1. 請求出所有G的循環子群

(1) $G = \langle Z_{6*}, \times \rangle$

$1^0 \bmod 6 = 1$

$5^0 \bmod 6 = 1$

$5^1 \bmod 6 = 5$

⇨ $H1$=<{1},×>、$H2$=G

(2) $G = \langle Z_{12*}, \times \rangle$

$1^0 \bmod 12 = 1$

$5^0 \bmod 12 = 1$

$5^1 \bmod 12 = 5$

$7^0 \bmod 12 = 1$

$7^1 \bmod 12 = 7$

$11^0 \bmod 12 = 1$

$11^1 \bmod 12 = 11$

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

(3) $G = \langle Z_{14*}, \times \rangle$

$1^0 \bmod 14 = 1$

$3^0 \bmod 14 = 1$

$3^1 \bmod 14 = 3$

$3^2 \bmod 14 = 9$

$3^3 \bmod 14 = 13$

$3^4 \bmod 14 = 11$

$3^5 \bmod 14 = 5$

$5^0 \bmod 14 = 1$

$5^1 \bmod 14 = 5$

$5^2 \bmod 14 = 11$

$5^3 \bmod 14 = 13$

$5^4 \bmod 14 = 9$

$5^5 \bmod 14 = 3$

$11^0 \bmod 14 = 1$

$11^1 \bmod 14 = 11$

$11^2 \bmod 14 = 9$

$13^0 \bmod 14 = 1$

$13^1 \bmod 14 = 13$

⇨ $H1$=<{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) $\langle \mathbb{Z}, +, \times \rangle$

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

(2) $\langle \mathbb{R}, +, \times \rangle$

+,x forms a field, because Addition and multiplication are closed operations on $\mathbb{R}$. 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) $\langle\{e, g, g^2, \ldots, g^{n-1}\}, +, \times\rangle$ where $g^n = e$

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$GF(2^8)$下，$a(x)$=x^7+x+1 在模$m(x)$下的乘法反元素，其中不可分解多項式$m(x)$=x^8+x^7+x^3+x+1。

q	r1	r2	r	t1	t2	t
x+1	$x^8+x^7+x^3+x+1$	x^7+x+1	x^3+x^2+x	0	1	x+1
x^4+x^3+x+1	x^7+x+1	x^3+x^2+x	x^3+x^2+x+1	1	x+1	$x^5+x^3+x^2+x+1$
1	x^3+x^2+x	x^3+x^2+x+1	1	x+1	$x^5+x^3+x^2+x+1$	$x^5+x^3+x^2$
x^3+x^2+x+1	x^3+x^2+x+1	1	0	$x^5+x^3+x^2+x+1$	$x^5+x^3+x^2$	0
	1	0		$x^5+x^3+x^2$	0	

=> $x^5+x^3+x^2$

4. 請計算在$GF(2^5)$下，(x^3+x+1)⊗(x^4+x^2)的結果，其中不可分解多項式為x^5+x^2+1。

P1⊗P2 = $x^3(x^4+x^2)$+x(x^4+x^2)+1(x^4+x^2)

P1⊗P2 = $x^7+x^5+x^5+x^3+x^4+x^2$

P1⊗P2 = $(x^7+x^4+x^3+x^2)$ mod (x^5+x^2+1) = x^3

5. 請找出多項 x^6+x^3+1 所代表的 7 位元字組

n = 7 => 階數=6

$1x^6+0x^5+0x^4+1x^3+0x^2+0x^1+1x^0$

⇨ 1001001