ANNALES SCIENTIFIQUES DE L'É.N.S.

J. A. DE SÉGUIER

Sur les transformations hermitiennes et quadratiques

Annales scientifiques de l'É.N.S. 3^e série, tome 42 (1925), p. 325-377

<http://www.numdam.org/item?id=ASENS_1925_3_42__325_0>

© Gauthier-Villars (Éditions scientifiques et médicales Elsevier), 1925, tous droits réservés.

L'accès aux archives de la revue « Annales scientifiques de l'É.N.S. » (http://www.elsevier.com/locate/ansens) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

SUR LES

TRANSFORMATIONS HERMITIENNES ET QUADRATIQUES

PAR M. DE SÉGUIER

L'étude des groupes linéaires conservant une forme bilinéaire ou quadratique dans un champ de Galois, a été faite d'abord par C. Jordan dans son *Traité des Substitutions*, puis par M. Dickson dans ses *Linear Groups*. J'ai repris et poursuivi cette étude dans deux Mémoires du *Journal de Mathématiques* (1916 et 1919) (1). Je voudrais ici montrer comment, en partant des résultats obtenus dans un champ galoisien, on peut faire l'étude des mêmes groupes dans d'autres champs. Je considérerai principalement le groupe hermitien dans le champ des nombres réels et complexes et le groupe quadratique dans le champ des nombres réels. On obtient ainsi en particulier très simplement les propositions établies par M. Giraud dans le premier Chapitre de sa Thèse (2). On pourra aussi consulter sur ces sujets les mémoires de M. E. Picard : *Sur les formes quadratiques binaires indéfinies à indéterminées conjuguées* (*Annales de l'École Normale*, 3e série, t. 1. 1884) et *Sur les formes quadratiques à indéterminées conjuguées* (*American Journal of Matematics*, vol. 11, 1889).

I. — Préliminaires.

1. Je désignerai par $\mathfrak{S}$ le champ considéré, par $\mathfrak{S}(\upsilon) = \mathfrak{S}'$ le champ

(1) Je renverrai au Mémoire de 1916 par le nombre I, et à celui de 1919 par le nombre II. Au n° 44 du premier Mémoire, au lieu de « car les normalisants... », il faut lire « car, pour $\nu > 2$, $C_{\nu+1} | C_1$ est abélien dans $B(n, \pi)$, mais ne l'est pas dans $\mathcal{G}(2\nu, \pi)$ ». Je renverrai aussi à mes *Éléments de la Théorie des groupes abstraits* par la lettre *E*, et à mes *Éléments de la Théorie des groupes de substitutions* par la lettre *S*. Les notations non précisées dans ce qui suit sont celles de ces deux Ouvrages.

(2) *Ann. Éc. Norm.*, 1915.

qui s'en déduit en lui adjoignant la racine υ d'une équation quadratique irréductible dans Ω, et généralement par $\dot{u}$ la conjuguée d'une quantité u de Ω'. Si Ω est le champ $\mathfrak{R}$ des nombres rationnels, $\Omega(\upsilon)$ varie avec υ, ce qui n'a pas lieu quand Ω est un champ galoisien ou le champ $\mathfrak{R}_1$ des nombres réels. Dans ce dernier cas, Ω' est le champ $\mathfrak{R}'_1$ des nombres réels et complexes.

J'aurai à considérer certains groupes dont les éléments dépendent d'un nombre fini de paramètres variant d'une façon continue, les paramètres du produit de deux éléments dépendant analytiquement des paramètres de ces deux éléments. Je dirai qu'un tel groupe est *paramétrique*. Ceux dont chaque élément peut se réduire à 1 par variation continue sans sortir du groupe, seront dits *continus*, et les autres *semi-continus* (1). Il s'agit, dans ces définitions, de groupes abstraits (les seules variables qui interviennent sont les paramètres). Mais, aucune confusion n'étant à craindre, j'identifierai dans le langage les groupes concrets avec les groupes abstraits isomorphes. On sait qu'un groupe paramétrique dépendant de r paramètres essentiels variant dans $\mathfrak{R}'_1$ ou dans $\mathfrak{R}_1$ est toujours de la forme $\Sigma_i G s_i$, G étant continu, à r paramètres essentiels et unique dans Γ (je dirai que G est le *diviseur continu maximum* de Γ), les s_i, en nombres fini ou non (mais dénombrables), ne contenant plus de paramètres variables, et les Gs_i étant premiers entre eux deux à deux (2).

M. Cartan a déterminé les groupes continus de $\mathfrak{R}'_1$ et $\mathfrak{R}^1$ qui n'ont aucun diviseur normal *continu* (3). Dans ce qui suit, il sera tenu compte des diviseurs et groupes facteurs non continus aussi bien que des diviseurs et groupes facteurs continus. Les mots *simple* et *isomorphe* n'auront donc plus le même sens que dans les travaux de Lie et de M. Cartan.

De même, le *groupe d'une forme bilinéaire ou quadratique* ne sera plus, comme dans ces travaux, supposé continu.

Quel que soit Ω, le groupe $\mathrm{L}(n, \Omega) = \mathrm{L}(n) = \mathrm{L}$ des substitutions

(1) Je prends ici le mot groupe dans le sens habituel (*E.*, 8, 22) qui est un peu plus restreint que celui de Lie.

(2) Lie-Engel, *Theorie der Transformations gruppen*, t. I, Chap. XVIII (p. 315-316, 331-332) *coll.* Ch. 21. — Bianchi, *Lezioni sulla Teoria dei gruppi continui finiti di Trasformazioni*, § 30, 44, 46. Les raisonnements valent pour $\mathfrak{R}_1$ comme pour $\mathfrak{R}'_1$.

(3) *Thèse* 1894, et *Ann. Éc. Norm.*, 1914.

linéaires homogènes à n variables $x_1, \ldots, x_n$ et à coefficients dans $\Im$, a évidemment pour diviseur normal le groupe $U(n, \Im) = U(n) = U$ formé de ses substitutions de déterminant 1, et le groupe Θ des similitudes de U est normal dans U comme dans L. On voit comme lorsque $\Im$ est galoisien (*S.*, 83) que U *dérive des substitutions* $u_{ik\lambda} = |x_i, x_i + \lambda x_k|$ $(i \neq k$; *les variables non écrites étant inaltérées*), et que *tout diviseur* I *normal dans* U *sans être* $\leqq \Theta$ *coïncide avec* U (1). *Donc* $U|\Theta$ *est simple.*

Je désignerai par $\mathfrak{L}(n, \Im) = \mathfrak{L}(n) = \mathfrak{L}$, $\mathfrak{v}(n, \Im) = \mathfrak{v}(n) = \mathfrak{v}$, les groupes déduits de L, U respectivement en regardant les variables comme homogènes. $\mathfrak{v} \equiv U|\Theta$ est simple (2).

Si $\Im$ est $\mathfrak{Gal}_1$ ou $\mathfrak{Gal}'_1$, L est continu, d'après sa définition, et U l'est aussi, d'après la forme de ses générateurs $u_{ik\lambda}$ (3).

---

(1) Une petite modification doit être apportée ici à la preuve du lemme que si I contient $u_{ik\lambda}$, il contient U. On voit comme lorsque $\Im$ est galoisien que I contient toutes les $u_{ik,-\lambda\alpha^2}$, α parcourant $\Im$. Or on verra au n° 2 que l'équation $\alpha^2 - \beta^2 = c$ est toujours résoluble dans $\mathfrak{Gal}$.

(2) *Comparer* LIE-ENGEL, *Op. cit.*, t. I, p. 560; t. III, p. 6 (les démonstrations subsistent dans $\mathfrak{Gal}_1$). On voit que la simplicité du groupe projectif (et de même celle du groupe gauche dont il sera question tout à l'heure) dans $\mathfrak{Gal}_1$ et $\mathfrak{Gal}'_1$ était virtuellement établie, avant les recherches de Lie, par celles de C. Jordan dans le champ de Galois (*Traité des substitutions*).

(3) La substitution infinitésimale générale de U est une combinaison linéaire des substitutions $X_{ik} = x_i \frac{\partial}{\partial x_k}$ et $Y_{ik} = x_i \frac{\partial}{\partial x_i} - x_k \frac{\partial}{\partial x_k} = Y_{1k} - Y_{1i}$ (LIE-ENGEL, *Op. cit.*, t. I, Chap. 26). Le groupe fini engendré par X_{ik} est formé des $u_{ik\lambda}$. Le groupe fini engendré par Y_{ik} est formé des

$$\begin{vmatrix} x_i & \lambda x_i \\ x_k & \lambda^{-1} x_k \end{vmatrix} = m_{ik\lambda}.$$

En posant

$$u_{ik\lambda}\, u_{ki,-\lambda^{-1}}\, u_{ik\lambda} = \varrho_{ik\lambda}\left(= \begin{vmatrix} x_i & \lambda x_k \\ x_k & -\lambda^{-1} x_i \end{vmatrix}\right),$$

on a $m_{ik\lambda} = \varrho_{ki1}\varrho_{ik\lambda}$. Mais les Y_{1i} sont nécessaires pour *former* la substitution infinitésimale correspondant au commutateur

$$u^{-1}_{ki\mu}\, u^{-1}_{ik\lambda}\, u_{ki\mu}\, u_{ik\lambda} = \begin{vmatrix} x_i & (1 + \lambda\mu + \lambda^2\mu^2)x_i - \mu\lambda^2 x_k \\ x_k & \lambda\mu^2 x_i + (1 - \lambda\mu)x_k \end{vmatrix},$$

qui coïncide au second ordre près avec $m_{ik,e^{\lambda\mu}}$ quand λ et μ sont infiniment petits. Les seuls diviseurs normaux *continus* de L sont U et le groupe S des similitudes (LIE-ENGEL, *loc. cit.*). Leur p. g. c. d. est Θ. On remarquera que

$$|\lambda x_1, \ldots, \lambda x_{n-1}, \lambda^{1-n} x_n| = \Pi_1^{n-1} m_{k,k+1,\lambda^k}$$

est dans S en même temps que dans Θ dès que $\lambda^n = 1$.

Soient $\mathrm{H}(n, \Omega) = \mathrm{H}(n) = \mathrm{H}$ le groupe (*groupe hermitien*) des substitutions linéaires de Ω' qui conservent la forme

$$h = \Sigma_1^{\nu} (x_i y_i - y_i x_i) + \eta \omega x_0 x_0,$$
$$(\eta = 0 \text{ ou } 1 ; \omega = \upsilon - \dot{\upsilon} ; n = 2\nu + \eta);$$

$\mathrm{H}^0(n, \Omega) = \mathrm{H}^0(n) = \mathrm{H}^0$ le groupe des substitutions de H dont le déterminant est 1; $\mathfrak{Je}(n, \Omega) = \mathfrak{Je}(n) = \mathfrak{Je}$ et $\mathfrak{Je}^0(n, \Omega) = \mathfrak{Je}^0(n) = \mathfrak{Je}^0$ les groupes déduits de H, H^0 en regardant les variables comme homogènes.

H dérive de H^0 et des

$$m_{1\rho} = \begin{vmatrix} x_1 & \rho x_1 \\ y_1 & \dot{\rho}^{-1} y_1 \end{vmatrix}.$$

En effet, soit $c\upsilon^2 + b\upsilon + c' = 0$ l'équation vérifiée par υ dans Ω, et s une substitution de H. On a $|s\dot{s}| = 1$ ou, en posant $|s| = f + \upsilon g$, f et g étant dans Ω, $cf^2 - bfg + c'g^2 = c$. Or on peut déterminer $\rho = \rho_0 + \upsilon\rho_1$, ρ_0 et ρ_1 étant dans Ω, de manière que le déterminant $\frac{\dot{\rho}}{\rho}$ de $m_{1\rho}^{-1}$ soit égal à $f + \upsilon g$, car cela revient aux deux équations

$$(f - 1) c\rho_0 - (bf - c'g)\rho_1 = 0,$$
$$-g\rho_0 + (f + 1)\rho_1 = 0,$$

dont le déterminant $c(f^2 - 1) - bfg + c'g^2$ est précisément nul. Alors $sm_{1\rho}^{-1}$ est dans H_0, donc s dans $\mathrm{H}^0 m_{1\rho}$.

H^0 *dérive des* τ, u, v (I, 6, 8), et l'on voit comme dans I, 13 (1) que *tous diviseur normal de* H *ou de* H^0, *non formé exclusivement de similitude, contient* H^0. *Donc* $\mathfrak{Je}^0$ *est simple.*

Soient $\mathrm{G}(n, \Omega) = \mathrm{G}(n) = \mathrm{G}$ le groupe (*groupe gauche*) des substitutions de Ω qui conservent la forme $\Sigma_1^{\nu} (x_i y'_i - y_i x'_i)$ $(n = 2\nu)$, les x'_i, y'_i étant cogrédientes aux x_i, y_i; $\mathcal{G}(n, \Omega) = \mathcal{G}(n) = \mathcal{G}$ le groupe déduit de G en regardant les variables comme homogènes.

G dérive des τ, u, V (I, 19) qui ont toutes le déterminant 1 (les V n'interviennent que si $n > 2$); donc $\mathrm{G}(2) = \mathrm{U}(2)$. Le groupe D des similitudes de G est d'ordre 2, et $\mathrm{G} \mid \mathrm{D} \equiv \mathcal{G}$ *est simple* (I, 21).

---

(1) A la première ligne du n° 13, au lieu de $n \geq 4$, il faut lire $n \geq 3$, et à la page 301, dans l'expression de β, il faut remplacer $\lambda(1 - \lambda\dot{\alpha}_{11}\beta_{11})y_1$ par $(1 - \lambda\dot{\alpha}_{11}\beta_{11})r_1$.

Soit $Q(n, C) = Q(n) = Q$ le groupe des substitutions de $\mathfrak{S}$ qui conservent l'invariant quadratique à n variables

$$a = \Sigma_1^{\nu} x_i y_i + \psi(x, y),$$

$\psi(x, y) = cx^2 + bxy + c'y^2$ étant irréductible dans $\mathfrak{S}$, ou se réduisant à cx^2 ou à 0. Ici encore ceux des résultats obtenus dans I, 26-28 où n'intervient pas l'ordre de $\mathfrak{S}$ subsistent évidemment. Je rappellerai seulement que Q dérive des substitutions

$$t_i = \begin{vmatrix} x_i & y_i \\ y_i & x_i \end{vmatrix}, \qquad m_{i\lambda} = \begin{vmatrix} x_i & \lambda x_i \\ y_i & \lambda^{-1} y_i \end{vmatrix}, \qquad V_{ik\lambda} = \begin{vmatrix} x_i & x_i + \lambda x_k \\ y_k & y_k - \lambda y_i \end{vmatrix},$$

$$V_{0k\lambda} = \begin{cases} \begin{vmatrix} x & x + \lambda x_k \\ y_k & y_k - b\lambda y - 2c\lambda x - c\lambda^2 x_k \end{vmatrix} & \text{si } \psi \text{ dépend de } x, \\ 1 \text{ si } \psi \text{ ne dépend pas de } x; \end{cases}$$

$$V_{k0\lambda} = \begin{cases} \begin{vmatrix} y & y - \lambda y_k \\ x_k & x_k + b\lambda x + 2c'\lambda y - c'\lambda^2 y_k \end{vmatrix} & \text{si } \psi \text{ dépend de } y, \\ 1 \text{ si } \psi \text{ ne dépend pas de } y, \end{cases}$$

($i, k \neq 0$; λ est dans $\mathfrak{S}$; les variables non écrites sont inaltérées) et du groupe Ψ de ψ. Si $\psi = 0$, $\Psi = 1$; si $\psi = cx^2$, $\Psi = |t_0|$, $t_0 = |x, -x|$; si ψ est irréductible, en posant

$$x_{\nu'} = \varkappa(x - \upsilon y), \qquad y_{\nu'} = \dot{\varkappa}(x - \dot{\upsilon} y) \qquad (\varkappa\dot{\varkappa} = c, \nu' = \nu + 1, \psi(\upsilon, 1) = 0),$$

Ψ dérive de $t_{\nu'} = |y_{\nu'}, x_{\nu'}|$ et des substitutions $m_{\nu'\rho} = |\rho x_{\nu'}, \dot{\rho} y_{\nu'}|$ où $\rho\dot{\rho} = 1$, ρ parcourant $\mathfrak{S}'$. Je poserai, pour $j = 0, \ldots, \nu$,

$$\begin{vmatrix} x_j & -x_j \\ y_j & -y_j \end{vmatrix} = d_j \qquad (d_0 = 1 \text{ si } \psi = 0;\ d_0 = t_0 \text{ si } \psi = cx^2),$$

$$d_{j_1} d_{j_2} \ldots d_{j_l} = d_{j_1 \ldots j_l}, \qquad d_{01\ldots\nu} = d, \qquad |d| = D.$$

Soit $Q^0(n, \mathfrak{S}) = Q^0(n) = Q^0$ le diviseur de Q formé des substitutions de déterminant 1. On a évidemment $Q = Q^0 + t_j Q^0$, t_j étant une quelconque des t. De plus Q^0 dérive des V, U, W et des m, et le p. p. c. m. des V, U, W y est normal (I, 28-32).

Je reprendrai d'ailleurs les notations déjà employées (I et II) qui conservent un sens dans les champs considérés ici.

II. — Groupes hermitiens.

2. Dans le champ $\mathfrak{R}'_1$ des nombres réels et complexes, on peut, par transformation linéaire, ramener toute forme hermitienne à n variables à l'un des types

$$\Sigma_1^h X_j \bar{X}_j - \Sigma_{h+1}^r X_j \bar{X}_j \qquad (h = 1, \ldots, r;\ r \leqq n),$$

qu'aucune substitution linéaire de $\mathfrak{R}'_1$ ne peut ramener à un autre; r est le rang, h l'indice d'inertie, et le plus petit ν des deux nombres h, $r - h$ la caractéristique de toute forme réductible au type considéré par une substitution linéaire de $\mathfrak{R}'_1$. Le groupe d'une forme hermitienne de caractéristique ν contient toujours une substitution de forme canonique monome où ν multiplicateurs ont un module > 1 (d'ailleurs arbitraire), ν autres étant les inverses des conjugués des précédents et les multiplicateurs restants étant de module 1 (d'ailleurs arbitraires) (1), et cette substitution ne conserve aucune forme de caractéristique $< \nu$ (2).

Donc les groupes des deux formes hermitiennes de caractéristiques différentes, ne peuvent être transformés l'un dans l'autre par une substitution linéaire.

Comme le groupe d'une forme a est évidemment aussi celui de la forme $-a$, on peut supposer $h \geqq r - h = \nu$. Je supposerai de plus ici que $r = n$. On aura donc $h \geqq \frac{n}{2}$ et $n - h = \nu$.

Prenons maintenant les variables

$$x_j = \frac{1}{i}(X_j + X_{h+j}), \qquad y_j = X_j - X_{h+j} \qquad (j = 1, \ldots, \nu),$$
$$X_{\nu+k} = z_k \qquad (k = 1, \ldots, h - \nu).$$

Les types à considérer sont les types

$$a = \varphi + \psi \qquad \text{où} \qquad \varphi = \frac{1}{2i}\Sigma_1^\nu (x_j \bar{y}_j - y_j \bar{x}_j), \quad \psi = \Sigma_1^{n-2\nu} z_k \bar{z}_k,$$

(1) Par exemple, avec les variables qui vont être introduites, la substitution qui multiplie $x_1, \ldots, x_\nu$ respectivement par $\lambda_1, \ldots, \lambda_\nu (|\lambda_i| > 1)$, $y_1, \ldots, y_\nu$ respectivement par $\lambda_1^{-1}, \ldots, \lambda_\nu^{-1}$, et les z par des multiplicateurs quelconques de module 1.

(2) LOEWY, *N. A. H.*, t. 71, 1898, p. 409. — *Voir* aussi DE SÉGUIER, *J. M.*, 1909, p. 25-27.

ν étant un des entiers ≥ 0 et $\leq \frac{n}{2}$. Ayant étudié les cas ou $n - 2\nu = 0, 1$, nous pouvons supposer $n - 2\nu \geq 2$.

Je désignerai par H le groupe de a dans $\mathfrak{H}'_1$; par H^1 son diviseur formé des substitutions de déterminant ± 1; par H^0 son diviseur formé des substitutions de déterminant 1; par I' le groupe des similitudes de $\mathfrak{H}'_1$; par J, J^1 et J^0 les p. g. c. d. respectifs de I' avec H, H^1, H^0; par D le groupe dérivé de la similitude d de multiplicateur -1; par H' le groupe de $a = 0$ dans $\mathfrak{H}'_1$, c'est-à-dire le groupe des substitutions de $\mathfrak{H}'_1$ qui multiplient a par un facteur [ce facteur sera nécessairement dans $\mathfrak{H}_1$ et, si $\nu = 0$, positif (I, p. 283 et 288)]; par $\mathfrak{K}$, $\mathfrak{K}^1$, $\mathfrak{K}^0$, $\mathfrak{K}'$ les actions respectives de H, H^1, H^0, H' sur les rapports des variables, et, de plus, en posant $\psi_k = z_k \dot{z}_k$, par H_k le groupe de $\varphi + \psi_k$; par H_{kl} le groupe de $\psi_k + \psi_l (l \neq k)$; par H^1_k, H^1_{kl} les diviseurs respectifs de H_k, H_{kl} formés de substitutions de déterminant ± 1; par H^0_k, H^0_{kl} ceux formés de substitutions de déterminant 1.

J est formé des similitudes de multiplicateur $e^{i\theta}$, θ étant réel quelconque, J^1 de celles de J où $n\theta$ est multiple de π, c'est-à-dire où les multiplicateurs sont racines de $x^{2n} = 1$; J^0 de celles où les multiplicateurs sont racines de $x^n = 1$.

H dérive de H^0 et des $\zeta_{k\rho} = |z_k, \rho z_k| (\rho\dot{\rho} = 1)$ où, k étant choisi arbitrairement $> \nu$ reste fixe, ρ variant seul; car si α est une substitution de H, donc $|\alpha\dot{\alpha}| = 1$, il suffit de prendre $\rho = |\alpha|^{-1}$ pour que $\alpha\zeta_{k\rho}^{-1}$ soit dans H^0.

Si $\nu \geq 1$, H dérive aussi de H^0 et des

$$m_{h\rho} = \begin{vmatrix} x_h & \rho x_h \\ y_h & \dot{\rho}^{-1} y_h \end{vmatrix}$$

où ρ seul varie, h étant choisi arbitrairement $\leq \nu$; car si α est une substitution de H, il suffit de prendre $\frac{\dot{\rho}}{\rho} = |\alpha|$ pour que $\alpha m_{i\rho}^{-1}$ soit dans H^0.

3. En particulier, *pour* $n = 1$, donc $\nu = 0$, H dérive des substitutions $|z_1, e^{i\theta} z_1|$, θ parcourant $\mathfrak{H}_1$. Donc H *est alors isomorphe au groupe additif des nombres réels, et* H^0 *est le* g_2 *engendré par* $|z_1, -z_1|$,

Soit $n = 2$. — Comme nous supposons $n - 2\nu \geq 2$, on a ici $\nu = 0$,

donc $a = \psi = z_1\dot{z}_1 + z_2\dot{z}_2$. Pour qu'une substitution

$$\begin{vmatrix} z_1 & \alpha z_1 + \beta z_2 \\ z_2 & \gamma z_1 + \delta z_2 \end{vmatrix}$$

de déterminant 1 conserve a, il faut et suffit qu'on ait

$$\alpha\dot{\alpha} + \gamma\dot{\gamma} = 1, \qquad \beta\dot{\beta} + \delta\dot{\delta} = 1, \qquad \alpha\dot{\beta} + \gamma\dot{\delta} = 0, \qquad \alpha\delta - \beta\gamma = 1.$$

Les deux dernières relations résolues en α, γ donnent, en tenant compte de la seconde, $\delta = \dot{\alpha}$, $\gamma = -\dot{\beta}$. Donc H^0 *est ici le* groupe des substitutions

$$\begin{vmatrix} z_1 & \alpha z_1 + \beta z_2 \\ z_2 & -\beta z_1 + \dot{\alpha} z_2 \end{vmatrix} \qquad (\alpha\dot{\alpha} + \beta\dot{\beta} = 1).$$

Pour $n > 2$, H^0 *dérive des* H^0_{kl} *et* (*si* $\nu > 0$) *des* H^0_k. — En effet, soient s une substitution de H et X_ρ, Y_ρ, Z_σ les fonctions qu'elle substitue à x_ρ, y_ρ, z_σ respectivement. *Si* $\nu > 0$, en multipliant α par des générateurs de H^0_k, on pourra, comme dans I, 8, rendre égal à 1 le coefficient de x_1 dans X_1, puis annuler le coefficient de x_1 dans X_2, Y_2, ..., X_ν, Y_ν, Z_1, ..., $Z_{n-2\nu}$. Alors $X_1 = x_1$, $Y_1 = y_1$ (*cf.* I, 1), et l'on est ramené à une substitution de $a - 2i(x_1\dot{y}_1 - y_1\dot{x}_1)$.

