ANNALES SCIENTIFIQUES DE L'É.N.S.

RAYMOND LE VAVASSEUR

Les groupes d'ordre p^2q^2, p étant un nombre premier plus grand que le nombre premier q

Annales scientifiques de l'É.N.S. 3^e série, tome 19 (1902), p. 335-355

<http://www.numdam.org/item?id=ASENS_1902_3_19__335_0>

© Gauthier-Villars (Éditions scientifiques et médicales Elsevier), 1902, tous droits réservés.

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

NUMDAM

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

LES GROUPES D'ORDRE p^2q^2,

p ÉTANT UN NOMBRE PREMIER PLUS GRAND QUE LE NOMBRE PREMIER q,

PAR M. RAYMOND LE VAVASSEUR.

1. Le groupe cherché contient un sous-groupe d'ordre p^2. On a

$$p^2q^2 = p^2m(1+hp) \qquad \text{(théorème de Sylow)};$$

donc

$$q^2 = m(1+hp).$$

On ne peut avoir $m=1$ que si p divise q^2-1, c'est-à-dire si $q=2$, $p=3$; $m=q$ donne $q=1+hp$, ce qui est impossible.

Ainsi, *sauf dans le cas où l'ordre du groupe est égal à* 36, *il y a nécessairement dans le groupe cherché un sous-groupe d'ordre* p^2 *conjugué de lui-même.*

Nous séparerons la discussion en trois parties :

I. Le sous-groupe Γ, d'ordre p^2, conjugué de lui-même est G_{p^2} (1);

II. Le sous-groupe Γ est $(G_p)^2$;

III. Groupes d'ordre 36 n'admettant pas un groupe, d'ordre 9, conjugué de lui-même.

2 (I). Le sous-groupe conjugué de lui-même est G_{p^2}.

1° Le groupe admet une opération d'ordre q^2. On a

$$a^{p^2} = b^{q^2} = 1, \qquad ab = ab^{\alpha},$$

avec $\alpha^{q^2} \equiv 1 \pmod{p^2}$; $\alpha = 1$ donne

$$G_{p^2q^2} = G_{p^2}G_{q^2}.$$

(1) Pour les diverses notations dont il est fait usage dans ce Travail, consulter mon Mémoire : *Énumération des groupes d'opérations d'ordre donné* (Paris, A. Hermann, ou Toulouse, Privat).

3. $G^1_{p^2q^2}$ est défini par les équations

$$a^{p^2} = b^{q^2} = 1, \qquad ab = ba^{\alpha},$$

α appartenant à l'exposant $q \pmod{p^2}$.

4. $G^2_{p^2q^2}$ est défini par les équations

$$a^{p^2} = b^{q^2} = 1, \qquad ab = ba^{\alpha},$$

α appartenant à l'exposant $q^2 \pmod{p^2}$.

5. 2° Le groupe n'admet pas d'opérations d'ordre q^2. On a

$$a^{p^2} = b^q = c^q = 1,$$
$$ab = ba^{\beta} \quad \text{avec} \quad \beta^q \equiv 1 \pmod{p^2},$$
$$ac = ca^{\gamma} \quad \text{avec} \quad \gamma^q \equiv 1 \pmod{p^2}.$$

Si $\beta = \gamma = 1$, on a le groupe décomposable

$$G_{p^2}(G_q)^2 = G_{p^2q}G_q.$$

6. Si $\beta = 1$, tandis que γ appartient à l'exposant $q \pmod{p^2}$, on a encore un groupe décomposable

$$G^1_{p^2q}G_q.$$

7. Supposons que β et γ appartiennent tous les deux à l'exposant $q \pmod{p^2}$; on a

$$a^{\beta}c^{\rho} = c^{\rho}a^{\beta\gamma^{\rho}},$$
$$abc^{\rho} = ba^{\beta}c^{\rho} = bc^{\rho}a^{\beta\gamma^{\rho}}.$$

Mais on a

$$\gamma = \beta^h, \qquad h \not\equiv 0.$$

La congruence $\beta\gamma^{\rho} \equiv 1 \pmod{p^2}$ devient

$$\beta^{1+h\rho} \equiv 1 \pmod{p^2}.$$

Il suffira de déterminer ρ par la condition

$$1 + h\rho \equiv 0 \pmod{q}.$$

Prenant alors $bc^{\rho} = b'$ au lieu de b comme opération génératrice, on a

$$ab' = b'a.$$

On retrouve

$$G^1_{p^2q}G_q.$$

8 (II). Le sous-groupe Γ est $(G_p)^2$.

Le sous-groupe Γ sera engendré par deux opérations a et b, d'ordre p, permutables l'une avec l'autre,

$$a^p = b^p = 1, \qquad ab = ba.$$

(1) Supposons que G contienne une opération c d'ordre q^2

$$c^{q^2} = 1, \qquad \{a, b\}c = c\{a, b\};$$

on aura

$$ac = ca^\alpha b^\beta,$$
$$bc = ca^\gamma b^\delta,$$
$$a^x b^y c = ca^{\alpha x+\gamma y} b^{\beta x+\delta y}.$$

A l'isomorphisme du groupe $\{a, b\}$ ainsi déterminé correspond une substitution linéaire faite sur les exposants

$$s = |x, y; \alpha x + \gamma y, \beta x + \delta y|,$$

les nombres α, β, γ, δ étant pris suivant le module p.

Il faut que l'on ait

$$s^{q^2} = 1.$$

Pour qu'il existe des sous-groupes d'ordre p du groupe $\{a, b\}$ avec lesquels l'opération c soit permutable, il faut que la congruence

$$\sigma^2 - \sigma(\alpha + \delta) + \alpha\delta - \beta\gamma \equiv 0 \pmod p$$

admette des solutions (1).

