NOUVELLES ANNALES DE MATHÉMATIQUES

J. DOLBNIA

# Sur le critère de Galois concernant la résolubilité des équations algébriques par radicaux

*Nouvelles annales de mathématiques 3e série*, tome 7 (1888), p. 467-485

<http://www.numdam.org/item?id=NAM_1888_3_7__467_1>

# SUR LE CRITÈRE DE GALOIS CONCERNANT LA RÉSOLUBILITÉ DES ÉQUATIONS ALGÉBRIQUES PAR RADICAUX;

PAR M. J. DOLBNIA,
Ingénieur des Mines à Nijni-Novgorod

1. Il est bien connu que les racines de l'équation cubique

$$x^3 + px + q = 0$$

s'expriment par les formules

$$(1)\quad \begin{cases} x_0 = R_1^{\frac{1}{3}} + R_2^{\frac{1}{3}}, \\ x_1 = \alpha R_1^{\frac{1}{3}} + \alpha^2 R_2^{\frac{1}{3}}, \\ x_2 = \alpha^2 R_1^{\frac{1}{3}} + \alpha R_2^{\frac{1}{3}}, \end{cases}$$

où $R_1$, $R_2$ sont les racines de l'équation

$$t^2 + qt - \frac{p^3}{27} = 0.$$

Abel, le premier, a remarqué [1] que les racines de chaque équation algébrique irréductible, résoluble par

[1] *Œuvres complètes*, t. II, p. 222; 1881.

radicaux, sont exprimables par des formules semblables à (1). Dans un des Mémoires posthumes *Sur la résolution algébrique des équations*, Abel a donné [1], sans démonstration, le théorème suivant :

*Si l'équation de premier degré n est résoluble par radicaux, ses racines sont exprimables par les formules*

$$(2)\quad \left\{\begin{aligned} x_0 &= n\left(R_1^{\frac{1}{n}} + R_2^{\frac{1}{n}} + \ldots + R_{n-1}^{\frac{1}{n}}\right), \\ x_1 &= n\left(\alpha R_1^{\frac{1}{n}} + \alpha^2 R_2^{\frac{1}{n}} + \ldots + \alpha^{n-1} R_{n-1}^{\frac{1}{n}}\right), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_{n-1} &= n\left(\alpha^{n-1} R_1^{\frac{1}{n}} + \alpha^{n-2} R_2^{\frac{1}{n}} + \ldots + \alpha R_{n-1}^{\frac{1}{n}}\right), \end{aligned}\right.$$

*où* $R_1, R_2, \ldots, R_{n-1}$ *sont les racines d'une équation du degré* $(n-1)$ *dont les coefficients sont des fonctions rationnelles des coefficients de la proposée.*

La vérité de ces formules a été démontrée par Malmsten dans le Tome XXXIV du *Journal de Crelle* [2].

2. La connaissance plus exacte des propriétés des fonctions $R_1^{\frac{1}{n}}, R_2^{\frac{1}{n}}, \ldots, R_{n-1}^{\frac{1}{n}}$ s'acquiert à l'aide des théorèmes suivants :

Théorème I. — *Si nous donnons à* $R_1^{\frac{1}{n}}$ *la forme de fonction rationnelle des racines* $x_0, x_1, x_2, \ldots, x_{n-1}$, *la substitution* $\begin{pmatrix} z+k \\ z \end{pmatrix}$ *réduit cette fonction à* $\alpha^k R_1^{\frac{1}{n}}$.

*Démonstration.* — Du système (2), on déduit

$$(3)\quad R_1^{\frac{1}{n}} = x_0 + \alpha^{n-1} x_1 + \ldots + \alpha^{n-k} x_k + \ldots + \alpha x_{n-1} + \ldots.$$

---

[1] *Œuvres complètes*, t. II, p. 217-243.

[2] Serret, *Cours d'Algèbre supérieure*, t. II, p. 657 ; 1886

En appliquant à cette équation la substitution $\begin{pmatrix} z+k \\ z \end{pmatrix}$, on a

$$(4)\qquad \left\{\begin{aligned} S_k\left(R_1^{\frac{1}{n}}\right) = {} & x_k + \alpha^{n-1} x_{k+1} + \ldots \\ & + \alpha^{n-i} x_{k+i} + \ldots + \alpha x_{k-1} + \ldots, \end{aligned}\right.$$

où $S_k = \begin{pmatrix} z+k \\ z \end{pmatrix}$. En multipliant les deux membres de (3) par $\alpha^k$, on obtient

$$(5)\qquad \left\{\begin{aligned} \alpha^k R_1^{\frac{1}{n}} = {} & \alpha^k x_0 + \alpha^{k-1} x_1 + \alpha^{k-2} x_2 + \ldots \\ & + x_k + \alpha^{n-1} x_{k+1} + \ldots + \alpha^{k+1} x_{n-1} + \ldots. \end{aligned}\right.$$

En comparant (4) et (5), on trouve

$$S_k\left(R_1^{\frac{1}{n}}\right) = \alpha^k R_1^{\frac{1}{n}} \qquad \text{C. Q. F. D.}$$

