SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

DOMINIQUE DUVAL

Sur la structure galoisienne du groupe des unités d'un corps abélien réel de type (p, p)

Séminaire de théorie des nombres de Grenoble, tome 7 (1978-1979), exp. n° 2, p. 1-41

<http://www.numdam.org/item?id=STNG_1978-1979__7__A2_0>

Séminaire de Théorie des Nombres
30 novembre 1978
Grenoble

SUR LA STRUCTURE GALOISIENNE DU GROUPE DES UNITES D'UN CORPS ABELIEN REEL DE TYPE (p,p)

(Suite du travail de Lyliane BOUVIER et Jean Jacques PAYAN [1,11]).

par
Dominique DUVAL

PLAN.

I. RAPPELS ET NOTATIONS.

Dans tout cet exposé, on note :

p un nombre premier,

ζ une racine primitive $p^{\text{ème}}$ de l'unité, fixée (dans une clôture algébrique de $\mathbb{Q}$),

$\mathbb{Q}^{(p)}(=\mathbb{Q}(\zeta))$ le $p^{\text{ème}}$ corps cyclotomique,

G le groupe $(\mathbb{Z}/p\mathbb{Z})^2$.

Pour tout groupe fini Γ , on note $\widetilde{\Gamma} = \sum_{\gamma\in\Gamma} \gamma$ (c'est un élément de $\mathbb{Z}[\Gamma]$).

DEFINITION. - Un $\mathbb{Z}[G]$-module M est dit <u>réalisable</u> (comme module d'unités) si M est $\mathbb{Z}$-libre de type fini, et s'il existe un $\mathbb{Q}[G]$-homomorphisme injectif de $\mathbb{Q}[G] \underset{\mathbb{Z}[G]}{\otimes} M$ dans $\mathbb{Q}[G]/\mathbb{Q}.\widetilde{G}$.

<u>Remarque</u> : Soit K une extension finie galoisienne réelle de $\mathbb{Q}$, de groupe de Galois Γ . Notons E_K le groupe des unités de K modulo torsion. On sait qu'alors les deux $\mathbb{Q}[\Gamma]$-modules $\mathbb{Q}[\Gamma] \underset{\mathbb{Z}[\Gamma]}{\otimes} E_K$ et $\mathbb{Q}[\Gamma]/\mathbb{Q}.\widetilde{\Gamma}$ sont isomorphes.

Donc, pour un $\mathbb{Z}[G]$-module M , les deux propriétés suivantes sont équivalentes :

i) M est réalisable.

ii) M est $\mathbb{Z}[G]$-isomorphe à un sous-$\mathbb{Z}[G]$-module du groupe des unités modulo torsion d'une extension abélienne réelle de $\mathbb{Q}$ de type (p,p) .

Soit M un $\mathbb{Z}[G]$-module réalisable. On note alors $\mathcal{H}_M$ l'ensemble des sous-groupes d'ordre p de G tels que M^H soit non nul (où M^H est l'ensemble des points de M fixes par H). On note r le cardinal de $\mathcal{H}_M$; on montre [1] que c'est la longueur de

$\mathbb{Q}[G] \underset{\mathbb{Z}[G]}{\otimes} M$ comme $\mathbb{Q}[G]$-module.

DEFINITION. - Le cardinal r de $\mathfrak{H}_M$ est appelé la longueur de M .

On a bien sûr $\boxed{r \leq p+1}$.

PROPOSITION [1]. - La somme des $\mathbb{Z}[G]$-modules M^H (pour H dans $\mathfrak{H}_M$) est directe dans M , et contient pM .

Conséquences :

- Si $r = 0$, alors $M = 0$.
- Si $r = 1$, notons $\mathfrak{H}_M = \{H\}$. Alors $M = M^H$, donc M est un $\mathbb{Z}[G/H]$-module, annulé par $\widetilde{G/H}$. Soit γ un générateur de G/H . On définit un isomorphisme φ de $\mathbb{Z}[G/H]/\mathbb{Z}.\widetilde{G/H}$ sur $\mathbb{Z}[\zeta]$ en posant $\varphi(\gamma \bmod \mathbb{Z}.\widetilde{G/H}) = \zeta$. Cet isomorphisme fait de M un idéal de $\mathbb{Q}^{(p)}$.

THEOREME [2,3]. - L'isomorphisme φ induit une bijection entre l'ensemble des classes de $\mathbb{Z}[G]$-isomorphisme des $\mathbb{Z}[G]$-modules réalisables M tels que $\mathfrak{H}_M = \{H\}$, et l'ensemble des classes d'idéaux de $\mathbb{Q}^{(p)}$.

De plus, changer de générateur γ pour G/H revient à faire agir un élément de $\mathrm{Gal}(\mathbb{Q}^{(p)}/\mathbb{Q})$ sur le groupe des classes d'idéaux de $\mathbb{Q}^{(p)}$.

- Si $r \geq 1$, et si $H \in \mathfrak{H}_M$, alors M^H est un $\mathbb{Z}[G]$-module réalisable de longueur 1 , et $\mathfrak{H}_{M^H} = \{H\}$. On peut donc appliquer à M^H ce qui précède.

II. PASSAGE AUX $\mathbb{F}_p[G]$-MODULES.

Dans toute la suite de l'exposé, on fixe :

- un entier r vérifiant $1 \leq r \leq p+1$,
- un ensemble $\{H_1, H_2, \ldots, H_r\}$ de r sous-groupes distincts d'ordre p de G ,
- un $\mathbb{Z}[G]$-module réalisable M_i , fixe par H_i , pour tout i de 1 à r .

On note $\overline{M_i}$ le $\mathbb{F}_p[G]$-module $p^{-1}M_i/M_i$, U le groupe des unités de $\mathbb{Q}^{(p)}$, et U_i l'image de U dans $\mathrm{Aut}_{\mathbb{F}_p[G]}\overline{M_i}$ (en effet, d'après I, on peut identifier M_i à un idéal de $\mathbb{Q}^{(p)}$; donc U agit sur M_i , et sur $\overline{M_i}$; on définit ainsi U_i , et on vérifie que U_i ne dépend pas du choix du générateur de G/H_i qui a servi à faire l'identification).

THEOREME. - *L'application* $M \mapsto Q = M/\bigoplus_{H \in \mathcal{H}_M} M^H$ *induit une bijection entre* :

- *l'ensemble des classes de* $\mathbb{Z}[G]$*-isomorphisme des* $\mathbb{Z}[G]$*-modules réalisables* M *tels que* $\mathcal{H}_M = \{H_1, H_2, \ldots, H_r\}$, *et tels que* M^{H_i} *soit* $\mathbb{Z}[G]$*-isomorphe à* M_i *pour tout* i *de* 1 *à* r ,
- *et l'ensemble des classes des sous-*$\mathbb{F}_p[G]$*-modules* Q *de* $\bigoplus_{i=1}^{r} \overline{M_i}$ *tels que* $Q \cap \overline{M_i}$ *soit nul pour tout* i , *modulo l'action de* $\prod_{i=1}^{r} U_i$.

Démonstration :

a) Soit M un $\mathbb{Z}[G]$-module réalisable tel que $\mathcal{H}_M = \{H_1, H_2, \ldots, H_r\}$, et tels que $M^{H_i} \simeq M_i$ pour tout i de 1 à r . On sait (cf. I) qu'alors on a $\bigoplus_{i=1}^{r} M^{H_i} \subset M \subset \bigoplus_{i=1}^{r} p^{-1}M^{H_i}$. Donc le quotient

$Q = M/\bigoplus_{i=1}^{r} M^{H_i}$ s'identifie à un sous-$\mathbb{F}_p[G]$-module de $\bigoplus_{i=1}^{r} \overline{M_i}$.

Réciproquement, soit Q un sous-$\mathbb{F}_p[G]$-module de $\bigoplus_{i=1}^{r} \overline{M_i}$, et soit M l'image réciproque de Q dans $\bigoplus_{i=1}^{r} p^{-1}M_i$ (par la projection canonique de $\bigoplus_{i=1}^{r} p^{-1}M_i$ sur $\bigoplus_{i=1}^{r} \overline{M_i}$). Il est alors clair que M est un $\mathbb{Z}[G]$-module réalisable, que $\mathcal{H}_M = \{H_1, H_2, \ldots, H_r\}$, et que $M_i \subset M^{H_i} \subset p^{-1}M_i$ pour tout i de 1 à r .

De plus, pour chaque i , les $\mathbb{F}_p[G]$-modules M^{H_i}/M_i et $Q \cap \overline{M_i}$ sont isomorphes. Donc $M^{H_i} = M_i$ si et seulement si $Q \cap \overline{M_i} = 0$.

On vérifie enfin que les deux applications $M \mapsto Q$ et $Q \mapsto M$ sont réciproques l'une de l'autre.

b) Si M et M' sont deux $\mathbb{Z}[G]$-modules réalisables, avec $\mathcal{H}_M = \mathcal{H}_{M'} = \{H_1, H_2, \ldots, H_r\}$, et si M^{H_i} et M'^{H_i} sont $\mathbb{Z}[G]$-isomorphes à M_i pour tout i , on identifie M^{H_i} , M'^{H_i} , et M_i par ces $\mathbb{Z}[G]$-isomorphismes. S'il existe un $\mathbb{Z}[G]$-isomorphisme θ de M sur M' , on a alors $\theta(M^{H_i}) = M'^{H_i}$ pour tout i , donc θ induit un $\mathbb{Z}[G]$-automorphisme θ_o de $\bigoplus_{i=1}^{r} M_i$.

Réciproquement, si θ_o est un $\mathbb{Z}[G]$-automorphisme de $\bigoplus_{i=1}^{r} M_i$, il se prolonge de manière unique en un $\mathbb{Z}[G]$-automorphisme (encore noté θ_o) de $\bigoplus_{i=1}^{r} p^{-1}M_i$, et induit un $\mathbb{F}_p[G]$-automorphisme $\overline{\theta_o}$ de $\bigoplus_{i=1}^{r} \overline{M_i}$. Il est alors clair que l'image de M par θ_o est égale à M' si et seulement si l'image de Q par $\overline{\theta_o}$ est égale à Q' (où $Q = M/\bigoplus_{i=1}^{r} M^{H_i}$, et $Q' = M'/\bigoplus_{i=1}^{r} M'^{H_i}$).

Or on a $\mathrm{Aut}_{\mathbb{Z}[G]} \bigoplus_{i=1}^{r} M_i = \prod_{i=1}^{r} \mathrm{Aut}_{\mathbb{Z}[G/H_i]} M_i$, et si on identifie (comme en I) M_i avec un idéal de $\mathbb{Q}^{(p)}$, on voit que $\mathrm{Aut}_{\mathbb{Z}[G/H_i]} M_i$ s'identifie à U ; donc les automorphismes $\overline{\theta_o}$ sont exactement les éléments de $\prod_{i=1}^{r} U_i$.

c.q.f.d.

III. QUELQUES PROPRIETES GENERALES DES $\mathbb{F}_p[G]$-MODULES Q .

Notations et définitions :

Notons I l'idéal d'augementation de $\mathbb{F}_p[G]$, c'est-à-dire l'idéal de $\mathbb{F}_p[G]$ engendré par les éléments $(g-1)$ (pour $g \in G\backslash\{1\}$). Pour tout $\mathbb{F}_p[G]$-module N et tout entier positif j , notons $N^{(j)}$ le noyau de I^j dans N ; autrement dit, $N^{(j)}$ est l'intersection des noyaux des endomorphismes $\prod_{k=1}^{j}(g_k - 1)$ de N , lorsque $\{g_k\}_{1\leq k\leq j}$ parcourt $(G\backslash\{1\})^j$. On a bien sûr $N^{(0)} = \{0\}$, $N^{(1)} = N^G$, et $N^{(j)} \subset N^{(j+1)}$ pour tout j .

Considérons l'ensemble des entiers positifs j tels que $N^{(j)} = N$. Si cet ensemble n'est pas vide, on dit que N est de hauteur finie, et on appelle hauteur de N le plus petit élément de cet ensemble (on note cet entier $ht(N)$). On a bien sûr $ht(N) = 0$ si et seulement si $N = 0$.

Soit Q un sous-$\mathbb{F}_p[G]$-module de $\bigoplus_{i=1}^{r}\overline{M_i}$ tel que $Q \cap \overline{M_i}$ soit nul pour tout i de 1 à r .

Remarque : Lorsqu'on identifie M_i à un idéal de $\mathbb{Q}^{(p)}$ (comme en I), on voit en localisant en p que $\overline{M_i}$ s'identifie à $\mathbb{F}_p[\zeta]/(\zeta-1)^{p-1}$, et ceci est indépendant du choix de l'identification, et de la classe de l'idéal de $\mathbb{Q}^{(p)}$ correspondant à M_i .

PROPOSITION. - Le $\mathbb{F}_p[G]$-module Q vérifie la propriété suivante :
(*) Pour tout sous-groupe H d'ordre p de G , on a $Q^H = Q^G$.

Démonstration : Soient H un sous-groupe d'ordre p de G , et i un entier de 1 à r . On a alors

$$\overline{M_i}^H = \begin{cases} \overline{M_i}^G & \text{si } H \neq H_i \\ \overline{M_i} & \text{si } H = H_i \ , \end{cases}$$

donc

$$\left(\overline{\bigoplus_{i=1}^{r} M_i}\right)^H = \begin{cases} \left(\overline{\bigoplus_{i=1}^{r} M_i}\right)^G & \text{si } H \notin \{H_1, H_2, \ldots, H_r\} \\ \left(\overline{\bigoplus_{\substack{i=1 \\ i \neq i_o}}^{r} M_i}\right)^G \oplus \overline{M_{i_o}} & \text{si } H = H_{i_o} \end{cases}.$$

On en déduit que $Q^H = Q^G$ pour tout $H \notin \{H_1, H_2, \ldots, H_r\}$. Si $H = H_{i_o}$ (avec $1 \leq i_o \leq r$), soient q dans Q^H et g dans G. On note $q = \sum_{i=1}^{r} q_i$, avec $q_i \in \overline{M_i}$. On a alors $(g-1)(q_i) = 0$ pour tout $i \neq i_o$ (par ce qui précède), donc $(g-1)q = (g-1)q_{i_o}$. Or ceci est dans $Q \cap \overline{M_{i_o}}$, c'est donc nul. Donc $Q^{H_{i_o}} = Q^G$.

c.q.f.d.

