Corrigé du DM 1.

HP* INP-HB / L. TINTINAGLIA

I.A.1 (1)

Le polynôme 1 est bien dans $A[X]$. On vérifie immédiatement que si $P, Q \in A[X]$, $\begin{cases} P-Q \in A[X] \\ PQ \in A[X] \end{cases}$.

Finalement, $\boxed{A[X] \text{ est bien un sous-anneau de } \mathbb{k}[X]}$

I.A.2 (1,5)

Par définition de $\mathrm{Res}_{\mathbb{k}}(P,Q)$ et par formule du déterminant, $\mathrm{Res}_{\mathbb{k}}(P,Q)$ est une somme de produits de coefficients de P et de Q, donc d'éléments de A.

Finalement, $\boxed{\mathrm{Res}_{\mathbb{k}}(P,Q) \in A}$.

I.A.3 (2,5)

• Soit $P \in \mathbb{k}[X][Y]$. Par définition, il existe une suite presque nulle de polynômes $(P_j) \in \mathbb{k}[X]^{\mathbb{N}}$, telle que $P = \sum_{j \in \mathbb{N}} P_j(X) Y^j$.

Puis on décompose chaque $P_j = \sum_{i \in \mathbb{N}} a_{i,j} X^i$. On a bien

$\boxed{P = \sum_{i,j \geq 0} a_{i,j} X^i Y^j}$ avec $a_{ij} \in \mathbb{k}$ nul sauf un nombre fini.

• Réciproquement, si $P(X,Y) = \sum_{i,j \geq 0} \underbrace{b_{i,j}}_{\in \mathbb{k}} X^i Y^j$ avec (b_{ij}) presque nulle.

On a $P = \sum_{j \in \mathbb{N}} \left(\sum_{i \in \mathbb{N}} b_{i,j} X^i \right) Y^i$, ces sommes étant toutes finies.

Comme les $(Y^j)_j$ forment une base du $\mathbb{k}(X)$-espace vectoriel $\mathbb{k}(X)[Y]$, pour tout $j \in \mathbb{N}$,

$\sum_{i\in\mathbb{N}} b_{ij} X^i = P_j = \sum_{i\in\mathbb{N}} a_{ij} X^i$. Comme les (X^i) forment une base du $\mathbb{K}$-ev $\mathbb{K}[X]$, on a : $\forall (i,j)$, $a_{ij} = b_{ij}$.

Il y a donc **l'unicité**

I.A.4 ①

Soit $P \neq 0$ un élément de $\mathbb{K}[X][Y]$ s'écrivant comme ci-dessus. $\{ i+j \mid a_{ij} \neq 0 \}$ est une partie finie non-vide de $\mathbb{N}$. Elle admet donc un maximum, et $d(P)$ est **bien défini**

I.B.1 ②

- Supposons $P \wedge Q = D$, $\deg(D) \geq 1$. Alors $\begin{cases} P = DB \\ Q = DA \end{cases}$ avec $\begin{cases} \deg A < m \\ \deg B < n \end{cases}$ et alors $AP = BQ$.
- Si $P \wedge Q = 1$, soient $(A,B) \in (\mathbb{K}[X] \setminus \{0\})^2$, tels que $AP = BQ$.

  Par lemme de Gauss, $\begin{cases} A \mid Q \\ B \mid P \end{cases}$ d'où $\begin{cases} \deg A \geq m \\ \deg B \geq n \end{cases}$, cela conclut.
- Finalement on a **l'équivalence voulue**

