Examen 2022/2023 (2ème Session) - Correction
4M003 - Algèbre commutative
Anna Cadoret

Durée: 2:00

Préambule: On rappelle que tous les anneaux sont commutatifs unitaires sauf mention du contraire. Si A est un anneau et $I_1, \dots, I_r \subset A$ un idéal, on rappelle aussi que $I_1 \cdots I_r \subset A$ est l'idéal engendré par les éléments de la forme $a_1 \cdots a_r$, $a_i \in I_i$, $i = 1, \dots, r$; autrement dit un élement de $I_1 \cdots I_r$ est une combinaison A-linéaire d'éléments de la forme $a_1 \cdots a_r$, $a_i \in I_i$, $i = 1, \dots, r$.

Problème Soit A un anneau. On dit qu'un idéal $\mathfrak{q} \subset A$ est primaire si $\mathfrak{q} \subsetneq A$ et pour tout $a, b \in A$, $ab \in \mathfrak{q}$ $\Rightarrow a \in \mathfrak{q}$ ou $b^n \in \mathfrak{q}$ pour un certain entier $n \geq 1$.

(1) On a tautologiquement:
- $\mathfrak{q} \subsetneq A$ ssi $A/\mathfrak{q} \neq 0$ et;
- ($ab \in \mathfrak{q} \Rightarrow a \in \mathfrak{q}$ ou $b^n \in \mathfrak{q}$) ssi ($\overline{a}\overline{b} = \overline{0}$ dans $A/\mathfrak{q} \Rightarrow \overline{a} = 0$ ou $\overline{b}^n = 0$ dans $A/\mathfrak{q}$).

(2) Soit $\phi : A \to B$ un morphisme d'anneaux. On a la factorisation canonique

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow & & \downarrow p_{\mathfrak{q}} \\ A/\phi^{-1}(\mathfrak{q}) & \xrightarrow{\overline{\phi}} & B/\mathfrak{q} \end{array}$$

avec, puisque $\phi^{-1}(\mathfrak{q}) = \ker(p_{\mathfrak{q}} \circ \phi)$, $\overline{\phi} : A/\phi^{-1}(\mathfrak{q}) \hookrightarrow B/\mathfrak{q}$ injectif; en particulier $\overline{\phi}^{-1}(\sqrt{\overline{0}}) \subset \sqrt{\overline{0}}$.

(3) Pour tout $a, b \in A$ on a $ab \in \sqrt{\mathfrak{q}}$ ssi il existe $n \geq 1$ tel que $a^n b^n \in \mathfrak{q}$ ce qui, puisque $\mathfrak{q}$ est primaire, équivaut à $a^n \in \mathfrak{q}$ ($\Rightarrow a \in \sqrt{\mathfrak{q}}$) ou il existe $N \geq 1$ tel que $b^{nN} \in \mathfrak{q}$ ($\Rightarrow b \in \sqrt{\mathfrak{q}}$). Cela montre donc que $\sqrt{\mathfrak{q}} \in \mathrm{spec}(A)$. Si maintenant $\mathfrak{p} \in \mathrm{spec}(A)$ est tel que $\mathfrak{q} \subset \mathfrak{p}$ alors

$$\sqrt{\mathfrak{q}} \stackrel{\mathrm{def}}{=} \bigcap_{\mathfrak{p}' \in \mathrm{spec}(A) \mid \mathfrak{p}' \supset \mathfrak{q}} \mathfrak{p}'.$$

Donc $\sqrt{\mathfrak{q}}$ est bien le plus petit idéal premier de A contenant $\mathfrak{q}$.

(4) Soit k un corps.

