20 Théorème de Carlitz

Soit A un anneau commutatif unitaire. On appelle idéal fractionnaire de A tout sous-A-module I de $\mathrm{Frac}(A)$ tel qu'il existe $m \in A$, $mI \subset A$. L'ensemble des idéaux fractionnaires de A est muni d'une structure de monoïde commutatif pour la multiplication.

On dit que A est un anneau de Dedekind si ce monoïde est un groupe, autrement dit si pour tout idéal fractionnaire I il existe un idéal fractionnaire J tel que $IJ = A$. On peut signaler qu'une définition équivalente est de dire qu'un anneau de Dedekind est un anneau noethérien intégralement clos.

Comme exemples d'anneaux de Dedekind, on peut citer les anneaux principaux et les anneaux d'entiers des corps de nombres.

Nous admettrons une propriété essentielle des anneaux de Dedekind, à savoir que tout idéal fractionnaire non nul se décompose de manière unique en produit d'idéaux premiers et d'inverses d'idéaux premiers.

Lorsque A est anneau de Dedekind, on appelle groupe de Picard de A (ou groupe des classes d'idéaux de A) le quotient du groupe des idéaux fractionnaires par le sous-groupe des idéaux fractionnaires principaux. C'est un groupe abélien qu'on note $(\mathrm{Pic}(A), +)$.

Donnons une dernière définition : on dit qu'un anneau est semi-factoriel lorsque la longueur des factorisations en irréductibles d'un élément de l'anneau ne dépend que de cet élément. Autrement dit, si des irréductibles π_1, ..., π_r, τ_1, ..., τ_s vérifient $\pi_1 ... \pi_r = \tau_1 ... \tau_s$, alors $r = s$.

Théorème (Carlitz). *Soit A un anneau de* Dedekind *dont le groupe de* Picard *est fini. Alors A est semi-factoriel si et seulement si $\#Pic(A) \leqslant 2$.*

Preuve.
On commence par montrer deux lemmes.

Lemme 1. Soient $\mathfrak{p}_1$, ..., $\mathfrak{p}_r$ des idéaux premiers de A tels que $\mathfrak{p}_1 ... \mathfrak{p}_r = (\pi)$ avec $\pi \in A$ non inversible. Alors π est irréductible si et seulement si aucun sous-produit strict de $\mathfrak{p}_1 ... \mathfrak{p}_r$ n'est principal.

Supposons qu'il existe un sous-produit strict principal, par exemple $\mathfrak{p}_1 ... \mathfrak{p}_k = (\gamma)$. Notons $I = \mathfrak{p}_{k+1} ... \mathfrak{p}_r$. I est un idéal strict de A (car $I \subset (\pi)$). On a alors $\gamma I = (\pi)$. En particulier, il existe $\delta \in I$ tel que $\gamma\delta = \pi$. γ est non inversible car $(\gamma) \subset (\pi)$. δ est non inversible car sinon $(\gamma) = (\pi)$ et $I = A$, ce qui est exclu. Ceci montre que π n'est pas irréductible.

Réciproquement, supposons que π soit réductible, par exemple $\pi = \gamma\delta$ avec γ, δ non inversibles. Les idéaux γ et δ admettent des décompositions en produits d'idéaux premiers et d'inverses d'idéaux premiers. Par unicité de la décomposition de (π) en produit d'idéaux premiers (et d'inverses d'idéaux premiers), les précédents sont des sous-produits stricts de $\mathfrak{p}_1...\mathfrak{p}_r$.

Lemme 2. Soit $\mathfrak{p}$ un idéal premier de A dont la classe $\bar{\mathfrak{p}}$ est d'ordre r dans $\mathrm{Pic}(A)$. Alors $\mathfrak{p}^r = (\pi)$ avec π irréductible.

$\bar{\mathfrak{p}}^r = 0$ (dans $\mathrm{Pic}(A)$) donc $\mathfrak{p}^r$ est principal : $\mathfrak{p}^r = (\pi)$ avec π non inversible. D'après le lemme précédent, π est irréductible. En effet, s'il existait un sous-produit strict principal de $\mathfrak{p}^r$, alors $\bar{\mathfrak{p}}$ serait d'ordre $< r$.

Passons maintenant à la preuve du théorème.

Si $\#\mathrm{Pic}(A) = 1$, alors A est principal donc factoriel et *a fortiori* semi-factoriel.

