103B - Homework 6 Solutions

1) a) \( f(x) = x^4 + x \) \( \Rightarrow f(0) = 0, f(1) = 2, f(-1) = 0 \)

\( g(x) = x^2 + x \) \( \Rightarrow g(0) = 0, g(1) = 2, g(-1) = 0 \)

b) \( 3x^2 + 2x + 1 = \frac{4x^2 + 3x + 6 - 1}{5x^4 + x^3 + 4x^2} \) in \( \mathbb{Z}_7 \)

\( 3 \cdot 4 = 12 = 5 \) (mod 7)

\( 3 \cdot 3 = 9 = 2 \) (mod 7)

\( 3 \cdot 4 = 12 \equiv 5 \) (mod 7)

\( 2x^2 + 3x^2 + 1 \)

\( 2x^2 + 6x^2 + 3x \)

\( \frac{4x^2 + 4x + 1}{4x^2 + 5x + 6} \)

\( + 6x + 2 \)

c) degree 1 irreducible in \( \mathbb{Z}_3 [x] \) with lead coefficient 1

\( x, x+1, x-1 \)

degree 2 irreducible in \( \mathbb{Z}_3 [x] \) with lead coefficient 1

\( x^2 + x + 2, x^2 + 2x + 2, x^2 + 1 \)

Note that the polynomials have no roots in \( \mathbb{Z}_3 \)

Thus they are irreducible by Gallian, p. 306.

Now we look for degree 3 irreducibles the same way,

degree 3 irreducible in \( \mathbb{Z}_3 [x] \) with lead coefficient 1

There are 18 \( x^3 + ax^2 + bx + c \) with \( c \neq 0 \)

\[ (a,b,c) = (0,0,1) \]

\( x^3 + 1 \)

\( (0,1,1) \)

\( x^3 + x + 1 \)

\( 0 \)

\( (0,-1,1) \)

\( x^3 - x + 1 \)

\( (1,0,1) \)

\( x^3 - x - 1 \)

\( 1 \)

\( (1,-1,1) \)

\( x^3 + x^2 + x \)

\( 0 \)

\( (1,1,1) \)

\( x^3 - x^2 - 1 \)

\( 1 \)

\( (1,-1,1) \)

\( x^3 + x^2 - x + 1 \)

\( -1 \)

\( (1,0,1) \)

\( x^3 + x^2 + x - 1 \)

\( 0 \)

\( (1,-1,1) \)

\( x^3 - x^2 - x + 1 \)

\( 1 \)

\( (1,1,1) \)

\( x^3 - x - 1 \)

\( -1 \)

\( (1,-1,1) \)

\( x^3 + x^2 + x - 1 \)

\( 1 \)

\( (1,0,1) \)

\( x^3 + x^2 + x + 1 \)

\( 0 \)

\( (1,-1,1) \)

\( x^3 - x^2 - x - 1 \)

\( 1 \)

\( (1,1,1) \)

\( x^3 - x^2 + x + 1 \)

\( 0 \)

The irreducible deg 3 with lead coeff 1 are

\( x^3 - x + 1 \)

\( x^3 + x^2 - x + 1 \)

\( x^3 + x^2 + x + 1 \)

\( x^3 - x^2 + x + 1 \)

\( x^3 + x - 1 \)

\( x^3 - x - 1 \)

\( x^3 + x^2 + x - 1 \)

\( x^3 - x^2 - x - 1 \)
2) a) \( \langle x \rangle \) is maximal since \( x \) is irreducible. 
   Thus \( \langle x \rangle \subset \langle f(x) \rangle \subset \mathbb{Z}_3[x] \)
   \[ x = f(x) \cdot g(x) \implies \text{either } \deg f \text{ or } \deg g = 0 \]
   \[ \implies \text{either } f \text{ or } g \text{ is a unit in } \mathbb{Z}_3[x] \]
   \[ f = \text{unit} \implies \langle f(x) \rangle = \mathbb{Z}_3[x] \]
   \[ g = \text{unit} \implies \langle x \rangle = \langle f(x) \rangle \]
   Thus \( \langle x \rangle \) is maximal

b) \( \mathbb{Z}_3[x]/\langle x \rangle \) is represented by

   the cosets \( f(x) + \langle x \rangle \)

   if we divide
   \[ f(x) = x \cdot g(x) + r(x) \]
   so that \( \deg r < 1 \) or \( r = 0 \), \( r \in \mathbb{Z}_3 \)
   Thus \( f(x) + \langle x \rangle = r + \langle x \rangle \) where \( r \in \mathbb{Z}_3 \)

   So our isomorphism is
   \[ \phi: \mathbb{Z}_3 \to \mathbb{Z}_3[x]/\langle x \rangle \]
   \[ \phi(r) = r + \langle x \rangle \quad \forall r \in \mathbb{Z}_3 \]

   \( \phi \) is onto by the preceding discussion
   \( \phi \) is well-defined clearly
   \( \phi \) is 1-1 as
   \[ \phi(r) = \phi(s) \implies r \in \langle x \rangle \implies r = s \]
   \[ 0 \text{ or } \degree 0 \]

   \( \phi \) preserves +
   \[ \phi(r+s) = r+s + \langle x \rangle = (r+\langle x \rangle) + (s+\langle x \rangle) \]
   \[ = \phi(r) + \phi(s) \]

   a similar argument works for multiplication
3) a) \( \mathbb{Z}_3[x]/\langle x^2 + x + 2 \rangle \)

