

Werk

Titel: Inventiones Mathematicae

Verlag: Springer

Jahr: 1974

Kollektion: Mathematica

Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen

Werk Id: PPN356556735_0027

PURL: http://resolver.sub.uni-goettingen.de/purl?PPN356556735_0027

LOG Id: LOG_0007

LOG Titel: Exercices dyadiques.

LOG Typ: article

Übergeordnetes Werk

Werk Id: PPN356556735

PURL: <http://resolver.sub.uni-goettingen.de/purl?PPN356556735>

OPAC: <http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=356556735>

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Exercices dyadiques

André Weil (Princeton)

A Jean-Pierre Serre

1. Soit k un p -corps, c'est-à-dire un corps localement compact à valuation discrète, de caractéristique résiduelle $p > 1$. Ecrivons, suivant l'usage, k_{sep} pour une clôture algébrique séparable de k , et k_{ab} pour l'extension abélienne maximale de k , contenue dans k_{sep} ; soient $\mathfrak{G}$, $\mathfrak{A}$ leurs groupes de Galois respectifs sur k . La théorie du corps de classes local établit un isomorphisme canonique entre le groupe des caractères de $\mathfrak{A}$ et le groupe des caractères d'ordre fini du groupe multiplicatif $k^\times$ du corps k ; la détermination de cet isomorphisme et de ses propriétés «fonctorielles» constitue même l'essentiel de la théorie en question.

Les caractères de $\mathfrak{A}$ ne sont pas autre chose que les représentations de $\mathfrak{G}$ dans $\mathbf{C}^\times = \text{GL}(1, \mathbf{C})$; on peut écrire $\text{GL}(1, k)$ pour $k^\times$. Des travaux récents (R. Langlands) suggèrent l'existence d'un lien analogue entre les représentations de $\mathfrak{G}$ dans $\text{GL}(n, \mathbf{C})$ et un certain type très général de représentations (dites «admissibles») de $\text{GL}(n, k)$; de même, il y aurait par exemple un lien entre les représentations de $\mathfrak{G}$ dans $\text{SL}(n, \mathbf{C})$ et les représentations «admissibles» de $\text{PL}(n, k)$. S'il en est bien ainsi, la découverte de tels liens fournirait une généralisation non abélienne de la théorie locale du corps de classes.

Notre connaissance des représentations de $\text{GL}(n, k)$ est encore des plus fragmentaires, sauf pour $n=2$, $p>2$. Même le cas $n=2$, $p=2$ n'a pas encore été élucidé. En attendant, il n'est peut-être pas inutile d'examiner les représentations des groupes de Galois des corps locaux dans $\text{GL}(2, \mathbf{C})$ et $\text{SL}(2, \mathbf{C})$, particulièrement dans le cas $p=2$. Tel est le but du présent article; si modeste que soit cet objectif, nous ne l'atteindrons même pas complètement. Pour la clarté de l'exposé, et aussi avec l'espoir de venir en aide aux futurs chercheurs, nous rassemblerons d'abord ici des remarques variées, dont aucune n'est nouvelle, sur les représentations dans $\text{GL}(n, \mathbf{C})$. Pour abrégé, on écrira GL_n , PL_n au lieu de $\text{GL}(n, \mathbf{C})$, $\text{PL}(n, \mathbf{C})$, et 1_n pour l'élément neutre de $\text{GL}(n, \mathbf{C})$; le centre de GL_n est $\mathbf{C}^\times \cdot 1_n$, et on a $\text{PL}_n = \text{GL}_n / (\mathbf{C}^\times \cdot 1_n)$. Par un *caractère* d'un groupe G , on entendra toujours une représentation de G dans $\text{GL}_1 = \mathbf{C}^\times$.

Soit φ le morphisme canonique de GL_n sur PL_n . Si M est une représentation d'un groupe G dans GL_n , on posera une fois pour toutes

$M^0 = \varphi \circ M$. On dira que deux représentations M, M' de G dans GL_n sont *associées* si $M^0 = M'^0$, c'est-à-dire si l'on a, pour tout $g \in G$, $M'(g) = M(g) \omega(g)$ avec $\omega(g) \in \mathbb{C}^\times$; alors ω est un caractère de G , et on a $M' = M \otimes \omega$.

2. Rappelons la solution (due essentiellement à I. Schur) du problème qui consiste à remonter d'une représentation dans PL_n à une représentation dans GL_n . Soient G un groupe, H un sous-groupe commutatif invariant de G , $\Gamma = G/H$; soient G' un groupe, H' un sous-groupe du centre de G' , et $\Gamma' = G'/H'$; soit μ un morphisme de Γ dans Γ' . Pour tout $\sigma \in \Gamma$, choisissons un représentant g_σ de σ dans G et un représentant z_σ de $\mu(\sigma)$ dans G' , et posons

$$h(\sigma, \tau) = g_{\sigma\tau}^{-1} g_\sigma g_\tau, \quad \zeta(\sigma, \tau) = z_{\sigma\tau}^{-1} z_\sigma z_\tau;$$

ces formules définissent, comme on sait, des cocycles h, ζ de Γ , dans H et dans H' respectivement. Soit Ω une représentation de H dans H' ; pour qu'il y ait une représentation M de G dans G' qui rende le «diagramme» (Ω, M, μ) «commutatif» (c'est-à-dire dont la restriction $M|_H$ à H soit Ω , et qui détermine μ par passage au quotient), il faut et il suffit que Ω soit invariant par les automorphismes intérieurs de G , et que l'image $\Omega(h)$ du cocycle h appartienne à la classe de cohomologie définie par le cocycle ζ dans $H^2(\Gamma, H')$.

En particulier, si $H = \{1\}$, $\Gamma = G$, $H^2(G, H') = 0$, toute représentation de G dans G' se relève à une représentation de G dans G' . Par exemple, soit $\mathfrak{G}$ le groupe de Galois introduit au n° 1. D'après un théorème qu'on peut qualifier de classique (cf. p. ex. S. S. Shatz, Ann. of Math. Studies n° 67, p. 232, Corollary), on a $H^3(\mathfrak{G}, \mathbb{Z}) = 0$, donc $H^2(\mathfrak{G}, \mathbb{C}^\times) = 0$. Par suite, toute représentation de $\mathfrak{G}$ dans PL_n se relève à une représentation dans GL_n . Bien entendu, $\mathfrak{G}$ est à considérer ici comme groupe «profini», c'est-à-dire comme groupe compact totalement discontinu, et il ne s'agit que de cocycles et de représentations continus, de sorte que les noyaux de celles-ci sont d'indice fini dans G .

3. Si H est un sous-groupe commutatif invariant d'un groupe G , et que s soit un représentant dans G d'un élément σ de $\Gamma = G/H$, on posera $h^\sigma = s^{-1} h s$ pour tout $h \in H$. Au n° 2, on a défini l'extension G de Γ par H au moyen du cocycle $h(\sigma, \tau)$; mais, comme on sait, ce n'est pas toujours le procédé le plus commode. Par exemple, si Γ est cyclique d'ordre n , il vaudra mieux prendre un générateur σ de Γ , un représentant s de σ dans G , et poser $h = s^n$. Le «cocycle» qui détermine G est alors l'unique élément h de H , soumis à la seule condition $h^\sigma = h$; il est trivial quand il est de la forme $h'^{1+\sigma+\dots+\sigma^{n-1}}$, ce qui donne:

$$H^2(\Gamma, H) = \{h \in H \mid h^{\sigma-1} = 1\} / \{h^{1+\sigma+\dots+\sigma^{n-1}} \mid h \in H\}.$$

Plus généralement, supposons Γ défini par des générateurs α_i et des relations $R_j(\alpha) = \varepsilon$, où ε est l'élément neutre de Γ . Supposons donné un morphisme de Γ dans le groupe des automorphismes de H , ou, ce qui revient au même, supposons donné, pour chaque i , un automorphisme A_i de H , de façon que les relations $R_j(A) = 1$ soient satisfaites. Pour chaque i , choisissons un représentant g_i de α_i dans G ; alors, pour tout j , on a $R_j(g) = h_j \in H$, et la structure de G est bien déterminée par la donnée des h_j . On peut donc considérer (h_j) comme «le cocycle» qui détermine G ; les h_j sont assujettis à des relations de la forme $M(h) = 1$, où chaque M est un monome formé au moyen des h_j^σ pour $\sigma \in \Gamma$. Pour que le cocycle (h_j) soit trivial, il faut et il suffit qu'on puisse écrire, pour tout i , $g_i = a_i h'_i$, où les a_i satisfont aux relations $R_j(a) = 1$; cela donne, pour tout j , $h_j = S_j(h')$, où les S_j sont des monomes formés au moyen des $h'_i{}^\sigma$; pour tout choix des h'_i , les éléments $S_j(h')$ satisfont aux relations $M(h) = 1$ qui définissent les «cocycles». Il serait aisé de formaliser ce qui précède, en écrivant Γ comme quotient d'un groupe libre par le plus petit sous-groupe invariant qui contient des éléments donnés R_j de ce groupe. Notons seulement qu'on peut souvent simplifier les relations $M(h) = 1$ en restreignant le choix des g_i par des conditions supplémentaires dépendant de la structure de Γ ; on en verra des exemples par la suite.

4. Le problème qui nous intéresse s'offre sous deux variantes essentiellement équivalentes, suivant qu'on considère les groupes de Galois ou bien les «W-groupes»; ceux-ci sont des groupes de Galois modifiés, possédant exactement les mêmes propriétés «fonctorielles». Tant qu'il ne s'agit que d'extensions finies, les deux notions coïncident; dans tout autre cas, le groupe de Galois est la compactification du W -groupe; k désignant toujours un p -corps, le W -groupe de k_{ab} sur k est canoniquement isomorphe à $k^\times$; par suite, si K est une extension galoisienne de degré fini de k , le W -groupe $W(K_{ab}/k)$ de K_{ab} sur k est une extension du groupe fini $\text{Gal}(K/k)$ par $W(K_{ab}/K) = K^\times$.

Toute représentation d'un groupe de Galois détermine une représentation du W -groupe correspondant; réciproquement, toute représentation d'un W -groupe dans GL_n est associée à une représentation du groupe de Galois (cf. A. Weil, Izv. Akad. Nauk SSSR 36 (1972), p. 5). Les uns et les autres ont donc mêmes représentations dans les groupes PL_n .