3. *Corollaire*. — En désignant $\begin{pmatrix} z+1 \\ z \end{pmatrix} = S$, nous avons

$$\begin{aligned} S\left(R_1^{\frac{1}{n}}\right) &= \alpha R_1^{\frac{1}{n}}, \\ S^2\left(R_1^{\frac{1}{n}}\right) &= \alpha^2 R_1^{\frac{1}{n}}, \\ &\ldots\ldots\ldots\ldots\ldots \\ S^{n-1}\left(R_1^{\frac{1}{n}}\right) &= \alpha^{n-1} R_1^{\frac{1}{n}}; \end{aligned}$$

d'où il suit que, si nous appliquons les divers degrés de substitution circulaire $S = \begin{pmatrix} z+1 \\ z \end{pmatrix}$ à $R_1^{\frac{1}{n}}$, nous aurons la série

$$(6)\qquad R_1^{\frac{1}{n}},\quad \alpha R_1^{\frac{1}{n}},\quad \alpha^2 R_1^{\frac{1}{n}},\quad \ldots,\quad \alpha^{n-1} R_1^{\frac{1}{n}},\quad \ldots.$$

En général, les divers degrés de substitution $S = \begin{pmatrix} z+1 \\ z \end{pmatrix}$

donnent à $R_i^{\frac{1}{n}}$ la série des valeurs suivantes :

$$R_i^{\frac{1}{n}},\quad \alpha^i R_i^{\frac{1}{n}},\quad \alpha^{2i} R_i^{\frac{1}{n}},\quad \ldots,\quad \alpha^{n-i} R_i^{\frac{1}{n}}.$$

4. Théorème II. — *Si nous appliquons la substitution* $T = \begin{pmatrix} kz \\ z \end{pmatrix}$ *à* $R_1^{\frac{1}{n}}$, *nous aurons*

$$T\left(R_1^{\frac{1}{n}}\right) = R_i^{\frac{1}{n}},$$

*où* $i$ *satisfait à la congruence*

$$ki \equiv 1 \pmod{n}.$$

*Démonstration.* — En appliquant la substitution $T = \begin{pmatrix} kz \\ z \end{pmatrix}$ à la fonction

$$R_1^{\frac{1}{n}} = x_0 + \alpha^{n-1}x_1 + \alpha^{n-2}x_2 + \ldots + \alpha^{n-i}x_i + \ldots + \alpha x_{n-1},$$

nous aurons

$$T\left(R_1^{\frac{1}{n}}\right) = x_0 + \alpha^{n-1}x_k + \alpha^{n-2}x_{2k} + \ldots + \alpha^{n-i}x_{ki} + \ldots + \alpha x_{n-k}.$$

Soit

$$ki \equiv 1 \pmod{n};$$

alors

$$2ki \equiv 2,\qquad 3ki \equiv 3,\qquad \ldots.$$

Par conséquent,

$$(7)\qquad T\left(R_1^{\frac{1}{n}}\right) = x_0 + \alpha^{n-i}x_1 + \alpha^{n-2i}x_2 + \ldots + \alpha^{i}x_{n-1}.$$

Mais, de l'équation (2), on déduit

$$(8)\qquad R_i^{\frac{1}{n}} = x_0 + \alpha^{n-i}x_1 + \alpha^{n-2i}x_2 + \ldots + \alpha^{i}x_{n-1}.$$

En comparant (7) et (8), on obtient

$$T\left(R_1^{\frac{1}{n}}\right) = R_i^{\frac{1}{n}} \qquad \text{C. Q. F. D.}$$

5. *Corollaire.* — Soit $\rho$ la racine primitive du nombre premier $n$; alors $\rho^{n-1} \equiv 1 \pmod n$, tous les autres degrés de $\rho$ sont congrus avec les nombres 2, 3, 4, ..., $n-1$. Posons

$$\rho^{n-2} \equiv a, \qquad \rho^{n-3} \equiv b, \qquad \ldots, \qquad \rho^2 \equiv k \qquad (\text{mod } n),$$

où $a, b, c, \ldots, k$ sont les divers termes de la suite 2, 3, ..., $\rho - 1$, $\rho + 1$, ..., $\overline{n-1}$. Posons $T = \begin{pmatrix} \rho z \\ z \end{pmatrix}$. En appliquant successivement tous les degrés de T, nous aurons

$$T\left(R_1^{\frac{1}{n}}\right) = R_a^{\frac{1}{n}},$$
$$T^2\left(R_1^{\frac{1}{n}}\right) = R_b^{\frac{1}{n}},$$
$$\ldots\ldots\ldots\ldots,$$
$$T^{n-2}\left(R_1^{\frac{1}{n}}\right) = R_\rho^{\frac{1}{n}},$$
$$T^{n-1}\left(R_1^{\frac{1}{n}}\right) = R_1^{\frac{1}{n}},$$

où les indices $a, b, c, \ldots, k$ sont les résidus minimum de $\rho^2, \rho^3, \ldots, \rho^{n-2}$, suivant le module $n$.