σ étant l'une de ces solutions, on pourra trouver des nombres x et y tels que l'on ait

$$(a^x b^y)c = c(a^x b^y)^\sigma.$$

On aura donc

$$\sigma^{q^2} \equiv 1 \pmod p.$$

Soient l le nombre des sous-groupes d'ordre p du groupe $\{a, b\}$ avec lesquels c est permutable, m et n les nombres des ensembles de q et

(1) Voir *Énumération des groupes d'opérations*, Chap. VII, p. 40. Paris, Hermann.

de q^2 sous-groupes d'ordre p de $\{a, b\}$, respectivement, tels que c transforme les uns dans les autres les sous-groupes d'un même ensemble; on a

$$l(p-1)+mq(p-1)+nq^2(p-1)=p^2-1$$

ou

$$l+mq+nq^2=p+1.$$

De cette formule on tire la conclusion suivante :

Si la congruence (1) *est irréductible, alors l est nul, et l'on voit que q sera nécessairement un diviseur de* $p+1$.

9. Nous allons maintenant distinguer deux cas :

a. La congruence (1) n'est pas irréductible;

b. Elle est irréductible.

a. La congruence (1) n'est pas irréductible. On ne peut avoir $l=1$, car on en conclurait

$$mq+nq^2=p,$$

q devrait diviser p, ce qui est impossible.

On a donc, au moins,

$$l=2.$$

Nous pouvons supposer que c est permutable avec $\{a\}$ et avec $\{b\}$. On aura

$$ac=ca^{\alpha}, \quad \text{avec} \quad \alpha^{q^2}\equiv 1 \pmod{p},$$
$$bc=cb^{\beta}, \quad \text{avec} \quad \beta^{q^2}\equiv 1 \pmod{p}.$$

Si $\alpha=\beta=1$, on a le groupe décomposable

$$(G_p)^2 G_{q^2}.$$

10. Si $\alpha=1$, tandis que β appartient à l'exposant $q \pmod{p}$, on a le groupe décomposable

$$G^1_{pq^2} G_p \ (^1).$$

11. Si $\alpha=1$, tandis que β appartient à l'exposant $q^2 \pmod{p}$, on a

(1) Voir *Énumération des groupes d'opérations*, p. 33.

le groupe décomposable

$$G^2_{pq^2} G_p \ (^1).$$

12. Prenons le cas où α et β appartiennent tous les deux à l'exposant $q \pmod p$. On aura

$$\beta = \alpha^r, \qquad r \not\equiv 0.$$

Les groupes $G^{1,r}_{p^2q^2}$ correspondants sont définis par les équations

$$a^p = b^p = c^{q^2} = 1, \qquad ab = ba, \qquad ac = ca^\alpha, \qquad bc = cb^{\alpha^r},$$

où α appartient à l'exposant $q \pmod p$. On a

$$a^x b^y a^\lambda b^\mu c^\nu = a^\lambda b^\mu c^\nu a^{x\alpha^\nu} b^{y\alpha^{r\nu}}.$$

Pour que $a^\lambda b^\mu c^\nu$ soit permutable avec le groupe $\{a^x, b^y\}$, il faut ou bien que l'on ait

$$x = 0, \qquad \text{ou bien} \qquad y = 0, \qquad \text{ou enfin} \qquad r = 1.$$

Si $r = 1$, chacun des $p + 1$ sous-groupes d'ordre p du groupe $\{a, b\}$ est conjugué de lui-même dans le groupe total.

Dans l'équation

$$l + mq + nq^2 = p + 1,$$

on a

$$m = n = 0.$$

Le groupe pour lequel $r = 1$ doit être mis à part.

Si r est différent de 1, les groupes $\{a\}$ et $\{b\}$ sont les seuls groupes d'ordre p conjugués d'eux-mêmes. On a

$$l = 2, \qquad n = 0, \qquad ac = ca^\alpha, \qquad bc = cb^{\alpha^r}.$$

Changeons c en c^{r_1} avec $r_1 r \equiv 1 \pmod q$. On a

$$ac^{r_1} = c^{r_1} a^{\alpha^{r_1}}, \qquad bc^{r_1} = c^{r_1} b^\alpha.$$

Permutons a et b, prenons c^{r_1} au lieu de c comme opération génératrice; on trouve le groupe correspondant à r_1.

On voit donc qu'après avoir pris à part le cas $r = 1$ et le cas

---

(1) Voir *Énumération des groupes d'opérations*, p. 33.

$r = q - 1$, deux valeurs de r associées $(\mathrm{mod}\, q)$ donnent le même groupe.

Si $q = 2$, on a un seul groupe $G_{p^2 4}^{1,1}$.

Si $q \geq 3$, le nombre des groupes $G_{p^2 q^2}^{1,r}$ est

$$\frac{q-3}{2} + 2 = \frac{q+1}{2}.$$

13. Nous arrivons au cas où α appartient à l'exposant q $(\mathrm{mod}\, p)$ et β à l'exposant q^2 $(\mathrm{mod}\, p)$.

On pourra alors supposer

$$\alpha = \beta^{q^r} \qquad (r \text{ premier avec } q).$$

Les groupes $G_{p^2 q^2}^{2,r}$ sont définis par les équations

$$a^p = b^p = c^{q^2} = 1, \qquad ab = ba, \qquad ac = ca^{\beta^{rq}}, \qquad bc = cb^{\beta},$$

où β appartient à l'exposant q^2 $(\mathrm{mod}\, p)$. On a

$$a^\lambda b^\mu c^\nu = c^\nu a^{\lambda \beta^{\nu r q}} b^{\mu \beta^\nu}.$$

Les groupes $\{a\}$ et $\{b\}$ sont les seuls groupes d'ordre p de $\{a, b\}$ conjugués d'eux-mêmes dans le groupe total.

On voit qu'il y a ainsi $q - 1$ groupes $G_{p^2 q^2}^{2,r}$.

