

Theorems on groups of substitutions.

By Mr. L. SYLOW at FREDERIKSHALD in NORWAY.

It is known that if the order of a group of substitutions is divisible by a prime number n , the group always contains a substitution [=element] of order n . This important theorem is contained in another more general than this: "If the order of a group is divisible by n^α , n being prime, the group contains a partial bundle [=subgroup] of order n^α ". The demonstration [=proof] itself of the theorem furnishes some other general properties of groups of substitutions. I append to these some more, less general, propositions which are connected with them or which follow from them, of which several however are already known by a work of Mr. E. Mathieu.

The notation and terms used are those of Mr. C. Jordan.

1. If G is a group of substitutions whose order N is divisible by the prime number n , it is known that G contains a substitution of order n , but we can suppose more generally that it contains a group g of order n^α , in which consequently each substitution is of order a divisor of n^α . We denote the substitutions of g by

$$1, \theta_1, \theta_2, \dots$$

whereas the substitutions of G in general are denoted by

$$1, \psi_1, \psi_2, \dots$$

Finally we shall suppose that G does not contain any partial group [=subgroup] whose order is a power of n greater than n^α . Now G always contains substitutions permutable with [=normalizing] g , to wit the substitutions of the latter themselves, but it is possible that it contains a larger number; in any case these substitutions form a group γ , which contains g , and whose order will be denoted $n^\alpha\nu$; this number is in turn a divisor of N ; thus we may set:

$$N = n^\alpha\nu h.$$

The substitutions of the group γ will be denoted by

$$1, \varphi_1, \varphi_2, \dots$$

The θ are thus comprised among the φ , just as the latter among the ψ .

That set, we are first going to show that the number ν must be prime to n . Let x_0, x_1, x_2, \dots be the letters which the group G permutes among themselves, and let y_0 be a rational function of the x , invariant under the substitutions of g but variable under every other function. [In effect, y_0 is a point whose stabilizer is g .] This function [=point] takes, under the substitutions of γ , the ν different values

$$y_0, y_1, y_2, \dots, y_{\nu-1}.$$

Every one of these functions is invariant under [=fixed by] the substitutions of g but variable under [=moved by] every other substitution. Indeed, if y_1 is obtained from y_0 by the substitution φ_1 , y_1 is invariant under the group transformed [=conjugated] from g by φ_1 , but variable under every other substitution; but φ_1 being permutable with g , the transformed group is the same as g . Now if one operates on the y by the substitutions of γ , one will have among these quantities [=points] a group γ' necessarily transitive and isomorphic to [=a quotient of] γ . In order to obtain its order we must divide that of γ by the number of substitutions φ which do not alter [=move] any of the y , that is by n^α . Thus the order of γ' is ν . If now ν were divisible by n , γ' would have to contain a substitution of order n ; a corresponding substitution φ_1 of γ would have to fulfil the condition

$$\varphi_1^n = \theta_a.$$

But since φ_1 is permutable with [=normalizes] g , one sees that in this case the substitutions $\theta_q \varphi_1^p$ would form a group of order $n^{\alpha+1}$ contained in G . That being contrary to the hypothesis, one concludes that ν is prime to n .

Let us note here that the θ are the only substitutions in γ whose orders are powers of n . Indeed, if φ_1 is a substitution of γ outside g , the substitutions $\theta_q \varphi_1^p$ form a group whose order is equal to $n^\alpha m$, m denoting the exponent of the least high power of φ_1 which belongs to g . Now one sees without difficulty that the only powers of φ_1 which belong to g are those whose exponents are multiples of m , whence it follows immediately that m is a divisor of the order of φ_1 . Thus if the order of φ_1 were a power of n , one would have $m = n^\beta$, which is impossible, the group of the $\theta_q \varphi_1^p$ not being able to be of order $n^{\alpha+\beta}$.

The number h is also not divisible by n . In order to see this, let us imagine a rational function of the x invariant under the substitutions of γ , but variable under every other substitution. Let z_0 be this function, and let us represent by

$$z_0, z_1, z_2, \dots, z_{h-1}$$

the h values it takes under the substitutions of G . [In effect, G permutes the points z_0, \dots, z_{h-1} and γ is the stabilizer of z_0 .] Let us carry out the substitutions of g on the z ; under this, z_0 does not vary, but every one of the other z takes a number of values which is a divisor of the order of g , that is a power of n . This power cannot be reduced to unity; if for example z_1 were invariant under

g and z_1 were obtained from [=the image of] z_0 by the substitution ψ_1 , z_0 would have to be invariant under the group transformed from g by ψ_1^{-1} ; now, the only group of order n^α contained in γ being g , ψ_1^{-1} would have to be permutable with g , which does not happen. Thus if one partitions the functions [=points] z_1, \dots, z_{h-1} into systems [=orbits], uniting together those which are permuted amongst themselves by the substitutions of g , the number of functions contained in each system will be a power of n . Consequently the number h is of the form $np + 1$. Thus the order of g equals the largest power of n which divides the order of G . The results obtained are summarised as follows:

Theorem 1 *If n^α denotes the largest power of the prime number n which divides the order of the group G , this group contains another, g , of order n^α ; if moreover $n^\alpha\nu$ denotes the order of the largest group contained in G whose substitutions are permutable with g , the order of G will be of the form $n^\alpha\nu(np + 1)$.*

2. Evidently g is not the only group of order n^α contained in G , except only the case $p = 0$. But one could ask if G contains any others than g and its transforms by the substitutions of G . That is what we are going to investigate. Let g' be a group of order n^α contained in G but different from g , and let

$$1, \theta'_1, \theta'_2, \dots$$

be its substitutions. Let us carry out these substitutions on the functions z , and combine into systems those which are exchanged amongst themselves by this [=orbits under g']. As we have already said, the number of functions contained in each system must be a divisor of n^α ; thus one must have an equality of the form

$$np + 1 = n^a + n^b + n^c + \dots$$

n^a, n^b, n^c, \dots denoting the number of functions [=points] contained in the various systems [=orbits]. But that requires that at least one of the exponents a, b, c, \dots is zero; in other terms, at least one of the functions z must be invariant under all the substitutions of g' . Let z_k be this function, and suppose that it is obtained from z_0 by the substitution ψ_k . Now z_k is only invariant under the substitutions $\psi_k^{-1}\varphi_a\psi_k$; moreover $\psi_k^{-1}\varphi_a\psi_k$ is similar to [=has the same cycle type as?] φ_a , and among the φ_a there are only the θ whose orders are powers of n . Thus one must have

$$\theta'_b = \psi_k^{-1}\theta_a\psi_k$$

for all the values of b . The group g' is thus the transform of g under ψ_k .

If furthermore one replaces ψ_k by $\varphi_r\psi_k$, one evidently has the same transformed group. On the other hand ψ_k can only be replaced by $\varphi_r\psi_k$. Indeed if one has

$$\psi_l^{-1}\theta_a\psi_l = \psi_k^{-1}\theta_b\psi_k$$

for every value of a , it follows that

$$\psi_k \psi_l^{-1} \theta_a \psi_l \psi_k^{-1} = \theta_b$$

whence one concludes that

$$\psi_l \psi_k^{-1} = \varphi_r$$

or

$$\psi_l = \varphi_r \psi_k.$$

One can thus state this theorem:

Theorem 2 *Everything being as in the preceding theorem, the group G contains precisely $np+1$ distinct groups of order n^α ; they are all obtained by transforming an arbitrary one among them by the substitutions of G , every group being given by $n^\alpha\nu$ distinct transformations.*

By analogous reasoning one sees that every group of order n^β contained in G , β being less than α , is the transform of a group contained in g by a substitution in G , and that there are *at least* $n^\alpha\nu$ ways of obtaining it by transformation. Indeed it is possible that there are more, since from the relation

$$\psi_k \psi_l^{-1} \theta_a \psi_l \psi_k^{-1} = \theta_b$$

one cannot conclude that

$$\psi_l \psi_k^{-1} = \varphi_r$$

unless it holds for every value of a .

3. Now we are going to concern ourselves with the group g . Let us form the transformations [=conjugates] of the substitutions $1, \theta_1, \theta_2, \dots$ by one of them; as by this one only reproduces them in a different order, one has a substitution [=permutation] among the substitutions θ themselves. If one transforms them successively by all the substitutions of g , one has a group of substitutions; indeed, this follows immediately from the identity:

$$\theta_b^{-1} \theta_a^{-1} \theta_r \theta_a \theta_b = (\theta_a \theta_b)^{-1} \theta_r (\theta_a \theta_b).$$

The group among the θ which one obtains in this way is necessarily intransitive, the identity substitution at least being invariant under the transformations; but there are also other invariant substitutions, as we shall see. Indeed, one can combine into systems those substitutions which are exchanged amongst themselves by the transformations; that done, the transformations will produce a transitive group among the substitutions of each system. Now the number of substitutions θ contained in a system is a divisor of the order of the corresponding group; but one sees by a familiar argument that the order of this group is equal to n^α divided

by the number of transformations which do not change any of the substitutions of the system being considered. So therefore the number of transformations contained in each system is a power of n . The identity substitution being invariant, one must have an equality of the form

$$n^\alpha = 1 + n^a + n^b + \dots$$

where $1, n^a, n^b, \dots$ are the numbers of substitutions in the various systems. That requires that at least $n - 1$ of the exponents a, b, \dots are zero. There are thus in the group g at least n substitutions, including the identity substitution, which are invariant; in other terms, there are in g at least n substitutions exchangeable [=commuting] with all the substitutions of the group.

Now since, two substitutions being exchangeable, their powers are also, there will always be among the substitutions exchangeable with all the others a substitution of order n . Let θ_0 be this substitution, and let y_0 be a rational function of the x , invariant under θ_0^i but variable under every other substitution, and let us represent by

$$y_0, y_1, y_2, \dots$$

the $n^{\alpha-1}$ values which it takes under the substitutions of g . By carrying out on the y the substitutions of g one will have among these functions a group isomorphic to [=quotient of] g , whose order is evidently $n^{\alpha-1}$. By virtue of what has just been demonstrated this group must contain a substitution of order n exchangeable with all the substitutions of the group. Now let θ_1 be a corresponding substitution in g . Applied n times in succession θ_1 must return all the y to their original places, thus

$$\theta_1^n = \theta_0^a.$$

Moreover, if ϑ denotes an arbitrary substitution of g , θ_1 must produce on the y the same substitution as its transform by ϑ , that is, one has

$$\vartheta^{-1}\theta_1\vartheta = \theta_0^b\theta_1.$$

The substitutions $\theta_0^i\theta_1^k$ evidently constitute a group of order n^2 . If now one forms a rational function of the x invariant under the $\theta_0^i\theta_1^k$, but variable under every other substitution, and one argues on this function as we have argued on y_0 , one sees that g must contain a substitution θ_2 which fulfils the conditions

$$\begin{aligned} \theta_2^n &= \theta_0^c\theta_1^d \\ \vartheta^{-1}\theta_2\vartheta &= \theta_0^e\theta_1^t\theta_2 \end{aligned}$$

Continuing thus one proves the following theorem:

Theorem 3 *If the order of a group is n^α , n being prime, an arbitrary substitution ϑ of the group can be expressed by the formula*

$$\vartheta = \theta_0^i\theta_1^k\theta_2^l \cdots \theta_{\alpha-1}^r$$

where

$$\begin{aligned}
 \theta_0^n &= 1 \\
 \theta_1^n &= \theta_0^a \\
 \theta_2^n &= \theta_0^b \theta_1^c \\
 \theta_3^n &= \theta_0^d \theta_1^e \theta_2^f \\
 &\dots \quad \dots
 \end{aligned}$$

and where one has

$$\begin{aligned}
 \vartheta^{-1} \theta_0 \vartheta &= \theta_0 \\
 \vartheta^{-1} \theta_1 \vartheta &= \theta_0^\beta \theta_1 \\
 \vartheta^{-1} \theta_2 \vartheta &= \theta_0^\gamma \theta_1^\delta \theta_2 \\
 \vartheta^{-1} \theta_3 \vartheta &= \theta_0^\varepsilon \theta_1^\zeta \theta_2^\eta \theta_3
 \end{aligned}$$

One sees that [the orders of] the composition factors of the group are all equal to n , thus we can state as a corollary the following proposition:

If the order of an algebraic equation is a power of a prime number, the equation is soluble by radicals.

Let us suppose that the group g is transitive and that the number of letters is equal to n^β . In this case the substitution which we have called θ_0 is regular [=semi-regular], that is it moves all the letters, and all its cycles contain the same number of them; for otherwise it evidently would not be exchangeable with all the substitutions of the group. Moreover the group will be imprimitive; indeed the substitutions will replace the letters contained in one cycle of θ_0 by the letters in another cycle. Thus the equation is divided by the solution of an equation of degree $n^{\beta-1}$ into $n^{\beta-1}$ equations of degree n . Evidently the groups of these last equations, as well as that of the auxiliary equation, will only contain substitutions whose orders are powers of n ; the equations of degree n will consequently be abelian. Thus:

Theorem 4 *If the degree of an irreducible equation is n^β , n being prime, and the order of its group is also a power of n , an arbitrary root will be determined by a series of β abelian equations of degree n .*

For the case $n = 2$ the last proposition has been proved by Mr. J. Petersen (Om de ligninger, der kunne løses ved Kvadratrod etc. Kjøbenhavn 1871). [On the equations which can be solved by square roots etc. Copenhagen.]

These results can even be generalized. Indeed, if the order of the group of an equation is equal to $n^\alpha m$, m being less than n , one has, using theorem 1, $p = 0$, $m = \nu$. Consequently all the substitutions in the group are permutable with [=normalize] the partial group [=subgroup] which we have denoted by g . The group is therefore reduced to g , if one adjoins the functions which we have denoted by y_0, y_1, \dots , and which are the roots of an equation whose order and degree are equal to m . Thus if the auxiliary equation is soluble by radicals, the given equation is also. From there it follows as an immediate consequence that:

Theorem 5 *If the order of an algebraic equation is*

$$n^\alpha n_1^{\alpha_1} n_2^{\alpha_2} n_3^{\alpha_3} \dots,$$

n, n₁, n₂, n₃, ... being primes, if moreover one has

$$\begin{aligned} n &> n_1^{\alpha_1} n_2^{\alpha_2} n_3^{\alpha_3} \dots \\ n_1 &> n_2^{\alpha_2} n_3^{\alpha_3} \dots \\ n_2 &> n_3^{\alpha_3} \dots \end{aligned}$$

the equation is soluble by radicals.

4. From the preceding one draws also a simple proof of the theorem of Mr. E. Mathieu: *Every transitive group on n^α letters, n denoting a prime number, contains a regular substitution of order n.* (See Mr. Liouville's journal 1861.)

Let G be a transitive group of degree $n^\alpha m$, and let N be its order. Now N is divisible by $n^\alpha m$; therefore let

$$N = n^{\alpha+\beta} m N',$$

N' being supposed prime to n ; let moreover G' be the group of order $n^\beta N'$ which contains the substitutions of G which do not move x_0 . Now G contains a group g of order $n^{\alpha+\beta}$, and the substitutions of the latter which do not move x_0 form a group g' , whose order we denote by n^γ . Now g' is evidently contained in G' , so we have $\gamma \leq \beta$.

But if one denotes by r the number of places which are successively occupied by x_0 , when one applies all the substitutions of g , one has, as is known,

$$rn^\gamma = n^{\alpha+\beta}$$

thus

$$r \geq n^\alpha.$$

The number r is necessarily a power of n ; furthermore, what has just been proved for x_0 holds for each of the x . Thus every letter takes under the group g a number of places which is a power of n equal to or greater than n^α .

If we now suppose $m = 1$, we see that g must be transitive. That being so, g must contain a regular substitution as we have already said. The theorem is therefore proved.

