

BULLETIN DE LA S. M. F.

JEAN DIEUDONNÉ

Sur la réduction canonique des couples de matrices

Bulletin de la S. M. F., tome 74 (1946), p. 130-146

http://www.numdam.org/item?id=BSMF_1946__74__130_0

© Bulletin de la S. M. F., 1946, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>) 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 LA RÉDUCTION CANONIQUE DES COUPLES DE MATRICES ;

PAR M. JEAN DIEUDONNÉ

Introduction. — Étant donnés deux couples de matrices (A, B) , (A_1, B_1) à m lignes et n colonnes, dont les éléments appartiennent à un même corps commutatif K , le problème d'équivalence de ces deux couples consiste à trouver des conditions nécessaires et suffisantes pour qu'il existe une matrice carrée inversible P d'ordre m et une matrice carrée inversible Q d'ordre n , ayant leurs éléments dans K , et telles qu'on ait simultanément $A_1 = PAQ$ et $B_1 = PBQ$. Lorsque $m = n$ et que A est une matrice inversible, A_1 doit aussi être inversible, et on a alors $B_1 A_1^{-1} = P(BA^{-1})P^{-1}$, autrement dit, les deux matrices BA^{-1} et $B_1 A_1^{-1}$ doivent être semblables; réciproquement, si cette condition est vérifiée, on a bien $A_1 = PAQ$ et $B_1 = PBQ$, avec $Q = A^{-1}P^{-1}A_1$; on est donc ramené à la recherche des conditions pour que deux matrices carrées soient semblables, problème résolu par Weierstrass lorsque K est le corps des nombres complexes, à l'aide de la théorie des diviseurs élémentaires, qui a depuis été étendue au cas où K est un corps commutatif quelconque ⁽¹⁾. En s'appuyant sur la solution de ce cas particulier, Kronecker put résoudre le problème général de l'équivalence de deux couples de matrices lorsque K est le corps des nombres complexes, et ici encore il est possible d'étendre sa méthode lorsque K est un corps commutatif quelconque ⁽²⁾. Elle

⁽¹⁾ K. WEIERSTRASS, *Monatsberichte Akad. Berlin*, 1868, p. 310, et *Werke*, t. 2, Berlin, 1895, p. 19. Pour un exposé moderne de la théorie, voir van der WAERDEN, *Moderne Algebra*, t. II, Chap. XV.

⁽²⁾ L. KRONECKER, *Monatsberichte Akad. Berlin*, 1874, p. 397, et *Sitzungsberichte Akad. Berlin*, 1830, p. 1225. La théorie de Kronecker est exposée dans l'*Encyclopédie des Sciences mathématiques* (édition française), I, 11, article de W. F. MEYER et J. DRACH). Pour une généralisation de cette théorie à un corps commutatif quelconque, voir L. E. DICKSON, *Trans. Amer. Math. Soc.*, t. 29, 1927, p. 239.

permet, pour tout couple (A, B) , de former un couple de matrices (A_0, B_0) (dit *canonique*) équivalent à (A, B) , entièrement caractérisé par la donnée d'un nombre fini d'invariants qui sont les mêmes pour tout couple équivalent à (A, B) ; pour que deux couples soient équivalents, il faut et il suffit qu'ils aient mêmes invariants, ou (comme on dit encore) qu'ils puissent être *réduits* (par équivalence) au même couple canonique.

Weierstrass et Kronecker considèrent, en réalité, non les matrices A, B , mais les formes bilinéaires qui leur correspondent, et ne parviennent à « réduire » ces formes qu'au moyen d'artifices algébriques variés, où la théorie des déterminants et celle des polynômes jouent un rôle considérable. Mais, tandis qu'il ne semble pas qu'on ait beaucoup cherché à simplifier et à rénover la théorie de Kronecker, celle de Weierstrass a été l'objet de nombreux travaux (en raison de son utilité beaucoup plus grande). La plupart des présentations modernes de cette théorie en éliminent la théorie des déterminants à peu près complètement, mais conservent (avec raison, d'un certain point de vue) la liaison avec la théorie des polynômes : il s'agit d'ailleurs de polynômes par rapport à une matrice carrée ⁽¹⁾, ce qui explique qu'on ne puisse songer à transporter ces méthodes à la théorie de Kronecker.

On sait d'autre part qu'une des tendances de l'algèbre moderne est de formuler les résultats de l'algèbre linéaire, non plus en termes de matrices, mais en considérant directement les *applications linéaires* correspondant à ces matrices : c'est le seul point de vue qui se montre fécond quand on cherche à étendre l'algèbre linéaire aux espaces vectoriels de dimension infinie. De ce point de vue, la présentation la plus satisfaisante de la théorie de Weierstrass n'est pas celle à laquelle nous faisons allusion plus haut, mais bien une méthode dont la première idée remonte sans doute à E. Weyr ⁽²⁾; elle ne s'applique d'ailleurs avec un plein succès que lorsque K est algébriquement fermé; mais la théorie des déterminants et la théorie des polynômes n'y interviennent plus que pour assurer l'existence d'une valeur propre au

⁽¹⁾ *Monatshefte Math. Phys.*, t. 1, 1890, p. 163.

moins pour toute matrice carrée, ce qui permet d'adapter la méthode aux espaces de dimension infinie (4).

Nous nous proposons, dans cet article, de montrer comment on peut utiliser des idées analogues pour donner un nouveau traitement de la théorie de Kronecker, et obtenir une interprétation simple des invariants qui s'y introduisent.

La même méthode nous permettra aussi, lorsque les matrices A , B sont des matrices carrées, dont l'une est symétrique et l'autre symétrique gauche, d'expliquer simplement certaines particularités des diviseurs élémentaires correspondants, découvertes par Kronecker (2), à l'aide de calculs assez compliqués qui n'en laissent guère apercevoir l'origine.

