Les $\mathbb{Z}$-modules de type fini sans torsion sont libres

Colas Bardavid
colas.bardavid@gmail.com

Février 2001

Notations :
$P \in \mathbb{Z}[X]$, unitaire, irréductible [1] : $P = \prod_{i \leq n}(X - x_i)$. En particulier, les x_i sont distincts.
$K = \mathbb{Q}(x_1, \ldots, x_n) = \mathbb{Q}|^P$. $A = \mathbb{Z}[x_1, \ldots, x_n]$, sous-anneau de K.
On fixe $p \in \mathcal{P}$. On suppose $\chi_p(P)$ séparable (dans $\mathbb{F}_p$).

1 Rang d'un $\mathbb{Z}$-module libre de type fini

Définition 1 *Soit A un $\mathbb{Z}$-module (*ie *un groupe abélien). On dit que A* est libre *ssi A admet une base : $\exists\, (e_i)_{i\in I} \;/\; \forall\, a \in A,\ \exists\,!\,(\lambda_i) \in \mathbb{Z}^{(I)} \;/\; a = \sum_{i\in I} \lambda_i e_i$.*

Théorème-Définition 1 *Soit A un $\mathbb{Z}$-module libre de type fini. (*ie *engendré par une sous partie finie). Alors toutes les bases ont même cardinal. Ce cardinal est le* rang de A*, noté rg A.*

Démonstration : Soit $(e_i)_{i\in I}$ une base de A. Soit $\{a_i\}_{i\leq n}$ une partie génératice de A. Chaque a_i est engendré par I_i sous-partie finie de I. Donc, A est engendré par $\bigcup_{i\leq n} I_i$. D'où l'existence d'une base finie.

On considère alors $A/_{2A}$. C'est une $\mathbb{F}_2$-espace vectoriel. En effet, $\left(A/_{2A}, +\right)$ est un groupe abélien et on vérifie le seul axiome non trivial : $\forall\, \lambda,\, \mu \in \mathbb{F}_2,\ (\lambda+\mu)x = \lambda x + \mu x$ (si $\lambda = 1 = \mu$, $x + x = 2x = 0$, dans $A/_{2A}$).

Notons $\phi : A \to A/_{2A}$ le morphisme surjectif canonique. Soit $(e_i)_{i\leq n}$ une base de A. Alors, on montre que $\mathcal{B} = (\phi(e_i))_{i\leq n}$ est une base du $\mathbb{F}_2$-espace vectoriel. $\mathcal{B}$ est clairement génératrice. Puis, si $\sum \lambda_i \phi(e_i) = 0$, où $(\lambda_i) \in (\mathbb{F}_2)^n$, on pose pour tout i, $\mu_i \in \mathbb{Z}$ tel que $\chi_2(\mu_i) = \lambda_i$. On a $\phi\left(\sum \mu_i e_i\right) = 0$ donc $\sum \mu_i e_i = 2a$, avec $a = \sum \nu_i e_i$. Donc, $\forall\, i,\ \mu_i = 2\nu_i$. Donc $\lambda_i = 0$.

Ainsi, le cardinal de toute base de A est égal à celui d'une base de $A/_{2A}$ donc à $dim_{\mathbb{F}_2}\left(A/_{2A}\right)$.

■

2 Un $\mathbb{Z}$-module de type fini sans torsion est libre

2.1 Complétion d'une famille libre en une une famille basique

La situation n'est pas simple. En effet, on ne peut pas compléter une quelconque famille libre en base. Par exemple, dans $\mathbb{Z}^2$, $(4, 6)$ n'est pas complétable en une base (comme tout vecteur du type $\delta(a, b)$, $|\delta| > 1$).

Lemme 1 *Soit $(\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n$ ($n \geq 2$) tel que les λ_i soient premiers dans leur ensemble. Alors, il existe $(\alpha_{i,j})_{\substack{1\leq i\leq n\\ 2\leq j\leq n}} \in \mathbb{Z}^{(n-1)n}$ telle que :*

$$\begin{vmatrix} \lambda_1 & \alpha_{12} & \ldots & \alpha_{1n} \\ \lambda_2 & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_n & \alpha_{n2} & \ldots & \alpha_{nn} \end{vmatrix} = 1$$

[1] Je me pose la question de savoir si cette hypothèse est nécessaire

Démonstration : On raisonne par récurrence sur n.

