croisse avec x, quand $x > 1$. (Il suffit, en effet, de savoir trouver les racines d'une équation qui sont plus grandes que l'unité.)

Nous aurons, pour la condition proposée,

$$1 + \frac{d\frac{X-Y}{kx^n}}{dx} > 0, \quad \text{ou bien} \quad 1 - \frac{nX - xX'}{kx^{n+1}} + \frac{nY - xY'}{kx^{n+1}} > 0;$$

or on a identiquement

$$nX - xX' > 0, \quad nY - xY' > 0;$$

il suffit donc de poser

$$\frac{nX - xX'}{kx^{n+1}} < 1 \quad \text{pour} \quad x > 1,$$

et il suffit pour cela de prendre pour k la valeur de la fonction $nX - xX'$ relative à $x = 1$.

On trouvera de même un nombre h tel, que la fonction

$$x - \frac{Fx}{hx^n}$$

croîtra avec x quand x sera > 1, en changeant Y en X.

Ainsi, l'équation donnée pourra se mettre sous l'une des formes

$$x = x + \frac{Fx}{kx^n}, \quad x = x - \frac{Fx}{hx^n},$$

qui sont toutes deux rationnelles, et donnent pour la résolution une méthode facile.

Sur la théorie des nombres [*].

Quand on convient de regarder comme nulles toutes les quantités qui, dans les calculs algébriques, se trouvent multipliées par un nom-

---

[*] *Bulletin*, tome XIII, page 428 (année 1830, cahier de juin). Avec la Note suivante : Ce Mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques. (J. L.)

bre premier donné p, et qu'on cherche, dans cette convention, les solutions d'une équation algébrique $Fx = 0$, ce que M. Gauss désigne par la notation $Fx \equiv 0$, on n'a coutume de considérer que les solutions entières de ces sortes de questions. Ayant été conduit par des recherches particulières à considérer les solutions incommensurables, je suis parvenu à quelques résultats que je crois nouveaux.

Soit une pareille équation ou congruence, $Fx = 0$, et p le module. Supposons d'abord, pour plus de simplicité, que la congruence en question n'admette aucun facteur commensurable, c'est-à-dire qu'on ne puisse pas trouver trois fonctions φx, ψx, χx telles que

$$\varphi x . \psi x = Fx + p\chi x.$$

Dans ce cas, la congruence n'admettra donc aucune racine entière, ni même aucune racine incommensurable de degré inférieur. Il faut donc regarder les racines de cette congruence comme des espèces de symboles imaginaires, puisqu'elles ne satisfont pas aux questions des nombres entiers, symboles dont l'emploi, dans le calcul, sera souvent aussi utile que celui de l'imaginaire $\sqrt{-1}$ dans l'analyse ordinaire.

C'est la classification de ces imaginaires, et leur réduction au plus petit nombre possible, qui va nous occuper.

Appelons i l'une des racines de la congruence $Fx = 0$, que nous supposerons du degré ν.

Considérons l'expression générale

$$(A) \qquad a + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1},$$

où $a, a_1, a_2, \ldots, a_{\nu-1}$ représentent des nombres entiers. En donnant à ces nombres toutes les valeurs, l'expression (A) en acquiert p^ν, qui jouissent, ainsi que je vais le faire voir, des mêmes propriétés que les nombres naturels dans la *théorie des résidus des puissances*.

Ne prenons des expressions (A) que les $p^\nu - 1$ valeurs où a, $a_1, a_2, \ldots,$ $a_{\nu-1}$ ne sont pas toutes nulles : soit α l'une de ces expressions.

Si l'on élève successivement α aux puissances 2^e, $3^e, \ldots$, on aura une suite de quantités de même forme [parce que toute fonction de i peu se réduire au $(\nu - 1)^{ième}$ degré]. Donc on devra avoir $\alpha^n = 1$, n étant un certain nombre; soit n le plus petit nombre qui soit tel que l'on ait

$\alpha^n = 1$. On aura un ensemble de n expressions toutes différentes entre elles,

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\ldots,\ \alpha^{n-1}.$$

Multiplions ces n quantités par une autre expression 6 de la même forme. Nous obtiendrons encore un nouveau groupe de quantités toutes différentes des premières, et différentes entre elles. Si les quantités (A) ne sont pas épuisées, on multipliera encore les puissances de α par une nouvelle expression γ, et ainsi de suite. On voit donc que le nombre n divisera nécessairement le nombre total des quantités (A). Ce nombre étant $p^\nu - 1$, on voit que n divise $p^\nu - 1$. De là suit encore que l'on aura

$$\alpha^{p^\nu - 1} = 1, \quad \text{ou bien} \quad \alpha^{p^\nu} = \alpha.$$

Ensuite on prouvera, comme dans la théorie des nombres, qu'il y a des racines primitives α, pour lesquelles on ait précisément $p^\nu - 1 = n$, et qui reproduisent par conséquent, par l'élévation aux puissances, toute la suite des autres racines.

