SUR LES ORDRES COMMUTATIFS AVEC UN NOMBRE FINI DE RÉSEAUX INDÉCOMPOSABLES

PAR

H. JACOBINSKI

Stockholm, Suède

Soit k un corps de nombres algébriques de degré fini et K/k une k-algèbre commutative et semi-simple de dimension finie. K est la somme directe d'un nombre fini de corps, $K = \oplus \sum_1^s K_i$, K_i/k étant des extensions de degré fini. Soit $\mathfrak{o}$ un anneau de Dedekind dont k est le corps des quotients. Un $\mathfrak{o}$-ordre R de K est un anneau contenu dans K avec $1 \in R$ et $kR = K$, qui est en même temps un $\mathfrak{o}$-module de type fini. Si l'on identifie $\mathfrak{o}$ avec $\mathfrak{o}1$, chaque R-module est donc aussi un $\mathfrak{o}$-module. On appelle R-réseau un R-module de type fini, qui est projectif comme $\mathfrak{o}$-module. Chaque R-réseau se décompose en une somme directe d'un nombre fini de R-réseaux indécomposables. Désignons par $n(R)$ le nombre des R-réseaux indécomposables et non-isomorphes.

Si $\mathfrak{p}$ est un idéal premier de $\mathfrak{o}$, soit $\mathfrak{o}_\mathfrak{p}$ le complété $\mathfrak{p}$-adique de $\mathfrak{o}$ et posons $R_\mathfrak{p} = \mathfrak{o}_\mathfrak{p} \otimes_\mathfrak{o} R$. On sait (v. Jones [4]), que $n(R)$ est fini si et seulement si $n(R_\mathfrak{p})$ est fini pour chaque $\mathfrak{p}$. Nous allons donner ici des conditions nécessaires et suffisantes pour que $n(R_\mathfrak{p})$ soit fini, ce qui permet de déterminer tous les $\mathfrak{o}$-ordres R pour lesquels $n(R)$ est fini. De plus, pour les ordres $R_\mathfrak{p}$ avec $n(R_\mathfrak{p}) < \infty$, nous déterminerons aussi les types des $R_\mathfrak{p}$-réseaux indécomposables.

Soit G un groupe fini, commutatif ou non, et kG son algèbre de groupe sur k. Alors $\mathfrak{o}G$ est un $\mathfrak{o}$-ordre de kG. On sait, que $n(\mathfrak{o}G)$ est fini si et seulement si $n(\mathfrak{o}G_p)$ est fini pour chaque groupe de Sylow G_p (v. Curtis–Reiner [1], p. 579 et Kneser [5]). Or l'étude de $n(\mathfrak{o}G_p)$ se ramène toujours à l'étude de $n(\mathfrak{o}C)$ pour un groupe cyclique C, donc à l'étude d'un ordre commutatif. De notre résultat on obtient donc des conditions nécessaires et suffisantes pour que $n(\mathfrak{o}G)$ soit fini, ce qui complète les resultats partiels déjà connus (Curtis–Reiner [1], l.c., Dade [2], Kneser [5], Gudivok [3]).

1 – 662905 *Acta mathematica.* 118. Imprimé le 10 avril 1967

Généralités

Si M est un R-réseau, il y a une injection canonique de M dans le K-module $k \otimes_{\mathfrak{o}} M$. Nous identifions M avec son image sous cette injection. Cela permet d'écrire kM ou KM au lieu de $k \otimes_{\mathfrak{o}} M$. Nous désignons par $\varrho(M) = \dim_k kM$ le rang de M comme $\mathfrak{o}$-module et par $\varrho(R)$ le rang maximal d'un R-réseau indécomposable. D'après le théorème de Jordan–Zassenhaus (Curtis–Reiner [1], p. 558), il y a seulement un nombre fini de R-réseaux non-isomorphes M, tels que kM est isomorphe à un K-module donné. Cela implique, que $n(R)$ est fini si et seulement si $\varrho(R)$ est fini.

Soit $\mathfrak{p}$ un idéal premier de $\mathfrak{o}$ et $\mathfrak{o}_\mathfrak{p}$ et $R_\mathfrak{p} = \mathfrak{o}_\mathfrak{p} \otimes_{\mathfrak{o}} R$ les complétés $\mathfrak{p}$-adiques correspondants. Jones [4] a montré, que $n(R)$ est fini si et seulement si $n(R_\mathfrak{p})$ est fini pour chaque $\mathfrak{p}$ — en effet il suffit de considérer les $\mathfrak{p}$ divisant l'idéal $i(R)$ de Higman (1). Dans la suite nous nous occuperons donc seulement du cas local, en supprimant l'indice $\mathfrak{p}$.

Soit k'/k une extension de degré fini, $\mathfrak{o}'$ l'anneau de valuation de k' et $R' = \mathfrak{o}' \otimes_{\mathfrak{o}} R$. La proposition suivante est valable pour un $\mathfrak{o}$-ordre dans une algèbre semi-simple quelquonque, non nécessairement commutative.

Proposition 1. *Soit k un corps $\mathfrak{p}$-adique complet et k'/k une extension non-ramifiée de degré fini. Alors $n(R)$ est fini si et seulement si $n(R')$ est fini.*

D'abord nous allons montrer que $n(R) = \infty$ implique $n(R') = \infty$. Cela est vrai pour une extension quelqonque k'/k, ramifiée ou non. Soit M un R-réseau et $\Delta = \mathrm{Hom}_R(M, M)$. Nous considérons M comme Δ-module à droite. Une décomposition $M = \oplus \sum_1^t M_i$ est équivalente à une décomposition $\Delta = \oplus \sum_1^t \Delta_i$ de Δ comme Δ-module à gauche. Or, d'après Maranda (Curtis–Reiner [1], p. 539) il existe un α tel qu'un Δ-réseau quelquonque X est décomposable si et seulement si $X/\mathfrak{p}^\alpha X$ est décomposable. Soit J le radical de $\Delta/\mathfrak{p}^\alpha\Delta$ et Δ_0 l'anneau quotient de $\Delta/\mathfrak{p}^\alpha\Delta$ modulo J. Or, $\Delta/\mathfrak{p}^\alpha\Delta$ étant artinien, une décomposition de $\Delta/\mathfrak{p}^\alpha\Delta$ en idéaux à gauche est équivalente à une décomposition en même nombre de facteurs directes de Δ_0. Donc

$$M = \oplus \sum_1^t M_j \iff \Delta_0 = \oplus \sum_1^t l_j.$$

Supposons maintenant que M est indécomposable. Alors Δ_0 est un corps gauche avec un nombre fini d'éléments, donc un corps commutatif.

Soit $M' = \mathfrak{o}' \otimes_{\mathfrak{o}} M$ et $\Delta' = \mathrm{Hom}_{R'}(M', M')$. Si α est suffisamment grand, on a comme ci-dessus qu'une décomposition de M' est équivalente à une décomposition de $\Delta'/\mathfrak{p}^\alpha\Delta'$

(1) La démonstration dans [4] (v. aussi [1], p. 580) est faite pour les ordres $\mathfrak{o}G$; elle reste valable dans notre cas.

et celle-ci à une décomposition de Δ_0'. Or, on a $\Delta' \cong \mathfrak{o}' \otimes_{\mathfrak{o}} \Delta$. Soit $\mathfrak{p}'$ l'idéal maximal de $\mathfrak{o}'$ et $\varphi: \Delta' \to \Delta'/\mathfrak{p}'^{\alpha}\Delta'$. Alors $\varphi(\mathfrak{p}' \otimes_{\mathfrak{o}} \Delta)$ et $\varphi(\mathfrak{o}' \otimes_{\mathfrak{o}} J)$ sont des idéaux nilpotents, donc contenus dans J'. Cela donne

$$\Delta_0' = \mathfrak{o}'/\mathfrak{p}' \underset{\mathfrak{o}/\mathfrak{p}}{\otimes} \Delta_0.$$

Une décomposition $M' = \oplus \sum_1^t M_i'$ entraîne une décomposition $\Delta_0' = \oplus \sum_1^t l_i'$. Or, $\Delta_?^0$ étant le produit tensoriel de deux corps, on a $t \leqslant (\mathfrak{o}'/\mathfrak{p}' : \mathfrak{o}/\mathfrak{p}) \leqslant (k':k)$. Cela donne $(k':k) \max \varrho_{\mathfrak{o}'}(M_i') \geqslant \varrho_{\mathfrak{o}}(M)$ et $\varrho(R) = \infty$ implique bien $\varrho(R') = \infty$.

Inversément, soit $M' = \oplus \sum_i \mathfrak{o}' x_i$ un R'-réseau indécomposable. Nous considérons R comme sous-anneau de R'. Pour $r \in R$ on a $r x_i = \sum_j \beta_{i,j} x_j$ avec $\beta_{i,j} \in \mathfrak{o}'$. L'extension k'/k étant non-ramifiée, c'est une extension normale. Pour chaque automorphisme σ de k'/k posons

$$M_\sigma' = \sum_i \mathfrak{o}' x_i^\sigma$$

et
$$r x_i^\sigma = \sum_j (\sigma \beta_{i,j}) x_j^\sigma.$$

Alors $T = \oplus \sum_\sigma M_\sigma'$ est un R'-réseau. Nous faisons opérer le groupe de Galois de k'/k sur T en posant $\tau(\beta x_i^\sigma) = (\tau\beta) x_i^{\tau\sigma}$. Soit $\Theta = \Sigma\sigma$. Alors $\Theta T = \{\sum_\sigma (\sigma\omega) x_i^\sigma,\ \omega \in \mathfrak{o}'\}$ est un R-réseau dans T et nous allons montrer que $\mathfrak{o}'\Theta T = T$. Si $\omega_1, \ldots, \omega_l$ est une $\mathfrak{o}$-base de $\mathfrak{o}'$, les $y_{i,j} = \sum_\sigma (\sigma\omega_i) x_j^\sigma$ sont une $\mathfrak{o}$-base de ΘT. Or, k'/k étant non-ramifiée la déterminante $|\omega_i^\sigma|$ est une unité de $\mathfrak{o}'$. Pour chaque j on a donc $\oplus \sum \mathfrak{o}' y_{i,j} = \oplus \sum_\sigma \mathfrak{o}' x_j^\sigma$, ce qui entraine $\mathfrak{o}'\Theta T = T$. Une décomposition $\Theta T = \oplus \sum_1^t S_i$ entraîne la décomposition $T = \oplus \sum_1^t \mathfrak{o}' S_i$. Or, T est par construction somme directe de $(k':k)$ réseaux indécomposables. D'aprés le théorème de Krull–Schmidt, cela entraîne $t \leqslant (k':k)$ et aussi $\varrho_{\mathfrak{o}}(S_i) = \varrho_{\mathfrak{o}'}(\mathfrak{o}' S_i) \geqslant \varrho_{\mathfrak{o}'}(M')$. Par conséquent $n(R') = \infty$ implique $n(R) = \infty$.

Remarque. Il s'ensuit de la démonstration, que chaque R'-réseau indécomposable s'obtient comme facteur directe d'un réseau de la forme $\mathfrak{o}' \otimes_{\mathfrak{o}} M$, ou M est un R-réseau indécomposable.

Soit Ω_i/k le corps d'inertie de K_i/k; c'est une extension non-ramifiée. Si k' contient le composé de tous les Ω_i, chaque K_i'/k' est somme directe de $(\Omega_i : k)$ extensions totalement ramifiées. D'après la proposition ci-dessus, il suffit donc de considérer les ordres dans une algèbre K/k, qui est somme directe d'extensions totalement ramifiées.

Dans la suite, nous employons donc les notations suivantes. Soit k le complété $\mathfrak{p}$-adique d'un corps de nombres algébriques et K_i/k, $i = 1, \ldots, s$, des extensions totalement ramifiées de degré fini. Soient $\mathfrak{o}$, $\mathfrak{O}_i$ les anneaux de valuation de k et K_i resp. et $\mathfrak{p}$, $\mathfrak{P}_i$ les idéaux maximaux correspondants. Alors nous posons

$$K/k = \oplus \sum_1^s K_i/k$$

$$\mathfrak{O} = \oplus \sum_1^s \mathfrak{O}_i$$

$$\mathfrak{P} = \oplus \sum_1^s \mathfrak{P}_i$$

$$1 = \sum_1^s e_i, \quad e_i^2 = e_i \in \mathfrak{O}_i.$$

Evidemment, $\mathfrak{O}$ est le $\mathfrak{o}$-ordre maximal de K et $\mathfrak{P}=J(\mathfrak{O})$ son radical. Les K_i/k étant totalement ramifiées, on a

$$\mathfrak{O} = \oplus \sum_1^s \mathfrak{o}e_i + \mathfrak{P}.$$

Nous identifions $\mathfrak{o}$ avec $\mathfrak{o}1 \subset \mathfrak{O}$. Alors $\mathfrak{p} \subset \mathfrak{P}$ et

$$\mathfrak{O}/\mathfrak{P} = \oplus \sum_1^s \mathfrak{o}/\mathfrak{p}\, e_i.$$

Si R est un $\mathfrak{o}$-ordre de K on a $R \subset \mathfrak{O}$. De plus, R est un $\mathfrak{o}$-module de type fini et il existe donc $a \in \mathfrak{o}$ tel que $a\mathfrak{O} \subset R$. Le conducteur $F(R)$ de R est le $\mathfrak{O}$-idéal maximal dans R. Comme $a\mathfrak{O} \subset F(R)$ on a $kF(R)=K$ et $F(R)$ est de la forme

$$F(R) = \oplus \sum_1^s \mathfrak{P}_i^{\eta_i}, \quad \eta_i \geqslant 0.$$

Si $\eta = \max \eta_i$, cela donne $\mathfrak{P}^\alpha \subset R$ si $\alpha \geqslant \eta$.

Lemme 1. *Soit R un $\mathfrak{o}$-ordre dans K. Alors il existe des idempotents orthogonaux $E_j \in R$ avec $1=\sum_1^t E_j$ tels que*

$$R = \oplus \sum_1^t \mathfrak{o}E_j + R \cap \mathfrak{P}$$

et $R \cap \mathfrak{P} = J(R)$ est le radical de R.

Soit φ l'application $\mathfrak{O} \to \mathfrak{O}/\mathfrak{P} = \oplus \sum_1^s \mathfrak{o}/\mathfrak{p}\, \varphi(e_i)$. Alors $R+\mathfrak{P}/\mathfrak{P}$ est une sous-algèbre de $\varphi(\mathfrak{O})$. Comme $\varphi(\mathfrak{O})$ est somme directe de corps isomorphes à $\mathfrak{o}/\mathfrak{p}$, il existe des idempotents orthogonaux $E_j \in \mathfrak{O}$ tels que

$$R+\mathfrak{P}/\mathfrak{P} = \oplus \sum_1^t \mathfrak{o}/\mathfrak{p}\, \varphi(E_i).$$

Donc il existe des $x_j \in \mathfrak{P}$ tels que $r_j = E_j + x_j$ est dans R. En remplaçant r_j par sa p^m-ième puissance, avec m suffisamment grand, on voit que R contient des éléments de la forme $E_j + y_j$ avec $y_j \in \mathfrak{P}^\eta \subset R$. Par conséquent, les E_j sont dans R et R est de la forme $R=$

$\sum_1^t \mathfrak{o}E_j + R \cap \mathfrak{P}$. Il reste à montrer que $J(R) = R \cap \mathfrak{P}$. Si A est un idéal de R avec $1 \notin A$, il en est de même avec $A + R \cap \mathfrak{P}$ et cela entraîne $R \cap \mathfrak{P} \subset J(R)$. De l'autre côté, $R/R \cap \mathfrak{P}$ est semi-simple, ce qui donne $J(R) \subset R \cap \mathfrak{P}$.

Inversément, si Q est une $\mathfrak{o}$-algèbre dans $\mathfrak{P}$ avec $E_j Q \subset Q$ et $\mathfrak{P}^\eta \subset Q$ pour un $\eta > 0$, on vérifie immédiatement que $\oplus \sum_1^t \mathfrak{o}E_j + Q$ est un $\mathfrak{o}$-ordre de K.

Si $t > 1$ dans l'expression du lemme, R est somme directe des $E_j R$ et chaque $E_j R$ est un $\mathfrak{o}$-ordre indécomposable de $E_j K$. Pour chaque R-réseau M il y a une décomposition $M = \oplus \sum_1^t E_j M$, où $E_j M$ est un $E_j R$-réseau. Cela montre, que $n(R)$ est fini si et seulement si tous les $n(E_j R)$ sont finis. Il suffit donc de déterminer les ordres R indécomposables, pour lesquels $n(R)$ est fini. On obtient immédiatement du lemme 1 le

COROLLAIRE. *Un $\mathfrak{o}$-ordre indécomposable R est de la forme*

$$R = \mathfrak{o}1 + J(R) \quad \textit{avec} \quad \mathfrak{P} \supset J(R) \supset \mathfrak{P}^\eta$$

et R est contenu dans l'ordre $\mathfrak{o}\,1 + \mathfrak{P}$, qui est l'ordre indécomposable maximal de K.