PROPOSITION. - Soit N un $\mathbb{F}_p[G]$-module vérifiant la propriété (*). Alors, pour tout entier positif j, et pour tout j-uple $\{g_k\}_{1 \leq k \leq j}$ dans $(G - \{1\})^j$, le noyau de l'endomorphisme $\prod_{k=1}^{j} (g_k - 1)$ de N est égal à $N^{(j)}$.

Démonstration : Par récurrence sur j. Le cas $j = 0$ est trivial, et le cas $j = 1$ est la propriété (*). Supposons donc $j \geq 2$, et soient $\{g_k\}_{1 \leq k \leq j}$ et $\{g'_k\}_{1 \leq k \leq j}$ deux j-uples de $(G - \{1\})^j$.

S'il existe 2 indices k_o et k_1 tels que $g_{k_o} = g'_{k_1}$, en appliquant l'hypothèse de récurrence à $(g_k)_{1 \leq k \leq j,\, k \neq k_o}$ et $(g'_k)_{1 \leq k \leq j,\, k \neq k_1}$, on voit qu'on a encore :

$$\operatorname{Ker} \prod_{k=1}^{j} (g_k - 1) = \operatorname{Ker} \prod_{k=1}^{j} (g'_k - 1).$$

Sinon, on peut définir $(g''_k)_{1 \leq k \leq j}$ dans $(G \setminus \{1\})^j$ en prenant $g''_1 = g_1$, $g''_2 = g_2$, g''_k quelconque pour $k > 2$ (c'est possible car $j \geq 2$). On a alors, par ce qui précède,

$$\operatorname{Ker} \prod_{k=1}^{j} (g_k - 1) = \operatorname{Ker} \prod_{k=1}^{j} (g''_k - 1) = \operatorname{Ker} \prod_{k=1}^{j} (g'_k - 1).$$

c.q.f.d.

PROPOSITION. - La hauteur de Q est inférieure ou égale à $r-1$.

Démonstration : Il suffit de montrer que $\prod_{i=1}^{r-1}(h_i - 1)$ annule Q, où h_i est un générateur de H_i pour chaque i. Soit q un élément de Q, et soit $q = \sum_{i=1}^{r} q_i$ sa décomposition dans $\bigoplus_{i=1}^{r} \overline{M_i}$. Comme $(h_i - 1)q_i$ est nul pour tout i, et G commutatif, on a $\prod_{i=1}^{r-1}(h_i-1)(q) = \prod_{i=1}^{r-1}(h_i-1)(q_r)$; c'est un élément de $Q \cap \overline{M_r}$, il doit donc être nul.

c.q.f.d.

PROPOSITION. - La hauteur de Q est inférieure ou égale à $p-1$.

Démonstration : Il suffit de montrer que $(g-1)^{p-1}$ annule Q, pour un $g \in G\backslash\{1\}$. Or, pour tout g de G, et tout i de 1 à r, g agit sur $\overline{M_i}$ (identifié à $\mathbb{F}_p[\zeta]/(\zeta-1)^{p-1}$) comme une puissance de ζ. Donc $(g-1)^{p-1}$ annule $\overline{M_i}$, donc il annule Q.

c.q.f.d.

Pour tout $\mathbb{F}_p[G]$-module N, et tout entier positif j, notons n_j la dimension de $N^{(j)}$ sur $\mathbb{F}_p$. Il est clair que, pour tout $j > 0$, et pour tout g dans $G-\{1\}$, l'endomorphisme $(g-1)$ de N induit un homomorphisme de $N^{(j+1)}$ dans $N^{(j)}$. Si de plus N vérifie la propriété (*), alors $(g-1)$ induit un homomorphisme injectif de $N^{(j+1)}/N^{(j)}$ dans $N^{(j)}/N^{(j-1)}$. On a donc $n_{j+1} - n_j \leq n_j - n_{j-1}$.

PROPOSITION. - Le $\mathbb{F}_p[G]$-module Q vérifie la propriété suivante :

(**) $n_{j+1} - n_j < n_j - n_{j-1}$ pour tout entier j tel que $1 \leq j \leq ht(Q)$.

Démonstration : Notons $\alpha = ht(Q)$. Pour $j = \alpha$, il résulte de

la définition de α que l'on a $n_{\alpha+1} - n_\alpha = 0$, et $n_\alpha - n_{\alpha-1} > 0$. Pour les autres j $(1 \leq j \leq \alpha-1)$, on a déjà $0 < n_\alpha - n_{\alpha-1} \leq n_{j+1} - n_j$; il existe donc un élément q de $Q^{(j+1)}$ qui n'est pas dans $Q^{(j)}$. Soit g un élément de $G\backslash\{1\}$. On va montrer que, pour un certain g' dans $G\backslash\{1\}$, l'image de l'homomorphisme injectif $(g'-1)$ de $Q^{(j+1)}/Q^{(j)}$ dans $Q^{(j)}/Q^{(j-1)}$ ne contient pas l'élément $(g-1)\ (q \bmod Q^{(j)})$. Cela prouvera la proposition.

Par hypothèse, $(g-1)^j(q)$ n'est pas nul. Si on note $q = \sum_{i=1}^{r} q_i$, avec q_i dans $\overline{M_i}$, il existe donc un indice i_o tel que $(g-1)^j(q_{i_o})$ soit non nul. Et comme $Q \cap \overline{M_{i_o}}$ est nul, il existe un deuxième indice i_1 , différent de i_o , tel que $(g-1)^j(q_{i_1})$ soit non nul. Or g ne peut pas être à la fois dans H_{i_o} et dans H_{i_1} ; quitte à intervertir i_o et i_1 , supposons que g n'est pas dans H_{i_o} , et notons g' un générateur de H_{i_o} .

S'il existait un élément q' de $Q^{(j+1)}$ tel que $(g-1)q$ et $(g'-1)q'$ soient congrus modulo $Q^{(j-1)}$, alors on aurait $(g-1)^j(q) = (g-1)^{j-1}(g'-1)(q')$. Donc en regardant les composantes sur $\overline{M_{i_o}}$, cela donnerait $(g-1)^j(q_{i_o}) = (g-1)^{j-1}(g'-1)(q'_{i_o})$. Or $(g-1)^j(q_{i_o})$ est non nul, et $(g'-1)(q'_{i_o})$ est nul, car g' est dans H_{i_o} . On a donc montré que l'homomorphisme injectif $(g'-1)$ de $Q^{(j+1)}/Q^{(j)}$ dans $Q^{(j)}/Q^{(j-1)}$ n'est pas surjectif.

c.q.f.d.

PROPOSITION. - *On a* $n_1 < r$.

Démonstration : Rappelons que $n_1 = \dim_{\mathbb{F}_p} Q^G$. Or Q^G est contenu dans $\bigoplus_{i=1}^{r} \overline{M_i}^G$, qui est de dimension r sur $\mathbb{F}_p$. On a donc $n_1 \leq r$, avec égalité si et seulement si Q^G est égal à $\bigoplus_{i=1}^{r} \overline{M_i}^G$. Mais ce dernier cas est impossible, car $Q^G \cap \overline{M_i}^G$ est nul pour tout i .

c.q.f.d.

IV. ETUDE DES $\mathbb{F}_p[G]$-MODULES Q AYANT AU PLUS 2 GENERATEURS.

1. Q est $\mathbb{F}_p[G]$-monogène.

Notons $\{h,h'\}$ un couple de générateurs de G . Alors $\{(h-1)^i(h'-1)^{i'}\}_{0\le i,i'<p}$ forme une base de $\mathbb{F}_p[G]$ sur $\mathbb{F}_p$, et $(h-1)^i(h'-1)^{i'} = 0$ dès que i ou i' est supérieur à p . Pour tout entier positif α , notons $\mathcal{K}_\alpha$ le sous-$\mathbb{F}_p$-espace vectoriel de $\mathbb{F}_p[G]$ de base $\{(h-1)^i(h'-1)^{i'}\}_{0\le i,i'<p}$. Il est clair que $\mathcal{K}_\alpha$ est un idéal de $\mathbb{F}_p[G]$, que $\mathcal{K}_0 = \mathbb{F}_p[G]$, que $\mathcal{K}_\alpha$ contient $\mathcal{K}_{\alpha+1}$ pour tout α , et que $\mathcal{K}_\alpha = \{0\}$ pour tout $j \ge 2p-1$. Notons enfin R_α le $\mathbb{F}_p[G]$-module monogène $\mathbb{F}_p[G]/\mathcal{K}_\alpha$.

LEMME. - *Pour tout entier positif α , l'idéal $\mathcal{K}_\alpha$ est indépendant du choix du couple de générateurs $\{h,h'\}$ de G . Pour $0 \le \alpha \le 2p-1$, le $\mathbb{F}_p[G]$-module R_α est de hauteur α et vérifie la propriété (*). Pour $0 \le \alpha \le p$, R_α vérifie la propriété (**).*

Démonstration : On voit que le produit $\mathcal{K}_{\alpha_1} \times \mathcal{K}_{\alpha_2}$ est contenu dans $\mathcal{K}_{\alpha_1+\alpha_2}$ pour tous α_1 , α_2 , et que $(g-1)$ est un élément de $\mathcal{K}_1$ pour tout g de $G\setminus\{1\}$. On en déduit que $\prod_{k=1}^{\alpha}(g_k-1)$ appartient à $\mathcal{K}_\alpha$ pour tout α et tout $\{g_k\}_{1\le k\le\alpha} \in (G\setminus\{1\})^\alpha$. Ceci prouve, d'une part que $\mathcal{K}_\alpha$ ne dépend pas du couple de générateurs $\{h,h'\}$ choisi, et d'autre part que R_α est de hauteur au plus égale à α .

Supposons de plus que $0 \le \alpha \le 2p-1$, et posons $i = [\frac{\alpha}{2}]$ (où $[.]$ désigne la partie entière d'un nombre réel), $i' = [\frac{\alpha}{2}]$ si α est impair, et $i' = [\frac{\alpha}{2}]-1$ si α est pair. On a alors $0 \le i,i' < p$ et $i+i' = \alpha-1 < \alpha$, donc $(h-1)^i(h'-1)^{i'}$ n'appartient pas à $\mathcal{K}_\alpha$. On en déduit que la hauteur de R_α est égale à α .

Pour montrer que R_α vérifie (*) , il suffit de vérifier que $(R_\alpha)^H$ est égal à $(R_\alpha)^{H'}$ dès que H et H' sont deux sous-groupes distincts d'ordre p de G . Notons h (resp. h') un générateur de

H (resp. de H') . Alors $\{h,h'\}$ est un couple de générateurs de G . Soit $\lambda = \sum_{0\le i,i'<p} \lambda_{i,i'}(h-1)^i(h'-1)^{i'}$ un élément quelconque de $\mathbb{F}_p[G]$ (les $\lambda_{i,i'}$ étant dans $\mathbb{F}_p$). Alors l'image de λ dans R_α est fixe par H si et seulement si $\sum_{0\le i,i'<p} \lambda_{i,i'}(h-1)^{i+1}(h'-1)^{i'}$ appartient à $\mathfrak{K}_\alpha$, c'est-à-dire si et seulement si λ appartient à $\mathfrak{K}_{\alpha-1}$. On a donc obtenu $(R_\alpha)^H = \mathfrak{K}_{\alpha-1}/\mathfrak{K}_\alpha$, et de même $(R_\alpha)^{H'} = \mathfrak{K}_{\alpha-1}/\mathfrak{K}_\alpha$, donc R_α vérifie (*).

De manière analogue, le noyau de $(h-1)^j$ dans R_α est égal à $\mathfrak{K}_{\alpha-j}/\mathfrak{K}_\alpha$ (pour $0\le j\le\alpha$). Donc n_j est égal à la dimension de $\mathfrak{K}_{\alpha-j}/\mathfrak{K}_\alpha$ sur $\mathbb{F}_p$, c'est-à-dire au nombre de couples d'entiers (i,i') vérifiant $0 \le i,i' < p$ et $\alpha - j \le i+i' < \alpha$. On obtient donc $n_{j+1} - n_j = \inf(\alpha-j,p)$. Ceci prouve que la propriété (**) est vérifiée par R_α si et seulement si $0 \le \alpha \le p$, et qu'on a alors $n_{j+1} - n_j = \alpha - j$ (pour $0 \le j \le \alpha$).

c.q.f.d.

LEMME. - Soit α un entier vérifiant $0 \le \alpha \le p$, et soit R un $\mathbb{F}_p[G]$-module monogène de hauteur α vérifiant (**). Alors R est isomorphe à R_α comme $\mathbb{F}_p[G]$-module (donc R vérifie (*)).

Démonstration : Notons q un générateur de R sur $\mathbb{F}_p[G]$, et $\mathfrak{K}$ le noyau du $\mathbb{F}_p[G]$-homomorphisme surjectif θ de $\mathbb{F}_p[G]$ sur R défini par $\theta(1) = q$. Puisque R est de hauteur α , $\mathfrak{K}$ contient $\mathfrak{K}_\alpha$. Comme on a supposé $0 \le \alpha \le p$, cela prouve que l'on a :

(1) $\dim_{\mathbb{F}_p} \mathfrak{K} \ge p^2 - \frac{\alpha(\alpha+1)}{2}$.

Puisque de plus R vérifie (**), on a $n_{j+1} - n_j \ge \alpha - j$ pour tout j de 0 à $\alpha - 1$, et la somme de ces inégalités donne :

(2) $\dim_{\mathbb{F}_p} R \ge \frac{\alpha(\alpha+1)}{2}$.