De cette manière, nous verrons que les différents degrés de substitution T donnent la série

$$T\left(R_i^{\frac{1}{n}}\right) = R_{ai}^{\frac{1}{n}},$$
$$T^2\left(R_i^{\frac{1}{n}}\right) = R_{bi}^{\frac{1}{n}},$$
$$\ldots\ldots\ldots\ldots,$$
$$T^{n-2}\left(R_i^{\frac{1}{n}}\right) = R_{\rho i}^{\frac{1}{n}},$$
$$T^{n-1}\left(R_i^{\frac{1}{n}}\right) = R_i^{\frac{1}{n}}.$$

6. A l'aide des deux substitutions $S = \begin{pmatrix} z+1 \\ z \end{pmatrix}$ et

$T = \begin{pmatrix} \rho\, z \\ z \end{pmatrix}$, nous formerons la Table suivante :

$$(9)\quad \left\{\begin{array}{lllll} 1, & S, & S^2, & \ldots, & S^{n-1}, \\ T, & ST, & S^2T, & \ldots, & S^{n-1}T, \\ T^2, & ST^2, & S^2T^2, & \ldots, & S^{n-1}T^2, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ T^{n-2}, & ST^{n-2} & S^2T^{n-2}, & \ldots, & S^{n-1}T^{n-2}. \end{array}\right.$$

La table (9) constitue *un système conjugué* [1]. Les substitutions de ce système, étant appliquées successivement à $R_1^{\frac{1}{n}}$, donnent à cette fonction les $n(n-1)$ valeurs suivantes :

$$(A)\quad \left\{\begin{array}{lllll} R_1^{\frac{1}{n}}, & \alpha R_1^{\frac{1}{n}}, & \alpha^2 R_1^{\frac{1}{n}}, & \ldots, & \alpha^{n-1} R_1^{\frac{1}{n}}, \\ R_a^{\frac{1}{n}}, & \alpha^a R_a^{\frac{1}{n}}, & \alpha^{2a} R_a^{\frac{1}{n}}, & \ldots, & \alpha^{n-a} R_a^{\frac{1}{n}}, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots, \\ R_\rho^{\frac{1}{n}}, & \alpha^\rho R_\rho^{\frac{1}{n}}, & \alpha^{2\rho} R_\rho^{\frac{1}{n}}, & \ldots, & \alpha^{n-\rho} R_\rho^{\frac{1}{n}}. \end{array}\right.$$

7. Théorème III. — *Les substitutions qui n'altèrent pas la fonction* $R_1^{\frac{1}{n}}$ *constituent un système conjugué dont l'ordre est*

$$M = 1, 2, 3, \ldots, (n-2);$$

*ce système se compose de toutes les substitutions qui n'altèrent pas les deux racines :* $x_0$ *et encore une certaine racine* $x_k$.

*Démonstration.* — En appliquant à $R_1^{\frac{1}{n}}$ tous les degrés de substitution $T = \begin{pmatrix} \rho\, z \\ z \end{pmatrix}$, nous aurons les $(n-1)$ valeurs différentes de cette fonction qui sont renfermées

---

[1] Serret, *Cours d'Algèbre supérieure*, t. II, p. 268-271; 1886.

dans la série

$$(10) \qquad R_1^{\frac{1}{n}},\quad R_2^{\frac{1}{n}},\quad R_3^{\frac{1}{n}},\quad \ldots,\quad R_{n-1}^{\frac{1}{n}},\quad \ldots.$$

Les substitutions $1$, $T$, $T^2$, $\ldots$, $T^{n-2}$ n'altèrent pas l'indice $z = 0$. D'autre part, si à l'équation

$$x_0 = R_1^{\frac{1}{n}} + R_2^{\frac{1}{n}} + \ldots + R_{n-1}^{\frac{1}{n}}$$

nous appliquons toutes les substitutions possibles des racines $x_1, x_2, \ldots, x_{n-1}$, la racine $x_0$ n'est pas altérée par cette opération. D'où il suit que toutes les substitutions de racines $x_1, x_2, \ldots, x_{n-1}$ donnent à $R_1^{\frac{1}{n}}$ les $(n-1)$ valeurs différentes. Le nombre des substitutions des racines de $x_1, x_2, \ldots, x_{n-1}$ est exprimable par le produit $N = 1, 2, 3, \ldots, (n-1)$. Ces substitutions forment un système conjugué qu'on peut former de la manière suivante. Du nombre général $n$ des racines de l'équation proposée nous excluons $x_0$, et encore une racine à volonté, par exemple $x_1$; de toutes les autres $(n-2)$ racines,

$$(11) \qquad x_2,\quad x_3,\quad \ldots,\quad x_{n-1}$$

nous formons tous les arrangements possibles semblables à (11). Le nombre de tels arrangements est égal au produit

$$M = 1, 2, 3, \ldots, (n-2).$$

Nommons les substitutions à l'aide desquelles nous recevons tous les M arrangements par

$$(12) \qquad 1,\ U_1,\ U_2,\ \ldots,\ U_{M-1}.$$

Les substitutions (12) constituent un système conjugué qui n'altère pas les deux indices 0 et 1. Des deux systèmes conjugués $(1, T, T^2, \ldots, T^{n-2})$ et (12), formons la Table

$$
(13)\quad \left\{ \begin{array}{lllll}
1, & T, & T^2, & \ldots, & T^{n-2}, \\
U_1, & U_1T, & U_1T^2, & \ldots, & U_1T^{n-2}, \\
U_2, & U_2T, & U_2T^2, & \ldots, & U_2T^{n-2}, \\
\ldots, & \ldots\ldots, & \ldots\ldots, & \ldots, & \ldots\ldots\ldots, \\
U_{M-1}, & U_{M-1}T, & U_{M-1}T^2, & \ldots, & U_{M-1}, T^{n-2}.
\end{array} \right.
$$