I.B.2 ②,5

$\forall (A_1, B_1) \in \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X]$, $\forall (A_2, B_2) \in \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X]$, $\forall (\alpha, \beta) \in \mathbb{K}^2$,

$$\phi(\alpha(A_1, B_1) + \beta(A_2, B_2)) = \phi(\alpha A_1 + \beta A_2, \alpha B_1 + \beta B_2)$$

$$= (\alpha A_1 + \beta A_2)P + (\alpha B_1 + \beta B_2)Q = \alpha(A_1 P + B_1 Q) +$$

$$\beta(A_2 P + B_2 Q) = \alpha \phi(A_1, B_1) + \beta \phi(A_2, B_2).$$

I.B.3 ①

On a $\mathcal{M}at_{\mathcal{B},\mathcal{B}_0}(\phi) = \mathcal{M}at_{\mathcal{B}_0}(\phi(1,0), \dots, \phi(X^{m-1},0), \phi(0,1), \dots, \phi(0,X^{n-1}))$

$= (P, XP, \dots, X^{m-1}P, Q, XQ, \dots, X^{n-1}Q)$

$= R(P,Q)$.

I.B.4 ①,5

Comme $\phi \in \mathcal{L}(E, \mathbb{K}_{m+n-1}[X])$ de mêmes dimensions,

ϕ est un isomorphisme ssi ϕ injective Or :

$P \wedge Q \neq 1 \iff \exists (A,B) \in \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X] \setminus \{0,0\}, \ AP = BQ$

$\iff$ ——— $AP - BQ = 0$

$\iff$ ——— $\phi(P,Q) = 0$

$P \wedge Q \neq 1 \iff \phi$ non injective D'où l'équivalence souhaitée

I.C.1 ①

On peut remarquer que l'on peut définir $\mathrm{Res}(P,Q)$ dès lors que $m+n \in \mathbb{N}^*$ (même si $m=0$ ou $n=0$).

Ici, $n=0$, $P=\alpha$ et $Q = \sum_{j=0}^{m} b_j X^j$ avec $m \geq 1$ d'où

$R(P,Q) \in \mathcal{M}_{n+m}(\mathbb{K}) = \mathcal{M}_m(\mathbb{K})$ et

$$R(P,Q) = \begin{pmatrix} \alpha & & (0) \\ & \ddots & \\ (0) & & \alpha \end{pmatrix}$$ d'où $\mathrm{Res}(\alpha, Q) = \alpha^m$

I.C.2 ②

On doit appliquer m fois le $(n+m)$-cycle $\sigma = (1\ 2 \dots n+m)$

Donc $\operatorname{Res}(P,Q) = (-1)^{m(n+m-1)} \operatorname{Res}(Q,P)$. Mais $m(m-1)$ est pair donc $\boxed{\operatorname{Res}(P,Q) = (-1)^{nm} \operatorname{Res}(Q,P)}$

I.C.3 (4)

On suppose $n \geq m \geq 1$. Soit R le reste de la division euclidienne de P par Q.

- Si $R=0$, $Q \mid P$ donc $P \wedge Q \neq 1$ et $\operatorname{Res}(P,Q) = 0$
- Sinon, soit $r = \deg(R) \in \mathbb{N}$ et $P = QA + R$ avec $A = \sum_{i=0}^{n-m} a_i X^i$. Suivons l'algo de la div. euclidienne :

à la première étape, on pose $a_{n-m} = \frac{a_n}{b_m}$ et $P_1 = P - a_{n-m} X^{n-m} Q$.

Ainsi pour $j \in [\![0, m-1]\!]$, $X^j P_1 = X^j P - a_{n-m} X^{n-m+j} Q$,

avec $n-m \leq n-m+j \leq n-1$.

Pour se ramener à $\operatorname{Res}(P_1, Q)$, on réalise :

$$C_j \leftarrow C_j - a_{n-m} C_{m+n+j}$$

Ainsi $\operatorname{Res}(P,Q) = \det(P_1, \dots, X^{m-1}P_1, Q, XQ, \dots, X^{n-1}Q)$

$$= \operatorname{Res}(P_1, Q) \text{ car } \deg(P_1) \neq n.$$

Soit $d = \deg(P_1)$, on a

$$R(P,Q) \equiv \begin{pmatrix} R(P_1,Q) & * \\ 0 & T \end{pmatrix} \text{ où } T = \begin{pmatrix} b_m & & (*) \\ & \ddots & \\ (0) & & b_m \end{pmatrix} \in \mathcal{M}_{n-d}(\mathbb{K})$$

d'où $\operatorname{Res}(P,Q) = b_m^{n-d} \operatorname{Res}(P_1, Q)$. On continue ainsi l'algorithme jusqu'à obtenir

$$\boxed{\operatorname{Res}(P,Q) = \operatorname{Res}(R,Q)\, b_m^{n-r}} \quad \text{(Clemme)}$$

