

DS 5 : Corrigé

Barème, sur un total de 62 points

- Premier problème : 28 points
 - Partie I, 9 points : 1,1,1,3,3.
 - Partie II, 10 points : 1,2,4,3.
 - Partie III, 9 points : 5,4.
- Second problème : 38 points
 - Partie I, 11 points : 3,2,3,3.
 - Partie II, 27 points :
 - Question 5 : 1
 - Question 6.a et b : 2
 - Question 6.c : 2
 - Question 6.d : 3
 - Question 7 : 6
 - Question 8.a : 2
 - Question 8.b : 4
 - Question 8.c : 5
 - Question 9 : 2

Premier problème : une application du théorème de Ramsey

Partie I : Racines d'un polynôme modulo p

1°) 1 est une racine évidente et on vérifie que $P_0(X) = (X - 1)(2X - 1)$, donc les racines réelles de P_0 sont exactement 1 et $\frac{1}{2}$.

2°) Soit $P \in \mathbb{Z}[X]$. Ainsi, $P(X) = \sum_{n \in \mathbb{N}} a_n X^n$, où $(a_n)_{n \in \mathbb{N}}$ est une famille presque nulle d'entiers relatifs. Alors, pour tout $h \in \mathbb{Z}$, d'après les règles de calcul dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{P(h)} = \sum_{n \in \mathbb{N}} \overline{a_n} \overline{h}^n$. Ainsi, $\overline{P(h)}$ est bien une fonction de \overline{h} et pas seulement de h , elle est bien définie.

3°) Soit $h \in \mathbb{Z}$. Alors $\overline{P_0}(\overline{h}) = \overline{P_0}(\overline{h}) = (\overline{h} - 1)(\overline{2h} - 1)$. Or $\mathbb{Z}/p\mathbb{Z}$ est intègre, donc $\overline{P_0}(\overline{h}) = 0 \iff (\overline{h} - 1 = 0 \text{ ou } \overline{2h} - 1 = 0) \iff (\overline{h} = 1 \text{ ou } \overline{h} = \overline{2}^{-1})$. En effet, $\overline{2} \neq 0$, donc $\overline{2}$ est inversible dans le corps $\mathbb{Z}/7\mathbb{Z}$. De plus $2 \cdot 4 = 8 \equiv 1[7]$, donc $\overline{2}^{-1} = \overline{4}$.

Ainsi, les racines modulo 7 de P_0 sont exactement $\overline{1}$ et $\overline{4}$.

4°) Supposons que $\deg(P) \leq 0$. Alors il existe $b \in \mathbb{Z}$ tel que $P(X) = b$, donc pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, $\overline{P}(x) = \overline{b}$. Or par hypothèse, $\overline{P}(\alpha) = 0$, donc $\overline{b} = 0$. On en déduit que $\overline{P} = 0$ ce qui est faux. Ainsi, $\deg(P) \geq 1$. Notons $n = \deg(P)$. Ainsi, il existe $a_0, \dots, a_n \in \mathbb{Z}$

tels que $P(X) = \sum_{k=0}^n a_k X^k$.

Soit $x \in \mathbb{Z}/p\mathbb{Z}$. $\overline{P}(x) = \overline{P}(x) - \overline{P}(\alpha) = \sum_{k=1}^n \overline{a_k}(x^k - \alpha^k)$, donc d'après la formule de

Bernoulli, $\overline{P}(x) = \sum_{k=1}^n \overline{a_k}(x - \alpha) \sum_{h=0}^{k-1} x^h \alpha^{k-1-h}$.

Il existe $c \in \mathbb{Z}$ tel que $\alpha = \overline{c}$. Alors, pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, $\overline{P}(x) = (x - \alpha)\overline{Q}(x)$, où

$Q(X) = \sum_{k=1}^n a_k \sum_{h=0}^{k-1} c^{k-1-h} X^h$. Q est bien un élément de $\mathbb{Z}[X]$

et $\deg(Q) \leq n - 1 = \deg(P) - 1$.

5°) \diamond Soit $k \in \mathbb{N}$. Notons $R(k)$ l'assertion suivante, que l'on se propose de démontrer par récurrence : si $P \in \mathbb{Z}[X]$, avec $\overline{P} \neq 0$, et si P admet k racines modulo p deux à deux distinctes, alors $\deg(P) \geq k$.

