# ESPACE PONCTUEL ASSOCIE A UN MODULE GEOMETRIE AFFINE DANS CET ESPACE

par R. MULLER (Lycée de Gérardmer)

Buts de cet exposé * : — donner des exemples de géométries affines indépendants de toute axiomatique autre que celle qui a servi à construire **N**, base de construction de **Z** et de **R** ; — faire pressentir que c'est la structure de corps de l'ensemble des opérateurs qui est à la base de la notion de *dimension* dans les espaces vectoriels.

*Rappel. Définition d'un module.* Etant donné un anneau **A**, on appelle module sur **A**, un ensemble E muni : — d'une loi de groupe commutatif (notée additivement) ; — d'une loi de composition externe dont le domaine d'opérateurs est l'anneau **A** et qui satisfait aux conditions suivantes :

$$\forall \alpha, \beta \in \mathbf{A} \qquad \alpha(\vec{x} + \vec{y}) = \alpha\vec{x} + \alpha\vec{y}$$
$$\forall \vec{x}, \vec{y} \in \mathrm{E} \qquad (\alpha + \beta)\vec{x} = \alpha\vec{x} + \beta\vec{x}$$
$$\alpha(\beta\vec{x}) = (\alpha\beta)\vec{x}.$$

*Remarque :* Pour éviter toute confusion entre les éléments de E et ceux de A, l'élément $x$ de E est noté $\vec{x}$.

*Exercice :* $\forall \alpha \in \mathbf{A}$, $\forall \vec{x} \in \mathrm{E}$, montrer que : $\alpha\vec{0} = \vec{0}$ et que $0\vec{x} = \vec{0}$.

On dit que le **A** - module E est unitaire si l'anneau **A** possède un élément unité noté 1 qui soit élément neutre pour la loi externe, c'est-à-dire :

$$\forall \alpha \in \mathbf{A} : \qquad \alpha \times 1 = 1 \times \alpha = \alpha$$
$$\forall \vec{x} \in \mathrm{E} : \qquad 1\vec{x} = \vec{x}.$$

*Définition d'un espace vectoriel :* si **A** est un corps **K** et si le **K** - module E est unitaire, celui-ci prend le nom d'espace vectoriel E sur le corps **K**.

*Espace ponctuel associé à un module ou à un espace vectoriel* E : ensemble ponctuel, noté $\mathcal{E}$, en correspondance biunivoque avec E.

*Remarque :* $\mathcal{E}$ ne dépend pas de l'anneau **A** ; c'est-à-dire que si un ensemble E est simultanément module sur un anneau **A** et sur un autre anneau **A'**, il ne lui sera associé qu'un seul espace ponctuel.

On définit l'application bijective $f : \mathcal{E} \to \mathrm{E}$. Si $\mathrm{M} \in \mathcal{E}$, $f(\mathrm{M}) = \vec{x} \in \mathrm{E}$ ; on parlera de l'image d'un point par $f$, qui est un vecteur, ou de l'image réciproque d'un vecteur, qui est un point.

Si nous introduisons le point O dans $\mathcal{E}$ tel que $f(\mathrm{O}) = \vec{0}$, on vérifie que l'application $g : \{\mathrm{O}\} \times \mathcal{E} \to \mathrm{E}$ telle que $g(\mathrm{O}, \mathrm{M}) = f(\mathrm{M})$ est bijective.

Soit alors l'application $h : \mathcal{E} \times \mathcal{E} \to \mathrm{E}$ définie par $(\mathrm{A}, \mathrm{B}) \in \mathcal{E} \times \mathcal{E}$,

$$h(\mathrm{A}, \mathrm{B}) = g(\mathrm{O}, \mathrm{B}) - g(\mathrm{O}, \mathrm{A}) = f(\mathrm{B}) - f(\mathrm{A}),$$

on pourra montrer: — que $g$ est la restriction de $h$ à $\{\mathrm{O}\} \times \mathcal{E}$ ; — que $h(\mathrm{A}, \mathrm{A}) = \vec{0}$, $h(\mathrm{A}, \mathrm{B}) = -h(\mathrm{B}, \mathrm{A})$ et que $h(\mathrm{A}. \mathrm{B}) = \vec{0} \Longleftrightarrow \mathrm{A} = \mathrm{B}$.