Quitte à se placer sur une clôture algébrique des corps, on suppose maintenant tous les polynômes scindés. Considérons

$$S : \left(\alpha \underbrace{\prod_{i=1}^{n}(X-\lambda_i)}_{=P}, \beta \underbrace{\prod_{j=1}^{m}(X-\mu_j)}_{=Q,\ m\geq 1}\right) \mapsto \beta^n \prod_{j=1}^{m} P(\mu_j)$$

On montre $S = Res$.

→ si $\underline{n=0}$, $P=\alpha$, $S(\alpha, Q) = \beta^0 \alpha^m = \alpha^m = Res(\alpha, Q)$.

→ On réalise une récurrence forte sur $n = \deg(P)$. On suppose la propriété pour tous polynômes (P, Q), avec $\deg P \leq n-1$ où $n \in \mathbb{N}^*$ fixé.
$\deg Q \geq 1$

- Si $m \leq n$, on réalise la division euclidienne de P par Q, et par le lemme, $Res(P, Q) = Res(R, Q)\, b_m^{n-r}$ où $r = \deg(R) < m \leq n$. Par HR avec $\beta = b_m$,

$$Res(P, Q) = b_m^{n-r} Res(R, Q) = b_m^{n-r+r} \prod_{j=1}^{m} R(\mu_j) = \beta^n \prod_{j=1}^{m} P(\mu_j)$$

car $\forall j$, $Q(\mu_j) = 0$ et $Q \mid P-R$ donc $P(\mu_j) = R(\mu_j)$.

- Si $n < m$, on utilise $Res(P, Q) = (-1)^{mn} Res(Q, P)$ et on applique le cas précédent.

On conclut ainsi.

I.C.4 ③

$R_\lambda = Res\left(\lambda^n P\left(\frac{X}{\lambda}\right), \lambda^m Q\left(\frac{X}{\lambda}\right)\right)$. On multiplie L_j par λ^{j-1} par $j \in [\![1, m+n]\!]$. Pour $i \in [\![1, m]\!]$, on factorise

X^{n+i-1} sur C_i. Pour $i \in [\![m+1, m+n]\!]$ on factorise X^{i-1}.

On a alors $R_X = X^{\Sigma}\,\mathrm{Res}(P,Q)$ où par multilinéarité du det : $\Sigma = \sum_{i=1}^{m}(n+i-1) + \sum_{i=m+1}^{m+n}(i-1) - \sum_{j=1}^{m+n}(j-1) = nm$

I.D.1 (2)

Soient $\beta_1, \beta_2 \in \mathbb{C}$ et $P_1, P_2 \in \mathbb{Z}[X]$ de degrés n_1, n_2 tels que $P_1(\beta_1) = P_2(\beta_2) = 0$. On considère $P_1(X-Y), P_2(Y) \in \mathbb{Q}(X)[Y]$ or $P_1, P_2 \in \mathbb{Z}[X]$ donc $P_1(X-Y), P_2(Y) \in \mathbb{Z}[X][Y]$ et ainsi $R(X) = \mathrm{Res}_{\mathbb{Q}(X)}(P_1(X-Y), P_2(Y)) \in \mathbb{Z}[X]$.

Par binôme de Newton, $P_1(X-Y) = \sum_{j=0}^{n_1} c_j(X)\,Y^j$ avec $c_j(X) = (-1)^j \sum_{k=j}^{n_1} a_k \binom{k}{j} X^{k-j} \in \mathbb{Z}[X]$. On a $c_0(X) = P_1$ et pour $j \in [\![1, n_1]\!]$, $\deg(c_j) = n_1 - j$.

