Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 11 (1938-1939)

Artikel: La théorie de Galois et ses généralisations.
Autor: Cartan, Elie
DOI: https://doi.org/10.5169/seals-11875

La théorie de Galois et ses généralisations

Par ELIE CARTAN, Paris[1])

I. Rappel des principes de la théorie de Galois

1. La théorie de Galois s'applique à certains systèmes *automorphes*; ce sont des systèmes (d'équations algébriques, d'équations différentielles, d'équations aux dérivées partielles) tels qu'on passe d'une solution particulière à une autre solution quelconque par les opérations d'un groupe G, dit *groupe fondamental.* Etant donné un *domaine de rationalité,* on suppose les équations du système rationnelles dans ce domaine; *on suppose aussi que les opérations du groupe G sont rationnelles.* Dans la théorie classique de Galois, on considère une équation algébrique à racines toutes distinctes, une solution étant ici l'ensemble des racines rangées dans un certain ordre: les opérations de G sont les permutations effectuées sur les racines. Dans la théorie de Picard-Vessiot des équations différentielles linéaires, une solution est formée par un système fondamental d'intégrales, les opérations de G étant les substitutions linéaires effectuées sur ces intégrales. Dans cette dernière théorie, le domaine de rationalité comprend obligatoirement les coefficients de l'équation différentielle donnée et toutes les fonctions qu'on en déduit par addition, multiplication, division et différentiation, ainsi que toutes les constantes complexes.

2. Admettons que l'une des solutions x du système donné satisfasse à un certain système rationnel *irréductible* $\Sigma(x)$ qui est, soit le système donné, soit ce système auquel on a adjoint une ou plusieurs équations rationnelles nouvelles: cette hypothèse est réalisée dans les cas classiques. Un système rationnel $\Sigma(x)$ est irréductible, d'après M. Drach, s'il est impossible de lui adjoindre une équation nouvelle qui laisse le système compatible et qui ne soit pas une conséquence rationnelle des équations de $\Sigma(x)$.

La théorie de Galois peut alors être traitée en quelques lignes; elle repose sur les deux théorèmes fondamentaux suivants.

1° *Les transformations s de G qui font passer de la solution particulière x à une solution sx de Σ forment un groupe g.* En effet par hypothèse x satisfait au système rationnel $\Sigma(sx)$; donc $\Sigma(sx)$ est une conséquence rationnelle de $\Sigma(x)$, sans quoi le système $\Sigma(x)$ ne serait pas irréductible.

[1]) Cet article a été rédigé il y a un certain nombre d'années; j'espère qu'il n'a pas perdu son intérêt.

Par suite l'opération s appliquée à une solution *quelconque* de Σ donne encore une solution de Σ: l'ensemble des opérations de G qui font passer de la solution particulière x aux différentes solutions de Σ jouit de la propriété de contenir ss', dès qu'il contient s et s'. D'autre part, si l'opération s fait passer de la solution particulière x de Σ à la solution sx de Σ, l'opération s^{-1} fait passer de la solution particulière sx à la solution x et par suite s^{-1} est une opération de l'ensemble considéré. Cet ensemble forme donc un groupe g. C. Q.F.D. C'est le *groupe de rationalité* ou le *groupe de Galois* du système.

2° *Tout système irréductible* $\bar{\Sigma}$ *auquel satisfait une solution particulière* $\bar{x}$ *du système donné est automorphe par rapport à un groupe* $\bar{g}$ *homologue de* g *dans* G. En effet soit t l'opération de G qui fait passer d'une solution particulière x du système irréductible Σ à une solution particulière $\bar{x}$ du système irréductible $\bar{\Sigma}$; $\bar{x}$ satisfait au système irréductible $\Sigma(t^{-1}\bar{x})$, dont le groupe $\bar{g}$ est évidemment le groupe tgt^{-1} homologue de g dans G.

3. Ajoutons la remarque importante que *le système de toutes les relations rationnelles auxquelles satisfait une solution particulière du système donné est irréductible*, puisque toute solution satisfait à un système irréductible et ne peut par suite satisfaire à des équations rationnelles qui n'en seraient pas des conséquences rationnelles.

Remarquons aussi que si l'on ne suppose pas l'existence d'un système irréductible rationnel compatible avec le système donné et si l'on appelle $\Sigma(x)$ l'ensemble des relations rationnelles auxquelles satisfait une solution particulière x de ce système, la première partie de la démonstration du premier théorème fondamental est encore valable: l'ensemble des opérations de G qui font passer de x à une autre solution de $\Sigma(x)$ jouit de la propriété de contenir le produit ss' dès qu'il contient s et s'; mais la deuxième partie tombe, de sorte qu'on ne peut pas démontrer que cet ensemble forme un groupe. La conclusion est cependant exacte si le groupe G ne contient qu'un nombre fini d'opérations, ou si le système $\Sigma(x)$ ne contient qu'un nombre fini de solutions. Dans la théorie classique de Galois, c'est ce qui se passe. L'irréductibilité du système $\Sigma(x)$ est dans ce cas assurée.

