Corrigé

Ex 1 :

1) $\mathbb{Q}$ corps et fd.

On utilise le théorème de structure des groupes abéliens finis :

$\exists ! k, d_1 | d_2 | \cdots | d_r$ tq $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$.

avec $d_1 \cdots d_r = p-1 = |(\mathbb{Z}/p\mathbb{Z})^*|$.

Mais alors tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ sont d'ordre divisant d_r. Ce sont donc des racines de $X^{d_r} - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$ dans le corps $\mathbb{Z}/p\mathbb{Z}$.

Comme ce polynôme a au plus autant de racines que son degré, on a $d_r \geq p-1$.

On a alors nécessairement $r = 1$ et $d_r = p-1$.

D'où $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/p-1\mathbb{Z}$.

2) $F = \{ (\alpha, \beta, \gamma) \in \mathbb{Z}/n\mathbb{Z},\ 2\alpha + 3\beta + 7\gamma = 0 \}$.

Posons $\delta = \alpha + \beta$.

$(\alpha, \beta, \gamma) \mapsto (\alpha+\beta, \beta, \gamma)$ ↓ | ↑ $(\delta-\beta, \beta, \gamma) \mapsto (\delta, \beta, \gamma)$

F est en bijection avec $G = \{ (\delta, \beta, \gamma) \in \mathbb{Z}/n\mathbb{Z},\ 2\delta + \beta + 7\gamma = 0 \}$

D'où $|F| = |G| = |\mathbb{Z}/n\mathbb{Z}|^2$

(L'équation est résolue : $\beta = -2\delta - 7\gamma$, avec δ et γ quelconques dans $\mathbb{Z}/n\mathbb{Z}$).

D'où $|F| = n^2 = (p-1)^2$.

3) Les triplets de E sont composés d'éléments inversibles donc

$$E = \{(a,b,c) \in (\mathbb{Z}/p\mathbb{Z})^*,\ a^{10}b^{15}c^{35} = 1\}$$

Soit $\varphi : (\mathbb{Z}/p\mathbb{Z})^\times \simeq (\mathbb{Z}/p-1, +)$ un isomorphisme (donné par le choix d'un générateur).

Pour $(a,b,c) \in (\mathbb{Z}/p\mathbb{Z})^\times$

Si $\varphi(a) = \alpha$, $\varphi(b) = \beta$ et $\varphi(c) = \gamma$, alors on a.

$(a,b,c) \in E$ ssi $10\alpha + 15\beta + 35\gamma = 0\ (= \varphi(1))$

Ainsi, on a $|E| \simeq \{(\alpha,\beta,\gamma) \in (\mathbb{Z}/n\mathbb{Z})^3,\ 10\alpha + 15\beta + 35\gamma = 0\}$.

Si $p \not\equiv 1\ [6]$, $5 \nmid p-1$.

Comme $5 \in \mathcal{P}$, $5 \wedge p-1 = 1$. et donc 5 est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

L'éq. $10\alpha + 15\beta + 35\gamma = 0$ (dans $\mathbb{Z}/n\mathbb{Z}$) $\Leftrightarrow$ $2\alpha + 3\beta + 7\gamma = 0$

(en multipliant par l'inverse de 5).

On a donc $|E| = |F| = n^2$.

Rq : si $p \equiv 1\ [5]$, on conclut de même que $|E| = 5n^2$.

Exercice 2 :

1) Si $\varphi : \mathbb{Z} \to k$, $1 \mapsto 1$ est l'unique morphisme d'anneaux,

on appelle caract de k le générateur ≥ 0 de ker φ.

. On dit que $P \in k[X]$ est irréductible ssi :

- P n'est pas constant (= inversible dans $k[X]$).
- P n'a pas de factorisation non triviale (ie de la forme $P = \lambda \frac{P}{\lambda}$) avec $\lambda \in k$.

2) Soit $\bar{A} \in k[X]$ tq $\bar{A} \in k[X]/(P)$ soit non nul.

On a donc $P \nmid A$ dans $k[X]$.

Comme P est irréductible, $P \wedge A = 1$ et donc il existe une ② relation de Bezout : $\exists U, V \in k[X]$ tq

$$UA + VP = 1.$$

Mais alors on a $\overline{U}\,\overline{A} = 1$ dans $k[X]/(P)$ ie $\overline{A}$ est bien inversible dans K, qui est donc un corps.

3) $\Rightarrow$: Soient $A, B \in k[X]$ tq $P = A^2 + B^2$.

alors Mq $P \nmid A$. ~~ou~~ $P \nmid B$.

~~En effet si c'était le cas, soit α (resp. β) la valuation de P dans A (resp. B) : $A = P^\alpha Q$ avec $Q \wedge P = 1$~~

~~$B = P^\beta Q'$ — $Q' \wedge P = 1$~~

Si on avait $P \mid A$ et $P \mid B$,

alors $P^2 \mid A^2$ et $P^2 \mid B^2$ donc $P^2 \mid A^2 + B^2 = P$ absurde.

Donc $P \nmid A$ ou $P \nmid B$. Disons $P \nmid A$.

Mais alors A est inversible dans K et dans k, on a

$\overline{A}^2 + \overline{B}^2 = 0$ ie $\overline{B}^2 = -\overline{A}^2$ ie $\left(\frac{B}{A}\right)^2 = -1$.

Donc -1 est bien un carré dans k.

