Modules-indices.

1.1 Notations, conventions.

Dans ce chapitre, nous présentons un outil algébrique que nous avons introduit dans [60], les modules-indices. On fixe un corps commutatif K et A un sous-anneau de K. On suppose que A est un anneau de Dedekind. Nous appelons idéal fractionnaire de A tout sous-A-module de type fini du corps $F \subseteq K$ des fractions de A. Nous rappelons que l'ensemble des idéaux fractionnaires non nuls de A forme un groupe, dont un sous-groupe est formé par les idéaux fractionnaires principaux non nuls. On note $\mathrm{Cl}\,(A)$ le groupe quotient, il s'agit du groupe des classes de A. Pour tout idéal fractionnaire non nul $\mathfrak{m}$ de A, on note $\mathrm{cl}(\mathfrak{m})$ la classe de $\mathfrak{m}$, c'est-à-dire l'image canonique de $\mathfrak{m}$ dans $\mathrm{Cl}\,(A)$.

Soit V un K-espace vectoriel. Pour M un sous-A-module de V, nous notons KM le sous-K-espace vectoriel de V engendré par M. Nous appelons A-réseau de V tout sous-A-module R de V, de type fini, dont le rang sur A est égal à la dimension du K-espace vectoriel KR,

$$\mathrm{rg}_A(R) \;=\; \dim_K (KR)\,.$$

Pour tout A-réseau R de V, on pose $d_R := \mathrm{rg}_A(R)$. D'après le théorème de structure des modules de type fini sur un anneau de Dedekind [7, §4, n°10, Proposition 24, p. 79], si $R \neq \{0\}$ alors il existe une K-base $B_R := (b_{R,i})_{i=0}^{d_R-1}$ de KR, et un idéal fractionnaire non nul $\mathfrak{m}_R$ de A, tels que $R = \mathfrak{m}_R b_{R,0} \oplus \bigoplus_{i=1}^{d_R-1} A b_{R,i}$. Le choix de $(B_R, \mathfrak{m}_R)$ n'est pas unique, cependant $\mathrm{cl}\,(\mathfrak{m}_R)$ est déterminée de façon unique par R. Il en résulte en particulier que :

- Si nécessaire on peut choisir $(B_R, \mathfrak{m}_R)$ de sorte que $\mathfrak{m}_R$ soit entier.
- Si S est un second A-réseau de V isomorphe à R en tant que A-module, on peut choisir $(B_R, \mathfrak{m}_R)$ et $(B_S, \mathfrak{m}_S)$ de sorte que $\mathfrak{m}_R = \mathfrak{m}_S$.

Enfin, remarquons que tout sous-A-module S d'un A-réseau R de V est un A-réseau de V. En effet S est aussi de type fini sur A (car A est nœthérien), et on a le diagramme commutatif suivant,

$$\begin{tikzcd} K \otimes_A S \arrow[r, hook] \arrow[d] & K \otimes_A R \arrow[d, "\wr"] \\ KS \arrow[r, hook] & KR, \end{tikzcd}$$

qui montre que $K \otimes_A S \to KS$ est un isomorphisme (et donc $\mathrm{rg}_A(S) = \dim_K (KS)$).

1.2 Définition et propriétés élémentaires.

1.2.1 Définition.

Proposition et définition 1.2.1.1 *Soient $R \neq \{0\}$ et S deux A-réseaux de V, et V' le sous-K-espace vectoriel de V engendré par R et S. On considère l'ensemble D, défini par :*

$$D := \{\det(u); u \in \mathrm{End}_K(V')/u(R) \subseteq S\}$$

Alors D est un sous-A-module de K, appelé le A-module-indice de S dans R, et noté $[R:S]_A$.

En outre :

– (i) *Si $d_S < d_R$, alors $[R:S]_A$ est nul.*

– (ii) *Si $d_R \leq d_S$ et $KS \neq KR$, alors $[R:S]_A = K$.*

– (iii) *Si $V' = KS = KR$, alors $[R:S]_A = \mathfrak{m}_S\mathfrak{m}_R^{-1}\det_{B_S,B_R}(\mathrm{Id}_{V'})$.*

Démonstration. Supposons d'abord que $d_S < d_R$. Soit u un endomorphisme du K-espace vectoriel V' tel que $u(R) \subseteq S$. Puisque $d_S < d_R$, u n'est pas injectif, et $\det(u) = 0$. On en déduit l'assertion (i).

Supposons maintenant que $d_R \leq d_S$ et $KS \neq KR$. Puisque $d_R \leq d_S$, il existe un automorphisme u du K-espace vectoriel V' tel que $u(R) \subseteq S$. Soit C une K-base de V' contenant B_R. Puisque $KS \neq KR$, il existe $c \in C \setminus B_R$. Pour tout $\lambda \in K$, soit u_λ l'unique endomorphisme du K-espace vectoriel V' tel que pour tout $b \in C \setminus \{c\}$, $u_\lambda(b) = u(b)$, et tel que $u_\lambda(c) = \lambda u(c)$. On a alors $\det(u_\lambda) = \lambda \det(u)$, ainsi que $u_\lambda(R) \subseteq S$, car u_λ coïncide avec u sur KR. Donc pour tout $\lambda \in K$, $\lambda \det(u) \in [R:S]_A$. Puisque $\det(u) \neq 0$, on a $[R:S]_A = K$. On en déduit l'assertion (ii).

Supposons enfin $V' = KS = KR$. On pose $d := d_R = d_S$ et $\Delta := \det_{B_S,B_R}(\mathrm{Id}_{V'})$.