\diamond Lorsque $k = 0$, la propriété est évidente car lorsque $\overline{P} \neq 0$, donc $P \neq 0$ donc $\deg(P) \geq 0$.

\diamond Soit $k \in \mathbb{N}$. On suppose $R(k)$.

Soit $P \in \mathbb{Z}[X]$ tel que $\overline{P} \neq 0$ et tel que P possède $k + 1$ racines de modulo p notées $\alpha_1, \dots, \alpha_{k+1}$, deux à deux distinctes. D'après la question 4, il existe $Q \in \mathbb{Z}[X]$ tel que, pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, $\overline{P}(x) = (x - \alpha_{k+1})\overline{Q}(x)$, avec $\deg(Q) \leq \deg(P) - 1$.

Soit $i \in \mathbb{N}_k$. $0 = \overline{P}(\alpha_i) = (\alpha_i - \alpha_{k+1})\overline{Q}(\alpha_i)$, or $\alpha_i - \alpha_{k+1} \neq 0$ et $\mathbb{Z}/p\mathbb{Z}$ est intègre, donc $\overline{Q}(\alpha_i) = 0$.

Ainsi, \overline{Q} admet k racines distinctes modulo p . De plus, $\overline{Q} \neq 0$, car $\overline{P} \neq 0$, donc d'après l'hypothèse de récurrence appliquée à Q , $\deg(Q) \geq k$.

Alors $\deg(P) \geq \deg(Q) + 1 \geq k + 1$.

Ceci démontre $R(k + 1)$.

\diamond D'après le principe de récurrence, $R(k)$ est vraie pour tout $k \in \mathbb{N}$.

Partie II : Puissances n -ièmes dans $\mathbb{Z}/p\mathbb{Z}$

6°) D'après le cours, $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est un groupe.

Montrons que S en est un sous-groupe.

$1^n = 1 \in S$, donc S est non vide.

Soit $x, y \in S$. Il existe $a, b \in (\mathbb{Z}/p\mathbb{Z})^*$ tels que $x = a^n$ et $y = b^n$.

Alors $xy^{-1} = a^n b^{-n} = (ab^{-1})^n \in S$, ce qui conclut.

7°) \diamond Soit $x, y, z \in (\mathbb{Z}/p\mathbb{Z})^*$.

$x^{-1}x = 1 \in S$, donc $x R x$, ce qui prouve que R est réflexive.

Si $x R y$, alors $y^{-1}x = (x^{-1}y)^{-1} \in S$, car S est un groupe et $x^{-1}y \in S$. Ainsi, R est symétrique.

Supposons que $x R y$ et $y R z$. Alors $x^{-1}z = (x^{-1}y)(y^{-1}z) \in S$, car S est stable pour le produit. Ainsi, R est transitive.

On a montré que R est bien une relation d'équivalence.

\diamond Soit $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Pour tout $y \in (\mathbb{Z}/p\mathbb{Z})^*$,

$a R y \iff (\exists h \in S, a^{-1}y = h) \iff (\exists h \in S, y = ah) \iff y \in aS$,

donc $\{aS / a \in (\mathbb{Z}/p\mathbb{Z})^*\}$ est l'ensemble des classes d'équivalence de R . D'après le cours, c'est une partition de $(\mathbb{Z}/p\mathbb{Z})^*$.

8°) Lorsque $s \in S$, notons $R_s = \{x \in (\mathbb{Z}/p\mathbb{Z})^* / x^n = s\}$.

Soit $s \in S$. Il existe $h \in \mathbb{Z}$ tel que $s = \bar{h}$. Posons $P(X) = X^n - h$.

$n \in \mathbb{N}^*$, donc $\bar{P}(0) = -\bar{h}$, or $s \neq 0$, donc $\bar{P}(0) \neq 0$. Ainsi, $\bar{P} \neq 0$, or $\deg(P) = n$ et R_s est égal à l'ensemble des racines de P modulo p , donc d'après la question 5, $|R_s| \leq n$.

Soit $s, s' \in S$ tels que $R_s \cap R_{s'} \neq \emptyset$. Alors il existe $x \in R_s \cap R_{s'}$. On a $s = x^n = s'$. Ainsi, lorsque $s, s' \in S$ avec $s \neq s'$, $R_s \cap R_{s'} = \emptyset$.