1. Commençons par rappeler rapidement l'exposé de la théorie des diviseurs élémentaires, suivant les idées dont nous venons de parler (5). Soit E un espace vectoriel de dimension finie n sur un corps commutatif K ; et soit f un endomorphisme de cet espace vectoriel. Pour tout entier $p \geq 1$, désignons par f_p le $p^{\text{ième}}$ itéré de l'endomorphisme f , défini par récurrence par la relation $f_p = f \circ f_{p-1}$; on a évidemment $f_p(E) = f_{p-1}(f(E)) \subset f_{p-1}(E)$. Soit r le plus petit entier tel que $f_{r+1}(E) = f_r(E)$, autrement dit $f(f_r(E)) = f_r(E)$; restreint au sous-espace vectoriel $f_r(E)$, f est une application linéaire de ce sous-espace sur lui-même, et par suite un *automorphisme* de $f_r(E)$. Il en est donc de même de tous les itérés de f , et en particulier de f_r ; donc l'intersection de $f_r(E)$ et de $f_r^{-1}(0)$ se réduit à 0 ; comme la somme des dimensions de ces deux sous-espaces est n , on voit que E est *somme directe* de $f_r(E)$ et de $f_r^{-1}(0)$. Posons $B_p = f_p^{-1}(0)$ pour $1 \leq p \leq r$; on a $B_p \subset B_{p+1}$, et comme $B_{p+1} = f^{-1}(B_p)$ on a aussi $f(B_{p+1}) \subset B_p$; remarquons en outre qu'on ne peut avoir $B_p = B_{p+1}$ pour $p < r$, sans quoi f_p et f_{p+1} auraient même rang, donc $f_p(E)$ et $f_{p+1}(E)$ même dimension, contrairement à l'hypothèse.

(4) Voir par exemple S. BANACH, *Opérations linéaires* (Warszawa, 1932), p. 153-154.

(5) Cf. H. FITTING, *Math. Zeitschr.*, t. 39, 1935, p. 16, où la même idée est appliquée à l'étude de la décomposition d'un groupe en produit direct de sous-groupes.

Soit C_r un sous-espace de B_r de dimension $h_r > 0$ tel que B_r soit somme directe de B_{r-1} et de C_r ; comme $f^{-1}(0) \subset B_{r-1}$, la restriction de f à C_r est un isomorphisme, donc $f(C_r) \subset B_{r-1}$ a même dimension que C_r ; en outre $f(C_r)$ et B_{r-2} n'ont que 0 en commun, sans quoi il existerait un point $x \neq 0$ de C_r tel que $x \in f^{-1}(B_{r-2}) = B_{r-1}$, contrairement au choix de C_r . Il existe donc un sous-espace C_{r-1} de B_{r-1} , de dimension $h_{r-1} \geq 0$, tel que B_{r-1} soit somme directe de $f(C_r)$, de C_{r-1} et de B_{r-2} . Si l'on pose $D_{r-1} = C_{r-1} + f(C_r)$, la restriction de f à D_{r-1} est un isomorphisme, $f(D_{r-1}) \subset B_{r-2}$ a même dimension $h_r + h_{r-1}$ que D_{r-1} , et n'a que 0 en commun avec B_{r-3} . De proche en proche, on définit ainsi pour $1 \leq p \leq r$, r sous-espaces C_p (dont certains peuvent se réduire à 0) de dimensions h_p , tels que, pour chaque p , la somme $F_p = C_p + f(C_p) + f^2(C_p) + \dots + f_{p-1}(C_p)$ soit *directe*, que $C_p \subset B_p$, et que B_r soit somme directe des sous-espaces $F_1 = C_1, F_2, \dots, F_r$; en outre, les restrictions de f, f_2, \dots, f_{p-1} à C_p sont des isomorphismes, et $f_p(C_p) = \{0\}$.

On forme alors aisément une base de B_r en prenant une base arbitraire dans chacun des C_p , puis en prenant pour base dans chaque $f_k(C_p)$ ($1 \leq k \leq p-1, 1' \leq p \leq r$) l'image de la base choisie dans C_p par l'isomorphisme f_k . Cela décompose F_p en somme directe de h_p espaces $G_{\alpha,p}$ ($1 \leq \alpha \leq h_p$), $G_{\alpha,p}$ étant engendré par un élément $a_{\alpha,p}$ de la base de C_p , et ses images $f(a_{\alpha,p}), f_2(a_{\alpha,p}), \dots, f_{p-1}(a_{\alpha,p})$; chacun des $G_{\alpha,p}$ est invariant par f , et la matrice de la restriction de f à $G_{\alpha,p}$, par rapport à la base précédente, n'est autre que la matrice carrée d'ordre p

$$\left(\begin{array}{cccccc} 0 & 0 & 0 & \dots & 0 & \\ 1 & 0 & 0 & \dots & 0 & \\ 0 & 1 & 0 & \dots & 0 & \\ \dots & \dots & \dots & \dots & \dots & \\ 0 & 0 & \dots & 1 & 0 & \end{array} \right).$$

On est ainsi ramené à trouver une base de $f_r(E)$ par rapport à laquelle la matrice de la restriction de f ait une forme canonique. Autrement dit, on est ramené au problème initial en supposant que f est un *automorphisme*. Mais, si K est algébriquement fermé, il existe alors au moins une valeur propre λ de f , c'est-à-dire que l'endomorphisme $x \rightarrow f(x) - \lambda x$ est de rang $< n$; en

appliquant à cet endomorphisme la même méthode qu'à f ci-dessus, et en répétant le procédé un nombre fini de fois, on arrive finalement à la forme canonique de Weierstrass pour la matrice de l'endomorphisme f donné initialement.

On notera que l'hypothèse que K est commutatif et algébriquement fermé n'est intervenue que pour assurer l'existence d'une valeur propre pour tout endomorphisme de E ; la première partie du raisonnement est valable pour un corps K *quelconque* (commutatif ou non).

