DÉVELOPPEMENT 5

THÉORÈME DE CARLITZ

On considère un anneau de Dedekind A dont le groupe des classes d'idéaux $\mathrm{C}(A)$ est fini.
On note $\overline{\mathfrak{I}}$ la classe de l'idéal $\mathfrak{I}$.

Lemme. — *Soit $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ des idéaux premiers de A tels que $\mathfrak{p}_1 \cdots \mathfrak{p}_r = A\pi$ alors π est irréductible si et seulement s'il n'existe par de sous-produit strict $\mathfrak{p}_{i_1} \cdots \mathfrak{p}_{i_s}$ principal.*

Démonstration. — $\boxed{\Rightarrow}$ Supposons qu'il existe $\emptyset \neq F \subsetneqq \{1, \dots, r\}$ telle que $\prod_{i \in F} \mathfrak{p}_i = A\gamma$ avec γ non inversible dans A. Alors $\prod_{i \notin F} \mathfrak{p}_i$ est aussi un idéal principal non trivial de A donc $\prod_{i \notin F} \mathfrak{p}_i = A\delta$ avec δ non inversible dans A, d'où

$$A\pi = \mathfrak{p}_1 \cdots \mathfrak{p}_r = A\gamma\delta$$

i.e. il existe u inversible dans A tel que $\pi = u\gamma\delta$. Puisque ni $u\gamma$, ni δ ne sont inversibles dans A, π n'est pas irréductible dans A.

$\boxed{\Leftarrow}$ Écrivons $\pi = \gamma\delta$ avec γ et δ non inversibles dans A. On considère les factorisations des idéaux $A\gamma$ et $A\delta$ en produits d'idéaux premiers de A

$$A\gamma = \mathfrak{q}_1 \cdots \mathfrak{q}_s \quad \text{et} \quad A\delta = \mathfrak{q}'_1 \cdots \mathfrak{q}'_t.$$

On a $A\pi = A\gamma\delta$ donc

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s \mathfrak{q}'_1 \cdots \mathfrak{q}'_t$$

et par unicité de la décomposition d'un idéal en produit d'idéaux premiers, il existe une partition non triviale F, F' de $\{1, \dots, r\}$ telle que

$$\{\mathfrak{q}_1, \dots, \mathfrak{q}_s\} = \{\mathfrak{p}_i ; i \in F\} \quad \text{et} \quad \{\mathfrak{q}'_1, \dots, \mathfrak{q}'_t\} = \{\mathfrak{p}_i ; i \in F'\},$$

on a donc

$$A\gamma = \prod_{i \in F} \mathfrak{p}_i \quad \text{et} \quad A\delta = \prod_{i \in F'} \mathfrak{p}_i$$

et le produit $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ admet donc un sous-produit strict principal. □

Lemme. — *Soit $\mathfrak{p}$ un idéal premier de A dont la classe $\overline{\mathfrak{p}}$ est d'ordre r dans $\mathrm{C}(A)$ alors on a $\mathfrak{p}^r = A\pi$ avec π irréductible dans A.*

Démonstration. — Puisque $\overline{\mathfrak{p}}$ est d'ordre r, on a $r\overline{\mathfrak{p}} = 0$ et $k\overline{\mathfrak{p}} \neq 0$, pour tout $0 \leq k < r$, ce qui signifie que $\mathfrak{p}^r$ est principal et que $\mathfrak{p}^k$ n'est pas principal. □

Définition. — On dit que A est un *anneau semi-factoriel* si la longueur des factorisations d'un élément ne dépend que de l'élément, *i.e.* toute égalité du type

$$\pi_1 \dots \pi_r = \tau_1 \dots \tau_s,$$

où les π_i, τ_j sont irréductibles dans A, implique $r = s$.