La relation binaire entre deux éléments de $\mathcal{E} \times \mathcal{E}$ définie par :

$$(\mathrm{A}, \mathrm{B}) \in \mathcal{E} \times \mathcal{E}, (\mathrm{C}, \mathrm{D}) \in \mathcal{E} \times \mathcal{E} : h(\mathrm{A}, \mathrm{B}) = h(\mathrm{C}, \mathrm{D})$$

(*) Régionale de Nancy, réunion du 7 décembre 1961.

est une relation d'équivalence dans $\mathcal{E} \times \mathcal{E}$ appelée *équipollence de deux couples de points*. Par convention, on écrit :

$h(A, B) = \overrightarrow{AB}$. Alors $\overrightarrow{AB} = \overrightarrow{CD} \Longleftrightarrow (A, B) \sim (C, D)$ *modulo l'équipollence.*

$\overrightarrow{AB}$ et $\overrightarrow{CD}$ sont des éléments de E, donc des éléments algébriques ; (A, B) et (C, D) sont des éléments de $\mathcal{E} \times \mathcal{E}$, c'est-à-dire des éléments géométriques.

Dans tout espace ponctuel associé à un module, on a donc $\overrightarrow{AB} = \overrightarrow{OB} - \overrightarrow{OA}$. Cette relation se généralise : C étant un point quelconque,

$$\overrightarrow{AB} = \overrightarrow{OB} - \overrightarrow{OA} = (\overrightarrow{OB} - \overrightarrow{OC}) - (\overrightarrow{OA} - \overrightarrow{OC}) = \overrightarrow{CB} - \overrightarrow{CA}.$$

**Géométrie affine dans un espace ponctuel.**

Possédant l'espace ponctuel associé à E, on va créer dans E une *géométrie* qui dépendra essentiellement de l'anneau **A** ; c'est-à-dire que les **A** - module E et A' - module E ont même espace ponctuel associé mais y engendrent des géométries différentes.

*Définition d'une droite :* A étant donné dans $\mathcal{E}$ et $\overrightarrow{x} \neq \overrightarrow{0}$ donné dans E, la droite D est l'ensemble des points M tels que $\overrightarrow{AM} = \lambda \overrightarrow{x}$ lorsque $\lambda$ décrit **A**.

*Exercice :* soit la droite AB dans l'espace vectoriel $\mathbf{R}^2$ sur **R** ; quelle est la droite AB dans le module $\mathbf{R}^2$ sur **Z** ?

Soit l'application $\varphi$ : **A** $\rightarrow$ droite D, c'est-à-dire $\varphi : \lambda \in \mathbf{A} \rightarrow M \in D$ avec $\overrightarrow{AM} = \lambda \overrightarrow{x}$. Cette application est-elle bijective ?

$\overrightarrow{AM} = \lambda \overrightarrow{x} = \lambda' \overrightarrow{x} \Rightarrow (\lambda - \lambda') \overrightarrow{x} = \overrightarrow{0}$. Si l'anneau **A** est un corps **K** :

$$(\lambda - \lambda') \overrightarrow{x} = \overrightarrow{0} \Rightarrow \lambda = \lambda'.$$

*Donc, si* **A** *est un corps* **K**, *toutes les droites sont en correspondance biunivoque puisque en correspondance biunivoque avec* **K**. *Si* **K** *est fini, toutes les droites ont le même nombre fini de points. Il n'en est pas de même, en général, si l'anneau* **A** *n'est pas un corps.*

*Exercice :* définition d'un plan P ; montrer qu'il existe une application de $\mathbf{A} \times \mathbf{A}$ sur P qui est bijective si **A** est un corps ; qu'en résulte-t-il pour tous les plans de $\mathcal{E}$ dans ce cas ?