(a) Notons $I := \langle X \rangle$ et $J := \langle Y^2 \rangle$ de sorte que $\mathfrak{q} := I + J$ donc $A/\mathfrak{q} \simeq (A/I)/((I+J)/I) \simeq k[Y]/Y^2$. Or pour tout $P, Q \in k[Y]$, $\overline{PQ} = \overline{0}$ dans $k[Y]/Y^2$ ssi $Y^2 | PQ$ ce qui, par factorialité de $k[Y]$, équivaut à $Y^2 | P$ ou $Y | Q$ ($\Rightarrow \overline{Q}^2 = \overline{0}$ dans $k[Y]/Y^2$). Donc $\mathfrak{q}$ est bien primaire. En outre, $\sqrt{\mathfrak{q}}$ est l'image inverse de $\sqrt{\overline{0}}$ par $A \twoheadrightarrow A/\mathfrak{q} \simeq (A/I)/(I + J/I) \simeq k[Y]/Y^2$ et comme $\sqrt{\overline{0}} = \langle \overline{Y} \rangle$, on a $\sqrt{\mathfrak{q}} = \langle X, Y \rangle$ donc $\mathfrak{p}^2 \subsetneq \mathfrak{q}$ puisque $X \notin \mathfrak{p}^2$ (factorialité de $k[X, Y]$) et $\mathfrak{q} \subsetneq \mathfrak{p}$ puisque $Y \notin \mathfrak{q}$ (factorialité de $k[X, Y]$).

(b) On a $A/\mathfrak{p} = (k[X, Y, Z]/\langle XY - Z^2 \rangle)/(\langle XY - Z^2, X, Z \rangle/\langle XY - Z^2 \rangle) \simeq k[X, Y, Z]/\langle XY - Z^2, X, Z \rangle \simeq k[Y]$ est intègre donc $\mathfrak{p}$ est bien un idéal premier de A. Par contre, on a $\mathfrak{p}^2 = \langle x^2, z^2, xz \rangle$ donc $A/\mathfrak{p}^2 = (k[X, Y, Z]/\langle XY - Z^2 \rangle)/(\langle XY - Z^2, X^2, Z^2, XZ \rangle/\langle XY - Z^2 \rangle) \simeq k[X, Y, Z]/\langle XY - Z^2, X^2, Z^2, XZ \rangle \simeq k[X, Y, Z]/\langle X^2, Z^2, XY, XZ \rangle$. En particulier, $y \in k[X, Y, Z]/\langle X^2, Z^2, XY, XZ \rangle$ est un diviseur de zéro qui n'est pas nilpotent.

(5) D'après (1), $\mathfrak{q} \subset A$ est primaire ssi, tout diviseur de zéro est nilpotent dans $A/\mathfrak{q}$. Mais,

$$\sqrt{\mathfrak{q}}/\mathfrak{q} = \sqrt{\overline{0}_{A/\mathfrak{q}}} = \bigcap_{\mathfrak{p} \in \mathrm{spec}(A) \mid \mathfrak{p} \supset \mathfrak{q}} (\mathfrak{p}/\mathfrak{q}).$$

Par maximalité de $\sqrt{\mathfrak{q}}$, cela impose que $A/\mathfrak{q}$ est local, d'unique idéal maximal $\sqrt{\overline{0}}$, dc tout élément de $A/\mathfrak{q}$ est soit inversible, soit nilpotent. Pour tout idéal strict $\mathfrak{m} \subsetneq A$ on a tjs $\mathfrak{m} \subset \sqrt{\mathfrak{m}^n} \subset A$. Si de plus $\mathfrak{m} \subset A$ est maximal, on a dc $\mathfrak{m} = \sqrt{\mathfrak{m}^n}$ et dc, par la première partie de la question, $\mathfrak{m}^n$ est $\mathfrak{m}$-primaire.

