R. LE VAVASSEUR

Étude du groupe des isomorphismes de $(G_p)^3$, p étant un nombre premier plus grand que 3

Annales scientifiques de l'É.N.S. 3e série, tome 16 (1899), p. 377-394.
<http://www.numdam.org/item?id=ASENS_1899_3_16__377_0>

ÉTUDE

DU

GROUPE DES ISOMORPHISMES

DE $(G_p)^3$,

p ÉTANT UN NOMBRE PREMIER PLUS GRAND QUE 3.

PAR M. R. LE VAVASSEUR,

PROFESSEUR AU LYCÉE DE TOULOUSE.

1. On sait que le groupe des isomorphismes de $(G_p)^3$ est simplement isomorphe avec le groupe G formé des substitutions

$$|x, y, z \quad \alpha_{11}x + \alpha_{12}y + \alpha_{13}z,\ \alpha_{21}x + \alpha_{22}y + \alpha_{23}z,\ \alpha_{31}x + \alpha_{32}y + \alpha_{33}z|,$$

où les nombres α_{ij} sont des entiers pris suivant le module p, avec l'unique condition

$$\begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{vmatrix} \not\equiv 0 \qquad (\text{mod}\, p).$$

L'ordre de G est égal à

$$(p^3 - 1)(p^3 - p)(p^3 - p^2).$$

2. Considérons la substitution

$$s = |x, y, z \quad \alpha_{11}x + \alpha_{12}y + \alpha_{13}z,\ \alpha_{21}x + \alpha_{22}y + \alpha_{23}z,\ \alpha_{31}x + \alpha_{32}y + \alpha_{33}z|.$$

Nous pouvons chercher les sous-groupes d'ordre p de $(G_p)^3$ que l'isomorphisme correspondant à la substitution s transforme chacun en lui-même.

Cela revient à résoudre les congruences simultanées

$$(1)\qquad \begin{cases} (\alpha_{11}-\sigma)x + \alpha_{12}y + \alpha_{13}z \equiv 0 \\ \alpha_{21}x + (\alpha_{22}-\sigma)y + \alpha_{23}z \equiv 0 \\ \alpha_{31}x + \alpha_{32}y + (\alpha_{33}-\sigma)z \equiv 0 \end{cases} \pmod{p};$$

σ doit être racine de la congruence

$$\Delta(\sigma) \equiv \begin{vmatrix} \alpha_{11}-\sigma & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22}-\sigma & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33}-\sigma \end{vmatrix} \equiv 0 \pmod{p}.$$

La congruence $\Delta(\sigma) \equiv 0 \pmod{p}$ sera appelée *congruence caractéristique* de la substitution s.

3. Le premier cas à considérer est celui où tous les deuxièmes mineurs du déterminant $\Delta(\sigma)$ sont nuls.

On a alors

$$\sigma \equiv \alpha_{11} \equiv \alpha_{22} \equiv \alpha_{33} \quad \text{et} \quad \alpha_{ij} \equiv 0, \qquad (i \neq j) \qquad \pmod{p}.$$

Les substitutions

$$|\, x, y, z \quad \alpha x, \alpha y, \alpha z \,|$$

seront dites *substitutions singulières*.

Supposons que α appartienne à l'exposant $p-1 \pmod{p}$.

La substitution

$$|\, x, y, z \quad \alpha x, \alpha y, \alpha z \,|$$

est d'ordre $p-1$ et engendre le groupe K des substitutions singulières, qui est un groupe cyclique d'ordre $p-1$.

Les substitutions singulières sont les seules substitutions du groupe G qui soient conjuguées d'elles-mêmes.

4. Le cas suivant est celui où tous les premiers mineurs du déterminant $\Delta(\sigma)$ sont nuls, un des deuxièmes déterminants mineurs au moins étant différent de zéro.

Supposons d'abord que l'on ait

$$\alpha_{23}\alpha_{32}\alpha_{31}\alpha_{13}\alpha_{12}\alpha_{21} \not\equiv 0 \pmod{p}.$$

Alors on a

$$\alpha_{23}\alpha_{31}\alpha_{12} \equiv \alpha_{32}\alpha_{13}\alpha_{21} \pmod{p},$$

puis, ρ étant un paramètre arbitraire,

$$\alpha_{11} \equiv \rho + \frac{\alpha_{31}\alpha_{12}}{\alpha_{32}},$$

$$\alpha_{22} \equiv \rho + \frac{\alpha_{12}\alpha_{23}}{\alpha_{13}},$$

$$\alpha_{33} \equiv \rho + \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}},$$

La congruence caractéristique devient

$$(\rho - \sigma)^2 \left(\rho - \sigma + \frac{\alpha_{31}\alpha_{12}}{\alpha_{32}} + \frac{\alpha_{12}\alpha_{23}}{\alpha_{13}} + \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}}\right) \equiv 0.$$

Posons

$$u = \frac{1}{\alpha_{23}\alpha_{32}} + \frac{1}{\alpha_{31}\alpha_{13}} + \frac{1}{\alpha_{12}\alpha_{21}}.$$

5. Supposons d'abord $u \not\equiv 0$. La congruence $\Delta(\sigma) \equiv 0$ admet une racine simple et une racine double. Si nous envisageons d'abord la racine simple

$$\sigma = \rho + \alpha_{23}\alpha_{31}\alpha_{12} u,$$

les congruences (1) admettent alors la solution

$$\frac{x}{\frac{1}{\alpha_{23}\alpha_{32}}} \equiv \frac{y}{\frac{1}{\alpha_{13}\alpha_{32}}} \equiv \frac{z}{\frac{1}{\alpha_{23}\alpha_{12}}},$$

Pour la racine double, les congruences (1) se réduisent à la congruence unique

$$\frac{x}{\alpha_{23}\alpha_{32}} + \frac{y}{\alpha_{31}\alpha_{23}} + \frac{z}{\alpha_{21}\alpha_{32}} \equiv 0,$$

laquelle n'admet pas la solution précédente.