De plus, lorsque $x \in (\mathbb{Z}/p\mathbb{Z})^*$, il est clair que $x \in R_{x^n}$, donc $\bigsqcup_{s \in S} R_s = (\mathbb{Z}/p\mathbb{Z})^*$. Ainsi,

en passant aux cardinaux,

$$p - 1 = \left| \bigsqcup_{s \in S} R_s \right| = \sum_{s \in S} |R_s| \leq \sum_{s \in S} n = n|S|. \text{ Ceci démontre que } |S| \geq \frac{p-1}{n}.$$

9°) Notons $\mathcal{P} = \{aS / a \in (\mathbb{Z}/p\mathbb{Z})^*\}$ et $k = |\mathcal{P}|$.

On a vu que \mathcal{P} est une partition de $(\mathbb{Z}/p\mathbb{Z})^*$,

donc en passant aux cardinaux, $p - 1 = \sum_{c \in \mathcal{P}} |c|$.

Soit $c \in \mathcal{P}$. Il existe $a \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $c = aS$.

Notons $f : (\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$. f est clairement une bijection dont la bijection réciproque est $x \mapsto a^{-1}x$, or $aS = f(S)$, donc $|c| = |S|$.

On en déduit que $p - 1 = |S| \sum_{c \in \mathcal{P}} 1 = |S|k$.

Ainsi, $k = \frac{p-1}{|S|}$, or d'après la question précédente, $n \geq \frac{p-1}{|S|}$, donc $k = |\mathcal{P}| \leq n$.

Partie III : Théorème de Schur

10°) Soit C un ensemble de cardinal n et soit d une application de $(\mathbb{Z}/p\mathbb{Z})^*$ dans C . Notons N' (à la place de N) l'entier fourni par le théorème de Ramsey. On peut imposer $N' \geq 2$.

Posons $V = (\mathbb{Z}/p\mathbb{Z})^*$. On munit V d'un ordre arbitraire total noté \leq , ce qui est possible car V est fini. On notera $<$ l'ordre strict associé.

Pour tout $i, j \in V$ avec $i < j$, posons $c(\{i, j\}) = d(i - j)$. Ainsi, c est un coloriage de $K(V)$ dans C .

Posons $N = N' + 1$ et supposons que $p \geq N$. Alors $|V| = p - 1 \geq N'$, donc d'après le théorème de Ramsey, il existe $i, j, k \in V$, deux à deux distincts, tels que

$$c(\{i, j\}) = c(\{i, k\}) = c(\{j, k\}).$$

Quitte à permuter i, j, k , on peut supposer que $i < j < k$.

Alors, $d(i - j) = d(j - k) = d(i - k)$.

Posons $x = i - j$, $y = j - k$ et $z = i - k$. Alors $d(x) = d(y) = d(z)$ et $x + y = z$.

11°) Notons à nouveau N l'entier de la question précédente et supposons que $p \geq N$. D'après la question 9, il existe un ensemble C de cardinal n tel que $\mathcal{P} \subset C$.

Pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^*$, posons $d(a) = aS$. Ainsi d est une application de $(\mathbb{Z}/p\mathbb{Z})^*$ dans C , donc d'après la question précédente, il existe $x', y', z' \in (\mathbb{Z}/p\mathbb{Z})^*$ tels que $d(x') = d(y') = d(z')$ et $x' + y' = z'$.

Il existe $a \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $d(x') = d(y') = d(z') = aS$.

$x' \in x'S = d(x') = aS$, donc il existe $x \in \mathbb{Z} \setminus p\mathbb{Z}$ tel que $x' = a\bar{x}^n$.

De même, il existe $y, z \in \mathbb{Z} \setminus p\mathbb{Z}$ tels que $y' = a\bar{y}^n$ et $z' = a\bar{z}^n$.

Dans $\mathbb{Z}/p\mathbb{Z}$, on a donc $a\bar{x}^n + a\bar{y}^n = a\bar{z}^n$, or $a \in (\mathbb{Z}/p\mathbb{Z})^*$ et $\mathbb{Z}/p\mathbb{Z}$ est intègre, donc $\bar{x}^n + \bar{y}^n = \bar{z}^n$. Ainsi, $x^n + y^n \equiv z^n [p]$.

De plus, $x, y, z \in \mathbb{Z} \setminus p\mathbb{Z}$, donc x, y et z sont tous les trois non congrus à 0 modulo p .