Comme $b_{n_2} = 1$,

$$R(X) = \begin{vmatrix} P_1(X) & 0 & \cdots & 0 & b_0 & 0 & 0 \\ c_1(X) & P_1(X) & \ddots & 0 & b_1 & \ddots & 0 \\ \vdots & c_1(X) & & 0 & \vdots & & b_0 \\ c_{n_1}(X) & \vdots & \ddots & P_1(X) & b_{n_2-1} & \ddots & \vdots \\ 0 & c_{n_1}(X) & \ddots & c_1(X) & 1 & \ddots & \vdots \\ \vdots & \ddots & & \vdots & 0 & & b_{n_2-1} \\ 0 & \cdots & 0 & c_{n_1}(X) & & & 1 \end{vmatrix}$$

donc par formule du det, le terme de + haut degré provient de $P_1(X)^{n_2} 1^{n_1}$. Donc R est unitaire de degré $n_1 n_2$.

I.D.2 (1,5)

$R(\beta_1+\beta_2) = \mathrm{Res}\left(P_1(\beta_1+\beta_2-Y), P_2(Y)\right)$. Mais β_2 est une racine commune de $P_1(\beta_1+\beta_2-Y)$ et de P_2.

Ces deux polynômes ne sont donc pas premiers entre eux et $\boxed{R(z_1+z_2)=0}$.

I.D.3 (2,5)

Dans le cas $z_1 \neq 0$ et $z_2 \neq 0$, on pose de même

$$S(X) = \mathrm{Res}_{\mathbb{Q}(X)}\left(4^{n_1} P_1\left(\frac{X}{4}\right), P_2(4)\right).$$

- Comme $n_1 = \deg(P_1)$, $4^{n_1} P_1\left(\frac{X}{4}\right) \in \mathbb{Z}[X][4]$.
  Ainsi $S \in \mathbb{Z}[X]$.
- De plus on montre comme ci-dessus que S est unitaire de degré $n_1 n_2$.
- $S(z_1 z_2) = \mathrm{Res}_{\mathbb{Q}}\left(4^{n_1} P_1\left(\frac{z_1 z_2}{4}\right), P_2(4)\right)$, et comme les deux polynômes de $\mathbb{Q}[4]$ en jeu s'annulent bien deux en z_2, ils ne sont pas premiers entre eux et $\boxed{S(z_1 z_2)=0}$

I.D.4 (1)

On a ainsi trouvé des polynômes à coefficients entiers qui annulent z_1+z_2 et $z_1 z_2$ pour $(z_1, z_2) \in \mathbb{C}^2$.

Comme $(-1)^n P(-X)$ est unitaire et annule $-z_1$, on peut conclure que $\boxed{\mathbb{G} \text{ est un sous-anneau de } \mathbb{C}}$.

I.D.5 (1,5)

On note $P(X) = X^3 - 3$ et $Q_y(X) = (y-X)^2 - 7$.

$$\text{Res}(P, Q_y) = \begin{vmatrix} -3 & 0 & y^2-7 & 0 \\ 0 & -3 & -2y & y^2-7 \\ 1 & 0 & 1 & -2y \\ 0 & 1 & 0 & 1 \end{vmatrix}$$

$$= y^4 - 20y^2 + 16 \quad \text{(en développant)}$$

Or P admet pour racines $\sqrt{3}$ et $-\sqrt{3}$ et Q_y admet pour racines $y+\sqrt{7}$ et $y-\sqrt{7}$. Donc P et Q_y admettent une racine commune <u>ssi</u> $\sqrt{3} = y \pm \sqrt{7}$ ou $-\sqrt{3} = y \pm \sqrt{7}$

Ainsi $\text{Res}(P, Q_y) = 0 \iff y \in \{\sqrt{3}+\sqrt{7} ; -\sqrt{3}+\sqrt{7}\}$ et donc $\underline{X^4 - 20X^2 + 16}$ admet pour racines $\sqrt{3}+\sqrt{7}$; $\sqrt{3}-\sqrt{7}$; $-\sqrt{3}+\sqrt{7}$; $-\sqrt{3}-\sqrt{7}$ et est de degré 4 à coefficients dans $\mathbb{Z}$.

