = 0$ or $b = d$.
  If $a = c = 0$, then $b+d = 3$ and $bd = 4$, so $b(3-b) = 4$, so $b^2-3b+4 = 0$, which has discriminant $(-3)^2-4(1)(4) = 9-16 = -7$, so no real roots, so no integer roots.
  So $b = d$ and then we have $b^2 = 4$ and $2b - a^2 = 3$.
  So $a^2 = 2b - 3$ and $b^2 = 4$, so $b = \pm 2$ and $a^2 = \pm 4 - 3$.
  So $a = \pm 1$, $c = \mp 1$ and $b = d = 2$.
  So we have:

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

  The quadratics $x^2 \pm x + 2$ have discriminant $(\pm 1)^2 - 4(1)(2) = -7 < 0$, so each has no real or integer roots.
  So the required factorization into irreducibles in $\mathbb{Z}[x]$ is:

  $$p(x) = (x^2 + x + 2)(x^2 - x + 2).$$

- $\mathbb{R}[x]$

  In $\mathbb{R}[x]$, we have shown above that the required factorization of $p(x)$ into irreducibles in $\mathbb{Z}[x]$ is:

  $$p(x) = (x^2 + x + 2)(x^2 - x + 2).$$

- $\mathbb{C}[x]$

  The roots of $x^2 + x + 2$ are:

  $$x = \frac{1}{2}\left(-1 \pm i\sqrt{7}\right).$$

  The roots of $x^2 - x + 2$ are:

  $$x = \frac{1}{2}\left(1 \pm i\sqrt{7}\right).$$

  So the required factorization of $p(x)$ into irreducibles in $\mathbb{Z}[x]$ is:

  $$p(x) = \frac{1}{16}\left(2x - 1 - i\sqrt{7}\right)\left(2x - 1 + i\sqrt{7}\right)\left(2x + 1 - i\sqrt{7}\right)\left(2x + 1 + i\sqrt{7}\right).$$

- In the field with four elements, $\mathbb{Z}_2[t]/(t^2 + t + 1)$.

  First we remark that if $f(t) = t^2 + t + 1$, then $f(0) = f(1) = 1 \mod 2$, so the polynomial f is irreducible in $\mathbb{Z}_2[t]$, so the given ring is indeed a field.

  Over $\mathbb{Z}_2$, we have the expression of $p(x)$ as a product of irreducibles:

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

  Since this is valid modulo 2, it is also valid in the given field.

Question 4

Let $\mathbb{S} = \mathbb{Z}_3[x]/(x^2+1)$.

- Prove that $\mathbb{S}$ is a field.

  Put $f(x) = x^2 + 1$.
  Then we have: $f(0) = 1$, $f(1) = 2$ and $f(2) = 2$, so f has no roots in $\mathbb{Z}_3$, so is irreducible in $\mathbb{Z}_3[x]$.
  So $\mathbb{S}$ is a field.

- How many elements of $\mathbb{S}$ are there?
  Explain your answer and list the distinct elements.

  By the division algorithm, the elements of $\mathbb{S}$ are uniquely represented as polynomials of degree at most one, with $\mathbb{Z}_3$ coefficients.
  There are nine such and therefore nine elements of $\mathbb{S}$

$$0, 1, 2, x, 1+x, 2+x, 2x, 1+2x, 2+2x.$$

- Write out the multiplication table for $\mathbb{S}$ and identify all those elements of $\mathbb{S}$ that are perfect squares.

  The multiplication table is as follows:

$\times$	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$1+x$	$2+x$	$2x$	$1+2x$	$2+2x$
2	0	2	1	$2x$	$2+2x$	$1+2x$	x	$2+x$	$1+x$
x	0	x	$2x$	2	$2+x$	$2+2x$	1	$1+x$	$1+2x$
$1+x$	0	$1+x$	$2+2x$	$2+x$	$2x$	1	$1+2x$	2	x
$2+x$	0	$2+x$	$1+2x$	$2+2x$	1	x	$1+x$	$2x$	2
$2x$	0	$2x$	x	1	$1+2x$	$1+x$	2	$2+2x$	$2+x$
$1+2x$	0	$1+2x$	$2+x$	$1+x$	2	$2x$	$2+2x$	x	1
$2+2x$	0	$2+2x$	$1+x$	$1+2x$	x	2	$2+x$	1	$2x$

  By inspection of the multiplication table, we see that the perfect squares are:

$$0 = 0^2, \quad 1 = (\pm 1)^2, \quad 2 = (\pm x)^2, \quad x = (\pm(2+x))^2, \quad 2x = (\pm(1+x))^2.$$

- Using your multiplication table and the quadratic formula, or otherwise, find all solutions of the equation $z^2 - z - 1 = 0$ in the field $\mathbb{S}$ and hence factorize the polynomial $z^2 - z - 1$ completely as a product of irreducible polynomials with coefficients in $\mathbb{S}$.