Ce Tableau renferme les $(n-1)$ M substitutions parmi lesquelles ne peuvent être deux substitutions égales, car l'équation

$$U_\alpha T^\beta = U_{\alpha'} T^{\beta'}$$

entraîne l'égalité

$$(14)\qquad T^{(\beta-\beta')} = U_\alpha^{-1} U_{\alpha'},$$

ce qui ne peut être, parce que le produit $U_\alpha^{-1} U_{\alpha'}$ transforme au plus les $(n-2)$ indices, alors que la substitution $T^{(\beta-\beta')}$ transforme tous les indices, excepté les zéros. D'où il suit que la Table (13) renferme

$$[1, 2, 3, \ldots, (n-1)]$$

substitutions diverses qui ne transforment pas $x_0$ et qui constituent un groupe dont l'ordre est

$$N = 1, 2, 3, \ldots, (n-1).$$

Il est facile de prouver que, dans chaque ligne horizontale du Tableau (13), il y a seulement une substitution qui n'altère pas $\overset{1}{R}{}''_1$. En effet, admettons que dans la ligne

$$U_\alpha, \quad U_\alpha T, \quad U_\alpha T^2, \quad \ldots,$$
$$U_\alpha T^k, \quad \ldots, \quad U_\alpha T^l, \quad \ldots, \quad U_\alpha T^{n-2}$$

il y ait deux substitutions $U_\alpha T^k$ et $U_\alpha T^l$ qui n'altèrent pas $\overset{1}{R}{}''_1$. Dans cette hypothèse, la substitution

$$(U_\alpha T^l)^{-1} = T^{-l} U_\alpha^{-1}$$

n'altère pas $R_1^{\frac{1}{n}}$; par conséquent, le produit

$$T^{-l} U_\alpha^{-1}, \quad U_\alpha T^k = T^{k-l}$$

n'altère pas non plus $R_1^{\frac{1}{n}}$, ce qui ne peut être. De là suit qu'il existe

$$M = 1, 2, 3, \ldots, (n-2)$$

diverses substitutions qui n'altèrent pas $R_1^{\frac{1}{n}}$. Ces substitutions ont les formes

$$U_\alpha T^\beta,$$

où

$$\alpha \leqq M - 1, \qquad \beta \leqq n - 2,$$

et évidemment constituent un système conjugué [1].

D'après les théorèmes bien connus de MM. Bertrand et Serret [2], nous connaissons que, *si l'ordre de système conjugué de* $(n-1)$ lettres est égal au produit $1, 2, 3, \ldots, (n-2)$, le système se compose des substitutions formées avec $(n-2)$ lettres; d'où il suit que le système conjugué qui n'altère pas $R_1^{\frac{1}{n}}$ se compose de toutes les substitutions qui n'altèrent pas $x_0$, et encore l'une des lettres $x_1, x_2, \ldots, x_{n-1}$. C. Q. F. D.

8. *Remarque nécessaire.* — Les théorèmes de MM. Bertrand et Serret dont nous nous sommes servis admettent une exception quand $n = 7$. Dans ce cas, $n - 1 = 6$, et alors, outre le système qui renferme toutes les substitutions de cinq lettres, on peut encore former un système de même ordre qui contient les substitutions circulaires des ordres 4, 5, 6. Il est bien compréhensible

(1) SERRET, *Cours d'Algèbre supérieure*, t. II, p. 386; 1886.
(2) *Ibid.*, t. II, p. 296.

que ce dernier groupe ne peut satisfaire aux conditions du théorème III. En effet, le groupe d'ordre 120, qui fait exception aux théorèmes de MM. Bertrand et Serret, renferme la substitution circulaire

$$\Phi = (x_1, x_5, x_2, x_3, x_4, x_6) \quad (^1).$$

En remarquant que 3 est la racine primitive du nombre premier 7, posons

$$T = \begin{pmatrix} 3z \\ z \end{pmatrix},$$

alors

$$T^2 = \begin{pmatrix} 9z \\ z \end{pmatrix} = \begin{pmatrix} x_2, & x_4, & x_6, & x_1, & x_3, & x_5 \\ x_1, & x_2, & x_3, & x_4, & x_5, & x_6 \end{pmatrix},$$

où

$$T^2 = (x_1, x_2, x_4)(x_3, x_6, x_5).$$

Il est clair que

$$\Phi^2 = T^2;$$

par conséquent, le groupe qui renferme les substitutions circulaires des ordres 4, 5, 6 ne peut être identique au groupe du même ordre, dont toutes les substitutions n'altèrent pas $R_1^{\frac{1}{n}}$.

9. Raisonnant comme ci-dessus, nous verrons que le groupe qui n'altère pas $\alpha^{pk} R_k$ se compose des $M = 1, 2, \ldots, (n-2)$ substitutions qui ne transforment pas $x_p$, et encore une certaine racine $x_q$.