Soit μ une représentation de $\mathfrak{G} = \text{Gal}(k_{\text{sep}}/k)$ dans PL_n ; comme on l'a déjà noté, elle a un noyau $\mathfrak{H}$ d'indice fini, qui correspond donc à une extension galoisienne K de k de degré fini. D'après le n° 2, il y a une représentation M de $\mathfrak{G}$ dans GL_n telle que $M^0 = \mu$; $M(\mathfrak{H})$ est alors contenu dans $C^\times \cdot 1_n$, et par suite le noyau de M contient le groupe $\mathfrak{H}^c$ engendré par les commutateurs de $\mathfrak{H}$. On peut donc considérer M comme une représentation dans GL_n du groupe $\mathfrak{G}/\mathfrak{H}^c = \text{Gal}(K_{ab}/k)$, et à

plus forte raison de $W(K_{ab}/k)$. Réciproquement, toute représentation M de $\mathfrak{G}$ (ou, ce qui revient au même, du W -groupe de k_{sep} sur k) dans GL_n détermine une représentation $\mu = M^0$ dans PL_n ; celle-ci se relève à une représentation M' d'un groupe $W(K_{ab}/k)$ dans GL_n , et M' , en un sens évident, est associée à M .

Dans la suite, nous parlerons de W -groupes. Le lecteur pourra, s'il veut, lire partout «groupe de Galois» au lieu de « W -groupe», à condition de substituer chaque fois à $K^\times$ la compactification de $K^\times$. D'après ce qu'on vient de voir, il suffira d'examiner les représentations des groupes $W(K_{ab}/k)$.

5. Plaçons-nous d'abord, plus généralement, dans la situation suivante. Soit G un groupe; soit H un sous-groupe commutatif invariant de G , d'indice fini n dans G ; soit $\Gamma = G/H$. Si $s \in G$, et si σ est l'image de s dans Γ , on a $h^{-1}s^{-1}hs = h^{\sigma-1}$; l'image $H^{\sigma-1}$ de H par $h \mapsto h^{\sigma-1}$ est donc un sous-groupe du groupe G^c des commutateurs de G .

Pour simplifier le langage, nous nous exprimerons toujours comme si G , H , etc. étaient munis seulement de leurs structures de groupe. En fait, les groupes que nous avons en vue sont localement compacts (et même compacts, si ce sont des groupes de Galois), et l'on ne s'intéresse qu'à leurs représentations continues. Nous laisserons au lecteur le soin de s'assurer que les précautions nécessaires ont été prises pour que nos conclusions restent valables dans ce cadre.

On posera $N = H \cap G^c$, et on notera J le sous-groupe de H engendré par les sous-groupes $H^{\sigma-1}$ pour $\sigma \in \Gamma$. Soit t le morphisme de transfert de G dans H ; sa restriction $t|_H$ à H est donnée par $t(h) = h^{\sum \sigma}$, où $\sum$ est étendu à tous les éléments de Γ . On notera N' le noyau de $t|_H$; on a $N' \supset N \supset J$. Si Γ est commutatif, on a $N = G^c$. Si Γ est cyclique, et si σ est un générateur de Γ , on a $G^c = H^{\sigma-1} = N = J$.

Pour $G = W(K_{ab}/k)$, $H = K^\times$, $\Gamma = \text{Gal}(K/k)$, on sait que l'image de G dans H par le transfert t n'est autre que le sous-groupe $k^\times$ de $K^\times$ invariant par les automorphismes $h \mapsto h^\sigma$; on a $t|_H = N_{K/k}$ et $N' = G^c$; le groupe $N = H \cap G^c$ est le noyau de $N_{K/k}$.

6. Les notations étant comme ci-dessus, on entendra toujours, par «représentation», une représentation de G dans un groupe GL_r ou PL_r , ou encore, mais exceptionnellement, dans un groupe $GL(r, F)$ ou $PL(r, F)$, F étant un corps autre que $\mathbb{C}$. On sait que, si M est une représentation irréductible de G dans GL_r , le «degré» r de M divise l'indice n de H dans G .

Une représentation M de G dans GL_r sera dite *centrale* si $M(H) \subset \mathbb{C}^\times \cdot 1_r$, c'est-à-dire si H est contenu dans le noyau de la représentation M^0 de G dans PL_r ; alors M^0 détermine une représentation μ

de $\Gamma = G/H$ dans PL_r ; souvent, par abus de langage, nous ne distinguerons pas entre M^0 et μ . Pour que μ soit « fidèle », c'est-à-dire injectif, sur Γ , il faut et il suffit qu'on ait $M^{-1}(\mathbb{C}^\times \cdot 1_r) = H$; alors M sera dite *propre* (et impropre dans le cas contraire).

Soit G' un groupe entre G et H (c'est-à-dire un sous-groupe de G , contenant H). Soit M' une représentation de G' de degré r' . On notera $[M'; G' \rightarrow G]$ la représentation de G induite par M' ; elle est de degré $r'[G : G']$. Toute représentation M de G , équivalente à une représentation $[M'; G' \rightarrow G]$ avec $G' \neq G$, $G' \supset H$, sera dite *imprimitive*, et on dira que G' est un *groupe d'imprimitivité* de M . Il est bien connu que, si M' est elle-même imprimitive, avec un groupe d'imprimitivité G'' , G'' est aussi un groupe d'imprimitivité pour M . On dira que M est *primitive* quand elle n'admet aucun groupe d'imprimitivité entre G et H ; on notera que cette définition dépend de H .

Soit H' un sous-groupe invariant de G entre G et H . Soit M une représentation irréductible de G dans GL_r . Alors, comme on sait, la restriction $M|_{H'}$ de M à H' est somme directe de ses composantes irréductibles; si M' est l'une de celles-ci, toutes les autres sont équivalentes aux transformées de M' par les automorphismes de H' induits sur H' par les automorphismes intérieurs de G . De plus, si ces transformées ne sont pas toutes équivalentes à M' , M admet un groupe d'imprimitivité entre G et H' . De toute manière, ces transformées ont même degré r' que M' ; par suite, r' divise à la fois r et $[H' : H]$; en particulier, si r est premier à $[H' : H]$, on a $r' = 1$. Pour que $M(H')$ soit un sous-groupe commutatif de GL_r , il faut et il suffit qu'on ait $r' = 1$; alors, si H'^c est le groupe des commutateurs de H' , M détermine une représentation du groupe $G_1 = G/H'^c$, et celui-ci admet le sous-groupe invariant commutatif $H_1 = H'/H'^c$. De plus, si $r' = 1$, M admet un groupe d'imprimitivité entre G et H' , à moins que $M(H')$ ne soit contenu dans $\mathbb{C}^\times \cdot 1_r$. En particulier, toute représentation irréductible est, soit imprimitive, soit centrale.

Si M est irréductible (resp. centrale, resp. propre, resp. primitive), il en est de même de toute représentation associée à M .

7. Supposons Γ cyclique; alors G est engendré par H et un élément s . Soit M une représentation irréductible de G , de degré $r > 1$. Si M était centrale, $M(G)$ serait contenu dans le sous-groupe de GL_r engendré par $\mathbb{C}^\times \cdot 1_r$ et $M(s)$, donc réductible. Donc M est équivalente à une représentation de la forme $[M; G' \rightarrow G]$, avec $G' \neq G$, $G' \supset H$; appliquant le même raisonnement à M' , ou autrement dit procédant par récurrence sur l'ordre de Γ , on voit que M est équivalente à $[M; G' \rightarrow G]$ avec M' de degré 1; il en est trivialement de même, avec $G' = G$, si $r = 1$. Si $r > 1$,

le groupe d'imprimitivité G' de M est l'unique sous-groupe d'indice r de G entre G et H , et $M(G')$ est commutatif.

Plus généralement, supposons qu'il y ait un sous-groupe invariant H' de G , entre G et H , tel que H'/H soit cyclique d'ordre $m > 1$. Soient M une représentation irréductible de G , M' une composante irréductible de $M|_{H'}$, et r' le degré de M' . Alors r' divise m ; de plus, d'après ce qui précède, si H'' est le sous-groupe d'indice r' de H' entre H' et H , H'' est un groupe d'imprimitivité de M' , et $M'(H'')$ est commutatif. Il s'ensuit que $M(H'')$ aussi est commutatif. Donc, ou bien M admet un groupe d'imprimitivité entre G et H'' , ou bien $M(H'') \subset \mathbb{C}^\times \cdot 1_r$. Si M est propre, et si $M(H'') \subset \mathbb{C}^\times \cdot 1_r$, on a $H'' = H$ et $r' = m$.

8. A toute représentation centrale M de G dans GL_r , on a associé une représentation μ de Γ dans PL_r , qui est fidèle si M est propre. Réciproquement, si on se donne μ , on a vu au n° 2 comment la méthode de Schur permet de construire une représentation M associée à μ , s'il en existe. Avec les notations du n° 2, on posera $M|_H = \Omega \cdot 1_r$, et on aura à satisfaire à la condition $\Omega(h) \sim \zeta$, où $\sim$ désigne l'homologie dans $H^2(\Gamma, \mathbb{C}^\times)$. Comme deux solutions M, M' du problème sont nécessairement « associées » (au sens du n° 1), elles coïncident sur G^c , de sorte que les caractères correspondants Ω, Ω' coïncident sur $N = H \cap G^c$.

Plus généralement, donnons-nous une représentation μ de Γ dans $\text{PL}(r, F)$, où F est un corps quelconque; pour simplifier, bornons-nous au cas où μ est fidèle. Soit Δ un sous-groupe de $\text{GL}(r, F)$, dont l'image dans $\text{PL}(r, F)$ soit $\mu(\Gamma)$; on pourra écrire $\Delta \cap (F^\times \cdot 1_r) = E \cdot 1_r$, où E est un sous-groupe de $F^\times$. Proposons-nous de rechercher une représentation M de G dans Δ , associée à μ ; pour une telle représentation, on pourra poser $M|_H = \Omega \cdot 1_r$, Ω étant un morphisme de H dans E . Pour cela on appliquera le n° 2, en prenant $G' = \Delta$, $H' = E \cdot 1_r$; ζ est alors un cocycle de Γ dans E , et le problème se ramène à la recherche de Ω tel que $\Omega(h) \sim \zeta$ dans $H^2(\Gamma, E)$. Si en particulier Δ est un groupe fini, E est cyclique; s'il est d'ordre s , c'est le groupe E_s des racines s -ièmes de 1 dans F . Si en même temps la classe de cohomologie ζ est d'ordre s dans $H^2(\Gamma, E_s)$, alors Δ ne contient aucun sous-groupe (autre que Δ) dont l'image dans $\text{PL}(r, F)$ soit $\mu(\Gamma)$, et une représentation M de G dans Δ , s'il en existe, est nécessairement surjective.