$\underline{n = 2}$: $\lambda_1 \wedge \lambda_2 = 1$, donc $\exists\,(m,\, n) \in \mathbb{Z}^2 \ / \ \lambda_1 m - n\lambda_2 = 1$, c'est-à-dire $\begin{vmatrix} \lambda_1 & n \\ \lambda_2 & m \end{vmatrix} = 1$.

$\underline{HR_{n-1} \Longrightarrow HR_n}$: On note δ le $pgcd$ de $\{\lambda_i\}_{i \leq n-1}$, et on note $\mu_i = \frac{\lambda_i}{\delta}$ pour $i \leq n-1$. Les μ_i sont premiers dans leur ensemble. Soit donc $(\alpha_{i,j})_{\substack{1 \leq i \leq n-1 \\ 2 \leq j \leq n-1}}$ telle que :

$$\begin{vmatrix} \mu_1 & \alpha_{12} & \dots & \alpha_{1n-1} \\ \mu_2 & \alpha_{22} & \dots & \alpha_{2n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{n-1} & \alpha_{n-12} & \dots & \alpha_{n-1n-1} \end{vmatrix} = 1$$

On sait que δ et λ_n sont premiers entre eux. Ainsi, $\exists\,(k,\, l) \in \mathbb{Z}^2 \ / \ k\delta + l\lambda_n = 1$. On vérifie alors que la matrice

$$\begin{pmatrix} \lambda_1 & \alpha_{12} & \dots & \alpha_{1n-1} & (-1)^{n-1} l\mu_1 \\ \lambda_2 & \alpha_{22} & \dots & \alpha_{2n-1} & (-1)^{n-1} l\mu_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \lambda_{n-1} & \alpha_{n-12} & \dots & \alpha_{n-1n-1} & (-1)^{n-1} l\mu_{n-1} \\ \lambda_n & 0 & \dots & 0 & (-1)^{n-1} k \end{pmatrix}$$

a pour déterminant 1, en développant par rapport à la dernière ligne. ■

Proposition 1 *Soit $\lambda = (\lambda_1,\, \dots,\, \lambda_n) \in \mathbb{Z}^n$ tel que les λ_i soient premiers dans leur ensemble. Alors, il existe $(e_i)_{i \leq n-1} \in (\mathbb{Z}^n)^{n-1}$ telle que $(\lambda,\, e_1,\, \dots,\, e_n)$ soit une $\mathbb{Z}$-base de $\mathbb{Z}^n$.*

Démonstration : On complète le vecteur colonne $(\lambda_1,\, \dots,\, \lambda_n)$ en une matrice

$$M = \begin{pmatrix} \lambda_1 & \alpha_{12} & \dots & \alpha_{1n} \\ \lambda_2 & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_n & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix} = (C_1,\, \dots,\, C_n)$$

de déterminant 1, grâce au lemme précédent. Sachant alors que $\widetilde{M}M = \det(M) I_n = I_n$, où $\widetilde{M}$ est la transposée de la comatrice de M, on en déduit que $M^{-1} \in \mathcal{M}_n(\mathbb{Z})$.

Vérifions que $(C_1,\, \dots,\, C_n)$ est une $\mathbb{Z}$-base de $\mathbb{Z}^n$. Notons $\varepsilon_i \in \mathcal{M}_{1n}(\mathbb{Z})$ tel que $(\varepsilon_i)_j = \delta_{ij}$. On a dans ce cas, $MX = \varepsilon_i \Longleftrightarrow X = M^{-1}\varepsilon_i \in \boldsymbol{\mathcal{M}_{1n}}(\mathbb{Z})$. Donc, $\varepsilon_i = \sum_{j \leq n} X_j C_j$. Ainsi, $(C_j)_{j \leq n}$ est génératrice de $\mathbb{Z}^n$ et libre car de bon cardinal. ■

2.2 Étude des quotients de $\mathbb{Z}^n$

On caractérise dans ce paragraphe les groupes quotients de $\mathbb{Z}^n$ sans torsion.

