Corrigé.

Ex1 1) $\Rightarrow$ Soit I maximal et $\bar{x} \neq 0$ dans A/I.
$\bar{x}$ est la classe d'un élément $x \in A \setminus I$.
L'idéal $J = I + (x) \supsetneq I$ (car $x \notin I$) donc par maximalité de I, $J = A$. En particulier, il existe $i \in I$ et $y \in A$ tel que $1 = i + xy$. Mais alors dans A/I : $1 = \overline{i+xy} = \bar{x}y = \bar{x}\bar{y}$.
D'où $\bar{x}$ est inversible. Ainsi A/I est un corps.

$\Leftarrow$ Réciproquement, Soit $I \subsetneq J$ des idéaux de A. Soit $x \in J \setminus I$. Dans A/I, $\bar{x} \neq 0$ et donc il existe $y \in A$ tq $\bar{x}\bar{y} = \bar{1}$. Il existe $i \in I$ tq $xy = 1 + i$, mais alors $1 = \underbrace{xy}_{\in J} - \underbrace{i}_{\in I \subset J} \in J$. D'où $J = A$.

2) Soit d un diviseur commun à α et β. Il existe $\alpha', \beta' \in \mathbb{Z}[i]$ tq $\alpha = d\alpha'$, $\beta = d\beta'$. Ainsi $N(\alpha) = N(d)N(\alpha')$ et $N(\beta) = N(d)N(\beta')$

$N(d)$ est un diviseur commun à $N(\alpha)$ et $N(\beta)$ et donc d'après l'hypothèse $N(\alpha) \wedge N(\beta) = 1$, on a $N(d) = 1$.
Mais alors d est bien inversible.

ii) Réciproquement, c'est Faux. $5 = (1+2i)(1-2i)$ est une factorisation $\neq$. $1+2i$ et $1-2i$ sont tous deux de même norme (5) mais ils sont premiers entre eux.

3) i) On calcule $\left(\frac{22}{43}\right) = \left(\frac{2}{43}\right)\left(\frac{11}{43}\right)$

$\left(\frac{2}{43}\right) = (-1)^{\frac{43^2-1}{8}} = -1$ d'après la LRQ.

$\left(\frac{11}{43}\right) = (-1)^{\frac{11-1}{2}\frac{43-1}{2}} \left(\frac{43}{11}\right) = -\left(\frac{-10}{11}\right) = -(-1)^{\frac{11-1}{2}} = 1$.

D'où $\left(\frac{22}{43}\right) = -1$. Donc 22 n'est pas un carré dans $\mathbb{Z}/43\mathbb{Z}$.

ii) $33 = 3 \times 11$ avec $3 \wedge 11 = 1$.
17 est un carré dans $\mathbb{Z}/33\mathbb{Z}$ ssi il est un carré dans $\mathbb{Z}/3\mathbb{Z}$ et dans $\mathbb{Z}/11\mathbb{Z}$.
$17 \equiv -1 [3]$ et -1 n'est pas un carré mod 3
Donc 17 n'est pas un carré dans $\mathbb{Z}/33\mathbb{Z}$.

Ex2. 1) $\mathbb{F}_p[X]/(Q)$ est un $\mathbb{F}_p$-ev de base $1, X, \dots, X^{\deg(Q)-1}$ et il admet donc $p^{\deg(Q)} = |Q|$ éléments.
En effet, si $P \in \mathbb{F}_p(X)$, en notant $P = AQ + R$ la div euclidienne de P par Q, avec $\deg(R) < \deg(Q)$, on a $\overline{P} = \overline{R}$ d'où $\overline{P} \in \mathrm{Vect}(1, \dots, X^{\deg(Q)-1})$.
De plus, $(1, \dots X^{\deg(Q)-1})$ est libre car si $a_0, \dots, a_{d-1}$ sont des scalaires tq $\overline{a_0 + \dots + a_{d-1}X^{d-1}} = \bar{0}$ on aurait $Q \mid (a_0 + \dots + a_{d-1}X^{d-1})$ et en comparant les degrés $a_0 + \dots + a_{d-1}X^{d-1} = 0$
D'où $a_0 = \dots = a_{d-1} = 0$.

