Corrigé

Exercice 1

a) $\Rightarrow$ si n n'est pas premier, $n = ab$ avec $1 \leq a < n$, $1 \leq b < n$ et $\bar{a} \cdot \bar{b} = \bar{0}$ dans $\mathbb{Z}/n\mathbb{Z}$, mais $\bar{a} \neq 0 \neq \bar{b}$ dans $\mathbb{Z}/n\mathbb{Z}$, donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre, donc pas un corps.

$\Leftarrow$ Supposons n premier. Pour $\bar{a} \neq 0$ dans $\mathbb{Z}/n\mathbb{Z}$, $n \nmid a$ et comme n est premier, $n \wedge a = 1$. Il existe donc une relation de Bézout $au + nv = 1$ dans $\mathbb{Z}$. En réduisant modulo n, on obtient $\bar{a} \cdot \bar{u} = \bar{1}$ et $\bar{a}$ est bien inversible.

b) Par le théorème chinois : $\chi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$\bar{a} \longmapsto (\bar{a}_m, \bar{a}_n)$

est un isomorphisme d'anneaux.

En particulier, χ envoie un carré sur un carré ($\chi(a^2) = \chi(a)^2$).

De même, l'isomorphisme inverse envoie un carré sur un carré, donc χ établit un isomorphisme entre les carrés de $\mathbb{Z}/mn\mathbb{Z}$ et les carrés de l'anneau produit $(\mathbb{Z}/m \times \mathbb{Z}/n)$. Un élément de cet anneau est un carré ssi chaque composante en est un. Ainsi, on a $\bar{a} \in \mathbb{Z}/mn\mathbb{Z}$ carré ssi $\bar{a}_m \in \mathbb{Z}/m\mathbb{Z}$ et $\bar{a}_n \in \mathbb{Z}/n\mathbb{Z}$ carrés

c) On calcule le pgcd entre 2 et $5+i$ dans $\mathbb{Z}[i]$ par l'algorithme d'Euclide : $5+i = 2 \times 2 + (1+i)$; $2 = (1+i)(1-i)$.

Ainsi $\text{pgcd}(5+i, 2) = (1+i)$ et $I = (1+i)$.

$$\mathbb{Z}[i]/I = \mathbb{Z}[i]/(1+i) \simeq \mathbb{Z}[X]/(X^2+1, 1+X) \cong \left(\mathbb{Z}[X]/(1+X)\right)/(1+\bar{X}^2).$$

Or $\mathbb{Z}[X]/(1+X) \simeq \mathbb{Z}$, $X \longmapsto -1$.

Ainsi $\mathbb{Z}[i]/I \simeq \mathbb{Z}/(1+(-1)^2) = \mathbb{Z}/2\mathbb{Z}$.

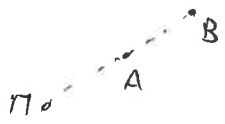
d) Si k est un corps, les polynômes de degré 1 de $k[X]$ sont irréductibles.

Soit P un pol de deg > 1 de $\mathbb{R}[X]$ qui est irréductible. P n'a aucune racine dans $\mathbb{R}$. Comme $\mathbb{C}$ est alg clos, P est scindé sur $\mathbb{C}$ et sa décomposition en irréductibles dans $\mathbb{C}[X]$ est $\lambda \prod_{i=1}^{n} (X - \alpha_i)$, α_i les racines dans $\mathbb{C} \setminus \mathbb{R}$.

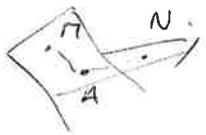
Or, puisque $P \in \mathbb{R}[X]$, $P(\alpha_1)=0 \Rightarrow P(\overline{\alpha_1})=0$. Donc $(X-\alpha_1)(X-\overline{\alpha_1})$ divise P.
(car $\alpha_1 \notin \mathbb{R}$ donc $\overline{\alpha_1} \neq \alpha_1$). Comme $(X-\alpha_1)(X-\overline{\alpha_1}) = X^2 - (\alpha_1+\overline{\alpha_1}) + |\alpha_1|^2 \in \mathbb{R}[X]$,
et que P est irréductible, on a nécessairement $\deg P = 2$ et $P = \lambda(X-\alpha_1)(X-\overline{\alpha_1})$.
Ainsi les irréductibles de $\mathbb{R}[X]$ sont les pol de deg 1 et les pol de deg 2 de discriminant < 0.

e) On a $P = 3(X^5 + 15X^3 + 5)$ dans $\mathbb{Z}[X]$ donc P n'est pas irréd dans cet anneau.
Par contre $3 \in \mathbb{Q}^\times$, et par le critère d'Eisenstein pour $p=5$, X^5+15X^3+5 est irréductible dans $\mathbb{Q}[X]$ et par conséquent P aussi.

b) On a $\overrightarrow{s_A \circ s_B} = \vec{s_A} \circ \vec{s_B} = (-\mathrm{id}) \circ (-\mathrm{id}) = \mathrm{id}$.
$s_A \circ s_B$ est donc une translation.
Notons $M = s_A(B)$, ainsi $\overrightarrow{BM} = 2\overrightarrow{BA}$
Comme $s_A \circ s_B(B) = s_A(B) = M = B + \overrightarrow{BM} = B + 2\overrightarrow{BA}$, $s_A \circ s_B$ est donc la translation de vecteur $2\overrightarrow{BA}$.



g) $\Rightarrow$ Soit $A \in F \cap G$ et $M \in F$, $N \in G$.
Alors $\overrightarrow{MN} = \underbrace{\overrightarrow{MA}}_{\in F \text{ car } M,A \in F} + \underbrace{\overrightarrow{AN}}_{\in G \text{ car } N,A \in G}$. Ainsi $\overrightarrow{MN} \in F+G$.