Second problème :

Inverses généralisés d'applications linéaires

Partie I : préliminaires

1°) \diamond Soit $x \in E$. $E = F + G$, donc il existe $f \in F$ et $g \in G$ tels que $x = f + g$.

Alors, par hypothèse, il existe $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ tels que $f = \sum_{i=1}^p \alpha_i e_i$ et $g = \sum_{i=p+1}^n \alpha_i e_i$,

donc $x = \sum_{i=1}^n \alpha_i e_i$, ce qui prouve que (e_1, \dots, e_n) est une famille génératrice de E .

\diamond Soit $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ tels que $\sum_{i=1}^n \alpha_i e_i = 0$. Posons $f = \sum_{i=1}^p \alpha_i e_i$ et $g = \sum_{i=p+1}^n \alpha_i e_i$.

Alors $f \in F$, $g \in G$ et $f + g = 0$, or la somme $F + G$ est directe, donc $f = g = 0$.

Cependant (e_1, \dots, e_p) et (e_{p+1}, \dots, e_n) sont libres, donc pour tout $i \in \mathbb{N}_n$, $\alpha_i = 0$. Ceci prouve que (e_1, \dots, e_n) est une famille libre de E .

En conclusion, (e_1, \dots, e_n) est une base de E .

\diamond La dimension d'un espace vectoriel étant égale au nombre d'éléments de l'une de ses bases, on a $\dim(F) = p$, $\dim(G) = n - p$ et $\dim(E) = n$,

donc $\dim(E) = \dim(F) + \dim(G)$.

2°) Soit $x \in E$. (e_1, \dots, e_n) étant une famille génératrice de E , il existe $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ tels que $x = \sum_{i=1}^n \alpha_i e_i$. Alors $x = \sum_{i=1}^p \alpha_i e_i + \sum_{i=p+1}^n \alpha_i e_i \in F + G$, donc $E = F + G$.

Soit $x \in F \cap G$. Alors, il existe $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ tels que $x = \sum_{i=1}^p \alpha_i e_i = \sum_{i=p+1}^n (-\alpha_i) e_i$.

Alors $\sum_{i=1}^n \alpha_i e_i = x - x = 0$, or (e_1, \dots, e_n) est libre, donc pour tout $i \in \mathbb{N}_n$, $\alpha_i = 0$.

Ainsi, $x = 0$, ce qui prouve que $F \cap G = \{0\}$.

On a donc montré que $E = F \oplus G$.

3°) \diamond Pour tout $x \in H$, $u(x) \in \text{Im}(u)$, donc l'application $u|_H^{\text{Im}(u)}$ est bien définie. Pour cette question, on pose $v = u|_H^{\text{Im}(u)}$.

Soit $x \in H$ tel que $v(x) = 0$. Alors $u(x) = 0$, donc $x \in \text{Ker}(u) \cap H = \{0\}$, car la somme $H + \text{Ker}(u)$ est directe. Ainsi, $\text{Ker}(v) = \{0\}$, donc v est injective.

Soit $y \in \text{Im}(u)$. Il existe $x \in E$ tel que $y = u(x)$. De plus, $\text{Ker}(u) \oplus H = E$, donc il existe $h \in H$ et $k \in \text{Ker}(u)$ tel que $x = h + k$. Alors $y = u(x) = u(h) = v(h)$. Ceci prouve que v est surjective.

D'après le cours, par restriction et corestriction d'une application linéaire, v reste linéaire. On a donc montré que v est un isomorphisme de H sur $\text{Im}(u)$.

\diamond On en déduit que $\dim(H) = \dim(\text{Im}(u)) = \text{rg}(u)$, de plus d'après la question précédente, $\dim(H) + \dim(\text{Ker}(u)) = \dim(E)$, donc $\dim(E) = \text{rg}(u) + \dim(\text{Ker}(u))$.

4°) \diamond Notons $F = \{x \in E \mid p(x) = x\}$.

Si $x \in F$, alors $x = p(x) \in \text{Im}(p)$, donc $F \subset \text{Im}(p)$.

Soit $x \in \text{Im}(p)$. Il existe $y \in E$ tel que $x = p(y)$. Alors $p(x) = p^2(y)$, or par hypothèse, $p^2 = p$, donc $p(x) = p(y) = x$. Ainsi $x \in F$, ce qui prouve que $\text{Im}(p) \subset F$.