Comme on doit avoir $\dim_{\mathbb{F}_p} \mathfrak{K} + \dim_{\mathbb{F}_p} R = \dim_{\mathbb{F}_p} \mathbb{F}_p[G] = p^2$, on

voit que les inégalités (1) et (2) sont des égalités ; donc $\aleph$ est égal à $\aleph_\alpha$, et R est $\mathbb{F}_p[G]$-isomorphe à R_α .

c.q.f.d.

Pour tout entier i de 1 à r , tout générateur γ_i de G/H_i , et tout j dans $\mathbb{N}$, le noyau de $(\gamma_i - 1)^j$ dans $\overline{M_i}$ est égal à $\overline{M_i}^{(j)}$. La hauteur de $\overline{M_i}$ est égale à $p-1$, et l'on a $\overline{M_i}^{(j+1)}/\overline{M_i}^{(j)} \simeq \mathbb{F}_p$ pour $0 \leq j \leq p-2$.

Pour tout élément q_i de $\overline{M_i}$, on définit la <u>hauteur</u> de q_i comme le plus petit entier j de $\mathbb{N}$ tel que q_i appartienne à $\overline{M_i}^{(j)}$.

PROPOSITION. - <u>Soit</u> $q = \sum_{i=1}^{r} q_i$ <u>un élément de</u> $\bigoplus_{i=1}^{r} \overline{M_i}$. <u>On note</u> $\alpha_i = ht(q_i)$, $\alpha = \operatorname{Max}_{1 \leq i \leq r} \alpha_i$, <u>et</u> $Q = \mathbb{F}_p[G].q$. <u>Alors</u> $Q \cap \overline{M_i}$ <u>est nul pour tout</u> i <u>de</u> 1 <u>à</u> r <u>si et seulement si le nombre d'indices</u> i <u>tels que</u> $\alpha_i = \alpha$ <u>est strictement supérieur à</u> α . <u>Si ces conditions sont réalisées, alors</u> Q <u>est</u> $\mathbb{F}_p[G]$-<u>isomorphe à</u> R_α .

<u>Démonstration</u> :

a) Supposons que $Q \cap \overline{M_i}$ soit nul pour tout i ; alors Q est de hauteur α , et (par III) Q vérifie (*) et (**). Donc par le lemme qui précède, Q est $\mathbb{F}_p[G]$-isomorphe à R_α .

Supposons de plus que le nombre des indices i tels que $\alpha_i = \alpha$ soit inférieur ou égal à α . Quitte à modifier la numérotation, on peut alors supposer que l'on a $\alpha_i \leq \alpha - 1$ pour tout $i > \alpha$. Mais alors, si h_j désigne un générateur de H_j pour tout j , on a $\prod_{j=2}^{\alpha} (h_j - 1)(q_i) = 0$ pour tout $i \neq 1$; en effet, pour $2 \leq i \leq \alpha$, cela vient du fait que G est commutatif et que $(h_i - 1)(q_i)$ est nul ; et pour $i > \alpha$, cela vient du fait que α_i est inférieur à $\alpha - 1$. Donc $\prod_{j=2}^{\alpha} (h_j - 1)(q) = \prod_{j=2}^{\alpha} (h_j - 1)(q_1)$, et c'est un élément de $Q \cap \overline{M_1}$; donc il est nul, et Q est égal à

$Q^{(\alpha-1)}$. Mais on a montré que $ht(Q) = \alpha$, donc ceci est impossible.

b) Supposons maintenant que le nombre des i tels que $\alpha_i = \alpha$ soit strictement supérieur à α , et soit i_o un indice quelconque $(0 \leq i_o \leq r)$. Quitte à modifier la numérotation, on peut supposer que $\alpha_i = \alpha$ pour $1 \leq i \leq \alpha+1$, et $i_o \geq \alpha+1$. Pour montrer que $Q \cap \overline{M_{i_o}}$ est nul, il suffit de montrer que, si λ est un élément de $\mathbb{F}_p[G]$ tel que λq_i soit nul pour tout i de 1 à α , alors λq_{i_o} est nul.

Pour tout i de 1 à α , notons h_i un générateur de H_i , et h_i' un élément de $G \backslash H_i$. Alors $\{(h_i-1)^j(h_i'-1)^k\}_{0\leq j,k<p}$ forme une base $\mathcal{B}_i$ de $\mathbb{F}_p[G]$ sur $\mathbb{F}_p$ (pour chaque i).

Nous allons montrer, par récurrence sur ℓ , que λ vérifie, pour tout ℓ de 1 à $\alpha+1$, la propriété suivante :

(P_ℓ) Il existe un élément λ_ℓ de $\mathbb{F}_p[G]$ tel que $\lambda \equiv \prod_{i=1}^{\ell-1} (h_i-1)\lambda_\ell$ (mod $\mathcal{K}_\alpha$).

La propriété (P_1) s'écrit $\lambda \equiv \lambda_1 \pmod{\mathcal{K}_\alpha}$, donc elle est vérifiée en prenant $\lambda_1 = \lambda$. Supposons (P_ℓ) vérifiée, avec $1 \leq \ell \leq \alpha$, et décomposons λ_ℓ dans la base $\mathcal{B}_\ell$ de $\mathbb{F}_p[G]$ sur $\mathbb{F}_p$; soit $\lambda_\ell = \sum_{0\leq j,k<p} \lambda_{\ell,j,k}(h_\ell-1)^j(h_\ell'-1)^k$ cette décomposition. L'hypothèse $\lambda.q_\ell = 0$ s'écrit donc : $\prod_{i=1}^{\ell-1}(h_i-1) \sum_{0\leq k<\alpha-\ell+1} \lambda_{\ell,0,k}(h_\ell'-1)^k q_\ell = 0$ (car $(h_\ell-1)$ annule q_ℓ , ainsi que $\left(\prod_{i=1}^{\ell-1}(h_i-1)\right)(h_\ell'-1)^{\alpha-\ell+1}$). Or les éléments $\left\{\left(\prod_{i=1}^{\ell-1}(h_i-1)\right)(h_\ell'-1)^k q_\ell\right\}_{0\leq k<\alpha-\ell+1}$ sont $\mathbb{F}_p$-linéairement indépendants dans $\overline{M_\ell}$, car $ht(q_\ell) = \alpha$. Donc $\lambda_{\ell,0,k}$ est nul pour $0 \leq k < \alpha-\ell+1$, et l'on a $\lambda \equiv \prod_{i=1}^{\ell}(h_i-1)\lambda_{\ell+1} \pmod{\mathcal{K}_\alpha}$, pour un $\lambda_{\ell+1}$ dans $\mathbb{F}_p[G]$. Autrement dit, la propriété $(P_{\ell+1})$ est vérifiée.

On a donc montré en particulier que la propriété $(P_{\alpha+1})$ est vérifiée, or cette propriété signifie que λ est dans $\mathcal{K}_\alpha$. Mais alors λq_{i_o} est nul, car $\alpha_{i_o} \leq \alpha$.

c.q.f.d.

COROLLAIRE. - Soit Q un sous-$\mathbb{F}_p[G]$-module de $\bigoplus_{i=1}^{r} \overline{M_i}$, tel que $Q \cap \overline{M_i}$ soit nul pour tout i de 1 à r. Si Q est $\mathbb{F}_p[G]$-monogène, sa classe modulo $\prod_{i=1}^{r} \mathrm{Aut}_{\mathbb{F}_p[G]}\overline{M_i}$ est déterminée de manière unique par la donnée d'un r-uple $(\alpha_i)_{1\leq i\leq r}$ dans $\mathbb{N}^r$ vérifiant, si on note $\alpha = \underset{1\leq i\leq r}{\mathrm{Max}}\ \alpha_i$, les deux propriétés suivantes :

- $\alpha \leq \inf(r-1, p-1)$;
- le nombre des indices i tels que α_i soit égal à α est strictement supérieur à α.

Démonstration : C'est une conséquence immédiate de la proposition précédente, en prenant pour α_i la hauteur de la composante sur $\overline{M_i}$ d'un générateur de Q, et en utilisant le fait que $\overline{M_i}^{(j)} \setminus \overline{M_i}^{(j-1)}$ forme une seule orbite sous l'action de $\mathrm{Aut}_{\mathbb{F}_p[G]}\overline{M_i}$, pour tout j dans $\mathbb{N}$.

c.q.f.d.

2. Q a deux générateurs sur $\mathbb{F}_p[G]$.

On montre seulement le résultat suivant :

LEMME. - Soit α un entier vérifiant $0 \leq \alpha \leq p$, et soit R un $\mathbb{F}_p[G]$-module de hauteur α admettant deux générateurs et vérifiant (*) et (**). Alors tout sous-$\mathbb{F}_p[G]$-module de R vérifie (*). Si l'on suppose de plus que tout sous-$\mathbb{F}_p[G]$-module de R vérifie (**), alors R est de la forme $R' + R''$, avec $R' \simeq R_\alpha$, $R'' \simeq R_\beta$, $R' \cap R'' \simeq R_\gamma$, et $0 \leq \gamma \leq \beta \leq \alpha$. De plus, les nombres β et γ sont déterminés de manière unique par R.

Démonstration : Si R vérifie (*) , et si $ht(R) = \alpha$, il est clair que tout sous-$\mathbb{F}_p[G]$-module de R vérifie (*) , et est de hauteur inférieure à α .

Notons $\{q',q''\}$ un système générateur de R sur $\mathbb{F}_p[G]$; notons $R' = \mathbb{F}_p[G]q'$ et $R'' = \mathbb{F}_p[G]q''$. Puisque R' et R'' vérifient (*), (**), et $ht(R')$ (resp. $ht(R'')$) $\leq \alpha \leq p$, d'après (IV,1) il existe deux entiers α' et α'' vérifiant : $0 \leq \alpha',\alpha'' \leq \alpha$, $R' \simeq R_{\alpha'}$, et $R'' \simeq R_{\alpha''}$. De plus, on a $R = R' + R''$, donc $Max(\alpha',\alpha'') = \alpha$. Quitte à modifier les notations, supposons que $\alpha' = \alpha$, et notons $\alpha'' = \beta$; on a donc $0 \leq \beta \leq \alpha$.

Notons γ le plus petit entier tel que $R' \cap R''$ soit contenu dans $R^{(\gamma)}$ (donc $\gamma \leq \beta$) ; il existe alors un élément q''' de $R' \cap R'' \cap R^{(\gamma)}$, tel que q''' n'appartienne pas à $R^{(\gamma-1)}$. D'après (IV,1) on a alors (en notant $R''' = \mathbb{F}_p[G]q'''$) $R''' \simeq R_\gamma$. Et bien sûr $R''' \subset R' \cap R''$. Il reste à montrer que $R''' = R' \cap R''$, et que β et γ sont déterminés par R .

Notons $\delta_j = (n_j - n_{j-1}) - (n_{j+1} - n_j)$ pour tout j de 1 à α . On a $\delta_j \geq 1$ pour tout j de 1 à α , par la propriété (**). D'autre part, on doit avoir $\delta_j = 1$ pour $\beta < j \leq \alpha$; $\delta_j = 2$ pour $\gamma < j \leq \beta$; et $\delta_j \leq 1$ pour $1 \leq j \leq \gamma$. On en déduit que $\delta_j = 1$ pour $1 \leq j \leq \gamma$, donc que R''' est égal à $R' \cap R''$, et que β et γ sont déterminés par la suite des δ_j , donc par la donnée de R .

c.q.f.d.

Remarque : Soit Q un sous-$\mathbb{F}_p[G]$-module de $\bigoplus_{i=1}^{r} \overline{M_i}$, tel que $Q \cap \overline{M_i}$ soit nul. Alors tout sous-$\mathbb{F}_p[G]$-module Q' de Q est un sous-$\mathbb{F}_p[G]$-module de $\bigoplus_{i=1}^{r} \overline{M_i}$ tel que $Q' \cap \overline{M_i}$ soit nul. Donc (par III) Q' vérifie (**).

3. Application.

Nous sommes maintenant en mesure d'énumérer les structures de $\mathbb{F}_p[G]$-modules possibles pour Q lorsque $r \in \{2,3,4\}$. Elles sont données par le tableau suivant :

r	α	$(n_j - n_{j-1})_{1\le j\le\alpha}$	structure de Q sur $\mathbb{F}_p[G]$
2	0	ϕ	0
	1	(1)	$\mathbb{F}_p$
3	0	ϕ	0
	1	(1)	$\mathbb{F}_p$
		(2)	$\mathbb{F}_p^2$
	2 (sip≥ 3)	(2,1)	R_2
4 (sip≥ 3)	0	ϕ	0
	1	(1)	$\mathbb{F}_p$
		(2)	$\mathbb{F}_p^2$
		(3)	$\mathbb{F}_p^3$
	2	(2,1)	R_2
		(3,1)	$R_2 \oplus \mathbb{F}_p$
		(3,2)	$R_2 + R_2'$ avec $R_2' \simeq R_2$ et $R_2 \cap R_2' \simeq \mathbb{F}_p$
	3 (sip≥ 5)	(3,2,1)	R_3

Le seul point non évident dans ce tableau est le fait que, pour des entiers $(r,\alpha,(n_j-n_{j-1})_{1\le j\le\alpha})$ convenables, la seule structure possible pour Q sur $\mathbb{F}_p[G]$ est celle qui est indiquée. Regardons par exemple le cas où $r = 4$, $\alpha = 2$, $n_1 = 3$, $n_2 - n_1 = 2$ (les autres cas se traitent de manière analogue).

