ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

EDMOND MAILLET

Sur les équations de la géométrie de la théorie des substitutions entre n lettres

Annales de la faculté des sciences de Toulouse 2^e série, tome 6, n° 3 (1904), p. 277-349

<http://www.numdam.org/item?id=AFST_1904_2_6_3_277_0>

SUR LES

ÉQUATIONS DE LA GÉOMÉTRIE

ET LA

THÉORIE DES SUBSTITUTIONS ENTRE n LETTRES,

PAR M. EDMOND MAILLET.

INTRODUCTION.

M. Jordan a montré, dans son *Traité des Substitutions* (Livre III, Chap. III), que l'on pouvait former pour un grand nombre d'équations, qui interviennent dans la détermination de points, courbes ou surfaces remarquables en Géométrie, un groupe Γ de substitutions contenant le groupe G de ces équations.

I. D'autre part nous avons fait voir (*Assoc. franç. pour l'avancement des Sciences,* Mémoires du Congrès de Saint-Étienne, 1897, p. 190) que, si une équation à coefficients réels possède $2k$ racines imaginaires exactement, son groupe contient une substitution d'ordre 2 à k cycles permutant deux à deux les racines imaginaires conjuguées; nous avons indiqué (1) plusieurs applications de ce théorème.

Le présent Mémoire a pour objet : 1° des perfectionnements ou des compléments à apporter aux théories de M. Jordan sur les équations de la Géométrie; 2° l'application de notre théorème ci-dessus, principalement à ces équations.

En particulier, nous obtenons les résultats suivants :

II. Soient les congruences

$$x'_\rho + x''_\rho + \ldots + x_\rho^{(r_1)} \equiv 0 \pmod{r}$$

(1) *Association française, loc. cit.; Comptes rendus,* décembre 1898, et *Journal de Mathématiques,* 1899, p. 205-216.

($\rho = 1, 2, \ldots, q$, r, r_1 donnés, $r_1 > 2$), et r^q lettres caractérisées par les q indices $x_1, x_2, \ldots, x_q \pmod r$. Soit C un système quelconque de r_1 de ces lettres, distinctes ou non, dont les indices forment une solution de ces congruences :

Quand r est une puissance exacte d'un nombre premier, l'ensemble des substitutions entre les r^q lettres qui permutent entre elles toutes ces combinaisons est le groupe Γ *dérivé du groupe* G″ *des substitutions linéaires homogènes*

$$| x_1, \ldots, x_q ; a_1^1 x_1 + \ldots + a_1^q x_q, \ldots, a_q^1 x_1 + \ldots + a_q^q x_q | \qquad (\mathrm{mod}\, r)$$

et du groupe G′ *des substitutions*

$$| x_1, \ldots, x_q ; x_1 + \alpha_1, \ldots, x_q + \alpha_q | \qquad (\mathrm{mod}\, r),$$

où $\alpha_1, \ldots, \alpha_q$ prennent $(\mathrm{mod}\, r)$ *toutes les valeurs possibles multiples de* $\frac{r}{\delta}$, *δ étant le plus grand commun diviseur de r et r_1.*

Ce théorème comprend, comme cas particuliers, plusieurs théorèmes de M. Jordan (1). Il est encore exact quand $r_1 = 3$, $q = 2$, $r = 6$.

III. Notre propriété I pose la question de la détermination de la classe des substitutions d'ordre 2, ou même de la classe d'un groupe quelconque, en vue des applications à la théorie des équations et à la Géométrie. Aux résultats déjà connus nous en ajoutons quelques-uns relatifs à la classe des substitutions des groupes linéaires, abéliens, etc. Ainsi, *le groupe linéaire général de degré $p^{\mu n}$ à n indices* $(\mathrm{mod}\, p^\mu)$ (p premier quelconque) *est de classe $p^{\mu n} - p^{\mu n - 1}$.*

Nous indiquons une méthode générale pour la détermination de la classe des substitutions d'un groupe et de la classe de ce groupe; nous en faisons application au groupe de l'équation aux 27 droites des surfaces du troisième degré, dont les substitutions d'ordre 2 déplacent 24, 20 ou 12 lettres; au groupe de l'équation aux 28 tangentes doubles des quartiques générales; au groupe de l'équation aux 27 points, autres que les points d'inflexion, où une cubique générale a, avec une conique, un contact du cinquième ordre : les substitutions de ce groupe déplacent 27, 26, 24 ou 18 lettres.

IV. Ce qui précède, joint à I, nous donne un certain nombre d'applications géométriques immédiates aux points d'inflexion des cubiques, aux cubiques ayant un contact du troisième ordre en 3 points avec une quartique générale, aux

(1) *Traité des Substitutions,* Livre III, Chap. III.

63 coniques (1) tangentes en 4 points (dont un réel choisi arbitrairement) à une quartique générale réelle, aux 16 plans stationnaires d'une courbe gauche du quatrième ordre, aux plans tangents et aux points singuliers de la surface de Kummer, aux 27 droites des surfaces du troisième degré, aux 28 tangentes doubles d'une quartique, etc.

Nous disons quelques mots des applications de la théorie des groupes de substitutions aux constructions par la règle ou la règle et le compas.

V. Nous sommes conduit incidemment à revenir sur les substitutions opérées par les substitutions d'un groupe G de degré d entre les combinaisons ν à ν de ses lettres :

1° Si $d = \nu' h - 1$ (h entier > 0), et si G est transitif entre les combinaisons ν à ν de ses d lettres $\left(\nu \leqq \frac{d}{2}\right)$, il est transitif entre les combinaisons ν' à ν' de ses d lettres quand $\nu' < \nu$; il en est de même pour d quelconque quand $\nu' = 1$, ou $\nu \leqq 3$.

2° Soient G, de degré d quelconque, transitif entre les combinaisons ν à ν de ses d lettres $\left(2 \leqq \nu \leqq \frac{d}{2}\right)$, p le plus grand nombre premier inférieur à $d - 2$ et $> \frac{d}{2}$: on a forcément $\nu \leqq d - p$. Quand $d \geqq 40$, $\nu < \frac{d}{5}$; quand $d < 40$, $\nu \leqq 8$; quand $11 < d < 9.10^6$, $\nu \leqq 4 (\log d)^2$ (2).

3° Si G, de degré d quelconque, est transitif entre les combinaisons ν à ν de ses lettres $\left(2 \leqq \nu \leqq \frac{d}{2}\right)$, il est primitif.

Il existe des groupes transitifs entre les combinaisons ν à ν ($\nu = 2$ ou 3) de leurs lettres et qui ne sont pas ν fois transitifs.

VI. En terminant, nous indiquons un certain nombre de sujets à traiter, comme suite de notre Mémoire (3).

---

(1) Parmi ces coniques, s'il y en a une d'imaginaire, il y en a 32, 48 ou 56.

(2) Cette formule a été obtenue à l'aide des Tables de nombres premiers. Le logarithme est un logarithme ordinaire.

(3) Sa lecture exige des connaissances assez étendues : *Traité des Substitutions* de M. Jordan (400 premières pages), *Fonctions algébriques* de MM. Appell et Goursat ou *Fonctions abéliennes* de Briot, un Mémoire de Clebsch (*J. de Crelle*, t. 63, p. 189) ou les *Leçons sur la Géométrie* de Clebsch et Lindemann, traduction Benoist (passim), *Algèbre supérieure* de Serret (passim); enfin un coup d'œil au moins sur les Mémoires de M. Jordan ou de nous, que nous citons.

Un résumé de ce Mémoire a été communiqué à l'Académie des Sciences de Paris (*Comptes rendus*, 11 avril 1904, p. 891 et 1012).

I.

Nous avons obtenu antérieurement le théorème suivant (¹) :

THÉORÈME I. — *Si une équation irréductible de degré n à coefficients réels a exactement* 2ν *racines imaginaires* $x_1, \ldots, x_{2\nu}$ (x_{2k-1}, x_{2k} *conjuguées*), *son groupe contient la substitution* $(x_1 x_2)\ldots(x_{2\nu-1} x_{2\nu})$.

En effet, soit $f(x) = 0$ une équation algébrique à coefficients rationnels réels, ces coefficients pouvant dépendre rationnellement d'un certain nombre de paramètres k_1, k_2, ... arbitraires. D'après un théorème connu (²), il existe entre les racines de l'équation un groupe G de substitutions tel que toute fonction F rationnelle des racines et des paramètres dont les substitutions de ce groupe n'altèrent pas la valeur numérique (³) soit rationnellement exprimable en fonction des paramètres; et, réciproquement, que toute fonction rationnelle des racines et des paramètres, rationnellement exprimable en fonction des paramètres, ait sa valeur numérique inaltérée par les substitutions de G. Or on sait qu'on peut toujours former une fonction rationnelle des racines de l'équation proposée, dont la valeur numérique soit invariable par les substitutions d'un groupe quelconque Γ entre les racines, et variable par toute substitution n'appartenant pas à Γ. On dit que cette fonction *appartient au groupe* Γ. Une fonction appartenant à G est rationnellement exprimable.

Ceci posé, n'attribuons à $k_1, k_2, \ldots$ que des valeurs réelles; soit $\varphi(x_1, x_2, \ldots, x_n)$ une fonction rationnelle des racines et des paramètres rationnellement exprimable et appartenant à G : la valeur numérique de φ est réelle et reste invariable quand on change $i = \sqrt{-1}$ en $-i$ dans celle des racines $x_1, x_2 \ldots, x_n$ qui sont imaginaires. Soient $x_1, x_2, \ldots, x_{2\nu-1}, x_{2\nu}$ ($\nu < 0$) les 2ν racines imaginaires de $f(x) = 0$ que l'on suppose ne pas avoir toutes ses racines réelles, x_{2k-1} et x_{2k} étant conjuguées. Le changement de i en $-i$ dans $\varphi(x_1, x_2, \ldots, x_n)$ revient à y opérer la substitution

$$S = (x_1 x_2)\ldots(x_{2k-1} x_{2k})\ldots(x_{2\nu-1} x_{2\nu}),$$

(¹) *Association française pour l'avancement des Sciences,* Mémoires du Congrès de Saint-Étienne, 1897, p. 195. Pour la clarté, nous reproduisons ici la démonstration, sous une forme toutefois un peu plus générale. Dans cette première démonstration, il faut supprimer l'avant-dernière ligne de la page 195 : « et le groupe de etc. ».

(²) JORDAN, *Traité des Substitutions,* p. 257 et 277.

(³) La valeur numérique de F est la fonction de $k_1, k_2, \ldots$ à coefficients numériques, que l'on obtient quand on substitue aux racines leurs expressions en fonction de $k_1, k_2, \ldots$.

en sorte que S laisse la valeur numérique de φ invariable, et appartient à G.

C. Q. F. D.

Nous avons fait connaître (1) une série d'applications de ce théorème à la théorie des équations algébriques. Nous nous proposons, dans ce qui suit, d'en indiquer de nouvelles, en nous occupant principalement d'équations que l'on rencontre en Géométrie (2).

II.

Rappelons d'abord quel est le principe des applications faites par M. Jordan de la théorie des substitutions à un certain nombre d'équations de la Géométrie.

Supposons que des points, lignes, surfaces, etc. en nombre fini d soient déterminés par une équation $X = 0$ de degré d et de racines inégales, à laquelle satisferont, par exemple, les coordonnées x des points, ou un des paramètres des lignes ou surfaces, les autres coordonnées ou paramètres s'exprimant rationnellement en fonction des racines. L'équation $X = 0$ pourra d'ailleurs contenir un certain nombre d'arbitraires $k_1, k_2, \ldots$ que nous adjoindrons au domaine de rationalité en les supposant réelles.

Admettons que les solutions (points, lignes ou surfaces) soient liées entre elles par certaines relations géométriques, c'est-à-dire, par exemple, que la connaissance de k d'entre elles entraîne, grâce à une propriété géométrique connue, la connaissance d'une $(k+1)^{\text{ième}}$ au moins. Exemple : si l'on se donne deux points d'inflexion d'une cubique plane, on sait que la droite qui les joint coupe la cubique en un troisième point, qui est d'inflexion. Cette propriété se traduit entre les coordonnées x ou les diverses valeurs d'un paramètre par une ou plusieurs relations $R = 0$, que nous supposons toujours rationnelles, par suite, si l'on veut, entières. Les fonctions R des racines de $X = 0$ et des arbitraires réelles $k_1, k_2, \ldots$ ont une valeur numérique rationnelle, puisque cette valeur est o. Le groupe G de l'équation $X = 0$ doit donc laisser numériquement invariable la valeur de R : autrement dit, le groupe de $X = 0$ est contenu dans le faisceau ou ensemble Γ commun aux fonctions R, c'est-à-dire l'ensemble des substitutions laissant invariables simultanément les valeurs numériques de ces fonctions.

La considération de toutes les relations $R = 0$ connues dans le problème pourra nous donner ainsi un faisceau $\Gamma > G$ et contenant G. Si tous les coefficients de

---

(1) *Association française, loc. cit.*

(2) JORDAN, *Traité des Substitutions,* Chap. III, p. 301. Il y a quelques années M. Jordan, à qui nous avions communiqué le théorème I, nous avait engagé à en chercher des applications géométriques.

$X = 0$, ainsi que k_1, k_2, ... sont réels, il suffira que Γ (1) ne contienne pas le groupe alterné de degré d pour que notre théorème I puisse donner une propriété géométrique intéressante ou remarquable des points, lignes ou surfaces au point de vue de la réalité : si ces points ne sont pas tous réels, il y en aura au moins n imaginaires, n étant la classe de Γ (c'est-à-dire le nombre minimum de lettres que déplace une substitution de Γ).

Supposons que l'équation $X = 0$ (rencontrée en Géométrie ou ailleurs) ait

---

(1) Ou même le faisceau Γ_1 d'une des équations $R = 0$, qui contient Γ, par suite G.

Ce faisceau Γ_1 n'est pas forcément un groupe : ainsi, soient trois points d'inflexion en ligne droite x_1, x_2, x_3 d'une cubique générale $R = \psi(x_1, x_2, x_3) = 0$, la relation exprimant que ces points sont en ligne droite; R est invariable par les substitutions du groupe linéaire (mod 3) à deux indices, et par les substitutions du groupe symétrique entre x_4, ..., x_9. Le groupe dérivé est le groupe symétrique de 9 éléments entre x_1, ..., x_9, qui ne laisse pas invariable la valeur numérique de $R = 0$, car la substitution $(x_3 x_4)$ donne $R \neq 0$.

Ceci pose ainsi ce problème général très intéressant :

Quelles conditions doivent remplir plusieurs fonctions $R = 0$ *pour que le faisceau commun* Γ *forme un groupe* (comp. NETTO-BATTAGLINI, *Teoria delle Sostituzioni*, 1885, p. 220, ou NETTO, *Substitutionentheorie, Tripelnsysteme*).

Nous nous contenterons de quelques indications à ce sujet.

Soient k relations $R = 0$, $R' = 0$, ..., formant un système E, entre les racines d'une équation $X = 0$, à racines distinctes, de groupe G, F le faisceau des substitutions entre ces racines laissant numériquement invariable chaque fonction de E : F contient G.

Soit S une substitution de F : en l'opérant sur E, on obtient un nouveau système de relations qu'on peut représenter par ES; le faisceau Φ correspondant à ES n'est autre que le faisceau $S^{-1}F$ formé du produit de S^{-1} par les substitutions de F; car $S^{-1}F$ appartient à Φ, et, si Σ est une substitution de Φ, $S\Sigma$ laisse chaque fonction de E numériquement invariable et appartient à F, par suite Σ à $S^{-1}F$; $S^{-1}F$ contient G.

Soient 1, S, S', ... les substitutions de F : l'ensemble des systèmes E, ES, ES', ... forme un nouveau système E_1, dont chaque fonction est numériquement invariable par les substitutions d'un faisceau F_1; ce faisceau est évidemment formé des substitutions communes à F, $S^{-1}F$, $S'^{-1}F$, ...; F_1 contient G.

On opérera sur E_1 et F_1 comme on l'a fait sur E et F, et ainsi de suite. Le nombre des fonctions algébriquement distinctes de E, E_1, ..., E_j ne pouvant augmenter indéfiniment avec j, on finira par obtenir un système E_j et un faisceau F_j de substitutions 1, S_j, S'_j, ... tel que $E_j S_j = E_j$, $E_j S'_j = E_j$, ..., $S_j^{-1} F_j = F_j$, $S_j'^{-1} F_j = F_j$, ...; F_j est alors évidemment un groupe dont les substitutions permutent entre elles les valeurs algébriques des fonctions de E_j; F_j contient G. E_j sera alors ce qu'on peut appeler un *système complet*, c'est-à-dire *un système de fonctions tel que les substitutions du faisceau laissant numériquement invariable chaque fonction du système permutent exclusivement entre elles les valeurs algébriques de ces fonctions.*

Un système complet qui ne contient aucun système complet plus petit sera dit *irréductible.*

Tout système de relations conduit, par le procédé ci-dessus, à un système complet *dérivé* et à un groupe corrélatif.

exactement 2ν racines imaginaires, $x_1, x_2, \ldots, x_{2\nu}$ (x_{2k-1} et x_{2k} étant conjuguées); G contient (théorème I)

$$S = (x_1 x_2) \ldots (x_{2k-1} x_{2k}) \ldots (x_{2\nu-1} x_{2\nu}).$$

Pour savoir combien $X = 0$ peut avoir de racines imaginaires, il suffira de connaître la classe [c'est-à-dire le nombre de lettres déplacées (1)] des substitutions d'ordre 2 de G.

Soient $2\lambda_1, 2\lambda_2, \ldots, 2\lambda_\alpha$ ces diverses classes; il n'en résultera pas forcément que $X = 0$ peut avoir, suivant la valeur des coefficients, supposés réels, $2\lambda_i$ racines imaginaires ($i = 1, 2, \ldots, \alpha$); mais il en résultera forcément que, si $X = 0$ a $2j$ racines imaginaires, *j est un des nombres* $0, \lambda_1, \ldots, \lambda_\alpha$. Autrement dit, parmi les points, courbes, etc., en question, il y en aura d, $d - 2\lambda_1, \ldots,$ ou $d - 2\lambda_\alpha$ réels, quelques-uns de ces $\alpha + 1$ cas pouvant d'ailleurs ne pas se présenter.

A défaut de la connaissance du groupe G, on pourra résoudre le même problème pour un faisceau ou un groupe Γ contenant G.

Enfin, la détermination de la classe de G ou Γ donnera une limite inférieure des λ_i.

Les applications algébriques et géométriques du théorème I nous conduisent ainsi à ces deux vastes problèmes dont le second a déjà fait l'objet de travaux de M. Jordan et des nôtres :

1° *Déterminer les classes des substitutions d'ordre* 2 *d'un groupe* G;

2° *A défaut, pour avoir une limite inférieure de ces classes, trouver la classe de* G *ou une limite inférieure de cette classe.*

III.

REMARQUES GÉNÉRALES SUR LES GROUPES G.

On peut établir, dans des cas étendus, que le groupe G ou le faisceau Γ n'est ni symétrique ni alterné.

En effet :

1° Supposons que l'une des relations $R = 0$ exprime que trois points x_1, x_2, x_3 sont en ligne droite, sans que les d points y soient : on aura une certaine relation $f(x_1, x_2, x_3) = 0$. Une substitution S du groupe G ou de Γ, opérée sur cette équation, donne la nouvelle relation $f(x'_1, x'_2, x'_3) = 0$ exprimant que les trois points x'_1, x'_2, x'_3 sont en ligne droite. Le groupe G ou Γ ne pourra contenir toutes les substitutions circulaires d'ordre 2 ou 3, car il contiendrait $(x_3 x_i)$ ou

(1) NETTO, *J. für Math.*, t. LXXXIII.

$(x_3 x_i x_j)$ $(i \neq 1, 2, 3)$ permettant de faire succéder à x_3 une autre quelconque des racines, et tous les points $x_1, \ldots, x_d$ seraient sur une même ligne droite. Même, le sous-groupe de G ou le sous-faisceau de Γ, qui laisse x_1 et x_2 immobiles, ne peut être transitif sans que les d points soient en ligne droite.

Si trois des points déterminés par $X = 0$ *sont en ligne droite, ces d points n'étant pas tous en ligne droite, le groupe de* $X = 0$ *n'est pas plus de deux fois transitif.*

Ou encore :

Si l'on peut trouver sur une courbe algébrique $C = 0$ *d points dont les abscisses sont distinctes et sont les racines d'une équation algébrique* $X = 0$ *de degré d à coefficients rationnels par rapport aux coefficients de* C *supposés réels et si trois de ces points sont en ligne droite, sans que les d points y soient, le groupe de* $X = 0$ *n'est pas plus de deux fois transitif.*

Si le groupe de $X = 0$ est deux fois transitif, la droite menée par deux quelconques des points en question passe par un troisième.

2° Supposons que λ des points déterminés par $X = 0$ doivent être sur une même courbe de degré μ, avec (1) $\mu_1 = \frac{\mu(\mu+3)}{2} < \lambda$; $x_1, x_2, \ldots, x_\lambda$, par exemple, sont liés par une relation $f(x_1, x_2, \ldots, x_\lambda) = 0$; G n'est pas plus de μ_1 fois transitif à moins que les d points soient sur cette courbe.

Si λ *des d points sont sur une même courbe de degré* $\mu\left(\lambda > \frac{\mu(\mu+3)}{2} = \mu_1\right)$, *sans que* (2) *les d points y soient, le groupe de* $X = 0$ *n'est pas plus de* μ_1 *fois transitif; même le sous-groupe des substitutions de* $X = 0$ *qui laissent* μ_1 *de ces points immobiles ne peut être transitif entre les autres* (3).

Ainsi, quand $\mu = 2$, $\mu_1 = 5$: si six des points sont sur une conique, sans que les d y soient tous, le groupe de $X = 0$ n'est pas plus de cinq fois transitif.

---

(1) Une courbe algébrique de degré μ est déterminée par $\frac{\mu(\mu+3)}{2}$ conditions. Il n'y aura ici de relation entre les $x_1, \ldots, x_d$ que si $\frac{\mu(\mu+3)}{2} < \lambda$.

(2) Cette restriction est essentielle, car le problème de l'intersection de deux courbes de degrés m et n conduit, en général, à une équation de degré mn. Pour $n = 1$, cette équation peut donner une équation $X = 0$ de degré m dont le groupe est symétrique; exemple : intersection d'une courbe générale de degré m avec $x = 0$. L'équation est

$$A_0 y^m + A_1 y^{m-1} + \ldots + A_m = 0,$$

équation générale de degré m.

(3) C'est-à-dire entre les abscisses des autres.

Voici des applications à des cas connus :

La droite qui passe par deux points d'inflexion arbitrairement choisis d'une cubique passe par un troisième; le groupe (1) de l'équation $X = 0$ aux abscisses de ces points d'inflexion n'est pas plus de deux fois transitif.

Soit une quartique générale C_4 : on sait (2) qu'il y a 63 systèmes distincts de coniques tangentes en quatre points à la quartique (en laissant de côté les droites du plan). Un point de contact M_1 pour ces coniques étant choisi arbitrairement (l'abscisse de ce point jouera dans $X = 0$ le rôle d'un paramètre k_1), les trois autres points de contact d'une conique forment 63 systèmes distincts; un des paramètres de la conique dépend d'une équation de degré 63.

Or, pour trois valeurs de k_1, ces coniques forment trois ensembles de 63 systèmes; en prenant une conique au hasard dans les deux premiers ensembles, et une convenablement choisie dans le troisième, on obtient douze points de contact qui sont sur une cubique.

On peut aussi considérer trois valeurs de k_1 identiques : les trois ensembles de 63 systèmes se réduisent à un seul et la cubique a trois points confondus en M_1 avec la quartique. Ainsi, soient les 63 coniques distinctes qui touchent la quartique en quatre points, dont un M_1 choisi arbitrairement; on peut prendre au hasard deux de ces coniques, faire passer par leurs points de contact et par M_1 une cubique ayant un contact du deuxième ordre en M_1 avec la quartique; cette cubique coupe la quartique en trois autres points qui sont les points de contact autres que M_1 d'une autre des 63 coniques.

Soit alors $X = 0$ l'équation qui détermine ces 63 coniques (l'inconnue étant, par exemple, un des paramètres) : la propriété ci-dessus se traduira entre trois racines a_1, a_2, a_3 de $X = 0$, par une condition $\psi(a_1, a_2, a_3) = 0$, où a_1 et a_2 sont arbitraires. Donc *le groupe de* $X = 0$ *est au plus deux fois transitif.*

IV.

LE GROUPE LINÉAIRE DANS LES ÉQUATIONS DE LA GÉOMÉTRIE.

Dans un grand nombre de théorèmes relatifs à l'application des fonctions elliptiques ou abéliennes à la Géométrie, en particulier dans plusieurs de ceux indiqués par Clebsch (3), l'équation algébrique $X = 0$ dont dépend le problème est

(1) JORDAN, *Traité des subst.*, p. 302.

(2) *Voir* HESSE, *Journ. de Crelle*, t. 49; CLEBSCH, *id.*, t. 63, p. 210; APPELL et GOURSAT, *Théorie des fonctions algébriques et de leurs intégrales*, 1895, p. 497.

(3) *Journ. de Crelle*, t. 63; *voir aussi* JORDAN, *Traité des subst.*, p. 302 et suiv.

déterminée par des relations (1)

$$u_1^{(j)}+\ldots+u_\delta^{(j)}=\frac{P+2\lambda_j\pi i+l_1\tau_1^{(j)}+\ldots+l_p\tau_p^{(j)}}{r} \qquad (j=1,2,\ldots,p \text{ et } \delta\geq p).$$

Le problème de l'inversion de Jacobi détermine p des points, courbes, etc. en fonction des $\delta-p$ autres choisis arbitrairement, par une équation de degré r^{2p}, irréductible ou non. On en conclut, si l'on représente par (2) $(x_1,\ldots,x_{2p})\pmod r$ les racines, que le groupe G de $X=0$ laisse invariable l'ensemble des solutions des congruences

$$x'_\rho+x''_\rho+\ldots+x_\rho^{(r_1)}\equiv 0 \pmod r \qquad (\rho=1,2,\ldots,2p),$$

où les $x_\rho^{(j)}$ peuvent être tous identiques aux $x_\rho^{(j')}$ $(j\neq j')$ quel que soit ρ.

Pour plus de généralité, nous supposerons $\rho=1,2,\ldots,q$, où q est pair ou impair, et nous déterminerons le groupe Γ des substitutions laissant invariable l'ensemble des solutions du système de congruences

$$x'_\rho+\ldots+x_\rho^{(r_1)}\equiv 0 \pmod r \qquad (\rho=1,2,\ldots,q); \tag{1}$$

quand $q=2p$, Γ contient G.

Soit $(x'_1,\ldots,x'_q),\ldots,(x_1^{(r_1)},\ldots,x_q^{(r_1)})$ une solution : si nous ajoutons simultanément à $x'_1,\ldots,x_1^{(r_1)}$ un même nombre α_1, à $x'_2,\ldots,x_2^{(r_1)}$ un même nombre α_2, etc., soit

$$x_\rho^{(j)}+\alpha_\rho=y_\rho^{(j)};$$

on a encore

$$y'_\rho+\ldots+y_\rho^{(r_1)}\equiv 0 \pmod r$$

dès que $r_1\alpha_\rho\equiv 0\pmod r$, en particulier, quel que soit α_ρ, si $r_1\equiv 0\pmod r$.