Conditions nécessaires pour que $n(R) < \infty$

Soit M un R-réseau et $\Delta_M = \mathrm{Hom}_R(M, M)$; nous considérons M comme Δ_M-module à droite. Chaque $\delta \in \Delta_M$ se prolonge d'une façon unique en un homomorphisme de kM. Donc Δ_M s'identifie à un sous-anneau de Δ_{kM}; en effet, c'est un $\mathfrak{o}$-ordre dans $\Delta_{kM} = k\Delta_M$ et on a

$$\Delta_M = \{\delta \mid M\delta \subset M,\ \delta \in \Delta_{kM}\}.$$

Plus généralement, soit X un $\mathfrak{o}$-module dans K tel que $kX = K$. Comme nous avons identifié M avec un sous-module de $k \otimes_{\mathfrak{o}} M$, xM est définie pour $x \in X$ et $XM = \{xm \mid x \in X,\ m \in M\}$ est un R-module. Si X est un $\mathfrak{o}$-module de type fini, XM est un R-réseau. Pour $\delta \in \Delta_M$ on a $(XM)\delta = X(M\delta) \subset XM$, ce qui donne une application de Δ_M dans Δ_{XM}. Comme nous avons supposé $kX = K$, c'est une injection et on obtient

$$\Delta_M = \{\delta \mid M\delta \subset M,\ \delta \in \Delta_{XM}\}. \tag{1}$$

Soit S un $\mathfrak{o}$-ordre de K avec $R \subset S$ et N un S-réseau. Un R-réseau M est appelé réseau générateur de N si $M \subset N$ et $SM = N$. En posant $X = S$ dans (1), on voit que Δ_M est alors contenu dans Δ_N. Supposons maintenant que N est indécomposable. Cela veut dire qu'il n'y a pas d'idempotent $\neq 0,1$ dans Δ_N. Par conséquent, il n'y en a pas non plus dans Δ_M et M est aussi indécomposable.

LEMME 2. *Soient S et R des $\mathfrak{o}$-ordres de K avec $R \subset S$. Alors $n(S) = \infty$ implique $n(R) = \infty$.*

Car un S-réseau indécomposable N peut être considérer comme R-réseau et il suffit de prendre $M=N$ dans la remarque ci-dessus.

Soit $J=R\cap\mathfrak{P}$ le radical de R et posons

$$R_1=\{x\,|\,xJ\subset J,\ x\in K\}.$$

R_1 est un $\mathfrak{o}$-ordre de K qui contient R. En comparant les conductuers de R et R_1 on voit que R_1 est strictement plus grand que R si $R\neq\mathfrak{O}$. De plus, J est contenu dans le radical J_1 de R_1, car d'après le lemme 1 on a $J_1=R_1\cap\mathfrak{P}\supset R\cap\mathfrak{P}=J$.

Soit N un R_1-réseau et M un R-réseau générateur de N. Alors $JM=JR_1M=JN$, c.-à-d. $JN\subset M$. Par conséquent, chaque R-réseau générateur de N est complètement déterminé par son image $\bar{M}$ sous l'application

$$\varphi:\ N\to N/JN=\bar{N}.$$

Posons $\bar{R}_1=R_1/J$, $\bar{R}=R/J$ et $\bar{\mathfrak{o}}=\mathfrak{o}/\mathfrak{p}$. Comme $\mathfrak{p}\subset J$, $\bar{R}_1$ est une $\bar{\mathfrak{o}}$-algèbre de dimension finie et $\bar{J}_1$ son radical. Nous supposons dans la suite que R est un ordre indécomposable. Alors $\bar{R}=\bar{\mathfrak{o}}$ et $\bar{M}$ est un $\bar{\mathfrak{o}}$-espace dans $\bar{N}$, tel que $\bar{R}_1\bar{M}=\bar{N}$. Inversément, si L est un $\bar{\mathfrak{o}}$-espace dans $\bar{N}$ avec $\bar{R}_1L=\bar{N}$, $\varphi^{-1}L$ est un R-réseau générateur de N.

Le R_1-réseau à gauche JN est en même temps un Δ_N-réseau à droite. Donc, chaque $\delta\in\Delta_N$ induit un R_1-homomorphisme $\bar{\delta}$ de $\bar{N}$, ce qui donne une application

$$\Delta_N\to\operatorname{Hom}_{R_1}(\bar{N},\bar{N}).$$

En général, cette application n'est pas surjective, c.-à-d. $\bar{\Delta}_N$ est une sous-algèbre, en général propre, de $\operatorname{Hom}_{R_1}(\bar{N},\bar{N})$. Comme $\Delta_M\subset\Delta_N$, $\bar{\Delta}_M$ est une sous-algèbre de $\bar{\Delta}_N$ et on a

$$\bar{\Delta}_M=\{x\,|\,\bar{M}x\subset\bar{M},\ x\in\bar{\Delta}_N\}. \tag{2}$$

LEMME 3. *Soit N un R_1-réseau et ε un idempotent de Δ_N, tel que $\bar{\varepsilon}$ est trivial* (*c.-à-d.* $=0$ *ou* $=1$). *Alors ε est trivial.*

Il suffit de considérer le cas $\bar{\varepsilon}=0$, autrement on remplace ε par $1-\varepsilon$. Or, $\bar{\varepsilon}=0$ entraine $N\varepsilon\subset JN$ et comme $\varepsilon^2=\varepsilon$, cela implique $N\varepsilon\subset JN\varepsilon$, c.-à-d., $N\varepsilon=0$.

Nous allons maintenant déduire certaines conditions auxquelles doit satisfaire $\bar{R}_1$ si $n(R)$ est fini. Cela se fera de la façon suivante. Soit

$$N=R_1a_1+\ldots+R_1a_t$$

un R_1-module libre de rang t, et soit $\bar{M}_t$ un $\bar{\mathfrak{o}}$-espace dans $\bar{N}$ tel que $\bar{R}_1\bar{M}_t=\bar{N}$. Supposons que, pour chaque t — ou, au moins pour une infinité de t — on peut choisir $\bar{M}_t$ tel que

$\bar{M}_t \bar{\varepsilon} \not\subset \bar{M}_t$ pour chaque idempotent non-trivial de $\mathrm{Hom}_{\bar{R}_1}(\bar{N}, \bar{N})$. Comme $\bar{\Delta}_N \subset \mathrm{Hom}_{\bar{R}_1}(\bar{N}, \bar{N})$, cela implique que chaque $M_t = \varphi^{-1}\bar{M}_t$ est indécomposable et, le rang de ces M_t n'étant pas borné, $n(R)$ est infini. – Le lemme suivant a été démontré par Dade [2] dans le cas où R est une algèbre de groupe.

LEMME 4. *Si R est un $\mathfrak{o}$-ordre indécomposable dans $K = \oplus \sum_1^s K_i$ avec $s > 3$, on a $n(R) = \infty$.*

Il suffit de montrer cela pour $s = 4$, car pour $s > 4$ soit $E = \sum_1^4 e_i$ et $E' = 1 - E$. Alors $R \subset ER \oplus E'R$ et $n(ER) = \infty$ implique $n(R) = \infty$. Soit donc $s = 4$. Chaque ordre indécomposable est contenu dans $\mathfrak{o}1 + \mathfrak{P}$ et d'après le lemme 2 il suffit de montrer $n(R) = \infty$ pour $R = \mathfrak{o}1 + \mathfrak{P}$. Pour cet ordre on a $J = \mathfrak{P}$, $R_1 = \mathfrak{O}$ et $\bar{R}_1 = \bar{\mathfrak{o}}e_1 + \ldots + \bar{\mathfrak{o}}e_4$. Soit N un $\mathfrak{O}$-module libre de base $a_1, \ldots, a_t$, $\bar{A}$ le $\bar{\mathfrak{o}}$-espace dans $\bar{N}$ engendré par les $\bar{a}_i$ et $\Omega = \mathrm{Hom}_{\bar{\mathfrak{o}}}(\bar{A}, \bar{A})$. On a $\bar{N} = e_1\bar{N} \oplus \ldots \oplus e_4\bar{N}$ et chaque $e_i\bar{N} = \sum_j \bar{\mathfrak{o}} e_i \bar{a}_j$ est invariant sous $\bar{\Delta}_N$. Donc, chaque $\delta \in \bar{\Delta}_N$ est de la forme

$$\delta = e_1\eta_1 + \ldots + e_4\eta_4, \text{ avec } \eta_i \in \Omega.$$

Choisissons $\vartheta \in \Omega$ tel que $\bar{\mathfrak{o}}(\vartheta)$ est un corps commutatif maximal de Ω (c.-à-d. tel que le polynome caracteristique de ϑ est irréductible) et posons

$$U = \{u(x) = e_1x + e_2x + e_3x,\ x \in \bar{A}\},$$
$$V = \{v(x) = e_2x + e_3x + e_4(x\vartheta),\ x \in \bar{A}\},$$
$$\bar{M} = \bar{A} + U + V.$$

$\bar{M}$ est un $\bar{\mathfrak{o}}$-espace dans $\bar{N}$ avec $\mathfrak{O}\bar{M} = \bar{N}$; donc $M = \varphi^{-1}\bar{M}$ est un R-réseau générateur de N. Nous allons montrer que M est indécomposable pour chaque t. D'après le lemme 3, il suffit pour cela de montrer que $\bar{M}\bar{\varepsilon} \subset \bar{M}$ pour un idempotent $\bar{\varepsilon}$ de $\bar{\Delta}_N$ implique que $\bar{\varepsilon}$ est trivial. Or, $\bar{\varepsilon}$ est de la forme $\bar{\varepsilon} = e_1\eta_1 + \ldots + e_4\eta_4$ avec $\eta_i \in \Omega$. Chaque $e_i\bar{N}$ est invariant sous $\bar{\varepsilon}$; donc il en est de même avec $M \cap \sum_{i \neq 4} e_i\bar{N} = U$. Or, chaque $u \in U$ est complètement déterminé par une quelquonque de ses projections e_iu, $i = 1, 2, 3$. Cela entraîne $\bar{\varepsilon}(u(x)) = u(x\eta_1)$ et $\eta_1 = \eta_2 = \eta_3 = \eta$. De la même façon on trouve $\bar{\varepsilon}(V) \subset V$, ce qui donne $\eta_4 = \eta$ et $\eta\vartheta = \vartheta\eta$. Or, η est un idempotent et la dernière relation implique $\eta \in \bar{\mathfrak{o}}(\vartheta)$, c.-à-d. η est trivial. Par conséquent, $\bar{\varepsilon} = e_1\eta + \ldots + e_4\eta$ est aussi trivial et M est indécomposable. Le nombre t des générateurs de N étant arbitraire, cela implique bien que $n(R)$ est infini.

PROPOSITION 2. *Soit R un $\mathfrak{o}$-ordre indécomposable, $J = J(R)$ son radical, $R_1 = \{x \mid xJ \subset J,\ x \in K\}$ et $J_1 = J(R_1)$. Alors $\bar{R}_1 = R_1/J$ est une $\bar{\mathfrak{o}}$-algèbre et si $n(R)$ est fini on a*

a) $\dim_{\bar{\mathfrak{o}}}(\bar{J}_1/\bar{J}_1^2) \leqslant 1$, *c.-à-d. si $\bar{J}_1 \neq 0$, il existe $q \in \bar{J}_1$ avec $q^{\nu+1} = 0$ tel que $q, q^2, \ldots, q^\nu$ est une $\bar{\mathfrak{o}}$-base de $\bar{J}_1$;*

b) $\dim_{\bar{\mathfrak{o}}}(\bar{R}_1) \leqslant 3$.

Soit N un R_1-module libre de base $a_1, \ldots, a_t$ avec $t > 1$ et soient $\bar{A}$, Ω, ϑ etc. comme ci-dessus. Choisissons deux éléments $z_1, z_2 \in \bar{R}_1$ qui sont linéairement indépendants sur $\bar{\mathfrak{o}}$ et posons

$$W = \{w(x) = z_1 x + z_2(x\vartheta),\ x \in \bar{A}\}.$$

z_1 et z_2 étant linéairement indépendants, la somme $z_1\bar{A} + z_2\bar{A}$ est directe et cela donne

$$W \cap z_1\bar{A} = W \cap z_2\bar{A} = 0. \tag{3}$$

Posons $$\bar{M} = \bar{A} + W.$$

Alors $M = \varphi^{-1}\bar{M}$ est un R-réseau générateur de N et nous allons montrer que si une des conditions ci-dessus n'est pas vérifiée, on peut choisir z_1 et z_2 tels, que M est indécomposable pour une infinité de t. Remarquons d'abord, que la somme $\bar{A} + W$ est directe. Ceci est évident si $1, z_1, z_2$ sont linéairement indépendants. Si $1 = \alpha_1 z_1 + \alpha_2 z_2$, $\alpha_i \in \bar{\mathfrak{o}}$, et $w(x) = y \in \bar{A}$, on a $w(x) - w(\alpha_1 y) = z_2(\alpha_2 y - \alpha_1 y\vartheta) \in W \cap z_2\bar{A} = 0$, c.-à-d. $y\vartheta \in \bar{\mathfrak{o}}y$. Donc $\bar{\mathfrak{o}}y$ est invariant sous $\bar{\mathfrak{o}}(\vartheta)$ ce qui est impossible si $y \neq 0$, car $\bar{\mathfrak{o}}(\vartheta)$ est un corps de degré $t > 1$ sur $\bar{\mathfrak{o}}$.

Soit $\bar{\varepsilon}$ un idempotent de $\bar{\Delta}_N$ tel que $\bar{M}\bar{\varepsilon} \subset \bar{M}$. La somme $A + W$ étant directe, $\bar{\varepsilon}$ est de la forme

$$\bar{\varepsilon}(x) = x\sigma + w(x\tau), \quad \text{avec } \sigma, \tau \in \Omega. \tag{4}$$

Or, $\bar{\varepsilon}$ est un $\bar{R}_1$-homomorphisme de $\bar{N}$, donc on a $\bar{\varepsilon}(z_i x) = z_i x\sigma + z_i w(x\tau)$ et cela donne

$$\bar{\varepsilon}(w(x)) = w(x\sigma) + z_2 x(\vartheta\sigma - \sigma\vartheta) + z_1^2 x\tau + z_2^2 x\vartheta\tau\vartheta + z_1 z_2(\tau\vartheta + \vartheta\tau). \tag{5}$$

Supposons maintenant que la condition a) n'est pas vérifiée et choisissons $z_1, z_2 \in \bar{J}_1$ de façon qu'ils soient indépendants modulo $\bar{J}_1^2$. Cela implique que la somme $W + z_2\bar{A} + \bar{J}_1^2\bar{A}$ est directe. $\bar{J}_1\bar{N}$ étant invariant sous $\bar{\varepsilon}$, il en est de même avec $\bar{M} \cap \bar{J}_1\bar{N} = W$. Or, z_1^2, z_2^2 et $z_1 z_2$ sont dans $\bar{J}_1^2$ et, comme $\bar{\varepsilon}(W) \subset W$, on obtient de (5) que

$$\bar{\varepsilon}(w(x)) = w(x\sigma) \quad \text{et} \quad \vartheta\sigma - \sigma\vartheta = 0.$$

D'après la première relation, σ est idempotent et la deuxième entraîne $\sigma \in \bar{\mathfrak{o}}(\vartheta)$. Donc, σ est trivial. Il suffit de supposer $\sigma = 0$, autrement on remplace $\bar{\varepsilon}$ par $1 - \bar{\varepsilon}$. D'après (4) cela implique $\bar{A}\bar{\varepsilon} \subset W$ et cela donne $\bar{N}\bar{\varepsilon} = \bar{R}_1(\bar{A}\bar{\varepsilon}) \subset \bar{R}_1 W \subset \bar{J}_1\bar{N}$. Donc $\bar{\varepsilon}$ est aussi trivial et M est indécomposable pour chaque t, ce qui démontre la condition a).

L'ordre R_1 est de la forme $R_1 = \oplus\sum_1^\mu \mathfrak{o}E_i + J_1$, où les E_i sont des idempotents orthogonaux, et cela donne

$$\bar{R}_1 = \oplus\sum_1^\mu \bar{\mathfrak{o}}E_i + \bar{J}_1.$$

D'après le lemme 4, $n(R) < \infty$ implique $\mathfrak{D} = \oplus\sum_1^s \mathfrak{D}_i$ avec $s \leq 3$. Comme μ est au plus égal à s, on a bien $\dim_{\bar{\mathfrak{o}}}(\bar{R}_1) \leq 3$ si $\bar{J}_1 = 0$.

Soit donc $\bar{J}_1 \neq 0$ et $\bar{J}_1/\bar{J}_1^2 = \bar{\mathfrak{o}}q$. Comme $\bar{J}_1 = \oplus \sum_1^\mu E_i \bar{J}_1$, on a $E_i q = 0$ pour tous les i sauf un; supposons p. ex. $E_1 q = q$. Si $q^{\nu+1} = 0$ et $q^\nu \neq 0$, les éléments $q, \ldots, q^\nu$ sont une $\bar{\mathfrak{o}}$-base de $\bar{J}_1$ et on a $\dim_{\bar{\mathfrak{o}}}(\bar{R}_1) = \mu + \nu$.

Si $\nu > 2$, choisissons $z_1 = q^\nu$ et $z_2 = q^{\nu-1}$. On a $z_1^2 = z_2^2 = z_1 z_2 = 0$ et $W = \bar{M} \cap \bar{J}_1 \bar{N}$ est invariant sous $\bar{\varepsilon}$. Donc, on obtient de (5) que $z_2 x(\vartheta\sigma - \sigma\vartheta)$ est dans W pour chaque $x \in \bar{A}$. Or, d'après (3), $W \cap z_2 \bar{A} = 0$ c.-à-d. $\vartheta\sigma - \sigma\vartheta = 0$. Comme ci-dessus, cela entraine que $\bar{\varepsilon}$ est trivial. Donc $n(R) < \infty$ implique $\nu \leqslant 2$. Pour montrer b) il reste à montrer que $n(R)$ est infini si $\nu = 2$, $\mu > 1$ ou si $\nu = 1$, $\mu = 3$.