**Génération de modules sur Z.**

Soit G un ensemble muni d'une structure de groupe commutatif. On considère $G^n$ ($n \in \mathbf{N}$) tel que :

1° $\alpha, \beta, \gamma, ..., \alpha', \beta', \gamma', ... \in G$ ; $(\alpha, \beta, \gamma, ...), (\alpha' \beta', \gamma', ...) \in G^n$, on pose :

$$(\alpha, \beta, \gamma, ...) + (\alpha', \beta', \gamma', ...) = (\alpha + \alpha', \beta + \beta', \gamma + \gamma', ...).$$

On vérifiera que cette loi de composition interne définit une structure de groupe commutatif sur $G^n$.

2° $G^n$ est doté d'une loi de composition externe définie ainsi qu'il suit :

$$(\alpha, \beta, \gamma, ...) \in G^n, \ a \in \mathbf{Z}^+.$$

$$a(\alpha, \beta, \gamma ...) = (\alpha, \beta, \gamma ...) + (\alpha, \beta, \gamma, ...) + ... \ [a \text{ termes}]$$

et pour $a \in \mathbf{Z}^-$ :

$$a(\alpha, \beta, \gamma, ...) = -(\alpha, \beta, \gamma, ...) - (\alpha, \beta, \gamma, ...) - ... \ [-a \text{ termes}].$$

On vérifie alors que $G^n$ a la structure d'un module sur **Z**, module unitaire et commutatif. On va utiliser comme groupe G (qui nous donnera le **Z** - module $G^n$) le groupe $\mathbf{R}/p\,\mathbf{Z}$, avec $p$ donné dans **R**.

*Rappelons donc la construction du groupe* $\mathbf{R}/p\,\mathbf{Z}$ : $p$ étant donné dans **R**, on définit dans **R** la relation binaire $\mathcal{R}$ :

$$a, b \in \mathbf{R} \ : \ a \mathcal{R} b \Longleftrightarrow a - b = kp \ (k \in \mathbf{Z}).$$

On vérifie que $\mathcal{R}$ est une relation d'équivalence ; elle détermine donc une partition sur $\mathbf{R}$ ; l'ensemble des classes d'équivalence constitue l'espace quotient $\mathbf{R}/p\,\mathbf{Z}$.

Il existe une application canonique $\varphi$ de $\mathbf{R}$ sur $\mathbf{R}/p\,\mathbf{Z}$. Désignons par $\dot{a}$, $\dot{b}$ les éléments de $\mathbf{R}/p\,\mathbf{Z}$.

On munit $\mathbf{R}/p\,\mathbf{Z}$ d'une loi de composition interne : si $\dot{a} = \varphi(a)$ et $\dot{b} = \varphi(b)$, on fait correspondre à $(\dot{a}, \dot{b})$ l'élément $\varphi\,(a + b)$. Cet élément est-il unique ? Ne dépend-il pas du choix de $a$ tel que $\varphi(a) = \dot{a}$ et du choix de $b$ tel que $\varphi(b) = \dot{b}$ ? Non, comme on le vérifie immédiatement :

$$\left.\begin{array}{l} a \sim a' \text{ (mod. } \mathcal{R}) \\ b \sim b' \text{ (mod. } \mathcal{R}) \end{array}\right\} \Rightarrow a + b \sim a' + b' \text{ (mod. } \mathcal{R}).$$

On écrit donc $\varphi(a) + \varphi(b) = \varphi\,(a + b)$.

Cette loi de composition munit $\mathbf{R}/p\,\mathbf{Z}$ d'une structure de groupe commutatif. Montrons par exemple *l'associativité :*

$$\dot{a}, \dot{b}, \dot{c} \in \mathbf{R}/p\,\mathbf{Z} \Rightarrow \exists\, a, b, c \in \mathbf{R} \text{ tels que :}$$

$$\begin{aligned} &\varphi(a) = \dot{a}\ ;\ \varphi(b) = \dot{b}\ ;\ \varphi(c) = \dot{c}, \\ &\dot{a} + \dot{b} = \varphi(a) + \varphi(b) = \varphi\,(a + b), \\ &(\dot{a} + \dot{b}) + \dot{c} = \varphi\,(a + b) + \varphi(c) = \varphi\,(a + b + c) = \varphi\,[a + (b + c)], \\ &\qquad\qquad = \varphi(a) + \varphi\,(b + c) = \varphi(a) + [\varphi(b) + \varphi(c)], \\ &\qquad\qquad = \dot{a} + (\dot{b} + \dot{c}). \end{aligned}$$

