GUIRAUD Yves
Maîtrise de mathématiques

Pierre – Louis Montagard

TER 1998 – 1999

Il n'y a pas de trou à l'infini dans un monoïde commutatif de type fini.

L'objectif du TER est de prouver le résultat suivant :
« il n'y a pas de trou à l'infini dans un monoïde commutatif de type fini ».
Pour expliciter, quitte à être (beaucoup) plus vague, on considère un monoïde commutatif de type fini et le groupe qu'il engendre ; alors l'assertion est la suivante : si l'on se place suffisamment loin de l'origine (l'élément neutre du monoïde), alors tous les points du groupe engendré par le monoïde, s'ils sont assez proches de points du monoïde, sont dans celui-ci.
L'exemple d'un sous-monoïde de $\mathbb{N}$ engendré par deux entiers premiers entre eux est donné dans l'annexe C.

Soyons plus précis et définissons les notations employées :

* soit Γ un sous-monoïde de $\mathbb{N}^s$ (donc commutatif), non monogène,
où s est choisi tel que Γ n'est pas canoniquement identifiable
à un sous-monoïde de $\mathbb{N}^{s-1}$,
c'est-à-dire que l'on plonge Γ dans un réseau de dimension minimale.

* soit M un monoïde. On note :
  - $G(M)$ le groupe engendré par M : $G(M) = \{ z_1 - z_2 \,;\, z_1, z_2 \in M \}$.
  - $\bar{M}$ le saturé de M : $\bar{M} = \{ \delta \in G(M) \,/\, \exists n \in \mathbb{N}^*, n.\delta \in M \}$.

* soit k un corps de caractéristique nulle
si M est un monoïde, on note $k[M]$ l'algèbre engendrée par M :
$$k[M] = \bigoplus_{\delta \in M} k.X^\delta \text{ , munie du produit } X^\delta . X^\tau = X^{\delta+\tau}$$
$k[M]$ est alors une algèbre associative et unitaire,
et commutative si M l'est.

* si M est un sous-monoïde de $\mathbb{N}^s$,
on note $\mathcal{C}(M)$ le cône convexe engendré par M :
$$\mathcal{C}(M) = \bigoplus_{\delta \in M} \mathbb{R}_+ . \delta \qquad (\mathcal{C}(M) \text{ est dans } \mathbb{R}^s)$$

* si A est un anneau, on note $\mathrm{Frac}(A)$ le corps des fractions de A.

Avec ces notations, le résultat à prouver est le suivant :

si Γ est de type fini, il existe un élément α_0 dans Γ tel que : $(\alpha_0 + \mathcal{C}(\Gamma)) \cap G(\Gamma) = (\alpha_0 + \mathcal{C}(\Gamma)) \cap \Gamma$.

Bibliographie

- David Eisenbud : Commutative algebra with a view toward algebraic geometry
  Graduate texts in mathematics - Springer-Verlag
- M.F. Atiyah, I.G. Macdonald : Introduction to commutative algebra
  Addison-Wesley
- William Fulton : Introduction to toric varieties
  Princeton university press.

① Résultat de finitude :

définitions :

ⓐ on dit que Γ est <u>de type fini</u> s'il existe $\alpha_1 - \alpha_r$ dans Γ tels que $\forall z \in \Gamma,\ \exists u_1 - u_r \in \mathbb{N},\ z = \sum_{i=1}^{r} u_i . \alpha_i$.

ⓑ on dit que $k[\Gamma]$ (ou une algèbre A) est <u>de type fini</u> si $k[\Gamma]$ est quotient d'une algèbre de polynômes.

proposition

> Γ est de type fini ssi $k[\Gamma]$ est de type fini

preuve :

$\Rightarrow$ on suppose que Γ est de type fini, engendré par $\alpha_1 - \alpha_r \in \Gamma$.

d'une part, $k[X^{\alpha_1}, -, X^{\alpha_r}] \subset k[\Gamma]$ puisque $X^{\alpha_1}, -, X^{\alpha_r} \in k[\Gamma]$

d'autre part, si $z \in \Gamma$: z s'écrit $\sum_{i=1}^{r} u_i . \alpha_i$ avec $u_1 - u_r \in \mathbb{N}$.

donc $X^z = (X^{\alpha_1})^{u_1} \times - \times (X^{\alpha_r})^{u_r} \in k[X^{\alpha_1}, -, X^{\alpha_r}]$

donc $k[\Gamma] \subset k[X^{\alpha_1}, -, X^{\alpha_r}]$

et donc $k[\Gamma] = k[X^{\alpha_1}, -, X^{\alpha_r}]$.

Soit alors $\varphi : k[X_1 - X_p] \longrightarrow k[\Gamma]$, $X_i \longmapsto X^{\alpha_i}$ un morphisme d'algèbres.

φ est surjective puisque les X^{α_i} engendrent $k[\Gamma]$,

donc $k[\Gamma] \simeq k[X_1 - X_p] / \ker\varphi$

donc $k[\Gamma]$ est de type fini Δ.

$\Leftarrow$ on suppose $k[\Gamma]$ de type fini.

alors $k[\Gamma] \simeq k[X_1 - X_m] / \ker\varphi$ où φ est un morphisme d'algèbres surjectif de $k[X_1 - X_m]$ dans $k[\Gamma]$.

pour $i \in \{1 - m\}$, on pose $P_i = \varphi(X_i)$.