Dans le premier cas choisissons $z_1 = E_2 + q$ et $z_2 = q^2$. Comme $q = E_1 q$, on a $z_1 z_2 = z_2^2 = 0$ et (5) se réduit à

$$\bar{\varepsilon}(w(x)) = w(x\sigma) + z_2 x(\vartheta\sigma - \sigma\vartheta) + z_1^2 x\tau, \quad x \in \bar{A}.$$

Or, $1, z_1, z_2, z_1^2$ sont linéairement indépendants, c.-à-d. la somme $\bar{A} + z_1\bar{A} + z_2\bar{A} + z_1^2\bar{A}$ est directe. Comme $\bar{M}$ est contenu dans $\bar{A} + z_1\bar{A} + z_2\bar{A}$, la condition $\bar{\varepsilon}(w(x)) \in \bar{M}$ entraîne $\tau = 0$. De plus, $\bar{J}_1\bar{N}$ et $E_2\bar{N}$ sont invariants sous $\bar{\varepsilon}$; donc $W = \bar{M} \cap (\bar{J}_1\bar{N} + E_2\bar{N})$ est aussi invariant sous $\bar{\varepsilon}$. Comme ci-dessus, cela entraîne que $\vartheta\sigma - \sigma\vartheta = 0$ et que $\bar{\varepsilon}$ est trivial. M est donc indécomposable pour chaque t et $n(R)$ est infini.

Si $\mu = 3$ et $\nu = 1$, choisissons $z_1 = q + E_2$ et $z_2 = q + E_3$. Alors $1, z_1, z_2, z_1^2 = E_2$ est une $\bar{\mathfrak{o}}$-base de $\bar{R}_1$, c.-à-d. la somme $\bar{A} + z_1\bar{A} + z_2\bar{A} + z_1^2\bar{A}$ est directe. Or, $\bar{M}$ étant contenu dans $\bar{A} + z_1\bar{A} + z_2\bar{A}$, la projection d'un élément de $\bar{M}$ sur $z_1^2\bar{A}$ est $= 0$. On a $z_1 z_2 = 0$ et $z_2^2 = z_1^2 + z_2 - z_1$; si l'on substitue cela dans (5), la condition $\bar{\varepsilon}(w(x)) \in \bar{M}$ donne

$$\tau + \vartheta\tau\vartheta = 0.$$

Pour chaque entier l, cela implique $\tau(-\vartheta^{-1})^l = \vartheta^l\tau$. Si $f(X) \in \bar{\mathfrak{o}}[X]$ est le polynome irréductible avec $f(\vartheta) = 0$, on a donc

$$\tau f(-\vartheta^{-1}) = f(\vartheta)\tau = 0.$$

$f(X)$ est un polynome de degré $t > 1$, t étant le nombre des générateurs de N. Pour t impair on a certainement $f(-\vartheta^{-1}) \neq 0$ et comme $f(-\vartheta^{-1})$ est un élément du corps $\bar{\mathfrak{o}}(\vartheta)$ cela implique $\tau = 0$. Donc, pour t impair, (5) se réduit à

$$\bar{\varepsilon}(w(x)) = w(x\sigma) + z_2 x(\sigma\vartheta - \vartheta\sigma).$$

Or, $\bar{J}_1\bar{N}$, $E_2\bar{N}$ et $E_3\bar{N}$ étant invariants sous $\bar{\varepsilon}$, il en est de même avec

$$W = \bar{M} \cap (\bar{J}_1\bar{N} + E_2\bar{N} + E_3\bar{N}).$$

Comme ci-dessus, cela entraîne que $\sigma\vartheta - \vartheta\sigma = 0$ et que $\bar{\varepsilon}$ est trivial. Par conséquent, M est indécomposable au moins pour t impair, ce qui achève la démonstration.

Nous allons maintenant déduire quelques conséquences de la proposition 2, dont nous aurons besoin dans la suite. La condition b) du corollaire suivant est du à M. Kneser ([5], Satz 2) pour le cas $R=\mathfrak{o}G$, G un p-groupe abelien.

COROLLAIRE 1. *Soit R un ordre indécomposable dans $K=\oplus\sum_1^s K_i$ et soit*

$$\mathfrak{O}J(R)=\oplus\sum \mathfrak{P}_i^{\alpha_i}.$$

Alors $n(R)<\infty$ implique

a) $\alpha_i=1$ *pour tous les i à l'exception d'un au plus;*

b) $\sum_1^s \alpha_i \leqslant 3$.

L'ordre $S=\mathfrak{o}1+\mathfrak{O}J(R)$ contient R et est indécomposable. Alors $n(R)<\infty$ implique $n(S)<\infty$ et on obtient le corollaire en appliquant la proposition 2 à l'ordre S.

COROLLAIRE 2. *Soit R un $\mathfrak{o}$-ordre indécomposable dans $K=\oplus\sum_1^s K_i$ avec $s<4$. Alors $n(R)<\infty$ entraîne*

$$J(R)+\mathfrak{P}_i=\mathfrak{P}$$

pour tous les i à l'exception d'un au plus.

Soit d'abord $S=R+\mathfrak{P}^2$. Alors on a $J(S)+\mathfrak{P}_i=\mathfrak{P}$ si et seulement si $J(R)+\mathfrak{P}_i=\mathfrak{P}$, c.-à-d. on peut supposer que $\mathfrak{P}^2\subset J(R)$. Or, la relation $\mathfrak{P}\supset J(R)\supset\mathfrak{P}^2$ entraîne $J_1=\mathfrak{P}$ et d'après la proposition 2 on a donc $\dim_{\bar{\mathfrak{o}}}(\mathfrak{P}/J(R))\leqslant 1$. Si cette dimension est $=0$, on a $J(R)=\mathfrak{P}$ et il n'y a rien à démontrer. Supposons donc que cette dimension est $=1$ et désignons par π_i une uniformisante de K_i. Alors $J(R)\neq\mathfrak{P}$ entraîne qu'au moins une des π_i n'est pas dans $J(R)$. Supposons par exemple $\pi_1\notin J(R)$; alors on a $\mathfrak{P}/J(R)=\bar{\mathfrak{o}}\bar{\pi}_1$, c.-à-d. $J(R)+\mathfrak{P}_1=\mathfrak{P}$. Ceci démontre le corollaire pour $s=2$. Soit $s=3$ et supposons que $J(R)+\mathfrak{P}_i\neq\mathfrak{P}$ pour $i=2,3$. Cela entraîne que π_2 et π_3 sont dans $J(R)$ et on a $J(R)=\mathfrak{P}_1^2+\mathfrak{P}_2+\mathfrak{P}_3$. Or, d'après le corollaire 1, cela implique $n(R)=\infty$, contrairement à l'hypothèse.

Ordres dans un corps

Nous allons montrer le théorème suivant :

THEORÈME 1. *Soit k un corps $\mathfrak{p}$-adique complet, K/k une extension totalement ramifiée de degré fini, $\nu(x)$ la valuation normée de K et R un $\mathfrak{o}$-ordre de K. Alors $n(R)$ est fini, si et seulement s'il existe ou $r\in R$ avec $\nu(r)=2$ ou $r, r'\in R$ avec $\nu(r)=3$ et $\nu(r')=4$ ou $=5$.*

La nécessité de ces conditions se déduit facilement de la proposition 2. Soit $\nu(J)=\{\nu(x),\ x\in J(R)\}$ et $\alpha=\min_{x\in J}\nu(x)$. Si $\alpha=1$, R contient une uniformisante de K, c.-à-d.

$R=\mathfrak{O}$, et $\mathfrak{O}$ satisfait évidemment aux conditions du théorème. Si $\alpha=2$, il existe $r\in R$ avec $\nu(r)=2$. Supposons donc $\alpha>2$. Or, on a $\mathfrak{O}J=\mathfrak{P}^{\alpha}$ et d'après le corollaire ci-dessus, $n(R)<\infty$ implique $\alpha\leqslant 3$. Donc $\alpha=3$ et il existe $r\in R$ avec $\nu(r)=3$. Désignons par S l'ordre $\mathfrak{o}1+\mathfrak{o}r+\mathfrak{P}^6$; nous allons montrer que $n(S)=\infty$. On a $S_1=\mathfrak{o}1+\mathfrak{P}^3=S+\mathfrak{o}\pi^4+\mathfrak{o}\pi^5$ où π est une uniformisante de K. Cela donne $\bar{J}_1=\mathfrak{o}\pi^4+\mathfrak{o}\pi^5/\mathfrak{P}^6$ et $\bar{J}_1^2=0$ et on a $\dim_{\bar{\mathfrak{o}}}(\bar{J}_1/\bar{J}_1^2)=2$. D'après la proposition 2, cela entraîne $n(S)=\infty$. Par conséquent, $n(R)<\infty$ implique que R n'est pas contenu dans S, c.-à-d. il y a un élément $r'\in R$ tel que $\nu(r')=4$ ou $\nu(r')=5$.

Pour montrer que ces conditions sont aussi suffisantes, nous allons d'abord construire un système de générateurs pour un R-réseau M quelconque. Désignons par $T=T(R)$ l'ensemble des entiers positifs non contenus dans $\nu(J)$. Si $F(R)=\mathfrak{P}^{\eta}$ est le conducteur de R, on a $1\leqslant\tau<\eta$ pour $\tau\in T$ et $\eta-1$ est dans T, car autrement $\mathfrak{P}^{\eta-1}$ serait déjà dans R.

Soit M un R-réseau, $N=\mathfrak{O}M$ et $\varphi:N\to N/\mathfrak{P}N=\bar{N}$. Choisissons des éléments $q_i\in\mathfrak{O}$ avec $\nu(q_i)=i$ et posons

$$\Theta_i(M)=\varphi(q_i^{-1}(\mathfrak{P}^iM\cap M)),\quad i=0,1,\ldots.$$

$\Theta_i(M)$ est un $\bar{\mathfrak{o}}$-espace dans $\bar{N}$, qui ne dépend pas du choix des q_i. Comme $J(\mathfrak{O})=\mathfrak{P}$ et $R+\mathfrak{P}=\mathfrak{O}$, on a $\Theta_0(M)=\bar{N}$; plus généralement on a

$$\Theta_i(M)=\bar{N}\quad\text{si}\quad i\notin T.$$

Soit $i=\nu(r_i)$ avec $r_i\in R$. Alors on a $\mathfrak{P}^i=\mathfrak{O}r_i$ et $r_i^{-1}(\mathfrak{P}^iM\cap M)=r_i^{-1}(r_iN\cap M)\supset M$. Cela implique que $\bar{M}\subset\Theta_i(M)$ et comme $\bar{M}=\Theta_0(M)=\bar{N}$, on a bien $\Theta_i(M)=\bar{N}$. $\Theta_i(M)$ est donc trivial si $i\notin T$. Pour σ, $\tau\in T$ écrivons $\sigma\succ\tau$ si $\sigma-\tau\in\nu(J)$. Alors on a

$$\Theta_\sigma(M)\supset\Theta_\tau(M)\quad\text{si}\quad\sigma\succ\tau.\tag{6}$$

Car soit $\sigma-\tau=\nu(x)$ avec $x\in R$. Alors on peut choisir $q_\sigma=xq_\tau$ et on obtient

$$q_\sigma^{-1}(\mathfrak{P}^\sigma M\cap M)\supset q_\sigma^{-1}(x\mathfrak{P}^\tau M\cap xM)=q_\tau^{-1}(\mathfrak{P}^\tau M\cap M),$$

ce qui entraîne (6).

Lemme 5. *Si B est un R-réseau contenu dans M tel que*

$$\Theta_i(M)=\Theta_i(B)\quad\textit{pour } i=0 \textit{ et } i\in T,$$

on a $B=M$.

D'abord, $\Theta_0(M)=\Theta_0(B)$ entraîne $\mathfrak{O}M=\mathfrak{O}B$ et aussi $\mathfrak{P}^lM=\mathfrak{P}^lB$ pour $l\geqslant 0$. Si $l\geqslant\eta$, on a $\mathfrak{P}^lB\subset B$, c.-à-d. $\mathfrak{P}^lM\cap M=\mathfrak{P}^lB\cap B$ pour $l\geqslant\eta$. Supposons que $M\neq B$ et soit λ l'exposant maximal tel que $\mathfrak{P}^\lambda M\cap M\neq\mathfrak{P}^\lambda B\cap B$. Alors $\Theta_\lambda(M)=\Theta_\lambda(B)$ implique que chaque élément m de $\mathfrak{P}^{\lambda}M \cap M$ est de la forme $m = b + u$ avec $b \in B$ et $u \in \mathfrak{P}^{\lambda+1}M$. Or, B étant contenu dans M, on a $u \in \mathfrak{P}^{\lambda+1}M \cap M$ et λ étant maximal, cela entraîne $u \in B$ et aussi $m \in B$ pour chaque $m \in \mathfrak{P}^{\lambda}M \cap M$, ce qui est une contradiction.

Nous allons utiliser ce lemme pour construire un système de générateurs de M. Choisissions d'abord des éléments $v_i \in M$ de façon que $\{\bar{v}_i\}$ est une base de $\bar{M}$ et posons

$$V = \sum_i Rv_i.$$

V est un R-réseau libre tel que $\Theta_0(V) = \Theta_0(M)$. Cela entraîne $\Theta_i(V) = \Theta_i(M)$ pour $i \notin T$. D'après le lemme, M est donc de la forme

$$M = V + \sum_{\tau \in T} Y_\tau, \tag{7}$$

où les réseaux $Y_\tau \subset \mathfrak{P}^\tau M \cap M$ sont choisis tels que $\Theta_i(V + \sum_{\tau \leqslant i} Y_\tau) = \Theta_i(M)$ pour $i \in T$. Plus précisément, soit $\tau \in T$ et supposons qu'on ait déjà construit un réseau $X = V + \sum_{\sigma<\tau} Y_\sigma$, tel que $\Theta_\sigma(X) = \Theta_\sigma(M)$ pour $\sigma < \tau$. Comme $X \subset M$, on a $\Theta_\tau(X) \subset \Theta_\tau(M)$; choisissons des éléments $y_{\tau,i} \in M \cap \mathfrak{P}^\tau M$ de façon que $\{\varphi(q_\tau^{-1} y_{\tau,i})\}$ est une base de $\Theta_\tau(M)/\Theta_\tau(X)$ et posons

$$Y_\tau = \sum Ry_{\tau,i}.$$

Alors pour $X' = V + \sum_{\sigma \leqslant \tau} Y_\sigma$ on a bien $\Theta_\sigma(X') = \Theta_\sigma(M)$ pour $\sigma \leqslant \tau$, ce qui justifie (7). Les Y_σ sont des R-réseaux libres, contenus dans $\mathfrak{P}^\sigma M$, dont les générateurs sont indépendants modulo $\mathfrak{P}^{\sigma+1}M$. Notons aussi que ni V ni Y_σ n'est uniquement déterminé par M. Au contraire, chaque générateur v_i de V peut être remplacé par $v_i + u$ avec $u \in \mathfrak{P}M \cap M$ et chaque $y_{\tau,i}$ par $y_{\tau,i} + u$ avec $u \in \mathfrak{P}^{\tau+1}M \cap M$.

Nous allons maintenant écrire les générateurs $y_{\tau,i}$ sous une forme différente. On a $\mathfrak{P}^\tau \subset J(R) + \sum Rq_\sigma$, avec $\sigma \in T$ et $\sigma \geqslant \tau$. Cela entraîne $\mathfrak{P}^\tau M = \mathfrak{P}^\tau V \subset V \cap \mathfrak{P}^\tau V + \sum q_\sigma V$. Or, V étant un R-réseau libre on a $\mathfrak{P}^\tau V \cap V \subset \mathfrak{P}^{\tau+1} V \cap V$ et d'après la remarque ci-dessus, on peut choisir les $y_{\tau,i}$ dans $\sum q_\sigma V$:

$$y_{\tau,i} = q_\tau v_{\tau,i} + \sum_{\sigma>\tau} q_\sigma z^\sigma_{\tau,i}, \quad \text{avec} \quad v_{\tau,i},\ z^\sigma_{\tau,i} \in V.$$

Posons $V_\tau = \sum_i Rv_{\tau,i}$; on a $\Theta_\tau(Y_\tau) = \bar{V}_\tau$ et $\Theta_\tau(y_{\tau,i}) = \bar{v}_{\tau,i}$. Or, les $y_{\tau,i}$ étant choisis de façon que $\Theta_\tau(y_{\tau,i})$ est une base de $\Theta_\tau(Y_\tau)$, on voit que V_τ est un R-réseau libre dans V, dont les générateurs sont indépendants modulo $\mathfrak{P}V \cap V$. Cela veut dire, que V_τ est facteur directe de V.