10. Théorème IV. — *Chaque fonction de la forme $\alpha^k R_l^{\frac{1}{n}}$ est exprimable rationnellement par deux racines de l'équation proposée convenablement choisie.*

*Démonstration.* — Prenons l'une des fonctions

(1) Serret, *Cours d'Algèbre supérieure*, t. II, p. 311 : 1866.

données $\alpha^{kp} R_p^{\frac{1}{n}}$. Cette fonction n'est pas altérée par toutes les substitutions possibles des racines

$$x_0, \quad x_1, \quad \ldots, \quad x_k, \quad \ldots, \quad x_l, \quad \ldots, \quad x_{n-1},$$

excepté $x_k$ et encore une certaine racine $x_l$; par conséquent, $\alpha^{kp} R_p^{\frac{1}{n}}$ est une fonction entière, rationnelle et symétrique des racines de l'équation

$$(15) \left\{ \begin{array}{l} (x - x_0)(x - x_1)\ldots(x - x_{k-1})(x - x_{k+1})\ldots \\ \qquad \times (x - x_{l-1})(x - x_{l+1})\ldots(x - x_{n-1}) = 0. \end{array} \right.$$

Si

$$(16) \qquad f(x) = 0$$

est l'équation proposée, la fonction $\alpha^{pk} R_p^{\frac{1}{n}}$ est exprimable rationnellement par les coefficients de l'équation

$$\frac{f(x)}{(x - x_k)(x - x_l)} = 0,$$

par conséquent, elle s'exprime rationnellement par $x_k$ et $x_l$. C. Q. F. D.

11. Théorème V. — *Chaque racine de l'équation proposée s'exprime rationnellement par chacune des fonctions* (A) ($n^o$ 5), *si les racines de l'équation binôme* $\alpha^n - 1 = 0$ *sont rationnellement connues.*

*Démonstration.* — Nous avons reproduit ici les raisonnements avec lesquels Galois a démontré l'un de ses théorèmes fondamentaux ([1]). Nous savons que le groupe des substitutions d'ordre $N = 1, 2, \ldots, (n-1)$ qui ne transforment pas $x_0$ donnent à $R_1^{\frac{1}{n}}$ les $(n-1)$ va-

([1]) Serret, *Cours d'Algèbre supérieure*, t. II, p. 389-395; 1866 leurs

$$\overset{1}{R}{}_{1}^{\prime}, \quad \overset{1}{R}{}_{2}^{\prime\prime}, \quad \ldots, \quad \overset{1}{R}{}_{n-1}^{\prime\prime}.$$

Composons l'équation

$$(17)\qquad \left(\zeta - R_1^{\frac{1}{n}}\right)\left(\zeta - R_2^{\frac{1}{n}}\right)\cdots\left(\zeta - R_{n-1}^{\frac{1}{n}}\right) = 0,$$

dont les coefficients sont les fonctions symétriques des racines de l'équation

$$\frac{f(x)}{x - x_0} = 0;$$

par conséquent, on peut donner à l'équation (17) la forme

$$F(\zeta, x_0) = 0$$

L'équation proposée $f(x) = 0$ a une racine commune avec chacune des équations

$$(18)\qquad \begin{cases} F\left(R_1^{\frac{1}{n}}, x\right) = 0, \\ F\left(R_2^{\frac{1}{n}}, x\right) = 0, \\ \cdots\cdots\cdots\cdots \\ F\left(R_{n-1}^{\frac{1}{n}}, x\right) = 0. \end{cases}$$

Il est facile de démontrer qu'aucune des équations (18) n'a d'autre racine commune avec l'équation proposée.

C'est pourquoi nous disons que l'équation

$$(19)\qquad F\left(R_k^{\frac{1}{n}}, x\right) = 0$$

est satisfaite par la substitution $x_j$ au lieu de $x$, c'est-à-dire que nous avons identiquement

$$(20)\qquad F\left(R_k^{\frac{1}{n}}, x_j\right) = 0.$$

L'équation

$$(21) \qquad F(\zeta, x_j) = 0$$

découle de (17) par la substitution circulaire $\binom{z+j}{z}$; par conséquent l'équation (21), dans la forme étendue, est

$$\left(\zeta - \alpha^j R_1^{\frac{1}{n}}\right)\left(\zeta - \alpha^{2j} R_2^{\frac{1}{n}}\right)\cdots\left(\zeta - \alpha^{n-j} R_{n-1}^{\frac{1}{n}}\right) = 0.$$

Il est évident qu'à cette dernière équation la racine $\zeta = R_k^{\frac{1}{n}}$ ne satisfait pas; par conséquent, l'égalité (20) n'est pas admissible, par conséquent notre hypothèse est illusoire.