There is another case where one can equally prove the existence of regular substitutions. Indeed suppose $\alpha = 1$ with $m < n$. Since $n^2 > mn$, one concludes that each letter takes precisely n different places under the substitutions of g . If therefore one combines into one system the letters which are exchanged amongst themselves, one has m systems [=orbits] each of n letters. Now if c is a cycle of a substitution of g , c will represent a circular [=cyclic] substitution of the n

letters in one system. Now if another substitution of g moves the same letters, this displacement cannot be other than a power of c , for in the contrary case one could derive from the two substitutions a third which would not be of order n . So if θ is a substitution of g , one has

$$\theta = c_1 c_2 \dots c_r$$

c_k denoting a circular substitution among the letters of the k^{th} system. If now $r < m$, the group g must contain a substitution θ_1 which permutes the letters of the $(r+1)^{\text{st}}$ system, and after what has just been said one has

$$\theta_1 = c_1^\delta c_2^\varepsilon \dots c_r^\zeta c_{r+1} c_{r+2} \dots c_s,$$

the numbers $\delta, \varepsilon, \dots, \zeta$ possibly being zero. One deduces from this

$$\theta^p \theta_1 = c_1^{p+\delta} c_2^{p+\varepsilon} \dots c_r^{p+\zeta} c_{r+1} c_{r+2} \dots c_s.$$

Now, since the number of systems is less than n , one can determine p such that none of the numbers $p+\delta, p+\varepsilon, \dots, p+\zeta$ is equal to zero. One thus obtains a substitution having $r+s$ [*sic: should be s , here and in the next sentence*] cycles. If $r+s < m$, one determines in the same way a substitution of g which has more than $r+s$ cycles; continuing thus one ends by finding a regular substitution.

Theorem 6 *A transitive group on nm letters, n being prime, and $m < n$, contains a regular [=semi-regular] substitution of order n .*

By virtue of these two theorems every transitive group on a number of letters less than 12 contains regular substitutions. But already for degree 12 there exist transitive groups which lack them. Thus the substitutions of the group derived from [=generated by]

$$\begin{aligned} \theta_0 &= (x_0 x_1 x_2)(x_3 x_4 x_5)(x_6 x_7 x_8) \\ \theta_1 &= (x_3 x_4 x_5)(x_6 x_8 x_7)(x_9 x_{10} x_{11}) \\ \varphi &= (x_0 x_3 x_6 x_9 x_1 x_4 x_8 x_{11})(x_2 x_5 x_7 x_{10}) \end{aligned}$$

are similar, some to θ_0 , the others to powers of φ . Another example is the group derived from θ_0, θ_1 and the following substitutions

$$\begin{aligned} &(x_0 x_3 x_1 x_4)(x_2 x_5)(x_6 x_9 x_7 x_{11})(x_8 x_{10}) \\ &(x_0 x_7 x_1 x_6)(x_2 x_8)(x_3 x_9 x_4 x_{11})(x_5 x_{10}). \end{aligned}$$

These two groups are of order 72, and characterize equations soluble by radicals.

5. Let us consider now the transitive groups of prime degree. Let n be the degree, N the order of the group. Since N is divisible by n but not divisible by n^2 , one has

$$N = n\nu(np + 1).$$

Let us suppose the letters arranged in an order such that a circular substitution of the group is expressed by

$$\theta = |k \ k+1|;$$

[i.e. $\theta : k \mapsto k + 1$]; then the substitutions permutable with the group derived from [=generated by] θ are of the form

$$|k \ ak+b|$$

Now $n\nu$ is equal to the order of this last group, so ν is equal to the number of substitutions of the given group which are of the form $|k \ ak|$; so ν is a divisor of $n - 1$. Thus one has this theorem:

Theorem 7 *The order of a transitive group on a prime number of letters is of the form $n\nu(np + 1)$, where n is the degree, $np + 1$ the number of essentially different regular substitutions, that is, which are not powers of each other, and where ν is the number of substitutions of the form $|k \ ak|$, an arbitrary circular substitution being denoted by $|k \ k+1|$.*

These results are in part known by the researches of Mr. E. Mathieu, who has proved that the number of essentially different circular substitutions is of the form $np + 1$, and that there are at least $\frac{N}{n\nu}$ of them, such a number being derivable from the $|k \ k+b|$ by transforming them by the substitutions of the group. What is necessary to add to the propositions of Mr. Mathieu to have the above theorem is thus that all the circular substitutions can be derived in the manner described, a point on which Mr. Mathieu seems to have some doubts.

Let us recall here these two propositions equally due to Mr. E. Mathieu:

1. *If $p > 0$, ν cannot be equal to 1.*
2. *If $p > 0$, and n is of the form $4h + 3$, ν cannot be equal to 2.*

Being given the order N of a transitive group on n letters, our theorem permits us to determine the number of circular substitutions and the number of substitutions permutable with the group derived from a circular substitution. Indeed ν , being smaller than n , is completely determined by the congruence

$$\frac{N}{n} \equiv \nu \pmod{n};$$

and then one has

$$np + 1 = \frac{N}{n\nu}.$$

Let us take as an example the group of degree $\frac{q^r-1}{q-1}$, q being a prime number, which one can derive from the linear group with r indices. If r is an odd prime number, it can happen that $\frac{q^r-1}{q-1}$ is a prime number. Set therefore

$$\begin{aligned} n &= \frac{q^r - 1}{q - 1} \\ N &= \frac{q^r - 1}{q - 1} (q^r - q)(q^r - q^2) \dots (q^r - q^{r-1}). \end{aligned}$$

Now one sees easily that q is a primitive root of the congruence

$$z^r \equiv 1 \pmod{n};$$

consequently one has

$$z^{r-1} + z^{r-2} + \dots + z + 1 \equiv (z - q)(z - q^2) \dots (z - q^{r-1}).$$

If one now sets

$$z \equiv q^r \equiv 1,$$

one obtains

$$(q^r - q)(q^r - q^2) \dots (q^r - q^{r-1}) \equiv r$$

that is

$$\frac{N}{n} \equiv r.$$

If therefore one chooses the indices so that a circular substitution is represented by $|k \ k+1|$, the group will contain r substitutions of the form $|k \ ak|$ to wit the $|k \ q^i k|$; the number of essentially different circular substitutions will be $\frac{q^r-1}{r}(q^r - q^2) \dots (q^r - q^{r-1})$.

The formula $N = n\nu(np+1)$ considerably reduces the number of divisors of the product $2.3.\dots.n$ which can denote the order of a transitive group. If for example one sets $n = 7$, ν must be equal to 6 or 3, except for equations soluble by radicals. But if there exists a group of order $7(7p+1)6$, there is also one of order $7(7p+1)3$ containing those substitutions of the first group which are equivalent to an even number of transpositions. In order to obtain the values of $7p+1$ it therefore suffices to examine the case $n = 3$; thus $7p+1$ must be a divisor of the number $2.5.4.3$, and consequently equal to one of the numbers $1, 2^3, 5.3, 5.3.2^3$, of which the third must be rejected, since there is no group of order 5.3 on 6 letters. For $n = 11$ there will only be 15 cases to examine, etc.

Let us examine now the composition of the groups in question. So let G and H be two transitive groups, and let G be contained in H and permutable with its substitutions. Moreover, let $n(np+1)\nu$ be the order of G , and denote by $\theta_0, \theta_1, \dots, \theta_{np}$ its essentially different circular substitutions. Thus G contains the $np+1$ groups of order n : $\theta_0^r, \theta_1^r, \dots, \theta_{np}^r$. If these groups are transformed by an arbitrary circular substitution in H , which will be denoted by θ' , they

must be reproduced in another order; thus one has a substitution on the $np + 1$ groups. But one sees without difficulty that if a group θ_i^r is not invariant under the transformation, it must form part of a cycle of n groups. Thus at least one of the groups is invariant under the transformation. If we suppose that it is θ_0^r , this group is permutable with θ' , whence one concludes

$$\theta' = \theta_0^b.$$

Indeed, if one chooses the indices such that

$$\theta_0 = |k \ k+1|,$$

there are among the $n(n-1)$ substitutions $|k \ ak+b|$, alone permutable with θ_0^r , only the $|k \ k+b|$ which are of order n . All the circular substitutions in H therefore form part of G .

Conversely, if G and H contain the same circular substitutions, and if H contains G , H is composed with G [i.e. G is a normal subgroup of H]. Always let $n(np+1)\nu$ be the order of G , that of H will be $n(np+1)\nu\nu_1$, ν_1 being a divisor of $\frac{n-1}{\nu}$. The substitutions of the form $|k \ ak|$ contained in H are powers of a single one of them; denote the latter by φ ; those which belong to G will consequently be the powers of φ^{ν_1} . Now it is easy to see that H derives from [=is generated by] the substitutions $\theta_0, \theta_1, \dots, \theta_{np}, \varphi$. Indeed the group derived from these substitutions is contained in H ; on the other hand its order cannot be less than $n(np+1)\nu\nu_1$, since there are $np+1$ circular substitutions and $\nu\nu_1$ substitutions $|k \ ak|$. Likewise G is derived from the substitutions $\theta_0, \theta_1, \dots, \theta_{np}, \varphi^{\nu_1}$. Thus G is permutable with the substitutions of H , if it is permutable with φ . Now the latter holds, for firstly the transforms of $\theta_0, \theta_1, \dots, \theta_{np}$ by φ are circular substitutions belonging to H and therefore to G ; secondly φ^{ν_1} is exchangeable with φ .

Thus we have proved the following theorem:

Theorem 8 *For a transitive group of prime degree to be composed with a partial group, it is necessary and sufficient that the second group contains all of the circular substitutions of the first.*

Let an equation be given whose group is H . If one forms a function of the roots invariant under the substitutions of G , but variable under every other substitution, it will evidently be a root of an abelian equation of degree ν_1 . By adjoining this function one reduces the group of the equation to G .

So if an irreducible equation of degree n is composite, it becomes simple by the adjunction of the root of an abelian equation, whose degree is a divisor of $n-1$.

By supposing $p = 0$, one recovers a known property of equations soluble by radicals.

Oeuvres de Lagrange. T. 3 /
publiées par les soins de M.
J.-A. Serret [et G. Darboux] ;
[précédé d'une notice sur la
vie [...]

Lagrange, Joseph-Louis (1736-1813). Auteur du texte. Oeuvres de Lagrange. T. 3 / publiées par les soins de M. J.-A. Serret [et G. Darboux] ; [précédé d'une notice sur la vie et les ouvrages de J.-L. Lagrange, par M. Delambre]. 1867-1892.

1/ Les contenus accessibles sur le site Gallica sont pour la plupart des reproductions numériques d'oeuvres tombées dans le domaine public provenant des collections de la BnF. Leur réutilisation s'inscrit dans le cadre de la loi n°78-753 du 17 juillet 1978 :

- La réutilisation non commerciale de ces contenus ou dans le cadre d'une publication académique ou scientifique est libre et gratuite dans le respect de la législation en vigueur et notamment du maintien de la mention de source des contenus telle que précisée ci-après : « Source gallica.bnf.fr / Bibliothèque nationale de France » ou « Source gallica.bnf.fr / BnF ».
- La réutilisation commerciale de ces contenus est payante et fait l'objet d'une licence. Est entendue par réutilisation commerciale la revente de contenus sous forme de produits élaborés ou de fourniture de service ou toute autre réutilisation des contenus générant directement des revenus : publication vendue (à l'exception des ouvrages académiques ou scientifiques), une exposition, une production audiovisuelle, un service ou un produit payant, un support à vocation promotionnelle etc.

[CLIQUEZ ICI POUR ACCÉDER AUX TARIFS ET À LA LICENCE](#)

2/ Les contenus de Gallica sont la propriété de la BnF au sens de l'article L.2112-1 du code général de la propriété des personnes publiques.

3/ Quelques contenus sont soumis à un régime de réutilisation particulier. Il s'agit :

- des reproductions de documents protégés par un droit d'auteur appartenant à un tiers. Ces documents ne peuvent être réutilisés, sauf dans le cadre de la copie privée, sans l'autorisation préalable du titulaire des droits.
- des reproductions de documents conservés dans les bibliothèques ou autres institutions partenaires. Ceux-ci sont signalés par la mention Source gallica.BnF.fr / Bibliothèque municipale de ... (ou autre partenaire). L'utilisateur est invité à s'informer auprès de ces bibliothèques de leurs conditions de réutilisation.

4/ Gallica constitue une base de données, dont la BnF est le producteur, protégée au sens des articles L341-1 et suivants du code de la propriété intellectuelle.

5/ Les présentes conditions d'utilisation des contenus de Gallica sont régies par la loi française. En cas de réutilisation prévue dans un autre pays, il appartient à chaque utilisateur de vérifier la conformité de son projet avec le droit de ce pays.

6/ L'utilisateur s'engage à respecter les présentes conditions d'utilisation ainsi que la législation en vigueur, notamment en matière de propriété intellectuelle. En cas de non respect de ces dispositions, il est notamment possible d'une amende prévue par la loi du 17 juillet 1978.

7/ Pour obtenir un document de Gallica en haute définition, contacter utilisation.commerciale@bnf.fr.

quatrième degré; de l'autre il sera utile à ceux qui voudront s'occuper de la résolution des degrés supérieurs, en leur fournissant différentes vues pour cet objet et en leur épargnant surtout un grand nombre de pas et de tentatives inutiles.

SECTION PREMIÈRE.

DE LA RÉSOLUTION DES ÉQUATIONS DU TROISIÈME DEGRÉ.

1. Comme la résolution des équations du second degré est très-facile, et n'est d'ailleurs remarquable que par son extrême simplicité, j'entrerai d'abord en matière par les équations du troisième degré, lesquelles demandent pour être résolues des artifices particuliers qui ne se présentent pas naturellement.

Soit donc l'équation générale du troisième degré

$$x^3 + mx^2 + nx + p = 0,$$

et comme on sait qu'on peut toujours faire disparaître le second terme de toute équation en augmentant ses racines du coefficient du second terme divisé par l'exposant du premier, on pourra supposer d'abord, pour plus de simplicité, $m = 0$, ce qui réduira la proposée à la forme

$$x^3 + nx + p = 0.$$

C'est dans cet état que les équations du troisième degré ont été d'abord traitées par Scipio Ferreo et par Tartalea, à qui l'on doit leur résolution; mais on ignore le chemin qui les y a conduits. La méthode la plus naturelle pour y parvenir me paraît celle que Hudde a imaginée, et qui consiste à représenter la racine par la somme de deux indéterminées qui permettent de partager l'équation en deux parties propres à faire en sorte que les deux indéterminées ne dépendent que d'une équation résoluble à la manière de celles du second degré.

Suivant cette méthode on fera donc $x = y + z$, ce qui étant substitué

dans la proposée la réduira à celle-ci

$$y^3 + 3y^2z + 3yz^2 + z^3 + n(y + z) + p = 0,$$

qu'on peut mettre sous cette forme plus simple

$$y^3 + z^3 + p + (y + z)(3yz + n) = 0.$$

Qu'on fasse maintenant ces deux équations séparées

$$y^3 + z^3 + p = 0,$$

$$3yz + n = 0,$$

on aura

$$z = -\frac{n}{3y},$$

et, substituant dans la première,

$$y^3 - \frac{n^3}{27y^3} + p = 0,$$

c'est-à-dire

$$y^6 + py^3 - \frac{n^3}{27} = 0.$$

Cette équation est à la vérité du sixième degré, mais comme elle ne renferme que deux différentes puissances de l'inconnue, dont l'une a un exposant double de celui de l'autre, il est clair qu'elle peut se résoudre comme celles du second degré. En effet, on aura d'abord

$$y^3 = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} + \frac{n^3}{27}},$$

et de là

$$y = \sqrt[3]{-\frac{p}{2} \pm \sqrt{\frac{p^2}{4} + \frac{n^3}{27}}}.$$

Ainsi l'on connaîtra y et z , et de là on aura

$$x = y + z = y - \frac{n}{3y}.$$

2. Il se présente différentes remarques à faire sur cette solution. D'abord il est clair que la quantité y doit avoir six valeurs, puisqu'elle dépend d'une équation du sixième degré; de sorte que la quantité x aura aussi six valeurs; mais comme x est la racine d'une équation du troisième degré, on sait qu'elle ne peut avoir que trois valeurs différentes;

donc il faudra que les six valeurs dont il s'agit se réduisent à trois, dont chacune soit double. C'est aussi de quoi on peut se convaincre par le calcul, en éliminant y des deux équations

$$y^6 + py^3 - \frac{n^3}{27} = 0, \quad x = y - \frac{n}{3y}.$$

Supposons, pour plus de généralité,

$$x = y - \frac{k}{y} \quad \text{ou bien} \quad y^2 - xy - k = 0,$$

on aura donc

$$y^2 = xy + k,$$

et de là

$$\begin{aligned} y^3 &= xy^2 + ky = y(x^2 + k) + kx, \\ y^6 &= y^2(x^2 + k)^2 + 2kx(x^2 + k)y + k^2x^2 \\ &= yx(x^2 + k)(x^2 + 3k) + kx^4 + 3k^2x^2 + k^3. \end{aligned}$$

Substituant donc ces valeurs de y^3 et y^6 , on aura

$$y(x^2 + k)(x^2 + 3kx + p) + kx(x^2 + 3kx + p) + k^3 - \frac{n^3}{27} = 0.$$

Soit, pour abréger,

$$\frac{n^3}{27} - k^3 = h \quad \text{et} \quad x^2 + 3kx + p = X,$$

on aura

$$[y(x^2 + k) + kx]X - h = 0,$$

d'où

$$y = \frac{\frac{h}{X} - kx}{x^2 + k},$$

de sorte qu'en substituant maintenant cette valeur de y dans l'équation

$$y^2 - xy - k = 0,$$

on aura

$$\left(\frac{h}{X} - kx\right)^2 - x\left(\frac{h}{X} - kx\right)(x^2 + k) - k(x^2 + k)^2 = 0,$$

ce qui se réduit à

$$h^3 X^2 + h X x (x^2 + 3k) - h^2 = 0,$$

ou bien, à cause de $x(x^2 + 3k) = X - p$, à

$$\frac{n^3}{27} X^2 - hp X - h^2 = 0,$$

c'est-à-dire à

$$\left(X - \frac{27hp}{2n^3}\right)^2 - \frac{27h^2}{n^3} \left(1 + \frac{27p^2}{4n^3}\right) = 0.$$

Maintenant il est clair qu'en faisant $k = \frac{n}{3}$ pour avoir $x = y - \frac{n}{3y}$ on aura $h = 0$, ce qui réduira l'équation précédente à

$$X^2 = 0,$$

savoir

$$(x^3 + nx + p)^2 = 0,$$

équation qui aura les mêmes racines que la proposée, mais dont chacune sera double.