Soit donc $\nu = 0$, et $s = |z_k \Sigma_l s_{kl} z_l|$. Soit

$$\zeta^{\alpha\beta}_{kl} = \begin{vmatrix} z_k & \alpha z_k + \beta z_l \\ z_l & -\beta z_k + \alpha z_l \end{vmatrix} \qquad (\alpha\alpha + \beta\beta = 1)$$

la substitution générale de H^0_{kl}. En multipliant s à droite par une $\zeta^{\alpha\beta}_{1k}$, on remplace s_{11} par $s'_{11} = \alpha s_{11} + \beta s_{k1}$, et s_{k1} par $s'_{k1} = -\dot{\beta} s_{11} + \dot{\alpha} s_{k1}$ sans altérer les autres α_{l1}. On pourra donc d'abord rendre $s'_{11} \neq 0$. Supposons donc $s_{11} \neq 0$, et cherchons à annuler s_{k1} (si $s_{k1} \neq 0$). Il faut pour cela qu'on ait

$$\alpha = \theta\dot{s}_{11}, \qquad \beta = \dot{\theta}\dot{s}_{k1}, \qquad \theta\dot{\theta}(s_{11}\dot{s}_{11} + s_{k1}\dot{s}_{k1}) = 1,$$

et la dernière équation est toujours résoluble en θ dans $\mathfrak{D}'_1$.

D'après la forme des générateurs indiqués, H et H^0 *sont continus*.

4. Je dis que, *pour* $n \geqq 2$, *tout diviseur normal* X *non* $\leqq J^0$ *de* H^0 *coincide avec* H^0.

Soit d'abord $n = 2$ (*donc* $\nu = 0$, et posons

$$\zeta_{12}^{\alpha\beta} = \zeta_{\alpha\beta} \qquad \zeta_{e^{i\varphi},0} = \tau_\varphi, \qquad \tau_\pi = d.$$

Alors $J^0 = |d|$.

Remarquons d'abord que la solution générale de $\alpha\dot{\alpha} + \beta\dot{\beta} = 1$ est

$$a = e^{i\alpha_0}\cos u, \qquad \beta = e^{i\alpha_0}\sin u \qquad \left(0 \leqq u \leqq \frac{\pi}{2};\ |\alpha_0|, |\beta_0| \leqq \pi\right).$$

Les multiplicateurs $e^{i\theta}$, $e^{-i\theta}(0 \leqq \theta \leqq \pi)$ de $\zeta_{\alpha\beta}$, ayant pour somme $\alpha + \dot{\alpha}$, sont déterminés par $\cos\theta = \cos\alpha_0 \cos u$. Je dirai que θ est *l'angle de* $\zeta_{\alpha\beta}$. Si $\theta \leqq \frac{\pi}{2}$, on a $|\alpha_0| \leqq \theta$; si $\theta > \frac{\pi}{2}$ $\left(\text{donc } |\alpha_0| > \frac{\pi}{2}\right)$, on a $\theta \leqq |\alpha_0| \leqq \pi$. Il est clair que toutes les conjuguées de $\zeta_{\alpha\beta}$ dans H^0 ont le même angle.

On vérifie directement que

$$\zeta_{\gamma\delta} \qquad \left(\gamma = e^{i\gamma_0}\cos\varphi,\ \delta = e^{i\delta_0}\sin\varphi;\ 0 \leqq \varphi \leqq \frac{\pi}{2};\ |\gamma_0|, |\delta_0| \leqq \pi\right)$$

tranforme τ_0 en une $\zeta_{\alpha\beta}$ (d'angle θ), où

$$\alpha = \cos\theta + i\sin\theta\cos 2\varphi, \qquad \beta = e^{i\left(\gamma_0 + \delta_0 - \frac{\pi}{2}\right)}\sin\theta\sin 2\varphi.$$

Comme $\cos\theta = \cos\alpha_0\cos u$, ces relations équivalent à

$$e^{i\left(\gamma_0 + \delta_0 - \frac{\pi}{2}\right)} = e^{i\beta_0}, \qquad \cos 2\varphi = \frac{\sin\alpha_0\cos u}{\sin\theta}, \qquad \sin 2\varphi = \frac{\sin u}{\sin\theta},$$

la somme des carrés des deux derniers seconds membres étant égale à 1. Donc H^0 transforme τ_0 en une $\zeta_{\alpha\beta}$ quelconque d'angle θ.

Si donc X contient une $\zeta_{\alpha\beta}$ d'angle θ, il contient toutes les $\zeta_{\alpha\beta}$ d'angle θ de H^0, donc en particulier τ_θ, donc toutes les $\tau_\theta\zeta_{\alpha\beta}$ où $\zeta_{\alpha\beta}$ a l'angle θ. Or, l'angle φ d'une telle $\tau_\theta\zeta_{\alpha\beta}$ est déterminé par

$$\cos\varphi = \cos u(\alpha_0 + \theta) = \cos^2\theta - \cos\theta\sin\theta\,\mathrm{tang}\,\alpha_0.$$

Soit d'abord $0 < \theta < \frac{\pi}{2}$, donc $|\alpha_0| \leqq \theta$. Si α_0 croît de $-\theta$ à $+\theta$, φ, qui est $\geqq 0$ et $\leqq \pi$, croît de 0 à 2θ.

Soit maintenant $\theta > \frac{\pi}{2}$, donc $\theta \leqq |\alpha_0| \leqq \pi$. En posant $\pi - \theta = \theta'$, on aura $\cos\varphi = \cos^2\theta' + \cos\theta'\sin\theta'\,\mathrm{tang}\,\alpha_0$. Or, quand α_0 croît de θ à π,

puis de $-\pi$ à $-\theta$, $\operatorname{tang}\alpha_0$ croît de $-\operatorname{tang}\theta'$ à $+\operatorname{tang}\theta'$, $\cos\varphi$ croît de $\cos 2\theta'$ à 1, et φ décroît de $2\theta'$ à 0.

En faisant jouer à 2θ ou à $2\theta'$ le rôle de θ, et en répétant le raisonnement, on voit que X contient une $\zeta_{\alpha\beta}$ d'angle $\frac{\pi}{2}$, donc toutes les $\zeta_{\alpha\beta}$ d'angle $\frac{\pi}{2}$, donc en particulier toutes les $\zeta_{0\beta}$. Or, les produits de deux $\zeta_{0\beta}$ parcourent les τ_φ. Donc X contient toutes les $\zeta_{\alpha\beta}$, et en particulier d. Donc $X = H^0$.

Donc $\mathfrak{H}$ *est simple.*

5. *Soit maintenant* $n > 2$ *et* $\nu = 0$. Montrons d'abord que *tout diviseur* X *non* $\leq J^0$ *de* H_0 *normal* DANS H^1 *coïncide avec* H^0.

Désignons par $0_{k_1, \ldots, k_r}$ la substitution qui multiplie $z_{k_1}, \ldots, z_{k_r}$ par -1 sans altérer les autres variables, et soit $s = (s_{ik})$ une substitution de X hors de S^0.

Supposons d'abord que s *ne soit pas permutable à toutes les* 0_k, et que, par exemple, la substitution $s^{-1}0_1 s 0_1 = t = t_0 0_1$, soit $\neq 1$; t est évidemment dans X, et t_0 d'ordre 2. Si les coefficients $s_{31}, \ldots, s_{n1}$ ne sont pas tous nuls, on peut, en changeant au besoin la notation, supposer $s_{21} \neq 0$. Faisons alors un changement de variables de la forme

$$\begin{aligned} z'_1 &= z_1, \\ z'_2 &= z_2, \\ z'_k &= c_{k2} z_2 + \ldots + c_{kn} z_n \qquad (k = 3, \ldots, n). \end{aligned}$$

s remplace $z'_k (k \geq 3)$ par

$$c_{k2}\Sigma''_1 s_{2l} z_l + \ldots + c_{kn}\Sigma''_1 s_{nl} z_l = (c_{k2}s_{21} + \ldots + c_{kn}s_{n1}) z'_1 + \varphi_k(z'_2, \ldots, z'_n).$$

s_{21} étant $\neq 0$, on peut déterminer les c_{k2} de manière que

$$c_{k2}s_{21} + \ldots + c_{kn}s_{n1}$$

soit nul pour $k = 3, \ldots, n$. Soit alors $s = |z'_k, \Sigma s'_{kl} z'_l|$; on aura

$$s'_{31} = \ldots = s'_{n1} = 0.$$

Comme $0_1 s 0_1$ remplace $z'_3, \ldots, z'_n$ par les mêmes fonctions que s, t et t_0 laissent $z'_3, \ldots, z'_n$ inaltérés. Or, soit m la matrice des coefficients de z'_1, z'_2 dans les fonctions que t_0 substitue à z'_1, z'_2. Les multiplicateurs

de t_0 sont ceux de m joints à $n-2$ multiplicateurs égaux à 1. Or, t_0 est semblable à θ_1. Donc les multiplicateurs de m sont égaux l'un à 1, l'autre à -1. Prenons, au lieu de z'_1, z'_2, des variables u_1, u_2 fonctions de z'_1, z'_2 seuls, telles que m ait la forme canonique, t_0 remplacera u_1 et u_2 par des fonctions de la forme $\varepsilon_1 u_1 + \zeta_1$, $\varepsilon_2 u_2 + \zeta_2$, ε_k étant égal à ± 1, $\varepsilon_1\varepsilon_2$ à -1, et ζ_l étant une fonction de $z'_3, \ldots, z'_n$. Soit ε_h celui des deux ε_k qui est égal à 1. La condition $t_0^2 = 1$ exige que $\zeta_h = 0$. Si alors ζ_k est $\neq 0$ pour $k \neq h$, prenons, au lieu de $z'_3, \ldots, z'_n$ des variables $u_3, \ldots, u_n$, fonctions de $z'_3, \ldots, z'_n$ seuls, telles que $\zeta_k = u_3$. Si $\zeta_k = 0$, écrivons simplement $u_3, \ldots, u_n$ pour $z'_3, \ldots, z'_n$. En omettant les variables inaltérées $u_3, \ldots, u_n$, t_0 aura l'une des formes

$$\begin{vmatrix} u_1 & -u_1 \\ u_2 & u_2 \end{vmatrix}, \quad \begin{vmatrix} u_1 & u_1 \\ u_2 & -u_2 \end{vmatrix}, \quad \begin{vmatrix} u_1 & u_1 \\ u_2 & -u_1+u_3 \end{vmatrix}, \quad \begin{vmatrix} u_1 & -u_1+u_3 \\ u_2 & u_2 \end{vmatrix}.$$

La première est inadmissible, puisque, par hypothèse, $t = t_0\theta$ est $\neq 1$. La troisième se ramène à la seconde en canonisant son action sur u_2 et u_3 (cela revient à prendre $u_2 - \frac{u_3}{2}$ pour variables au lieu de u_2).

Les formes de t qui correspondent aux deux formes restantes de t_0 sont, en changeant u_3 en $-u_3$,

$$\begin{vmatrix} u_1 & -u_1 \\ u_2 & -u_2 \end{vmatrix}, \quad \begin{vmatrix} u_1 & u_1+u_2 \\ u_2 & u_2 \end{vmatrix}.$$

La seconde forme est inadmissible, car a, pour être conservée par elle, ne devrait pas contenir u_1, ce qui est absurde. Donc t a la première forme, et a doit alors avoir la forme $a_1 + a_2$, a_1 ne dépendant que de u_1, u_2, et a_2 que de $u_3, \ldots, u_n$.

Or, comme $\nu = 0$, on peut ramener, par un changement de variables, a_1 à la forme $z_1\dot{z}_1 + z_2\dot{z}_2$, et a_2 à la forme $\Sigma_3^n z_k\dot{z}_k$ sans altérer $t\,(=\theta_{12})$. On peut même, en multipliant une des variables par un facteur arbitraire ρ de module 1, multiplier le déterminant de ce dernier changement de variables par ρ. On peut donc assimiler le changement de variables résultant de tous les changements de variables opérés depuis les variables primitives à une substitution ξ de H *ou même de* H^0 telle que $\xi^{-1}s^{-1}\theta_1 s\theta_1\xi = \theta_{12}$. Donc X contient θ_{12}, donc aussi

$$\theta_{12}(\zeta_{13}^{\alpha\beta})^{-1}\theta_{12}\zeta_{13}^{\alpha\beta} = \zeta_{13}^{\alpha\dot{\alpha}-\beta\dot{\beta},2\alpha\beta}$$

(c'est-à-dire si $\alpha = e^{i\alpha_0}\cos u$, $\beta = e^{i\beta_0}\sin u$, $\zeta_{13}^{\cos 2u,\ \sin 2u}$). Donc X contient H_{13}^0 et, en transformant par des substitutions

$$\tau_{rs} = \begin{vmatrix} z_r & z_s \\ z_s & z_r \end{vmatrix},$$

chaque H_{kl}^0. Donc $X = H^0$.

Supposons maintenant s permutable à toutes les θ_k. Alors s se réduit à une multiplication $|\mu_1 z_1,\ \mu_2 z_2,\ \ldots|(\mu_k \mu_k = 1)$, et comme s est hors de J^0, on peut supposer que $\frac{\mu_1}{\mu_2} = \mu$ est $\neq 1$. La substitution

$$s^{-1}\tau_{12}^{-1} s \tau_{12} = \zeta_{12}^{\mu,0},$$

qui est dans X, est donc $\neq 1$. Si $\mu \neq -1$, X contient donc H_{12}. Si $\mu = -1$ contient, comme tout à l'heure, H_{13}, et l'on conclut de même que $X = H^0$.

6. Reprenons l'étude faite au n° 5 en supposant que, dans a, $\nu(\geqq 1)$ des $z_k \dot{z}_k$ tels que $z_n \dot{z}_n$, $z_{n-1}\dot{z}_{n-1}$, ..., $z_{n-\nu+1}\dot{z}_{n-\nu+1}$ soient remplacés par $-z_n\dot{z}_n$, ..., $-z_{n-\nu+1}\dot{z}_{n-\nu+1}$. Alors, par un changement des variables de a_1 et des variables de a_2, on peut seulement ramener a_1 à la forme $\pm z_1\dot{z}_1 \pm z_2\dot{z}_2$, et a_2 à la forme $\Sigma_3^n(\pm z_k\dot{z}_k)$ sans altérer t. En opérant alors une permutation de $z_1, \ldots, z_n$, on peut ramener a à la forme primitive. Mais ce changement de variables transforme t en une substitution de la forme $\theta_{\lambda\mu}$ où le nombre des indices λ, μ qui sont $> n - \nu$ peut être 0, 1 ou (si $\nu > 1$) 2.

Dans le premier cas, comme $n - 2\nu$ est supposé $\geqq 2$, $n - \nu$ est $\geqq 3$, et l'on voit, comme au n° 5, que X contient toutes les $\zeta_{hk}^{\alpha\beta}$ où h, k sont $\leqq n - \nu$.

Dans le second cas, si $k \leqq n - \nu$ et $l > n - \nu$, X contient le groupe des substitutions de déterminant 1 de $z_h\dot{z}_k + z_k\dot{z}_k - z_l\dot{z}_l$ ($h \leqq n - \nu$ et $\pm k$) (1). Donc X contient θ_{hk}, et l'on est ramené au cas précédent.

Dans le troisième cas X contient de même le groupe des substitutions de déterminant 1 de $z_h\dot{z}_h - z_k\dot{z}_k - z_l\dot{z}_l$ ($h \leqq n - \nu$; k, $l > n - \nu$). Donc X contient θ_{hk}, et l'on est ramené au cas précédent.

En revenant aux relations du n° 2, on voit donc que X contient tous les H_k^0 et tous les H_{kl}^0, donc aussi H^0.

7. Je dis maintenant que *tout diviseur normal* X *de* H^0 *est normal dans* H'.

Prenons a sous la forme $\Sigma_1^n c_k z_k z_k (c_k = \pm 1)$, et désignons encore par H, H', H^0, J, J', J^0 l'expression de ces groupes par les variables actuelles.

On peut supposer n pair, sans quoi $H' = DH^0$, et X, permutable à d, est évidemment normal dans H'. On peut évidemment aussi supposer X non $\leq J$.

Comme θ_k est hors de H^0, l'unique conjugué $\neq X$ de X dans H' est $X' = \theta_k X \theta_k$, normal dans H^0 comme X, et XX′ est normal dans H'. Donc $XX' = H^0$. Le p. g. c. d. Θ de X, X′ est normal dans H', et $XX'|\Theta$ est produit direct de $X|\Theta$ par $X'|\Theta$. Donc Θ ne contient pas H^0. Donc Θ divise J^0, et, en prenant XJ^0 pour X, on peut supposer que $\Theta = J^0$.

Soit $\rho = \left[e^{\frac{2i\pi}{n}}\right]$ un générateur de J^0, $\mu = (\mu_{\alpha\beta})$ une multiplication de H^0, et $\mu = \xi\xi' = \xi'\xi\rho^m$, $\xi = (\xi_{\alpha\beta})$ étant dans X, et $\xi' = (\xi'_{\alpha\beta})$ dans X′. Posons $\theta_k \xi \theta_k = \xi'_k$, $\theta_k \xi' \theta_k = \xi_k$; ξ_k est dans X et ξ'_k dans X′. Comme μ est permutable à θ_k, on a $\mu = \xi'_k \xi_k = \xi_k \xi'_k \rho^m$. Donc $\xi'_k \xi_k = \xi'\xi\rho^m$, et $\xi_k \xi'_k \rho^m = \xi\xi'$.

On a donc des relations de la forme

$$\xi'^{-1}\xi'_k = \xi\xi_k^{-1}\rho^m = \rho^{r_k},$$
$$\xi_k^{-1}\xi = \xi'_k\xi'^{-1}\rho^m = \rho^{s_k}.$$

D'où

$$(1) \qquad \xi_k = \xi\rho^{m-r_k} = \xi\rho^{-s_k}, \qquad \xi'_k = \xi'\rho^{s_k-m} = \xi'\rho^{r_k},$$

ou, en transformant par θ_k,

$$(2) \qquad \xi'_k = \xi'\rho^{r_k-m} = \xi'\rho^{s_k}, \qquad \xi_k = \xi\rho^{m-s_k} = \xi\rho^{-r_k}.$$

Donc, en comparant (1) et (2), $\rho^m = 1$, et $\rho^{r_k} = \rho^{s_k}$. J'écrirai désormais ρ_k pour ρ^{r_k}.

On a maintenant, en développant l'égalité $\theta_k \xi \theta_k = \xi' \rho_k$;

$$(3) \qquad \begin{cases} \xi_{kk} = \rho_k \xi'_{kk}, \quad \xi_{k\alpha} = -\rho_k \xi'_{k\alpha}, \quad \xi_{\alpha k} = -\rho_k \xi'_{\alpha k} \quad (\alpha \neq k), \\ \xi_{\alpha\beta} = \rho_k \xi'_{\alpha\beta} \quad (\alpha, \beta \neq k). \end{cases}$$

Faisons $k = 1, 2$. On aura, pour $\alpha, \beta > 2$, $\rho_1 \xi'_{\alpha\beta} = \rho_2 \xi'_{\alpha\beta}$.

Si $n > 4$ (on suppose n pair), les $\xi'_{\alpha\beta}$ où α, β sont > 2 ne sont pas tous nuls (sans quoi $|\xi'|$ serait nul). Donc $\rho_1 = \rho_2$, et de même $\rho_1 = \rho_3 = \ldots = \rho_n$. En comparant alors les deux lignes de (3), on voit

que les ξ_{rs} et les ξ'_{rs} non diagonaux sont tous nuls. Mais alors ξ et ξ', étant des multiplications, sont permutables à 0_k. Donc $\xi_k = \xi'$ et $\xi'_k = \xi$. Donc ξ' est dans X, et ξ dans X'. Donc ξ et ξ' sont dans J^0. Donc μ serait nécessairement une similitude, ce qui est absurde Donc X est normal dans H^1.

Soit $n = 4$, et supposons $\rho_1 \neq \rho_2$. Alors les $\xi'_{\alpha\beta}$ où α, β sont > 2 sont nuls. Si alors $\rho_1 \neq \rho_3$ et $\rho_1 \neq \rho_4$, on a $\xi'_{21} = \xi'_{31} = 0$, d'où $|\xi'| = 0$. Donc $\rho_1 = \rho_3$ ou $\rho_1 = \rho_4$.

Soit $\rho_1 = \rho_4$ et $\rho_1 \neq \rho_3$, donc $\xi'_{22} = \xi'_{24} = \xi'_{42} = 0$. Alors ξ'_{11}, ξ'_{23}, ξ'_{13}, ξ'_{32} sont $\neq 0$ sans quoi $|\xi'| = 0$. On a d'ailleurs généralement

$$\mu_{\alpha\beta} = \Sigma_s \xi'_{\alpha s} \xi_{s\beta} = \Sigma_s \xi_{\alpha s} \xi'_{s\beta} \qquad (\alpha, \beta = 1, \ldots, n), \tag{4}$$

et en particulier, d'après (3),

$$0 = \Sigma_s \xi_{\alpha s} \xi_{s\beta} = \Sigma_s \xi'_{\alpha s} \xi'_{s\beta} \qquad (\alpha, \beta = 1, \ldots, n;\ \alpha \neq \beta). \tag{5}$$

En faisant successivement $\alpha = 1$, $\beta = 4$; $\alpha = 2$, $\beta = 4$; $\alpha = 3$, $\beta = 4$; $\alpha = 4$, $\beta = 2$; $\alpha = 4$, $\beta = 3$, on tire de là $\xi'_{11} = 0$, $\xi'_{21} = 0$, $\xi'_{31} = 0$, $\xi'_{12} = 0$, $\xi'_{13} = 0$. Dès lors (4) et (3) donnent

$$\mu_{11} = -\rho_1 \xi'_{14} \xi'_{41}, \qquad \mu_{22} = -\rho_2 \xi'_{23} \xi'_{32},$$
$$\mu_{33} = -\rho_1 \xi'_{32} \xi'_{23}, \qquad \mu_{44} = -\rho_4 \xi'_{41} \xi'_{14},$$

d'où $\mu_{11} = \mu_{44}$ et $\mu_{22} = \mu_{33}$. Or cela est absurde, car on peut toujours prendre pour μ_{11}, μ_{22}, μ_{33}, μ_{44} quatre quantités distinctes (il suffit que $|\mu_{kk}| = 1$, et que $\Pi_1^n \mu_{kk} = 1$; on peut prendre par exemple $\mu_{kk} = e^{\frac{2\pi i}{5} k}$). Donc, pour $n = 4$ et $\rho_1 = \rho_2$, on ne peut avoir $\rho_1 = \rho_4$ avec $\rho_1 \neq \rho_3$.

De même on ne peut avoir $\rho_1 = \rho_3$ avec $\rho_1 \neq \rho_4$.

Donc, comme pour $n > 4$, on a $\rho_1 = \rho_2 = \rho_3 = \rho_4$, et l'on conclut de même que X est normal dans H^1.

Ainsi tout diviseur normal de H^0 *non* $\leqq J^0$ *coïncide avec* H^0. *Donc* $H^0 \,|\, J^0$ et $\mathfrak{K}^0 \equiv H^0 \,|\, J^0$ sont simples.

III. — Groupes quadratiques.

8. *Supposons d'abord que* Ω *soit le champ* $\mathfrak{R}$ *des nombres rationnels. Soit* $n = 2$. *Si* $\psi = 0$ *et* $a = x_1 y_1$, le p. p. c. m. R des $m_{1\lambda}$ où λ est

carré dans $\mathfrak{o}$, est $< Q^0$ et normal dans Q^0. Si d'ailleurs α et β sont deux nombres entiers, $m_{1,\frac{\alpha}{\beta}} = m_{1,\beta^2}^{-1} m_{1,\alpha\beta}$ est dans $R m_{1,\alpha\beta}$. Donc Q^0 dérive de R et des $m_{1\lambda}$ où λ parcourt -1 et l'ensemble $\mathfrak{P}$ des nombres premiers positifs. Il est clair que $Q^0|R$ est un groupe abélien formé d'une infinité d'éléments d'ordre 2.

