14). Verify properties required of a vector space: $p(x) = p_0 + p_1 x + \cdots + p_r x^r$, $q(x) = q_0 + q_1 x + \cdots + q_r x^r$, $p_i, q_i \in GF(2)$

1. $p(x) + q(x) = q(x) + p(x)$ Commutative
2. $ap(x) = 0$ if $a = 0$; $ap(x) = p(x)$ if $a = 1$
3. $a(p(x) + q(x)) = ap(x) + aq(x) \quad = p(x) + q(x) \quad$ if $a = 1$
   $\qquad\qquad\qquad\qquad\qquad\qquad\quad = 0 + 0 \qquad\quad$ if $a = 0$

   $$\begin{aligned}(a+b)p(x) &= ap(x) + bp(x)\\ &= 0 \text{ if } a = b = 0\\ &= p(x) \text{ if } a = 0, b = 1 \text{ or } b = 0, a = 1\\ &= p(x) + p(x) \text{ if } a = b = 1\end{aligned}$$

4. $$\begin{aligned}(a \cdot b)p(x) &= a \cdot (b \cdot p(x))\\ &= p(x) \text{ if } a = b = 1\\ &= 0 \text{ else}\end{aligned}$$
5. 1·p(x) = p(x)

Basis: Let basis $= \{1, x, x^2, \ldots, x^r\} \Rightarrow \text{Dim}\{v\} = r + 1$

28). $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5 \bmod 11, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6, 2^{10} = 1$

30).
a) irreducible, see class
b) $x^3 + x^2 + 1$, see class
c) reducible ($\div$ by $x^2 + x + 1$)
d) $x^4 + x^3 + x^2 + 1$
$\Rightarrow$ Not $\div$ by any polynomial of deg 1 because 0,1 are not roots
$\Rightarrow$ Not $\div$ by any polynomial of deg 3
$\Rightarrow$ Only potential polynomial of deg 2 is $x^2 + x + 1$
$\Rightarrow$ Irreducible, since not $\div$ by $x^2 + x + 1$
e) see d)
f) reducible, 1 is a root, $(x + 1)$ is factor of $x^5 + x^4 + x^3 + x^2 + x + 1$
g,h) Any factor of these must be of degree 3. Prove that this is not possible
$(x^3 + bx^2 + cx + 1)(x^3 + ex^2 + fx + 1) = x^6 + (e + b)x^5 + (f + be + c)x^4 + (bf + ce)x^3 + (b + e + cf)x^2 + (c + f)x + 1$
g) $x^6 + x^5 + x^2 + x + 1$
$5 \Rightarrow b + e = 1$
$4 \Rightarrow f + be + c = 0$
$3 \Rightarrow bf + ce = 0$
$2 \Rightarrow b + cf + e = 1$
$1 \Rightarrow c + f = 1$
There is no solution to equations $\Rightarrow$ irreducible
h) $x^6 + x^3 + 1$
$5 \Rightarrow b + e = 0$
$4 \Rightarrow f + be + c = 0$
$3 \Rightarrow bf + ce = 1$

$2 \Rightarrow b + cf + e = 0$
$1 \Rightarrow c + f = 0$
There is no solution to equations $\Rightarrow$ irreducible

7). GF(2): $\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}, \alpha^{64}, \alpha^{128}, \alpha^{256}, \alpha^{512}\}$
GF(4): (Now $q = 4$) $\{\alpha, \alpha^4, \alpha^{16}, \alpha^{64}, \alpha^{256}\}$
GF(32): ($q = 32$) $\{\alpha, \alpha^{32}\}$

9). Let α be root of $x^2 + 2x + 2 \Rightarrow \alpha^2 = \alpha + 1$
$0, 1, \alpha, \alpha^2 = \alpha + 1, \alpha^3 = 2\alpha + 1, \alpha^4 = \alpha, \alpha^5 = 2\alpha, \alpha^6 = 2\alpha + 2, \alpha^7 = \alpha + 2$

cyclotomic cosets		minimal polynomials
$\{0\}$	$\leftrightarrow$	$m_0(x) = (x + 2)$
$\{1, 3\}$	$\leftrightarrow$	$m_1(x) = (x + 2\alpha)(x + 2\alpha^3) = x^2 + 2x + 2$
$\{2, 6\}$	$\leftrightarrow$	$m_2(x) = (x + 2\alpha^2)(x + 2\alpha^6) = x^2 + 1$
$\{4\}$	$\leftrightarrow$	$m_4(x) = (x + 2\alpha^4) = x + 1$
$\{5, 7\}$	$\leftrightarrow$	$m_5(x) = (x + 2\alpha^5)(x + 2\alpha^7) = x^2 + x + 2$

12).
a) $x^3 + 1 = (x + 1)(x^2 + x + 1)$
b) $x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$
c) $x^7 + 1 = (x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)$
d) $x^{15} + 1 = (x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)$
e) $x^{21} + 1 = (x^6 + x^5 + x^4 + x^2 + 1)(x^6 + x^4 + x^2 + x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)(x^2 + x + 1)(x + 1)$
f) $x^{31} + 1 = (x^5 + x^4 + x^3 + x^2 + 1)(x^5 + x^4 + x^3 + x + 1)(x^5 + x^4 + x^2 + x + 1)(x^5 + x^3 + x^2 + x + 1)(x^5 + x^3 + 1)(x^5 + x^2 + 1)(x + 1)$

13).
a) $\{0\}, \{1, 2, 4, 8, 7, 5\}, \{3, 6\} \rightarrow 3$ polynomials in factorization of $x^9 + 1$
b) $\{0\}, \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\} \rightarrow 2$ polynomials
c) $\{0\}, \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\} \rightarrow 2$ polynomials
d) $\{0\}, \{1, 2, 4, 8, 16, 15, 13, 9\}, \{3, 6, 12, 7, 14, 11, 5, 10\} \rightarrow 3$ polynomials