De là il s'ensuit que la résolution d'une équation du troisième degré est, à proprement parler, la résolution d'une équation du sixième degré, inconvénient qui n'a pas lieu dans le second degré, dont la résolution est tout à fait propre à ce degré, mais qui devient encore plus considérable pour les équations des degrés supérieurs, comme on le verra plus bas.

3. Puis donc que parmi les six valeurs de y il n'y en a que trois qui donnent des valeurs différentes de x , il s'agit maintenant de distinguer ces valeurs. Pour cela il faut trouver l'expression particulière de chacune des six valeurs de y ; et si l'on nomme 1 , α et β les trois racines cubiques de l'unité, c'est-à-dire les trois racines de l'équation $x^3 - 1 = 0$, il est facile de voir que les six valeurs de y seront, en faisant, pour abréger,

$$\frac{p^2}{4} + \frac{n^3}{27} = q,$$

$$\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}}, \quad \alpha \sqrt[3]{-\frac{p}{2} \pm \sqrt{q}}, \quad \beta \sqrt[3]{-\frac{p}{2} \pm \sqrt{q}};$$

de là les valeurs correspondantes de $z = -\frac{n}{3\gamma}$ seront, à cause de

$$\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}} \sqrt[3]{-\frac{p}{2} \mp \sqrt{q}} = \sqrt[3]{\frac{p^2}{4} - q} = -\frac{n}{3},$$

et par conséquent

$$\sqrt[3]{-\frac{p}{2} \mp \sqrt{q}} = -\frac{n}{3\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}}},$$

ces valeurs seront, dis-je,

$$\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}}, \quad \frac{1}{\alpha} \sqrt[3]{-\frac{p}{2} \mp \sqrt{q}}, \quad \frac{1}{\beta} \sqrt[3]{-\frac{p}{2} \mp \sqrt{q}}.$$

Or, sans connaître même les valeurs de α et de β , il est facile de s'assurer que $\alpha\beta$ doit être égal à 1; car puisque 1, α et β sont les trois racines de l'équation $x^3 - 1 = 0$, on aura donc leur produit $1 \cdot \alpha \cdot \beta$ égal au dernier terme 1; donc $\alpha\beta = 1$; donc $\frac{1}{\alpha} = \beta$ et $\frac{1}{\beta} = \alpha$; de sorte que les trois valeurs ci-dessus deviendront

$$\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}}, \quad \beta \sqrt[3]{-\frac{p}{2} \mp \sqrt{q}}, \quad \alpha \sqrt[3]{-\frac{p}{2} \mp \sqrt{q}}.$$

Donc, puisque $x = y + z$, on aura, en ajoutant ensemble les valeurs correspondantes de y et de z ,

$$\begin{aligned} & \sqrt[3]{-\frac{p}{2} \pm \sqrt{q}} + \sqrt[3]{-\frac{p}{2} \mp \sqrt{q}}, \\ & \alpha \sqrt[3]{-\frac{p}{2} \pm \sqrt{q}} + \beta \sqrt[3]{-\frac{p}{2} \mp \sqrt{q}}, \\ & \beta \sqrt[3]{-\frac{p}{2} \pm \sqrt{q}} + \alpha \sqrt[3]{-\frac{p}{2} \mp \sqrt{q}}, \end{aligned}$$

où il est facile de voir que, des signes ambigus de \sqrt{q} soit qu'on prenne le supérieur ou l'inférieur, on aura toujours les trois mêmes valeurs de x .

De là il s'ensuit donc que l'on peut prendre indifféremment le radi-

cal $\sqrt[3]{q}$ en plus ou en moins, et que les trois racines de l'équation proposée résulteront immédiatement des trois valeurs du radical cubique

$$\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}}.$$

4. Nous avons fait voir (2) que la résolution de toute équation du troisième degré appartient essentiellement à une équation du sixième degré; cependant si l'on voulait délivrer l'équation

$$x = \sqrt[3]{-\frac{p}{2} + \sqrt{q}} + \sqrt[3]{-\frac{p}{2} - \sqrt{q}}$$

des radicaux, on tomberait dans une équation du neuvième degré; car en prenant d'abord les cubes on aurait

$$x^3 = -p + 3x \sqrt[3]{\frac{p^2}{4} - q},$$

et prenant de nouveau les cubes, après avoir fait passer dans le premier membre le terme $-p$, on aurait

$$(x^3 + p)^3 = 27 \left(\frac{p^2}{4} - q \right) x^3,$$

c'est-à-dire, à cause de $\frac{p^2}{4} - q = -\frac{n^3}{27}$,

$$x^9 + 3px^6 + (3p^2 + n^3)x^3 + p^3 = 0.$$

Mais il faut remarquer que cette équation renferme, outre les trois racines de la proposée $x^3 + nx + p = 0$, encore six autres étrangères; en effet elle peut se décomposer en ces trois-ci

$$x^3 + nx + p = 0,$$

$$x^3 + \alpha nx + p = 0,$$

$$x^3 + \beta nx + p = 0,$$

dont les deux dernières sont, comme on voit, différentes de la proposée; ainsi l'on ne peut rien conclure de cette équation pour le degré auquel

doit se rapporter la résolution des équations du troisième degré, comme nous l'avons fait plus haut (2), d'après l'équation $X^2 = 0$, laquelle renferme toutes les mêmes racines que la proposée.

5. L'équation du sixième degré

$$y^6 + py^3 - \frac{n^3}{27} = 0$$

s'appelle la *réduite* du troisième degré, parce que c'est à sa résolution que se réduit celle de la proposée

$$x^3 + nx + p = 0.$$

Or nous avons déjà vu plus haut comment les racines de cette dernière équation dépendent des racines de celle-là; voyons réciproquement comment les racines de la *réduite* dépendent de celles de la proposée; mais pour rendre cette recherche plus générale et plus lumineuse il sera bon de considérer une équation qui ait tous ses termes telle que

$$x^3 + mx^2 + nx + p = 0,$$

et dont les racines soient représentées généralement par a, b, c . On commencera donc par faire évanouir le second terme en supposant $x = x' - \frac{m}{3}$, et, faisant, pour abréger,

$$n' = n - \frac{m^2}{3}, \quad p' = p - \frac{mn}{3} + \frac{2m^3}{27},$$

on aura la transformée

$$x'^3 + n'x' + p' = 0,$$

qui a la forme requise. Faisant maintenant $x' = y - \frac{n'}{3y}$, on aura la réduite

$$y^6 + p'y^3 - \frac{n'^3}{27} = 0;$$

d'où, en nommant r la racine cubique de

$$-\frac{p'}{2} + \sqrt{\frac{p'^2}{4} + \frac{n'^3}{27}},$$

on aura ces trois valeurs de γ , savoir

$$\gamma = r, \quad \gamma = \alpha r, \quad \gamma = \beta r,$$

lesquelles donneront les trois racines

$$x' = r - \frac{n'}{3r}, \quad x' = \alpha r - \frac{n'}{3\alpha r}, \quad x' = \beta r - \frac{n'}{3\beta r};$$

d'où, à cause de $x = x' - \frac{m}{3}$, on aura, en faisant, pour abréger, $\frac{n'}{3r} = s$, ces trois valeurs de x , savoir

$$-\frac{m}{3} + r - s, \quad -\frac{m}{3} + \alpha r - \frac{s}{\alpha}, \quad -\frac{m}{3} + \beta r - \frac{s}{\beta};$$

donc

$$a = -\frac{m}{3} + r - s,$$

$$b = -\frac{m}{3} + \alpha r - \frac{s}{\alpha},$$

$$c = -\frac{m}{3} + \beta r - \frac{s}{\beta}.$$

Retranchant successivement la seconde et la troisième de ces équations de la première, on aura

$$a - b = (1 - \alpha) \left(r + \frac{s}{\alpha} \right),$$

$$a - c = (1 - \beta) \left(r + \frac{s}{\beta} \right),$$

d'où l'on tire

$$\frac{\alpha(a - b)}{1 - \alpha} = \alpha r + s,$$

$$\frac{\beta(a - c)}{1 - \beta} = \beta r + s;$$

et retranchant de nouveau l'une de l'autre, ensuite divisant par $\alpha - \beta$, il viendra

$$r = \frac{\frac{\alpha(a - b)}{1 - \alpha} - \frac{\beta(a - c)}{1 - \beta}}{\alpha - \beta},$$

c'est-à-dire

$$r = \frac{a}{(1-\alpha)(1-\beta)} + \frac{\alpha b}{(\alpha-1)(\alpha-\beta)} + \frac{\beta c}{(\beta-1)(\beta-\alpha)}.$$

Or, 1 , α et β étant (hypothèse) les trois racines de l'équation $x^3 - 1 = 0$, on aura

$$x^3 - 1 = (x - 1)(x - \alpha)(x - \beta),$$

et différentiant

$$3x^2 = (x - \alpha)(x - \beta) + (x - 1)(x - \beta) + (x - 1)(x - \alpha);$$

de sorte qu'en faisant successivement $x = 1$, α , β , on aura

$$3 = (1 - \alpha)(1 - \beta),$$

$$3\alpha^2 = (\alpha - 1)(\alpha - \beta),$$

$$3\beta^2 = (\beta - 1)(\beta - \alpha);$$

donc, substituant ces valeurs dans l'expression précédente de r , on aura

$$r = \frac{a}{3} + \frac{b}{3\alpha} + \frac{c}{3\beta},$$

ou bien, à cause de $\alpha\beta = 1$,

$$r = \frac{a + \beta b + \alpha c}{3}.$$

Telle est donc la valeur de r , et par conséquent aussi de y ; de sorte qu'on aura en changeant, ce qui est permis, α en β et *vice versa*

$$y = \frac{a + \alpha b + \beta c}{3}.$$

6. On voit d'abord par cette expression de y pourquoi la *réduite* est nécessairement du sixième degré; car comme cette réduite ne dépend pas immédiatement des racines a , b , c de la proposée, mais seulement des coefficients m , n , p , où les trois racines entrent également, il est clair que dans l'expression de y on doit pouvoir échanger à volonté les quantités a , b , c entre elles; par conséquent la quantité y devra avoir autant de valeurs différentes que l'on en pourra former par toutes les

permutations possibles dont les trois racines α, b, c sont susceptibles; or on sait par la théorie des combinaisons que le nombre des permutations, c'est-à-dire des arrangements différents de trois choses, est $3 \cdot 2 \cdot 1$; donc la réduite en y doit être aussi du degré $3 \cdot 2 \cdot 1$, c'est-à-dire du sixième.

Il y a plus: la même expression de y montre aussi pourquoi la réduite est résoluble à la manière des équations du second degré; car il est clair que cela vient de ce que cette équation ne renferme que les puissances y^3 et y^6 , c'est-à-dire des puissances dont les exposants sont multiples de 3; en sorte que, si r est une des valeurs de y , il faut que αr et βr en soient aussi à cause de $\alpha^3 = 1$ et $\beta^3 = 1$; or c'est ce qui a lieu dans l'expression de y trouvée ci-dessus. Pour le faire voir plus aisément nous remarquerons que $\beta = \alpha^2$, car, puisqu'on a $\alpha\beta = 1$ et $\alpha^3 - 1 = 0$, on aura aussi $\alpha\beta = \alpha^3$, et de là $\beta = \alpha^2$; de sorte que l'expression de y pourra se mettre sous cette forme

$$y = \frac{a + \alpha b + \alpha^2 c}{3},$$

d'où, en faisant toutes les permutations possibles des quantités a, b, c , on tire les six valeurs suivantes

$$\frac{a + \alpha b + \alpha^2 c}{3},$$

$$\frac{a + \alpha c + \alpha^2 b}{3},$$

$$\frac{b + \alpha a + \alpha^2 c}{3},$$

$$\frac{b + \alpha c + \alpha^2 a}{3},$$

$$\frac{c + \alpha b + \alpha^2 a}{3},$$

$$\frac{c + \alpha a + \alpha^2 b}{3},$$

qui seront donc les six racines de la réduite. Maintenant si l'on multiplie la première par α , et ensuite par β ou par α^2 , on aura, à cause de $\alpha^3 = 1$,

ces deux-ci

$$\frac{c + \alpha a + \alpha^2 b}{3} \quad \text{et} \quad \frac{b + \alpha c + \alpha^2 a}{3},$$

qui sont la sixième et la quatrième; et si l'on multiplie de même la seconde par α et par α^2 , on aura

$$\frac{b + \alpha a + \alpha^2 c}{3} \quad \text{et} \quad \frac{c + \alpha b + \alpha^2 a}{3},$$

qui sont la troisième et la cinquième. Il en sera de même si l'on multiplie la troisième et la quatrième, ou la cinquième et la sixième par α et par α^2 , car on aura par là également toutes les autres.

7. Cela nous conduit à une méthode directe pour trouver la réduite d'où dépend la résolution des équations du troisième degré; car soit

$$x^3 + mx^2 + nx + p = 0$$

l'équation proposée dont les racines soient a, b, c , et supposons que les racines de la réduite soient représentées généralement par une fonction du premier degré des racines a, b, c , telle que

$$Aa + Bb + Cc,$$

A, B, C étant des coefficients indépendants des quantités a, b, c ; en faisant toutes les permutations possibles des quantités a, b, c , on aura ces quantités

$$Aa + Bb + Cc,$$

$$Aa + Bc + Cb,$$

$$Ab + Ba + Cc,$$

$$Ab + Bc + Ca,$$

$$Ac + Bb + Ca,$$

$$Ac + Ba + Cb,$$

qui seront les six racines de la réduite. Or, pour que cette équation n'ait que des puissances dont les exposants soient multiples de 3, il faut, comme nous l'avons vu plus haut, que, nommant r une de ses racines,

αr et βr ou $\alpha^2 r$ en soient aussi; donc, prenant la quantité

$$Aa + Bb + Cc$$

pour r , il faudra que la quantité

$$\alpha Aa + \alpha Bb + \alpha Cc$$

soit égale à une des cinq autres quantités ci-dessus; or elle ne saurait devenir égale à

$$Aa + Bc + Cb$$

ni à

$$Ab + Ba + Cc$$

qu'en faisant $\alpha = 1$, car dans le premier cas on aurait

$$\alpha A = A,$$

et dans le second

$$\alpha C = C;$$

mais en la comparant à la quantité

$$Ab + Bc + Ca,$$

on aura

$$\alpha A = C, \quad \alpha B = A \quad \text{et} \quad \alpha C = B,$$

d'où l'on tire

$$C = \alpha A, \quad B = \alpha^2 A \quad \text{et} \quad \alpha^3 A = A,$$

c'est-à-dire

$$\alpha^3 = 1;$$

ce qui montre que α doit être en effet une des racines de l'équation

$$x^3 - 1 = 0;$$

ainsi en faisant, pour plus de simplicité, $A = 1$, on aura

$$A = 1, \quad B = \alpha \quad \text{et} \quad C = \alpha^2,$$

ce qui donne les mêmes formules qu'on a trouvées plus haut en faisant abstraction du dénominateur 3.