2) i) $\Rightarrow$ ii) Si $A/(Q)$ est un corps il est intègre.
Or, si Q n'était pas irréductible, disons $Q = Q_1 Q_2$ avec $\deg(Q_1)$ et $\deg(Q_2) < \deg(Q)$, on aurait $\overline{Q_1} \neq 0 \neq \overline{Q_2}$ et $\overline{Q_1 Q_2} = \overline{Q} = 0$

(ii)⇒(i) Soit $\bar{P} \in A/(Q)$ tq $\bar{P} \neq 0$. Alors $Q \nmid P$ dans $\mathbb{F}_p(X)$.
et comme Q est irréductible, $\gcd(Q,P) = 1$.
Par Bezout, il existe $U, V \in \mathbb{F}_p(X)$, $UQ + VP = 1$ dans $\mathbb{F}_p(X)$
D'où $\bar{V}\bar{P} = 1$ dans $A/(Q)$.

3) De même, $\bar{P} \in A/(Q^\alpha)$ est inversible ssi $P \wedge Q^\alpha = 1$
ie ssi $P \wedge Q = 1$ (Q est irréductible).
$(A/(Q^\alpha))^\times$ est donc le complémentaire dans $A/(Q^\alpha)$ des
classes des multiples de Q, soit les $\overline{QA}$ avec
$A \in \mathbb{F}_p(X)$, $\deg(QA) < \deg(Q^\alpha)$ ie $\deg(A) < \deg(Q)(\alpha-1)$.
On a donc $\Phi(Q^\alpha) = p^{\alpha d} - p^{d(\alpha-1)} = |Q|^{\alpha-1}(|Q|-1)$

4) Si Q_1 et Q_2 sont premiers entre eux, est un
$$A/(Q_1Q_2) \longrightarrow A/(Q_1) \times A/(Q_2)$$
$$P \longmapsto (\bar{P}[Q_1], \bar{P}[Q_2])$$
isomorphisme d'anneaux (th chinois).

D'où un isomorphisme de groupes :
$$(A/(Q_1Q_2))^\times \simeq (A/(Q_1) \times A/(Q_2))^\times \simeq (A/(Q_1))^\times \times (A/(Q_2))^\times$$
et donc $\Phi(Q_1Q_2) \simeq \Phi(Q_1) \cdot \Phi(Q_2)$.

5) On en déduit donc la formule :
Si $Q = u Q_1^{\alpha_1} \cdots Q_r^{\alpha_r}$ est la décomp de Q en prod de
facteurs irréductibles, $\Phi(Q) = \prod_{i=1}^{r} |Q_i|^{\alpha_i - 1}(|Q_i|-1)$

6) $(A/Q)^\times$ est de cardinal $|Q|-1 = p^d - 1$ où $d = \deg Q$.
Soient $d_1 | \cdots | d_r$ ses facteurs invariants : $(A/Q)^\times \simeq \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_r$.
Comme $d_1 | \cdots | d_r$, tous les éléments de $(A/Q)^\times$ sont d'ordre divisant d_r,
soit $\forall \bar{P} \in (A/Q)^\times$, $P^{d_r} = 1$ ($\in \mathbb{F}(X)$)
Ainsi le polynôme $X^{d_r} - 1$ aurait $|Q|-1$ racines dans $\mathbb{F}(= A/(Q))$
Comme $|Q|-1 = d_1 \cdots d_r$ et qu'un polynôme ($\neq \mathbb{F}(X)$) a au plus autant
de racines que son degré, on en déduit $r = 1$ et $d_r = |Q|-1$.
D'où $(A/Q)^\times$ est cyclique.

7) Via l'isomorphisme $(A/Q)^\times \simeq \mathbb{Z}/(|Q|-1)$,
le sous-groupe des cubes est envoyé sur le sous-groupe $\langle 3 \rangle$
ce sous-groupe est → tout $\mathbb{Z}/(|Q|-1)$ si $3 \wedge (|Q|-1) = 1$.
→ le seul sous-groupe de cardinal $\frac{|Q|-1}{3}$ si $|Q| \equiv 1 (3)$.

Réponse : il y a → $|Q|-1$ cubes si $|Q| \not\equiv 1 (3)$
→ $\frac{|Q|-1}{3}$ cubes si $|Q| \equiv 1 (3)$.