D'où il suit que chaque équation (18) n'a qu'une seule racine commune avec l'équation proposée; par conséquent, le polynôme $f(x)$ a un plus grand commun diviseur avec chacun des polynômes (18), et ce commun diviseur est un polynôme du premier degré en $x$. Nous chercherons ce diviseur parmi $f(x)$ et $F(\zeta, x)$; ayant obtenu le reste du premier degré en $x$, nous égalerons ce reste à zéro; par cela même, $x$ se transforme en $x_0$, lequel s'exprime rationnellement par $\zeta$; au lieu de $\zeta$, nous pouvons substituer chacune des fonctions $R_1^{\frac{1}{n}}, R_2^{\frac{1}{n}}, \ldots, R_{n-1}^{\frac{1}{n}}$. De la même manière, nous démontrerions que, en général, $x_k$ s'exprime rationnellement par $\alpha^k R_1^{\frac{1}{n}}, \alpha^{2k} R_2^{\frac{1}{n}}, \ldots, \alpha^{n-k} R_{n-1}^{\frac{1}{n}}$. D'où il suit que chacune des racines s'exprime rationnellement par chacune des fonctions (A), n° 5. C. Q. F. D.

12. *Corollaire*. — Il résulte des théorèmes précédents que chacune des fonctions

$$R_1^{\frac{1}{n}}, \quad R_2^{\frac{1}{n}}, \quad \ldots, \quad R_{n-1}^{\frac{1}{n}}$$

s'exprime rationnellement l'une par l'autre. En effet, chacune de ces fonctions s'exprime rationnellement par les racines $x_0, x_1, \ldots, x_{n-1}$; chaque racine s'exprime rationnellement par l'une quelconque des fonctions (A), n° 5; par conséquent, une fonction quelconque $R_l^{\frac{1}{n}}$ s'exprime rationnellement par $R_k^{\frac{1}{n}}$, où $l$ et $k$ sont des entiers arbitraires.

13. Théorème VI (Galois). — *Si une équation irréductible de degré premier n est résoluble par radicaux, les racines sont toutes exprimables en fonction rationnelle de deux quelconques d'entre elles.*

*Démonstration.* — Nous avons vu que chaque racine de l'équation proposée s'exprime rationnellement en chacune des fonctions (A), n° 5; chacune de ces fonctions, par exemple $R_1^{\frac{1}{n}}$, s'exprime rationnellement en fonction de deux certaines racines; par conséquent, nous aurons

$$R_1^{\frac{1}{n}} = \Psi(x_k, x_l).$$

En appliquant à cette équation toutes les substitutions de la forme $\begin{pmatrix} az+b \\ z \end{pmatrix}$, nous obtenons, pour le premier membre de l'équation, le Tableau suivant :

$$(\mathrm{B})\quad \left\{ \begin{array}{lllll} R_1^{\frac{1}{n}}, & R_2^{\frac{1}{n}}, & R_3^{\frac{1}{n}}, & \ldots, & R_{n-1}^{\frac{1}{n}}, \\ \alpha R_1^{\frac{1}{n}}, & \alpha R_2^{\frac{1}{n}}, & \alpha R_3^{\frac{1}{n}}, & \ldots, & \alpha R_{n-1}^{\frac{1}{n}}, \\ \ldots, & \ldots, & \ldots & \ldots, & \ldots\ldots, \\ \alpha^{n-1} R_1^{\frac{1}{n}}, & \alpha^{n-1} R_2^{\frac{1}{n}}, & \alpha^{n-1} R_3^{\frac{1}{n}}, & \ldots, & \alpha^{n-1} R_{n-1}^{\frac{1}{n}}. \end{array} \right.$$

D'autre part, toutes les valeurs possibles de $\Psi$ sont renfermées dans la Table

$$(\mathrm{C})\left\{\begin{array}{llll}\Psi(x_0, x_1), & \Psi(x_0, x_2), & \ldots, & \Psi(x_0, x_{n-1}),\\ \Psi(x_1, x_0), & \Psi(x_1, x_2), & \ldots, & \Psi(x_1, x_{n-1}),\\ \ldots\ldots\ldots, & \ldots\ldots\ldots, & \ldots, & \ldots\ldots\ldots,\\ \Psi(x_{n-1}, x_0), & \Psi(x_{n-1}, x_1), & \ldots, & \Psi(x_{n-1}, x_{n-2}).\end{array}\right.$$

Exprimons $x_k$ par $x_i$ et $y_j$. Cherchons dans la Table (C) la fonction $\Psi(x_i, x_j)$; cette fonction sera égale à un des termes du Tableau (B), soit

$$\Psi(x_i, x_j) = \alpha^m \mathrm{R}_p^{\frac{1}{n}}.$$

Comme $x_k$ s'exprime rationnellement par $\alpha^m \mathrm{R}_p^{\frac{1}{n}}$, la racine $x_k$ s'exprimera rationnellement en $\Psi(x_i, x_j)$ et, par conséquent, en $x_i$, $x_j$. C. Q. F. D.