2. Avant de passer à la théorie de Kronecker, remarquons encore que la méthode précédente permet de déterminer aisément les *facteurs de composition* du groupe $\Gamma(f)$ des automorphismes u de E qui sont *permutables* avec f . Bornons-nous au cas où $f_r(E)$ est réduit à 0 (donc $E = B_r$); le cas général s'y ramène aussitôt⁽⁶⁾. Comme l'automorphisme u est aussi permutable avec f_2, f_3, \dots, f_r , il laisse invariant chacun des sous-espaces B_p ; par passage aux quotients, il donne donc un automorphisme u_p de chacun des espaces quotients E/B_{p-1} ($2 \leq p \leq r$). L'ensemble des automorphismes $u \in \Gamma(f)$ tels que u_p soit l'automorphisme identique (autrement dit, tels qu'ils laissent invariants chaque classe mod. B_{p-1}), est un *sous-groupe distingué* Γ_p de Γ . Étudions le groupe quotient Γ/Γ_r ; il est isomorphe à l'image de Γ par la représentation $u \rightarrow u_r$, et ce dernier est un sous-groupe du groupe $GL(h_r)$ de tous les automorphismes de E/B_{r-1} ; montrons qu'en fait il est *identique* à $GL(h_r)$. Il suffit pour cela de voir que pour tout automorphisme v de C_r , il existe un automorphisme $u \in \Gamma$ qui coïncide avec v sur C_r ; or les relations $u(f(x)) = f(u(x)), u(f_2(x)) = f_2(u(x)), \dots, u(f_{r-1}(x)) = f_{r-1}(u(x))$ définissent u dans F_r quand on prend $u(x) = v(x)$ dans C_r , et la restriction de u à F_r ainsi définie est un automorphisme de F_r ; si l'on prend $u(x) = x$ dans F_1, F_2, \dots, F_{r-1} , on obtient bien un automorphisme u appartenant à $\Gamma(f)$ et coïncidant avec v sur C_r .

(6) De façon précise, E est somme directe d'un nombre fini de sous-espaces E_k analogues à B_r , et dont chacun correspond à une valeur propre de f ; le groupe $\Gamma(f)$ est isomorphe au *produit* des groupes $\Gamma(f_k)$, f_k désignant la restriction de f à E_k .

Étudions maintenant la structure de Γ_r . Commençons par le cas simple où $r = 2$. L'ensemble des automorphismes $u \in \Gamma_2$, tels que la restriction $u_{1,1}$ de u à B_1 soit l'automorphisme identique, est un *sous-groupe distingué* Γ'_2 de Γ_2 (il est aussi distingué dans Γ). Pour tout $u \in \Gamma'_2$, on peut écrire $u(x) = x + \nu(x)$, où ν est une application linéaire de $E = B_2$ dans B_1 , telle que $\nu(x) = 0$ dans B_1 ; réciproquement, pour toute application linéaire ν de B_2 dans B_1 satisfaisant à cette condition, $x \rightarrow x + \nu(x)$ est un automorphisme de E , dont $x \rightarrow x - \nu(x)$ est l'automorphisme réciproque, et ces automorphismes appartiennent à Γ'_2 comme on le vérifie aussitôt. On en conclut sans peine que Γ'_2 est un groupe *abélien* isomorphe au groupe additif des applications linéaires de C_2 dans B_1 , ou, ce qui revient au même, au groupe additif des matrices à coefficients dans K , ayant h_2 colonnes et $h_1 + h_2$ lignes; ce dernier groupe lui-même est somme directe de $h_2(h_1 + h_2)$ groupes abéliens identiques au groupe additif K .

Quant au groupe quotient Γ_2/Γ'_2 , il est isomorphe à l'image de Γ_2 par la représentation $u \rightarrow u_{1,1}$, qui est un sous-groupe γ_2 du groupe de tous les automorphismes de B_1 . Pour étudier ce sous-groupe, remarquons d'abord que l'on a nécessairement $u_{1,1}(x) = x$ pour tout $x \in f(B_2) = f(C_2)$; en effet, on a $x = f(y)$, où $y \in B_2$, donc $u(x) = u(f(y)) = f(u(y)) = f(y)$, puisque $u(y) - y$ appartient à B_1 par hypothèse. Réciproquement, pour tout automorphisme ν de B_1 tel que $\nu(x) = x$ dans $f(B_2)$, il existe $u \in \Gamma_2$ tel que $u_{1,1} = \nu$; il suffit de définir u dans C_2 par la condition $u(x) = x$. Comme tout automorphisme ν appartenant à γ_2 laisse invariant $f(B_2)$, par passage au quotient il donne un automorphisme ν' de l'espace quotient $B_1/f(B_2)$; soit γ_2'' le sous-groupe des automorphismes ν appartenant à γ_2 et tels que ν' soit l'automorphisme identique de $B_1/f(B_2)$; γ_2'' est un sous-groupe distingué de γ_2 , et le groupe quotient γ_2/γ_2'' est isomorphe à l'image de γ_2 par la représentation $\nu \rightarrow \nu'$; on constate immédiatement que cette image n'est autre que le groupe $GL(h_1)$ de tous les automorphismes de l'espace vectoriel $B_1/f(B_2)$. D'autre part, pour tout automorphisme $\nu \in \gamma_2''$ et tout $x \in B_1$, on peut écrire $\nu(x) = x + \omega(x)$, où ω est une application linéaire de B_1 dans $f(B_2)$ telle que $\omega(x) = 0$ dans $f(B_2)$; réciproquement, on voit aussitôt que toute application linéaire ν de cette forme appar-

tient à γ_2'' , d'où on conclut que γ_2'' est un groupe *abélien*, isomorphe au groupe additif des matrices ayant h_1 colonnes et h_2 lignes, ou encore à la somme directe de $h_1 h_2$ groupes abéliens isomorphes au groupe additif de K .

Revenons maintenant au groupe Γ_2 . L'image réciproque de γ_2'' par l'homomorphisme de Γ_2 sur γ_2 est le sous-groupe distingué Γ_2'' de Γ_2 , formé des automorphismes u tels que $u(x) = x + v(x)$, avec $v(x) \in B_1$ pour tout $x \in B_2$, $v(x) \in f(B_2)$ pour tout $x \in B_1$ et $v(x) = 0$ dans $f(B_2)$; on vérifie sans peine que Γ_2'' est distingué dans Γ . Le groupe Γ_2''/Γ_2' , isomorphe à γ_2'' , est abélien, et le groupe Γ_2/Γ_2'' , isomorphe à γ_2/γ_2'' , est isomorphe à $GL(h_2)$; par contre il est facile de voir que le groupe Γ_2'' , qui est *métabélien* d'après ce qui précède, n'est pas abélien en général.