$\Leftarrow$ Réciproquement, soit $M \in F$ et $N \in G$. Décomposons $\overrightarrow{MN} = \vec{u} + \vec{v}$ avec $\vec{u} \in F$ et $\vec{v} \in G$. Posons $A = \underbrace{M+\vec{u}}_{\in F \text{ car } M \in F \text{ et } \vec{u} \in F} = \underbrace{N-\vec{v}}_{\in G \text{ car } N \in G \text{ et } \vec{v} \in G}$.
Ainsi $A \in F \cap G$ et $F \cap G$ est donc non vide.

ii) Si $F \oplus G = E$, d'après i), $F \cap G$ est non vide.
Soient $A, B \in F \cap G$. Alors $\overrightarrow{AB} \in F \cap G$. et donc $\overrightarrow{AB} = \vec{0}$.
D'où $A = B$. Ainsi $F \cap G$ est réduit à un point.

Exercice 2 : a) Puisque $\mathbb{F}_q$ est de caractéristique p, pour tous $\alpha, \beta \in \mathbb{F}_q$.

$$Tr(\alpha+\beta) = \sum_{i=0}^{n-1} (\alpha+\beta)^{p^i} = \sum_{i=0}^{n-1} \alpha^{p^i} + \beta^{p^i} = Tr(\alpha) + Tr(\beta).$$

$\forall \lambda \in \mathbb{Z}/p$, $\lambda^p = \lambda$ et donc $\forall i \geq 1$, $\lambda^{p^i} = \lambda$. Ainsi $Tr(\lambda\alpha) = \sum_{i=0}^{n-1} (\lambda\alpha)^{p^i} = \sum_{i=0}^{n-1} \lambda^{p^i}\alpha^{p^i} = \sum_{i=0}^{n-1} \lambda\alpha^{p^i}$
$= \lambda Tr(\alpha)$.

Donc Tr est bien une ~~forme~~ application linéaire.

Montrons que son image est bien contenue dans $\mathbb{Z}/p = \mathbb{F}_p \subset \mathbb{F}_q$.
$\mathbb{F}_p$ est le sous-ensemble des éléments $x \in \mathbb{F}_q$ tq $x^p = x$.

Or, $Tr(\alpha)^p = \left(\sum_{i=0}^{n-1} \alpha^{p^i}\right)^p = \sum_{i=1}^{n} \alpha^{p^i}$

Or, dans $\mathbb{F}_q$, $\alpha^{p^n} = \alpha$. Et donc $Tr(\alpha)^p = Tr(\alpha)$ et donc $Tr(\alpha) \in \mathbb{F}_p$.

b) L'application Tr est polynomiale, de degré p^{n-1}, à coefficients dans $\mathbb{F}_q$.
~~Cette application~~ Le polynôme $\sum_{i=0}^{n-1} X^{p^i}$ admet au plus p^{n-1} racines dans $\mathbb{F}_q$, qui est de cardinal p^n.
Il existe donc $\alpha \in \mathbb{F}_q$ tq $Tr(\alpha) \neq 0$.

c) $\Leftarrow$ Si α est de la forme $\beta^p - \beta$, alors $Tr(\alpha) = Tr(\beta^p - \beta) = Tr(\beta)^p - Tr(\beta)$
$= 0$

$\Rightarrow$ $\begin{array}{l}\mathbb{F}_q \to \mathbb{F}_q \\ \beta \mapsto \beta^p - \beta\end{array}$ est une application linéaire, de noyau $\mathbb{F}_p$.

Par le th du rang, l'image de cette application est un $\mathbb{Z}/p$-ev de dim $n-1$, contenu dans le noyau de Tr, lui aussi un $\mathbb{Z}/p$-ev de dim $n-1$ car $Tr \neq 0$.
Par égalité des dimensions, on a égalité entre ces espaces vectoriels.

Exercice 3 : a) $\Phi_n(X) = \prod_{\xi \in \mu_n^X} (X - \xi)$, où μ_n^X est l'ens des racines $n$ème primitives de 1.

Car a $\prod_{d|n} \Phi_d = X^n - 1$, et on montre par récurrence que $\Phi_n \in \mathbb{Z}[X]$ $\forall n$.
et Φ_n est unitaire.