Et l'une quelconque de ces racines primitives ne dépendra que d'une congruence du degré ν, congruence *irréductible*, sans quoi l'équation en i ne le serait pas non plus, parce que les racines de la congruence en i sont toutes des puissances de la racine primitive.

On voit ici cette conséquence remarquable, que toutes les quantités algébriques qui peuvent se présenter dans la théorie sont racines d'équations de la forme

$$x^{p^\nu} = x.$$

Cette proposition, énoncée algébriquement, est celle-ci : Étant donnés une fonction Fx et un nombre premier p, on peut poser

$$fx.Fx = x^{p^\nu} - x + p\varphi x,$$

fx et φx étant des fonctions entières, toutes les fois que la congruence $Fx \equiv 0 \pmod{p}$ sera irréductible.

Si l'on veut avoir toutes les racines d'une pareille congruence au moyen d'une seule, il suffit d'observer que l'on a généralement

$$(Fx)^{p^n} = F(x^{p^n})$$

et que, par conséquent, l'une des racines étant x, les autres seront

$$x^p,\ x^{p^2},\ldots,\ x^{p^{\nu-1}} \quad [*].$$

Il s'agit maintenant de faire voir que, réciproquement à ce que nous venons de dire, les racines de l'équation ou de la congruence $x^{p^\nu} = x$ dépendront toutes d'une seule congruence du degré ν.

Soit en effet i une racine d'une congruence irréductible, et telle que toutes les racines de la congruence $x^{p^\nu} = x$ soient fonctions rationnelles de i. (Il est clair qu'ici, comme dans les équations ordinaires, cette propriété a lieu) [**].

Il est d'abord évident que le degré μ de la congruence en i ne saurait être plus petit que ν, sans quoi la congruence

$$(\nu) \qquad x^{p^{\nu-1}} - 1 = 0$$

---

[*] De ce que les racines de la congruence irréductible de degré ν

$$Fx = 0$$

sont exprimées par la suite

$$x,\ x^p,\ x^{p^2},\ldots,\ x^{p^{\nu-1}},$$

on aurait tort de conclure que ces racines soient toujours des quantités exprimables par radicaux. Voici un exemple du contraire :

La congruence irréductible

$$x^2 + x + 1 = 0 \qquad \text{(mod. 2)}$$

donne

$$x = \frac{-1 + \sqrt{-3}}{2},$$

qui se réduit à

$$\frac{0}{0}, \qquad \text{(mod. 2)}$$

formule qui n'apprend rien.

[**] La proposition générale dont il s'agit ici peut s'énoncer ainsi : Étant donnée une équation algébrique, on pourra trouver une fonction rationnelle θ de toutes ses racines, de telle sorte que, réciproquement, chacune des racines s'exprime rationnellement en θ. Ce théorème était connu d'Abel, ainsi qu'on peut le voir par la première partie du Mémoire que ce célèbre géomètre a laissé sur les fonctions elliptiques.

aurait toutes ses racines communes avec la congruence

$$x^{p^{\mu}-1} - 1 = 0,$$

ce qui est absurde, puisque la congruence (ν) n'a pas de racines égales, comme on le voit en prenant la dérivée du premier membre. Je dis maintenant que μ ne peut non plus être $> \nu$.

En effet, s'il en était ainsi, toutes les racines de la congruence

$$x^{p^{\mu}} = x$$

devraient dépendre rationnellement de celles de la congruence

$$x^{p^{\nu}} = x.$$

Mais il est aisé de voir que si l'on a

$$i^{p^{\nu}} = i,$$

toute fonction rationnelle $h = fi$ donnera encore

$$(fi)^{p^{\nu}} = f(i^{p^{\nu}}) = fi, \quad \text{d'où} \quad h^{p^{\nu}} = h.$$

Donc toutes les racines de la congruence $x^{p^{\mu}} = x$ lui seraient communes avec l'équation $x^{p^{\nu}} = x$. Ce qui est absurde.

Nous savons donc enfin que toutes les racines de l'équation ou congruence $x^{p^{\nu}} = x$ dépendent nécessairement d'une *seule* congruence *irréductible* de degré ν.