Passons au cas général où r est quelconque. L'étude du groupe quotient Γ_r/Γ_{r-1} se fait exactement comme celle du groupe Γ_2 dans le cas $r = 2$ qui vient d'être examiné, mais en raisonnant dans l'espace quotient E/B_{r-2} (c'est-à-dire sur les classes modulo B_{r-2}). De proche en proche, on obtient finalement le résultat suivant :

Il existe dans le groupe Γ une suite de composition

$$\Gamma, \Gamma_r, \Gamma_r'', \Gamma_r', \Gamma_{r-1}, \Gamma_{r-1}'', \Gamma_{r-1}', \dots, \Gamma_2, \Gamma_2'', \Gamma_2', \{e\}$$

dont tous les termes sont des sous-groupes distingués de Γ , qui ont les propriétés suivantes : Γ/Γ_r est isomorphe au groupe linéaire $GL(h_r)$, Γ_p/Γ_p'' est isomorphe au groupe linéaire $GL(h_{p-1})$ pour $2 \leq p \leq r$; enfin, Γ_p''/Γ_p' est un groupe abélien somme directe de $h_{p-1}(h_p + h_{p+1} + \dots + h_r)$ groupes isomorphes au groupe additif K , et Γ_p'/Γ_{p-1} est un groupe abélien somme directe de

$$(h_{p-1} + h_p + \dots + h_r)(h_p + h_{p+1} + \dots + h_r)$$

groupes isomorphes à K , pour $2 \leq p \leq r$.

3. Abordons maintenant la réduction d'un couple de matrices quelconques. Conformément au point de vue exposé dans l'introduction, ce problème revient, étant donné deux applications linéaires f, g d'un espace vectoriel E dans un espace vectoriel F , à trouver des bases de E et de F telles que les matrices de f et g , par rapport à ces bases, aient une forme canonique.

Définissons dans E une suite décroissante de sous-espaces A_i , dans F une suite décroissante de sous-espaces B_i , par les conditions $A_0 = E$, $B_0 = f(A_0) = f(E)$, puis $B_i = g(A_{i-1}) \cap f(E)$ et $A_i = \bar{f}^{-1}(B_i) = \bar{f}^{-1}(g(A_{i-1}))$ pour $i \geq 1$. Soit r le plus petit entier ≥ 0 tel que $B_{r+1} = B_r$, ce qui entraîne (en raison de $f(A_i) = B_i$) que r est aussi le plus petit entier tel que $A_{r+1} = A_r$; on a donc $f(A_r) = B_r = g(A_r) \cap f(E) \subset g(A_r)$.

Nous allons former un sous-espace E_1 de E supplémentaire de A_r et tel que les images de E_1 par f et g soient contenues toutes deux dans un supplémentaire F_1 de $g(A_r)$ dans F . Dans l'espace vectoriel A_{r-1} , désignons par M_{r-1} un sous-espace supplémentaire de $A_r + (\bar{g}^{-1}(0) \cap A_{r-1})$; décomposons d'autre part

$$A_r + (\bar{g}^{-1}(0) \cap A_{r-1})$$

en somme directe de A_r et d'un sous-espace L_{r-1} contenu dans $\bar{g}^{-1}(0)$; A_{r-1} est donc somme directe de A_r , L_{r-1} et M_{r-1} . Comme $\bar{f}^{-1}(0) \subset A_r$, $B_{r-1} = f(A_{r-1})$ est somme directe de B_r et de $P_{r-1} = f(L_{r-1} + M_{r-1})$, f étant d'ailleurs un isomorphisme de $L_{r-1} + M_{r-1}$ sur P_{r-1} ; d'autre part, $g(A_{r-1})$ est somme directe de $g(A_r)$ et de $N_{r-1} = g(M_{r-1})$, g étant un isomorphisme de M_{r-1} sur N_{r-1} ; il en résulte que $N_{r-1} \cap f(E)$ se réduit à 0.

En second lieu, dans l'espace vectoriel A_{r-2} , désignons par M_{r-2} un sous-espace supplémentaire de $A_{r-1} + (\bar{g}^{-1}(B_{r-1}) \cap A_{r-2})$; nous pouvons d'autre part décomposer $A_{r-1} + (\bar{g}^{-1}(B_{r-1}) \cap A_{r-2})$ en somme directe de A_{r-1} , d'un sous-espace L_{r-2} contenu dans $\bar{g}^{-1}(0)$, et d'un sous-espace Q_{r-2} tel que la restriction de g à Q_{r-2} soit un isomorphisme de Q_{r-2} sur P_{r-1} ; A_{r-2} est donc somme directe de A_{r-1} , L_{r-2} , Q_{r-2} et M_{r-2} . On en déduit que $B_{r-2} = f(A_{r-2})$ est somme directe de B_{r-1} et de $P_{r-2} = f(L_{r-2} + Q_{r-2} + M_{r-2})$, f étant un isomorphisme de $L_{r-2} + Q_{r-2} + M_{r-2}$ sur P_{r-2} ; d'autre part, $g(A_{r-2})$ est somme directe de $g(A_{r-1})$, de $P_{r-1} = g(Q_{r-2})$ et du sous-espace $N_{r-2} = g(M_{r-2})$, g étant un isomorphisme de M_{r-2} sur N_{r-2} , et l'intersection de N_{r-2} et de $f(E)$ se réduisant à 0.