Faisant donc, pour abréger,

$$\begin{aligned}r &= a + \alpha b + \alpha^2 c, \\s &= a + \alpha c + \alpha^2 b,\end{aligned}$$

on aura r , αr , $\alpha^2 r$ et s , αs , $\alpha^2 s$ pour les six racines de la transformée; or, nommant y l'inconnue de cette équation, on trouvera d'abord que le produit des trois facteurs $y - r$, $y - \alpha r$, $y - \alpha^2 r$ sera $y^3 - r^3$, et que de même le produit des trois autres sera $y^3 - s^3$, de sorte que le produit total, c'est-à-dire la réduite elle-même, sera représentée par

$$y^6 - (r^3 + s^3) y^3 + r^3 s^3 = 0,$$

qui a la forme demandée. Il ne s'agit donc plus maintenant que de trouver les valeurs de $r^3 + s^3$ et de $r^3 s^3$: or, en élevant au cube la quantité r et faisant attention que $\alpha^3 = 1$, on trouve

$$r^3 = a^3 + b^3 + c^3 + 6abc + 3\alpha(a^2b + b^2c + c^2a) + 3\alpha^2(ab^2 + bc^2 + ca^2),$$

et par conséquent, en changeant b en c , on aura de même

$$s^3 = a^3 + b^3 + c^3 + 6abc + 3\alpha(a^2c + c^2b + b^2a) + 3\alpha^2(c^2a + b^2c + a^2b).$$

Soit, pour plus de simplicité,

$$\begin{aligned}a^3 + b^3 + c^3 + 6abc &= L, \\a^2b + b^2c + c^2a &= M, \\a^2c + b^2a + c^2b &= N,\end{aligned}$$

on aura donc

$$r^3 = L + 3\alpha M + 3\alpha^2 N,$$

$$s^3 = L + 3\alpha N + 3\alpha^2 M,$$

donc

$$r^3 + s^3 = 2L + 3(\alpha + \alpha^2)(M + N);$$

mais comme 1 , α et α^2 sont les trois racines de l'équation $x^3 - 1 = 0$ qui manque du second terme, on doit avoir

$$1 + \alpha + \alpha^2 = 0;$$

donc

$$r^3 + s^3 = 2L - 3(M + N).$$

Multipiant ensuite les valeurs de r^3 et s^3 ensemble, on aura

$$r^3 s^3 = L^2 + 9(M^2 + N^2) + 3(\alpha + \alpha^2)[L(M + N) + 3MN],$$

ou bien, à cause de $\alpha + \alpha^2 = -1$,

$$r^3 s^3 = L[L - 3(M + N)] + 9[(M + N)^2 - 3MN];$$

or il est facile de voir que les quantités L , $M + N$ et MN doivent être données par les coefficients m , n , p de la proposée, et cela sans extraction de racines, ce qui suit de ce que ces quantités ne changent point, quelques permutations des quantités a , b , c qu'on y fasse, de sorte qu'elles ne peuvent avoir chacune qu'une valeur unique.

8. En effet, ayant

$$-m = a + b + c, \quad n = ab + ac + bc, \quad -p = abc,$$

on aura d'abord par les règles connues

$$a^2 + b^2 + c^2 = m^2 - 2n, \quad a^3 + b^3 + c^3 = -m^3 + 3mn - 3p,$$

et l'on trouvera de là

$$a^3 b^3 + a^3 c^3 + b^3 c^3 = n^3 - 3mnp + 3p^2;$$

donc

$$L = -m^3 + 3mn - 9p,$$

$$M + N = 3p - mn,$$

$$MN = n^3 + p(m^3 - 6mn) + 9p^2;$$

d'où l'on trouvera

$$r^3 + s^3 = -2m^3 + 9mn - 27p,$$

$$r^3 s^3 = m^6 - 9m^4 n + 27m^2 n^2 - 27n^3 = (m^2 - 3n)^3,$$

de sorte que notre réduite sera

$$y^6 + (2m^3 - 9mn + 27p)y^3 + (m^2 - 3n)^3 = 0,$$

qui revient au même que celle qu'on a trouvée plus haut (5), en faisant seulement attention que l'inconnue y de celle-ci est triple de l'inconnue y

de celle-là. Résolvant donc cette équation à la manière de celles du second degré, ou bien faisant, pour abréger, $y^3 = z$, en sorte que l'on ait

$$z^2 + (2m^3 - 9mn + 27p)z + (m^2 - 3n)^3 = 0,$$

et nommant z' et z'' les racines de cette équation du second degré, on aura

$$y^3 = z', \quad y^3 = z'',$$

donc

$$y = \sqrt[3]{z'} \quad \text{ou} \quad y = \sqrt[3]{z''};$$

par conséquent, puisqu'on a supposé que r et s étaient deux valeurs de y , on aura

$$r = a + \alpha b + \alpha^2 c = \sqrt[3]{z'},$$

$$s = a + \alpha c + \alpha^2 b = \sqrt[3]{z''},$$

équations qui étant combinées avec l'équation

$$a + b + c = -m$$

serviront à trouver les trois racines a, b, c ; en effet on aura, à cause de $\alpha^3 = 1$ et de $1 + \alpha + \alpha^2 = 0$,

$$a = \frac{-m + \sqrt[3]{z'} + \sqrt[3]{z''}}{3},$$

$$b = \frac{-m + \alpha^2 \sqrt[3]{z'} + \alpha \sqrt[3]{z''}}{3},$$

$$c = \frac{-m + \alpha \sqrt[3]{z'} + \alpha^2 \sqrt[3]{z''}}{3},$$

ce qui s'accorde avec ce qu'on a trouvé plus haut.

9. Il est à propos de remarquer encore, pour éclaircir davantage cette matière, que les quantités M et N du n° 7 sont telles que l'une devient toujours l'autre en y faisant une permutation quelconque entre les trois racines a, b, c , de sorte que ces quantités M et N ne peuvent être que les racines d'une équation du second degré. En effet, nommant t l'inconnue de cette équation, il est clair qu'elle aura nécessairement cette forme

$$t^2 - (M + N)t + MN = 0;$$

donc, substituant pour $M + N$ et MN leurs valeurs trouvées ci-dessus (8), on aura

$$t^2 - (3p - mn)t + n^3 + (m^3 - 6mn)p + 9p^2 = 0.$$

Ainsi l'on aura, par la résolution de cette équation, les valeurs de M et N ; et comme d'ailleurs la quantité L est déjà donnée, puisqu'on a

$$L = -m^3 + 3mn - 9p,$$

on aura les valeurs de r^3 et de s^3 (7), ou bien celles de z' et z'' (8), les-
quelles seront donc

$$z' = L + 3\alpha M + 3\alpha^2 N,$$

$$z'' = L + 3\alpha N + 3\alpha^2 M,$$

et moyennant ces valeurs on aura celles des racines a , b , c , comme on l'a vu tantôt.

Au reste cette propriété des fonctions M et N fait voir clairement pourquoi la quantité

$$z = y^3 = (a + \alpha b + \alpha^2 c)^3$$

ne dépend que d'une équation du second degré, de sorte que l'équation en y ne peut renfermer que les puissances y^3 et y^6 .

10. La résolution des équations du troisième degré que nous venons d'examiner est appelée communément la *Règle de Cardan*, et elle est la seule que les Analystes connaissent. Mais il y a encore une autre méthode qui est due à M. Tschirnaus, et qui, quoique moins simple que celle de Cardan, a cependant l'avantage d'être plus directe et plus générale. Cette méthode est exposée dans les *Acta Eruditorum* de l'année 1683, et elle consiste à faire disparaître autant de termes intermédiaires que l'on veut d'une équation quelconque; l'Auteur la propose comme générale pour cet objet, et nous verrons qu'elle l'est en effet, mais qu'elle demande souvent la résolution d'équations d'un degré supérieur à celui de la proposée, ce qui empêche qu'elle ne réussisse au delà du quatrième degré.

M. Tschirnaus remarque que comme on peut faire évanouir un terme

quelconque d'une équation dont x est l'inconnue, par la supposition de

$$x = y + a,$$

y étant une nouvelle inconnue et a une quantité indéterminée, de même on pourra en faire évanouir deux quelconques en supposant

$$x^2 = bx + a + y,$$

ou trois en supposant

$$x^3 = cx^2 + bx + a + y,$$

et ainsi de suite, a, b, c, \dots étant tous des coefficients indéterminés dont le nombre doit être égal à celui des termes qu'on veut faire évanouir, afin que l'on ait autant d'inconnues que de conditions à remplir.

Ainsi il n'y aura qu'à éliminer l'inconnue x de l'équation proposée par le moyen de la nouvelle équation qu'on a supposée, et l'on aura une équation en y qui sera toujours du même degré que la proposée, et dans laquelle on pourra supposer autant de termes égaux à zéro qu'il y a d'indéterminées a, b, c, \dots

Prenons donc l'équation du troisième degré

$$x^3 + mx^2 + nx + p = 0,$$

et supposons

$$x^2 = bx + a + y,$$

pour qu'on soit en état d'éliminer dans la transformée les deux termes intermédiaires; on aura donc

$$x^3 = bx^2 + ax + yx,$$

et, en substituant la valeur de x^2 ,

$$x^3 = (b^2 + a + y)x + b(a + y);$$

donc, substituant ces valeurs dans la proposée, on aura

$$(A) \quad (b^2 + mb + n + a + y)x + (b + m)(a + y) + p = 0,$$

d'où l'on tire

$$x = -\frac{(b + m)(a + y) + p}{b^2 + mb + n + a + y},$$

valeur qui étant substituée dans l'équation

$$x^2 = bx + a + y$$

donnera celle-ci, où je fais, pour plus de simplicité, $b + m = c$, $b^2 + mb + n = d$,

$$[c(a + y) + p]^2 + b[c(a + y) + p](d + a + y) - (a + y)(d + a + y)^2 = 0,$$

c'est-à-dire, en ordonnant les termes par rapport aux puissances de $a + y$, et remettant les valeurs de c et d ,

$$(B) \left\{ \begin{array}{l} (y + a)^3 - (mb + m^2 - 2n)(y + a)^2 \\ \quad + [nb^2 + (mn - 3p)b + n^2 - 2mp](y + a) - p(b^3 + mb^2 + nb + p) = 0, \end{array} \right.$$

de sorte qu'en développant les puissances de $y + a$, on aura l'équation

$$y^3 + A y^2 + B y + C = 0,$$

dans laquelle

$$A = 3a - mb - m^2 + 2n,$$

$$B = 3a^2 - 2a(mb + m^2 - 2n) + nb^2 + (mn - 3p)b + n^2 - 2mp,$$

$$C = a^3 - (mb + m^2 - 2n)a^2 + [nb^2 + (mn - 3p)b + n^2 - 2mp]a - p(b^3 + mb^2 + nb + p).$$

Maintenant on peut faire évanouir le second et le troisième terme en supposant $A = 0$ et $B = 0$, ce qui donnera ces deux équations

$$3a - mb - m^2 + 2n = 0,$$

$$3a^2 - 2a(mb + m^2 - 2n) + nb^2 + (mn - 3p)b + n^2 - 2mp = 0,$$

par lesquelles on pourra déterminer a et b ; et l'équation en y sera réduite à la forme

$$y^3 + C = 0,$$

laquelle donne sur-le-champ ces trois racines

$$y = -\sqrt[3]{C}, \quad y = -\alpha\sqrt[3]{C}, \quad y = -\alpha^2\sqrt[3]{C},$$

1 , α et α^2 étant les racines de l'équation $x^3 - 1 = 0$. Ainsi mettant

d'abord dans l'expression de x trouvée ci-dessus les valeurs de a et b qui résultent des équations précédentes, et ensuite pour y les trois racines de l'équation $y^3 + C = 0$, on aura tout d'un coup les trois racines x de l'équation proposée.

Or, comme des deux équations qui doivent donner a et b la première est du premier degré et la seconde du second, il est visible que la détermination de ces quantités ne dépendra que d'une équation du degré 1.2, c'est-à-dire du second degré; en effet, on aura d'abord

$$a = \frac{mb + m^2 - 2n}{3},$$

et, substituant cette valeur dans la seconde équation, on aura

$$(m^2 - 3n)b^2 + (2m^3 - 7mn + 9p)b + m^4 - 4m^2n + 6mp + n^2 = 0,$$

d'où l'on tirera deux valeurs de b qui pourront être employées indifféremment, parce qu'elles donneront toujours les mêmes valeurs de x .

Cette méthode a donc l'avantage de conduire immédiatement à une réduite du second degré, au lieu que par la méthode ordinaire on tombe dans une réduite du sixième; mais la résolution qu'elle donne n'est pas pour cela exempte de l'inconvénient que nous avons remarqué dans la résolution de Cardan, et qui consiste en ce que cette résolution est plutôt celle d'une équation du sixième degré que d'une équation du troisième (2). En effet, puisque la quantité y a trois valeurs, et que les quantités b et a en ont chacune deux, il est visible qu'il doit résulter six valeurs de x , lesquelles ne peuvent être par conséquent que les racines d'une équation du sixième degré; il est vrai que ces six valeurs se réduiront à trois, dont chacune sera double, comme il est facile de le démontrer, et comme nous l'avons déjà fait voir à l'égard de la formule de Cardan.

11. Il y a une remarque importante à faire touchant cette méthode de M. Tschirnhaus, c'est que, dès qu'on a trouvé les valeurs de a , de b et de y , on ne doit pas prendre indifféremment pour x une des racines de l'équation supposée

$$x^2 - bx - a - y = 0,$$

ainsi que l'Auteur le fait; car, pour que cela fût permis, il faudrait que cette équation renfermât deux des racines de la proposée, et par conséquent que b fût la somme de ces deux racines; or, comme il n'y a pas plus de raison pour que b soit la somme de deux quelconques des trois racines de la proposée que de deux autres quelconques, il s'ensuit que b devrait avoir autant de valeurs différentes qu'il y a de manières de prendre les trois racines deux à deux, c'est-à-dire trois valeurs, à cause que le nombre des combinaisons de trois choses prises deux à deux est $\frac{3 \cdot 2}{2} = 3$; au lieu que nous avons vu que la quantité b n'a que deux valeurs, puisqu'elle ne dépend que d'une équation du second degré.

L'esprit de la méthode que nous examinons consiste à faire en sorte que l'équation supposée ait une racine commune avec la proposée; ainsi, quand on a déterminé les valeurs de a , b et y en sorte que cette condition ait lieu, il faut prendre pour la valeur de x celle des racines de l'équation

$$x^2 - bx - a - y = 0,$$

qui sera commune à l'équation proposée

$$x^3 + mx^2 + nx + p = 0;$$

pour cela il n'y aura qu'à chercher le plus grand diviseur commun de ces deux équations, et ce diviseur, où x sera nécessairement linéaire, donnera une valeur de x qui sera aussi une des racines de la proposée; or il est facile de comprendre que cette valeur de x ne peut être que celle que nous avons trouvée en éliminant successivement les puissances plus hautes de x des deux équations données.

En effet, la méthode ordinaire d'élimination, suivant laquelle on fait disparaître successivement les plus hautes puissances de l'inconnue en déduisant, des deux équations données où la même inconnue se trouve élevée à des puissances quelconques, une suite d'autres équations où le plus haut degré de l'inconnue est successivement moindre, jusqu'à ce qu'on arrive à une équation où l'inconnue ne se trouve plus, et qui est le résultat de l'élimination; cette méthode, dis-je, revient dans le fond à la

même que celle qui sert à trouver le plus grand commun diviseur des deux quantités qui forment les premiers membres des deux équations données; les restes que l'on aura par les divisions successives qu'il faudra faire donneront, étant égalés à zéro, les mêmes équations que celles qui proviennent de l'élimination; le dernier reste où l'inconnue ne se trouve plus devra être égal à zéro pour que les deux quantités proposées aient un diviseur commun du premier degré, lequel sera par conséquent l'avant-dernier reste où l'inconnue ne sera que linéaire; de sorte qu'en égalant aussi à zéro cet avant-dernier reste on aura une valeur de l'inconnue qui sera la racine commune des deux équations.