Si $a = \psi$ est irréductible, on peut supposer que $\psi = cx^2 + c'y^2$, c et c' étant des entiers positifs ou négatifs sans diviseur carré. Soit υ une racine de $c\upsilon^2 + c' = 0$, et $\varkappa = \varkappa_0 + \upsilon\varkappa_1$ ($\varkappa_0$ et $\varkappa_1$ étant dans $\mathfrak{o}$) une solution de $\varkappa\dot{\varkappa} = c$, c'est-à-dire de $\psi(\varkappa^0, \varkappa_1) = c^2$. En posant

$$x_1 = \varkappa(x + \upsilon y), \qquad y_1 + \dot{\varkappa}(x - \upsilon y),$$

on a $a = x_1 y_1$, et Q^0 dérive des m_{1s} où $s = s_0 + \upsilon s_1$, s_0 et s_1 étant dans $\mathfrak{o}$, et vérifiant $cs_0^2 + c's_1^2 = c$. La forme rationnelle de m_{1s} est

$$m_{0s_0s_1} = \begin{vmatrix} x & s_0 x + \dfrac{c'}{c} s_1 y \\ y & -s_1 x + s_0 y \end{vmatrix}.$$

Soit $cc' = Mc_1^2$, c_1^2 étant le plus grand diviseur carré de cc' (M peut se réduire à 1, mais non à -1, car ψ serait réductible), et $\frac{c_1}{c} s_1 = s_1'$. La condition $cs_0^2 + c's_1^2 = c$ s'écrit $s_0^2 + Ms_1'^2 = 1$. Posons $s_0 = \frac{\alpha}{\gamma}$, $s_1' = \frac{\beta}{\gamma}$, α, β, γ étant des entiers premiers entre eux. On aura $\alpha^2 + M\beta^2 = \gamma^2$ ou $(\gamma + \alpha)(\gamma - \alpha) = M\beta^2$. Soit δ le p. g. c. d. positif de $\gamma + \alpha$, $\gamma - \alpha$. Comme δ^2 divise $M\beta^2$, δ *divise* β. Mais δ divise la somme 2γ et la différence 2α de $\gamma + \alpha$, $\gamma - \alpha$. Donc $\delta = 1$ ou 2. Soit q le p. g. c. d. (pris avec un signe arbitraire) de $\frac{\gamma + \alpha}{\delta} = qX$ et de $M = qr$; r divise $\frac{\gamma - \alpha}{\delta} = rY$, et qX est premier à rY. Comme d'ailleurs $XY = \left(\frac{\beta}{\delta}\right)^2$, X est un carré u^2, et Y un carré v^2. Donc

$$(1) \quad \gamma = \frac{\delta}{2}(qu^2 + rv^2), \quad \alpha = \frac{\delta}{2}(qu^2 - rv^2), \quad \beta = \delta uv, \quad M = qr, \quad \delta = 1 \text{ ou } 2.$$

Mais qu et rv sont premiers entre eux. Si donc $\delta = 1$, il faut, pour que γ et α soient entiers, que qu et rv soient impairs. Si $\delta = 2$, il faut,

pour que α, β, γ soient premiers entre eux, que qu et rv aient des parités différentes. Inversement, si qu et rv sont impairs, il faut, pour que α, β, γ soient premiers entre eux, que $\delta = 1$. Si qu et rv ont des parités différentes, il faut, pour que γ et α soient entiers, que $\delta = 2$.

Ainsi, q, r, u, v étant des entiers positifs, négatifs ou nuls, tels seulement que qu soit premier à rv, et δ étant égal à 1 ou à 2 suivant que leur produit est impair ou pair, les formules (1) *fournissent toutes les solutions α, β, γ en nombres premiers entre eux de $\alpha^2 + M\beta^1 = \gamma^2$* (1).

Soit R *le p. p. c. m. des m_{1s} qui sont des carrés dans* Q^0. Si $s = \rho^2$, $m_{1\rho}$ étant dans Q_0 (la condition $\rho\dot{\rho} = 1$ résulte de $s\dot{s} = 1$), et si

$$s^2 + b's + 1 = 0 \qquad (-b' = s + \dot{s} = 2s_0),$$

on a

$$-b' = \rho^2 + \rho^2 = (\rho + \rho)^2 - 2.$$

Donc $2 - b' = 2 + 2s_0$ est un carré de $\mathfrak{o}$. Si inversement $2 - b'$ est un carré β^2 de $\mathfrak{o}$, et si l'on pose $s = \rho^2$, on a $\rho^2 + \beta\rho + \gamma = 0$, le signe de β restant arbitraire, d'où $\rho = \frac{1}{2}\left(\beta + \varepsilon\frac{s - \dot{s}}{\beta}\right)$ $(\varepsilon = \pm 1)$, et la condition $\rho^2 = s$ donne $\varepsilon = 1$. Donc ρ est dans $\mathfrak{o}(v)$, et *m_{1s} est un carré de* Q_0.

On remarquera aussi que, *si $s\dot{s} = 1$, on peut mettre s sous la forme $\frac{\alpha}{\dot{\alpha}}$, α étant un entier de* $\mathfrak{R}'$ (2). Si s est une unité, cela est clair, car $-1 = \frac{i}{-i}$, et $i = \frac{1+i}{1-i}$. Soit $s = \frac{\alpha}{\beta}$, α et β étant des entiers de $\mathfrak{R}'$ premiers entre eux. La condition $s\dot{s} = 1$ s'écrit $\alpha\dot{\alpha} = \beta\dot{\beta}$. Donc β divise $\dot{\alpha} = \beta\gamma$, et $\alpha = \dot{\beta}\dot{\gamma}$. Donc $\gamma\dot{\gamma} = 1$. Donc γ est une unité, et s a la forme indiquée.

Quand s est mis sous la forme $\frac{\alpha}{\dot{\alpha}} = \frac{\alpha^2}{\alpha\dot{\alpha}}$, on voit de suite que s est carré en même temps que $\alpha\dot{\alpha}$, ou, puisque $s + \dot{s} + 2 = \frac{(\alpha + \alpha)^2}{\alpha\alpha}$, en même temps que $s + \dot{s} + 2$.

Comme toute m_{1s} de Q^0 a son carré dans R, $Q^0|R$ *est un groupe abélien formé d'une infinité dénombrable d'éléments d'ordre* 2.

---

(1) *Cf.* BACHMANN, *Zahlentheorie*, t. 4, p. 198-220.

(2) Sur la théorie des entiers de $\mathfrak{R}'$, *voir*, par exemple, BACHMANN, *Die Lehre von der Kreistheilung*, p. 150-185.

9. *Soit* $n > 2$, et définissons R comme le p.p.c.m. des V, U, W. Ici, comme lorsque Ω était galoisien, $m_{i\mu^2}$ ($i \leq \nu$; μ *rationnel*) *est dans* R [I, 29, formule (29)], *et* $m_{\nu' s}$ ($s\dot{s} = 1$) *est dans* R *si* $s + s^{-1} + 2$ *est carré dans* Ω (I, 32) (1), *c'est-à-dire si* s *est carré dans* Ω'.

Je dis que $m_{i\mu}$ *est hors de* R *si* μ *n'est pas carré dans* Ω, *et de même* $m_{\nu' s}$ *si* $s + s^{-1} + 2$ ($s\dot{s} = 1$) *n'est pas carré dans* Ω (*c'est-à-dire si* s *est non carré dans* Ω').

Tout d'abord si $\mu = \frac{\alpha}{\beta}$ (α, β entiers), $m_{i\mu} = m_{i\beta}^{-1} m_{1,\alpha\beta}$, et, comme $m_{i\beta^2}$ est dans R, on peut supposer μ entier. On peut évidemment aussi supposer μ sans diviseur carré. Soit $\mu = \pm 2^{\alpha}\mu'$, μ' étant impair > 0. Cherchons un nombre premier p tel que la conguence $x^2 \equiv \mu \bmod p$ soit impossible, c'est-à-dire tel que $\left(\frac{\mu}{p}\right) = -1$, $\left(\frac{\mu}{p}\right)$ étant le symbole de Legendre. On sait que toute progression arithmétique formée de nombres entiers contient une infinité de nombres premiers (2). Si $\mu' = 1$, μ est égal à -1 ou à ± 2, et il suffit de prendre p respectivement parmi les nombres $\equiv 3 \bmod 4$ ou $\equiv 5 \bmod 8$. Si $\mu' = q_1 \dots q_m$, les q_i étant premiers impairs distincts, il suffit de prendre p parmi les nombres $\equiv 1 \bmod \frac{8\mu'}{q_1}$ et en même temps congru à un non reste quadratique de q_1, car alors on aura $\left(\frac{\mu}{p}\right) = \left(\frac{p}{q_1}\right) = -1$.

Considérons alors le champ galoisien C_p d'ordre p tel que $\left(\frac{\mu}{p}\right) = -1$. Si $m_{i\mu}$ était dans R, cela aurait encore lieu lorsqu'on prend C_p pour Ω en supposant p plus grand que tous les dénominateurs, pris positivement, des coefficients des U, V, W par lesquelles $m_{i\mu}$ est exprimable. Or cela est impossible.

De même, si $s + s^{-1} + 2$ ($s\dot{s} = 1$) est un nombre rationnel $\frac{\alpha}{\beta}$ (α, β entiers), et si p est un nombre premier tel que $\left(\frac{\alpha\beta}{p}\right) = -1$, $m_{\nu' s}$ ne peut être dans R sans que cela ait lieu aussi pour $\Omega = C_p$, si p est assez grand, et cela est encore impossible.

---

(1) Comme -1 est ici non carré dans Ω, le nombre désigné dans I, 32 par M vérifie, si $s = -1$, la condition que $-M$ soit carré.

(2) *Voir*, par exemple, DIRICHLET, *Vorlesungen ueber Zahlentheorie*, 4e édition, §132-137.

Pour $n \geq 2$, je dirai que $\mathrm{R}(n) = \mathrm{R}$ *est le groupe réduit de a dans* $\mathfrak{R}$

10. On voit comme lorsque $\mathfrak{S}$ est galoisien que, *pour* $n = 3$, R *est isomorphe à* $\mathfrak{V}(2)$ *qui est simple* (1); *que, pour* $n = 4$ *et* $\psi = 0$, R | D *est produit direct de deux groupes simples isomorphes à* $\mathfrak{V}(2)$, R *étant ici le groupe* **VW** *de* I, 40; *que, pour* $n = 4$ *et* ψ *irréductible*, R *n'a pas d'autre diviseur normal que* D, R | D *étant isomorphe au groupe* $\mathfrak{V}(2)$ *de* $\mathfrak{S}'$ *qui est simple.*

11. Supposons $n \geq 5$, et soit Γ un diviseur normal de Q, Q^0 ou R non $\leq$ D. Écrivons la substitution générale de Q sous la forme

$$\alpha = \begin{vmatrix} x_i & \Sigma_k(\alpha_{ik}x_k + \alpha'_{ik}y_k) = \mathrm{X}_i \\ y_i & \Sigma_k(\beta_{ik}x_k + \beta'_{ik}y_k) = \mathrm{Y}_i \end{vmatrix} \quad (i, k = 1, \ldots, \nu, 0),$$

en convenant de supprimer toutes les quantités relatives à $x_0 = x$ ou à $y'_0 = y$ si x ou y ne figure pas dans a.

Tout d'abord Γ contient des α qui ne sont pas des multiplications, car les conditions que α, $\mathrm{V}_{ik\lambda}^{-1}\alpha\mathrm{V}_{ik\lambda}$, $\mathrm{U}_{ik\lambda}^{-1}\alpha\mathrm{U}_{ik\lambda}$ $(i, k \geq 0)$ soient des multiplications donnent (*cf.* I, 47) $\alpha_{ii} = \alpha_{kk}$, $\beta'_{ii} = \beta'_{kk}$, $\alpha_{ii} = \beta'_{kk}$ $(i, k \geq 0)$, et α serait dans D.

Soit donc α une substitution de Γ autre qu'une multiplication. *On peut y supposer non nul un coefficient de second indice* $\neq 0$ *hors de la diagonale.* Sans cela, en effet, les équations (4)-(6) de I, 26, montrent (pour j ou k nul) que les α_{i0}, α'_{i0}, β_{i0}, β'_{i0} où $i \neq 0$ sont tous nuls. Et si, pour ψ irréductible, α'_{00} ou β_{00} est $\neq 0$, $\mathrm{V}_{0k\lambda}^{-1}\alpha\mathrm{V}_{0k\lambda}$ ou $\mathrm{V}_{k0\lambda}^{-1}\alpha\mathrm{V}_{k0\lambda}$ a, dans l'une des deux dernières lignes et hors des deux dernières colonnes, un coefficient $\neq 0$.

En transformant alors au besoin α par une $(d_1\mathrm{T}_{1k})^r t_{12}^s$ [une telle substitution est dans R quels que soient r et s (I, 39)], *on peut supposer* $\neq 0$ *un des* α_{j1}, β_{j1} *autres que* α_{11}.

Supposons maintenant β_{11} *nul*, et cherchons à le rendre $\neq 0$. Pour cela cherchons d'abord à rendre $\beta_{21} \neq 0$. Si $\psi \neq 0$, et si tous les α_{j1}, β_{j1} où $j > 1$ sont nuls, β_{21} est remplacé dans $\mathrm{V}_{02\lambda}^{-1}\alpha\mathrm{V}_{02\lambda}$ par

$$-\lambda(b\beta_{01} + 2c\alpha_{01}),$$

et dans $\mathrm{W}_{02\lambda}^{-1}\alpha\mathrm{W}_{02\lambda}$ par $-\lambda(b\alpha_{01} + 2c'\beta_{01})$; or si $\psi = cx^2$, la première

de ces quantités est $\neq 0$, et si ψ est irréductible, ces deux quantités ne peuvent être nulles à la fois. Si α_{21} ou un des α_{k1}, β_{k1} où $k > 2$ est $\neq 0$, on rendra de même $\beta_{21} \neq 0$ en transformant par une $(d_2 T_{2k})^r t_{23}^s$ ou une $(d_2 T_{2k})^r (t_{02} m_{2\lambda})^s$ de R (I, 39). *Si alors* $\beta_{22} \neq 0$, on rendra $\beta_{11} \neq 0$ en transformant par $d_1 T_{12}$. *Soit donc* $\beta_{22} = 0$, et exceptons d'abord le cas où $n = 5$ et le cas où $n = 6$ avec $\psi \neq 0$. On rendra $\beta_{11} \neq 0$ par les trois opérations suivantes (*cf.* I, 13) : 1° une transformation par $V_{13\lambda}$ qui, sans altérer β_{21}, rend $\beta_{23} \neq 0$ (elle remplace β_{23} par $\beta_{23} - \lambda\beta_{21}$); 2° une transformation par $U_{13\lambda}$ qui, sans altérer β_{21} rend $\beta'_{21} \neq 0$ (elle remplace β'_{21} par $\beta'_{21} + \lambda\beta_{23}$); 3° la substitution à α, soit, si $\beta_{12} \neq 0$, de $\alpha^{-1} V_{21\lambda}^{-1} \alpha V_{21\lambda}$, ce qui remplace β_{11} par $\beta_{11} - \lambda^2 \beta_{12} \beta'_{21}$, soit, si $\beta_{12} = 0$, de $V_{21\lambda}^{-1} \alpha V_{21\lambda}$, ce qui remplace alors β_{11} par $\beta_{11} - \lambda\beta_{21}$. Si $n = 5$ ou si $n = 6$ avec $\psi \neq 0$, on rendra $\beta_{11} \neq 0$ en substituant aux deux premières opérations une seule transformation par $U_{01\lambda}$, ce qui remplace β'_{21} par $\beta'_{21} + \lambda\beta_{20} - c\lambda^2\beta_{21}$, ou par $V_{10\lambda}$, ce qui remplace β'_{21} par $\beta'_{21} - \lambda\beta'_{20} - c'\lambda^2\beta_{21}$.

En transformant alors par des V_{1j}, U_{1j}, on annulera tous les α_{j1}, β_{j1} où $j \neq 1$ sans altérer β_{11}. D'après les équations (7), (4), (5) de I, 26, il en résulte que $\alpha_{11} = 0$, que $\alpha'_{11}\beta_{11} = 1$, et que tous les α_{1j}, α'_{1j} où $j \neq 1$ sont nuls.

Considérons maintenant la matrice α_1 déduite de α en supprimant les deux premières lignes et les deux premières colonnes, et *supposons* β_{22} *nul. Si* α_1 *n'est pas une multiplication*, on peut, en opérant sur α_1 comme sur α, rendre d'abord $\neq 0$ un coefficient non diagonal de la colonne de α_{22} [donc n est > 5, et si $n = 6$, ψ est nul, sans quoi, β_{22} étant nul, α_{02} et β_{02} seraient nuls, d'après l'équation (7) de I, 26, contre l'hypothèse], puis rendre $\beta_{22} \neq 0$, puis annuler les α_{j2}, β_{j2} où $j \neq 1, 2$. Alors $\alpha_{22} = 0$, et en désignant par X_i, Y_i ($i = 1, \ldots, \nu, 0$) les fonctions que α^{-1} substitue à x_i, y_i respectivement,

$$Y'_1 = \beta_{11} x_1, \qquad Y'_2 = \beta_{12} x_1 + \beta_{22} x_2,$$

d'où (*cf.* I, 13)

$$\alpha^{-1} U_{12\lambda}^{-1} \alpha U_{12\lambda} = W_{21,\lambda\beta_{11}\beta_{22}} U_{12\lambda}.$$

Si α_1 *est une multiplication*,

$$\alpha_{-1} U_{12\lambda}^{-1} \alpha U_{12\lambda} = V_{21,\lambda\alpha_{22}\beta_{11}} U_{12\lambda}.$$

Donc, en désignant par R_{ikj} le groupe réduit de la portion de a où figurent les seules variables d'indices i, k, j (≥ 0 et distincts), Γ *contient un diviseur normal d'ordre* > 2 *de* R_{ikj}.

Or on voit, comme dans I, 43-46, que, *pour* $n = 5$, R *est isomorphe à* $\mathfrak{G}(4)$, *et que, pour* $n = 6$, R|D *est isomorphe à* $\mathfrak{o}(4)$ *si* $\psi = 0$, *et à* $\mathfrak{H}^0(4)$ *si* $\psi = 0$.

Donc Γ contient R_{12j} et de même tous les R_{ikj}. *Donc* Γ *contient* R (I, 41).

Donc, pour $n \geq 5$, *tout diviseur normal de* Q, Q^0 *ou* R *non* $\leq$ D *contient* R. *Donc* RD|D *est simple.*

12. On voit comme lorsque $\mathfrak{S}$ est galoisien que, si $\nu \geq 2$, $m_{i\mu}m_{k\mu}$ ($1 < k \leq \nu$) *est dans* R [I, 29, formule (29)].

Il résulte immédiatement de là que, *pour* $\psi = 0$ *ou* x^2 *avec* $n \geq 2$, Q^0 *dérive de* R *et des* $m_{1\mu}$ *où* μ *parcourt* $\mathfrak{P}$ *et* -1.

Considérons maintenant, en supposant *n pair et* $\psi \neq 0$, le groupe réduit (p. p. c. m. des V, U, W) $\mathbf{R}$ de $\Sigma_1^{\nu'} x_i y_i$ dans $\mathfrak{S}'$, et cherchons le p. g. c. d. $\mathbf{R}^0$ de $\mathbf{R}$, Q^0 : je dirai que $\mathbf{R}^0$ ($\geq$ R) est le groupe *semi-réduit* de a. Toute substitution ξ de Q^0 est dans un complexe

$$m_{1\lambda} \dots m_{\nu\rho} m_{\nu' s} \mathrm{R} \qquad (s\dot{s} = 1).$$

Comme d'ailleurs $m_{i\mu}m_{k\mu}$ ($i, k \leq \nu$) est dans R, on peut supposer que ξ est dans un complexe $m_{1\lambda}m_{\nu' s}$R. Soient $s = \frac{\dot{\sigma}}{\sigma}$, $\sigma\dot{\sigma} = \tau$. Les substitutions $m_{\nu'\tau}m_{\nu' s}^{-1} = m_{\nu'\sigma^2}$ et $m_{1\tau}m_{\nu'\tau}^{-1}$ sont dans $\mathbf{R}$ (I, 29), donc aussi leur produit $m_{1\tau}m_{\nu' s}^{-1}$. Donc $m_{\nu' s}$ est dans $m_{1\tau}\mathbf{R}$, et ξ dans $m_{1,\lambda\tau}\mathbf{R}$. Supposons maintenant ξ dans $\mathbf{R}$. Alors $m_{1,\lambda\tau}$ est dans $\mathbf{R}$. Donc $\lambda\tau$ est carré dans $\mathfrak{S}'$, donc de la forme $\pm h^2$ (h réel). En posant $\frac{h}{\sigma} = \alpha$, on a donc $\lambda = \pm \alpha\dot{\alpha}$, $s = \frac{\alpha}{\dot{\alpha}}$. Si $\lambda = \alpha\dot{\alpha}$, on voit directement (*cf.* I. 40) que $m_{1\lambda}m_{\nu' s}$ est dans le groupe réduit de $x_1 y_1 + x_{\nu'} y_{\nu'}$, donc dans R. Si $\lambda = -\alpha\dot{\alpha}$, $m_{1\lambda}m_{\nu' s}$ est dans d_1R. Donc ξ est dans R ou dans d_1R. *Donc le p. g. c. d.* $\mathbf{R}^0$ *de* Q_0, $\mathbf{R}$ *est* $\mathrm{R} + d_1\mathrm{R}$.

On voit en même temps, puisque $\tau = \sigma\dot{\sigma}$, que $m_{1\tau}m_{\nu' s}$ *et de même* $m_{1\tau}m_{\nu' s}^{-1}$ *sont dans* R. Comme la relation $s = \frac{\dot{\sigma}}{\sigma}$ détermine σ par s à un

facteur réel près $\left(\text{si } s = \frac{\sigma'}{\sigma}, \text{ on a } \frac{\tau}{\tau'} = \frac{\sigma}{\sigma'}\right)$, τ *est déterminé par* s *à un facteur réel carré arbitraire près.* Si d'ailleurs $m_{i\tau}m_{\nu's}$ est dans R, $m_{i,l\tau}m_{\nu's}$ y est toujours et seulement si $(m_{i\tau}m_{\nu's})^{-1}m_{i,l\tau}m_{\nu's} = m_{il}$ est dans R, c'est-à-dire si l est carré dans $\mathfrak{o}$.

Comme toute substitution de Q^0 est dans un complexe $m_{i\mu}\mathbf{R}$, et que $m_{i\mu}$ n'est dans $\mathbf{R}$ que si $\pm\mu$ est carré dans $\mathfrak{o}$, on voit que, *pour* $\psi = cx^2 + c'y^2$ *avec* $n > 2$, *comme pour* $\psi = cx^2$ *ou* 0 *avec* $n \geq 2$, Q^0 *dérive de* R *et des* $m_{i\mu}$ *où* μ *parcourt* $\mathfrak{P}$ *et* -1. Si d'ailleurs α et β sont des entiers positifs ou négatifs, sans diviseurs carrés et premiers entre eux, $m_{i\alpha}$ et $m_{i\beta}$ sont incongrus mod R, car $m_{i\alpha}m_i^{-1} = m_{i,\beta^2}^{-1}m_{i,\alpha\beta}$ est hors de R. *Donc* $Q^0 \mid R$ (R *est évidemment normal dans* Q^0) *est un groupe abélien formé d'une infinité d'éléments d'ordre* 2.

On a vu (9) que, pour $k \leq \nu$, d_k est hors de R, et que, si $\psi = cx^2 + c'y^2$, $d_{\nu'}$ est dans R (donc $d_{k\nu'}$ est alors hors de R), que, d'autre part, $d_{kl}(k,\ l \leq \nu)$ est dans R. *Donc, pour* $\psi = 0$ *ou* $cx^2 + c'y^2$, d *est dans* R *toujours et seulement si* ν *est pair.*

13. *Soit* $R'(n) = R'_a = R'$ *un groupe défini comme il suit. Pour* $n = 1$ *et pour* $n = 2$, ψ *étant irréductible*, $R' = Q^0$. *Dans tous les autres cas* R' *est le p. p. c. m. de* R *et des* m_{ip} *où* p *parcourt* $\mathfrak{P}$; *alors* $Q_0 = R' + d_1 R'$ (12).