Γ contient alors toutes les substitutions

$$|\,x_1,\ \ldots,\ x_q;\ x_1+\alpha_1,\ \ldots,\ x_q+\alpha_q\,| \pmod r,$$

telles que $\alpha_1,\ldots,\alpha_q$ soient des multiples de $\frac{r}{\delta}$, δ étant le plus grand commun diviseur de r et de r_1. Ces substitutions forment un groupe G', d'ordre δ^q.

Considérons, de même, la substitution linéaire homogène

$$\begin{vmatrix} x_1 & a_1^1x_1+a_1^2x_2+\ldots+a_1^qx_q \\ \ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\ x_q & a_q^1x_1+a_q^2x_2+\ldots+a_q^qx_q \end{vmatrix} \pmod r, \tag{2}$$

(1) Pour les notations, *voir* le Mémoire de Clebsch ou la *Théorie des fonctions algébriques* de MM. Appell et Goursat, p. 497, par exemple.

(2) $x_1=\lambda_1,\ \ldots,\ x_p=\lambda_p,\ x_{p+1}=l_1,\ \ldots,\ x_{2p}=l_p$.

et opérons-la dans le premier membre de la congruence (1), on obtient

$$(a_\rho^1 x_1' + a_\rho^2 x_2' + \ldots + a_\rho^q x_q') + \ldots + (a_\rho^1 x_1^{(r_1)} + \ldots + a_\rho^q x_q^{(r_1)}),$$

ou

$$a_\rho^1 (x_1' + \ldots + x_1^{(r_1)}) + a_\rho^2 (x_2' + \ldots + x_2^{(r_1)}) + \ldots + a_\rho^q (x_q' + \ldots + x_q^{(r_1)}),$$

qui, d'après (1), est $\equiv 0 \pmod r$ quel que soit ρ. Le groupe Γ contient donc toutes les substitutions du groupe linéaire $(\mathrm{mod}\, r)$ à q indices non homogène quand $r_1 \equiv 0 \pmod r$, et, quand $r_1 \not\equiv 0 \pmod r$, toutes les substitutions du groupe linéaire homogène G'', qui ne déplacent pas la racine dont tous les indices sont zéro.

Désignons par $\beta_1, \beta_2, \ldots, \beta_q$ les lettres $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, 1)$ (pour β_i, $x_i \equiv 1$, $x_j \equiv 0$ quand $j \not\equiv i$), *et supposons* $r = p_1^\mu$ (p_1 premier), $r_1 > 2$.

Les transformations (2) qui laissent $\beta_1, \beta_2, \ldots, \beta_i$ immobiles sont de la forme

$$(3) \qquad \left| \begin{array}{ll} x_1 & x_1 + a_1^{i+1} x_{i+1} + \ldots + a_1^q x_q \\ \ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\ x_i & x_i + a_i^{i+1} x_{i+1} + \ldots + a_i^q x_q \\ x_{i+1} & a_{i+1}^{i+1} x_{i+1} + \ldots + a_{i+1}^q x_q \\ \ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\ x_q & a_q^{i+1} x_{i+1} + \ldots + a_q^q x_q \end{array} \right| \pmod r.$$

On le voit en remarquant que cette forme est vraie pour $i = 0$, et que, si on la regarde comme exacte sans spécifier la valeur de i, les substitutions qui laissent $\beta_1, \ldots, \beta_{i+1}$ immobiles sont comprises parmi les substitutions (3), et, pour elles évidemment,

$$a_1^{i+1} \equiv \ldots \equiv a_i^{i+1} \equiv a_{i+2}^{i+1} \equiv \ldots \equiv a_q^{i+1} \equiv 0, \qquad a_{i+1}^{i+1} \equiv 1 \qquad (\mathrm{mod}\, r).$$

Soit S une substitution de Γ qui laisse immobile $(0, 0, \ldots, 0) = \beta_0$. Le groupe des substitutions (2) contient la substitution

$$(4) \qquad \left| \begin{array}{ll} x_1 & \alpha_1 x_1 + \ldots + \alpha_q x_q \\ \ldots & \ldots\ldots\ldots\ldots\ldots \\ x_q & \ldots\ldots\ldots\ldots\ldots \end{array} \right| \pmod r,$$

où $\alpha_1, \ldots, \alpha_q$ sont arbitraires, pourvu que l'un d'eux soit premier à r; car si, par exemple, α_i est premier à r, il suffit de considérer la substitution qui laisse invariable $x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_q$, et qui remplace x_i par x_1. C'est une substitution, car le déterminant est égal à $\pm \alpha_i$ premier à r.

Je dis, d'autre part, que S doit substituer à l'une des lettres $\beta_1 = (1, 0, \ldots, 0)$, $\beta_2, \ldots$ ou β_q une lettre A dont un indice est premier à r (c'est-à-dire à p_1).

En effet, ceci est évident si r est premier, puisque β_0 est la seule racine dont tous les indices sont $\equiv 0 \pmod r$. Supposons r non premier.

Considérons les congruences (1) : ces congruences admettent, en particulier, des solutions telles que

$$x'_1 + x''_1 \equiv 0, \quad \ldots, \quad x'_q + x''_q \equiv 0 \pmod r, \tag{5}$$

tous les $x_\rho^{(i)} (i > 2)$ étant nuls $(\mathrm{mod}\, r)$. S laissant β_0 invariable permutera entre elles les solutions de ces congruences (5); supposons que S substitue à β_1 une lettre dont les indices sont tous non premiers à r : $(1, 0, \ldots, 0)$ et $(r-1, 0, \ldots, 0)$ étant solutions simultanées de (5) (ici $r \geq 4$), $(r-1, 0, \ldots, 0) = (-1, 0, \ldots, 0)$ est aussi remplacée par une lettre jouissant de la même propriété : si S remplace $(1, 0, \ldots, 0)$ par $(\xi_1, \ldots, \xi_q)$, elle remplace $(-1, 0, \ldots, 0)$ par $(-\xi_1, \ldots, -\xi_q)$.

Nous supposons $r_1 \geq 3$. Les congruences (1) admettent encore des solutions telles que

$$x'_\rho + x''_\rho + x'''_\rho \equiv 0 \pmod r \quad \text{avec} \quad x_\rho^{(i)} \equiv 0 \quad (i > 3), \tag{6}$$

ces congruences sont satisfaites pour

$$x'_1 \equiv x''_1 \equiv 1, \quad x'''_1 \equiv -2, \quad x'_\rho \equiv x''_\rho \equiv x'''_\rho \equiv 0 \pmod r \quad (\rho > 1).$$

Donc $(-2, 0, \ldots, 0)$ est remplacé par une lettre ayant tous ses facteurs non premiers à r; par suite aussi $(2, 0, \ldots, 0)$, d'après (5). Si l'on prend

$$x'_1 \equiv 1, \quad x'_2 \equiv 2, \quad x'_3 \equiv -3, \quad x'_\rho \equiv x''_\rho \equiv x'''_\rho \equiv 0 \pmod r,$$

on voit qu'il en est de même de $(-3, 0, \ldots, 0)$ et $(3, 0, \ldots, 0)$, etc. Donc, ceci a lieu pour $(x_1, 0, \ldots, 0)$ quel que soit x_1. De plus, d'après le même raisonnement, les lettres $(x_1, 0, \ldots, 0)$ sont remplacées par des lettres dont le $j^{\text{ième}}$ indice a avec r un plus grand commun diviseur, qui est une puissance de p_1.

Si la même chose n'avait pas lieu pour $(0, 1, 0, \ldots, 0)$, c'est-à-dire si $(0, 1, 0, \ldots, 0) = \beta_2$ était remplacée dans S par une lettre d'indices non tous divisibles par p_1, S substituerait à β_2 une lettre dont un indice est premier à r : la permutation des indices x_2 et x_1 nous permettrait de raisonner comme dans le cas où S substitue A (p. 289) à β_1, etc. Finalement, les indices étant convenablement choisis, si S ne substitue pas à β_1 une lettre A, on peut admettre que

$$(x_1, 0, \ldots, 0), \quad (0, x_2, 0, \ldots, 0), \quad \ldots, \quad (0, \ldots, 0, x_q)$$

sont remplacées par des lettres à indices tous non premiers à r.

Considérons alors les congruences

$$\left.\begin{aligned} -x_1 + 0 \quad + x_1''' &\equiv 0 \\ 0 \quad - x_2 + x_2''' &\equiv 0 \end{aligned}\right\} \pmod r.$$

Ceci nous montre que, d'après (6), les lettres $(x_1''', x_2''', 0, \ldots, 0)$ ou $(x_1, x_2, 0, \ldots, 0)$ sont remplacées par des lettres d'indices tous non premiers à r, puisque $r = p_1^{\mu}$. Alors, d'après (6), et

$$\left.\begin{aligned} -x_1 + 0 \quad + x_1''' &\equiv 0 \\ -x_2 + 0 \quad + x_2''' &\equiv 0 \\ 0 \quad - x_3 + x_3''' &\equiv 0 \end{aligned}\right\} \pmod r,$$

les lettres $(x_1, x_2, x_3, 0, \ldots, 0)$ jouissent de la même propriété, etc. Finalement, toutes les lettres jouiraient de cette propriété et S ne serait pas une substitution, contrairement à l'hypothèse.

On pourra donc, en faisant, au besoin, une permutation d'indices, supposer que la lettre substituée à β_1 par S ait un indice premier à r.

Prenons maintenant la substitution déduite de (4) en changeant a_j^i en a_i^j : (4) devient

$$\mathrm{T} = \begin{vmatrix} x_1 & \alpha_1 x_1 + \ldots \\ \ldots & \ldots\ldots\ldots \\ x_q & \alpha_q x_q + \ldots \end{vmatrix} \pmod r$$

et substitue à $(1, 0, \ldots, 0)$ une lettre que l'on peut prendre identique à A, moyennant un choix convenable des $\alpha_1, \ldots, \alpha_q$: ST^{-1} laisse $(1, 0, \ldots, 0)$ immobile, et appartient à Γ. D'après les congruences (5), $\mathrm{S}_1 = \mathrm{ST}^{-1}$ laisse $(-1, 0, \ldots, 0)$ immobile. D'après les congruences (6), S_1 laisse $(2, 0, \ldots, 0)$, $(x_1' \equiv x_1'' \equiv -1,\ x_1''' \equiv 2$, les autres indices nuls), puis $(-2, 0, \ldots, 0)$ d'après (5), puis, d'après (6), $(3, 0, \ldots, 0)$, $(x_1' \equiv -1, x_1' \equiv -2, x_1''' \equiv 3)$, etc., immobiles. Finalement, S_1 laisse $(x_1, 0, \ldots, 0)$ immobile, comme les substitutions Σ_{01} de la forme (2) qui laissent β_0 et β_1 immobiles [formule (3) pour $i = 1$].

Considérons maintenant $\beta_2 = (0, 1, 0, \ldots, 0)$: S_1 remplacera β_2 par une lettre A_2 ; si l'un des indices $\xi_2, \ldots, \xi_q$ de A_2 est premier à r, il y a une substitution Σ_{01} de la forme

$$\mathrm{T}_1 = \begin{vmatrix} x_1 & x_1 + \alpha_1 x_2 + \ldots \\ x_2 & \alpha_2 x_2 + \ldots \\ \ldots & \ldots\ldots\ldots \\ x_q & \alpha_q x_q + \ldots \end{vmatrix} \pmod r,$$

où α_i $(i \geq 2)$, par exemple, est premier à r, les $q - 1$ autres α étant arbitraires;

car, prenant

$$a_3^3 \equiv a_4^4 \equiv \ldots \equiv a_q^q \equiv a_2^i \equiv 1 \qquad \text{sauf} \qquad a_i^i \equiv 0 \pmod r,$$

les autres coefficients non écrits étant nuls, le déterminant de la substitution est $\pm \alpha_i$ premier à r. Cette substitution remplace $(0, 1, 0, \ldots, 0)$ par $(\alpha_1, \alpha_2, \ldots, \alpha_q)$, que l'on peut prendre $= A_2$, et $S_1 T_1^{-1}$ laisse $(0, 1, 0, \ldots, 0)$ immobile.

Admettons pour un moment que $\xi_2, \ldots, \xi_q$ sont tous non premiers à r. S_1 remplacera β_2 par une lettre où $x_2, \ldots, x_q$ sont non premiers à r; de même, d'après (5), pour $(0, -1, 0, \ldots, 0)$. D'après (6) $(1 + 1 - 2 \equiv 0, \; -1 - 1 + 2 \equiv 0)$, il en sera de même pour $(0, -2, 0, \ldots, 0)$, $(0, 2, 0, \ldots, 0)$, etc.; finalement pour $(0, x_2, 0, \ldots, 0)$, quel que soit x_2.

On peut alors admettre encore que cela a lieu pour $(0, 0, \ldots, 0, x_i, 0, \ldots, 0)$ $(i > 2)$, sans quoi, en permutant x_i et x_2, on pourrait raisonner sur S_1 et une certaine substitution linéaire T_1' comme nous l'avons fait ou le ferons tout à l'heure sur S_1 et T_1.

D'après (6), et

$$\left.\begin{aligned} -x_2 + 0 \; + x_2''' &\equiv 0 \\ 0 \; - x_3 + x_3''' &\equiv 0 \end{aligned}\right\} \pmod r,$$

on voit que $(0, x_2, x_3, 0, \ldots, 0)$ jouit de la même propriété; finalement aussi $(0, x_2, x_3, \ldots, x_q)$, $(x_2, x_3, \ldots, x_q$ non tous nuls).

D'après (6), et

$$\left.\begin{aligned} -x_1 + 0 \; + x_1 &\equiv 0 \\ 0 \; - x_2 + x_2 &\equiv 0 \\ \cdots\cdots\cdots\cdots & \\ 0 \; - x_q + x_q &\equiv 0 \end{aligned}\right\} \pmod r,$$

il en est de même de $(x_1, x_2, \ldots, x_q)$ quand $x_2, \ldots, x_q$ ne sont pas tous nuls : S_1 ne serait pas une substitution, ni S non plus, contrairement à l'hypothèse.

Dès lors, $S_2 = S_1 T_1^{-1}$ appartient à Γ et laisse $\gamma_2 = (0, 1, 0, \ldots, 0)$ immobile, par suite, d'après (5) et (6), $(0, 2, 0, \ldots, 0)$, $\ldots$, $(0, x_2, 0, \ldots, 0)$, et, encore d'après (6), $(x_1, x_2, 0, \ldots, 0)$, quels que soient x_1 et x_2.

Nous considérons ensuite $\beta_3 = (0, 0, 1, 0, \ldots, 0)$: S_2 remplace β_3 par une lettre A_3, etc.

Supposons que nous ayons établi que le produit S_i de S par une substitution linéaire convenable (mod r) laisse $(x_1, x_2, \ldots, x_i, 0, \ldots, 0)$ immobile, quels que soient $x_1, x_2, \ldots, x_i$, et considérons $\beta_{i+1} = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$ (où $x_1 \equiv \ldots \equiv x_i \equiv x_{i+2} \equiv \ldots \equiv x_q \equiv 0$, $x_{i+1} \equiv 1$). On formera la substitution

linéaire

$$T_i = \begin{vmatrix} x_1 & x_1 + \alpha_1 x_{i+1} \\ \cdot\cdot & \cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot \\ x_i & x_i + \alpha_i x_{i+1} \\ x_{i+1} & \alpha_{i+1} x_{i+1} + x_j \\ x_{i+2} & \alpha_{i+2} x_{i+1} + x_{i+2} \\ \cdot\cdot\cdot\cdot & \cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot \\ x_j & \alpha_j x_{i+1} \\ \cdot\cdot & \cdot\cdot\cdot\cdot\cdot\cdot \\ x_q & \alpha_q x_{i+1} + x_q \end{vmatrix} \pmod r,$$

où α_j premier à r ($j > i$), qui a pour déterminant $\pm \alpha_j$ premier à r, et substitue à β_{i+1} la lettre $(\alpha_1, \ldots, \alpha_q)$ telle que l'un des indices $\alpha_{i+1}, \ldots, \alpha_q$ est premier à r. Si S_i substitue à β_{i+1} une lettre dont un des $q - i$ derniers indices est premier à r, en choisissant convenablement T_i, $S_{i+1} = S_i T_i^{-1}$ laisse β_{i+1} immobile, ainsi que $(x_1, x_2, \ldots, x_i, 0, \ldots, 0)$. D'après (5), S_{i+1} laisse $(0, \ldots, 0, x_{i+1} = -1, 0, \ldots)$ immobile, et, d'après (6), $(0, \ldots, 0, x_{i+1} = 2, 0, \ldots, 0)$, etc., par suite, $(0, \ldots, 0, x_{i+1}, 0, \ldots, 0)$ quel que soit x_{i+1}. S_{i+1} laisse d'après (6) $(x_1, x_2, \ldots, x_i, x_{i+1}, 0, \ldots, 0)$ immobile, et l'on peut continuer le raisonnement.

Supposons donc que S_i substitue à β_{i+1} une lettre $(\xi_1, \ldots, \xi_q)$ dont les $q - i$ derniers indices sont non premiers à r. D'après (5) il en est de même pour $(0, 0, \ldots, 0, x_{i+1} = -1, 0, \ldots, 0)$; d'après (6) il en est de même pour $(0, \ldots, 0, x_{i+1} = \pm 2, 0, \ldots, 0)$; et ainsi de suite; finalement, il en est de même pour $(0, \ldots, 0, x_{i+1}, 0, \ldots, 0)$ quel que soit x_{i+1}.

On peut alors admettre que cela a lieu pour $(0, \ldots, 0, x_j, 0, \ldots, 0)$, avec j quelconque $> i + 1$; sinon, en effet, en permutant x_j et x_{i+1}, on déduit de S_i une substitution analogue à S_{i+1} sur laquelle on peut raisonner comme tout à l'heure. D'après (6) et

$$\left.\begin{array}{rrr} -x_{i+1} + 0 & + x'''_{i+1} & \equiv 0 \\ 0 & -x_{i+2} + x'''_{i+2} & \equiv 0 \end{array}\right\} \pmod r,$$

on voit que $(0, \ldots, 0, x_{i+1}, x_{i+2}, 0, \ldots, 0)$ jouit de la même propriété, etc. Finalement, il en est de même de $(0, \ldots, 0, x_{i+1}, \ldots, x_q)$. D'après (6) et

$$\left.\begin{array}{rrr} -x_1 + 0 & + x'''_1 & \equiv 0 \\ \cdots\cdots\cdots\cdots & & \\ -x_i + 0 & + x'''_i & \equiv 0 \\ 0 & -x_{i+1} + x'''_{i+1} & \equiv 0 \\ \cdots\cdots\cdots\cdots & & \\ 0 & -x_q + x'''_q & \equiv 0 \end{array}\right\} \pmod r,$$

il en est de même de $(x_1, \ldots, x_q)$ quand $x_{i+1}, \ldots, x_q$ ne sont pas tous nuls, c'est-à-dire pour toutes les lettres que déplace S : S ne serait pas une substitution.

Finalement, en faisant varier i, on voit que, en multipliant S par une substitution linéaire convenable on obtiendra une substitution qui se réduit à 1. Donc S est linéaire homogène.

Il reste à voir toutefois que Γ, qui contient G' et G'' (p. 286-287), est bien dérivé de ces deux groupes.

Cherchons combien de lettres distinctes Γ peut substituer à $(0, \ldots, 0) = \beta_0$: posons dans (1)

$$x'_\rho \equiv x''_\rho \equiv \ldots \equiv x_\rho^{(r_1)};$$

on a les congruences

$$\frac{r_1}{\delta} x'_1 \equiv 0, \quad \ldots, \quad \frac{r_1}{\delta} x'_q \equiv 0 \qquad \left(\mathrm{mod}\ \frac{r}{\delta}\right), \tag{7}$$

qui admettent comme solutions $(0, \ldots, 0)$. Γ permute alors exclusivement entre elles les solutions distinctes $(\mathrm{mod}\, r)$ des congruences (7), au nombre de δ^q (δ plus grand commun diviseur de r et r_1). L'ordre de Γ est au plus égal, par suite, à

$$\delta^q \times \text{ordre } G'';$$

or,

$$\text{ordre } \Gamma \geq \text{ordre } G' \times \text{ordre } G'',$$

et

$$\text{ordre } G' = \delta^q.$$

Donc

$$\text{ordre } \Gamma = \text{ordre } G' \times \text{ordre } G'',$$

et Γ est bien dérivé de G' et G''; G' est bien évidemment un sous-groupe invariant de Γ.

Il résulte de là que, pour $r_1 \geq 3$, Γ n'est transitif entre les r^q lettres que si

$$\delta = r, \qquad r_1 \equiv 0 \qquad (\mathrm{mod}\, r).$$

D'autre part, si $r = p_1^\mu$ n'est pas premier ($\mu > 1$), G'' permute exclusivement entre elles les lettres d'indices tous multiples de p_1 autres que β_0, tout en les déplaçant, car

$$| x_1, \ldots, x_n;\ \alpha_1 x_1, \alpha_2 x_1 + x_2, \ldots, \alpha_n x_1 + x_n | \qquad (\mathrm{mod}\, r),$$

où α_1 est premier à p_1, est une substitution quels que soient $\alpha_2, \ldots, \alpha_n$, et remplace $(p_1, 0, \ldots, 0)$ par $(\alpha_1 p_1, \alpha_2 p_1, \ldots, \alpha_n p_1)$; donc G'' est intransitif entre les lettres qu'il déplace. Si $r = p_1$ est premier ($\mu = 1$), la même substitution remplace $(1, 0, \ldots, 0)$ par $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ qui est arbitraire (mais $\neq \beta_0$) : G'' est transitif, mais ne l'est deux fois que si $p_1 = 2$, $r = 2$.

Nous traiterons tout à l'heure le cas où $r_1 = 2$.

Nous avons obtenu ainsi le théorème suivant :

THÉORÈME II. — *Soient les congruences*

$$x'_\rho + x''_\rho + \ldots + x_\rho^{(r_1)} \equiv 0 \pmod r \qquad (1)$$

($\rho = 1, 2, \ldots, q$; r_1 *donné* > 2) *et* r^q *lettres* $(x_1, x_2, \ldots, x_q)$ *caractérisées par* q *indices* (mod r) (1), $r = p_1^\mu$ *et* p_1 *premier. On peut associer ces lettres* r_1 *à* r_1, *une même lettre pouvant être répétée plusieurs fois, de façon que les indices de même rang* $1, 2, \ldots, q$ *satisfassent aux congruences ci-dessus, et l'on forme ainsi des combinaisons de* r_1 *lettres : l'ensemble des substitutions entre les* r^q *lettres qui permutent entre elles toutes ces combinaisons est le groupe* Γ *dérivé du groupe* G'' *des substitutions linéaires homogènes*

$$| x_1, \ldots, x_q ;\ a_1^1 x_1 + \ldots + a_1^q x_q, \ldots, a_q^1 x_1 + \ldots + a_q^q x_q | \pmod r,$$

et du groupe G' *des substitutions*

$$| x_1, \ldots, x_q ;\ x_1 + \alpha_1, \ldots, x_q + \alpha_q | \pmod r,$$

où $\alpha_1, \ldots, \alpha_q$ *prennent* (mod r) *toutes les valeurs possibles multiples de* $\frac{r}{\delta}$, δ *étant le plus grand commun diviseur de* r *et* r_1.

En particulier, si $\delta = r$, *c'est-à-dire* $r_1 \equiv 0 \pmod r$, Γ *est le groupe linéaire général* (mod r) *non homogène à* q *indices. Dans ce cas, et dans ce cas seulement,* Γ *est transitif; mais il n'est pas primitif si* r *n'est pas premier* (2).

La condition nécessaire et suffisante pour que Γ *soit deux fois transitif est* $r_1 \equiv 0 \pmod r$, $r = p_1$. *Alors même, si* $p_1 = 2$, Γ *est exactement trois fois transitif.*

Remarque I. — G' est formé de substitutions échangeables, et ses facteurs de composition, puisque $\delta = p_1^{\mu_1}$, $\mu_1 \leq \mu$, sont tous égaux à p_1 (il y en a $\mu_1 q$). Donc Γ a $\mu_1 q$ facteurs de composition égaux à p_1, les autres étant ceux du groupe linéaire homogène (mod r) à q indices.

Remarque II. — Nous avons supposé précédemment (p. 288) $r_1 > 2$. Soit maintenant $r_1 = 2$: les congruences (1) se réduisent aux congruences (5).

---

(1) C'est-à-dire prenant chacun les valeurs $0, 1, \ldots, r-1 \pmod r$.

(2) Car G'' n'est pas maximum dans Γ, puisqu'il permute exclusivement entre elles les lettres d'indices multiples de p_1, comme les substitutions de G' pour lesquelles les α sont tous multiples de p_1.

Si $r = 2$, ces congruences sont satisfaites par $x'_\rho \equiv x''_\rho$, quel que soit x'_ρ : (5) est illusoire; Γ est le groupe symétrique de 2^q éléments.

Soit $r > 2$. Une substitution S de Γ qui remplace $(x_1, \ldots, x_q)$ par $(\xi_1, \ldots, \xi_q)$, remplace $(-x_1, \ldots, -x_q)$ par $(-\xi_1, \ldots, -\xi_q)$.

1° $r = p_1^\mu$ (p_1 impair). Prenons les $r^q - 1$ lettres autres que $\beta_0 = (0, 0, \ldots, 0)$ (Γ laisse β_0 immobile), et associons deux à deux les $r' = \dfrac{r^q - 1}{2}$ paires de lettres autres que β_0 pour lesquelles, dans chaque paire, les indices correspondants sont égaux et de signe contraire; ceci est possible, puisque $(\xi_1, \ldots, \xi_q)$, $(-\xi_1, \ldots, -\xi_q)$ sont distinctes. Désignons par $a_1, b_1; \ldots; a_{r'}, b_{r'}$ ces r' paires.

Nous formerons toutes les $r'!$ substitutions possibles entre $a_1, \ldots, a_{r'}$,

$$\sigma_1, \quad \sigma_2, \quad \ldots \quad \sigma_{r'!},$$

puis les substitutions déduites de celles-là en remplaçant a par b,

$$\tau_1, \quad \tau_2, \quad \ldots, \quad \tau_{r'!},$$

et le groupe g des substitutions

$$\sigma_1\tau_1, \quad \sigma_2\tau_2, \quad \ldots, \quad \sigma_{r'!}\tau_{r'!}$$

correspondant, d'ordre $r'!$.