On voit clairement comment on continuera la décomposition de E et de F en somme directe de sous-espaces; finalement, on aboutit au résultat suivant : E est somme directe de A_r et d'un sous-espace E_1 , lui-même somme directe de trois suites finies de

sous-espaces (dont certains peuvent se réduire à zéro) : $L_{r-1}, L_{r-2}, \dots, L_0; M_{r-1}, M_{r-2}, \dots, M_0; Q_{r-2}, Q_{r-3}, \dots, Q_0$. De même, l'espace F est somme directe de $g(A_r)$ et d'un sous-espace F_1 , lui-même somme directe d'un sous-espace R , supplémentaire de $f(E) + g(E)$ dans F , et de deux suites finies de sous-espaces : $N_{r-1}, N_{r-2}, \dots, N_0; P_{r-1}, P_{r-2}, \dots, P_0$. Les relations entre ces sous-espaces sont les suivantes : f est un isomorphisme de $L_i + M_i + Q_i$ sur P_i [$0 \leq i \leq r-1$, en prenant $Q_{r-i} = \{0\}$]; g est nulle dans les L_i , est un isomorphisme de M_i sur N_i pour $0 \leq i \leq r-1$, et de Q_{i-1} sur P_i pour $1 \leq i \leq r-1$; $f(E)$ est somme directe de B_r et des P_i ($0 \leq i \leq r-1$), $g(E)$ est somme directe de $g(A_r)$, des P_i ($1 \leq i \leq r-1$) et des N_i ($0 \leq i \leq r-1$).

On forme alors une base de E_i et une base de F_i de la manière suivante : on prend une base arbitraire dans chacun des L_i et dans chacun des M_i (non réduits à zéro) pour $0 \leq i \leq r-1$ ainsi que dans R ; dans N_i ($0 \leq i \leq r-1$) on prend pour base l'image de la base de M_i par g ; dans les P_i et les Q_i on définit les bases par récurrence, de sorte que la base de P_i soit l'image par f de la base de $L_i + M_i + Q_i$, et que la base de Q_{i-1} soit l'image de celle de P_i par l'isomorphisme réciproque de la restriction de g à Q_{i-1} ; nous désignerons cet isomorphisme (défini dans la somme directe des P_i d'indice ≥ 1) par g^{-1} (par abus de langage), et nous désignerons par h l'isomorphisme composé $g^{-1} \circ f$, qui applique $L_i + M_i + Q_i$ sur Q_{i-1} pour $1 \leq i \leq r-1$, par h_k ($2 \leq k \leq r-1$) l'itéré d'ordre k de l'isomorphisme h . Soit alors p_i la dimension de L_i ; pour chaque élément $a_{\alpha,i}$, de la base de L_i ($1 \leq \alpha \leq p_i$), les éléments $a_{\alpha,i}, h(a_{\alpha,i}), h_2(a_{\alpha,i}), \dots, h_i(a_{\alpha,i})$ forment une base d'un sous-espace $C'_{\alpha,i}$ de dimension $i+1$ de E_i ; les images par f de ces éléments forment une base d'un sous-espace $D'_{\alpha,i}$ de dimension $i+1$ de F_1 ; on a $f(C'_{\alpha,i}) = D'_{\alpha,i}$, $g(C'_{\alpha,i}) \subset D'_{\alpha,i}$, et les matrices carrées d'ordre $i+1$ des restrictions de f et g à $C'_{\alpha,i}$ par rapport aux bases ainsi formées dans ces deux espaces, sont respectivement de la forme

$$(I) \quad \left\{ \begin{array}{cccc} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{array} \right\}, \quad \left\{ \begin{array}{cccc} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{array} \right\}$$

De même, soit q_i la dimension de M_i ; pour chaque élément $b_{\beta,i}$ ($1 \leq \beta \leq q_i$), les éléments $b_{\beta,i}, h(b_{\beta,i}), h_2(b_{\beta,i}), \dots, h_i(b_{\beta,i})$ forment une base d'un sous-espace $C_{\beta,i}''$ de dimension $i+1$ de E_i ; les images par f de ces éléments, et l'élément $g(b_{\beta,i})$, forment une base d'un sous-espace $D_{\beta,i}''$ de dimension $i+2$ de F_i ; on a $f(C_{\beta,i}'') \subset D_{\beta,i}''$, $g(C_{\beta,i}'') \subset D_{\beta,i}''$ et les matrices (à $i+2$ lignes et $i+1$ colonnes) des restrictions de f et g à $C_{\beta,i}''$, par rapport aux bases ainsi formées, sont respectivement de la forme

$$(II) \quad \left(\begin{array}{cccc} 0 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{array} \right) \quad \left(\begin{array}{cccc} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{array} \right)$$

Avant de poursuivre la construction des bases de E et de F , nous ajouterons la remarque suivante : si f est un *isomorphisme* de E dans F , $f(A_r)$ a même dimension que A_r ; comme d'autre part $g(A_r)$ a une dimension au plus égale à celle de A_r , on ne peut avoir $f(A_r) \subset g(A_r)$ que si $f(A_r) = g(A_r)$, et si en outre la restriction de g à A_r est un *isomorphisme* de A_r sur $f(A_r) = B_r$.

4. Les résultats du n° 3 nous ramènent à former des bases des espaces $A_r \subset E$ et $g(A_r) \subset F$; nous pouvons donc désormais considérer f et g comme des applications de A_r dans $g(A_r)$. Les *transposées* f^* et g^* de ces deux applications sont donc des applications du dual $(g(A_r))^*$ dans le dual A_r^* ; en outre, comme g est une application de A_r sur $g(A_r)$, g^* est un *isomorphisme* de $(g(A_r))^*$ dans A_r^* (7). Appliquons alors la méthode du n° 3, en remplaçant E par $(g(A_r))^*$, F par A_r^* , f par g^* et g par f^* . Tenant compte de la remarque finale du n° 3, et revenant par dualité à f et g , on voit (7) qu'on décompose A_r en somme directe : 1° d'un sous-espace C_s tel que $f(C_s) = g(C_s)$, et que f et g soient des *isomorphismes* de C_s sur $D_s = f(C_s)$; 2° de sous-espaces $G'_{\gamma,j}$ ($0 \leq j \leq s-1, 1 \leq \gamma \leq p'_j$ pour chaque j) tels que $G'_{\gamma,j}$ soit de dimension $j+1$, que $f(G'_{\gamma,j}) \subset g(G'_{\gamma,j}) = H'_{\gamma,j}$, et que les matrices (carrées d'ordre $j+1$) des restrictions de f et g

(7) Pour ces propriétés élémentaires de la dualité, voir les *Éléments de Mathématique* de N. BOURBAKI, Livre II, Chap. II (à paraître prochainement).