II° Cas où les opérations du groupe fondamental ne sont pas rationnelles

4. Dans l'exposé précédent, deux hypothèses jouent un rôle important, à savoir l'existence d'un système rationnel irréductible compatible avec le système donné et la propriété des opérations du groupe fondamental d'être rationnelles. Cette seconde est la plus importante; du reste, la première est une conséquence de la seconde si le groupe fondamental est fini. Il est à présumer que si nous laissons tomber cette hypothèse de la rationalité des opérations du groupe fondamental, tout ou partie de la théorie de Galois tombera en défaut. Les exemples que nous allons donner pourraient même conduire à la conclusion qu'en général rien ne subsiste de cette théorie. Néanmoins les recherches de MM. *Drach* et *Vessiot*[2]) sur le système formé d'une équation aux dérivées partielles linéaire et homogène du premier ordre à une fonction inconnue z de n variables indépendantes $x_1, x_2, \ldots, x_n$, système automorphe par rapport au groupe infini de toutes les transformations $Z = f(z)$, montrent qu'au moins dans ce cas une partie des théorèmes de la théorie de Galois subsiste. On sait en effet que dans ce cas

1° il existe un système rationnel Σ irréductible et automorphe par rapport à un groupe g de transformations $Z = f(z)$;

2° les solutions de tout système rationnel $\overline{\Sigma}$ compatible avec l'équation aux dérivées partielles donnée se partagent en familles dans chacune desquelles les solutions se déduisent de l'une d'entre elles par les opérations d'un groupe, variable d'une famille à l'autre, homologue de g (semblable à g).

Le groupe $\bar{g}$ est le groupe de rationalité, ou le groupe de Drach-Vessiot, de l'équation donnée.

5. Il est intéressant de rechercher comment les choses se passent dans des cas très simples.

Premier Exemple. Considérons l'équation

$$x^4 - 4 = 0 \,, \tag{1}$$

automorphe par rapport au groupe fondamental $X^4 = x^4$ (ce groupe, comme tous ceux que nous considérerons dans la suite, a des équations de définition rationnelles). Le domaine de rationalité est formé des nombres rationnels.

---

[2]) *J. Drach,* Essai sur une théorie générale de l'intégration, etc. (Annales Ecole Norm., 1898); Sur le problème logique de l'intégration des équations différentielles (Annales Toulouse, 1908, 1912); — *E. Vessiot,* Sur la théorie de Galois et ses diverses généralisations (Annales Ecole Norm., 1904); Sur la réductibilité et l'intégration des systèmes complets (Annales Ecole Norm., 1912); Sur la réductibilité des équations aux dérivées partielles du premier ordre (Annales Ecole Norm., 1915).

Ici deux des racines de (1) satisfont à l'équation irréductible

$$x^2 - 2 = 0\ , \tag{2}$$

les deux autres à l'équation irréductible

$$x^2 + 2 = 0\ . \tag{3}$$

Elles sont toutes les deux automorphes, et par rapport au même groupe $X = \pm x$. La théorie de Galois subsiste, avec néanmoins la différence que les irrationnelles définies par (2) et (3) ne sont pas de même nature.

2[me] **Exemple.** Considérons maintenant l'équation

$$x^6 - 8 = 0\ , \tag{4}$$

automorphe par rapport au groupe fondamental $X^6 = x^6$, avec le même domaine de rationalité que dans le premier exemple. Les solutions de (4) satisfont aux équations irréductibles

$$x^2 - 2 = 0, \tag{5}$$

$$x^4 + 2x^2 + 4 = 0; \tag{6}$$

la première est automorphe par rapport au groupe $X = \pm x$; *la seconde n'est pas automorphe*. Néanmoins les solutions de la seconde équation se partagent en deux familles dans chacune desquelles on passe d'une solution à l'autre par les opérations du groupe $X = \pm x$. Nous retrouvons les deux propriétés fondamentales de la théorie de Drach-Vessiot; le groupe de Drach-Vessiot de l'équation (4) est $X = \pm x$.

3[me] **Exemple.** Prenons l'équation

$$x^6 + 27 = 0\ , \tag{7}$$

automorphe par rapport au groupe fondamental $X^6 = x^6$. Les différentes racines de (7) satisfont aux trois équations irréductibles

$$x^2 + 3 = 0, \tag{8}$$

$$x^2 + 3x + 3 = 0, \tag{9}$$

$$x^2 - 3x + 3 = 0. \tag{10}$$

L'équation (8) est automorphe par rapport au groupe $X = \pm x$, mais aucune des deux autres n'est automorphe. Par exemple l'équation (10) admet les racines $\dfrac{3 - i\sqrt{3}}{2}$ et $\dfrac{3 + i\sqrt{3}}{2}$; les transformations du groupe fondamental qui font passer de la racine $\frac{3-i\sqrt{3}}{2}$ à ces deux racines sont $X=x$ et $X=\frac{1+i\sqrt{3}}{2}\,x$; elles ne forment pas un groupe. De plus les racines de l'équation (10) ne forment pas une famille de racines se déduisant de l'une d'entre elles par les opérations du groupe $X=\pm x$ ou d'un groupe homologue, puisque cette équation n'est pas automorphe. *Le deuxième théorème fondamental de la théorie de Drach-Vessiot tombe en défaut.*

4[me] **Exemple.** L'équation

$$x^4+4=0 \tag{11}$$

est automorphe par rapport au groupe fondamental $X^4=x^4$. Elle se décompose en deux équations irréductibles

$$x^2-2x+2=0, \tag{12}$$

$$x^2+2x+2=0; \tag{13}$$

aucune n'est automorphe. Tous les théorèmes de la théorie de Drach-Vessiot tombent.