Pour tout $a \in \mathfrak{m}_S\mathfrak{m}_R^{-1}$, soit u_a l'unique automorphisme du K-espace vectoriel V' tel que $u_a(b_{R,0}) = a.b_{S,0}$, et tel que pour tout $i \in \{1, ..., d-1\}$, $u_a(b_{R,i}) = b_{S,i}$. On a clairement $u_a(R) \subseteq S$, et :

$$\det_{B_R,B_R}(u_a) = \det_{B_R,B_S}(u_a)\det_{B_S,B_R}(\mathrm{Id}_{V'}) = a\Delta.$$

On en déduit

$$\mathfrak{m}_S\mathfrak{m}_R^{-1}\Delta \subseteq [R:S]_A. \tag{1.2.1.1}$$

Soit $\delta \in [R:S]_A$. Il existe un endomorphisme u du K-espace vectoriel V' tel que $u(R) \subseteq S$ et $\det(u) = \delta$. Soit $M := \mathrm{mat}_{B_R,B_S}(u)$. Pour tout $a \in \mathfrak{m}_R$, on a

$$u(ab_{R,0}) \in S \iff \left(\sum_{i=0}^{d-1} aM_{i,0}b_{S,i}\right) \in \left(\mathfrak{m}_S b_{S,0} \oplus \bigoplus_{i=1}^{d-1} Ab_{S,i}\right),$$

d'où

$$M_{0,0} \in \mathfrak{m}_S\mathfrak{m}_R^{-1} \quad \text{et} \quad M_{i,0} \in \mathfrak{m}_R^{-1} \quad \text{pour tout } i \in \{1, ..., d-1\}. \tag{1.2.1.2}$$

Pour tout $j \in \{1, ..., d-1\}$, on a

$$u(b_{R,j}) \in S \iff \left(\sum_{i=0}^{d-1} M_{i,j}b_{S,i}\right) \in \mathfrak{m}_S b_{S,0} \oplus \bigoplus_{i=1}^{d-1} Ab_{S,i},$$

d'où

$$M_{0,j} \in \mathfrak{m}_S \quad \text{et} \quad M_{i,j} \in A \quad \text{pour tout } i \in \{1, ..., d-1\}. \tag{1.2.1.3}$$

Soit σ une permutation de $\{0, ..., d-1\}$. Si $\sigma(0) = 0$, alors pour tout $i \in \{1, ..., d-1\}$, $\sigma(i) \in \{1, ..., d-1\}$. Dans ce cas, $M_{\sigma(0),0}$ (c'est-à-dire $M_{0,0}$) appartient à $\mathfrak{m}_S\mathfrak{m}_R^{-1}$ d'après (1.2.1.2), et pour tout $i \in \{1, ..., d-1\}$, $M_{\sigma(i),i} \in A$ d'après (1.2.1.3). On en déduit $\prod_{i=0}^{d-1} M_{\sigma(i),i} \in \mathfrak{m}_S\mathfrak{m}_R^{-1}$.

Si $\sigma(0) \in \{1, ..., d-1\}$, alors $M_{\sigma(0),0} \in \mathfrak{m}_R^{-1}$ d'après (1.2.1.2). Il existe $k \in \{1, ..., d-1\}$ tel que $0 = \sigma(k)$, et alors $M_{\sigma(k),k}$ (c'est-à-dire $M_{0,k}$) appartient à $\mathfrak{m}_S$ d'après (1.2.1.3). Pour tout $j \in \{1, ..., d-1\} \setminus \{k\}$, on a $M_{\sigma(j),j} \in A$ d'après (1.2.1.3). On en déduit $\prod_{i=0}^{d-1} M_{\sigma(i),i} \in \mathfrak{m}_S\mathfrak{m}_R^{-1}$.

Finalement, $\det_{B_R,B_S}(u) \in \mathfrak{m}_S\mathfrak{m}_R^{-1}$, car $\det_{B_R,B_S}(u) = \sum_{\sigma} \prod_{i=0}^{d-1} M_{\sigma(i),i}$, où la somme est sur toutes les permutations de $\{0, ..., d-1\}$. Puisque

$$\delta = \det_{B_R,B_S}(u)\det_{B_S,B_R}(\mathrm{Id}_{V'}) = \det_{B_R,B_S}(u)\Delta,$$

on a $\delta \in \mathfrak{m}_S\mathfrak{m}_R^{-1}\Delta$. On a ainsi vérifié

$$[R : S]_A \subseteq \mathfrak{m}_S\mathfrak{m}_R^{-1}\Delta. \tag{1.2.1.4}$$

De (1.2.1.1) et (1.2.1.4) on déduit l'assertion (iii). □

Remarque 1.2.1.2 *Soient $R \neq 0$ et S deux A-réseaux de V. Soit V' un sous-K-espace vectoriel de V contenant R et S. Alors le module-indice de R et S, considérés comme A-réseaux de V ou de V', est le même.*

Remarque 1.2.1.3 *Soit K' un sous-corps de K, contenant A. Soient $R \neq 0$ et S deux A-réseaux de V, tels que $d_S < d_R$ ou tels que $K'S \subseteq K'R$. Alors le module-indice de R et S, considérés comme A-réseaux du K-espace vectoriel V ou du K'-espace vectoriel V, est le même.*

Remarque 1.2.1.4 *Soient $R \neq 0$ et S deux A-réseaux de V. Soit $u : V \to W$ un isomorphisme de K-espaces vectoriels. Alors $u(R)$ et $u(S)$ sont des A-réseaux de W, et*

$$[R : S]_A = [u(R) : u(S)]_A .$$

Démonstration. Il est clair que $u(R)$ et $u(S)$ sont des A-réseaux de W. Soit V' le sous-K-espace vectoriel engendré par R et S. Alors $u(V')$ est le sous-K-espace vectoriel engendré par $u(R)$ et $u(S)$. Soient $\mathcal{X}$ (respectivement $\mathcal{X}'$) l'ensemble des endomorphismes v de V' (respectivement $u(V')$) tels que $v(R) \subseteq S$ (respectivement $v(u(R)) \subseteq u(S)$). On note $\tilde{u} : V' \to u(V')$ l'isomorphisme obtenu par restriction de u. Il est clair que l'application suivante est bijective

$$\mathcal{X} \to \mathcal{X}',\ v \mapsto \tilde{u} \circ v \circ \tilde{u}^{-1},$$

et puisque pour tout $v \in \mathcal{X}$, $\det(v) = \det\left(\tilde{u} \circ v \circ \tilde{u}^{-1}\right)$, on en déduit la remarque. □

Proposition 1.2.1.5 *Soient R et S deux A-réseaux non nuls de V. On suppose $KR = KS$. Alors les propriétés suivantes sont équivalentes :*

- (i) *Les A-modules R et S sont isomorphes.*
- (ii) *Il existe un automorphisme u du K-espace vectoriel KR tel que $u(R) = S$.*
- (iii) *$[R : S]_A$ est un A-module monogène.*

Lorsque ces propriétés sont vérifiées, pour tout automorphisme v du K-espace vectoriel KR tel que $v(R) = S$, on a $[R : S]_A = A\det(v)$.

