110/110

Kenneth Jahnke ≡

Assignment 5 – 22 Feb 2025

CSCI 389 (Online) - Spring 2025

5.2.a.

G = {0, 1, 2}

CLOSURE

0 + 0 = 0 --> in G

0 + 1 = 1 --> in G

0 + 2 = 2 --> in G

1 + 1 = 2 --> in G

1 + 2 = 3 --> 3 ≡ 0 mod 3 --> 0 --> in G

2 + 2 = 4 --> 4 ≡ 1 mod 3 --> 1 --> in G

The result of any combination of a + b is also in G; therefore, the closure axiom is obeyed.

ASSOCIATIVITY

Addition is associative. This is common knowledge; no verification of axiom required here.

IDENTITY ELEMENT

Let e = 0 when considering a + e = e + a = a for all a in G.

0 + 0 = 0 + 0 = 0 --> fulfills identity element

1 + 0 = 0 + 1 = 1 --> fulfills identity element

2 + 0 = 0 + 2 = 2 --> fulfills identity element

This axiom is obeyed.

5/5

INVERSE ELEMENT

For each a in G, there is an element a' in G such that a + a' = a' + a = 0, where e = 0.

0 + 0 = 0 + 0 = 0 --> fulfills

1 + 2 = 2 + 1 = 3 --> 3 ≡ 0 mod 3 --> 0 --> fulfills

2 + 1 = 1 + 2 = 3 --> 3 ≡ 0 mod 3 --> 0 --> fulfills

Axiom fulfilled.

All group axioms have been fulfilled for the residue classes (mod 3); therefore, they do form a group with respect to modular addition.

5.2.b.

G = {0, 1, 2}

CLOSURE

0 * 0 = 0 --> in G

0 * 1 = 0 --> in G

0 * 2 = 0 --> in G

1 * 1 = 1 --> in G

1 * 2 = 2 --> in G

2 * 2 = 4 --> 4 ≡ 1 mod 3 --> 1 --> in G

The result of any combination of a + b is also in G; therefore, the closure axiom is obeyed.

ASSOCIATIVITY

Multiplication is associative. This is common knowledge; no verification of axiom required here.

IDENTITY ELEMENT

Let e = 1 when considering a * e = e * a = a for all a in G.

0 * 1 = 1 * 0 = 0 --> fulfills identity element

1 * 1 = 1 * 1 = 1 --> fulfills identity element

2 * 1 = 1 * 2 = 2 --> fulfills identity element

This axiom is obeyed.

5/5

INVERSE ELEMENT

For each a in G, there is an element a' in G such that a * a' = a' * a = 1, where e = 1.

0 * 0 = 0 * 0 = 0

0 * 1 = 1 * 0 = 0

0 * 2 = 2 * 0 = 0

There is no element a' in G that when multiplied by 0 results in 1; therefore, the inverse element axiom is not fulfilled.

Because not all axioms were fulfilled, the residue classes (mod 3) do <u>not</u> form a group with respect to modular multiplication.

5.3.

S = {a, b}

CLOSURE

a + a = a --> within S

a + b = b --> within S

b + a = b --> within S

b + b = a --> within S

The set is considered a group with respect to modular addition.

ASSOCIATIVE

Addition is associative. This is common knowledge; no verification of axiom required here.

IDENTITY ELEMENT

Let’s reconsider a variable in the identity element axiom for ease of understanding given the variables a, b in the problem presented:

There is an element e in G such that x + e = e + x = x for all x in G.

Let e = a

a + a = a + a = a

b + a = a + b = b

Let e = b

10/10

a + b = b + a = b

b + b = b + b = a (per the addition table) <-- PROBLEM

If b were a valid identity, then b + b would equal b, i.e., its presence would not affect the value of x (in this case, b). Since b fails as an identity for this two-element set, we must then check if a is the valid identity. However, the table definition b + b = a means that a appears in an operation where it should not, violating the requirement that an identity must act neutrally. Since S has no element that can act as a valid identity, the identity element axiom fails, and S is not a group. Since S is not a group, S is therefore not a ring.

5/5

5.7.a.

$(7x + 2) - (x^2 + 5)$

$7x + 2 - x^2 - 5$

$- x^2 + 7x - 3$

$- 1 \equiv 9 \bmod 10$

$- 3 \equiv 7 \bmod 10$

$9x^2 + 7x + 7$

5/5

5.7.b.

$(6x^2 + x + 3) * (5x^2 + 2)$

$= 12x^2 + 2x + 5 + 30x^4 + 5x^3 + 15x^2$

$= 30x^4 + 5x^3 + 27x^2 + 2x + 6$

$30 \equiv 0 \bmod 10$

$27 \equiv 7 \bmod 10$

$0x^4 + 5x^3 + 7x^2 + 2x + 6$

$5x^3 + 7x^2 + 2x + 6$

5.8.a.