On a montré par double inclusion que $\text{Im}(p) = \{x \in E \mid p(x) = x\}$.

\diamond Soit $x \in \text{Im}(p) \cap \text{Ker}(p)$. Alors d'après le point précédent, $x = p(x) = 0$, donc $\text{Im}(p) \cap \text{Ker}(p) = \{0\}$, ce qui prouve que la somme $\text{Im}(p) + \text{Ker}(p)$ est directe.

Soit $x \in E$. $p(x - p(x)) = p(x) - p^2(x) = 0$, donc $x - p(x) \in \text{Ker}(p)$.

Ainsi, $x = p(x) + (x - p(x)) \in \text{Im}(p) \oplus \text{Ker}(p)$. Ceci prouve que $E = \text{Im}(p) \oplus \text{Ker}(p)$.

Partie II : g-inverses

5°) \diamond Soit $v \in L(F, E)$. v est un g-inverse de 0 si et seulement si $0 = 0$, donc tout élément de $L(F, E)$ est un g-inverse de 0.

\diamond Supposons que u est un isomorphisme. Soit $v \in L(F, E)$.

Supposons que v est un g-inverse de u . Alors $uvu = u$, donc en multipliant cette égalité respectivement à gauche et à droite par u^{-1} , on obtient que $vu = \text{Id}_E$ et $uv = \text{Id}_F$.

Ainsi, $v = u^{-1}$.

Réciproquement, si $v = u^{-1}$, il est clair que $uvu = u$.

Ainsi, lorsque u est un isomorphisme, il possède un unique g-inverse, égal à son inverse. Ainsi la notion de g-inverse généralise bien la notion d'inverse.

6.a) Par associativité de la composition, $q^2 = (uv)(uv) = (uvu)v = uv = q$, donc q est un projecteur. De même, $p^2 = vuvv = vu = p$, donc p est un projecteur.

6.b) \diamond Soit $x \in \text{Im}(q)$. Alors d'après la question 4, $x = q(x) = u(v(x)) \in \text{Im}(u)$.

Réciproquement, si $x \in \text{Im}(u)$, il existe $y \in F$ tel que $x = u(y)$.

Alors $q(x) = uvu(y) = u(y) = x$, donc $x \in \text{Im}(q)$.

Ainsi, on a montré que $\text{Im}(q) = \text{Im}(u)$.

\diamond Soit $x \in \text{Ker}(u)$. Alors $p(x) = v(u(x)) = v(0) = 0$, donc $x \in \text{Ker}(p)$.

Réciproquement, soit $x \in \text{Ker}(p)$. Alors $u(x) = uvu(x) = u(p(x)) = 0$,

donc $x \in \text{Ker}(u)$. Ainsi, on a montré que $\text{Ker}(p) = \text{Ker}(u)$.

6.c) $p \in L(E)$, donc d'après la formule du rang,

$$\text{rg}(p) = \dim(E) - \dim(\text{Ker}(p)) = \dim(E) - \dim(\text{Ker}(u)) = \text{rg}(u).$$

De plus, $\text{Im}(q) = \text{Im}(u)$, donc $\text{rg}(u) = \text{rg}(q)$. Ainsi, $\text{rg}(p) = \text{rg}(q) = \text{rg}(u)$.

Si $x \in \text{Im}(p)$, alors $x = p(x) = vu(x) = v(u(x)) \in \text{Im}(v)$, donc $\text{Im}(p) \subset \text{Im}(v)$, puis en passant aux dimensions, $\text{rg}(p) \leq \text{rg}(v)$, ce qui conclut.

6.d) \diamond Posons $E_1 = \text{Im}(p)$. p étant un projecteur, d'après la question 4,

$$E = E_1 \oplus \text{Ker}(p) = E_1 \oplus \text{Ker}(u).$$

Alors d'après la question 3, la quantité $\left(u|_{E_1}^{\text{Im}(u)}\right)^{-1}$ est bien définie.

\diamond Soit $y \in \text{Im}(u)$. Alors $v(y) \in v(\text{Im}(u)) = v(u(E)) = \text{Im}(vu) = \text{Im}(p) = E_1$. Ainsi, la quantité $v|_{\text{Im}(u)}^{E_1}$ est également bien définie.