Donc, à la racine simple correspond un sous-groupe unique d'ordre p, que l'isomorphisme transforme en lui-même.

A la racine double correspondent $p+1$ sous-groupes d'ordre p que l'isomorphisme transforme chacun en lui-même et qui sont les $p+1$ sous-groupes d'ordre p d'un sous-groupe d'ordre p^2.

On pourra choisir les opérations génératrices de $(G_p)^3$ de telle sorte que l'isomorphisme envisagé devienne

$$\begin{pmatrix} a & b & c \\ a^\alpha & b^\beta & c^\beta \end{pmatrix} \qquad (\alpha \not\equiv \beta),$$

et la substitution correspondante prendra alors la forme

$$|x, y, z \quad \alpha x, \beta y, \beta z| \qquad (\alpha \not\equiv \beta).$$

6. Si u est nul, $(\bmod p)$, la congruence $\Delta(\sigma) \equiv 0$ admet la racine triple $\sigma \equiv \rho$. Alors les seuls groupes d'ordre p de $(G_p)^3$ que l'isomorphisme transforme chacun en lui-même sont ceux qui correspondent à la congruence

$$\frac{x}{\alpha_{23}\alpha_{32}} + \frac{y}{\alpha_{31}\alpha_{23}} + \frac{z}{\alpha_{21}\alpha_{32}} \equiv 0.$$

Les substitutions correspondantes pourront se mettre sous la forme

$$|x, y, z \quad \alpha x + \beta z,\ \alpha y + \gamma z,\ \alpha z|,$$

à condition de choisir convenablement les opérations génératrices de $(G_p)^3$.

Nous avons fait l'hypothèse que l'on avait

$$\alpha_{23}\alpha_{32}\alpha_{31}\alpha_{13}\alpha_{12}\alpha_{21} \not\equiv 0 \qquad (\bmod p).$$

Une discussion facile montre que les conclusions sont les mêmes au cas où l'on supposerait nuls quelques-uns de ces six coefficients.

7. Considérons les substitutions

$$|x, y, z,\ \alpha x, \beta y, \beta z|.$$

Elles forment un groupe H d'ordre $(p-1)^2$ qui contient le groupe K des substitutions singulières.

D'ailleurs les substitutions permutables avec le groupe H sont de la forme

$$t = |x, y, z,\ a_{11}x,\ a_{22}y + a_{23}z,\ a_{32}y + a_{33}z|.$$

Le groupe H' des substitutions t est d'ordre $(p-1)(p^2-1)(p^2-p)$.

On en déduit que le nombre des groupes conjugués de H est

$$p^2(p^2+p+1).$$

D'ailleurs l'isomorphisme considéré transforme en lui-même : 1° le groupe $\{a\}$; 2° chacun des $p+1$ sous-groupes de $\{b, c\}$.

Or il y a p^2+p+1 manières de choisir le sous-groupe $\{b, c\}$; et, le sous-groupe $\{b, c\}$ choisi, il y a p^2 manières de choisir le sous-groupe $\{a\}$.

Il y a donc en tout $p^2(p^2+p+1)$ groupes H, formant une suite complète unique de sous-groupes conjugués.

8. J'arrive aux substitutions

$$|\ x, y, z \quad \alpha x + \beta z,\ \alpha y + \gamma z,\ \alpha z\ |.$$

Leur ordre est un multiple de p. Ces substitutions forment un groupe I, d'ordre $p^2(p-1)$, contenant le groupe K des substitutions singulières.

Les substitutions t permutables avec le groupe I sont de la forme

$$t = |\ x, y, z \quad a_{11}x + a_{12}y + a_{13}z,\ a_{21}x + a_{22}y + a_{23}z,\ a_{33}z\ |.$$

Elles forment un groupe I' d'ordre $(p-1)(p^2-1)(p^2-p)p^2$.

Le nombre des groupes conjugués de I est donc p^2+p+1.

D'ailleurs l'isomorphisme correspondant à l'une des substitutions envisagées est

$$\begin{pmatrix} a, & b, & c \\ a^\alpha, & b^\alpha, & a^\beta b^\gamma c^\alpha \end{pmatrix}.$$

Il y a p^2+p+1 manières de choisir le groupe $\{a, b\}$.

Donc il y a en tout p^2+p+1 groupes I, formant dans $(G_p)^3$ une suite complète unique de sous-groupes conjugués.

