Opgave 1.
(a) Neem $x - y \in I$. Aangezien $I = I_1 I_2 \subset I_1$, deduceren we $x - y \in I_1$ en evenzo $x - y \in I_2$. Derhalve $\phi(\overline{x}) = \phi(\overline{y})$ (**1/4 punt**). Vanwege de definitie van optelling op het codomein krijgen we (**1/2 punt**)

$$\phi(\overline{x} + \overline{y}) = \phi(\overline{x+y}) = (\overline{x+y}, \overline{x+y}) = (\overline{x} + \overline{y}, \overline{x} + \overline{y}) = (\overline{x}, \overline{x}) + (\overline{y}, \overline{y}) = \phi(\overline{x}) + \phi(\overline{y})$$

en evenzo voor vermenigvuldiging.
(b) Neem $x, y \in R$, dan $x - y = i_1 + i_2$ voor $i_1 \in I_1$, $i_2 \in I_2$. Derhalve $-i_1 \in I_1$ en (**3/4 punt**)

$$\phi(\overline{x - i_1}) = (\overline{x - i_1}, \overline{x - i_1}) = (\overline{x - i_1}, \overline{y + i_2}) = (\overline{x}, \overline{y}).$$

(c) Het voldoet aan te tonen dat $\ker \phi = \{0\}$ (**1/4 punt**). Stel $x \in I_1 \cap I_2$. Het voldoet aan te tonen dat $x \in I_1 I_2 = I$ (**1/4 punt**). Omdat $1 = i_1 + i_2$, hebben we $x = i_1 x + i_2 x \in I_1 I_2 = I$ (**1/2 punt**).

Opgave 2.
(a) $F(y)$ is een lichaam en dus heeft $F(y)[x]$ een Euclidisch algoritme (feit uit hcs/boek, **1/2 punt**). Omdat $h(x) := f(x) - f(y) \in F[x, y] \subset F(y)[x]$ en $h(y) = 0$ voor $y \in F(y)$, volgt uit de factorstelling (opgave wc of eenvoudig gevolg Euclidisch algoritme) dat er een $q(x) \in F(y)[x]$ is zodat $h(x) = q(x)(x - y)$ (**1/2 punt**). Het resultaat volgt. De term $c(x, y)$ expliciet berekenen mag ook.
(b) Opnieuw geeft de factorstelling $f(y) = (y - \alpha)q(y)$ voor een $q(y) \in F[y]$ (**1/4 punt**). Bovendien is α een wortel met multipliciteit 1, omdat $f'(\alpha) \neq 0$. Dus komt de irreducibele term $y - \alpha$ maar een keer voor in de priemontbinding van $f(y)$ (**1/4 punt**). Aangezien $F[y]$ een UFD is (feit hc/boek, **1/4 punt**), volgt het resultaat uit Eisenstein met priem $y - \alpha$ (**1/2 punt**).
(c) Neen. Voorbeeld: $F = \mathbb{F}_3$, dan $x^3 + y^3 + 1 = (x + y + 1)^3$ is reducibel (**1/2 punt**).

Opgave 3. Vanwege de hint willen we van $f(x)$ de term x^2+1 afsplitsen. Dit geeft $f(x) = (x^2+1)(x^2+x+1)$ (**1/4 punt**). De factor x^2+1 heeft wortels $-i, i$. Verder is x^2+x+1 de tweede cyclotome veelterm en heeft dus wortels ω, ω^2, waar $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+i\sqrt{3}}{2}$ (feit uit hcs/boek/wcs, of d.m.v. korte berekening met $\frac{x^3-1}{x-1} = x^2+x+1$). De veelterm $f(x)$ heeft dus $E := \mathbb{Q}(i,\omega)$ als splijtlichaam over $\mathbb{Q}$ (**1/4 punt**). We kunnen schrijven $E = \mathbb{Q}(i,\sqrt{3})$. Omdat $\sqrt{3}+i \neq \sqrt{3}-i, -\sqrt{3}-i$, vinden we dat $i+\sqrt{3}$ een primitief element is (bewijs stelling van het primitieve element, **1/4 punt**). (Andere primitieve elementen zijn uiteraard mogelijk.) We kunnen schrijven $E = \mathbb{Q}(i,\sqrt{3}) \supset \mathbb{Q}(\sqrt{3}) \supset \mathbb{Q}$. Omdat $m_{\sqrt{3}/\mathbb{Q}} = x^2-3$ (Eisenstein) en $m_{i/\mathbb{Q}(\sqrt{3})} = x^2+1$ ($i \notin \mathbb{Q}(\sqrt{3})$ want imaginair), deduceren we (**1/2 punt**)

$$[E:\mathbb{Q}] = [E:\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}] = 2\times 2 = 4.$$