9. Toujours avec les mêmes hypothèses qu'au n° 8, on a $\Omega(h^\sigma) = \Omega(h)$ pour tout $h \in H$ et tout $\sigma \in \Gamma$; donc Ω et M sont triviales sur le sous-groupe J de H engendré par les $H^{\sigma-1}$ (cf. n° 5). On peut donc, quand G est donné, passer au quotient par J , et substituer $G^* = G/J$, $H^* = H/J$ à G et H ; H^* est contenu dans le centre de G^* . Si H^* n'est pas le centre de G^* , soit H'^* ce centre, et soit H' l'image réciproque de H'^* dans G .

Alors, si M est une représentation irréductible de G dans GL_r , on a $M(H') \subset \mathbb{C}^\times \cdot 1_r$, donc M^0 est triviale sur H' . Si donc μ est fidèle et projectivement irréductible (c'est-à-dire si μ ne laisse invariante aucune sous-variété linéaire de l'espace projectif P^{r-1} sur lequel opère PL_r), il ne peut exister aucune représentation M de G dans GL_r , telle que $M^0 = \mu$, à moins que H^* ne soit le centre de G^* .

10. Nous pouvons maintenant passer à la recherche des représentations de degré 2. Si une telle représentation de G est imprimitive (au sens du n° 6), elle admet un groupe d'imprimitivité d'indice 2 dans G ; suivant qu'elle en admet un seul ou plusieurs, on dira qu'elle est *simple* ou *multiplement* imprimitive.

Soit M une représentation de G dans GL_2 ; supposons-la irréductible et imprimitive, et soit G_1 un groupe d'imprimitivité de M ; G_1 est d'indice 2, donc invariant dans G . Écrivons $G = G_1 \cup sG_1$ et $M = [M_1; G_1 \rightarrow G]$; M_1 est de degré 1, et $M|_{G_1}$ se décompose en M_1 et sa transformée M'_1 par l'automorphisme $x \mapsto s^{-1}xs$ de G_1 . Si on avait $M'_1 = M_1$, $M(G_1)$ serait contenu dans le centre $\mathbb{C}^\times \cdot 1_2$ de GL_2 , $M(G)$ dans le groupe engendré par $M(s)$ et ce centre, et M serait réductible. Donc on a $M'_1 \neq M_1$, et $M(G_1)$ est commutatif et non contenu dans $\mathbb{C}^\times \cdot 1_2$. Réciproquement, on a vu au n° 6 que, si ces dernières conditions sont remplies, M admet un groupe d'imprimitivité entre G et G_1 , qui ne peut être que G_1 .

Par suite, avec les notations ci-dessus, M est donnée (à une équivalence près) par les formules

$$M(g) = \begin{pmatrix} M_1(g) & 0 \\ 0 & M'_1(g) \end{pmatrix}, \quad M(sg) = \begin{pmatrix} 0 & M'_1(g) \\ M_1(s^2g) & 0 \end{pmatrix} \quad (g \in G_1). \quad (1)$$

Comme $M'_1 \neq M_1$, il y a $g_1 \in G_1$ tel que $M(g_1)$ ne soit pas dans $\mathbb{C}^\times \cdot 1_2$, et les formules (1) montrent que, si g_1 est un tel élément, G_1 est l'ensemble des éléments g de G tels que $M(g)$ soit permutable avec $M(g_1)$.

11. Nous distinguerons deux cas, suivant que M est simplement ou multiplement imprimitive. Le premier cas se ramène au cas $G_1 = H$; il suffit de remplacer G par G/G_1^c et H par G_1/G_1^c . On a alors $n=2$, et on peut prendre pour M n'importe quelle représentation irréductible de G ; d'après ce qui précède, une telle représentation est nécessairement non centrale.

Supposons maintenant que M admette un groupe d'imprimitivité $G_2 \neq G_1$, et posons $H' = G_1 \cap G_2$. Pour $i=1, 2$, notons f_i l'homomorphisme canonique de G sur G/G_i , et identifions ce dernier groupe de la manière évidente avec le sous-groupe $E_2 = \{\pm 1\}$ de $\mathbb{C}^\times$. Alors (f_1, f_2) détermine un isomorphisme de G/H' sur $E_2 \times E_2$. Supposons qu'il y ait $h \in H'$ tel que $M(h)$ ne soit pas dans $\mathbb{C}^\times \cdot 1_2$; alors, comme on a vu au n° 10, G_1 est

l'ensemble des $g \in G$ tels que $M(g)$ soit permutable avec $M(h')$, et il en est de même de G_2 , contrairement à l'hypothèse $G_2 \neq G_1$. Donc $M(H') \subset C^\times \cdot 1_2$; compte tenu de (1), on a même $M^{-1}(C^\times \cdot 1_2) = H'$. Par suite, si M admet un troisième groupe d'imprimitivité, celui-ci doit contenir H' et ne peut donc être autre que le noyau G_3 du morphisme $f_1 f_2$ de G dans E_2 . D'ailleurs G_3 est en effet un groupe d'imprimitivité de M ; car H' est d'indice 2 dans G_3 , de sorte qu'on peut écrire $G_3 = H' \cup g' H'$, et $M(G_3)$ est alors engendré par $M(g')$ et le sous-groupe $M(H')$ de $C^\times \cdot 1_2$ et est donc commutatif, mais non contenu dans $C^\times \cdot 1_2$. En définitive, on voit que M est triplement imprimitive; si on remplace G par G/H'^c et H par H'/H'^c , on est ramené au cas où G/H est isomorphe à $E_2 \times E_2$ et où M est centrale et propre.

12. Enfin, si la représentation M est irréductible et primitive, elle est nécessairement centrale. Posant alors $H' = M^{-1}(C^\times \cdot 1_2)$, on se ramène au cas d'une représentation propre en remplaçant G par G/H'^c et H par H'/H'^c .

Dorénavant, nous écarterons le cas d'une représentation simplement imprimitive. D'après ce qui précède, on peut donc supposer une fois pour toutes qu'on a affaire à une représentation M centrale et propre de G dans GL_2 ; d'après le n° 9, elle est triviale sur J ; elle détermine un morphisme fidèle μ de $\Gamma = G/H$ dans PL_2 . On identifiera désormais Γ avec son image $\mu(\Gamma)$ dans PL_2 .

Les sous-groupes finis de PL_2 ont été déterminés par F. Klein. Un tel sous-groupe est contenu dans un sous-groupe compact maximal de PL_2 , et celui-ci est isomorphe au groupe des rotations dans l'espace euclidien à 3 dimensions; la question se ramène donc à la recherche des polyèdres réguliers. On trouve qu'un sous-groupe fini de PL_2 est cyclique ou diédral, ou bien isomorphe à $\mathfrak{A}_4$ (groupe alterné sur 4 symboles, ou groupe du tétraèdre), à $\mathfrak{S}_4$ (groupe symétrique sur 4 symboles, ou groupe du cube et de l'octaèdre), ou à $\mathfrak{A}_5$ (groupe alterné sur 5 symboles, ou groupe du dodécaèdre et de l'icosaèdre); à des isomorphismes près, chacun de ces derniers groupes ne peut se plonger dans PL_2 que d'une seule manière.

13. D'après le n° 7, le cas où Γ est cyclique nous fait retomber sur une représentation simplement imprimitive, ce qu'on a exclu. Si Γ est diédral, G admet un sous-groupe H' d'indice 2 tel que H'/H soit cyclique; alors, si on définit r' et H'' comme au n° 7, on voit, d'après le n° 7, que $H'' = H$ et $r' = 2$, ou bien que M est imprimitive. Dans l'un et l'autre cas, d'après le n° 11 et les hypothèses faites ci-dessus, Γ ne peut être autre que le groupe $E_2 \times E_2$ déjà considéré au n° 11. À côté de ce groupe, nous n'avons plus à examiner que $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$.

Le groupe $\mathfrak{A}_5$ est simple d'ordre 60 et ne peut figurer comme groupe de Galois d'une extension d'un corps local; nous l'excluons aussi désormais. Nous poserons $\Gamma_0 = \mathfrak{S}_4$, $\Gamma_1 = \mathfrak{A}_4$, $\Gamma_2 = E_2 \times E_2$. Nous regarderons $\mathfrak{A}_4$ comme sous-groupe de $\mathfrak{S}_4$ de la manière évidente, et nous identifierons Γ_2 avec l'unique sous-groupe d'ordre 4 de $\mathfrak{A}_4$. On a ainsi $\Gamma_0 \supset \Gamma_1 \supset \Gamma_2$; Γ_0 admet les suites de composition $(\Gamma_0, \Gamma_1, \Gamma_2, \Gamma')$, où Γ' est l'un des trois sous-groupes d'ordre 2 de Γ_2 , et n'en admet pas d'autre. On en conclut facilement que, si $p > 2$, un p -corps ne peut avoir d'extension dont le groupe de Galois soit Γ_0 ou Γ_1 . Si l'on accepte l'«hypothèse de travail» mentionnée au n° 1, cela «explique» la non-existence de représentations «extraordinaires» de $\text{GL}(2, k)$ quand k est un p -corps et que $p > 2$.

14. On posera $\Gamma_2 = \{\varepsilon, \alpha, \beta, \gamma\}$, où ε est l'élément neutre; on a $\alpha\beta\gamma = \varepsilon$. Il y a un élément ρ d'ordre 3 de Γ_1 (et un seul) tel que l'automorphisme intérieur $\sigma \mapsto \rho^{-1}\sigma\rho$ transforme α, β, γ en β, γ, α respectivement. Il y a un élément λ d'ordre 2 de Γ_0 (et un seul) tel que $\sigma \mapsto \lambda^{-1}\sigma\lambda$ transforme $\rho, \alpha, \beta, \gamma$ en $\rho^{-1}, \beta, \alpha, \gamma$ respectivement. On choisira un plongement fixe μ_0 de Γ_0 dans PL_2 , et on écrira μ_1, μ_2 pour ses restrictions à Γ_1, Γ_2 . Comme les μ_i sont uniques à des automorphismes près, on pourra supposer que les images de $\alpha, \beta, \gamma, \rho, \lambda$ par μ_0 sont respectivement les images dans PL_2 des éléments

$$\begin{aligned} z_\alpha &= \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, & z_\beta &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, & z_\gamma &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \\ z_\rho &= \frac{1+i}{2} \begin{pmatrix} i & 1 \\ i & -1 \end{pmatrix}, & z_\lambda &= \frac{i}{\sqrt{2}} \begin{pmatrix} 1 & i \\ -i & -1 \end{pmatrix} \end{aligned} \quad (2)$$

de SL_2 . Pour $i=0, 1, 2$, on notera Δ_i l'image réciproque de Γ_i dans SL_2 ; Δ_0 est engendré par $z_\alpha, z_\beta, z_\rho, z_\lambda$ et Δ_1 par $z_\alpha, z_\beta, z_\rho$; Δ_2 est le groupe $\{\pm 1, \pm z_\alpha, \pm z_\beta, \pm z_\gamma\}$ et est isomorphe au groupe U_8 des «unités quaternioniques» ($\{\pm 1, \pm i, \pm j, \pm k\}$ dans la notation usuelle des quaternions).