14. Enfin, supposons que α et β appartiennent simultanément à l'exposant q^2 $(\mathrm{mod}\, p)$. On a

$$\beta = \alpha^r \qquad (r \text{ premier avec } q).$$

Les groupes $G_{p^2 q^2}^{(3,r)}$ sont définis par les équations

$$a^p = b^p = c^{q^2} = 1, \qquad ab = ba, \qquad ac = ca^{\alpha}, \qquad bc = cb^{\alpha^r},$$

où α appartient à l'exposant q^2 $(\mathrm{mod}\, p)$, r étant premier avec q.

On a

$$a^\lambda b^\mu c^\nu = c^\nu a^{\lambda \alpha^\nu} b^{\mu \alpha^{r\nu}}.$$

Le cas $r = 1$ doit encore être mis à part : le groupe correspondant est tel que les $p + 1$ sous-groupes correspondants d'ordre p du groupe $\{a, b\}$ sont conjugués d'eux-mêmes dans le groupe total. Pour

les autres valeurs de r, deux valeurs de r associées $(\mathrm{mod}\, q^2)$, c'est-à-dire telles que $rr' \equiv 1 \pmod{q^2}$, donnent le même groupe.

D'ailleurs, la congruence $x^2 \equiv 1 \pmod{q^2}$ admet les deux racines 1 et $q^2 - 1$.

Donc, il y a

$$\frac{q(q-1)-2}{2} + 2 = \frac{q(q-1)+2}{2}$$

groupes $G^{3,r}_{p^2q^2}$ $(q \geqq 3)$.

Pour $q = 2$, il y a seulement deux groupes au plus,

$$G^{3,1}_{4p^2}, \quad G^{3,2}_{4p^2}.$$

15. *b*. La congruence (1) est irréductible.

Nous avons vu que, dans ce cas, q divise $p + 1$.

On peut choisir les opérations a et b, d'ordre p, de façon que l'une soit la transformée de l'autre au moyen de l'opération c, d'ordre q^2. La substitution

$$s = |x, y;\ \alpha x + \gamma y,\ \beta x + \delta y|$$

devient, puisqu'on a $\alpha = 0$, $\beta = 1$,

$$s = |x, y;\ \gamma y,\ x + \delta y|.$$

1° Examinons d'abord le cas où $q = 2$:

On a

$$s^2 = |x, y;\ \gamma x + \gamma\delta y,\ \delta x + (\gamma + \delta^2) y|,$$

puis

$$s^4 = |x, y;\ \gamma(\gamma + \delta^2) x + \gamma\delta(2\gamma + \delta^2) y,\quad \delta(2\gamma + \delta^2) x + (3\gamma\delta^2 + \gamma^2 + \delta^4) y|.$$

Comme $s^4 = 1$, on doit avoir, ou

$$\delta \equiv 0 \pmod{p},$$

ou

$$2\gamma + \delta^2 \equiv 0 \pmod{p};$$

puis

$$\gamma^2 + \gamma\delta \equiv 1 \pmod{p}$$

et

$$\gamma^2 + \gamma\delta^2 + 2\gamma\delta^2 + \delta^4 \equiv 1 \pmod{p}.$$

Soit d'abord

$$\delta \equiv 0 \pmod{p},$$
$$\gamma^2 \equiv 1 \pmod{p},$$

$\delta = 0$, $\gamma = 1$ donne

$$s = |x, y; y, x|,$$
$$a^x b^y c = c a^y b^x, \qquad ac = cb, \qquad bc = ca,$$

alors

$$abc = cba = cab.$$

Il existerait donc un sous-groupe $|ab|$, avec lequel c serait permutable.

16. $\delta = 0$, $\gamma = -1$ donnent

$$s = |x, y; -y, x|,$$
$$a^x b^y c = c a^{-y} b^x, \qquad ac = cb, \qquad bc = ca^{-1}.$$

Les congruences

$$x \equiv -\sigma y \pmod p,$$
$$y \equiv \sigma x \pmod p$$

donnent

$$\sigma^2 + 1 \equiv 0 \pmod p.$$

Nous devons nous placer dans le cas où cette congruence est irréductible. p doit donc être de la forme $4m + 3$.

Soit i une racine (imaginaire de Galois) de la congruence irréductible

$$x^2 + 1 \equiv 0 \qquad [\mathrm{mod}(p = 4m + 3)].$$

Posons $b = a^i$ (en introduisant les exposants imaginaires de Galois). On a alors

$$ac = ca^i, \qquad ac^2 = c^2 a^{i^2} = c^2 a^{-1}, \qquad ac^3 = c^3 a^{-i}, \qquad ac^4 = c^4 a.$$

Le groupe $G^3_{4p^2}$ est défini par les équations

$$a^{(p, i^2+1)} = b^4 = 1, \qquad ab = ba^i \qquad (p = 4m + 3).$$

17. Supposons maintenant

$$2\gamma + \delta^2 \equiv 0 \pmod p,$$
$$\gamma^2 + \gamma\delta^2 \equiv 0 \pmod p,$$

d'où

$$\gamma^2 \equiv -1 \pmod p.$$

p devra donc être de la forme $4m + 1$, car il faut que γ soit réel. La congruence

$$\delta^2 \equiv (-2\gamma) \pmod p$$

n'admet de racine que si l'on a

$$(-2\gamma)^{\frac{p-1}{2}} = (-2\gamma)^{2m} \equiv 1 \pmod{p}.$$

Mais si l'on a

$$(-2\gamma)^{2m} \equiv 1 \pmod{p}$$

on a aussi

$$(2\gamma)^{2m} \equiv 1 \pmod{p}.$$

Or

$$ac = cb, \qquad bc = ca^{\gamma}b^{\delta}, \qquad a^{\lambda}b^{\mu}c = ca^{\gamma\mu}b^{\lambda+\delta\mu}.$$

Les congruences

$$\gamma\mu \equiv \sigma\lambda \pmod{p},$$
$$\lambda + \delta\mu \equiv \sigma\mu \pmod{p}$$

exigent, pour être compatibles, que σ vérifie la congruence

$$\sigma^2 - \delta\sigma \equiv \gamma \pmod{p},$$

ou

$$(2\sigma - \delta)^2 \equiv \delta^2 + 4\gamma \equiv 2\gamma \pmod{p}.$$

Mais cette congruence n'est pas irréductible, puisque

$$(2\gamma)^{2m} \equiv (2\gamma)^{\frac{p-1}{2}}$$

est congru à 1 $(\mathrm{mod}\, p)$.