D'autre part, formons encore le groupe g' dérivé de

$$(a_1 b_1), \quad (a_2 b_2), \quad \ldots, \quad (a_{r'} b_{r'}),$$

d'ordre $2^{r'}$. Le groupe cherché Γ est dérivé de ces deux groupes et d'ordre $r'!\, 2^{r'}$. En effet, Γ contient les substitutions de ces deux groupes; de plus, toute substitution de Γ est égale à une substitution qui permute les paires d'une certaine manière par une substitution qui les laisse immobiles, c'est-à-dire au produit d'une substitution de g par une de g'. On voit de suite que Γ est une fois, et une fois seulement, transitif entre les $2r'$ lettres autres que β_0, car Γ n'est pas primitif (1).

2° $r = 2^\mu$. — Les lettres $(\xi_1, \ldots, \xi_q)$ dont les indices satisfont à

$$2\xi_1 \equiv \ldots \equiv 2\xi_q \equiv 0 \pmod{2^\mu}$$

sont permutées exclusivement entre elles par Γ. On a pour elles $\xi_i = 0$ ou $2^{\mu-1}$: ces lettres sont au nombre de 2^q. Γ contient le groupe symétrique entre ces 2^q lettres.

---

(1) Ce groupe rentre dans une catégorie de groupes déjà considérée par nous (*J. de Math.*, 1895, p. 9).

Au contraire on peut raisonner sur les $2r''' = 2^{pq} - 2^q$ autres lettres comme tout à l'heure. Le groupe Γ est d'ordre $r'''!\, 2^q!\, 2^{r'''}$.

Remarque III. — Le théorème II précédent a été établi par M. Jordan dans les cas particuliers suivants :

$$r_1 = r = 3, \qquad q = 2,$$
$$r_1 = r = 4, \qquad q = 6,$$

et indiqué comme résultant de raisonnements semblables pour les cas où

$$r_1 = r = 3, \qquad q = 20,$$
$$r_1 = r = 4, \qquad q = 2,$$
$$r_1 = r = 3, \qquad q = 8 \quad (1).$$

Le théorème II précédent a l'avantage de résumer les solutions des cinq cas ci-dessus envisagés par M. Jordan et, éventuellement, de fournir la solution de cas analogues.

Notre procédé de démonstration diffère sur un point de celui employé par M. Jordan pour ces cas particuliers. Pour montrer nettement la dissemblance, prenons, par exemple, le groupe de Hesse ou groupe de l'équation aux abscisses des points d'inflexion des courbes du troisième degré. Ce groupe est contenu dans le groupe Γ_1 formé de l'ensemble des substitutions entre les 9 lettres (x_1, x_2) (mod 3) qui permutent entre elles les solutions des congruences

$$x'_1 + x''_1 + x'''_1 \equiv x'_2 + x''_2 + x'''_2 \equiv 0 \pmod 3 \tag{8}$$

telles que

$$(x'_1, x'_2), \quad (x''_1, x''_2), \quad (x'''_1, x'''_2)$$

soient des lettres *distinctes*. En effet, d'après la théorie des fonctions elliptiques (2), les points d'inflexion d'une courbe du troisième degré sont déterminés par

$$3u_1 = \mathrm{P} + 2x_1\omega_1 + 2x_2\omega_2 = \mathrm{P} + \text{période} \qquad (x_1, x_2 \text{ entiers}).$$

Les congruences (8) expriment précisément que 3 de ces points distincts sont en ligne droite : le groupe cherché doit, comme Γ_1, permuter entre eux ces systèmes de 3 points ou les droites passant par ces 3 points. Mais, si nous prenons les solutions de (8) pour lesquelles $(x'_1, x'_2), (x''_1, x''_2), (x'''_1, x'''_2)$ ne sont pas distinctes,

(1) *Traité des substitutions,* p. 302, 306 et 308.

(2) JORDAN, *Cours d'Analyse lithographié de l'École Polytechnique,* 1re division. — APPELL et GOURSAT, *Fonctions algébriques,* p. 490.

on remarque que $x'_1 \equiv x''_1$, $x'_2 \equiv x''_2$ entraînent $x'_1 \equiv x'''_1$, $x'_2 \equiv x'''_2$. Les 3 points correspondants de la cubique sont confondus. Le groupe de Hesse permute aussi entre eux ces points, qui sont les points d'inflexion, et les tangentes d'inflexion qui passent par ces 3 points confondus; par suite, il est contenu dans le groupe des substitutions entre les 9 lettres qui permutent entre elles les solutions de (8), les 3 lettres (x'_1, x'_2), (x''_1, x''_2), (x'''_1, x'''_2) étant *distinctes ou non*. Mais ce dernier groupe n'est autre que le groupe Γ de notre théorème II dans le cas particulier où $r = r_1 = 3$, $q = 2$.

Un même mode de raisonnement est applicable aux autres cas particuliers mentionnés tout à l'heure et étudiés par M. Jordan, ou plus généralement aux équations

$$u_1^{(j)} + \ldots + u_\delta^{(j)} = \frac{\mathrm{P} + 2x_j\pi i + x_{p+1}\tau_1^{(j)} + \ldots + x_{2p}\tau_p^{(j)}}{r} \qquad (j = 1, 2, \ldots, p \text{ et } \delta \geq p)$$

de la page 286 : les congruences (1), que les lettres $(x'_1, \ldots, x'_{2p}), \ldots, (x_1^{(r_1)}, \ldots, x_{2p}^{(r_1)})$ dont les indices y entrent soient *distinctes ou non,* expriment certaines propriétés géométriques et équivalent à des relations rationnelles $\mathrm{R} = 0$ entre les abscisses ou les paramètres solutions de $\mathrm{X} = 0$. L'ensemble des fonctions $\mathrm{R} = 0$ est laissé invariable par le groupe de $\mathrm{X} = 0$, par suite aussi l'ensemble des solutions des congruences (1), que les lettres $(x'_1, \ldots, x'_{2p}), \ldots, (x_1^{(r_1)}, \ldots, x_{2p}^{(r_1)})$ qui y entrent soient distinctes ou non. Il y a donc lieu à application du théorème II; mais il est bien évident que le groupe de $\mathrm{X} = 0$ permute aussi exclusivement entre elles les solutions de (1) pour lesquelles les r_1 lettres sont distinctes. Dans chaque cas, ce qui précède comportera d'ailleurs une interprétation géométrique.

Indiquons-la encore dans le cas des cubiques C ayant en 3 points un contact du troisième ordre avec une quartique générale (sans point double).

Les solutions du problème sont données par les 3 relations (1)

$$(9) \qquad \begin{cases} u_1 + u_2 + \ldots + u_{12} = 3\mathrm{P} + 2x_1\pi i + x_4\mathrm{A} + x_5\mathrm{B}'' + x_6\mathrm{B}', \\ v_1 + v_2 + \ldots + v_{12} = 3\mathrm{Q} + 2x_2\pi i + x_4\mathrm{B}'' + x_5\mathrm{A}' + x_6\mathrm{B}, \\ w_1 + w_2 + \ldots + w_{12} = 3\mathrm{R} + 2x_3\pi i + x_4\mathrm{B}' + x_5\mathrm{B} + x_6\mathrm{A}'', \end{cases}$$

où u, v, w sont des intégrales abéliennes de première espèce attachées à la courbe, et où l'on fait

$$\begin{cases} u_1 = u_2 = u_3 = u_4 = u_1^{(j)}, & u_5 = \ldots = u_8 = u_2^{(j)}, & u_9 = \ldots = u_{12} = u_3^{(j)}, \\ v_1 = \ldots\ldots = v_4 = v_1^{(j)}, & v_5 = \ldots = v_8 = v_2^{(j)}, & v_9 = \ldots = v_{12} = v_3^{(j)}, \\ w_1 = \ldots\ldots = w_4 = w_1^{(j)}, & w_5 = \ldots = w_8 = w_2^{(j)}, & w_9 = \ldots = w_{12} = w_3^{(j)}. \end{cases}$$

(1) Appell et Goursat, *Fonctions algébriques*, p. 498.

On a ainsi

$$\begin{cases} u_1^{(j)} + u_2^{(j)} + u_3^{(j)} = \dfrac{3\,\mathrm{P} + 2x_1^{(j)}\pi i + x_4^{(j)}\mathrm{A} + x_5^{(j)}\mathrm{B}'' + x_6^{(j)}\mathrm{B}'}{4}, \\ v_1^{(j)} + v_2^{(j)} + v_3^{(j)} = \dfrac{3\,\mathrm{Q} + 2x_2^{(j)}\pi i + x_4^{(j)}\mathrm{B}'' + x_5^{(j)}\mathrm{A}' + x_6^{(j)}\mathrm{B}}{4}, \\ w_1^{(j)} + w_2^{(j)} + w_3^{(j)} = \dfrac{3\,\mathrm{R} + 2x_3^{(j)}\pi i + x_4^{(j)}\mathrm{B}' + x_5^{(j)}\mathrm{B} + x_6^{(j)}\mathrm{A}''}{4}. \end{cases}$$

A chaque système de valeurs des $x_1^{(j)}, \ldots, x_6^{(j)}$ correspondent ainsi 3 points de contact et une cubique C qu'on peut caractériser par $(x_1^{(j)}, \ldots, x_6^{(j)})$.

Prenons 4 de ces cubiques, *distinctes ou non,*

$$c^{(1)} = (x_1^{(1)}, \ldots, x_6^{(1)}), \qquad \ldots, \qquad c^{(4)} = (x_1^{(4)}, \ldots, x_6^{(4)}),$$

mais telles que

(1 *bis*) $\qquad x_\rho^{(1)} + x_\rho^{(2)} + x_\rho^{(3)} + x_\rho^{(4)} \equiv 0 \pmod 4 \qquad (\rho = 1, 2, 3, 4, 5 \text{ et } 6).$

Les 3 relations (9) exprimant la condition nécessaire et suffisante pour que 12 points de la quartique soient sur une cubique, on voit que les 12 points de contact des 4 cubiques $c^{(1)}, \ldots, c^{(4)}$ sont sur une cubique γ.

Mais il n'est aucunement nécessaire de supposer que ces 4 cubiques sont distinctes.

Prenons d'abord

$$x_\rho^{(1)} = x_\rho^{(2)}, \qquad c^{(1)} = c^{(2)};$$

la cubique correspondante γ' est tangente en 3 points à la quartique.

Prenons maintenant

$$x_\rho^{(1)} = x_\rho^{(2)} = x_\rho^{(3)},$$

on a forcément

$$x_\rho^{(1)} = x_\rho^{(4)}.$$

La cubique correspondante est la cubique $c^{(1)}$.

Il est bien évident ici que chaque substitution du groupe de $\mathrm{X} = 0$ doit permuter entre elles les cubiques $c^{(j)}$, les cubiques γ, les cubiques γ' respectivement (1), par suite, permuter entre eux les systèmes de solutions, formées de lettres *distinctes ou non,* de (1 *bis*). Le groupe de $\mathrm{X} = 0$ est donc contenu dans le groupe linéaire général (mod 4) à 6 indices, d'après le théorème II.

On pourrait aussi traiter le cas des cubiques ayant en 4 points un contact du

(1) Comparer CLEBSCH, *Journal de Crelle,* t. 63, 1864, p. 205, où sont signalées ces diverses catégories de cubiques.

deuxième ordre avec la quartique : on en trouverait (1) 3^6 systèmes. Le groupe de $X = o$ est compris, d'après le théorème II, dans le groupe linéaire général (mod 3), à 6 indices, et même dans le groupe linéaire homogène, puisque l'un des systèmes est formé des droites du plan (ce groupe permute entre elles les solutions des congruences $x'_\rho + x''_\rho \equiv o \pmod 3$).

Considérons encore, comme à la page 285, l'équation $X = o$ qui détermine les 63 systèmes distincts de coniques tangentes en 4 points à une quartique générale; ces coniques étant caractérisées par $(x_1, \ldots, x_6) \pmod 2$, le groupe de $X = o$ laisse invariables les solutions des congruences

$$x_\rho + x'_\rho + x''_\rho \equiv o \pmod 2.$$

Ici $r_1 = 3$, $r = 2$, $q = 6$, $\delta = 1$. D'après le théorème II, le groupe de $X = o$ est contenu dans le groupe linéaire homogène (mod 2) à 6 indices.

V.

LA CLASSE DU GROUPE LINÉAIRE ET DE SES SUBSTITUTIONS.

Méthode générale pour la détermination de la classe des substitutions d'un groupe. — Indiquons d'abord une méthode générale pour la détermination de la classe des substitutions d'un groupe et de la classe de ce groupe.

Soient G un groupe de substitutions, a, b, ... ses lettres, en nombre n, ces lettres étant effectivement déplacées par G. Classons les lettres de G en catégories, en mettant ensemble celles que G permute entre elles. Soient

$$(10) \qquad \left\{ \begin{array}{llll} a, & b, & \ldots, \\ a', & b', & \ldots, \\ a'', & b'', & \ldots, \\ \ldots, & \ldots, & \ldots \end{array} \right.$$

ces catégories, H_α le sous-groupe des substitutions de G qui laissent α immobile. Classons les groupes H_α en catégories, deux de ces groupes appartenant à une même catégorie pour les valeurs de α appartenant à une même ligne de (10), c'est-à-dire à une même catégorie de lettres; les groupes d'une même catégorie sont les transformés d'un d'entre eux par les substitutions de G, par suite sont semblables. Donc H_a, H_b, ... sont semblables; de même $H_{a'}$, $H_{b'}$, ... Prenons dans chaque catégorie de groupes H_α un groupe la représentant : soient H_a,

(1) APPELL et GOURSAT, *Fonctions algébriques*, p. 498.

$H_{a'}$, ... ces représentants; une substitution de G ou bien est de classe n, ou bien laisse une lettre immobile et est semblable à une substitution de H_a, ou $H_{a'}$, ou .... Pour avoir sa classe il suffit de trouver la classe des substitutions de H_a, $H_{a'}$, ...

On opérera alors sur chacun de ces groupes comme on l'a fait sur G; et ainsi de suite.

Dans les opérations successives que l'on fera, on pourra être amené à considérer des sous-groupes, par exemple $H_{a\beta\gamma}$, qui soient contenus dans des sous-groupes déjà étudiés au point de vue de la classe, par exemple $H_{a\gamma}$: il sera inutile de s'en occuper. A un moment quelconque du raisonnement, nous pourrons admettre que l'on ne considère que des sous-groupes non contenus dans les sous-groupes déjà étudiés. *C'est ce que nous appellerons la condition* (A).

Cette méthode est aussi, *a fortiori,* applicable pour trouver la classe de G. Elle se simplifie même, puisqu'il est inutile de s'occuper du degré des sous-groupes considérés, tant qu'on n'arrive pas à un sous-groupe dont chaque substitution déplace toutes les lettres de ce sous-groupe, et pour lequel la classe est égale au degré.

Application au groupe linéaire (mod r) (r premier). — Considérons d'abord le groupe linéaire général L non homogène à m indices (mod r), r étant premier. Nous allons établir le théorème suivant :

THÉORÈME III. — *Le groupe linéaire général homogène à m indices* (mod r). *r étant premier, renferme des substitutions de classe $r^m - 1$, $r^m - r$, $r^m - r^2$, ..., $r^m - r^{m-i}$, ..., $r^m - r^{m-1}$ exclusivement. Il est m fois incomplètement transitif.*

Le groupe linéaire général non homogène renferme en outre des substitutions de classe r^m; il est $m+1$ fois incomplètement transitif.

La classe des deux groupes est $r^m - r^{m-1}$ (1).

---

(1) JORDAN, *Comptes rendus,* décembre 1872, p. 1754. Rappelons que le groupe linéaire général non homogène (mod r) est deux fois transitif quand $r > 2$, trois fois quand $r = 2$ (Jordan).

Le *groupe abélien* (JORDAN, *Traité des Substitutions,* p. 174) contient la substitution ($m = 2m_1$)

$$| x_1, y_1, x_2, \ldots, y_{m_1}; x_1 + y_1, y_1, x_2, \ldots, y_{m_1} | \qquad (\text{mod } r)$$

qui laisse immobiles les r^{2m_1-1} lettres pour lesquelles $y_1 \equiv 0$: sa classe est donc celle du groupe linéaire général.

De même pour le *groupe orthogonal* (JORDAN, *Traité des Substitutions,* p. 155) qui contient la substitution

$$| x_1, x_2, x_3, \ldots, x_m; x_2, x_1, x_3, \ldots, x_m | \qquad (\text{mod } r)$$

laissant immobiles les r^{m-1} lettres pour lesquelles $x_1 \equiv x_2$.

En effet, *rappelons d'abord la définition de la transitivité incomplète* (1).

Soient A un groupe transitif entre les n lettres $\alpha_1, \ldots, \alpha_n$ qu'il déplace; A_{α_i} le sous-groupe de A laissant α_i immobile : A_{α_i} est le transformé de A_{α_1} par une substitution de A.

A_{α_1} peut laisser en même temps $\alpha_2, \ldots, \alpha_{p_1}$ immobiles en déplaçant toutes les autres lettres :

$$A_{\alpha_1} = A_{\alpha_2} = \ldots = A_{\alpha_{p_1}} = A_{\alpha_1\alpha_2\ldots\alpha_{p_1}};$$

A_{α_1} déplace toute autre lettre $\alpha_j (j > p_1)$. Supposons que A_{α_1} soit transitif entre les lettres $\alpha_{p_1+1}, \ldots, \alpha_n$: si $p_1 = 1$, on dit que A est deux fois transitif; il est alors primitif; si $p_1 > 1$, A est imprimitif (2), mais on peut dire dans ce cas que A est *deux fois incomplètement transitif* (3).

Toute substitution de A qui laisse une lettre α_k immobile est transformée d'une substitution de $A_{\alpha_1\ldots\alpha_{p_1}}$ par une substitution de A, et elle appartient à un sous-groupe $A_{\alpha'_1\ldots\alpha'_{p_1}}$ de A laissant exactement p_1 lettres immobiles, comme $A_{\alpha_1\ldots\alpha_{p_1}}$; parmi ces lettres se trouve α_k, et $\alpha'_1, \ldots, \alpha'_{p_1}$ diffèrent toutes de ces p_1 lettres $\alpha_1, \ldots, \alpha_{p_1}$, ou leur sont toutes identiques, sans quoi le groupe dérivé de $A_{\alpha_1\ldots\alpha_{p_1}}$, $A_{\alpha'_1\ldots\alpha'_{p_1}}$ laisserait au moins une lettre immobile, sans en laisser p_1 : un de ses transformés serait contenu dans $A_{\alpha_1} = A_{\alpha_1\ldots\alpha_{p_1}}$, et le contiendrait, tout en étant plus grand que lui, ce qui est absurde. Finalement (4), A admet une répartition de ses n lettres p_1 à p_1 en systèmes $s_1, s_2, \ldots, s_{\frac{n}{p_1}}$.

Soit dans $A_{\alpha_1\ldots\alpha_{p_1}}$ le sous-groupe $A_{\alpha_1\ldots\alpha_{p_1}\alpha_{p_1+1}}$ des substitutions laissant α_{p_1+1} immobile. Tout sous-groupe A' des substitutions de A laissant immobile une des lettres d'un des systèmes, s_i par exemple, et une autre lettre de A non contenue dans ce système, est semblable à $A_{\alpha_1\ldots\alpha_{p_1}\alpha_{p_1+1}}$. En effet, par une substitution convenable, on transformera A' en un groupe A'_1 de la forme $A_{\alpha_1\ldots\alpha_{p_1}\alpha_{p_1+j}}$ $(j \geqq 1)$, puis, si $j \neq 1$, par une substitution de $A_{\alpha_1\ldots\alpha_{p_1}}$, qui est transitif entre $\alpha_{p_1+1}, \ldots, \alpha_n$, on transformera A'_1 en $A_{\alpha_1\ldots\alpha_{p_1}\alpha_{p_1+1}}$.

$A_{\alpha_1\ldots\alpha_{p_1}\alpha_{p_1+1}}$ peut laisser immobiles d'autres lettres : soient $\alpha_{p_1+2}, \ldots, \alpha_{p_1+p_2}$ ces

---

(1) *Intermédiaire des Mathématiciens*, 1900, p. 157-158.

(2) *Voir* JORDAN, *Traité des Substitutions*, p. 283-285, et notre Mémoire des *Annales de la Faculté des Sciences de Toulouse*, 1895, D.18, théorème VII.

(3) La définition donnée par Lie de la transitivité multiple dans les groupes finis continus est précisément analogue à celle de la transitivité incomplète dans les groupes de substitutions (*Voir* notre Mémoire du *Journal de Mathématiques*, 1901, p. 62 .

(4) *Loc. cit.*, note (2) ci-dessus.

lettres, $\alpha_{p_1+p_2+j}$ $(j \geq 1)$ étant déplacé par $A_{\alpha_1 \ldots \alpha_{p_1+1}}$; on a

$$A_{\alpha_1 \ldots \alpha_{p_1}\alpha_{p_1+1}} = A_{\alpha_1 \ldots \alpha_{p_1}\alpha_{p_1+2}} = \ldots = A_{\alpha_1 \ldots \alpha_{p_1}\alpha_{p_1+p_2}} = A_{\alpha_1 \ldots \alpha_{p_1+p_2}}.$$

Si $A_{\alpha_1 \ldots \alpha_{p_1+p_2}}$ est transitif entre les lettres qu'il permute, on dira que A est *trois fois incomplètement transitif*, et ainsi de suite.

Dans un groupe A $n+1$ fois transitif ou incomplètement transitif, le sous-groupe A_{α_1} des substitutions de A laissant une des lettres, α_1, immobile est n fois transitif ou incomplètement transitif; le sous-groupe $A_{\alpha_1\beta_1}$ des substitutions de A_{α_1} laissant une des lettres déplacées par A_{α_1} immobile est $n-1$ fois transitif ou incomplètement transitif, et ainsi de suite; une substitution S qui laisse une lettre immobile est semblable à une substitution S_{α_1} de A_{α_1}; une substitution de A_{α_1} qui laisse une lettre de A_{α_1}, déplacée par A_{α_1}, immobile est semblable à une substitution de $A_{\alpha_1\beta_1}$, etc.

Ceci posé, considérons en particulier le groupe linéaire général L à m indices (mod r).

Une de ses substitutions S peut déplacer r^m lettres : elle est alors de classe r^m, mais ne peut être d'ordre 2 que si $r = 2$, cas où l'on a toujours des substitutions d'ordre 2 et de classe r^m.

Considérons une substitution S′ de L laissant une lettre immobile : L étant transitif, cette substitution est semblable à une substitution S'_1 laissant immobile la lettre $\alpha_{00\ldots0}$, dont tous les indices sont nuls : pour avoir la classe de S′, il suffit d'avoir celle de S'_1. Le groupe $L_{\alpha_{0\ldots0}}$ des substitutions de L laissant $\alpha_{00\ldots0}$ immobile est le groupe linéaire homogène qui est transitif entre $r^m - 1$ lettres, car il remplace $\alpha_{1\ldots0}$ par une lettre arbitraire [formule (4), p. 287]. Si S'_1 est de classe $r^m - 1$, elle n'est d'ordre 2 que si r impair. On sait d'ailleurs que $L_{\alpha_{00\ldots0}}$, transitif entre $r^m - 1$ lettres, renferme des substitutions de classe $r^m - 1$ (1).

Si S'_1 est de classe $< r^m - 1$, elle laisse une autre lettre déplacée par $L_{\alpha_{00\ldots0}}$ immobile. Elle est semblable à une substitution S″ de $L_{\alpha_{00\ldots0}}$ laissant immobile la lettre $\alpha_{10\ldots0}$, par suite à une du groupe $L_{\alpha_{00\ldots0}\alpha_{10\ldots0}}$. Les substitutions de $L_{\alpha_{00\ldots0}\alpha_{10\ldots0}}$ sont de la forme

$$\left|\begin{array}{ll} x_1 & x_1 + a_1^2 x_2 + \ldots + a_1^m x_m \\ x_2 & a_2^2 x_2 + \ldots + a_2^m x_m \\ \ldots & \ldots\ldots\ldots\ldots\ldots \\ x_m & a_m^2 x_2 + \ldots + a_m^m x_m \end{array}\right| \quad (\text{mod } r);$$

$L_{\alpha_{00\ldots0}\alpha_{10\ldots0}}$ laisse invariables les r lettres pour lesquelles l'indice x_1 est quelconque, les autres indices étant nuls. Il suffit d'avoir la classe de S″.

(1) JORDAN, *Journal de Mathématiques*, 1872, p. 351; *voir* encore plus loin, p. 312.

$L_{\alpha_{00\ldots0}\alpha_{10\ldots0}\ldots}$ remplace $(0, 1, 0, \ldots, 0) = \alpha_{010\ldots0}$ par la lettre $(a_1^2, \ldots, a_m^2)$ qui est arbitraire parmi les lettres pour lesquelles $x_2, \ldots, x_m$ ne sont pas tous nuls (p. 289-290); donc $L_{\alpha_{00\ldots0}\alpha_{10\ldots0}\ldots}$ est transitif entre les lettres qu'il déplace, en nombre $r^m - r$, et contient des substitutions de classe $r^m - r$; $r^m - r$ est pair, que r soit $= 2$ ou > 2.

S'' peut être de classe $r^m - r$ ou non; si non, S'' est semblable à une substitution de $L_{\alpha_{00\ldots0}\alpha_{10\ldots0}\ldots}$ laissant invariable $\alpha_{010\ldots0}$, c'est-à-dire appartient à $L_{\alpha_{00\ldots0}\alpha_{10\ldots0}\alpha_{010\ldots0}\ldots}$. Les substitutions de ce groupe sont de la forme

$$\left|\begin{array}{ll} x_1 & x_1 + a_1^3 x_3 + \ldots + a_1^m x_m \\ x_2 & x_2 + a_2^3 x_3 + \ldots + a_2^m x_m \\ x_3 & a_3^3 x_3 + \ldots + a_3^m x_m \\ \ldots & \ldots\ldots\ldots\ldots\ldots \\ x_m & a_m^3 x_3 + \ldots + a_m^m x_m \end{array}\right| \pmod r,$$

et ce groupe laisse invariables les r^2 lettres $(x_1, x_2, 0, \ldots, 0)$. On voit encore que ce groupe est transitif entre les $r^m - r^2$ autres lettres, et ainsi de suite. Plus généralement le sous-groupe des substitutions de L laissant $(x_1, x_2, \ldots, x_i, 0, \ldots, 0)$ immobile est transitif entre les $r^m - r^i$ autres lettres. Il est aussi formé des substitutions laissant $(0, 0, \ldots, 0)$, $(1, 0, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, x_i = 1, 0, \ldots, 0)$ immobiles.

Dès lors, pour $i = m - 1$, ce sous-groupe est transitif; pour $i = m - 2$, deux fois incomplètement transitif, etc.; pour $i = 0$, m fois incomplètement transitif.

Finalement on voit que le groupe linéaire homogène (mod r) à m indices renferme exclusivement des substitutions de classe r^m, $r^m - 1$, $r^m - r$, $r^m - r^2$, $\ldots$, $r^m - r^{m-1}$; le groupe linéaire non homogène renferme en outre des substitutions de classe r^m. C. Q. F. D.