15. D'autre part, Γ_0 est isomorphe à $\text{PL}(2, \mathbf{F}_3)$, où $\mathbf{F}_3$ est le corps premier $\mathbf{Z}/3\mathbf{Z}$. On définit un isomorphisme μ'_0 de Γ_0 sur $\text{PL}(2, \mathbf{F}_3)$ en prenant pour images de $\alpha, \beta, \gamma, \rho, \lambda$ par μ'_0 les images dans $\text{PL}(2, \mathbf{F}_3)$ des éléments

$$\begin{aligned} z'_\alpha &= \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, & z'_\beta &= \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, & z'_\gamma &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\ z'_\rho &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, & z'_\lambda &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned}$$

de $GL(2, F_3)$. Ces matrices engendrent $GL(2, F_3)$, et on posera $\Delta'_0 = GL(2, F_3)$. On écrira aussi $\Delta'_1 = SL(2, F_3)$; c'est le groupe engendré par $z'_\alpha, z'_\beta, z'_\rho$; il est isomorphe à Δ_1 , et par suite le groupe Δ'_2 engendré par z'_α, z'_β est isomorphe à Δ_2 . En revanche, Δ'_0 n'est pas isomorphe à Δ_0 ; on le vérifiera tout à l'heure. L'intérêt des groupes Δ' tient à ce qu'ils interviennent dans la trisection des courbes elliptiques.

Pour $i=0, 1, 2$, l'intersection de Δ_i (resp. Δ'_i) avec $C^\times \cdot 1_2$ (resp. $F_3^\times \cdot 1_2$) est $E_2 = \{\pm 1_2\}$. Comme U_8 ne contient aucun sous-groupe isomorphe à $E_2 \times E_2$, Δ_2 (resp. Δ'_2) n'a pas de sous-groupe strict dont l'image dans PL_2 (resp. dans $PL(2, F_3)$) soit F_2 ; il en est donc de même pour tous les Δ_i, Δ'_i . D'après la remarque de la fin du n° 8, il s'ensuit que toute représentation (du type que nous étudions ici) d'un groupe G dans l'un de ces groupes est surjective.

16. Désormais on supposera $G/H = \Gamma_i$ avec $i=0, 1$ ou 2 ; on se propose principalement de classifier les représentations centrales M de G dans GL_2 , telles que $M^0 = \mu_i$, et subsidiairement de rechercher celles d'entre elles qui appliquent G sur Δ_i , et aussi, pour $i=0$, les représentations analogues sur Δ'_0 . Ces représentations seront dites respectivement «de type M_i », «de type Δ_i » et «de type Δ'_0 ». Comme précédemment, on posera toujours $M|_H = \Omega \cdot 1_2$.

Si $G/H = \Gamma_i$, avec $i=0, 1$ ou 2 , on conviendra d'écrire G_i au lieu de G , et on notera G_j , pour $i \leq j \leq 2$, l'image réciproque de F_j dans G_i , de sorte qu'on aura $G_j/H = \Gamma_j$. On posera $N_j = H \cap G_j^c$, donc en particulier $N_2 = G_2^c$ puisque F_2 est commutatif. On écrira J_j pour le sous-groupe de H engendré par les groupes $H^{\sigma-1}$ pour $\sigma \in \Gamma_j$, de sorte qu'on a $J_j \subset N_j$. On posera $G_j^* = G_j/J_j$, $H_j^* = H/J_j$; H_j^* est alors contenu dans le centre de G_j^* , et est en tout cas le centre de G_j^* pour $i=0$ ou 1 .

Pour $i \leq j \leq 2$, on notera M_j la restriction de M à G_j ; en particulier, on écrira M_i au lieu de M . Comme on l'a vu au n° 9, une telle représentation M_i est triviale sur J_i et peut être considérée comme une représentation de G_i^* ; de plus, d'après le n° 9, il ne peut exister de telle représentation M_i que si H_i^* est le centre de G_i^* . On va commencer par étudier les groupes G_i^* et leurs représentations, successivement pour $i=2, 1$ et 0 . Pour simplifier les notations, nous écrirons provisoirement G_i, H_i au lieu de G_i^*, H_i^* , ou, ce qui revient au même, nous supposerons (jusqu'au n° 20 inclus) que H_i est le centre de G_i .

17. Soit d'abord $i=2$. Soient A, B, C des représentants de α, β, γ dans G_2 . Posons $A^2=a, B^2=b, C^2=c, ABC=d, ABA^{-1}B^{-1}=f$; a, b, c, d, f sont dans H . Il est clair que G_2 est bien défini par H et par le «cocycle» (a, b, c, d) ; donc celui-ci détermine f , et en effet on a $f=d^{-2}abc$. Pour que (a, b, c, d) soit un cocycle, c'est-à-dire détermine

une extension G_2 de H , il faut et il suffit qu'on ait $f^2=1$. Le cocycle (a, b, c, d) est trivial s'il est de la forme (u^2, v^2, w^2, uvw) , avec u, v, w dans H ; on a alors $f=1$.

Le groupe G_2 est engendré par A, B et H ; donc $G_2^c = \{1, f\}$.

Soit Ω un caractère de H . D'après le n° 8, pour qu'il existe M_2 induisant $\Omega \cdot 1_2$ sur H , il faut et il suffit que l'image par Ω du cocycle (a, b, c, d) appartienne à la classe déterminée dans $H^2(\Gamma_2, \mathbb{C}^\times)$ par les éléments $z_\alpha, z_\beta, z_\gamma$ donnés par (2) au n° 14. Ceux-ci déterminent le cocycle $(-1, -1, -1, -1)$; la condition imposée à Ω s'écrit donc:

$$\Omega(a) = -x^2, \quad \Omega(b) = -y^2, \quad \Omega(c) = -z^2, \quad \Omega(d) = -xyz. \quad (3)$$

Pour que ces équations aient une solution (x, y, z) dans $(\mathbb{C}^\times)^3$, il faut et il suffit que l'on ait $\Omega(f) = -1$. Pour qu'il existe un tel caractère Ω , il faut et il suffit que $f \neq 1$. De même, pour que Ω détermine une représentation M_2 de type Δ_2 , il faut et il suffit que Ω soit d'ordre 2 et que (3) ait une solution dans $(E_2)^3$, c'est-à-dire qu'on ait

$$\Omega(a) = \Omega(b) = \Omega(c) = -1.$$

18. On obtient des résultats plus précis lorsque le groupe G_2 du n° 17 est muni d'un automorphisme ρ d'ordre 3 qui laisse H invariant et transforme α, β, γ en β, γ, α . On peut alors «normaliser» le choix de A, B, C , d'abord en convenant de prendre $B = A^\rho$, $C = B^\rho$, d'où $A = C^\rho$; cela donne $b = a^\rho$, $c = a^{\rho^2}$, $d = d^\rho$, $f = f^\rho = d^{-2} a^{1+\rho+\rho^2}$. Cela fait, posons

$$A_1 = A d^{-1} a, \quad B_1 = A_1^\rho = B d^{-1} b, \quad C_1 = B_1^\rho = C d^{-1} c,$$

puis

$$a_1 = A_1^2, \quad d_1 = A_1 B_1 C_1.$$

On trouve alors $d_1 = f$ et $a_1 = (a^{\rho+2})^{\rho-1} f$. Après avoir au besoin remplacé A, B, C par A_1, B_1, C_1 , on peut donc supposer le cocycle qui définit G_2 normalisé sous la forme $(a, a^\rho, a^{\rho^2}, f)$ avec $f = f^\rho$, $f^2 = 1$ et $a \in f \cdot H^{\rho-1}$. On a $f = f^{1+\rho+\rho^2}$; par conséquent f et a ne peuvent être dans $H^{\rho-1}$ que si $f = 1$.

19. Passons au cas $i=1$, H étant le centre de G_1 . Soit R un représentant de ρ dans G_1 ; alors $R^3 = h \in H$. On peut appliquer les résultats des n°s 17–18 au groupe G_2 muni de l'automorphisme $X \mapsto X^\rho = R^{-1} X R$; on a ici $H^{\rho-1} = 1$, et on peut prendre pour α, β, γ des représentants A, B, C normalisés comme au n° 18. Alors le cocycle qui définit G_2 est (f, f, f, f) , c'est-à-dire qu'on a

$$A^2 = B^2 = C^2 = ABC = ABA^{-1}B^{-1} = f, \quad f^2 = 1.$$

Elles expriment que A et B engendrent le groupe

$$\{1, A, B, C, f, fA, fB, fC\} \quad (4)$$

et que celui-ci est isomorphe à Δ_2 si $f \neq 1$ et à Γ_2 si $f = 1$. Dans ces conditions, G_1 est défini par le cocycle (f, h) , soumis à la seule condition $f^2 = 1$; il est trivial s'il est de la forme $(1, h'^3)$ avec $h' \in H$. Le groupe G_1^c est engendré par f et les commutateurs $X^{-1}R^{-1}XR$ pour $X = A, B, C$. Mais on a par exemple:

$$A^{-1}R^{-1}AR = A^{-1}B = A^{-2}(ABC)C^{-1} = C^{-1}.$$

Donc G_1^c n'est autre que le groupe (4), et on a $J_1 = \{1, f\}$.

D'après (2), le cocycle qui définit Δ_1 est $(-1, 1)$. Alors, pour qu'un caractère Ω de H détermine une représentation de type M_1 , il faut et il suffit qu'on ait $\Omega(f) = -1$; pour qu'il existe de tels caractères, il faut et il suffit que $f \neq 1$. Pour que Ω détermine une représentation de type Δ_1 , il faut et il suffit que Ω soit d'ordre 2 et que $\Omega(f) = -1$.