18. Supposons maintenant q premier impair.

On doit avoir

$$(-\gamma)^{q^2} \equiv 1 \pmod{p}.$$

Or q est impair et divise $p+1$; donc il ne divise pas $p-1$. Donc $\gamma = -1$,

$$s = |x, y; -y, x + \delta y|.$$

En raisonnant comme nous l'avons déjà fait en un problème analogue (1), on a

$$\delta = j + j^p, \qquad j^{p+1} \equiv 1,$$

et enfin

$$j^{q^2} \equiv 1 \qquad (\mathrm{modd}\, p,\ x^2 - u),$$

u étant non résidu quadratique $(\mathrm{mod}\, p)$.

---

(1) Voir *Énumération des groupes d'opérations*, p. 58.

Deux cas sont à distinguer :

1° j appartient à l'exposant q (modd p, $x^2 - u$).

Alors $s^q = 1$, c^q est permutable à toutes les opérations du groupe.

Le groupe $G^3_{p^2q^2}$ est défini par les équations

$$a^{(p,x^2-u)} = b^{q^2} = 1, \qquad ab = ba^j,$$

j appartient à l'exposant q (modd p, $x^2 - u$). q divise $p + 1$, q est premier impair, u est non résidu quadratique (mod p).

19. 2° j appartient à l'exposant q^2 (modd p, $x^2 - u$); ceci exige que q^2 divise $p + 1$.

Le groupe $G^4_{p^2q^2}$ est défini par les équations

$$a^{(p,x^2-u)} = b^{q^2} = 1, \qquad ab = ba^j,$$

q premier impair, j appartient à l'exposant q^2 (modd p, $x^2 - u$), u est non résidu quadratique (mod p).

Le groupe $G^4_{4p^2}$ rentre dans cette catégorie.

20. (2) Supposons maintenant que le groupe ne contienne pas d'opération d'ordre q^2.

Comme il contient au moins un sous-groupe d'ordre q^2, il admettra au moins deux sous-groupes distincts d'ordre q permutables l'un avec l'autre. On pourra prendre comme opérations génératrices deux opérations a et b d'ordre p, permutables l'une avec l'autre, et deux opérations c et d d'ordre q, permutables l'une avec l'autre.

Les opérations $c^\lambda d^\mu$ devront être toutes permutables avec le groupe $\{a, b\}$.

On a

$$\{a, b\}\{c, d\} = \{c, d\}\{a, b\}.$$

Première hypothèse. — Le groupe $\{a, b\}$ contient au moins deux sous-groupes d'ordre p avec chacun desquels c et d sont séparément permutables.

On a

$$\left.\begin{array}{ll} ac = ca^\alpha, & \alpha^q \equiv 1 \\ ad = da^{\alpha'}, & \alpha'^q \equiv 1 \\ bc = cb^\beta, & \beta^q \equiv 1 \\ bd = db^{\beta'}, & \beta'^q \equiv 1 \end{array}\right\} \pmod p.$$

Alors

$$a^{\lambda}b^{\mu}c^{\lambda'}d^{\mu'}=a^{\lambda}c^{\lambda'}b^{\mu}\beta^{\lambda'}d^{\mu'}=c^{\lambda'}a^{\lambda}\alpha^{\lambda'}d^{\mu'}b^{\mu}\beta^{\lambda'}\beta'^{\mu'}=c^{\lambda'}d^{\mu'}a^{\lambda}\alpha^{\lambda'}\alpha'^{\mu'}b^{\mu}\beta^{\lambda'}\beta'^{\mu'}.$$

L'hypothèse est acceptable.

Si $\alpha=\beta=\alpha'=\beta'=1$, on trouve

$$(G_{pq})^2=(G_p)^2(G_q)^2=G_pG_qG_{pq}.$$

21. Si $\alpha=\beta=\alpha'=1$, β' appartenant à l'exposant $q\pmod p$, on a le groupe décomposable

$$G^1_{pq}G_pG_q=G^1_{pq}G_{pq}.$$

22. Si $\alpha=\beta=1$, tandis que α' et β' appartiennent tous les deux à l'exposant $q\pmod p$, on trouve les groupes

$$G^{2,r}_{p^2q}G_q \quad (1).$$

23. Supposons qu'on ait $\alpha=\alpha'=1$, tandis que β et β' appartiennent à l'exposant $q\pmod p$; l'opération a, conjuguée d'elle-même, se sépare. Les opérations b, c, d engendrent le groupe

$$G^1_{pq}G_q \quad (2).$$

On retrouve donc

$$G^1_{pq}G_{pq}.$$

24. Supposons $\alpha=\beta'=1$, tandis que β et α' appartiennent à l'exposant $q\pmod p$. On a

$$ac=ca, \qquad ad=da^{\alpha'},$$
$$bc=cb^{\beta}, \qquad bd=db.$$

On pourra supposer

$$\alpha'=\beta=\alpha.$$

Les opérations a, d engendrent un groupe G^1_{pq}; de même, les opérations b, c; d'ailleurs, toute opération du groupe $\{a, d\}$ est permutable avec toute opération de $\{b, c\}$.

On trouve donc ainsi le groupe

$$(G^1_{pq})^2.$$

---

(1) Voir *Énumération des groupes d'opérations*, p. 57.

(2) *Loc. cit.*, p. 32, 33.