By problem 1c), \( x^2 + x + 2 \) is irreducible.
So by the same argument as in 2a),
\( \langle x^2 + x + 2 \rangle \) is a maximal ideal which \( \Rightarrow \)
the factor ring is a field, whose elements
are the cosets of the remainders of polynomials
\( f(x) \in \mathbb{Z}_3[x] \) upon division by \( x^2 + x + 2 \).
Such remainders look like \( bx + a \), \( a, b \in \mathbb{Z}_3 \)
There are thus 9 elements

\[ \mathbb{Z}_3[\theta] = \left\{ a + b\theta \mid a, b \in \mathbb{Z}_3 \right\} \text{ with } \theta^2 + \theta + 2 = 0 \]

So we can define a map

\[ T : \mathbb{Z}_3[\theta] \rightarrow \mathbb{Z}_3[x] \]

\[ T(a + b\theta) = a + bx + \langle x^2 + x + 2 \rangle, \quad a, b \in \mathbb{Z}_3 \]

\( T \) is well-defined, 1-1, onto using preceding
discussion + preserves \( + \) and \( x \).

+ \( T(a + b\theta + a' + b'\theta) = T(a + a' + (b + b')\theta) \)
\[ = a + a' + (b + b')x + \langle x^2 + x + 2 \rangle \]
\[ \text{def \&} \quad \text{for cosets} \]
\[ = a + bx + \langle x^2 + x + 2 \rangle + a' + b'x + \langle x^2 + x + 2 \rangle \]
\[ = T(a + b\theta) + T(a' + b'\theta) \]

\[ T(a + b\theta)(a' + b'\theta) = T( a + b \theta)(a' + b' \theta) \]
\[ \theta^2 = -\theta - 2 \]
\[ \Rightarrow \theta^2 = 2\theta + 1 \]
\[ = T(a + b\theta + (a'b + ab')\theta) \]
\[ = aa' + bb' + (ab' + ba')x + \langle x^2 + x + 2 \rangle \]

We want to see this last quantity is
\( (a + bx + \langle x^2 + x + 2 \rangle)(a' + bx + \langle x^2 + x + 2 \rangle) \)
\[ = aa' + bb'x^2 + (ab' + ba')x + \langle x^2 + x + 2 \rangle \]
\[ \text{Now} \quad x^2 + \langle x^2 + x + 2 \rangle = -x + \langle x^2 + x + 2 \rangle = 2x + 1 + \langle x^2 + x + 2 \rangle \]
So \((a+bx+\langle x^2+x+2 \rangle)(a'+b'x + \langle x^2+x+2 \rangle)\)
\[
= aa' + ab' + ba'x + \langle x^2+x+2 \rangle
+ bb'(2x+1) + \langle x^2+x+2 \rangle
\]
\[
= (aa' + bb') + (ab'+ba'+2bb')x + \langle x^2+x+2 \rangle
\]
which was what we wanted to show.

T onto as every coset has the form \(r(x)+\langle x^2+x+2 \rangle\)
where \(r(x)\) is a possible remainder of \(f(x) \in \mathbb{Z}_3[x]\)
on division by \(x^2+x+2\). Such a remainder has degree \(\leq 2\) or the remainder is \(0\).
So \(r(x) = a+bx\), \(a, b \in \mathbb{Z}_3\).
Thus \(f(x) + \langle x^2+x+2 \rangle = a+bx + \langle x^2+x+2 \rangle = T(a+b\theta)\)

\(T^{-1} a+b\theta = T(a'+b'\theta) \iff\)
\[
a+bx = (a'+b'x) + \langle x^2+x+2 \rangle
\]
\[
\overset{\text{degree} \ = \ 1}{\uparrow}
\]
But degree 1 poly \(\neq (x^2+x+2)\). \(g(x)\)
unless it is the 0-poly.
So \(a = a'\) & \(b = b'\)
and \(a+b\theta = a'+b'\theta\)
\[ \theta^2 + \theta + 2 = 0 \]

Elements of \( \mathbb{F}_9 \) have form \( a_0 + a_1 \theta \) \( \theta \in \mathbb{Z}_3 \)

\[ \theta (a_0 + a_1 \theta) = a_0 \theta + a_1 \theta^2 = a_0 \theta + a_1 (-\theta - 2) \]
\[ = a_0 \theta - a_1 \theta - 2a_1 \]
\[ = a_1 + (a_0 - a_1) \theta \]

\((a_0; a_1) \rightarrow (a_1; a_0 - a_1)\)

<table>
<thead>
<tr>
<th>Element of ( \mathbb{F}_9 )</th>
<th>( a_0 )</th>
<th>( a_1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( a_0 + \theta \theta = \theta )</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>( \theta^2 )</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>( \theta^3 )</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>( \theta^4 )</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>( \theta^5 )</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>( \theta^6 )</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>( \theta^7 )</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>( \theta^8 = 1 )</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

So \( G = \{ \theta^g \mid g \in \mathbb{Z}_3 \} \) is a cyclic group under multiplication of order 8

and \( G = \mathbb{F}_9^* = \mathbb{F}_9 - \{0\} \).

c) Yes

Why?
4) a) \( x^n(x^2-1)^n \), \( n \in \mathbb{Z}^+ \)

b) \( f(a) = 0 \Rightarrow f(x) = (x-a)h(x), h(x) \in \mathbb{Z}[x] \)

by Cor 2, p. 298 in Gallian

So, by the product rule

\[ f'(x) = h(x) + (x-a)h'(x) \]

\[ 0 = f'(a) = h(a) \Rightarrow h(x) = (x-a)g(x) \]

using Cor. 2, p. 298 again

So \( f(x) = (x-a)^2g(x) \).