Soit Q un sous-$\mathbb{F}_p[G]$-module de $\bigoplus_{i=1}^{r} \overline{M}_i$ tel que $Q \cap \overline{M}_i$ soit nul pour tout i , et tel que Q corresponde à ces données. Soit q'

un élément de $Q^{(2)} \setminus Q^{(1)}$ (q' existe car $n_2 > n_1$) . Notons $Q' = \mathbb{F}_p[G]q'$. Alors Q' est un sous-$\mathbb{F}_p[G]$-module de Q , et Q' est isomorphe à R_2 d'après (IV,1). Considérons maintenant le sous-espace $Q^{(1)} + Q'^{(2)}$ de $Q^{(2)}$; comme $\dim_{\mathbb{F}_p} Q^{(1)} = 3$ et $\dim_{\mathbb{F}_p} Q'^{(2)} = 3$, et comme $Q^{(1)} \cap Q'^{(2)} = Q'^{(1)}$ est de dimension 2 sur $\mathbb{F}_p$, on obtient $\dim_{\mathbb{F}_p} (Q^{(1)} + Q'^{(2)}) = 4$, alors que $\dim_{\mathbb{F}_p} Q^{(2)} = 5$. Il existe donc un élément q'' de $Q^{(2)} \setminus (Q^{(1)} + Q'^{(2)})$. Notons $Q'' = \mathbb{F}_p[G]q''$. Alors Q'' est un sous-$\mathbb{F}_p[G]$-module de Q , et Q'' est isomorphe à R_2 d'après (IV,1). De plus, Q' et Q'' sont distincts. D'après (IV,2), l'intersection de Q' et Q'' est de la forme R_γ avec $\gamma \in \{0,1,2\}$. Si $\gamma = 0$, alors $Q' + Q'' = Q' \oplus Q''$, et $\dim_{\mathbb{F}_p} (Q'+Q'')^{(1)} = 4$; ceci est impossible, puisque $(Q'+Q'')^{(1)}$ est contenu dans $Q^{(1)}$ qui est de dimension 3 . Si $\gamma = 2$, alors les dimensions de $Q' \cap Q''$, Q' , Q'' (sur $\mathbb{F}_p$) sont les mêmes, donc $Q' \cap Q'' = Q' = Q''$, ce qui est contraire à la construction de Q' et Q'' . On a donc $\gamma = 1$, et $\dim_{\mathbb{F}_p} (Q'+Q'') = 5 = \dim_{\mathbb{F}_p} Q$, donc $Q' + Q''$ est égal à Q .

Remarque : Soit une famille d'entiers $\{r, \alpha, (n_j)_{1 \le j \le \alpha}\}$ vérifiant $r \le p+1$, $\alpha \le \inf(r-1, p-1)$, et

$$0 < n_\alpha - n_{\alpha-1} < \ldots < n_{j+1} - n_j < n_j - n_{j-1} < \ldots < n_2 - n_1 < n_1 < r .$$

Considérons les problèmes suivants : existe-t-il un sous-$\mathbb{F}_p[G]$-module Q de $\bigoplus_{i=1}^{r} \overline{M}_i$, tel que $Q \cap \overline{M}_i$ soit nul pour tout i , de hauteur α , et tel que n_j soit égal à $\dim_{\mathbb{F}_p} Q^{(j)}$ pour tout j de 1 à α ? Si un tel module Q existe, est-il unique à $\mathbb{F}_p[G]$-isomorphisme près ?

On verra en VI qu'un tel module Q existe lorsque $r \le 4$, et on peut sans doute montrer que c'est encore vrai pour $r \ge 5$.

D'autre part, le tableau ci-dessus montre qu'un tel Q est unique à $\mathbb{F}_p[G]$-isomorphisme près lorsque $r \le 4$. Il est facile de montrer que ce n'est plus vrai pour $r \ge 5$. Prenons par exemple $r \ge 5$, $\alpha = 2$,

$n_1 = 4$, $n_2 - n_1 = 2$; on peut alors avoir pour Q , à $\mathbb{F}_p[G]$-isomorphisme près :

- ou bien $R_2 \oplus R_2'$, avec $R_2' \simeq R_2$;
- ou bien $(R_2 + R_2') \oplus \mathbb{F}_p$, avec $R_2' \simeq R_2$ et $R_2 \cap R_2' \simeq \mathbb{F}_p$.

V. ETUDE DES $\mathbb{F}_p[G]$-MODULES Q DE HAUTEUR 1 OU 2 .

1. Q est de hauteur 1 .

Autrement dit, Q est fixe par G et non nul, ou encore Q est $\mathbb{F}_p[G]$-isomorphe à $\mathbb{F}_p^n$, avec $1 \leq n < r$ (cf. III).

LEMME. - Soit n un entier tel que $1 \leq n < r$. Le nombre de classes, modulo $\prod_{i=1}^{r} U_i$, des sous-$\mathbb{F}_p[G]$-modules Q de $\bigoplus_{i=1}^{r} \overline{M}_i$ tels que $Q \cap \overline{M}_i$ soit nul pour tout i de 1 à r , et tels que Q soit fixe par G et de dimension n sur $\mathbb{F}_p$, est égal au nombre de classes de matrices à n lignes et r colonnes, à coefficients dans $\mathbb{F}_p$, dont toutes les matrices extraites à n lignes et $(r-1)$ colonnes sont de rang n , modulo l'action de $GL_n(\mathbb{F}_p)$ à gauche et de $\mathrm{Diag}_r^*(\mathbb{F}_p)$ à droite.

(On note $\mathrm{Diag}_r^*(\mathbb{F}_p)$ le groupe des matrices carrées d'ordre r , diagonales, inversibles, à coefficients dans $\mathbb{F}_p$).

Notons $N_{p,r,n}$ ce nombre.

Démonstration : Par hypothèse, Q est contenu dans $\bigoplus_{i=1}^{r} \overline{M}_i^G$. Or $\overline{M}_i^G$ est un $\mathbb{F}_p$-espace vectoriel de dimension 1 (pour tout i). Notons $\{m_i\}$ une base de $\overline{M}_i^G$ sur $\mathbb{F}_p$ pour chaque i . Soit V un sous-espace vectoriel de $\bigoplus_{i=1}^{r} \overline{M}_i^G$ de dimension n . En associant à toute base $\mathcal{B}$ de V sur $\mathbb{F}_p$ la matrice A de $\mathcal{M}_{n,r}(\mathbb{F}_p)$

(matrices à n lignes et r colonnes à coefficients dans $\mathbb{F}_p$) dont la $j^{\text{ème}}$ ligne est formée des coordonnées du $j^{\text{ème}}$ vecteur de $\mathcal{B}$ dans la base $\{m_1, m_2, \ldots, m_r\}$ de $\bigoplus_{i=1}^{r} \overline{M_i}^G$, on voit que la donnée de V correspond à la donnée d'une classe, modulo $GL_n(\mathbb{F}_p)$, de matrices de $\mathcal{M}_{n,r}(\mathbb{F}_p)$ de rang n.

Dire que $V \cap \overline{M_i}^G$ est nul équivaut à dire que le $\mathbb{F}_p$-espace vectoriel $V + \overline{M_i}^G$ est de dimension $n+1$, ou encore que la matrice obtenue en ajoutant à A la ligne $(0,0,\ldots,0,1,0,\ldots,0)$ (où le coefficient 1 est dans la i^e colonne) est de rang $(n+1)$. Il est clair que ceci équivaut à dire que la matrice obtenue en enlevant à A sa $i^{\text{ème}}$ colonne est de rang n.

Enfin, U_i agit sur $\overline{M_i}^G$ comme $\mathbb{F}_p^*$, donc les classes de Q modulo $\overline{\prod_{i=1}^{r} U_i}$ correspondent aux classes de matrices modulo $GL_n(\mathbb{F}_p)$ et $\mathrm{Diag}_r^*(\mathbb{F}_p)$.

c.q.f.d.

On va mainteant calculer $N_{p,r,n}$, où r et n sont deux entiers vérifiant $n < r \leq p+1$. On aura besoin pour cela des notations suivantes : pour tout couple (r,n) d'entiers vérifiant $n < r$, on note $\mathcal{E}_{r,n}$ l'ensemble des familles $\mathcal{J} = \{I_j\}_{1 \leq j \leq r-n}$, où I_j est un sous-ensemble non vide de $\{1,2,\ldots,n\}$ pour chaque j, et où la réunion des I_j $(1 \leq j \leq r-n)$ est égale à $\{1,2,\ldots,n\}$.

Pour tout élément $\mathcal{J} = \{I_j\}_{1 \leq j \leq r-n}$ de $\mathcal{E}_{r,n}$, on note $c(\mathcal{J}) = \sum_{j=1}^{r-n} \mathrm{Card}(I_j)$, et $\mathfrak{L}(\mathcal{J}) = \sum_{\ell_2=1}^{\ell_2(\mathcal{J})} \sum_{\ell_3=\ell_2}^{\ell_3(\mathcal{J})} \cdots \sum_{\ell_n=\ell_{n-1}}^{\ell_n(\mathcal{J})} 1$, où $\ell_{k+1}(\mathcal{J})$ désigne le plus petit entier j tel que I_j ne soit pas contenu dans $\{1,2,\ldots,k\}$ (pour tout k de 1 à $n-1$). Enfin, on définit une relation d'équivalence (notée $\sim$) sur l'ensemble des éléments de $\mathcal{J}$ par : $I_j \sim I_{j'}$, s'il existe une suite d'indices $j_o = j, j_1, \ldots, j_\ell = j'$, tels que $I_{j_{i-1}} \cap I_{j_i}$ soit non vide pour tout i de 1 à ℓ ; et on note

$\nu(\mathfrak{J})$ le nombre de classes pour la relation $\sim$ dans $\mathfrak{J}$.

On peut alors énoncer :

PROPOSITION. - Le nombre $N_{p,r,n}$ est égal à $\sum_{s=n+1}^{r} \binom{r}{s} N'_{p,s,n}$, où $N'_{p,s,n}$ est défini par

$$N'_{p,s,n} = \sum_{\mathfrak{J} \in \mathcal{C}_{s,n}} \ell(\mathfrak{J})(p-1)^{c(\mathfrak{J})+\nu(\mathfrak{J})-s} .$$

Démonstration (faite avec l'aide de Claude Moser) : Si $N''_{p,s,n}$ désigne le nombre de classes de matrices de $\mathcal{M}_{n,s}(\mathbb{F}_p)$, dont tous les vecteurs colonnes sont non nuls, et dont toutes les matrices extraites à n lignes et $(s-1)$ colonnes sont de rang n , modulo l'action de $GL_n(\mathbb{F}_p)$ à gauche et de $\mathrm{Diag}_s^*(\mathbb{F}_p)$ à droite, alors il est clair que l'on a

$$N_{p,r,n} = \sum_{s=n+1}^{r} \binom{r}{s} N''_{p,s,n} .$$

Il suffit donc de montrer que $N''_{p,s,n} = N'_{p,s,n}$, pour tous les triplets (p,s,n) convenables.

Soit A une matrice de $\mathcal{M}_{n,s}(\mathbb{F}_p)$; notons A_j le $j^{\text{ème}}$ vecteur colonne de A $(1 \le j \le s)$, et supposons que A_j est non nul pour tout j , et que le rang de $(A_j)_{\substack{1 \le j \le s \\ j \ne j_o}}$ est égal à n pour tout j_o . Définissons la permutation σ_A de $\{1,2,\dots,s\}$ de la manière suivante : $\sigma_A(1) = 1$, $\sigma_A(k)$ = le plus petit entier j tel que A_j n'appartienne pas à $\sum_{i=1}^{k-1} \mathbb{F}_p A_{\sigma_A(i)}$ (pour $2 \le k \le n$) , puis $\sigma_A(n+1) < \sigma_A(n+2) < \dots < \sigma_A(s)$ (l'existence de σ_A est due au fait que A est de rang n). Par construction, la matrice $\left(A_{\sigma_A(j)}\right)_{1 \le j \le n}$ est inversible ; notons Λ_A son inverse (c'est donc un élément de $GL_n(\mathbb{F}_p)$). Il est alors clair que la matrice $\Lambda_A \circ A$ est indépendante du choix de A modulo $GL_n(\mathbb{F}_p)$, et détermine de manière unique la classe de A modulo $GL_n(\mathbb{F}_p)$.

D'autre part, notons P_A la matrice de permutation d'ordre s correspondant à σ_A ; c'est-à-dire que P_A est définie par

$A \circ P_A = \left(A_{\sigma_A(j)}\right)_{1\le j\le s}$. La matrice $\Lambda_A \circ A \circ P_A$ est de la forme $(I_n A')$, où A' est un élément de $\mathcal{M}_{n,s-n}(\mathbb{F}_p)$. Et les hypothèses faites sur A sont équivalentes au fait que chaque colonne et chaque ligne de A' est non nulle.

Etant donnée une telle matrice A' , notons $a'_{i,j}$ ses coefficients $(1\le i\le n\ ,\ 1\le j\le s-n)$, et $I_{A',j}$ l'ensemble des indices i tels que $a'_{i,j}$ soit non nul (pour tout j de 1 à $s-n$). Il est alors clair que la famille $\mathcal{I}_{A'} = \{I_{A',j}\}_{1\le j\le s-n}$ est un élément de $\mathcal{E}_{s,n}$, et que le nombre de classes modulo $GL_n(\mathbb{F}_p)$ de matrices A "convenables" donnant la matrice $(I_n A')$ par le procédé décrit ci-dessus est égal à $\mathcal{L}(\mathcal{I}_{A'})$.

Soient maintenant A et B deux matrices de $\mathcal{M}_{n,s}(\mathbb{F}_p)$ "convenables", congrues modulo $GL_n(\mathbb{F}_p)$ et $Diag^*_s(\mathbb{F}_p)$. Alors P_A et P_B sont égales, et les matrices $(I_n A')$ et $(I_n B')$ correspondantes sont congrues modulo $GL_n(\mathbb{F}_p)$ et $Diag^*_s(\mathbb{F}_p)$, ce qui équivaut à dire que les matrices A' et B' sont congrues modulo $Diag^*_n(\mathbb{F}_p)$ à gauche, et $Diag^*_{s-n}(\mathbb{F}_p)$ à droite.