9. Envisageons actuellement les substitutions telles que les racines de la congruence caractéristique $\Delta(\sigma) \equiv 0$ n'annulent pas tous les premiers mineurs du déterminant $\Delta(\sigma)$. Supposons d'abord que la congruence $\Delta(\sigma) \equiv 0$ ait trois racines réelles, α, β, γ, ces racines étant

distinctes. On pourra choisir les opérations génératrices du groupe $(G_p)^3$, de façon que la substitution correspondante prenne la forme

$$s = (\alpha x, \beta y, \gamma z).$$

Les substitutions s forment un groupe L, d'ordre $(p-1)^3$. Ce groupe L comprend le groupe K des substitutions singulières, puis les substitutions de l'une des formes $(\alpha x, \beta y, \beta z)$, $(\alpha x, \beta y, \alpha z)$, $(\alpha x, \alpha y, \beta z)$.

Les substitutions permutables au groupe L sont de l'une des formes

$$(ax, by, cz), \quad (ax, bz, cy), \quad (ay, bz, cx).$$

Elles forment un groupe L' d'ordre $3!(p-1)^3$.

Il a donc $\frac{(p^2+p+1)(p^2+p)p^2}{3!}$ groupes conjugués de L.

Or, c'est précisément le nombre des groupes L, puisque c'est le nombre de manières dont on peut choisir trois par trois les p^2+p+1 sous-groupes d'ordre p de $(G_p)^3$.

Donc tous les groupes L font partie d'une suite complète unique de sous-groupes conjugués.

10. Supposons que la congruence $\Delta(\sigma) \equiv 0 \pmod p$ admette une racine simple et une racine double, la racine double n'annulant pas tous les premiers mineurs du déterminant $\Delta(\sigma)$.

On pourra choisir les opérations génératrices de $(G_p)^3$ de façon que la substitution considérée soit de la forme

$$s = (\alpha x + \gamma z, \beta y + \delta z, \beta z).$$

Ces substitutions forment donc un groupe M, d'ordre $p^2(p-1)^2$.

Pour que les premiers mineurs de $\Delta(\sigma)$ ne soient pas tous nuls, il suffit que β ne soit pas nul $(\text{mod } p)$.

Les substitutions permutables au groupe M sont de la forme

$$t = (a_{11}x + a_{13}z, a_{22}y + a_{23}z, a_{33}z).$$

Elles forment un groupe M' d'ordre $(p-1)^3p^2$.

Le nombre des groupes conjugués de M est donc

$$(p^2+p+1)\,p(p+1).$$

Or l'isomorphisme correspondant à la substitution s est

$$\begin{pmatrix} a, & b, & c \\ a^\alpha, & b^\beta, & a^\gamma b^\delta c^\beta \end{pmatrix}.$$

D'ailleurs, il y a p^2+p+1 manières de choisir le groupe $\{a\}$, ensuite p^2+p manières de choisir le groupe $\{b\}$, ce qui donne $(p^2+p+1)(p^2+p)$ groupes M.

Les groupes M forment donc une suite complète unique de sous-groupes conjugués.

11. La congruence $\Delta(\sigma)\equiv 0 \pmod p$ peut avoir une racine triple n'annulant pas tous les premiers mineurs du déterminant $\Delta(\sigma)$. La substitution s correspondante sera de la forme

$$s=(\alpha x+\alpha' y+\alpha'' z,\ \alpha y+\beta z,\ \alpha z)$$

ou bien de la forme

$$\left[\alpha x+\alpha' y+\alpha'' z,\ \beta' y-\frac{1}{\gamma'}(\alpha-\beta')^2 z,\ \gamma' y+(2\alpha-\beta')z\right],\quad \text{avec } \gamma'\not\equiv 0.$$

On ramène cette seconde forme à la première en remplaçant l'opération c par

$$b^{\frac{\beta'-\alpha}{\gamma'}}c=c',$$

puis en permutant les opérations b et c'.

Les substitutions s forment un groupe N, d'ordre $(p-1)p^3$.

Celles qui n'ont pas encore été énumérées sont celles pour lesquelles on a $\alpha'\beta\not\equiv 0$.

Les substitutions permutables au groupe N sont de la forme

$$t=(a_{11}x+a_{12}y+a_{13}z,\ a_{22}y+a_{23}z,\ a_{33}z).$$

Elles forment un groupe N' d'ordre $(p-1)^3p^3$.

Le nombre des groupes conjugués de N est donc $(p^2+p+1)(p+1)$.

D'ailleurs, l'isomorphisme correspondant à s est de la forme

$$\begin{pmatrix} a, & b, & c \\ a^\alpha, & a^{\alpha'}b^\alpha, & a^{\alpha''}b^\beta c^\alpha \end{pmatrix}.$$

Il y a p^2+p+1 manières de choisir le groupe $\{a\}$. Il y a ensuite p^2+p manières de choisir le groupe $\{b\}$; mais, le groupe $\{b\}$ étant choisi, on peut le remplacer par n'importe quel sous-groupe d'ordre p de $\{a, b\}$ autre que $\{a\}$.

Il y a donc $(p^2+p+1)(p+1)$ groupes N.

Les groupes N forment donc une suite complète unique de sous-groupes conjugués.

12. Examinons le cas où la congruence $\Delta(\sigma)\equiv 0 \pmod p$ a une racine simple et deux racines imaginaires de Galois.