Posons $a = u|_{E_1}^{\text{Im}(u)}$ et $b = v|_{\text{Im}(u)}^{E_1}$. Il reste à montrer que $ab = \text{Id}_{\text{Im}(u)}$ et que $ba = \text{Id}_{E_1}$, c'est-à-dire que, pour tout $x \in E_1$ et $y \in \text{Im}(u)$, $ba(x) = x$ et $ab(y) = y$.

\diamond Soit $x \in E_1$. $ba(x) = vu(x) = p(x) = x$ car $E_1 = \text{Im}(p)$ et p est un projecteur.

Soit $y \in \text{Im}(u)$. $ab(y) = uv(y) = q(y)$, or $y \in \text{Im}(q)$ et q est un projecteur, donc $q(y) = y$, puis $ab(y) = y$, ce qui conclut.

7°) \diamond Soit $v \in L(F, E)$.

Notons (C) la condition suivante : il existe un sous-espace vectoriel E_1 de E vérifiant

$$E = E_1 \oplus \text{Ker}(u), v(\text{Im}(u)) \subset E_1 \text{ et } v|_{\text{Im}(u)}^{E_1} = \left(u|_{E_1}^{\text{Im}(u)}\right)^{-1}.$$

La question précédente montre que si v est un g-inverse de u , alors (C) est vraie.

Réciproquement, supposons que (C) est vraie et montrons que v est un g-inverse de u .

Soit $x \in E$. Posons $y = u(x)$. Alors $y \in \text{Im}(u)$, donc $v(y) \in E_1$.

Ainsi, $uv(y) = u|_{E_1}^{\text{Im}(u)} \circ v|_{\text{Im}(u)}^{E_1}(y) = \text{Id}_{\text{Im}(u)}(y) = y$, or $y = u(x)$, donc $uvu(x) = u(x)$, pour tout $x \in E$. Ceci prouve que $uvu = u$, ce qui conclut : on a montré que v est un g-inverse si et seulement si (C) est vérifiée.

\diamond Notons $r = \text{rg}(u)$ et $n = \dim(E)$. Alors d'après la formule du rang,

$\dim(\text{Ker}(u)) = n - r$. Ainsi, d'après le cours, il existe une base (e_{r+1}, \dots, e_n) de $\text{Ker}(u)$.

Toujours d'après le cours, on peut compléter cette famille libre en une base de E , notée (e_1, \dots, e_n) . Posons $E_1 = \text{Vect}(e_1, \dots, e_r)$. Alors d'après la question 2, $E_1 \oplus \text{Ker}(u) = E$.

◇ On effectue une construction similaire dans F : il existe une base (f_1, \dots, f_r) de $\text{Im}(u)$, que l'on complète en une base (f_1, \dots, f_p) de F , où $p = \dim(F)$.

Alors, en posant $G = \text{Vect}(f_{r+1}, \dots, f_p)$, on a $G \oplus \text{Im}(u) = F$.

◇ Soit s un entier compris entre $\text{rg}(u) = r$ et $\min(\dim(E), \dim(F)) = \min(n, p)$.

Pour tout $i \in \mathbb{N}_r$, $f_i \in \text{Im}(u)$, donc on peut poser $v(f_i) = \left(u|_{E_1}^{\text{Im}(u)}\right)^{-1}(f_i)$.

Pour tout $i \in \{r+1, \dots, s\}$, posons $v(f_i) = e_i$ et

pour tout $i \in \{s+1, \dots, p\}$, posons $v(f_i) = 0$. On a ainsi défini les images par v des vecteurs de la base (f_1, \dots, f_n) de F , donc ces conditions définissent une application $v \in L(F, E)$.

Par construction, $v|_{\text{Im}(u)}^{E_1}$ est bien défini et coïncide avec $\left(u|_{E_1}^{\text{Im}(u)}\right)^{-1}$ sur les vecteurs de la base (f_1, \dots, f_r) de $\text{Im}(u)$, donc $v|_{\text{Im}(u)}^{E_1} = \left(u|_{E_1}^{\text{Im}(u)}\right)^{-1}$. Ainsi, la condition (C) est réalisée, ce qui prouve que v est un g-inverse de u .

◇ Posons $H = \text{Vect}(e_{r+1}, \dots, e_s)$. $H \subset \text{Ker}(u)$, donc $H \cap E_1 \subset \text{Ker}(u) \cap E_1 = \{0\}$. Ainsi H et E_1 sont en somme directe et on peut poser $E' = E_1 \oplus H$.