Comme φ est surjective, P a un antécédent $Q(X_1 - X_m)$ par φ dans $k[X_1 - X_m]$
or φ est un morphisme d'algèbres, donc $\varphi(Q(X_1 - X_m)) = Q(P_1 - P_m) = P$
donc $k[\Gamma]$ est engendrée en tant qu'algèbre par $P_1 - P_m$.

par définition de $k[\Gamma]$, il existe $n \in \mathbb{N}^*$, des λ_{ij} $(i \in \{1-m\}, j \in \{1-n\})$ dans k et des α_{ij} $(i \in \{1-m\}, j \in \{1-n\})$ tels que:

$$P_i = \sum_{j=1}^{n} \lambda_{ij} \cdot X^{\alpha_{ij}} \quad \text{pour tout } i \in \{1-m\}.$$

donc $k[\Gamma]$ est engendrée, en tant qu'algèbre, par des X^{δ_i}, $i \in \{1-r\}$, où les δ_i sont supposés deux à deux distincts

soit $\zeta \in \Gamma$: il existe une famille de multiindices $\alpha = (\alpha_i)_{i \in \{1-r\}}$

$$\text{tels que } X^\zeta = \sum_\alpha \lambda_\alpha \cdot X^\alpha \quad \text{où } X^\alpha = \prod_{i \in \{1-r\}} (X^{\delta_i})^{\alpha_i}.$$

or, par construction de $k[\Gamma]$, on doit avoir tous les λ_α nuls, sauf un qui vaut 1; alors, il existe une famille $(\alpha_i)_{i \in \{1-r\}} \in \mathbb{N}^r$

$$\text{telle que } X^\zeta = \prod_{i=1}^{r} (X^{\delta_i})^{\alpha_i},$$

$$\text{c'est-à-dire } \zeta = \sum_{i=1}^{r} \alpha_i \cdot \delta_i$$

donc Γ est engendré, comme monoïde, par les $(\delta_i)_{i \in \{1-r\}}$

donc Γ est de type fini ▲.

<u>Hypothèse</u>: dans toute la suite, on supposera que Γ est de type fini, engendré par des éléments $\delta_1 - \delta_r \in \Gamma$.

<u>remarque</u>: sous cette hypothèse, on peut appliquer les résultats en annexe A sur les cônes convexes. On a alors:

il existe des formes linéaires $u_1 - u_p$

$$\text{telles que: } C(\Gamma) = \bigcap_{i=1}^{p} D_i \quad \text{avec} \begin{cases} D_i = \{v \in \mathbb{Q}^s \mid u_i(v) \geq 0\} \\ H_i = \ker u_i \text{ est une facette de } C(\Gamma). \end{cases}$$

on pose alors, pour $i \in \{1-p\}$, $\Gamma_i = G(\Gamma) \cap D_i$.

② Cloture intégrale de $k[\Gamma]$:

Le but du paragraphe est de montrer que $k[\bar{\Gamma}]$ est la cloture intégrale de $k[\Gamma]$; pour cela, nous allons, dans un premier temps, prouver l'assertion suivante :

Γ est saturé si et seulement si $k[\Gamma]$ est intégralement clos.

ⓐ on veut montrer ici : Γ saturé $\Rightarrow$ $k[\Gamma]$ intégralement clos.

on suppose donc, dans tout le paragraphe, que Γ est saturé ($\Gamma = \bar{\Gamma}$).

proposition

$$\Gamma = \bigcap_{i=1}^{p} \Gamma_i$$

Preuve : remarquons que $\bigcap_{i=1}^{p} \Gamma_i = \bigcap_{i=1}^{p} (G(\Gamma) \cap D_i) = G(\Gamma) \cap \left(\bigcap_{i=1}^{p} D_i\right) = G(\Gamma) \cap \mathcal{C}(\Gamma)$.

* comme $G(\Gamma)$ et $\mathcal{C}(\Gamma)$ sont engendrés par Γ,
on a forcément $\Gamma \subset G(\Gamma)$ et $\Gamma \subset \mathcal{C}(\Gamma)$
donc $\Gamma \subset \bigcap_{i=1}^{p} \Gamma_i$.

* réciproquement, soit $\delta \in G(\Gamma) \cap \mathcal{C}(\Gamma)$.

- d'une part, $\delta \in \mathcal{C}(\Gamma)$, donc d'après le théorème de Carathéodory (annexe A), il existe une sous-famille $(\delta_{i_1} - \delta_{i_s})$ libre de $(\delta_1 - \delta_r)$ telle que :

$$\delta \in \bigoplus_{j=1}^{s} \mathbb{R}_+ \cdot \delta_{i_j}.$$

quitte à réindexer les δ_i, on peut supposer que $(\delta_1 - \delta_s)$ convient.
donc, il existe une unique famille $\alpha_1 - \alpha_s$ de réels positifs tels que :

$$\delta = \alpha_1 \cdot \delta_1 + \dots + \alpha_s \cdot \delta_s \quad (\text{car } (\delta_1 - \delta_s) \text{ forme une base de } \mathbb{R}^s).$$