Supposons maintenant que $\#\mathrm{Pic}(A) = 2$. Soit x un élément non nul et non inversible de A ayant une décomposition en produit d'éléments irréductibles $x = \pi_1...\pi_r\tau_1...\tau_s$, où on a noté π_i les facteurs premiers et τ_i ceux qui ne le sont pas. Il s'agit de montrer que l'entier $r + s$ est entièrement déterminé par x.
On écrit que $Ax = (A\pi_1)...(A\pi_r)(A\tau_1)...(A\tau_s)$. L'idéal $A\tau_i$ n'étant pas premier, il se décompose en produit d'idéaux premiers $\mathfrak{q}_{i1}...\mathfrak{q}_{\mathfrak{i}\mathfrak{t}_\mathfrak{i}}$ avec $t_i \geqslant 2$. Le produit de deux idéaux non principaux étant principal (car $\#\mathrm{Pic}(A) = 2$), on a en fait $t_i = 2$ en vertu du premier lemme, par irréductibilité de τ_i. L'idéal Ax se décompose alors en produit d'idéaux premiers $(A\pi_1)...(A\pi_r)\mathfrak{q}_{i1}\mathfrak{q}_{i2}...\mathfrak{q}_{\mathfrak{s}1}\mathfrak{q}_{\mathfrak{s}2}$. Cette décomposition étant unique, le nombre de facteurs principaux l'est aussi ainsi que le nombre de facteurs non principaux, ce qui détermine r et s.

Enfin, supposons que $\#\mathrm{Pic}(A) \geqslant 3$, il s'agit d'exhiber des éléments de A qui contredisent sa semi-factorialité. On distingue deux cas :

- Il existe un élément g de $\#\mathrm{Pic}(A)$ d'ordre $m \geqslant 3$. La classe $-g$ est également d'ordre m. Soit $\mathfrak{p}$ et $\mathfrak{q}$ des représentants premiers de ces deux classes. Les idéaux $\mathfrak{p}^m$ et $\mathfrak{q}^m$ sont principaux, engendrés par des éléments irréductibles π et τ (d'après le second lemme). D'autre part, le produit $\mathfrak{p}\mathfrak{q}$ est principal et engendré par un élément irréductible θ d'après le premier lemme. On remarque que $(\mathfrak{p}\mathfrak{q})^m = \mathfrak{q}^m\mathfrak{q}^m$ soit encore $A\theta^m = A\pi\tau$, ce qui signifie qu'il existe u inversible tel que $\theta^m = u\pi\tau$. Comme $m \geqslant 3$, l'anneau A n'est pas semi-factoriel.

- S'il n'existe pas d'éléments d'ordre $\geqslant 3$ dans $\#\mathrm{Pic}(A)$, alors $\mathrm{Pic}(A) \approx (\mathbb{Z}/2\mathbb{Z})^d$ avec $d \geqslant 2$. On peut alors trouver des classes g et h telles que la classe $g + h$ soit non nulle et distincte de g et de h. Considérons alors des idéaux premiers $\mathfrak{p}$, $\mathfrak{q}$ et $\mathfrak{r}$ respectivement dans les classes g, h et $g + h$. Ces trois classes sont d'ordre 2 dans $\mathrm{Pic}(A)$ donc les idéaux $\mathfrak{p}^2$, $\mathfrak{q}^2$ et $\mathfrak{r}^2$ sont principaux engendrés par des éléments irréductibles de A, notons-les $\mathfrak{p}^2 = A\pi$, $\mathfrak{q}^2 = A\tau$ et $\mathfrak{r}^2 = A\theta$. La classe $g+h+(g+h)$ est elle-même nulle donc l'idéal $\mathfrak{pqr}$ est principal engendré par un élément irréductible, notons-le $\mathfrak{pqr} = A\psi$. On remarque que $\mathfrak{p}^2\mathfrak{q}^2\mathfrak{r}^2 = (\mathfrak{pqr})^2$ donc $A\pi\tau\theta = A\psi^2$, ce qui montre que l'anneau A n'est pas semi-factoriel.

$\square$

Leçons possibles
149 Groupes de petits cardinaux.
104 Groupes finis. Exemples et applications.
111 Exemples d'applications des idéaux d'un anneau commutatif unitaire.
108 Exemples de parties génératrices d'un groupe.

Références
?