R' *contient toujours le groupe* Ψ^0 *des substitutions de déterminant* 1 *de* Ψ. Cela résulte du n° 12 si $n \geq 4$, Ψ étant irréductible, et cela est évident dans les autres cas.

Toute substitution de Q^0 *suffisamment voisine de* 1 *est dans* R' (Q^0 contient évidemment des substitutions aussi voisines de 1 que l'on veut, par exemple parmi les $m_{i\mu}$). En effet, soit α une telle substitution avec les notations du n° 11. Les coefficients diagonaux, supposés assez voisins de 1, sont > 0. En multipliant donc α à droite par une m_i de R', on ramène à 1 le premier coefficient diagonal. En multipliant alors α à droite par des V_{j1}, W_{j1}, on ramène à 0 les α_{j1}, β_{j1}, où $j \neq 1$. Donc $\beta_{11} = 0$, et $\beta'_{11} = 1$. En multipliant alors α à droite par des V_{1j}, U_{1j}, on annulera les α'_{j1}, β'_{j1} où $j \neq 1$. La substitution initiale étant supposée assez voisine de 1, la substitution actuellement obtenue peut être supposée aussi voisine de 1 que l'on veut, et les relations entre les coefficients des deux premières colonnes et des suivantes montrent

que les α_{1j}, α'_{1j}, β_{1j}, β'_{1j} où $j \neq 1$ sont nuls. On est ainsi ramené au cas de $n-2$ variables. Or, pour $n=2$ et $\psi=0$ on peut faire le raisonnement précédent, et si $n=2$, ψ étant irréductible, ou si $n=1$, la proposition est évidente.

14. *Supposons maintenant que* $\mathfrak{D}$ *soit le champ* $\mathfrak{R}_1$ *des nombres réels. Soit d'abord* $n=2$. Si $a=x_1 y_1$ ($\psi=0$), le p. p. c. m. $R(n)=R$ des $m_{1\mu}$ où μ est positif est normal dans Q^0, et $Q^0=R+d_1 R$.

Si $a=\psi$ *est irréductible*, on peut supposer ici que $\psi=x^2+y^2$. Alors, avec les notations de I, 25, Q^0 dérive des m_{1s} où $s=s_0+is_1$ ($i^2=-1$; s_0, s_1 réels) vérifie $s_0^2+s_1^2=1$, et la condition nécessaire et suffisante pour que m_{1s} soit un carré dans Q^0 est encore que $s+\dot{s}+2=2(1+s_0)$ soit carré dans $\mathfrak{D}$, c'est-à-dire soit $\geqq 0$ (*cf.* 8). Elle est toujours remplie. *Donc le groupe* $R(n)=R$ *des* m_{1s} *qui sont des carrés dans* Q^0 *coïncide avec* Q^0. D'ailleurs, en posant $x+iy=z$, $s=e^{i\theta}$, on a $m_{1s}=m'_\theta=|z, e^{i\theta}z|$, et θ parcourt les nombres réels. Il est clair que m'_θ est toujours le carré de $m'_{\frac{\theta}{2}}$. On voit en même temps que Q^0 *est isomorphe au groupe additif des nombres réels.*

15. *Soit* $n \geqq 3$ et définissons $R(n)=R_n=R$ comme le p. p. c. m. des V, U, W. Comme au n° 9, R contient toutes les $m_{k\lambda}$ ($k=1, \ldots, \nu$) où λ est >0 et toutes les $m_{\nu' s}$ (*cf.* I, 29, 32; $s+\dot{s}+2$ est ici toujours positif). Si maintenant d_1 était exprimable sous la forme $\Pi_k \gamma_{k,\rho_k}$, γ_{k,ρ_k} étant une des substitutions $V_{jj'\rho_k}$, $U_{jj'\rho_k}$, $W_{jj'\rho_k}$ ($j, j'=0, \ldots, \nu_i$), et les ρ_k étant réels, on aurait, en remplaçant chaque ρ_k par un nombre rationnel r_k suffisamment approché, une relation de la forme $d_1 e=\Pi_k \gamma_{k,r_k}$, e étant une substitution aussi voisine de 1 que l'on veut, et cette relation elle-même montre que les coefficients de e sont rationnels. On voit alors *comme au* n° 13 que e est dans le p. p. c. m. R′ des U, V, W à coefficients rationnels et des $m_{1\mu}$ où μ est rationnel >0. Donc d_1 serait dans R′ contrairement à ce que l'on a vu (13). *Donc* $Q^0=R+d_1 R$.

On voit en même temps que R *est continu* (d'après ses générateurs), *et* Q^0 *semi-continu*. Car si $d_1 R$ contenait des substitutions aussi voisines de 1 que l'on veut, il en contiendrait aussi de la forme $d_1 r$, r ayant des coefficients rationnels. Alors $d_1 r$ serait dans R′ (13), donc aussi d_1, ce qui ne se peut (12).

Pour $n \geqq 5$, on voit au n° 11 que *tout diviseur normal de* Q, Q^0 *ou* R *non* $\leqq$ D, *contient* R (RD | D *est donc simple*), et que R *contient* D *toujours et seulement si* ν *est pair.*

16. *Considérons en particulier les cas* $n = 3, 4, 5, 6$.

Soit d'abord $n = 3$ *avec* $\psi = cx^2$ (on peut évidemment supposer c égal à 1). Alors Q^0 est isomorphe au groupe $\mathfrak{L}$ des substitutions $z = \frac{\alpha z + \beta}{\gamma z + \delta}$, et $m_{1\lambda}$, $V_{01\lambda}$, $U_{01\lambda}$ correspondent respectivement à λz, $\frac{z}{1+\lambda z} = \varphi_\lambda$, $z - c\lambda = u_\lambda$ (I, 40) qui engendrent $\mathfrak{L}$. La substitution de Q^0 qui répond à σ est alors

$$s = \begin{vmatrix} x_1 \Delta^{-1}\left(\alpha^2 x_1 - \frac{\beta^2}{c} y_1 + 2\alpha\beta x\right) \\ y_1 \Delta^{-1}(-c\gamma^2 x_1 + \delta^2 y_1 - 2c\gamma x) \\ x \ \Delta^{-1}\left[\alpha\gamma x_1 - \frac{\beta\delta}{c} y_1 + (\alpha\delta + \beta\gamma) x\right] \end{vmatrix} = \begin{cases} U_{01,-\frac{\beta}{c\alpha}} V_{01,\frac{\alpha\gamma}{\Delta}} m_{1,\frac{\alpha^2}{\Delta}} & \text{si } \alpha \neq 0, \\ t_{01} m_{1,-\frac{\Delta}{c\gamma^2}} V_{01,-\frac{\gamma\delta}{\Delta}} & \text{si } \alpha = 0 \end{cases}$$

(α, β, γ, δ étant dans $\mathfrak{o}$; $\Delta = \alpha\delta - \beta\gamma$).

R correspond au diviseur $\mathfrak{v}$ de $\mathfrak{L}$ qui dérive des φ_λ et des u_λ. Or $\mathfrak{v}$ est formé des σ où Δ est carré dans $\mathfrak{o}$ (c'est-à-dire ici > 0) (1), et $\mathfrak{L} = \mathfrak{V} + (-z)\mathfrak{v}$. On retrouve donc que R est $< Q^0$, et que $Q^0 = R + d_1 R$.

$\mathfrak{v}$ est simple (1) et continu ($\mathfrak{L}$ n'est évidemment pas continu). *Donc* R *est simple.*

Soit $n = 4$, *et* $\psi = 0$. Comme dans le cas où $\mathfrak{o}$ est galoisien, R | D *est produit direct de deux groupes simples isomorphes à* $\mathfrak{v}(2)$ *et ne contient que les* $m_{1\lambda}$ *où* λ *est carré dans* $\mathfrak{o}$ (I, 40). On retrouve donc que $Q^0 = R + d_1 R$.

Soit $n = 4$ *et* $\psi = x^2 + y^2$. On voit encore de même (*cf.* I, 40) que

---

(1) En effet $\mathfrak{V}$ contient $u_1 \varphi_1 u_1 = -z^{-1}$ et $u_k^{-1} \varphi_k (u_1 \varphi_1 u_1) \varphi_{-k} = k^2 z$; donc toutes les λz où $\lambda > 0$. Or si $\alpha \neq 0$, on a $\sigma = u_{-\frac{\beta}{c\alpha}} \left(\frac{\alpha^2}{\Delta} z\right) \varphi_{\frac{\gamma}{\alpha}}$. Si $\alpha = 0$, donc $\beta\gamma = -\Delta$, $\sigma = u_{-\frac{\delta}{c\gamma}} \left(\frac{\Delta}{\beta^2} z\right) \left(\frac{-1}{z}\right)$. Donc $\mathfrak{V}$ contient toutes les σ où $\Delta > 0$, et il n'en contient évidemment pas d'autres. Plus généralement d'ailleurs la proposition résulte de ce que le groupe U (n) de variables $x_1, \ldots, x_n$ dérive des substitutions $| x_i, x_i + \lambda x_k |$ (1).

R|D *est isomorphe au groupe* $\mathfrak{v}(2)$ *de* $\mathfrak{S}'$, *qu'il ne contient que les* $m_{1\lambda}$ *où* λ *est carré dans* $\mathfrak{S}$, *mais qu'il contient toutes les* $m_{2\rho}$ *où* $\rho\dot{\rho} = 1$ (la condition $\rho^2\dot{\rho}^2 = 1$ équivaut ici à $\rho\dot{\rho} = 1$). On retrouve donc encore que $Q^0 = R + d_1 R$.

17. *Soit* $n = 5$. Considérons le groupe G de variables ξ_1, η_1, ξ_2, η_2 dont l'invariant est $\Sigma_1^2(\xi_k\eta'_k - \eta_k\xi'_k)$, les ξ'_k, η'_k étant cogrédients aux ξ_k, η_k. Désignons par Δ le g_2 normal de G engendré par la similitude d'ordre 2. Adjoignons aux variables x_1, y_1, x_2, y_2 de R la variable auxiliaire inaltérée y. Posons $x + y = -y_3$, $x - y = x_3$, et identifions les variables $-x_3$, x_2, $-x_1$, y_1, y_2, y_3 avec les déterminants

$$Z_{12} = \begin{vmatrix} \xi_1 & \xi'_1 \\ \eta_1 & \eta'_1 \end{vmatrix}, \quad Z_{13} = \begin{vmatrix} \xi_1 & \xi'_1 \\ \xi_2 & \xi'_2 \end{vmatrix}, \quad Z_{14} = \begin{vmatrix} \xi_1 & \xi'_1 \\ \eta_2 & \eta'_2 \end{vmatrix},$$

$$Z_{23} = \begin{vmatrix} \eta_1 & \eta'_1 \\ \xi_2 & \xi'_2 \end{vmatrix}, \quad Z_{24} = \begin{vmatrix} \eta_1 & \eta'_1 \\ \eta_2 & \eta'_2 \end{vmatrix}, \quad Z_{34} = \begin{vmatrix} \xi_2 & \xi'_2 \\ \eta_2 & \eta'_2 \end{vmatrix}$$

respectivement. Les générateurs

$$\begin{vmatrix} \xi_1 & \eta_1 \\ \eta_1 & -\xi_1 \end{vmatrix}, \quad \begin{vmatrix} \xi_2 & \eta_2 \\ \eta_2 & -\xi_2 \end{vmatrix}, \quad |\xi_1, \xi_1 + \lambda\eta_1|, \quad |\xi_2, \xi_2 + \lambda\eta_2|, \quad \begin{vmatrix} \xi_2 & \xi_2 + \lambda\xi_1 \\ \eta_1 & \eta_1 - \lambda\eta_2 \end{vmatrix}$$

de G opèrent sur x_1, y_1, x_2, y_2, $x = \frac{1}{2}(x_3 + y_3)$, $y = \frac{1}{2}(x_3 - y_3)$ les substitutions respectives $t_{12}d_2T_{12} = S_{12,-1}$, $T_{12}d_2 = R_{121}$, $U_{12,-\lambda}$, $V_{21,-\lambda}$, $V_{01\lambda}$. Or, $S_{12,-1}R_{121} = t_{12}$ transforme $U_{12\lambda}$ en $W_{12\lambda}$, $V_{21\lambda}$ en $V_{12,-\lambda}$, et $V_{01\lambda}$ en $U_{01\lambda}$. Donc G opère sur x_1, y_1, x_2, y_2, x toutes les substitutions de R (*cf.* I, 41, 43).

D'ailleurs les substitutions de G qui répondent ainsi à l'unité de R sont celles de Δ, puisque G|Δ est simple (1). *Donc* R *est isomorphe au second combiné* (1) G_2 *de* G, *donc aussi à l'action* G|Δ *de* G *sur les rap-*

(1) Pour la définition et les principales propriétés des combinés d'un système de substitutions linéaires, *voir*, par exemple *S.*, 75. En particulier si $\alpha e\bar{\alpha} = e'$, e et e' étant des matrices symétriques d'ordre n représentant des formes quadratiques, et $\bar{\alpha}$ la trans-

ports des variables ξ_k, η_k (¹). G_2 conserve $\Sigma_1^3 x_k y_k$, et il en est de même de R, puisque R conserve $a - y^2 = \Sigma_1^3 x_k y_k$.

Considérons maintenant la similitude σ qui multiplie ξ_1, η_1, ξ_2, η_2 par une même racine carrée de -1 et la substitution $g = \begin{vmatrix} \xi_1 & -\xi_1 \\ \xi_2 & -\xi_2 \end{vmatrix}$. Elles multiplient toutes deux $\Sigma_1^2(\xi_k\eta'_k - \eta_k\xi'_k)$ par -1 et opèrent sur les variables x_1, y_1, x_2, y_2 les substitutions respectives d et dd_2 (l'action de $\{\sigma, g\}$ sur x_1, y_1, x_2, y_2, x est isomorphe à son action sur x_1, y_1, x_2, y_2, x, y). Donc

$$\{G, \sigma\}|\Delta \equiv \{R, d\}, \qquad \{G, \sigma g\}|\Delta \equiv \{R, d_2\} \equiv Q^0,$$
$$\{G, g\}|\Delta \equiv \{R, dd_2\} \equiv Q^0$$

(dd_2 transforme R comme d_2) (*cf.* I, 48), et $\{G, \sigma, g\}|\Delta \equiv Q$. Q^0 n'ayant pas de g_2 normal $\{G, g\}$ et $\{G, \sigma g\}$ n'ont pas de similitude hors de Δ. *Donc* $\{G, g\}|\Delta$ et $\{G, \sigma g\}|\Delta$ *sont isomorphes aux actions de* $\{G, g\}$ et $\{G, \sigma g\}$ *sur les rapports des variables.* Mais $\{G, \sigma\}$ contient des similitudes hors de Δ, et $\{G, \sigma\}|\Delta$ est produit direct de $G|\Delta$ par $\{\sigma\}|\Delta$.

18. Supposons que x_1, y_1, x_2, y_2, x soient dans $\mathfrak{X}'_1$. R, qui conserve $a = \Sigma_1^2 x_k y_k + x^2$, conserve aussi la forme hermitienne a' qui est sa polaire relativement au point $\dot{x}_1$, $\dot{y}_1$, $\dot{x}_2$, $\dot{y}_2$, $\dot{x}$ (*cf.*, I, 1, 9). Si donc une substitution de R remplace x_k, y_k, x respectivement par X_k, Y_k, X, elle remplace $\frac{a'}{x_1\dot{x}_1}$ par $\frac{a'}{X_1\dot{X}_1} = \frac{a'}{x_1\dot{x}_1}\frac{x_1\dot{x}_1}{X_1\dot{X}_1}$ qui a évidemment le même signe. Or soit

$$x_k = x'_k + ix''_k, \qquad y_k = y'_k + iy''_k, \qquad x = x' + ix'',$$
$$f = \frac{x_2}{x_1}, \qquad g = -\frac{y_2}{x_1}, \qquad h = \frac{x}{x_1},$$

---

posée de la matrice α d'ordre n, on a aussi $AE\overline{A} = E'$, A, E, $\overline{A}$, E′ étant les $n^{\text{ièmes}}$ combinées de α, e, $\overline{\alpha}$, e' respectivement (*Comparer* GIRAUD, *A. E. N.*, 1919, p. 217-218).

(¹) *Cf.* CARTAN, *A. E. N.*, 1914, p. 354.

et

$$f = f' + if'' = \frac{\frac{x'_2}{x''_1} + \frac{x''_2}{x'_1} + i\left(\frac{x''_2}{x''_1} - \frac{x'_2}{x'_1}\right)}{\frac{x'_1}{x''_1} + \frac{x''_1}{x'_1}} = \frac{f'_0 + if''_0}{l}, \qquad l = \frac{x'_1}{x''_1} + \frac{x''_1}{x'_1},$$

$$g = g' + ig'' = \frac{-\frac{y'_2}{x''_1} - \frac{y''_2}{x'_1} + i\left(-\frac{y''_2}{x''_1} + \frac{y'_2}{x'_1}\right)}{l} = \frac{g'_0 + ig''_0}{l},$$

$$h = h' + ih'' = \frac{\frac{x'}{x''_1} - \frac{x''}{x'_1} + i\left(\frac{x''}{x''_1} - \frac{x'}{x'_1}\right)}{l} = \frac{h'_0 + ih''_0}{l}.$$

Supposons maintenant $a = 0$. On aura

$$\frac{y_1}{x_1} = fg - h^2, \qquad \frac{a'}{x_1 x_1} = -4(f''g'' - h''^2).$$

Donc $f''g'' - h''^2$ conserve son signe par toute substitution de R. De plus, si $f''g'' - h''^2 \geq 0$, f'' et g'' ont le même signe. Or

$$(x'^2_1 + x''^2_1) f'' = x'_1 x''_2 - x'_2 x''_1$$

est conservé par R_{121}, $V_{12\lambda}$, $V_{01\lambda}$ (qui conservent par suite le signe de g''), et

$$(x'^2_1 + x''^2_1) g'' = x''_1 y'_2 - x'_1 y''_2$$

par $S_{12,-1}$, $U_{12\lambda}$, donc aussi par leur produit t_{12}. Si donc $f''g'' - h''^2$ est ≥ 0, le *signe commun de* f'', g'' *est conservé par* R (17) [si f'' et g'' ont des signes opposés, $t_{02} d_2$, qui est dans R (1, 32), et qui échange f'' et g'', change les signes de f'', g''].

Donc R conserve les six domaines suivants dans l'espace $(f', g', h', f'', g'', h'')$:

(1) $f''g'' - h''^2 > 0, \quad f'' + g'' > 0;$

(2) $f''g'' - h''^2 > 0, \quad f'' + g'' < 0;$

(3) $f''g'' - h''^2 < 0;$

(4) $f''g'' - h''^2 = 0, \quad f'' + g'' > 0;$

(5) $f''g'' - h''^2 = 0, \quad f'' + g'' < 0;$

(6) $f'' = g'' = h'' = 0.$

Je dis que R *permute transitivement les points de chacun de ces domaines*. Tout d'abord les substitutions $V_{21\lambda}$, $W_{12\mu}$, $V_{02\nu}$ ajoutent à f,

g, h les quantités réelles arbitraires λ, μ, ν. Donc la proposition est établie pour le domaine (6), et, pour les autres, il suffit de considérer les parties imaginaires f'', g'', h''. Or, R a un diviseur F dérivé des $V_{02\lambda}$, $U_{02\lambda}$, des $m_{2\mu}$ où $\mu < 0$ et de $d_1 d_2$, qui conserve $x_2 y_2 + x^2$ et permute transitivement les points de $x_2 y_2 + x^2 = \text{const.}$ (II, 15) (1). Mais F agit sur x'_2, y'_2, x', sur x''_2, y''_2, x'' et sur $x''_2 - x'_2$, $y''_2 - y'_2$, $x'' - x'$ comme sur x_2, y_2, x, et le groupe F' déduit de F en remplaçant le générateur $d_1 d_2$ par d_2 (d_1 est évidemment permutable à toute substitution de F et de F') agit de même sur f''_0, $-g''_0$, h''_0 que je vais considérer maintenant comme coordonnées, et que je désignerai par ξ, η, ζ. Comme d'ailleurs d n'a d'autre effet sur ξ, η, ζ que de changer leur signe, F et F' conservent la quadrique φ_λ définie par $-\xi\eta - \zeta^2 = \lambda$, F' permutant transitivement ses points, et F transitivement ses diamètres. En observant que $d_1 d_2$ conserve ξ et η, et change ζ en $-\zeta$, on voit donc que F contient une substitution s changeant le point $(\varepsilon, -\varepsilon\lambda, 0)$ $(\varepsilon = \pm 1)$ de φ_λ en $(\varepsilon'\xi, \varepsilon'\eta, \zeta)$ $(\varepsilon' = \pm 1)$, (ξ, η, ζ) étant un point quelconque de φ_λ, et les déterminations de ε, ε' étant choisies arbitrairement.

Si $\lambda \geqq 0$, F, qui divise R et conserve l, conserve le signe commun de ξ et de $-\eta$. Donc $(\varepsilon', \varepsilon'\eta, \zeta)$ est un point arbitraire de la partie de φ_λ où $\varepsilon'\xi$ et $\varepsilon'\eta$ ont le signe de ε. D'autre part $m_{1\mu}$ $(\mu > 0)$, qui conserve aussi l, multiplie ξ, η, ζ par -1. Donc R permute transitivement les points de chacun des domaines (1), (2), (4), (5).

Soit $\lambda = -1$, $\varepsilon = 1$, $\varepsilon' = -1$. Alors $d_1 s$ change $(1, 1, 0)$ en (ξ, η, ζ). Donc $t_{02} d_2 . d_1 s$ change $(-1, -1, 0)$ en (ξ, η, ζ). Donc $d_1 . t_{02} d_2 . d_1 s$, qui est dans R (I, 32), change $(1, 1, 0)$ en (ξ, η, ζ). On en déduit,

---

(1) Pour appliquer ici le théorème invoqué de I, 27, on remarquera que l'équivalence de $a - F(x_l, y_l)$ et de a_l résulte du principe d'inertie. De plus, on remplacera la seconde note de II, p. 29, par cette observation que le plan $a(x_1, \ldots ; \xi_1, \ldots) = 1$ coupe toujours le cône q_0 (les coordonnées courantes étant $\xi_1, \ldots$) en des points réels. Enfin, dans le cas $n = 3$, la substitution $m_{1\lambda} t_1$ doit être remplacée par une substitution de A^0, hors de B fixant le point $1\,\lambda\,0$. Pour qu'une substitution de la forme générale donnée au n° 16 remplisse ces conditions, il faut et suffit, on le voit directement, qu'à $\alpha^2 - \beta^2 \frac{\lambda}{c} = \Delta$, Δ étant non carré dans C, et que $\gamma = \frac{\beta\lambda}{c}$, $\delta = \alpha$.

comme dans le cas précédent, que R permute transitivement les points de (3).

19. *Soit* $n = 6$. Considérons les groupes L, U, H, H′, H⁰, J⁰ de variables $\xi_1, \eta_1, \xi_2, \eta_2$, l'invariant de H étant $\Sigma_1^2(\xi_k\eta_k - \mu_k\xi_k) = \alpha$, et désignons par $x_1, y_1, x_2, y_2, x_3, y_3$ les mêmes déterminants qu'au n° 17. La similitude σ qui multiplie $\xi_1, \eta_1, \xi_2, \eta_2$ par $\sqrt{-1}$ et la substitution $g = \begin{vmatrix} \xi_1 & -\xi_1 \\ \xi_2 & -\xi_2 \end{vmatrix}$ (σ est dans H⁰ ; g est dans U et dans H′, mais hors de H) opèrent respectivement sur $x_1, \ldots, y_3$ les substitutions d et dd_2. Le groupe des similitudes de U est $\Delta = \{\sigma^2\}$, et $J^0 = \{\sigma\}$.

Si $\psi = 0$, ν est impair, et R ne contient pas D. *Alors* R *est isomorphe au second combiné* U_2 *de* U *ou à* $U|\Delta$. Cela résulte de I, 45 *et de ce que* R *est simple, ainsi que* $U_2 \equiv \mathfrak{v}$. *De plus* $\{U, \sigma\}|\Delta = \{R, d\} = Q^0$ (¹). Aucune substitution de L hors de U ne peut opérer sur les x_k, y_k la substitution t_1. Car une telle substitution ayant son carré dans U aurait pour déterminant -1 et serait par suite dans 0U, 0 étant la substitution qui change ξ_1 en $-\xi_1$. Or, 0 changeant les signes des x_k sans altérer les y_k, aucune substitution de 0U ne conserve a.