Démonstration. On pose $d := d_R = d_S$. Montrons (i) $\Rightarrow$ (ii). On suppose (i) vraie. Puisque les A-modules R et S sont isomorphes, $(B_R, \mathfrak{m}_R)$ et $(B_S, \mathfrak{m}_S)$ peuvent être choisis de sorte que $\mathfrak{m}_R = \mathfrak{m}_S$. Soit u l'unique automorphisme du K-espace vectoriel KR tel que pour tout $i \in \{0, ..., d-1\}$, $u(b_{R,i}) = b_{S,i}$. Il est alors clair que $u(R) = S$, ce qui montre (ii).

Montrons (ii) $\Rightarrow$ (iii). On suppose (ii) vraie. u se restreint en un isomorphisme de A-modules de R vers S. On peut donc choisir $(B_R, \mathfrak{m}_R)$ et $(B_S, \mathfrak{m}_S)$ de sorte que $\mathfrak{m}_R = \mathfrak{m}_S$. De la proposition-définition 1.2.1.1, (iii), on déduit alors

$$[R : S]_A = A\det_{B_S,B_R}(\mathrm{Id}_{KR}),$$

et alors (iii) est vraie.

Montrons (iii) $\Rightarrow$ (i). On suppose (iii) vraie. D'après la proposition-définition 1.2.1.1, (iii), on a

$$[R : S]_A = \mathfrak{m}_S\mathfrak{m}_R^{-1}\det_{B_S,B_R}(\mathrm{Id}_{KR}),$$

Or $[R : S]_A$ est monogène. On en déduit que $\mathfrak{m}_S\mathfrak{m}_R^{-1}$ est un A-module monogène, ce qui équivaut à $\mathrm{cl}\left(\mathfrak{m}_S\mathfrak{m}_R^{-1}\right) = 1$, ou encore à $\mathrm{cl}(\mathfrak{m}_R) = \mathrm{cl}(\mathfrak{m}_S)$. On sait que si $\mathrm{cl}(\mathfrak{m}_R) = \mathrm{cl}(\mathfrak{m}_S)$, alors $\mathfrak{m}_R$ et $\mathfrak{m}_S$ sont isomorphes en tant que A-modules, et il en résulte que les A-modules R et S sont isomorphes. D'où (i).

Supposons (i), (ii), et (iii) vérifiées. Soit v un automorphisme du K-espace vectoriel KR tel que $v(R) = S$. On choisit alors $(B_R, \mathfrak{m}_R)$ et $(B_S, \mathfrak{m}_S)$ de telle sorte que $\mathfrak{m}_R = \mathfrak{m}_S$ et que pour tout $i \in \{0, ..., d-1\}$, $v(b_{R,i}) = b_{S,i}$. D'après la proposition-définition 1.2.1.1, (iii), on a

$$[R : S]_A = A\det_{B_S,B_R}(\mathrm{Id}_{KR}) = A\det_{B_R,B_S}(v)\det_{B_S,B_R}(\mathrm{Id}_{KR}) = A\det(v).$$

$\square$

Remarque 1.2.1.6 *En particulier, pour tout A-réseau $R \neq \{0\}$ de V, on a l'égalité $[R : R]_A = A$.*

1.2.2 Formule de multiplicativité des indices.

Proposition 1.2.2.1 *Soient $R \neq \{0\}$, $S \neq \{0\}$ et T trois A-réseaux de V. On suppose $KT \subseteq KS \subseteq KR$. Alors :*

$$[R : S]_A[S : T]_A = [R : T]_A$$

($[R : S]_A[S : T]_A$ étant le sous-A-module de K engendré par les éléments de la forme xy, avec $x \in [R : S]_A$ et $y \in [S : T]_A$.)

Démonstration. Si $d_T < d_R$ on a $[R : T]_A = \{0\}$ d'après la proposition-définition 1.2.1.1, (i). Nécessairement, on a aussi $d_S < d_R$ ou $d_T < d_S$, donc $[R : S]_A = \{0\}$ ou $[S : T]_A = \{0\}$. On en déduit la proposition dans ce cas.

Supposons maintenant $d_T = d_R$. Alors on a $KR = KS = KT$. D'après la proposition-définition 1.2.1.1, (iii), on a

$$\begin{aligned}
[R : T]_A &= \mathfrak{m}_T \mathfrak{m}_R^{-1} \det_{B_T, B_R} (\mathrm{Id}_{KR}) \\
&= \mathfrak{m}_S \mathfrak{m}_R^{-1} \det_{B_S, B_R} (\mathrm{Id}_{KR}) \mathfrak{m}_T \mathfrak{m}_S^{-1} \det_{B_T, B_S} (\mathrm{Id}_{KR}) \\
&= [R : S]_A [S : T]_A,
\end{aligned}$$

d'où la proposition. □

Corollaire 1.2.2.2 *Soient $R \neq \{0\}$ et S deux A-réseaux de V. On suppose que $KR \subseteq KS$, ou bien qu'on a à la fois $KS \subsetneq KR$ et $A \neq K$. Alors $[R : S]_A = ([S : R]_A)^{-1}$, où $([S : R]_A)^{-1}$ désigne le sous-A-module de K inverse de $[R : S]_A$, c'est-à-dire le sous-A-module de K sur-jacent à l'ensemble $\{x \in K / x[R : S]_A \subseteq A\}$.*

Démonstration. Supposons d'abord $KS \subsetneq KR$ et $A \neq K$. Alors d'après la proposition-définition 1.2.1.1, on a

$$[R : S]_A = \{0\} = K^{-1} = ([S : R]_A)^{-1}.$$

Supposons ensuite $KR \subsetneq KS$. Alors d'après la proposition-définition 1.2.1.1, on a

$$[R : S]_A = K = \{0\}^{-1} = ([S : R]_A)^{-1}.$$

Supposons enfin $KR = KS$. D'après la proposition 1.2.2.1 et la remarque 1.2.1.6, on a

$$[R : S]_A [S : R]_A = [R : R]_A = A,$$

d'où $[R : S]_A = ([S : R]_A)^{-1}$. □

Remarque 1.2.2.3 *Si on suppose que $d_R = d_S$ et que $KR \neq KS$, on a $[R : S]_A = K = [S : R]_A$.*