5[me] **Exemple.** Terminons par un dernier exemple, fourni par l'équation différentielle

$$x\frac{dx}{dt}=t-\frac{1}{2t^3}, \tag{14}$$

automorphe par rapport au groupe fondamental défini par l'équation

$$X\frac{dX}{dx}=x\ . \tag{15}$$

Le domaine de rationalité est formé par les fonctions rationnelles *à coefficients rationnels* de la variable indépendante t.

Les différentes solutions de (14) sont données par l'équation

$$x^2=t^2+\frac{1}{2t^2}+C\ . \tag{16}$$

Plusieurs cas sont à distinguer.

a) Si la constante C est rationnelle, l'équation (16) est irréductible et automorphe, son groupe étant $X=\pm x$.

b) Si la constante C est égale à $\pm\sqrt{2}$, l'équation (16) fournit deux couples de solutions satisfaisant respectivement aux équations rationnelles irréductibles

$$x^2-2tx+t^2-\frac{1}{2t^2}=0\,, \tag{17}$$

$$x^2+2tx+t^2-\frac{1}{2t^2}=0\ ; \tag{18}$$

aucune n'est automorphe.

c) Si la constante C est une irrationnelle algébrique autre que $\pm\sqrt{2}$, les solutions satisfont à une équation algébrique rationnelle irréductible

$$P\left(x^2 - t^2 - \frac{1}{2t^2}\right) = 0 \ , \tag{19}$$

P étant un polynôme irréductible du second degré au moins; cette équation n'est pas automorphe.

d) Si la constante C est transcendante, les seules relations rationnelles auxquelles satisfasse une des solutions de (16) se réduisent à l'équation (14). *On a là un exemple du cas où le système de toutes les équations rationnelles auxquelles satisfait une solution particulière n'est pas irréductible.*

En résumé, nous avons une infinité de systèmes rationnels irréductibles automorphes (16) avec le même groupe $X = \pm x$; le premier théorème fondamental de la théorie de Drach-Vessiot est vérifié, mais il n'en est pas de même du second, comme le montre le système irréductible (17) ou (18).

6. Comme on le voit, le cas le plus favorable qui puisse se présenter est celui où il existe un système rationnel irréductible automorphe Σ tel que les solutions de tout système rationnel compatible avec le système donné se partagent en familles dans chacune desquelles les différentes solutions se déduisent par une même opération du groupe fondamental des solutions du système Σ. Nous disons qu'un tel système est un *système de Drach-Vessiot*, et le groupe de Σ sera le *groupe de Drach-Vessiot* du système donné.

On peut énoncer au sujet de ces systèmes le théorème suivant.

Théorème. *Pour qu'un système automorphe par rapport à un groupe fondamental G soit un système de Drach-Vessiot, il faut et il suffit qu'il existe un système rationnel irréductible Σ compatible avec le système donné et jouissant de la propriété que si une solution de Σ, après avoir été soumise à une opération, rationnelle ou irrationnelle, de G, satisfait à une certaine équation rationnelle, la transformée par la même opération de G de toute autre solution de Σ satisfait à la même équation rationnelle.*

La condition est évidemment nécessaire. Elle est suffisante, car si s est une opération de G transformant une solution particulière x de Σ en une autre solution sx de Σ, toutes les autres solutions x' de Σ seront changées elles aussi en des solutions sx' de Σ; d'autre part la solution x de Σ se déduisant de la solution sx par l'opération s^{-1}, la transformée

$s^{-1}x'$ de toute solution de Σ sera transformée encore en une solution de Σ. Par suite, le système Σ est automorphe et le système donné est un système de Drach-Vessiot.

Ajoutons la remarque que si Σ' est un second système rationnel irréductible jouissant des mêmes propriétés que Σ, Σ' est automorphe et son groupe g' est homologue de g dans le groupe fondamental. En effet, si t est l'opération de G faisant passer d'une solution particulière x de Σ à une solution particulière x' de Σ', toutes les opérations tgt^{-1} appartiennent à g' et réciproquement toutes les opérations $t^{-1}g't$ appartiennent à g; les deux groupes sont donc homologues et $g' = tgt^{-1}$. Enfin, si $\overline{\Sigma}$ est un système rationnel automorphe quelconque, chaque opération du groupe $\bar{g}$ de $\overline{\Sigma}$ est contenue dans un sous-groupe homologue de g.

III° Une classe de systèmes de Drach-Vessiot

7. J'ai posé depuis longtemps[3]) la question de savoir ce qui subsiste de la théorie de Picard-Vessiot des équations différentielles linéaires quand, dans le domaine de rationalité, on ne prend pas toutes les constantes complexes, mais seulement par exemple les constantes rationnelles, au cas où les coefficients de l'équation sont des fonctions rationnelles à coefficients rationnels de la variable indépendante; les opérations du groupe fondamental cessent alors d'être rationnelles.