Maintenant, pour avoir cette congruence irréductible d'où dépendent les racines de la congruence $x^{p^{\nu}} = x$, la méthode la plus générale sera de délivrer d'abord cette congruence de tous les facteurs communs qu'elle pourrait avoir avec des congruences de degré inférieur et de la forme

$$x^{p^{\mu}} = x.$$

On obtiendra ainsi une congruence qui devra se partager en congruences irréductibles de degré ν. Et, comme on sait exprimer toutes les racines de chacune de ces congruences irréductibles au moyen d'une seule, il sera aisé de les obtenir toutes par la méthode de M. Gauss.

Le plus souvent, cependant, il sera aisé de trouver par le tâtonnement une congruence irréductible d'un degré donné ν, et l'on doit en déduire toutes les autres.

Soient, pour exemple. $p = 7$, $\nu = 3$. Cherchons les racines de la congruence

$$x^{7^3} = x \pmod 7. \tag{1}$$

J'observe que la congruence

$$i^3 = 2 \pmod 7 \tag{2}$$

étant irréductible, et du degré 3, toutes les racines de la congruence (1) dépendent rationnellement de celle de la congruence (2), en sorte que toutes les racines de (1) sont de la forme

$$a + a_1 i + a_2 i^2, \quad \text{ou bien} \quad a + a_1 \sqrt[3]{2} + a_2 \sqrt[3]{4}. \tag{3}$$

Il faut maintenant trouver une racine primitive, c'est-à-dire une forme de l'expression (3) qui, élevée à toutes les puissances, donne toutes les racines de la congruence

$$x^{7^3-1} = 1, \quad \text{savoir} \quad x^{2^1 \cdot 3^2 \cdot 19} = 1 \pmod 7,$$

et nous n'avons besoin pour cela que d'avoir une racine primitive de chaque congruence

$$x^2 = 1, \quad x^{3^2} = 1, \quad x^{19} = 1.$$

La racine primitive de la première est -1; celles de $x^{3^2} - 1 = 0$ sont données par les équations

$$x^3 = 2, \quad x^3 = 4,$$

en sorte que i est une racine primitive de $x^{3^2} = 1$.

Il ne reste qu'à trouver une racine de $x^{19} - 1 = 0$, ou plutôt de

$$\frac{x^{19} - 1}{x - 1} = 0,$$

et essayons pour cela si l'on ne peut pas satisfaire à la question en posant simplement $x = a + a_1 i$, au lieu de $a + a_1 i + a_2 i^2$; nous de-

vrons avoir

$$(a + a_1 i)^{19} = 1,$$

ce qui, en développant par la formule de Newton, et réduisant les puissances de a, de a_1 et de i, par les formules

$$a^{m(p-1)} = 1, \quad a_1^{m(p-1)} = 1, \quad i^3 = 2,$$

se réduit à

$$3[a - a^4 a_1^3 + (a^5 a_1^2 + a^2 a_1^5) i^2] = 1,$$

d'où, en séparant,

$$3a - 3a^4 a_1^3 = 1, \quad a^5 a_1^2 + a^2 a_1^5 = 0.$$

Ces deux dernières équations sont satisfaites en posant $a = -1$, $a_1 = 1$. Donc

$$-1 + i$$

est une racine primitive de $x^{19} = 1$. Nous avons trouvé plus haut, pour racines primitives de $x^2 = 1$ et de $x^3 = 1$, les valeurs -1 et i; il ne reste plus qu'à multiplier entre elles les trois quantités

$$-1, \quad i, \quad -1 + i,$$

et le produit $i - i^2$ sera une racine primitive de la congruence

$$x^{7^3-1} = 1.$$

Donc ici l'expression $i - i^2$ jouit de la propriété, qu'en l'élevant à toutes les puissances, on obtiendra $7^3 - 1$ expressions différentes et de la forme

$$a + a_1 i + a_2 i^2.$$

Si nous voulons avoir la congruence de moindre degré d'où dépend notre racine primitive, il faut éliminer i entre les deux équations

$$i^3 = 2, \quad \alpha = i - i^2.$$

On obtient ainsi

$$\alpha^3 - \alpha + 2 = 0.$$

Il sera convenable de prendre pour base des imaginaires et de re-

présenter par i la racine de cette équation, en sorte que

$$(i) \qquad i^3 - i + 2 = 0,$$

et l'on aura toutes les imaginaires de la forme

$$a + a_1 i + a_2 i^2,$$

en élevant i à toutes les puissances, et réduisant par l'équation (i).