1.2.3 Sommes directes.

Lemme 1.2.3.1 *Soient $n \in \mathbb{N}^*$, $(\mathfrak{m}_i)_{i=1}^n$ et $(\mathfrak{n}_i)_{i=1}^n$ deux familles d'idéaux fractionnaires de A, $B := (b_i)_{i=1}^n$ et $C := (c_i)_{i=1}^n$ deux familles K-libres de V, qui engendrent le même sous-K-espace vectoriel de V. On pose $R := \bigoplus_{i=1}^n \mathfrak{m}_i b_i$ et $S := \bigoplus_{i=1}^n \mathfrak{n}_i c_i$. On suppose que pour tout $i \in \{1, ..., n\}$, $\mathfrak{m}_i \neq (0)$. Alors*

$$[R : S]_A = \left(\prod_{i=1}^n \mathfrak{n}_i \mathfrak{m}_i^{-1} \right) \det_{C,B} (\mathrm{Id}_{KR}).$$

Démonstration. Si il existe $i \in \{1, ..., n\}$ tel que $\mathfrak{n}_i = (0)$, alors le lemme résulte immédiatement de la proposition-définition 1.2.1.1, (i). On suppose donc que pour tout $i \in \{1, ..., n\}$, $\mathfrak{n}_i \neq (0)$. On divise la démonstration en deux étapes.

Première étape : le cas où $b_i = c_i$ pour tout $i \in \{1, ..., n\}$. Pour tout $i \in \{1, ..., n\}$, soit $x_i \in \mathfrak{n}_i\mathfrak{m}_i^{-1}$. Soit u l'endomorphisme du K-espace vectoriel V tel que pour tout $i \in \{1, ..., n\}$, on a $u(b_i) = x_i b_i$. Alors on a clairement $u(R) \subseteq S$, et $\det(u) = \prod_{i=1}^{n} x_i$. Ceci montre que

$$\prod_{i=1}^{n} \mathfrak{n}_i\mathfrak{m}_i^{-1} \subseteq [R : S]_A. \tag{1.2.3.1}$$

Soit v un endomorphisme du K-espace vectoriel KR tel que $v(R) \subseteq S$. Soit $M := \mathrm{mat}_{B,B}(u)$. Pour tout $j \in \{1, ..., n\}$, et tout $a \in \mathfrak{m}_j$, on a :

$$v(ab_j) \in S \quad \Longleftrightarrow \quad \sum_{i=1}^{n} M_{i,j} a b_i \in \bigoplus_{i=1}^{n} \mathfrak{n}_i b_i$$

D'où $M_{i,j} \in \mathfrak{n}_i\mathfrak{m}_j^{-1}$, pour tout $i \in \{1, ..., n\}$. Pour toute permutation σ de $\{1, ..., n\}$, on a $\prod_{i=1}^{n} M_{\sigma(i),i} \in \prod_{i=1}^{n} \mathfrak{n}_{\sigma(i)}\mathfrak{m}_i^{-1}$, c'est-à-dire $\prod_{i=1}^{n} M_{\sigma(i),i} \in \prod_{i=1}^{n} \mathfrak{n}_i\mathfrak{m}_i^{-1}$. On en déduit $\det(v) \in \prod_{i=1}^{n} \mathfrak{n}_i\mathfrak{m}_i^{-1}$. On a ainsi vérifié

$$[R : S]_A \subseteq \prod_{i=1}^{n} \mathfrak{n}_i\mathfrak{m}_i^{-1}. \tag{1.2.3.2}$$

Finalement, de (1.2.3.1) et (1.2.3.2) on déduit le lemme dans ce cas.

Seconde étape : le cas général. D'après la proposition 1.2.2.1 on a

$$[R : S]_A = \left[R : \overset{n}{\underset{i=1}{\oplus}} Ab_i\right]_A \left[\overset{n}{\underset{i=1}{\oplus}} Ab_i : \overset{n}{\underset{i=1}{\oplus}} Ac_i\right]_A \left[\overset{n}{\underset{i=1}{\oplus}} Ac_i : S\right]_A. \tag{1.2.3.3}$$

De la première étape, on déduit

$$\left[R : \overset{n}{\underset{i=1}{\oplus}} Ab_i\right]_A = \prod_{i=1}^{n} \mathfrak{m}_i^{-1} \quad \text{et} \quad \left[\overset{n}{\underset{i=1}{\oplus}} Ac_i : S\right]_A = \prod_{i=1}^{n} \mathfrak{n}_i. \tag{1.2.3.4}$$

D'autre part, d'après la proposition 1.2.1.5, on a

$$\left[\overset{n}{\underset{i=1}{\oplus}} Ab_i : \overset{n}{\underset{i=1}{\oplus}} Ac_i\right]_A = A\det(v),$$

où v est l'unique endomorphisme du K-espace vectoriel KR tel que pour tout $i \in \{1, ..., n\}$, $v(b_i) = c_i$. On a

$$\det(v) = \det_{B,C}(v)\det_{C,B}(\mathrm{Id}_{KR}) = \det_{C,B}(\mathrm{Id}_{KR}),$$

d'où

$$\left[\overset{n}{\underset{i=1}{\oplus}} Ab_i : \overset{n}{\underset{i=1}{\oplus}} Ac_i\right]_A = A\det_{C,B}(\mathrm{Id}_{KR}). \tag{1.2.3.5}$$

De (1.2.3.3), (1.2.3.4) et (1.2.3.5) on déduit le lemme. □

Proposition 1.2.3.2 *Soient $R \neq \{0\}$ et S deux A-réseaux de V. Soient $n \in \mathbb{N}^*$, $(R_i)_{i=1}^n$ une famille de sous-A-modules de R, et $(S_i)_{i=1}^n$ une famille de sous-A-modules de S, telles que :*

$$R = \overset{n}{\underset{i=1}{\oplus}} R_i \quad \text{et} \quad S = \overset{n}{\underset{i=1}{\oplus}} S_i$$

On suppose que pour tout $i \in \{1, ..., n\}$, $KS_i \subseteq KR_i \neq 0$. Alors :

$$[R : S]_A = \prod_{i=1}^{n} [R_i : S_i]_A$$

Démonstration. Supposons d'abord qu'il existe $i \in \{1, ..., n\}$ tel que $KS_i \neq KR_i$. Alors $KS \neq KR$. D'après la proposition-définition 1.2.1.1, (i), on a alors $[R_i : S_i]_A = 0$ et $[R : S]_A = 0$, d'où $\prod_{i=1}^{n} [R_i : S_i]_A = [R : S]_A$.