(6) Soit $\mathfrak{p} \subset A$ un idéal premier. Soit $I_1, \dots, I_r$ des idéaux $\mathfrak{p}$-primaires et $I := I_1 \cap \cdots \cap I_r$. On a tautologiquement $\sqrt{I} \subset \sqrt{I_1} \cap \cdots \cap \sqrt{I_r} = \mathfrak{p}$. Inversement, pour tout $a \in \mathfrak{p} = \sqrt{I_1} = \cdots = \sqrt{I_r}$ et pour

$i = 1, \dots, r$, il existe $n_i \geq 1$ such that $a^{n_i} \in I_i$. Donc pour $n \geq n_1, \dots, n_r$ on a $a^n \in I_1 \cap \cdots \cap I_r = I$ *i.e.* $\mathfrak{p} \subset \sqrt{I}$. Cela montre déjà que $\mathfrak{p} = \sqrt{I}$. Soit maintenant $a, b \in A$ tels que $a \notin \sqrt{I}$ mais $ab \in I$. Comme $a \notin \sqrt{I}$, Il existe $1 \leq i \leq r$ tel que $a \notin \sqrt{I_i}$ mais comme $ab \in I_i$ et I_i est ($\mathfrak{p}$-)primaire, $b \in \sqrt{I}_i = \mathfrak{p} = \sqrt{I}$. Cela montre que I est primaire.

(7) Pour tout $x \in J$, la multiplication par x définit un morphisme de A-modules $R_x : A \to A$, $a \mapsto ax$; en particulier, $R_x^{-1}(I) \subset A$ est un sous-A module *viz* un idéal de A donc $(I : J) = \cap_{x \in J} R_x^{-1}(I)$ est un idéal de A comme intersection d'idéaux de A. Soit maintenant $\mathfrak{q} \subset A$ un idéal $\mathfrak{p}$-primaire et $a \in A$.

(a) Supposons $a \in \mathfrak{q}$. On a tautologiquement $1 \cdot a \in \mathfrak{q}$ donc $1 \in (\mathfrak{q} : a)$;

(b) Supposons $a \notin \mathfrak{q}$. Pour tout $x \in \sqrt{(\mathfrak{q} : a)}$ il existe $n \geq 1$ tq $x^n a \in \mathfrak{q}$. Mais comme $\mathfrak{q}$ est primaire et $a \notin \mathfrak{q}$, $x^n \in \mathfrak{q}$ *i.e.* $x \in \sqrt{\mathfrak{q}} = \mathfrak{p}$. Cela montre déjà que $\sqrt{(\mathfrak{q} : a)} \subset \mathfrak{p}$. Inversement, comme, tautologiquement, $\mathfrak{q} \subset (\mathfrak{q} : a)$, on a $\mathfrak{p} = \sqrt{\mathfrak{q}} \subset \sqrt{(\mathfrak{q} : a)}$. Soit maintenant $x, y \in A$ tels que $x \notin (\mathfrak{q} : a)$ mais $xy \in (\mathfrak{q} : a)$ *i.e.* $xya \in \mathfrak{q}$. Comme $x \notin (\mathfrak{q} : a)$, $xa \notin \mathfrak{q}$ et comme $\mathfrak{q}$ est primaire, cela impose $y \in \sqrt{\mathfrak{q}} = \mathfrak{p} = \sqrt{(\mathfrak{q} : a)}$. Donc $(\mathfrak{q} : a)$ est bien primaire.

(c) Supposons $a \notin \mathfrak{p} = \sqrt{\mathfrak{q}}$. On a toujours $\mathfrak{q} \subset (\mathfrak{q} : a)$. Inversement, pour tout $x \in (\mathfrak{q} : a)$, $xa \in \mathfrak{q}$. Or comme $\mathfrak{q}$ est $\mathfrak{p}$-primaire et $a \notin \mathfrak{p}$, nécessairement $x \in \mathfrak{q}$.

(8) On dit qu'un idéal $I \subset A$ est décomposable s'il existe des idéaux primaires $\mathfrak{q}_1, \dots, \mathfrak{q}_r \subset A$ tels que

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r.$$

(a) Supposons $I \subset A$ décomposable et soit $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ une décomposition de I en idéaux primaires. Par (6), on peut supposer (i) puis, si $\cap_{j \neq i} \mathfrak{q}_j \subset \mathfrak{q}_i$ supprimer $\mathfrak{q}_i$ donc supposer (ii).