II.A.1 (1)

- Pour tout $a \in X$, $a = \rho_e(a)$ donc $a \mathcal{R} a$ et la relation est donc réflexive
- Soit $(a,b) \in X^2$ tel que $a \mathcal{R} b$. On fixe $g \in G$, $\rho_g(a) = b$. Alors $a = \rho_{g^{-1}}(b)$ et donc $b \mathcal{R} a$. D'où la symétrie
- Si $a \mathcal{R} b$ et $b \mathcal{R} c$, $\begin{cases} b = \rho_g(a) \\ c = \rho_h(b) \end{cases}$ avec $(g,h) \in G^2$.

  $c = \rho_h(\rho_g(a)) = \rho_{hg}(a)$ avec $hg \in G$ donc $a \mathcal{R} c$. On a la transitivité.

$\underline{\mathcal{R} \text{ est une relation d'équivalence}}$

II.A.2 (1)

- Soit $a \in X$. Par définition $\mathrm{Stab}(a) \subseteq G$. Comme $\rho_e(a) = a$, $e \in \mathrm{Stab}(a)$, qui n'est donc pas vide.
- Soit $(g, g') \in \mathrm{Stab}(a)^2$. Ainsi $\rho_{gg'}(a) = \rho_g(\rho_{g'}(a)) = \rho_g(a) = a$ et $gg' \in \mathrm{Stab}(a)$.
- Soit $g \in \mathrm{Stab}(a)$. Alors $\rho_g(a) = a$ donc $a = \rho_e(a) = \rho_{g^{-1}} \circ \rho_g(a)$ donc $g^{-1} \in \mathrm{Stab}(a)$. $a = \rho_{g^{-1}}(a)$
- $\underline{\mathrm{Stab}(a) \text{ est un sous-groupe de } G.}$

II.A.3 (1,5)

Soit $a \in X$. Soit $b \in \mathrm{Orb}(a)$. Soit $h \in G$ tel que $b = \rho_h(a)$. Pour tout $g \in G$,

$$g \in \mathrm{Stab}(b) \iff \rho_g(b) = b \iff \rho_g(\rho_h(a)) = \rho_h(a)$$
$$\iff \rho_{h^{-1}} \circ \rho_g \circ \rho_h(a) = a$$
$$\iff h^{-1}gh \in \mathrm{Stab}(a)$$
$$\iff \exists g' \in \mathrm{Stab}(a),\ g' = h^{-1}gh$$
$$\iff \text{——},\ g = hg'h^{-1}$$
$$\iff \underline{g \in h\,\mathrm{Stab}(a)\,h^{-1}}$$

II.A.4 (2,5)

Soit $a \in X$. On remarque que $G = \bigsqcup_{b \in \mathrm{Orb}(a)} \{g \in G \mid \rho_g(a) = b\}$ (*)

Par ailleurs pour $b \in \mathrm{Orb}(g)$, si $b = \rho_h(a)$, on a alors pour $g \in G$, $\rho_g(a) = b \iff h^{-1}g \in \mathrm{Stab}(a) \iff g \in h\,\mathrm{Stab}(a)$

comme précédemment.

donc $|\{g \in G \mid \rho_g(a) = b\}| = |\mathrm{Stab}(a)|$. Ainsi on a

$$\boxed{|G| = |\mathrm{Stab}(a)|\,|\mathrm{Orb}(a)|}$$

II.A.5 (1,5)