*Exercice :* montrer qu'*on ne peut pas* munir $\mathbf{R}/p\,\mathbf{Z}$ d'une seconde loi de composition interne qui serait notée multiplicativement par $\varphi(a) \times \varphi(b) = \varphi(ab)$ ; montrer pour cela que $a \sim a'$ (mod. $\mathcal{R}$) et $b \sim b'$ (mod. $\mathcal{R}$) n'implique pas $ab \sim a'b'$ (mod. $\mathcal{R}$).

*En conclusion* $(\mathbf{R}/p\,\mathbf{Z})^n$ *est un* $\mathbf{Z}$ *- module.*

*Remarque :* on montre facilement que tous les $\mathbf{R}/p\,\mathbf{Z}$ modules en $\mathbf{Z}$ sont isomorphes, c'est-à-dire qu'il existe une application bijective $f : (\mathbf{R}/p\,\mathbf{Z}) \to (\mathbf{R}/p'\,\mathbf{Z})$ où $p \neq p'$ dans $\mathbf{R}$ telle que :

$$f(\dot{a} + \dot{b}) = f(\dot{a}) + f(\dot{b}) \quad \text{et} \quad f(\lambda\,\dot{a}) = \lambda\, f(\dot{a}),$$
$$\text{avec } \dot{a}, \dot{b} \in \mathbf{R}/p\,\mathbf{Z} \text{ et } \lambda \in \mathbf{Z}.$$

Il en résulte que tous les $\mathbf{Z}$ - modules $(\mathbf{R}/p\,\mathbf{Z})^n$ sont isomorphes pour un $n$ donné (dans $\mathbf{N}$) et $p$ quelconque (dans $\mathbf{R}$).

**Espace ponctuel associé à $(\mathbf{R}/p\,\mathbf{Z})^n$.**

On utilise l'espace ponctuel associé à $\mathbf{R}^n$ et on identifie les points de $\mathbf{R}^n$ qui sont images de $(a + kp, b + k'p, \ldots)$, $a, b \ldots$ étant *donnés* dans $\mathbf{R}$, $k, k', \ldots$ décrivant $\mathbf{Z}$. Les géométries de ces espaces seront des géométries *en utilisant l'anneau* $\mathbf{Z}$.

***Premier exemple :*** $\mathbf{R}/2\pi\,\mathbf{Z}$. L'espace associé à $\mathbf{R}$ est la droite numérique. Si on confond les points qui sont images de $a + k.2\pi$ ($k$ décrivant $\mathbf{Z}$), on obtient *le cercle*. On vérifie qu'il existe bien une *correspondance biunivoque* entre les éléments de $\mathbf{R}/2\pi\,\mathbf{Z}$ et les points du cercle, condition nécessaire et suffisante pour que celui-ci soit l'espace ponctuel associé.

Construisons une géométrie sur cet espace en utilisant la structure de $\mathbf{Z}$ - module. On obtient *la géométrie des arcs orientés* qui n'est rien d'autre que la géométrie affine du $\mathbf{Z}$ - module $\mathbf{R}/2\pi\,\mathbf{Z}$.

*Exercice :* soit deux points A, B du cercle ; que représente la droite AB ? Trouvez une condition pour qu'elle possède un nombre fini de points ; ce nombre est variable.

*Remarques :* écrire $\overrightarrow{AB} + \overrightarrow{CD} = \overrightarrow{EF} + k.2\pi$, c'est faire de la géométrie dans le $\mathbf{Z}$ - module $\mathbf{R}$ ; écrire $\overrightarrow{AB} + \overrightarrow{CD} \sim \overrightarrow{EF}$ (mod. $2\pi$), c'est encore faire de la géomé-

trie dans le $\mathbf{Z}$ - module $\mathbf{R}$ muni d'une relation d'équivalence. Mais écrire $\widehat{\overrightarrow{AB}} + \widehat{\overrightarrow{CD}} = \widehat{\overrightarrow{EF}}$, c'est faire de la géométrie affine dans le $\mathbf{Z}$ - module $\mathbf{R}/2\pi\,\mathbf{Z}$.