Il y a un cas où l'on est sûr que l'équation différentielle est un système de Drach-Vessiot: il suffit pour cela qu'à l'un des systèmes irréductibles Σ considérés dans la théorie classique de Picard-Vessiot, rationnels dans le domaine de rationalité R de cette théorie classique, on puisse faire correspondre un système irréductible Σ' automorphe par rapport au groupe de Galois g de l'équation ou par rapport à un groupe homologue, et qui soit rationnel dans le domaine de rationalité R' *qui ne contient que les constantes rationnelles* (R se déduit de R' par l'adjonction de toutes les constantes). En effet, supposons qu'il en soit ainsi et soit x une solution particulière de Σ'; la solution sx, où s est une opération du groupe fondamental, satisfera au système $\overline{\Sigma}$ qui se déduit de Σ' par l'opération s. Ce système $\overline{\Sigma}$ est rationnel et irréductible dans R, mais il ne sera pas en général rationnel dans R'; en tout cas toute équation $F = 0$ rationnelle dans R' à laquelle satisfait sx est aussi rationnelle dans R et, à ce titre, est une conséquence de $\overline{\Sigma}$; par suite, l'opération s, appliquée à toute solution de Σ' autre que x, donnant une solution de $\overline{\Sigma}$, cette solution satisfera à l'équation $F = 0$ rationnelle dans R'. D'après le théorème du

[3]) *E. Cartan,* La théorie des Groupes (Revue du Mois, 17, 1914, p. 465).

n° **6**, l'équation différentielle donnée constitue, dans le domaine de rationalité R', un système de Drach-Vessiot.

8. Nous allons nous contenter de traiter un problème plus simple, qui s'apparente au précédent. Nous allons montrer que l'équation différentielle

$$\frac{\dfrac{d^3x}{dt^3}}{\dfrac{dx}{dt}} - \frac{3}{2}\left(\frac{\dfrac{d^2x}{dt^2}}{\dfrac{dx}{dt}}\right)^2 = R(t) \ , \tag{20}$$

où $R(t)$ est une fonction rationnelle de t à coefficients rationnels, équation automorphe par rapport au groupe homographique de la variable x, est une équation de Drach-Vessiot, le domaine de rationalité R' étant formé des fonctions rationnelles de t à coefficients rationnels et *ne contenant pas les constantes irrationnelles*. Les opérations du groupe fondamental sont en général irrationnelles.

L'équation (20) serait justiciable de la théorie de Galois si le domaine de rationalité était étendu en R par l'adjonction de toutes les constantes complexes. Nous allons passer en revue tous les groupes de Galois correspondants qui peuvent se présenter et vérifier que pour chacun d'eux g il existe une solution de l'équation (20) satisfaisant à un système rationnel irréductible dans R' et automorphe par rapport à un groupe homologue de g dans le groupe homographique total. Pour cela, nous utiliserons la remarque que si, dans la théorie de Galois (groupe de rationalité R) on a deux systèmes rationnels irréductibles correspondant au même groupe g, on passe de l'un à l'autre par une transformation du groupe fondamental *laissant le groupe g invariant*.

9. Les groupes de Galois possibles, dans le domaine de rationalité R (contenant toutes les constantes complexes) sont homologues à l'un des groupes suivants:

I° Le groupe homographique total;

II° Le groupe continu à deux paramètres $X = ax + b$ défini par

$$\frac{d^2X}{dx^2} = 0 \ ; \tag{21}$$

III° Le groupe continu à un paramètre $X = ax$ défini par

$$x\frac{dX}{dx} = X \ ; \tag{22}$$

IV° Le groupe mixte à un paramètre $X = ax$, $X = \frac{a}{x}$, défini par

$$x^2 \left(\frac{dX}{dx}\right)^2 = X^2 \, ; \tag{23}$$

V° Le groupe, continu ou mixte, à un paramètre $X = \varepsilon x + a\,(\varepsilon^n = 1)$, défini par

$$\left(\frac{dX}{dx}\right)^n = 1 \; ; \tag{24}$$

VI° Le groupe du dièdre $X = \varepsilon x\,(\varepsilon^n = 1)$, défini par

$$X^n = x^n \qquad (n \geqslant 1) \; ; \tag{25}$$

VII° Le groupe défini par

$$X^n + \frac{1}{X^n} = x^n + \frac{1}{x^n} \, (n \geqslant 2) \; ; \tag{26}$$

VIII° IX° X° Le groupe du tétraèdre, le groupe du cube et le groupe de l'icosaèdre.

10. La question ne se pose pas pour le cas I, où l'équation (20) est générale. Dans le cas II, le système irréductible dans R automorphe par rapport au groupe (21) est de la forme

$$\frac{d^2x}{dt^2} = A\,(t)\,\frac{dx}{dt} \, , \tag{27}$$

$A(t)$ étant une fonction rationnelle de t à coefficients quelconques. Ces coefficients satisfont aux équations algébriques *à coefficients rationnels* qui expriment que les solutions de (27) satisfont à l'équation donnée (20); ces équations s'obtiennent en exprimant qu'on a identiquement

$$A'(t) - \tfrac{1}{2}\, A^2(t) \equiv R(t) \; . \tag{28}$$

Appelons *conjuguée* de $A(t)$ et désignons par $\overline{A}(t)$ une fonction rationnelle dont les coefficients satisfont aux mêmes relations algébriques que $A(t)$, c'est-à-dire qui vérifie l'identité (28). L'équation (27), où l'on remplace $A(t)$ par $\overline{A}(t)$, est encore une équation rationnelle dans le domaine R et automorphe par rapport au groupe (21); elle est d'autre part irréductible, sinon le groupe de Galois de l'équation (20) serait un vrai sous-groupe du groupe (21); par suite on passe de l'une de ces équations à l'autre par une transformation homographique laissant invariant le groupe (21). Or ce groupe n'est invariant que dans lui-même (toute homographie le laissant invariant laisserait invariant le point $x = \infty$). Par suite on a identiquement $\overline{A}(t) = A(t)$. Les relations algébriques entre les coefficients de $A(t)$ qui résultent de l'identité (28) n'admettent donc pas d'autre solution que celle fournie par les coefficients de $A(t)$; ces coefficients sont donc rationnels, et l'équation (27) est rationnelle et irréductible dans le domaine R' [4]). C. Q.F.D.

