1. 請求出所有𝐺的循環子群

(1) 𝐺 =〈𝑍6∗,×〉

10 mod 6 = 1

50 mod 6 = 1

51 mod 6 = 5

* 𝐻1=<{1},×>、𝐻2=G

(2) 𝐺 =〈𝑍12∗,×〉

10 mod 12 = 1

50 mod 12 = 1

51 mod 12 = 5

70 mod 12 = 1

71 mod 12 = 7

110 mod 12 = 1

111 mod 12 = 11

* 𝐻1=<{1},×>、𝐻2=<{1,5},×>、𝐻3=<{1,7},×>、𝐻4=<{1,11},×>

(3) 𝐺 =〈𝑍14∗,×〉

10 mod 14 = 1

30 mod 14 = 1

31 mod 14 = 3

32 mod 14 = 9

33 mod 14 = 13

34 mod 14 = 11

35 mod 14 = 5

50 mod 14 = 1

51 mod 14 = 5

52 mod 14 = 11

53 mod 14 = 13

54 mod 14 = 9

55 mod 14 = 3

110 mod 14 = 1

111 mod 14 = 11

112 mod 14 = 9

130 mod 14 = 1

131 mod 14 = 13

* 𝐻1=<{1},×>、𝐻2=<{1,13},×>、𝐻3=<{1,9,11},×>、𝐻4=G

2. Which of the following is a ring and which is a field? Please explain your answer.

(1) 〈ℤ, +, ×〉

+,x forms a ring, because Addition and Multiplication are closed operations on ℤ. They are both associative, and also exists an additive identity (0), but not every element in ℤ has a multiplicative inverse (ex: no integer can multiply by 2 to get 1), so ℤ is not a field.

(2) 〈ℝ, +, ×〉

+,x forms a field, because Addition and multiplication are closed operations on ℝ. They are both associative and commutative, and also exist additive and multiplicative identities (0 and 1, respectively). Every nonzero element has a multiplicative inverse (ex: multiplicative inverse of 2 is 1/2).

(3) 〈{𝑒, 𝑔, 𝑔2, …, 𝑔𝑛−1}, +, ×〉 where 𝑔𝑛 = 𝑒

It’s a ring not a field. It doesn't have the properties necessary to be a field, such as closure under multiplication and addition, existence of additive and multiplicative identities, and existence of multiplicative inverses for all nonzero elements.And it has the properties of ring in additive & multiplicative identities.

3. 請求出在𝐺𝐹(28)下，𝑎(𝑥)=𝑥7+𝑥+1在模𝑚(𝑥)下的乘法反元素，其中不可分解多項式𝑚(𝑥)=𝑥8+𝑥7+𝑥3+𝑥+1。

q r1 r2 r t1 t2 t

x+1 𝑥8+𝑥7+𝑥3+𝑥+1 𝑥7+𝑥+1 𝑥3+ 𝑥2+x 0 1 x+1

𝑥4+𝑥3+𝑥+1 𝑥7+𝑥+1 𝑥3+ 𝑥2+x 𝑥3+ 𝑥2+x+1 1 x+1 𝑥5+𝑥3+𝑥2+𝑥+1

1 𝑥3+ 𝑥2+x 𝑥3+ 𝑥2+x+1 1 x+1 𝑥5+𝑥3+𝑥2+𝑥+1 𝑥5+𝑥3+𝑥2

𝑥3+ 𝑥2+x+1 𝑥3+ 𝑥2+x+1 1 0 𝑥5+𝑥3+𝑥2+𝑥+1 𝑥5+𝑥3+𝑥2 0

1 0 𝑥5+𝑥3+𝑥2 0

=> 𝑥5+𝑥3+𝑥2

4. 請計算在𝐺𝐹(25)下，(𝑥3+𝑥+1)⊗(𝑥4+𝑥2)的結果，其中不可分解多項式為𝑥5+𝑥2+1。

P1⊗P2 = 𝑥3(𝑥4+𝑥2)+x(𝑥4+𝑥2)+1(𝑥4+𝑥2)

P1⊗P2 = 𝑥7+𝑥5+𝑥5+𝑥3+𝑥4+𝑥2

P1⊗P2 = (𝑥7+𝑥4+𝑥3+𝑥2) mod (𝑥5+𝑥2+1) = x3

5. 請找出多項x6+𝑥3+1所代表的7位元字組

n = 7 => 階數=6

1x6+0x5+0x4+1𝑥3+0x2+0x1+1x0

* 1001001