La relation $\widehat{\overrightarrow{AC}} + \widehat{\overrightarrow{CB}} = \widehat{\overrightarrow{AB}}$, dite de Chasles, n'est donc rien d'autre que la relation fondamentale dans l'espace ponctuel associé à ce $\mathbf{Z}$ - module.

***Second exemple :*** $(\mathbf{R}/p\,\mathbf{Z})^2$. On utilise l'espace ponctuel associé à $\mathbf{R}^2$. Si on confond les points qui sont images de $(a + kp,\ b + k'p)$, on obtient *un tore.*

*Exercice :* soient la droite AB dans la géométrie affine du $\mathbf{Z}$ - module $(\mathbf{R}/p\,\mathbf{Z})^2$ avec A image de $(\dot{0}, \dot{0})$ et B image de $(\dot{a}, \dot{b})$. Montrer que si $\dot{a}$, $\dot{b}$ sont rationnels, la droite AB a un nombre fini de points ; trouver le nombre des « enroulements » et le nombre des « tours ».

**Autre génération de modules.**

Etant donné l'anneau $\mathbf{A}$, considérons l'ensemble $\mathbf{A}^n$ avec $n \in \mathbf{N}$. En raison de la structure de groupe de $\mathbf{A}$, on peut définir $\mathbf{A}^n$ comme un module sur $\mathbf{Z}$. Mais on peut aussi définir dans $\mathbf{A}^n$ une loi de composition externe ayant l'anneau $\mathbf{A}$ pour domaine d'opérateurs :

$$\lambda, \alpha, \beta, \gamma, \ldots \in \mathbf{A}, \qquad \overrightarrow{x} = (\alpha, \beta, \gamma, \ldots) \in \mathbf{A}^n,$$
$$\lambda\,\overrightarrow{x} = \lambda\,(\alpha, \beta, \gamma, \ldots) = (\lambda\alpha, \lambda\beta, \lambda\gamma, \ldots).$$

On vérifie alors que $\mathbf{A}^n$ est muni d'une structure de module sur $\mathbf{A}$. Finalement, $\mathbf{A}^n$ est un $\mathbf{Z}$ - module et un $\mathbf{A}$ - module.

***Exemple :*** $\mathbf{Z}/p$ ($p$ donné dans $\mathbf{Z}$).

Dans $\mathbf{Z}$, on définit la relation binaire :

$$a, b, k \in \mathbf{Z} \ : \ a\ \mathcal{R}\ b \Longleftrightarrow a - b = kp.$$

On vérifie que $\mathcal{R}$ est une relation d'équivalence ; l'ensemble des classes d'équivalence constitue l'espace-quotient $\mathbf{Z}/p$. On note $\varphi : \mathbf{Z} \to \mathbf{Z}/p$, $\dot{a} = \varphi(a)$ avec $a \in \mathbf{Z}$.

*Exercice :* montrer que $\mathbf{Z}/p$ peut être muni de deux lois de composition interne, notées $+$ et $.$, telles que :

$$\varphi(a) + \varphi(b) = \varphi\,(a + b),$$
$$\varphi(a)\ .\ \varphi(b) = \varphi\,(a.b).$$

Montrer que ces deux lois déterminent sur $\mathbf{Z}/p$ une structure d'anneau unitaire commutatif.

*Cas de p premier :* si $p$ est premier, $\mathbf{Z}/p$ est un anneau d'intégrité :

$$\dot{a}.\dot{b} = \dot{0} \Rightarrow \varphi(a).\varphi(b) = \dot{0} \Rightarrow \varphi(ab) = \dot{0} \Rightarrow ab = kp\ ;$$

$p$ étant premier divisera, par exemple, $a$ ; donc :

$$a = k'p \quad \text{et} \quad \varphi(a) = \dot{a} = \dot{0}.$$

En résumé, $\dot{a}.\dot{b} = \dot{0} \Rightarrow \dot{a} = \dot{0}$ ou $\dot{b} = \dot{0}$.