Les orbites forment une partition de X donc $X = \bigsqcup_{j=1}^{N} \mathrm{Orb}(a_j)$

et on en déduit $|X| = \sum_{j=1}^{N} |\mathrm{Orb}(a_j)| = \sum_{j=1}^{N} \frac{|G|}{|\mathrm{Stab}(a_j)|}$

II.A.6 (2,5)

- D'une part $A = \{(g,x) \in G \times X \mid \rho_g(x) = x\}$

$$= \bigsqcup_{g \in G} \{g\} \times \{\underbrace{x \in X,\ \rho_g(x) = x}_{= \mathrm{Fix}(g)}\}$$

Donc $|A| = \sum_{g \in G} |\{x \in X,\ \rho_g(x) = x\}| = \sum_{g \in G} |\mathrm{Fix}(g)|$

- D'autre part $A = \bigsqcup_{x \in X} \mathrm{Stab}(x) \times \{x\}$ donc

$$|A| = \sum_{x \in X} |\mathrm{Stab}(x)| = \sum_{j=1}^{N} \sum_{x \in \mathrm{Orb}(a_j)} |\mathrm{Stab}(x)|$$

$$= \sum_{j=1}^{N} \sum_{x \in \mathrm{Orb}(a_j)} \frac{|G|}{|\mathrm{Orb}(a_j)|} = \sum_{j=1}^{N} |G| = |G|N$$

$$= |G| \cdot |O|$$

- Ainsi $\boxed{N = |O| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}(g)|}$

II.B.1 (0,5)

On considère l'identité de $\mathfrak{S}_n$.

II.B.2 ②

- Par tout $g \in G$, $\rho_g : x \in G \mapsto gx$ est bien une bijection de G dans G d'inverse $g \mapsto g^{-1}x$. On vérifie de plus que pour tout $(g, g') \in G^2$, $\rho_g \circ \rho_{g'} : x \mapsto gg'x = \rho_{gg'}(x)$. L'application $\Theta : g \mapsto \rho_g$ est donc bien un morphisme de groupes de G vers $\mathfrak{S}(G)$
- On vérifie que celui-ci est injectif : si $\rho_g = Id_G$, en particulier $e = \rho_g(e) = g$. Ainsi G est isomorphe à $\Theta(G)$, sous-groupe de $\mathfrak{S}(G)$, qui est lui-même naturellement isomorphe à $\mathfrak{S}_n$ où $n = |G|$.

II.B.3 ①

De même, on vérifie que $x \mapsto gxg^{-1}$ est bijective et que $g \mapsto \rho_g$ est un morphisme de groupes de G vers $\mathfrak{S}(G)$

II.B.4 ①

On remarque $Z(G) = \ker\left(g \mapsto (\rho_g : x \mapsto gxg^{-1})\right)$, il s'agit bien d'un sous-groupe.

II.B.5 ③ (cours : VI.A.3)

On suppose $|G| = p^d$, $d \in \mathbb{N}^*$, $p \in \mathbb{P}$. On considère l'action de conjugaison.

Si $a \in G$, alors $Orb(a) = \{gag^{-1}, g \in G\}$ et $|orb(a)| = 1 \Leftrightarrow a \in Z(G)$.

Les orbites forment une partition de G, soient donc $(a_1, \dots, a_n)$ des représentants de chaque classe, avec par exemple $(a_1, \dots, a_d) \in Z(G)^d$ et $|Orb(a_j)| \geq 2$ pour $j \geq d+1$.

$$p^d = |G| = \sum_{j=1}^{n} |orb(a_j)| = |Z(G)| + \sum_{j=d+1}^{n} |Orb(a_j)|$$

$$= |Z(G)| + \sum_{j=d+1}^{n} \frac{p^d}{|Stab(a_j)|}) = p^{\beta_j} \text{ par Lagrange}$$

$$p^d = |Z(G)| + (n-d)\, p^{\alpha - \beta_j}$$

donc $p \mid |Z(G)|$ qui est non-nulle d'où $|Z(G)| \geq p$

II.B.6 (2,5)

Par ce qui précède, $|Z(G)| \in \{p, p^2\}$. Mais $|G| = p^2$ donc $|Z(G)| = p$ car sinon $G = Z(G)$ et il serait abélien.