14. Théorème VII. — *La fonction*

$$\mathrm{R}_1 = (x_0 + \alpha^{n-1}x_1 + \alpha^{n-2}x_2 + \ldots + \alpha x_{n-1})^n$$

*est la racine d'une équation abélienne du degré* $(n-1)$, *dont les coefficients sont des fonctions rationnelles de celles de la proposée.*

*Détermination.* — Les quantités $\mathrm{R}_1$, $\mathrm{R}_2$, $\ldots$, $\mathrm{R}_{n-1}$ sont les racines de l'équation

$$(22) \qquad (\zeta - \mathrm{R}_1)(\zeta - \mathrm{R}_2)\ldots(\zeta - \mathrm{R}_{n-1}) = 0.$$

Démontrons, en premier lieu, que les coefficients de cette équation sont *rationnellement connus*. A cet effet, formons toutes les substitutions possibles de $n$ racines $x_0$, $x_1$, $\ldots$, $x_{n-1}$; ces substitutions forment un groupe de l'ordre $(1.2.3\ldots n)$. Chaque substitution de ce groupe est équivalente au produit de quelques transpositions; mais la transposition $(x_i, x_j)$ remplace la suite

$$\alpha^i R_1^{\frac{1}{n}}, \quad \alpha^{2i} R_2^{\frac{1}{n}}, \quad \ldots, \quad \alpha^{(n-1)i} R_{n-1}^{\frac{1}{n}}$$

par la suite

$$\alpha^j R_1^{\frac{1}{n}}, \quad \alpha^{2j} R_2^{\frac{1}{n}}, \quad \ldots, \quad \alpha^{(n-1)j} R_1^{\frac{1}{n}}.$$

Mais

$$\left(\alpha^{ki} R_k^{\frac{1}{n}}\right)^n = R_k.$$

Alors la transposition $(x_i, x_j)$ remplace dans la série $R_1, R_2, \ldots, R_{n-1}$ un terme par l'autre; par conséquent, la fonction symétrique des quantités $R_1, R_2, R_3, \ldots, R_{n-1}$ n'est altérée par aucune transposition. D'où il suit que chaque fonction symétrique des $R_1, R_2, \ldots, R_{n-1}$ sera *rationnellement connue;* par conséquent, les coefficients de l'équation (22) seront rationnellement connus.

Démontrons, en second lieu, que les racines de l'équation (22) sont toutes exprimables rationnellement par l'une quelconque d'entre elles.

Nous avons

$$R_1 = (x_0 + \alpha^{n-1} x_1 + \alpha^{n-2} x_2 + \ldots + \alpha x_{n-1})^n.$$

Comme $x_0, x_1, \ldots, x_{n-1}$ sont toutes exprimables rationnellement dans l'une quelconque des fonctions

$$R_1^{\frac{1}{n}}, \quad R_2^{\frac{1}{n}}, \quad \ldots, \quad R_{n-1}^{\frac{1}{n}},$$

la fonction $R_1$ peut être exprimée rationnellement, par exemple par $R_2^{\frac{1}{n}}$; par conséquent, nous aurons

$$(23) \qquad R_1 = \frac{\Phi\left(R_2^{\frac{1}{n}}\right)}{\theta\left(R_2^{\frac{1}{n}}\right)},$$

où $\Phi$ et $\theta$ sont des fonctions entières. En faisant disparaître le dénominateur, nous aurons

$$(24)\quad R_1 = a_0 + a_1 R_2^{\frac{1}{n}} + a_2 R_2^{\frac{2}{n}} + a_3 R_2^{\frac{3}{n}} + \ldots + a_{n-1} R_2^{\frac{n-1}{n}},$$

où $a_0$, $a_1$, $a_2$, $\ldots$, $a_{n-1}$ sont des fonctions rationnelles de $R_2$.

En appliquant à l'équation (24) tous les degrés de substitution $S = \begin{pmatrix} z+1 \\ z \end{pmatrix}$, nous aurons (théorème I),

$$\begin{aligned}
R_1 &= a_0 + a_1 R_2^{\frac{1}{n}} + a_2 R_n^{\frac{2}{n}} + \ldots + a_{n-1} R_2^{\frac{n-1}{n}},\\
R_1 &= a_0 + a_1 \alpha^2 R_2^{\frac{1}{n}} + a_2 \alpha^4 R_2^{\frac{2}{n}} + \ldots + a_{n-1} \alpha^{n-2} R_n^{\frac{n-1}{n}}.\\
R_1 &= a_0 + a_1 \alpha^4 R_2^{\frac{1}{n}} + a_2 \alpha^8 R_2^{\frac{2}{n}} + \ldots + a_{n-1} \alpha^{n-4} R_2^{\frac{n-1}{n}},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
R_1 &= a_0 + a_1 \alpha^{n-2} R_2^{\frac{1}{n}} \qquad + \ldots + a_{n-1} \alpha^2 {R^2}_2^{\frac{n-1}{n}}.
\end{aligned}$$

En ajoutant ces égalités, nous trouvons

$$R_1 = a_0,$$

par conséquent $R_1$ s'exprime rationnellement en $R_2$. D'où il résulte, comme l'a remarqué, pour la première fois, Kronecker (¹), que l'équation (22) se rapporte à la catégorie des équations *abéliennes* (²).

15. Théorème VIII (Galois). — *Si toutes les racines d'une équation irréductible de degré premier n sont exprimables rationnellement en fonction de deux quelconques d'entre elles, l'équation est résoluble par radicaux.*

---

(¹) Serret, *Cours d'Algèbre supérieure*. t. II, p. 654-664; 1886.

(²) N.-H. Abel, *Œuvres complètes*, t. I, p. 478-507; 1881.