25. Si $\alpha = 1$, tandis que β, α', β' appartiennent à l'exposant q (mod p), on a

$$ac = ca, \qquad ad = da^{\alpha'},$$
$$bc = cb^{\beta}, \qquad bd = db^{\beta'}.$$

Soit $\beta' = \beta^r$

$$bc^{\lambda}d = c^{\lambda}b^{\beta^{\lambda}}d = c^{\lambda}db^{\beta^{\lambda+r}};$$

donc l'opération $c^{-r}d$ est permutable avec b.

On retrouve le groupe

$$(G^1_{pq})^2.$$

26. Supposons enfin que les quatre nombres α, β, α', β' appartiennent tous les quatre à l'exposant q (mod p).

On peut, sans nuire à la généralité de nos considérations, supposer que l'on a

$$ac = ca^{\alpha}, \qquad ad = da^{\alpha},$$
$$bc = cb^{\alpha''}, \qquad bd = db^{\alpha''},$$

α appartient à l'exposant q (mod p).

On en déduit

$$ad^{-1} = d^{-1}a^{\alpha^{-1}},$$
$$acd^{-1} = ca^{\alpha}d^{-1} = cd^{-1}a.$$

Prenant $cd^{-1} = c'$ au lieu de c comme opération génératrice, on est ramené au cas précédent.

27. *Deuxième hypothèse.* — La première hypothèse revient à supposer qu'il existe au moins deux sous-groupes d'ordre p du groupe $\{a, b\}$, conjugués d'eux-mêmes dans le groupe total $\{a, b, c, d\}$.

Nous allons, actuellement, supposer qu'il n'y a qu'un sous-groupe d'ordre p, conjugué de lui-même dans le groupe total.

Cette hypothèse est inadmissible : en effet, soit $\{a\}$ le sous-groupe d'ordre p conjugué de lui-même dans le groupe total.

L'opération c, d'ordre q, étant déjà permutable avec le sous-groupe $\{a\}$, sera permutable à *deux* sous-groupes d'ordre p, au moins, dans le groupe $\{a, b\}$.

On peut supposer que $\{b\}$ est le deuxième sous-groupe d'ordre p avec lequel c est permutable.

Alors on aura

$$ac = ca^{\alpha}, \qquad bc = cb^{\beta}$$
$$ad = da^{\gamma}, \qquad bd = da^{\lambda}b^{\mu}.$$

1° On doit avoir $\alpha \neq \beta$.

En effet, si l'on avait $\alpha = \beta$, c serait permutable avec les $p+1$ sous-groupes d'ordre p du groupe $\{a, b\}$, et comme d est permutable avec *deux* d'entre eux au moins, il existerait deux sous-groupes d'ordre p conjugués d'eux-mêmes dans le groupe total. C'est contraire à l'hypothèse.

2° A l'isomorphisme du groupe $\{a, b\}$ en lui-même, obtenu en le transformant par l'opération c, correspond la substitution d'ordre q

$$s = |x, y; \quad \alpha x, \quad \beta y|.$$

A l'isomorphisme du groupe $\{a, b\}$ en lui-même obtenu en le transformant par l'opération d, correspond la substitution d'ordre q

$$t = |x, y; \quad \gamma x + \lambda y, \quad \mu y|.$$

Puisqu'on a $cd = dc$, on en déduit $st = ts$.

Or

$$st = |x, y; \quad \gamma\alpha x + \lambda\beta y, \quad \mu\beta y|,$$
$$ts = |x, y; \quad \alpha\gamma x + \alpha\lambda y, \quad \mu\beta y|.$$

Donc on a $\alpha = \beta$, puisque λ est différent de zéro.

Il y a contradiction.

28. *Troisième hypothèse.* — Il existe des sous-groupes d'ordre p du groupe $\{a, b\}$ avec lesquels c est permutable; il existe des sous-groupes d'ordre p du groupe $\{a, b\}$ avec lesquels d est permutable; mais il n'y a pas, dans le groupe total, de sous-groupe d'ordre p conjugué de lui-même.

Cette hypothèse est inacceptable.

En effet, on aurait

$$a^p = b^p = c^q = d^q = 1, \qquad ab = ba, \qquad cd = dc,$$
$$ac = ca^{\alpha}, \qquad bd = db^{\beta},$$
$$ad = da^{\gamma}b^{\lambda}, \qquad bc = ca^{\mu}b^{\delta},$$

d'où les substitutions

$$\begin{aligned} s &= |x, y;\quad \alpha x + \mu y,\quad \delta y|,\\ t &= |x, y;\quad \gamma x,\quad \lambda x + \beta y|,\\ st &= |x, y;\quad \gamma\alpha x + \gamma\mu y,\quad \lambda\alpha x + (\lambda\mu + \beta\delta) y|,\\ ts &= |x, y;\quad (\alpha\gamma + \mu\lambda) x + \beta\mu y,\quad \delta\lambda x + \beta\delta y|. \end{aligned}$$

L'égalité $st = ts$ exige $\lambda\mu \equiv 0 \pmod p$, tandis que, d'autre part, l'hypothèse exige que λ et μ soient l'un et l'autre différents de zéro.

29. *Quatrième hypothèse.* — Il existe des sous-groupes d'ordre p du groupe $\{a, b\}$ avec lesquels c est permutable; mais d n'est permutable avec aucun des sous-groupes d'ordre p.

1° Imaginons que c soit permutable avec *toutes* les opérations du groupe $\{a, b\}$.

On a alors le groupe

$$G^3_{p^2q} G_q \ (^1).$$

30. 2° Si l'opération c n'est pas permutable avec toutes les opérations du groupe $\{a, b\}$, alors q doit diviser $p - 1$; mais, d'après l'hypothèse faite sur d, q doit aussi diviser $p + 1$; donc $q = 2$.