Le rapprochement du théorème III et du théorème I nous donne alors ce résultat :

Corollaire. — *Une équation de degré r^m* (r premier), *dont le groupe est contenu dans le groupe linéaire général non homogène à m indices* (mod r), *ne peut avoir que $r^m - 1$, $r^m - r$, $\ldots$, $r^m - r^{m-1}$ ou* 0 *racines imaginaires si r est impair*, 2^m, $2^m - 2$, $2^m - 2^2$, $\ldots$, $2^m - 2^{m-1} = 2^{m-1}$, *ou* 0 *si* $r = 2$ (1).

Nous allons encore appliquer la méthode générale ci-dessus (p. 298) à la détermination plus ou moins complète de la classe des substitutions contenues dans le groupe linéaire général non homogène L (mod p^μ) à n indices (p premier, $\mu > 1$)

(1) Même, d'après ce que nous verrons plus loin (p. 314), il y a 0 ou $2^m - 2^{m-k}$ racines imaginaires $\left[k = 1, 2. \ldots \text{ ou } E\left(\frac{m}{2}\right)\right]$ quand $r = 2$.

et aussi à la détermination de la classe de ces groupes, qui, croyons-nous, n'a pas encore été évaluée pour $\mu > 1$.

Déterminons d'abord la classe de L.

Le groupe L, de degré $p^{\mu n}$, contient les substitutions

$$| x_1, \ldots, x_n ; x_1 + \alpha_1, \ldots, x_n + \alpha_n | \qquad (\mathrm{mod}\, p^{\mu}),$$

en nombre $p^{\mu n}$, qui forment un groupe transitif et dont toutes les substitutions sont de classe $p^{\mu n}$. Une substitution de L est de classe $p^{\mu n}$ ou semblable à une substitution du sous-groupe H_{β_0} des substitutions de L laissant la lettre $\beta_0 = (0, 0, \ldots, 0)$, dont tous les indices sont nuls (mod p^{μ}), invariable. H_{β_0} est formé des substitutions linéaires homogènes

$$(11) \qquad \begin{vmatrix} x_1 & a_1^1 x_1 + \ldots + a_1^n x_n \\ \cdot\cdot & \cdots\cdots\cdots\cdots \\ x_n & a_n^1 x_1 + \ldots + a_n^n x_n \end{vmatrix} \qquad (\mathrm{mod}\, p^{\mu}).$$

D'après la méthode générale indiquée au début du paragraphe, formons les catégories (10) pour H_{β_0}, catégories qui ne doivent comprendre que des lettres déplacées par H_{β_0}.

Soit $\beta_1 = (1, 0, \ldots, 0)$; $H_{\beta_0\beta_1}$ laisse invariable β_1; ses substitutions sont telles que

$$a_1^1 \equiv 1, \qquad a_2^1 \equiv \ldots \equiv a_n^1 \equiv 0 \qquad (\mathrm{mod}\, p^{\mu}),$$

c'est-à-dire de la forme

$$(12) \qquad \begin{vmatrix} x_1 & x_1 + a_1^2 x_2 + \ldots + a_1^n x_n \\ x_2 & a_2^2 x_2 + \ldots + a_2^n x_n \\ \cdot\cdot & \cdots\cdots\cdots\cdots \\ x_n & a_n^2 x_2 + \ldots + a_n^n x_n \end{vmatrix} \qquad (\mathrm{mod}\, p^{\mu});$$

et, réciproquement, les substitutions de cette forme appartiennent à $H_{\beta_0\beta_1}$.

Désignons, avec M. Jordan, par [1] $\Omega(p^{\mu n})$ l'ordre $\mathcal{H}_{\beta_0}$ de H_{β_0}. La condition nécessaire et suffisante pour que (12) représente une substitution est que son déterminant [2] soit premier à p, par suite que

$$(13) \qquad \begin{vmatrix} x_2 & a_2^2 x_2 + \ldots + a_2^n x_n \\ \cdot\cdot & \cdots\cdots\cdots\cdots \\ x_n & a_n^2 x_2 + \ldots + a_n^n x_n \end{vmatrix} \qquad (\mathrm{mod}\, p^{\mu})$$

---

(1) *Traité des Substitutions,* p. 93.

(2) *Id.*

représente une substitution; $a_1^2, \ldots, a_1^n$ sont arbitraires. Le nombre des substitutions (13) est $\Omega(p^{\mu(n-1)})$; le nombre des systèmes $a_1^2, \ldots, a_1^n$ est $p^{\mu(n-1)}$. Donc l'ordre $\mathcal{H}_{\beta_0\beta_1}$ de $H_{\beta_0\beta_1}$ est

$$\mathcal{H}_{\beta_0\beta_1} = p^{\mu(n-1)}\Omega(p^{\mu(n-1)}).$$

β_1 est donc permuté par H_{β_0} avec (1)

$$\frac{\mathcal{H}_{\beta_0}}{\mathcal{H}_{\beta_0\beta_1}} = \frac{\Omega(p^{\mu n})}{p^{\mu(n-1)}\Omega(p^{\mu(n-1)})} = (p^\mu, n) \text{ lettres},$$

(m, ρ) désignant en général le nombre de manières différentes de déterminer un système de ρ nombres $\lambda_1, \lambda_2, \ldots, \lambda_\rho$ inférieurs à m, et dont le plus grand commun diviseur est premier à m. Or, parmi les $p^{\mu n}$ systèmes de nombres $\lambda_1, \lambda_2, \ldots, \lambda_n$ où $\lambda_1, \lambda_2, \ldots, \lambda_n$ sont égaux à 0, 1, 2, ..., ou $p^\mu - 1 \pmod{p^\mu}$, ceux qui ont un plus grand commun diviseur > 1 sont ceux pour lequels $\lambda_1, \ldots, \lambda_n$ sont tous $\equiv 0 \pmod{p}$, en nombre $p^{(\mu-1)n}$. Donc

$$(14) \qquad (p^\mu, n) = p^{\mu n} - p^{(\mu-1)n} = p^{\mu n}\left(1 - \frac{1}{p^n}\right).$$

Les lettres correspondantes sont les lettres de la première catégorie (10), et H_{β_0} les permute transitivement avec β_1. D'autre part H_{β_0} permute exclusivement entre elles les lettres dont tous les indices sont $\equiv 0 \pmod{p}$, en nombre $p^{(\mu-1)n}$, lettres qui ne comprennent pas β_1. Il résulte, par suite, de (14) que les lettres de la première catégorie comprennent toutes celles dont un indice est $\not\equiv 0 \pmod{p}$, et H_{β_0} est transitif entre ces dernières. De plus, une substitution S de H_{β_0} ne peut laisser immobiles toutes les lettres de la première catégorie sans se réduire à l'unité.

En effet, S laisserait immobiles les lettres

$$(15) \qquad \beta_1, \quad \beta_2, \quad \ldots, \quad \beta_n,$$

pour lesquelles un des indices est $\equiv 1 \pmod{p^\mu}$, les autres étant tous nuls; par exemple, S laissera immobile β_i telle que $x_i \equiv 1$, les autres indices étant nuls $\pmod{p^\mu}$, ce qui entraîne, d'après (11), $a_i^i \equiv 1$, $a_j^i \equiv 0 \pmod{p^\mu}$ quand $j \neq i$. Ceci devant avoir lieu pour S quel que soit i, il faudrait $S = 1$. Donc une substitution quelconque de H_{β_0} déplace quelque lettre de la première catégorie.

Si alors γ_1 est une lettre de H_{β_0} n'appartenant pas à la première catégorie, les substitutions de $H_{\beta_0\gamma_1}$ ou bien laissent immobile une autre lettre β_0' de la première

(1) D'après la formule de M. Jordan : $\Omega(m^n) = (m, n)\, m^{n-1}\Omega(m^{n-1})$ (*Traité des Substitutions*, p. 96).

catégorie, ou bien déplacent toutes les lettres de cette première catégorie, c'est-à-dire sont de classe $\geq p^{\mu n} - p^{(\mu-1)n}$. Finalement, une substitution de $H_{\beta_0\gamma_1}$ ne peut être de classe inférieure à ce nombre que si elle appartient à un groupe semblable à $H_{\beta_0\beta_1}$, qu'il nous suffira de considérer [condition (A), p. 299]. Il y a bien d'ailleurs dans $H_{\beta_0\beta_1}$ des substitutions de classe plus petite que $p^{\mu n} - p^{(\mu-1)n}$: $H_{\beta_0\beta_1}$ contient la substitution

$$(16) \quad |x_1, \ldots, x_{n-1}, x_n;\ x_1 + p^{\mu-1}x_n, \ldots, x_{n-1} + p^{\mu-1}x_n, x_n(1 + p^{\mu-1})| \pmod{p^\mu},$$

laissant invariables les lettres pour lesquelles $x_n \equiv 0 \pmod{p}$, en nombre $p^{\mu(n-1)+\mu-1} = p^{\mu n-1}$; cette substitution a sa classe $\leq p^{\mu n} - p^{\mu n-1} < p^{\mu n} - p^{(\mu-1)n}$ quand $n > 1$. Il nous suffit donc, pour avoir la classe de H_{β_0}, de chercher la classe de $H_{\beta_0\beta_1}$.

Opérons de la même manière sur $H_{\beta_0\beta_1}$, et répartissons ses lettres en catégories (10).

D'abord $H_{\beta_0\beta_1}$ laisse immobiles les lettres $(x_1, 0, \ldots, 0)$, en nombre p^μ. D'après (12), $H_{\beta_0\beta_1}$ déplace la lettre $\beta_2 = (0, 1, 0, \ldots, 0)$ dont tous les indices, sauf le second $\equiv 1$, sont nuls, puisque $H_{\beta_0\beta_1}$ contient la substitution

$$|x_1, x_2, \ldots, x_n;\ x_1 + x_2, x_2, \ldots, x_n| \qquad (\mathrm{mod}\, p^\mu).$$

Nous classerons dans la première catégorie de $H_{\beta_0\beta_1}$ les lettres que ce groupe permute avec β_2. Les substitutions de $H_{\beta_0\beta_1\beta_2}$ sont de la forme

$$(17) \quad \left|\begin{array}{ll} x_1 & x_1 + a_1^3 x_3 + \ldots + a_1^n x_n \\ x_2 & x_2 + a_2^3 x_3 + \ldots + a_2^n x_n \\ x_3 & a_3^3 x_3 + \ldots + a_3^n x_n \\ \cdot\cdot & \cdots\cdots\cdots\cdots \\ x_n & a_n^3 x_3 + \ldots + a_n^n x_n \end{array}\right| \qquad (\mathrm{mod}\, p^\mu).$$

Leur nombre $\mathfrak{H}_{\beta_0\beta_1\beta_2}$ est, puisque $a_1^3, \ldots, a_1^n, a_2^3, \ldots, a_2^n$ sont arbitraires,

$$\Omega(p^{\mu(n-2)})p^{2\mu(n-2)}.$$

β_2 est permuté par $H_{\beta_0\beta_1}$ avec

$$B_2 = \frac{\mathfrak{H}_{\beta_0\beta_1}}{\mathfrak{H}_{\beta_0\beta_1\beta_2}} = \frac{p^{\mu(n-1)}\Omega(p^{\mu(n-1)})}{p^{2\mu(n-2)}\Omega(p^{\mu(n-2)})}.$$

Or,

$$\Omega(p^{\mu(n-1)}) = (p^\mu, n-1)p^{\mu(n-2)}\Omega(p^{\mu(n-2)})$$

donc, d'après (14),

$$(18) \qquad B_2 = (p^\mu, n-1)p^\mu = p^{\mu(n-1)+\mu}\left(1 - \frac{1}{p^{n-1}}\right) = p^{\mu n}\left(1 - \frac{1}{p^{n-1}}\right),$$

et $H_{\beta_0\beta_1}$ permute avec $\beta_2\, p^{\mu n}\left(1-\frac{1}{p^{n-1}}\right)$ lettres. D'autre part, $H_{\beta_0\beta_1}$ permute exclusivement entre elles les lettres pour lesquelles x_1 est arbitraire, $x_2, \ldots, x_n$ étant $\equiv 0 \pmod p$, lettres en nombre $p^{(\mu-1)(n-1)+\mu} = p^{(\mu-1)n+1}$, et qui ne comprennent pas β_2. D'après (18), β_2 est alors permutée transitivement par $H_{\beta_0\beta_1}$ avec toutes les lettres pour lesquelles un des indices $x_2, \ldots, x_n$ est $\not\equiv 0 \pmod p$. De plus, une substitution S de $H_{\beta_0\beta_1}$ ne peut laisser immobiles toutes les lettres (15), par suite les lettres que $H_{\beta_0\beta_1}$ permute avec β_2, sans se réduire à l'unité.

Si γ_2 est une lettre déplacée par $H_{\beta_0\beta_1}$ et n'appartenant pas à la première catégorie, les substitutions de $H_{\beta_0\beta_1\gamma_2}$, ou bien laissent immobile une autre lettre de la première catégorie, ou bien déplacent toutes les lettres de cette catégorie, c'est-à-dire sont de classe au moins égale à $p^{\mu n}\left(1-\frac{1}{p^{n-1}}\right)$. Une substitution de $H_{\beta_0\beta_1}$ ne peut ainsi être de classe inférieure à

$$p^{\mu n}\left(1-\frac{1}{p^{n-1}}\right), \tag{19}$$

que si elle appartient à un groupe semblable à $H_{\beta_0\beta_1\beta_2}$, qu'il nous suffira de considérer pour avoir la classe de L. D'ailleurs. à cause de (16), $H_{\beta_0\beta_1}$ est bien de classe $\leq p^{\mu n} - p^{\mu n-1} < p^{\mu n} - p^{\mu n-n+1}$, si $\mu n - 1 > \mu n - n + 1$, ou $n > 2$ (1).

On continuera de la sorte.

Admettons qu'on arrive ainsi à montrer, si la lettre β_i a tous ses indices nuls, sauf $x_i \equiv 1 \pmod{p^\mu}$: 1° que $H_{\beta_0\beta_1\beta_2\ldots\beta_i}$ permute exclusivement entre elles les lettres pour lesquelles $x_1, \ldots, x_i$ étant arbitraires, les autres indices sont $\equiv 0 \pmod p$, lettres en nombre $p^{(\mu-1)(n-i)+\mu i}$, et qui ne comprennent pas β_{i+1}; 2° que β_{i+1} est permuté transitivement par $H_{\beta_0\ldots\beta_i}$ avec l'ensemble E_{i+1} de toutes les lettres pour lesquelles un des indices $x_{i+1}, \ldots, x_n$ est $\not\equiv 0 \pmod p$; 3° qu'aucune substitution de $H_{\beta_0\ldots\beta_i}$ ne peut laisser immobiles toutes les lettres de E_{i+1} sans se réduire à l'unité. Enfin une substitution de $H_{\beta_0\beta_1\ldots\beta_i}$ ne peut être de classe inférieure à

$$p^{\mu n}\left(1-\frac{1}{p^{n-i}}\right), \tag{20}$$

que si elle appartient à un groupe semblable à $H_{\beta_0\beta_1\ldots\beta_{i+1}}$, qu'il nous suffira de considérer pour avoir la classe de L, cette classe, à cause de (16), ne pouvant être supérieure à (20).

Nous classerons dans la première catégorie de $H_{\beta_0\beta_1\ldots\beta_{i+1}}$ les lettres que ce

(1) Quand $n = 2$, $H_{\beta_0\beta_1\beta_2} = 1$; $H_{\beta_0\beta_1}$ est de classe à la fois au plus et au moins égale à $p^{2\mu} - p^{2\mu-1}$, c'est-à-dire précisément de classe $p^{2\mu} - p^{2\mu-1}$.

groupe permute avec β_{i+2}. Les substitutions de $H_{\beta_0 \dots \beta_{i+2}}$ sont de la forme

$$(21) \qquad \left| \begin{array}{ll} x_1 & x_1 + a_1^{i+3} x_{i+3} + \dots + a_1^n x_n \\ \dots & \dots\dots\dots\dots\dots\dots\dots \\ x_{i+2} & x_{i+2} + a_{i+2}^{i+3} x_{i+3} + \dots + a_{i+2}^n x_n \\ x_{i+3} & a_{i+3}^{i+3} x_{i+3} + \dots + a_{i+3}^n x_n \\ \dots & \dots\dots\dots\dots\dots\dots\dots \\ x_n & a_n^{i+3} x_{i+3} + \dots + a_n^n x_n \end{array} \right| \pmod{p^\mu}.$$

Leur nombre est

$$\Omega(p^{\mu(n-i-2)}) p^{\mu(n-i-2)(i+2)}.$$

β_{i+2} est alors permutée par $H_{\beta_0 \dots \beta_{i+1}}$ avec

$$B_{i+2} = \frac{\mathcal{H}_{\beta_0 \beta_1 \dots \beta_{i+1}}}{\mathcal{H}_{\beta_0 \dots \beta_{i+2}}} = \frac{\Omega(p^{\mu(n-i-1)}) p^{\mu(n-i-1)(i+1)}}{\Omega(p^{\mu(n-i-2)}) p^{\mu(n-i-2)(i+2)}}.$$

Or, d'après (14) et la page 304,

$$\Omega(p^{\mu(n-i-1)}) = (p^\mu, n-i-1)\, p^{\mu(n-i-2)} \Omega(p^{\mu(n-i-2)}),$$

$$(p^\mu, n-i-1) = p^{\mu(n-i-1)} \left(1 - \frac{1}{p^{n-i-1}}\right),$$

$$B_{i+2} = p^\lambda \left(1 - \frac{1}{p^{n-i-1}}\right),$$

$$\begin{aligned} \lambda &= \mu(n-i-1)(i+1) - \mu(n-i-2)(i+2) + \mu(n-i-2) + \mu(n-i-1) \\ &= \mu(i+1) + \mu(n-i-1) = \mu n, \end{aligned}$$

$$(22) \qquad B_{i+2} = p^{\mu n} \left(1 - \frac{1}{p^{n-i-1}}\right).$$

D'autre part, $H_{\beta_0 \dots \beta_{i+1}}$ permute exclusivement entre elles les lettres pour lesquelles $x_1, \dots, x_{i+1}$ étant arbitraires, les autres indices sont $\equiv 0 \pmod{p}$, lettres en nombre

$$(23) \qquad p^{\mu(i+1)+(\mu-1)(n-i-1)} = p^{(\mu-1)n+i+1}$$

et qui ne comprennent pas β_{i+2}. Il résulte de (22) et (23) que $H_{\beta_0 \dots \beta_{i+1}}$ permute transitivement β_{i+2} avec l'ensemble E_{i+2} des lettres pour lesquelles un des indices $x_{i+2}, \dots, x_n$ est $\not\equiv 0 \pmod{p}$. Enfin, aucune substitution de $H_{\beta_0 \dots \beta_{i+1}}$ ne peut laisser immobiles toutes les lettres de E_{i+2} sans se réduire à l'unité et, par suite, ou bien est de classe au moins égale à

$$(22) \qquad p^{\mu n} - p^{\mu n - n + i + 1},$$

ou bien appartient à un groupe semblable à $H_{\beta_0 \dots \beta_{i+2}}$, qu'il nous suffit de considérer, sous la condition que ce groupe soit de classe $\leq p^{\mu n} - p^{\mu n - n + i + 1}$.

Il est ainsi établi, en général, que le raisonnement peut se continuer tant que $i + 2 \leq n$. Supposons $i + 2 = n$.

$H_{\beta_0 \dots \beta_n}$ se réduit à l'unité : $H_{\beta_0 \dots \beta_{n-1}}$ déplace toutes les lettres de E_n et ne peut être de classe inférieure à

$$p^{\mu n} - p^{\mu n - 1} = p^{\mu n}\left(1 - \frac{1}{p}\right).$$

Les substitutions de $H_{\beta_0 \dots \beta_{n-1}}$ sont de la forme

$$U = | x_1, \dots, x_{n-1}, x_n ; x_1 + a_1^n x_n, \dots, x_{n-1} + a_{n-1}^n x_n, a_n^n x_n | \pmod{p^\mu},$$

avec la condition $a_n^n \not\equiv 0 \pmod{p}$. Parmi elles, il y a la substitution (16), qui laisse invariables $p^{\mu n - 1}$ lettres exactement et déplace la lettre $(0, \dots, 0, 1)$. On en conclut, d'une part, que $H_{\beta_0 \dots \beta_{n-2}}$ ne peut être de classe inférieure à $p^{\mu n} - p^{\mu n - 1}$, d'autre part qu'il ne peut être de classe supérieure; donc il est de classe $p^{\mu n} - p^{\mu n - 1}$.

Nous obtenons ainsi le théorème suivant :

THÉORÈME IV. — *Le groupe linéaire général de degré $p^{\mu n}$ à n indices* $\pmod{p^\mu}$, *p étant un nombre premier quelconque, est de classe $p^{\mu n} - p^{\mu n - 1}$.*

Nous allons compléter ce théorème en donnant quelques indications sur la classe des substitutions contenues dans ce groupe linéaire L.

D'après ce que nous avons vu (p. 306-307), $H_{\beta_0 \beta_1 \dots \beta_i}$ permute transitivement entre elles exactement $p^{\mu n}\left(1 - \frac{1}{p^{n-i}}\right)$ lettres de sa première catégorie. Une substitution de $H_{\beta_0 \dots \beta_i}$ déplace donc ces $p^{\mu n} - p^{(\mu - 1)n + i}$ lettres, ou est semblable à une substitution de $H_{\beta_0 \dots \beta_{i+1}}$.

$H_{\beta_0 \beta_1 \dots \beta_i}$ permute transitivement entre elles, exactement, $p^{\mu n} - p^{\mu n - n + i}$ lettres de sa première catégorie. Une substitution de $H_{\beta_0 \beta_1 \dots \beta_i}$ qui ne déplace pas toutes ces lettres est semblable à une substitution de $H_{\beta_0 \beta_1 \dots \beta_{i+1}}$. Considérons une substitution S de $H_{\beta_0 \beta_1 \dots \beta_i}$ qui les déplace toutes :

$$S = \left| \begin{array}{ll} x_1 & x_1 + a_1^{i+1} x_{i+1} + \dots + a_1^n x_n \\ \dots & \dots \dots \dots \dots \dots \dots \\ x_i & x_i + a_i^{i+1} x_{i+1} + \dots + a_i^n x_n \\ x_{i+1} & a_{i+1}^{i+1} x_{i+1} + \dots + a_{i+1}^n x_n \\ \dots & \dots \dots \dots \dots \dots \dots \\ x_n & a_n^{i+1} x_{i+1} + \dots + a_n^n x_n \end{array} \right| \pmod{p^\mu}.$$

S peut laisser immobiles certaines des lettres λ pour lesquelles $x_1, \dots, x_i$ sont

arbitraires, les autres indices $\equiv 0 \pmod p$, en nombre $p^{\mu n-n+i}$, lettres qui n'appartiennent pas à la première catégorie de $H_{\beta_0\beta_1\dots\beta_i}$. On les détermine, si $x_{i+1}=\xi_{i+1}p, \dots, x_n=\xi_n p$, par les congruences

$$(24)\qquad \left\{\begin{array}{l} a_1^{i+1}\xi_{i+1}+\dots+a_1^n\xi_n\equiv 0 \\ \dots\dots\dots\dots\dots\dots \\ a_n^{i+1}\xi_{i+1}+\dots+(a_n^n-1)\xi_n\equiv 0 \end{array}\right\} \pmod{p^{\mu-1}}.$$

Si ces congruences ont θ systèmes de solutions en $\xi_{i+1}, \dots, \xi_n$, le nombre de ces lettres est $p^{\mu i}\theta$. S déplace ainsi $p^{\mu n}-p^{\mu i}\theta$ lettres.

D'autre part, ces congruences (24) donnent aussi le nombre $p^{(\mu-1)i}\theta$ de lettres laissées immobiles par la substitution

$$\Sigma=\left|\begin{array}{ll} \xi_1 & \xi_1+a_1^{i+1}\xi_{i+1}+\dots+a_1^n\xi_n \\ \cdot\cdot & \dots\dots\dots\dots\dots\dots \\ \xi_i & \xi_i+a_i^{i+1}\xi_{i+1}+\dots+a_i^n\xi_n \\ \xi_{i+1} & a_{i+1}^{i+1}\xi_{i+1}+\dots+a_{i+1}^n\xi_n \\ \dots & \dots\dots\dots\dots\dots\dots \\ \xi_n & a_n^{i+1}\xi_{i+1}+\dots+a_n^n\xi_n \end{array}\right| \pmod{p^{\mu-1}}.$$

Soit $\Theta_{i,\mu}$ l'expression la plus générale du nombre de lettres déplacées par une substitution quelconque de $H_{\beta_0\beta_1\dots\beta_i}$; $p^{(\mu-1)n}-p^{(\mu-1)i}\theta$ est de la forme $\Theta_{i,\mu-1}$ et le nombre de lettres déplacées par S est compris dans la forme $p^{\mu n}-p^{\mu n-n+i}+p^i\Theta_{i,\mu-1}$. Le nombre de lettres déplacées par une substitution de $H_{\beta_0\beta_1\dots\beta_{i+1}}$ analogue à S est compris dans la forme

$$p^{\mu n}-p^{\mu n-n+i+1}+p^{i+1}\Theta_{i+1,\mu-1}.$$

Etc.,

Finalement $\Theta_{i,\mu}$ est compris dans la forme $p^{\mu n}-p^{\mu n-n+j}+p^j\Theta_{j,\mu-1}$, où $j=i, i+1, \dots,$ ou n. On en conclut que $\Theta_{0\mu}$ est compris dans la forme

$$p^{\mu n}-p^{(\mu-k)n+j_1+j_2+\dots+j_k}+p^{j_1+j_2+\dots+j_k}\Theta_{j_k,\mu-k}$$

où $j_1=0, 1, \dots,$ ou n; $j_2=j_1, j_1+1, \dots,$ ou n; $\dots$; $j_k=j_{k-1}, j_{k-1}+1, \dots,$ ou n, car on établit, de suite, cette formule exacte pour $k=1$, pour des valeurs de k croissantes. Finalement, puisque $\Theta_{j_{\mu-1},1}=p^n-p^{j_\mu}$, avec $j_\mu=j_{\mu-1}, j_{\mu-1}+1, \dots,$ ou n, $\Theta_{0,\mu}$ est compris dans la forme

$$p^{\mu n}-p^{j_1+j_2+\dots+j_\mu}.$$

Si nous prenons $j_\mu=j_{\mu-1}=\dots=j_{m+1}=n$, j_m quelconque $=0, 1, 2, \dots,$ ou n, $j_1=j_2=\dots=j_{m-1}=0$, ce qui est possible, $j_1+\dots+j_\mu=(\mu-m)n+j_m$

est un quelconque des nombres o à μn. Finalement, $\Theta_{0\mu}$ est compris dans la forme $p^{\mu n} - p^{\eta}$ où $\eta = 0, 1, 2, \ldots,$ ou $\mu n - 1$.

Le maximum est bien $p^{\mu n} - 1$ et le minimum $p^{\mu n} - p^{\mu n - 1}$.