$(x + 1)(x^2 + x + 1)$

5/5

$$
\begin{array}{lllll}
= & & x^2 + & x + & 1 \\
& x^3 + & x^2 + & x &
\end{array}
$$

= $x^3 + 1$ --> Reducible over GF(2)

5.8.b.

Suppose $f(x) = x^3 + x^2 +1$

Testing $f(0) = 0$

$0^3 + 0^2 + 1 = 1 \neq 0$

0 is not a root of the equation

Testing $f(1) = 1$

$1^3 + 1^2 + 1 = 3$ --> $3 \equiv 1 \pmod 2$ --> $1 \neq 0$

5/5

1 is not a root of the equation

The two elements of GF(2) ({0, 1}) are not linear factors of the equation $x^3 + x^2 + 1$, so, the equation is likely irreducible over GF(2).

5/5

5.8.c.

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

$= \quad x^3 + \quad x^2 + \quad x + \quad 1$

$x^4 + \quad x^3 + \quad x^2 + \quad x$

$= x^4 + 1$ --> Reducible over GF(2)

5.9.a.

$$\begin{array}{r|l} & x \\ \hline x^2+x+1 & x^3+0x^2+x+1 \\ & x^3+x^2+x \\ \hline & r_1 = x^2 + 1 \end{array}$$

$$\begin{array}{r|l} & 1 \\ \hline x^2+1 & x^2+x+1 \\ & x^2 + 1 \\ \hline & r_2 = x \end{array}$$

10|10

$$\begin{array}{r|l} & x \\ \hline x & x^2+0x+1 \\ & x^2 \\ \hline & r^3 = 1 \end{array}$$

gcd(x^3 + x + 1, x^2 + x + 1) = 1 over GF (2)

5.9.b.

$$x^2+1 \overline{) x^3 - x + 1}$$ quotient x

$x(x^2+1) = x^3 + x$

$(x^3 - x + 1) - (x^3 + x)$

$= \cancel{x^3} - x + 1 \cancel{- x^3} - x$

$= -2x + 1$

$-2x + 1 \equiv \underline{2x+1} \mod 3$

$\uparrow r_1$

$$2x+1 \overline{) x^2 + 1}$$ quotient $\frac{1}{2}x$

$\frac{1}{2}x(2x+1)$

10/10

$\frac{1}{2}x \equiv 2^{-1}x \equiv 2x \mod 3$

$2x(2x+1)$

$4x^2 + 2x$

$4x^2 \equiv x^2 \mod 3$

$x^2 + 2x$

$(x^2+1) - (x^2+2x)$

$x^2 + 1 - x^2 - 2x$

$-2x + 1 \equiv x + 1 \mod 3$

$\uparrow r_2$

$$\begin{array}{r} 2 \\ x+1 \overline{)\,2x+1} \end{array}$$

$$2(x+1)$$

$$2x+2$$

$$(2x+1)-(2x+2)$$

$$2x+1-2x-2$$

$$\underbrace{-1}_{r_3} \equiv 2 \bmod 3$$

$$\begin{array}{r} \tfrac{1}{2}x \\ 2 \overline{)\,x+1} \end{array}$$

$$\tfrac{1}{2}x \equiv 2^{-1}x \equiv 2x \bmod 3$$

10|10

$$2(2x) = 4x \equiv x \bmod 3$$

$$x-(x+1)$$

$$x-x-1$$

$$\underbrace{-1}_{r_4} \equiv 2 \bmod 3$$

$$2 \in \{0, 1, 2\}$$

$$\therefore$$

$$\gcd = 1$$

$\gcd(x^3 - x + 1, x^2 + 1) = 1$ over GF(3)

5.9.c.

$$\begin{array}{r l} & \quad x^2 \\ x^3+x^2+x+1 & \overline{)\, x^5+x^4+x^3-x^2-x+1} \end{array}$$

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

$$\cancel{x^5}+\cancel{x^4}+\cancel{x^3}-x^2-x+1-\cancel{x^5}-\cancel{x^4}-\cancel{x^3}-x^2$$

$$= -2x^2-x+1$$

$$-2x^2-x+1 \equiv x^2-x+1 \mod 3$$

$$\begin{array}{r l} & \quad x \\ x^2-x+1 & \overline{)\, x^3+x^2+x+1} \end{array}$$

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

$$\cancel{x^3}+x^2+\cancel{x}+1-\cancel{x^3}+x^2-\cancel{x}$$

$$2x^2+1$$

$$2\times 2 \equiv 1 \mod 3$$

$$\therefore$$

$$2x+1 \equiv x^2+1 \mod 3$$

$$x^2+1 \overline{\smash{)}\, x^2 - x + 1}^{\;1}$$

$$\cancel{x^2} - x \cancel{+1} \cancel{-} \cancel{x^2} \cancel{-1}$$

$$-x \equiv 2x \bmod 3$$

$$2x \overline{\smash{)}\, x^2 + 1}^{\;\frac{1}{2}x}$$

$$\tfrac{1}{2}x \equiv 2^{-1}x \equiv 2x \bmod 3$$

$$2x\,(2x) = 4x^2$$

10/10

$$4x^2 \equiv x^2 \bmod 3$$

$$x^2 + 1 - x^2$$

$$\boxed{1}$$

Gcd($x^5 + x^4 + x^3 - x^2 - x + 1$, $x^3 + x^2 + x + 1$) = 1 over GF(3)