Considérons l'application $v_{\tau,i} \to z^\sigma_{\tau,i}$; comme V_τ est un R-réseau libre, elle se prolonge en un R-homomorphisme

$$\delta_{\tau,\sigma}:\ V_\tau \to V.$$

Nous allons montrer, qu'on peut choisir les $z^{\sigma}_{\tau,i}$ de façon que Im $\delta_{\tau,\sigma}$ est un R-réseau libre, dont les générateurs sont indépendants modulo $V \cap \mathfrak{P}V$, c.-à-d. de façon que Im $\delta_{\tau,\sigma}$ est facteur directe de V. Soit $\bar{\delta}_{\tau,\sigma}: \bar{V}_\tau \to \bar{V}$ l'homomorphisme induit par $\delta_{\tau,\sigma}$ et posons

$$\bar{V}_\tau = \operatorname{Ker} \bar{\delta}_{\tau,\sigma} \oplus \bar{X}.$$

On peut choisir les générateurs $v_{\tau,i}$ tels que $\bar{v}_{\tau,1}, \ldots, \bar{v}_{\tau,l}$ est une base de Ker $\bar{\delta}_{\tau,\sigma}$. Pour $i \leqslant l$ on a $v_{\tau,i}\delta_{\tau,\sigma} = z^{\sigma}_{\tau,i} \in V \cap \mathfrak{P}V$ ce qui entraîne $q_\sigma z^{\sigma}_{\tau,i} \in \mathfrak{P}^{\sigma+1}V$. Or, on a $\mathfrak{P}^{\sigma+1}V \subset \mathfrak{P}^{\sigma+1}V \cap V + \sum_{\mu>\sigma} q_\mu V$ et il existe donc $u \in P^{\sigma+1}V \cap V$ et $u_\mu \in V$ avec

$$q_\sigma z^{\sigma}_{\tau,i} = u + \sum_{\mu>\sigma} q_\mu u_\mu.$$

En remplaçant $y_{\tau,i}$ par $y_{\tau,i} - u$ et en changeant les $z^{\mu}_{\tau,i}$ pour $\mu > \sigma$, on peut donc obtenir que $z^{\sigma}_{\tau,i} = 0$. Donc on peut supposer que $\bar{v}_{\tau,i}\bar{\delta}_{\tau,\sigma} = 0$ entraîne $v_{\tau,i}\delta_{\tau,\sigma} = 0$ par un choix convenable de Y_τ et en modifiant les $\delta_{\tau,\mu}$ pour $\mu > \sigma$. Alors Im $\delta_{\tau,\sigma}$ est engendré par les $v_{\tau,i}\,\delta_{\tau,\sigma}$ pour $i > l$ et ces générateurs sont en effet indépendants modulo $V \cap \mathfrak{P}V$.

Soit σ' le plus petit élément de T avec $\sigma' > \sigma$. Alors d'une façon analogue, en modifiant les $\delta_{\tau,\mu}$ pour $\mu \geqslant \sigma'$ — donc sans changer ni $\delta_{\tau,\sigma}$ ni Im $\delta_{\tau,\sigma}$ — on peut obtenir que Im $\delta_{\tau,\sigma'}$ est un R-réseau libre dont les générateurs sont indépendants modulo $V \cap \mathfrak{P}V$. En continuant ainsi, on obtient la

Proposition 3. *Soit K/k un corps $\mathfrak{p}$-adique complet totalement ramifié sur k, R un $\mathfrak{o}$-ordre de K, M un R-réseau quelqonque et $V \subset M$ un R-réseau libre avec $\bar{V} = \bar{M}$. Alors il existe des réseaux $V_\tau \subset V$ pour $\tau \in T$ et des R-homomorphismes $\delta_{\tau,\sigma}: V_\tau \to V$ pour $\sigma \in T$, $\sigma > \tau$, tels que V_τ et $V_\tau\delta_{\tau,\sigma}$ sont des R-réseaux libres dont les générateurs sont indépendants modulo $V \cap \mathfrak{P}V$ et tels qu'on ait*

$$M = V + \sum_\tau Y_\tau$$

avec

$$\Theta_\tau(M) = \bar{V}_\tau \oplus \Theta_\tau(V + \sum_{\sigma<\tau} Y_\sigma)$$

et

$$Y_\tau = \{q_\tau v + \sum_{\sigma>\tau} q_\sigma v \delta_{\tau,\sigma},\ v \in V_\tau\}.$$

Nous avons encore besoin de quelques propiétés des V_τ et $\delta_{\tau,\sigma}$.

$$\textit{Si } \tau_1 \succ \tau_2 \succ \ldots, \textit{ la somme } V_{\tau_1} + V_{\tau_2} + \ldots \textit{ est directe.} \tag{8}$$

Remarquons d'abord que si X_1 et X_2 sont des R-réseaux libres dans V dont les générateurs sont indépendants modulo $V \cap \mathfrak{P}V$, la somme $X_1 + X_2$ est directe, si $\bar{X}_1 + \bar{X}_2$ est directe. Donc il suffit de montrer, que la somme $\bar{V}_{\tau_1} + \bar{V}_{\tau_2} + \ldots$ est directe. D'après

(6) on a pour $\sigma \prec \tau$, $\Theta_\tau(Y_\sigma) \supset \Theta_\sigma(Y_\sigma) = \bar{V}_\sigma$, ce qui entraîne $\sum_{i>l} \bar{V}_{\tau_i} \subset \Theta_{\tau_l}(\sum_{\sigma<\tau_l} Y_\sigma)$ pour chaque l. Donc on a $\bar{V}_{\tau_l} \cap \sum_{i>l} \bar{V}_{\tau_i} = 0$ et la somme $\bar{V}_{\tau_1} + \bar{V}_{\tau_2} + \dots$ est en effet directe.

Le réseau M est complètement déterminé par V, V_τ et $\delta_{\tau,\sigma}$. De l'autre coté, ni les V_τ ni les $\delta_{\tau,\sigma}$ ne sont uniquement déterminés par M. Par exemple, chaque générateur $v_{\tau,i}$ peut être remplacé par $v_{\tau,i} + u$, avec $u \in \mathfrak{P}V \cap V$. Si l'on modifie les $v_{\tau,i}$ de cette façon, on peut en effet obtenir que

$$\delta_{\tau,\sigma} = 0 \quad \text{si} \quad \tau \prec \sigma. \tag{9}$$

Car, si $\tau \prec \sigma$, on peut supposer $q_\sigma = xq_\tau$, avec $x \in R$ et on obtient

$$q_\tau v + \sum_{\mu > \tau} q_\mu v \delta_{\tau,\mu} = q_\tau(v + xv\delta_{\tau,\sigma}) + \sum_{\mu \neq \sigma} q_\mu v \delta_{\tau,\mu}.$$

Donc si l'on remplace les $v_{\tau,i}$ par $v_{\tau,i} + xv_{\tau,i}\delta_{\tau,\sigma}$, on a bien $\delta_{\tau,\sigma} = 0$.

Retournons maintenant aux ordres R satisfaisant aux conditions du théorème 1. Nous avons à montrer, que $n(R) < \infty$ pour chacun de ces ordres. Or, d'après le lemme 2, il suffit de montrer cela si R est minimal, c.-à-d. s'il n'y a pas dans R d'ordre $S \neq R$ qui satisfait aux conditions du théorème 1. On vérifie facilement, que ces ordres minimaux sont de l'un des trois types suivants :

I. $R_{\mathrm{I}} = \mathfrak{o}[r] + \mathfrak{P}^\eta$, avec $\nu(r) = 2$ et $\eta \equiv 0$ (2).
Ici on a $T = \{\tau \mid \tau \equiv 1 \ (2),\ 1 \leq \tau < \eta\}$; comme $\eta - 1$ est dans T, on a $\eta \equiv 0$ (2).

II. $R_{\mathrm{II}} = \mathfrak{o}[r, r']$, avec $\nu(r) = 3$ et $\nu(r') = 4$.
$\mathfrak{o}[r, r']$ contient $\mathfrak{P}^6$ qui est engendré comme R_{II}-module par (r^2, rr', r'^2). On a $F(R_{\mathrm{II}}) = \mathfrak{P}^6$ et

$$T_{\mathrm{II}} = \{1, 2, 5\}.$$

III. $R_{\mathrm{III}} = \mathfrak{o}[r, r']$ avec $\nu(r) = 3$ et $\nu(r') = 5$.
$\mathfrak{o}[r, r']$ contient $\mathfrak{P}^8$ qui est engendré comme R_{III}-module par (rr', r^3, r'^2). On a $F(R_{\mathrm{III}}) = \mathfrak{P}^8$ et

$$T_{\mathrm{III}} = \{1, 2, 4, 7\}.$$

Proposition 4. *Soit $R = \mathfrak{o}[r] + \mathfrak{P}^\eta$, avec $\nu(r) = 2$. Alors chaque R-réseau M indécomposable est isomorphe à un réseau contenu dans $\mathfrak{O}$, c.-à-d. $M \cong R$ ou $\cong R + \mathfrak{P}^\tau$, avec $\tau \in T$.*

Soient σ, τ deux éléments de T; alors pour cet ordre, $\sigma > \tau$ entraine toujours $\sigma \succ \tau$. Par conséquent, la somme $X = \sum_{\tau \in T} \bar{V}_\tau$ est directe. Choisissons des éléments $v_{\eta,i} \in V$ de façon que $\{\bar{v}_{\eta,i}\}$ est une base de $\bar{V}/X$ et posons $T' = T \cup \eta$. Alors on a $\bar{V} = \oplus \sum_{\tau \in T'} \bar{V}_\tau$ et cela implique $V = \oplus \sum_{\tau \in T'} V_\tau$. Si les générateurs $v_{\tau,i}$ sont convenablement choisis modulo $V \cap \mathfrak{P}V$, tous les $\delta_{\tau,\sigma}$ sont $= 0$. Alors on a $Y_\tau = q_\tau V_\tau$ et on obtient

$$M = \oplus \sum_{\tau \in T'} (V_\tau + q_\tau V_\tau)$$

et chaque facteur directe $(V_\tau + q_\tau V_\tau)$ est la somme directe de réseaux de la forme $Rv + Rq_\tau v \cong R + \mathfrak{P}^\tau$, ce qui achève la démonstration.

Pour les deux autres ordres, la situation est plus compliquée car $\sigma > \tau$ n'entraîne pas toujours $\sigma \succ \tau$. Désignons par $\varrho(M)$ le rang de $\mathfrak{O}M$ comme $\mathfrak{O}$-module (ceci est un change de notation comparé avec l'introduction) et par $\varrho(R)$ la valeur maximale de $\varrho(M)$ pour un R-réseau M indécomposable. Si $\varrho(M)=1$, M est trivialement indécomposable et isomorphe à un réseau contenu dans $\mathfrak{O}$.

PROPOSITION 5. *Pour l'ordre $R = \mathfrak{o}[r, r']$ avec $v(r)=3$ et $v(r')=4$ on a $\varrho(R)=2$; plus précisément, soit π une uniformisante de K, $\mathfrak{O}u_1 + \mathfrak{O}u_2$ un $\mathfrak{O}$-réseau libre de rang 2 et M un R-réseau indécomposable. Alors on a ou*

$\varrho(M)=1$ et M est isomorphe à R, $R+\pi R$ ou à $R+\mathfrak{P}^i$, avec $i \in T$, ou

$\varrho(M)=2$ et M est isomorphe à $L = Ru_1 + Ru_2 + R(\pi u_1 + \pi^2 u_2)$ ou à $L + R\pi^2 u_1$.

Pour cet ordre on a $T=\{1,2,5\}$ et $1 \prec 5$, $2 \prec 5$. Posons $\overline{W} = \overline{V}_1 + \overline{V}_2 + \overline{V}_1 \delta_{1,2}$; nous allons d'abord montrer que $\overline{W} \cap \overline{V}_5 = 0$. Soit $M_2 = V + Y_1 + Y_2$; d'après la construction des Y_τ, on a $\Theta_5(M_2) \cap \overline{V}_5 = 0$ et il suffit de montrer que $\overline{W} \subset \Theta_5(M_2)$. Soit $y_1 = q_1 v + q_2 v \delta_{1,2} + \ldots$ avec $v \in V_1$ et désignons par r_i un élément de R avec $v(r_i)=i$ pour $i \in v(J)$. Alors on a $r_4 y_1 \in M$ et $r_4 y_1 \equiv r_4 q_1 v$ $(\mathfrak{P}^6 M)$. Or, $\mathfrak{P}^6$ étant le conducteur de R, on a $\mathfrak{P}^6 M \subset M$, ce qui entraîne $r_4 q_1 v \in M$ et $\mathfrak{P}^3 V_1 \subset M$. De cela on obtient $r_3 y_1 \equiv r_3 q_2 v \delta_{1,2} (M)$, ce qui entraîne $\mathfrak{P}^3 V_1 \delta_{1,2} \subset M$. Comme aussi $\mathfrak{P}^3 V_2 \subset M$, on a bien $\overline{W} \subset \Theta_5(M_2)$, c.-à-d. $\overline{W} \cap \overline{V}_5 = 0$. Choisissons maintenant des éléments $v_{6,i} \in V$ de façon que $\{\bar{v}_{6,i}\}$ est une base de $\overline{V}/\overline{W} \oplus \overline{V}_5$ et posons $V_6 = \sum_i R v_{6,i}$. Alors on a

$$\overline{V} = (\overline{V}_1 + \overline{V}_2 + \overline{V}_1 \delta_{1,2}) \oplus \overline{V}_5 \oplus \overline{V}_6.$$

Nous allons montrer maintenant que, par un choix convenable de V_1 et Y_1 on peut obtenir que $(\overline{V}_1 + \overline{V}_2) \cap \overline{V}_1 \delta_{1,2} = 0$. Chaque générateur v de V_1 peut être remplacé par $v' = v + z$ avec $z \in M \cap \mathfrak{P}M$; comme $Y_1 \subset M \cap \mathfrak{P}M$, on peut prendre $z \in Y_1$, c.-à-d. $z = q_1 w + q_2 w \delta_{1,2} + \ldots$ avec $w \in V_1$. Alors on trouve $y_1 \equiv q_1 v' + q_2 (v \delta_{1,2} - w) + \ldots$ $(M \cap \mathfrak{P}^3 M)$. Cela montre qu'on peut faire varier $\overline{V}_1 \delta_{1,2}$ librement modulo $\overline{V}_1$. De plus, en remplaçant y_1 par $y_1 + y_2$ avec $y_2 \in Y_2$ on peut faire varier $\overline{V}_1 \delta_{1,2}$ librement modulo $\overline{V}_2$. Par conséquent on peut obtenir que $(\overline{V}_1 + \overline{V}_2) \cap \overline{V}_1 \delta_{1,2} = 0$.

Posons $\overline{V}_{1,2} = \overline{V}_1 \cap \overline{V}_2$ et $\overline{V}_1 = \overline{V}_{1,2} \oplus \overline{V}_{1,1}$, $\overline{V}_2 = \overline{V}_{1,2} \oplus \overline{V}_{2,2}$. Alors on a $\overline{W} = \overline{V}_{1,2} \oplus \overline{V}_{1,1} \oplus \overline{V}_{2,2} \oplus \overline{V}_1 \delta_{1,2}$ et en choisissant les générateurs des $\overline{V}_\tau$ en accord avec cette décomposition, on a

$$V = V_{1,2} \oplus V_{1,1} \oplus V_{2,2} \oplus V_1\delta_{1,2} \oplus V_5 \oplus V_6. \tag{10}$$

En changeant les générateurs de V_τ modulo $V \cap \mathfrak{P}V$ — ce qui n'affecte pas la décomposition ci-dessus — on peut d'après (9) obtenir que $\delta_{\tau,\sigma}=0$ pour $\sigma \succ \tau$. Comme $5 \succ 1$ et $5 \succ 2$ on peut donc supposer que $V_{1,1}\delta_{1,5} = V_2\delta_{2,5} = 0$. Soit $v \in V_{1,2}$ et $\bar{v} \neq 0$; alors on a $y_2 = q_2 v \in M$ et

$$y_1 = q_1 v + q_2 v\delta_{1,2} + q_5 v\delta_{1,5} \equiv q_1(v + r_4 z) + q_2 v\delta_{1,2} \ (\mathfrak{P}^6 V)$$

avec $z \in V$. Si l'on remplace v par $v' = v + r_4 z$ on a $v'\delta_{1,5} = 0$ et comme $q_2 v \equiv q_2 v'$ $(\mathfrak{P}^6 V)$ on a aussi $v'\delta_{2,5}=0$. Cela veut dire que la décomposition (10) peut se faire de façon que $\delta_{1,5} = \delta_{2,5} = 0$ et cela donne

$$M = ((V_1 \oplus V_1\delta_{1,2}) + Y_1) \oplus (V_{2,2} + q_2 V_{2,2}) \oplus (V_5 + q_5 V_5) \oplus V_6.$$

Maintenant il est facile de montrer la proposition 4. D'abord on vérifie qu'il n'y a pas d'autres réseaux avec $\varrho(M)=1$. Supposons donc M indécomposable et $\varrho(M)>1$; cela entraîne $V_{2,2} = V_5 = V_6 = 0$ car autrement M contiendrait un facteur directe isomorphe à $R + q_2 R$, $R + q_5 R$ ou R. Supposons que $V_{1,1} \neq 0$ et soit $v \in V_{1,1}$ avec $\bar{v} \neq 0$. Alors M contient l'élément $y_1 = q_1 v + q_2 v\delta_{1,2}$. Si $v\delta_{1,2}=0$, le réseau $Rv + Rq_1 v$ est facteur directe de M, contrairement à l'hypothèse $\varrho(M)>1$. Si $v\delta_{1,2} \neq 0$, le réseau $Rv + Rv\delta_{1,2} + Ry_1$ est facteur directe de M, donc égal à M, et il est isomorphe au réseau L ci-dessus. Si $V_{1,1}=0$ et $V_{1,2} \neq 0$ on trouve d'une façon analogue que M est isomorphe à $L + Rq_2 u_1$, ce qui achève la démonstration.

Proposition 6. *Pour l'ordre $R = \mathfrak{o}[r, r']$ avec $v(r)=3$ et $v(r')=5$ on a $\varrho(R)=4$; plus précisément, soit $\sum_1^4 \mathfrak{O}u_i$ un $\mathfrak{O}$-réseau libre de rang 4 et π une uniformisante de K. Alors un R-réseau M indécomposable est de l'un des types suivants :*

$\varrho(M)=1$ a) $R + \mathfrak{P}^\tau$, $\tau \in T$, $R + \pi^i R$, $i = 1, 2$ *ou* R, $\mathfrak{O}$.