à $G'_{\gamma,j}$, par rapport aux bases déduites par dualité de celles formées comme il a été dit au n° 3, soient respectivement de la forme

$$(III) \quad \left\{ \begin{array}{cccccc} 0 & 0 & \dots & 0 & 0 & \\ 1 & 0 & \dots & 0 & 0 & \\ 0 & 1 & \dots & 0 & 0 & \\ \cdot & \cdot & \dots & \cdot & \cdot & \\ 0 & 0 & \dots & 1 & 0 & \end{array} \right\} \quad \left\{ \begin{array}{cccccc} 1 & 0 & 0 & \dots & 0 & \\ 0 & 1 & 0 & \dots & 0 & \\ 0 & 0 & 1 & \dots & 0 & \\ \cdot & \cdot & \cdot & \dots & \cdot & \\ 0 & 0 & 0 & \dots & 1 & \end{array} \right\}.$$

3° de sous-espaces $G''_{\delta,j}$ ($0 \leq j \leq s-1$, $1 \leq \delta \leq q_j$ pour chaque j) tels que $G''_{\delta,j}$ soit de dimension $j+2$, $f(G''_{\delta,j}) = g(G''_{\delta,j}) = H''_{\delta,j}$ de dimension $j+1$, et que les matrices (à $j+1$ lignes et $j+2$ colonnes) des restrictions de f et g à $G''_{\delta,j}$ soient respectivement de la forme

$$(IV) \quad \left\{ \begin{array}{cccccc} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{array} \right\}, \quad \left\{ \begin{array}{cccccc} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 1 & 0 \end{array} \right\}$$

4° d'un sous-espace S tel que $f(S) = g(S) = \{0\}$. En outre, $g(A_r)$ est somme directe de D , et des sous-espaces $H'_{\gamma,j}$ et $H''_{\delta,j}$.

Reste enfin à former des bases canoniques dans C_s et D_s ; comme $g \circ f^{-1}$ est alors un *automorphisme* de D_s , on est ramené à appliquer la réduction de Weierstrass à cet automorphisme. En effet, supposons formée une base de D , par rapport à laquelle la matrice de $g \circ f^{-1}$ ait la forme réduite de Weierstrass; en prenant comme base dans C_s l'image par f^{-1} de la base formée dans D_s , on décompose C_s en somme directe de sous-espaces G_k tels que D_s soit somme directe des $H_k = f(G_k) = g(G_k)$, et que les matrices (carrées) des restrictions de f et g à chaque G_k soient respectivement de la forme

$$(V) \quad \left\{ \begin{array}{cccccc} 1 & 0 & 0 & \dots & 0 & \\ 0 & 1 & 0 & \dots & 0 & \\ 0 & 0 & 1 & \dots & 0 & \\ \cdot & \cdot & \cdot & \dots & \cdot & \\ 0 & 0 & 0 & \dots & 1 & \end{array} \right\} \quad \left\{ \begin{array}{cccccc} \lambda & 0 & 0 & \dots & 0 & 0 \\ 1 & \lambda & 0 & \dots & 0 & 0 \\ 0 & 1 & \lambda & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 1 & \lambda \end{array} \right\}$$

les valeurs propres λ étant toutes $\neq 0$.

On aboutit donc à former dans E et dans F deux bases telles que, par rapport à ces bases, les matrices de f et de g aient respectivement la forme

$$A_0 = \begin{pmatrix} P_1 & & & \\ & P_2 & & \\ & & \ddots & \\ & & & P_p \\ & & & & 0 \end{pmatrix} \quad B_0 = \begin{pmatrix} Q_1 & & & \\ & Q_2 & & \\ & & \ddots & \\ & & & Q_p \\ & & & & 0 \end{pmatrix}$$

où les cases non remplies sont formées de termes nuls, et où chaque couple de matrice (P_μ, Q_μ) a l'une des formes (I), (II), (III), (IV) ou (V). Ces matrices sont entièrement déterminées par la donnée des applications linéaires f et g [à l'ordre près dans la suite des couples (P_μ, Q_μ)]; pour tout couple de matrices (A, B) à m lignes et n colonnes, il existe un couple (A_0, B_0) et un seul équivalent à (A, B) ; on dira que ce couple est obtenu par réduction de (A, B) à la *forme canonique*; pour que deux couples de matrices soient équivalents, il faut et il suffit que leurs formes canoniques coïncident. On caractérise donc tout couple de matrices, d'une part par les quatre suites de nombres p_i, q_i, p'_j, q'_j , et d'autre part par les diviseurs élémentaires de l'automorphisme $g \circ f^{-1}$ du sous-espace D_s introduit ci-dessus.

On observera que toute la partie de la réduction canonique qui ne fait pas intervenir la théorie de Weierstrass ne s'appuie sur aucune hypothèse sur le corps K , qui peut être *commutatif ou non*; c'est seulement pour l'introduction des matrices de la forme (V) qu'il faut supposer que le corps K est commutatif, et que toutes les valeurs propres de l'automorphisme $g \circ f^{-1}$ appartiennent à ce corps.

5. Soient E un espace vectoriel de dimension n sur un corps commutatif K (de caractéristique *quelconque*), E^* son dual; pour tout $x \in E$ et toute forme linéaire $x' \in E^*$, nous poserons $\langle x, x' \rangle = x'(x)$ (forme bilinéaire canonique). Nous allons examiner les particularités que présente la réduction canonique de Kronecker lorsque f et g sont deux applications linéaires de E

dans son dual E^* , telles que $F(x, y) = \langle x, f(y) \rangle$ soit une forme bilinéaire *symétrique* sur $E \times E$ [autrement dit, $\langle x, f(y) \rangle = \langle y, f(x) \rangle$] et que $G(x, y) = \langle x, g(y) \rangle$ soit une forme bilinéaire *alternée* sur $E \times E$ [c'est-à-dire $\langle x, g(z) \rangle = 0$, pour tout $x \in E$, ce qui entraîne $\langle x, g(y) \rangle = -\langle y, g(x) \rangle$].