D'autre part, H_{β_0} est transitif entre toutes les lettres de la première catégorie, c'est-à-dire entre toutes les lettres dont un indice est premier à p, lettres qu'il permute exclusivement entre elles; mais H_{β_0} qui contient la substitution

$$| x_1, x_2, \ldots, x_n; x_1 + x_2, x_2, \ldots, x_n | \qquad (\mathrm{mod}\, p^{\mu}),$$

remplace $(0, p, 0, \ldots, 0)$ par $(p, p, 0, \ldots, 0)$ et n'est pas transitif entre les lettres qu'il déplace.

On a ainsi ce théorème :

Théorème V. — *Le groupe linéaire général non homogène de degré $p^{\mu n}$ à n indices* $(\mathrm{mod} p^{\mu})$ *ne peut contenir que des substitutions déplaçant $p^{\mu n}$ ou*

$$P = p^{\mu n} - p^{\eta} \text{ lettres}$$

avec $\eta = 0, 1, 2, \ldots,$ *ou* $\mu n - 1$ (1).

Le groupe linéaire général non homogène n'est ni deux fois complètement, ni deux fois incomplètement transitif, quand $\mu > 1$. *Il est imprimitif* (2).

On en déduira facilement la classe des substitutions d'ordre 2 que peut renfermer le groupe. Il suffira de faire $P \equiv 0 (\mathrm{mod}\, 2)$.

Supposons, en particulier, $\mu = 2$:

$$P = p^{2n} - p^{\eta}.$$

P est pair quand p est impair, mais ne peut être égal à p^{2n}; si $p = 2$, P n'est pair que si $\eta \geq 1$.

Nous obtenons ainsi, à titre d'exemple d'application du théorème I, le corollaire suivant :

Corollaire. — *Une équation de degré p^{2n}, et dont le groupe est contenu dans le groupe linéaire* $(\mathrm{mod} p^2)$ *à n indices a :*

1° *Si* $p > 2$, *ou* $p^{2n} - p^{\eta} < p^{2n}$ ($\eta = 0, 1, 2, \ldots,$ *ou* $2n - 1$) *racines imaginaires;*

2° *Si* $p = 2$, o *ou* $2^{2n} - 2^{\eta}$ ($\eta = 0, 1, 2, \ldots,$ *ou* $2n - 1$) *racines imaginaires.*

---

(1) Ce qui précède ne prouve d'ailleurs pas qu'il en contient effectivement de chacune de ces classes, sauf de la classe $p^{\mu n} - p^{\mu n - 1}$. La formule du théorème V perfectionne une formule indiquée par nous dans les *Comptes rendus*, 11 avril 1904, p. 891.

(2) Jordan, *Traité*, p. 110.

VI.

LES SUBSTITUTIONS D'ORDRE 2 DANS LE GROUPE LINÉAIRE.

On peut perfectionner les énoncés du paragraphe précédent en ce qui concerne la classe des substitutions d'ordre 2.

Quand on applique le théorème I, on est, en effet, conduit à n'envisager, dans le groupe G, que les substitutions d'ordre 2. Supposons déterminées les classes des substitutions du groupe G, μ_1, μ_2, ... Les substitutions d'ordre 2 de G ne pourront avoir comme classe que ceux des nombres μ_1, μ_2, ... qui sont pairs : soient $2\lambda_1$, $2\lambda_2$, ... ces nombres.

Si, de plus, nous avons pu établir par un procédé quelconque que G ne contient que des substitutions paires, c'est-à-dire (1) équivalentes à un nombre pair de transpositions, les substitutions d'ordre 2 de G seront formées d'un nombre pair de cycles, c'est-à-dire sont de classe multiple de 4. Finalement les substitutions d'ordre 2 de G ne pourront avoir comme classe que ceux des nombres $2\lambda_1$, $2\lambda_2$, ... qui sont multiples de 4, $4\lambda_1'$, $4\lambda_2'$, ...

Cherchons à appliquer cette remarque aux groupes linéaires. D'après un théorème de M. Jordan (2), nous savons que le groupe linéaire homogène à n indices est dérivé :

1° Des substitutions

$$g = | x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n;\ x_1, \ldots, x_{i-1}, x_i + x_j;\ x_{i+1}, \ldots, x_n | \qquad (\mathrm{mod}\, m);$$

2° Des substitutions

$$g' = | x_1, \ldots, x_{n-1}, x_n;\ x_1, \ldots, x_{n-1}, cx_n | \qquad (\mathrm{mod}\, m),$$

où c est un quelconque des nombres premiers à m.

La première, g, de ces substitutions laisse invariables, exactement, les lettres pour lesquelles $x_j \equiv 0 \,(\mathrm{mod}\, m)$, en nombre m^{n-1}. Sa classe est

$$m^n - m^{n-1} = m^{n-1}(m-1).$$

Son ordre est m.

La deuxième, g', laisse invariables les lettres telles que $(c-1)x_n \equiv 0 \,(\mathrm{mod}\, m)$. Soit δ le plus grand diviseur de $c-1$ et m :

$$\frac{c-1}{\delta} x_n \equiv 0 \left(\mathrm{mod}\, \frac{m}{\delta}\right);$$

(1) SERRET, *Algèbre supérieure*, t. II, 5e édition, 1885, p. 273-277.

(2) *Traité des substitutions*, p. 93.

x_n a δ valeurs distinctes multiples de $\frac{m}{\delta}$, et la substitution g' en question laisse exactement δm^{n-1} lettres immobiles, c'est-à-dire est de classe

$$m^n - \delta m^{n-1} = m^{n-1}(m - \delta);$$

δ peut prendre ici une quelconque des valeurs des diviseurs de m qui sont $< m$.

Supposons d'abord m premier $= p$; $\delta = 1$. La classe des substitutions g, g', *génératrices* du groupe, est $p^{n-1}(p-1)$: c'est aussi (théorème III, p. 299) la classe du groupe. L'ordre de g est p, celui de g' est un des diviseurs, quelconque, δ' de $p-1$.

Si $p = 2$, cette classe, 2^{n-1}, est toujours multiple de 4 quand $n \geq 3$; $g' = 1$ et ordre de $g = 2$.

LEMME. — *Le groupe linéaire* (mod 2) *à n indices* ($n \geq 3$) *ne contient que des substitutions paires. En particulier, il ne contient pas* (1) *de substitution d'ordre* 2 *et de classe* $2^n - 2$.

Nous allons encore traiter le cas des substitutions d'ordre 2 du groupe linéaire (mod p), ($p > 2$).

Si l'on se reporte à la forme canonique des substitutions linéaires (mod p) indiquée par M. Jordan (2) et à la détermination de l'ordre d'une substitution linéaire de forme canonique donnée, on voit que les quantités $k_0, k_1, \ldots$, qui y figurent, devraient satisfaire [formule (4) de la page 127 du *Traité des substitutions* de M. Jordan] à $k_0^2 \equiv k_1^2 \equiv \ldots \equiv 1 \pmod{p}$, ce qui donne $k_0, k_1, \ldots, \equiv \pm 1 \pmod{p}$; les autres relations (4), du même Traité, étant impossibles, montrent que la forme canonique est

$$|\, y_1, \ldots, y_n;\ \varepsilon_1 y_1, \ldots, \varepsilon_n y_n \,| \qquad (\mathrm{mod}\, p)$$

où $\varepsilon_1, \ldots, \varepsilon_n$ sont égaux à ± 1. Les quantités $k_0, k_1, \ldots$, *étant réelles, on peut ramener une substitution linéaire d'ordre* 2 (mod p) *à sa forme canonique par une transformation d'indices réelle; toute substitution* (3) *linéaire d'ordre* 2 *est semblable à la substitution*

$$g'' = |\, x_1, \ldots, x_n;\ \varepsilon_1 x_1, \ldots, \varepsilon_n x_n \,| \qquad (\mathrm{mod}\, p)$$

où $\varepsilon_1, \ldots, \varepsilon_n$ *sont égaux à* ± 1.

---

(1) Ceci résulte d'ailleurs du fait que le groupe linéaire homogène à n indices (mod 2) est simple pour $n \geq 3$ (JORDAN, *Traité des substitutions*, p. 106).

(2) *Traité des substitutions*, p. 126.

(3) *Comp.* notre Thèse de Doctorat, p. 86.

Il ne nous reste plus qu'à voir dans quels cas, parmi les substitutions g'', il y a des substitutions impaires.

Si k des quantités $\varepsilon_1, \ldots, \varepsilon_n$ sont $= -1$, nous pourrons toujours supposer que ce sont les k premières, et

$$g'' = |\, x_1, \ldots, x_k, x_{k+1}, \ldots, x_n;\ -x_1, \ldots, -x_k, x_{k+1}, \ldots, x_n \,| \qquad (\mathrm{mod}\, p).$$

Cette substitution d'ordre 2 laisse immobiles exactement les lettres telles que

$$x_1 \equiv \ldots \equiv x_k \equiv 0,$$

en nombre p^{n-k}, et renferme $\frac{1}{2}(p^n - p^{n-k}) = p^{n-k}\,\frac{p^k-1}{2}$ cycles de 2 lettres. Cette substitution est de classe $p^n - p^{n-k}$ ($k = 1, 2, \ldots,$ ou n); elle sera donc impaire à la condition nécessaire et suffisante que

$$\frac{p^k-1}{2} = 2\lambda + 1, \qquad p^k - 1 \equiv 2 \qquad (\mathrm{mod}\, 4),$$

$$p^k \equiv 3 \equiv -1 \qquad (\mathrm{mod}\, 4),$$

ce qui exige k impair et $p = 4h - 1$; quand $p = 4h + 1$, au contraire, on n'a que des substitutions paires d'ordre 2.

Théorème. — *Les substitutions d'ordre* 2 *d'un groupe linéaire* (mod p) ($p > 2$) *à n indices sont paires quand* $p = 4h + 1$, *paires ou impaires quand* $p = 4h - 1$. *Il y en a de chacune des classes* $p^{n-k}(p^k - 1)$ ($k = 1, 2, \ldots,$ *ou n*).

La première partie de ce théorème peut d'ailleurs s'établir plus simplement : la substitution g' pour $c = -1$ est d'ordre 2 à $p^{n-1}\,\frac{p-1}{2}$ cycles et est impaire quand $p = 4h - 1$; d'autre part, quand $p = 4h + 1$, les seules classes possibles sont (théorème III, p. 299) multiples de 4, et les substitutions d'ordre 2 sont toutes paires.

Mais on peut appliquer au groupe linéaire homogène (mod 2) un raisonnement semblable : en effet, d'après la forme canonique des substitutions de ce groupe (*Traité des substitutions* de M. Jordan, p. 127), $k_0^2 \equiv k_1^2 \equiv \ldots \equiv 1$, $2k_0^2 \equiv 2k_1^2 \equiv \ldots \equiv 0$, les autres relations (4) de M. Jordan étant impossibles. La moitié des indices d'une substitution d'ordre 2 du groupe linéaire homogène (mod 2) au moins, doit rester invariable, c'est-à-dire a toujours la forme

$$g''' = |\, x_1, \ldots, x_n;\ x_1, x_2 + x_1, x_3, x_4 + x_3, \ldots, x_{2k-1}, x_{2k} + x_{2k-1}, x_{2k+1}, x_{2k+2}, \ldots, x_n \,| \qquad (\mathrm{mod}\, 2),$$

les indices pouvant encore être supposés réels, puisque $k_0 \equiv k_1 \equiv \ldots \equiv 1 \pmod 2$. Autrement dit (JORDAN, *Journal de Mathématiques*, 1872, p. 351-357) :

Toute substitution linéaire homogène d'ordre $2 \pmod 2$ *à n indices est semblable à la substitution*

$$g''' = | x_1, \ldots, x_n ; x_1, x_2 + x_1, \ldots, x_{2k-1}, x_{2k} + x_{2k-1}, x_{2k+1}, x_{2k+2}, \ldots, x_n | \pmod 2,$$

et de classe $2^n - 2^{n-k}\left[k = 1, 2, \ldots, \text{ou } \mathrm{E}\left(\frac{n}{2}\right)\right]$.

Cette substitution g''' laisse invariables les lettres d'indices

$$x_1 \equiv x_3 \equiv \ldots \equiv x_{2k-1} \equiv 0 \pmod 2,$$

c'est-à-dire est de classe $2^n - 2^{n-k}\left[k = 1, 2, \ldots, \mathrm{E}\left(\frac{n}{2}\right)\right]$; il existe toujours des substitutions d'ordre 2 pour chacune de ces $\mathrm{E}\left(\frac{n}{2}\right)$ valeurs de k.

Examinons encore le cas où $m = 2^\nu (\nu > 1)$, et voyons si le groupe linéaire homogène $(\mathrm{mod}\, 2^\nu)$ contient des substitutions impaires d'ordre 2, en étudiant les substitutions g et g'.

Parité de g. — g est de classe $2^{\nu(n-1)}(2^\nu - 1)$; son ordre est 2^ν. Si $x_j = 2^\varphi \xi$, où $\varphi < \nu$, ξ impair, g remplace x_i par $x_i + 2^\varphi \xi$, $x_i + 2^\varphi \xi$ par $x_i + 2 \cdot 2^\varphi \xi$, ..., $x_i + a \cdot 2^\varphi \xi$ par $x_i + (a+1) 2^\varphi \xi$, ..., c'est-à-dire que g comprend $2^{\nu(n-2)}$ cycles de $2^{\nu-\varphi}$ lettres correspondant à $x_j = 2^\varphi \xi$, et à une même valeur de x_i, d'où

$$2^{\nu(n-2)} \frac{2^{\nu-\varphi}}{2} \frac{2^\nu}{2^{\nu-\varphi}} = 2^{\nu(n-1)-1}$$

cycles de $2^{\nu-\varphi}$ lettres correspondant à l'ensemble des lettres pour lesquelles x_j est divisible par 2^φ sans l'être par $2^{\varphi+1}$. Ces cycles équivalent, comme on sait, à

$$2^{\nu(n-1)-1}(2^{\nu-\varphi} - 1)$$

transpositions.

Il est, en général, inutile de calculer à combien de transpositions équivaut g : nous savons que g est une substitution paire dès que

$$\nu(n-1) - 1 \geq 1, \qquad \nu(n-1) \geq 2,$$

ce qui a lieu dès que $n \geq 3$ ou $n = 2$, $\nu \geq 2$.

Si $n = 1$, $\nu = 2$, G est un groupe de degré 4 à un seul indice

$$|x, ax + b| \pmod 4.$$

La substitution $|x, -x| \pmod 4$ est d'ordre et de classe 2, par suite impaire.

Parité de g'. — En général, on remarquera que g' permute entre elles les lettres pour lesquelles $x_1, \ldots, x_{n-1}$ ont mêmes valeurs : si g' opère une substitution circulaire d'ordre a entre les lettres correspondant à un certain système de valeurs de $x_1, \ldots, x_{n-1}$, et aux valeurs $x_n', x_n'', \ldots, x_n^{(a)}$ de x_n, g' opère une substitution circulaire de même ordre a entre les lettres qu'on déduit de celles-là en donnant à $x_1, \ldots, x_{n-1}$ des valeurs quelconques : l'ensemble de ces substitutions circulaires équivaut alors à $(a-1)2^{\nu(n-1)}$ transpositions. Donc g' équivaut à

$$2^{\nu(n-1)} \Sigma (a-1)$$

transpositions : quand $n > 1$, ce nombre est pair, et g' est paire.

Au contraire, si $n = 1$

$$g' = |x_1, -x_1| \pmod{2^\nu}$$

est d'ordre 2 et laisse immobiles exactement les lettres telles que $x_1 \equiv -x_1 \pmod{2^\nu}$, c'est-à-dire 0, $2^{\nu-1}$; donc g' déplace $2^\nu - 2$ lettres et est une substitution impaire.

Nous conclurons ce théorème :

THÉORÈME. — *Le groupe linéaire* $\pmod{2^\nu}$ $(\nu > 1)$ *à n indices ne contient que des substitutions paires quand* $n > 1$. *Il en est différemment pour* $n = 1$.

VII.

APPLICATIONS GÉOMÉTRIQUES.

Le rapprochement du théorème I, de la remarque III du théorème II, des théorèmes III, IV et V et de leurs corollaires nous donne dès lors, de suite, un certain nombre de propriétés géométriques.

Ainsi (p. 295), le groupe de l'équation aux points d'inflexion des courbes du troisième degré est contenu dans le groupe linéaire non homogène (mod 3) à 2 indices, dont la classe est 6 (théorème III) : donc

I. — *Si un des points d'inflexion d'une cubique (à coefficients réels) est*

imaginaire, 6 ou 8 des points d'inflexion de la cubique sont imaginaires (1).

L'équation aux 4^6 cubiques ayant en trois points un contact du troisième ordre avec une quartique générale a son groupe contenu dans le groupe linéaire non homogène (mod 4) à 6 indices (p. 297). D'après le corollaire du théorème V et le théorème IV (et la page 315).

II. — *Parmi les* 4^6 *cubiques ayant en* 3 *points un contact du troisième ordre avec une quartique générale (réelle) il y en a* 0 *ou* 4^6 *ou* $4^6 - 2^{r_i}$ ($r_i = 2, 3, \ldots,$ *ou* 11) *qui sont imaginaires.*

En particulier, s'il y en a une imaginaire, $2^{11} = \frac{1}{2} 4^6$ *au moins sont imaginaires.*

L'équation aux $3^6 - 1$ systèmes de cubiques (p. 298) ayant en 4 points un contact du deuxième ordre avec une quartique générale a son groupe contenu dans le groupe linéaire homogène (mod 3) à 6 indices. Choisissant, parmi ces cubiques, celles qui ont, en particulier, un point réel déterminé de contact sur la quartique, nous déduisons des théorèmes I et III le résultat suivant :

III. — *Parmi les* $3^6 - 1$ *cubiques ayant en* 4 *points, dont un réel arbitrairement choisi, un contact du deuxième ordre avec une quartique générale (réelle), si une est imaginaire, il y en a*

$$3^6 - 3^5, \quad 3^6 - 3^4, \quad \ldots, \quad 3^6 - 3 \quad \text{ou} \quad 3^6 - 1$$

qui sont imaginaires.

En particulier, s'il y en a une imaginaire, $3^6 - 3^5 = \frac{2}{3} 3^6$ *au moins sont imaginaires.*

L'équation aux $2^6 - 1 = 63$ systèmes de coniques tangentes en 4 points à une quartique générale (p. 285 et 298) a son groupe contenu dans le groupe linéaire homogène (mod 2) à 6 indices. Raisonnant comme ci-dessus (d'après la page 314) :

IV. — *Parmi les* $2^6 - 1 = 63$ *coniques tangentes en* 4 *points, dont un réel choisi arbitrairement, à une quartique générale (réelle), si une est imaginaire,*

$$2^6 - 2^5 = 2^5 = 32, \qquad 2^6 - 2^4 = 48 \qquad \text{ou} \qquad 2^6 - 2^3 = 56$$

sont imaginaires.

---

(1) *Comparer* SERRET, *Algèbre supérieure,* t. II, 5e édition, 1885, p. 613. — SALMON, *Géométrie analytique* (*Courbes planes*), traduction Chemin, Paris, 1884, Chapitre V, en particulier Section III.

En particulier, si une est imaginaire, $2^5 = 32 = \frac{1}{2}\,2^6$ *au moins sont imaginaires.*

V. — *Parmi* (1) *les* 3^{20} *courbes du cinquième ordre ayant en* 10 *points un contact du second ordre avec une sextique générale (réelle), il y en a*

$$0,\quad 3^{20}-3^{19},\quad 3^{20}-3^{18},\quad \ldots,\quad 3^{20}-3 \quad \text{ou} \quad 3^{20}-1$$

qui sont imaginaires.

En particulier, si une est imaginaire, $3^{20}-3^{19} = \frac{2}{3}\,3^{20}$ *au moins sont imaginaires.*

VI. — *Parmi les* $4^2 = 16$ *plans* (2) *qui coupent une courbe gauche du quatrième ordre en* 4 *points consécutifs, s'il y en a d'imaginaires,* 8, 12 *ou* 16 *sont imaginaires.*

On pourrait évidemment multiplier ces exemples.

L'application du théorème I réussit encore dans des cas où il n'y a pas lieu à l'application des théorèmes II et suivants.

On sait (3) que les 16 plans tangents singuliers de la surface de Kummer dépendent d'une équation du seizième degré dont le groupe G est contenu dans le groupe linéaire non homogène de degré 16 à 4 indices (mod 2). De plus, le groupe G est dérivé de 6 substitutions (substitutions A, B, C, D, E, F de M. Jordan) toutes paires. D'après le théorème III, les substitutions d'ordre 2 de G, qui doivent être paires, par suite déplacer $4h$ lettres, ne pourront être que des classes 8, 12 ou 16.

Des propriétés semblables ont lieu pour les 16 points singuliers de la surface de Kummer : les 16 points étant 6 à 6 dans les plans tangents singuliers, on peut leur appliquer les raisonnements que M. Jordan applique aux plans tangents singuliers.

VII. — *Parmi les* 16 *plans tangents singuliers de la surface de Kummer, il y en a* 0, 8, 12 *ou* 16 *qui sont imaginaires; de même parmi les* 16 *points singuliers de cette surface.*

Il est encore intéressant d'utiliser la méthode générale indiquée au début du paragraphe V pour déterminer la classe des substitutions d'ordre 2 du groupe G

---

(1) JORDAN, *Traité des substitutions,* p. 308.

(2) *Id.,* p. 308. Le groupe correspondant contient effectivement des substitutions d'ordre 2 et de classe 8 ou 12.

(3) JORDAN, *Traité des substitutions,* p. 313.

qui contient celui de l'équation aux 27 droites des surfaces du troisième degré, et est dérivé des substitutions A, B, C, D, E, F de M. Jordan (*Traité*, p. 316).

G est transitif entre les 27 lettres a, b, c, d, e, f, g, h, i, k, l, m, n, p, q, r, s, t, u, m', n', p', q', r', s', t', u'. Les catégories (10) se réduisent à une. Il suffit de déterminer la classe de H_a.

H_a permute transitivement entre elles, d'une part,

$$b, \quad c, \quad d, \quad e, \quad f, \quad g, \quad h, \quad i, \quad k, \quad l,$$

c'est-à-dire les 10 lettres qui figurent avec a dans un même trio du Tableau des 45 triangles (1), d'autre part les 16 autres lettres de G,

$$m, \quad n, \quad p, \quad \ldots, \quad u',$$

comme on le vérifie en considérant successivement les 15 substitutions

$$\begin{array}{llll}
\mathrm{DECD^2} = (mn \ldots)\ldots, & & \mathrm{DECB} = (mn' \ldots)\ldots, \\
\mathrm{DE} = (mp \ldots)\ldots, & & \mathrm{D^2B} = (mp' \ldots)\ldots, \\
\mathrm{DC^2} = (mq \ldots)\ldots, & & \mathrm{DECBDE} = (mq' \ldots)\ldots, \\
\mathrm{D^2} = (mr \ldots)\ldots, & & \mathrm{DEB^2} = (mr' \ldots)\ldots, \\
\mathrm{DEC^2} = (ms \ldots)\ldots, & & \mathrm{DECBD^2} = (ms' \ldots)\ldots, \\
\mathrm{D} = (mt \ldots)\ldots, & & \mathrm{DEB} = (mt' \ldots)\ldots, \\
\mathrm{DEC} = (mu \ldots)\ldots, & & \mathrm{DECBD} = (mu' \ldots)\ldots. \\
\mathrm{DEB^2D} = (mm' \ldots)\ldots, & &
\end{array}$$

Pour déterminer la classe de H_a, il suffira de déterminer celle des groupes H_{ab} et H_{am}.

Premier cas : *Groupe* H_{ab}. — *abc* est laissé immobile par H_{ab}, en sorte que $H_{ab} = H_{abc}$ ($H_{\alpha_1\alpha_2\alpha_3\ldots}$ est le groupe des substitutions de G qui laissent α_1, α_2, α_3, ... immobiles). L'ordre $\mathfrak{H}_{ab}$ de H_{ab} est

$$\frac{\mathrm{G}}{27.10} = 8.24.$$

H_{abc} peut déplacer une quelconque des 24 autres lettres. H_a permutant exclusivement entre elles b, c, ..., l d'une part, m, n, ..., u' d'autre part, il en est de même de H_{abc}.

---

(1) Le dixième triangle du Tableau de M. Jordan est $cm'n'$ et non $cm'n$.

H_{abc} permute transitivement

$$d,\ h,\ k,\ g,\ f,\ i,\ l,\ e,$$

comme le montrent les substitutions C, D, E, ED, DC. De même, il permute transitivement m, n, ..., u d'une part, m', n', ..., u' d'autre part.

Les catégories (10) correspondant à H_{abc} seront alors représentées ici par les groupes

$$H_{abcd},\quad H_{abcm},\quad H_{abcm'}.$$

D'où 3 sous-cas à distinguer.

Premier sous-cas : H_{abcd}. — Comme l'a montré M. Jordan, et comme on le voit de suite,

$$H_{abcd} = H_{abcde}$$

et

$$\mathcal{H}_{abcde} = \frac{8.24}{8} = 24.$$

Opérons sur H_{abcde} comme nous l'avons déjà fait sur G et ses sous-groupes : H_{abcde} contient D, E, F, et en est évidemment dérivé, car on vérifie que le groupe dérivé des substitutions opérées par D, E, F entre m, p, r, t est le groupe symétrique de 4 éléments.

Formons les catégories analogues à (10). H_{abcde} permute transitivement

$$\begin{gathered} f,\ g,\ h,\ i,\ k,\ l; \\ m,\ p,\ r,\ t; \\ m',\ p',\ r',\ t'; \\ n,\ q,\ s,\ u; \\ n',\ q',\ s',\ u'. \end{gathered}$$

Il suffit de considérer les sous-groupes suivants :

H_{abcdef}, d'ordre 4, qui contient F et DEDF de classe 12, DED de classe 20, et est de classe 12; H_{abcdem}, d'ordre 6, dérivé de E et F, et dont la classe est évidemment 12;

$$H_{abcdem'} = H_{abcdem} = H_{abcden} = H_{abcden'}.$$

Deuxième sous-cas : $H_{abcm} = H_{abcmn}$. — Il est encore d'ordre 24, et contient les substitutions C, E, F dont il est dérivé.

Formons les catégories analogues à (10). H_{abcmn} permute transitivement

$$d,\ h,\ k,\ f;$$
$$e,\ i,\ l,\ g;$$
$$p,\ q,\ r,\ s,\ t,\ u;$$
$$m',\ s',\ u',\ q';$$
$$n',\ r',\ t',\ p'.$$

Appliquant la condition (A) (p. 299), nous n'avons à considérer que

$$H_{abcmnu} \quad \text{d'ordre } 4,$$
$$H_{abcmnm'} \quad \text{d'ordre } 6$$

ou

$$H_{abcmnn'} \quad \text{d'ordre } 6.$$

$H_{abcmnm'}$ est dérivé de E et F et contient 1, E, E^2, F, $E^{-1}FE$, $E^{-2}FE^2$; sa classe est 12 :

$$H_{abcmnn'} = H_{abcmnm'}.$$

Enfin H_{abcmnu} laisse t immobile, et contient

$$CE = (dk)(hf)(el)(ig)(m'u')(s'q')(pq)(rs)(n't')(p'r') \quad \text{de classe 20,}$$
$$C^{-1}FC = (dk)(el)(t'n')(m'u')(qr)(ps)$$

et

$$CE.C^{-1}FC = (fh)(gi)(q's')(p'r')(pr)(qs) = EFE^{-1}.$$

H_{abcmnu} est de classe 12.