(b) Soit $I \subset A$ un idéal décomposable et $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ une décomposition minimale. Pour tout $a \in A$ on a

$$(I : a) = (\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r : a) = (\mathfrak{q}_1 : a) \cap \cdots \cap (\mathfrak{q}_r : a)$$

donc

$$\sqrt{(I : a)} = \sqrt{(\mathfrak{q}_1 : a) \cap \cdots \cap (\mathfrak{q}_r : a)} = \sqrt{(\mathfrak{q}_1 : a)} \cap \cdots \cap \sqrt{(\mathfrak{q}_r : a)} = \cap_{a \notin \mathfrak{q}_i} \mathfrak{p}_i,$$

où la dernière égalité résulte de (7). Comme la décomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ est minimale, on peut toujours trouver $a \in \cap_{j \neq i} \mathfrak{q}_j$ tel que $a \notin \mathfrak{q}_i$. Pour un tel a, on a $\sqrt{(I : a)} = \mathfrak{p}_i$, ce qui montre $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \supset \{\sqrt{(I : a)} \mid a \in A\} \cap \operatorname{spec}(A)$. Inversement, si $a \in A$ est tel que $\sqrt{(I : a)} \in \operatorname{spec}(A)$, on a vu en T.D. que $\sqrt{(I : a)} = \cap_{a \notin \mathfrak{q}_i} \mathfrak{p}_i$ implique $\sqrt{(I : a)} = \mathfrak{p}_i$ pour un certain $1 \leq i \leq r$ tel que $a \notin \mathfrak{q}_i$. (On rappelle l'argument: soit $I_1, \dots, I_r \subset A$ des idéaux de A tels que $\mathfrak{p} = \cap_{1 \leq i \leq r} I_i \in \operatorname{spec}(A)$. Supposons que pour tout $i = 1, \dots, r$ il existe $a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$. Alors $a_1 \cdots a_r \in \cap_{1 \leq i \leq r} \mathfrak{p}_i$ mais, puisque : $\mathfrak{p}$ est premier, $a_1 \cdots a_r \notin \mathfrak{p}$: contradiction).

(c) On a $I \subset \langle X \rangle \cap \langle X^2, Y \rangle$, Inversement, si $P \in \langle X \rangle \cap \langle X^2, Y \rangle$, on peut écrire $P = AX = BX^2 + CY$ donc $X | C$, ce qui montre que $\langle X \rangle \cap \langle X^2, Y \rangle \subset I$. L'idéal $\mathfrak{p} := \langle X \rangle$ est premier donc $\mathfrak{p}$-primaire. L'idéal $\mathfrak{q} := \langle X^2, Y \rangle$ n'est pas premier mais $A/\mathfrak{q} \simeq k[X]/\langle X^2 \rangle \simeq k[\epsilon]$ a un unique idéal non trivial: $\langle \epsilon \rangle$ donc $A/\mathfrak{q} = (A/\mathfrak{q})^\times \cup \langle \epsilon \rangle$, ce qui montre que tout élément de $A/\mathfrak{q}$ est soit inversible, soit nilpotent. On conclut par (1) que $\mathfrak{q}$ est primaire. En outre, $\langle X, Y \rangle \subset \sqrt{\mathfrak{q}} \subsetneq A$ donc, comme $\langle X, Y \rangle \subset A$ est un idéal maximal, $\langle X, Y \rangle = \sqrt{\mathfrak{q}}$. La décomposition $I = \langle X \rangle \cap \langle X^2, Y \rangle$ est donc bien une décomposition primaire minimale.