- $G(\Gamma)$ est un groupe libre abélien de type fini (engendré par $\delta_1 - \delta_r$) et engendre l'espace vectoriel total $\mathbb{R}^s$ par hypothèse sur s.
donc, d'après le théorème de structure des $\mathbb{Z}$-modules ($\mathbb{Z}$ principal), il existe une base $(e_1 - e_s)$ de $\mathbb{R}^s$ telle que :

$$G(\Gamma) = \bigoplus_{i=1}^{s} \mathbb{Z} \cdot e_i.$$

comme, pour $i \in \{1 - s\}$, $\delta_i \in G(\Gamma)$,

il existe des coefficients n_{ij}, $i,j \in \{1-s\}$, pris dans $\mathbb{Z}$, tels que :

$$\begin{bmatrix} \delta_1 \\ | \\ \delta_s \end{bmatrix} = \begin{bmatrix} n_{11} & \cdots & n_{1s} \\ | & & | \\ n_{s1} & \cdots & n_{ss} \end{bmatrix} \cdot \begin{bmatrix} e_1 \\ | \\ e_s \end{bmatrix}$$

or $(\delta_1 - \delta_s)$ et $(e_1 - e_s)$ sont des bases de $\mathbb{R}^s$,

donc la matrice $(n_{ij})_{i,j \in \{1-s\}}$ est inversible en une matrice $(m_{ij})_{i,j \in \{1-s\}}$ dont les coefficients sont alors dans $\mathbb{Q}$:

$$\begin{bmatrix} e_1 \\ | \\ e_s \end{bmatrix} = \begin{bmatrix} m_{11} & \cdots & m_{1s} \\ | & & | \\ m_{s1} & \cdots & m_{ss} \end{bmatrix} \cdot \begin{bmatrix} \delta_1 \\ | \\ \delta_s \end{bmatrix}$$

Comme $\delta \in G(\Gamma) = \bigoplus_{i=1}^{s} \mathbb{Z}.e_i$, il existe $(\beta_1 - \beta_s) \in \mathbb{Q}^s$

tels que $\delta = \beta_1 . \delta_1 + \cdots + \beta_s . \delta_s$

or $\delta = \alpha_1 . \delta_1 + \cdots + \alpha_s . \delta_s$ donc, comme $(\delta_1 - \delta_s)$ est une base de $\mathbb{R}^s$, on a identité des coefficients α_i et β_i, $i \in \{1-s\}$

donc $\delta = \alpha_1 . \delta_1 + \cdots + \alpha_s . \delta_s$ avec $\left\{ \begin{array}{l} \alpha_i \in \mathbb{R}_+ \cap \mathbb{Q} = \mathbb{Q}^+ \\ i \in \{1-s\} \end{array} \right.$.

- comme $\alpha_i \in \mathbb{Q}_+$, il existe $p_i \in \mathbb{N}^*$, tel que $p_i . \alpha_i \in \mathbb{N}$

on pose alors $u = p_1 \times \cdots \times p_s \in \mathbb{N}^*$.

on a alors $n.\delta \in \Gamma$ puisque $u.\delta$ est combinaison linéaire entière des $\delta_1 - \delta_s$, donc des $\delta_1 - \delta_r$.

donc $\delta \in \overline{\Gamma} = \Gamma$ donc $\bigcap_{i=1}^{p} \Gamma_i \subset \Gamma$. ▲

proposition

$$\boxed{k[\Gamma] = \bigcap_{i=1}^{p} k[\Gamma_i]}$$

preuve : d'une part, $\Gamma \subset \Gamma_i$ donc $k[\Gamma] \subset k[\Gamma_i]$ donc $k[\Gamma] \subset \bigcap_{i=1}^{p} k[\Gamma_i]$

réciproquement, si $X^\delta \in \bigcap_{i=1}^{p} k[\Gamma_i]$, alors $X^\delta \in k[\Gamma_i]$

donc $\delta \in \Gamma_i$ donc $\delta \in \bigcap_{i=1}^{p} \Gamma_i$ donc $\delta \in \Gamma$. ▲

proposition

pour tout $i \in \{1,\dots,p\}$, $\mathrm{Frac}\,k[\Gamma_i] = \mathrm{Frac}\,k[\Gamma]$

preuve :

on a $k[\Gamma] \subset k[\Gamma_i]$ donc $\mathrm{Frac}\,k[\Gamma] \subset \mathrm{Frac}\,k[\Gamma_i]$

réciproquement, $\Gamma_i = G(\Gamma) \cap D_i$

donc $\Gamma_i \subset G(\Gamma)$ donc $k[\Gamma_i] \subset k[G(\Gamma)]$

or $k[G(\Gamma)] \subset \mathrm{Frac}\,k[\Gamma]$

donc $\mathrm{Frac}\,k[\Gamma_i] \subset \mathrm{Frac}\,k[\Gamma]$. ▲.

proposition

soit $i \in \{1,\dots,p\}$.

Γ_i est engendré, en tant que monoïde, par des éléments du type : $e_1, \dots, e_{s-1}, -e_1, \dots, -e_{s-1}, y$.

preuve :

* $G(\Gamma)$ est un groupe libre abélien de type fini

et $G(\Gamma) \cap H_i$ est un sous-groupe de corang 1 dans $G(\Gamma)$

(car $H_i \cap C(\Gamma)$ est une facette du cône $C(\Gamma)$).

donc, d'après le théorème de structure des $\mathbb{Z}$-modules :

il existe $\begin{cases} (e_1,\dots,e_s) \text{ une base de } G(\Gamma) \\ a_1,\dots,a_{s-1} \in \mathbb{Z} \text{ tels que } a_1 \mid \dots \mid a_{s-1} \end{cases}$

qui vérifient $G(\Gamma) \cap H_i = \bigoplus_{j=1}^{s-1} \mathbb{Z}.a_j.e_j$.

de plus, quitte à remplacer e_j par $-e_j$, on peut prendre $a_j e_j$ dans D_i

(si $a_j e_j \notin D_i$, alors $u_i(a_j e_j) < 0$ donc $u_i(-a_j e_j) > 0$ donc $-a_j e_j \in D_i$).