11. Passons au cas III du groupe $X = ax$; toute équation irréductible automorphe par rapport à ce groupe dans le domaine de rationalité R est de la forme

$$\frac{dx}{dt} = xA(t) \ , \tag{29}$$

$A(t)$ étant une fonction rationnelle. On peut, comme dans le cas précédent, définir les fonctions rationnelles $\overline{A}(t)$ conjuguées de $A(t)$. On passera de l'équation (29) à toute équation conjuguée par une homographie effectuée sur x et laissant invariant le groupe (22) $X = ax$. Ces homographies laissant invariant le couple des points doubles ($x = 0$, $x = \infty$) du groupe (22), sont soit de la forme $X = ax$, soit de la forme $X = \frac{a}{x}$; dans le premier cas on a $\overline{A}(t) = A(t)$, dans le second cas on a $\overline{A}(t) = -A(t)$.

Si c'est le premier cas qui se présente pour toutes les fonctions conjuguées $\overline{A}(t)$, c'est que la fonction $A(t)$ est à coefficients rationnels et l'équation (29) est rationnelle dans le domaine R'. Si au contraire le second cas se présente pour une des fonctions conjuguées $\overline{A}(t)$ de $A(t)$, c'est que, au moins pour une certaine valeur rationnelle t_0 de t, $A(t_0)$ est un nombre irrationnel algébrique qui, d'après ce qui précède, est de degré 2 et est égal et opposé à son conjugué; il est donc de la forme $\sqrt{D}$, D étant rationnel. Si l'on adjoint maintenant $\sqrt{D}$ au domaine de rationalité R', tous les conjugués de $A(t)$, *par rapport à ce nouveau domaine* de rationalité, sont identiques à $A(t)$, puisque l'égalité $\overline{A}(t) = -A(t)$ est impossible à cause de $A(t_0) = \overline{A}(t_0) = \sqrt{D}$. Par conséquent les coefficients de $A(t)$ appartiennent au corps quadratique défini par $\sqrt{D}$; on a même $A(t) = \sqrt{D}H(t)$, $H(t)$ étant à coefficients rationnels. Cela posé, si l'on remplace dans l'équation (29) x par $\frac{x - \sqrt{D}}{x + \sqrt{D}}$, on obtient l'équation irréductible *à coefficients rationnels dans* R'

---

[4]) Cela ne veut pas dire que l'identité (28) ne puisse pas être vérifiée par des fonctions rationnelles $A(t)$ à coefficients irrationnels: mais c'est qu'alors le groupe de Galois de l'équation donnée (20) est un vrai sous-groupe de (21). C'est ainsi que si $R(t) = -\frac{1}{2t^2}$, on peut prendre $A(t) = \frac{\sqrt{2}-1}{t}$; l'équation (27) admet alors la solution $x = t^{\sqrt{2}}$ qui satisfait à l'équation irréductible $\left(\frac{dx}{dt}\right)^2 = \frac{2x^2}{t^2}$, dont le groupe est le groupe (23).

$$\frac{dx}{dt} = \frac{1}{2}(x^2 - D)\, H(t) \ , \tag{29'}$$

automorphe par rapport à un groupe homologue du groupe (21).

Dans le cas III on a donc certainement une équation irréductible automorphe, rationnelle dans le domaine de rationalité R', soit de la forme (29), soit de la forme (29′).

12. Le groupe (23) du cas IV donne lieu à un raisonnement identique à celui qui a été fait pour le cas II; cela tient à ce que ce groupe n'est invariant que dans lui-même. Toute équation irréductible rationnelle dans R et automorphe par rapport au groupe (23), supposé le groupe de Galois de l'équation (20), est de la forme

$$\left(\frac{dx}{dt}\right)^2 = x^2 A(t) \ , \tag{30}$$

$A(t)$ étant à coefficients rationnels.

13. Passons au cas V. Au groupe (24), supposé groupe de Galois de l'équation (20), correspond une équation irréductible, rationnelle dans R, de la forme

$$\left(\frac{dx}{dt}\right)^n = A(t) \ , \tag{31}$$

$A(t)$ étant une fonction rationnelle de t. Ici on doit modifier un peu le raisonnement; on peut multiplier x par une constante de manière que la fonction rationnelle $A(t)$ prenne la valeur 1 pour une valeur particulière rationnelle t_0 de t. C'est seulement pour les fonctions jouissant de cette propriété qu'on définira les fonctions conjuguées, qui naturellement prendront aussi la valeur 1 pour $t = t_0$. Le groupe qui laisse invariant le groupe (24) est le groupe $X = ax + b$; par suite l'homographie qui fait passer de l'équation (31) à une équation conjuguée multipliera $A(t)$ par a^n: $\overline{A}(t) = a^n A(t)$; mais comme $\overline{A}(t_0) = A(t_0) = 1$, c'est qu'on a $\overline{A}(t) = A(t)$. Par conséquent la fonction rationnelle $A(t)$ est à coefficients rationnels.