$v|_{\text{Im}(u)}^{E_1}$ est un isomorphisme de $\text{Im}(u)$ dans E_1 , donc $(v(f_1), \dots, v(f_r))$ est une base de E_1 . De plus (e_{r+1}, \dots, e_s) est libre en tant que sous-famille d'une famille libre, donc c'est une base de H . Alors d'après la question 1, $(v(f_1), \dots, v(f_r), e_{r+1}, \dots, e_s)$ est une base de E' .

◇ $v(F) = v(\text{Vect}(f_1, \dots, f_p))$, donc d'après le cours,

$$\begin{aligned} v(F) &= \text{Vect}(v(f_1), \dots, v(f_p)) \\ &= \text{Vect}(v(f_1), \dots, v(f_r), e_{r+1}, \dots, e_s, 0, \dots, 0) \\ &= \text{Vect}(v(f_1), \dots, v(f_r), e_{r+1}, \dots, e_s) = E'. \end{aligned}$$

Ainsi, $\text{rg}(v) = \dim(v(F)) = \dim(E') = s$.

On a donc montré qu'il existe un g-inverse de rang s .

◇ $r = \text{rg}(u) \leq p$ car $\text{Im}(u) \subset F$ et d'après la formule du rang, $r = n - \dim(\text{Ker}(u)) \leq n$, donc $r \leq \min(p, n)$. Ainsi, il existe au moins un entier compris entre $\text{rg}(u) = r$ et $\min(\dim(E), \dim(F)) = \min(n, p)$. Alors ce qui précède montre que u possède bien au moins un g-inverse.

8.a) Soit $v \in L(F, E)$. Notons (E) l'équation $uvu = u$, d'inconnue v .

Notons
$$\begin{array}{ccc} \varphi : L(F, E) & \longrightarrow & L(E, F) \\ v' & \longmapsto & uv'u \end{array}$$
. Alors (E) $\iff \varphi(v) = u$.

Pour tout $v', v'' \in L(F, E)$, pour tout $\alpha \in \mathbb{K}$, il est clair que $u(\alpha v' + v'')u = \alpha uv'u + uv''u$, car u est linéaire. Ceci montre que φ est une application linéaire, donc (E) est une équation linéaire. Alors,

(E) $\iff \varphi(v) = \varphi(v_0) \iff \varphi(v - v_0) = 0 \iff v - v_0 \in \text{Ker}(\varphi)$.

Ceci montre que l'ensemble des g-inverses de u est $v_0 + A$, où $A = \text{Ker}(\varphi)$ est bien un sous-espace vectoriel de $L(F, E)$. On a $A = \{w \in L(F, E) \mid uww = 0\}$.

8.b) ◇ Soit $w \in L(F, E)$.

$$\begin{aligned}
w \in A &\iff (\forall x \in E, uw(u(x)) = 0) \\
&\iff (\forall y \in \text{Im}(u), u(w(y)) = 0) \\
&\iff (\forall y \in \text{Im}(u), w(y) \in \text{Ker}(u)) \\
&\iff w(\text{Im}(u)) \subset \text{Ker}(u).
\end{aligned}$$

En particulier, lorsque $w \in A$, la quantité $w|_{\text{Im}(u)}^{\text{Ker}(u)}$ est bien définie. On peut donc poser $\varphi(w) = w|_{\text{Im}(u)}^{\text{Ker}(u)}$.

$$\begin{aligned}
\diamond \text{ Soit } w, w' \in A \text{ et } \alpha \in \mathbb{K}. \text{ Soit } x \in \text{Im}(u). \text{ Alors} \\
\varphi(\alpha w + w')(x) &= (\alpha w + w')(x) = \alpha(w(x)) + w'(x) \\
&= \alpha\varphi(w)(x) + \varphi(w')(x) = (\alpha\varphi(w) + \varphi(w'))(x).
\end{aligned}$$

C'est vrai pour tout $x \in \text{Im}(u)$, donc $\varphi(\alpha w + w') = \alpha\varphi(w) + \varphi(w')$, ce qui prouve que φ est linéaire.