* $(e_1,\dots,e_s)$ est une base de $\mathbb{R}^s$ donc l'espace engendré par $G(\Gamma) \cap H_i$ admet dans $\mathbb{R}^s$ un supplémentaire de dimension 1, orienté par un $a_s.e_s$, $a_s.e_s \in D_i$

alors, si $\delta \in \Gamma_i$: $\delta = \alpha_1 f_1 + \dots + \alpha_s f_s$, $\alpha_1,\dots,\alpha_s \in \mathbb{Z}$, $f_i = a_i e_i$

or $\delta \in D_i$ donc $u_i(\delta) \geq 0$

or $u_i(\delta) = \sum_{j=1}^{s} \alpha_j u_i(f_j) = \alpha_s u_i(f_s)$ car $f_1 - f_{s-1} \in \ker u_i$.

on a donc $\begin{cases} v_i(\delta) \geq 0 \\ v_i(\delta) = \alpha_s \cdot v_i(f_s) \end{cases}$

or $f_s \in D_i \setminus H_i$ donc $v_i(f_s) > 0$

donc $\alpha_s \geq 0$

donc $\Gamma_i \subset \left\{ \sum_{i=1}^{s} \alpha_i \cdot f_i ;\ \alpha_1 - \alpha_{s-1} \in \mathbb{Z},\ \alpha_s \geq 0 \right\}$

réciproquement, si $\delta = \sum_{i=1}^{s} \alpha_i \cdot f_i$ avec $\begin{cases} \alpha_1 - \alpha_{s-1} \in \mathbb{Z} \\ \alpha_s \geq 0 \end{cases}$

alors $\delta \in G(\Gamma)$ et $v_i(\delta) = \alpha_s \cdot v_i(f_s) \geq 0$

donc $\delta \in G(\Gamma) \cap D_i = \Gamma_i$

donc Γ_i est engendré comme monoïde par des éléments du type :

$f_1 - f_{s-1}, -f_1, \dots, -f_{s-1}, y$. $(y = f_s)$. ▲

proposition

soit $i \in \{1 - p\}$. Alors $k[\Gamma_i]$ est intégralement clos

preuve :

on pose, $\begin{cases} \text{pour } i \in \{1 - s-1\} : X_i = X^{e_i},\ X_i^{-1} = X^{-e_i} \\ Y = X^{y}. \end{cases}$

alors $k[\Gamma_i] = k[X_1 - X_{s-1}, X_1^{-1}, \dots, X_{s-1}^{-1}, Y]$.

* k est un corps, donc k est factoriel,

donc l'anneau de polynômes $k[X_1 - X_{s-1}, Y]$ est factoriel

on peut donc appliquer le résultat de l'appendice B :

$k[X_1 - X_{s-1}, Y]$ est intégralement clos.

* de plus, $k[X_1 - X_{s-1}, Y, X_1^{-1}, \dots, X_{s-1}^{-1}] = k[X_1 - X_{s-1}, Y][X_1^{-1} - X_{s-1}^{-1}]$

est le localisé d'un anneau intégralement clos par rapport à la partie multiplicative engendrée par $X_1 - X_{s-1}$,

donc $k[\Gamma_i] = k[X_1 - X_{s-1}, X_1^{-1} - X_{s-1}^{-1}, Y]$ est intégralement clos. ▲

corollaire

$k[\Gamma]$ est intégralement clos

preuve :

on a donc, pour $i \in \{1 \dots p\}$: $\begin{cases} k[\Gamma_i] \text{ est intégralement clos} \\ \text{Frac}\, k[\Gamma] = \text{Frac}\, k[\Gamma_i] \end{cases}$

de plus, $k[\Gamma] = \bigcap_{i=1}^{p} k[\Gamma_i]$

$k[\Gamma]$ est donc l'intersection d'anneaux intégralement clos ayant même corps de fractions, donc, d'après l'appendice B,

$k[\Gamma]$ est intégralement clos. ▲

ⓑ montrons ici l'implication réciproque :

proposition

$k[\Gamma]$ intégralement clos $\Rightarrow$ Γ saturé

preuve : on suppose que $k[\Gamma]$ est intégralement clos.

Soient alors $\delta \in \overline{\Gamma}$ et $n \in \mathbb{N}^*$ tel que $n\delta \in \Gamma$.

d'une part, $\delta \in G(\Gamma)$

d'autre part, $X^{n\delta} \in k[\Gamma]$, donc X^{δ} est racine du polynôme unitaire $Y^n - X^{n\delta}$ de $k[\Gamma][Y]$. Comme $\delta \in G(\Gamma)$, $X^{\delta} \in \text{Frac}\, k[\Gamma]$

donc X^{δ} est entier sur $k[\Gamma]$ intégralement clos,

donc $X^{\delta} \in k[\Gamma]$ et donc $\delta \in \Gamma$.

donc $\overline{\Gamma} \subset \Gamma$ et $\Gamma = \overline{\Gamma}$. ▲

ⓒ on a donc démontré le théorème :

théorème

Γ est saturé ssi $k[\Gamma]$ est intégralement clos

on en déduit le résultat cherché :

Corollaire

$k[\bar{\Gamma}]$ est la clôture intégrale de $k[\Gamma]$

preuve : notons C la clôture intégrale de $k[\Gamma]$ (dans $\mathrm{Frac}(k[\Gamma])$).

* tout d'abord, on peut appliquer la proposition précédente à $\bar{\Gamma}$ saturé : $k[\bar{\Gamma}]$ est intégralement clos.

* on a : $\Gamma \subset \bar{\Gamma}$ donc $\begin{cases} k[\Gamma] \subset k[\bar{\Gamma}] \\ \mathrm{Frac}[\Gamma] \subset \mathrm{Frac}[\bar{\Gamma}] \end{cases}$

donc $C \subset k[\bar{\Gamma}]$ (puisque $k[\bar{\Gamma}]$ est intégralement clos).