20. Soit enfin $i=0$, H étant le centre de G_0 ; on choisira A, B, C, R comme au n° 19, de sorte que G_1 est déterminé par le cocycle (f, h) .

Soit L un représentant de λ dans G_0 ; on a $L^2 = h_0 \in H$, et l'automorphisme $X \mapsto L^{-1}XL$ de G_0 est d'ordre 2. Il transforme G_1 , donc aussi G_1^c , en eux-mêmes; comme il transforme α, β, γ en β, α, γ , il doit transformer A, B, C en B, f, A ou Bf, A ou Af, C ou Cf , respectivement; s'il transforme R en R' , il transforme R' en R . L'image de R' dans Γ_0 est ρ^{-1} , donc on peut écrire $R' = R^{-1}h_1$ avec $h_1 \in H$; par suite, R et R' sont permutables. Appliquant l'automorphisme $X \mapsto L^{-1}XL$ aux relations $A = R^{-1}CR$, $B = RCR^{-1}$, on voit qu'il transforme (A, B, C) , soit en (B, A, C) , soit en (Bf, Af, Cf) ; en l'appliquant à la relation $ABC = f$, on voit qu'il transforme (A, B, C) en (Bf, Af, Cf) .

Posons $S = R^{-1}L^{-1}RL = R^{-1}R'$. Comme $R^3 = h$, on a aussi $R'^3 = h$; comme R et R' sont permutables, on a $S^3 = R^{-3}R'^3 = 1$. On a $S = R^{-2}h_1$, donc $S = Rh_2$ avec $h_2 = h^{-1}h_1$; donc S peut être substitué à R comme représentant de ρ dans G_1 ; la relation $S^3 = 1$ signifie que dans le cas présent G_1 est l'extension triviale de Γ_1/Γ_2 par G_2 . De plus, $X \mapsto L^{-1}XL$ transforme $S = Rh_2$ en $S' = R'h_2 = RS h_2 = S^2$; l'effet de cet automorphisme sur G_1 est ainsi complètement déterminé.

Le groupe G_0^c est engendré par S , par les commutateurs $X^{-1}L^{-1}XL$ pour $X = A, B, C$, et par G_1^c ; d'après ce qui précède, on a donc $G_0^c = G_1^c \cup SG_1^c \cup S^2G_1^c$, et $J_0 = \{1, f\}$. Le groupe G_0 est déterminé par le cocycle (f, h_0) , avec la seule condition $f^2 = 1$; il est trivial s'il est de la forme $(1, h'^2)$ avec $h' \in H$. Les cocycles qui déterminent Δ_0 et Δ'_0 sont respectivement $(-1, -1)$ et $(-1, 1)$; ils ne sont pas équivalents dans

$H^2(I_0, E_2)$, ce qui vérifie que Δ_0 et Δ'_0 ne sont pas isomorphes. Pour qu'un caractère Ω de H détermine une représentation de type M_0 , il faut et il suffit que $\Omega(f) = -1$; si de plus il est d'ordre 2, il déterminera une représentation de type Δ_0 ou de type Δ'_0 suivant que $\Omega(h_0)$ est -1 ou 1 .

21. Revenons au cas général où on ne suppose pas H central dans G_i ; on peut appliquer les n°s 17–20 aux groupes $G_i^* = G_i/J_i$.

Pour $i=0, 1, 2$, on choisira des représentants A, B de α, β dans G_i ; on posera $A^2=a, B^2=b, ABA^{-1}B^{-1}=f$; a, b, f sont des éléments de H , bien déterminés modulo $H^{1+\alpha}$, modulo $H^{1+\beta}$, et modulo J_2 , respectivement; on a $f^2 \in J_2$. Pour $i=0$ ou 1 , on peut appliquer à G_i/J_2 ce qui a été démontré au n° 18; comme l'image de J_1 dans ce groupe est alors le groupe $(H_2^*)^{p-1}$ avec $H_2^* = H/J_2$, on voit que, si $f \notin J_2$, on a aussi $f \notin J_1$.

Pour $i=0$, on choisira aussi un représentant L de λ dans G_0 et on posera $L^2=h_0$; c'est un élément de H , bien déterminé modulo $H^{1+\lambda}$.

Nous avons démontré entre autre ce qui suit:

(A) On a toujours $N_i = H \cap G_i^c = J_i \cup fJ_i$; on a $G_2^c = N_2$; G_1^c/J_1 est isomorphe à I_2 ou à Δ_2 suivant que f est ou non dans J_1 ; G_0^c/J_0 est isomorphe à I_1 ou à Δ_1 suivant que f est ou non dans J_0 .

(B) Pour que G_i admette une représentation de type M_i , il faut et il suffit que f ne soit pas dans J_i .

(C) Pour que G_i admette une représentation de type Δ_i (resp. Δ'_0), il faut et il suffit que H admette un caractère Ω d'ordre 2, trivial sur J_i , satisfaisant aux conditions suivantes:

$$\begin{aligned} &\text{pour } i=2, \quad \Omega(f) = -1 \quad \text{et} \quad \Omega(a) = \Omega(b) = -1; \\ &\text{pour } i=1, \quad \Omega(f) = -1; \\ &\text{pour } i=0, \quad \Omega(f) = -1 \quad \text{et} \quad \Omega(h_0) = -1 \quad \text{pour le type } \Delta_0 \\ &\hspace{15em} (\text{resp. } \Omega(h_0) = 1 \text{ pour le type } \Delta'_0). \end{aligned}$$

22. Le cas qui nous importe est celui où on se donne une extension galoisienne finie K d'un corps local k et où on prend $G = W(K_{\text{ab}}/k)$, $H = K^\times$. $\Gamma = \text{Gal}(K/k)$. On a vu au n° 2 que tout morphisme μ de Γ dans un groupe PL_n se relève à une représentation M de G dans GL_n , telle que $M^0 = \mu$. Il en sera ainsi en particulier chaque fois que $n=2$ et qu'on prend pour Γ et μ l'un des groupes I_i et le morphisme μ_i correspondant. Autrement dit, chaque fois qu'on se donne un corps local k , une extension K de k de groupe de Galois Γ_i , et qu'on prend $G = W(K_{\text{ab}}/k)$, $H = K^\times$, ces données satisfieront à la condition (B) du n° 21. Bien entendu, on pourrait le vérifier directement sans faire appel à la théorie générale citée au n° 2; nous en laisserons l'amusement au lecteur.

23. Pour aller plus loin, nous adopterons les notations suivantes. Soit K un p -corps admettant Γ_i comme groupe d'automorphismes. Pour $i \leq j \leq 2$, on notera k_j le corps des invariants de Γ_j dans K , et on prendra $G_j = W(K_{ab}/k_j)$, $H = K^\times$; comme on l'a noté au n° 5, on peut identifier $k_j^\times$ avec G_j/G_j^c , et la norme N_{K/k_j} avec la restriction à $K^\times$ de l'homomorphisme canonique de G_j sur G_j/G_j^c . On écrira $N^{(j)}$ au lieu de N_{K/k_j} ; le noyau de $N^{(j)}$ est $N_j = J_j \cup fJ_j$. Pour $\sigma \in \Gamma_i$, on notera K_σ le corps des invariants de σ dans K , et on posera $N_\sigma = N_{K/K_\sigma}$; le noyau de N_σ est $(K^\times)^{\sigma-1}$. On écrira aussi $k = k_i$, et on notera π, π_j, Π des éléments premiers de k, k_j, K , respectivement. On notera R l'anneau des entiers de K ; alors $R^\times$ est le groupe des «unités» de K , et les groupes N_j sont contenus dans $R^\times$.

En vertu des résultats connus sur la ramification des corps locaux, les cas qui peuvent se présenter sont les suivants. Si $p > 2$, i ne peut prendre que la valeur 2; si k est donné, il admet une seule extension K de groupe de Galois Γ_2 . Si $p = 2$, i peut prendre les valeurs 2, 1 et 0. Si $i = 1$ et qu'on se donne $k = k_1$, il y a une seule extension cyclique k_2 de degré 3 de k , ou il y en a quatre, suivant que k contient ou non les racines cubiques de 1; l'une est non ramifiée sur k , et les autres, s'il y en a, sont modérément ramifiées. Si $i = 0$, k_1 est l'unique extension non ramifiée de k de degré 2; k_2 est cyclique de degré 3, modérément ramifié sur k_1 . Pour $i = 1$ ou 0, K est totalement (et même «sauvagement») ramifié sur k_2 .

24. On a vu au n° 22 que la condition (B) du n° 21 est toujours vérifiée. En ce qui concerne (C), la question n'est pas si simple. On va voir d'abord, pour $i = 0$, que les conditions relatives à Δ_0 et à Δ'_0 sont équivalentes. Dans ce cas, en effet, le groupe de Galois de K sur K_λ est $\{\varepsilon, \lambda\}$ et s'identifie au groupe de k_1 sur k ; donc $K = K_\lambda k_1$. Comme k_1 est non ramifié sur k , K l'est sur K_λ . Alors, si L est un représentant de λ dans $W(K_{ab}/K_\lambda)$ et si $L^2 = h_0$, on sait que h_0 est un élément de K_λ d'ordre impair; on peut par exemple choisir L de façon que h_0 soit n'importe quel élément premier dans K_λ , et alors c'est aussi un élément premier dans K . Soit θ le caractère de $K^\times$ donné par $\theta(x) = (-1)^{\text{ord } x}$; on a $\theta(h_0) = -1$, et θ est trivial sur $R^\times$, donc sur $N_0 = J_0 \cup fJ_0$. Si donc Ω est un caractère d'ordre 2 de $K^\times$, trivial sur J_0 et tel que $\Omega(f) = -1$, il en est de même de $\Omega\theta$, et l'un des caractères $\Omega, \Omega\theta$ de $K^\times$ prend la valeur 1 en h_0 tandis que l'autre y prend la valeur -1 .

Pour qu'un caractère de H soit d'ordre 2, il faut et il suffit qu'il soit trivial sur H^2 . On voit donc que, pour $i = 0$ ou 1, la condition (C) du n° 21 peut être remplacée par la suivante: (C') $K^\times$ admet un caractère trivial sur $(K^\times)^2 J_i$ et $\neq 1$ en f ; ou bien encore: $fJ_i \cap (K^\times)^2 = \emptyset$. Comme le noyau de $N^{(i)}$ est $N_i = J_i \cup fJ_i$, cela revient à dire que, pour $x \in K^\times$, $N^{(i)}(x^2) = 1$ entraîne $x^2 \in J_i$. Mais $N^{(i)}(x) = 1$ entraîne $x \in J_i$ ou $x \in fJ_i$,

donc $x^2 \in J_i$ puisque $f^2 \in J_i$. Par suite (C) équivaut à dire que $N^{(i)}(x) = -1$ entraîne $x^2 \in J_i$. On voit en particulier que cette condition est toujours vérifiée si K est de caractéristique 2, puisqu'alors $-1 = 1$.