On a

$$\begin{aligned} ac &= ca^{\alpha}, \qquad bc = cb^{\beta}, \qquad \alpha, \beta = \pm 1,\\ ad &= da^{\lambda} b^{\mu},\\ bd &= da^{\lambda'} b^{\mu'}. \end{aligned}$$

J'en déduis

$$\begin{aligned} ad^2 &= da^{\lambda} b^{\mu}\, d = da^{\lambda}\, da^{\mu\lambda'} b^{\mu\mu'} = d^2 a^{\lambda^2 + \mu\lambda'} b^{\lambda\mu + \mu'\mu},\\ bd^2 &= da^{\lambda'} b^{\mu'} d = da^{\lambda'}\, da^{\lambda'\mu'} b^{\mu'^2} = d^2 a^{\lambda\lambda' + \lambda'\mu'} b^{\lambda'\mu + \mu'^2}, \end{aligned}$$

d'où

$$\lambda^2 + \mu\lambda' \equiv 1, \qquad \lambda + \mu' \equiv 0, \qquad \lambda'\mu + \mu'^2 \equiv 1 \pmod p,$$

donc

$$\begin{gathered} \mu' \equiv -\lambda, \qquad \mu\lambda' + \lambda^2 \equiv 1 \pmod p,\\ a^x b^y d = da^{\lambda x + \lambda' y} b^{\mu x - \lambda y}. \end{gathered}$$

Les congruences

$$\begin{aligned} \lambda x + \lambda' y &\equiv \sigma x\\ \mu x - \lambda y &\equiv \sigma y \end{aligned} \pmod p$$

(1) Voir *Énumération des groupes d'opérations*, p. 60.

seront compatibles si l'on a

$$\sigma^2 - \lambda^2 - \mu\lambda' \equiv 0 \pmod{p},$$

et, par suite,

$$\sigma \equiv \pm 1.$$

Il existe donc des groupes d'ordre p auxquels d est permutable.

31. *Cinquième hypothèse.* — Aucune opération du groupe $\{c, d\}$ n'est permutable avec un groupe d'ordre p de $\{a, b\}$.

D'après ce que nous avons démontré (¹), les substitutions à congruence caractéristique irréductible se répartissent en groupes cycliques J formant une suite complète unique de sous-groupes conjugués : donc deux isomorphismes correspondant à de telles substitutions ne peuvent être permutables que si l'un est une puissance de l'autre.

Donc la cinquième hypothèse est inadmissible.

32 (III). Il nous reste à nous occuper des groupes particuliers à l'ordre 36 pour lesquels il n'y a pas de sous-groupe d'ordre q conjugué de lui-même.

Soit G le groupe cherché, d'ordre 36; Γ un sous-groupe de G, conjugué de lui-même, et d'ordre maximum; $\frac{G}{\Gamma}$ sera un groupe simple; car si $\frac{G}{\Gamma}$ admettait un sous-groupe conjugué de lui-même qui ne fût pas uniquement composé de l'opération identique, G admettrait un sous-groupe conjugué de lui-même dont l'ordre dépasserait l'ordre de Γ.

Le groupe $\frac{G}{\Gamma}$ ne peut être que d'ordre 2 ou 3, car il n'y a pas de groupe simple d'ordre 36. En effet, on a

$$36 = 9m(3h+1) \qquad \text{(théorème de Sylow).}$$

Donc

$$4 = m(3h+1).$$

Comme par hypothèse il n'y a pas de sous-groupe conjugué de lui-

(¹) Voir *Énumération des groupes d'opérations*, p. 52.

même, d'ordre 9, on a

$$m = h = 1.$$

Supposons que les quatre groupes transformés d'ordre 9 n'aient pas d'autre opération commune que l'opération identique, alors on a 32 opérations dont l'ordre est multiple de 3, et 3 opérations d'ordre 2 : donc un sous-groupe d'ordre 4, conjugué de lui-même.

Si les quatre groupes d'ordre 9 admettaient des opérations communes, on aurait un sous-groupe d'ordre 3 conjugué de lui-même.

$\frac{G}{\Gamma}$ ne peut donc être que d'ordre 2 ou 3.

Donc Γ sera ou d'ordre 18, ou d'ordre 12.

S'il est d'ordre 18, il admet un sous-groupe conjugué de lui-même et d'ordre 9 (1). Comme 9 et $\frac{18}{9} = 2$ sont des nombres premiers entre eux, ce sera aussi un sous-groupe conjugué de lui-même dans le groupe total G (théorème de Fröbenius).

Donc Γ sera d'ordre 12.

Nous avons donc à étudier les groupes d'isomorphismes des groupes d'ordre 12.

33. Groupe des isomorphismes de G_{12}

$$(a^{12} = 1).$$

Il y a 4 isomorphismes : l'isomorphisme identique 1, puis les isomorphismes

$$\begin{aligned} u &= (a, a^5)(a^2, a^{10})(a^4, a^8)(a^7, a^{11}), \\ v &= (a, a^7)(a^3, a^9)(a^5, a^{11}), \\ uv &= (a, a^{11})(a^2, a^{10})(a^3, a^9)(a^4, a^8)(a^5, a^7). \end{aligned}$$

Il n'y a pas, pour G_{12}, d'isomorphisme d'ordre 3.

$G_{12}G_3$ et G_4G_9 contiennent un sous-groupe conjugué de lui-même d'ordre 9.

34. Groupe des isomorphismes de $G_3(G_2)^2$.

---

(1) Voyez *Énumération des groupes d'opérations*, p. 53.

Soient

$$\alpha^3 = \beta^2 = \gamma^2 = 1$$

les équations de définition (1).