* soit $\delta \in \bar{\Gamma}$: il existe $n \in \mathbb{N}^*$ tel que $n\delta \in \Gamma$

on a vu qu'alors $\begin{cases} X^\delta \text{ est racine du polynôme unitaire } Y^n - X^{n\delta} \text{ de } k[\Gamma][Y] \\ X^\delta \in \mathrm{Frac}[\Gamma] \end{cases}$

donc X^δ est entier sur $k[\Gamma]$

donc $X^\delta \in C$ donc, comme $k[\bar{\Gamma}]$ est engendré par les X^δ, $\delta \in \bar{\Gamma}$,

on a $k[\bar{\Gamma}] \subset C$. ▲

③ Conclusion :

Proposition

$k[\bar{\Gamma}]$ est un $k[\Gamma]$-module de type fini

preuve :

$k[\Gamma]$ est une algèbre de type fini, de clôture intégrale $k[\bar{\Gamma}]$.

on peut donc appliquer le théorème de normalisation de Noether (voir appendice B), qui donne le résultat. ▲

Reste à voir un lemme avant le résultat final.

Lemme

$$\bar{\Gamma} = G(\Gamma) \cap \mathcal{C}(\Gamma)$$

preuve : * on a vu que si Γ est saturé, alors $\Gamma = G(\Gamma) \cap \mathcal{C}(\Gamma)$
donc, comme $\bar{\Gamma}$ est saturé, on a $\bar{\Gamma} = G(\bar{\Gamma}) \cap \mathcal{C}(\bar{\Gamma})$.
comme $\Gamma \subset \bar{\Gamma}$, on a : $G(\Gamma) \subset G(\bar{\Gamma})$ et $\mathcal{C}(\Gamma) \subset \mathcal{C}(\bar{\Gamma})$
donc $\left(G(\Gamma) \cap \mathcal{C}(\Gamma)\right) \subset \bar{\Gamma}$.

* réciproquement, soit $\delta \in \bar{\Gamma}$:
alors, d'une part, $\delta \in G(\Gamma)$
et, d'autre part, il existe $u \in \mathbb{N}^*$ tel que $u\delta \in \Gamma$
donc $\frac{1}{u} \cdot (u\delta)$ est dans $\mathcal{C}(\Gamma)$
donc $\bar{\Gamma} \subset (G(\Gamma) \cap \mathcal{C}(\Gamma))$. ▲

théorème

il existe δ_0 dans Γ tel que :
$$\left(\delta_0 + \mathcal{C}(\Gamma)\right) \cap G(\Gamma) = \left(\delta_0 + \mathcal{C}(\Gamma)\right) \cap \Gamma$$

démonstration :

* $k[\bar{\Gamma}]$ est un $k[\Gamma]$-module de type fini,
donc $k[\bar{\Gamma}]$ est engendré comme $k[\Gamma]$-module par des $P_1 - P_k$ de $k[\bar{\Gamma}]$
or, par construction de $k[\bar{\Gamma}]$, on a :
pour $i \in \{1-k\}$, $P_i = \sum_{j=1}^{u} \alpha_{ij} \cdot X^{\gamma_{ij}}$ avec $\begin{cases} \alpha_{i1} - \alpha_{iu} \in k \\ \gamma_{i1} - \gamma_{iu} \in \bar{\Gamma} \end{cases}$.

donc $k[\bar{\Gamma}]$ est engendré comme $k[\Gamma]$-module par les $X^{\gamma_{ij}}$, $\begin{cases} i \in \{1-k\} \\ j \in \{1-u\} \end{cases}$
ou par des X^{γ_i}, $i \in \{1-l\}$ en réindexant la famille.
de plus, pour $i \in \{1-l\}$, $\gamma_i \in \bar{\Gamma} \subset G(\Gamma)$,

donc il existe des éléments $a_1 - a_\ell, b_1 - b_\ell$ dans Γ
tels que, pour $i \in \{1 - \ell\}$, on a : $z_i = a_i - b_i$.

posons alors $\alpha_0 = \sum_{i=1}^{\ell} b_i$.

* remarquons, dans un premier temps, que :

$$(\alpha_0 + \mathcal{C}(\Gamma)) \cap G(\Gamma) = \alpha_0 + \mathcal{C}(\Gamma) \cap G(\Gamma) = \alpha_0 + \bar{\Gamma}$$

car $\begin{cases} \alpha_0 \in G(\Gamma) \\ G(\Gamma) \text{ est un groupe} \end{cases}$

de même, $(\alpha_0 + \mathcal{C}(\Gamma)) \cap \Gamma \supset \alpha_0 + \mathcal{C}(\Gamma) \cap \Gamma \supset \alpha_0 + \Gamma$

puisque $\begin{cases} \alpha_0 \in \Gamma \\ \Gamma \subset \mathcal{C}(\Gamma) \end{cases}$.