Supposons maintenant que pour tout $i \in \{1, ..., n\}$, $KS_i = KR_i$. Alors $KS = KR$. Pour tout $i \in \{1, ..., n\}$, soient $d_i := \dim_K(KR_i)$, $B_i := (b_{i,j})_{j=1}^{d_i}$ et $C_i := (c_{i,j})_{j=1}^{d_i}$ deux K-bases de KR_i, $(\mathfrak{m}_{i,j})_{j=1}^{d_i}$ et $(\mathfrak{n}_{i,j})_{j=1}^{d_i}$ deux familles d'idéaux fractionnaires non nuls de A tels que

$$R_i = \overset{d_i}{\underset{j=1}{\oplus}} \mathfrak{m}_{i,j} b_{i,j} \quad \text{et} \quad S_i = \overset{d_i}{\underset{j=1}{\oplus}} \mathfrak{n}_{i,j} c_{i,j}.$$

D'après le lemme 1.2.3.1, on a

$$[R_i : S_i]_A = \left(\prod_{j=1}^{d_i} \mathfrak{n}_{i,j} \mathfrak{m}_{i,j}^{-1} \right) \det_{C_i, B_i}(\mathrm{Id}_{KR_i}). \tag{1.2.3.6}$$

$B := (b_{1,1}, b_{1,2}, ..., b_{1,d_1}, b_{2,1}, ..., b_{n,d_n})$ est une K-base de KR. De la même faï¿½on, $C := (c_{1,1}, c_{1,2}, ..., c_{1,d_1}, c_{2,1}, ..., c_{n,d_n})$ est une K-base de KR. On a

$$R = \overset{n}{\underset{i=1}{\oplus}} \overset{d_i}{\underset{j=1}{\oplus}} \mathfrak{m}_{i,j} b_{i,j} \quad \text{et} \quad S = \overset{n}{\underset{i=1}{\oplus}} \overset{d_i}{\underset{j=1}{\oplus}} \mathfrak{n}_{i,j} c_{i,j}.$$

D'après le lemme 1.2.3.1, puis d'après (1.2.3.6), on obtient

$$\begin{aligned} [R : S]_A &= \det_{C,B}(\mathrm{Id}_{KR}) \prod_{i=1}^{n} \prod_{j=1}^{d_i} \mathfrak{n}_{i,j} \mathfrak{m}_{i,j}^{-1} = \prod_{i=1}^{n} \left(\left(\prod_{j=1}^{d_i} \mathfrak{n}_{i,j} \mathfrak{m}_{i,j}^{-1} \right) \det_{C_i, B_i}(\mathrm{Id}_{KR_i}) \right) \\ &= \prod_{i=1}^{n} [R_i : S_i]_A . \end{aligned}$$

□

1.2.4 Extension des scalaires.

Proposition 1.2.4.1 *Soit A' un sous-anneau de K contenant A. On suppose que A' est un anneau de Dedekind. Soient $R \neq \{0\}$ et S deux A-réseaux de V. Alors les sous-B-modules $A'R$ et $A'S$ de V respectivement engendrés par R et S sont des A'-réseaux de V, et*

$$[A'R : A'S]_{A'} = A'[R : S]_A,$$

où $A'[R : S]_A$ est le sous-A'-module de K engendré par $[R : S]_A$.

Démonstration. Puisque R est de type fini sur A, $A'R$ est de type fini sur A'. D'autre part on a les inégalités suivantes,

$$\dim_K(KR) \leq \mathrm{rg}_{A'}(A'R) \leq rg_A(R) = \dim_K(KR),$$

qui prouvent que $A'R$ est un A'-réseau de V (et que $d_{A'R} = d_R$). De même on vérifie que $A'S$ est un A'-réseau de V (et que $d_{A'S} = d_S$).

Si $d_S < d_R$, alors $[A'R : A'S]_{A'} = 0 = A'[R : S]_A$. Si $d_R \leq d_S$, avec $KS \neq KR$, alors $[A'R : A'S]_{A'} = K = A'[R : S]_A$.

Supposons maintenant $KR = KS$. Il est clair qu'on peut choisir $(B_{A'R}, \mathfrak{m}_{A'R})$ de sorte que $B_{A'R} = B_R$ et $\mathfrak{m}_{A'R} = A'\mathfrak{m}_R$, l'idéal de A' engendré par $\mathfrak{m}_R$. De même on choisit $(B_{A'S}, \mathfrak{m}_{A'S})$ de sorte que $B_{A'S} = B_S$ et $\mathfrak{m}_{A'S} = A'\mathfrak{m}_S$, l'idéal de A' engendré par $\mathfrak{m}_S$. D'après la proposition-définition 1.2.1.1, on a

$$\begin{aligned}[A'R : A'S]_{A'} &= \mathfrak{m}_{A'S}\mathfrak{m}_{A'R}^{-1}\det_{B_S,B_R}(\mathrm{Id}_{KR}) = A'\mathfrak{m}_S\mathfrak{m}_R^{-1}\det_{B_S,B_R}(\mathrm{Id}_{KR}) \\ &= A'[R : S]_A.\end{aligned}$$

□

Proposition 1.2.4.2 *Soit A' un sous-anneau de Dedekind de K contenant A. On suppose que $A' \cap F = A$, où $F \subseteq K$ est le corps des fractions de A. Soient $R \neq \{0\}$ et S deux A-réseaux de V. Alors*

$$[A'R : A'S]_{A'} \cap F[R : S]_A = [R : S]_A,$$

où $F[R : S]_A$ est le sous-F-espace vectoriel de K engendré par $[R : S]_A$.