Dans l'Exemple du n° 10 les équations (A) et (B) sont celles que l'on aurait en faisant égal à zéro l'avant-dernier et le dernier reste; par conséquent la valeur de x tirée de l'équation (A) est la seule qui puisse donner en même temps une racine de l'équation proposée.

12. A l'occasion de cette remarque, nous croyons devoir encore en faire une autre touchant la manière de faire en sorte que deux équations aient plus d'une racine commune; il est évident que si l'on veut qu'elles aient deux racines communes il faudra qu'elles soient divisibles exactement par un facteur du second degré; par conséquent, en cherchant le plus grand commun diviseur des deux quantités qui forment les premiers membres des équations proposées, dès qu'on sera parvenu à un reste où l'inconnue se trouvera au second degré, il faudra, pour que ce reste soit un diviseur commun des deux équations, que le reste suivant soit nul de lui-même; or ce dernier reste ne renfermera que deux termes, l'un où l'inconnue ne se trouvera pas, et l'autre où elle se trouvera à la première dimension; c'est pourquoi il faudra faire chacun de ces termes en particulier égal à zéro, ce qui donnera deux équations contenant les conditions nécessaires pour qu'il y ait dans les proposées deux racines communes. Ce serait la même chose si l'on voulait employer la voie de l'élimination; alors il faudrait s'arrêter à l'équation où l'inconnue serait au premier degré, et vérifier cette équation indépendamment de l'inconnue, en égalant à zéro l'un et l'autre des deux termes dont elle serait compo-

sée; moyennant quoi l'équation précédente du second degré renfermerait les deux racines communes aux deux équations proposées.

On voit par là comment il faudrait s'y prendre pour trouver les conditions qui donnent trois racines communes, ou davantage, à deux équations données; mais dès qu'on aura trouvé la condition nécessaire pour que ces deux équations aient une racine commune, on pourra aisément en déduire celles qui rendront deux ou plusieurs racines communes.

Pour cela, supposons que les deux équations données qui renferment une même inconnue x soient représentées, en général, par

$$P = 0 \quad \text{et} \quad Q = 0;$$

si, au lieu de prendre $P = 0$, je prends $P = y$, et que j'élimine ensuite x des deux équations, j'en aurai une en y que je représenterai par

$$y^m + ay^{m-1} + \dots + py^2 + qy + r = 0;$$

or, pour que les deux équations $P = 0$ et $Q = 0$ aient une racine commune en sorte qu'elles puissent subsister à la fois, il faut que y ait une valeur égale à zéro; donc

$$r = 0$$

sera la condition nécessaire pour l'existence d'une racine commune à ces deux équations; mais si l'on veut qu'elles aient deux racines communes, alors il faudra que y ait deux valeurs égales à zéro; par conséquent on aura les deux conditions

$$r = 0 \quad \text{et} \quad q = 0;$$

de même, s'il devait y avoir trois racines communes, il faudrait que y eût trois valeurs égales à zéro, ce qui donnerait les trois conditions

$$r = 0, \quad q = 0 \quad \text{et} \quad p = 0,$$

et ainsi de suite.

Je remarque maintenant que pour changer l'équation $P = 0$ en $P = y$, ou $P - y = 0$, il n'y a qu'à diminuer le dernier terme de l'équation $P = 0$ de la quantité y ; de sorte que si l'on suppose

$$P = x^n + \alpha x^{n-1} + \dots + \rho,$$

il n'y aura qu'à écrire $\rho - y$ à la place de ρ ; or l'équation

$$y^m + ay^{m-1} + \dots + py^2 + qy + r = 0$$

est celle qui résulte de l'élimination de x dans les deux équations $P = y$ et $Q = 0$ (hypothèse); par conséquent, en y faisant $y = 0$, l'équation $r = 0$ sera celle qui résultera de l'élimination de x dans les équations $P = 0$ et $Q = 0$; donc, ayant l'équation $r = 0$, il n'y aura qu'à y substituer $\rho - y$ à la place de ρ pour avoir immédiatement l'équation

$$y^m + ay^{m-1} + \dots + py^2 + qy + r = 0;$$

mais on sait que si r est une fonction de ρ et qu'on veuille y substituer $\rho - y$ à la place de ρ , on aura, en employant les différentiations, la transformée

$$r - \frac{dr}{d\rho} y + \frac{1}{2} \frac{d^2 r}{d\rho^2} y^2 - \frac{1}{2 \cdot 3} \frac{d^3 r}{d\rho^3} y^3 + \dots;$$

donc on aura, par la comparaison des termes,

$$q = -\frac{dr}{d\rho}, \quad p = \frac{1}{2} \frac{d^2 r}{d\rho^2}, \dots,$$

d'où je tire cette conclusion, que si

$$r = 0$$

est la condition nécessaire pour que les équations $P = 0$ et $Q = 0$ aient une racine commune, on aura, pour les conditions de deux racines communes,

$$r = 0 \quad \text{et} \quad \frac{dr}{d\rho} = 0;$$

pour trois racines communes,

$$r = 0, \quad \frac{dr}{d\rho} = 0 \quad \text{et} \quad \frac{d^2 r}{d\rho^2} = 0,$$

et ainsi de suite, ρ étant le dernier terme de l'une des équations proposées.

13. Il est clair au reste que les racines de l'équation en y ne sont autre chose que les valeurs de P qui résultent en substituant à la place de x chacune des racines de l'autre équation $Q = 0$, que nous désignerons par x', x'', x''', \dots ; donc, si l'on suppose que P', P'', P''', \dots soient les valeurs de P qui viendraient de ces substitutions, c'est-à-dire où l'on aurait mis x', x'', x''', \dots à la place de x , on aura

$$\pm r = P' P'' P''' \dots;$$

d'où l'on voit que l'équation $r = 0$, résultante de l'élimination de l'inconnue x des deux équations $P = 0$ et $Q = 0$, n'est autre chose que le produit de toutes les équations particulières

$$P' = 0, \quad P'' = 0, \quad P''' = 0, \dots;$$

or ce produit $P' P'' P''' \dots$ peut toujours se trouver sans connaître les racines de l'équation $Q = 0$, comme il est facile de s'en convaincre en considérant que le produit en question demeurera toujours le même, quelque permutation qu'on y fasse entre les racines x', x'', x''', \dots , c'est-à-dire entre les quantités P', P'', P''', \dots qui sont des fonctions semblables de ces racines; de sorte qu'il doit être donné par une équation linéaire et sans extraction de racines. En effet, les multiplications des quantités P', P'', P''', \dots étant faites, on trouvera toujours que les différentes fonctions de x', x'', x''', \dots qui entreront dans le produit total seront exprimables par les seuls coefficients de l'équation $Q = 0$, dont x', x'', x''', \dots sont les racines. On peut consulter là-dessus l'*Introduction à l'Analyse des lignes courbes* de M. Cramer, où l'on trouvera des règles pour calculer toutes les fonctions dont il s'agit, et avoir par conséquent la valeur du produit $P' P'' P''' \dots$; nous avons aussi traité ce sujet dans un Mémoire particulier, où nous avons donné des formules générales pour trouver immédiatement la valeur du même produit, sans passer par les différentes opérations que la méthode de M. Cramer exige (*); ainsi nous ne nous arrêterons pas davantage là-dessus. Nous nous contenterons seulement de re-

(*) *Oeuvres de Lagrange*, t. III, p. 141.

marquer que, de ce que l'équation résultante de l'élimination de x par le moyen des équations $P = 0$ et $Q = 0$ peut être représentée par

$$P' P'' P''' \dots = 0,$$

il s'ensuit que cette équation doit être telle, que les coefficients de l'équation $P = 0$ y forment partout des produits d'autant de dimensions qu'il y a de quantités P', P'', P''', \dots ou de racines x', x'', x''', \dots dans l'équation $Q = 0$, c'est-à-dire autant qu'il y a d'unités dans le degré de cette dernière équation; il en sera de même des coefficients de l'équation $Q = 0$, qui devront former partout dans la même équation résultante de l'élimination des produits d'autant de dimensions qu'il y a d'unités dans l'exposant du degré de l'autre équation $P = 0$.

14. D'où l'on peut conclure, en général, que, suivant la méthode de M: Tschirnaus, on aura toujours une transformée en y du même degré que l'équation proposée, et que dans cette transformée les quantités y, a, b, c, \dots (y compris l'unité, coefficient de la plus haute puissance de x dans l'équation proposée) formeront partout des produits du même nombre de dimensions, c'est-à-dire d'autant de dimensions qu'il y a d'unités dans le degré de la proposée.

Ainsi, supposant que l'équation proposée dont x est l'inconnue soit du degré m , et qu'on prenne une équation *subsidiare* telle que

$$y^r + a + bx + cx^2 + \dots = x^r,$$

on aura une transformée en y du degré m qui, étant représentée par

$$y^m + A y^{m-1} + B y^{m-2} + C y^{m-3} + \dots = 0,$$

sera telle que le coefficient A sera une fonction linéaire de a, b, c, \dots , que le coefficient B sera une fonction de deux dimensions des mêmes quantités, que le coefficient C en sera une de trois dimensions, et ainsi de suite.

Et en général le coefficient du terme $n^{\text{ème}}$ sera toujours une fonction rationnelle et entière de a, b, c, \dots de $n - 1$ dimensions. Ainsi, prenant

autant d'indéterminées a, b, c, \dots qu'il y a de termes à faire disparaître, il est clair que pour faire disparaître le second terme on n'aura qu'à résoudre une équation du premier degré à une seule inconnue; pour faire disparaître le second terme et le troisième il faudra résoudre deux équations à deux inconnues, l'une du premier degré et l'autre du second, ce qui donnera toujours une équation finale du second, comme nous l'avons vu plus haut; pour faire disparaître le second terme, le troisième et le quatrième, on aura à résoudre trois équations à autant d'inconnues, dont l'une sera du premier degré, la seconde du second degré et la troisième du troisième degré, en sorte que l'équation finale sera, en général, du degré $1 \cdot 2 \cdot 3 = 6$.

En général, pour faire disparaître à la fois les termes $p^{i\text{ème}}, q^{i\text{ème}}, r^{i\text{ème}}, \dots$, on aura à résoudre autant d'équations qu'il y aura de ces termes, avec un même nombre d'inconnues, et ces équations seront des degrés $p-1, q-1, r-1, \dots$, en sorte que l'équation finale montera, en général, au degré $(p-1)(q-1)(r-1) \dots$. Donc, pour chasser par cette méthode tous les termes intermédiaires de la transformée

$$\gamma^m + A\gamma^{m-1} + B\gamma^{m-2} + \dots + M = 0,$$

en sorte qu'elle se réduise à la forme $\gamma^m + M = 0$ qui est toujours résoluble, on tombera, en général, dans une équation du degré $1 \cdot 2 \cdot 3 \dots (m-1)$, qui sera par conséquent toujours plus haut que le degré m de la proposée, excepté le seul cas où $m = 3$.

15. Revenons maintenant à la résolution du troisième degré trouvée d'après la méthode de M. Tschirnhaus, et voyons *à priori*, et indépendamment de la théorie de l'élimination que nous venons d'expliquer, la raison pourquoi cette méthode conduit directement à une réduite du second degré, tandis que la méthode ordinaire mène à une réduite du sixième. Pour cela je considère l'équation subsidiaire

$$x^2 = bx + a + \gamma,$$

dans laquelle γ doit être déterminé par une équation du troisième degré

à deux termes telle que

$$y^3 + C = 0,$$

dont les racines sont

$$y = -\sqrt[3]{C}, \quad y = -\alpha\sqrt[3]{C}, \quad y = -\alpha^2\sqrt[3]{C};$$

et je remarque que ces trois racines devant répondre aux trois valeurs de x qui sont les racines de la proposée

$$x^3 + mx^2 + nx + p = 0,$$

on aura donc, en désignant ces dernières racines par x', x'', x''' , les trois équations suivantes

$$(C) \quad \begin{cases} x'^2 = bx' + a - \sqrt[3]{C}, \\ x''^2 = bx'' + a - \alpha\sqrt[3]{C}, \\ x''''^2 = bx''' + a - \alpha^2\sqrt[3]{C}, \end{cases}$$

d'où l'on pourra tirer les valeurs de α et b , après avoir chassé $\sqrt[3]{C}$; pour cet effet, il n'y a qu'à ajouter ensemble les trois équations dont il s'agit, après avoir multiplié la seconde par α et la troisième par α^2 ; car on aura, à cause de $\alpha^3 = \alpha$ et de $1 + \alpha + \alpha^2 = 0$, comme on l'a déjà vu plus haut, on aura, dis-je,

$$x'^2 + \alpha x''^2 + \alpha^2 x''''^2 = b(x' + \alpha x'' + \alpha^2 x'''),$$

d'où l'on tire

$$b = \frac{x'^2 + \alpha x''^2 + \alpha^2 x''''^2}{x' + \alpha x'' + \alpha^2 x'''}$$

Cette expression de b doit nous faire juger immédiatement du degré de l'équation par laquelle la quantité b doit être déterminée; en effet, il est clair que cette équation doit avoir autant de racines qu'il peut y avoir de valeurs de b ; or les différentes valeurs de b ne peuvent venir que des permutations qu'on peut faire entre les racines x', x'', x''' ; et ces permutations sont au nombre de six, comme nous l'avons déjà remarqué plus haut (*voyez* les n°s 6 et suivants, où les lettres a , b , c désignent les mêmes quantités qui sont nommées ici x', x'', x'''); ainsi la quantité b

pourra avoir en tout six valeurs, qui seront

$$\frac{x'^2 + \alpha x''^2 + \alpha^2 x'''^2}{x' + \alpha x'' + \alpha^2 x'''},$$

$$\frac{x'^2 + \alpha x''^2 + \alpha^2 x''^2}{x' + \alpha x''' + \alpha^2 x''},$$

$$\frac{x''^2 + \alpha x'''^2 + \alpha^2 x'^2}{x'' + \alpha x' + \alpha^2 x''},$$

$$\frac{x''^2 + \alpha x'^2 + \alpha^2 x'''^2}{x'' + \alpha x' + \alpha^2 x'''},$$

$$\frac{x'''^2 + \alpha x'^2 + \alpha^2 x''^2}{x''' + \alpha x' + \alpha^2 x''},$$

$$\frac{x'''^2 + \alpha x''^2 + \alpha^2 x'^2}{x''' + \alpha x'' + \alpha^2 x'},$$

de sorte que, généralement parlant, l'équation en b devrait être du sixième degré; mais j'observe que des six valeurs précédentes la première, la troisième et la cinquième sont égales, ainsi que la seconde, la quatrième et la sixième. En effet, en multipliant le numérateur et le dénominateur de la première par α , ce qui ne la change pas, elle devient la cinquième, à cause de $\alpha^3 = 1$ et de $\alpha^4 = \alpha$; et multipliant par α^2 , elle devient la troisième; de même, en multipliant le haut et le bas de la seconde par α , on aura la quatrième, et en multipliant par α^2 , on aura la sixième. Donc l'équation en b du sixième degré aura nécessairement trois racines égales entre elles et trois autres aussi égales entre elles; ce qui l'abaissera au second degré, puisqu'elle ne pourra être que le cube d'une équation du second degré; et voilà pourquoi la quantité b est donnée simplement par une équation du second degré, comme nous l'avons vu ci-dessus (10). A l'égard de la quantité a , si l'on ajoute ensemble les trois équations (C), on aura, à cause de $1 + \alpha + \alpha^2 = 0$,

$$x'^2 + x''^2 + x'''^2 = b(x' + x'' + x''') + 3a;$$

mais on a

$$x' + x'' + x''' = -m \quad \text{et} \quad x'^2 + x''^2 + x'''^2 = m^2 - 2n;$$

donc

$$m^2 - 2n = -bm + 3a,$$

et de là

$$a = \frac{bm + m^2 - 2n}{3};$$

de sorte qu'en connaissant la valeur de b on connaîtra aussitôt celle de a .