* comme $\Gamma \subset G(\Gamma)$, il est clair que $[(\alpha_0 + \mathcal{C}(\Gamma)) \cap \Gamma] \subset [(\alpha_0 + \mathcal{C}(\Gamma)) \cap G(\Gamma)]$
* soit $z \in \bar{\Gamma}$: alors il existe $\lambda_1 - \lambda_\ell$ dans $k[\Gamma]$
tels que $X^z = \sum_{i=1}^{\ell} \lambda_i \cdot X^{z_i}$

donc $X^{\alpha_0 + z} = \sum_{i=1}^{\ell} \lambda_i \cdot X^{\alpha_0 + z_i}$

or $\forall i \in \{1 - \ell\}$, $\alpha_0 + z_i = \sum_{j=1}^{\ell} b_j + a_i - b_i = a_i + \sum_{\substack{j=1 \\ (\neq i)}}^{\ell} b_j \in \Gamma$

donc $\begin{cases} \lambda_1 - \lambda_\ell \in k[\Gamma] \\ X^{\alpha_0 + z_1}, \ldots, X^{\alpha_0 + z_\ell} \in k[\Gamma] \end{cases}$

donc $X^{\alpha_0 + z} \in k[\Gamma]$ donc $\alpha_0 + z \in \Gamma$

donc $(\alpha_0 + \bar{\Gamma}) \subset (\alpha_0 + \Gamma) \subset (\alpha_0 + \mathcal{C}(\Gamma)) \cap \Gamma$

or $\alpha_0 + \bar{\Gamma} = (\alpha_0 + \mathcal{C}(\Gamma)) \cap G(\Gamma)$

donc, on a bien $(\alpha_0 + \mathcal{C}(\Gamma)) \cap G(\Gamma) = (\alpha_0 + \mathcal{C}(\Gamma)) \cap \Gamma$. ∎

Appendice A : Résultats sur les cônes convexes

soit $C = \{ p_1 \cdot v_1 + \dots + p_r \cdot v_r,\ p_1 \dots p_r \in \mathbb{R}_+ \}$ un cône convexe plongé dans $\mathbb{R}^s = V$, où s est minimal tel que $C \subset \mathbb{R}^s$ ($v_1 \dots v_r \in \mathbb{R}^s$)

on appelle cône dual de C, et on note $C^\vee = \{ u \in V^* / \forall v \in C,\ u(v) \geq 0 \}$

lemme

soit $v \in \mathbb{R}^s$
si $v \notin C$, alors il existe $u \in C^\vee$ tel que $u(v) < 0$

preuve :

C est un cône convexe fermé et $v \notin C$
donc, d'après le théorème de séparation de Hilbert, il existe un hyperplan P qui sépare $\{v\}$ et C.
on choisit donc $u \in V^*$ tel que $\begin{cases} \ker u = P \\ u(v) < 0 \end{cases}$.

alors $\forall w \in C$, $u(w) \geq 0$ donc $\begin{cases} u \in C^\vee \\ u(v) < 0 \end{cases}$. ▲.

définitions :

ⓐ on appelle face de C l'intersection de C avec le noyau d'un élément u du cône dual : $\Sigma = C \cap \ker u = \{ v \in C / u(v) = 0 \}$

ⓑ on appelle face propre de C une face de C distincte de C.

ⓒ on appelle facette de C une face de C qui engendre un hyperplan de V

proposition

toute face propre de C est contenue dans une facette de C

preuve : admis.

proposition

la frontière topologique de C est la réunion de ses faces propres (et donc de ses facettes)

preuve :

* soit $\mathcal{Z} = C \cap \ker u$ une face propre de C $(u \in C^\vee)$.
on prend $v \in \mathcal{Z}$.
- $v \in C$ puisque $v \in C \cap \ker u$
- montrons que $v \notin \mathring{C}$, c'est-à-dire que $\forall \varepsilon > 0$, $\mathcal{B}(v,\varepsilon) \not\subset C$.
$\ker u$ passe par le centre v de la boule $\mathcal{B}(v,\varepsilon)$.
$\mathcal{B}(v,\varepsilon)$ est ouverte et $\ker u$ est fermé et distinct de l'espace total ($\mathcal{Z}$ face propre)
donc $\mathcal{B}(v,\varepsilon)$ contient un élément w qui n'est pas dans $\ker u$ $(u(w) \neq 0)$
. si $u(w) < 0$: c'est bon
. si $u(w) > 0$: on change w en $2v - w \in \mathcal{B}(v,\varepsilon)$ $(d(2v-w, v) = d(v,w) < \varepsilon)$
et $u(2v-w) = 2u(v) - u(w) = -u(w) < 0$.
dans tous les cas on se ramène à $u(w) < 0$
donc $w \notin C$ car sinon $u(w) \geq 0$ $(u \in C^\vee)$.
donc $v \in \partial C$.

* soit $v \in \partial C$: il existe une suite $(w_n)_{n \in \mathbb{N}} \in V^{\mathbb{N}}$
telle que : $\begin{cases} \forall n \in \mathbb{N},\ w_n \notin C \\ \lim\limits_{n \to +\infty} w_n = v. \end{cases}$

d'après le lemme, il existe une suite $(u_n)_{n \in \mathbb{N}} \in (C^\vee)^{\mathbb{N}}$
telle que $\forall n \in \mathbb{N}$, $u_n(w_n) < 0$.
de plus, on peut prendre les u_n, $n \in \mathbb{N}$, de norme 1 dans V^*.
or $S(V^*)$ est compacte, donc on peut extraire de $(u_n)_{n \in \mathbb{N}}$ une sous-suite $(u_{n_k})_{k \in \mathbb{N}}$ qui converge vers u.
de plus, $u \in C^\vee$ car $\forall w \in C$, $\forall n \in \mathbb{N}$, $u_n(w) \geq 0 \Rightarrow \forall w \in C$, $u(w) \geq 0$
alors, par passage à la limite, $u(v) \leq 0$,
or $u(v) \geq 0$ car $u \in C^\vee$ et $v \in C$, donc $u(v) = 0$
donc $v \in \mathcal{Z} = \partial \cap \ker u$.

de plus, les u_i sont de norme 1 donc u aussi

donc $\ker u \neq V$ donc Z est bien une face propre de C. ▲

proposition

C n'a qu'un nombre fini de faces (et donc de facettes)

preuve :

soit Z une face de C : $Z = C \cap \ker u$ où $u \in C^\vee$.