Démonstration. Si $d_S < d_R$, alors $[R : S]_A = \{0\}$, et la proposition s'en déduit dans ce cas. Si $d_R \leq d_S$ et $KR \neq KS$, alors $[A'R : A'S]_{A'} = K$ et $[R : S]_A = K$, donc la proposition est triviale dans ce cas. Supposons maintenant $KR = KS$. De la proposition 1.2.4.1, on déduit

$$[A'R : A'S]_{A'} \cap F[R : S]_A \supseteq [R : S]_A. \tag{1.2.4.1}$$

Il ne reste donc à montrer que l'inclusion

$$[A'R : A'S]_{A'} \cap F[R : S]_A \subseteq [R : S]_A. \tag{1.2.4.2}$$

D'après la proposition-définition 1.2.1.1, (iii), il existe un idéal fractionnaire non nul $\mathfrak{m}$ de A, et $y \in K^*$ tel que

$$[R : S]_A = \mathfrak{m}y. \tag{1.2.4.3}$$

Soit $x \in [A'R : A'S]_{A'} \cap F[R : S]_A$. Puisque $x \in F[R : S]_A$, et d'après (1.2.4.3), il existe $\lambda \in F$ tel que

$$x = \lambda y. \tag{1.2.4.4}$$

D'après la proposition 1.2.4.1 on a $x \in A'[R : S]_A$, donc de (1.2.4.4) et (1.2.4.3) on déduit $\lambda \in A'\mathfrak{m}$, l'idéal fractionnaire de A' engendré par $\mathfrak{m}$. Alors

$$\lambda \in F \cap (A'\mathfrak{m}). \tag{1.2.4.5}$$

Pour tout $a \in \mathfrak{m}^{-1}$, de (1.2.4.5) on déduit $\lambda a \in F \cap A'$, c'est-à-dire $\lambda a \in A$ par hypothèse. Alors $\lambda \in \mathfrak{m}$, et de (1.2.4.4) on déduit $x \in \mathfrak{m}y$. Ceci étant valable pour tout $x \in [A'R : A'S]_{A'} \cap F[R : S]_A$, d'après (1.2.4.3) on a vérifié l'inclusion (1.2.4.2), ce qui achève la démonstration. □

1.3 Liens avec diverses notions classiques.

1.3.1 Modules-indices et idéaux de Fitting.

Nous référons le lecteur à la sous-section A.3.6 pour la définition et les propriétés élémentaires des idéaux de Fitting.

Théorème 1.3.1.1 *Soient M un A-module de type fini non nul, sans torsion, et N un sous-A-module de M. M et N sont identifiés à leurs images dans $K \otimes_A M$. Ce sont alors des A-réseaux de $K \otimes_A M$, et*

$$\mathrm{Fit}_A\,(M/N) \;=\; [M : N]_A\,.$$

Démonstration. Il est trivial que M est un A-réseau de $K \otimes_A M$. N est un sous-A-module de M, donc un A-réseau de $K \otimes_A M$.

Première étape : le cas où M est libre. On choisit alors $(B_M, \mathfrak{m}_M)$ de sorte que $\mathfrak{m}_M = A$. Soit $\mathcal{T}$ l'ensemble des matrices carrées $T := (T_{i,j})_{(i,j)\in\{0,\ldots,d_M-1\}^2}$ d'ordre d_M, à coefficients dans A, telles que pour tout $j \in \{0, ..., d_M - 1\}$, $\left(\sum_{i=0}^{d_M-1} T_{i,j} b_{M,i}\right) \in N$. Alors par définition, l'idéal de Fitting de M/N est l'idéal de A engendré par les déterminants des matrices $T \in \mathcal{T}$. Pour toute matrice carrée $T := (T_{i,j})_{(i,j)\in\{0,\ldots,d_M-1\}^2}$ d'ordre d_M à coefficients dans K, soit f_T l'endomorphisme du K-espace vectoriel $K \otimes_A M$ défini par T, par rapport à la base B_M. Il est trivial que $f_T(M) \subseteq N$ équivaut à $T \in \mathcal{T}$. Alors par définition, $[M : N]_A$ est le sous-A-module de K engendré par les déterminants des f_T, $T \in \mathcal{T}$. On en déduit le théorème dans ce cas.

Seconde étape : le cas général. On choisit $(B_M, \mathfrak{m}_M)$ de sorte que $\mathfrak{m}_M$ est un idéal de A. Soit L le sous-A-module de $K \otimes_A M$ librement engendré par B_M. Alors M et N sont des sous-A-modules de L, donc d'après la première étape on a

$$\mathrm{Fit}_A\,(L/M) = [L : M]_A \quad \text{et} \quad \mathrm{Fit}_A\,(L/N) = [L : N]_A\,. \tag{1.3.1.1}$$

Puisque A est un anneau de Dedekind (et en vertu de la proposition A.3.6.4, (iii)), la suite exacte

$$0 \longrightarrow M/N \longrightarrow L/N \longrightarrow L/M \longrightarrow 0$$

donne

$$\mathrm{Fit}_A\,(L/N) \;=\; \mathrm{Fit}_A\,(L/M)\,\mathrm{Fit}_A\,(M/N)\,. \tag{1.3.1.2}$$

De (1.3.1.1) et (1.3.1.2) on déduit

$$[L : N]_A \;=\; [L : M]_A\,\mathrm{Fit}_A\,(M/N)\,. \tag{1.3.1.3}$$

Or $KM = KL$ et $KN \subseteq KL$, donc en multipliant par $[M : L]_A$ on obtient, d'après la proposition 1.2.2.1 et la remarque 1.2.1.6, la formule du théorème. □

1.3.2 Indices et modules-indices.

Pour G un groupe et H un sous-groupe de G, on note $[G : H]$ l'indice de H dans G, c'est-à-dire le nombre cardinal (fini ou infini) de l'ensemble des classes de G modulo l'action de H par translation à gauche.

Proposition 1.3.2.1 *Soient $R \neq \{0\}$ et S deux A-réseaux de V, tels que $S \subseteq R$. Si l'anneau de Dedekind A est un corps on suppose en outre que $d_R = d_S$ ou que A est infini. Alors $[R : S]_A$ est un idéal de A, et :*

$$[A : [R : S]_A] = [R : S].$$

Démonstration. On distingue différents cas.

Premier cas : le cas où A est un corps et où $d_R = d_S$. Dans ce cas $R = S$ et $[R : S]_A = A$ par la remarque 1.2.1.6. Le théorème est donc trivial dans ce cas.