Pour $n = 1$, $\Phi_1 = X - 1$.
Supposons l'avoir déjà montré jusqu'au rang n, alors
$\Phi_{n+1} = \prod_{\substack{d|(n+1) \\ d \neq n+1}} \frac{X^{n+1} - 1}{\Phi_d}$. Ce quotient reste dans $\mathbb{Z}[X]$ et unitaire car le dénominateur est unitaire dans $\mathbb{Z}[X]$ par hyp. de récurrence.

b) On a $\phi_1(X) = X-1$ Donc $\phi_1\left(\frac{1}{X}\right) = \frac{1}{X} - 1 = \frac{1}{X}(1-X) = \frac{1}{X}\left(-\phi_1(X)\right) = -\frac{1}{X}\phi_1(X)$.

Montrons que pour $n \geq 2$. $\phi_n\left(\frac{1}{X}\right) = \frac{1}{X^{\varphi(n)}}\phi_n(X)$.

Pour $n=2$, $\phi_2(X) = 1+X$ donc c'est vrai.

Supposons l'assertion vérifiée jusqu'au rang n.

$\prod_{d \mid n+1} \phi_d = X^n - 1$. D'où, $\prod_{d \mid n+1} \phi_d\left(\frac{1}{X}\right) = \frac{1}{X^{n+1}} - 1 = -\frac{1}{X^n}\left(X^{n+1}-1\right) = -\frac{1}{X^{\varphi(n+1)}} \prod_{d \mid n+1} \phi_d(X)$.

$$= -\prod_{d \mid n+1} \frac{1}{X^{\varphi(d)}} \phi_d(X).$$

En simplifiant par $\prod_{\substack{d \mid n+1 \\ d \neq n+1}} \phi_d\left(\frac{1}{X}\right)$ qui vaut par hyp de réc $-\prod_{\substack{d \mid n+1 \\ d \neq n+1}} \frac{1}{X^{\varphi(d)}} \phi_d(X)$,

il reste $\phi_{n+1}\left(\frac{1}{X}\right) = \frac{1}{X^{\varphi(n+1)}} \phi_{n+1}(X)$.

Les coefficients a_k vérifient donc $a_{\varphi(n)-k} = a_k$. $\forall\, 0 \leq k \leq \varphi(n)$.

c) Comme Φ_n annule $e^{2i\pi/n}$ et est irréductible sur $\mathbb{Q}$, on a $\left[\mathbb{Q}(e^{2i\pi/n}) : \mathbb{Q}\right] = \varphi(n)$.

d) Montrons que $\left[\mathbb{Q}[e^{2i\pi/n}) : \mathbb{Q}(\cos(2\pi/n)\right] \leq 2$.

On a $2\cos(2\pi/n) = e^{2i\pi/n} + \frac{1}{e^{2i\pi/n}}$. Donc $e^{2i\pi/n}$ est annulé par.

$X^2 - 2\cos(2\pi/n)X + 1 \in \mathbb{Q}(\cos(\frac{2\pi}{n}))[X]$.

Comme $\mathbb{Q}(\cos(\frac{2\pi}{n})) \subset \mathbb{R}$ et $\mathbb{Q}(e^{2i\pi/n}) \not\subset \mathbb{R}$ si $n>2$, ces corps sont distincts et on a $\left[\mathbb{Q}(e^{2i\pi/n}) : \mathbb{Q}(\cos(\frac{2\pi}{n}))\right] = 2$.

e) Par le lemme de la base télescopique, on a $\left[\mathbb{Q}(\cos(\frac{2\pi}{n})) : \mathbb{Q}\right] = \frac{\varphi(n)}{2}$

Pour $n>2$, $\phi_n = X^{\frac{\varphi(n)}{2}}\left(\sum_{k=0}^{\varphi(\frac{n}{2})-1} a_k + a_{\varphi(\frac{n}{2})} + \sum_{\ell=1}^{\varphi(n)/2} a_{\varphi(\frac{n}{2})+\ell} X^\ell\right)$

$$= X^{\frac{\varphi(n)}{2}}\left(\underbrace{\sum_{\ell=0}^{\varphi(\frac{n}{2})} a_{\varphi(\frac{n}{2})+\ell}\left(X^\ell + \frac{1}{X^\ell}\right) + a_{\varphi(\frac{n}{2})}}_{=: \psi_n}\right).$$

Ψ_n est un polynôme unitaire, dans $\mathbb{Z}[X]$, annulant $2\cos\left(\frac{2\pi}{n}\right)$
Comme il est de degré $\varphi\left(\frac{n}{2}\right)$, c'est son polynôme minimal.

b) Comme Ψ_n est unitaire dans $\mathbb{Z}[X]$, ses racines rationnelles sont en fait entières.

Ainsi, si $2\cos\left(\frac{2\pi}{n}\right) \in \mathbb{Q}$, $2\cos\left(\frac{2\pi}{n}\right) \in \mathbb{Z}$.

Cela laisse comme valeurs possibles pour $\cos\left(\frac{2\pi}{n}\right)$: $0, \pm 1, \pm \frac{1}{2}$.

Ces valeurs sont obtenues pour $n = 1, 2, 3, 4$ et 6 et comme cos est décroissante sur $[0, 2\pi]$, ce sont les seules arguments qui donnent ces valeurs.