Les substitutions correspondantes peuvent se mettre sous la forme

$$(\alpha x, \gamma z, y+\delta z),$$

avec la condition que le polynome $\sigma^2-\delta\sigma-\gamma$ soit irréductible $(\bmod p)$ ou bien (en admettant dans les substitutions envisagées des coefficients entiers complexes, réels ou imaginaires de Galois) sous la forme

$$s=(\alpha x, jy, j^p z),$$

j et j^p étant des imaginaires.

Les substitutions s forment un groupe P d'ordre $(p-1)^2(p+1)$. On voit aisément que les substitutions t, permutables à s, forment un groupe P′ d'ordre $2(p-1)^2(p+1)$.

Le nombre des sous-groupes conjugués de P est donc

$$\frac{(p^2+p+1)p^3(p-1)}{2}.$$

C'est d'ailleurs le nombre total des groupes P, ainsi que le montre le raisonnement suivant :

On voit aisément que l'isomorphisme envisagé peut, au moyen d'un choix convenable des opérations génératrices, se mettre sous la forme

$$\begin{pmatrix} a, & b, & c \\ a^\alpha, & c, & b^\gamma c^\delta \end{pmatrix}.$$

Il y a p^2+p+1 manières de choisir $\{b, c\}$. On sait d'ailleurs que dans le groupe des isomorphismes de $(G_p)^2$ il y a $\frac{p(p-1)}{2}$ sous-groupes cycliques engendrés chacun par une substitution à congruence irréductible, d'ordre p^2-1.

Ensuite le groupe $\{b, c\}$ contient $p+1$ sous-groupes d'ordre p.

Il y a donc encore p^2 manières de choisir $\{a\}$.

Cela fait en tout $(p^2+p+1)\frac{p(p-1)}{2}p^2$ sous-groupes P.

Les sous-groupes P forment donc, dans le groupe G, une suite complète unique de sous-groupes conjugués.

13. Restent les substitutions dont la congruence caractéristique a trois racines imaginaires de Galois. Par un changement de variables (en admettant des coefficients entiers complexes, réels ou imaginaires de Galois), on peut mettre l'une de ces substitutions sous la forme

$$s=(jx, j^p y, j^{p^2} z).$$

Si l'on suppose que j est une imaginaire appartenant à l'exposant p^3-1, on voit que les substitutions s forment un groupe cyclique Q d'ordre p^3-1.

Les substitutions t permutables avec le groupe Q transforment s en elle-même ou en

$$s^p=(j^p x, j^{p^2} y, jz),$$

ou en

$$s^{p^2}=(j^{p^2} x, jy, j^p z).$$

Le groupe Q' des substitutions t est donc d'ordre $3(p^3-1)$.

Il en résulte qu'il y a $\frac{(p^3-p)(p^3-p^2)}{3}$ groupes cycliques conjugués du groupe Q.

D'ailleurs, en faisant le total de toutes les substitutions énumérées jusqu'ici, avec l'hypothèse que les groupes Q forment une suite complète unique de sous-groupes conjugués, on trouve

$$(p^3-1)(p^3-p)(p^3-p^2)$$

pour ce total, ce qui justifie l'hypothèse.

14. Voici maintenant comment on obtient les diverses substitutions que je viens d'énumérer.

Les substitutions singulières sont les $p - 1$ substitutions

$$| \; x, y, z \quad \alpha x, \alpha y, \alpha z \; |, \qquad \alpha = 1, 2, \ldots, p-1.$$

Les substitutions pour lesquelles la congruence $\Delta(\sigma) \equiv 0 \pmod p$ a une racine triple annulant tous les premiers mineurs du déterminant $\Delta(\sigma)$ sont en nombre

$$(p^2 + p + 1)(p+1)(p-1)^2.$$

On les obtient comme il suit :

1° Soit $\alpha_{21} \not\equiv 0$; on posera

$$\alpha_{12} \equiv \frac{1}{4\alpha_{21}} \left[\frac{\alpha_{23}^2 \alpha_{31}^2}{\alpha_{21}^2} - (\alpha_{11} - \alpha_{22})^2 \right],$$

$$\alpha_{13} \equiv \frac{\alpha_{23}}{2\alpha_{21}} \left(\alpha_{11} - \alpha_{22} - \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}} \right),$$

$$\alpha_{32} \equiv \frac{\alpha_{31}}{2\alpha_{21}} \left(\alpha_{22} - \alpha_{11} - \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}} \right),$$

$$\alpha_{33} \equiv \frac{\alpha_{11} + \alpha_{22}}{2} + \frac{3}{2} \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}}.$$

Alors

$$\Delta = \frac{1}{8} \left(\alpha_{11} + \alpha_{22} + \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}} \right)^3;$$

on fera

$$\alpha_{11} + \alpha_{22} + \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}} = \lambda,$$

et l'on regardera α_{11}, par exemple, comme déterminé par cette équation.

En résumé, λ et α_{21} pourront prendre les valeurs $1, 2, \ldots, p-1$; $\alpha_{22}, \alpha_{23}, \alpha_{31}$ pourront prendre les valeurs $0, 1, 2, \ldots, p-1$.

$\alpha_{11}, \alpha_{33}, \alpha_{32}, \alpha_{13}, \alpha_{12}$ sont alors déterminés.