Nous bornerons à ces remarques l'examen de la condition (C), et nous laisserons au lecteur le soin de vérifier que, pour $p > 2$, un corps local k n'admet aucune extension de groupe de Galois $\Delta_2 = U_8$, ou bien en admet une et une seule, suivant qu'il contient ou non $\sqrt{-1}$.

25. Supposant dorénavant k donné, avec $p=2$, nous allons procéder à la construction et à l'énumération des extensions K de k de groupe de Galois Γ_0 ou Γ_1 ; les notations seront comme ci-dessus.

Pour $i=0$, on a déjà dit que k_1 ne peut être que l'unique extension non ramifiée de degré 2 de $k_0=k$, et que k_2 doit être cyclique et modérément ramifiée sur k_1 . Soit $q=2^m$ le module de k_0 (nombre d'éléments du corps résiduel $\mathbf{F}_q$); celui de k_1, k_2, K sera q^2 , et k_1 contiendra les racines de $x^3=1$; un élément premier π de k en sera un aussi pour k_1 . Soit η un générateur du groupe des racines de l'unité d'ordre impair dans k_1 ; ce groupe est d'ordre q^2-1 , et η^{q+1} engendre le groupe analogue pour k_0 . Il y a trois extensions modérément ramifiées de degré 3 de k_1 ; ce sont les corps $k_1(y)$, où y est racine d'une des équations $y^3 = \eta^a \pi$ avec $a \equiv 0, 1$ ou $2 \pmod{3}$. Si $q \equiv 1 \pmod{3}$, donc si k_0 contient les racines de $x^3=1$, on peut prendre en même temps $a \equiv 0 \pmod{q+1}$; mais alors $\eta^a \pi$ est dans k_0 , et $k_0(y)$, donc aussi $k_1(y)$, sont abéliens sur k_0 , ce qui est exclu. Dans le cas présent, on doit donc avoir $q \equiv 2 \pmod{3}$, c'est-à-dire que m est impair. Mais alors $k_1(y)$ n'est galoisien sur k_0 que pour $a=0$. Donc on a $k_2 = k_1(\pi_2)$ avec $\pi_2 = \pi^{\frac{1}{3}}$.

26. Pour $i=1$, on peut en tout cas prendre pour k_2 l'unique extension non ramifiée de degré 3 de $k=k_1$. Si le module de k_1 est $q=2^m$ avec m impair, c'est là la seule extension cyclique de degré 3 de k_1 ; on prendra alors $\pi_2 = \pi$. Si $q=2^m$ avec m pair, k_1 contient les racines de $x^3=1$ et admet trois extensions modérément ramifiées de degré 3; ce sont les corps $k_1(\pi_2)$ avec $\pi_2^3 = \eta^a \pi$, où η est de nouveau un générateur du groupe des racines de 1 d'ordre impair dans k_1 , et $a=0, 1$ ou 2 . Dans tous les cas, π_2^3 est dans k_1 .

27. Pour chaque i , on notera P_i l'idéal maximal (π_i) dans l'anneau des entiers de k_i ; $1+P_i$ est alors le groupe des éléments $\equiv 1 \pmod{P_i}$ dans cet anneau, et $k_i^\times$ est produit direct de $1+P_i$, du groupe des racines de 1 d'ordre impair dans k_i et du groupe engendré par π_i . Si $\mathbf{Z}_2$ désigne comme d'habitude l'anneau des entiers dyadiques, on peut, comme on sait, considérer le groupe multiplicatif $1+P_i$ comme $\mathbf{Z}_2$ -module; si N est le plus grand entier tel que k_i contienne les racines de 1 d'ordre 2^N , ces racines forment le module de torsion du module $1+P_i$;

on a $N=0$ si k_i est de caractéristique 2. En tout cas, $1+P_i$ est produit direct de son module de torsion et d'un module libre, dont le rang δ_i sur $\mathbf{Z}_2$ est dénombrablement infini si k_i est de caractéristique 2, et est égal au degré de k_i sur $\mathbf{Q}_2$ dans le cas contraire. Comme k_2 est de degré 3 sur k_1 , le module de torsion de $1+P_2$ est le même que celui de $1+P_1$.

28. Il s'agit maintenant de construire l'extension K de k_2 ; on peut le faire, soit directement, soit au moyen de la théorie du corps de classes local; nous commencerons par cette dernière méthode, qui s'applique également aux cas de caractéristique 0 et 2. De ce point de vue, tout revient à construire un sous-groupe g de $k_2^\times$ tel que $k_2^\times/g$ soit isomorphe à Γ_2 et que le groupe de Galois de k_2 sur k opère sur $k_2^\times/g$ conformément aux données du problème. Soit χ l'un des trois caractères non triviaux de Γ_2 , si $i=1$; soit χ celui des trois qui est donné par $\chi(\gamma)=1$, si $i=0$; les deux autres sont χ^ρ, χ^{ρ^2} ; on a $\chi^{1+\rho+\rho^2}=1$, et $\chi=\chi^\lambda$ si $i=0$. On est donc ramené à construire un caractère ψ d'ordre 2 de $k_2^\times$ satisfaisant à $\psi^{1+\rho+\rho^2}=1$, et à $\psi=\psi^\lambda$ pour $i=0$; K sera l'extension de k_2 correspondant à l'intersection des noyaux de $\psi, \psi^\rho, \psi^{\rho^2}$; s'il y a N caractères ψ , il y aura $N/3$ corps K pour $i=1$, et il y en aura N pour $i=0$.

La condition $\psi^{1+\rho+\rho^2}=1$ s'écrit aussi $\psi(x^{1+\rho+\rho^2})=1$ pour tout $x \in k_2^\times$, ce qui revient à dire que ψ est trivial sur l'image de $k_2^\times$ par la norme N_{k_2/k_1} ; comme cette image est d'indice 3 dans $k_1^\times$ et que ψ est d'ordre 2, il revient au même de dire que ψ est trivial sur $k_1^\times$. Comme on a vu qu'en tout cas π_2^3 est dans $k_1^\times$, on a donc $\psi(\pi_2)=1$. Evidemment, ψ est trivial aussi sur le groupe des racines de 1 d'ordre impair dans $k_2^\times$. Il n'y a donc à examiner que la restriction de ψ à $1+P_2$.

29. Pour la commodité de l'écriture, on va noter additivement les modules $1+P_i$; au lieu de $1+P_i$, on écrira $\mathfrak{M}_i$, et, pour $m \in \mathfrak{M}_i$, on notera σm l'image de m par un automorphisme σ de k_i . On rappelle que le module de torsion de $\mathfrak{M}_2$ est contenu dans $\mathfrak{M}_1$.

Pour $m \in \mathfrak{M}_2$, posons $m_1 = (1+\rho+\rho^2)m$; alors m_1 est dans $\mathfrak{M}_1$, et il en est de même de $\frac{1}{3}m_1$ puisque $\frac{1}{3}$ est dans $\mathbf{Z}_2$. Si on pose $m' = m - \frac{1}{3}m_1$, m' sera dans le noyau $\mathfrak{M}'$ de l'endomorphisme $1+\rho+\rho^2$ de $\mathfrak{M}_2$. On voit donc que $\mathfrak{M}_2$ est somme directe de $\mathfrak{M}_1$, sur lequel ψ est trivial, et de $\mathfrak{M}'$, qui est donc un module libre sur $\mathbf{Z}_2$, de rang $2\delta_1$ sur $\mathbf{Z}_2$. Puisque $(1+\rho+\rho^2)\mathfrak{M}'=0$, on peut même considérer $\mathfrak{M}'$ comme module de rang δ_1 sur l'anneau $\mathbf{Z}_2[\rho]$ des entiers de l'extension $\mathbf{Q}_2(\rho)$ de $\mathbf{Q}_2$ par une racine cubique de 1; $\mathbf{Q}_2(\rho)$ est l'unique extension non ramifiée de degré 2 de $\mathbf{Q}_2$. Tout caractère ψ d'ordre 2 de $\mathfrak{M}'$ satisfait évidemment à la condition $\psi^{1+\rho+\rho^2}=1$. Il y a $2^{2\delta_1}-1$ tels caractères. Donc, pour un choix donné de k_2 , il y a $(2^{2\delta_1}-1)/3$ extensions K de k_2 dont le groupe de Galois sur k_1 est Γ_1 .

30. Pour $i=0$, il est clair que $\mathfrak{M}_1$ et $\mathfrak{M}'$ sont invariants par λ ; λ est une involution «antilinéaire» du module $\mathfrak{M}'$ sur $\mathbf{Z}_2[\rho]$, c'est-à-dire qu'elle transforme ρ en ρ^{-1} . Pour $m \in \mathfrak{M}'$, posons:

$$m_1 = \frac{1}{3}(\lambda + 1)(1 - \rho)m, \quad m_2 = -\frac{1}{3}(\lambda + 1)(1 + 2\rho)m.$$

On vérifie aussitôt que $m = m_1 + \rho m_2$; de plus, si $\mathfrak{M}''$ désigne l'ensemble des $m \in \mathfrak{M}'$ qui sont invariants par λ (c'est un module sur $\mathbf{Z}_2$, mais non sur $\mathbf{Z}_2[\rho]$), on a $m_1 \in \mathfrak{M}''$, $m_2 \in \mathfrak{M}''$. De plus, on vérifie immédiatement que $\mathfrak{M}' \cap (\rho \mathfrak{M}'') = \{0\}$. Donc $\mathfrak{M}'$ est somme directe de $\mathfrak{M}''$ et de $\rho \mathfrak{M}''$, ou autrement dit on peut mettre tout $m \in \mathfrak{M}'$, d'une manière et d'une seule, sous la forme $m_1 + \rho m_2$ avec m_1, m_2 dans $\mathfrak{M}''$. On a, dans ces conditions,

$$\lambda(m_1 + \rho m_2) = (m_1 - m_2) - \rho m_2.$$

Par suite, pour qu'un caractère ψ de $\mathfrak{M}'$ soit invariant par λ , il faut et il suffit qu'on ait, pour tout $m_2 \in \mathfrak{M}''$:

$$\psi(\rho m_2) = \psi(-m_2) \psi(-\rho m_2),$$

ce qui, pour ψ d'ordre 2, équivaut à dire que ψ doit être trivial sur $\mathfrak{M}''$; il peut alors être choisi arbitrairement sur $\rho \mathfrak{M}''$. Comme $\mathfrak{M}''$ et $\rho \mathfrak{M}''$ sont de rang δ_1 sur $\mathbf{Z}_2$, cela revient à dire qu'il y a $2^{\delta_1} - 1$ choix possibles pour ψ , donc aussi pour K , lorsqu'on s'est donné k_0, k_1, k_2 comme au n° 25.