$\varrho(M)=2$ b) $L_1 = Ru_1 + Ru_2 + R(\pi u_1 + \pi^2 u_2)$ *ou* $L_1 + R\pi^2 u_1$, $L_1 + R\pi^4 u_2$, $L_1 + R\pi^2 u_1 + R\pi^4 u_2$.

c) $L_2 = Ru_1 + Ru_2 + R(\pi^2 u_1 + \pi^4 u_2)$ *ou* $L_2 + R\pi^i u_1$, $i = 1, 4$.

$\varrho(M)=3$ d) $L_3 = \sum_1^3 Ru_i + R(\pi u_1 + \pi^2 u_2) + R(\pi^2 u_1 + \pi^4 u_3)$ *ou* $L_3 + R\pi^4 u_2$.

e) $L_4 = \sum_1^3 Ru_i + R(\pi u_1 + \pi^2 u_2) + R\pi^2 u_1 + R(\pi u_2 + \pi^2 u_3)$ *ou* $L_4 + R\pi^4 u_3$.

$\varrho(M)=4$ f) $L_5 = \sum_1^4 Ru_i + R(\pi u_1 + \pi^2 u_2) + R(\pi^2 u_1 + \pi^4 u_3) + R(\pi u_2 + \pi^2 u_4)$ *ou* $L_5 + R\pi^4 u_4$.

Ici on a $T = \{1, 2, 4, 7\}$ et $1 \prec 4 \prec 7$, $2 \prec 7$. Posons

$$\overline{W} = \overline{V}_1 + \overline{V}_2 + \overline{V}_1\delta_{1,2} + \overline{V}_2\delta_{2,4}$$

et choisissons des éléments $v_{8,i} \in V$ de façon que $\{\bar{v}_{8,i}\}$ et une base de $\overline{V}/\overline{W}+\overline{V}_4+\overline{V}_7$, et posons encore $\overline{V}_4'=\overline{V}_4 \cap \overline{W}$ et $\overline{V}_4=\overline{V}_4' \oplus \overline{V}_4''$. Nous allons montrer que

$$\overline{V}=\overline{W} \oplus \overline{V}_4'' \oplus \overline{V}_7 \oplus \overline{V}_8. \tag{11}$$

D'abord on vérifie d'une façon analogue que dans la démonstration de la proposition 5 que $\mathfrak{P}^3 V_1$, $\mathfrak{P}^5 V_2$, $\mathfrak{P}^5 V_1 \delta_{1,2}$ et $\mathfrak{P}^5 V_2 \delta_{2,4}$ sont tous dans $M_4 = V + Y_1 + Y_2 + Y_4$. Cela entraine que $\overline{W}+\overline{V}_4 \subset \Theta_7(M_4)$. D'après la construction des Y_τ, on a $\Theta_7(M_4) \cap \overline{V}_7=0$ et on voit, que la décomposition (11) est directe.

Posons comme ci-dessus $\overline{V}_{1,2}=\overline{V}_1 \cap \overline{V}_2$ et $\overline{V}_1=\overline{V}_{1,1} \oplus \overline{V}_{1,2}$ et $\overline{V}_2=\overline{V}_{2,2} \oplus \overline{V}_{1,2}$. Maintenant nous allons montrer, que, par un choix convenable des V_τ et Y_τ on peut obtenir que

$$\overline{W}=(\overline{V}_{1,1}+\overline{V}_{1,2}\delta_{1,2}) \oplus \overline{V}_2 \oplus \overline{V}_{1,1}\delta_{1,2} \oplus \overline{V}_2\delta_{2,4}$$

et

$$\overline{V}_4'=\overline{V}_4 \cap \overline{V}_{2,2} \oplus \overline{V}_4 \cap \overline{V}_{1,1}\,\delta_{1,2} \oplus \overline{V}_4 \cap \overline{V}_{1,2}\,\delta_{1,2}. \tag{12}$$

Considérons un élément $y_2=q_2v+q_4v\delta_{2,4}+\dots$ avec $v \in V_2$. On peut remplacer v par un élément $v' \in V$ tel que $v'-v \in M \cap \mathfrak{P}M$. Soit $w_1 \in V_1$ et $w_2 \in V_2$ et posons $v'=v+(q_1w_1+q_2\delta_{1,2}+\dots)+(q_2w_2+q_4w_2\delta_{2,4}+\dots)$. Comme $\mathfrak{P}^3w_1 \subset M$, on trouve que

$$y_2 \equiv q_2v'+q_4(v\delta_{2,4}-w_1\delta_{1,2}-w_2)+\dots\ (M).$$

Cela montre qu'on peut faire varier $\overline{V}_2\,\delta_{2,4}$ librement modulo $\overline{V}_1\,\delta_{1,2}+\overline{V}_2$. Comme $\mathfrak{P}^3 V_1 \subset M$, on peut également le faire varier librement modulo $\overline{V}_1$. Donc, par un choix convenable de V_2 on peut obtenir que

$$\overline{W}=(\overline{V}_1+\overline{V}_2+\overline{V}_1\,\delta_{1,2}) \oplus \overline{V}_2\delta_{2,4}.$$

Soit maintenant $v \in V_1$ et $y_1=q_1v+q_2v\delta_{1,2}+\dots \in Y_1$. Si l'on remplace y_1 par y_1+y_2, avec $y_2 \in Y_2$, on peut faire varier $\overline{V}_1\delta_{1,2}$ librement modulo V_2. Donc on peut obtenir que $\overline{W}=(\overline{V}_{1,1}+\overline{V}_1\delta_{1,2}) \oplus \overline{V}_2 \oplus \overline{V}_2\delta_{2,4}$. Choisissons maintenant les générateurs de V_1 et V_2 de façon que $V_1=V_{1,1} \oplus V_{1,2}$ et $V_2=V_{2,2} \oplus V_{1,2}$. Comme $V_{1,2} \subset V_2$, les générateurs de $V_{1,2}$ sont déjà fixés modulo $\mathfrak{P}^3M \cap M$, mais ceux de $V_{1,1}$ on peut encore faire varier modulo $M \cap \mathfrak{P}M$. Comme on l'a vu dans la démonstration de la proposition 5, cela fait varier $\overline{V}_{1,1}\delta_{1,2}$ librement modulo $\overline{V}_{1,1}$. Or, $\overline{V}_{1,1}$ étant définie comme un complément quelquonque de $\overline{V}_{1,2}=\overline{V}_1 \cap \overline{V}_2$, on peut le faire varier librement modulo $\overline{V}_{1,2}$ et cela fait varier $\overline{V}_{1,1}\delta_{1,2}$ librement modulo $\overline{V}_{1,2}\,\delta_{1,2}$. Donc on obtient enfin la décomposition (12) de $\overline{W}$.

Quant à la décomposition de $\overline{V}_4'$, on a d'abord $\overline{V}_1 \cap \overline{V}_4'=0$, car $1 \prec 4$. De plus, $\overline{V}_2\,\delta_{2,4}$ peut être varié librement modulo $\overline{V}_4$ et on peut donc supposer que

$$\overline{V}_4' \subset \overline{V}_{2,2}+\overline{V}_1\,\delta_{1,2}=\overline{V}_{2,2} \oplus \overline{V}_{1,1}\delta_{1,2} \oplus \overline{V}_{1,2}\,\delta_{1,2}.$$

Or, on a vu plus haut, que $\bar{V}_1\delta_{1,2}$ peut être varié librement modulo $\bar{V}_2$ et $\bar{V}_{1,1}\delta_{1,2}$ librement modulo $\bar{V}_{1,2}\delta_{1,2}$ et de cela on obtient la décomposition de $\bar{V}_4'$.

Si l'on choisit les générateurs des V_τ et Y_τ en accord aves les décompositions (11) et (12) on a la décomposition suivante de V

$$V = (V_{1,1} + V_{1,2}\delta_{1,2}) \oplus V_2 \oplus V_{1,1}\delta_{1,2} \oplus V_2\delta_{2,4} \oplus V_4'' \oplus V_7 \oplus V_8. \tag{13}$$

Nous allons montrer, que cette décomposition peut se faire de façon que tous les $\delta_{\tau,\sigma}$ sont $=0$, à l'exception de $\delta_{1,2}$ et $\delta_{2,4}$. Les générateurs de V_1 sont fixés modulo $M \cap \mathfrak{P}^3 M$ pour obtenir la décomposition (13). Or, d'après (9), il suffit de les changer modulo $V \cap \mathfrak{P} V \subset M \cap \mathfrak{P}^3 M$ pour obtenir que $\delta_{1,4} = \delta_{1,7} = 0$. Comme $V_1 \cap V_{2,2} = 0$, on peut également supposer que $V_{2,2}\delta_{2,7} = 0$. Supposons que $v\delta_{2,7} \neq 0$ pour $v \in V_{1,2}$, et $\bar{v} \neq 0$. Alors on a

$$y_2 = q_2 v + q_4 v\delta_{2,4} + q_7 v\delta_{2,7} \equiv q_2(v + r_5 z) + q_4 v\delta_{2,4} \quad (M)$$

avec $z \in V$. Si l'on remplace v par $v' = v + r_5 z$ on a $v'\delta_{2,7} = 0$ et

$$y_1 \equiv q_1 v' + q_2 v\delta_{1,2} + q_7 z' \equiv q_1(v' + r_6 z') + q_2 v\delta_{1,2} \quad (M)$$

avec $z' \in V$. Si l'on remplace v' par $v'' = v' + r_6 z'$ on a $v''\delta_{1,4} = v''\delta_{1,7} = 0$ et aussi $v''\delta_{2,7} = 0$ car y_2 est seulement changé modulo $\mathfrak{P}^3 M \subset M$ par cette substitution. Cela montre qu'on peut faire la décomposition $V_{1,2} \oplus V_{1,1} \oplus V_{2,2}$ de façon que $\delta_{1,4} = \delta_{1,7} = \delta_{2,7} = 0$.

Soit maintenant $\bar{X} = \bar{V}_{1,1} \cap \bar{V}_{1,2}\delta_{1,2}$ et choisissons des éléments $x_i \in V$ de façon que $\{\bar{x}_i\}$ est une base de $\bar{X}$ et soit $X = \sum_i R x_i$. Alors il existe des R-réseaux libres X_1 et X_2 tels que $V_{1,1} = X \oplus X_1$ et $V_{1,2}\delta_{1,2} = X \oplus X_2$. Par un calcul analogue à celui ci-dessus, on voit que cette décomposition peut se faire sans qu'un $\delta_{\tau,\sigma}$ autre que $\delta_{1,2}$ et $\delta_{2,4}$ soit $\neq 0$. Si les $V_{i,l}$ et les X_i sont ainsi choisis, la somme (13) est automatiquement directe.

Finalement on vérifie qu'on peut aussi obtenir que

$$V_4' = V_4 \cap V_{2,2} \oplus V_4 \cap V_{1,2}\delta_{1,2} \oplus V_4 \cap V_{1,1}\delta_{1,2} \tag{14}$$

sans affecter les relations $\delta_{\tau,\sigma} = 0$ pour $\delta_{\tau,\sigma} \neq \delta_{1,2}, \delta_{2,4}$.

Supposons maintenant que M est indécomposable avec $\varrho(M) > 1$. Cela entraîne $V_4'' = V_7 = V_8 = 0$, car autrement M contiendrait un facteur directe L avec $\varrho(L) = 1$, ce qui est une contradiction.

Soit donc $V = W$ et supposons que $V_{1,1} \not\subset V_{1,2}\delta_{1,2}$. Alors il existe $v \in V_{1,1}$ avec $\bar{v} \neq 0$ et $v \notin V_{1,2}\delta_{1,2}$. Si $v\delta_{1,2} = 0$, le réseau $Rv + R\pi v$ est facteur directe de M et on aurait $\varrho(M) = 1$. Donc, $v\delta_{1,2} \neq 0$ et le module $M \cap (\mathfrak{O}v + \mathfrak{O}v\delta_{1,2})$ est facteur directe de M, donc égal à M, et M est isomorphe à L_1 ou, si $v\delta_{1,2} \in V_4'$, à $L_1 + R\pi^4 u_2$.

Supposons maintenant que $V_{1,2}\delta_{1,2} \not\subset V_{1,1}$ et soit $v \in V_{1,2}$ avec $\bar{v} \neq 0$ et $v\delta_{1,2} \notin V_{1,1}$; cela implique $v\delta_{1,2} \neq 0$. Posons $I = (\mathfrak{O}v + \mathfrak{O}v\delta_{1,2} + \mathfrak{O}v\delta_{2,4}) \cap M$. Alors la décomposition (13) montre, que I est facteur directe de M, donc égal à M. Si $v\delta_{2,4} \neq 0$, M est isomorphe à l'un des modules d), suivant que $v\delta_{1,2}$ est dans V_4' ou non. Si $v\delta_{2,4} = 0$, M est isomorphe à $L_1 + R\pi^2 u_1$ ou à $L_1 + R\pi^2 u_1 + R\pi^4 u_2$ suivant que $v\delta_{1,2}$ est dans V_4' ou non.

Soit donc $V_{1,1} = V_{1,2}\delta_{1,2}$ et $v \in V_{1,1}$ avec $\bar{v} \neq 0$. Alors il existe $w \in V_{1,2}$ tel que $w\delta_{1,2} = v$, et on obtient de (13) que $(\mathfrak{O}v + \mathfrak{O}v\delta_{1,2} + \mathfrak{O}w + \mathfrak{O}w\delta_{2,4}) \cap M$ est facteur directe de M donc égal à M. Si $w\delta_{2,4} \neq 0$, M est isomorphe à l'un des réseaux f) et si $w\delta_{2,4} = 0$, M est isomorphe à l'un des réseaux e).

Supposons donc $V_{1,1} = V_{1,2}\delta_{1,2} = 0$ et soit $v \in V_{1,2}$ avec $\bar{v} \neq 0$. Comme $v\delta_{1,2} = 0$, le module $(\mathfrak{O}v + \mathfrak{O}v\delta_{2,4}) \cap M$ est facteur directe de M, et on voit que M est isomorphe à $L_2 + R\pi u_1$.

Supposons enfin qu'on a aussi $V_{1,2} = 0$ et soit $v \in V_{2,2}$ avec $\bar{v} \neq 0$. Alors $\varrho(M) > 1$ entraîne $v\delta_{2,4} \neq 0$ et M est isomorphe à $L_2 + R\pi^4 u_1$ ou à L_2, suivant que v est dans V_4' ou non. Ceci achève la démonstration de la proposition 6 et aussi du théorème 1, car si de plus $V_{2,2} = 0$ on a $W = 0$ et $M = 0$. — On peut encore vérifier, que les réseaux a)–f) sont en effet indécomposables et non-isomorphes. Cette vérification ne présente pas de difficultés et nous n'insistons pas là-dessus.

Ordres dans une algébre commutative et semi-simple

Nous allons montrer le théorème suivant :

Théorème 2. *Soit k le complété $\mathfrak{p}$-adique d'un corps de nombres algébriques, K_i/k des extensions totalement ramifiées de degré fini, $K = \oplus \sum_1^s K_i$ avec $s > 1$, et soit R un $\mathfrak{o}$-ordre indécomposable de K. Alors $n(R)$ est fini si et seulement si R satisfait à l'une ou l'autre des conditions suivantes :*

a) *$s \leqslant 3$ et pour au moins deux des $\mathfrak{P}_i$ on a $J(R) + \mathfrak{P}_i = \mathfrak{P}$.*

b) *$s = 2$ et il existe un $\mathfrak{P}_i$ tel que $J(R) + \mathfrak{P}_i = \mathfrak{P}$ et tel que $\mathfrak{O}_i J(R) = \mathfrak{P}_i^2$ et $\mathfrak{O}_i \cap J(R) \not\subset \mathfrak{P}_i^4$.*

La nécessité de ces conditions se déduit facilement de la proposition 2. Nous avons déjà montré, que $n(R) < \infty$ implique $s \leqslant 3$ et pour $s = 3$ la condition a) est nécessaire d'après le corollaire 2. Soit donc $s = 2$; alors, d'après le corollaire 2, on a $J(R) + \mathfrak{P}_i = \mathfrak{P}$ pour au moins un i. Supposons p. ex. $J(R) + \mathfrak{P}_1 = \mathfrak{P}$. Or, $\mathfrak{P}$ contient une uniformisante π_2 de K_2 et R contient donc un élément $r = x + \pi_2$ avec $x \in \mathfrak{P}_1$. Cela implique que $\mathfrak{P}_2 \subset \mathfrak{O}J(R)$ et on obtient que $\mathfrak{O}J(R) = \mathfrak{P}^\alpha + \mathfrak{P}_2$. Si $\alpha = 1$, R contient un élément $\pi_1 + y$ avec $y \in \mathfrak{P}_2$ et on a aussi $J(R)+\mathfrak{P}_2=\mathfrak{P}$, c.-à-d. R satisfait à la condition a). Supposons donc que $\alpha>1$. D'après le corollaire 1, $n(R)<\infty$ implique $\alpha=2$, c.-à-d. on a $\mathfrak{O}_1 J(R)=\mathfrak{P}_1^2$. Donc il reste à montrer que $U=J(R)\cap\mathfrak{P}_1$ n'est pas contenu dans $\mathfrak{P}_1^4$. Or on a vu que R contient un élément $r=x+\pi_2$ et on a $R=\mathfrak{o}[r]+U$. Supposons maintenant que U est contenu dans $\mathfrak{P}_1^4$ et désignons par ν_i la valuation normée de K_i. Alors la relation $\mathfrak{O}_1 R=\mathfrak{P}_1^2$ entraîne $\nu_1(x)=2$. De plus R est contenu dans l'ordre $S=\mathfrak{o}[r]+\mathfrak{P}_1^4$ et il suffit de montrer que $n(S)=\infty$. Avec les notations de la proposition 2 on a $S_1=\mathfrak{o}1+\mathfrak{P}_1^2+\mathfrak{P}_2$ et $\bar{J}_1=\mathfrak{o}\pi_1^2+\mathfrak{o}\pi_1^3/\mathfrak{P}_1^4$ ce qui donne dim $\bar{J}_1/\bar{J}_1^2=2$. Donc on a $n(S)=\infty$ ce qui démontre la nécessité de la condition $U\not\subset\mathfrak{P}_1^4$.