(9) On dit qu'un idéal $I \subset A$ est irréductible si pour tout iéaux $I_1, I_2 \subset A$, $I = I_1 \cap I_2$ implique $I = I_1$ ou $I = I_2$. On suppose maintenant que A est noetherien.

(a) Soit $\mathcal{E}$ l'ensemble des idéaux de A qui ne sont pas intersection finie d'idéaux irréductibles. Supposons $\mathcal{E} \neq \emptyset$. Par noetherianité, $\mathcal{E}$ admet un élément maximal, I. Comme $I \in \mathcal{E}$, I n'est en particulier pas irréductible, donc on peut écrire $I = I_1 \cap I_2$ avec $I \subsetneq I_1, I_2$. Par mximalitd de I, I_1, I_2 devrait être tout deux intersection finie d'idéaux irréductibles - donc $I = I_1 \cap I_2$ aussi: contradiction.

(b) Soit $I \subset A$ un idéal irréductible et soit $a \in A$. Par noetherianité la suite croissante d'idéaux $(I : a) \subset (I : a^2) \subset \cdots$ est stationnaire à partir d'un certain rang: $(I : a^n) = (I : a^{n+1})$. Donc pour tout $b \in A \setminus I$ tel que $ab \in I$, on doit avoir $Aa^n \cap Ab = I$ sinon, il existerait $c \in Aa \cap Ab$, $c \notin I$. Mais $c \in Ab$ implique $ac \in Aab \subset I$ alors que si $c = \alpha a^n \in Aa^n$, implique $ac = \alpha a^{n+1} \in I$ donc $\alpha \in (I : a^{n+1}) = (I : a^n)$ donc $c = \alpha a^n \in I$: contradiction. On a donc montré que $Aa^n \cap Ab = I$. Comme I est orréductible, on en déduit $I = Aa^n$ ou $I = Ab$ *i.e.* $a^n \in I$ ou $b \in I$.

(c) Cela résulte immédiatement de (9) (a)+(b).

Exercice Soit A un anneau (que l'on pourra supposer noetherien si l'on ne veut pas invoquer le lemme de Zorn).

(1) Soit M_1, M_2 deux A-modules simples non isomorphes et $\phi : M_1 \to M_2$ un morphisme de A-modules. Comme M_1 est simple, $\ker(\phi) = 0$ ou $\ker(\phi) = M_1$ (*i.e.* ϕ est le morphisme nul). Si $\ker(\phi) = 0$, $\phi : M_1 \to M_2$ est injectif dc non-nul et, comme M_2 est simple, cela force $im(\phi) = M_2$ *i.e.* $\phi : M_1 \tilde{\to} M_2$ est un isomorphisme: contradiction. Dc, nécessairement, ϕ est le morphisme nul.

(2) Soit M un A-module. L'implications (b) $\Rightarrow$ (a) est immédiate. Notons aussi que si $N', N'' \subset M$ sont deux sous-A-modules avec N' simple soit $N' \cap N'' = 0$ soit $N' \subset N''$.