Troisième sous-cas : $H_{abcm'} = H_{abcm'n'}$. — Il est encore d'ordre 24 et contient E et F. $H_{abcm'}$ contient également

$$K = (gd)(hk)(il)(ef)(np)(su)(mq)(rt)(r's')(t'u'),$$

par suite,

$$K^{-1}EK = (ekh)(dli)(ntr)(mus)(p's'u')(q'r't').$$

Nous considérerons le sous-groupe de celles des substitutions de $H_{abcm'n'}$ qui laissent une autre lettre immobile.

Si cette lettre est une des lettres d, e, f, g, h, i, k, l, le sous-groupe correspondant est semblable à un sous-groupe de H_{abcd}; on applique la condition (A) (p. 299). Si c'est une des lettres m, n, p, q, r, s, t, u, le sous-groupe correspondant est semblable à un sous-groupe de H_{abcm}; on applique encore la condition (A). Il suffit de considérer le cas où c'est une des lettres p', q', r', s', t', u'.

Ces 6 lettres appartiennent certainement à une même catégorie, puisqu'elles sont permutées transitivement ensemble par E, $K^{-1}EK$ et leurs dérivées. Il suffira donc de considérer $H_{abcm'n'p'} = H_{abcm'n'p'q'}$, qui contient F, mais non E, et permute exclusivement entre elles r', s', t', u'. $H_{abcm'n'p'q'}$ est d'ordre 4, et contient F et K. D'ailleurs,

$$KF = (dg)(ef)(np)(mq)(r'u')(s't').$$

Donc $H_{abcm'n'p'q'}$ est de classe 12.

Deuxième cas : *Groupe* H_{am},

$$\mathcal{H}_{am} = \frac{27.10.8.24}{27.16} = 5.24.$$

Nous diviserons les lettres déplacées par H_{am} en catégories analogues à (10) : les lettres b, c, ..., l qui figurent dans les trios où entre a sont permutées exclusivement entre elles par H_{am}; elles forment une ou plusieurs de ces catégories. Il est inutile de les considérer, car H_{adm}, par exemple, est un sous-groupe de H_{ad}, semblable au groupe H_{ab} déjà étudié [condition (A)].

H_{am} est dérivé de C, E, F, B; en effet, C, E, F, B permutent exclusivement entre elles n, q', s', u', m'; C, E, F et leurs dérivées opèrent entre m', q', s', u' les substitutions du groupe symétrique de 4 éléments. Donc C, E, F, B et leurs dérivées opèrent entre n, m', q', s', u' les substitutions du groupe symétrique de 5 éléments. Il en résulte que les 15 lettres de G autres que a, b, ..., l et m se répartissent en 2 catégories analogues à (10) comme il suit :

$$n,\ m',\ q',\ s',\ u',$$
$$p,\ q,\ r,\ s,\ t,\ u,\ n',\ p',\ r',\ t'.$$

Nous avons à considérer les 2 sous-groupes

$$H_{amn},\quad H_{amq}.$$

Premier sous-cas : $H_{amn} = H_{abnm}$ est contenu dans H_{ab}; il suffit d'appliquer la condition (A).

Deuxième sous-cas : H_{amq}. — Ce groupe, d'ordre 12, contient

$$B,\ F \quad \text{et} \quad E^{-1}C^{-1}FCE = (df)(eg)(n'p')(m'q')(ru)(st),$$

qui permutent entre elles transitivement

$$p,\ r',\ t' \qquad \text{d'une part,}$$
$$n',\ p',\ r,\ s,\ t,\ u \qquad \text{d'autre part,}$$

H_{amq} est dérivé de ces 3 substitutions, car $H_{amqp'}$ contient F et est d'ordre 2. Nous n'avons d'ailleurs à répartir en catégories que les 9 lettres précédentes.

Il suffit de considérer

$$H_{amqp} \quad \text{et} \quad H_{amqp'}.$$

$H_{amqp} = H_{amqpb}$ et est contenu dans H_{ab}; la condition (A) s'applique.

$H_{amqp'}$ se réduit aux substitutions 1 et F et est de classe 12.

Tous les cas sont ainsi épuisés, et nous voyons que la classe du groupe G de l'équation aux 27 droites des surfaces du troisième degré est 12.

Mais on peut aussi déterminer les classes des substitutions d'ordre 2 contenues dans ce groupe G. D'abord G ne contient que des substitutions dérivées de A, B, C, D, E, F qui sont paires : ses substitutions d'ordre 2 auront leur classe multiple de 4 et déplaceront 12, 16, 20 ou 24 lettres. Nous avons rencontré une substitution d'ordre 2 et de classe 20 (p. 319); mais nous allons voir qu'il n'y a pas de classe 16.

S'il y avait une substitution de classe 16 et d'ordre 2, il y en aurait une dans le groupe H_a, par suite dans $H_{ab} = H_{abc}$, ou H_{am}.

1° Si c'était dans H_{abc}, il y en aurait une dans

$$H_{abcd} = H_{abcde}, \qquad H_{abcm} = H_{abcmn} \qquad \text{ou} \qquad H_{abcm'} = H_{abcm'n'}.$$

Si c'était dans H_{abcde}, ce groupe est dérivé de D, E, F, et déplace exactement 22 lettres; donc il y aurait une substitution de classe 16 dans H_{abcdef}, ce qui n'est pas, ou dans H_{abcdem} dérivé de E et de F, ce qui n'est pas.

Si c'était dans H_{abcmn}, ce groupe est dérivé de C, E, F et déplace exactement 22 lettres; donc il y aurait une substitution de classe 16 dans H_{abcmnu} dont les substitutions sont de classe 12 et 20, ou dans $H_{abcmnm'} = H_{abcmnn'}$ dérivé de E et F et dont les substitutions d'ordre 2 sont de classe 12.

Si c'était dans $H_{abcm'n'}$, ce groupe est dérivé de E, F et $K^{-1}EK$ et déplace encore exactement 22 lettres; donc il y aurait une substitution d'ordre 16 dans $H_{abcm'n'p'}$ dont les substitutions sont de classe 12 et 20.

Finalement H_{abc} ne contient pas de substitution de classe 16.

2° Si H_{am} en contenait une, il y en aurait une dans H_{amq}, dérivé de B, F et $E^{-1}C^{-1}FCE$, et qui déplace 24 lettres. Il y en aurait donc une dans $H_{amqp'}$ qui ne contient qu'une substitution de classe 12. H_{am} ne contient pas de substitution de classe 16.

Finalement G ne contient pas de substitution de classe 16, et nous obtenons, grâce au théorème I, ce résultat :

VIII. — *Le groupe de l'équation aux 27 droites des surfaces du troisième*

degré est de classe 12; *ses substitutions d'ordre* 2 *déplacent* 24, 20 *ou* 12 *lettres. Cette équation possède* 3, 7, 15 *ou* 27 *racines réelles.*

Parmi les 27 *droites d'une surface du troisième degré, si* α *sont réelles,* α *est un des nombres* 3, 7, 15 *ou* 27 (1).

Ce qui précède va encore nous donner une application dans la théorie des courbes du quatrième degré (c'est-à-dire des quartiques). On sait que ces courbes possèdent en général 28 tangentes doubles; le groupe G_2 de l'équation déterminant ces 28 tangentes est contenu dans un groupe Γ, dont le sous-groupe H formé des substitutions laissant une même lettre immobile coïncide avec le groupe de G de l'équation aux 27 droites des surfaces du troisième degré. Γ est donc de classe 12, et ses substitutions d'ordre 2 déplacent 12, 20, 24 ou 28 lettres.

IX. — *Le groupe de l'équation aux* 28 *tangentes doubles des quartiques générales est de classe* 12; *ses substitutions d'ordre* 2 *déplacent* 28, 24, 20 *ou* 12 *lettres.*

Cette équation possède 0, 4, 8, 16 *ou* 28 *racines réelles.*

Parmi les 28 *tangentes doubles des quartiques générales, si* α *sont réelles,* α *est un des nombres* 0, 4, 8, 16 *ou* 28 (2).

On peut songer encore à faire application du théorème I à d'autres problèmes de contact, étudiés par Clebsch et à des équations corrélatives envisagées par M. Jordan (*Traité,* p. 329-333). Ces groupes sont :

1° Les deux groupes de Steiner, dont nous venons d'étudier un cas particulier (groupe de l'équation aux 28 tangentes doubles des quartiques générales);

2° D'autres groupes non linéaires (*Traité,* p. 331).

Ce qui précède pose le problème de la détermination de la classe de ces groupes et de celles des substitutions d'ordre 2 qui y sont contenues.

Nous nous contenterons de remarquer à ce sujet que le premier groupe $G^{(n)}$ de Steiner à $2n$ indices est dérivé (*Traité,* p. 231) de substitutions d'ordre 2 et de classe $2\mathfrak{R}_{n-1}$, où

$$\mathfrak{R}_n = 2^{2n-1} - 2^{n-1}.$$

Ces substitutions sont paires dès que

$$\mathfrak{R}_{n-1} = 2^{2n-3} - 2^{n-2} \equiv 0 \pmod 2,$$

(1) Comparer, par exemple, D'OCAGNE, *Nouvelles Annales,* 1895, p. 339 et suivantes. — L. LÉVY, *id.,* p. 334 et suivantes.

(2) D'après SALMON, *Géométrie analytique* (*courbes planes*), traduction Chemin, Paris, 1884, p. 312, Zeuthen a montré qu'une quartique peut posséder exactement 4, 8, 16 ou 28 bitangentes réelles (*Math. Ann.,* t. VII, p. 411). Il resterait à voir si le groupe de l'équation contient des substitutions d'ordre 2 et de classe 28.

c'est-à-dire $n \geq 3$. Il en sera, *a fortiori*, de même pour le second groupe de Steiner $G_1^{(n)}$ qui est contenu dans $G^{(n)}$. Donc :

X. — *Les deux groupes de Steiner à 2 n indices, de degré* $\mathfrak{R}_n = 2^{2n-1} - 2^{n-1}$, *ne contiennent que des substitutions paires, quand* $n \geq 3$. *Une équation de même degré, dont le groupe est contenu dans un de ces groupes, a* $4h$ *racines imaginaires* (h *entier*).

Le théorème II est susceptible d'extensions au cas où la quantité r (p. 286) n'est pas un nombre premier, ni une puissance de nombre premier. Nous allons le vérifier sur un cas particulier.

On sait que les points (1) où une conique a avec une cubique générale un contact du cinquième ordre sont déterminés par

$$u = \frac{2P + x_1\omega_1 + x_2\omega_2}{6}, \tag{25}$$

ω_1 et ω_2 étant les périodes d'une fonction elliptique de paramètre u dépendant de la cubique, et x_1, x_2 des entiers prenant les valeurs 0, 1, 2, 3, 4, 5. Quand x_1, x_2 sont pairs simultanément, on obtient les points d'inflexion, au nombre de 9. Sur les 36 points (25), il y en a véritablement 27 de surosculation par une conique. Les 36 points dépendent d'une équation $X = 0$ du trente-sixième degré.

La condition nécessaire et suffisante pour que trois de ces points soient en ligne droite est que

$$x + x_1'' + x_1''' \equiv x_2' + x_2'' + x_2''' \equiv 0 \pmod 6. \tag{26}$$

Par exemple, les points d'inflexion pris 3 à 3 constituent un cas particulier des solutions de ces congruences; de même que les trois points de surosculation qui sont les points de contact des 3 tangentes issues d'un point d'inflexion. Le groupe G de $X = 0$ est contenu dans le groupe Γ entre les 36 lettres $(x_1, x_2) \pmod 6$ dont les substitutions laissent invariable l'ensemble des solutions de ces congruences (2). D'après ce que nous avons vu (p. 286), le groupe Γ contient : 1° les

(1) JORDAN, *Cours lithographié d'Analyse de l'Ecole Polytechnique*, I^re^ division. — APPELL et GOURSAT, *Fonctions algébriques*, p. 490. — SERRET, *Algèbre supérieure*, t. II, 5^e^ édition, 1885, p. 624.

(2) Les seuls cas analogues traités par M. Jordan sont ceux où le module est premier ou une puissance de nombre premier, et sont compris comme cas particulier dans notre théorème II.

substitutions

$$(27) \qquad |x_1, x_2;\ x_1+\alpha_1, x_2+\alpha_2| \qquad (\text{mod } 6),$$

telles que α_1, α_2 soient des nombres pairs quelconques (mod 6), puisque le plus grand commun diviseur de $r_1 = 3$ et $r = 6$ est 3, substitutions qui forment un groupe G'_1 d'ordre 9; 2° les substitutions

$$(28) \qquad |x_1, x_2;\ a_1^1 x_1 + a_1^2 x_2,\ a_2^1 x_1 + a_2^2 x_2| \qquad (\text{mod } 6),$$

qui forment un groupe G''_1. L'ordre de G''_1 est (1) $\Omega(6^2) = (6, 2)6(6, 1) = 24.6.2$. Ces 2 catégories de substitutions permutent entre elles les 9 lettres dont les 2 indices sont pairs.

Je dis que Γ ne contient pas d'autres substitutions que celles dérivées de G'_1 et G''_1.

Considérons une substitution S de Γ qui ne laisse aucune lettre immobile, et faisons dans (26)

$$x'_1 = x''_1 = x'''_1, \qquad x'_2 = x''_2 = x'''_2,$$

$$(29) \qquad 3x'_1 \equiv 3x'_2 \equiv 0 \qquad (\text{mod } 6).$$

On obtient 9 solutions correspondant aux 9 systèmes de valeurs paires de x_1 et x_2, c'est-à-dire aux points d'inflexion; la droite définie par les 3 points identiques satisfaisant à (29) est la tangente d'inflexion; Γ remplace une solution de (29) par une autre solution, c'est-à-dire permute entre eux ces 9 points, par suite, les 27 autres des 36 points solutions de $X = 0$.

S remplace un de ces 9 points (2) a_{00} par un autre de ces 9 points $a_{x'_1 x'_2}$; mais, parmi les substitutions (27), il y a une substitution Σ remplaçant a_{00} par $a_{\alpha_1 \alpha^2}$, avec $\alpha_1 = x'_1$, $\alpha_2 = x'_2$. Donc $S\Sigma^{-1}$ laisse a_{00} invariable et appartient au sous-groupe H de Γ laissant a_{00} invariable.

Soit S_1 une substitution de H. Faisons dans (26)

$$x'''_1 \equiv x'''_2 \equiv 0, \qquad x'_1 \equiv x''_1, \qquad x'_2 \equiv x''_2 \qquad (\text{mod } 6) :$$

(26) devient

$$2x'_1 \equiv 2x''_2 \equiv 0 \qquad (\text{mod } 6).$$

---

(1) JORDAN, *Traité des substitutions*, p. 96, où l'on trouvera la signification du symbole (m, ρ), indiquée d'ailleurs plus haut, p. 304 :

$$(6, \rho) = 6\rho\left(1 - \frac{1}{2\rho}\right)\left(1 - \frac{1}{3\rho}\right).$$

(2) Nous désignerons, en général, ici le point d'indice x_1, x_2 par $a_{x_1 x_2}$.

S_1, qui laisse a_{00} immobile, permute entre elles les solutions de cette congruence, c'est-à-dire les lettres dont les indices sont tous deux multiples de 3; géométriquement, les points solutions $a_{x_1' x_1''}$ (autres que a_{00}) sont les points de contact des tangentes issues de a_{00} à la cubique; les 3 droites correspondantes sont ces tangentes, que S_1 permute entre elles.

Ceci posé, S_1 remplace a_{10} par une lettre $a_{\xi_1 \xi_2}$ dont les indices ont leur plus grand commun diviseur premier à 6. Mais, parmi les substitutions (28), il existe une substitution Σ_1 jouissant de cette propriété : il suffit, en effet, de prendre $a_1^1 \equiv \xi_1$, $a_2^1 \equiv \xi_2$, $\xi_1 a_2^2 - \xi_2 a_1^2 \equiv \pm 1 \pmod 6$: l'équation $\xi_1 a_2^2 - \xi_2 a_1^2 = 1$ ($|\xi_1|, |\xi_2| \leq 3$), et, *a fortiori*, la congruence $\xi_1 a_2^2 - \xi_2 a_1^2 \equiv 1 \pmod 6$, possèdent toujours une solution a_2^2, a_1^2. Alors $S_2 = S_1 \Sigma_1^{-1}$ laisse a_{10} immobile; de plus, d'après

$$0 + 1 - 1 \equiv 1 + 1 - 2 \equiv 0 + 2 - 2 \equiv 2 + 1 - 3 \pmod 6, \tag{30}$$

cette substitution laisse $a_{x_1 0}$ immobile quel que soit x_1.

Les substitutions (28) qui laissent $a_{x_1 0}$ immobile sont telles que $a_1^1 \equiv 1$, $a_2^1 \equiv 0$, c'est-à-dire de la forme

$$\Sigma_2 = | x_1, x_2;\ x_1 + a_1^2 x_2,\ a_2^2 x_2 | \qquad \pmod 6 \qquad a_2^2 \equiv \pm 1;$$

elles remplacent a_{01} par $a_{a_1^2 a_2^2}$, où $a_2^2 = \pm 1$.

Considérons S_2 : S_2 permute entre elles les lettres dont les indices sont divisibles tous deux par 2 ou 3, et laisse $a_{x_1 0}$ immobile, par suite remplace a_{01} par $a_{\xi_1 \xi_2}$; si ξ_2 n'est pas premier à 6, S_2, qui laisse a_{00} immobile, remplace, d'après (30), $a_{0 x_2}$ par 6 lettres $a_{\xi_1' \xi_2'}$, telles que ξ_2' a, avec 6, un commun diviseur > 1. D'après

$$-x_1' + 0 + x_1' \equiv 0 - x_2 + x_2' \equiv 0, \tag{31}$$

on voit qu'il en serait de même de $a_{x_1' x_2'}$, puisque S_2 laisse $a_{-x_1' 0}$ immobile. Ce résultat est absurde; donc S_2 remplace, comme Σ_2, a_{01} par $a_{\xi_1 \xi_2}$, où $\xi_2 = \pm 1$. On peut donc trouver Σ_2 telle que $S_3 = S_2 \Sigma_2^{-1}$ laisse a_{01} immobile. D'après (30), S_3 laisse $a_{0 x_2}$ immobile, comme aussi $a_{x_1 0}$; d'après (31), S_3 laisse $a_{x_1' x_2'}$ immobile, quels que soient x_1', x_2', et se réduit à 1. Donc :

Le groupe Γ *est dérivé des substitutions* (27) *et* (28). Il permute entre eux les 27 points où les 2 indices ne sont pas pairs à la fois, et l'équation de degré 36 précitée, réductible, se décompose en 2 : une de degré 9 aux abscisses des points d'inflexion, une de degré 27 donnant les 27 autres points. Dès lors :

Théorème. — *Le groupe de l'équation aux 27 points (autres que les points d'inflexion), où une cubique générale possède un contact du cinquième ordre avec une conique, est contenu dans le groupe* Γ_1 *des substitutions que le*

groupe Γ *dérivé du groupe* G_1' *des substitutions*

$$|x_1, x_2;\ x_1+\alpha_1, x_2+\alpha_2| \qquad (\text{mod } 6)$$

[α_1, α_2 *pairs* (mod 6)], *et du groupe* G_1'' *des substitutions*

$$|x_1, x_2;\ a_1^1 x_1 + a_1^2 x_2,\ a_2^1 x_1 + a_2^2 x_2| \qquad (\text{mod } 6)$$

opère entre les 27 *lettres* $a_{x_1 x_2}$ *dont un des indices est impair.*

Il nous reste à trouver la classe de Γ_1 et la classe de ses substitutions d'ordre 2.

Γ_1 est transitif entre ses 27 lettres a_{x_1, x_2} telles que x_1, x_2 ne sont pas pairs à la fois. En effet, il contient la substitution

$$|x_1, x_2;\ a_1^1 x_1 + a_1^2 x_2 + \alpha_1,\ a_2^1 x_1 + a_2^2 x_2 + \alpha_2| \qquad (\text{mod } 6),$$

où α_1, α_2 sont pairs à la fois, substitution qui remplace a_{10} par la lettre arbitraire $a_{\xi_1 \xi_2}$, avec $\xi_1 = a_1^1 + \alpha_1$, $\xi_2 = a_2^1 + \alpha_2$, $a_1^1 a_2^2 - a_2^1 a_1^2 \equiv \pm 1$. ξ_1 ou ξ_2 est impair; si, par exemple, c'est ξ_1, on prend α_1 tel que a_1^1 soit $= \pm 1$; puis $a_1^2 = 0$, $a_2^2 = 1$, $a_2^1 = \xi_2 - \alpha_2$, et l'on obtient bien une substitution remplaçant a_{01} par $a_{\xi_1 \xi_2}$.

Appliquons encore la méthode générale (p. 298) pour la détermination de la classe des substitutions d'un groupe; il suffit de considérer le groupe H des substitutions de Γ_1, laissant a_{30} immobile : les substitutions de H sont telles que

$$3a_1^1 + \alpha_1 \equiv 3, \qquad 3a_2^1 + \alpha_2 \equiv 0 \qquad (\text{mod } 6);$$

α_1, α_2 sont divisibles par 2 et 3, par suite nuls. On a

$$3(a_1^1 - 1) \equiv 0, \qquad 3a_2^1 \equiv 0;$$

a_1^1 est impair quelconque, a_2^1 pair quelconque; les substitutions de H sont de la forme

$$S' = |x_1, x_2;\ a_1^1 x_1 + a_1^2 x_2,\ a_2^1 x_1 + a_2^2 x_2| \qquad (\text{mod } 6)$$

avec $a_1^1 a_2^2 - a_1^2 a_2^1 \equiv \pm 1$ (mod 6); a_2^2 est impair.

Formons les catégories correspondantes : H contient les substitutions [1] (mod 6)

$$T = |x_1, x_2;\ x_1 + x_2,\ 2x_1 + x_2| \quad \text{d'ordre 8,}$$
$$T_1 = |x_1, x_2;\ x_1 + x_2,\ 2x_1 + 3x_2| \quad \text{d'ordre 6,}$$
$$T_2 = |x_1, x_2;\ x_1 + x_2,\ x_2| \quad \text{d'ordre 6,}$$
$$T_3 = |x_1, x_2;\ x_1 - x_2,\ -x_2| \quad \text{d'ordre 2,}$$
$$T_4 = |x_1, x_2;\ x_1,\ 2x_1 + x_2| \quad \text{d'ordre 3,}$$
$$T_5 = |x_1, x_2;\ -x_1,\ x_2| \quad \text{d'ordre 2.}$$

---

[1] Nous prions le lecteur de former, en cas de besoin, les substitutions correspondantes entre les $a_{x_1 x_2}$.

T et T_1 permutent a_{10} transitivement avec 8 lettres au moins; T_2, T_3 laissent a_{10} immobile, et le groupe dérivé de T_2, T_3 est formé des substitutions de H

$$S'' = |\, x_1, x_2;\ x_1 + a_1^2 x_2, \pm x_2 \,| \qquad (\mathrm{mod}\, 6)$$

(a_1^2 quelconque) au nombre de 12, qui laissent a_{10} immobile : c'est le groupe $H_{a_{10}}$. La catégorie représentée par a_{10} comprend alors 8 lettres, puisque ordre $H = \mathfrak{H} = 96$.

T et T_1 permutent transitivement a_{01} avec 16 lettres au moins; T_4, T_5 laissent a_{01} immobile, et le groupe dérivé de T_4, T_5 est d'ordre 6 et formé des substitutions de H,

$$S_1'' = |\, x_1, x_2;\ \pm x_1, 2kx_1 + x_2 \,| \qquad (\mathrm{mod}\, 6)$$

($k = 0$, 1 ou 2), au nombre de 6 : c'est le groupe $H_{a_{01}}$. La catégorie représentée par a_{01} comprend 16 lettres.

Enfin la catégorie représentée par a_{03} comprend a_{03} et a_{33}.

Une substitution de H déplace 26 lettres (cas de la substitution T_1^3 d'ordre 2), ou appartient à $H_{a_{10}}$, $H_{a_{01}}$, $H_{a_{03}}$.

Au lieu de continuer à former les catégories (10), il sera plus simple d'étudier directement les substitutions de ces trois groupes.

$H_{a_{10}}$. — S'' laisse $a_{x_1 x_2}$ immobile si

$$a_1^2 x_2 \equiv 0, \qquad x_2 \equiv \pm x_2.$$

Avec le signe +, $a_1^2 \not\equiv 0$, et l'on obtient 6, 12 ou 18 lettres laissées immobiles, $a_{x_1 0}$, ou $a_{x_1 0}$ et $a_{x_1 3}$, ou $a_{x_1 0}$, $a_{x_1 2}$ et $a_{x_1 4}$. Avec le signe —, $x_2 = 0$ ou 3, et l'on obtient 6 ou 12 lettres laissées immobiles, $a_{x_1 0}$, ou $a_{x_1 0}$ et $a_{x_1 3}$.

Il faut négliger, parmi elles, celles dont les 2 indices sont pairs, au nombre de 3, 3 ou 9; on obtient ainsi 3 ou 9 lettres laissées immobiles, sur 27 : les substitutions de $H_{a_{10}}$ sont de classe 24 (exemple T_3), ou 18.

$H_{a_{01}}$. — S_1'' laisse $a_{x_1 x_2}$ immobile si

$$x_1 \equiv \pm x_1, \qquad 2kx_1 \equiv 0 \qquad (k = 0, 1 \text{ ou } 2).$$

Avec le signe +, $k \not\equiv 0$, $x_1 = 0$ ou 3; les lettres laissées immobiles sont $(0, x_2)$, $(3, x_2)$. Avec le signe —, on a les mêmes lettres : parmi les 27 lettres de Γ_1, il en reste 9 laissées immobiles, et les substitutions de $H_{a_{01}}$ sont de classe 18 (exemple T_5).

$H_{a_{03}}$. — Une substitution de ce groupe est de classe 24, ou laisse une autre lettre immobile, c'est-à-dire est semblable à une lettre de $H_{a_{10}}$ ou $H_{a_{01}}$. Donc :

Corollaire I. — *Le groupe de l'équation aux 27 points (autres que les points*

d'inflexion) *où une cubique générale a un contact du cinquième ordre avec une conique est de classe* 18; *ses substitutions déplacent* 27, 26, 24 *ou* 18 *lettres. Cette équation possède* 27, 9, 3 *ou* 1 *racines réelles.*

Parmi ces 27 *points de surosculation, si* α *sont réels,* α *est* (1) *un des nombres* 1, 3, 9 *ou* 27.

On sait que l'équation en question est résoluble par radicaux : cela pourrait aussi se déduire de l'étude (2) des facteurs de composition de Γ.

