$\alpha_3(a) = d$
$\alpha_3(b) = \alpha_3(a \cdot a) = \alpha_3(a) \cdot \alpha_3(a) = d \cdot d = a$
$\alpha_3(c) = \alpha_3(a \cdot b) = \alpha_3(a) \cdot \alpha_3(b) = d \cdot a = e$
$\alpha_3(d) = \alpha_3(a \cdot c) = \alpha_3(a) \cdot \alpha_3(c) = d \cdot e = b$
$\alpha_3(e) = \alpha_3(a \cdot d) = \alpha_3(a) \cdot \alpha_3(d) = d \cdot b = f$
$\alpha_3(f) = \alpha_3(e \cdot a) = \alpha_3(e) \cdot \alpha_3(a) = f \cdot d = c$
$\alpha_3(0) = 0$
$\alpha_3(1) = 1$

6/6

4) i) a) Normal field extension $\Leftrightarrow$ every irreducible polynomial over Z_2 with a zero in F_8 splits in F_8. But $F_8 = Z_2(a)$, and every element of Z_2 (except 0) is a power of a (or 0). Hence if an irreducible polynomial over Z_2 has a zero in F_8, it must be a power of a; in fact all its zeros must be powers of a, and the polynomial splits in F_8. Hence, extension normal. 6/6 Rem M 3.2 (HB p 35)

b) $m'(t) = t^3 + t^2 + 1$

My strategy is: a, b, d and c, e, f occupy separate cycles. The polynomial must have degree 3, since $Z_2(a) = Z_2(c)$.

$c^3 = \alpha^7 = b$

The polynomial becomes
$b + ? + 1 = f + ? = 0 \Rightarrow ? = f = c^2$
$\therefore c^3 + c^2 + 1 = 0$
$\Rightarrow t^3 + t^2 + 1 = m'(t)$ is minimum polynomial of c. [illegible] $m'(0) \neq 0$, $m'(1) \neq 0$

6/6

c) Irreducible polynomial splits in $F_8 \Rightarrow$ it has no of zeros equal to its degree. (=3)

$m(e) = e^3 + e^2 + 1 = ce + c + 1 = a + c + 1 = 0$
$m(f) = f^3 + f^2 + 1 = ef + e + 1 = d + e + 1 = 0$

2/2

ie c, e, f are 3 zeros of $m' \Rightarrow$ minimum polynomial of c splits in F_8.