Second cas : le cas où $d_S < d_R$. Tout anneau intègre fini étant un corps, A est infini par hypothèse. Le A-module R/S est de type fini, de rang supérieur à 1, donc équipotent à A. D'après la proposition-définition 1.2.1.1, (i) on a $[R : S]_A = \{0\}$. Donc $A/[R : S]_A$ s'identifie à A. On en déduit $[A : [R : S]_A] = [R : S]$ dans ce cas.

Troisième cas : le cas où A est un anneau de valuation discrète et où $d_R = d_S$. Soit π une uniformisante de A. Il existe $n \in \mathbb{N}$, et $(m_i)_{i=1}^n \in (\mathbb{N}^*)^n$ tel que $R/S \simeq \bigoplus_{i=1}^n A/\pi^{m_i}A$. D'après le théorème 1.3.1.1 et les propriétés élémentaires des idéaux de Fitting (proposition A.3.6.3 et proposition A.3.6.4, (ii)) on a alors

$$[R : S]_A = \mathrm{Fit}_A(R/S) = \pi^{\sum_{i=1}^n m_i} A,$$

puis

$$[A : [R : S]_A] = \#\left(A/\pi^{\sum_{i=1}^n m_i} A\right). \tag{1.3.2.1}$$

D'autre part il est clair que les ensembles $A/\pi^{\sum_{i=1}^n m_i} A$ et $\prod_{i=1}^n (A/\pi^{m_i} A)$ sont équipotents. Donc de (1.3.2.1) on déduit

$$[A : [R : S]_A] = \prod_{i=1}^n \#(A/\pi^{m_i} A) = [R : S].$$

Quatrième cas : le cas où A est un anneau de Dedekind qui n'est pas un corps et où $d_R = d_S$. Puisque R/S est de torsion, on a un isomorphisme de A-modules

$$R/S \simeq \bigoplus_{\mathfrak{p} \in \mathrm{Max}(A)} A_{\mathfrak{p}} \otimes_A (R/S), \tag{1.3.2.2}$$

où $\mathrm{Max}(A)$ est le spectre maximal de A (voir [7, §4, n°10, Proposition 23, p. 79]). Pour tout $\mathfrak{p} \in \mathrm{Max}(A)$, $A_{\mathfrak{p}}$ est un A-module plat, et en particulier

$$\#(A_{\mathfrak{p}} \otimes_A (R/S)) = [A_{\mathfrak{p}} \otimes_A R : A_{\mathfrak{p}} \otimes_A S].$$

D'autre part les morphismes canoniques de $A_{\mathfrak{p}}$-modules $A_{\mathfrak{p}}\otimes_A R \to A_{\mathfrak{p}}R$ et $A_{\mathfrak{p}}\otimes_A S \to A_{\mathfrak{p}}S$ sont des isomorphismes (la surjectivité est triviale, et tous ces $A_{\mathfrak{p}}$-modules sont libres de rang d_R). De (1.3.2.2) on déduit alors

$$[R : S] = \prod_{\mathfrak{p}\in \mathrm{Max}(A)} [A_{\mathfrak{p}}R : A_{\mathfrak{p}}S] . \tag{1.3.2.3}$$

D'après le troisième cas on a alors

$$[R : S] = \prod_{\mathfrak{p}\in \mathrm{Max}(A)} \Big[A_{\mathfrak{p}} : [A_{\mathfrak{p}}R : A_{\mathfrak{p}}S]_{A_{\mathfrak{p}}}\Big] .$$

De la proposition 1.2.4.1 on déduit

$$[R : S] = \prod_{\mathfrak{p}\in \mathrm{Max}(A)} [A_{\mathfrak{p}} : A_{\mathfrak{p}}\,[R : S]_A] . \tag{1.3.2.4}$$

D'autre part on a un isomorphisme de A-modules

$$A/\,[R : S]_A \simeq \prod_{\mathfrak{p}\in \mathrm{Max}(A)} (A_{\mathfrak{p}}/A_{\mathfrak{p}}\,[R : S]_A) . \tag{1.3.2.5}$$

On déduit donc de (1.3.2.4) et (1.3.2.5) que

$$[R : S] = [A : [R : S]_A] .$$

□

Corollaire 1.3.2.2 *Soient R et S deux A-réseaux non nuls de V, tels que $S \subseteq R$ et $d_R = d_S$. On suppose que $A = \mathcal{S}^{-1}\mathbb{Z}$, où $\mathcal{S}$ est une partie multiplicative de $\mathbb{Z}$ qui ne contient pas 0. Alors on a*

$$[R : S]_A = [R : S]\, A.$$

Démonstration. On remarque d'abord que pour tout idéal non nul $\mathfrak{a}$ de A, on a $[A : \mathfrak{a}]\, A = \mathfrak{a}$. En particulier, on a

$$[R : S]_A = [A : [R : S]_A]\, A. \tag{1.3.2.6}$$

Une application directe de la proposition 1.3.2.1 donne ensuite

$$[R : S]_A = [R : S]\, A.$$

On peut aussi déduire le corollaire 1.3.2.2 du théorème 1.3.1.1 et de la proposition A.3.6.5. □

1.3.3 Module-indice et indice généralisé de Sinnott.

Soient R et S deux A-réseaux non nuls de V. On suppose que $KR = KS = V$ (donc $d_R = d_S$). On suppose aussi que l'on est dans un des cas suivants :

- (i) $A = \mathbb{Z}$, $K = \mathbb{Q}$ ou $K = \mathbb{R}$.
- (ii) $A = \mathbb{Z}_p$ avec p un nombre premier, et $K = \mathbb{Q}_p$.

Sous ces conditions, W. Sinnott a défini dans [56] un indice généralisé $(R:S)$ de la façon suivante. Il existe un automorphisme u du K-espace vectoriel V tel que $u(R)=S$. On pose alors

$$(R:S) \;=\; \begin{cases} |\det(u)| & \text{dans le cas (i),} \\ p^{v(\det(u))} & \text{dans le cas (ii),} \end{cases}$$

où v est la valuation normalisée sur $\mathbb{Q}_p$.

Proposition 1.3.3.1 $[R:S]_A \;=\; A\,(R:S)$.