$\dot{a}$ étant donné différent de $\dot{0}$, soit alors l'application $f : \mathbf{Z}/p \to \mathbf{Z}/p$ définie par $\dot{x} \in \mathbf{Z}/p$ : $f(\dot{x}) = \dot{a}.\dot{x}$. Montrer que l'intégrité de $\mathbf{Z}/p$ entraîne la biunivocité de $f$. Comme $\mathbf{Z}/p$ est fini, la biunivocité entraîne la surjectivité de $f$. Donc, il existe $\dot{b} \in \mathbf{Z}/p$ tel que $\dot{b}.\dot{a} = \dot{1}$ ; $\dot{a}$ possède donc un inverse : $\mathbf{Z}/p$ *est un corps.*

*Exercice :* trouver les tables d'addition et de multiplication de $\mathbf{Z}/2$, $\mathbf{Z}/3$, $\mathbf{Z}/5$ ; $\mathbf{Z}/6$ (dans ce dernier cas, trouver les diviseurs de zéro).

En résumé, d'après ce qui précède, $(\mathbf{Z}/p)^n$ est muni d'une structure de $\mathbf{Z}$ - module ou de $\mathbf{Z}/p$ - module (c'est un èspace vectoriel sur $\mathbf{Z}/p$, si $p$ est premier). Le $\mathbf{Z}$ - module $(\mathbf{Z}/p)^n$ et le $\mathbf{Z}/p$ - module $(\mathbf{Z}/p)^n$ sont liés par la relation :

$$\left.\begin{array}{l} a \in \mathbf{Z} \\ \varphi(a) \in \mathbf{Z}/p \\ \overrightarrow{x} \in (\mathbf{Z}/p)^n \end{array}\right\} \quad \overrightarrow{ax} = \varphi(a)\overrightarrow{x} \qquad \text{(I)}$$

[démonstration : en revenant aux composantes de $\overrightarrow{x}$].

**Espace ponctuel associé à $(\mathbf{Z}/p)^n$.**

Il est aisé de montrer qu'il existe une application du $\mathbf{Z}$-module $(\mathbf{Z}/p)^n$ *dans* le $\mathbf{Z}$-module $(\mathbf{R}/p\mathbf{Z})^n$ qui soit *biunivoque* et qui soit une application linéaire. On pourra alors identifier $(\mathbf{Z}/p)^n$ avec son image dans $(\mathbf{R}/p\mathbf{Z})^n$, autrement dit considérer $(\mathbf{Z}/p)^n$ comme une partie de $(\mathbf{R}/p\,\mathbf{Z})^n$ et, par suite, *considérer l'espace ponctuel associé à* $(\mathbf{Z}/p)^n$ *comme une partie de l'espace ponctuel associé à* $(\mathbf{R}/p\,\mathbf{Z})^n$ ; les géométries du $\mathbf{Z}$-module $(\mathbf{Z}/p)^n$ et du $\mathbf{Z}/p$-module $(\mathbf{Z}/p)^n$ sont identiques d'après la relation (I) ci-dessus.

***Exemple 1*** : l'espace ponctuel associé à $\mathbf{Z}/p$ est une partie de l'espace ponctuel associé à $\mathbf{R}/p\,\mathbf{Z}$, donc une partie du cercle. Si $p$ est premier, l'espace a $p$ points qui forment *une* droite.

*Exercice.* Soit $\mathbf{Z}/4$, espace ponctuel à 4 points. Trouver le nombre de droites de la géométrie du $\mathbf{Z}/4$ module $\mathbf{Z}/4$.