Nous dirons que x, y sont *conjugués* par rapport à F (resp. G) si $F(x, y) = 0$ [resp. $G(x, y) = 0$]; cela équivaut à $F(y, x) = 0$ [resp. $G(y, x) = 0$]. L'ensemble F_0 (resp. G_0) des $x \in E$ qui sont conjugués de *tous* les éléments de E par rapport à la forme F (resp. G) n'est autre que le sous-espace $\bar{f}(0)$ (resp. $\bar{g}(0)$). La valeur de $F(x, y)$ [resp. $G(x, y)$] ne dépend que des classes mod. F_0 (resp. mod. G_0) de x et de y ; par passage aux quotients, on obtient donc à partir de F (resp. G) une forme bilinéaire *symétrique* sur E/F_0 (resp. une forme bilinéaire *alternée* sur E/G_0) dont le rang est *égal à la dimension* de E/F_0 (resp. E/G_0); on en déduit (*) que la dimension de E/G_0 est un nombre *pair* $2h$; nous désignerons par k la dimension de E/F_0 ; la dimension de F_0 est donc $n - k$, celle de G_0 est $n - 2h$.

Pour tout sous-espace vectoriel U de E , l'ensemble des $y \in E$ qui sont conjugués de *tous* les éléments de U par rapport à F (resp. G) est un sous-espace U' de E que nous appellerons le *conjugué* de U par rapport à la forme F (resp. G). Le conjugué de U' n'est pas en général U , mais $U + F_0$ (resp. $U + G_0$). On a les lemmes suivants :

I. Si U est de dimension m , et si l'intersection $U \cap F_0$ (resp. $U \cap G_0$) est de dimension μ , le conjugué U' de U par rapport à F (resp. G) est de dimension $n - m + \mu$.

En effet, l'image canonique U_1 de U dans l'espace quotient E/F_0 est de dimension $m - \mu$; donc le sous-espace U'_1 de E/F_0 , conjugué de U_1 , est de dimension $k - (m - \mu)$; l'image réci-

(*) Pour les propriétés (classiques) des formes bilinéaires *symétriques* ou *alternées* de rang égal à la dimension de l'espace sur lequel elles sont définies, voir par exemple un mémoire de l'auteur intitulé *Sur les groupes classiques* (à paraître prochainement dans les *Publications de l'Institut mathématique de l'Université de Strasbourg*).

proque de U'_1 par l'application canonique de E sur E/F_0 , n'est autre que U' , qui a par suite une dimension égale à

$$n - k + (k - (m - \mu)) = n - m + \mu.$$

Démonstration identique pour la forme G .

II. Soient U, V deux sous-espaces de E , U' et V' leurs conjugués respectifs par rapport à F (resp. G). Si $V + U'$ est de dimension m , et si $U \cap F_0$ (resp. $U \cap G_0$) est de dimension μ , $U \cap V'$ est de dimension $n - m + \mu$.

En effet, soient U_1, V_1 les images canoniques de U et V dans E/F_0 , U'_1 et V'_1 celles de U' et V' ; comme F_0 est contenu dans U' et dans V' , $V_1 + U'_1$ est l'image canonique de $V + U'$, et $U_1 \cap V'_1$ celle de $U \cap V'$; $V_1 + U'_1$ est de dimension $m - (n - k)$, et si p est la dimension de $U \cap V'$, celle de $U_1 \cap V'_1$ est $p - \mu$. Or, $U_1 \cap V'_1$ et $V_1 + U'_1$ sont deux sous-espaces conjugués dans E/F_0 ; on a donc $p - \mu + m - (n - k) = k$, ce qui démontre la proposition (le raisonnement étant identique pour G).

III. Si U est un sous-espace de E , U' son conjugué par rapport à la force alternée G , la différence des dimensions de U et de $U \cap U'$ est un nombre pair.

En effet, soient m la dimension de U , μ celle de $U \cap G_0$; l'image canonique U_1 de U dans E/G_0 est de dimension $m - \mu$; si U'_1 est le conjugué de U_1 dans E/G_0 , la différence des dimensions de U_1 et de $U_1 \cap U'_1$ est un nombre pair (*). Mais on passe des dimensions de U_1 et $U_1 \cap U'_1$ à celles de U et $U \cap U'$ en leur ajoutant respectivement μ , d'où la proposition.

6. Ces préliminaires étant établis, appliquons la méthode du n° 3. Les sous-espaces A_i de E peuvent être définis par récurrence à partir de $A_0 = E$ par la formule $A_{i+1} = \overline{f(g(A_i))}$ ($0 \leq i \leq r-1$). Nous allons voir que, si A'_i désigne le conjugué du sous-espace A_i par rapport à G , A_{i+1} n'est autre que le conjugué de A'_i par rapport à F . En effet, la relation $x \in A_{i+1}$ signifie qu'il existe

$y \in A_i$ tel que $f(x) = g(y)$; pour tout $z \in A'_i$, on a donc $F(x, z) = \langle z, f(x) \rangle = \langle z, g(y) \rangle = G(z, y) = 0$ d'après la définition de A'_i ; réciproquement, si $F(x, z) = \langle z, f(x) \rangle = 0$ pour tout $z \in A'_i$, il existe $y \in A_i$ tel que $f(x) = g(y)$, puisque le conjugué de A'_i par rapport à G est le sous-espace $A_i + G_0$. En d'autres termes, si l'on exprime le fait que U' est conjugué de U par rapport à F (resp. G) par la notation $U \perp U'$ (resp. $U \psi U'$), on a pour déterminer les A_i la suite des relations

$$(1) \quad A_0 = E \psi A'_0 = G_0 \perp A_1 \psi A'_1 \perp A_2 \psi A'_2 \perp \dots \perp A_{r-1} \psi A'_{r-1} \perp A_r.$$

Pour tout $i \geq 0$, désignons alors par m_i la dimension de $A_i \cap G_0$, par n_i la dimension de $A'_i \cap F_0$; on a $m_0 = n - 2h$. Comme la dimension de A'_0 est $n - 2h$, celle de A_1 est $2h + n_0$ d'après le lemme 1; celle de A'_1 est $n - (2h + n_0) + m_1$, d'après le même lemme; par récurrence, on voit que la dimension de A_i est

$$2h + (n_0 + n_1 + \dots + n_{i-1}) - (m_1 + m_2 + \dots + m_{i-1}) \quad \text{pour } i > 1$$

et que la dimension de A'_i est

$$n - 2h + (m_1 + m_2 + \dots + m_i) - (n_0 + n_1 + \dots + n_{i-1}) \quad \text{pour } i > 0.$$