si $v \in Z$: alors $\begin{cases} v = \sum_{i=1}^{r} p_i v_i & p_1, \dots, p_r \in \mathbb{R}_+ \\ u(v) = 0 \end{cases}$.

alors $u(v) = \sum_{i=1}^{r} p_i \cdot u(v_i) = 0$

or $\forall i \in \{1, \dots, r\}$, $\begin{cases} p_i \geq 0 \\ u(v_i) \geq 0 \text{ car } u \in C^\vee \text{ et } v_i \in C \end{cases}$

donc $p_i = 0$ sauf si $u(v_i) = 0$

donc Z est engendrée par les v_i, $i \in \{1, \dots, r\}$ tels que $u(v_i) = 0$

donc C n'a qu'un nombre fini de faces.

notation : on note $Z_1, \dots, Z_p$ les facettes de C.

pour $i \in \{1, \dots, p\}$, on a $Z_i = C \cap \ker u_i$, $u_i \in C^\vee$

on pose alors $D_i = \{v \in V / u_i(v) \geq 0\}$ $i \in \{1, \dots, p\}$.

proposition

$$C = \bigcap_{i=1}^{p} D_i$$

preuve :

* soit $v \in C$: alors $\forall u \in C^\vee$, $u(v) \geq 0$

en particulier, $\forall i \in \{1, \dots, p\}$, $u_i(v) \geq 0$

donc $v \in \bigcap_{i=1}^{p} D_i$

* soit $v \in \bigcap_{i=1}^{p} D_i$:

Supposons que $v \notin C$.

C est d'intérieur non vide car sinon $C \subset \mathbb{R}^{s-1}$ (impossible par hypothèse sur s)

on choisit donc $w \in \mathring{C}$.

Soit alors $z \in [v, w] \cap \partial C$.

$z \in \partial C$ donc il existe une face $C_i = C \cap$ hyperplan telle que $u_i(z) = 0$

on a alors : $\begin{cases} u_i(w) > 0 \\ u_i(z) = 0 \\ u_i(v) \geq 0 \end{cases}$ avec $\begin{cases} z \in]v, w[\\ u_i \text{ forme linéaire} \end{cases}$

c'est impossible, donc $v \in C$

et donc $C = \bigcap_{i=1}^{p} D_i$. ▲

Théorème de Carathéodory

C est la réunion des ensembles $\bigoplus_{j=1}^{s} \mathbb{R}_+ \cdot v_{ij}$

pour $(v_{i1} \dots v_{is})$ une sous-famille libre de $(v_1 \dots v_r)$

admis.

Appendice B: Résultats sur les clotures intégrales théorème de normalisation

proposition

Soit A un anneau factoriel
alors A est intégralement clos.

preuve:

soit $\frac{P}{Q} \in Frac A$ entier sur A.
avec P et Q premiers entre eux.

alors il existe $a_0 \dots a_{n-1} \in A$
tels que : $\frac{P^n}{Q^n} + a_{n-1}.\frac{P^{n-1}}{Q^{n-1}} + \dots + a_0 = 0$.

en multipliant par Q^n, on obtient: $P^n + a_{n-1}.P^{n-1}.Q + \dots + a_0.Q^n = 0$

donc, comme A est factoriel
Q divise P^n, donc comme Q et P sont premiers entre eux,
Q est inversible et donc $\frac{P}{Q} \in A$. ▲

proposition

soient B un anneau
A un sous-anneau de B
C la cloture intégrale de A dans B
S une partie multiplicative de A
alors $S^{-1}C$ est la cloture intégrale de $S^{-1}A$ dans $S^{-1}B$

preuve:

* montrons que $S^{-1}C$ est entier sur $S^{-1}A$.

soit $\frac{x}{s} \in S^{-1}C$, $x \in C$, $s \in S$.

x est entier sur A donc il existe $a_0 \dots a_{n-1} \in A$ tels que $x^n + a_{n-1}.x^{n-1} + \dots + a_0 = 0$

donc $\frac{x^n}{s^n} + \frac{a_{n-1}}{s}.\frac{x^{n-1}}{s^{n-1}} + \dots + \frac{a_0}{s^n} = 0$

donc $\frac{x}{s}$ est racine d'un polynôme unitaire de $(S^{-1}A)[X]$

donc $\frac{x}{s}$ est entier sur $S^{-1}A$.

* réciproquement, soit $\frac{x}{s} \in S^{-1}B$ entier sur $S^{-1}A$.

alors il existe $\frac{a_0}{s_0}$ —— $\frac{a_{n-1}}{s_{n-1}} \in S^{-1}A$ tels que :

$$\frac{x^n}{s^n} + \frac{a_{n-1}}{s_{n-1}} \cdot \frac{x^{n-1}}{s^{n-1}} + \text{——} + \frac{a_0}{s_0} = 0$$

on pose $t = s_0 \text{——} s_{n-1}$ et on multiplie par $t^n s^n$:

alors $t^n x^n + a_{n-1} \cdot s \cdot s_0 \text{——} s_{n-2} \cdot t^{n-1} \cdot x^{n-1} + \text{——} + a_0 \cdot s^n \cdot s_0^{n-1} \cdot s_1^n \text{——} s_{n-1}^{n-1} = 0$

donc tx est racine d'un polynôme de $A[X]$, unitaire

donc tx est entier sur A donc $tx \in C$.

or $st = s \cdot s_0 \text{——} s_{n-1} \in S$ donc $\frac{tx}{ts} = \frac{x}{s} \in S^{-1}C$ ▲.

théorème de normalisation d'Emmy Noether

Soient { A une algèbre de type fini, associative et unitaire
B sa cloture intégrale (dans son corps des fractions)

alors B est un A-module de type fini.