2° On fera

$$\alpha_{21} \equiv \alpha_{31} \equiv \alpha_{23} \equiv \alpha_{32} \equiv 0,$$
$$\alpha_{11} \equiv \alpha_{22} \equiv \alpha_{33} \equiv \lambda;$$

on donnera à λ les valeurs $1, 2, \ldots, p-1$ et à α_{12}, comme à α_{13} les valeurs $0, 1, 2, \ldots, p-1$.

Cependant on exclut le cas

$$\alpha_{12} \equiv 0, \qquad \alpha_{13} \equiv 0.$$

3° On fera

$$\alpha_{21} \equiv \alpha_{31} \equiv \alpha_{23} \equiv \alpha_{13} \equiv 0,$$
$$\alpha_{11} \equiv \alpha_{22} \equiv \alpha_{33} \equiv \lambda;$$

on donnera à λ, α_{12} les valeurs $1, 2, \ldots, p-1$ et à α_{12} les valeurs $0, 1, 2, \ldots, p-1$.

4° On fera

$$\alpha_{21} \equiv \alpha_{31} \equiv \alpha_{32} \equiv \alpha_{12} \equiv 0,$$
$$\alpha_{11} \equiv \alpha_{22} \equiv \alpha_{33} \equiv \lambda;$$

on donnera à λ, α_{23} les valeurs $1, 2, \ldots, p-1$ et à α_{13} les valeurs $0, 1, 2, \ldots, p-1$.

5° On fera

$$\alpha_{21} \equiv \alpha_{31} \equiv 0, \qquad \alpha_{11} \equiv \frac{\alpha_{22}+\alpha_{33}}{2},$$

$$\left.\begin{array}{l} \alpha_{23} \equiv \dfrac{\alpha_{22}-\alpha_{33}}{2\rho} \\ \alpha_{32} \equiv \dfrac{\rho}{2}(\alpha_{33}-\alpha_{22}) \\ \alpha_{12} \equiv \rho\alpha_{13} \end{array}\right| \quad \alpha_{22}+\alpha_{33} \equiv \lambda;$$

λ et ρ prennent les valeurs $1, 2, \ldots, p-1$; α_{33} prend toute valeur, sauf la valeur $\frac{1}{2}\lambda$; α_{13} prend toute valeur.

6° On fera

$$\alpha_{21} \equiv \alpha_{23} \equiv \alpha_{13} \equiv \alpha_{12} \equiv 0,$$
$$\alpha_{11} \equiv \alpha_{22} \equiv \alpha_{33} \equiv \lambda;$$

λ et α_{31} prendront les valeurs $1, 2, \ldots, p-1$; α_{32} prendra toute valeur.

7° Enfin on fera

$$\begin{array}{ll} \alpha_{31} \equiv \dfrac{\alpha_{33}-\alpha_{11}}{2\rho}, & \\ & \alpha_{22} \equiv \dfrac{\alpha_{33}+\alpha_{11}}{2}, \\ \alpha_{13} \equiv \dfrac{\rho}{2}(\alpha_{11}-\alpha_{33}), & \\ & \alpha_{11}+\alpha_{33} \equiv \lambda. \\ \alpha_{12} \equiv -\rho\alpha_{32}, & \end{array}$$

λ et ρ prendront les valeurs $1, 2, \ldots, p-1$; α_{33} prendra toute valeur, sauf $\frac{\lambda}{2}$. α_{32} prendra toute valeur.

15. Les substitutions pour lesquelles la congruence $\Delta(\sigma) \equiv 0$ a une racine simple et une racine double, la racine double annulant tous les premiers mineurs du déterminant $\Delta(\sigma)$, sont en nombre égal à $p^2(p^2+p+1)(p-1)(p-2)$.

On les obtient comme il suit :

1° On pose

$$\begin{aligned}
\alpha_{33} &\equiv \lambda + \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}}, \\
\alpha_{11} &\equiv \mu + \lambda - \alpha_{22} - \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}}, \\
\alpha_{32} &\equiv \frac{\alpha_{31}}{\alpha_{21}}(\alpha_{22}-\lambda), \\
\alpha_{12} &\equiv \frac{1}{\alpha_{21}}\left(\mu - \alpha_{22} - \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}}\right)(\alpha_{22}-\lambda), \\
\alpha_{13} &\equiv \frac{\alpha_{23}}{\alpha_{21}}\left(\mu - \alpha_{22} - \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}}\right);
\end{aligned}$$

on donne à λ, α_{21} les valeurs $1, 2, \ldots, p-1$; on donne à μ une valeur différente de 0 et différente de λ; α_{22}, α_{31}, α_{23} sont arbitraires.

2° On fera

$$\left.\begin{aligned}
\alpha_{21} &\equiv \alpha_{23} \equiv 0 \\
\alpha_{13} &\equiv \frac{1}{\alpha_{31}}(\alpha_{33}-\alpha_{22})(\alpha_{11}-\alpha_{22}) \\
\alpha_{12} &\equiv \frac{\alpha_{32}}{\alpha_{31}}(\alpha_{11}-\alpha_{22})
\end{aligned}\right| \quad \alpha_{11}+\alpha_{33} \equiv \alpha_{22}+\lambda;$$

on donnera à α_{22}, α_{31} les valeurs $1, 2, \ldots, p-1$; on donnera à λ une valeur quelconque différente de 0 et de α_{22}. α_{33}, α_{32} sont arbitraires.