Or, étant donnée une matrice $A' = (a'_{i,j})_{\substack{1\le i\le n\\ 1\le j\le s-n}}$ de $\mathcal{M}_{n,s-n}(\mathbb{F}_p)$, dont toutes les lignes et toutes les colonnes sont non nulles, le nombre de matrices B' du même type, qui sont congrues à A' modulo $Diag^*_n(\mathbb{F}_p)$ à gauche et $Diag^*_{s-n}(\mathbb{F}_p)$ à droite, est égal à $(p-1)^{n+(s-n)}/C_{A'}$, où $C_{A'}$ est le cardinal de

$$\left\{(\lambda_i,\mu_j)_{\substack{1\le i\le n\\ 1\le i\le s-n}} \in (\mathbb{F}_p^*)^{n+(s-n)} / \forall i,\forall j,\ a'_{ij}(\lambda_i^{-1}\mu_j - 1) = 0\right\} .$$

Il est facile de voir que $C_{A'} = (p-1)^{\nu(\mathcal{I}_{A'})}$, donc le nombre des matrices B' cherchées est égal à $(p-1)^{s-\nu(\mathcal{I}_{A'})}$.

Enfin, étant donné un $\mathcal{I}$ dans $\mathcal{E}_{s,n}$, le nombre de matrices A' (comme ci-dessus) telles que $\mathcal{I}_{A'}$ soit égal à $\mathcal{I}$ est bien sûr égal à $(p-1)^{C(\mathcal{I})}$. On a donc obtenu

$$N''_{p,s,n} = \sum_{\mathcal{I}\in\mathcal{E}_{s,n}} (p-1)^{C(\mathcal{I})}\mathcal{L}(\mathcal{I})/(p-1)^{s-\nu(\mathcal{I})} ,$$

c'est-à-dire $N''_{p,s,n} = N'_{p,s,n}$.

c.q.f.d.

Exemples :

$$N'_{p,s,1} = 1 \quad (\text{pour } 1 < s \leq p+1) .$$

$$N'_{p,s,2} = \left(\sum_{\ell=1}^{s-2} \ell\, 2^{s-2-\ell} \right) - 1 + \sum_{k=1}^{s-2} (p-1)^{k-1} \left(s-1-k + \sum_{\ell=1}^{s-2-k} \ell . 2^{s-2-\ell-k} \left(2 \binom{s-2-\ell}{k-1} + \binom{s-2-\ell}{k} \right) \right)$$

(pour $2 < s \leq p+1$) .

$$N'_{p,n+1,n} = 1 \quad (\text{pour } n \leq p) .$$

2. Q est de hauteur 2 .

Dans ce cas, Q est une extension, sur $\mathbb{F}_p[G]$, de Q/Q^G par Q^G ; et Q/Q^G est fixe par G et non nul. De plus, cette extension est une "sous-extension" de l'extension

$$0 \longrightarrow \bigoplus_{i=1}^{r} \overline{M}_i(1) \longrightarrow \bigoplus_{i=1}^{r} \overline{M}_i(2) \longrightarrow \bigoplus_{i=1}^{r} \overline{M}_i(2)/\overline{M}_i(1) \longrightarrow 0 ,$$

au sens suivant : le diagramme de $\mathbb{F}_p[G]$-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q^G & \longrightarrow & Q & \longrightarrow & Q/Q^G & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \bigoplus_{i=1}^{r} \overline{M}_i(1) & \longrightarrow & \bigoplus_{i=1}^{r} \overline{M}_i(2) & \longrightarrow & \bigoplus_{i=1}^{r} \overline{M}_i(2)/\overline{M}_i(1) & \longrightarrow & 0 \end{array}$$

est commutatif, et ses lignes sont exactes (les inclusions "verticales" sont induites par l'injection de Q dans $\bigoplus_{i=1}^{r} \overline{M}_i$).

Notons maintenant $0 \longrightarrow Y_1 \xrightarrow{i} Y \xrightarrow{j} Y_2 \longrightarrow 0$ une suite exacte de $\mathbb{F}_p$-espaces vectoriels de dimension finie, et s une section fixée de j . On identifiera Y_1 et son image $i(Y_1)$ dans Y .

Soit X un sous-$\mathbb{F}_p$-espace vectoriel de Y . Notons X_1 (resp. X_2)

les sous-$\mathbb{F}_p$-espace vectoriel de Y_1 (resp. Y_2) égal à $X \cap Y_1$ (resp. à $j(X)$). Alors le diagramme suivant de $\mathbb{F}_p$-espaces vectoriels est commutatif, et ses lignes sont exactes :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X_1 & \longrightarrow & X & \xrightarrow{j|_X} & X_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i_2} & & \\ 0 & \longrightarrow & Y_1 & \longrightarrow & Y & \xrightarrow{j} & Y_2 & \longrightarrow & 0 \ . \end{array}$$

Notons s_X une section quelconque de $j|_X$ (donc $s_X : X_2 \to X$), et k_X un $\mathbb{F}_p$-homomorphisme quelconque de Y_2 dans Y_1 dont la restriction à X_2 soit égale à $s|_{X_2} - s_X$. Enfin, pour tout couple (Y'_1, Y'_2) où Y'_1 (resp. Y'_2) est un sous-$\mathbb{F}_p$-espace vectoriel de Y_1 (resp. Y_2), désignons par $\underset{Y'_1,Y'_2}{\sim}$ la relation d'équivalence sur $\mathrm{Hom}_{\mathbb{F}_p}(Y_2, Y_1)$ définie par : $k \underset{Y'_1,Y'_2}{\sim} k'$ si et seulement si $(k-k')(Y'_2) \subset Y'_1$. Et notons $\overline{k_X}$ la classe de k_X modulo $\underset{Y'_1,Y'_2}{\sim}$.

LEMME 1. - *L'application* Φ *définie par* $\Phi(X) = (X_1, X_2, \overline{k_X})$, *est une bijection entre l'ensemble des sous-*$\mathbb{F}_p$*-espaces vectoriels de* Y *et l'ensemble des triplets* $(Y'_1, Y'_2, \bar{k})$, *où* Y'_1 (resp. Y'_2) *est un sous-*$\mathbb{F}_p$*-espace vectoriel de* Y_1 (resp. Y_2), *et* $\bar{k}$ *une classe de* $\mathrm{Hom}_{\mathbb{F}_p}(Y_2, Y_1)$ *modulo* $\underset{Y'_1,Y'_2}{\sim}$.

L'application réciproque Φ^{-1} *est définie par*

$\Phi^{-1}(Y'_1, Y'_2, \bar{k}) = Y'_1 \oplus (s-k)Y'_2$,

où k *est un représentant quelconque de* $\bar{k}$ *dans* $\mathrm{Hom}_{\mathbb{F}_p}(Y_2, Y_1)$.

Démonstration : La démonstration de ce lemme est faite d'une suite de vérifications faciles ; vérifier que Φ et Φ^{-1} sont deux applications bien définies, c'est-à-dire que $\overline{k_X}$ ne dépend pas du choix de s_X ni de celui de k_X, que $Y'_1 \cap (s-k)Y'_2$ est nul dans Y' et que $Y'_1 \oplus (s-k)Y'_2$ ne dépend pas du choix de k ; puis vérifier que $\Phi^{-1} \circ \Phi(X) = X$, et que $\Phi \circ \Phi^{-1}(Y'_1, Y'_2, \bar{k}) = (Y'_1, Y'_2, \bar{k})$.

c.q.f.d.

Soit maintenant f un $\mathbb{F}_p$-automorphisme de Y laissant stable Y_1 (c'est-à-dire tel que $f(Y_1) \subset Y_1$). Alors f induit un $\mathbb{F}_p$-automorphisme f_1 (resp. f_2) de Y_1 (resp. Y_2) ; si y_1 est dans Y_1 , alors $f_1(y_1) = f(y_1)$; et si y_2 est dans Y_2 , alors $f_2(y_2) = j \circ f \circ s(y_2)$. Notons enfin h_f le $\mathbb{F}_p$-homomorphisme de Y_2 dans Y_1 égal à $s - f \circ s \circ f_2^{-1}$.

LEMME 2. - L'application ψ définie par $\psi(f) = (f_1, f_2, h_f)$, est une bijection entre l'ensemble des $\mathbb{F}_p$-automorphismes de Y laissant Y_1 stable, et l'ensemble des triplets (f_1, f_2, h) où f_1 (resp. f_2) est un $\mathbb{F}_p$-automorphisme de Y_1 (resp. Y_2) , et h un $\mathbb{F}_p$-homomorphisme de Y_2 dans Y_1 .

L'application réciproque ψ^{-1} est définie par

$$(\psi^{-1}(f_1, f_2, h))(y_1 + s(y_2)) = f_1(y_1) + (s-h)(f_2(y_2)) ,$$

où y_1 (resp. y_2) est un élément quelconque de Y_1 (resp. Y_2) .

Démonstration : Il suffit de vérifier que $\psi^{-1}(f_1, f_2, h)$ est bien un $\mathbb{F}_p$-automorphisme de Y , puis que ψ et ψ^{-1} sont des applications réciproques l'une de l'autre.

c.q.f.d.

LEMME 3. - Soient X, X' deux sous-$\mathbb{F}_p$-espaces vectoriels de Y , et f un $\mathbb{F}_p$-automorphisme de Y laissant Y_1 stable. Notons $\Phi(X) = (X_1, X_2, \bar{k})$, $\Phi(X') = (X'_1, X'_2, \overline{k'})$, et $\psi(f) = (f_1, f_2, h)$. On a alors $f(X) = X'$ si et seulement si $f_1(X_1) = X'_1$, $f_2(X_2) = X'_2$, et $(f_1 \circ k - k' \circ f_2 + h \circ f_2)(X_2) \subset X'_1$.

Démonstration : Si $f(X) = X'$, alors $f(X \cap Y_1) = X' \cap Y_1$, autrement dit $f(X_1) = X'_1$; et $j \circ f \circ s(X_2)$ est contenu dans $j \circ f(X) = j(X') = X'_2$, de même $j \circ f^{-1} \circ s(X'_2)$ est contenu dans X_2 , donc $f_2(X_2) = X'_2$.

Supposons maintenant que $f_1(X_1) = X'_1$ et $f_2(X_2) = X'_2$. On a

alors $\dim_{\mathbb{F}_p} X_1 = \dim_{\mathbb{F}_p} X'_1$, et $\dim_{\mathbb{F}_p} X_2 = \dim_{\mathbb{F}_p} X'_2$, donc $\dim_{\mathbb{F}_p} X = \dim_{\mathbb{F}_p} X'$, et $f(X) = X'$ si et seulement si $f(X) \subset X'$.
Or, pour tout x_1 dans X_1 et tout x_2 dans X_2 , on a :

$$f(x_1 + (s-k)x_2) = f(x_1 - kx_2 + sx_2) = f_1(x_1 - kx_2) + (s-h)(f_2(x_2))$$
$$= f_1(x_1) + (s-k')(f_2(x_2)) - f_1 \circ k(x_2) + (k'-h) \circ f_2(x_2) \quad ;$$

et ici $f_1(x_1) + (s-k')(f_2(x_2))$ appartient à $X'_1 + (s-k')X'_2 = X'$. On a donc $f(X) \subset X'$ si et seulement si $(f_1 \circ k - k' \circ f_2 + h \circ f_2)(X_2) \subset X'$.
Or, l'image de Y_2 par $f_1 \circ h$ (resp. $k' \circ f_2$, resp. $h \circ f_2$) est contenue dans Y_1 ; et $X' \cap Y_1$ est égal à X'_1 .

c.q.f.d.

Supposons maintenant, de plus, que Y est un $\mathbb{F}_p[G]$-module (pour un groupe fini quelconque G), que Y_1 est égal à Y^G , et que Y_2 est fixe par G . Alors la suite $0 \to Y_1 \to Y \xrightarrow{j} Y_2 \to 0$ est exacte sur $\mathbb{F}_p[G]$. Notons $T = \mathrm{Hom}_{\mathbb{F}_p}(Y_2, Y_1)$, et θ l'homomorphisme de G dans T associé à cette suite exacte ; autrement dit, θ est défini par

$$g(y_1 + s'y_2) = (y_1 + \theta_g y_2 + s'y_2)$$

pour tous g de G , y_1 de Y_1 , y_2 de Y_2 , et toute section s' de j sur $\mathbb{F}_p$. (cf. [3], et utiliser le fait qu'ici on a $H^1(G,T) = \mathrm{Hom}(G,T)$, car T est fixe par G).

LEMME 4. - Soit X un sous-$\mathbb{F}_p$-espace vectoriel de Y , et $\Phi(X) = (X_1, X_2, k)$. Alors X est un sous-$\mathbb{F}_p[G]$-module de Y si et seulement si, pour tout g de G , on a $\theta_g(X_2) \subset X_1$.

Démonstration : Pour tous g de G , x_1 de X_1 et x_2 de X_2 , on a $g(x_1 + (s-k)(x_2)) = x_1 + \theta_g(x_2) + (s-k)(x_2)$.

c.q.f.d.

LEMME 5. - Soit f un $\mathbb{F}_p$-automorphisme de Y laissant Y_1 stable, et soit $\psi(f) = (f_1, f_2, h)$. Alors, f est $\mathbb{F}_p[G]$-linéaire si et seulement si, pour tout g de G , on a $\theta_g \circ f_2 = f_1 \circ \theta_g$. De plus, pour tout $\mathbb{F}_p$-automorphisme f_1 de Y_1 , il existe au plus un $\mathbb{F}_p$-automorphisme f_2 de Y_2 tel que l'on ait, pour tout g dans G , $\theta_g \circ f_2 = f_1 \circ \theta_g$.

Démonstration : Pour tous g dans G , y_1 dans Y_1 , y_2 dans Y_2 , on a $f(g(y_1+sy_2)) = f_1(y_1+\theta_g y_2) + (s-h)(f_2(y_2))$, et $g(f(y_1+sy_2)) = f_1(y_1) + \theta_g \circ f_2(y_2) + (s-h)(f_2(y_2))$, d'où la première partie du lemme.

Soient maintenant f_2 et f_2' deux $\mathbb{F}_p$-automorphismes de Y_2 tels que l'on ait, pour tout g de G , $\theta_g \circ f_2 = \theta_g \circ f_2'$. Alors l'image de $f_2 - f_2'$ est contenue dans $(\bigcap_{g\in G} \operatorname{Ker} \theta_g) = Y_2 \cap Y^G = y_2 \cap Y_1 = 0$; donc $f_2 = f_2'$.

c.q.f.d.