Pour montrer que les conditions du théorème 2 sont aussi suffisantes, il suffit de montrer que $n(R)$ est fini si R est un ordre minimal satisfaisant à ces conditions. Ces ordres minimaux sont de l'un des trois types suivants :

I. $R=\mathfrak{o}[r,r']+\mathfrak{P}_1^\eta$, $s=3$
avec $r=\pi_1+\pi_2$, $r'=\omega+\pi_3$, $\omega\in\mathfrak{P}_1$ et $\nu_1(\omega)=\eta-1$ ou $\omega=0$.

II. $R=\mathfrak{o}[r,q]+\mathfrak{P}_1^\eta$, $s=2$
avec $r=\omega+\pi_2$, $\omega\in\mathfrak{P}_1$, $\omega=0$ ou $\nu_1(\omega)=\eta-1$, $q\in P_1$ et $\nu_1(q)=2$.

III. $R=\mathfrak{o}[r,q]+\mathfrak{P}_1^5+\mathfrak{P}_2^3$, $s=2$
avec $r=\omega+\pi_2$, $\omega\in\mathfrak{P}_1$ et $\nu_1(\omega)=2$, $q\in\mathfrak{P}_1$ et $\nu_1(q)=3$.

Ici on suppose les K_i numerotés de façon que $J(R)+\mathfrak{P}_i=\mathfrak{P}$ pour $i<s$. Soit R un ordre satisfaisant aux conditions du théorème; nous allons montrer, qu'il contient l'un de ces trois ordres. Pour $s=3$, R satisfait nécessairement à la condition a). Alors $J(R)+\mathfrak{P}_1=\mathfrak{P}$ entraîne que R contient des éléments $r=x_1+\pi_2$ et $r'=x_2+\pi_3$ avec x_1, $x_2\in\mathfrak{P}_1$. Alors la relation $J(R)+\mathfrak{P}_2=\mathfrak{P}$ entraîne que x_1 est ou une uniformisante $=\pi_1$ ou que $\pi_1\in R$. Dans le deuxième cas on peut remplacer r par $r+\pi_1$ et on voit que R contient un ordre de la forme I. Il reste à vérifier que $\nu_1(\omega)=\eta-1$ ou $\omega=0$. Pour $n\geqslant 1$ on a $r^n r'=\pi_1^n x_2\in R$, ce qui implique $\mathfrak{P}_1 x_2\subset R$, c.-à-d. $\nu_1(x_2)\geqslant\eta-1$. Si $\nu_1(x_2)>\eta-1$, on a $x_2\in\mathfrak{P}_1^\eta\subset R$, et donc aussi $\pi_3\in R$.

Soit donc $s=2$. Si R satisfait à la condition a), on voit que R contient l'ordre $(e_1+e_2)R_{\mathrm{I}}=\mathfrak{o}[r]+\mathfrak{P}_1^\eta$. Or, on a $R_{\mathrm{I}}\subset(e_1+e_2)R_{\mathrm{I}}\oplus e_3 R_{\mathrm{I}}$ et $n(R_{\mathrm{I}})<\infty$ implique $n((e_1+e_2)R_{\mathrm{I}})<\infty$, c.-à-d. on n'a pas besoin d'étudier l'ordre $(e_1+e_2)R_{\mathrm{I}}$.

Supposons donc que R satisfait à la condition b). Alors on a $\mathfrak{O}_1 R=\mathfrak{P}_1^2\supset U$ et $U\not\subset P_1^4$, c.-à-d. $\mathfrak{O}_1 U$ est égal à $\mathfrak{P}_1^2$ ou à $\mathfrak{P}_1^3$. Dans le premier cas la relation $J(R)+\mathfrak{P}_1=\mathfrak{P}$ entraîne que R contient un ordre du type II. Dans le deuxième cas, soit $q\in R\cap\mathfrak{P}_1$ avec $\nu_1(q)=3$. La relation $R+\mathfrak{P}_1=\mathfrak{P}$ entraîne que R contient un élément $r=\omega+\pi_2$ avec $\omega\in\mathfrak{P}_1$, et $\mathfrak{O}_1 R=\mathfrak{P}_1^2$

entraîne $\nu_1(\omega)=2$. Par conséquent, R contient un ordre du type III. On vérifie que cet ordre contient $\mathfrak{P}_1^5+\mathfrak{P}_2^3$, qui est le conducteur de R_{III}.

Soit R un quelquonque de ces trois ordres et soit $S=\mathfrak{o}1+\mathfrak{P}$ l'ordre indécomposable maximal de K. Alors $n(S)<\infty$ est une condition nécessaire pour que $n(R)<\infty$. Nous allons d'abord montrer que $n(S)$ est en effet fini et en même temps nous allons déterminer les types de S-réseaux indécomposables.

Soit $\varrho_i(M)$, $i=1, ..., s$, le rang de $\mathfrak{O}_i M$ comme $\mathfrak{O}_i$-réseau et $\varrho_i(R)$ la valeur maximale de $\varrho_i(M)$ pour un R-réseau indécomposable. Posons encore $\varrho(M)=\max_i\varrho_i(M)$ et $\varrho(R)=\max_i\varrho_i(R)$; alors $\varrho(R)$ est fini si et seulement si $n(R)$ est fini.

Proposition 7. *Soit $S=\mathfrak{o}1+\mathfrak{P}$ l'ordre indécomposable maximal de $K=\oplus\sum_1^s K_i$ avec $s=2, 3$. Alors $\varrho(S)=1$; plus précisément, un S-réseau indécomposable est ou cyclique ou, pour $s=3$, isomorphe au réseau $S(e_1+e_3)+S(e_2+e_3)$ contenu dans $\mathfrak{O}$.*

Soit M un S-réseau, $N=\mathfrak{O}M$ et $\varphi: N\to N/\mathfrak{P}N=\bar N$. Une décomposition $M=M_1\oplus M_2$ entraîne une décomposition $N=\mathfrak{O}M_1\oplus\mathfrak{O}M_2$ et aussi une décomposition simultanée

$$\bar M=X_1\oplus X_2,\quad X_i=\bar M_i,$$
$$\bar N=Y_1\oplus Y_2\quad \text{avec } Y_i=\mathfrak{O}X_i.$$

Inversément, une telle décomposition simultanée de $\bar M$ et $\bar N$ entraîne une décomposition de M. Car d'abord il existe une décomposition $N=N_1\oplus N_2$ avec $\bar N_i=Y_i$. Posons $M_i=M\cap N_i$ et $V=M_1\oplus M_2$. Alors on a $\bar M_i=X_i$ et $\bar V=\bar M$. Cela entraîne $\mathfrak{O}V=\mathfrak{O}M$. Par conséquent, $\mathfrak{P}M=\mathfrak{P}V$ est contenu dans V et M est $=V$. Au lieu de considérer les décompositions de M, on peut donc considérer les décompositions simultanées de $\bar M$ et $\bar N$.

Deux S-réseaux cycliques Sx et Sx' sont isomorphes si et seulement si e_ix et e_ix' sont $=0$ en même temps. Posons $\tau_i(x)=1$ si $e_ix\neq 0$ et $\tau_i(x)=0$ ailleurs, et soit $\tau(x)=(\tau_1(x), ..., \tau_s(x))$. Alors Sx est isomorphe à Sx' si et seulement si $\tau(x)=\tau(x')$.

Soit maintenant M un S-réseau indécomposable. Pour $x\in\bar N$ posons $\lambda(x)=\sum\tau_i(x)$ et soit $\bar M_\mu$ le $\bar{\mathfrak{o}}$-espace engendré par les $x\in\bar M$ avec $\lambda(x)\leqslant\mu$. Si x est un élément quelquonque de $\bar N$, il existe une décomposition $N=\mathfrak{O}x\oplus N'$. Supposons que $x\in\bar M$ et $\lambda(x)=1$. Alors il existe un e_i tel que $e_ix=x$ et on a $\mathfrak{O}x=\mathfrak{O}_ix=Sx\subset\bar M$. Donc on obtient une décomposition $\bar M=\mathfrak{O}x\oplus\bar M'$ avec $\mathfrak{O}\bar M'=\bar N'$. Comme M est indécomposable, cela entraîne $\bar M=\mathfrak{O}x$ et $M\cong\mathfrak{O}_i$.

Supposons donc que $\bar M_1=0$ et posons

$$\bar M=\bar M_{s-1}\oplus X$$

où X est un complément quelquonque de $\bar M_{s-1}$. Nous allons montrer, que la somme $\mathfrak{O}\bar M_{s-1}+$

$\mathfrak{O}X$ est directe. Si par exemple, $\mathfrak{O}_1\bar{M}_{s-1} \cap \mathfrak{O}_1 X \neq 0$, il existe $x \in X$ et $m \in \bar{M}_{s-1}$ avec $e_1 x = e_1 m$, c.-à-d. $\lambda(x-m) < s$. Donc $x-m$ est dans $\bar{M}_{s-1}$ et cela implique $x=0$. La décomposition ci-dessus entraîne donc une décomposition simultanée de $\bar{M}$ et $\bar{N}$. Si $X \neq 0$, soit $\{x_j\}$ une base de X. Alors $\bar{M}_{s-1}=0$ entraîne que la somme $\sum \mathfrak{O}x_j$ est directe et on voit que $\bar{M}=\mathfrak{o}x$ et $M \cong S$.

Il reste à considérer le cas $\bar{M}_1=0$ et $\bar{M}_{s-1}=\bar{M}$, c.-à-d. $s=3$ et $\bar{M}=\bar{M}_2$. Alors il existe une base $\{\bar{m}_j\}$ de $\bar{M}$ telle que $\lambda(\bar{m}_j)=2$ pour $j=1, \ldots$. Cela veut dire que chaque $\bar{m}_j$ est annihilé par exactement un des e_i et on obtient une décomposition

$$\bar{M} = W_1 \oplus W_2 \oplus W_3 \quad \text{avec} \quad e_i W_i = 0.$$

Les W_i ne sont pas uniquement déterminés par $\bar{M}$; supposons que W_3 est minimal dans la décomposition ci-dessus. Alors la somme $\mathfrak{O}(W_1+W_2)+\mathfrak{O}W_3$ est directe. Car si par exemple $\mathfrak{O}_1(W_1+W_2) \cap \mathfrak{O}_1 W_3 \neq 0$, il existe $y_2 \in W_2$ et $y_3 \in W_3$ tels que $e_1 y_2 = e_1 y_3$. Si l'on pose $y=y_2-y_3$ et $W_1' = W_1 + \mathfrak{o}y$ on obtient $\bar{M}=W_1' \oplus W_2 \oplus W_3'$ et W_3' est strictement contenu dans W_3 ce qui est impossible. Donc on obtient une décomposition simultanée de $\bar{N}$ et $\bar{M}$. Si $W_3 \neq 0$ on a $\bar{M}=W_3$ et on voit que M est isomorphe à $S(e_1+e_2)$.

Soit donc $\bar{M}=W_1 \oplus W_2$ et $0 \neq x \in W_1$. Posons $W_1 = \mathfrak{o}x \oplus W_1'$ et $Y = W_1' \oplus W_2$. Si $\mathfrak{O}x \cap \mathfrak{O}Y = 0$, on a $\bar{M}=\mathfrak{o}x$ et M est isomorphe à $S(e_2+e_3)$. Si $\mathfrak{O}x \cap \mathfrak{O}Y \neq 0$, il existe $x' \in W_2$ avec $e_3 x = e_3 x'$. Alors on pose $M = \mathfrak{o}x + \mathfrak{o}x' + Y' = X \oplus Y'$ et maintenant $\bar{M}_1=0$ entraîne que la somme $\mathfrak{O}X + \mathfrak{O}Y'$ est directe. Donc on a $\bar{M}=X$ et M est isomorphe à $S(e_1+e_3)+S(e_2+e_3)$. Si finalement aussi $W_1=0$, on a $\bar{M}=W_2$ et on voit, que M est isomorphe à $S(e_1+e_3)$, ce qui achève la démonstration.

Revenons maintenant aux ordres R qui satisfont aux conditions du théorème 2. Rappelons qu'on suppose les K_i numerotés de façon que $J(R)+\mathfrak{P}_i=\mathfrak{P}$ pour $i<s$.

Lemme 6. *Soit R un $\mathfrak{o}$-ordre satisfaisant aux conditions du théorème 2, M un R-réseau, S l'ordre $\mathfrak{o}1+\mathfrak{P}$ et L un S-réseau indécomposable, facteur directe de SM. Si M est indécomposable avec $\varrho(M)>1$, L est de l'un des deux types suivants :*

1) *$L=Sa$, avec $e_i a \neq 0$ pour $i<s$.*
2) *$L=Sx$, avec $e_s x = x$, et $x \notin M$.*

De plus, il existe une décomposition de SM en réseaux indécomposables telle que $a \in M$ pour chaque composante de type 1).

Supposons d'abord que L est cyclique, $L=Sy$ avec $e_i y \neq 0$ pour un $i<s$. Alors on a aussi $e_i \bar{y} \neq 0$, car $\mathfrak{O}y$ est facteur directe de $\mathfrak{O}M$. Comme $R+P_i=S$, il existe $m \in M$ et

$z \in \mathfrak{P}_i M$ avec $y = m + z$. Alors $\tau(y) = \tau(m)$ et $\tau(\bar{y}) = \tau(\bar{m})$ et il existe un isomorphisme $Sy \to Sm$ qui se prolonge en un automorphisme de SM. Donc on peut supposer que $L = Sm$ et nous avons à démontrer que $e_j m \neq 0$ pour $j < s$. Si $e_j m = 0$, on a $Sm = (R + \mathfrak{P}_j)m = Rm \subset M$. Or Rm est un facteur directe de SM, donc il est aussi facteur directe de M, et on aurait $M = Rm$, contrairement à l'hypothèse $\varrho(M) > 1$.

Si L n'est pas cyclique, on a $L = Sy_1 + Sy_2$ avec $e_1 y_1 \neq 0$ et $e_2 y_2 \neq 0$ et comme ci-dessus on peut supposer $L = Sm_1 + Sm_2$ avec m_1, $m_2 \in M$. Or, on a aussi $e_2 m_1 = e_1 m_2 = 0$, ce qui entraîne $L = Rm_1 + Rm_2 \subset M$. Donc L serait facteur directe de M, contrairement à l'hypothèse $\varrho(M) > 1$.

Alors il reste à considérer le cas $L = Sy$ avec $e_i y = 0$ pour $i < s$, c.-à-d. $y = e_s y$. Si y était dans M, on aurait $Sy = (R + \mathfrak{P}_1) = Ry \subset M$, ce qui est impossible.

Supposons tojours que M est indécomposable avec $\varrho(M) > 1$. Soit

$$SM = \sum Sa_i \oplus \sum Sx_i, \quad \text{avec} \quad a_i \in M,$$

et posons $A = \oplus \sum Ra_i$. Les éléments a_i sont encore de deux espèces différentes suivant que $e_s a_i = 0$ ou non; posons $A_0 = \sum_{e_s a_i = 0} Ra_i$. Pour les composantes du type 2), on a $x_i \notin M$ mais $x_i \in SM = (R + \mathfrak{P}_1)M$. Donc il existe des $u_i \in \mathfrak{P}_1 M$ tels que $u_i + x_i \in M$. Alors $M_1 = A + \sum R(u_i + x_i)$ est dans M et on a $SM = SM_1 = M_1 + \mathfrak{P}_1 M_1$. Donc il existe un R-réseau $Y \subset \mathfrak{P}_1 M_1 \cap M$ tel que

$$M = A + \sum R(u_i + x_i) + Y. \tag{15}$$

Remarquons, que les u_i ne sont pas uniquement déterminés par les x_i; ils peuvent être variés librement modulo $M \cap \mathfrak{P}_1 M$. Posons $U = \sum \mathfrak{o} u_i$ et $X = \sum \mathfrak{o} x_i$. Alors l'application $\sigma : x_i \to u_i$ induit un $\mathfrak{o}$-homomorphisme surjectif $X \to U$. Or σ est un isomorphisme, car autrement on pourrait choisir les x_i de façon que $x_1 \sigma = 0$, c.-à-d. on aurait $x_1 \in M$ et Sx_1 serait facteur directe de SM, ce qui est impossible d'après le lemme 6.