3° On fera

$$\left.\begin{aligned}
\alpha_{21} &\equiv \alpha_{31} \equiv 0 \\
\alpha_{23} &\equiv \frac{1}{\alpha_{32}}(\alpha_{22}-\alpha_{11})(\alpha_{33}-\alpha_{11}) \\
\alpha_{13} &\equiv \frac{\alpha_{12}}{\alpha_{32}}(\alpha_{33}-\alpha_{11})
\end{aligned}\right| \quad \alpha_{11}-\alpha_{22}-\alpha_{33} \equiv \lambda;$$

on donnera à α_{11}, α_{32} les valeurs $1, 2, \ldots, (p-1)$; on donnera à λ une valeur quelconque différente de 0 et de α_{11}.

α_{33}, α_{12} sont arbitraires.

4° On fera

$$\alpha_{21} \equiv \alpha_{31} \equiv \alpha_{32} \equiv \alpha_{23} \equiv 0, \qquad \alpha_{22} \equiv \alpha_{33};$$

on donnera à α_{11}, α_{12} les valeurs $1, 2, \ldots, p-1$; α_{22} prendra une valeur quelconque, différente de 0 et de α_{11}; α_{13} est arbitraire.

5° On fera

$$\alpha_{21} \equiv \alpha_{31} \equiv \alpha_{32} \equiv 0, \qquad \alpha_{33} \equiv \alpha_{11}, \qquad \alpha_{23} \equiv \frac{\alpha_{13}}{\alpha_{12}}(\alpha_{22} - \alpha_{33});$$

on donnera à α_{11}, α_{12} les valeurs $1, 2, \ldots, p-1$; α_{22} prendra une valeur quelconque différente de 0 et de α_{11}; α_{13} est arbitraire.

6° On fera

$$\alpha_{21} \equiv \alpha_{31} \equiv \alpha_{32} \equiv \alpha_{12} \equiv \alpha_{23} \equiv 0, \qquad \alpha_{22} \equiv \alpha_{33};$$

on donnera à α_{11}, α_{13} les valeurs $1, 2, \ldots, p-1$; α_{22} prendra une valeur quelconque, différente de 0 et de α_{11}.

7° On fera

$$\alpha_{21} \equiv \alpha_{31} \equiv \alpha_{32} \equiv \alpha_{12} \equiv 0, \qquad \alpha_{22} \equiv \alpha_{11};$$

α_{11} et α_{13} prendront les valeurs $1, 2, \ldots, (p-1)$; α_{22} prendra une valeur quelconque différente de 0 et de α_{11}; α_{23} est arbitraire.

8° On fera

$$\alpha_{21} \equiv \alpha_{31} \equiv \alpha_{32} \equiv \alpha_{12} \equiv \alpha_{13} \equiv 0, \qquad \alpha_{11} = \alpha_{22};$$

α_{11} et α_{23} prendront les valeurs $1, 2, \ldots, p-1$; α_{23} prendra une valeur quelconque, autre que 0 et que α_{11}.

9° On fera

$$\alpha_{21} \equiv \alpha_{31} \equiv \alpha_{32} \equiv \alpha_{12} \equiv \alpha_{13} \equiv 0, \qquad \alpha_{11} \equiv \alpha_{33};$$

α_{11} et α_{23} prendront les valeurs $1, 2, \ldots, p-1$; α_{22} prendra une valeur quelconque, autre que 0 et α_{11}.

10° On fera

$$\alpha_{21} \equiv \alpha_{31} \equiv \alpha_{32} \equiv \alpha_{12} \equiv \alpha_{13} \equiv \alpha_{23} \equiv 0,$$

puis

$$\alpha_{22} \equiv \alpha_{33} \left\{ \begin{array}{l} \alpha_{22} \text{ prendra les valeurs } 1, 2, \ldots, p-1, \\ \alpha_{11} \text{ sera différent de zéro et de } \alpha_{22}, \end{array} \right.$$

ou bien

$$\alpha_{33} \equiv \alpha_{11} \left\{ \begin{array}{l} \alpha_{33} \text{ prendra les valeurs } 1, 2, \ldots, p-1, \\ \alpha_{22} \text{ sera différent de zéro et de } \alpha_{33}, \end{array} \right.$$

ou bien

$$\alpha_{11} \equiv \alpha_{22} \left\{ \begin{array}{l} \alpha_{21} \text{ prendra les valeurs } 1, 2, \ldots, p-1, \\ \alpha_{33} \text{ sera différent de zéro et de } \alpha_{11}. \end{array} \right.$$

16. Proposons-nous, actuellement, le problème suivant : *De combien de manières peut-on déterminer les coefficients α_{ij} de façon que le polynome $\Delta(\sigma)$ soit identique à $\gamma - \beta\sigma + \alpha\sigma^2 - \sigma^3$, où γ est un nombre entier donné, différent de zéro, α et β étant deux nombres entiers donnés quelconques.*