Si ψ *est irréductible,* ν est pair, et R contient D. *Alors* R *est isomorphe au second combiné* H_2^0 *de* H⁰, *ou à* $H^0|\Delta$. Cela résulte de I, 46 et de ce que $\mathfrak{R}(6)$ et $\mathfrak{K}^0(4)$ sont simples. Donc $\mathfrak{R}(6) \equiv \mathfrak{K}^0(4)$. *De plus* $\{H^0, g\}|J^0 \equiv \{R, d_2\} \equiv Q^0$ (²). Aucune substitution de H′ hors de H⁰ ne peut opérer sur les x_k, y_k la substitution t_1. Car si une telle substitution t est dans H, son déterminant est -1, et t est dans μH^0, μ étant la substitution $\begin{vmatrix} \xi_1 & i\xi_1 \\ \eta_1 & i\eta_1 \end{vmatrix}$. Or, aucune substitution de μH^0 ne conserve a. Si t est dans H′ hors de H, elle multiplie α par -1 et est par conséquent dans gH^0. Elle opère donc sur les x_k, y_k une substitution de Q⁰.

20. *Dans le champ* $\mathfrak{R}_1$ *des nombres réels,* on peut, par transformation

(¹) *Cf.* CARTAN, *Annales École Normale,* 1914, p. 354.
(²) *Cf.* CARTAN, *loc. cit.*

linéaire, ramener toute forme quadratique à n variables à l'un des types $\Sigma_1^h X_j^2 - \Sigma_{h+1}^r X_j^2$ ($h = 1, \ldots, r$; $r < n$), qu'aucune substitution linéaire réelle ne peut ramener l'un à l'autre. r est le *rang*, h *l'indice d'inertie*, et le plus petit ν des deux nombres h, $r - h$, la *caractéristique* de toute forme réductible au type considéré par une substitution linéaire réelle.

Je supposerai ici que $r = n$.

Le groupe d'une forme de caractéristique ν contient toujours une substitution de forme canonique monome où ν multiplicateurs sont réels > 1, ν autres inverses des précédents, et les autres égaux à ± 1 (1), et *cette substitution ne conserve aucune forme de caractéristique* $< \nu$ (2). *Donc les groupes de deux formes de caractéristiques différentes ne peuvent être transformés l'un dans l'autre par une substitution linéaire réelle.* Comme d'ailleurs le changement de variables $X'_k = iX_k (k = 1, \ldots, n)$ transforme l'un dans l'autre deux des types précédents où h prend les valeurs h_1 et $n - h_1$, leurs groupes coïncident, et *l'on peut supposer que* h *est* $\geq n - h = \nu$. *On a alors* $h \geq \frac{n}{2}$. Le groupe du type où $\nu = 0$ et ses substitutions sont dits *orthogonaux*. Les substitutions orthogonales de déterminant 1 sont des *rotations* (3).

Prenons maintenant les variables

$$x_j = X_j + X_{h+j},\ y_j = X_j - X_{h+j} (j = 1, \ldots, \nu),\ X_{\nu+k} = z_k (k = 1, \ldots, h - \nu).$$

Les types à considérer seront les types $a = \varphi + \psi$ où

$$\varphi = \Sigma_1^\nu x_j y_j, \qquad \psi = \Sigma_1^{n-2\nu} z_k^2,$$

ν étant un des entiers ≥ 0 et $\leq \frac{n}{2}$.

Je désignerai par $Q_a = Q$ le groupe de a dans $\mathfrak{H}_1$, par $Q_a^0 = Q^0$ son diviseur formé des substitutions de déterminant 1 (groupe *unimodulaire* de a), par I le groupe des similitudes de multiplicateur réel,

(1) Par exemple, avec les variables qui vont être introduites la substitution qui multiplie $x_1, \ldots, x_\nu$ par $\lambda (> 1)$, $y_1, \ldots, y_\nu$ par λ^{-1}, et les z par ± 1.

(2) LOEWY, *N. A. H.*, t. 71, 1898, p. 444. *Voir* aussi mon Mémoire *Sur les formes bilinéaires et quadratiques* (*J. M.*, 1909, p. 42-44).

(3) *Voir* C. JORDAN, *S. M. F.*, t. 3, 1875, p. 152-174.

par $D = |d|$ son diviseur d'ordre 2 (p. g. c. d. de I, Q), par $Q'_a = Q'$ le groupe de $a = 0$ dans $\mathfrak{R}_1$, c'est-à-dire le groupe des substitutions de $\mathfrak{R}_1$ qui multiplient a par un facteur réel, par $\mathfrak{Q}_a = \mathfrak{Q}$, $\mathfrak{Q}'_a = \mathfrak{Q}'$ et $\mathfrak{Q}^0_a = \mathfrak{Q}^0$ les actions respectives de Q, Q', Q^0 sur les rapports des variables, et de plus, en posant $z^2_{2k-1} + z^2_{2k} = \psi_k$ $(2k \leqq n - 2\nu)$ et, si n est impair, $z^2_{n-2\nu} + \psi_0$, par Q_k le groupe de $\varphi + \psi_k$ (pour $\nu \geqq 0$) dans $\mathfrak{R}_1$, par Q_{kl} celui de $\psi_k + \psi_l$ $(k \neq l)$ dans $\mathfrak{R}_1$, par $\Phi_{i_1,\ldots,i_m}$ celui de $\varphi + \sum_{\mu=1}^{m} z^2_{i_\mu}$ dans $\mathfrak{R}_1$ (même si $\nu = 0$; $\Phi_{2k-1,\,2k} = Q_k$, et, si n est impair, $\Phi_{n-2\nu} = Q_0$), par $q_{i_1,\ldots,i_m}$ celui de $\sum_{\mu=1}^{m} z^2_{i_\mu}$ dans $\mathfrak{R}_1$ (pour $m = 4$ et $i_1 = 2k-1$, $i_2 = 2k$, $i_3 = 2l-1$, $i_4 = 2l$, $k \neq l$, $q_{i_1,\ldots,i_m} = Q_{kl}$; si $\nu = 0$, $q_{i_1,\ldots,i_m} = \Phi_{i_1,\ldots,i_m}$). par Q^0_k, Q^0_{kl}, $\Phi^0_{i_1,\ldots,i_m}$, $q^0_{i_1,\ldots,i_m}$ les diviseurs respectifs de Q_k, Q_{kl}, $\Phi_{i_1,\ldots,i_m}$, $q_{i_1,\ldots,i_m}$ formés de substitutions de déterminant 1, par R_k le groupe réduit de $\varphi + \psi_k$ dans $\mathfrak{R}_1$ (1), par $z^{\lambda\mu}_{kl}$ la substitution générale $\begin{vmatrix} z_k & \lambda z_k + \mu z_l \\ z_l & -\mu z_k + \lambda z_l \end{vmatrix}$ $(\lambda^2 + \mu^2 = 1$, λ et μ étant dans $\mathfrak{R}_1)$ de q^0_{kl}, par $\theta_{i_1,\ldots,i_m}$ la substitution qui change les signes de $z_{i_1}, \ldots, z_{i_m}$ sans altérer les autres variables.

Il est clair que Q^0 et Q sont normaux dans Q'_1, et que $\mathfrak{Q}^0$ et $\mathfrak{Q}$ le sont dans $\mathfrak{Q}'$.

Si n est impair, on a $Q = Q^0 D$ et $\mathfrak{Q} = QI|\,I \equiv Q\,|D \equiv Q^0 \equiv \mathfrak{Q}^0$.

Si $n > 2\nu$, Q', qui conserve la caractéristique de a, ne peut multiplier a que par des facteurs positifs. Alors $Q' = QI$, et $\mathfrak{Q}' = \mathfrak{Q}$.

Si $n = 2\nu$, la substitution γ qui multiplie les x par -1 sans altérer les y multiplie a par -1. En désignant donc par Q'' le diviseur de Q' qui multiplie a par des facteurs positifs, on a $Q' = Q'' + Q''\gamma$ et $Q'' = QI$, donc $Q'I = QI + QI\gamma$. L'action de Q'' sur les rapports des variables coïncide avec $\mathfrak{Q}$, et, en écrivant encore γ pour l'action de γ sur les rapports des variables, $\mathfrak{Q}' = \mathfrak{Q} + \mathfrak{Q}\gamma$.

Dans l'étude de Q nous pourrons supposer $n \geqq 2\nu + 3$, puisque les cas où 2ν est $\geqq n - 2$ ont déjà été considérés.

21. *Soit d'abord* $n = 3$ *et* $\nu = 0$. Prenons les variables $x_1 = z_1 + iz_2$, $y_1 = z_1 - iz_2$, $x = z_3$, et désignons par **Q** le groupe de $x_1 y_1 + x^2$

(1) Les symboles Q_k, Q^0_k, R_k n'auront jamais ici, pour $k = 1, 2$, le sens qui leur a été donné dans I, 24.

dans $\mathfrak{R}'_1$. $\mathbf{Q}$ dérive de $t_1 = \begin{vmatrix} x_1 & y_1 \\ y_1 & x_1 \end{vmatrix}$ et de son diviseur $\mathbf{Q}^0$ formé des substitutions de déterminant 1, et $\mathbf{Q} = \mathbf{Q}^0 + t_1 \mathbf{Q}^0$. Les substitutions de $\mathbf{Q}^0$ ont la forme s du n° 16 (avec $c = 1$), α, β, γ, δ étant ici dans $\mathfrak{R}_1$. *Tout nombre de* $\mathfrak{R}'_1$ *étant carré*, on peut supposer que $\Delta = 1$. *Donc ici* $\mathfrak{L} = \mathfrak{O}$, $\mathbf{Q}^0 \equiv \mathfrak{O}$ *est simple* (1) *et coïncide avec le p. p. c. m. des* U, V *dans* $\mathfrak{R}'$. Comme t_1 est réelle, et que Q^0 est formé des substitutions réelles de $\mathbf{Q}^0$, on a aussi $Q = Q^0 + t_1 Q^0$. Les conditions de réalité de s sont

$$\delta^2 = \dot{\alpha}^2, \qquad \gamma^2 = \dot{\beta}^2, \qquad \gamma\delta = -\dot{\alpha}\dot{\beta}, \qquad \beta\delta = -\dot{\alpha}\dot{\gamma}, \qquad \alpha\delta - \beta\gamma = 1,$$

ou

$$\delta = \varepsilon\dot{\alpha}\ (\varepsilon = \pm 1), \qquad \gamma = \varepsilon'\dot{\beta}\ (\varepsilon' = \pm 1), \qquad \varepsilon' = -\varepsilon, \qquad \alpha\dot{\alpha} + \beta\dot{\beta} = \varepsilon,$$

ou, puisque $\alpha\alpha + \beta\dot{\beta}$ est > 0, donc $\varepsilon = 1$,

$$\delta = \dot{\alpha}, \qquad \gamma = -\dot{\beta}, \qquad \alpha\dot{\alpha} + \beta\dot{\beta} = 1.$$

On obtient la substitution $m_{1\rho}$ (avec les notations du n° 1) en faisant $\beta = 0$, donc $\alpha\dot{\alpha} = 1$, et $\alpha^2 = \rho$ (donc $\rho\dot{\rho} = 1$).

On obtient $z_{13}^{\lambda\mu}$ en faisant $\alpha = \alpha_0$, $\beta = \beta_0$ (α_0, β_0 réels), $\alpha_0 + \beta_0^2 = 1$, $\alpha_0^2 - \beta_0^2 = \lambda$, $2\alpha_0\beta_0 = \mu$ (toujours compatibles puisque $\lambda^2 + \mu^2 = 1$), et $z_{23}^{\gamma\mu}$ en faisant $\alpha = \alpha_0$, $\beta = i\beta_0$ (α_0, β_0 réels), $\alpha_0^2 + \beta_0^2 = 1$, $\alpha_0^2 - \beta_0^2 = \lambda$, $2\alpha_0\beta_0 = -\mu$.

On voit que Q_0 *est continu, et* Q (*qui contient* des substitutions de déterminant -1) *semi-continu.*

Désignons par $s_{\alpha\beta}$ la forme réelle de s ainsi obtenue, et posons

$$\sigma_{\alpha\beta} = \begin{vmatrix} x_1 & \alpha x_1 + \beta y_1 \\ y_1 & -\dot{\beta} x_1 + \dot{\alpha} y_1 \end{vmatrix}.$$

En faisant correspondre $s_{\alpha\beta}$ à $\sigma_{\alpha\beta}$, on voit que Q^0 est holomorphe au groupe des $\sigma_{\alpha\beta}$ qui est le groupe H^0 relatif à la forme $z_1\dot{z}_1 + z_2\dot{z}_2$ (3). A l'unité de Q^0 répond d'ailleurs le g_2 normal de H^0. *Donc* $Q^0 \equiv \mathfrak{K}^0$ *qui est simple* (1).

---

(1) Cf. CARTAN, *A. E. N.*, 1914, p. 353. On peut voir très simplement comme il suit que, *le champ étant toujours* $\mathfrak{R}'_1$, *tout diviseur fini* Γ *de* $\mathfrak{O}$ *est conjugué dans* $\mathfrak{O}$ *d'un*

On peut d'ailleurs, sans passer par $\mathfrak{H}^0$, démontrer géométriquement que Q^0 est simple. Soit en effet X un diviseur normal de Q^0. Tout axe de rotation pouvant être transformé par une rotation en un axe quelconque de rotation, X doit contenir toutes les rotations d'angle $\pm\theta$ s'il en contient une seule. Or soient B et B′ les pieds de deux rotations β, β' de Q^0 d'un même angle θ, et C le pied de $\beta\beta'$ (cf. *E.*, 172, 163). On peut supposer que $0<\theta\leqq\pi$, et que l'arc de grand cercle BB′ est $<\pi$. Soit CA l'arc de grand cercle perpendiculaire à BB′ en son milieu A, et CB un arc de grand cercle faisant avec BB′ l'angle $\frac{\theta}{2}$. Désignons, comme de coutume, par A $\left(=\frac{\pi}{2}\right)$, B $\left(=\frac{\theta}{2}\right)$, C les angles du triangle ABC en A, B, C respectivement, par a, b, c les côtés

---

diviseur fini de $\mathfrak{H}^0$ (*donc tout diviseur fini de* $\mathbf{Q}^0$ *est conjugué dans* $\mathbf{Q}^0$ *d'un diviseur fini de* Q^0). Tout d'abord, pour qu'une substitution $\sigma=\frac{\alpha z+\beta}{\gamma z+\delta}$ $(\alpha\delta-\beta\gamma=1)$ de Γ soit d'ordre fini n, il faut et suffit que les multiplicateurs s, s^{-1} de la matrice $\begin{pmatrix}\alpha\beta\\ \gamma\delta\end{pmatrix}$ soient des racines de $x^{2n}=1$; soit $s=e^{i\theta}$ $(0\leqq\theta\leqq\pi$; θ sera dit l'angle de $\sigma)$. On voit que

$$\alpha+\delta=2\cos\theta$$

est réel. Supposons $\sigma\neq 1$. Comme $2\cos\theta$ est alors <2 en valeur absolue, les pôles de σ sont distincts. En prenant donc au besoin pour Γ un de ses conjugués dans $\mathfrak{V}$, on peut supposer que Γ contient une substitution de pôles 0, ∞ telle que $\tau=\frac{e^{i\varphi}}{e^{-i\varphi}}z$, qui est dans $\mathfrak{H}^0$. Si Γ est $>\{\tau\}$, supposons σ hors de $\{\tau\}$ dans Γ. Le cosinus de l'angle de $\tau\sigma$ est $\frac{1}{2}(\alpha e^{i\varphi}+\delta e^{-i\varphi})$. En égalant cette expression à sa conjuguée on voit que $\frac{\alpha-\delta}{e^{i\varphi}}$ a une valeur réelle h. Or $^{\alpha}-\delta={}^{\alpha}+\alpha-2\cos\theta$ est réel, et φ est $\neq 0$. Donc $h=0$, et $\delta=\dot{\alpha}$. Donc $\beta\gamma=\alpha\dot{\alpha}-1$ est réel. De plus en désignant par ω l'angle de $\sigma^{-1}\tau^{-1}\sigma\tau$, on a

$$\cos\omega=\alpha\delta-\beta\gamma\cos\varphi,$$

d'où $\beta\gamma=\frac{\cos\omega-1}{1-\cos\varphi}<0$. Or, $\beta\gamma$ étant réel, c'est précisément là la condition nécessaire et suffisante pour l'existence d'une substitution $\zeta=\frac{kz}{k^{-1}}$ transformant σ en une substitution de la forme $\frac{az+b}{-bz+a}=\rho$ où b est réel $\neq 0$. En prenant au besoin $\zeta^{-1}\Gamma\zeta$ pour Γ, on peut admettre que Γ contient ρ. Mais alors, σ étant de nouveau une substitution quelconque de Γ, si l'on écrit pour ρ^{σ} la condition correspondant à $\delta=\dot{\alpha}$, on obtient $\gamma=-\dot{\beta}$. On voit alors que Γ *est le transformé stéréographique d'un groupe polyédral* [*S.*, p. 207; *cf.* CAYLEY, *M. A.*, t. 15 (1879)].

opposés (¹). On aura $\cos C = \cos c \sin B$ (et quand B décroît de $\frac{\pi}{2}$ à o, C croît de c à $\frac{\pi}{2}$; donc $c \leqq C < \frac{\pi}{2}$). En faisant donc croître c, dont on dispose, de o à $\frac{\pi}{2}$, on pourra faire croître C de $\frac{\pi}{2} - B$ à $\frac{\pi}{2}$; alors l'angle $2(\pi - 2C)$ de la rotation $\beta\beta'$ décroît de 2θ à o. Si donc Q^0 contient toutes les rotations d'angle θ, il contient toutes celles d'angle $\leqq 2\theta$, donc de même toutes celles d'angle $\leqq 4\theta$, ..., donc toutes les rotations possibles (²).

22. *Soit* $n = 4$ *avec* $\nu = o$. Prenons les variables $x_1 = z_1 + iz_2$, $y_1 = z_1 - iz_2$, $x_2 = z_3 + iz_4$, $y_2 = z_3 - iz_4$, et désignons par $\mathbf{Q}$ le groupe de $\Sigma_1^2 x_k y_k$ dans $\mathfrak{H}_1'$. $\mathbf{Q}$ dérive de la substitution $t_k = \begin{vmatrix} x_k & y_k \\ y_k & x_k \end{vmatrix}$ et de son diviseur $\mathbf{Q}^0$ formé des substitutions de déterminant 1. Ici encore on a $\mathbf{Q} = \mathbf{Q}^0 + t_k \mathbf{Q}^0$, et, t_k étant réelle, $Q = Q^0 + t_k Q^0$. Comme tout élément de $\mathfrak{H}_1'$ est carré, $\mathbf{Q}^0$ *coïncide ici avec le groupe* $\mathbf{VW}$ de I, 40, et ses seuls diviseurs normaux sont 1, D, $\mathbf{V}$, $\mathbf{W}$, $\mathbf{Q}^0$ (II, p. 76).

Les substitutions de $\mathbf{W}$ ont la forme

$$r = \begin{vmatrix} x_1 & \alpha x_1 & & + \beta y_2 \\ y_1 & & \delta y_1 - \gamma x_2 & \\ x_2 & & - \beta y_1 + \alpha x_2 & \\ y_2 & \gamma x_1 & & + \delta y_2 \end{vmatrix} \qquad (\alpha\delta - \beta\gamma = 1),$$

et les substitutions de $\mathbf{V}$ la forme

$$s = \begin{vmatrix} x_1 & \alpha' x_1 & & + \beta' x_2 & \\ y_1 & & \delta' y_1 & & - \gamma' y_2 \\ x_2 & \gamma' x_1 & & + \delta' x_2 & \\ y_2 & & - \beta' y_1 & & + \alpha' y_2 \end{vmatrix} \qquad (\alpha'\delta' - \beta'\gamma' = 1).$$

(¹) On ne confondra pas le côté a avec la forme a.

(²) Tout groupe linéaire réel autre que le groupe projectif opérant sur les rapports de trois variables et ne fixant ni un point ni une droite, peut être transformé par une substitution linéaire réelle dans le groupe $\mathfrak{Q}$ qui conserve l'une des coniques $\Sigma_1^3 z^2 = o$, $x_1 y_1 + z_1^2 = o$ (LIE-ENGEL, *Theorie der Transformations gruppen*, t. III, p. 380-381).

La substitution générale de $\mathbf{Q}_0$ est donc

$$rs = sr = \begin{vmatrix} x_1 & \alpha\alpha' x_1 - \beta\beta' y_1 + \alpha\beta' x_2 + \beta\alpha' y_2 \\ y_1 & -\gamma\gamma' x_1 + \delta\delta' y_1 - \gamma\delta' x_2 - \delta\gamma' y_2 \\ x_2 & \alpha\gamma' x_1 - \beta\delta' y_1 + \alpha\delta' x_2 + \beta\gamma' y_2 \\ y_2 & \gamma\alpha' x_1 - \gamma\beta' y_1 + \gamma\beta' x_2 + \delta\alpha' y_2 \end{vmatrix}.$$

On remarquera que les substitutions rs où $\alpha' = \alpha$, $\beta' = \beta$, $\gamma' = \gamma$, $\delta' = \delta$ engendrent le groupe unimodulaire de $x_1 y_1 + z_3^2$ dans $\mathfrak{R}'_1$ (*cf.* 16); que la substitution rs où $\alpha' = \alpha$, $\beta' = \beta$, $\gamma' = \gamma$, $\delta' = \delta$ avec $\gamma = -\beta$, $\delta = \alpha$ (donc $\alpha^2 + \beta^2 = 1$), $\alpha^2 - \beta^2 = \lambda$, $2\alpha\beta = \mu$ est la substitution unimodulaire générale $\begin{vmatrix} z_1 & \lambda z_1 + \mu z_3 \\ z_3 & -\mu z_1 + \lambda z_3 \end{vmatrix}$ $(\lambda^2 + \mu^2 = 1)$ de $z_1^2 + z_3^2$ dans $\mathfrak{R}'_1$; enfin que la substitution rs où $\alpha' = \alpha$, $\beta' = \beta = 0$, $\gamma' = \gamma = 0$, $\delta' = \delta$ est la substitution unimodulaire générale de $x_1 y_1 = z_1^2 + z_2^2$ dans $\mathfrak{R}'_1$.