Soit $a \in G \setminus Z(G)$. Comme $\begin{cases} a \in Stab(a) \\ Z(G) \subseteq Stab(a) \end{cases}$,

$|Stab(a)| \geq p+1$ et $|Stab(a)| \mid p^2$. Ainsi $|Stab(a)| = p^2$ et $a \in Z(G)$: absurde

Donc G est abélien

II.C.1 (1)

- $0, 1 \in Z$
- Si $x, y \in Z$, pour $\alpha \in k$, $(y-x)\alpha = y\alpha - x\alpha = \alpha y - \alpha x$ $= \alpha(y-x)$

  $(Z, +)$ est donc un sous-groupe de $(k, +)$.
- De même, $\alpha(yz) = (yz)\alpha$ si $\alpha \in Z$, c'est un sous-anneau

◁ Par ailleurs si $z \in Z^\times$, pour $x \in \mathbb{K}$, $xz = zx$ donc $z^{-1}x = xz^{-1}$ et $z^{-1} \in Z$, c'est donc un sous-corps de $\mathbb{K}$, à fortiori commutatif

II.C.2 (2,5)

On munit $\mathbb{K}$ d'une structure de Z-espace vectoriel :

$$\cdot : \begin{cases} (Z, \mathbb{K}) \longrightarrow \mathbb{K} \\ (z, x) \longmapsto zx \end{cases}$$

On vérifie que $\cdot$ munit $\mathbb{K}$ d'une loi de composition externe :

◁ $\forall z \in Z, \forall x \in \mathbb{K}, zx \in \mathbb{K}$ car $Z \subseteq \mathbb{K}$

◁ $\forall x \in \mathbb{K}, 1_Z \cdot x \in \mathbb{K}$

◁ $\forall (x,y) \in \mathbb{K}^2, \forall z \in Z, \quad z \cdot (x+y) = zx + zy = xz + yz$
$= (x+y) \cdot z$

◁ $\forall x \in \mathbb{K}, \forall (z_1, z_2) \in Z^2, \quad (z_1 + z_2)x = z_1 x + z_2 \cdot x$

◁ $\forall x \in \mathbb{K}, \forall (z_1, z_2) \in Z^2, \quad z_1 \cdot (z_2 \cdot x) = (z_1 z_2) \cdot x$

Notons $p = |Z|$ et $n \geq 1$ la dimension de $\mathbb{K}$ sur Z (finie puisque $\mathbb{K}$ est fini). Ainsi $\mathbb{K} \simeq Z^n$ et donc $|\mathbb{K}| = |Z^n| = \underline{p^n}$.

II.C.3 (1,5)

◁ Nécessairement $0 \in Z_a$ (et même $Z \subseteq Z_a$). De plus soient $h, g \in Z_a$; ainsi $(g+h)a = a(g+h)$ et $g+h \in Z_a$.

◁ De plus si $z \in Z$, $(z \cdot x)a = zxa = zax = a(z \cdot x)$ ainsi $zx \in Z_a$. On en déduit que Z_a est un sev de $\mathbb{K}$.

« En notant $d_a \geq 1$ la dimension de Z_a, $\boxed{|Z_a| = p^{d_a}}$

II.C.4 (0,5)

Pour tout $g \in G$, φ_g est bien une bijection (d'inverse $\varphi_{g^{-1}}$). Et on vérifie immédiatement que $\varphi_g \circ \varphi_h = \varphi_{gh}$.

II.C.5 (1,5)

Par définition, $H_a = Z_a \setminus \{0\}$. $|H_a| = p^{d_a} - 1$.

Or $|G| = |\mathrm{Orb}(a)| \cdot |H_a|$, d'où $|\mathrm{Orb}(a)| = \dfrac{p^n - 1}{p^{d_a} - 1}$.