Oublions momentanément le groupe G , mais supposons donnés : un entier r strictement positif, et pour tout entier i de 1 à r une suite exacte de $\mathbb{F}_p$-espaces vectoriels de dimension finie $0 \to Y_{1,i} \to Y_i \xrightarrow{j_i} Y_{2,i} \to 0$. Supposons que l'on a $Y = \bigoplus_{i=1}^{r} Y_i$, $Y_1 = \bigoplus_{i=1}^{r} Y_{1,i}$, $Y_2 = \bigoplus_{i=1}^{r} Y_{2,i}$, et $j = \prod_{i=1}^{r} j_i$, et que la section s de j est choisie de la forme $\prod_{i=1}^{r} s_i$, où s_i est une section de j_i pour chaque i .

LEMME 6. - Soit f un $\mathbb{F}_p$-automorphisme de Y laissant stable Y_1 , et soit $\psi(f) = (f_1, f_2, h)$. Soit i un entier entre 1 et r . Alors f laisse stable Y_i si et seulement si f_1 (resp. f_2) laisse stable $Y_{1,i}$ (resp. $Y_{2,i}$) , et $h(Y_{2,i})$ est contenu dans $Y_{1,i}$.

Démonstration : Si $f(Y_i) \subset Y_i$, alors

$$f_1(Y_{1,i}) = f(Y_{1,i}) = f(Y_1 \cap Y_i) \subset f(Y_1) \cap f(Y_i) \subset Y_1 \cap Y_i = Y_{1,i} ,$$

et $$f_2(Y_{2,i}) = (j \circ f \circ s)(Y_{2,i}) \subset j \circ f(Y_i) \subset j(Y_i) = Y_{2,i} .$$

Si $f_1(Y_{1,i}) \subset Y_{1,i}$ et $f_2(Y_{2,i}) \subset Y_{2,i}$, alors, pour tout $y_{1,i}$ de $Y_{1,i}$ et tout $y_{2,i}$ de $Y_{2,i}$ on a :

$$f(y_{1,i} + s_i y_{2,i}) = f_1(y_{1,i}) + (s-h)(f_2(y_{2,i})) = f_1(y_{1,i}) + s_i(f_2(y_{2,i})) - h(f_2(y_{2,i})) ,$$

où $f_1(y_{1,i}) + s_i(f_2(y_{2,i}))$ appartient à Y_i . On a donc $f(Y_i) \subset Y_i$ si et seulement si $h(Y_{2,i}) \subset Y_i$. Or, par définition de h , on a toujours $h(Y_2) \subset Y_1$.

c.q.f.d.

Supposons de plus que chaque Y_i est un $\mathbb{F}_p[G]$-module (pour un groupe fini quelconque G), que $Y_{1,i} = Y_i^G$, et que $Y_{2,i}$ est fixe par G . Alors Y vérifie les hypothèses du lemme 4, et si on note, pour tout i , $T_i = \mathrm{Hom}_{\mathbb{F}_p}(Y_{2,i}, Y_{1,i})$, et θ_i l'homomorphisme de G dans T_i correspondant à la suite exacte de $\mathbb{F}_p[G]$-modules $0 \to Y_{1,i} \to Y_i \xrightarrow{j_i} Y_{2,i} \to 0$, on a $\theta = \prod_{i=1}^{r} \theta_i$.

LEMME 7. - Soit X un sous-$\mathbb{F}_p[G]$-module de Y , et i un entier entre 1 et r . Soit $\Phi(X) = (X_1, X_2, \bar{k})$. Alors $X \cap Y_i$ est nul si et seulement si $X_1 \cap Y_{1,i}$ est nul, et alors $X_2 \cap Y_{2,i}$ est nul.

Démonstration : Comme $X_1 \cap Y_{1,i} = (X \cap Y_i) \cap Y_1$, il est clair que $X_1 \cap Y_{1,i}$ est nul dès que $X \cap Y_i$ est nul.

Inversement, supposons que $X_1 \cap Y_{1,i}$ soit nul. Comme on a, pour tout g de G , $\theta_g(X_2 \cap Y_{2,i}) \subset X_1 \cap Y_{1,i}$, on en déduit que $X_2 \cap Y_{2,i} \subset \bigcap_{g \in G} \mathrm{Ker}\, \theta_g$. Or, on a déjà vu (dans la démonstration du

lemme 5) que $\bigcap_{g\in G} \mathrm{Ker}\,\theta_g$ est nul. Donc $X_2 \cap Y_{2,i}$ est nul.

Or, $j(X\cap Y_i)$ est contenu dans $X_2\cap Y_{2,i}$, donc $j(X\cap Y_i)$ est nul. On a donc $X\cap Y_i \subset Y_1$, c'est-à-dire $X\cap Y_i = X_1\cap Y_{1,i}$, qui est nul par hypothèse. Donc $X\cap Y_i$ est nul.

c.q.f.d.

Supposons de plus qu'il existe r sous-groupes $\{H_i\}_{1\le i\le r}$ de G, à quotients cycliques d'ordre p, tels que pour tout i on ait Y_i fixe par H_i, et que θ_{i,g_i} soit un isomorphisme de $Y_{2,i}$ sur $Y_{1,i}$ pour un relèvement g_i dans G d'un générateur de G/H_i.

LEMME 8. - *Soit* $f_1 = \prod_{i=1}^{r} f_{1,i}$ *un élément de* $\prod_{i=1}^{r} \mathrm{Aut}_{\mathbb{F}_p} Y_{1,i}$. *Alors il existe un élément* $f_2 = \prod_{i=1}^{r} f_{2,i}$ *de* $\prod_{i=1}^{r} \mathrm{Aut}_{\mathbb{F}_p} Y_{2,i}$ *tel que l'on ait* $\theta_g \circ f_2 = f_1 \circ \theta_g$ *pour tout* g *de* G.

Démonstration : On pose, pour chaque i, $f_{2,i} = \theta_{i,g_i}^{-1} \circ f_{1,i} \circ \theta_{i,g_i}$. On a alors $\theta_{i,g}\circ f_{2,i} = f_{1,i}\circ\theta_{i,g}$ pour tout g de G ; en effet, si g est dans H_i, chacun des 2 membres est nul ; et si g n'est pas dans H_i, alors $\theta_{i,g}$ est de la forme $\alpha\theta_{i,g_i}$ avec un α dans $\mathbb{F}_p^*$, donc l'égalité provient de la définition de $f_{2,i}$.

c.q.f.d.

En groupant les résultats obtenus dans les lemmes 1 à 8, on obtient le résultat suivant (avec toutes les hypothèses sur Y) :

PROPOSITION. - *L'ensemble des classes des* $\mathbb{F}_p[G]$*-sous-modules* X_r *de* Y *tels que l'on ait* $X\cap Y_i = 0$ *pour tout* i, *modulo* $\prod_{i=1}^{r} \mathrm{Aut}_{\mathbb{F}_p[G]} Y_i$, *est en bijection avec l'ensemble des classes des triplets* (X_1, X_2, k), *où* X_1 *est un sous-*$\mathbb{F}_p$*-espace vectoriel de* Y_1 *tel que l'on ait* $X_1\cap Y_{1,i} = 0$ *pour tout* i ; *où* X_2 *est un sous-*$\mathbb{F}_p$*-espace vectoriel de* Y_2 *tel que l'on ait* $\theta_g(X_2) \subset X_1$

pour tout g de G ; et où k est un $\mathbb{F}_p$-homomorphisme de Y_2 dans Y_1 ; modulo la relation d'équivalence $\sim$ définie par : $(X_1,X_2,k) \sim (X'_1,X'_2,k')$ si et seulement si il existe un élément $f_1 = \prod_{i=1}^{r} f_{1,i}$ dans $\prod_{i=1}^{r} \mathrm{Aut}_{\mathbb{F}_p} Y_{1,i}$, et un élément $h = \prod_{i=1}^{r} h_i$ dans $\prod_{i=1}^{r} \mathrm{Hom}_{\mathbb{F}_p}(Y_{2,i}, Y_{1,i})$ tels que l'on ait, (en notant $f_2 = \prod_{i=1}^{r} f_{2,i}$ et $f_{2,i} = \theta_{i,g_i}^{-1} \circ f_{1,i} \circ \theta_{i,g_i}$) $f_1(X_1) = X'_1$, $f_2(X_2) = X'_2$, et $(f_1 \circ k - k' \circ f_2 + h \circ f_2)(X_2) \subset X'_1$.

Remarque : On peut prendre en particulier dans ce qui précède $G = (\mathbb{Z}/p\mathbb{Z})^2$. Dans ce cas, tout générateur h_i de H_i est le relèvement dans G d'un générateur de $G/H_{i'}$, si i et i' sont distincts. On en déduit le résultat suivant :

Si X_1 est un sous-$\mathbb{F}_p$-espace vectoriel de Y_1 tel que $X_1 \cap Y_{1,i}$ soit nul pour tout i , et si X_2 est un sous-$\mathbb{F}_p$-espace vectoriel de Y_2 tel que $\theta_g(X_2)$ soit contenu dans X_1 pour tout g de G , alors, pour tout couple (i,i') d'indices distincts entre 1 et r , $X_2 \cap (Y_{2,i} \oplus Y_{2,i'})$ est nul.

En effet, on a déjà vu (lemme 7) que $X_2 \cap Y_{2,i}$ est nul pour tout i . Soit $x_2 = y_{2,i} + y_{2,i'}$ un élément de $X_2 \cap (Y_{2,i} \oplus Y_{2,i'})$; il suffit de montrer que $y_{2,i'}$ est nul. Or $\theta_{i,h_i}(y_{2,i}) = 0$, donc $\theta_{h_i}(x_2) = \theta_{i',h_i}(y_{2,i'}) \in X_1 \cap Y_{1,i'}$, qui est nul, donc $\theta_{i',h_i}(y_{2,i'})$ est nul, ce qui prouve que $y_{2,i'}$ est nul ; d'où le résultat.

VI. CLASSIFICATION DES $\mathbb{Z}[G]$-MODULES REALISABLES DE LONGUEUR INFERIEURE A 4 .

D'après II, il s'agit maintenant d'étudier les sous-$\mathbb{F}_p[G]$-modules Q de $\bigoplus_{i=1}^{r} \overline{M_i}$ tels que $Q \cap \overline{M_i}$ soit nul pour tout i de 1 à r , modulo $\prod_{i=1}^{r} U_i$, avec $r \leq 4$.

LEMME. - Pour $r \leq 4$, $\prod_{i=1}^{r} U_i$ agit sur Q comme $\prod_{i=1}^{r} \mathrm{Aut}_{\mathbb{F}_p[G]} \overline{M_i}$ tout entier.

Démonstration : Notons U' le sous-groupe de U engendré par les racines $2p$-èmes de l'unité, et les unités cyclotomiques $\frac{\zeta^a - 1}{\zeta - 1}$ (pour $a \in \{2,3,\ldots,\frac{p-1}{2}\}$).

a) On a vu que $\mathrm{Aut}_{\mathbb{F}_p[G]} \overline{M_i}$ s'identifie à $(\mathbb{F}_p[\zeta]/(\zeta-1)^{p-1})^*$; pour $p \leq 3$, il est facile de voir que l'homomorphisme canonique de U' dans $(\mathbb{F}_p[\zeta]/(\zeta-1)^{p-1})^*$ est surjectif (ce résultat est faux dès que l'on a $p \geq 5$, et que p ne divise pas le nombre de classes du sous-corps réel maximal de $\mathbb{Q}^{(p)}$).

b) Pour $p \geq 5$ et $r \leq 4$, on a vu que $Q = Q^{(\alpha)}$, avec $\alpha \leq 3$; donc $\prod_{i=1}^{r} \mathrm{Aut}_{\mathbb{F}_p[G]} \overline{M_i}$ agit sur Q comme $\prod_{i=1}^{r} \mathrm{Aut}_{\mathbb{F}_p[G]} \overline{M_i}^{(3)}$.

Or $\mathrm{Aut}_{\mathbb{F}_p[G]} \overline{M_i}^{(3)}$ s'identifie à $(\mathbb{F}_p[\zeta]/(\zeta-1)^3)^*$, et il est facile de voir que l'homomorphisme canonique de U' dans $(\mathbb{F}_p[\zeta]/(\zeta-1)^3)^*$ est surjectif.

c.q.f.d.

Lorsque Q est $\mathbb{F}_p[G]$-monogène, on peut donc appliquer le corollaire de (IV,1) ; lorsque Q est fixe par G , on connait le résultat par (V,1). Il reste donc à étudier les deux cas suivants : $R_2 \oplus \mathbb{F}_p$, et $R_2 + R_2'$ avec $R_2' \simeq R_2$ et $R_2 \cap R_2' \simeq \mathbb{F}_p$ (on notera simplement $R_2 + R_2'$ ce dernier cas).

Pour cela, nous utilisons la proposition de (V,2), et les résultats obtenus en (V,1) lorsque Q est de hauteur 1. Dans les deux cas ($R_2 \oplus \mathbb{F}_p$ et $R_2 + R_2'$) , nous avons $n_1 = 3$. Or (par V,1) il existe, à $\prod_{i=1}^{4} \mathrm{Aut}_{\mathbb{F}_p} \overline{M_i}$ près, un seul sous-$\mathbb{F}_p$-espace vectoriel X_1 de $\bigoplus_{i=1}^{4} \overline{M_i}^{(1)}$ de dimension 3 tel que l'on ait $X_1 \cap \overline{M_i}^{(1)} = 0$ pour tout i ; et on

peut supposer que X_1 correspond à la matrice $\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$; ou encore, qu'un élément $y = \sum_{i=1}^{4} y_i m_i$ avec $y_i \in \mathbb{F}_p$ est dans X_1 si et seulement si l'on a $y_4 = y_1 + y_2 + y_3$ (on rappelle que $\{m_i\}$ désigne une base de $\overline{M_i}^{(1)}$ sur $\mathbb{F}_p$, pour chaque i).