*Démonstration.* — Formons la fonction

$$\Pi_1 = x_0 + \alpha^{n-1} x_1 + \alpha^{n-2} x_2 + \ldots + \alpha x_{n-1},$$

où $\alpha$ est l'une des racines de l'équation $\dfrac{\alpha^n - 1}{\alpha - 1} = 0$. Comme toutes les racines de l'équation $f(x) = 0$ sont exprimables rationnellement par deux racines à volonté, on peut écrire

$$\Pi_1 = \varphi(x_0, x_1), \tag{26}$$

où $\varphi$ est une fonction rationnelle.

En appliquant à l'équation (26) toutes les substitutions de la forme $\left(\dfrac{az + b}{z}\right)$ (Table IX, n° 6), nous obtenons pour $\Pi_1$ la série de valeurs

$$\text{(D)} \quad \left\{ \begin{array}{lllll} \Pi_1, & \alpha \Pi_1, & \alpha^2 \Pi_1, & \ldots & \alpha^{n-1} \Pi_1, \\ \Pi_a, & \alpha^a \Pi_a, & \alpha^{2a} \Pi_a, & \ldots, & \alpha^{n-a} \Pi_a, \\ \ldots, & \ldots\ldots, & \ldots\ldots, & \ldots, & \ldots\ldots, \\ \ldots, & \ldots\ldots, & \ldots\ldots, & \ldots, & \ldots\ldots, \\ \Pi_\rho, & \alpha^\rho \Pi_\rho, & \alpha^{2\rho} \Pi_\rho, & \ldots, & \alpha^{n-\rho} \Pi_\rho, \end{array} \right.$$

où $a, b, c, \ldots, \rho$ ont les valeurs désignées dans le n° 5. A la fonction $\varphi(x_0, x_1)$ répond la série

$$\text{(E)} \quad \left\{ \begin{array}{llll} \varphi(x_0, x_1), & \varphi(x_1, x_2), & \ldots & \varphi(x_{n-1}, x_n), \\ \varphi(x_0, x_\rho), & \varphi(x_1, x_{\rho+1}), & \ldots & \varphi(x_{n-1}, x_{\rho-1}), \\ \ldots\ldots, & \ldots\ldots, & \ldots, & \ldots\ldots, \\ \ldots\ldots, & \ldots\ldots, & \ldots, & \ldots\ldots, \\ \varphi(x_0, x_a), & \varphi(x_1, x_{a+1}), & \ldots, & \varphi(x_{n-1}, x_{a-1}). \end{array} \right.$$

La Table (E) contient toutes les valeurs de la fonction $\varphi$; par conséquent, la Table (D) contient toutes les valeurs de la fonction $\Pi_1$. Nommons $\lambda$ l'une des racines de l'équation $\lambda^{n-1} - 1 = 0$, sans en excepter l'unité, et formons la fonction

$$(\Pi_1^n + \lambda \Pi_a^n + \lambda^2 \Pi_b^n + \ldots + \lambda^{n-2} \Pi_\rho^n)^{n-1} = \theta_1 = \Phi(x_0, x_1).$$

Il est évident que $\theta_1 = \Phi(x_0, x_1)$ n'est pas altérée par la substitution $S = \begin{pmatrix} z+1 \\ z \end{pmatrix}$; en outre $\theta_1$ n'est pas altérée par la substitution $T = \begin{pmatrix} \rho z \\ z \end{pmatrix}$, car

$$T(\Pi_1) = \Pi_a, \qquad T(\Pi_a) = T^2(\Pi_1) = \Pi_b, \qquad .. ;$$

par conséquent,

$$\theta_1 = \frac{1}{n(n-1)}[\Phi(x_0, x_1) + \Phi(x_1, x_2) + \ldots + \Phi(x_{n-1}, x_{a-1})].$$

Il est évident que $\theta_1$ est une fonction symétrique et rationnelle des racines $x_0, x_1, x_2, \ldots$, et par conséquent elle est rationnellement connue. Nous aurons, évidemment, les $(n-1)$ équations

$$\begin{gathered} \Pi_1^n + \Pi_a^n + \ldots + \Pi_\rho^n = \sqrt[n-1]{\theta_0}, \\ \Pi_1^n + \lambda\Pi_a^n + \ldots + \lambda^{n-2}\Pi_\rho^n = \sqrt[n-1]{\theta_1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \Pi_1^n + \lambda^{n-2}\Pi_a^n + \ldots + \lambda\Pi_\rho^n = \sqrt[n-1]{\theta_{n-2}}, \end{gathered}$$

où $\theta_0, \theta_1, \theta_2, \ldots, \theta_{n-2}$ sont des quantités rationnellement connues. A l'aide de ces équations, $\Pi_1^n, \Pi_2^n, \ldots, \Pi_{n-1}^n$ s'exprimeront par des fonctions rationnelles et linéaires des $\sqrt[n-1]{\theta_0}, \sqrt[n-1]{\theta_1}, \sqrt[n-1]{\theta_2}, \ldots, \sqrt[n-1]{\theta_{n-2}}$; par conséquent, nous trouverons $\Pi_1, \Pi_2, \ldots$ par radicaux; donc nous trouverons par radicaux les racines de l'équation proposée.

C. Q. F. D.