Pour que rs soit réelle, il faut et suffit que l'on ait

$$(1)\quad \begin{cases} \delta\delta' = \dot\alpha\dot\alpha', & \gamma\gamma' = \dot\beta\dot\beta', & \gamma\delta' = -\dot\beta\dot\alpha', & \delta\gamma' = -\dot\alpha\dot\beta', \\ \gamma\alpha' = -\dot\beta\dot\delta', & \delta\beta' = -\dot\alpha\dot\gamma', & \gamma\beta' = \dot\beta\dot\gamma', & \delta\alpha' = \dot\alpha\dot\delta'. \end{cases}$$

Supposons d'abord $\alpha, \beta, \gamma, \delta, \alpha', \beta', \gamma', \delta'$ *tous* $\neq 0$. Les équations (1) où figurent $\dot\alpha$ et δ donnent

$$\frac{\dot\alpha}{\delta} = \frac{\delta'}{\dot\alpha'} = \frac{-\gamma'}{\dot\beta'} = \frac{-\beta'}{\dot\gamma'} = \frac{\alpha'}{\dot\delta'} = \frac{\sqrt{\alpha'\beta' - \gamma'\delta'}}{\sqrt{\dot\alpha'\dot\beta' - \dot\beta'\dot\gamma'}} = \varepsilon \qquad (\varepsilon = \pm 1),$$

et les équations (1) où figurent $\dot\beta$, γ (ce sont les équations restantes)

$$\frac{\dot\beta}{\gamma} = \frac{\gamma'}{\dot\beta'} = \frac{-\delta'}{\dot\alpha'} = \frac{-\alpha'}{\dot\delta'} = \frac{\beta'}{\dot\gamma'} = -\varepsilon.$$

Donc $\alpha\delta - \beta\gamma = \varepsilon(\alpha\dot\alpha + \beta\dot\beta)$, ou $\alpha\dot\alpha + \beta\dot\beta = \varepsilon$. Or $\alpha\dot\alpha + \beta\dot\beta$ est > 0. Donc $\varepsilon = 1$. Donc $\delta = \dot\alpha$, $\gamma = -\dot\beta$, $\delta' = \dot\alpha'$, $\gamma' = -\dot\beta'$. *Donc r et s sont réelles.*

Soit maintenant $\alpha\delta = 0$. Si $\alpha = 0$ et $\delta \neq 0$, on a, d'après (1), $\delta' = \gamma' = 0$, ce qui ne se peut. Si $\delta = 0$ et $\alpha \neq 0$, on a, d'après (1), $\alpha' = \beta' = 0$, ce qui ne se peut. *Donc* $\alpha = \delta = 0$. Donc $\beta\gamma = -1$, et (1) se réduit à

$$\gamma\gamma' = \dot\beta\dot\beta', \qquad \gamma\delta' = -\dot\beta\dot\alpha', \qquad \gamma\alpha' = -\dot\beta\dot\delta', \qquad \gamma\beta' = \dot\beta\dot\gamma',$$

d'où, en multipliant par β,

$$(2) \qquad -\gamma' = \beta\dot{\beta}\beta', \quad \delta' = \beta\dot{\beta}\dot{\alpha}', \quad \alpha' = \beta\dot{\beta}\dot{\delta}', \quad -\beta' = \beta\dot{\beta}\dot{\gamma}',$$

d'où

$$\alpha'\delta' - \beta'\gamma' = \beta^2\dot{\beta}^2(\dot{\alpha}'\dot{\delta}' - \dot{\beta}'\dot{\gamma}') \qquad \text{ou} \qquad \beta^2\dot{\beta}^2 = 1.$$

Donc $\beta\dot{\beta} = 1$, et comme $\beta\gamma = -1$, $\gamma = -\dot{\beta}$. *Donc r est réelle.* De plus (2) donne alors $\delta' = \dot{\alpha}'$, $\gamma' = -\dot{\beta}'$. *Donc s est réelle.*

Soit maintenant $\beta\gamma = 0$. Si $\beta = 0$, $\gamma \neq 0$, (1) donne $\gamma' = \delta' = 0$, ce qui ne se peut, si $\gamma = 0$, $\beta \neq 0$, (1) donne $\beta' = \alpha' = 0$, ce qui ne se peut. *Donc* $\beta = \gamma = 0$. Donc $\alpha\delta = 1$, et (1) se réduit à

$$\delta\delta' = \alpha\dot{\alpha}', \qquad \delta\gamma' = -\dot{\alpha}\dot{\beta}', \qquad \delta\beta' = -\dot{\alpha}\dot{\gamma}', \qquad \delta\alpha' = \dot{\alpha}\dot{\delta}',$$

d'où, en multipliant par α,

$$(3) \qquad \delta' = \alpha\dot{\alpha}\dot{\alpha}', \quad \gamma' = -\alpha\dot{\alpha}\dot{\beta}', \quad \beta' = -\alpha\dot{\alpha}\dot{\gamma}', \quad \alpha' = \alpha\dot{\alpha}\dot{\delta}',$$

d'où, comme tout à l'heure, $\alpha\dot{\alpha} = 1$. Or $\alpha\delta = 1$. Donc $\delta = \dot{\alpha}$. *Donc r est réelle.* De plus (3) donne alors $\delta' = \dot{\alpha}'$, $\gamma' = -\dot{\beta}'$. *Donc s est réelle.*

Comme les équations (1) ne changent pas quand on échange à la fois α et α', β et β', γ et γ', δ et δ', les cas $\alpha'\delta' = 0$, $\beta'\gamma' = 0$ peuvent être négligés, et l'on conclut de suite que, *pour la réalité de rs, il faut et suffit que r et s soient réelles, c'est-à-dire que l'on ait*

$$\gamma = -\dot{\beta}, \qquad \delta = \dot{\alpha}, \qquad \gamma' = -\dot{\beta}', \qquad \delta' = \dot{\alpha}'.$$

On obtient en particulier $m_{1\rho}$ (*cf.* I, 40) en faisant $\beta = \beta' = 0$, donc $\alpha\dot{\alpha} = 1$, et $\alpha' = \alpha$, $\alpha^2 = \rho$. On obtient $m_{2\rho}$ en faisant $\beta = \beta' = 0$, donc $\alpha\dot{\alpha} = 1$, et $\alpha' = \alpha$, $\alpha^2 = \rho$. On obtient T_{12} en faisant $\alpha = i$, $\beta = 0$, $\alpha' = 0$, $\beta' = -i$. On obtient t_{12} en faisant $\alpha = \alpha' = 0$, $\beta = 1$, $\beta' = -1$.

On obtient $z_{12}^{\lambda\mu}$ en faisant $\alpha' = \alpha = \alpha_0$, $\beta' = \beta = \beta_0$, α_0 et β_0 étant réels (donc $\alpha_0^2 + \beta_0^2 = 1$) avec $\alpha_0^2 - \beta_0^2 = \lambda$, $2\alpha_0\beta_0 = \mu$ (d'où, en posant $\lambda + i\mu = e^{2i\theta}$, $\alpha_0 + i\beta_0 = \pm e^{i\theta}$).

Ici encore Q_0 *est continu, et* Q *semi-continu.*

En désignant le groupe des r réelles par $\mathbf{W}_0$, *et celui des s réelles par* $\mathbf{V}_0$, *on a* $Q^0 = \mathbf{V}_0\mathbf{W}_0$, et $\mathbf{V}_0 \equiv \mathbf{W}_0$ *est isomorphe au groupe* H_0

(1) *Cf.* CARTAN, *A. E. N.*, 1916, p. 354.

relatif à $z_1\dot{z}_1 + z_2\dot{z}_2$. $Q_0 \mid D$ *est le produit direct de* $\mathbf{V}_0 \mid D$ *par*

$$\mathbf{W}_0 \mid D, \qquad \text{et} \qquad \mathbf{V}_0 \mid D = \mathbf{W}_0 \mid D \equiv \mathfrak{H}^0.$$

Faisons correspondre à r la substitution $\left(u, \frac{\alpha u + \beta}{\gamma u + \delta}\right)$, et à s la substitution $\left(z, \frac{\alpha' z + \beta'}{\gamma' z + \delta'}\right)$. Soient $\mathfrak{v}_u$ le groupe des premières, $\mathfrak{v}_z$ celui des secondes, $\mathbf{V} \mid D$ est isomorphe à $\mathfrak{v}_u$, $\mathbf{W} \mid D$ à $\mathfrak{v}_z$, et $Q^0 \mid D \equiv \mathbf{VW} \mid D$ à $\mathfrak{v}_u \mathfrak{v}_z$. Soit $\mathfrak{K}_u^0$ le groupe des substitutions de $\mathfrak{v}_z$ où $\delta' = \alpha'$ et $\gamma' = -\beta'$. On a $\mathbf{V}_0 \mid D \equiv \mathbf{W}_0 \mid D \equiv \mathfrak{H}_z^0 = \mathfrak{H}_u^0 \equiv \mathfrak{H}^0$ et $Q^0 \mid D \equiv \mathfrak{H}_u^0 \mathfrak{H}_z^0$ (1).

Tout diviseur normal de Q^0 *autre que* D, $\mathbf{V}_0$, $\mathbf{W}_0$ *coïncide avec* Q^0, car il doit contenir $\mathbf{V}_0$ et $\mathbf{W}_0$ (4).

On remarquera que $\mathbf{W}_0$ et $\mathbf{V}_0$ *permutent transitivement les points* (x_1, y_1, x_2, y_2) *de* $x_1 y_1 + x_2 y_2 = 1$. Car une r réelle substitue au point (1, 1, 0, 0) le point $(\alpha, \alpha, -\beta, -\beta)$ qui est un point quelconque de $x_1 y_1 + x_2 y_2 = 1$, et de même pour les s.

23. *Pour* $n > 2$, Q *dérive des* Q_{kl} *et* (si $\nu > 0$) *des* Q_k. En effet, pour $n = 3, 4$, cela est clair. *Soit donc* $n > 4$, et posons $n = 2\nu'$ ou $2\nu' + 1$ selon que n est pair ou impair. Remplaçons les variables $z_1, \ldots, z_{2\nu'-2\nu}$ par $x_{\nu+k} = z_{2k-1} + iz_{2k}$, $y_{\nu+k} = z_{2k-1} - iz_{2k}$ ($k = 1, \ldots, \nu' - \nu$) et, si $n = 2\nu' + 1$, posons en outre $z_{n-2\nu} = x$. Soit alors α une substitution de Q, et prenons les notations de I, 26-28. *Si* $\nu > 0$, on pourra, comme dans I, 30, en multipliant α à droite par des générateurs des Q_k, rendre α_{11} égal à 1 et annuler les α_{k1}, β_{k1} où $k \neq 1$.

---

(1) Lie a énoncé sans démonstration que le groupe $\mathfrak{Q} \equiv Q \mid D$ pour $n = 4$ avec $\nu = 0$ dans le champ $\mathfrak{IC}$ est simple (*Theorie der Transformations gruppen*, t. III, p. 363). Cela n'est pas exact.

Tout diviseur *fini* de $\mathbf{Q}^0 \mid D$ est isomorphe au produit direct d'un diviseur *fini* de $\mathfrak{v}_u$ par un diviseur *fini* de $\mathfrak{v}_z$. Or on a vu que tout diviseur fini de $\mathfrak{v}_u$ est conjugué dans $\mathfrak{v}_u$ d'un diviseur de $\mathfrak{H}_u^0$ (20). *Donc tout diviseur fini de* $\mathbf{Q}^0 \mid D$ *est conjugué dans* $\mathbf{Q}^0 \mid D$ *d'un diviseur fini de* $Q^0 \mid D$.

Il est clair que tout diviseur fini de $Q^0 \mid D$ correspond au produit direct d'un diviseur fini de $\mathfrak{H}_u^0$ par un diviseur fini de $\mathfrak{H}_z^0$. Or ces diviseurs sont ceux correspondant aux groupes polyédraux. On connait donc tous les diviseurs finis de $\mathbf{Q}^0$ et de Q^0. On retrouve ainsi immédiatement les résultats obtenus autrement par M. Goursat (*A. E. N.*, 1889) et M. Bagnera (*R. C. M. P.*, 1901).

D'où encore $\beta_{11}=0$, $\beta'_{11}=1$, $\alpha'_{11}=0$, et l'on est ramené à une substitution de $a-x_1y_1$.

Soit donc $\nu=0$. En multipliant au besoin α à droite par une T_{1k} et une t_1, on peut supposer $\alpha_{11}\neq 0$. Multiplions alors α à droite par une substitution de la forme s (22) de Q_{12}. α_{11} sera remplacé par $\alpha'\alpha_{11}+\beta'\alpha_{21}=A_{11}$, et α_{21} par $-\dot\beta'\alpha_{11}+\dot\alpha'\alpha_{21}=A_{21}$. On peut annuler A_{21} en faisant $\dot\beta'=\dot\alpha'\dfrac{\alpha_{21}}{\alpha_{11}}$ et en même temps $|\alpha'|=\dfrac{|\alpha_{11}|}{|\alpha_{11}|+|\alpha_{21}|}$ pour satisfaire à la condition $|\alpha'|+|\beta'|=1$. Alors A_{11} sera $\neq 0$, sans quoi on aurait $\alpha_{11}=\alpha_{21}=0$ contre l'hypothèse.

Par des opérations analogues on pourra annuler tous les α_{k1} où $k>1$, α_{11} restant $\neq 0$. En multipliant α à droite par une r et par des substitutions analogues des Q_{1k}, on pourra de même annuler les β_{k1} où $k>1$. Si n est impair, α_{01} peut encore être $\neq 0$. Pour l'annuler, on multipliera α à droite par la substitution qui se déduit de la substitution $s_{\alpha\beta}$ du n° 20 en y remplaçant l'indice 1 par 2 et en y faisant $\alpha=\beta=\dfrac{1+i}{2}$, $c=1$. Mais α_{21} et β_{21} peuvent être redevenus $\neq 0$: on les annulera comme précédemment. La relation entre les coefficients de la première colonne donne alors $\beta_{11}=0$, et la relation entre les coefficients des deux premières colonnes $\alpha_{11}\beta'_{11}=1$. Or la réalité de α exige que l'on ait $\beta'_{k1}=\dot\alpha_{k1}$, $\alpha'_{k1}=\dot\beta_{k1}$ $(k\geq 1)$ et, si n est impair, $\alpha'_{01}=\dot\alpha_{01}$. Donc $\beta'_{11}=\dot\alpha_{11}$ est le seul élément $\neq 0$ de la seconde colonne. Comme d'ailleurs $\alpha_{11}\beta'_{11}=1$, on peut, en multipliant à droite par une $m_{1\rho}$ $(\rho\dot\rho=1)$, réduire α_{11} et β'_{11} à 1.

Dès lors, les relations qui lient les éléments des deux premières colonnes à ceux des suivantes montrent que α_{1k}, α'_{1k}, β_{1k}, β'_{1k} sont nuls pour $k\neq 1$, et l'on est ramené à une substitution de $a-x_1y_1$ pour laquelle on peut admettre le théorème.

Pour $n>2$, Q^0 *dérive des* Q^0_{kl} *et* (*si* $\nu>0$) *des* Q^0_k. En effet, soit M le p. p. c. m. des Q^0_{kl} et (si $\nu>0$) des Q^0_k, Le p. p. c. m. Q des Q_{kl} et (si $\nu>0$) des Q_k dérive de M et des t_j. D'ailleurs, les t_j sont permutables à M et entre eux, et $t_jt_{j'}$ est dans M. Donc $Q=M+Mt_1$, et Q_0 divise M. Mais M est $\leq Q^0$. Donc $M=Q^0$.

Comme Q^0_{kl} et Q^0_k sont continus, Q^0 *est continu. Mais* Q, contenant des substitutions de déterminant -1, *est semi-continu.*

24. *Si* $\nu = 0$ *et* $n \geq 2$, Q^0 *dérive des* q^0_{kl} (*c'est-à-dire des* $z^{\lambda\mu}_{kl}$). En effet, soit $\alpha = |x_k \ \Sigma_l \alpha_{kl} x_l|$ une substitution de Q^0. En la multipliant à droite par $z^{\lambda\mu}_{1k}$, on remplace α_{11} par $\alpha'_{11} = \lambda\alpha_{11} + \mu\alpha_{k1}$, et α_{k1} par $\alpha'_{k1} = -\mu\alpha_{11} + \lambda\alpha_{k1}$ sans altérer les autres α_{l1}. On pourra donc rendre $\alpha'_{11} \neq 0$. Supposons donc $\alpha_{11} \neq 0$. Si $\alpha_{k1} \neq 0$, il y a toujours, dans $\mathfrak{Ot}_1$, une solution de $\lambda^2 + \mu^2 = 1$ qui annule α'_{k1} : car la condition $\alpha'_{k1} = 0$ donne $\lambda = 0\alpha_{11}$, $\mu = 0\alpha_{k1}$, 0 étant indéterminé, et la condition $\lambda^2 + \mu^2 = 1$ donne $0^2(\alpha^2_{11} + \alpha^2_{k1}) = 1$, qui a toujours une solution en 0 dans $\mathfrak{Ot}_1$ (1). On pourra donc annuler tous les α_{k1} où $k \neq 1$. Alors $\alpha^2_{11} = 1$ et $\alpha_{12} = \ldots = \alpha_{1n} = 0$. En multipliant au besoin à droite par $z^{-1,0}_{12}$, on peut supposer α_{11} égal à 1 et l'on est ramené au cas de $n-1$ variables.

On remarquera que $z^{\lambda\mu}_{kl}$ est la transformée de $z^{\lambda\mu}_{hk}$ par z^{01}_{hl}. *Donc* Q_0 *dérive de* $q^0_{12}, q^0_{13}, \ldots, q^0_{1n}$, *ou encore de* $q^0_{12}, q^0_{23}, \ldots, q^0_{n-1,n}$.

Comme Q^0_{kl} et Q^0_k sont continus, Q^0 *est continu*. Mais Q, contenant des substitutions de déterminant -1, *est semi-continu*.

On peut remarquer dès maintenant que, *si* $\nu = 0$, Q^0 *n'a aucun diviseur d'indice* 2 (c'est ce qu'on a déjà trouvé pour $n = 2, 3, 4$; pour $n = 1$, $Q^0 = 1$). Car un tel diviseur X ne pouvant contenir tous les q^0_{kl}, le p. g. c. d. Y de X et d'un q^0_{kl} tel que q^0_{12} devrait être d'indice 2 dans q^0_{12} ($Q^0 = Xq^0_{12}$, et $Q^0 | X = q^0_{12} | Y$). Or q^0_{12} n'a pas de diviseur d'indice 2.

Pour étudier plus complètement la structure de Q^0 quand ν est ≥ 0, il convient de considérer d'abord Q dans le champ des nombres rationnels (comme dans le cas $n - 2\nu \leq 2$).

25. *Supposons donc maintenant que* C *est le champ* $\mathfrak{Ot}$ *des nombres rationnels*, et, les cas où $n - 2\nu$ est ≤ 2 ayant été étudiés, supposons $n - 2\nu \geq 3$.

Soit $\mathfrak{Ot}'$ le champ déduit de $\mathfrak{Ot}$ par l'adjonction de $i = \sqrt{-1}$, et gardons les mêmes notations. Soit **Q** le groupe de a dans $\mathfrak{Ot}'$ avec les variables x_k, y_k ($k = 1, \ldots, \nu$) et x si $n = 2\nu' + 1$; **Q** dérive d'une t_j et de son diviseur $\mathbf{Q}^0$ formé des substitutions de déterminant 1. Ici

(1) Cela n'est évidemment pas vrai dans $\mathfrak{Ot}$. Cela n'est pas vrai non plus dans $\mathfrak{Ot}'_1$, car $\alpha^2_{11} + \alpha^2_{k1}$ peut s'annuler dans $\mathfrak{Ot}'_1$ pour $\alpha_{11}\alpha_{k1} \neq 0$.

encore $\mathbf{Q} = \mathbf{Q}^0 + t_1\mathbf{Q}^0$, $Q = Q^0 + t_1 Q^0$, et l'on voit de même que Q^0 *dérive des* Q^0_{kl} *et* ($si\ \nu > 0$) *des* Q^0_k.

Soit $\mathbf{R} \leqq \mathbf{Q}^0$ le p. p. c. m. des V, U, W dans $\mathfrak{o}'$, et $\mathbf{R}^0 (\leqq Q^0)$ le groupe des substitutions réelles de $\mathbf{R}$, qui est le p. g. c. d. de Q^0, $\mathbf{R}$. Je dirai que $\mathbf{R}$ est le groupe *réduit* de a dans $\mathfrak{o}'$, et $\mathbf{R}^0$ le groupe *semi-réduit* de a dans $\mathfrak{o}$. $\mathbf{R}$ est normal dans $\mathbf{Q}^0$, et $\mathbf{R}^0$ dans Q^0.

Comme dans le cas des groupes galoisiens, $\mathbf{R}$ contient toutes les $m_{k\mu}$ ($k = 1, \ldots, \nu'$) où μ est carré dans $\mathfrak{o}'$. Donc $m_{k\mu}\mathbf{R} = m_{k\mu}^{-1}\mathbf{R}$, et m_{ki} est dans $m_{k2}\mathrm{R} = m_{k2}^{-1}\mathrm{R}$ [car $2i = (1+i)^2$]. Si d'ailleurs $\mu = \frac{u}{v}$, $m_{k\mu} = m_{kv^2}^{-1} m_{k,uv}$. Donc $\mathbf{Q}_0$ dérive de $\mathbf{R}$ et des $m_{k\mu}$ où μ est entier dans $\mathfrak{o}'$ et n'a aucun diviseur carré. De plus, si $m_{k\mu}$ est hors de $\mathbf{R}$, $m_{k\mu} m_{l\mu}$ ($k, l = 1, \ldots, \nu'$) est dans $\mathbf{R}$ (I, 29). Donc $\mathbf{Q}^0$ dérive de $\mathbf{R}$ et des $m_{k\mu}$ où k est un nombre fixe choisi parmi les nombres $1, \ldots, \nu'$, et où μ parcourt i $\left(\sqrt{i} = \frac{1+i}{\sqrt{2}}\right.$ n'est pas dans $\left.\mathfrak{o}'\right)$ et l'ensemble $\mathfrak{P}'$ formé des nombres premiers primaires (1) de $\mathfrak{o}'$ et de $1 \pm i$ (facteurs premiers de 2).

Je dis que, si μ *est un entier non carré de* $\mathfrak{o}'$, $m_{k\mu}$ *est hors de* $\mathbf{R}$. Comme -1 est carré dans $\mathfrak{o}'$, on peut négliger le signe de μ, et supposer μ sans diviseur carré $\neq \pm 1$.

Supposons d'abord μ *réel.* On trouvera comme au n° 9 une série de nombres premiers p tels que μ soit non carré dans le champ C_p d'ordre p, et l'on voit de même que $m_{k\mu}$ est hors de $\mathbf{R}$.

Soit $\mu = i\mu_1$, μ_1 *étant réel* > 2 ($2i$ est le carré de $1+i$). En faisant jouer à μ_1 le rôle que jouait μ dans le cas précédent, on pourra employer la même série de nombres premiers, puisque, tous les nombres premiers de cette série étant $\equiv 1 \bmod 8$ (*cf.* 9), i est carré dans C_p.

Soit $\mu = i$. On pourra employer la série des nombres premiers $\equiv 5 \bmod 8$.

Soit $\mu = i^\alpha \mu_1 \mu_2$, μ_1 *étant réel* > 0, *et* $\mu_2 = (1 \pm i)^\beta \varpi_1 \ldots \varpi_m$ ($\beta = 0$ *ou* 1) *les* ϖ_j *étant premiers complexes impairs, primaires, distincts, et*

---

(1) *Voir*, pour la théorie des nombres entiers de $\mathfrak{o}'$, BACHMANN, *Die Lehre von der Kreistheilung*, p. 150–184.

aucun d'eux n'étant conjugué d'un autre. Cherchons alors une série de nombres premiers $p \equiv 3 \bmod 4$ tels que μ soit non carré dans le champ C_{p^2} d'ordre p^2. Dans C_{p^2}, $\left(\frac{i^\alpha \mu_1}{p}\right) = 1$ (1). Donc

$$\left(\frac{\mu}{p}\right) = \left(\frac{\mu_2}{p}\right) = \left(\frac{1 \pm i}{p}\right)^\beta \Pi \left(\frac{\varpi_j}{p}\right).$$

Soit d'abord $\beta = 0$. Alors $\left(\frac{\varpi_j}{p}\right) = \left(\frac{p}{\varpi_j}\right)$ (2). Or si $\varpi_j \dot{\varpi}_j = p_j$, il y a $(\bmod \varpi_j)$ $\frac{p_j - 1}{2}$ carrés et $\frac{p_j - 1}{2}$ non carrés (3). Si d'ailleurs ξ est un des $\frac{p_j - 1}{2}$ restes quadratiques de p_j dans $\mathfrak{o}$, on a

$$\xi^{\frac{p_j - 1}{2}} \equiv 1 \pmod{p_j} \equiv 1 \pmod{\varpi_j}.$$

Donc les $\frac{p_j - 1}{2}$ restes quadratiques de p_j dans $\mathfrak{o}$ sont restes quadratiques de ϖ_j dans $\mathfrak{o}'$. Ils sont d'ailleurs incongrus mod ϖ_j dans $\mathfrak{o}'$, car la différence δ de deux d'entre eux, étant réelle, ne peut être divisible par ϖ_j sans l'être par $\dot{\varpi}_j$ (le conjugué de $\frac{\delta}{\varpi_j}$ est entier comme $\frac{\delta}{\varpi_j}$). De même les $\frac{p_j - 1}{2}$ non restes de p_j dans $\mathfrak{o}$ sont des non restes incongrus de ϖ_j dans $\mathfrak{o}'$. Il suffit donc de prendre, dans la série des nombres premiers $p \equiv 3 \bmod 4$, celle des nombres qui sont $\equiv 1 \bmod \frac{\mu_2 \dot{\mu}_2}{p_1}$ et en même temps congrus à un non reste de p_1.

Soit enfin $\beta = 1$. Comme $\left(\frac{1 \pm i}{p}\right) = (-1)^{\frac{p+1}{4}}$ (4), il suffit de prendre, dans la série des nombres premiers qu'on vient d'obtenir, celle des nombres premiers $\equiv 7 \bmod 8$.

Si donc $m_{k\mu}$ était dans $\mathbf{R}$, cela aurait encore lieu lorsqu'on prend C_{p^2} pour $\mathfrak{o}$ (en identifiant alors $\mathbf{R}$ avec le groupe réduit de la forme $\Sigma_1^{\nu'} x_k y_k$ ou $\Sigma_1^{\nu'} x_k y_k + x^2$ tel qu'il a été défini dans I, 39), en supposant p supérieur aux normes des dénominateurs des coefficients des substitutions U, V, W, par lesquelles $m_{k\mu}$ est exprimable. Or cela n'a pas lieu.