31. Quant à la construction effective de K , nous nous contenterons d'énoncer les résultats, en commençant par le cas de caractéristique 2; dans ce cas, d'après le n° 24, toute solution K du problème admet une extension quadratique K' dont le groupe de Galois sur k est Δ_1 (resp. Δ'_0).

Pour $i=1$, supposons d'abord que $k=k_1$ ne contienne pas les racines de $j^3=1$. Alors $k_2=k\mathbf{F}_Q$ avec $Q=q^3$, q étant toujours le module de k , et ρ est l'automorphisme de Frobenius de k_2 sur k , donné par $x^\rho = x^q$ pour $x \in \mathbf{F}_Q$. Dans ce cas, K est de la forme $K=k_2(x, x', x'')$ avec $x^2 - x = a$, $x'^2 - x' = a^\rho$, $x''^2 - x'' = a^{\rho^2}$, où a est un élément de k_2 tel que $a + a^\rho + a^{\rho^2} = 0$ et que K soit de degré 4 sur k_2 .

Supposons maintenant qu'on ait $i=1$ et que $k=k_1$ contienne les racines de $j^3=1$, ou bien que $i=0$; dans les deux cas on a $k_1=k(j)$. On trouve que K est de la forme $K=k(x, y)$ avec $x^3=a$, $y^4-y=x$, avec a dans $k^\times$ et tel que K soit de degré 12 sur k_1 . Si on prend $K'=K(z)$ avec $z^2-z=y^3$, K' est le corps défini sur k par la trisection de la courbe elliptique $Y^2+XY=X^3+X^2+a$; son groupe de Galois sur k est Δ_1 si $i=1$ et Δ'_0 si $i=0$.

Soit maintenant k de caractéristique 0. Au n° 29, on a noté $\mathfrak{M}_i$ le module $1+P_i$, écrit additivement, et on a introduit un sous-module $\mathfrak{M}'$

de $\mathfrak{M}_2$, qui est le noyau de $1 + \rho + \rho^2$. Nous noterons maintenant U' le sous-groupe de $1 + P_2$ qui correspond à $\mathfrak{M}'$; c'est l'intersection de $1 + P_2$ avec le noyau de la norme N_{k_2/k_1} dans $k_2^\times$. Pour $i=0$, on a aussi introduit au n° 30 un sous-module $\mathfrak{M}''$ de $\mathfrak{M}'$; on notera U'' le sous-groupe correspondant de U' ; c'est le groupe des éléments de U' invariants par λ ; d'après le n° 30, il s'écrit aussi $U'' = U'^{1+\lambda}$.

Cela posé, pour k_1 et k_2 donnés comme aux n°s 25–26, K sera donné par $K = k_2(x^{\frac{1}{p}}, y^{\frac{1}{p}}, z^{\frac{1}{p}})$ avec $y = x^p$, $z = x^{p^2}$, $x \in U'$ si $i=1$, et $x \in U''$ si $i=0$.

32. Une fois construites les représentations de type M_i des groupes $G = W(K_{ab}/k)$, la question la plus importante qui se pose à leur sujet est la détermination de leurs conducteurs. Nous ferons dépendre ce calcul de quelques lemmes généraux sur la «distribution de Herbrand» (cf. A. Weil, *Basic Number Theory*, Chap. VIII, § 3, et App. IV).

Soit k un p -corps. Dans k_{sep} , soit k_{nr} l'extension non ramifiée maximale de k , et soit k_{mr} son extension modérément ramifiée maximale; k_{nr} et k_{mr} sont engendrés, respectivement, par les racines de toutes les équations $X^n = 1$, et par celles de toutes les équations $X^n = \pi$, où π est un élément premier de k et où on prend pour n tous les entiers premiers à p . Soient $\mathfrak{G}$, $\mathfrak{G}_0$, $\mathfrak{G}_1$ les groupes de Galois de k_{sep} sur k , k_{nr} , k_{mr} , respectivement; $\mathfrak{G}_0$, $\mathfrak{G}_1$ sont aussi les W -groupes de k_{sep} sur k_{nr} , k_{mr} , et la distribution de Herbrand H sur G est nulle en dehors de $\mathfrak{G}_0$ (*loc. cit.* App. IV). De plus:

Lemme 1. Sur $\mathfrak{G}_0 - \mathfrak{G}_1$, $-H$ coïncide avec la mesure de Haar H_0 sur $\mathfrak{G}_0$, normée par $H_0(\mathfrak{G}_0) = 1$.

C'est une conséquence immédiate des définitions. Par «fonctorialité» (*loc. cit.* App. IV), on en déduit une propriété analogue pour tout groupe de Galois et tout W -groupe. Soit en particulier K une extension galoisienne de k de degré fini, de groupe de Galois Γ ; soit $G = W(K_{ab}/k)$. Posons $k' = K \cap k_{nr}$, $k'' = K \cap k_{mr}$; soient Γ' , Γ'' les sous-groupes correspondants de Γ , c'est-à-dire le groupe d'inertie et le premier groupe de ramification de K sur k . Les images réciproques de Γ' , Γ'' dans G sont les groupes $G' = W(K_{ab}/k')$, $G'' = W(K_{ab}/k'')$. Le sous-groupe compact maximal de G est $G_c = W(K_{ab}/k_{nr})$; c'est aussi le groupe de Galois de K_{ab} sur k_{nr} . Notons de même G'_c , G''_c les sous-groupes compacts maximaux de G' , G'' ; comme $k' \subset k_{nr}$, on a $G_c = G'_c$; G'_c , G''_c sont respectivement des extensions de Γ' et de Γ'' par le groupe $R^\times$ des «unités» de $K^\times$. Soit alors H la distribution de Herbrand sur G ; elle est 0 en dehors de G_c . Le lemme 1 donne alors:

Lemme 2. Sur $G_c - G''_c$, $-H$ coïncide avec la mesure de Haar H_0 sur G_c , normée par $H_0(G_c) = 1$.

Soit maintenant M une représentation centrale de G dans GL_r au sens du n° 6, c'est-à-dire telle que sa restriction à $H=K^\times$ soit de la forme $M|_H = \Omega \cdot 1_r$; supposons de plus que Ω ne soit pas trivial sur $R^\times$. Posons $\chi = \text{tr } M$. L'ordre F du conducteur de M est donné, comme on sait, par $F = H(\chi)$.

Pour tout $\sigma \in \Gamma'$, on peut prendre un représentant g_σ dans G'_c . Comme H est 0 en dehors de G'_c , on a donc:

$$F = H(\chi) = \sum_{\sigma \in \Gamma'} \int_{g_\sigma R^\times} \chi(g) dH(g) = \sum_{\sigma \in \Gamma'} \chi(g_\sigma) \int_{R^\times} \Omega(x) dH(g_\sigma x).$$

Puisque Ω n'est pas trivial sur $R^\times$, les termes relatifs aux éléments σ de $\Gamma' - \Gamma''$ sont nuls dans cette dernière somme, en vertu du lemme 2. On a donc $F = \int_{G''} \chi dH$. Soit H'' la distribution de Herbrand sur $G'' = W(K_{ab}/k'')$; on sait (*loc. cit.* App. IV) qu'on a $H'' = eH - d\delta_1$, où δ_1 est la masse 1 concentrée en l'élément neutre, où e est l'ordre de ramification de k'' sur k , et d son «exposant différentiel»; on a $e = [k'':k']$ et $d = e - 1$. Par suite, avec ces hypothèses:

Lemme 3. *Soit M'' la restriction de M à G'' ; soit F'' l'ordre du conducteur de M'' , relativement au corps de base k'' . Alors $eF = F'' + r(e-1)$, avec $e = [k'':k']$.*

33. En ce qui concerne les représentations de type M_i étudiées plus haut, le lemme 3 du n° 32 ramène le calcul de leurs conducteurs à ce même calcul pour $i=2$; dans ce lemme, on doit prendre $r=2$, $k''=k_2$, $M''=M_2$, et $e=3$ ou 1 suivant que k_2 est ramifié ou non sur le corps de base k ; cela donne $F = \frac{1}{3}(F''+4)$ resp. $F = F''$.

Quant au type M_2 , soit K_α , comme précédemment, le corps des invariants de α dans K . Toujours avec les mêmes notations, le caractère Ω de $H=K^\times$ est trivial sur le noyau $H^{\alpha-1}$ de la norme $N_\alpha = N_{K/K_\alpha}$; donc on peut écrire $\Omega = \omega_\alpha \circ N_\alpha$, où ω_α est un caractère de $K_\alpha^\times$. Soit F_α l'ordre du conducteur de ω_α dans K_α . Si G_α est l'image réciproque dans G_2 du sous-groupe $\{\varepsilon, \alpha\}$ de Γ_2 , on peut identifier $K_\alpha^\times$ avec G_α/G_α^c et par suite considérer ω_α comme représentation de G_α de degré 1. Alors, d'après le n° 10, M'' n'est autre que $[\omega_\alpha; G_\alpha \rightarrow G_2]$; on sait que l'ordre du conducteur de M'' est alors $F'' = 2F_\alpha$ si K_α est non ramifié sur k_2 (ce qui ne peut arriver pour $i=0$ ou 1), et $F'' = F_\alpha + D$ dans le cas contraire, D étant l'exposant différentiel de K_α sur k_2 .