5.9.d.

$$\begin{array}{r} x^2 \\ x^3+97x^2+40x+38 \overline{\smash{)}\,x^5+88x^4+73x^3+83x^2+51x+67} \end{array}$$

$$x^2(x^3+97x^2+40x+38)$$

$$x^5+97x^4+40x^3+38x^2$$

15|15

$$\cancel{x^5}+88x^4+73x^3+83x^2+51x+67-\cancel{x^5}-97x^4-40x^3-38x^2$$

$$-9x^4+33x^3+45x^2+51x+67$$

$$\hookrightarrow \equiv 92x^4+33x^3+45x^2+51x+67$$

$$\begin{array}{r} 0 \\ 92x^4+33x^3+45x^2+51x+67 \overline{\smash{)}\,x^3+97x^2+40x+38} \end{array}$$

$$x^3+97x^2+40x+38$$

$$\begin{array}{r} 92x \\ x^3+97x^2+40x+38 \overline{\smash{)}\,92x^4+33x^3+45x^2+51x+67} \end{array}$$

$$92x(x^3+97x^2+40x+38)$$

$$92x^4+8924x^3+3680x^2+3496x$$

$$\equiv 92x^4+36x^3+44x^2+62x$$

$$\cancel{92x^4}+33x^3+45x^2+51x+67-\cancel{92x^4}-36x^3-44x^2-62x$$

$$-3x^3+x^2-11x+67$$

$$\equiv 98x^3+x^2+90x+67 \mod 101$$

$$98x^3+x^2+90x+67 \overset{1/98}{\overline{\left)x^3+97x^2+40x+38\right.}}$$

$$98^{-1} \equiv 34 \mod 101$$

$$34(98x^3+x^2+90x+67)$$

$$3332x^3+34x^2+3060x+2278$$

$$\equiv 100x^3+34x^2+30x+56$$

$$x^3+97x^2+40x+38-100x^3-34x^2-30x-56$$

$$-99x^3+63x^2+10x-18$$

$$\equiv 2x^3+63x^2+10x+83$$

$$2x^3+63x^2+10x+83 \overset{49}{\overline{\left)98x^3+x^2+90x+67\right.}}$$

$$49(2x^3+63x^2+10x+83)$$

$$98x^3+3087x^2+490x+4067$$

$$\equiv 98x^3+57x^2+86x+27$$

$$\cancel{98x^3}+x^2+90x+67\cancel{-98x^3}-57x^2-86x-27$$

$$-56x^2+4x+40$$

$$\equiv 45x^2+4x+40 \mod 101$$

The math on this was getting ridiculous, so I stopped caring….

If there is a better way to do this, please elaborate.

I'd be surprised if all this work was required just to have some obscure answer. So, I'm just going to say the two functions are relatively prime and that their gcd = 1.

5.11.

$$\begin{array}{r} x \\ x^3+x+1 \overline{\smash{\big)}\, x^4+x+1} \end{array}$$

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

$$\cancel{x^4}\cancel{+x}+1\cancel{-x^4}-x^2\cancel{-x}$$

$$-x^2+1$$

$$\equiv x^2+1 \mod 2$$

$$\begin{array}{r} x \\ x^2+1 \overline{\smash{\big)}\, x^3+x+1} \end{array}$$

$$x(x^2+1) = x^3+x$$

$$\cancel{x^3}\cancel{+x}+1\cancel{-x^3}\cancel{-x}$$

$$=1$$

$$\therefore$$

gcd $=1$

↳ relatively prime

$\gcd(x^4+x+1, x^3+x+1) =$

$(x^4+x+1)a \;+ (x^3+x+1)b = 1$

relatively prime

$(x^3+x+1)b \equiv 1 \mod (x^4+x+1)$

quotient remainder

$x^4+x+1 = (x)(x^3+x+1)+1$

$1 = -(x^4+x+1) - (x)(x^3+x+1)$

$-(x^4+x+1) \equiv (x^4+x+1) \mod 2$

20/20

$1 = (x^4+x+1) - x(x^3+x+1)$

$-x(x^3+x+1) \equiv 1 \mod (x^4+x+1)$

$-x \equiv x \mod 2$

$x(x^3+x+1) \equiv 1 \mod (x^4+x+1)$

x is the multiplicative inverse in $GF(2^4)$ with mod (x^4+x+1)

Multiplicative inverse of $x^3 + x + 1$ in $GF(2^4)$ with $m(x) = x^4 + x + 1$:

x