Théorème de Carlitz. — *Si toute classe d'idéaux non nulle contient des idéaux premiers alors A est semi-factoriel si et seulement si $|\mathrm{C}(A)| \leq 2$.*

Démonstration. — On note $h = |\mathrm{C}(A)|$; si $h = 1$ alors l'anneau A est principal donc factoriel et *a fortiori* semi-factoriel. Supposons maintenant que $h = 2$, on considère un élément $x \in A$ non nul non inversible et une factorisation de x en produit d'éléments irréductibles

$$x = \pi_1 \dots \pi_r \tau_1 \dots \tau_s$$

où les π_i sont premiers et les τ_j ne le sont pas. Pour $1 \leq i \leq r$, on pose $\mathfrak{p}_i = A\pi_i$, c'est un idéal premier de A, on a alors

$$Ax = \mathfrak{p}_1 \dots \mathfrak{p}_r A\tau_1 \dots \tau_s.$$

Pour tout $1 \leq j \leq s$, l'élément τ_j n'est pas premier donc l'idéal $A\tau_j$ n'est pas premier *i.e.* on peut écrire $A\tau_j = \mathfrak{q}_{j,1} \dots \mathfrak{q}_{j,s_j}$ où les $\mathfrak{q}_{j,i}$ sont des idéaux premiers de A et où $s_j \geq 2$. Puisque $\mathrm{C}(A) = \mathbb{Z}/2\mathbb{Z}$, la somme de deux classes non nulles est nulle *i.e.* le produit de deux idéaux non principaux est principal. Puisque τ_j est irréductible, on déduit du lemme précédent que $s_j = 2$. On a donc

$$Ax = \mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{q}_{1,1}\mathfrak{q}_{1,2} \dots \mathfrak{q}_{s,1}\mathfrak{q}_{s,2}.$$

La décomposition d'un idéal en produit d'idéaux premiers étant unique, le nombre d'idéaux premiers principaux intervennant dans cette décomposition l'est aussi *i.e.* l'entier r ne dépend que de x. De même, le nombre d'idéaux premiers non principaux intervennant dans cette décomposition l'est aussi *i.e.* l'entier s ne dépend que de x. Finalement, la longueur $r + s$ de la factorisation initiale de x ne dépend que de x.

Pour montrer la réciproque, on suppose que $h \geq 3$ et on va exhiber des factorisations d'un même élément qui ne comportent pas le même nombre de facteurs. Il y a deux cas à considérer : soit il existe une classe d'ordre $m \geq 3$, soit le groupe des classes de A est $(\mathbb{Z}/2\mathbb{Z})^{h/2}$.

– Dans le premier cas, notons g une classe d'ordre $m \geq 3$, alors la classe $-g$ est aussi d'ordre m. Considérons dans ces deux classes deux idéaux premiers $\mathfrak{p}$ et $\mathfrak{q}$. Alors les idéaux $\mathfrak{p}^m$ et $\mathfrak{q}^m$ sont principaux engendrés par des éléments irréductibles de l'anneau, notons-les $\mathfrak{p}^m = A\pi$ et $\mathfrak{q}^m = A\tau$. D'autre part, la classe $g + (-g)$ est nulle donc l'idéal $\mathfrak{pq}$ est principal engendré par un élément irréductible, notons le $\mathfrak{pq} = A\theta$. On remarque alors que $\mathfrak{p}^m\mathfrak{q}^m = (\mathfrak{pq})^m$ donc

  $$A\pi\tau = (A\theta)^m = A\theta^m$$

  ce qui signifie qu'il existe u inversible tel que $\pi\tau = u\theta^m$. Puisque $m \geq 3$, l'anneau A n'est pas semi-factoriel.

– Dans le second cas, *i.e.* lorsque $\mathrm{C}(A) = (\mathbb{Z}/2\mathbb{Z})^{h/2}$, on peut trouver des classes g et h distinctes telles que la classe $g + h$ soit non nulle et elle-même distincte des classes g et 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 $\mathrm{C}(A)$ 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 $\mathfrak{r}^2 = A\theta$. D'autre part, 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 signifie qu'il existe u inversible tel que $\pi\tau\theta = u\psi^2$ et l'anneau A n'est donc pas semi-factoriel. □

Leçons concernées

01 Méthodes combinatoires, problèmes de dénombrements

04 Sous-groupes distingués, groupes quotients. Exemples et applications

05 Groupes finis. Exemples et applications

11 Idéaux d'un anneau commutatif unitaire. Exemples et applications

43 Exemples de parties génératrices d'un groupe

Sébastien Pellerin