(1) BACHMANN, *op. cit.*, p. 167.
(2) *Ibid.*, p. 180.
(3) *Ibid*, p. 159 et 161.
(4) *Ibid.*, p. 181-182.

Il résulte de là que *si* $m_{k\mu}\mathbf{R} = m_{l\mu'}\mathbf{R}$, $\mu\mu'$ *est carré dans* $\mathfrak{o}'$. En effet, $m_{k\mu}m_{l\mu}$ étant dans $\mathbf{R}$ (I 29), on a $m_{k\mu}\mathbf{R} = m_{l\mu}^{-1}\mathbf{R}$. Donc $m_{l,\mu\mu'}$ est dans $\mathbf{R}$. Donc $\mu\mu'$ est carré dans $\mathfrak{o}'$.

Désignons maintenant d'une manière générale par $m_{k\rho}$ un élément réel de $m_{k\rho}\mathbf{R}$, s'il en existe (on peut supposer que $m'_{1i} = m_{1i}$). Il est clair que $m'_{k\rho}$ est déterminé mod R^0, et les relations

$$m_{k,\rho\sigma}\mathbf{R} = m_{k\rho}\mathbf{R}\, m_{k\sigma}\mathbf{R}, \qquad m_{k\mu}m_{k\mu}\mathbf{R} = \mathbf{R}$$

donnent

$$m'_{k,\rho\sigma}\mathbf{R}^0 = m'_{k\rho}m_{k\sigma}\mathbf{R}^0 \qquad m'_{k\mu}m'_{l\mu}\mathbf{R}^0 = \mathbf{R}^0.$$

Je désignerai encore par $\mathbf{R}'$ le p. p. c. m. de $\mathbf{R}$ et des $m'_{1\mu}$ où μ parcourt $\mathfrak{P}$ (si $\nu > 0$, on peut supposer que $m'_{h\mu} = m_{h\mu}$ pour $h \leq \nu$, et par $\mathbf{R}'^0$ le p. g. c. d. de $\mathbf{R}'$, Q^0. Il est clair que $\mathbf{R}'^0$ dérive de $\mathbf{R}^0$ est des $m'_{1\mu}$, que $\mathbf{R}$ est normal dans $\mathbf{R}'$, $\mathbf{R}^0$ dans $\mathbf{R}'^0$, et que

$$\mathbf{R}'^0 \,|\, \mathbf{R}^0 \equiv \mathbf{R}' \,|\, \mathbf{R}.$$

26. *Soit d'abord* $\nu = 0$, $n = 3$. — D'après le n° 21, en reprenant les mêmes notations (sauf que $\mathfrak{o}_1$ est ici remplacé par $\mathfrak{o}$, et $\mathfrak{o}'_1$ par $\mathfrak{o}'$), $\mathbf{Q}^0$ est formé des substitutions s et est isomorphe à $\mathfrak{L}$. Dans cet isomorphisme $\mathbf{R}$ correspond au diviseur $\mathfrak{v}$ de $\mathfrak{L}$ qui dérive des u_λ, v_λ ; $\mathfrak{v}$ est formé des σ où Δ est carré dans $\mathfrak{o}'$, et l'on peut supposer que, dans $\mathfrak{v}$, $\Delta = 1$ (dans $\mathfrak{o}'$, $\mathfrak{L}$ dérive de $\mathfrak{v}$ et des μz où μ parcourt $\mathfrak{P}'$ $1 \pm i$ et i).

$\mathbf{R}^0$ *correspond au diviseur* $\mathfrak{H}^0$ de $\mathfrak{v}$ *formé des* $\left(\frac{\alpha z + \beta}{\gamma z + \delta}\right)$ *où* $\gamma = -\dot{\beta}$, $\alpha\dot{\alpha} + \beta\dot{\beta} = 1$ (21). *Pour qu'une* $m_{1\mu}$ *soit dans* $\mathbf{R}^0$, *il faut donc et il suffit que* $\alpha^2 = \delta^2 = \mu$, $\gamma = \beta = 0$, $\alpha\dot{\alpha} = 1$, c'est-à-dire *que* μ *ait la forme* $\frac{\alpha}{\dot{\alpha}}$ *avec* $\alpha\dot{\alpha} = 1$. Pour $\alpha = i$, on a $\mu = 1$. *Donc* d_1 *est dans* $\mathbf{R}^0$, et c'est, dans $\mathbf{R}^0$, la seule $m_{1\mu} \neq 1$ où μ soit réel.

m_{1i}, *qui est dans* Q^0, *n'est pas dans* $\mathbf{R}^0$, puisque i n'est pas carré dans $\mathfrak{o}'$. Mais, comme $2i$ est carré, m_{1i} est dans $m_{12}\mathbf{R}^0$, donc dans $\mathbf{R}'^0$.

Toute substitution s de Q^0 hors de $\mathbf{R}$ est dans un complexe de $\mathbf{Q}^0 \,|\, \mathbf{R}$ tel que $m_{1\mu}\mathbf{R}$, μ étant un entier de $\mathfrak{o}'$ sans diviseur carré et $\neq \pm 1$. La substitution correspondante de $\mathfrak{L}$ a la forme $\frac{\alpha\mu z + \beta}{\gamma\mu z + \delta}$ $(\alpha\delta - \beta\gamma = 1)$.

Les conditions de réalité de s sont (ici $\Delta = \mu$)

$$\delta^2 = \alpha^2 \mu\dot{\mu}, \qquad \gamma^2 \mu\dot{\mu} = \beta^2, \qquad \gamma\delta = -\alpha\beta, \qquad \beta\delta = -\alpha\gamma\mu\dot{\mu},$$
$$\alpha\delta + \beta\gamma = \alpha\dot{\delta} + \beta\dot{\gamma}.$$

Donc $\mu\dot{\mu}$ est un carré m^2, et, $\mu\dot{\mu}$ étant un entier > 0, m est un entier réel que je supposerai > 0. La relation $\mu\dot{\mu} = m^2$ montre de plus que, si μ a un facteur premier complexe ϖ, il a aussi le facteur $\dot{\varpi}$. Donc μ est de la forme $i^0 m$, et l'on voit que m est un produit de facteurs premiers réels, positifs et distincts. En désignant par ε, ε' des unités égales à ± 1, les conditions de réalité de s s'écrivent

$$\delta = \varepsilon\alpha m, \qquad \gamma = \frac{\varepsilon'\beta}{m}, \qquad \gamma\delta = -\alpha\beta, \qquad \beta\delta = -\alpha\gamma m^2,$$

avec $\alpha\delta - \beta\gamma = 1$, ou $\varepsilon\alpha\dot{\alpha} m - \varepsilon' \dfrac{\beta\dot{\beta}}{m} = 1$.

L'éliminination de γ, δ donne $(\varepsilon + \varepsilon'\alpha\beta = 0$.

Si m n'a, dans $\mathfrak{R}'$, que des facteurs premiers complexes, il a la forme $m = q\dot{q}$, q étant un produit de facteurs premiers complexes dont aucun n'est conjugué d'un autre, et l'on peut faire, ou bien $\alpha = 0$, $\varepsilon' = -1$, $\beta = q$, ou bien $\beta = 0$, $\varepsilon = 1$, $\alpha = \frac{1}{q}$.

Si m a, dans $\mathfrak{R}'$, des facteurs premiers réels, $\alpha\beta$ est $\neq 0$, sans quoi on aurait une équation de la forme $f\dot{f} = mg\dot{g}$, f et g étant des entiers premiers entre eux, ce qui est évidemment impossible. Donc $\varepsilon' = -\varepsilon$, et, en posant $\alpha = \frac{\alpha'}{m}$, on a $\alpha'\dot{\alpha}' + \beta\dot{\beta} = \varepsilon m$. Donc $\varepsilon = 1$. Comme tout nombre entier > 0 est une somme de quatre carrés (1), on peut résoudre cette équation en α', β (et même les supposer entiers).

Donc Q^0 contient tous les $m'_{1\mu}\mathbf{R}^0$, c'est-à-dire que $Q^0 = \mathbf{R}'^0$.

Pour $\nu = 0$, $n = 3$, je définirai le groupe réduit R de a comme coïncidant avec $\mathbf{R}^0$, et je désignerai par R' le p. p. c. m. de R et des $m'_{1\mu}$ où μ parcourt $\mathfrak{P}$. Il est clair que $R' = \mathbf{R}'^0$. *Donc* $Q^0 = R'$.

(1) *Voir*, par exemple, BACHMANN, *Niedere Zahlentheorie*, t. II, p. 326-328, 369-373.

27. *Soit* $\nu = 0$, $n = 4$. — D'après le n° 21, en reprenant les mêmes notations (sauf que $\mathfrak{H}_1$ est ici remplacé par $\mathfrak{H}$, et $\mathfrak{H}'_1$ par $\mathfrak{H}'$), $\mathbf{R}$ est ici formé des substitutions rs et coïncide avec $\mathbf{VW}$ de I, 40, $\mathbf{R}^0$ coïncide avec $\mathbf{V}^0\mathbf{W}^0$. Ici encore

$$\mathbf{V}^0 \equiv \mathbf{W}^0 \equiv \mathrm{H}^0(2, \mathfrak{H}),$$

et $\mathbf{V}^0$, comme $\mathbf{W}^0$, permute transitivement les points x_1, y_1, x_2, y_2) de $\Sigma_1^2 x_k y_k = 1$.

Pour que $m_{1\mu}$ soit dans $\mathbf{R}^0$, il faut et suffit que l'on ait $\alpha^2 = \mu$, $\alpha' = \alpha$, $\beta = \beta' = 0$. Pour que $m_{2\mu}$ soit dans $\mathbf{R}^0$, il faut et suffit que l'on ait $\alpha^2 = \mu$, $\alpha' = \dot{\alpha}$, $\beta = \beta' = 0$. Donc, comme au n° 25, $d_k (k = 1, 2)$ *est dans* $\mathbf{R}^0$, et c'est, dans $\mathbf{R}^0$, la seule $m_{k\mu} \neq 1$ où μ soit réel. Ici encore m_{k1}, *qui est évidemment dans* Q^0, est dans $m_{k2}\,\mathbf{R}^0$ *hors de* $\mathbf{R}^0$.

Toute substitution σ de Q^0 hors de $\mathbf{R}^0$ est, comme au n° 25, dans un complexe $m_{1\mu}\mathbf{R}$ où μ est un entier non carré de $\mathfrak{H}'$. Les conditions de réalité d'une substitution $m_{1\mu}rs$ sont

$$(1)\quad \begin{cases} \dfrac{\delta\delta'}{\mu} = \alpha\dot{\alpha}'\dot{\mu}, & \gamma\gamma'\mu = \dfrac{\beta\dot{\beta}'}{\dot{\mu}}, & \gamma\alpha'\mu = -\dfrac{\beta\dot{\delta}'}{\dot{\mu}}, & \dfrac{\delta\beta'}{\mu} = -\alpha\dot{\gamma}'\mu, \\ \gamma\delta' = -\beta\dot{\alpha}', & \delta\gamma' = -\alpha\dot{\beta}', & \gamma\beta' = \beta\dot{\gamma}', & \delta\alpha' = \alpha\dot{\delta}'. \end{cases}$$

Donc, comme au n° 25, μ est de la forme $i^\varepsilon m$, m étant un produit de facteurs premiers réels, positifs et distincts.

Supposons d'abord α, β, γ, δ *non nuls*, et posons

$$\delta = \theta\alpha, \qquad \gamma = -\frac{\beta}{\zeta}.$$

Les équations (1) et (2) s'écrivent alors

$$(3)\quad \theta\delta' = m^2\dot{\alpha}', \qquad m^2\gamma' = -\zeta\dot{\beta}', \qquad m^2\alpha' = \zeta\dot{\delta}', \qquad \theta\beta' = -m^2\dot{\gamma}',$$

$$(4)\quad \delta' = \zeta\dot{\alpha}', \qquad \theta\gamma' = -\dot{\beta}', \qquad \beta' = -\zeta\dot{\gamma}', \qquad \theta\alpha' = \dot{\delta}'.$$

On déduit de (4)

$$\theta(\alpha'\delta' - \beta'\gamma') = \zeta(\dot{\alpha}'\dot{\delta}' - \dot{\beta}'\dot{\gamma}'), \qquad \text{d'où} \qquad \zeta = \theta.$$

En éliminant alors δ' et γ', on obtient de suite $\theta = \dot{\theta}$, $\theta^2 = m^2$. La condition $\alpha\delta - \beta\gamma = 1$ donne alors

$$\theta^2\alpha\dot{\alpha} + \beta\dot{\beta} = \theta.$$

Donc θ est positif, et $\theta = m$. On a donc

$$(5) \qquad \hat{\delta} = m\dot{\alpha}, \qquad \gamma = -\frac{\dot{\beta}}{m}, \qquad \delta' = m\dot{\alpha}', \qquad \gamma' = -\frac{\dot{\beta}'}{m}.$$

Soit $\alpha = 0$, donc $\beta\gamma = 1$. Alors (1) donne $\delta\hat{\delta}' = \hat{\delta}\beta' = 0$, d'où $\hat{\delta} = 0$. En posant $\dot{\beta} = -\theta\gamma$ (la condition $\beta\gamma = -1$ donne $\beta\dot{\beta} = \theta$; donc θ est réel > 0), les équations (1) et (2) s'écrivent

$$m^2\gamma' = -\theta\dot{\beta}', \qquad m^2\alpha' = \theta\hat{\delta}', \qquad \delta' = \theta\dot{\alpha}', \qquad \beta' = -\theta\dot{\gamma}',$$

d'où

$$m^2(\alpha'\hat{\delta}' - \beta'\gamma') = \theta^2(\dot{\alpha}'\hat{\delta}' - \dot{\beta}'\dot{\gamma}'),$$

d'où $\theta = m$, et l'on a encore (5).

Si $\hat{\delta} = 0$, (1) donne $\alpha\alpha' = \alpha\gamma' = 0$, d'où $\alpha = 0$, et l'on rentre dans le cas précédent.

Soit $\beta = 0$, donc $\alpha\hat{\delta} = 1$. Alors (1) donne $\gamma\gamma' = \gamma\alpha' = 0$, d'où $\gamma = 0$. En posant $\hat{\delta} = \theta\dot{\alpha}$, et en raisonnant d'une manière toute semblable, on obtient encore (5).

Si $\gamma = 0$, (1) donne $\beta\beta' = \beta\hat{\delta}' = 0$, donc $\beta = 0$, et l'on rentre dans le cas précédent.

Ainsi quels que soient α, β, γ, $\hat{\delta}$, α', β', γ', $\hat{\delta}'$, les conditions de réalité de $m_{\lambda\mu}rs$ se réduisent à (5) avec

$$\alpha\hat{\delta} - \beta\gamma = \alpha'\hat{\delta}' - \beta'\gamma' = 1 \qquad \text{ou} \qquad \alpha\dot{\alpha}m^2 + \beta\dot{\beta} = \alpha'\dot{\alpha}'m^2 + \beta'\dot{\beta}' = m.$$

Donc, comme au n° 25, $Q^0 = \mathbf{R}'^0$.

Pour $\nu = 0$, $n = 4$, *je définirai encore le groupe réduit* R *de a comme coïncidant avec* $\mathbf{R}^0$, *et je désignerai par* R′ *le p. p. c. m. de* R *et des* $m'_{\lambda\mu}$ *où* μ *parcourt* $\mathfrak{P}$. *Donc* $Q^0 = \mathbf{R}'^0 = R'$. *Ici* D *divise* R.

Faisons correspondre à r (dans le champ $\mathfrak{Z}'$) la substitution $\left(u, \frac{\alpha u + \beta}{\gamma u + \hat{\delta}}\right)$, à s la substitution $\left(z, \frac{\alpha' z + \beta'}{\gamma' z + \hat{\delta}'}\right)$, à $m_{1\lambda}$ la substitution

$$\begin{vmatrix} z & \lambda z \\ u & \lambda u \end{vmatrix} = m_\lambda,$$

à t_1 la substitution $\begin{vmatrix} z & u \\ u & z \end{vmatrix} = 1$. Alors $m_{1\lambda}m_{2\lambda}$ (qui est dans $\mathbf{R}$) corres-

pond à $|u, \lambda^2 u|$, et $m_{2\lambda} = m_{1\lambda} \cdot m_{1\lambda} m_{2\lambda}$ à $\begin{vmatrix} z & \lambda^{-1} z \\ u & \lambda u \end{vmatrix}$. Posons $\mathfrak{X} = \mathfrak{v}_z \mathfrak{v}_u$, $\mathfrak{X}_0 = \mathfrak{H}_z^0 \mathfrak{X}_u^0$, et soit $\mathfrak{F}$ le p. p. c. m. de $\mathfrak{X}$ et des ω_μ où μ parcourt $\mathfrak{P}$. Alors $\mathbf{R}|\mathrm{D}$ correspond à $\mathfrak{X}$, $\mathbf{Q}^0|\mathrm{D}$ à $\mathfrak{F}$, $\mathbf{Q}|\mathrm{D}$ à

$$|\mathfrak{F}, t| = \mathfrak{F} + t\mathfrak{F},$$

et $\mathrm{R}|\mathrm{D}$ à $\mathfrak{X}_0$. En désignant par ω'_μ la correspondante de $m'_{1\mu}$ (μ parcourant $\mathfrak{P}$) dans $\mathfrak{F}$, $\mathrm{R}'|\mathrm{D}$ correspond au p. p. c. m. $\mathfrak{X}'_0$ de $\mathfrak{X}_0$ et des ω'_μ.

28. Supposons maintenant $n \geq 5$, $\nu \geq 0$ et $n - 2\nu \geq 3$. Désignons par k, $l (k \neq l)$ deux des nombres $\nu + 1, \ldots, \nu' - \nu, 0$. Soient, pour $k, l \neq 0$, $\mathrm{R}_{kl} = \mathrm{R}_{lk}$, $\mathrm{Q}_{kl} = \mathrm{Q}_{lk}$, r_{kl}, s_{kl}, $m'^{(l)}_{k\mu}$ ce que deviennent respectivement les groupes R, Q et les substitutions r, s, m'_μ du n° 22 quand on y remplace $\mathfrak{X}_1$ par $\mathfrak{X}$, x_1 par $x_{\nu+k}$, y_1 par $y_{\nu+k}$, x_2 par $x_{\nu+l}$, y_2 par $y_{\nu+l}$ (et z_1 par z_{2k-1}, z_2 par z_{2k}, z_3 par z_{2l-1}, z_4 par z_{2l}). Soient $\mathrm{R}_{k0} = \mathrm{R}_{0k}$, $\mathrm{Q}_{k0} = \mathrm{Q}_{0k}$ et $m'^{(0)}_{k\mu}$ ce que deviennent respectivement les groupes R, Q et la substitution $m'_{1\mu}$ du n° 21 quand on y remplace $\mathfrak{X}_1$ par $\mathfrak{X}$, x_1 par $x_{\nu+k}$, y_1 par $y_{\nu+k}$ (et z_1 par z_{2k-1}, z_2 par z_{2k}, z_3 par $z_{n-2\nu}$). R_{kl} est le groupe réduit de $\psi_k + \psi_l$. Soit, pour $\nu > 0$, R_k le groupe réduit de $\varphi + \psi_k$, et posons $|d_k| = \mathrm{D}_k$, $|d_{kl}| = \mathrm{D}_{kl}$.

Je définirai ici le groupe réduit $\mathrm{R}_a = \mathrm{R}$ *de a comme étant le p. p. c. m. des* R_{kl} *et (si* $\nu > 0$*) des* R_k.

Tout d'abord, *si* $\nu > 0$, *et si* μ *est un entier réel positif ou négatif, sans diviseur carré,* $m_{1\mu}$ *est hors de* R. Supposons en effet que l'on ait $m_{1\mu} = s_1 s_2 \ldots, s_1, s_2, \ldots$ étant des substitutions des R_{kl} ou des R_k. On peut trouver comme au n° 9 un nombre premier p supérieur aux dénominateurs des coefficients des s_j et tel que $\left(\frac{\mu}{p}\right) = -1$. Dans le champ C_p d'ordre p, les s_j sont toutes paires (I, 39). Donc, dans C_p, $m_{1\mu}$ serait paire. Mais, par un changement des seules variables $z_1, \ldots, z_{n-2\nu}$, on peut ramener a dans C_p à un type où $n - 2\nu \leq 2$, et l'on a vu alors (*loc. cit.*) que $m_{1\mu}$ est impaire.

En particulier, *si* $\nu > 0$, d_1 *est hors de* R.

Considérons maintenant une substitution α de $\mathbf{R}^0$, et reprenons les notations du n° 23.

Soit d'abord $\nu = 0$. En multipliant α à droite par une r_{1k} ou une s_{1k},

on peut rendre $\alpha_{11} \neq 0$. En multipliant encore à droite, comme au n° 23, par des substitutions de R, on ramène α à une substitution de la forme $\Pi'_{j=1} m_{j\rho_j} (\rho_j \dot{\rho}_j = 1)$. Or $m_{j\rho_j}$, qui est dans un Q^0_{kl}, est permutable à R, et $m_{1\rho_j} m_{j\rho_j}$ est dans R (c'est une r_{1j}). Donc, en multipliant encore par des substitutions de R, on ramène α à $m_{1\rho}(\rho = \Pi_{\rho_j})$. Comme $\rho\dot{\rho} = 1$, ρ a la forme $\frac{\sigma}{\dot{\sigma}}$, σ étant entier dans $\mathfrak{o}'(8)$. De plus, $m_{1\rho}$ étant dans $\mathbf{R}^0$, ρ est ici carré (25), et de même $\sigma\dot{\sigma} = \rho\dot{\sigma}^2$. Soit $\sigma = u^2\mu$, μ n'ayant pas de diviseur carré $\neq \pm 1$. Il faut que $\mu\dot{\mu}$ soit carré. Si donc μ a le facteur premier complexe ϖ, il a aussi le facteur $\dot{\varpi}$. Donc μ est le produit d'une unité par un entier réel, et $\rho = \pm \left(\frac{u}{\dot{u}}\right)^2$. Donc $m_{1\rho}$ est dans R (22). Donc α est dans R. *Donc*, *pour* $\nu = 0$, $\mathbf{R}^0 = \mathrm{R}$.

Soit maintenant $\nu > 0$. En multipliant α à droite par une V, une U, ou une $t_{01} d_1$, qui est dans R (I, 32), on peut rendre $\alpha_{11} \neq 0$. En multipliant au besoin à droite par d_1, on rendra α_{11} positif (α_{11} est réel). En multipliant ensuite à droite par une $m_{1,\sigma\dot{\sigma}} m_{k,\frac{\sigma}{\dot{\sigma}}}$ (σ étant dans $\mathfrak{o}'$), qui est dans R (12), on ramène α_{11} à 1. On pourra alors, comme dans I, 30, à l'aide de substitutions de R, annuler tous les α_{j1}, β_{j1} où j est $\neq 1$. Dès lors, comme au n° 23, on est ramené au cas $\nu = 0$. On voit donc qu'ici, à cause de l'emploi éventuel de d_1, α est dans $\mathrm{R} + d_1 \mathrm{R}$. *Donc*, *pour* $\nu > 0$, $\mathbf{R}^0 = \mathrm{R} + d_1 \mathrm{R}$.

Ainsi R *est normal dans* Q^0, *et l'on peut identifier* $m'^{\prime}_{k\mu}$ (μ parcourant $\mathfrak{P}$) *avec* $m'_{k\mu}$. Donc Q^0, dérivant des Q^0_{kl} et, si $\nu > 0$, des Q^0_k, dérive de R, des $m'_{k\mu}$ et, si $\nu > 0$, des $m_{1\mu}$ et de d_1 (12). Or si $\nu = 0$, $m'_{1\mu} m_{k\mu}$ est dans $\mathbf{R}^0 = \mathrm{R}$. Si $\nu > 0$, $m_{1\mu} m_{k\mu}$, donc aussi $m_{1\mu} m'_{k\mu}$, est dans $\mathbf{R}$. Donc $m_{1\mu} m'_{k\mu}$, étant réel, est dans $\mathbf{R}^0 = \mathrm{R}$. *Donc* Q^0 *dérive de* R, *des* $m'_{1\mu}$, *et*, *si* $\nu > 0$, *de* d_1.