Les seuls éléments de $\prod_{i=1}^{4} \mathrm{Aut}_{\mathbb{F}_p[G]} \overline{M_i}^{(1)}$ laissant stable X_1 sont les homothéties, donc la proposition (V,2) donne ici le résultat suivant :

l'ensemble des classes, modulo $\prod_{i=1}^{4} \mathrm{Aut}_{\mathbb{F}_p[G]} \overline{M_i}$, des sous-$\mathbb{F}_p[G]$-modules Q de $\bigoplus_{i=1}^{4} \overline{M_i}$ tels que l'on ait $Q \cap \overline{M_i} = 0$ pour tout i de 1 à 4, et tels que Q soit $\mathbb{F}_p[G]$-isomorphe à $R_2 \oplus \mathbb{F}_p$ (resp. à $R_2 + R_2'$), est en bijection avec l'ensemble des couples $(X_2, \bar{\bar{k}})$, où X_2 est un sous-$\mathbb{F}_p$-espace vectoriel de dimension 1 (resp. 2) de $\bigoplus_{i=1}^{4} \overline{M_i}^{(2)} / \overline{M_i}^{(1)}$ tel que l'on ait $\theta_g(X_2) \subset X_1$ pour tout g de G, et où $\bar{\bar{k}}$ est un élément de $\mathrm{Hom}_{\mathbb{F}_p}\left(\bigoplus_{i=1}^{4} \overline{M_i}^{(2)} / \overline{M_i}^{(1)}, \bigoplus_{i=1}^{4} \overline{M_i}^{(1)} \right)$, modulo la relation d'équivalence $\underset{X_1, X_2}{\approx}$ définie par : $k \underset{X_1, X_2}{\approx} k'$ s'il existe un élément h de $\prod_{i=1}^{4} \mathrm{Hom}_{\mathbb{F}_p}\left(\overline{M_i}^{(2)} / \overline{M_i}^{(1)}, \overline{M_i}^{(1)} \right)$ tel que l'on ait $(k - k' + h)(X_2) \subset X_1$.

D'autre part, la remarque faite à la fin (V,2) et l'étude faite en (V,1) lorsque $Q \simeq \mathbb{F}_p$ (resp. $Q \simeq \mathbb{F}_p^2$) montrent que les seuls sous-$\mathbb{F}_p$-espaces vectoriels X_2 de $\bigoplus_{i=1}^{4} \overline{M_i}^{(2)} / \overline{M_i}^{(1)}$ susceptibles de vérifier $\theta_g(X_2) \subset X_1$ pour tout g de G correspondent aux matrices $(\lambda_1, \lambda_2, \lambda_3, 0)$ et à ses 3 autres conjuguées par $\mathfrak{S}_4$, ou $(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ $\left(\text{resp. } \begin{pmatrix} \lambda_1 & 0 & \lambda_3 & \lambda_4 \\ 0 & \lambda_2 & \lambda_3 & \mu\lambda_4 \end{pmatrix} \text{ avec } \mu \in \mathbb{F}_p - \{0,1\} \right)$ (les λ_i sont tous dans $\mathbb{F}_p^*$). Par ailleurs, il est clair que l'on a $\theta_g(X_2) \subset X_1$ pour tout g de G, dès que c'est vrai pour $g = h_1$ et pour $g = h_2$ (comme

d'habitude, h_i désigne un générateur de H_i). Or $\theta_{h_j} = \prod_{i=1}^{4} \theta_{i,h_j}$ avec $\theta_{j,h_j} = 0$, et θ_{i,h_j} est un isomorphisme de $\overline{M_i}(2)/\overline{M_i}(1)$ sur $\overline{M_i}(1)$ pour $i \neq j$; en choisissant une base pour chacun de ces espaces, cela donne $\theta_{i,h_j} \in \mathbb{F}_p^*$ pour $i \neq j$. De plus, on peut choisir ces bases de sorte que l'on ait : $\theta_{i,h_1} = 1$ pour $i \in \{2,3,4\}$ et $\theta_{1,h_2} = 1$. Alors θ_{3,h_2} et θ_{4,h_2} (notés respectivement t_3 et t_4) sont deux éléments distincts de $\mathbb{F}_p^*$.

Ainsi, la propriété $\theta_g(X_2) \subset X_1$ pour tout g de G est équivalente à l'existence d'une solution pour un système de 2 (resp. 4) équations linéaires homogènes à 4 inconnues (les λ_i) dans $\mathbb{F}_p^*$.

Lorsque X_2 correspond à $(\lambda_1,\lambda_2,\lambda_3,0)$, ce système est

$$\begin{cases} 0 = \lambda_2 + \lambda_3 \\ 0 = \lambda_1 + t_3\lambda_3 \end{cases}.$$

Il a donc une solution unique modulo $\mathbb{F}_p^*$, et le seul X_2 convenable correspond à $(-t_3,-1,1,0)$.

Lorsque X_2 correspond à $(\lambda_1,\lambda_2,\lambda_3,\lambda_4)$, ce système est

$$\begin{cases} \lambda_4 = \lambda_2 + \lambda_3 \\ t_4\lambda_4 = \lambda_1 + t_3\lambda_3 \end{cases}.$$

Il a donc $p-3$ solutions modulo $\mathbb{F}_p^*$, et les X_2 convenables correspondent à $(t_4\lambda - t_3 , \lambda - 1 , 1 , \lambda)$, avec $\lambda \in \mathbb{F}_p - \{0,1,t_3/t_4\}$.

Lorsque X_2 correspond à $\begin{pmatrix} \lambda_1 & 0 & \lambda_3 & \lambda_4 \\ 0 & \lambda_2 & \lambda_3 & \mu\lambda_4 \end{pmatrix}$, ce système est

$$\begin{cases} \lambda_4 = \lambda_3 \\ t_4\lambda_4 = \lambda_1 + t_3\lambda_3 \\ \mu\lambda_4 = \lambda_2 + \lambda_3 \\ t_4\mu\lambda_4 = t_3\lambda_3 \end{cases}.$$

Si $\mu \neq t_3/t_4$, il n'a pas de solution. Par contre, si $\mu = t_3/t_4$, il a une solution, unique modulo $\mathbb{F}_p^*$, et le seul X_2 convenable correspond

à $\begin{pmatrix} t_4-t_3 & 0 & 1 & 1 \\ 0 & t_3t_4^{-1}-1 & 1 & t_3t_4^{-1} \end{pmatrix}$.

Montrons enfin que, pour n'importe lequel de ces X_2 , et n'importe quel $\mathbb{F}_p$-homomorphisme k de Y_2 dans Y_1 , il existe un élément $h = \prod_{i=1}^{4} h_i$ dans $\prod_{i=1}^{4} \mathrm{Hom}_{\mathbb{F}_p}(Y_{2,i}, Y_{1,i})$ tel que l'on ait $(k+h)(X_2) \subset X_1$. En effet, pour tout élément x_2 de X_2 , on a $(k+h)(x_2) \in X_1$ si et seulement si :

$$h_1x_{2,1} + h_2x_{2,2} + h_3x_{2,3} - h_4x_{2,4}$$
$$= -((k(x_2))_1 + (k(x_2))_2 + (k(x_2))_3) + (k(x_2))_4 .$$

Donc il existe $h = \prod_{i=1}^{4} h_i$ tel que $(k+h)(X_2) \subset X_1$ si et seulement si un système linéaire de 1 (resp. 2) équations à 4 inconnues (les h_i) dans $\mathbb{F}_p$ a une solution. Or ce système a pour matrice la matrice obtenue en remplaçant, dans la matrice correspondant à X_2 , la 4e colonne par son opposée. C'est donc toujours une matrice de rang 1 (resp. 2), et h existe toujours.

D'où le résultat pour $Q \simeq R_2 \oplus \mathbb{F}_p$, et $Q \simeq R_2 + R_2'$.

Ces résultats sont résumés dans le tableau suivant (lorsque $r = 2$ ou 3, on retrouve bien les résultats de L. Bouvier et J.J. Payan [1,11]).

r	α	$(n_j - n_{j-1})_{1\le j\le\alpha}$	structure de Q sur $\mathbb{F}_p[G]$	$\{\alpha_i\}_{1\le i\le r}$ (non ordonnés)	nbre de classes de $\mathbb{Z}[G]$-isomorphisme de M
2	0	ϕ	0	0,0	1
	1	1	$\mathbb{F}_p$	1,1	1
3	0	ϕ	0	0,0,0	1
	1	1	$\mathbb{F}_p$	1,1,0	3
				1,1,1	1
		2	$\mathbb{F}_p^2$	1,1,1	1
	2	2,1	R_2	2,2,2	1 (si $p\ge 3$)
4 (si $p\ge 3$)	0	ϕ	0	0,0,0,0	1
	1	1	$\mathbb{F}_p$	1,1,0,0	6
				1,1,1,0	4
				1,1,1,1	1
		2	$\mathbb{F}_p^2$	1,1,1,0	4
				1,1,1,1	$p+7$
		3	$\mathbb{F}_p^3$	1,1,1,1	1
	2	2,1	R_2	2,2,2,0	4
				2,2,2,1	4
				2,2,2,2	1
		3,1	$R_2 \oplus \mathbb{F}_p$	2,2,2,1	4
				2,2,2,2	$p-3$
		3,2	$R_2 + R_2'$	2,2,2,2	1
	3	3,2,1	R_3	3,3,3,3	1 (si $p\ge 5$)

VII. APPLICATION A L'EXISTENCE D'UNITES DE MINKOWSKI.

Soit $K/\mathbb{Q}$ une extension abélienne de type (p,p) (réelle si $p = 2$). On note :

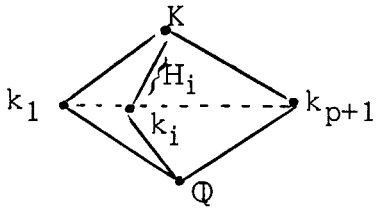
$G = \mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^2$;

$H_1, H_2, \ldots, H_{p+1}$ les sous-groupes cycliques d'ordre p de G ;

k_i le sous-corps de K fixe par H_i (pour tout i de 1 à r) ;

E (resp. E_i) le groupe des unités de K (resp. k_i) modulo torsion.

Il est facile de voir qu'on a ici $E^{H_i} = E_i$.



DEFINITION. - On dit que K admet une unité de Minkowski si E est $\mathbb{Z}[G]$-monogène.
On sait que cela équivaut à dire que E est $\mathbb{Z}[G]$-isomorphe à $\mathbb{Z}[G]/\mathbb{Z}.\tilde{G}$ (cf. N. Moser [9], prop. I.3).
Notons M le $\mathbb{Z}[G]$-module $\mathbb{Z}[G]/\mathbb{Z}\tilde{G}$. Il est bien sûr réalisable, au sens de (I).

PROPOSITION. - Le $\mathbb{Z}[G]$-module réalisable $M = \mathbb{Z}[G]/\mathbb{Z}\tilde{G}$ est de longueur $p+1$; pour tout i de 1 à $p+1$, le $\mathbb{Z}[G/H_i]$-module M^{H_i} s'identifie à un idéal principal de $\mathbb{Q}^{(p)}$; le $\mathbb{F}_p[G]$-module $Q = M/\bigoplus_{i=1}^{p+1} M^{H_i}$ est $\mathbb{F}_p[G]$-isomorphe à R_{p-1} ; et si $q = \sum_{i=1}^{p+1} q_i$ désigne un générateur de Q, avec q_i dans $p^{-1}M^{H_i}/M^{H_i}$ pour tout i, alors la hauteur de q_i est égale à $p-1$ pour tout i .

Démonstration : Il est facile de voir que, pour tout i de 1 à $p+1$, on a $\tilde{H}_i M = M^{H_i} \simeq \mathbb{Z}[G/H_i]/\mathbb{Z}.\widetilde{G/H_i}$ (cf. [9], prop. I.4). D'autre part, Q est $\mathbb{F}_p[G]$-monogène car M est $\mathbb{Z}[G]$-monogène. Donc Q

est $\mathbb{F}_p[G]$-isomorphe à R_α , avec $\alpha = \underset{1\le i\le p+1}{\mathrm{Max}}\ \alpha_i$ (où $\alpha_i = \mathrm{ht}(q_i)$) (d'après IV,1). Il reste donc à montrer que α_i est égal à $p-1$ pour tout i de 1 à $p+1$. Or ceci est une conséquence du fait que $\widetilde{H}_i M = M^{H_i}$ pour tout i , et du lemme ci-dessous.

c.q.f.d.

LEMME. - *Pour tout $\mathbb{Z}[G]$-module réalisable M , et tout H_i dans $\mathcal{H}_M$, notons α_i la dimension sur $\mathbb{F}_p$ de la projection de Q sur $\overline{M}_i$ parallèlement à $\overset{r}{\underset{\substack{i'=1\\ i'\neq i}}{\oplus}} \overline{M}_{i'}$. On a alors*

$$\dim_{\mathbb{F}_p}\left(M^{H_i}/\widetilde{H}_i M\right) + \alpha_i = p-1 \ .$$

Remarque : Si $Q = \mathbb{F}_p[G]q$, avec $q = \sum_{i=1}^{r} q_i$, et $q_i \in \overline{M}_i$ pour tout i , alors α_i est la hauteur de q_i .