On peut encore le voir directement : Γ opère entre les abscisses des 9 points d'inflexion les substitutions du groupe linéaire $g \pmod 3$ à 2 indices, d'ordre 9.8.6. Γ contient donc un sous-groupe invariant d'ordre 6 laissant les abscisses de ces 9 points immobiles. Γ est alors composé avec ce groupe d'ordre 6 (ou un isomorphe holoédrique de ce groupe) qui est résoluble, et le groupe g qui l'est aussi. Donc (3) Γ et tout groupe qu'il contient (4) sont résolubles.

APPLICATION AUX CONSTRUCTIONS QUE L'ON PEUT EFFECTUER AVEC LA RÈGLE, OU PAR LA RÈGLE ET LE COMPAS.

Étant donnée l'équation $X = 0$ de degré d, si l'on peut résoudre complètement l'équation en lui adjoignant (5) quelques-unes de ses racines $x_1, x_2, \ldots, x_\delta$ convenablement choisies, les autres racines sont des fonctions rationnelles de $x_1, x_2, \ldots x_\delta$, que l'on sait, dès lors, construire géométriquement avec *la règle seule* (6). La connaissance du groupe de $X = 0$ ou d'un groupe Γ le contenant permettra de fixer la valeur exacte ou une limite supérieure de δ.

Exemples. — Pour résoudre une équation dont le groupe est contenu dans le groupe linéaire général non homogène à q indices $\pmod r$ (r premier), il suffit de

---

(1) On sait (SALMON, *loc. cit.*, p. 160. — SERRET, *loc. cit.*, p. 613) qu'une cubique générale a au plus 3 points d'inflexion réels. La tangente en un point de surosculation réel passant par un point d'inflexion réel, on voit que, en réalité, $\alpha \neq 27$.

(2) Il suffit de s'appuyer sur la théorie générale des facteurs de composition du groupe linéaire (JORDAN, *Traité*, p. 99).

(3) JORDAN, *Traité*, p. 395.

(4) *Ibid.*, p. 387.

(5) Pour le sens de ce mot, *voir* JORDAN, *Traité*, p. 253.

(6) On sait, en effet, construire le produit $\alpha\beta$ et le quotient $\frac{\alpha}{\beta}$ à l'aide de la règle seule, par suite une fonction rationnelle quelconque des quantités connues et adjointes. De même les radicaux carrés se construisent à l'aide de la règle et du compas (*voir*, par exemple, PRUVOST, *Géométrie analytique*, t. I, 1888, p. 10).

connaître les racines

$$(0, 0, \ldots, 0), \quad (1, 0, \ldots, 0), \quad (0, 1, 0, \ldots, 0), \quad \ldots, \quad (0, \ldots, 0, 1),$$

dont un seul indice est $\not\equiv 0$ et $\equiv 1 \pmod r$, au nombre de $q+1$. Donc ici $\delta \leqq q+1$. Si ce groupe coïncide avec le groupe linéaire général non homogène ou homogène, en vertu du théorème III, $\delta = q+1$ ou q respectivement.

La connaissance de 3 points d'inflexion convenablement choisis d'une courbe du troisième degré suffit pour construire les autres par la règle seule.

En général, d'ailleurs, quand on adjoint $d-1$ racines de $X=0$, la $d^{\text{ième}}$ racine est déterminée rationnellement. Si u est la classe du groupe de $X=0$, la connaissance de $d-u$ racines détermine les autres rationnellement.

Application. — Connaissant $mn-1$ des points d'intersection de 2 courbes de degré m et n, le $mn^{\text{ième}}$ peut être construit à l'aide de la règle seule.

Dans certains cas, la considération du groupe Γ permettra encore de dire combien il faut connaître au minimum de racines pour construire les autres à l'aide *de la règle et du compas.*

Soit Δ une fonction alternée : elle est susceptible de 2 valeurs au plus, et dépend d'une équation du second degré au plus, à coefficients rationnels; on peut la construire par la règle et le compas. En l'adjoignant à $X=0$, on réduit le groupe Γ aux substitutions de Γ qui sont contenues dans le groupe alterné, et forment un groupe Γ'. Adjoignons alors à $X=0$, Δ et $d-2$ racines de X : le groupe de $X=0$ se réduit à l'unité. La connaissance de $d-2$ racines permet donc de construire les autres par la règle et le compas. Ainsi : quand on connaît $mn-2$ des points d'intersection de 2 courbes de degré m et n, on peut construire les 2 autres par la règle et le compas; quand on connaît 7 points de l'intersection de 2 cubiques, les 2 derniers peuvent se construire par la règle et le compas.

D'ailleurs, ces résultats relatifs aux constructions par la règle ou par la règle et le compas sont plus ou moins connus, ou sont des conséquences du Livre III du *Traité des substitutions* de M. Jordan.

Mais *nous allons indiquer une méthode pour déterminer le nombre minimum de points, courbes, etc. déterminés par une équation* $X=0$, *qu'il suffit de connaître pour que les autres puissent être construits par la règle seule ou par la règle et le compas.*

On sait que l'adjonction d'une racine a à une équation réduit le groupe de cette équation à celles de ses substitutions qui laissent a immobile. Pour résoudre l'équation, il suffit de lui adjoindre successivement assez de racines pour que le nouveau groupe de l'équation se réduise à l'unité.

La méthode générale à employer pour déterminer le nombre minimum des racines nécessaires à la résolution complète est identique à celle que nous avons indiquée pour la détermination de la classe d'un groupe (p. 298).

On remarque, en effet, que 2 groupes semblables ne diffèrent que par la notation; soient 2 équations qui ont pour groupes ces 2 groupes : si la résolution de l'une s'obtient par l'adjonction de k racines convenablement choisies, la résolution de l'autre s'obtiendra par l'adjonction de k racines convenablement choisies.

Dès lors, avec les notations de la page 298, l'adjonction d'une racine réduit le groupe G de l'équation à l'un des groupes H_a, $H_{a'}$, ..., ou à un groupe semblable à l'un de ceux-là; il suffit d'étudier un représentant de chacune des catégories de groupes correspondant à (10), en opérant sur chacun d'eux comme on l'a fait sur G, etc. Dans la suite des opérations, on applique encore la condition (A).

Soit n le degré de G,

$$n_1, \quad n_2, \quad \ldots$$

les degrés de H_a, $H_{a'}$, ... L'adjonction d'une racine déplacée par H_a à H_a, autrement dit, la considération du sous-groupe des substitutions de H_a laissant immobile une lettre déplacée par H_a conduit à de nouveaux groupes représentants de degrés

$$n_{1,1}, \quad n_{1,2}, \quad \ldots, \quad < n_1;$$

de même $H_{a'}$ conduit à de nouveaux groupes représentants, de degrés

$$n_{2,1}, \quad n_{2,2}, \quad \ldots, \quad < n_2;$$

et ainsi de suite. En général, on obtiendra des sous-groupes de degrés

$$n_{i_1, i_2, \ldots, i_k}$$

constamment décroissants.

Le nombre cherché ici, M_r, *relatif aux constructions par la règle seule, est la valeur minima* (1) *qu'il faut attribuer à k pour que*

$$n_{i_1, i_2, \ldots, i_k} = 1.$$

---

(1) On pourra aussi chercher la valeur maxima, ou même les valeurs exactes : si u est la classe de G, ces divers nombres sont $\leqq n - u$. Si, en laissant de côté le sous-groupe de G formé de la substitution 1, on peut trouver dans G des groupes déplaçant $n - u_0$, $n - u_1$, ..., $n - u_{\lambda-1}$ lettres, avec $u_0 < u_1 < \ldots < u_{\lambda-1}$, et non $n - u_\lambda$, avec $u_\lambda \neq u_0$, u_1, ..., $u_{\lambda-1}$, G est dit *un groupe à* λ *degrés* (*voir* notre Note du *Bull. Soc Math.*, 1897, t. XXV, p. 189). La connaissance de λ donnera ici $M_r \leqq \lambda$.

Considérant les divers nombres $n_{i_1,\ldots,i_k}$ satisfaisant à cette égalité, le plus petit des nombres $n_{i_1,i_2,\ldots,i_k}$ corrélatifs est égal à la classe du groupe G.

Pour déterminer le nombre M_{rc}, analogue à M_r, mais relatif aux constructions par la règle et le compas, on remarquera d'abord que $M_{rc} \leqq M_r$. On considérera, en appliquant la même méthode, les sous-groupes de degrés

$$n_{i_1,i_2,\ldots,i_k}.$$

La condition nécessaire et suffisante pour qu'une équation soit résoluble à l'aide d'équations du second degré, autrement dit pour que ses racines puissent être construites par la règle et le compas, est que l'ordre du groupe G de cette équation soit une puissance de 2.

En effet, on sait qu'un groupe résoluble d'ordre m a pour facteurs de composition (1) les divers diviseurs premiers de m, c'est-à-dire que sa résolution se ramène à celles d'équations d'ordre et de degré égaux à ces divers facteurs : ces équations seront du deuxième degré à la condition nécessaire et suffisante que les facteurs de composition soient tous égaux à 2. Par conséquent, l'ordre de G doit être une puissance de 2.

Réciproquement, si ordre $G = 2^m$, on sait (2) que G est résoluble par radicaux du second degré, c'est-à-dire que tous ses facteurs de composition sont premiers et égaux à 2.

Le nombre cherché ici, M_{rc}, *relatif aux constructions par la règle et le compas, est la valeur minima qu'il faut attribuer à* k *pour que le sous-groupe correspondant soit d'ordre* $= 2^m$.

Appliquons cette méthode à l'équation aux 27 droites des surfaces du troisième degré, et au groupe G (p. 317) qui comprend le groupe de cette équation. Les développements des pages 317 et suivantes montrent que la construction de ces droites par la règle et le compas est possible quand on se donne (3) a, b, d, f, la construction par la règle seule quand on se donne a, b, d, f, h.

XI. *Il suffit de connaître* 4 *des* 27 *droites, convenablement choisies, d'une surface du troisième degré, pour que l'on puisse construire les autres à l'aide de la règle et du compas. Il suffit de connaître* 5 *de ces droites, convenablement choisies, pour que l'on puisse construire les autres à l'aide de la règle seule.*

---

(1) JORDAN, *Traité des substitutions,* p. 387.

(2) VOGT, *Résolution alg. des équations,* Nony, 1895, p. 136.

(3) D'autres groupes de lettres conduisent au même résultat; ainsi la construction par la règle et le compas est possible quand on se donne a, b, m, u ou a, b, m', p' ou a, m, q, p'.

On vérifie encore qu'on ne peut diminuer ces nombres en adjoignant d'autres séries de racines.

Considérons maintenant les 28 tangentes doubles d'une quartique générale. En adjoignant à l'équation du vingt-huitième degré correspondante une de ses racines, on réduit le groupe à un groupe contenu dans le groupe G précédent. Donc :

XII. *Il suffit de connaître* 5 *des* 28 *tangentes doubles, convenablement choisies, d'une quartique générale, pour que l'on puisse construire les autres à l'aide de la règle et du compas. Il suffit de connaître* 6 *de ces bitangentes, convenablement choisies, pour que l'on puisse construire les autres à l'aide de la règle seule* (1).

VIII.

SUR LA TRANSITIVITÉ ENTRE LES COMBINAISONS DE ν LETTRES.

Reprenons la propriété 2° énoncée page 284 : on peut la préciser un peu plus. Sans être $\mu_1 + 1$ fois transitif, le groupe G de $X = 0$ pourrait être transitif entre les combinaisons $\mu_1 + 1$ à $\mu_1 + 1$ des d points; cela suffit pour entraîner que les d points sont sur la même courbe de degré μ.

De même, s'il y a une relation géométrique entre les points, courbes, etc. définis par $X = 0$, relation où l'on peut faire figurer μ_2 de ces points, courbes, etc. choisis arbitrairement (2), et s'il n'y en a pas où $\mu_2 + 1$ arbitrairement choisis puissent figurer, il est bien évident que le groupe de $X = 0$ ne pourrait permuter transitivement les combinaisons des lettres $\mu_2 + 1$ à $\mu_2 + 1$.

Nous sommes ainsi amené incidemment à envisager dans la théorie des substitutions, en vue d'applications géométriques possibles, et, de plus, en raison de son intérêt propre, un genre de transitivité relative ainsi défini :

Si un groupe G *de substitutions entre d lettres* $a_1, a_2, \ldots, a_d$ *contient une substitution remplaçant une combinaison quelconque de* ν *des d lettres par une autre arbitrairement choisie, nous dirons que* G *est transitif entre les combinaisons* ν *à* ν *de ces d lettres.*

L'étude de ce genre de transitivité a déjà été envisagée dans plusieurs de nos

---

(1) *Comparer* CLEBSCH, *Leçons sur la Géométrie,* trad. A. Benoist, t. III. Paris, 1883, p. 451.

(2) L'ensemble de ces relations forme alors ce que nous avons appelé (Note au bas de la p. 282) *un système complet;* le faisceau des substitutions laissant invariable la valeur numérique de chacune des fonctions du système forme un groupe, qui contient G.

Mémoires antérieurs (1). Un groupe ν fois transitif entre les d lettres est transitif entre les combinaisons ν à ν des d lettres; mais la réciproque n'est pas vraie; ainsi (2), le groupe des substitutions $W = |x; a^2x + b| \pmod{p}$, ($p$ premier), d'ordre $p\frac{p-1}{2}$, quand $p = 4h + 3$, est transitif entre les combinaisons 2 à 2 des p lettres 0, 1, 2, ..., $p - 1$, et, cependant, il n'est pas deux fois transitif.

Nous savons encore (3) que, si un groupe G est transitif entre les combinaisons ν à ν de d lettres, il est transitif entre ces d lettres; que si G est transitif entre les combinaisons 3 à 3 de ces d lettres, il l'est aussi entre les combinaisons 2 à 2.

Mais l'on peut, plus généralement, se poser les problèmes suivants :

I. *Si* G, *de degré d, est transitif entre les combinaisons* ν *à* ν *de d lettres* $\left(\nu \leqq \frac{d}{2}\right)$, *est-il transitif entre les combinaisons* ν' *à* ν', *quand* $\nu' < \nu$?

La réponse est affirmative pour $\nu' = 1$, ou pour $\nu \leqq 3$.

II. *Si* G *ne contient pas le groupe alterné de degré d,* ν $\left(supposé \leqq \frac{d}{2}\right)$ *est-il limité en fonction de d, comme l'est* (4) *la transitivité de* G?

III. *Si* G *ne contient pas le groupe alterné de degré d, et si* G *est transitif entre les combinaisons* ν *à* ν *de ses lettres, sa classe est-elle limitée inférieurement en fonction de d*?

Plus généralement, on pourra songer à traiter, pour ce genre de transitivité, les mêmes problèmes (5) que pour la transitivité ordinaire.

Nous allons indiquer ci-dessous un résultat relatif à la question I, et résoudre affirmativement les questions II et III.

I. Il y a, en dehors des cas où soit $\nu' = 1$, soit $\nu \leqq 3$, une infinité de valeurs de d pour lesquelles la propriété I comporte une réponse affirmative.

---

(1) *J. de Math.*, 1895, 1897. — *Mém. des Savants étrangers*, t. XXXII. — *Bull. Soc. Math.*, t. XXIV, 1896, p. 89.

(2) *Bull. Soc. Math.*, t. XXIV, 1896, p. 90.

(3) *Id.*, p. 89.

(4) JORDAN, *Traité des subst.*, p. 76 et *J. de Math.*, 1895, p. 35. — A. BOCHERT, *Math. Ann.*, t. XXIX, XXXIII et XL.

(5) On peut d'ailleurs encore se poser les mêmes problèmes à propos de la transitivité incomplète, définie plus haut, page 300.

En effet, supposons G transitif entre les C_d^ν combinaisons des d lettres ν à ν : chaque combinaison de ν lettres comprend ν combinaisons de $\nu-1$ lettres. Si G n'est pas transitif entre les combinaisons de $\nu-1$ lettres, il permute exclusivement entre elles λ des $C_d^{\nu-1}$ combinaisons des d lettres $\nu-1$ à $\nu-1$, avec $\lambda < C_d^{\nu-1}$. Si une combinaison de ν lettres comprend exactement λ_1 combinaisons de $\nu-1$ lettres appartenant à ces λ, il en est de même pour chaque combinaison de ν lettres en vertu de la transitivité de G entre les combinaisons des d lettres ν à ν. On peut alors supposer $\lambda_1 \leqq \frac{\nu}{2}$.

Ces λ combinaisons comprennent en tout $\lambda_1 C_d^\nu$ combinaisons de $\nu-1$ lettres, chacune étant comptée ainsi $d-\nu+1$ fois, puisque chacune appartient à $d-\nu+1$ combinaisons de ν lettres. Donc

$$\lambda = \frac{\lambda_1 C_d^\nu}{d-\nu+1}, \qquad \text{avec} \qquad \lambda_1 \leqq \frac{\nu}{2};$$

$$\lambda = \lambda_1 \frac{d(d-1)\ldots(d-\nu+2)}{\nu!}.$$

Prenons

$$d = \nu!\, h - 1 \qquad (h \text{ entier} > 0);$$

$d-i$, $(i = 0, 1, 2, \ldots, \nu-2)$, a avec $\nu!$ le plus grand commun diviseur $i+1$. Donc $d(d-1)\ldots(d-\nu+2)$ a avec $\nu!$ le plus grand commun diviseur $(\nu-1)!$: $\frac{\lambda_1}{\nu}$ devrait être entier, comme λ, ce qui n'est pas. Donc G est transitif entre les combinaisons $\nu-1$ à $\nu-1$ de ses d lettres.

Posant $\nu-1=\nu_1$, on peut raisonner sur les combinaisons de ν_1 et ν_1-1 lettres, comme on vient de raisonner sur celles de ν et $\nu-1$ lettres. Les conclusions seront les mêmes, car si $h\nu = h_1$, $d = \nu_1!\, h_1 - 1$. G est transitif entre les combinaisons $\nu-2$ à $\nu-2$ de ses d lettres.

On pourra évidemment ensuite raisonner de même sur $\nu_2 = \nu_1 - 1 = \nu - 2$, ..., $\nu_j = \nu - j$, ... Donc :

THÉORÈME. — *Si un groupe* G, *de degré* $d = \nu!\, h - 1$, $(h$ *entier* $> 0)$, *est transitif entre les combinaisons* ν *à* ν *de ces d lettres, il est transitif entre les combinaisons* ν' *à* ν' *de ses d lettres, quand* $\nu' < \nu$.

Il en est de même pour d quelconque quand $\nu' = 1$ *ou quand* $\nu \geqq 3$.

II. Si G est transitif entre les combinaisons des d lettres ν à ν, il l'est aussi entre les combinaisons des d lettres $d-\nu$ à $d-\nu$: car soient c_1, c_2 2 combinaisons ν à ν; C_1, C_2 les combinaisons $d-\nu$ à $d-\nu$ des d lettres formées par celles des d lettres qui n'appartiennent pas à c_1 ou c_2; une substitution de G qui rem-

place c_1 par c_2 remplace forcément C_1 par C_2. On peut donc se contenter d'examiner ce qui se passe dans le cas où G est transitif entre les combinaisons ν à ν des d lettres, avec $\nu \leq \frac{d}{2}$. La propriété à établir est alors la suivante :

$$\frac{d}{2} - \nu \leq \varphi(d),$$

où $\varphi(d)$ est une certaine fonction > 0 de d.

Nous indiquerons d'abord une démonstration directe du lemme suivant de M. Jordan (1), démonstration indépendante de la considération des facteurs de composition.

LEMME I. — *Si un groupe* Γ, *transitif et de degré* d, *a son ordre divisible par un nombre premier* $p > \frac{d}{2}$, *autrement dit si* Γ *contient une substitution circulaire d'ordre* $p > \frac{d}{2}$, Γ *est primitif, par suite* $d - p + 1$ *fois transitif.*

Nous savons d'abord que ce lemme est vrai quand Γ est primitif (2); mais nous allons montrer que Γ ne peut être transitif, sans être primitif.

En effet, supposons Γ transitif, mais non primitif, Γ contenant une substitution circulaire d'ordre $p > \frac{d}{2}$. Γ admet une répartition de ses d lettres en systèmes de non-primitivité de θ lettres $\left(\theta \leq \frac{d}{2} < p\right)$. On a $p < d$, puisque d est divisible par $\theta < d$, par suite non premier.

Désignons par H_α le sous-groupe des substitutions de Γ qui laissent la lettre α immobile : H_α contient une substitution circulaire S d'ordre p. Soit s_1 le système d'imprimitivité auquel appartient α : H_α permute exclusivement entre elles les $\theta - 1$ lettres de ce système autres que α, lettres dont aucune, par suite, n'appartient à la substitution S, puisque $\theta - 1 < p$. Soient $a_1, a_2, \ldots, a_p$ les lettres de $S = (a_1 a_2 \ldots a_p)$.

Si a_1 et a_{k+1} $(0 < k \leq p-1)$ appartiennent à un même système s_2 de non-primitivité, $S^k = (a_1 a_{k+1} a_{2k+1} \ldots)$ montre que S^k laisse s_2 invariable; a_{k+1} est remplacé par une lettre a_{2k+1} de s_2, a_{2k+1} par une lettre a_{3k+1} de s_2, etc. Finalement, les p lettres de S appartiendraient au système s_2, ce qui est absurde, puisque $p > \theta$. Donc les p lettres de S appartiennent à p systèmes distincts, ce qui est

---

(1) JORDAN, *Traité des substitutions*, p. 284.

(2) *Id.*, Note C, p. 664. — JORDAN, *Journal de Mathématiques*, 1871, p. 384. — E. NETTO-BATTAGLINI, *Teoria delle Sostituzioni*, p. 79-80.

encore absurde, car le nombre $\frac{d}{\theta}$ des systèmes est $\leqq \frac{d}{2} < p$, puisque $\theta \geqq 2$. Donc F ne peut être imprimitif. C. Q. F. D.

Ce lemme en entraîne un autre quand on s'appuie sur le théorème suivant (1) de M. Jordan :

Quand p est un nombre premier impair, un groupe de degré $p + k$ ne peut être plus de k fois transitif, si $k \geqq 3$, à moins de contenir le groupe alterné.

Soit alors $\frac{d}{2} < p \leqq d - 3$: tout étant posé comme au lemme I, Γ sera $d - p + 1$ fois transitif; $p + k = d$, $k \geqq 3$, $d - p + 1 = k + 1$. Γ serait de degré $p + k$ avec $k \geqq 3$, et plus de k fois transitif, ce qui est impossible d'après le théorème ci-dessus. Si donc nous admettons que, d étant quelconque, il y a toujours un ou des nombres premiers plus petits que $d - 2$ et plus grands que $\frac{d}{2}$, nous obtenons ainsi une limite de transitivité des groupes de degré d où intervient le plus grand de ces nombres premiers :

Lemme II. — *Si p est le plus grand des nombres premiers inférieurs à $d - 2$, un groupe* G *de substitutions transitif entre d lettres et qui ne contient pas le groupe alterné de d lettres n'est pas plus de $d - p$ fois transitif, ou, ce qui revient au même, est d'ordre premier à p; on a*

$$\frac{d}{2} < p < d - 2 \quad (2).$$

Ce n'est qu'une transformation de l'énoncé de M. Jordan. Mais cette nouvelle limite de transitivité s'étend à la transitivité entre les combinaisons ν à ν des d lettres.

En effet, considérons un groupe G transitif entre les combinaisons ν à ν des d lettres $\left(\nu \leqq \frac{d}{2}\right)$, et qui ne contient pas le groupe alterné des d lettres. Son ordre $\mathcal{G}$ est divisible par

$$C_d^\nu = \frac{d(d-1)\dots(d-\nu+1)}{\nu!}.$$

Soit encore p le plus grand des nombres premiers plus grands que $\frac{d}{2}$ et infé-

(1) *Bulletin de la Société mathématique,* t. I, 1872-1873, p. 42.

(2) D'après Tchebychef; *voir* ci-dessous.

rieurs à $d-2$: si $d-\nu+1 \leqq p$ ou $\nu \geqq d-p+1$, G contiendra une substitution d'ordre p et sera $d-p+1$ fois transitif contrairement au lemme II. Donc

$$\nu \leqq d-p.$$

Mais, d'après Tchebychef et Serret (*Algèbre supérieure*, t. II, 5me édition, 1885, p. 238), il y a toujours un nombre premier $\leqq d-3$ et plus grand que

$$\delta_d = \frac{5}{6}(d-3) - 2\sqrt{d-3} - 25\frac{\log^2(d-3)}{16\mathrm{A}\log 6} - 125\frac{\log(d-3)}{24\mathrm{A}} - \frac{25}{6\mathrm{A}'},$$

où

$$\mathrm{A} = 0,92129\ldots,$$

$$\delta_d = \frac{5}{6}d(1-\varepsilon_d), \qquad (\varepsilon_d > 0,\ \varepsilon_\infty = 0);$$

les logarithmes sont ici népériens, et $d \geqq 6$.

Donc, dès que d est supérieur à une certaine limite Δ,

$$\delta_d > \frac{4}{5}d,$$

et il y a toujours un nombre premier au plus égal à $d-3$ et $> \frac{4}{5}d$.

On vérifie que, si l'on prend $\Delta = 10\,003$, $\delta'_d - \frac{4}{5}$ est positif pour $d \geqq \Delta$, $\delta_\Delta - \frac{4}{5}\Delta$ est aussi positif, par suite aussi $\delta_d - \frac{4}{5}d$ quand $d > 10\,003$ (1).

---

(1) Pour les valeurs de $d \leqq 10\,003$, on vérifiera à l'aide d'une Table de nombres premiers qu'il y a un nombre premier p avec $\frac{4}{5}d < p \leqq d-3$ tant que $d \geqq 40$. Un des moyens les plus rapides de le faire est de se reporter à la Table suivante de M. J. Glaisher : *Factor Table for the Fourth Million*, London, Taylor and Francis, 1879, p. 48; où l'on trouve tous les nombres premiers jusqu'à 30 341 avec la différence Δ_1 des nombres premiers consécutifs 2 à 2 (on peut aussi se contenter du Tableau de la page 340). On remarque que $\Delta_1 \leqq 36$, quand $d \leqq 10\,003$; p existera donc tant que

$$d-3-\frac{4}{5}d = \frac{d}{5} - 3 \geqq 37, \qquad d \geqq 200.$$

Quand $d < 200$, $\Delta_1 \leqq 14$; p existe tant que

$$\frac{d}{5} - 3 \geqq 15, \qquad d \geqq 90.$$

Nous obtenons ainsi ce lemme :

LEMME. — *Quel que soit le nombre d, il y a toujours un nombre premier p au plus égal à* $d-3$ *et supérieur à* $\frac{4}{5}d$, *dès que d est supérieur à* 39.