Supposons maintenant qu'il existe des $e_1 R$-réseaux B, C tels que

$$e_1 A = B \oplus C$$

et

$$e_1 A_0 = B_0 \oplus C_0 \text{ avec } B_0 \subset B \text{ et } C_0 \subset C.$$

Alors on obtient une décomposition $A = A' \oplus A''$ de A en posant $A' = \{a \in A,\ e_1 a \in B\}$ et $A'' = \{a \in A,\ e_1 a \in C\}$. Supposons que la décomposition $e_1 A = B \oplus C$ entraîne une décomposition simultanée de Y et de $Y + U$, c.-à-d.

$$Y = Y \cap \mathfrak{O}_1 B \oplus Y \cap \mathfrak{O}_1 C$$

et

$$Y + U = (Y + U) \cap \mathfrak{O}_1 B \oplus (Y + U) \cap \mathfrak{O}_1 C. \tag{16}$$

Alors on obtient de (15) une décomposition directe de M en posant $M' = M \cap \mathfrak{O}A'$ et $M'' = M \cap \mathfrak{O}A''$. Or, M étant indécomposable, cela entraîne $B=0$ ou $C=0$. Nous allons utiliser cela pour montrer la

PROPOSITION 8. *Soit R un $\mathfrak{o}$-ordre satisfaisant aux conditions du théorème 2. Alors on a $\varrho(R) \leqslant 3$; plus précisément, pour les ordres R_{I} et R_{II} on a $\varrho_i(R)=1$ pour $i<s$ et $\varrho_s(R)=2$, tandis que pour R_{III} on a $\varrho_1(R)=2$ et $\varrho_2(R)=3$.*

Considérons d'abord l'ordre I, $R = \mathfrak{o}[r, r'] + \mathfrak{P}_1^{\eta_1}$ avec $r = \pi_1 e_1 + \pi_2 e_2$, $r' = \omega e_1 + \pi_3 e_3$, $\omega \in \mathfrak{P}_1$. Ici $e_1 R = \mathfrak{O}_1$ et Y est un $\mathfrak{O}_1$-réseau. Pour chaque élément u de U il existe $x = u\sigma^{-1} \in \mathfrak{O}_3 M$ tel que $u + x = m$ est dans M. Alors $rm = \pi_1 u$ est aussi dans M, ce qui entraîne $\mathfrak{P}_1 U \subset Y$. Par conséquent, $U + Y$ est aussi un $\mathfrak{O}_1$-réseau. Nous allons montrer de plus, que $\mathfrak{P}_1 U$ est facteur directe de Y, c.-à-d. que $\mathfrak{P}_1 U$ est un sous-réseau primitif de Y. Sinon on peut choisir les générateurs de U de façon que $u_1 \in Y$. Or, chaque u_i peut être librement varié modulo Y, et on peut donc obtenir que $u_1 = 0$. Ceci est une contradiction, car on a montré que l'application $\sigma : x_i \to u_i$ est un isomorphisme.

D'après la théorie des diviseurs élémentaires, il existe une base de $e_1 A$ telle que

$$e_1 A = \oplus \sum \mathfrak{O}_1 a_i,$$
$$Y = \oplus \sum \mathfrak{P}_1^{\alpha_i} a_i, \quad \alpha_{i+1} \geqslant \alpha_i.$$

Posons $\alpha = \max_i \alpha_i$ et $C = \sum_{\alpha_i = \alpha} \mathfrak{O}_1 a_i$. Alors on obtient une décomposition

$$e_1 A = B \oplus C,$$
$$Y = B' \oplus \mathfrak{P}_1^{\alpha} C \quad \text{avec} \quad B' \subset B, \ \mathfrak{P}_1^{\alpha-1} B \subset B'.$$

Soit $\varphi : e_1 A \to e_1 A / \mathfrak{P}_1 A = \overline{e_1 A}$ et $\psi : e_1 A \to \overline{e_1 A}/\bar{B}$. Alors on voit que $\bar{B}$ est uniquement déterminé par Y; si l'on choisit des éléments $c_i \in e_1 A$ de façon que $\{\psi(c_i)\}$ est une base de $\overline{e_1 A}/\bar{B}$, on a aussi $e_1 A = B \oplus \sum \mathfrak{O}_1 c_i$ et $Y = B' \oplus \sum \mathfrak{P}_1^{\alpha} c_i$.

Posons maintenant $U' = K_1 U \cap e_1 A$ et $\bar{C}_1 = \psi(A_0 \cap U')$, et soit a un élément de A_0 avec $0 \neq \psi(e_1 a) \in \bar{C}_1$. Alors il existe $b \in B$ tel que $\mathfrak{P}_1^{\alpha-1}(e_1 a + b)$ est dans $Y + U$. Or on a $\mathfrak{P}_1^{\alpha-1} b \subset B' \subset Y$, c.-à-d. $\mathfrak{P}_1^{\alpha-1} a$ est dans $Y + U$. Si l'on choisit des éléments $a_i \in A_0$ de façon que $\{\psi(e_1 a_i)\}$ est une base de $\bar{C}_1$, on voit donc que $\sum \mathfrak{P}_1^{\alpha-1} a_i$ est facteur directe de $Y + U$ et $\sum \mathfrak{P}_1^{\alpha} a_i$ facteur directe de Y. Posons

$$\psi(e_1 A_0) = \bar{C}_1 \oplus \bar{C}_2, \quad \psi(U') = \bar{C}_1 \oplus \bar{C}_3, \quad \psi(e_1 A) = \bar{C}_1 \oplus \bar{C}_2 \oplus \bar{C}_3 \oplus \bar{C}_4.$$

Si l'on choisit une base de C en accord avec cette décomposition, on a

$$e_1 A = B \oplus C_1 \oplus C_2 \oplus C_3 \oplus C_4$$

et cette décomposition entraîne une décomposition simultanée de e_1A_0, $Y+U$ et Y. Par conséquent on a $B=0$ et e_1A est égal à l'un des C_i. D'après la construction des C_i on a alors ou $A_0=0$ ou $e_1A_0=e_1A$ et aussi ou $Y=\mathfrak{P}_1U$ ou $Y=Y+U$. Donc, chaque décomposition simultanée de e_1A et Y satisfait aux conditions (16). Si l'on choisit une base de e_1A de façon que $e_1A=\sum \mathfrak{O}_1a_i$ et $Y=\sum \mathfrak{P}_1^{\alpha_i}a_i$ on voit que e_1A est de rang 1, c.-à-d. $A=Ra$ et $\varrho_1(R)=\varrho_2(R)=1$. Le rang de U est $\leqslant 1$, parce que $U\subset \mathfrak{P}_1A$, ce qui donne $\varrho_3(R)\leqslant 2$. Pour $M=Ra+R(u+x)$ avec $\tau(a)=(1,1,1)$ on a $\varrho_3(M)=2$, ce qui entraîne $\varrho_3(R)=2$.

Considérons maintenant l'ordre II, $R=\mathfrak{o}[r,q]+\mathfrak{P}_1^\eta$, $r=\omega e_1+\pi_2e_2$ avec ω, $q\in\mathfrak{P}_1$ et $\nu_1(q)=2$. Posons $Q=\mathfrak{o}e_1+R\cap\mathfrak{P}_1$; c'est un ordre dans K_1 dont on a déterminé les réseaux indécomposables dans la proposition 4. Alors $Z=e_1A+Y$ est un Q-réseau et e_1A est un Q-réseau libre avec $\overline{e_1A}=\bar{Z}$. D'après la proposition 4 il existe donc une décomposition

$$e_1A=V_1\oplus V_3\oplus\ldots\oplus V_{\eta-1}\oplus V_\eta$$

telle que Z est la somme directe des réseaux $V_\tau+\mathfrak{P}_1^\tau V_\tau$. Alors on peut poser

$$Y=\mathfrak{P}_1V_1\oplus\mathfrak{P}_1^3V_3\oplus\ldots\oplus\mathfrak{P}_1^\eta V_\eta.$$

Soit σ l'indice maximal avec $V_\sigma\neq 0$ et posons $B=\sum_{\tau<\sigma}V_\tau$. Alors on a

$$e_1A=B\oplus V_\sigma,$$
$$Y=B'\oplus\mathfrak{P}_1^\sigma V_\sigma \quad\text{et}\quad B'\subset B,\ \mathfrak{P}_1^{\sigma-1}B\subset B'.$$

Posons $\psi:\mathfrak{O}_1A\to\overline{e_1A}/\bar{B}$ et soient c_i des éléments de e_1A tels que $\{\psi(c_i)\}$ est une base de $\psi(e_1A)$ et posons $C=\sum Qc_i$. Alors on a aussi

$$e_1A=B\oplus C,$$
$$Y=B'\oplus\mathfrak{P}_1^\sigma C \quad\text{avec}\quad B'\subset B,\ \mathfrak{P}_1^{\sigma-1}B\subset B'.$$

Comme U est contenu dans $\mathfrak{P}_1A$, un générateur quelquonque se met sous la forme $u=e_1a'+\pi_1^\tau e_1a$ avec $\tau\equiv 1$ (2) et $e_1a\in e_1A$, $e_1a'\in\mathfrak{P}_1A\cap A$. Or on peut varier u librement modulo $\mathfrak{P}_1A\cap A$, c.-à-d. on peut supposer $u=\pi_1^\tau e_1a$. Alors $m=u+x\in M$ avec $x\in e_2M$ et on a $qm=q\pi_1^\tau e_1a\in M$. Or q^le_1a est aussi dans M pour $l\geqslant 1$ et on obtient donc que $\mathfrak{P}_1U\subset Y$. La situation est maintenant tout à fait la même que pour l'ordre R_{I} ci-dessus. Par un argument analogue on trouve que $A=Ra$ et $\varrho_1(R)=1$ et $\varrho_2(R)=2$.

Considérons enfin l'ordre III, $R=\mathfrak{o}[r,q]+\mathfrak{P}_1^5+\mathfrak{P}_2^3$, $r=\omega e_1+\pi_2e_2$ et $\omega,q\in\mathfrak{P}_1$ avec $\nu_1(\omega)=2$, $\nu_1(q)=3$. Soit Q l'ordre $e_1\mathfrak{o}+R\cap\mathfrak{P}_1=\mathfrak{o}e_1+\mathfrak{o}q+\mathfrak{P}_1^5$; c'est un ordre dans K_1 avec $n(Q)<\infty$ d'après la proposition 6. Alors

$$Z=\sum Qe_1a_i+Y$$

est un Q-réseau et chaque décomposition $Z=Z_1 \oplus Z_2$ entraîne une décomposition simultanée de $e_1 A$ et Y.

Reprenons maintenant les notations de la proposition 6. Il faut d'abord choisir un Q-réseau libre V avec $\bar{V}=\bar{Z}$; choisissons $V=\sum Qe_1 a_i$. Alors il existe une décomposition

$$V = W \oplus V_4'' \oplus V_7 \oplus V_8, \tag{17}$$

qui entraîne une décomposition correspondante de Z. Ici on a $V_8=0$, parce que $\mathfrak{P}_1^5 Z \subset Z$. Nous allons d'abord montrer, que cette décomposition entraîne aussi une décomposition de $e_1 A_0$ et de $Y+U$.

On a $e_1 R = e_1 \mathfrak{o} + \mathfrak{P}_1^2$ et cela entraîne $\mathfrak{P}_1^2 A_0 \subset Z$. Par conséquent, on a $\overline{e_1 A_0} \subset \bar{V}_2 \cap \bar{V}_4 \subset \bar{W}$ et on peut supposer que les générateurs de $e_1 A_0$ sont dans $V_2 \cap V_4 \subset W$. Donc (17) entraîne bien une décomposition directe de $e_1 A_0$.

Remarquons que $\mathfrak{P}_1^2 M \subset e_1 M$, car $\mathfrak{P}_1^2 \subset e_1 R$. Si b est un élément quelquonque de $\mathfrak{P}_1^2 M$ il existe $c \in \mathfrak{P}_2 M$ tel que $b+c \in M$. Soit u_i l'un des générateurs de U et $u_i + x_i \in M$. Alors on peut remplacer $u_i + x_i$ par $(u_i+b)+(x_i+c)$, c.-à-d. u_i peut être varié librement modulo $\mathfrak{P}_1^2 M$. Donc on peut supposer $u_i = \pi_1 u_i'$ avec $u_i' \in V$ et on obtient $U=\pi_1 U'$. De plus les u_i sont indépendants modulo $\mathfrak{P}_1^2 M$ et cela entraîne que U' est facteur directe de V. De plus, $\pi_1 u' + x = m \in M$ entraîne $qm = q\pi_1 u' \in Z$ et on voit que $\mathfrak{P}_1^4 U'$ est dans Z. Cela entraîne $\bar{U}' \subset \bar{V}_1 \oplus \bar{V}_4$. Or, $\bar{U}' \cap \bar{V}_1$ est $=0$, car autrement les u_i ne serait pas indépendants modulo $\mathfrak{P}_1^2 M$. Par conséquent, U' est facteur directe de V_4. Dans la décomposition (17), V_4'' est un complément quelquonque de $V_4' = V_4 \cap W$, et on peut donc obtenir que

$$U' = U' \cap V_4' \oplus U' \cap V_4''.$$

Par conséquent, (17) entraîne en effet une décomposition simultanée de $e_1 A$, $e_1 A_0$, $Y+U$ et Y, c.-à-d. une décomposition de M, et V est égal à l'un de ces facteurs directes. Si $V=V_4''$ ou $V=V_7$ on voit que l'on peut continuer la décomposition simultanée en facteurs directes de rang 1. Alors on obtient $A=Ra$, c.-à-d. $\varrho_1(M)=1$, $\varrho_2(M) \leqslant 2$.

Supposons donc $V=W=V_1+V_2+V_1\delta_{1,2}+V_2\delta_{2,4}$. Ici on peut toujours obtenir que $\delta_{2,4}=0$. Soit $v_2 \in V_2$ et $y_2 = \pi_1^2 v_2 + \pi_1^4 v_2 \delta_{2,4} \in Z$. Si v_2 est dans $e_1 A_0$, on a $\mathfrak{P}_1^2 v_2 \subset Z$ et on peut poser $y_2 = \pi_1^2 v_2 \in Z$. Autrement on a $y_2 = \pi_1^2(v_2+b)$ avec $b \in \mathfrak{P}_1^2 M$, et il existe $c \in \mathfrak{P}_2 M$ tel que $b+c \in M \cap \mathfrak{P}M$. Or, on peut supposer que $v_2 = e_1 a_1$ est l'un des générateurs de $e_1 A$ et comme a_1 est du type $(1, 1)$ et $b+c \in \mathfrak{P}M$, on peut remplacer a_1 par $a_1' = a_1 + (b+c)$ et en même temps v_2 par $v_2' = v_2 + b$. Cela change Z en Z' et on a $v_2' \in Z'$ et $y_2 = \pi_1^2 v_2'$, c.-à-d. $v_2' \delta_{2,4} = 0$. En continuant ainsi, on voit que si les générateurs a_i de A sont convenablement choisis, on a en effet $\delta_{2,4}=0$ et $V=V_1+V_2+V_1\delta_{1,2}$.

Remarquons maintenant que $Z \cap \mathfrak{P}_1 Z = \mathfrak{P}_1 M \cap M$ permet l'ordre $e_1 R = \mathfrak{o} e_1 + \mathfrak{P}_1^2$. Donc si $y_1 = \pi_1 v_1 + \pi_1^2 v_1 \delta_{1,2}$, $\mathfrak{P}_1^2 y_1$ est dans Z. Cela implique que $\mathfrak{P}_1^3 V_1$ et $\mathfrak{P}_1^3 V_1 \delta_{1,2}$ sont dans Z et d'une façon analogue on voit que $\mathfrak{P}_1^3 V_2 \subset Z$. Par conséquent, Z permet déjà l'ordre $\mathfrak{o} e_1 + \mathfrak{P}_1^3$. D'après la proposition 5 il existe donc une décomposition

$$V = V_{1,2} \oplus V_{1,1} \oplus V_{2,2} \oplus V_1 \delta_{1,2}. \tag{18}$$

Nous allons maintenant montrer que cette décomposition entraîne une décomposition simultanée de $e_1 A_0$ et de U'. On a vu plus haut, que les générateurs de $e_1 A_0$ figurent parmi les générateurs de V_2 et on peut supposer que $V_2 = V_{1,2} \oplus V_{2,2}$ entraîne une décomposition de $e_1 A_0$. De plus, on a $\bar{U}' \cap \bar{V}_1 = 0$, c.-à-d. $\bar{U}' \subset \bar{V}_{2,2} \oplus \bar{V}_1 \delta_{1,2}$. Posons $\bar{U}_0' = \bar{U}' \cap \overline{e_1 A_0} \subset \bar{V}_{2,2}$ et soit $e_1 a \in e_1 A_0$ avec $0 \neq \overline{e_1 a} \in \bar{U}_0'$. Les générateurs de U' peuvent être variés librement modulo $\mathfrak{P}_1 Z$ et on peut donc prendre $e_1 a$ comme l'un des générateurs de U'. Cela montre que (18) entraîne une décomposition simultanée de $e_1 A_0$ et de U'.

On a déjà noté, que chaque décomposition de Z entraîne une décomposition simultanee de $e_1 A$ et de Y. Or, d'après la proposition 5, on obtient de (18) une décomposition $Z = \oplus \sum Z_i$ en réseaux indécomposables Z_i. Comme (18) entraîne une décomposition de $e_1 A_0$ et de U', on voit que cette décomposition de Z peut se faire de façon qu'elle aussi entraîne une décomposition simultanée de $e_1 A_0$ et de U'. Donc on trouve enfin, que la décomposition $Z = \oplus \sum Z_i$ entraîne une décomposition correspondante de M. Comme M est indécomposable, cela veut dire que Z est un réseau indécomposable, c.-à-d. $\varrho_1(Z) \leqslant 2$. Si $\varrho_1(Z) = 1$ on a $\varrho_1(M) = 1$ et $\varrho_2(M) \leqslant 2$. Soit donc $\varrho_1(Z) = 2$. Alors, d'après la proposition 5, le rang de V_1 est $= 1$, et on sait, que $V_1 \cap U' = 0$. Le rang de U' est donc au plus $= 1$, c.-à-d. on a $\varrho_2(M) \leqslant 3$. Pour $A_0 = 0$ et $U \neq 0$ on a en effet $\varrho_2(M) = 3$ et cela montre que $\varrho_1(R) = 2$ et $\varrho_2(R) = 3$. Ceci achève la démonstration de la proposition 8 et du théorème 2.