16. La formule

$$\frac{x'^2 + \alpha x''^2 + \alpha^2 x'''^2}{x' + \alpha x'' + \alpha^2 x'''},$$

qui exprime la valeur de b , est donc très-remarquable en ce que, quelques permutations qu'on y fasse entre les quantités x' , x'' , x''' , elle ne peut que demeurer la même, ou se changer en cette autre-ci

$$\frac{x'^2 + \alpha x'''^2 + \alpha^2 x''^2}{x' + \alpha x'' + \alpha^2 x'''};$$

de sorte que ces deux quantités ne peuvent être que les racines d'une équation du second degré; on pourrait trouver *à priori* cette équation en cherchant la somme et le produit des deux quantités dont il s'agit, et il en résulterait après le calcul achevé une équation telle que l'équation en b qu'on a trouvée plus haut (10).

On peut encore remarquer que si l'on multiplie ensemble les deux dénominateurs

$$x' + \alpha x'' + \alpha^2 x''' \quad \text{et} \quad x' + \alpha x''' + \alpha^2 x'',$$

on aura pour produit

$$x'^2 + x''^2 + x'''^2 + (\alpha + \alpha^2)(x'x'' + x'x''' + x''x'''');$$

mais

$$x'^2 + x''^2 + x'''^2 = m^2 - 2n, \quad x'x'' + x'x''' + x''x''' = n \quad \text{et} \quad \alpha + \alpha^2 = -1;$$

de sorte que ce produit deviendra $m^2 - 3n$. De plus, si l'on multiplie le numérateur

$$x'^2 + \alpha x''^2 + \alpha^2 x'''^2$$

par le dénominateur

$$x' + \alpha x''' + \alpha^2 x'',$$

on aura pour produit la quantité

$$x'^3 + x''^3 + x'''^3 + \alpha(x'^2x''' + x''^2x' + x'''^2x'') + \alpha^2(x'^2x'' + x''^2x''' + x'''^2x'),$$

laquelle (à cause que x' , x'' , x''' sont les mêmes racines que nous avons nommées ailleurs a , b , c) se réduit (7) à

$$L - 6x'x''x''' + \alpha M + \alpha^2 N,$$

ou bien à

$$L + 6p + \alpha M + \alpha^2 N,$$

puisque $x'x''x''' = -p$; de sorte que la fraction

$$\frac{x'^2 + \alpha x''^2 + \alpha^2 x'''^2}{x' + \alpha x'' + \alpha^2 x'''}$$

deviendra, en multipliant le haut et le bas par $x' + \alpha x'' + \alpha^2 x'''$, celle-ci

$$\frac{L + 6p + \alpha M + \alpha^2 N}{m^2 - 3n};$$

et de même l'autre fraction

$$\frac{x'^2 + \alpha x''^2 + \alpha^2 x'''^2}{x' + \alpha x'' + \alpha^2 x'''}$$

deviendra, en multipliant le haut et le bas par $x' + \alpha x'' + \alpha^2 x'''$,

$$\frac{L + 6p + \alpha N + \alpha^2 M}{m^2 - 3n}.$$

Mais dans le numéro cité on avait

$$r^3 = L + 3\alpha M + 3\alpha^2 N \quad \text{et} \quad s^3 = L + 3\alpha N + 3\alpha^2 M;$$

donc

$$\alpha M + \alpha^2 N = \frac{r^3 - L}{3} \quad \text{et} \quad \alpha N + \alpha^2 M = \frac{s^3 - L}{3};$$

par conséquent les deux fractions dont il s'agit seront

$$\frac{r^3 + 2L + 18p}{3(m^2 - 3n)} \quad \text{et} \quad \frac{s^3 + 2L + 18p}{3(m^2 - 3n)},$$

ou bien (8)

$$\frac{z' + 2L + 18p}{3(m^2 - 3n)} \text{ et } \frac{z'' + 2L + 18p}{3(m^2 - 3n)},$$

z' et z'' étant les racines de l'équation

$$z^2 + (2m^3 - 9mn + 27p)z + (m^2 - 3n)^3 = 0$$

qui est la réduite que donne la méthode de Cardan.

Ce qui fait voir clairement la liaison et l'analogie de cette méthode avec celle de Tschirnhaus.

17. L'expression de x trouvée (10) d'après la méthode de Tschirnhaus peut se mettre évidemment sous cette forme

$$x = \frac{f + gy}{k + y},$$

f , g et k étant des indéterminées et y la racine d'une équation du troisième degré à deux termes telle que

$$y^3 + h = 0.$$

Ainsi il n'y aurait qu'à éliminer y par le moyen de ces deux équations, dont la première donne

$$y = \frac{f - kx}{x - g},$$

ce qui étant substitué dans la seconde, il vient

$$h + \left(\frac{f - kx}{x - g} \right)^3 = 0,$$

équation du troisième degré qu'on pourra comparer avec la proposée; et cette comparaison servira à déterminer les quantités f , g , k , h , dont une restera arbitraire et pourra être prise à volonté.

Cette méthode de résoudre les équations du troisième degré a déjà été employée par M. Bezout dans un excellent Mémoire qu'il a donné sur cette matière dans le volume des *Mémoires de l'Académie des Sciences* de

Paris, pour l'année 1762, et dans lequel l'Auteur a fait un usage utile et heureux de ces substitutions pour résoudre une classe très-étendue d'équations de tous les degrés. Nous nous contenterons de remarquer ici que si l'on voulait savoir d'avance ce que l'on peut se promettre des substitutions dont il s'agit pour la résolution des équations du troisième degré, il n'y aurait qu'à chercher *à priori* le degré et la forme de l'équation qui donnera l'un des coefficients f , ou g , etc.; pour cela on considérera que, puisque $y^3 + h = 0$, on aura ces trois valeurs de y , savoir $-\sqrt[3]{h}$, $-\alpha\sqrt[3]{h}$, $-\alpha^2\sqrt[3]{h}$, lesquelles étant substituées dans l'expression de

$$x = \frac{f + gy}{k + y}$$

donneront les trois valeurs de x , savoir x' , x'' , x''' .

Ainsi prenant l'équation

$$x(k + y) = f + gy,$$

ou bien

$$kx - f + (x - g)y = 0,$$

on en déduira ces trois-ci

$$kx' - f - (x' - g)\sqrt[3]{h} = 0,$$

$$kx'' - f - \alpha(x'' - g)\sqrt[3]{h} = 0,$$

$$kx''' - f - \alpha^2(x''' - g)\sqrt[3]{h} = 0,$$

qui étant d'abord ajoutées ensemble donnent, à cause de $x' + x'' + x''' = -m$ et $1 + \alpha + \alpha^2 = 0$,

$$mk + 3f + (x' + \alpha x'' + \alpha^2 x''')\sqrt[3]{h} = 0;$$

de plus, multipliant la seconde par α et la troisième par α^2 , et les ajoutant ensuite toutes trois ensemble, on aura

$$k(x' + \alpha x'' + \alpha^2 x''') - (x' + \alpha^2 x'' + \alpha x''')\sqrt[3]{h} = 0.$$

Celle-ci donne

$$\sqrt[3]{h} = \frac{k(x' + \alpha x'' + \alpha^2 x''')}{x' + \alpha x'' + \alpha^2 x''},$$

et, cette valeur étant substituée dans la première, on aura en divisant par k

$$m + \frac{3f}{k} + \frac{(x' + \alpha x'' + \alpha^2 x''')^2}{x' + \alpha x'' + \alpha^2 x''} = 0,$$

d'où l'on tire

$$\frac{f}{k} = -\frac{m}{3} - \frac{(x' + \alpha x'' + \alpha^2 x''')^2}{3(x' + \alpha x'' + \alpha^2 x'')}$$

Il est d'abord facile de voir par cette expression que la quantité $\frac{f}{k}$ ne peut avoir que deux valeurs différentes, et que par conséquent elle ne pourra être donnée que par une équation du second degré; car la fraction

$$\frac{(x' + \alpha x'' + \alpha^2 x''')^2}{x' + \alpha x'' + \alpha^2 x'''}$$

ne peut que demeurer la même, ou se changer dans la fraction

$$\frac{(x' + \alpha x'' + \alpha^2 x'')^2}{x' + \alpha x'' + \alpha^2 x'''},$$

en faisant telle permutation que l'on voudra entre les trois racines x' , x'' , x''' . C'est ce qu'on comprendra encore plus aisément en multipliant le haut et le bas de la première fraction par

$$x' + \alpha x'' + \alpha^2 x''',$$

et le haut et le bas de la seconde par

$$x' + \alpha x'' + \alpha^2 x'';$$

car alors elles deviendront (16)

$$\frac{(x' + \alpha x'' + \alpha^2 x''')^3}{m^2 - 3n} \quad \text{et} \quad \frac{(x' + \alpha x'' + \alpha^2 x'')^3}{m^2 - 3n},$$

c'est-à-dire (7)

$$\frac{r^3}{m^2 - 3n} \quad \text{et} \quad \frac{s^3}{m^2 - 3n},$$

ou bien

$$\frac{z'}{m^2 - 3n} \quad \text{et} \quad \frac{z''}{m^2 - 3n},$$

de sorte que les deux valeurs de $\frac{f}{k}$ seront

$$-\frac{m}{3} - \frac{z'}{3(m^2 - 3n)} \quad \text{et} \quad -\frac{m}{3} - \frac{z''}{3(m^2 - 3n)},$$

z' et z'' étant les racines de l'équation en z donnée ci-dessus.

18. Reprenons l'expression de x

$$\frac{f + gy}{k + y},$$

et comme y est un radical donné par l'équation $y^3 + h = 0$, faisons évanouir ce radical du dénominateur $k + y$ en multipliant le haut et le bas de la fraction par $k^2 - ky + y^2$, ce qui la changera en celle-ci

$$\frac{k^2f + (k^2g - kf)y + (f - kg)y^2 + gy^3}{k^3 + y^3},$$

c'est-à-dire, en substituant $-h$ à la place de y^3 ,

$$\frac{k^2f - hg + (k^2g - kf)y + (f - kg)y^2}{k^3 - h},$$

quantité qu'on peut réduire à cette forme plus simple

$$a + by + cy^2,$$

de sorte que l'on aura, en général,

$$x = a + by + cy^2,$$

a, b, c étant des coefficients indéterminés et y la racine d'une équation du troisième degré à deux termes telle que $y^3 + h = 0$.

Cette expression de x est la même que MM. Euler et Bezout ont adoptée pour exprimer les racines des équations du troisième degré, et que ces Auteurs croient pouvoir étendre, en général, aux équations de tous les degrés. Voyez les *Nouveaux Commentaires de Pétersbourg*, tome IX, et les *Mémoires de l'Académie des Sciences* de Paris, pour l'année 1765.

Pour résoudre donc les équations du troisième degré d'après cette mé-

thode, il n'y a qu'à éliminer y par le moyen des deux équations

$$x = a + by + cy^2 \quad \text{et} \quad y^3 + h = 0,$$

ce qui donnera nécessairement une équation en x du troisième degré, comme on peut s'en assurer par la théorie de l'élimination que nous avons donnée plus haut; cette équation étant ensuite comparée terme à terme avec la proposée donnera trois équations par lesquelles on pourra déterminer trois des quatre indéterminées a, b, c, h , la quatrième pouvant être prise à volonté. M. Bezout fait d'abord, pour plus de simplicité, $h = -1$; mais M. Euler conserve dans le calcul toutes les indéterminées, et il prend ensuite égale à l'unité celle qui lui paraît devoir donner un résultat plus simple; c'est toute la différence qui se trouve entre les procédés de ces deux Auteurs.

19. Pour apprécier cette méthode *à priori*, nous allons chercher d'après nos principes la forme et le degré des équations finales qui serviront à la détermination des coefficients a, b, \dots ; et comme l'équation $y^3 + h = 0$ donne les trois racines $-\sqrt[3]{h}, -\alpha\sqrt[3]{h}, -\alpha^2\sqrt[3]{h}$, il est clair qu'on aura sur-le-champ les trois équations

$$\begin{aligned} x' &= a - b\sqrt[3]{h} + c\sqrt[3]{h^2}, \\ x'' &= a - \alpha b\sqrt[3]{h} + \alpha^2 c\sqrt[3]{h^2}, \\ x''' &= a - \alpha^2 b\sqrt[3]{h} + \alpha c\sqrt[3]{h^2}, \end{aligned}$$

qui étant ajoutées ensemble donneront d'abord

$$a = x' + x'' + x''' = -m;$$

ensuite, multipliant la seconde par α^2 , la troisième par α et les ajoutant toutes trois, on aura

$$x' + \alpha^2 x'' + \alpha x''' = -3b\sqrt[3]{h};$$

enfin, multipliant la seconde par α , la troisième par α^2 et les ajoutant de même, on aura

$$x' + \alpha x'' + \alpha^2 x''' = 3c\sqrt[3]{h^2}.$$

Si l'on fait $h = -1$, on aura

$$b = \frac{x' + \alpha x''' + \alpha^2 x''}{3},$$

$$c = \frac{x' + \alpha x'' + \alpha^2 x'''}{3}.$$

Or ces expressions sont les mêmes que celles que nous avons trouvées plus haut pour les racines de la réduite du troisième degré d'après la règle de Cardan; de sorte qu'on peut conclure d'abord que les quantités b et c seront données par une même équation du sixième degré résoluble à la manière de celles du second, et qui sera (5)

$$y^6 + \left(p - \frac{mn}{3} + \frac{2m^3}{27}\right) y^3 - \frac{1}{27} \left(n - \frac{m^2}{3}\right)^3 = 0;$$

c'est aussi ce que M. Bezout a trouvé d'après son calcul.

Mais si, au lieu de supposer avec M. Bezout $h = -1$, on fait avec M. Euler $b = 1$, on aura

$$x' + \alpha x''' + \alpha^2 x'' = -3\sqrt[3]{h} \quad \text{et} \quad x' + \alpha x'' + \alpha^2 x''' = 3c\sqrt[3]{h^2};$$

la première étant élevée au cube donnera

$$-h = \frac{1}{27} (x' + \alpha x''' + \alpha^2 x'')^3,$$

ou bien, en adoptant les dénominations du n° 8,

$$-h = \frac{s^3}{27} = \frac{z''}{27},$$

d'où l'on voit d'abord que la quantité $-h$ sera donnée par une simple équation du second degré, dont les racines seront $\frac{z'}{27}$ et $\frac{z''}{27}$. Ayant trouvé h , il n'y aura qu'à multiplier la première équation par la seconde pour avoir

$$-9ch = (x' + \alpha x'' + \alpha^2 x''')(x' + \alpha x''' + \alpha^2 x''),$$

ce qui se réduit (16) à

$$-9ch = m^2 - 3n,$$

d'où

$$c = \frac{3n - m^2}{9h}.$$

20. Telles sont les principales méthodes qu'on a trouvées jusqu'à présent pour résoudre les équations du troisième degré. Par l'analyse que nous venons d'en faire il est visible que ces méthodes reviennent toutes au même pour le fond, puisqu'elles consistent à trouver des réduites dont les racines soient représentées en général par $x' + \alpha x'' + \alpha^2 x'''$, ou par $(x' + \alpha x'' + \alpha^2 x''')^3$, ou bien, ce qui est la même chose, par des quantités proportionnelles à celles-ci. Dans le cas où la racine de la *réduite* est $x' + \alpha x'' + \alpha^2 x'''$, cette réduite est du sixième degré, résoluble à la manière du second parce qu'elle ne renferme que la troisième et la sixième puissance de l'inconnue. Nous en avons donné la raison dans le n° 6. Dans l'autre cas, où la racine de la *réduite* est $(x' + \alpha x'' + \alpha^2 x''')^3$, cette réduite ne peut être que du second degré, ce qui suit nécessairement du cas précédent, et que nous avons aussi démontré d'une manière directe (9).

21. Avant de terminer cette Section nous dirons un mot de la résolution de l'équation

$$x^3 - 1 = 0,$$

dont nous avons supposé les racines 1, α et β ; et nous ferons en même temps quelques remarques sur la résolution générale de l'équation

$$x^n - 1 = 0,$$

lesquelles pourront nous être utiles dans la suite.