Désignons désormais par $\mathrm{R}' (= \mathbf{R}'^0)$ *le p.p.c.m. de* R *et des* $m'_{1\mu}$. *Si* $\nu = 0$, $Q = R'$. *Si* $\nu > 0$ (*alors on peut supposer que* $m'_{1\mu} = m_{1\mu}$), $Q^0 = R' + d_1 R'$.

Comme -1 est carré dans $\mathfrak{o}'$, d_1 est dans $\mathbf{R}$. *Donc*, *pour* $\nu \geq 0$, Q_0 *divise* $\mathbf{R}'$.

Si $\nu \geq 2$, d_2, qui est, comme d_1, hors de R, est dans $d_1 \mathrm{R}$. Donc d_{12} est dans R, ce qu'on savait d'ailleurs déjà (I, 29). Or R_{kl} contient d_k.

Donc, pour n pair, D *divise* R *toujours et seulement si* ν *est pair. Pour n impair*, D *est premier à* Q^0.

Si $\nu = 0$, R qui est $< Q^0$, ne peut contenir tous les Q^0_{kl}. Donc il n'en contient aucun, le rôle de chacun d'eux étant le même. Or $m'_{k\mu}$, comme $m'_{1\mu}$, est hors de R, puisque $m'_{1\mu} m'_{k\mu}$ est dans R. *Donc le p. g. c. d. de* R, Q^0_{kl} est R_{kl}.

29. *Pour* $\nu > 0$, *toute substitution* α *de* Q^0 (*dans* $\mathfrak{A}$) *suffisamment voisine de* 1 *est dans* R'. — Prenons en effet les notations du n° 23. Les coefficients diagonaux de α d'indices $\leq \nu$, supposés assez voisins de 1, sont réels > 0. Donc, en multipliant α à droite par des substitutions de R, on peut, comme au n° 28, et sans employer d_1, ramener α à une substitution $m_{1\rho}$ de R'.

30. *Revenons maintenant au cas où* $\Im = \mathfrak{A}_1$, *et soit* R *le p. p. c. m. des* Q^0_{kl} *et, si* $\nu > 0$, *des* R_k. R sera dit le *groupe réduit de a dans* $\mathfrak{A}_1$.

D'après ses générateurs R *est continu*.

Pour $\nu = 0$, *on a déjà vu que* $Q^0 = R$ (23). *Alors* Q^0 *est continu, et* Q^0 *contient* D *toujours et seulement si n est pair* (22, 24).

Soit $\nu > 0$. Comme $Q^0_k = R_k + d_1 R_k$ (15), Q^0 dérive de R et de d_1. Mais d_1 est-il dans R ? Supposons que $d_1 = s_1 s_2 \ldots, s_1, s_2, \ldots$ étant des substitutions des Q^0_{kl} et des R_k. On pourra trouver dans le groupe R_k ou Q^0_{kl} auquel appartient s_j une substitution s'_j à coefficients rationnels (*appartenant au groupe* R_{kl} *de* $\mathfrak{A}$ *si* s_j *est dans* Q^0_{kl}) aussi voisine qu'on le veut de s_j. Si s_j est dans R_k, cela est clair. Supposons donc s_j dans Q^0_{kl}, et remarquons d'abord qu'on peut trouver sur le cercle $x^2 + y^2 = 1$ un point (x', y') à coordonnées rationnelles aussi voisin qu'on le veut de (x, y) : cela résulte immédiatement de la représentation unicursale $x = \frac{2t}{1+t^2}$, $y = \frac{1-t^2}{1+t^2}$. Si donc α et β sont deux nombres complexes tels que $\alpha\bar{\alpha} + \beta\bar{\beta} = 1$, c'est-à-dire tels que $\alpha = e^{i\alpha_0}\cos u$, $\beta = e^{i\beta_0}\sin u$, on pourra trouver α'_0, β'_0, u', ν' aussi voisins qu'on le veut de α_0, β_0, u respectivement, et tels que $\cos\alpha'_0$, $\sin\alpha'_0$, $\cos u'$, $\sin u'$ soient rationnels. Alors $\alpha' = e^{i\alpha'_0}\cos u'$ et $\beta' = e^{i\beta'_0}\sin u'$ sont dans $\mathfrak{A}'$, et $\alpha'\bar{\alpha}' + \beta'\bar{\beta}' = 1$. De là résulte l'existence de s'_j. On aura donc une relation de la forme $d_1 e = s'_1 s'_3 \ldots$, e étant, d'après cette

relation même, une substitution du groupe Q^0 de a dans $\mathfrak{T}$ aussi voisin de 1 qu'on le veut (*cf.* 15). Donc e est dans le groupe R′ du n° 28. Mais alors d_1 serait dans R′ ce qui n'a pas lieu (28). *Donc, dans le champ* $\mathfrak{T}_1$, *si* $\nu > 0$, d_1 *est hors de* R, *et* $Q^0 = R + d_1 R$ (R *est évidemment normal dans* Q^0).

On voit alors comme au n° 15, en tenant compte des observations précédentes, que *si* $\nu > 0$, Q^0 *est semi-continu*,

Si n est impair, Q^0 est évidemment premier à D. Supposons n pair. Q^0_{kl} contient d_{kl} (22). Si d'ailleurs ν est > 0 et pair, R_k contient $d_1 d_2 \dots d_\nu$ (12). Si ν est impair ≥ 3, R_k contient $d_2 \dots d_\nu$. Comme R ne contient jamais d_1, on voit que, *pour n pair*, R *contient* D *toujours et seulement si* ν *est pair* (≥ 0).

31. Théorème. — *Pour* $n \geq 5$, $RD \mid D$ *est simple* (1).

Soit d'abord $\nu = 0$ (*alors* $Q^0 = R$), *et montrons que tout diviseur* X *non* $\leq D$ *de* Q^0, *normal dans* Q, *coïncide avec* Q^0.

Soit $s = (s_{ik})$ une substitution de X hors de D, et *supposons d'abord que s ne soit pas permutable à toutes les substitutions* θ_k (19). En raisonnant comme au n° 5 (il suffit de remplacer $z_1 z_1 + z_2 z_2$ par $z_1^2 + z_2^2$, $\Sigma_3^n z_k z_k$ par $\Sigma_3^n z_k^2$, et le facteur arbitraire ρ de module 1 par -1), on voit que X contient θ_{12}. Donc X contient chaque R_{1k} et, en transformant par T_{1l}, chaque R_{kl}. Donc $X = Q^0$.

Supposons maintenant s permutable à toutes les θ_k. Alors s se réduit à une multiplication, et comme s conserve a, ses multiplicateurs sont tous égaux à ± 1, Comme d'ailleurs s est hors de D, on peut supposer que $s = | -\varepsilon z_1, \varepsilon z_2, \varepsilon z_3, \dots | (\varepsilon = \pm 1)$. Q contient évidemment une substitution τ qui échange z_1 et z_2, et X contient $s^{-1}\tau^{-1}s\tau = \theta_{12}$. Donc, comme tout à l'heure, $X = Q^0$.

32. Supposons maintenant que ν des z_j^2 [$1 \leq \nu \leq \frac{n}{2}$ (20)], tels que z_n^2, $z_{n-1}^2, \dots, z_{n-\nu+1}^2$, soient remplacés par $-z_n^2, \dots, -z_{n-\nu+1}^2$. En raisonnant comme au n° 6 (avec les modifications indiquées au n° 31) on voit

(1) *Cf.* Cartan, *A. E. N.*, 1914, p. 286.

que X contient $\theta_{\lambda,\mu}$, le nombre des indices λ, μ qui sont $> n-\nu$ pouvant être 0, 1 ou (si $\nu > 1$) 2. Donc, en revenant maintenant aux notations du n° 28, on peut supposer que X contient, ou d_k ($k > \nu$), ou d_1, ou $\left(\text{si } 1 < \nu \leq \frac{n}{2}\right) t_{12}$. Si X contient d_k, il contient

$$T_{kl} d_k T_{kl} = d_l \quad (l > \nu),$$

donc chacun des deux diviseurs dont Q^0_{kl} est le produit, donc tous les Q^0_{kl}, et de plus tous les R_k, donc aussi R. Si X contient d_1, il contient R_k (15), donc tous les d_k (15), donc encore R. Si X contient t_{12} (pour $\nu > 1$), il contient tous les R_k, donc tous les d_k et R.

Donc, si $\nu > 0$ (*alors* $Q^0 = R + d_1 R$), *tout diviseur* X *non* $\leq D$ *de* Q^0, *normal dans* Q, *contient* R.

33. Je dis maintenant que *tout diviseur normal* X *de* Q^0 *est normal dans* Q.

Prenons a sous la forme $\Sigma_1^n \zeta_j z_j^2$ ($\zeta_j = \pm 1$), et désignons encore par les mêmes lettres les expressions de Q, Q^0, R, D et de leurs substitutions par les variables actuelles.

On peut supposer n pair, sans quoi $Q = Q^0 D$, et X, permutable à d, est évidemment normal dans Q.

Comme θ_j est hors de Q^0, l'unique conjugué de X autre que X est $X' = \theta_j X \theta_j$, normal dans Q^0 comme X, et XX′ est normal dans Q. Donc XX′ contient R. Donc $XX' = R$ ou Q^0. Le p. g. c. d. Θ de X, X′ est normal dans Q, et $XX'|\Theta$ est produit direct de $X|\Theta$ par $X'|\Theta$. Donc Θ ne contient pas R ($XX'|R$ est d'ordre 1 ou 2). Donc Θ divise D, et, en prenant XD pour X, *on peut supposer que* $\Theta = D$.

Soit $d_k = \xi\xi' = \xi'\xi d^\delta$, $\xi = (\xi_{\alpha\beta})$ étant dans X, et $\xi' = (\xi_{\alpha\beta})$ dans X′ ($\nu < k \leq \nu'$). Posons $\theta_j \xi \theta_j = \xi'_i$, $\theta_j \xi'_j \theta_j = \xi_j$; ξ_j est dans X, et ξ'_j dans X′. Comme d_k est permutable à θ_j, on a

$$d_k = \xi_j \xi'_j d^\delta.$$

Donc

$$\xi_j^{-1} \xi = \xi'_j \xi'^{-1} d^\delta = d^{\varepsilon_j} \qquad (\varepsilon_j = 0 \text{ ou } 1).$$

Donc $\theta_j \xi \theta_j = \xi' d^{\varepsilon_j + \delta}$, et $\theta_j \xi' \theta_j = \xi d^{\varepsilon_j}$. Donc $\delta = 0$, et, en posant

$$d^{\varepsilon_j} = [\rho_j] \qquad (\rho_j = \pm 1),$$

on aura

$$(1)\qquad \xi'_{jj}=\rho_j\xi_{jj},\qquad \xi'_{j\alpha}=-\rho_j\xi_{j\alpha},\qquad \xi'_{\alpha j}=-\rho_j\xi_{\alpha j}\qquad (\alpha\neq j),$$

$$(2)\qquad \xi'_{\alpha\beta}=\rho_j\xi_{\alpha\beta}\qquad (\alpha,\ \beta\neq j).$$

Faisons $j=1$ et 2. Comme les $\xi_{\alpha\beta}$ où α, β sont >2 ne sont pas tous nuls (le déterminant de ξ est $\neq 0$), on a $\rho_1=\rho_2$, et de même

$$\rho_1=\rho_3=\ldots=\rho_n.$$

Donc, d'après (1), les $\xi_{\alpha\beta}$ où $\alpha\neq\beta$ sont nuls, c'est-à-dire que ξ et ξ' sont des multiplications, et $\xi'=d^\varepsilon\xi$ ($\varepsilon=0$ ou 1). Mais ξ' est dans X′, et ξ dans X. Donc ξ et ξ' sont dans D, et d_h devrait être une similitude.

34. Soit maintenant X un diviseur normal de R non normal dans Q^0, et supposons X minimum parmi les diviseurs normaux de R qui ne sont pas normaux dans Q^0. On suppose ici $R<Q^0$, donc $\nu>0$. Alors

$$Q^0=R+d_hR\qquad (h=1,\ \ldots,\ \nu).$$

Comme au n° 33, l'unique conjugué de X autre que X dans R est $X'=d_hXd_h$, normal aussi dans R; XX′, étant normal dans Q^0, donc dans Q (33), coïncide avec R, et le p. g. c. d. Θ de X, X′ divise D. Si R contient D, c'est-à-dire si ν est pair (30), on peut, comme précédemment, supposer que $\Theta=D$. Si R ne contient pas D, $\Theta=1$. *Ainsi* Θ *est le p. g. c. d. de* R, D.

Posons $n-2\nu=m$ et

$$x_h=z_{m+h}+z_{m+\nu+h},\qquad y_h=z_{m+h}-z_{m+\nu+h}\qquad (h=1,\ \ldots,\ \nu).$$

Soit encore

$$\theta_j=|z_j-z_j|,\qquad \theta_j\theta_{j'}=\theta_{jj'},\qquad (j,j'=1,\ \ldots,\ n)$$

et

$$\theta_jX\theta_j=X_j\qquad \theta_{jj'}X\theta_{jj'}=X_{jj'}.$$

On aura

$$d_h=\theta_{m+h,m+\nu+h},\qquad \theta_{m+h}=t_hd_h,\qquad \theta_{m+\nu+h}=t_h.$$

Posons, pour abréger, $m+h=e$, $m+\nu+h=f$; alors

$$d_h=\theta_{ef},\qquad \theta_e=d_ht_h,\qquad \theta_f=t_h,\qquad \text{et}\qquad Q=R+R\theta_e+R\theta_f+R\theta_{ef}.$$

$Q|R$ est d'ordre 4, et Q a exactement 3 diviseurs d'indice 2 qui sont

$$Q^{0} = |R, \theta_{ef}|, \qquad Q^{0e} = |R, \theta_{e}|, \qquad Q^{0f} = |R, \theta_{f}|.$$

Il est clair que X_e et X_f sont, comme X, normaux dans R, et l'on a

$$X_{ef} = X', \qquad d_h X_e d_h = X_f, \qquad R = X_e X_f.$$

Les relations $\theta_e X \theta_e = X_e$, $\theta_e X' \theta_e = X_f$ montrent d'ailleurs que le p. g. c. d. de X_e, X_f est $\theta_e \Theta \theta_e = \Theta$. Donc $R|\Theta$ est le produit direct de $X_e|\Theta$ par $X_f|\Theta$.

Supposons $X_e|\Theta$ *premier à* $X|\Theta$ *et à* $X'|\Theta$. Alors : 1° $XX_e|\Theta$ est produit direct de $X|\Theta$ par $X_e|\Theta$; 2° chaque élément $\neq \Theta$ de $X_e|\Theta$, étant hors de $X|\Theta$ et de $X'|\Theta$, a la forme $\Theta g g'$, *g étant dans* X *hors de* Θ *et g' dans* X' *hors de* Θ; 3° ξ étant quelconque dans X, on aura $\Theta g g'^{\xi} = \Theta^{\xi} g g'$ ou, puisque $XX'|\Theta$ est produit direct de $X|\Theta$ par $X'|\Theta$, $\Theta g^{\xi} = \Theta^{\xi} g$. Donc Θg est normal dans X et par suite aussi dans $XX'|\Theta = R|\Theta$. Donc R aurait un central ou un second central $(E., 94) > \Theta$. Mais ce central de R, étant évidemment normal dans Q, devrait coïncider avec R (32), tandis que $R|\Theta$ n'est pas abélien.

Donc $X_e|\Theta$ *ne peut être premier à la fois à* $X|\Theta$ *et à* $X'|\Theta$ (*cf. E.*, 72). Supposons que X_e et X aient un p. g. c. d. $> \Theta$. Ce p. g. c. d. est normal dans R. Donc, d'après l'hypothèse faite sur X, *on a* $X_e = X$. De même, $X_f|\Theta$ n'étant pas premier à la fois à $X|\Theta$ et à $X'|\Theta$, *on a* $X_f = X'$.

Ainsi on a, ou bien $X_e = X$, $X_f = X'$, ou bien $X_f = X$, $X_e = X'$. Dans le premier cas θ_e est permutable à X et à X', et θ_f les transforme l'un dans l'autre. Dans le second cas θ_f est permutable à X et à X', et θ_e les transforme l'un dans l'autre.

Désignons maintenant par u un indice parcourant les nombres $1, 2, \ldots, m + \nu = n - \nu (\geq \nu + 3)$. Alors $\theta_{ue} = \theta_u t_h d_h$ *est dans* R (1., 29, 32), *donc permutable à* X *et à* X'. *Donc* θ_u *transforme* X *et* X' *comme* θ_e, *et* $\theta_{uf} = \theta_{uc} d_h$ *transforme* X *et* X' *l'un dans l'autre* (comme d_h).

Considérons encore ici $d_k = \xi \xi' = \xi' \xi d^{\delta}$, $\xi = (\xi_{\alpha\beta})$ étant dans X et $\xi' = (\xi'_{\alpha\beta})$ dans X' ($k > \nu$), *et supposons d'abord* θ_e *permutable à* X *et à* X'. On a alors

$$\theta_u \xi \theta_u = \xi_u, \qquad \theta_u \xi' \theta_u = \xi'_u,$$

ξ_u étant dans X, et ξ'_u dans X′, et

$$\xi_u\xi'_u=\xi\xi', \qquad \text{d'où} \qquad \xi^{-1}\xi_u=\xi'\xi'^{-1}_u=d^{\varepsilon_u} \qquad (\varepsilon_u=0 \text{ ou } 1).$$

Donc $\theta_u\xi\theta_u=\xi\, d^{\varepsilon_u}$, et, en posant $d^{\varepsilon_u}=[\rho_u]$ $(\rho_u=\pm 1)$,

$$\xi_{uu}=\rho_u\xi_{uu}, \quad \xi_{u\alpha}=-\rho_u\xi_{u\alpha}, \qquad \xi_{\alpha u}=-\rho_u\xi_{\alpha u} \qquad (\alpha\neq u),$$
$$\xi_{\alpha\beta}=\rho_u\xi_{\alpha\beta} \qquad (\alpha,\beta\neq u).$$

Si $\rho_u=-1$, tous les $\xi_{\alpha\beta}$ où α, β sont $\neq u$ sont nuls, et $|\xi|$ est nul, ce qui ne se peut. Donc $\rho_u=1$, et $\xi_{u\alpha}=\xi_{\alpha u}=0$. Donc ξ et, de même, ξ' opèrent sur $z_1,\ldots,z_{n-\nu}$ des multiplications, et substituent à $z_{n-\nu+1},\ldots,$ z_n des fonctions des seules variables $z_{n-\nu+1},\ldots,z_n$. D'autre part $\theta_f(f=n-\nu+1,\ldots,n)$ transforme X et X′ l'un dans l'autre. Donc, comme au n° 33,

$$\theta_f\xi'\theta_f=\xi[\rho_f] \qquad (\rho_f=\pm 1).$$

Donc $\xi'_{uu}=\rho_f\xi_{uu}$, et si, par exemple, $d_k=d_{\nu+1}=\theta_{12}$, on a

$$\rho_f\xi^2_{11}=\rho_f\xi^2_{22}=-1, \qquad \rho_f\xi^2_{33}=1 \qquad (n-2\nu \text{ est } \geq 3),$$

ce qui est impossible dans $\mathfrak{R}_4$.

Supposons maintenant θ_f permutable à X *et à* X′. On voit de même que ξ et ξ' opèrent sur $z_{n-\nu+1},\ldots,z_n$ des multiplications, et transforment $z_1,\ldots,z_{n-\nu}$ en fonctions des seules variables $z_1,\ldots,z_{n-\nu}$. D'autre part θ_u transforme ici X et X′ l'un dans l'autre. Donc, comme au n° 33, $\theta_u\xi'\theta_u=\xi[\rho_u]$. Si n ou ν est impair, R est premier à D; donc tous les ρ_u sont égaux à 1. Si n et ν sont pairs, donc $n\geq 6$, et $\nu\geq 2$, $n-\nu\ \ \nu+3$ est ≥ 5, et l'on voit comme au n° 33 que les ρ_u sont tous égaux. Donc, comme au n° 33, quel que soit $n\geq 5$, ξ et ξ' sont des multiplications, et $\xi'=d^{\varepsilon}\xi$ $(\varepsilon=0$ ou $1)$, ce qui conduit à la même impossibilité.

Donc, *dans $\mathfrak{R}_4$ pour $n\geq 5$ et* ν 0, RD | D *est simple.*

35. *Considérons en particulier le cas où $n=6$ et $\nu=0$*, et les groupes H, H⁰, H¹, H′, J, J⁰, J¹ de variables $\zeta_1,\ \zeta_2,\ \zeta_3,\ \zeta_4$, relatifs à la forme $\Sigma_1^4\zeta_k\zeta_k(2)$ (¹). J⁰ est d'ordre 4 et J¹ d'ordre 8. Désignons par *e*, *f*, *g*, *h*

(¹) *Cf.* CARTAN, *A. E. N.*, 1914, p. 355.

une permutation de 1, 2, 3, 4, et considérons les déterminants

$$Z_{ef}=\begin{vmatrix}\zeta_e & \zeta'_e\\ \zeta_f & \zeta'_f\end{vmatrix},$$

ζ'_1, ζ'_2, ζ'_3, ζ'_4 étant cogrédients à ζ_1, ζ_2, ζ_3, ζ_4. Les substitutions $\zeta^{\alpha\beta}_{ef}$, $\zeta^{\alpha\beta}_{gh}$ (3) fixent Z_{ef} et Z_{gh}, et opèrent sur Z_{eg}, Z_{hf}, Z_{fg}, Z_{eh} les substitutions respectives

$$s^{\alpha\beta}_{ef}=\begin{Vmatrix}\alpha & 0 & \beta & 0\\ 0 & \dot\alpha & 0 & \dot\beta\\ -\dot\beta & 0 & \dot\alpha & 0\\ 0 & -\beta & 0 & \alpha\end{Vmatrix},\qquad r^{\alpha\beta}_{gh}=\begin{Vmatrix}\alpha & 0 & 0 & \beta\\ 0 & \dot\alpha & \dot\beta & 0\\ 0 & -\beta & \alpha & 0\\ -\dot\beta & 0 & 0 & \dot\alpha\end{Vmatrix}.$$

Donc, en écrivant x_1, y_1, x_2, y_2, x_3, y_3 pour Z_{ef}, Z_{gh}, Z_{eg}, Z_{hf}, Z_{eh}, Z_{fg} respectivement (1), $\{H^0_{eh}, H^0_{fg}\}$ fixe x_3 et y_3, et opère sur x_1, y_1, x_2, y_2, donc aussi, avec les notations du n° 21, sur z_1, z_2, z_3, z_4 toutes les substitutions du groupe $Q^0_{a_1}$ relatif à

$$a_1=\Sigma_1^2 x_k y_k=\Sigma_1^4 z_k^2.$$

Donc H^0, qui est le p. p. c. m. des H^0_{ef}(2) opère sur

$$a=\Sigma_1^6 z_k^2 \qquad (z_5=x_3+iy_3, z_6=x_3-iy_3)$$

toutes les substitutions de $Q^0_a=Q^0$.

La similitude σ qui multiplie ζ_1, ζ_2, ζ_3, ζ_4 a $\sqrt{-1}$ opère sur $z_1, \ldots, z_6$ la similitude $d(\sigma^2$ conserve les $z_k)$, et $J^0=\{\sigma\}$. D'ailleurs ici $Q^0=R$, et Q^0 contient $d(30)$. Donc R est isomorphe au second combiné (17) H^0_2 de H^0 ou à $H^0|\{\sigma^2\}$, et $R|D\equiv H^0|J^0$.

Soit $X=H^0+H^0 t$ *un diviseur de* H' *tel que* $X|\{\sigma^2\}=Q$. Alors t^2 est dans H^0. Si donc $|t|\neq 1$, $|t|$ est égal à -1, et $X=H'$. Mais, J' étant d'ordre 8, $H'|\{\sigma^2\}$ ne peut être isomorphe à Q. Donc $|t|=1$. Mais alors t, qui est hors de H^0, multiplie $\Sigma^4\zeta_k\zeta_k$ par un facteur positif $\rho\neq 1$ (1), et ρ^2 devrait être égal à 1, ce qui ne se peut. *Donc* X *n'existe pas.*

(1) On remarquera que, dans la relation

$$\Sigma_1^3 x_k y_k=Z_{ef}Z_{gh}+Z_{eg}Z_{hf}+Z_{eh}Z_{fg},$$

les permutations *efgh*, *eghf*, *ehfg* des indices du second membre se déduisent de la première en y permutant circulairement f, g, h.