II.C.6 (0,5)

Dans le cas où $a \in \mathbb{Z}^\alpha$, $xa = ax$ pour $x \in \mathbb{K}$ et donc $Z_a = \mathbb{K}$, $H_a = G$. $\tilde{a} = \{a\}$.

II.C.7 (3)

Soit $a \in G$ quelconque. D'après ci-dessus, $|H_a| \mid |G|$, c'est-à-dire $p^{d_a} - 1 \mid p^n - 1$.

Écrivons $n = q d_a + r$, où $0 \leq r < d_a$:

$$p^n - 1 = p^{q d_a + r} - 1 = p^r (p^{q d_a} - 1) + p^r - 1$$

$$= (p^{d_a} - 1) \underbrace{p^r \sum_{j=0}^{q-1} p^{q-1-j}}_{= \tilde{q}} + \underbrace{p^r - 1}_{= \tilde{r}} \qquad (\alpha)$$

avec $\tilde{r} = p^r - 1 < p^{d_a} - 1$ donc (α) est la division euclidienne de $p^n - 1$ par $p^{d_a} - 1$. Par unicité, comme $p^{d_a} - 1 \mid p^n - 1$, $\tilde{r} = 0$ donc

$p^\nu - 1 = 0$ et $\nu = 0$. Ainsi $n = q d_a$ et $\boxed{d_a \mid n}$.
De plus si $a \notin \mathcal{Z}^a$, $H_a \subsetneq G$ et donc $\boxed{d_a \neq n}$

II.C.8 (1,5)

Les classes d'équivalence pour $\sim$ forment une partition de G. Donc $|G| = \sum_{\tilde{a} \in \tilde{G}} |\tilde{a}|$.

Pour $a \in \mathcal{Z}^a$, $|\tilde{a}| = 1$, donc $|G| = |\mathcal{Z}^\nu| + \sum_{\substack{\tilde{a} \in \tilde{G} \\ a \notin \mathcal{Z}^a}} |\tilde{a}|$

En conservant les notations introduites, on obtient finalement :

$$\boxed{p^n - 1 = p - 1 + \sum_{\substack{\tilde{a} \in \tilde{G} \\ a \in \mathcal{Z}^a}} \frac{p^n - 1}{p^{d_a} - 1} \quad (C_a a)}$$

II.C.9 (4)

Supposons par l'absurde que $n > 1$ (i.e. $\mathbb{K} \neq \mathbb{Z}$). On sait que $\Phi_n \mid X^n - 1$ dans $\mathbb{Z}[X]$; on écrit donc $X^n - 1 = \Phi_n Q$ avec $Q \in \mathbb{Z}[X]$.

Ainsi $p^n - 1 = \Phi_n(p) Q(p)$ et donc $\Phi_n(p) \mid p^n - 1$.

De plus par $d \mid n$ avec $d < n$, $\dfrac{X^n - 1}{X^d - 1} = \prod_{\substack{d' \mid n \\ d' \neq d}} \Phi_{d'}$ est divisible par Φ_n dans $\mathbb{Z}[X]$; ainsi $\Phi_n(p) \mid \dfrac{p^n - 1}{p^{d_a} - 1}$ dans $\mathbb{Z}$. Par $(C_a a)$, $\boxed{\Phi_n(p) \mid p - 1}$.

Or $|\Phi_n(p)| = \prod_{\omega \in \mathbb{U}_n} |p - \omega|$. Mais : $\forall \omega \in \mathbb{U}_n$, $\omega \in \mathbb{K} \setminus \{1\}$

donc : $\forall \omega \in \mu_n$, $|p - \omega| > p - 1$. Ainsi

$$|\Phi_n(p)| > (p-1)^n \geq p - 1$$

c'est une contradiction.

II.C.10 (0,5)

Finalement, $n = 1$ c'est-à-dire $\mathbb{Z} = \mathbb{K}$ donc

$\mathbb{K}$ est commutatif