Il est d'abord clair que l'unité est une des racines de l'équation $x^3 - 1 = 0$, de sorte que pour trouver les deux autres il n'y aura qu'à diviser d'abord cette équation par $x - 1$, ce qui donnera celle-ci

$$x^2 - x + 1 = 0,$$

d'où l'on tire

$$x = \frac{-1 \pm \sqrt{-3}}{2}.$$

Ainsi l'on aura

$$\alpha = \frac{-1 + \sqrt{-3}}{2} \quad \text{et} \quad \beta = \frac{-1 - \sqrt{-3}}{2},$$

et il est facile de se convaincre que β est en effet égal à α^2 , comme nous l'avons déjà trouvé *a priori*; car faisant le carré de α on a

$$\frac{1 - 2\sqrt{-3} - 3}{4} = \frac{-1 - \sqrt{-3}}{2} = \beta.$$

En général, soit l'équation à deux termes

$$x^n - 1 = 0;$$

on remarquera d'abord que si n est un nombre composé, en sorte que $n = pq$, la résolution de cette équation se réduira toujours à celle de deux équations semblables, l'une du degré p et l'autre du degré q . Car, faisant $x^q = y$, on aura $x^n = y^p$, et par conséquent

$$y^p - 1 = 0.$$

Supposons donc qu'on ait résolu cette équation du degré p et que α soit une des racines, on aura ensuite

$$x^q - \alpha = 0,$$

ou bien, faisant $x = t \sqrt[q]{\alpha}$,

$$t^q - 1 = 0;$$

et cette nouvelle équation étant résolue, on aura la valeur de t et par conséquent celle de x .

De là on voit que la difficulté de résoudre l'équation $x^n - 1 = 0$, lorsque n est un nombre composé, se réduit à résoudre autant de pareilles équations que n a de facteurs simples, et dont les degrés soient ces mêmes facteurs de n .

Ainsi toute la difficulté consiste à résoudre l'équation $x^n - 1 = 0$ lorsque n est un nombre premier.

Considérons, en général, le cas où n est impair, en sorte que l'équation à résoudre soit

$$x^{2p+1} - 1 = 0;$$

puisque l'unité est toujours une des valeurs de x , on pourra diviser par $x - 1$, et le quotient sera

$$x^{2p} + x^{2p-1} + x^{2p-2} + \dots + x^2 + x + 1 = 0.$$

Or cette équation qui est du degré $2p$ peut toujours s'abaisser au degré p , car, en la divisant par x^p et mettant ensemble les termes qui sont également éloignés de celui du milieu, on aura

$$x^p + \frac{1}{x^p} + x^{p-1} + \frac{1}{x^{p-1}} + \dots + x^2 + \frac{1}{x^2} + x + \frac{1}{x} + 1 = 0.$$

Qu'on fasse $x + \frac{1}{x} = y$ et éllevant y au carré, au cube, etc., on trouvera

$$y^2 = x^2 + \frac{1}{x^2} + 2, \quad y^3 = x^3 + \frac{1}{x^3} + 3 \left(x + \frac{1}{x} \right), \dots;$$

donc

$$x^2 + \frac{1}{x^2} = y^2 - 2, \quad x^3 + \frac{1}{x^3} = y^3 - 3y,$$

et, en général,

$$x^r + \frac{1}{x^r} = y^r - r y^{r-2} + \frac{r(r-3)}{2} y^{r-4} - \frac{r(r-4)(r-5)}{2 \cdot 3} y^{r-6} + \dots,$$

en ne continuant la série que tant que l'on aura des puissances positives de y .

Faisant donc ces substitutions dans l'équation ci-dessus, on aura une transformée en y où toutes les puissances de y seront positives et où la plus haute sera y^p , de sorte que l'équation ne sera plus que du degré $p^{\text{ème}}$.

Donc, si l'on peut résoudre cette dernière équation, on aura p valeurs de y , dont chacune donnera ensuite deux valeurs de x par la résolution de l'équation quadratique

$$x^2 - xy + 1 = 0;$$

moyennant quoi on aura $2p$ valeurs de x , auxquelles joignant la première racine $x = 1$, on aura toutes les racines de l'équation

$$x^{2p+1} - 1 = 0.$$

Ainsi l'on pourra avoir par l'extraction de la seule racine carrée les

racines des équations

$$x^2 - 1 = 0, \quad x^3 - 1 = 0 \quad \text{et} \quad x^5 - 1 = 0;$$

par conséquent on pourra résoudre de même toute équation

$$x^n - 1 = 0,$$

lorsque n ne contiendra d'autres facteurs simples que 2, 3 et 5, c'est-à-dire lorsque n sera de la forme $2^{\lambda} \cdot 3^{\mu} \cdot 5^{\nu}$. En admettant la résolution des équations du troisième degré, on pourra résoudre encore l'équation

$$x^7 - 1 = 0,$$

et par conséquent toute équation

$$x^n - 1 = 0,$$

lorsque n sera de la forme $2^{\lambda} \cdot 3^{\mu} \cdot 5^{\nu} \cdot 7^{\omega}$.

Mais on ne saurait aller plus loin, puisque, le nombre premier qui suit 7 étant 11, il faudrait pouvoir résoudre l'équation

$$x^{11} - 1 = 0,$$

ce qui demanderait la résolution d'une équation du cinquième degré.

Cependant on peut toujours exprimer les racines de toute équation $x^n - 1 = 0$, quel que soit n , par la division de la circonference du cercle en n parties, comme on le verra ci-après.

22. La méthode que nous avons employée pour abaisser l'équation

$$x^{2p} + x^{2p-1} + \dots + x + 1 = 0$$

au degré p peut s'appliquer, en général, à toute équation d'un degré pair, et où les coefficients des termes équidistants de celui du milieu sont les mêmes; car prenant l'équation

$$x^{2p} + ax^{2p-1} + bx^{2p-2} + \dots + bx^2 + ax + 1 = 0,$$

et la divisant par x^p , elle pourra se mettre sous la forme

$$x^p + \frac{1}{x^p} + a \left(x^{p-1} + \frac{1}{x^{p-1}} \right) + b \left(x^{p-2} + \frac{1}{x^{p-2}} \right) + \dots = 0,$$

de sorte qu'on y pourra faire usage des substitutions

$$x + \frac{1}{x} = y, \quad x^2 + \frac{1}{x^2} = y^2 - 2, \dots,$$

au moyen desquelles la transformée en y ne sera que du degré $p^{ième}$.

Si l'on avait l'équation du degré impair $2p+1$,

$$x^{2p+1} + ax^{2p} + bx^{2p-1} + \dots + hx^{p+1} + hx^p + \dots + bx^2 + ax + 1 = 0,$$

on la disposerait d'abord ainsi

$$x^{2p+1} + 1 + ax(x^{2p-1} + 1) + bx^2(x^{2p-3} + 1) + \dots + hx^p(x + 1) = 0,$$

où l'on voit que chaque terme est divisible par $x + 1$, et, la division faite, on aura

$$\left. \begin{aligned} & x^{2p} + x^{2p-1} + x^{2p-2} + x^{2p-3} + \dots + 1 \\ & + ax(x^{2p-2} + x^{2p-3} + \dots + 1) \\ & + bx^2(x^{2p-4} + x^{2p-5} + \dots + 1) \\ & \dots \dots \dots \dots \dots \dots \\ & + hx^p \end{aligned} \right\} = 0,$$

équation qui, étant ordonnée par rapport aux puissances de x , se trouvera dans le cas de l'équation ci-dessus et pourra par conséquent s'abaisser par la même méthode au degré p .

M. de Moivre est, je crois, le premier qui ait remarqué cette propriété des équations dont nous parlons, et il a donné dans ses *Miscellanea analytica* la formule générale de la transformée dont le degré n'est que la moitié de celui de la proposée. Nous donnerons plus bas la raison *à priori* pourquoi ces sortes d'équations sont susceptibles d'une pareille réduction.

23. Reprenons la formule trouvée dans le n° 21, savoir

$$x^r + \frac{1}{x^r} = y^r - ry^{r-2} + \frac{r(r-3)}{2} y^{r-4} - \dots,$$

et remarquons que, par les théorèmes connus de la multisection angulaire, la quantité

$$y^r - ry^{r-2} + \frac{r(r-3)}{2} y^{r-4} - \dots$$

représente, dans un cercle dont le rayon est égal à 1, la corde du complément à 180° d'un arc r de l'angle φ de celui dont la corde du complément serait y ; de sorte qu'en nommant ce dernier arc 2φ on aura

$$y = 2 \cos \varphi \quad \text{et} \quad y^r - ry^{r-2} + \frac{r(r-3)}{2} y^{r-4} - \dots = 2 \cos r\varphi,$$

les cordes des compléments étant, comme on sait, égales aux doubles des cosinus de la moitié des angles.

Ainsi faisant $x + \frac{1}{x} = 2 \cos \varphi$, on aura, en général, $x^n + \frac{1}{x^n} = 2 \cos n\varphi$; par conséquent les deux équations

$$\begin{aligned} x^2 - 2x \cos \varphi + 1 &= 0, \\ x^{2n} - 2x^n \cos n\varphi + 1 &= 0 \end{aligned}$$

subsisteront à la fois, quel que soit le nombre n , en sorte que la première sera nécessairement un diviseur de la seconde; c'est le fondement du fameux théorème de M. Cotes.

Maintenant, si l'on résout ces deux équations à la manière des équations quadratiques, on aura ces deux-ci

$$\begin{aligned} x &= \cos \varphi \pm \sin \varphi \sqrt{-1}, \\ x^n &= \cos n\varphi \pm \sin n\varphi \sqrt{-1}, \end{aligned}$$

où il est facile de prouver que les signes ambigus doivent être les mêmes dans l'une et l'autre; car supposant φ très-petit, on aura, aux infiniment petits du second ordre près,

$$\cos \varphi = 1, \quad \sin \varphi = \varphi, \quad \text{et de même} \quad \cos n\varphi = 1, \quad \sin n\varphi = n\varphi,$$

de sorte que les deux équations deviendront

$$\begin{aligned} x &= 1 \pm \varphi \sqrt{-1}, \\ x^n &= 1 \pm n\varphi \sqrt{-1}; \end{aligned}$$

or, en élevant la première à la puissance n , et négligeant le carré et les puissances plus hautes de φ , on aurait

$$x^n = 1 \pm n\varphi \sqrt{-1},$$

valeur qui devant être la même que celle qui est donnée par la seconde équation, on en conclura l'identité des signes ambigus + ou - dans les deux équations. Faisant donc abstraction de l'ambiguïté des signes, il est clair que

$$x = \cos \varphi + \sin \varphi \sqrt{-1}$$

sera la résolution de l'équation

$$x^n - \cos n\varphi - \sin n\varphi \sqrt{-1} = 0.$$

Donc, si l'on suppose $\sin n\varphi = 0$ et $\cos n\varphi = 1$, ce qui donne $n\varphi = 360^\circ$ ou $= 720^\circ$, ou, en général, égal à $m \times 360^\circ$, m étant un nombre entier quelconque, on aura l'équation

$$x^n - 1 = 0,$$

dont la résolution sera, à cause de $\varphi = \frac{m}{n} \times 360^\circ$,

$$x = \cos \left(\frac{m}{n} \times 360^\circ \right) + \sin \left(\frac{m}{n} \times 360^\circ \right) \sqrt{-1}.$$

Cette expression est générale pour chacune des racines de l'équation proposée $x^n - 1 = 0$, et on les aura toutes en faisant successivement $m = 1, 2, 3, \dots, n$ inclusivement; il serait inutile de faire $m > n$, puisqu'il en résultera de nouveau les mêmes valeurs que lorsque $m < n$.

24. Nous remarquerons d'abord sur cette solution que toutes les racines de l'équation $x^n - 1 = 0$ doivent être différentes entre elles, puisque dans la circonférence il n'y a pas deux arcs différents qui aient un même sinus et un même cosinus à la fois. De plus il est facile de voir que toutes les racines seront imaginaires, à l'exception de la dernière qui répond à $m = n$ et qui sera toujours égale à 1, et de celle qui répon-

dra à $m = \frac{n}{2}$, lorsque n sera pair, laquelle sera égale à -1 ; car pour que la partie imaginaire de l'expression de x disparaîsse, il faut que l'on ait

$$\sin\left(\frac{m}{n} \times 360^\circ\right) = 0,$$

ce qui n'arrive que lorsque l'arc est égal à 360° ou à 180° ; de sorte qu'on aura ou $\frac{m}{n} = 1$ ou $= \frac{1}{2}$, et par conséquent ou $m = n$ ou $m = \frac{n}{2}$; dans le premier cas la partie réelle $\cos\left(\frac{m}{n} \times 360^\circ\right)$ deviendra $\cos 360^\circ = 1$; et dans le second elle deviendra $\cos 180^\circ = -1$.

Maintenant, si l'on fait

$$\alpha = \cos \frac{360^\circ}{n} + \sin \frac{360^\circ}{n} \sqrt{-1},$$

on aura par les formules ci-dessus

$$\alpha^n = \cos\left(\frac{m}{n} \times 360^\circ\right) + \sin\left(\frac{m}{n} \times 360^\circ\right) \sqrt{-1};$$

de sorte que les différentes racines de $x^n - 1 = 0$ seront toutes exprimées par les puissances de la quantité α ; et qu'ainsi ces racines seront $\alpha, \alpha^2, \alpha^3, \dots, \alpha^n$, dont la dernière α^n sera toujours égale à 1 , ce qui est évident par l'équation même $x^n - 1 = 0$, laquelle doit donner $\alpha^n - 1 = 0$, et dont celle qui sera représentée par $\alpha^{\frac{n}{2}}$, lorsque n est pair, sera égale à -1 , comme on l'a vu plus haut.

Il est bon d'observer ici que si n est un nombre premier, on pourra toujours représenter toutes les racines de $x^n - 1 = 0$ par les puissances successives d'une quelconque de ces mêmes racines, la dernière seule exceptée; car soit, par exemple, $n = 3$, les racines seront $\alpha, \alpha^2, \alpha^3$; si l'on prend à la place de α la racine suivante α^2 , on aura les trois racines $\alpha^2, \alpha^4, \alpha^6$; mais, à cause de $\alpha^3 = 1$, il est clair que $\alpha^4 = \alpha$ et que $\alpha^6 = \alpha^3$; de sorte que ces racines seront $\alpha^2, \alpha, \alpha^3$, les mêmes qu'auparavant; de même, si $n = 5$, les racines seront $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$; et si l'on

prend la racine α^2 au lieu de la racine α , on aura celles-ci $\alpha^2, \alpha^4, \alpha^6, \alpha^8, \alpha^{10}$, lesquelles, à cause de $\alpha^5 = 1$, deviennent $\alpha^2, \alpha^4, \alpha, \alpha^3, \alpha^5$; que si l'on prend à la place de α la racine α^3 , on trouvera de même, en rabattant des exposants de α qui surpassent 5 le nombre 5 autant de fois que l'on peut, on trouvera, dis-je, les racines $\alpha^3, \alpha, \alpha^4, \alpha^2, \alpha^5$; enfin, prenant pour α la racine α^4 , on trouvera celles-ci $\alpha^4, \alpha^3, \alpha^2, \alpha, \alpha^5$; de sorte qu'on aura toujours les mêmes racines, mais dans un ordre différent.

En général, soit α^m une quelconque des n racines $\alpha, \alpha^2, \alpha^3, \dots, \alpha^n$, m étant plus petit que n , et n étant un nombre premier; prenant cette racine à la place de α , on aura celles-ci $\alpha^m, \alpha^{2m}, \alpha^{3m}, \dots, \alpha^{nm}$; or, si l'on retranche des exposants $2m, 3m, 4m, \dots$, lorsqu'ils surpassent n , le plus grand multiple de n qu'ils contiennent, et qu'on dénote les restes par p, q, r, \dots , on aura les racines $\alpha^m, \alpha^p, \alpha^q, \alpha^r, \dots, \alpha^n$; et je dis que les nombres m, p, q, r, \dots, n , dont aucun n'est plus grand que n , seront nécessairement tous différents entre eux; car si deux quelconques comme p et r étaient égaux, comme ces nombres ne sont que les restes des nombres $2m, 4m$, après en avoir retranché les plus grands multiples de n , il est clair qu'il faudrait que la différence de ces derniers $2m, 4m$, fût divisible par n ; ce qui ne se peut tant que n est premier et $m < n$. Donc, puisque les nombres m, p, q, r, \dots , dont le nombre est $n - 1$, sont tous différents entre eux et tous moindres que n , il est clair qu'ils ne peuvent être autre chose que les nombres $1, 2, 3, \dots, n - 1$; par conséquent les racines $\alpha^m, \alpha^p, \alpha^q, \alpha^r, \dots, \alpha^n$ seront les mêmes que les racines $\alpha, \alpha^2, \alpha^3, \dots, \alpha^n$. Il est facile de voir que la démonstration précédente n'en subsistera pas moins lorsque n ne sera pas premier, pourvu que l'on prenne m premier à n ; mais si m n'est pas premier à n , et que leur plus grande mesure soit l , on verra aisément que tous les nombres m, p, q, r, \dots seront mesurés par l ; de sorte que ces nombres ne pourront être que des multiples de l moindres que n .