- (a) $\Rightarrow$ (b): Notons $\mathcal{E}$ l'ensemble des sous-ensembles $J \subset I$ tq $M_J := \sum_{j\in J} M_j = \oplus_{i\in J} M_j$, $J \in \mathcal{E}$. Comme $I = \emptyset$, $\mathcal{E} \neq \emptyset$ (contient les singletons) et, muni de l'inclusion, $\mathcal{E}$ est ordonné inductif car si $J_1 \subset J_2 \subset \cdots I$ est une suite de sous-ensembles de I dans $\mathcal{E}$, on a, avec $J_\infty := \cup_{n\geq 1} J_n \subset I$, $\sum_{j\in J_\infty} M_j = \cup_{n\geq 1}(\sum_{j\in J_n} M_j) = \cup_{n\geq 1}(\oplus_{j\in J_n} M_j) = \oplus_{j\in J_\infty} M_j$. Dc, par Zorn, $\mathcal{E}$ admet un élément maximal J pour $\subset$. Supposons $M' := \oplus_{j\in J} M_j \subsetneq M$. Comme $M = \oplus_{i\in I} M_i$ avec les M_i, $i \in I$ simples, il existe au moins un $i \in I$ tq $M_i \cap M' = 0$ *i.e.* $M' \oplus M_i$ dc $J \subsetneq J \cup \{i\} \in \mathcal{E}$: contradiction.
- (a) $\Rightarrow$ (c): Soit $\mathcal{E}(M')$ l'ensemble des sous-A-modules N de M tq $N \cap M' = 0$. Comme $M' \subsetneq M$ et que $M = \oplus_{i\in I} M_i$ avec les M_i, $i \in I$ simples, il existe au moins un $i \in I$ tq $M_i \in \mathcal{E}(M')$ dc $\mathcal{E}(M') \neq \emptyset$. On vérifie facilement que $\mathcal{E}(M')$ muni de l'inclusion $\subset$ est ordonné inductif dc, par Zorn, admet un élément maximal M'' pour l'inclusion. Comme $M'' \in \mathcal{E}(M')$, $M' \oplus M''$. Si on avait $M' \oplus M'' \subsetneq M$, en réitérant l'argument, on aurait $\mathcal{E}(M' \oplus M'') \neq \emptyset$ donc pour tout $N \in \mathcal{E}(M' \oplus M'')$, $M'' \subsetneq M'' \oplus N \in \mathcal{E}(M')$: contradiction.
- (c) $\Rightarrow$ (a): Commençons par utiliser l'indication. Notons $\mathcal{E}$ l'ensemble des sous-A-modules de M qui sont somme de sous-A-modules simples. D'après l'indication, $\mathcal{E}$ est non vide. De plus $\mathcal{E}$ muni de l'inclusion est ordonné inductif car si $M_1 \subset M_2 \subset \cdots \subset M$ est une suite de sous-A-modules de M dans $\mathcal{E}$ alors $M_\infty := \cup_{n\geq 1} M_n \subset M$ est un sous-A-module de M et si on note $M_n = \sum_{i\in I_n} M_{i,n}$ avec $M_{i,n} \subset M_n$ sous-A-module simple, $i \in I_n$, $n \geq 1$ on a $M_\infty = \sum_{n\geq 1} \sum_{i\in I_n} M_{i,n}$ dc $M_\infty \in \mathcal{E}$. Donc par Zorn, $\mathcal{E}$ admet un élément maximal M' pour $\subset$. Si $M' \subsetneq M$, par (c) il existerait un sous-A-module $M'' \subset M$ non nul tel que $M \simeq M' \oplus M''$. Mais par l'indication M'' contiendrait alors un sous-A-module simple $N'' \subset M''$ donc on aurait $M' \subsetneq M' \oplus N''$ avec $M' \oplus N'' \in \mathcal{E}$, contredisant la maximalité de M'. Montrons maintenant l'indication. Soit $N \subset M$ un sous-A-module non-nul et $0 \neq n \in N$. Notons $I \subset A$ le noyau du morphisme de A-modules $R_n : A \to N$, $a \mapsto an$; I est un idéal de A dc, par Zorn, est contenu dans un idéal maximal $I \subset \mathfrak{m} \subset A$. On a $\mathfrak{m}/I \subset A/I \tilde{\to} An \subset N$. Notons N' l'image de $\mathfrak{m}/I$ dans An. Par (c), il existe un sous-A-module $N'' \subset M$ tel que $M = N' \oplus N''$. Mais alors $An = N' \oplus N'' \cap An$ (en effet, $an = n' + n''$ avec $n' \in N' \subset An$, $n'' \in N''$ implique $n'' = an - n' \in An$) et $N'' \cap An \subset N$ est un sous-A-module simple car pour tout sous A-module $N_1'' \subsetneq N'' \cap An$ on a $\mathfrak{m} \subset R_n^{-1}(N' \oplus N_1'') \subsetneq A$ dc, par maximalité de $\mathfrak{m}$, $\mathfrak{m} = R_n^{-1}(N' \oplus N_1'')$ et dc $N_1'' = 0$.