Dès lors, si d est assez grand, $\nu \leqq d-p$, $p > \frac{4}{5}d$, $\nu < \frac{d}{5}$. Nous obtenons ainsi ce résultat :

THÉORÈME. — *Soit* G *un groupe de substitutions entre d lettres qui permute transitivement les combinaisons* ν *à* ν *de ces d lettres* $\left(\nu \leqq \frac{d}{2}\right)$, *p le plus grand nombre premier inférieur à* $d-2$ *et plus grand que* $\frac{d}{2}$: *on a forcément*

$$\nu \leqq d-p.$$

Quand $d \geqq 40$, *on a*

$$\nu < \frac{d}{5},$$

pour $d < 40$,

$$\nu \leqq 8.$$

Ce théorème comprend le lemme II comme cas particulier, car un groupe de degré d ν fois transitif est transitif entre les combinaisons des d lettres ν à ν.

Remarque. — MM. A. Bochert (1) et Jordan ont indiqué pour un groupe t fois transitif de degré d des limites de transitivité très avantageuses en général. Ainsi M. Jordan a démontré (2) que pour ce groupe

$$\log(d-t) \geqq a\sqrt{t\log t} \qquad (\lim_{d=\infty} a = \log 2).$$

Mais la formule $\nu \leqq d-p$ du théorème précédent est susceptible de nous donner une formule analogue $\nu \leqq \psi(d)$ si l'on connaît une limite supérieure de la diffé-

---

Quand $d < 90$, $\Delta_1 \leqq 6$; p existe tant que

$$d \geqq 50.$$

Pour $40 \leqq d < 50$, on vérifie la chose directement.
Enfin, quand $d < 40$, on voit de suite que

$$\nu \leqq 8.$$

(1) *Math. Ann.*, t. XXIX, XXXIII et XL.
(2) *Journal de Mathématiques*, 1895, p. 35.

rence $d-p$ en fonction de d : l'utilisation de la valeur de $\psi(d)$ déduite des résultats de Tchebychef nous a précisément donné en général $\nu < \frac{d}{5}$.

On ne connaît pas, croyons-nous, de valeur plus avantageuse de $\psi(d)$, ou mieux, de la limite supérieure de la différence Δ_1 entre 2 nombres premiers consécutifs ϖ_1, ϖ_2 ($\varpi_2 > \varpi_1$) en fonction de ϖ_2 ou ϖ_1, quel que soit ϖ_2. Mais, dans les limites des Tables des nombres premiers, on peut chercher une valeur de $\psi(d)$ aussi avantageuse que possible. En particulier, on peut chercher à vérifier ainsi jusqu'à $d = 9.10^6$ par exemple (Tables de Burckhardt et de M. Glaisher), pour la transitivité entre les combinaisons de ν lettres, une formule analogue à celle de MM. Bochert ou Jordan.

Voici comment on peut opérer : formons (par la pensée) un Tableau où les nombres premiers sont rangés par ordre de grandeur croissante, et où nous portons, vis-à-vis de chaque nombre premier, la différence Δ_1 avec le nombre premier précédent; puis ne conservons dans ce Tableau que les différences Δ_1 qui sont supérieures à toutes les précédentes. Nous obtenons le Tableau suivant (1), valable pour les 9.10^6 premiers nombres :

Nombres premiers.	Différence Δ_1 avec le précédent.	Valeur $\Delta_1 + 2$.	Valeur de $2\log_{10}\varpi_2$.	Valeur de $(2\log_{10}\varpi_2)^2$.
2	1	3	0,602	0,36
5	2	4	1,398	1,96
11	4	6	2,083	4,34
29	6	8	2,925	8,56
97	8	10	3,974	15,80
127	14	16	4,208	17,70
541	18	20	5,466	29,88
907	20	22	5,915	34,99
1 151	22	24	6,122	37,48
1 361	34	36	6,268	39,29
9 587	36	38	7,963	63,41
15 727	44	46	8,393	70,44
19 661	52	54	8,587	73,74
31 469	72	74	8,996	80,87
156 007	86	88	10,386	107,77
360 749	96	98	11,114	123,59
370 373	112	114	11,137	124,03
492 227	114	116	11,384	129,60
1 349 651	118	120	12,260	150,31
1 357 333	132	134	12,265	150,43
2 010 881	148	150	12,607	158,94
4 652 507	154	156	13,335	177,82

(1) Pour les 100 000 premiers nombres, nous avons déjà un Tableau analogue, ne compre-

Soit x_i le nombre premier qui figure dans la $i^{\text{ème}}$ ligne de ce Tableau, δ_i la différence Δ_1 correspondante : quand $d-2 \leqq x_{i+1}-\delta_{i+1}$, le nombre premier p immédiatement inférieur à $d-2$ est au moins égal à $d-2-\delta_i$, et

$$\nu \leqq d-p \leqq d-(d-2-\delta_i)=\delta_i+2.$$

Donc :

COROLLAIRE I. — *Quand* $d-2 \leqq x_{i+1}-\delta_{i+1}$, *on a*

$$\nu \leqq \delta_i+2,$$

---

nant que les deux premières colonnes, dressé par M. J. Glaisher (*Messenger of Math.*, 1878, t. VII, p. 174-175), et rectifié ici par nous d'après J. GLAISHER, *Factor Table for the Fourth Million*, London, Taylor and Francis, 1879, p. 48. Au delà, nous nous sommes servi du Tableau des différences Δ_1 de 80 et au-dessus pour le premier million (*Mess., loc. cit.*, p. 104), 100 et au-dessus pour les 9 premiers millions (GLAISHER, *Factor Table for the Sixth Million*, etc., 1883, p. 64-65). Enfin nous avons vérifié personnellement, d'après les Tables de Burkhardt (Paris, 1817), l'exactitude du Tableau précédent entre 100 000 et 405 000.

Les mêmes résultats et vérifications nous ont encore permis de constater l'exactitude, dans les limites des Tables, de ce théorème empirique :

h étant donné, on peut toujours trouver 2 nombres premiers consécutifs dont la différence est $2h$.

Ce théorème était déjà vérifié implicitement par M. Glaisher, qui, toutefois, ne l'a pas énoncé, jusqu'à $h=32$ (pour les 100 000 premiers nombres, *Mess., loc. cit.*, p. 174, et *Factor Table for the Fourth Million*, p. 48). Pour $40 \leqq h \leqq 70$, il résulte des Tableaux de *séquences* de nombres non premiers (valeurs de $\Delta_1 - 1$) indiqués par M. Glaisher (*Tables et Mess., loc. cit.*, p. 104 et 171). Pour $33 \leqq h \leqq 39$, on a :

Pour 162 209.....	$\Delta_1 = 66$	Pour 404 671.....	$\Delta_1 = 74$
134 581.....	68	212 777.....	76
173 429.....	70	188 107.....	78
31 469.....	72 (Glaisher)		

Enfin, d'après les Tableaux de M. Glaisher, on peut encore avoir

$$h = 73,\ 74,\ 76,\ 77.$$

Finalement, ce théorème est vrai pour $h \leqq 70$. On sait de plus (*Mess., loc. cit.*, p. 106 et E. LUCAS, vol. VIII, 1879, p. 81) que la différence $2h$ de 2 nombres premiers consécutifs peut croître indéfiniment.

Mentionnons les différences

$$265\,703 - 265\,621 = 82, \qquad 360\,749 - 360\,653 = 96,$$
$$396\,833 - 396\,733 = 100, \qquad 404\,941 - 404\,851 = 90,$$

qui ne figurent pas dans la Table de M. Glaisher (*Mess., loc. cit.*, p. 104).

Notre travail personnel nous permet d'affirmer, sauf erreur de notre part, et sous réserve de l'exactitude de la Table des nombres premiers de Burckhardt (Paris, 1817), les résultats précédents pour les nombres $\leqq 405\,000$. Au delà, une vérification spéciale serait utile.

x_i et δ_i étant le nombre premier et la différence Δ_1 correspondante de la $i^{ième}$ ligne (2 premières colonnes) du Tableau précédent ($d < 4\,652\,356$). Quand $9.10^6 \geqq d \geqq 4\,652\,356$,

$$\nu \leqq 156.$$

On peut substituer à ce Tableau une formule valable dans les limites des Tables, en cherchant une limite supérieure de $d - p$ en fonction de d à l'aide de ce Tableau.

Nous écrivons dans le même Tableau les valeurs de $\Delta_1 + 2$, les logarithmes ordinaires de d (base 10), enfin le nombre $(2\log_{10} d)^2$. On constate que l'on a constamment, pour les nombres $\geqq 29$,

$$\Delta_1 + 2 < (2\log_{10} d)^2.$$

D'ailleurs, $4\log_{10}^2 d \geqq 6$ dès que

$$\log_{10} d \geqq \frac{\sqrt{6}}{2} = 1,224\ldots, \qquad d \geqq 16,79 \qquad \text{ou} \qquad d \geqq 17.$$

Par conséquent :

Lemme. — *Dans les limites des Tables de nombres premiers (ϖ_2 et $d \leqq 9.10^6$), la différence Δ_1 entre 2 nombres premiers consécutifs ϖ_1, ϖ_2 ($\varpi_2 > \varpi_1$) satisfait à*

$$\Delta_1 \leqq 4(\log_{10} \varpi_2)^2 - 2,$$

quand $\varpi_2 > 17$. De même, la différence Δ_2 entre un nombre quelconque $d > 13$ et le nombre premier p immédiatement inférieur à $d - 2$ est telle que

$$\Delta_2 \leqq 4(\log_{10} d)^2.$$

Corollaire II. — *On a*

$$\nu \leqq 4(\log_{10} d)^2,$$

quand $13 < d < 9.10^6$.

C'est là, bien entendu, jusqu'à nouvel ordre, une formule empirique.

Il est bon de signaler ici que δ_i doit croître indéfiniment avec x_i, ainsi que l'ont remarqué MM. Glaisher (1) et E. Lucas (2).

En effet, si p est premier impair, les nombres $p! + i (i = 2, 3, \ldots, p + 1)$ ne

(1) *Mess., loc., cit.*, p. 106.

(2) *Mess., loc. cit.*, vol. VIII, 1879, p. 81.

sont pas premiers. Quand

$$d = p! + p + 4 = \left(\frac{p}{e}\right)^{p+\frac{1}{2}} \sqrt{2\pi e}(1+\varepsilon),$$

$$\Delta_2 \geqq p + 3;$$

$$\log d = (p+\tfrac{1}{2})(\log p - \log e)(1+\varepsilon') = p \log p (1+\varepsilon'');$$

$$\log\log d = \log p + \log\log p + \log(1+\varepsilon'') = \log p (1+\varepsilon''');$$

$$p = \frac{\log d}{\log\log d}(1+\varepsilon^{(IV)}).$$

Finalement, pour une infinité de valeurs de d,

$$\Delta_2 \geqq \frac{\log d}{\log\log d}(1+\varepsilon^{(V)}),$$

($\lim \varepsilon^{(j)} = 0$ pour $d = \infty$) et Δ_2 croît indéfiniment avec d.
On peut améliorer un peu cette limite inférieure en considérant, au lieu des nombres $p! + i$, les nombres $2.3.5.7.11\ldots p + i$, où figure seulement le produit des nombres premiers au plus égaux à p. En remarquant que, si

$$\theta(p) = \log_e 2.3\ldots p,$$

on a, d'après Tchebychef (1),

$$(1+\eta)Ap < \theta(p) < (1+\eta_1)\tfrac{6}{5}Ap, \qquad (A = 0{,}92129\ldots, \text{ lim de } \eta \text{ et } \eta_1 = 0 \text{ pour } d = \infty),$$

on trouverait

$$\Delta_2 \geqq \lambda \log_{10} d \qquad (\lambda \text{ fini})$$

pour une infinité de valeurs de d.

III. — On sait (2) que si un groupe G de degré d est ν fois transitif $\left(\frac{d}{2} \geqq \nu \geqq 2\right)$, sa classe u est limitée inférieurement en fonction de $d\left(u \geqq \frac{n}{4}, \text{ quand } n > 29\right)$. On peut se demander si un théorème analogue n'a pas lieu pour la transitivité entre les combinaisons de ν lettres. Nous allons établir le théorème suivant, qui permet de répondre affirmativement, mais est, sans doute, susceptible de perfectionnements :

---

(1) *Journal de mathématiques*, 1852, p. 379, ou SERRET, *Algèbre supérieure*, t. II, 5e édition, 1885, p. 236. L'emploi de la formule d'Halphen, $\theta(p) = p(1+\varepsilon^{(VI)})$ (HADAMARD, *Bulletin de la Société mathématique*, 1896, p. 217) conduit à une inégalité de même forme.

(2) A. BOCHERT, *Math. Ann.*, t. XL, 1892, p. 181.

THÉORÈME. — *Si un groupe* G, *de degré d, est transitif entre les combinaisons de ses lettres* ν *à* $\nu\left(\frac{d}{2} \geq \nu \geq 2\right)$, *il est primitif; par suite* (1) *sa classe u est limitée inférieurement en fonction de d.*

En effet, supposons que G admette une répartition de ses lettres en systèmes de non-primitivité de k lettres,

$$a_1,\ a_2,\ \ldots,\ a_k;\ a_{k+1},\ \ldots,\ a_{2k};\ \ldots, \qquad \text{et} \qquad d = k\delta \geq 2k.$$

On peut écrire

$$\nu = kl + m \qquad \text{avec} \qquad 0 \leq m < k.$$

Prenons la combinaison c_1

$$a_1,\ \ldots,\ a_k;\ a_{k+1},\ \ldots,\ a_{2k};\ \ldots;\ a_{kl+1},\ \ldots,\ a_{kl+m}:$$

si $m = 0$ ou 1, $l \geq 1$; $kl + m = \nu \leq \frac{d}{2}$.

Supposons d'abord que, en dehors des $l+1$ systèmes d'imprimitivité (l si $m = 0$) qui ont des lettres dans c_1, il y en ait au moins 2 autres, c'est-à-dire $(l+3)k \leq d$ (quand $m = 0$, $(l+2)k \leq d$). Ceci aura toujours lieu, puisque $2kl + 2m \leq d$, $d \geq 2kl + k$, dès que $(l+3)k \leq 2kl + k$, c'est-à-dire $l \geq 2$ (quand $m = 0$, $2kl \leq d$, dès que $(l+2)k \leq 2kl$, ou $l \geq 2$).

Nous pourrons trouver une combinaison c_2 contenant les lettres de c_1, sauf 2, arbitrairement choisies, et de plus 2 lettres a_i, a_j appartenant à 2 systèmes différents et différents de ceux qui ont des lettres communes avec c_1 : il y a une substitution S remplaçant c_1 par c_2; elle substitue à une des lettres $a_1, \ldots, a_{kl}$ la lettre a_i ou a_j, et à une lettre du même système une des lettres $a_1, \ldots, a_{kl+m}$, c'est-à-dire que G n'admettrait pas la répartition en systèmes considérée.

Supposons alors $l < 2$:

1° $l = 1$, $1 \leq m \leq k-1$, $d \geq 2k + 2m$, $d \geq 4k$ ou $d = 3k$.

Si $d \geq 4k$, $(l+3)k = 4k \leq d$, et le même raisonnement réussit.

Si $d = 3k$, soit $k > 2$, $d > 6$ (pour $d \leq 6$, le théorème résulte du théorème qui suit); nous prendrons 2 lettres a_j, $a_{j'}$ appartenant au troisième système; il y a une substitution T remplaçant $a_1, \ldots, a_{k+m}$ par ces mêmes lettres, moins deux arbitraires appartenant au premier système, et par a_j, $a_{j'}$. Parmi les $k+m$ nouvelles lettres, il y en a forcément, puisque $k > 2$, une appartenant au premier système. Les lettres $a_1, \ldots, a_{k+m}$ comprennent les lettres de 2 systèmes, les lettres substituées, celles de 3 systèmes : résultat absurde.

---

(1) JORDAN, *J. für Math.*, t. LXXIX, 1875, p. 248-258.

2° $l=1, m=0$, $d\geqq 2k$. Quand $d\geqq 3k$, on raisonne comme quand $l\geqq 2$; quand $d=2k$, on raisonne comme pour $l=1$, $m>0$.

3° $l=0$, $\nu=m\leqq k-1$, $d\geqq 2m$, $d\geqq 2k$.

Si $d\geqq 3k$, on peut raisonner à peu près comme quand $l\geqq 2$. Soit donc $d=2k$: $a_1, \ldots, a_{m-1}a_m$ appartiennent au premier système; il y aurait une substitution S remplaçant $a_1, \ldots, a_{m-1}a_m$ par $a_1, \ldots, a_{m-1}a_j$ où a_j appartient au deuxième système, ce qui est absurde. C. Q. F. D.

Nous allons encore établir le théorème suivant :

Théorème — *Soit* G *un groupe de substitutions de degré d, transitif entre les combinaisons de ses lettres* 3 *à* 3 *ou* 2 *à* 2 : G *est primitif. S'il n'est pas* 2 *fois transitif, d est impair, et le sous-groupe de ses substitutions laissant une lettre* a_1 *immobile permute transitivement entre elles les* $d-1$ *autres lettres* $\frac{d-1}{2}$ *à* $\frac{d-1}{2}$.

En effet, soit G un groupe de substitutions de degré d entre les lettres

$$a_1, \quad a_2, \quad \ldots, \quad a_d;$$

supposons ce groupe transitif entre les combinaisons 2 à 2 de ces lettres, et soit H_{a_1} le sous-groupe des substitutions de G qui laissent a_1 immobile. Le cas où G serait transitif entre les combinaisons 3 à 3 se ramène à celui-là (théorème de la page 335).

H_{a_1} est d'ordre $\mathfrak{H}$, et ses substitutions sont

$$1=h_1, \quad h_2, \quad \ldots, \quad h_{\mathfrak{H}};$$

elles permutent entre elles, transitivement, $\theta-1$ des lettres $a_2, \ldots, a_d$ autres que a_1, par exemple

$$a_2, \quad \ldots, \quad a_\theta.$$

Désignons par $s_{\lambda\mu}$ la combinaison $a_\lambda a_\mu$: si g_2 remplace a_1 par a_{λ_1}, et

$$s_{12}, \quad \ldots, \quad s_{1\theta},$$

par

$$s_{\lambda_1\lambda_2}, \quad \ldots, \quad s_{\lambda_1\lambda_\theta},$$

$h_j g_2$ est de la forme

$$\begin{pmatrix} a_1 & a_2 & \ldots \\ a_1 & a_k & \ldots \end{pmatrix}\begin{pmatrix} a_1 & a_k & \ldots \\ a_{\lambda_1} & a_{\lambda_k} & \ldots \end{pmatrix}=\begin{pmatrix} a_1 & a_2 & \ldots \\ a_{\lambda_1} & a_{\lambda_k} & \ldots \end{pmatrix}$$

($k=2, 3, \ldots,$ ou θ), et remplace s_{12} par une des combinaisons $s_{\lambda_1\lambda_2}, \ldots, s_{\lambda_1\lambda_\theta}$.

Formant le tableau des substitutions de G

$$\begin{cases} h_1, & h_2, & \ldots, & h_{\mathcal{H}}, \\ h_1 g_2, & h_2 g_2, & \ldots, & h_{\mathcal{H}} g_2, \\ \ldots\ldots & \ldots\ldots & \ldots, & \ldots\ldots, \\ h_1 g_d, & h_2 g_d, & \ldots, & h_{\mathcal{H}} g_d, \end{cases}$$

où $h_i g_i = g_i$ est une substitution n'appartenant pas aux lignes précédentes, on voit que ces substitutions remplacent s_{12} par au plus $d\theta$ combinaisons distinctes. Or, G est transitif entre les combinaisons 2 à 2, $s_{\lambda\mu}$, au nombre de $d\frac{d-1}{2}$, en sorte que $d\theta \geqq d\frac{d-1}{2}$, $\theta \geqq \frac{d-1}{2}$.

Si $\theta = d-1$, G est 2 fois transitif; sinon, nous opérerons sur $a_1 a_{\theta+1}$ comme nous venons de le faire sur $a_1 a_2$, et nous trouverons encore que H_{a_1} permute $a_{\theta+1}$ avec $\theta' \geqq \frac{d-1}{2}$ lettres distinctes, et forcément distinctes de $a_2, \ldots, a_\theta$.

Or $\theta + \theta' \leqq d-1$; donc $\theta = \theta' = \frac{d-1}{2}$, d impair.

Enfin, G est primitif; en effet, il en est bien ainsi quand G est 2 fois transitif; si G n'est pas 2 fois transitif, soit G imprimitif : G devrait admettre une répartition de ses lettres en systèmes de non-primitivité δ à δ, δ divisant d : H_{a_1} permute entre elles les lettres du système de non-primitivité dont fait partie a_1, et ce système comprendrait au moins $1 + \frac{d-1}{2}$ lettres, ce qui serait absurde. G est donc toujours primitif. C. Q. F. D.

Nous avons vu (1) qu'il y avait des groupes de substitutions G entre d lettres (d premier $= 4h+3$) qui ne sont pas 2 fois transitifs, et qui permutent transitivement les combinaisons de leurs lettres 2 à 2. De même, il y a des groupes G entre d lettres qui ne sont pas 3 fois transitifs, et qui permutent transitivement les combinaisons de leurs lettres 3 à 3.

En effet, nous allons obtenir ce résultat :

THÉORÈME. — *Le groupe de degré $p+1$ (p premier) et d'ordre $\frac{(p+1)p(p-1)}{2}$ formé des substitutions linéaires fractionnaires* (mod p) *dont le déterminant est résidu quadratique* (mod p) *et qui n'est que 2 fois transitif entre ses $p+1$ indices, permute transitivement les combinaisons 3 à 3 de ses $p+1$ indices quand $p = 4h+3$.*

---

(1) *Bulletin de la Société mathématique,* 1896, p. 90 et ci-dessus, p. 334.

En effet, considérons le groupe G des substitutions linéaires fractionnaires

$$\left| z, \frac{az+b}{a'z+b'} \right| \qquad (\mathrm{mod}p), \qquad ab'-ba' \not\equiv 0,$$

où p est premier, 3 fois transitif, de degré $p+1$ entre les nombres 0, 1, 2, ..., $p-1$, ∞, et d'ordre $\mathcal{G}=(p+1)p(p-1)$. Soit $p=4h+3$.

L'ensemble des substitutions de ce groupe dont le déterminant est résidu quadratique (mod$p$) forme un groupe G_1 deux fois transitif, qui ne contient pas la substitution $|z, -z|(\mathrm{mod}p)$, et qui est d'ordre $\frac{(p+1)p(p-1)}{2}=\mathcal{G}_1=\frac{\mathcal{G}}{2}$.

G opère entre les combinaisons 3 à 3 de ses nombres ou indices les substitutions d'un groupe transitif F de degré C^3_{p+1}. Le sous-groupe L des substitutions de G laissant une de ces combinaisons, 0, 1, -1, immobile est d'ordre 6; ce sous-groupe comprend la substitution $|z, -z|(\mathrm{mod}p)$, dont le déterminant, pour $p=4h+3$, n'est pas résidu quadratique (mod$p$). Le sous-groupe M de G_1 laissant la combinaison 0, 1, -1 immobile est formé des substitutions de L dont le déterminant est résidu quadratique (mod$p$), c'est-à-dire est d'ordre 3. Donc G_1 permute transitivement entre elles au moins

$$\frac{\mathcal{G}_1}{3}=C^3_{p+1}$$

combinaisons 3 à 3, c'est-à-dire est transitif entre ces combinaisons.

Remarque. — Ce qui précède suggère l'idée suivante :

Un groupe G *transitif entre les combinaisons* ν *à* ν *de ses lettres, n'est-il pas* $\nu-1$ *fois transitif?*

Si l'on pouvait répondre affirmativement, on en déduirait certains des résultats précédents comme corollaires.

Inversement, ce qui précède peut aider à élucider cette question.

IX.

INDICATION DE SUJETS A ÉTUDIER COMME CONSÉQUENCE DE CE QUI PRÉCÈDE (1).

I. — Détermination plus complète de la classe des substitutions d'ordre 2, ou

(1) Nous nous contenterons de signaler l'application immédiate des théorèmes I, etc. aux équations de la division des fonctions elliptiques, hyperelliptiques, à l'équation modulaire (JORDAN, *Traité,* p. 343, 344, 354).

même d'ordre $\neq 2$, des groupes connus, en particulier pour les groupes linéaires à n indices (mod m), m étant quelconque, pour les groupes orthogonaux, abéliens, hypoabéliens (indices réels ou imaginaires) et pour les groupes de Steiner (*voir* p. 323 ci-dessus). Consulter JORDAN, *Traité des substitutions* et L.-E. DICKSON, *Linear Groups,* Leipzig, Teubner, 1901.

II. Détermination de la classe des mêmes groupes ou d'une limite inférieure de cette classe.

III. Extensions du théorème II au cas où le module r est quelconque : la même marche, avec des modifications convenables, est peut-être applicable.

IV. Application géométrique des théorèmes I, II, III, etc., et des déterminations proposées ci-dessus à d'autres théorèmes de Clebsch (CLEBSCH, *Journal de Crelle,* t. 63 et 64; CLEBSCH et LINDEMANN, *Leçons sur la Géométrie,* traduction Benoist, Paris, Gauthier-Villars; JORDAN, *Traité des substitutions*, Livre III, Chap. III), aux travaux de M. Humbert sur la Géométrie (par exemple, *Journal de Mathématiques,* 1886, p. 308 et suivantes).

V. Continuation de l'étude de la transitivité entre les combinaisons de ν lettres ou de la transitivité incomplète. En particulier, si un groupe G, de degré d, est transitif entre les combinaisons de ν lettres $\left(\nu \leq \frac{d}{2}\right)$, l'est-il, *en général,* entre les combinaisons de ν' lettres ($\nu' < \nu$), ou peut-on citer des cas où cette propriété n'ait pas lieu?

Quand $\nu \geq 2, 3, 4$, peut-on assigner une limite inférieure à la classe u de G, analogue à la limite inférieure de la classe trouvée par M. A. Bochert (*Math. Annalen,* t. XL, 1892, p. 176 et suivantes), pour les groupes 2, 3, 4 fois transitifs? Peut-on trouver pour ν une limite supérieure en fonction de d, *quel que soit d*, analogue à celle indiquée par MM. A. Bochert (*Math. Annalen,* t. XXIX, XXXIII et XL) et Jordan (*Journal de Mathématiques,* 1895, p. 35).

G n'est-il pas $\nu - 1$ fois transitif entre ses d lettres?

VI. Soit

$$\Phi = \Sigma x_1 x_2 \ldots x_\lambda \ldots x_{\lambda'} \qquad (\lambda' > \lambda)$$

une somme de produits de d lettres $x_1, x_2, \ldots, x_d$, ces produits contenant une fois, et une seule, chaque combinaison de λ lettres, mais non toutes les combinaisons de $\lambda + 1$ lettres : étude des groupes de substitutions entre d lettres

laissant Φ invariable. Sont-ils transitifs, et dans quels cas? Classe des substitutions de ces groupes. Applications géométriques, s'il y a lieu.

Cas où $\lambda = 2$, $\lambda' = 3$ (*Comparer* JORDAN, *Traité des substitutions,* Livre III, Chap. III, en particulier, ses systèmes de trios; et NETTO, *Substitutionentheorie, Tripelnsysteme* ou NETTO-BATTAGLINI, *Teoria delle Sostituzioni, equazione ternaria,* p. 220).

Bourg-la-Reine, avril 1904.