Comme $G_0 = \bar{g}(0)$, la définition des nombres p_i (n° 3) donne $p_i = m_i - m_{i+1}$ pour $0 \leq i \leq r-1$; celle des nombres q_i donne la relation

$$p_i + p_{i+1} + \dots + p_{r-1} + q_i + q_{i+1} + \dots + q_{r-1} = m_i - n_i,$$

qui exprime que A_i est somme directe de A_{i+1} et de $2(r-i)$ sous-espaces de dimensions $p_i, p_{i+1}, \dots, p_{r-1}, q_i, q_{i+1}, \dots, q_{r-1}$. De cette relation, on tire $q_{r-1} = m_r - n_{r-1}$, et $q_i = n_{i+1} - n_i$ pour $0 \leq i \leq r-2$.

Cela étant, nous allons démontrer que les nombres p_i d'indice impair sont pairs (Kronecker); il nous suffira de prouver que les sommes $m_{2j-1} + m_{2j}$ sont toutes paires. Considérons pour cela le sous-espace $A'_0 + A_{2j}$; comme la dimension de $A_{2j} \cap A'_0$ est m_{2j} , la dimension de $A'_0 + A_{2j}$ est

$$\begin{aligned} n - 2h + [2h + (n_0 + \dots + n_{2j-1}) - (m_1 + \dots + m_{2j-1})] - m_{2j} \\ = n + (n_0 + \dots + n_{2j-1}) - (m_1 + \dots + m_{2j}). \end{aligned}$$

D'après la relation (1) et le lemme II (appliqué à la forme F), la dimension de $A_1 \cap A'_{2j-1}$ est donc

$$\begin{aligned} n - [n + (n_0 + \dots + n_{2j-1}) - (m_1 + \dots + m_{2j})] + n_{2j-1} \\ = (m_1 + \dots + m_{2j}) - (n_0 + \dots + n_{2j-2}). \end{aligned}$$

Le lemme II, appliqué cette fois à la forme G, montre que la dimension de $A'_1 + A_{2j-1}$ est

$$n + (n_0 + \dots + n_{2j-2}) - (m_2 + \dots + m_{2j}).$$

Appliqué ensuite à la forme F, le lemme II donne pour dimension de $A_2 \cap A_{2j-2}$

$$(m_2 + \dots + m_{2j}) - (n_0 + \dots + n_{2j-3}).$$

En continuant à appliquer alternativement le lemme II à la forme G et à la forme F, on voit finalement que la dimension de $A_j \cap A'_j$ est

$$(m_j + m_{j+1} + \dots + m_{2j}) - (n_0 + n_1 + \dots + n_{j-1}).$$

Or, le lemme III montre que la différence entre la dimension de A_j et celle de $A_j \cap A'_j$ est *paire*; comme la dimension de A_j est $2h + (n_0 + \dots + n_{j-1}) - (m_1 + m_2 + \dots + m_{j-1})$, on en conclut aussitôt que la somme $m_1 + m_2 + \dots + m_{2j-1} + m_{2j}$ est *paire* pour tout indice j , ce qui entraîne que chacune des sommes $m_{2j-1} + m_{2j}$ est *paire*.

On démontre de la même manière que *les nombres p'_j d'indice pair sont pairs* (Kronecker). En effet, pour avoir ces nombres, il suffit d'appliquer la méthode du n° 3 en permutant les rôles de f et de g ; on a alors pour déterminer les sous-espaces A_i tels que $A_0 = E$ et $A_{i+1} = g^{-1}(f(A_i))$, la suite de relations

$$(2) \quad A_0 = E \perp A'_0 = F_0 \vee A_1 \perp A'_1 \vee A_2 \perp A'_2 \vee \dots \vee A_{s-1} \perp A'_{s-1} \vee A_s$$

Désignons cette fois par m_i la dimension de $A_i \cap F_0$, par n_i celle de $A'_i \cap G_0$; on voit que la dimension de A_i est égale à $k + (n_0 + \dots + n_{i-1}) - (m_1 + \dots + m_{i-1})$, celle de A'_i à $n - k - (n_0 + \dots + n_{i-1}) + (m_1 + \dots + m_i)$; on aura cette fois encore $p'_i = m_i - m_{i+1}$. Cela étant, par application alternée du lemme II aux formes F et G, à partir du sous-espace $A'_0 \cap A_{2j+1}$,

de dimension m_{2j+1} ; on voit que la dimension de $A'_j \cap A_{j+1}$ est

$$(m_{j+1} + \dots + m_{2j+1}) - (n_0 + \dots + n_{j-1}).$$

Or, d'après le lemme III, la différence des dimensions de A'_j et de $A'_j \cap A_{j+1}$ est paire; on en conclut que la somme

$$n - k + m_1 + m_2 + \dots + m_{2j+1}$$

est *paire* pour tout j , ce qui entraîne que $p'_0 = n - k - m_1$ et tous les p'_i d'indice pair sont pairs.

Remarquons enfin (Kronecker) que l'on a $q_i = q'_i$ pour tout indice i en raison du fait de la transposée de f est égale à f , et la transposée de g égale à $-g$.

7. Pour terminer, remarquons que les résultats du n° 6 sont encore valables sans modification lorsque $F(x, y) = \langle x, f(y) \rangle$ est une forme bilinéaire *hermitienne* pour un automorphisme involutif $\lambda \rightarrow \bar{\lambda}$ du corps K (c'est-à-dire que $F(y, x) = \overline{F(x, y)}$).

Si enfin on suppose que F et G sont *toutes deux des formes alternées*, le raisonnement du n° 6 prouve cette fois que *tous les nombres p_i et p'_j sont pairs* (car on peut alors appliquer aussi le lemme III à la forme F).

(Manuscrit reçu le 28 février 1946.)