Théorème 1 (Structure des quotients sans torsion de $\mathbb{Z}^n$) *Soit G un sous-groupe de $\mathbb{Z}^n$ tel que $\mathbb{Z}^n/_G$ soit sans torsion. Alors il existe $k \in \mathbb{N}$ tel que $\mathbb{Z}^n/_G \simeq \mathbb{Z}^k$.*

Démonstration : On raisonne par récurrence sur n.

<u>n=1</u> : Dans ce cas, soit G est le groupe nul, soit G est $\mathbb{Z}$ entier. En effet, on sait que les quotients de $\mathbb{Z}$ sont les $\mathbb{Z}/_{n\mathbb{Z}}$, qui sont cycliques dès que $n > 1$.

$\underline{HR_{n-1} \Longrightarrow HR_n}$: Soit G un sous-groupe, supposé non nul, de $\mathbb{Z}^n$ tel que $\mathbb{Z}^n/_G$ soit sans torsion. Soit $\lambda \in \mathbb{Z}^n$ non nul. Soit δ le plus grand diviseur commun aux λ_i. Alors, $\mu = \left(\frac{\lambda_i}{\delta}\right)_{i \leq n} \in G$; en effet, sinon, on aurait, en notant $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n/_G$ le morphisme surjectif canonique, $\varphi(\mu) \neq 0$ et $\delta\varphi(\mu) = 0$. On peut alors compléter μ en une base $(e_i)_{i\leq n}$ où $e_1 = \mu$, et considérer :

$$\psi : \begin{array}{c} \mathbb{Z}^{n-1} \to \mathbb{Z}^n/_G \\ (x_2,\, \dots,\, x_n) \mapsto \varphi(\sum_{i\geq 2} x_i e_i) \end{array}.$$

Ce morphisme est bien défini et surjectif car $\mu \in G$. Ainsi :

$$\mathbb{Z}^n/_G \simeq \mathbb{Z}^{n-1}/_{ker\,\psi},$$

ce qui permet de conclure grâce à l'hypothèse de récurrence. ■

2.3 Les $\mathbb{Z}$-modules de type fini sans torsion sont libres

Les modules ont ceci de différent d'avec les espaces vectoriels qu'ils n'admettent pas forcément de base, même s'ils sont de type fini. On peut donner l'exemple de $\mathbb{Z}/_{n\mathbb{Z}}$, qui n'admet pas de famille libre. Cependant, on a le théorème suivant :

Théorème 2 *Soit M un $\mathbb{Z}$-module de type fini et sans torsion. Alors, M est libre.*

Démonstration : Soit M un tel module et soit $(a_i)_{i\leq n}$ une famille génératrice de M. Soit

$$\varphi : \begin{array}{c} \mathbb{Z}^n \to M \\ \lambda \mapsto \sum_{i\leq n} \lambda_i a_i \end{array}.$$

φ est surjective : $M \simeq \mathbb{Z}^n/_{ker\,\varphi} \simeq \mathbb{Z}^k$, d'après les hypothèses faites. Soient $(\varepsilon_i)_{i\leq k}$ la base canonique de $\mathbb{Z}^k$ et f un isomorphisme de $\mathbb{Z}^k$ vers M. Alors, $(f(\varepsilon_i))_{i\leq k}$ est une $\mathbb{Z}$-base de M. ■

3 Étude de A

Fait 1 *A est un $\mathbb{Z}$-module non nul, libre et de type fini.*
Par ailleurs, on a $rg(A) = [K : \mathbb{Q}]$.

Démonstration : La première assertion provient de l'étude faite précédemment sur les $\mathbb{Z}$-modules sans torsion, de type fini. Soit donc $e = (e_i)_{i\leq p}$ une base de A. Comme on sait que $K = \{R(x_1,\, \dots,\, x_n),$ $R \in \mathbb{Q}(X_1,\, \dots,\, X_n)\}$ et $A = \{R(x_1,\, \dots,\, x_n),\, R \in \mathbb{Z}(X_1,\, \dots,\, X_n)\}$, si x est un élément de K, alors $x = \frac{x'}{m}$ où $x' \in A$ et $m \in \mathbb{Z}$. On en déduit le caractère généracteur de e. La liberté s'obtient par un argument similaire. ■

4 A/pA est un anneau (fini) non nul

Fait 2 *Soit A un $\mathbb{Z}$-module non nul libre de type fini. Alors $A/_{pA}$ est un anneau fini non nul.*

Démonstration : Le fait que $A/_{pA}$ soit un anneau est acquis dès la construcation de $A/_{pA}$.