Il y a 12 isomorphismes, savoir :

1,
$(\gamma, \beta\gamma)(\alpha\gamma, \alpha\beta\gamma)(\alpha^2\gamma, \alpha^2\beta\gamma)$,
$(\beta, \gamma)(\alpha\beta, \alpha\gamma)(\alpha^2\beta, \alpha^2\gamma)$,
$(\beta, \beta\gamma)(\alpha\beta, \alpha\beta\gamma)(\alpha^2\beta, \alpha^2\beta\gamma)$,
$(\beta, \gamma, \beta\gamma)(\alpha\beta, \alpha\gamma, \alpha\beta\gamma)(\alpha^2\beta, \alpha^2\gamma, \alpha^2\beta\gamma)$,
$(\beta, \beta\gamma, \gamma)(\alpha\beta, \alpha\beta\gamma, \alpha\gamma)(\alpha^2\beta, \alpha^2\beta\gamma, \alpha^2\gamma)$,
$(\alpha, \alpha^2)(\alpha\beta, \alpha^2\beta)(\alpha\gamma, \alpha^2\gamma)(\alpha\beta\gamma, \alpha^2\beta\gamma)$,
$(\alpha, \alpha^2)(\alpha\beta, \alpha^2\beta)(\alpha\gamma, \alpha^2\beta\gamma)(\alpha^2\gamma, \alpha\beta\gamma)(\gamma, \beta\gamma)$,
$(\alpha, \alpha^2)(\beta, \gamma)(\alpha\beta, \alpha^2\gamma)(\alpha^2\beta, \alpha\gamma)(\alpha\beta\gamma, \alpha^2\beta\gamma)$,
$(\alpha, \alpha^2)(\beta, \beta\gamma)(\alpha\beta, \alpha^2\beta\gamma)(\alpha^2\beta, \alpha\beta\gamma)(\alpha\gamma, \alpha^2\gamma)$,
$(\alpha, \alpha^2)(\beta, \gamma, \beta\gamma)(\alpha\beta, \alpha^2\gamma, \alpha\beta\gamma, \alpha^2\beta, \alpha\gamma, \alpha^2\beta\gamma)$,
$(\alpha, \alpha^2)(\beta, \beta\gamma, \gamma)(\alpha\beta, \alpha^2\beta\gamma, \alpha\gamma, \alpha^2\beta, \alpha\beta\gamma, \alpha^2\gamma)$.

35. $(G_3)^2(G_2)^2$ et $G_9(G_2)^2$ ont chacun un sous-groupe distingué d'ordre 9.

36. Soit

$$a^3 = b^2 = c^2 = 1, \qquad ab = ba, \qquad ac = ca, \qquad bc = cb.$$

Soit d une opération d'ordre 3 permutable avec a et telle que $\overline{d} = (b, c, bc)$.

On trouve ainsi

$$G_3 G_{12}^3.$$

37. Soit d une opération d'ordre 9 (d est alors permutable avec a) et telle que $\overline{d} = (b, c, bc)$.

---

(1) Les lettres grecques désignent des opérations permutables deux par deux.

G_{36}^{5} est défini par les équations

$$a^9 = b^2 = c^2 = 1, \qquad bc = cb, \qquad \overline{a} = (b, c, bc).$$

38. Si l'on voulait adjoindre à $G_3(G_2)^2$ une opération d'ordre 6, son carré devrait être égal à l'une des opérations d'ordre 2.

Elle ne pourrait donc donner lieu à l'un des deux derniers isomorphismes énumérés ci-dessus (n° 34).

39. Groupe des isomorphismes de $G_6^1 G_2$

$$(a^3 = b^2 = \alpha^2 = 1, \ ab = ba^2).$$

Il y a 12 isomorphismes, savoir :

$$1,$$
$$(b, ab, a^2 b)\,(b\alpha, ab\alpha, a^2 b\alpha),$$
$$(b, a^2 b, ab)\,(b\alpha, a^2 b\alpha, ab\alpha),$$
$$(b, b\alpha)\,(ab, ab\alpha)\,(a^2 b, a^2 b\alpha),$$
$$(b, ab\alpha, a^2 b, b\alpha, ab, a^2 b\alpha),$$
$$(a, a^2)\,(ab, a^2 b)\,(a\alpha, a^2\alpha)\,(ab\alpha, a^2 b\alpha),$$
$$(a, a^2)\,(b, ab)\,(a\alpha, a^2\alpha)\,(b\alpha, ab\alpha),$$
$$(a, a^2)\,(b, a^2 b)\,(a\alpha, a^2\alpha)\,(b\alpha, a^2 b\alpha),$$
$$(a, a^2)\,(b, b\alpha)\,(ab, a^2 b\alpha)\,(a\alpha, a^2\alpha)\,(ab\alpha, a^2 b),$$
$$(a, a^2)\,(b, ab\alpha)\,(ab, b\alpha)\,(a^2 b, a^2 b\alpha)\,(a\alpha, a^2\alpha),$$
$$(a, a^2)\,(a\alpha, a^2\alpha)\,(b, a^2 b\alpha)\,(b\alpha, a^2 b)\,(ab, ab\alpha).$$

40. $G_6^1 G_2 G_3$ contient un sous-groupe d'ordre 9 conjugué de lui-même.

Si une opération d'ordre 9, a, est permutable avec b, $a^3 = a'$ sera aussi permutable avec b.

Une opération d'ordre 6 dont le carré serait égal à a serait permutable avec a.

Une opération d'ordre 6 dont le cube serait égal à b serait permutable avec b.

Soit enfin une opération d, d'ordre 3, telle qu'on ait

$$\overline{d} = (b, ab, a^2b)(b\alpha, ab\alpha, a^2b\alpha).$$

L'opération α, dans le groupe

$$\{a, b, \alpha, d\},$$

se sépare. On a un groupe décomposable.