1° On donnera à α_{21} et à μ les valeurs $1, 2, \ldots, (p-1)$; à α_{22}, α_{33}, α_{23}, α_{31} des valeurs arbitraires, puis on fera

$$\alpha_{11} \equiv \alpha - \alpha_{22} - \alpha_{33},$$

$$\alpha_{12} \equiv \frac{\alpha_{22}\alpha_{33} + \alpha(\alpha_{22} + \alpha_{33}) - (\alpha_{22} + \alpha_{33})^2 - \alpha_{23}\alpha_{32} - \alpha_{31}\alpha_{13} - \beta}{\alpha_{21}},$$

$$\alpha_{32} \equiv \frac{\alpha_{22}\alpha_{21}\alpha_{31} + \alpha_{23}\alpha_{31}^2 - \alpha_{21}\alpha_{31}\alpha_{33} + \mu}{\alpha_{21}^2},$$

$$\begin{aligned} \mu\alpha_{21}^2\alpha_{13} \equiv\ & \alpha_{22}\alpha_{33}\alpha_{21}^3(\alpha_{22} + \alpha_{33} - \alpha) + \alpha_{21}^2(\alpha_{33}\alpha_{21} - \alpha_{23}\alpha_{31}) \\ & \qquad \times [\alpha_{22}\alpha_{33} + \alpha(\alpha_{22} + \alpha_{33}) - (\alpha_{22} + \alpha_{33})^2 - \beta) \\ & + (\alpha\alpha_{21} - \alpha_{21}\alpha_{22} - 2\alpha_{21}\alpha_{33} + \alpha_{23}\alpha_{21}) \\ & \qquad \times \alpha_{23}(\alpha_{22}\alpha_{21}\alpha_{31} + \alpha_{23}\alpha_{31}^2 - \alpha_{21}\alpha_{31}\alpha_{33} + \mu) + \gamma\alpha_{21}^3. \end{aligned}$$

2° *a*. La congruence

$$\sigma^3 - \alpha\sigma^2 + \beta\sigma - \gamma \equiv 0$$

a une racine triple λ. On donnera à α_{21} une valeur différente de zéro, à α_{22}, α_{23}, α_{31}, α_{13} des valeurs arbitraires. Puis on fera

$$\alpha_{11} \equiv 3\lambda - \alpha_{22} - \alpha_{33} \equiv \alpha - \alpha_{22} - \alpha_{33},$$

$$\alpha = 3\lambda, \qquad \beta = 3\lambda^2, \qquad \gamma = \lambda^3,$$

$$\alpha_{12} \equiv \frac{\alpha_{22}\alpha_{33} + \alpha(\alpha_{22} + \alpha_{33}) - (\alpha_{22} + \alpha_{33})^2 - \alpha_{23}\alpha_{32} - \alpha_{31}\alpha_{13} - \beta}{\alpha_{21}},$$

$$\alpha_{33} \equiv \lambda + \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}},$$

$$\alpha_{32} \equiv \frac{\alpha_{22}\alpha_{21}\alpha_{31} + \alpha_{23}\alpha_{31}^2 - \alpha_{21}\alpha_{31}\alpha_{33}}{\alpha_{21}^2}.$$

b. La congruence

$$\sigma^3 - \alpha\sigma^2 + \beta\sigma - \gamma \equiv 0$$

a une racine double λ et une racine simple μ. On fera comme au cas précédent; mais

$$\alpha = 2\lambda + \mu, \qquad \beta = \lambda^2 + 2\lambda\mu, \qquad \gamma = \lambda^2\mu,$$

et l'on aura, soit

$$\alpha_{33} \equiv \lambda + \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}},$$

soit

$$\alpha_{33} \equiv \mu + \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}}.$$

c. La congruence

$$\sigma^3 - \alpha\sigma^2 + \beta\sigma - \gamma \equiv 0$$

a trois racines distinctes, λ, μ, ν. Alors

$$\alpha = \lambda + \mu + \nu, \qquad \beta = \mu\nu + \nu\lambda + \lambda\mu, \qquad \gamma = \lambda\mu\nu.$$

On aura, soit

$$\alpha_{33} \equiv \lambda + \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}},$$

soit

$$\alpha_{33} \equiv \mu + \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}},$$

soit

$$\alpha_{33} \equiv \nu + \frac{\alpha_{23}\alpha_{31}}{\alpha_{21}}.$$

Il faudra prendre successivement ces trois formules.

d. La congruence

$$\Delta(\sigma) \equiv -\sigma^3 + \alpha\sigma^2 - \beta\sigma + \gamma \equiv 0$$

a une racine réelle λ et deux racines imaginaires de Galois.

On se servira des formules 2° *a*, où λ désignera l'unique racine réelle. (Bien entendu, α n'est plus égal à 3λ, ni β à $3\lambda^2$, ni γ à λ^3.)