14. Dans le cas VI on a le groupe du dièdre (25) qui correspond à une équation irréductible, rationnelle dans R, de la forme

$$x^n = A(t); \tag{32}$$

on peut là encore supposer $A(t_0) = 1$. Si $n > 1$, toute homographie qui laisse invariant le groupe (25) est soit de la forme $X = ax$, soit de la forme $X = \dfrac{a}{x}$. Par suite si $\overline{A}(t)$ est une fonction rationnelle conjuguée de $A(t)$, on aura, à cause de $\overline{A}(t_0) = A(t_0) = 1$,

$$\text{soit} \quad \overline{A}(t) = A(t) \quad , \qquad \text{soit} \quad \overline{A}(t) = \frac{1}{A(t)} .$$

Si c'est le premier cas qui se présente pour toutes les fonctions conjuguées $\overline{A}(t)$, c'est que $A(t)$ est à coefficients rationnels. Si le second cas se présente, soit t_1 un nombre rationnel pour lequel $\overline{A}(t_1) \neq A(t_1)$; le nombre $A(t_1)$ est un nombre algébrique, nécessairement de degré 2; il appartient donc à un corps quadratique défini par une irrationnelle $\sqrt{D}$. On montre, comme dans le cas III, que les coefficients de $A(t)$ appartiennent tous à ce corps, le changement de $\sqrt{D}$ en $-\sqrt{D}$ changeant $A(t)$ en $\dfrac{1}{A(t)}$. Cela posé, l'équation irréductible

$$\left(\frac{x - \sqrt{D}}{x + \sqrt{D}}\right)^n = A(t) \ ,$$

dont le groupe est homologue du groupe (25), est invariante par le changement de $\sqrt{D}$ en $-\sqrt{D}$. On pourra l'écrire sous la forme, rationnelle dans R',

$$\frac{x^n + C_n^2 D x^{n-2} + C_n^4 D^2 x^{n-4} + \cdots}{C_n^1 x^{n-1} + C_n^3 D x^{n-3} + \cdots} = H(t) \ , \tag{32'}$$

$H(t)$ étant à coefficients rationnels.

Ce qui précède suppose $n > 1$. Si $n = 1$, l'équation (20) admet la solution rationnelle $x = A(t)$ et par suite aussi la solution $x = \dfrac{\alpha A(t) + \beta}{\gamma A(t) + \delta}$. On peut disposer des constantes α, β, γ, δ de manière à avoir, pour une valeur rationnelle t_0 de t,

$$A(t_0) = 0 \ , \qquad A'(t_0) = 1 \ , \qquad A''(t_0) = 0 \ ;$$

le passage de $A(t)$ à une fonction conjuguée $\overline{A}(t)$ ne pourra alors se faire que par l'homographie identique, de sorte que $A(t)$ est à coefficients rationnels.

15. Passons au groupe (26) et supposons d'abord $n > 2$ (pour $n = 1$, le groupe est semblable au groupe $X^2 = x^2$). Il lui correspond une équation irréductible de la forme

$$x^n + \frac{1}{x^n} = A(t) \ . \tag{33}$$

Le groupe (26) est invariant par les homographies $X = \varepsilon x$ et $X = \frac{\varepsilon}{x}$ avec $\varepsilon^{2n} = 1$. Par suite toute fonction conjuguée de $A(t)$ est égale soit à $A(t)$, soit à $-A(t)$. Un raisonnement déjà fait montre que les coefficients de $A(t)$ sont rationnels ou appartiennent à un corps quadratique défini par $\sqrt{D}$; le changement de $\sqrt{D}$ en $-\sqrt{D}$ change alors $A(t)$ en $-A(t)$. Dans le premier cas, l'équation (33) est rationnelle dans le domaine de rationalité R'; dans le second cas l'équation

$$\frac{x^{2n} + D}{x^n} = H(t) \; , \tag{33'}$$

où $H(t) = \frac{1}{\sqrt{D}} A(t)$, est à coefficients rationnels, et automorphe par rapport à un groupe homologue du groupe (26).

16. Prenons maintenant le cas du groupe (26) avec $n = 2$. Nous pouvons écrire l'équation (33) sous la forme

$$\frac{-(x^2+1)^2}{\lambda A(t)} = \frac{(x^2-1)^2}{\mu B(t)} = \frac{4x^2}{\nu C(t)} \, , \tag{34}$$

$A(t)$, $B(t)$, $C(t)$ étant des *polynomes* entiers en t, qu'on peut toujours supposer égaux à 1 pour une valeur particulière rationnelle t_0 de t. On a du reste entre ces polynomes la relation identique

$$\lambda A(t) + \mu B(t) + \nu C(t) \equiv 0,$$

et on peut prendre pour λ, μ, ν les valeurs

$$\lambda = \beta - \gamma, \quad \mu = \gamma - \alpha, \quad \nu = \alpha - \beta,$$

où l'on a posé

$$\alpha = A(t_1), \quad \beta = B(t_1), \quad \gamma = C(t_1),$$

t_1 étant une valeur rationnelle de t convenablement choisie, assujettie du reste à la seule condition qu'on n'ait pas $A(t_1) = B(t_1) = C(t_1)$. Les équations (34) s'écrivent alors

$$\frac{-(x^2+1)^2}{(\beta-\gamma)A(t)} = \frac{(x^2-1)^2}{(\gamma-\alpha)B(t)} = \frac{4x^2}{(\alpha-\beta)C(t)} \, . \tag{34}$$