***Exemple 2*** $(\mathbf{Z}/3)^2$ : son espace ponctuel est une partie de $(\mathbf{R}/3\mathbf{Z})^2$ ; il est constitué de 9 points. La géométrie dans l'espace ponctuel associé à l'espace vectoriel $(\mathbf{Z}/3)^2$ sur le corps $\mathbf{Z}/3$ comprend 12 droites portant chacune trois points, chaque point étant, de plus, le « milieu » des deux autres.

*Exercice.* Montrer que, dans $(\mathbf{Z}/3)^2$, le barycentre de quatre points existe et est unique. En déduire la géométrie du parallélogramme.

Le barycentre de trois points existe-t-il dans $(\mathbf{Z}/3)^2$ ? Comment peut-on y définir le parallélisme de deux droites ? Quelles transformations géométriques y sont-elles encore définies (translation, homothétie, etc...) ?

Dans l'espace ponctuel associé à l'espace vectoriel $(\mathbf{Z}/p)^n$ sur $(\mathbf{Z}/p)$, $p$ premier, trouver : 1) le nombre de droites passant par un point ; 2) le nombre de droites incluses dans un plan ; 3) le nombre de plans passant par une droite.

**Le problème de la géométrie métrique.**

On a ainsi construit une géométrie affine dans les espaces ponctuels associés à des espaces vectoriels (ou plus généralement à des modules). Un problème se pose naturellement : peut-on y construire une géométrie *métrique ?*

Prenons le cas de $(\mathbf{Z}/p)^n$ sur le corps $\mathbf{Z}/p$ (donc $p$ premier). Définir une distance (AB), c'est définir une *norme* dans $(\mathbf{Z}/p)^n$. La norme est une application $\mathbf{N}$ : $(\mathbf{Z}/p)^n \to \mathbf{R}+$ telle que : $\vec{x}, \vec{y} \in (\mathbf{Z}/p)^n$

$$\mathrm{N}(\vec{x}) = 0 \Longleftrightarrow \vec{x} = \vec{0}$$

$$\mathrm{N}(\vec{x} + \vec{y}) \leqslant \mathrm{N}(\vec{x}) + \mathrm{N}(\vec{y})$$

$\lambda \in \mathbf{Z}/p$

$$\mathrm{N}(\lambda\vec{x}) = |\lambda|\,\mathrm{N}(\vec{x})$$

Cela suppose d'abord que $\mathbf{Z}/p$ est un espace *valué*, c'est-à-dire qu'il existe une application $g : \mathbf{Z}/p \to \mathbf{R}+$, notée $g(\lambda) = |\lambda|$, telle que :

$\lambda \in \mathbf{Z}/p$,

$$g(\lambda\lambda') = |\lambda\lambda'| = |\lambda|\,|\lambda'|$$

$$|\lambda| = 0 \Longleftrightarrow \lambda = \dot{0}$$

$$|\lambda + \lambda'| \leqslant |\lambda| + |\lambda'|.$$

On sait que, dans $\mathbf{Z}/p$, $\lambda^{p-1} = \dot{1}$ avec $\lambda \neq \dot{0}$. Il en résulte $|\lambda|^{p-1} = |\dot{1}|$ ; or $\lambda.\dot{1} = \lambda$, donc $|\lambda|\,|\dot{1}| = |\lambda| \Rightarrow |\dot{1}| = 1$, donc :
$|\lambda| = 1$ si $\lambda \neq 0$, $|\lambda| = 0$ si $\lambda = 0$.

La valeur absolue d'un élément de $\mathbf{Z}/p$ étant définie, on peut trouver une norme dans $(\mathbf{Z}/p)^n$. Par exemple :

$$\mathrm{N}(\vec{x}) = \sup\{|\dot{a}|, |\dot{b}|, \ldots\}$$

$$\dot{a}, \dot{b}, \ldots, \in \mathbf{Z}/p.$$

On vérifie que ceci définit bien une norme. Alors :

$$\mathrm{N}(\vec{x}) = 1 \text{ si } \vec{x} \neq \vec{0} ; \quad \mathrm{N}(\vec{x}) = 0 \text{ si } \vec{x} = \vec{0}.$$

c'est-à-dire que la distance de deux points distincts quelconques est 1. La métrique introduite est très simple.