Zij $\sigma \in G := \mathrm{Gal}(f/\mathbb{Q})$, dan stuurt σ de wortels $\sqrt{3}, i$ naar $\mathbb{Q}$-geconjugeerden $\pm\sqrt{3}$, $\pm i$. Dit geeft vier mogelijkheden. Aangezien $|G| = 4$, definiëren alle vier de mogelijkheden inderdaad elementen van G (**1/4 punt**). Zij $\sigma : \sqrt{3} \mapsto -\sqrt{3}, i \mapsto i$, $\tau : \sqrt{3} \mapsto \sqrt{3}, i \mapsto -i$. Dan $G = \{1, \sigma, \tau, \sigma\tau\}$ met relaties $\sigma^2 = \tau^2 = 1$ en $\sigma\tau = \tau\sigma$, dus $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (**1/2 punt**). De deelgroepen hiervan zijn $\mathbb{Z}_2 \times \{0\}$, $\{0\} \times \mathbb{Z}_2$ en $\Delta = \{(0,0),(1,1)\} \cong \mathbb{Z}_2$ (**1/4 punt**). De bijbehorende fixlichamen zijn $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{3})$ en $\mathbb{Q}(\omega)$ (zo evident dat geen verdere berekening gevraagd wordt **1/4 punt**).

Opgave 4.
(a) Stel α, β zijn verschillende wortels van $f(x)$ in een splijtlichaam E/F. Hier is E dus een eindig lichaam. Omdat α, β F-geconjugeerd zijn, zijn $F(\alpha), F(\beta)$ F-isomorfe deellichamen van E (**1/4 punt**). Maar voor iedere mogelijke orde van een deellichaam van E is er maar 1 deelichaam van die orde (feit hc/boek) en dus $F(\alpha) = F(\beta)$ (**1/4 punt**). Derhalve splijt f over $F(\alpha)$ (β was willekeurig gekozen).
(b) Zij K het splijtlichaam van $x^{q^n} - x$, i.e. het lichaam met q^n elementen. Omdat $f \mid x^{q^n} - x$, hebben we dat het splijtlichaam $F(\alpha)$ van f over F (onderdeel (a)) bevat is in K (**1/4 punt**). We deduceren $n = [K:F] = [K:F(\alpha)][F(\alpha):F] = [K:F(\alpha)]m$ (**1/2 punt**).
(c) Gebruik de notatie van voorgaande onderdelen. Stel $m \mid n$, dan geldt voor het lichaam L van q^m elementen dat $F \subset L \subset K$ (**1/4 punt**, feit hc/boek). Het splijtlichaam van f heeft ook precies q^m elementen (onderdeel (a)). We zien dus dat L en $F(\alpha)$ F-isomorf zijn (hint). Derhalve splijt f over L (**1/4 punt**). Voorts is E het splijtlichaam van $x^{q^n} - x$ en dus $f \mid x^{q^n} - x$, want f is separabel (opgave wc, **1/4 punt**).
(d) Ten eerste is $f(x)$ reducibel over F, want anders bevat haar splijtlichaam $(p^{p_1})^{p_1 p_2}$ elementen, maar we weten dat het splijtlichaam E van $f(x)$ over $\mathbb{F}_p$ slechts $p^{p_1 p_2}$ elementen bevat (onderdeel (a)). Omdat $f(x)$ separabel is (opgave wc), is $f(x) = f_1(x)\cdots f_N(x)$ voor *verschillende* irreducibele $f_i(x) \in F[x]$ (**1/4 punt**). We passen (b), (c) toe met $q = p^{p_1}$, irreducibele veelterm $f_i(x) \in F[x]$, $m = \deg(f_i)$ en $n = p_2$. Omdat $f_i(x)$ splijt over E, hebben we $\deg(f_i) \mid p_2$. Voorts heeft $f(x)$ geen nulpunten over F (anders splijt $f(x)$ al over F, onderdeel (a)) en dus $\deg(f_i) = p_2$ en $N = p_1$ (**1/4 punt**).