Le groupe (26) fait intervenir trois couples de valeurs de x: $(i, -i)$, $(1, -1)$, $(0, \infty)$; ce sont les couples de racines des polynomes x^2+1, x^2-1, x dont les carrés figurent aux numérateurs de (34). Toute transformation homographique qui laisse invariant le groupe (26) échangera entre eux ces trois couples. Il en résulte que si $\overline{A}(t)$, $\overline{B}(t)$, $\overline{C}(t)$ constituent un système de polynomes conjugués de $A(t)$, $B(t)$, $C(t)$, l'homographie qui transforme le système (34) dans le système conjugué effectuera sur $A(t)$, $B(t)$, $C(t)$ une certaine permutation: c'est une simple permutation parce qu'on a $A(t_0) = B(t_0) = C(t_0) = \overline{A}(t_0) = \overline{B}(t_0) = \overline{C}(t_0)$. Cette même permutation sera naturellement effectuée sur α, β, γ.

Cela posé, α, β, γ sont racines d'une équation du troisième degré *à coefficients rationnels* puisque dans le corps algébrique auquel ils appartiennent, le passage de α, β, γ à leurs conjugués se fait toujours par une simple permutation. Soit

$$u^3 + pu^2 + qu + r = 0$$

l'équation qui a pour racines α, β, γ. Considérons les trois polynomes

$$\begin{aligned} P(x) &\equiv x^2 - 2\alpha x + \varrho \ , \\ Q(x) &\equiv x^2 - 2\beta x + \sigma \ , \\ R(x) &\equiv x^2 - 2\gamma x + \tau \ , \end{aligned}$$

où ϱ, σ, τ sont choisis par la condition que les racines de deux quelconques de ces trois polynomes se divisent harmoniquement. On aura

$$\sigma + \tau = 2\beta\gamma \, , \qquad \tau + \varrho = 2\gamma\alpha \, , \qquad \varrho + \sigma = 2\,\alpha\beta \, ,$$

d'où

$$\begin{aligned} \varrho &= -2\alpha^2 - 2p\alpha - q \ , \\ \sigma &= -2\beta^2 - 2p\beta - q \ , \\ \tau &= -2\gamma^2 - 2p\gamma - q \ . \end{aligned}$$

On vérifie facilement l'identité

$$(\beta - \gamma)P^2(x) + (\gamma - \alpha)Q^2(x) + (\alpha - \beta)R^2(x) \equiv 0 \ .$$

Cela posé, le système irréductible

$$\frac{P^2(x)}{A(t)} = \frac{Q^2(x)}{B(t)} = \frac{R^2(x)}{C(t)} \ ,$$

qui admet un groupe homologue au groupe (26), est rationnel dans le domaine de rationalité R', car le passage de $A(t)$, $B(t)$, $C(t)$ à $\overline{A}(t)$, $\overline{B}(t)$, $\overline{C}(t)$ effectue sur α, β, γ une certaine permutation, la même que celle qui fait passer de A, B, C à $\overline{A}$, $\overline{B}$, $\overline{C}$, et c'est aussi la permutation que subissent les numérateurs $P^2(x), Q^2(x), R^2(x)$. Ce système peut donc s'écrire de manière à ne contenir aucune irrationnelle.

On vérifie en effet facilement qu'on a

$$A(t) = \alpha H(t) + K(t) \ , \qquad B(t) = \beta H(t) + K(t) \ , \qquad C(t) = \gamma H(t) + K(t) \ ,$$

les polynomes $H(t)$ et $K(t)$ étant à coefficients rationnels. Le système prend alors la forme rationnelle en R'

$$\frac{x^4 - 2qx^2 - 8rx + q^2 - 4pr}{x^3 + px^2 + qx + r} = -4\frac{K(t)}{H(t)} . \tag{34'}$$

17. Il ne nous reste plus à examiner que les trois groupes des polyèdres réguliers[5]).

Dans le cas VIII du groupe du tétraèdre, dont les équations de définition peuvent être ramenées à la forme

$$\frac{(X^4 + 2X)^3}{(x^4 + 2x)^3} = \frac{(4X^3 - 1)^3}{(4x^3 - 1)^3} = \frac{(2X^6 - 10X^3 - 1)^2}{(2x^6 - 10x^3 - 1)^2},$$

tout système irréductible correspondant, rationnel en R, est de la forme

$$\frac{-4(x^4 + 2x)^3}{(\beta - \gamma)A(t)} = \frac{(4x^3 - 1)^3}{(\gamma - \alpha)B(t)} = \frac{(2x^6 - 10x^3 - 1)^2}{(\alpha - \beta)C(t)} . \tag{35}$$

On peut supposer $A(t_0) = B(t_0) = C(t_0) = 1$ pour t_0 rationnel, ainsi que $\alpha = A(t_1)$, $\beta = B(t_1)$, $\gamma = C(t_1)$ pour t_1 rationnel. La somme des numérateurs de (35) est identiquement nulle, ainsi que celle des dénominateurs.