4) si $i \in k$, on a $P = \left(\frac{1+P}{2}\right)^2 - \left(\frac{1-P}{2}\right)^2 = A_0^2 + (iB_0)^2$

donc P est bien une somme de deux carrés dans $k[X]$.

5) $L := k[i]$ est un corps.

Il est isomorphe à $k[Y]/(Y^2+1)$ avec $Y^2+1 \in k[Y]$ irréductible car sans racine dans k par hypothèse (si i est une racine, l'autre est $-i \neq i$ en caract 2).

Donc $L[X]$ est un anneau euclidien, donc principal, donc factoriel.

6) On a $L[X]/(P) \simeq \left(k[X]/(X^2+1)\right)[X]/(P)$

$\simeq k[X,Y]/(Y^2+1, P) \simeq \left(k[X]/(P)\right)[Y]/(Y^2+1)$

$\simeq K[Y]/(Y^2+1)$

7) Dans $K[Y]$, Y^2+1 a 2 racines distinctes. i et $-i$. $Y^2+1 = (Y+i)(Y-i)$
avec $Y+i \wedge Y-i = 1$.
Donc $K[Y]/(Y^2+1)$ n'est pas intègre ($(\overline{Y+i})(\overline{Y-i}) = 0$)

donc $L[X]/(P)$ non plus. Donc P n'est pas un élément premier. Comme $L[X]$ est factoriel, P n'est pas irréductible dans $L[X]$.

8) Tout élément $\ell \in L$ s'écrit de manière unique
$x+iy$ avec $x, y \in k$ (car $[L:k] = 2$ et. $(1, i)$ en est une k-base)

En isolant ainsi parties "réelle" et "imaginaire", des coefficients d'un polynôme $\varphi \in L(X)$, on a $\varphi = \alpha + i\beta$, avec $\alpha \in k[X]$, $\beta \in k[X]$.

L'écriture est unique par unicité de l'écriture dans L.

9) On pose $N(\alpha+i\beta) = \alpha^2+\beta^2 = (\alpha+i\beta)(\alpha-i\beta)$.

On vérifie sans peine que $\alpha+i\beta \longmapsto \alpha-i\beta$ est multiplicative (comme par la conjugaison complexe).

Mais alors $N(P_1P_2) = P_1P_2\,\overline{P_1P_2} = P_1\overline{P_1}\,P_2\overline{P_2}$

$= N(P_1)\,N(P_2)$.

10) Pq $N(P)$ est constant ssi P est constant.

Si P est constant c'est clair.

Réciproquement si $P = \alpha+i\beta$.

posons $a = \deg(\alpha)$ et $b = \deg(\beta)$.

Si $a \neq b$, disons $a > b$, alors $\deg(\alpha^2+\beta^2) = 2a$.

Comme $\deg(\alpha^2+\beta^2) = 0$ on a ~~une contradiction~~ $a = 0$ et $(b = -\infty)$.

Si $a = b > 0$ le coefficient de $\deg 2a$ de $\alpha^2+\beta^2$ est $a_n^2+b_n^2$

mais on a alors $a_n^2+b_n^2 = 0$

Comme $a_n \neq 0$, on have $-1 = \left(\frac{a_n}{b_n}\right)^2$ donc $i \in k$. Absurde.

11). Soit $\alpha+i\beta$ un facteur non trivial de P dans $L[X]$. $P = (\alpha+i\beta)\,Q$.

On a $N(P) = P^2 = N(\alpha+i\beta)\,N(Q)$

Comme $N(\alpha+i\beta)$ et $N(Q)$ sont non constants, on a

$N(\alpha+i\beta) = P$ car P est irréductible. D'où $P = \alpha^2+\beta^2$.

12) Φ_n est une somme de 2 carrés ssi (-1) est un carré dans $K = \mathbb{Q}[X]/\Phi_n \simeq \mathbb{Q}(e^{2i\pi/n})$.

La question revient donc à déterminer pour quelle on a $i \in \mathbb{Q}[e^{2i\pi/n}]$.

<u>1er Cas</u> : si $4 \mid n$, alors $i = e^{i\pi/2} = \left(e^{2i\pi/n}\right)^{n/4} \in \mathbb{Q}[e^{2i\pi/n}]$.

<u>2ème cas</u> : Rq si $4 \nmid n$, alors $i \notin \mathbb{Q}(e^{2i\pi/n}) = K$.

<u>Raisonnons par l'absurde</u>. Supposons $i \in K$.

<u>Si n est impair</u> : On a $4 \wedge n = 1$ donc il existe

$u, v \in \mathbb{Z}$ tq $4u + nv = 1$.

Mais alors $e^{2i\pi/4n} = \left(e^{2i\pi/n}\right)^u \cdot \left(e^{2i\pi/4}\right)^v \in K$.

Or $[\mathbb{Q}(e^{2i\pi/4n}) : \mathbb{Q}] = \varphi(4n) = 2\varphi(n) > \varphi(n) = [K : \mathbb{Q}]$.

(contredit le fait que $e^{2i\pi/4n} \in K$].

Si $2 \mid n$ et $4 \nmid n$: on a $4 \wedge n = 2$.

De même, on aurait $e^{2i\pi/2n} \in K$.

Mais comme $2 \mid n$, $\varphi(2n) = 2\varphi(n) > \varphi(n)$.

et on aboutit là encore à une contradiction.

<u>Conclusion</u> : Φ_n est une somme de 2 carrés ssi $4 \mid n$.