Il est maintenant facile, de faire la liste complète des types de réseaux indécomposables pour les ordres R_{I}, R_{II} et R_{III}; en effet nous les avons plus ou moins explicitement déterminés au cours de la démonstration ci-dessus. Comme il y a quand même un nombre de cas à distinguer, nous n'insistons pas sur les détails. Notons seulement la généralisation suivante de la proposition 7 :

COROLLAIRE. *Soit R un ordre indécomposable dans $K = \oplus \sum_1^s K_i$ avec $s = 2, 3$. Si $J(R) + \mathfrak{P}_i = \mathfrak{P}$ pour chaque i, on a $\varrho(R) = 1$.*

D'abord la condition $J(R) + \mathfrak{P}_i = \mathfrak{P}$ pour chaque i entraîne, que R contient l'ordre R_{I} (ou $(1 - e_3) R_{\mathrm{I}}$ pour $s = 2$). Soit donc M un R_{I}-réseau indécomposable avec $\varrho(M) > 1$. Si M permet l'ordre R, il n'y a pas dans la décomposition de SM de composante Sx de type 2). Car la relation $J(R) + \mathfrak{P}_3 = \mathfrak{P}$ entraîne que x peut toujours être choisi dans M. Donc on a $X = U = 0$ et $\varrho(M)$ est $= 1$.

Algèbres de groupe

Reprenons maintenant les notations de l'introduction. Soit k un corps de nombres algébriques de degré fini sur Q et $\mathfrak{o}$ un anneau de Dedekind, dont k est le corps des quotients. Alors $\mathfrak{o}$ contient l'anneau des entiers de k, mais peut être plus grand que celui-ci. Soit G un groupe fini, commutatif ou non. Nous allons déduire du théorème 2 des conditions nécessaires et suffisantes pour que $n(\mathfrak{o}G)$ soit fini.

Soit $\mathfrak{p} \neq \mathfrak{o}$ un idéal premier de $\mathfrak{o}$ qui divise l'ordre de G et soit G_p un groupe de Sylow de G avec $\mathfrak{p}/p$. Jones [4] a montré(1), que $n(\mathfrak{o}G)$ est fini si et seulement si $n(\mathfrak{o}_\mathfrak{p} G_p)$ est fini pour chaque $\mathfrak{p}$ qui divise $|G|$. Nous avons donc à trouver des conditions nécessaires et suffisantes pour que $n(\mathfrak{o}_\mathfrak{p} G_p)$ soit fini.

Le lemme suivant est du à Dade [2]; nous donnons ici une autre démonstration, basée sur la proposition 1.

LEMME 7. *$n(\mathfrak{o}_\mathfrak{p} G_p) = \infty$, sauf peut être si G_p est cyclique d'ordre p^2 au plus.*

Soit Q_p le complété p-adique du corps des nombres rationels et Z_p son anneau de valuation. Alors $k_\mathfrak{p}$ est de degré fini sur Q_p et on a $\mathfrak{o}_\mathfrak{p} G_p = \mathfrak{o}_\mathfrak{p} \otimes_{Z_p} Z_p G_p$. D'après la proposition 1, $n(\mathfrak{o}_\mathfrak{p} G_p)$ et $n(Z_p G_p)$ sont finis en même temps, si $k_\mathfrak{p}$ est non-ramifié sur Q_p. De plus, comme on l'a noté au cours de la démonstration, $n(Z_p G_p) = \infty$ implique $n(\mathfrak{o}_\mathfrak{p} G_p) = \infty$ même si $k_\mathfrak{p}$ est ramifié sur Q_p. Par conséquent, il suffit de montrer le lemme pour $\mathfrak{o}_\mathfrak{p} = Z_p$.

Supposons d'abord, que G_p est abélien. Alors $Q_p G_p = \oplus \sum K_i$, où K_i est le corps des racines p^{t_i}-ièmes de l'unité. De plus, $Z_p G_p$ est un ordre indécomposable, car pour chaque $g \in G_p$, une puissance de $1-g$ est divisible par p. Cela entraîne $1-g \in \mathfrak{P}$ et $Z_p G_p$ est indécomposable d'après le lemme 1. Comme les extensions K_i/Z_p sont totalement ramifiées, $Z_p G_p$ satisfait aux hypothèses du théorème 2. Donc, $n(Z_p G_p) < \infty$ implique $s \leqslant 3$ et on vérifie facilement que ceci est vrai seulement pour un groupe cyclique d'ordre p^2 au plus.

Si G_p n'est pas abélien, soit G_p' son groupe de commutateurs. Alors $H = G_p/G_p'$ est abélien mais non pas cyclique. Donc on a $n(Z_p H) = \infty$. Or, si M est un $Z_p H$-réseau indécomposable, on peut en faire un $Z_p G_p$-réseau indécomposable en posant $g'm = m$ pour $g' \in G_p'$ et $m \in M$. Par conséquent on a aussi $n(Z_p G_p) = \infty$, ce qui achève la démonstration.

Désignons par $E(\mathfrak{p})$ l'indice de ramification absolu de p. Cela veut dire que $\mathfrak{p}^{E(\mathfrak{p})}$ est la puissance exacte de $\mathfrak{p}$ dans p. Nous allons montrer le

THÉORÈME 3. *Soit $\mathfrak{o}$ un anneau de Dedekind, dont le corps des quotients est de degré fini sur Q et soit G un groupe fini. Alors $n(\mathfrak{o}G)$ est fini si et seulement si $\mathfrak{o}G$ satisfait aux deux conditions suivantes :*

(1) La démonstration dans [4] est faite pour le cas où $\mathfrak{o}$ est l'anneau des entiers de k; elle reste valable si $\mathfrak{o}$ est un anneau de Dedekind quelquonque dont k est le corps des quotients.

1) *Si p n'est pas une unité dans* $\mathfrak{o}$, *le groupe G_p est cyclique d'ordre p^m avec $m \leqslant 2$ et*
2) *pour chaque* $\mathfrak{p}$ *qui divise p on a*

$$\begin{aligned} E(\mathfrak{p}) &= 1 \quad \textit{si} \quad m=2, \\ E(\mathfrak{p}) &\leqslant 2 \quad \textit{si} \quad m=1,\ p>3, \\ E(\mathfrak{p}) &\leqslant 3 \quad \textit{si} \quad m=1 \textit{ et } p=3. \end{aligned}$$

Soit $C=(c)$ un groupe cyclique d'ordre p^m. D'après le lemme ci-dessus il suffit de montrer que $n(\mathfrak{o}_\mathfrak{p} C)$ est fini, si et seulement si m et $E(\mathfrak{p})$ satisfont à la condition 2). (1)

Désignons par Ω le corps d'inertie de $k_\mathfrak{p}/Z_p$; c'est le corps non-ramifié maximal contenu dans $k_\mathfrak{p}/Z_p$. Alors $k_\mathfrak{p}$ est totalement ramifié sur Ω et on a $E(\mathfrak{p})=(k_\mathfrak{p}:\Omega)$. Soit $\Delta_i=\Omega(\xi_i)$ le corps des racines p^i-ièmes de l'unité sur Ω. Alors on a

$$\Omega C = \varepsilon_0 \Delta_0 \oplus \varepsilon_1 \Delta_1 \oplus \dots \oplus \varepsilon_m \Delta_m$$

où les ε_i sont des idempotents orthogonaux. Supposons $k_\mathfrak{p}$ et les Δ_i plongés dans un même corps Σ, et soit K_i le composé de $k_\mathfrak{p}$ et Δ_i dans Σ et L_i leur intersection. Or, l'extension Δ_i/Ω est normale et on obtient

$$\varepsilon_i(k_\mathfrak{p} \underset{\Omega}{\otimes} \Delta_i) = e_{i,1} K_i \oplus \dots \oplus e_{i,r_i} K_i$$

où les $e_{i,j}$ sont des idempotents orthogonaux et $r_i=(L_i:\Omega)$. Alors on a

$$k_\mathfrak{p} C = \oplus \sum_{i=0}^{m} \sum_{j=1}^{r_i} e_{i,j} K_i.$$

Soit Ω_i le corps d'inertie de K_i sur Z_p. Alors $\Omega_i \supset \Omega$ et Ω_i/Ω est non-ramifié. Désignons par $k'_\mathfrak{p}$ le composé de $k_\mathfrak{p}$ avec tous les Ω_i. Alors $k'_\mathfrak{p}/k_\mathfrak{p}$ est non-ramifié. Si l'on remplace $k_\mathfrak{p}$ par $k'_\mathfrak{p}$, on ne change pas $E(\mathfrak{p})$ et d'après la proposition 1, $n(\mathfrak{o}_\mathfrak{p} C)$ et $n(\mathfrak{o}'_\mathfrak{p} C)$ sont finis en même temps. Or, pour $k'_\mathfrak{p} C$ on a $\Omega'_i = \Omega'$ pour chaque i. Donc on peut supposer dès le début que $\Omega_i=\Omega$; cela veut dire que K_i est totalement ramifié sur Ω. Désignons par n_i le degré $(\Delta_i:\Omega)$. Alors on a $(K_i:k_\mathfrak{p})=n_i r_i^{-1}$ et $(K_i:\Delta_i)=E(\mathfrak{p}) r_i^{-1}$. Si $\mathfrak{P}_i$ est l'idéal maximal de l'anneau de valuation de K_i et $\mathfrak{T}_i$ celui de Δ_i, on a donc

$$\mathfrak{T}_i = \mathfrak{P}_i^{E(\mathfrak{p}) r_i^{-1}},$$

$$\mathfrak{p} = \mathfrak{P}_i^{n_i r_i^{-1}}.$$

(1) La nécessité des deux premières conditions dans 2) pour que $n(\mathfrak{o}_\mathfrak{p} C)$ soit fini, a été démontré par Kneser [5]. De l'autre coté, Gudivok [3] a montré que ces deux conditions sont suffisantes, si $k_\mathfrak{p}$ est de degré 2 sur Q_p.

Considérons d'abord le cas $m=2$. Alors ΩC est la somme directe de trois corps et la condition $s \leqslant 3$ implique que, si $n(\mathfrak{o}_\mathfrak{p} C)$ est fini, tous les r_i sont $=1$. Alors d'après le théorème 2, $n(\mathfrak{o}_\mathfrak{p} C)$ est fini, si et seulement si $J(\mathfrak{o}_\mathfrak{p} C)+\varepsilon_i \mathfrak{P}_i=\sum \varepsilon_i \mathfrak{P}_i=\mathfrak{P}$ pour au moins deux i. Le radical $J(\mathfrak{o}_\mathfrak{p} C)$ est engendré par $\mathfrak{p}\cdot 1$ et $1-c=(1-\xi_1)\varepsilon_1+(1-\xi_2)\varepsilon_2$ et on sait que $1-\xi_i$ est une uniformisante de Δ_i. Si $E(\mathfrak{p})=1$ on a $K_i=\Delta_i$ et $J(\mathfrak{o}_\mathfrak{p} C)+\varepsilon_i \mathfrak{T}_i=\sum \varepsilon_i \mathfrak{T}_i$ pour $i=1, 2$, c.-à-d. $n(\mathfrak{o}_\mathfrak{p} C)<\infty$. Supposons donc $E(\mathfrak{p})>1$. Alors $\varepsilon_2 J(\mathfrak{o}_\mathfrak{p} C)$ est engendré par $\varepsilon_2 \mathfrak{p}$ et $\varepsilon_2(1-\xi_2)$, donc il est contenu dans $\varepsilon_2 \mathfrak{P}_2^\alpha$, avec $\alpha=\min(n_2, E(\mathfrak{p}))$. Or $n_2=p(p-1)$ est toujours >1, c.-à-d. on a $\alpha>1$. Donc pour $i=0,1$ on a $J(\mathfrak{o}_\mathfrak{p} C)+\varepsilon_i \mathfrak{P}_i \subset \varepsilon_0 \mathfrak{P}_0+\varepsilon_1 \mathfrak{P}_1+\varepsilon_2 \mathfrak{P}_2^\alpha \neq \mathfrak{P}$, ce qui entraîne $n(\mathfrak{o}_\mathfrak{p} C)=\infty$.

Considerons maintenant le cas $m=1$. Alors on a

$$k_\mathfrak{p} C=\varepsilon_0 k_\mathfrak{p} \oplus \sum_1^{r_1} e_{1,j} K_1$$

et le radical de $\mathfrak{o}_\mathfrak{p} C$ est engendré par $\mathfrak{p}\cdot 1$ et $1-c=(1-\xi_1)\sum e_{1,j}$. Si $p=2$, on a $k_\mathfrak{p} C= \varepsilon_0 k_\mathfrak{p} \oplus \varepsilon_1 k_\mathfrak{p}$ et $J(\mathfrak{o}_\mathfrak{p} C)+\varepsilon_i \mathfrak{p} \supset \mathfrak{p}\cdot 1+\mathfrak{p}\varepsilon_i=\mathfrak{P}$ pour $i=0,1$. Donc $n(\mathfrak{o}_\mathfrak{p} C)$ est toujours fini.

Soit donc $p>2$. La condition $s \leqslant 3$ entraine que $r_1 \leqslant 2$. Si $r_1=2$, $E(\mathfrak{p})$ est pair $=2a$ avec $a=(K_1:\Delta_1)$. Pour $a=1$ on a $K_1=\Delta_1$ et comme $1-\xi_1$ est une uniformisante de Δ_1, on voit que $J(\mathfrak{o}_\mathfrak{p} C)+e_{1,j}\mathfrak{P}_1=\mathfrak{P}$ pour $j=1, 2$ et $n(\mathfrak{o}_\mathfrak{p} C)$ est fini. Si $a>1$, on a $\mathfrak{T}_1=\mathfrak{P}_1^a$ et l'élément $1-c$ est dans $\mathfrak{P}_1^a(e_{1,1}+e_{1,2})$. Donc on voit que $J(\mathfrak{o}_\mathfrak{p} C) \subset \mathfrak{p}\cdot 1+\mathfrak{P}_1^a(e_{1,1}+e_{1,2})$ et $J(\mathfrak{o}_\mathfrak{p} C)+\mathfrak{P}_1 e_{1,j} \neq \mathfrak{P}$ pour $j=1,2$, ce qui entraîne $n(\mathfrak{o}_\mathfrak{p} C)=\infty$.

Soit donc finalement $r_1=1$, c.-à-d.

$$k_\mathfrak{p} C=\varepsilon_0 k_\mathfrak{p} \oplus \varepsilon_1 K_1.$$

Le radical $J(\mathfrak{o}_\mathfrak{p} C)$ est engendré par $\mathfrak{p}\cdot 1$ et $1-c=(1-\xi_1)\varepsilon_1$. Pour $E(\mathfrak{p})=1$, $1-\xi_1$ est une uniformisante de K_1. Alors $J(\mathfrak{o}_\mathfrak{p} C)=\mathfrak{P}$ et $n(\mathfrak{o}_\mathfrak{p} C)$ est fini. Soit $\alpha=\min(p-1, E(\mathfrak{p}))$; alors $E(\mathfrak{p})>1$ implique $\alpha>1$ et on a $J(\mathfrak{o}_\mathfrak{p} C)+\varepsilon_0 \mathfrak{p} \subset \varepsilon_0 \mathfrak{p}+\varepsilon_1 \mathfrak{P}_1^\alpha$. Donc pour $E(\mathfrak{p})>1$, $n(\mathfrak{o}_\mathfrak{p} C)$ est fini si et seulement si $\mathfrak{o}_\mathfrak{p} C$ satisfait à la condition b) du théorème 2. Cette condition donne $\alpha=2$ et $E(\mathfrak{p})<4$, c.-à.-d. $E(\mathfrak{p})=2$ si $p>3$ et $E(\mathfrak{p}) \leqslant 3$ si $p=3$.

En résumant les cas $r_1=1$ et $r_1=2$ on voit donc que la condition $E(\mathfrak{p}) \leqslant 2$ est nécessaire et suffisante si $p>3$. Pour $p=3$ et $E(\mathfrak{p})=3$ on a nécessairement $r_1=1$, parce que $E(\mathfrak{p})$ est pair si $r_1=2$. Donc, pour $p=3$ la condition $E(\mathfrak{p}) \leqslant 3$ est aussi nécessaire et suffisante, ce qui achève la démonstration.

Bibliographie

[1]. CURTIS, C. W. & REINER, I., *Representation theory of finite groups and associative algebras.* Intersc. Publishers, New York, 1962.

[2]. DADE, E. C., Some indecomposable group representations. *Ann. of Math.*, 77 (1963), 406–412.

[3]. GUDIVOK, P. M., Representation of finite groups over quadratic rings. *Dokl. Akad. Nauk SSSR*, 159 (1964), 1210–1213 = *Soviet Math. Dokl.*, 5 (1964), 1669–1672.

[4]. JONES, A., Groups with a finite number of indecomposable integral representations. *Michigan Math. J.*, 10 (1963), 257–261.

[5]. KNESER, M. Einige Bemerkungen über ganzzahlige Darstellungen endlicher Gruppen. *Arch. Math.*, 17 (1966), 377–379.

Reçu le 27 décembre 1965