Pour montrer qu'il est fini non nul, on montre $\left(\boldsymbol{A/_{pA}},\, +\right) \simeq \left(\mathbb{Z}/_{\boldsymbol{p}\mathbb{Z}}\right)^{\boldsymbol{n}}$, où $n = \text{rg } A$. Notons $(e_i)_{i\leq n}$ une base de A. D'abord, $\phi : \begin{array}{c} A \to \mathbb{Z}^n \\ \sum \lambda_i e_i \mapsto (\lambda_i)_{i\leq n} \end{array}$ est un isomorphisme. Puis, notant $f : A \to A/_{pA}$ le morphisme surjectif canonique, on considère $\psi : \begin{array}{c} A/_{pA} \to \left(\mathbb{Z}/_{p\mathbb{Z}}\right)^n \\ f(\sum \lambda_i e_i) \mapsto (\chi_p(\lambda_i))_{i\leq n} \end{array}$. Pour prouver que ψ est bien définie, on note que $f(\sum \lambda_i e_i) = f(\sum \mu_i e_i) \Longrightarrow \sum(\lambda_i - \mu_i)e_i = pa = p\sum \beta_i e_i$. Donc $\mod(\lambda_i, p) = \mod(\mu_i, p)$. Il est clair que ψ est injective et surjective. ∎

5 Les préliminaires à la démonstration

Lemme 2 *$\sigma \in Gal_{\mathbb{Q}}(P) \Longrightarrow \sigma_{|A} \in Aut(A)$, et ψ :* $\begin{array}{c} Gal_{\mathbb{Q}}(P) \to Aut(A) \\ \sigma \mapsto \sigma_{|A} \end{array}$ *est un isomorphisme de groupes.*

Démonstration :

a) Soit $\sigma \in Gal_{\mathbb{Q}}(P) \simeq Aut_{\mathbb{Q}}\left(\mathbb{Q}|^{P}\right)$. $\sigma_{|A}$ hérite de l'injectivité et des propriétés de morphisme de σ. Puis, σ permute les racines, qui sont disctinctes et génératrice de A. Donc $\sigma(A) = A$.

b) ψ est clairement un morphisme. Si $\psi(\sigma) = Id$, $\sigma_{|A}(x_i) = \sigma(x_i) = x_i$, alors $\sigma = Id$. Enfin, soit $\rho \in Aut(A)$. Soit σ : $\begin{array}{c} K \to K \\ R(x_1, \ldots, x_n) \mapsto R(\rho(x_1), \ldots, \rho(x_n)) \end{array}$. σ est bien défnie car ρ l'est. σ est un morphisme et est surjectif car les x_i sont distincts et car ρ les permute.

∎

Lemme 3 *$Hom(A, \mathbb{E}_p) \neq \varnothing$.*

Démonstration : Soit $\mathcal{M}$ un idéal de A maximal contenant p (l'existence est assurée par le fait 2 et le lemme de Krull). Soit $\phi : A \to A/_{\mathcal{M}}$ le morphisme surjectif canonique d'anneaux. On a $\mathbb{F}_p \subset A/_{\mathcal{M}}$ car $\phi(p) = 0$ et $\phi(1) \neq 0$ ($A/_{pA}$ est non nul). Par ailleurs, $A/_{\mathcal{M}}$ est généré par $(\phi(x_i))_{i \leq n}$ et est un corps. Enfin, $\phi(P) = \chi_p(P) = \prod_{i \leq n}(X - \phi(x_i))$, donc les $\phi(x_i)$ sont les racines de $\chi_p(P)$.

Donc $A/_{\mathcal{M}} = \mathbb{F}_p|^{\chi_p(P)} = \mathbb{E}_p$. Donc, $\phi \in Hom(A, \mathbb{E}_p)$. ∎

Fixons $\tau \in Hom(A, \mathbb{E}_p)$ une fois pour toutes.