Le principal avantage de la nouvelle théorie que nous venons d'exposer est de ramener les congruences à la propriété (si utile dans les équations ordinaires) d'admettre précisément autant de racines qu'il y a d'unités dans l'ordre de leur degré.

La méthode pour avoir toutes ces racines sera très-simple. Premièrement on pourra toujours préparer la congruence donnée $Fx = 0$, de manière à ce qu'elle n'ait plus de racines égales, ou, en d'autres termes, à ce qu'elle n'ait plus de facteur commun avec $F'x = 0$, et le moyen de le faire est évidemment le même que pour les équations ordinaires.

Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$.

Si maintenant on veut avoir les solutions imaginaires du second degré, on cherchera le plus grand facteur commun à $Fx = 0$ et à $x^{p^2-1} = 1$, et, en général, les solutions de l'ordre ν seront données par le plus grand commun diviseur à $Fx = 0$ et à $x^{p^\nu - 1} = 1$.

C'est surtout dans la théorie des permutations, où l'on a sans cesse besoin de varier la forme des indices, que la considération des racines imaginaires des congruences paraît indispensable. Elle donne un moyen simple et facile de reconnaître dans quel cas une équation primitive est soluble par radicaux, comme je vais essayer d'en donner en deux mots une idée.

Soit une équation algébrique $fx = 0$ de degré p^ν; supposons que les p^ν racines soient désignées par x_k, en donnant à l'indice k les p^ν valeurs déterminées par la congruence $k^{p^\nu} = k \pmod{p}$.

Prenons une fonction quelconque rationnelle V des p^ν racines x_k. Transformons cette fonction en substituant partout à l'indice k l'in-

dice $(ak+b)^{p^r}$, a, b, r étant des constantes arbitraires satisfaisant aux conditions de $a^{p^\nu-1}=1$, $b^{p^\nu}=b$ (mod. p) et de r entier.

En donnant aux constantes a, b, r toutes les valeurs dont elles sont susceptibles, on obtiendra en tout $p^\nu(p^\nu-1)\nu$ manières de permuter les racines entre elles par des substitutions de la forme $[x_k, x_{(ak+b)^{p^r}}]$, et la fonction V admettra en général par ces substitutions $p^\nu(p^\nu-1)\nu$ formes différentes.

Admettons maintenant que l'équation proposée $fx=0$ soit telle, que toute fonction des racines invariable par les $p^\nu(p^\nu-1)\nu$ permutations que nous venons de construire, ait pour cela même une valeur numérique rationnelle.

On remarque que, dans ces circonstances, l'équation $fx=0$ sera soluble par radicaux, et, pour parvenir à cette conséquence, il suffit d'observer que la valeur substituée à k, dans chaque indice, peut se mettre sous les trois formes

$$(ak+b)^{p^r}=[a(k+b^1)]^{p^r}=a^1k^{p^r}+b''=a'(k+b')^{p^r}.$$

Les personnes habituées à la théorie des équations le verront sans peine.

Cette remarque aurait peu d'importance si je n'étais parvenu à démontrer que, réciproquement, une équation primitive ne saurait être soluble par radicaux, à moins de satisfaire aux conditions que je viens d'énoncer. (J'excepte les équations du neuvième et du vingt-cinquième degré.)

Ainsi, pour chaque nombre de la forme p^ν, on pourra former un groupe de permutations tel, que toute fonction des racines invariable par ces permutations devra admettre une valeur rationnelle quand l'équation de degré p_μ sera primitive et soluble par radicaux.

D'ailleurs, il n'y a que les équations d'un pareil degré p^ν qui soient à la fois primitives et solubles par radicaux.

Le théorème général que je viens d'énoncer précise et développe les conditions que j'avais données dans le *Bulletin* du mois d'avril. Il indique le moyen de former une fonction des racines dont la valeur sera rationnelle, toutes les fois que l'équation primitive de degré p^ν sera soluble par radicaux, et mène, par conséquent, aux caractères de réso-

lubilité de ces équations, par des calculs sinon praticables, du moins qui sont possibles en théorie.

Il est à remarquer que, dans le cas où $\nu = 1$, les diverses valeurs de k ne sont autre chose que la suite des nombres entiers. Les substitutions de la forme $(x_k,\ x_{ak+b})$ seront au nombre de $p(p-1)$.

La fonction qui, dans le cas des équations solubles par radicaux, doit avoir une valeur rationnelle, dépendra, en général, d'une équation de degré $1.2.3\ldots(p-2)$, à laquelle il faudra, par conséquent, appliquer la méthode des racines rationnelles.