Démonstration. C'est un corollaire immédiat de la proposition 1.2.1.5. □

1.3.4 Modules-indices et invariants relatifs.

Soient R et S deux A-réseaux non nuls de V. On suppose que K est le corps des fractions de A, et que $KR = KS = V$ (donc $d_R = d_S$). Sous ces conditions, Bourbaki définit l'invariant relatif $\chi\,(S,R)$ de S et R, de la façon suivante. Pour tout choix d'une K-base de V, on a un isomorphisme canonique $\overset{d_R}{\wedge} V \simeq K$. Via cet isomorphisme, l'image canonique de R^{d_R} dans $\overset{d_R}{\wedge} V$ est identifiée à un idéal fractionnaire non nul $\mathfrak{a}$ de A. De même, l'image canonique de S^{d_R} dans $\overset{d_R}{\wedge} V$ est identifiée à un idéal fractionnaire non nul $\mathfrak{b}$ de A. L'invariant relatif de S et R est alors défini par $\mathfrak{b}\mathfrak{a}^{-1}$. Il ne dépend pas du choix de la K-base de V. Nous utilisons une notation multiplicative pour l'invariant relatif, contrairement à la notation additive habituellement employée, car c'est plus adapté à notre situation. Nous référons le lecteur à [7, §4, n°6] pour plus de détails et pour les propriétés de l'invariant relatif. Nous mentionnons seulement les deux propriétés suivantes :

- (i) Si H, I, et J sont trois A-réseaux de V, tels que $d_H = d_I = d_J = d_R$, alors $\chi\,(H,J) = \chi\,(H,I)\,\chi\,(I,J)$ (voir [7, §4, n°6]).
- (ii) Si H et I sont deux A-réseaux de V, tels que $d_H = d_I = d_R$, et si u est un automorphisme du K-espace vectoriel V tel que $u(H) = I$, alors $\chi(I,H) = A\det(u)$ (voir [7, §4, n°6, Proposition 13]).

La proposition suivante montre que les invariants relatifs sont un cas particulier des modules-indices.

Proposition 1.3.4.1 $\chi(S,R) = [R:S]_A$.

Démonstration. On pose $M := \overset{d_R-1}{\underset{i=0}{\oplus}} Ab_{R,i}$. L'image canonique de M^{d_R} dans $\overset{d_R}{\wedge} V$ est le A-module librement engendré par $b_{R,0} \wedge \cdots \wedge b_{R,d_R-1}$. L'image canonique de R^{d_R} dans $\overset{d_R}{\wedge} V$ est $\mathfrak{m}_R b_{R,0} \wedge \cdots \wedge b_{R,d_R-1}$. Donc

$$\chi\,(M,R) = \mathfrak{m}_R^{-1}. \tag{1.3.4.1}$$

On pose $N := \overset{d_R-1}{\underset{i=0}{\oplus}} Ab_{S,i}$. Procédant de la même façon que précédemment, on obtient

$$\chi\,(S,N) = \mathfrak{m}_S. \tag{1.3.4.2}$$

Soit u l'unique automorphisme du K-espace vectoriel V tel que pour tout $i \in \{0, ..., d_R\}$, $u\,(b_{R,i}) = b_{S,i}$. D'après la propriété (ii) des invariants relatifs, on a

$$\chi\,(N,M) = A\det(u) = A\mathrm{det}_{B_S,B_R}(\mathrm{Id}_V)\det_{B_R,B_S}(u) = A\mathrm{det}_{B_S,B_R}(\mathrm{Id}_V)\,. \tag{1.3.4.3}$$

D'après la propriété (i) des invariants relatifs, on a

$$\chi(S, R) = \chi(S, N)\,\chi(N, M)\,\chi(M, R)\,. \tag{1.3.4.4}$$

Compte tenu de (1.3.4.2), (1.3.4.3), et (1.3.4.1), on déduit de (1.3.4.4) que

$$\chi(S, R) = \mathfrak{m}_S \mathfrak{m}_R^{-1} \det_{B_S, B_R}(\mathrm{Id}_V)\,. \tag{1.3.4.5}$$

De (1.3.4.5) et de la proposition-définition 1.2.1.1, (iii), on déduit alors

$$\chi(S, R) = [R : S]_A\,.$$

□

1.3.5 Les modules index de Fröhlich.

Soient R et S deux A-réseaux non nuls de V. On suppose que K est le corps des fractions de A, et que $KR = KS = V$ (donc $d_R = d_S$). Sous ces conditions, Frölich définit dans [15, 3, p. 10] un module index de la façon suivante. Pour tout idéal maximal $\mathfrak{p}$ de A, $A_{\mathfrak{p}}$ étant le localisé de A en $\mathfrak{p}$, les sous-$A_{\mathfrak{p}}$-modules $A_{\mathfrak{p}}R$ et $A_{\mathfrak{p}}S$ de V respectivement engendrés par R et S sont libres (et isomorphes). Il existe alors un automorphisme $u_{\mathfrak{p}}$ du K-espace vectoriel V tel que $u_{\mathfrak{p}}$ se restreint en un isomorphisme de $A_{\mathfrak{p}}$-modules de $A_{\mathfrak{p}}M$ vers $A_{\mathfrak{p}}N$. Le module index de R et S est par définition l'unique idéal fractionnaire $[R : S]'_A$ tel que pour tout idéal maximal $\mathfrak{p}$ de A, $A_{\mathfrak{p}}[R : S]'_A = A_{\mathfrak{p}} \det(u_{\mathfrak{p}})$. Nous référons le lecteur à [15] pour vérifier qu'un tel idéal fractionnaire existe et ne dépend pas du choix des $u_{\mathfrak{p}}$.

La proposition suivante montre que les modules index sont un cas particulier des modules-indices.

Proposition 1.3.5.1 $[R : S]'_A = [R : S]_A$.

Démonstration. Soit $\mathfrak{p}$ un idéal maximal de A. D'après la proposition 1.2.4.1 et la proposition 1.2.1.5, on a

$$A_{\mathfrak{p}}[R : S]_A = [A_{\mathfrak{p}}R : A_{\mathfrak{p}}S]_{A_{\mathfrak{p}}} = A_{\mathfrak{p}} \det(u_{\mathfrak{p}})\,.$$

Par unicité de $[R : S]'_A$, on déduit la proposition. □