Démonstration : Puisque H_i agit sur M^{H_i} comme p , on a les inclusions $pM^{H_i} \subset \widetilde{H}_i M \subset M^{H_i}$. D'où

$$0 \longrightarrow \widetilde{H}_i M/pM^{H_i} \longrightarrow M^{H_i}/pM^{H_i} \longrightarrow M^{H_i}/\widetilde{H}_i M \longrightarrow 0 \ .$$

On a donc

$$\dim_{\mathbb{F}_p}\left(M^{H_i}/\widetilde{H}_i M\right) + \dim_{\mathbb{F}_p}\left(\widetilde{H}_i M/pM^{H_i}\right) = \dim_{\mathbb{F}_p}\left(M^{H_i}/pM^{H_i}\right) = p-1 \ ,$$

et il suffit de montrer que l'on a

$$\alpha_i = \dim_{\mathbb{F}_p}\left(\widetilde{H}_i M/pM^{H_i}\right) \ .$$

Appliquons le lemme du serpent au diagramme commutatif à lignes exactes suivant :

$$\begin{array}{ccccccccc} & & 0 & \longrightarrow & M^{H_i} & \xrightarrow{\widetilde{H}_i = p} & pM & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M \cap \overset{r}{\underset{\substack{i'=1\\ i'\neq i}}{\oplus}} p^{-1}M^{H_{i'}} & \longrightarrow & M & \xrightarrow{\widetilde{H}_i} & \widetilde{H}_i M & \longrightarrow & 0 \end{array} \ .$$

Cela donne

$$\widetilde{H}_i M/pM^{H_i} \simeq (M/M^{H_i})\Big/\left(M \cap \overset{r}{\underset{\substack{i'=1\\ i'\neq i}}{\oplus}} p^{-1}M^{H_{i'}}\right) \ ,$$

c'est-à-dire

$$\widetilde{H}_i M/pM^{H_i} \simeq M/\left(M^{H_i} \oplus \left(M \cap \bigoplus_{\substack{i'=1 \\ i' \neq i}}^{r} p^{-1} M^{H_{i'}}\right)\right) .$$

D'autre part, α_i est par définition la dimension sur $\mathbb{F}_p$ de $Q/Q \cap \bigoplus_{\substack{i'=1 \\ i' \neq i}}^{r} \overline{M}^{H_{i'}}$, qui est isomorphe à $M/M \cap \left(M^{H_i} \oplus \bigoplus_{\substack{i'=1 \\ i' \neq i}}^{r} p^{-1} M^{H_{i'}}\right)$.

Or M contient M^{H_i}, donc les deux $\mathbb{F}_p$-espaces vectoriels $\widetilde{H}_i M/pM^{H_i}$ et $Q/Q \cap \bigoplus_{\substack{i'=1 \\ i' \neq i}}^{r} \overline{M}^{H_{i'}}$ sont isomorphes.

c.q.f.d.

THEOREME. - <u>Une condition nécessaire pour qu'une extension abélienne réelle</u> $K/\mathbb{Q}$ <u>de type</u> (p,p) <u>admette une unité de Minkowski est que l'on ait</u> :

(i) $N_{K/k_i}(E) = E_i$ <u>pour tout</u> i <u>de</u> 1 <u>à</u> $p+1$, <u>et</u>

(ii) $\left[E : \prod_{i=1}^{p+1} E_i\right] = p^{\frac{p(p-1)}{2}}$.

<u>Si de plus</u> p <u>est égal à</u> 2 <u>ou</u> 3 , <u>alors ces conditions (i) et (ii) sont suffisantes</u>.

<u>Remarques</u> :

▪ La condition (i) est connue, et valable pour toute extension galoisienne réelle (cf. N. Moser [9] corollaire de la prop. I.4).

▪ La condition (ii) est équivalente à la condition

$$p^{p-1} h_K = \prod_{i=1}^{p+1} h_i ,$$

où h_K (resp. h_i) désigne le nombre de classes de K (resp. k_i) . En effet, on sait (d'après H. Nehrkorn [10] et S. Kuroda [6]), que l'on a la relation

$$h_K = \left[E : \prod_{i=1}^{p+1} E_i\right] . p^{1 - \frac{p(p+1)}{2}} \prod_{i=1}^{p+1} h_i .$$

■ La condition (ii) est connue lorsque $p = 2$ ou 3 , ainsi que la deuxième partie du théorème lorsque $p = 2$ (cf. L. Bouvier et J.J. Payan [1], prop. III.2 et rem. III.2).

Démonstration : En notant $M = \mathbb{Z}[G]/\mathbb{Z}\tilde{G}$, on voit que la condition (i) traduit $\tilde{H}_i M = M^{H_i}$ pour tout i , et la condition (ii) traduit $\dim_{\mathbb{F}_p} M \Big/ \bigoplus_{i=1}^{p+1} M^{H_i} = \frac{p(p-1)}{2}$. Donc la première partie du théorème est une conséquence immédiate de la proposition ci-dessus.

Montrons maintenant la deuxième partie du théorème ; lorsque p est égal à 2 ou 3 , le corps $\mathbb{Q}^{(p)}$ est principal, donc la donnée de M à $\mathbb{Z}[G]$-isomorphisme près correspond bijectivement à la donnée de Q à $\prod_{i=1}^{p+1} U_i$ près (d'après II). Or, on a vu (en VI) que, pour $p = 2$ ou 3 , on a $\prod_{i=1}^{p+1} U_i = \prod_{i=1}^{p+1} \mathrm{Aut}_{\mathbb{F}_p[G]} \overline{M_i}$.

D'autre part, la condition (i) signifie, d'après le lemme ci-dessus, que $\alpha_i = p-1$ pour tout i de 1 à $p+1$; et la condition (ii) signifie que $\dim_{\mathbb{F}_p} Q = \frac{p(p-1)}{2}$; donc Q est de hauteur $p-1$ et de dimension $\frac{p(p-1)}{2}$, ce qui n'est possible (par IV,1) que si Q est isomorphe à R_{p-1} . Mais alors (d'après IV,1), la classe de Q modulo $\prod_{i=1}^{p+1} \mathrm{Aut}_{\mathbb{F}_p[G]} \overline{M_i}$ est déterminée de manière unique par la famille des $(\alpha_i)_{1 \le i \le p+1}$.

On a donc montré que, pour $p = 2$ ou 3 , les conditions (i) et (ii) sont équivalentes au fait que E soit $\mathbb{Z}[G]$-isomorphe à $\mathbb{Z}[G]/\mathbb{Z}.\tilde{G}$.

c.q.f.d.

Remarque : Pour p quelconque, le nombre de classes de $\mathbb{Z}[G]$-isomorphisme de $\mathbb{Z}[G]$-modules réalisables M vérifiant les conditions :

(i)' $\tilde{H}_i M = M^{H_i}$ pour tout i de 1 à $p+1$,

(ii)' $\dim_{\mathbb{F}_p} M / \overset{p+1}{\underset{i=1}{\oplus}} M^{H_i} = \frac{p(p-1)}{2}$,

(iii)' M^{H_i} s'identifie à un idéal principal de $\mathbb{Q}^{(p)}$ pour tout i de 1 à $p+1$,
est au plus égal à $(\nu_p)^{p+1}$, où ν_p désigne l'indice de l'image de U dans $\left(\mathbb{F}_p[\zeta]/(\zeta-1)^{p-1}\right)^*$.

En effet, un raisonnement analogue à celui qui précède, montre que les deux premières conditions déterminent une et une seule classe de $\mathbb{F}_p[G]$-modules Q à $\overset{p+1}{\underset{i=1}{\|}} \mathrm{Aut}_{\mathbb{F}_p[G]} \overline{M_i}$ près, à savoir $Q = \mathbb{F}_p[G]q$, avec $q = \Sigma q_i$ et q_i dans $\overline{M_i}^{(p-1)} \setminus \overline{M_i}^{(p-2)}$ (qui correspond à $\left(\mathbb{F}_p[\zeta]/(\zeta-1)^{p-1}\right)^*$) pour tout i . Ces deux premières conditions déterminent donc $(\nu_p)^{p+1}$ classes de $\mathbb{F}_p[G]$-modules Q , à $\overset{p+1}{\underset{i=1}{\|}} U_i$ près. Comme de plus la troisième condition fixe les classes de $\mathbb{Z}[G]$-isomorphisme des modules M^{H_i} , l'ensemble des trois conditions est vérifié par au plus $(\nu_p)^{p+1}$ classes de $\mathbb{Z}[G]$-isomorphisme de modules M .

Exemple : Montrons que les extensions abéliennes de $\mathbb{Q}$ de type (3,3) citées par L. Bouvier et J.J. Payan à la fin de [1] possèdent effectivement une unité de Minkowski.

Rappelons leur construction ; soient p_1 et p_2 deux nombres premiers distincts, congrus à 1 modulo 3 . Notons k_1 (resp. k_2) l'unique corps cyclique de degré 3 ramifié en p_1 (resp. p_2) ; son discriminant est égal à p_1^2 (resp. p_2^2) (H. Hasse [13] ou M.N. Montouchet [14]). Notons K le composé de k_1 et k_2 ; c'est une extension abélienne de $\mathbb{Q}$ à groupe de Galois de type (3,3) , et les nombres premiers ramifiés dans $K/\mathbb{Q}$ sont exactement p_1 et p_2 . Notons k_3 et k_4 les deux autres corps cubiques intermédiaires de $K/\mathbb{Q}$. Leur discriminant est alors égal à $(p_1p_2)^2$, et celui de K (sur $\mathbb{Q}$) est égal à $(p_1p_2)^6$.

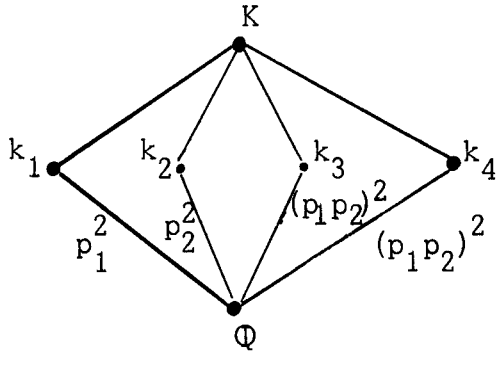
Ainsi, les extensions K/k_3 et K/k_4 sont non ramifiées, alors que K/k_1 (resp. K/k_2) est ramifiée seulement en p_2 (resp. en p_1) .

Notons $h_i^{(3)}$ la 3-composante du nombre de classes h_i de k_i ($1 \leq i \leq 4$) . On sait que $h_1^{(3)} = h_2^{(3)} = 1$, et que $h_3^{(3)} \geq 3$ et $h_4^{(3)} \geq 3$ (cf. G. Gras [4], J. Martinet [8]).

Supposons de plus que p_1 n'est pas reste cubique modulo p_2 , et que p_2 n'est pas reste cubique modulo p_1 . Alors $h_3^{(3)} = h_4^{(3)} = 3$ (cf. [4], [8]), donc $\prod_{i=1}^{4} h_i^{(3)} = 3^2$. D'autre part, le fait que K/k_3 soit une extension cyclique de degré 3 non ramifiée, et le fait que $h_3^{(3)} = 3$, prouvent que h_K n'est pas divisible par 3 , d'après H. Kisilevski [4] (voir aussi N. Moser [9], thm. C).

Mais alors, on a $3^2 h_K = \prod_{i=1}^{4} h_i$, ce qui équivaut, comme on l'a vu, à la condition (ii) du théorème.

Il reste à montrer que la condition (i) est vérifiée, c'est-à-dire que l'on a $N_{K/k_i} E = E_i$ pour tout i de 1 à 4 . Lorsque $i = 1$ (resp. $i = 2$) , l'extension K/k_i est cyclique de degré premier impair 3 , le nombre de classes h_i est premier à 3 , et seule la place finie p_2 (resp. p_1) se ramifie dans K/k_i . Le résultat est alors donné par un théorème de S.N. Kuroda [7] (voir aussi N. Moser [9], thm. B 1). Lorsque $i = 3$ ou 4 , la 3-composante du nombre de classes d'idéaux de k_i qui deviennent principales dans K est égale à 3 (puisque la 3-composante de h_K (resp. h_i) est égale à 1 (resp. 3)) ; d'autre part, l'extension K/k_i est cyclique non ramifiée de degré 3 . C'est donc ici un résultat de H. Yokoi [12] (voir aussi N. Moser [9], thm. B 2) qui permet de conclure.



BIBLIOGRAPHIE

[1] L. BOUVIER, J.J. PAYAN, Sur la structure galoisienne du groupe des unités d'un corps abélien de type (p,p) , Ann. Inst. Fourier 29,1 (1979).

[2] A. BRUMER, On the group of units of an absolutely cyclic number field of prime degree, J. Math. Soc. Japan 21 (1969).

[3] D. DUVAL, Représentations entières des groupes cycliques d'ordre premier, Sém. théorie des nombres, Grenoble (1973-1974).

[4] G. GRAS, Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ (1ère partie), Ann. Inst. Fourier, 23,3 (1973).

[5] H. KISILEVSKI, Some results related to Hilbert's theorem 94, J. of Number theory, 2 (1970).

[6] S. KURODA, Über die Klassenzahlen algebraischer Zahkörper, Nagoya Math. J. 1 (1950), pp. 1-10.

[7] S.N. KURODA, Über die Klassenzahl eines relativ zyklischen Zahlkörpers von Primzahlgrade, Proc. Japan Academy, 40 (1964).

[8] J. MARTINET, A propos de classes d'idéaux, Sém. théorie des nombres, Bordeaux (1971-1972).

[9] N. MOSER, Unités et nombre de classes d'une extension galoisienne diédrale de $\mathbb{Q}$, Abh. Math. Sem. Univ. Hamburg (à paraître).

[10] H. NEHRKORN, Über absolute Idealklassengruppen und Einheiten in algebraischen Zahlkörpern, Abh. Math. Sem. Univ. Hamburg 9 (1933), pp. 318-334.

[11] J.J. PAYAN, Sur la structure galoisienne du groupe des unités d'un corps abélien de type (p,p) (d'après un travail avec L. Bouvier), Sém. théorie des nombres, Grenoble (1978-1979).

[12] H. YOKOI, On the class number of a relatively cyclic number field, Nagoya Math. Journal, 29 (1967).

[13] H. HASSE, Vorselungen über Zahlentheorie, Berlin (1964).

[14] M.N. MONTOUCHET, Sur le nombre de classes du sous-corps cubique cyclique de $\mathbb{Q}(p)$, $p \equiv 1 \mod 3$, Sém. théorie des nombres, Grenoble (1970).

Laboratoire de Mathématiques Pures - Institut Fourier
dépendant de l'Université Scientifique et Médicale de Grenoble
associé au C.N.R.S.
B.P. 116
38402 ST MARTIN D'HERES (France)