\diamond Soit $\omega \in L(\text{Im}(u), \text{Ker}(u))$. Notons à nouveau (f_1, \dots, f_r) une base de $\text{Im}(u)$ et (e_{r+1}, \dots, e_n) une base de $\text{Ker}(u)$. On les complète en une base (f_1, \dots, f_p) de F et une base (e_1, \dots, e_n) de E .

pour tout $i \in \mathbb{N}_r$, posons $w(f_i) = \omega(f_i)$ et pour tout $i \in \{r+1, \dots, p\}$, posons $w(f_i) = 0$. Ceci définit une unique application $w \in L(F, E)$.

De plus, $w(\text{Im}(u)) = w(\text{Vect}(f_1, \dots, f_r)) = \text{Vect}(\omega(f_1), \dots, \omega(f_r)) \subset \text{Ker}(u)$, donc d'après ce qui précède, $w \in A$.

De plus, $\varphi(w)$ et ω coïncident par construction sur (f_1, \dots, f_r) qui est une base de $\text{Im}(u)$, donc $\varphi(w) = \omega$. Ceci prouve que φ est surjective.

8.c)

$$\diamond \text{ Soit } w \in A. w \in \text{Ker}(\varphi) \iff (\forall x \in \text{Im}(u), w(x) = 0) \iff w(\text{Im}(u)) = \{0\}.$$

Reprenons les notations du 7.b. Pour tout $w \in \text{Ker}(\varphi)$, posons $\Psi(w) = (w(f_{r+1}), \dots, w(f_p))$. Ainsi, Ψ est une application de $\text{Ker}(\varphi)$ dans E^{p-r} . Elle est clairement linéaire.

Soit $g = (g_{r+1}, \dots, g_p) \in E^{p-r}$. Soit $w \in \text{Ker}(\varphi)$.

$$\text{Alors } \Psi(w) = g \iff [(\forall i \in \mathbb{N}_r, w(f_i) = 0) \text{ et } (\forall i \in \{r+1, \dots, p\}, w(f_i) = g_i)].$$

D'après le cours, ceci définit une unique application linéaire w de F dans E , car (f_1, \dots, f_p) est une base de F . De plus cette application w est bien dans A , donc Ψ est une bijection. C'est donc un isomorphisme.

$$\diamond \text{ On en déduit que } \dim(\text{Ker}(\varphi)) = \dim(E^{p-r}) = n(p-r).$$

Alors, d'après la formule du rang,

$$\begin{aligned}
\dim(A) &= \dim(\text{Ker}(\varphi)) + \dim(\text{Im}(\varphi)) \\
&= n(p-r) + \dim(L(\text{Im}(u), \text{Ker}(u))) \\
&= n(p-r) + r(n-r) \\
&= np - r^2.
\end{aligned}$$

En conclusion, $\boxed{\dim(A) = \dim(E)\dim(F) - \text{rg}(u)^2}$.

9°) \diamond Supposons que (\mathcal{E}) possède au moins une solution $x \in E$.

$$\text{Alors } b = u(x) = uvu(x) = uv(u(x)) = uv(b).$$

\diamond Réciproquement, supposons que $uv(b) = b$. Soit $x \in E$.

$(\mathcal{E}) \iff u(x) = b = uv(b) \iff u(x-v(b)) = 0 \iff x-v(b) \in \text{Ker}(u)$. Ainsi l'ensemble \mathcal{S} des solutions de l'équation (\mathcal{E}) est $v(b) + \text{Ker}(u)$.

Ce dernier ensemble est non vide, car il contient $v(b)$, donc on a montré que (\mathcal{E}) possède au moins une solution si et seulement si $b = (uv)(b)$.

De plus, d'après la question 6.b, $\text{Ker}(u) = \text{Ker}(p)$.

Soit $x \in \text{Ker}(p)$. Alors $x = x - p(x) \in \{(\text{Id}_E - p)(z) / z \in E\}$.

Réciproquement, s'il existe $z \in E$ tel que $x = (\text{Id}_E - p)(z)$, alors $p(x) = p(z) - p^2(z) = 0$, car p est un projecteur, donc $x \in \text{Ker}(p)$.

Ceci démontre que $\text{Ker}(u) = \text{Ker}(p) = \{(\text{Id}_E - p)(z) / z \in E\}$, or $p = vu$, donc $\mathcal{S} = \{v(b) + (\text{Id}_E - vu)(z) / z \in E\}$, ce qui conclut.