(3) Soit A un anneau principal. Soit M un A-module simple. Pour tout $0 \neq m \in M$ le morphisme de A-modules $R_m : A \to M$, $a \mapsto am$ est alors nécessairement surjectif et $R_m : A \to M$ induit un isomorphisme de A-modules $A/\ker(R_m) \tilde{\to} M$. En écrivant $\ker(R_m) := Aa$ et $a = \prod_p p^{v_p(a)}$ la décomposition de a en produit d'irréductible, par le lemme Chinois on a $\oplus A/p^{v_p(a)} \tilde{\to} M$. On en déduit immédiatement que M est simple ssi $M \simeq A/p$, $Ap \in spec(A)$. Puis M semisimple ssi $M \simeq \oplus_p (A/p)^{v_p(M)}$ avec les $v_p(M)$ des entiers positifs presque tous nuls.

(4) Soit maintenant k un corps et V un k-espace vectoriel de dimension fini.

(a) Soit $u \in End_k(V)$. Comme $k[T]$ est principal, on sait que $V_u \simeq \oplus_P \oplus_{n\geq 0} (k[T]/P^n)^{\oplus v_{P,n}}$. On a donc $u \in End_k(V)$ semisimple ssi $v_{P,n} = 0$, $n \geq 2$. Mais par ailleurs, le polynôme minimal de u vaut exactement $\Pi_u := \prod_P P^{n_{P,\infty}}$, où $n_{P,\infty} = 0$ si $v_{p,n} = 0$, $n \geq 1$ et $n_{P,\infty} = max\{n \geq 1 \mid v_{p,n} \neq 0\}$ sinon. Donc Π_u est sans facteurs carrés ssi $v_{P,n} = 0$, $n \geq 2$.

(b) On suppose ici $k = \mathbb{F}_2$ et V de $\mathbb{F}_2$-dimension 3. On se fixe une base de sorte qu'on identifie $End_{\mathbb{F}_2}(V) \simeq M_3(\mathbb{F}_2)$. Les classes de conjugaison dans $M_3(\mathbb{F}_2)$ sont en bijection avec les suites de polynômes unitaires de la forme P_1, $P_1|P_2$ ou $P_1|P_2|P_3$ tq $\sum_{i\geq 1} deg(P_i) = 3$ et le polynôme minimal des matrices dans la classe de conjugaison correspondant à P_1 (resp. $P_1|P_2$, resp. $P_1|P_2|P_3$) est P_1 (resp. P_2, resp. P_3). Les matrices semisimples correspondent donc aux suites P_1 (resp. $P_1|P_2$, resp. $P_1|P_2|P_3$) tq P_1 (resp. P_2, resp. P_3) est sans facteur carré *i.e.*‘

- P_1: avec P_1 unitaire de degré 3 non divisible par X^2, $(X+1)^2$, soit: X^3+1, X^3+X+1, X^3+X^2+1, X^3+X^2+X, dont un représentant correspondant est:
$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$
- $P_1|P_2$: avec P_2 unitaire de degré 2 non divisible par X^2, $(X+1)^2$, soit: $X|X(X+1)$ (matrice diagonale $(0,0,1)$), $X+1|X(X+1)$ (matrice diagonale $(1,1,0)$);
- $P_1|P_2|P_3$: avec P_1 unitaire de degré 1 soit: $X|X|X$ (matrice nulle), $X+1|X+1|X+1$ (matrice identité);

On a donc 8 classes de conjugaison d'éléments semisimples.

anna.cadoret@imj-prg.fr
IMJ-PRG- Sorbonne Université.