  The discriminant D of the quadratic $z^2 - z - 1$ is:

  $$D = (-1)^2 - 4(1)(-1) = 5 = 2 = (\pm x)^2.$$

  So the required solutions are:

  $$z = \frac{1}{2}(-(-1) \pm \sqrt{D}) = 2(1 \pm x) = -1 \mp x.$$

  So we have the factorization:

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

  Check:

  $$(z+1-x)(z+1+x) = (z+1)^2 - x^2 = z^2 + 2z + 1 - 2 = z^2 - z - 1 + 3z = z^2 - z - 1.$$

Question 5

Find all ring homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_6$ and for each determine its image and kernel.
How many ring homomorphisms are there from $\mathbb{Z}_6$ to $\mathbb{Z}_{12}$?
Explain your answer.

Let a homomorphism f map $\mathbb{Z}_{12}$ to $\mathbb{Z}_6$.
Then if $f(1) = m$, we have $f(t) = mt$, for any $t \in \mathbb{Z}_{12}$.
This is a well-defined map, since if $t' = t \mod 12$, then $t' = t + 12k$, for some integer k and then we have:

$$f(t') = mt' = m(t + 12k) = mt + 6(2mk) = mt \mod 6 = f(t) \mod 6.$$

Then for any s and $t \in \mathbb{Z}_{12}$, we have in $\mathbb{Z}_6$:

$$f(s+t) - f(s) - f(t) = m(s+t) - ms - mt = 0,$$

$$0 = f(st) - f(s)f(t) = mst - (ms)(mt) = st(m - m^2).$$

When $s = t = 1$ this gives $m = m^2 \mod 6$ and provided $m = m^2 \mod 6$, the equation $f(st) = f(s)f(t)$ holds for all s and t in $\mathbb{Z}_{12}$ and f is a ring homomorphism, as required.

Put $g(m) = m^2 - m \mod 6$.
Then we have $g(0) = g(1) = g(3) = g(4) = 0$ and $g(2) = g(5) = 2$.
So the required homomorphisms are given by $m = 0, 1, 3,$ and 4.

- When $m = 0$, we have $f(t) = 0$, for all $t \in \mathbb{Z}_{12}$, so the kernel is $\mathbb{Z}_{12}$ and the image is $\{0\}$.
- When $m = 1$, we have $f(t) = t \mod 6$, for all $t \in \mathbb{Z}_{12}$, so the kernel is $\{0, 6\}$ and the image is $\mathbb{Z}_6$.
- When $m = 3$, we have $f(t) = 3t \mod 6$, for all $t \in \mathbb{Z}_{12}$, so the kernel is $\{0, 2, 4, 6, 8, 10\}$ and the image is $\{0, 3\}$.
- When $m = 4$, we have $f(t) = 4t \mod 6$, for all $t \in \mathbb{Z}_{12}$, so the kernel is $\{0, 3, 6, 9\}$ and the image is $\{0, 2, 4\}$.

If now g is a ring homomorphism from $\mathbb{Z}_6$ to $\mathbb{Z}_{12}$, then we have, if $g(1) = n$, $g(t) = nt \mod 12$, for all $t \in \mathbb{Z}_6$.
This is well-defined provided $g(6u) = 0$, for all integer u, so provided $6un = 0 \mod 12$, so n must be even.
Then the homomorphism is $g(t) = 2mt \mod 12$, for some integer m and is well-defined. We have for any s and t:

$$g(s+t) - g(s) - g(t) = 2m(s+t) - 2ms - 2mt = 0,$$

$$0 = g(st) - g(s)g(t) = 2mst - (2ms)(2mt) = st(2m - 4m^2).$$

So we need $2m = 4m^2 \mod 12$, so $2m - 4m^2 = 12p$, for some integer p, so $m - 2m^2 = 6p$, so $2m^2 - m = 0 \mod 6$.
Put $h(m) = 2m^2 - m \mod 6$.
Then we have:

$$h(0) = 0, \quad h(1) = 1, \quad h(2) = 0, \quad h(3) = 3, \quad h(4) = 4, \quad h(5) = 3.$$

So $m = 0$ or $m = 2$, and there are exactly two ring homomorphisms, q and r, from $\mathbb{Z}_6$ to $\mathbb{Z}_{12}$, namely:

- $q(t) = 0 \mod 12$, for all $t \in \mathbb{Z}_6$
  This has image $\{0\}$ in $\mathbb{Z}_{12}$ and kernel $\mathbb{Z}_6$.