34. Pour terminer, nous donnerons l'énumération des types M_1, M_0 quand le corps de base est $k = \mathbf{Q}_2$.

Quant au type M_1 , le n° 29 montre que K est déterminé d'une manière unique. On doit d'abord prendre $k_2 = \mathbf{Q}_2(\eta)$ avec $\eta^7 = 1$. Soit $a = (1-8)^{\frac{1}{2}} =$

$1 - \frac{1}{2} \cdot 8 + \dots$; on a $a \in \mathbf{Z}_2$ et $a \equiv 5 \pmod{8}$. Si on pose $y = \eta + \eta^2 + \eta^4$, on a $y^2 + y + 2 = 0$, $y = \frac{1}{2}(\pm a - 1)$; on peut supposer qu'on ait choisi la racine η de $\eta^7 = 1$ de façon que $y = \frac{1}{2}(a - 1)$. On a alors:

$$\begin{aligned} N(Y - \eta) &= (Y - \eta)(Y - \eta^2)(Y - \eta^4) \\ &= Y^3 - \frac{a-1}{2} Y^2 - \frac{a+1}{2} Y - 1, \end{aligned}$$

d'où résulte que $N(1 + 2\eta) = 6 - a \equiv 1 \pmod{8}$. On peut donc écrire $N(1 + 2\eta) = x^2$, puis $x = z^3$, avec x, z dans $\mathbf{Z}_2$ et $x \equiv z \equiv 1 \pmod{4}$. Par suite $z^{-2}(1 + 2\eta)$ est dans le sous-groupe $1 + P_2$ de $k_2^\times$, et en même temps dans le noyau de la norme $N_{k_2/k}$. D'après le n° 31, on pourra donc prendre $K = k_2(\xi, \xi', \xi'')$, avec

$$\xi^2 = 1 + 2\eta, \quad \xi'^2 = 1 + 2\eta^2, \quad \xi''^2 = 1 + 2\eta^4,$$

et il n'y a pas d'autre corps K satisfaisant aux conditions imposées. On peut supposer les notations choisies de manière que $\eta^\rho = \eta^2$.

35. On va montrer, au moyen du critère du n° 24, que la condition (C) du n° 21 n'est pas vérifiée, et même qu'on a $f \in (K^\times)^2 J_2$.

Si K_ρ est le corps des éléments de K invariants par ρ , on a $K = K_\rho(\eta)$; donc K_ρ est totalement ramifié sur $\mathbf{Q}_2$, et un élément premier Π de K_ρ (qui en est un aussi pour K) est racine d'un polynôme d'Eisenstein sur $\mathbf{Q}_2$. Réciproquement, donnons-nous un tel polynôme

$$F(X) = X^4 + 2aX^3 + 2bX^2 + 2cX + 2,$$

avec a, b, c dans $\mathbf{Z}_2$; soit Π une racine de F . On sait que F est irréductible sur $\mathbf{Q}_2$ et que Π est un élément premier de $\mathbf{Q}_2(\Pi)$; donc le groupe de Galois de F , considéré comme groupe g de permutations sur Π et ses conjugués, est transitif. Si le discriminant de F est un carré dans $\mathbf{Q}_2$, g est un sous-groupe de $\mathfrak{A}_4 = \Gamma_1$; c'est donc Γ_1 ou bien Γ_2 . Si $g = \Gamma_1$, le corps engendré par Π et ses conjugués sur $\mathbf{Q}_2$ ne peut être que K ; on peut identifier $\mathbf{Q}_2(\Pi)$ avec K_ρ ; les autres racines de F sont alors $\Pi^\alpha, \Pi^\beta, \Pi^\gamma$ et sont dans $K = \mathbf{Q}_2(\Pi, \eta)$. Si $g = \Gamma_2$, toutes les racines de F sont dans $\mathbf{Q}_2(\Pi)$. Soit Π' une racine de F autre que Π ; on peut en tout cas écrire $\Pi' = \sum_{i=1}^{\infty} \varepsilon_i \Pi^i$, où les coefficients ε_i sont 0 ou 1 si Π' est dans $\mathbf{Q}_2(\Pi)$ et sont 0 ou bien de la forme η^m si Π' est dans $\mathbf{Q}_2(\Pi, \eta)$. Ecrivant $F(\Pi') = 0$, on trouve successivement $\varepsilon_1 = 1$, $c \equiv 0 \pmod{2}$, puis que ε_2 ne peut être 0 ou 1 que si $a \equiv 0$ ou $b \equiv 0 \pmod{2}$. D'ailleurs, si $a \equiv b \equiv 1$ et $c \equiv 0 \pmod{2}$, on vérifie que le discriminant de F est bien un carré dans $\mathbf{Z}_2$. On pourra prendre par exemple

$$F(X) = X^4 - 2X^3 - 2X^2 + 2.$$

Par approximations successives, on trouve alors que F admet une racine de la forme $\Pi' = \Pi + \eta \Pi^2 + \eta^2 \Pi^3 + \dots$; on peut supposer les notations choisies de manière que $\Pi^a = \Pi'$. On aura alors

$$\Pi^\beta = \Pi'^\rho = \Pi + \eta^2 \Pi^2 + \eta^4 \Pi^3 + \dots$$

Cela posé, on a $N_{K/\mathbf{Q}_2}(1 - \Pi) = -1$, c'est-à-dire

$$(1 - \Pi)^{1+\alpha+\beta+\gamma} = -1.$$

D'après le n° 24, il nous suffira, pour achever la démonstration, de faire voir qu'on ne peut satisfaire à l'équation

$$(1 - \Pi)^2 = u^{\alpha-1} v^{\beta-1}$$

avec u, v dans $K^\times$. On peut mettre u sous la forme

$$u = \eta^m \Pi^a \cdot (1 + e \Pi) u',$$

avec m et a dans $\mathbf{Z}$, e égal à 0 ou bien de la forme η^n , et $u' \equiv 1 \pmod{\Pi^2}$. On a alors, si a est pair:

$$u^{\alpha-1} \equiv 1 + \left(e \eta + \frac{a}{2} \eta^2 \right) \Pi^2 + (e \eta^2 + e^2 \eta) \Pi^3 \pmod{\Pi^4},$$

et $u^{\alpha-1} \equiv 1 + \eta \Pi \pmod{\Pi^2}$ si a est impair. On a bien entendu des formules analogues pour $v^{\beta-1}$. Il est facile alors de vérifier que même la congruence

$$(1 - \Pi)^2 \equiv u^{\alpha-1} v^{\beta-1} \pmod{\Pi^4}$$

n'a pas de solution.

36. Passons au type M_2 , toujours sur le corps de base $k = \mathbf{Q}_2$. Il faut prendre alors $k_1 = k(j)$, avec $j^2 + j + 1 = 0$ (donc $j^3 = 1$), puis $k_2 = k_1(\pi)$ avec $\pi^3 = 2$; on peut supposer les notations choisies de manière que $j^\lambda = j^2$, $\pi^\lambda = \pi$, $\pi^\rho = j\pi$. D'après le n° 30, il y a trois extensions K de k_2 satisfaisant aux conditions du problème; d'après le n° 31, elles sont de la forme $k_2(x^{\frac{1}{2}}, y^{\frac{1}{2}}, z^{\frac{1}{2}})$, où $y = x^\rho$, $z = x^{\rho^2}$, $x^\lambda = x$, $x \equiv 1 \pmod{\pi}$, et où $xyz = 1$; on peut d'ailleurs, sans rien changer, remplacer cette dernière condition par la condition plus faible $xyz \in (k_1^\times)^2$, c'est-à-dire $xyz \equiv 1 \pmod{4}$. Pour que deux éléments x, x' satisfaisant à ces conditions déterminent le même corps K , il faut et il suffit que $x^{-1} x'$ soit dans $(k_2^\times)^2$, et il suffit que $x' \equiv x \pmod{4}$. On pourra donc prendre pour x un produit de facteurs distincts de la forme $1 + \pi^m$ avec $1 \leq m < 6$. Tenant compte des conditions ci-dessus, on trouve, comme prévu, trois solutions

$$K_{ab} = k_2((x_{ab})^{\frac{1}{2}}, (x_{ab}^\rho)^{\frac{1}{2}}),$$

avec $x_{ab} = (1 + \pi)^a (1 + \pi^2)^b (1 + \pi^3)^a$ et $(a, b) = (1, 0), (0, 1)$ ou $(1, 1)$.

Les corps K_{10} et K_{01} proviennent de la trisection d'une courbe elliptique; plus précisément, la trisection des courbes

$${}_c Y^2 = X^3 + 3X + 2, \quad {}_c Y^2 = X^3 - 3X + 1,$$

avec $c \in \mathbf{Q}_2^\times$, détermine des extensions quadratiques, de K_{10} et de K_{01} respectivement, dont le groupe de Galois sur $\mathbf{Q}_2$ est Δ'_0 . Pour obtenir des extensions dont le groupe de Galois sur $\mathbf{Q}_2$ soit Δ_0 , il faut, d'après le n° 24, «tordre» celles-là par une extension quadratique non ramifiée de k_1 ; comme cette extension est engendrée par $(1+4j)^{\frac{1}{2}}$, il s'ensuit qu'on obtiendra les corps en question par la trisection des courbes

$$c(1+4j) Y^2 = X^3 + 3X + 2, \quad c(1+4j) Y^2 = X^3 - 3X + 1,$$

avec $c \in \mathbf{Q}_2^\times$. Quant à K_{11} , on trouve que ce corps ne peut être obtenu par la trisection d'une courbe elliptique sur $\mathbf{Q}_2$. Nous laisserons à l'ordinateur de service le soin d'examiner si K_{11} admet une extension quadratique de groupe de Galois Δ_0 sur $\mathbf{Q}_2$, c'est-à-dire s'il satisfait ou non à la condition (C) du n° 21.

37. La recherche des extensions d'un corps k dont le groupe de Galois sur k est $\mathfrak{S}_4$ ou $\mathfrak{A}_4$ n'est pas autre chose, du point de vue des algébristes du XIX^e siècle, que la théorie de l'équation du 4^e degré. C'est un problème pour lequel ces algébristes n'avaient que du mépris; ils faisaient porter toute leur attention sur l'équation du 5^e degré et sa résolution par l'équation modulaire du 5^e degré, c'est-à-dire en somme par la quintisection des courbes elliptiques.

Pourtant, même dans le cadre modeste que nous nous étions fixé, nous n'avons pas élucidé complètement toutes les questions posées. Nous n'avons pu faire l'énumération des extensions qui satisfont à la condition (C) du n° 21, et nous n'avons pas obtenu de critère pour qu'une extension donnée puisse s'engendrer par la trisection d'une courbe elliptique. Comme disait Poincaré, il n'y a pas de problème résolu; il n'y a que des problèmes plus ou moins résolus.

André Weil
Institute for Advanced Study
Princeton, N.J. 08540
USA

(Reçu le 20 mai 1974)