6 Structure de $Hom(A, \mathbb{E}_p)$

Lemme 4 *Soit M un $\mathbb{Z}$-module libre de type fini et L un corps. Alors, $End_{\mathbb{Z}}(M, L)$ est de dimension égale au rang de M.*

Démonstration : Notons $(e_i)_{i \leq n}$ une base de M. On démontre que f : $\begin{array}{c} End_{\mathbb{Z}}(M, L) \to L^n \\ \phi \mapsto (\phi(e_i))_{i \leq n} \end{array}$ est un isomorphisme. En fait, on a juste à montrer la surjectivité. Soit donc $(\mu_i)_{i \leq n} \in L^n$ et soit g : $\begin{array}{c} M \to K \\ \sum \lambda_i e_i \mapsto \sum \lambda_i \mu_i \end{array}$; on a bien $\phi(g) = (\mu_i)_{i \leq n}$. ∎

Proposition 2 (description des prolongements de la réduction modulo p)

$$Hom(A, \mathbb{E}_p) = \{\tau \circ \sigma, \sigma \in Aut(A)\}.$$

Démonstration : On a déjà $Hom(A, \mathbb{E}_p) \subset \{\tau \circ \sigma, \sigma \in Aut(A)\}$. On conclut par un argument de cardinalité.

Le théorème de Dedekind permet d'affirmer que les élément de $Hom\,(A,\,\mathbb{E}_p)$ sont linéairement indépendants. Or, $Hom\,(A,\,\mathbb{E}_p) \subset End_{\mathbb{Z}}(A,\,\mathbb{E}_p)$. Donc,

$$\begin{array}{ccccc} dim_{\mathbb{E}_p}(End_{\mathbb{Z}}(A,\,\mathbb{E}_p)) & \geq & \#Hom\,(A,\,\mathbb{E}_p) & \geq & [K:\mathbb{Q}] \\ || & & & & \\ \text{rg } A = [K:\mathbb{Q}] & & & & \end{array},$$

l'inégalité de droite provenant du fait que les $\tau\circ\sigma$ sont deux-à-deux distincts et $\#Aut\,(A) = \#Gal_{\mathbb{Q}}(P) = [K:\mathbb{Q}]$. Pourquoi les $\tau\circ\sigma$ sont-il deux-à-deux distincts ? $\boldsymbol{\chi_p(P)}$ **est séparable** : donc τ est injectif sur $\{x_i\}_{i\leq n}$. Or, $\sigma \neq \sigma' \Longrightarrow \exists\, i \;/\; \sigma(x_i) \neq \sigma'(x_i)$ (les x_i engendrent A). D'où le résultat. ■

7 Groupe de Galois et réduction modulo p

Théorème 3 *Soit $P \in \mathbb{Z}[X]$, unitaire, irréductible [1] de racines distinctes $x_1,\,\ldots,\,x_n$, tel que $\chi_p(P)$ soit encore à racines simples dans son corps de décomposition. Alors,*

$$\boldsymbol{Gal_{\mathbb{F}_p}(\chi_p(P))} \textbf{\textit{ est un sous-groupe de }} \boldsymbol{Gal_{\mathbb{Q}}(P)}.$$

Démonstration : Soit $\sigma \in Gal_{\mathbb{F}_p}(\chi_p(P))$. Soit $\tilde{\sigma}$ l'unique élément de $Aut\,(A)$ tel que $\sigma\circ\tau = \tau\circ\tilde{\sigma}$, d'après la proposition 2.

Alors, $\Phi : \begin{array}{c} Gal_{\mathbb{F}_p}(\chi_p(P)) \to Aut\,(A) \simeq Gal_{\mathbb{Q}}(P) \\ \sigma \mapsto \tilde{\sigma} \end{array}$ est un morphisme injectif de groupes.

Vérifions que c'est un morphisme : $\sigma_1\circ\sigma_2\circ\tau = \tau\circ\Phi(\sigma_1\circ\sigma_2) = \sigma_1\circ(\sigma_2\circ\tau) = (\sigma_1\circ\tau)\circ\Phi(\sigma_2) = \tau\circ\Phi(\sigma_1)\circ\Phi(\sigma_2)$. D'après la même proposition : $\Phi(\sigma_1\circ\sigma_2) = \Phi(\sigma_1)\circ\Phi(\sigma_2)$.

Enfin, il estinjectif car si $\Phi(\sigma) = Id$, *ie* $\sigma\circ\tau = \tau$, σ laisse forcément invariants les $\tau(x_i)$, qui sont disctincts. Donc $\sigma = Id$. ■