Toute homographie laissant invariante le groupe du tétraèdre laisse invariante l'équation $2x^6 - 10x^3 - 1 = 0$. Deux cas sont alors possibles: ou bien l'homographie laisse invariant le rapport $\dfrac{x^4 + 2x}{4x^3 - 1}$ à un facteur constant près, ou bien elle le remplace par son inverse à un facteur constant près. Il en résulte que si $\overline{A}(t)$, $\overline{B}(t)$, $\overline{C}(t)$ constituent un système de polynomes conjugués de $A(t)$, $B(t)$, $C(t)$, on a $\overline{C}(t) = C(t)$ et en outre

$$\begin{aligned} &\text{ou bien} \quad \overline{A}(t) = A(t), \quad \overline{B}(t) = B(t), \text{ avec } \overline{\alpha} = \alpha, \overline{\beta} = \beta \ , \\ &\text{ou bien} \quad \overline{A}(t) = B(t), \quad \overline{B}(t) = A(t), \text{ avec } \overline{\alpha} = \beta, \overline{\beta} = \alpha \ . \end{aligned}$$

Si c'est le premier cas qui se présente toujours, les polynomes $A(t)$, $B(t)$, $C(t)$ sont à coefficients rationnels et le système (35) est rationnel dans R'. Si le second cas se présente, γ est rationnel, α et β sont des nombres conjugués d'un corps algébrique du second degré défini par une irrationnelle $\sqrt{D}$. Il suffit alors de remplacer les numérateurs de (35) respectivement par les polynomes

[5]) Voir sur ces groupes les Leçons sur l'Icosaèdre de *F. Klein*.

$$-(x^4+6\sqrt{D}x^2-3D)^3\,,\quad (x^4-6\sqrt{D}x^2-3D)^3\,,\quad 36\sqrt{D}\,(x^5+3Dx)^2\,,$$

dont la somme est identiquement nulle, pour obtenir un nouveau système invariant par le changement de signe de $\sqrt{D}$. On peut donc l'écrire de manière qu'il ne contienne aucune irrationnelle. Sa nouvelle forme sera

$$\frac{(x^4-3D)^3+108Dx^4(x^4-3D)}{x^2(x^4+3D)^2}=H(t)\ ,$$

ou encore, en remplaçant $3D$ par D,

$$\frac{(x^4-D)\,(x^8+34Dx^4+D^2)}{x^2\,(x^4+D)^2}=H(t)\ , \tag{35'}$$

$H(t)$ étant une fonction rationnelle à coefficients rationnels.

18. Passons au groupe du cube, dont on peut ramener les équations de définition à la forme

$$\frac{[P(X)]^3}{[P(x)]^3}=\frac{[Q(X)]^4}{]Q(x)]^2}=\frac{[R(X)]^2}{[R(x)]^2}\ ,$$

où $P(x)$, $Q(x)$, $R(x)$ sont trois polynomes respectivement de degrés 8, 6 et 12 [6])

$$\begin{aligned} P(x) &= x^8+14x^4+1,\\ Q(x) &= x^5-x,\\ R(x) &= x^{12}-33x^8-33x^4+1, \end{aligned}$$

liés par la relation identique

$$P^3-108\,Q^4-R^2=0\ .$$

Tout système irréductible correspondant sera de la forme

$$\frac{-P^3}{(\beta-\gamma)\,A(t)}=\frac{108\,Q^4}{(\gamma-\alpha)B(t)}=\frac{R^2}{(\alpha-\beta)\,C(t)}\ , \tag{36}$$

avec les mêmes conventions que dans les cas précédents.

Toute homographie qui laisse invariant le groupe du cube, laisse invariante chacune des équations $P=0$, $Q=0$, $R=0$. Par suite, tout système de polynomes $\overline{A}(t)$, $\overline{B}(t)$, $\overline{C}(t)$ conjugués de $A(t)$, $B(t)$, $C(t)$ redonne les mêmes polynomes, qui sont ainsi à coefficients rationnels.

---

[6]) Le polynome $Q(x)$ doit être regardé comme étant du sixième degré avec la racine $x=\infty$.

19. La démonstration est la même pour le groupe de l'icosaèdre défini par les équations

$$\frac{[P(X)]^5}{[P(x)]^5} = \frac{[Q(X)]^3}{[Q(x)]^3} = \frac{[R(X)]^2}{[R(x)]^2} ,$$

où les polynomes $P(x)$, $Q(x)$, $R(x)$, de degrés respectifs 12, 20, 30, sont

$$P(x) = x^{11} + 11x^6 - x ,$$
$$Q(x) = x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1 ,$$
$$R(x) = x^{30} + 522x^{25} - 10.005x^{20} - 10.005x^{10} - 522x^5 + 1 ;$$

ces polynomes sont liés par la relation

$$1728\, P^5 + Q^3 - R^2 = 0 .$$

Le système irréductible correspondant est de la forme

$$\frac{1728\, P^5}{(\beta - \gamma)\, A(t)} = \frac{Q^3}{(\gamma - \alpha)\, B(t)} = \frac{-R^2}{(\alpha - \beta)\, C(t)} , \tag{37}$$

et on démontre, comme pour le groupe du cube, qu'il est à coefficients rationnels.

La démonstration est ainsi achevée. Le système rationnel irréductible dans le domaine de rationalité R', qui est automorphe par rapport au groupe de Drach-Vessiot de l'équation (20), est réductible à l'une des formes (29), (29′), (30), (31), (32), (32′), (33), (33′), (34), (34′), (35), (35′), (36), (37), du moins si l'équation (20) n'est pas générale.

(Reçu le 27 juillet 1938.)