déduis.

proposition

Soient { $A_1 \text{——} A_n$ des anneaux intégralement clos
$A = \bigcap_{i=1}^{n} A_i$

on suppose que pour $i \in \{1 \text{——} n\}$, $\text{frac } A = \text{frac } A_i$

alors A est intégralement clos.

preuve :

soit $P \in \text{Frac } A$ entier sur A.

alors il existe un polynôme unitaire $Q(X)$ dans $A[X]$

tel que $Q(P) = 0$

soit $i \in \{1 \text{——} n\}$: alors { $P \in \text{frac } A_i = \text{frac } A$
$Q(X) \in A_i[X]$ (puisque $A[X] = \bigcap_{j=1}^{n} A_j[X]$)
Q unitaire et $Q(P) = 0$

donc P est entier sur A_i intégralement clos,

donc $P \in A_i$

donc $P \in \bigcap_{i=1}^{n} A_i$ donc $P \in A$. ▲

Appendice C : Cas de la dimension 1

On s'intéresse ici au cas où Γ est un sous-monoïde de $\mathbb{N}$, engendré par deux entiers u et v premiers entre eux, $(u,v \in \mathbb{N}^*)$

ici : $\begin{cases} \Gamma = \{au+bv,\ a,b \in \mathbb{N}\} \\ G(\Gamma) = \mathbb{Z} \quad \text{puisque, d'après Bezout, il existe } u \text{ et } v \in \mathbb{Z} \text{ tels que } uu+vv=1 \\ \mathcal{C}(\Gamma) = \mathbb{N} \end{cases}$

On veut donc montrer qu'il existe $p_0 \in \Gamma$ tel que :

$$(p_0+\mathbb{N}) \cap \Gamma = p_0+\mathbb{N}$$

En d'autres termes, il existe un entier $p_0 \in \Gamma$ à partir duquel tous les entiers sont dans Γ.

On pose $p_0 = (u-1).(v-1)$.

* 1er cas : $u=1$ ou $v=1$:

alors $p_0 = 0$ et $\forall p \in \mathbb{N}$, $p = \begin{cases} pu \text{ si } u=1 \\ pv \text{ si } v=1 \end{cases}$

donc $\Gamma = \mathbb{N}$ et p_0 convient.

* 2e cas : $u \geq 2$ et $v \geq 2$.

- montrons que : $\forall k \in \mathbb{N}$, $p_0+k \in \Gamma$. soit $k \in \mathbb{N}$.

d'après Bezout, comme $u \wedge v = 1$, il existe $u, v \in \mathbb{Z}$ tels que $uu+vv=1$.

- $uv \neq 0$ car sinon $(uu=1$ ou $vv=1)$ donc $(u=1$ ou $v=1)$ car $u,v \in \mathbb{N}$ impossible.
- $uv < 0$ car $\begin{cases} (u>0,\ v>0) \Rightarrow (uu+vv \geq 4) & \text{impossible} \\ (u<0,\ v<0) \Rightarrow (uu+vv \leq -4) & \text{impossible} \end{cases}$

On suppose, par exemple, $u<0$.

Si $(k+1).u \leq -v$, on effectue, dans $\mathbb{Z}$, la division euclidienne de $-v$ par $(k+1).u$:

il existe $q \in \mathbb{N}$ et $u' \in \{-u+1, \dots, 0\}$

tels que : $(k+1).u = -qv + u'$,

alors $(k+1).(uu+vv) = u.(-qv+u') + v.(k+1).v = uu' + v.[(k+1).v - qu]$

On pose $v' = (k+1).v - q.u$

alors $k+1 = uu' + vv'$.

Comme $u' \leq 0$, on a forcément $v' \geq 1$.

En effet, si $v' \leq 0$, on a $uu' + vv' \leq 0$ donc $k+1 \leq 0$ (impossible car $k+1 \geq 1$).

99

ou a alors : $p_0 + k = (u-1).(u-1) + k$

$= uu - u - u + k + 1$

$= uu - u - u + uu' + uv'$

$= u.(u - 1 + u') + u.(v' - 1)$

or $u' \in \{-u+1, \dots, 0\}$ et $v' \geq 1$

donc, en posant $a = u - 1 + u'$ et $b = v' - 1$, on a : $p_0 + k = ua + ub$, $a, b \in \mathbb{N}$

et donc $p_0 + k \in \Gamma$.

- montrons à présent que $p_0 - 1 \notin \Gamma$

Sinon : il existe $a, b \in \mathbb{N}$ tels que $p_0 - 1 = au + bu$.

donc $uu - u - u = au + bu$

donc $u.(u - 1 - a) = u.(b+1)$

comme $u \wedge u$, et que $\mathbb{Z}$ est factoriel, on a : $u / (b+1)$

donc, il existe $k \in \mathbb{N}$ tel que $b+1 = ku$

alors $u.(u - 1 - a) = kuu$

or $u \neq 0$ et $\mathbb{Z}$ est intègre donc $u - 1 - a = ku$

donc $a + 1 = (1 - k).u$

or $a + 1 \geq 1$ donc, comme $u \geq 1$, on a $1 - k \geq 1$

donc $k \leq 0$ donc $ku \leq 0$ (car $u \geq 0$)

donc $b + 1 \leq 0$ impossible car $b \in \mathbb{N}$.

donc $(p_0 - 1) \notin \Gamma$

Conclusion : le plus petit entier $p \in \mathbb{N}$ tel que $(p + \mathbb{N}) \cap \Gamma = p + \mathbb{N}$ est $p_0 = (u-1).(u-1)$