P1 Como ~~m.c~~ $MCD(p, p^n-1) = 1$

$\Rightarrow [p] \in \mathbb{Z}_m^*$.

Por otro lado $p^n - 1 \equiv 0 \mod m$

$\Rightarrow [p^n] = [p]^n = 1$. Como n es el entero >0 más pequeño que cumple esto, $|\langle [p] \rangle| = n$

Lagrange $\Rightarrow n \mid |\mathbb{Z}_m^\times| = \varphi(m) = \varphi(p^n - 1)$ //

$R = \{ x : \exists n > 0 \text{ con } x^n = 0 \}$

$\Rightarrow (R,+)$ es subgrupo de $(A,+)$

$0 \in R \Rightarrow R \neq \emptyset$.

$R \subseteq A$ ✓

Sean $x, y \in R \Rightarrow \exists n, m > 0 : x^n = y^m = 0$.

$$\Rightarrow (x-y)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} x^{n+m-i} y^{i}$$

↑

R conmutativo.

SPG: ~~...~~ $n > m$

$$\Rightarrow \forall i = 0, \dots, m \quad x^{n+m-i} = (x^n)\, x^{\overbrace{m-i}^{\geq 0}} = 0 \cdot x^{m-i} = 0 \; //$$

$$\wedge \; \forall i = m+1, \dots, n \quad y^i = y^{m+k} = y^m \cdot y^k = 0 \; //$$

$\Rightarrow (x-y)^{m+n} = 0 \Rightarrow x - y \in R$ //

Además, $\forall a \in A \; \forall x \in R \quad (ax)^n = a^n x^n = a^n 0 = 0$ //

↑

conmut.

$\Longrightarrow R \trianglelefteq A$ //

Sea $x+R$ tal que $\exists n>0\ (x+R)^n = R$

R ideal $\Rightarrow (x+R)^n = x^n + R = R$

$\Rightarrow x^n \in R \Rightarrow \exists k$ tq $(x^n)^k = 0$

$\Rightarrow x \in R$ //

b) $R = \bigcap_{\substack{P \trianglelefteq A \\ \text{primos}}} P$

$\subseteq]$ Sea $x \in R \Rightarrow \exists n>0$ tq $x^n = 0 \in P \Rightarrow x \cdot x^{n-1} \in P$

$\Rightarrow x \in P \quad \vee \quad x^{n-1} \in P$

$\downarrow \qquad\qquad \downarrow$

Listo $\qquad$ inducción ✓

$\supseteq]$ Sea $x \notin R$. PDQ $\exists P \trianglelefteq A$ primo tal q $x \notin P$.

Sea $\Sigma = \{ I \trianglelefteq A : \forall n>0\ x^n \notin I \}$

$(0) = \{0\} \in \Sigma \Rightarrow \Sigma \neq \emptyset$.

Consideremos en $(\Sigma, \subseteq)$ una cadena I_i $i \in J$.

Luego $C_i \subseteq \sum_{i \in J} C_i$

además $x^n \notin \sum C_i \quad \forall n$ pues sino

$\exists j_1, \dots, j_k$ tq $x^n = c_{j_1} + \dots + c_{j_k}$ con

$c_{j_i} \in C_{j_i}$

Como C_i es cadena $c_{j_i} \in C_{\max_i j_i} \quad \forall i$

$\Rightarrow x^n \in C_{\max_i j_i}$ $\cancel{}$

$\overset{\text{Zorn}}{\Longrightarrow} \exists P$ ideal maximal en Σ.

Veamos que P es primo, ie,

$z \cdot y \in P \Rightarrow z \in P \lor y \in P$

$\Leftrightarrow z \notin P \land y \notin P \Longrightarrow zy \notin P$.

En efecto, $P \subsetneq P + (z)$
$P \subsetneq P + (y)$

Maximalidad en $P \Rightarrow \exists n, m$ tq $x^n \in P + (z)$
$x^m \in P + (y)$

$$\Rightarrow x^{n+m} \in (P+(z))\cdot(P+(y))$$

~~$\Rightarrow \exists p \in P \wedge a$~~

$\Rightarrow \exists p_1, p_2 \in P,\ a_1, a_2 \in A$

$$x^{n+m} = (p_1 + a_1 z)(p_2 + a_2 y)$$

$$= (\underbrace{p_1 p_2 + p_1 a_2 y + a_1 z p_2}_{\in P} + \underbrace{a_1 a_2 z y}_{\in (zy)})$$

$$\Rightarrow x^{n+m} \in P + (zy)$$

$$\Rightarrow zy \notin P \ //$$

$$\Rightarrow x^n \notin P \Rightarrow x \notin P \ //$$

c) $\mathcal{R} = \bigcap_{\substack{I \trianglelefteq A \\ \text{maximal}}} I$

$x \in \mathcal{R} \Leftrightarrow 1 - xy$ invertible $\forall y \in A$.

$\Rightarrow)$ $1-xy \notin A^{\times} \rightarrow (1-xy) \neq A$

$\Rightarrow \exists I^{*}$ maximal tq $(1-xy) \subseteq I^{*}$

Como $x \in \mathcal{R} = \bigcap_{I\,max} I \subseteq I^{*}$

$\Rightarrow \forall y \in A \quad xy \in I^{*} \quad (I^{*} \trianglelefteq A)$

$\Rightarrow 1 = \underbrace{(1-xy)}_{\in I^{*}} + \underbrace{xy}_{\in I^{*}} \in I^{*}$

$\Rightarrow I = A$ ↯ //

$\Leftarrow)$ $x \notin \mathcal{R} \Rightarrow \exists I^{*}$ maximal tq $x \notin I$

$I^{*} + (x) = A = (1)$

$\Rightarrow I^{*} \subsetneq I^{*} + (x) \underset{\text{maximalidad}}{\Rightarrow}$

$\Rightarrow \exists u \in I^{*}, r \in A$ tq

$u + rx = 1$

$\Rightarrow u = 1 - rx \in I^{*} \neq A$

$\Rightarrow \exists r \in A$ tq $1 - rx \in A^{*}$ //

[3] a) $f(x)\cdot f(y) = f(xy) \in J \Rightarrow f(x) \in J \vee f(y) \in J$
$\Rightarrow x \in J^c \vee y \in J^c$ //

b). $x \in I \Rightarrow f(x) \in I^e \Rightarrow x \in f^{-1}(\{f(x)\}) \subseteq I^{ec}$ //

$\cdot\ f(f^{-1}(J)) \subseteq J \Rightarrow (f(f^{-1}(J))) \subseteq (J) = J$ //

c) b) $\Rightarrow \underbrace{J^{ce}}_{(J^c)^e} \subseteq J \Rightarrow J^c \subseteq (J^c)^{ec} \subseteq (J^{ce})^c \subseteq J$ //

~~Reiterado~~

$I^{ec} \subseteq J^{ec} = (I^e)^c$

$\Rightarrow I^{ece} = (I^e)^{ce} \subseteq I^e$

$\Rightarrow I^e \subseteq I^{ece} \subseteq I^e$ //

d) $I \in C \Rightarrow \exists J$ tq

$I = J^c \Rightarrow I^{ec} = I^{cec} = I$ //

y si $I = I^{ec} \Rightarrow I = J^c$ con $J = I^e$ //

Análogo para E //

$f(I) = I^e$

$g(J) = J^c$

$\Rightarrow g \circ f(I) = g(I^e) = I^{ec} = I$ //

$f \circ g(J) = f(J^c) = J^{ce} = J$ //

$\Rightarrow$ f biyectiva con inversa g //,