3° On fera

$$\alpha_{21} \equiv 0.$$

On donnera à α_{23}, α_{31} l'une des valeurs $1, 2, \ldots, p-1$ et à α_{22}, α_{33}, α_{32}

des valeurs arbitraires; puis on fera

$$\begin{aligned}
\alpha_{11} &\equiv \alpha - \alpha_{22} - \alpha_{33},\\
\alpha_{31}\alpha_{13} &\equiv \alpha_{22}\alpha_{33} + (\alpha_{22} + \alpha_{33})(\alpha - \alpha_{22} - \alpha_{33}) - \alpha_{23}\alpha_{32} - \beta,\\
\alpha_{23}\alpha_{31}\alpha_{12} &\equiv (\alpha_{23}\alpha_{32} - \alpha_{22}\alpha_{33})(\alpha - \alpha_{22} - \alpha_{33})\\
&\quad + \alpha_{22}^2\alpha_{33} + \alpha_{22}(\alpha_{22} + \alpha_{33})(\alpha - \alpha_{22} - \alpha_{33})\\
&\quad - \alpha_{22}\alpha_{23}\alpha_{32} - \beta\alpha_{22} + \gamma;
\end{aligned}$$

4° *a*. La congruence

$$\sigma^3 - \alpha\sigma^2 + \beta\sigma - \gamma \equiv 0$$

a une racine triple λ, ou bien une racine simple λ et deux racines imaginaires de Galois. On fera

$$\alpha_{22} \equiv \lambda, \qquad \alpha_{23} \equiv 0, \qquad \alpha_{21} \equiv 0.$$

On donnera à α_{31} une valeur différente de zéro, à α_{33}, α_{32}, α_{12} des valeurs arbitraires, puis on fera

$$\begin{aligned}
\alpha_{11} &\equiv \alpha - \alpha_{22} - \alpha_{33},\\
\alpha_{31}\alpha_{13} &\equiv \alpha_{22}\alpha_{33} + (\alpha_{22} + \alpha_{33})(\alpha - \alpha_{22} - \alpha_{33}) - \beta.
\end{aligned}$$

b. La congruence

$$\sigma^3 - \alpha\sigma^2 + \beta\sigma - \gamma \equiv 0$$

a une racine double λ et une racine simple μ. On fera successivement

$$\alpha \equiv \lambda, \qquad \alpha \equiv \mu;$$

le reste, comme au cas *a*.

c. La congruence a trois racines distinctes λ, μ, ν. On fera successivement

$$\alpha \equiv \lambda, \qquad \alpha \equiv \mu, \qquad \alpha \equiv \nu;$$

le reste, comme au cas *a*.

5° On fera

$$\alpha_{21} \equiv 0, \qquad \alpha_{31} \equiv 0.$$

On donnera à α_{32} une des valeurs $1, 2, \ldots, p-1$, à α_{33}, α_{13}, α_{12} des valeurs arbitraires. On égalera α_{11} à l'une des racines *réelles* de la congruence donnée

$$\sigma^3 - \alpha\sigma^2 + \beta\sigma - \gamma \equiv 0.$$

α_{23} sera déterminé par la congruence

$$\alpha_{23}\alpha_{32} \equiv -\beta + \alpha_{22}\alpha_{33} + (\alpha_{22}+\alpha_{33})(\alpha - \alpha_{22} - \alpha_{33}),$$

et α_{22} par la congruence

$$\alpha_{22} \equiv \alpha - \alpha_{11} - \alpha_{33}.$$

6° On fera

$$\alpha_{21} \equiv 0, \qquad \alpha_{31} \equiv 0, \qquad \alpha_{32} \equiv 0.$$

On donnera à α_{12}, α_{13}, α_{23} des valeurs arbitraires; α_{11}, α_{22}, α_{33} sont égaux (à l'ordre près) aux racines supposées toutes réelles (mais non forcément distinctes) de la congruence donnée.

17. Les considérations qui précèdent ne sont pas exactes pour $p = 2$ ou $p = 3$, car on n'aurait pas le droit, pour ces cas particuliers, de diviser ou multiplier les deux membres d'une congruence par 2 ou 3; mais la même méthode est applicable.

Voici, par exemple, les résultats pour le groupe simple d'ordre 168, correspondant au cas $p = 2$. Il n'y a qu'une substitution singulière, (x, y, z).

Il y a 21 sous-groupes d'ordre 2 formant une suite complète unique de sous-groupes conjugués. Leur congruence caractéristique est

$$\sigma^3 + \sigma^2 + \sigma + 1 \equiv 0;$$

elle admet la racine triple $\sigma = 1$, et cette racine annule tous les premiers mineurs du déterminant caractéristique $\Delta(\sigma)$.

Il y a 21 sous-groupes d'ordre 4, formant une suite complète unique de sous-groupes conjugués. Les substitutions d'ordre 4 admettent encore comme congruence caractéristique la congruence

$$\sigma^3 + \sigma^2 + \sigma + 1 \equiv 0.$$

Mais ici la racine triple $\sigma = 1$ n'annule pas tous les premiers mineurs de $\Delta(\sigma)$.

Il y a 28 groupes d'ordre 3, formant une suite complète unique de sous-groupes conjugués.

La congruence caractéristique de chaque substitution d'ordre 3 est

$$\sigma^3 + 1 \equiv 0 \pmod 2.$$

Elle admet la racine réelle $\sigma = 1$ et deux racines imaginaires de Galois, les racines de la congruence irréductible

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

Enfin, il y a 8 sous-groupes d'ordre 7, formant une suite complète unique de sous-groupes conjugués.

24 substitutions d'ordre 7 ont pour congruence caractéristique la congruence irréductible

$$\sigma^3 + \sigma^2 + 1 \equiv 0 \pmod 2.$$

Les 24 autres ont pour congruence caractéristique la congruence irréductible

$$\sigma^3 + \sigma + 1 \equiv 0 \pmod 2.$$