- $r(t) = 4t \mod 12$, for all $t \in \mathbb{Z}_6$.
  This has image $\{0, 4, 8\}$ in $\mathbb{Z}_{12}$ and kernel $\{0, 3\}$ in $\mathbb{Z}_6$.

Question 6

Let $\mathbb{A} = \mathbb{Z}_6$, $\mathbb{B} = \mathbb{Z}_8$, $\mathbb{C} = \mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{D} = \mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{E} = \mathbb{Z}_2[x]/(x^3 + x + 1)$. Decide with proof, which, if any, of the rings $\mathbb{A}$, $\mathbb{B}$, $\mathbb{C}$, $\mathbb{D}$ or $\mathbb{E}$ are pairwise isomorphic.

The rings $\mathbb{A}$ and $\mathbb{D}$ each have six elements, whereas the rings $\mathbb{B}$, $\mathbb{C}$ and $\mathbb{E}$ each have eight elements, so the only possible isomorphisms are between the rings $\mathbb{A}$ and $\mathbb{D}$ and amongst the rings $\mathbb{B}$, $\mathbb{C}$ and $\mathbb{E}$.

Since $\mathbb{A}$ is generated by 1 and since the identity of $\mathbb{D}$ is $(1,1)$, the only possible isomorphism from $\mathbb{A}$ to $\mathbb{D}$ maps $1 \to (1,1)$ and is therefore $f(x) = (x,x)$, for any $x \in \mathbb{A}$. It is easily checked that this is one-to-one and onto and is a ring homomorphism, so $\mathbb{A}$ and $\mathbb{D}$ are isomorphic. Specifically one has:

$$f(0) = (0,0), \quad f(1) = (1,1), \quad f(2) = (0,2), \quad f(3) = (1,0), \quad f(4) = (0,1), \quad f(5) = (1,2).$$

Next put $g(x) = x^3 + x + 1 \mod 2$. Then we have $g(0) = g(1) = 1$, so g is irreducible, so $\mathbb{E}$ is a field. But in $\mathbb{B} = \mathbb{Z}_8$, we have $2(4) = 0$ and in $\mathbb{C} = \mathbb{Z}_4 \times \mathbb{Z}_2$, we have $(2,0)(0,1) = (0,0)$, so both $\mathbb{B}$ and $\mathbb{C}$ have divisors of zero, so are not fields, so neither $\mathbb{B}$ nor $\mathbb{C}$ can be isomorphic to $\mathbb{E}$.

Finally the squares in $\mathbb{B} = \mathbb{Z}_8$ are:

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9 = 1, \quad 4^2 = 16 = 0, \quad 5^2 = 25 = 1, \quad 6^2 = 36 = 4, \quad 7^2 = 49 = 1.$$

In particular in $\mathbb{B}$, there are four distinct solutions of the equation $x^2 = 1$, namely, $1, 3, 5, 7$. The squares in $\mathbb{C} = \mathbb{Z}_4 \times \mathbb{Z}_2$ are:

$$(0,0)^2 = (0,0), \quad (1,0)^2 = (1,0), \quad (2,0)^2 = (4,0) = (0,0), \quad (3,0)^2 = (9,0) = (1,0),$$

$$(0,1)^2 = (0,1), \quad (1,1)^2 = (1,1), \quad (2,1)^2 = (4,1) = (0,1), \quad (3,1)^2 = (9,1) = (1,1).$$

Here there are only two solutions of the equation $x^2 = 1$ in $\mathbb{C}$ (whose multiplicative identity is $(1,1)$), namely $x = \pm(1,1)$ (since we have $-(1,1) = (-1,-1) = (3,1)$).
Since the equation $x^2 = 1$ has different numbers of solutions in the rings $\mathbb{B}$ and $\mathbb{C}$, the two rings cannot be isomorphic.
So amongst the (distinct) pairs of the given rings there are isomorphisms only between $\mathbb{A}$ and $\mathbb{D}$ and vice-versa (the latter using the inverse isomorphism to the isomorphism f given above).