8) le morphisme (d'anneaux) de réduction :
$\tilde{\rho} : A/(Q^\alpha) \to A/(Q)$ induit un morphisme de
groupes : $\rho : (A/Q^\alpha)^\times \to (A/Q)^\times$.
Ce morphisme est surjectif : pour $\bar{P} \in (A/Q)^\times$ avec $\deg P < d-1$,
on a $\rho(\bar{P}) = \bar{P}$!
et $\bar{P}$ est bien inversible dans A/Q^α : $P \wedge Q = 1 \Leftrightarrow P \wedge Q^\alpha = 1$.

Ainsi il existe $R \in (A/Q^\alpha)^\times$ tq $\rho(R)$ soit un générateur
de $(A/Q)^\times$.

L'ordre de R dans $(A/\mathfrak{Q}^\alpha)^\times$ est alors un multiple de $|\mathfrak{Q}|-1$, disons $k(|\mathfrak{Q}|-1)$

(car si $R^\ell = 1$ dans $(A/\mathfrak{Q}^\alpha)^\times$, $\rho(R^\ell) = \rho(R)^\ell = 1$ dans $A/\mathfrak{P}$ et donc $|\mathfrak{Q}|-1 \mid \ell$.)

Alors R^k est d'ordre $(|\mathfrak{Q}|-1)$.

9) Montrons que $\varphi : \Gamma \times \mathbb{Z}/(|\mathfrak{Q}|-1) \longrightarrow A/\mathfrak{Q}^\alpha)^\times$ est un isomorphisme $(\gamma, r) \mapsto \gamma . R^r$ de groupes

Par construction, $|\Gamma| = |\mathfrak{Q}|^{d-1}$ donc les groupes ont même cardinal et il suffit de montrer que φ est injectif. Or si $\gamma . R^r = 1$, alors $\gamma = R^{-r}$ est un élément de $\langle R \rangle \cap \Gamma$.
Comme $|\langle R \rangle| = |\mathfrak{Q}|-1$ et $|\Gamma| = |\mathfrak{Q}|^{d-1}$ sont premiers entre eux, $\langle R \rangle \cap \Gamma = \{1\}$ d'où $R^r = 1$ et $\gamma = 1$.

10) Soit $\gamma \in \Gamma$, on a $\gamma = \overline{1 + \mathfrak{Q}B}$ pour un certain $B \in A$ par définition de Γ.
Alors $\gamma^{p^b} = (1 + \mathfrak{Q}B)^{p^b} \equiv 1 + (\mathfrak{Q}B)^{p^b}$
car A est de caractéristique p donc $(a+b)^p = a^p + b^p$.
Comme $p^b \geq \alpha$, $(\mathfrak{Q}B)^{p^b} \equiv 0 \ [\mathfrak{Q}^\alpha]$.
Comme $(1+\mathfrak{Q})^{p^{b-1}} \neq 0$, p^b est l'exposant de Γ.

11) Si $\alpha = 2$ et $d = 1$ on a $f = 1$. Tous les éléments de Γ sont d'ordre $\leq p$ et comme $d = \deg(\mathfrak{Q}) = 1$, $|\Gamma| = p$. $\Gamma \simeq \mathbb{Z}/p\mathbb{Z}$.

$$(A/\mathfrak{Q}^2)^\times \simeq \mathbb{Z}/p-1 \times \mathbb{Z}/p \overset{\simeq}{\uparrow} \mathbb{Z}/(p(p-1))\mathbb{Z}.$$
th chinois

~~Réciproquement~~,
De plus si $p=2$, $\alpha = 3$ et $d = 1$, alors $f = 2$
$(A/\mathfrak{Q}^\alpha)^\times \simeq \left(\mathbb{Z}_2[X]/X^3\right)^\times_{\simeq \Gamma}$ est un groupe d'ordre 4.
et d'exposant $2^b = 4$. Donc c'est $\mathbb{Z}/4\mathbb{Z}$.

Si $(A/\mathfrak{Q}^\alpha)^\times$ est cyclique, alors Γ doit être cyclique, En particulier, son exposant doit être son ordre, d'où $p^b = p^{(\alpha-1)d}$ ie $f = (\alpha-1)d$.
On constate que les seules solutions de cette équation sont :
$\alpha = 1$, d quelconque
$\alpha = 2$, $d = 1$.
$\alpha = 3$, $d = 1$ si $p = 2$.
C'est pénible à écrire bien ...