D'ailleurs

$$ad = ca, \qquad db = a^2bd = bad,$$
$$a^2db = a^2bad = ba^2d.$$

Soit $a^2d = c$; on a

$$a^3 = b^2 = c^3 = 1, \qquad ab = ba^2, \qquad ac = ca, \qquad bc = cb.$$

Bref, on retrouve

$$G_6^1 G_6.$$

41. Groupe des isomorphismes de G_{12}^1

$$(a^3 = b^4 = 1,\ ab = ba^2).$$

Il y a 12 isomorphismes, savoir : l'isomorphisme identique, puis

$$(b, b^3)(ab, ab^3)(a^2b, a^2b^3),$$
$$(b, ab, a^2b)(b^3, ab^3, a^2b^3),$$
$$(b, a^2b, ab)(b^3, a^2b^3, ab^3),$$
$$(b, ab^3, a^2b, b^3, ab, a^2b^3),$$
$$(b, a^2b^3, ab, b^3, a^2b, ab^3),$$
$$(a, a^2)(ab^2, a^2b^2)(ab, a^2b)(ab^3, a^2b^3),$$
$$(a, a^2)(b, b^3)(ab^2, a^2b^2)(ab, a^2b^3)(ab^3, a^2b),$$
$$(a, a^2)(ab^2, a^2b^2)(b, ab)(b^3, ab^3),$$
$$(a, a^2)(ab^2, a^2b^2)(b, a^2b)(b^3, a^2b^3),$$
$$(a, a^2)(ab^2, a^2b^2)(b, ab^3)(b^3, ab)(a^2b, a^2b^3),$$
$$(a, a^2)(ab^2, a^2b^2)(b, a^2b^3)(ab, ab^3)(b^3, a^2b).$$

42. Soit c une opération d'ordre 6, telle que

$$\{a, b, c\}$$

soit d'ordre 36.

On aurait $c^3 = b^2$; c est donc permutable avec b^2.

Soit, en outre,

$$\overline{c} = (b, ab^3, a^2b, b^3, ab, a^2b^3).$$

Alors on aurait

$$\overline{c}^3 = (b, b^3)(ab^3, ab)(a^2b, a^2b^3).$$

Or ceci est impossible, puisque $c^3 = b^2$.

Soit donc c une opération d'ordre 3, avec la condition

$$\overline{c} = (b, ab, a^2b)(b^3, ab^3, a^2b^3).$$

On aura alors $\overline{ac} = 1$.

D'ailleurs ac est d'ordre 3. Ce sera une opération conjuguée d'elle-même. Comme on pourra poser $ac = c'$, le groupe trouvé est

$$G^1_{12} G_3.$$

Il admet un sous-groupe d'ordre 9 conjugué de lui-même.

43. Nous nous sommes déjà occupé du groupe des isomorphismes de G^3_{12} (1). Il n'y a pas d'isomorphismes contragrédients d'ordre multiple de 3.

On n'a donc que le groupe

$$G^3_{12} G_3.$$

44. Résumé :

$$G_{p^2q^2} = G_{p^2} G_{q^2},$$
$$G_{p^2} (G_q)^2 = G_{p^2q} G_q,$$
$$G^1_{p^2} G_q,$$
$$G_{p^2q} G_q,$$
$$(G_p)^2 G_{q^2} = G_p G_{pq^2},$$
$$G^1_{pq^2} G_p,$$
$$G^2_{pq^2} G_p,$$
$$(G_{pq})^2 = (G_p)^2 (G_q)^2 = G_p G_q G_{pq},$$
$$G^1_{pq} G_{pq} = G^1_{pq} G_p G_q,$$
$$G^2_{p^2q^2} G_q, \quad (G^1_{pq})^2, \quad G^3_{p^2q} G_q, \quad G^3_{12} G_3.$$

(1) Voir *Énumération des groupes d'opérations*, p. 122.

$G^{1}_{p^2q^2}$ $[a^{p^2} = b^{q^2} = 1,\ ab = ba^{\alpha},\ \ \alpha$ appartient à l'exposant $q \pmod{p^2}]$,

$G^{2}_{p^2q^2}$ $[a^{p^2} = b^{q^2} = 1,\ ab = ba^{\alpha},\ \ \alpha$ appartient à l'exposant $q^2 \pmod{p^2}]$,

$G^{1,r}_{p^2q^2}$ $[a^{p} = b^{p} = c^{q^2} = 1,\ ab = ba,\ ac = ca^{\alpha},\ bc = cb^{\alpha^r}$,
α appartient à l'exposant $q \pmod{p}$, r est premier avec $q]$,

$G^{2,r}_{p^2q^2}$ $[a^{p} = b^{p} = c^{q^2} = 1,\ ab = ba,\ ac = ca^{\alpha},\ bc = cb^{\alpha^{rq}}$,
α appartient à l'exposant $q^2 \pmod{p}$, r est premier avec $q]$,

$G^{3,r}_{p^2q^2}$ $[a^{p} = b^{p} = c^{q^2} = 1,\ ab = ba,\ ac = ca^{\alpha},\ bc = cb^{\alpha^r}$,
α appartient à l'exposant $q^2 \pmod{p}$, r est premier avec $q]$,

$G^{4}_{4p^2}$ $[a^{(p,i^2+1)} = b^{4} = 1,\ ab = ba^{i}$,
p est un nombre premier de la forme $4m+3]$,

$G^{3}_{p^2q^2}$ $\left\{a^{(p,x^2-u)} = b^{q^2} = 1,\ ab = ba^{j}\right.$,
j appartient à l'exposant $q \pmod{(p, x^2-u)}$,
u est non résidu quadratique $(\mathrm{mod}\ p)$,
$\left.q \text{ est premier impair}\right\}$,

$G^{4}_{p^2q^2}$ $\left\{a^{(p,x^2-u)} = b^{q^2} = 1,\ ab = ba^{j}\right.$,
j appartient à l'exposant $q^2 \pmod{(p, x^2-u)}$,
u est non résidu quadratique $(\mathrm{mod}\ p)$,
$\left.q \text{ est premier impair}\right\}$,

G^{5}_{36} $[a^{(2,x^2-x-1)} = b^{9} = 1,\ ab = ba^{x}]$.