Dé là il est aisé de conclure, en général, que l'on peut représenter toutes les racines $\alpha, \alpha^2, \alpha^3, \dots, \alpha^n$ de l'équation $x^n - 1 = 0$ par les puissances $1^{\text{re}}, 2^{\text{e}}, 3^{\text{e}}, \dots, n^{\text{ième}}$ d'une quelconque de ces racines comme α^m , pourvu que m soit premier à n ; mais que si m n'est pas premier à n , en

sorte que leur plus grande mesure soit l , on n'aura de cette manière que les seules racines $\alpha^l, \alpha^{2l}, \alpha^{3l}, \dots, \alpha^n$, donc chacune se trouvera répétée autant de fois qu'il y a d'unités dans $\frac{n}{l}$; et il est facile de voir par les formules ci-dessus que ces dernières racines seront aussi celles de l'équation $x^f - 1 = 0$, en supposant $lf = n$.

Or, comme les racines de l'équation $x^n - 1 = 0$ sont représentées par

$$\alpha, \alpha^2, \alpha^3, \dots, \alpha^n,$$

et que $\alpha^n = 1$, il est clair qu'on pourra les représenter aussi, si l'on veut, par

$$\frac{1}{\alpha}, \frac{1}{\alpha^2}, \frac{1}{\alpha^3}, \dots, \frac{1}{\alpha^n},$$

puisqu'on aura $\frac{1}{\alpha} = \alpha^{n-1}, \frac{1}{\alpha^2} = \alpha^{n-2}, \dots$

De plus, à cause que l'équation $x^n - 1 = 0$ manque du second terme, il est clair qu'on aura toujours, en général,

$$\alpha + \alpha^2 + \alpha^3 + \dots + \alpha^n = 0,$$

et de même

$$\frac{1}{\alpha} + \frac{1}{\alpha^2} + \frac{1}{\alpha^3} + \dots + \frac{1}{\alpha^n} = 0.$$

Et lorsque n est un nombre composé comme lf , on aura en particulier

$$\alpha^l + \alpha^{2l} + \alpha^{3l} + \dots + \alpha^n = 0,$$

$$\frac{1}{\alpha^l} + \frac{1}{\alpha^{2l}} + \frac{1}{\alpha^{3l}} + \dots + \frac{1}{\alpha^n} = 0,$$

et de même

$$\alpha^f + \alpha^{2f} + \alpha^{3f} + \dots + \alpha^n = 0,$$

$$\frac{1}{\alpha^f} + \frac{1}{\alpha^{2f}} + \frac{1}{\alpha^{3f}} + \dots + \frac{1}{\alpha^n} = 0;$$

c'est-à-dire que les sommes des puissances tant positives que négatives de α dont les exposants sont divisibles par l ou par f seront égales à zéro; par conséquent aussi la somme des puissances dont les exposants ne seront point divisibles par l sera nulle, comme aussi la somme de celles dont les exposants ne seront point divisibles par f . Ces différentes remarques pourront nous être utiles dans la suite.

25. Maintenant voici les valeurs de α pour les équations $x^n - 1 = 0$ depuis $n = 1$ jusqu'à $n = 6$:

$$n=2 \left\{ \begin{array}{l} \alpha = -1, \\ \alpha^2 = 1; \end{array} \right.$$

$$n=3 \left\{ \begin{array}{l} \alpha = \frac{-1 + \sqrt{-3}}{2}, \\ \alpha^2 = \frac{-1 - \sqrt{-3}}{2}, \\ \alpha^3 = 1; \end{array} \right.$$

$$n=4 \left\{ \begin{array}{l} \alpha = \sqrt{-1}, \\ \alpha^2 = -1, \\ \alpha^3 = -\sqrt{-1}, \\ \alpha^4 = 1; \end{array} \right.$$

$$n=5 \left\{ \begin{array}{l} \alpha = \frac{\sqrt{5} - 1}{4} + \frac{\sqrt{10 + 2\sqrt{5}}}{4} \sqrt{-1}, \\ \alpha^2 = -\frac{\sqrt{5} + 1}{4} + \frac{\sqrt{10 - 2\sqrt{5}}}{4} \sqrt{-1}, \\ \alpha^3 = -\frac{\sqrt{5} + 1}{4} - \frac{\sqrt{10 - 2\sqrt{5}}}{4} \sqrt{-1}, \\ \alpha^4 = \frac{\sqrt{5} - 1}{4} - \frac{\sqrt{10 + 2\sqrt{5}}}{4} \sqrt{-1}, \\ \alpha^5 = 1; \end{array} \right.$$

$$n=6 \left\{ \begin{array}{l} \alpha = \frac{1 + \sqrt{-3}}{2}, \\ \alpha^2 = \frac{-1 + \sqrt{-3}}{2}, \\ \alpha^3 = -1, \\ \alpha^4 = \frac{-1 - \sqrt{-3}}{2}, \\ \alpha^5 = \frac{1 - \sqrt{-3}}{2}, \\ \alpha^6 = 1. \end{array} \right.$$

Si l'on voulait avoir la valeur de α pour l'équation

$$x^7 - 1 = 0,$$

il faudrait, comme on l'a dit plus haut, résoudre une équation du troisième degré. En effet, en faisant $p = 3$ dans les formules du n° 21, on trouvera cette transformée en y

$$y^3 + y^2 - 2y - 1 = 0,$$

qui, étant du troisième degré, aura toujours une racine réelle; et cette racine étant substituée dans l'équation

$$x^2 - xy + 1 = 0,$$

on en tirera x , ou

$$\alpha = \frac{y + \sqrt{y^2 - 4}}{2}.$$

Quant aux équations

$$x^8 - 1 = 0, \quad x^9 - 1 = 0 \quad \text{et} \quad x^{10} - 1 = 0,$$

on en pourra aussi exprimer la racine α par de simples radicaux carrés; mais l'équation

$$x^{11} - 1 = 0$$

exigerait la résolution de l'équation du cinquième degré

$$y^5 + y^4 - 4y^3 - 3y^2 + 3y + 1 = 0,$$

laquelle étant supposée, on aura pour α la même expression en y que ci-dessus.

SECTION SECONDE.

DE LA RÉSOLUTION DES ÉQUATIONS DU QUATRIÈME DEGRÉ.

26. On sait que Louis Ferrari, contemporain et même disciple de Cardan, est le premier qui ait trouvé une règle générale pour la résolution des équations du quatrième degré. Sa méthode consiste à partager

l'équation proposée en deux membres, et à ajouter à l'un et à l'autre une même quantité telle, qu'on puisse extraire séparément la racine carrée des deux membres de l'équation, en sorte qu'elle soit par là abaissée au second degré. Cette méthode, qu'on peut regarder comme la plus ingénieuse de toutes celles qui ont été inventées depuis pour le même objet, a été adoptée par tous les Analystes qui ont précédé Descartes; mais cet illustre Géomètre a cru devoir lui en substituer une autre moins simple à la vérité et moins directe, mais à quelques égards plus conforme à la nature des équations: c'est celle que la plupart des Auteurs suivent aujourd'hui. Nous commencerons donc par examiner ces deux méthodes l'une après l'autre; ensuite nous viendrons aux méthodes connues pour la résolution de ces sortes d'équations, parmi lesquelles on doit surtout distinguer celles de M. Tschirnaus et de MM. Euler et Bezout.

Je suppose d'abord avec Ferrari que l'équation du quatrième degré qu'il s'agit de résoudre soit privée de son second terme, ce qu'on sait d'ailleurs être toujours possible, en sorte que cette équation soit représentée ainsi

$$x^4 + nx^2 + px + q = 0.$$

Qu'on fasse passer dans le second membre tous les termes excepté le premier, et qu'ensuite on ajoute à l'un et l'autre membre la quantité $2yx^2 + y^2$, y étant une indéterminée, on aura

$$x^4 + 2yx^2 + y^2 = (2y - n)x^2 - px + y^2 - q,$$

équation où le premier membre est évidemment le carré de $x^2 + y$, de sorte qu'il ne s'agira plus que de rendre aussi carré le second; or pour cela il faut, comme on sait, que le carré de la moitié du coefficient du second terme $-px$ soit égal au produit des coefficients des deux autres, ce qui donne cette condition

$$\frac{p^2}{4} = (2y - n)(y^2 - q),$$

laquelle produit l'équation cubique

$$y^3 - \frac{n}{2}y^2 - qy + \frac{4nq - p^2}{8} = 0.$$

Supposant donc la résolution de cette équation en sorte qu'on connaisse une valeur de y , le second membre de la proposée deviendra

$$(2y - n) \left[x - \frac{p}{2(2y - n)} \right]^2;$$

done, tirant la racine carrée des deux membres, on aura

$$x^2 + y = \left[x - \frac{p}{2(2y - n)} \right] \sqrt{2y - n},$$

équation où l'inconnue x ne monte qu'au second degré, et qui n'a par conséquent plus de difficulté. Faisons, pour plus de simplicité,

$$z = \sqrt{2y - n},$$

on aura

$$x^2 - zx + y + \frac{p}{2z} = 0,$$

d'où l'on tire sur-le-champ

$$x = \frac{z + \sqrt{z^2 - \frac{2p}{z} - 4y}}{2},$$

ou bien, en remettant la valeur de z ,

$$x = \frac{\sqrt{2y - n} + \sqrt{-2y - n - \frac{2p}{\sqrt{2y - n}}}}{2},$$

et cette expression donnera à la fois les quatre racines de la proposée en prenant successivement les deux radicaux carrés en plus et en moins.

27. Nous remarquerons d'abord que cette méthode ne demande pas absolument l'évanouissement du second terme dans l'équation proposée, et qu'elle peut tout aussi bien s'appliquer aux équations complètes telles que

$$x^4 + mx^3 + nx^2 + px + q = 0,$$

en supposant que le premier membre ne soit pas simplement le carré

de $x^2 + y$, mais celui de $x^2 + \frac{mx}{2} + y$; en effet, en faisant passer comme ci-devant les trois derniers termes dans le second membre et ajoutant de part et d'autre la quantité

$$\left(2y + \frac{m^2}{4}\right)x^2 + myx + y^2,$$

on aura l'équation

$$\left(x^2 + \frac{mx}{2} + y\right)^2 = \left(2y + \frac{m^2}{4} - n\right)x^2 + (my - p)x + y^2 - q.$$

On fera donc, pour rendre aussi le second membre carré,

$$\left(\frac{my - p}{2}\right)^2 = \left(2y + \frac{m^2}{4} - n\right)(y^2 - q),$$

d'où l'on tire l'équation cubique

$$y^3 - \frac{n}{2}y^2 + \frac{mp - 4q}{4}y + \frac{(4n - m^2)q - p^2}{8} = 0.$$

La valeur de y étant déterminée par cette équation, que nous appellerons dorénavant la *réduite*, si l'on fait, pour plus de simplicité,

$$z = \sqrt{2y + \frac{m^2}{4} - n},$$

on aura

$$\left(x^2 + \frac{mx}{2} + y\right)^2 = z^2 \left(x + \frac{my - p}{2z}\right)^2,$$

et, tirant la racine carrée des deux membres,

$$x^2 + \frac{mx}{2} + y = zx + \frac{my - p}{2z},$$

ou bien

$$x^2 + \left(\frac{m}{2} - z\right)x + y - \frac{my - p}{2z} = 0,$$

d'où enfin

$$x = \frac{1}{2} \left[z - \frac{m}{2} + \sqrt{z^2 - mz + \frac{m^2}{4} - 4y + \frac{2(my - p)}{z}} \right],$$

et, remettant la valeur de z ,

$$x = \frac{1}{2} \left(-\frac{m}{2} + \sqrt{2y + \frac{m^2}{4} - n} + \sqrt{-2y + \frac{m^2}{2} - n - \frac{\frac{1}{4}m^3 - mn + 2p}{\sqrt{2y + \frac{m^2}{4} - n}}} \right),$$

expression qui donnera pareillement les quatre racines de la proposée, en prenant successivement chacun des deux radicaux carrés qui y entrent en plus et en moins.

28. Puisque la réduite en y est du troisième degré, elle aura nécessairement trois racines, dont chacune pourra être également substituée dans l'expression de x , de sorte qu'à cause de l'ambiguïté des deux signes radicaux que cette expression contient, il en résultera douze valeurs de x ; d'où il est aisé de conclure que la résolution précédente est essentiellement celle d'une équation du douzième degré.

Pour trouver cette équation, il faudra éliminer y de l'expression de x et en faire disparaître ensuite tous les radicaux, ou bien on pourra remonter d'abord à l'équation rationnelle

$$\left(x^2 + \frac{mx}{2} + y \right)^2 = z^2 \left(x + \frac{my - p}{2z^2} \right)^2,$$

et il n'y aura plus qu'à en éliminer x après y avoir substitué pour z^2 sa valeur

$$2y + \frac{m^2}{4} - n.$$

Supposons pour plus de généralité que la valeur de z^2 , au lieu d'être simplement $2y + \frac{m^2}{4} - n$, soit

$$k \left(2y + \frac{m^2}{4} - n \right);$$

il est évident que le coefficient k ne peut aucunement changer le degré auquel doit monter l'équation en x après l'élimination de y ; on aura de

cette manière l'équation

$$\left(x^2 + \frac{mx}{2} + y\right)^2 = k \left(2y + \frac{m^2}{4} - n\right) x^2 + (my - p)x + \frac{(my - p)^2}{4k \left(2y + \frac{m^2}{4} - n\right)};$$

ou bien, à cause de

$$\frac{(my - p)^2}{4} = \left(2y + \frac{m^2}{4} - n\right) (y^2 - q),$$

en vertu de l'équation en y ,

$$\left(x^2 + \frac{mx}{2} + y\right)^2 = k \left(2y + \frac{m^2}{4} - n\right) x^2 + (my - p)x + \frac{y^2 - q}{k},$$

c'est-à-dire

$$x^4 + mx^3 + \left[kn + (1 - k)\left(2y + \frac{m^2}{4}\right)\right]x^2 + px + \frac{q + (k - 1)y^2}{k} = 0.$$

Soit, pour abréger,

$$x^4 + mx^3 + nx^2 + px + q = X,$$

et, faisant $k - 1 = h$, l'équation précédente deviendra celle-ci

$$X + h \left[\left(n - \frac{m^2}{4} - 2y\right) x^2 + \frac{y^2 - q}{k} \right] = 0,$$

d'où il ne s'agira plus que d'éliminer y par le moyen de l'équation

$$y^3 - \frac{n}{2}y^2 + \frac{mp - 4q}{4}y + \frac{(4n - m^2)q - p^2}{8} = 0.$$

Nommons y' , y'' , y''' les trois racines de cette dernière équation, et l'équation en x résultant de l'élimination de l'inconnue y pourra être représentée (13) par le produit des trois quantités

$$\begin{aligned} & X + h \left[\left(n - \frac{m^2}{4} - 2y'\right) x^2 + \frac{y'^2 - q}{k} \right], \\ & X + h \left[\left(n - \frac{m^2}{4} - 2y''\right) x^2 + \frac{y''^2 - q}{k} \right], \\ & X + h \left[\left(n - \frac{m^2}{4} - 2y'''\right) x^2 + \frac{y''''^2 - q}{k} \right], \end{aligned}$$

ce produit étant égalé à zéro. Faisons, pour abréger,

$$A = X + h \left[\left(n - \frac{m^2}{4} \right) x^2 - \frac{q}{k} \right],$$

$$B = -2hx^2,$$

$$C = \frac{h}{k},$$

et, supposant

$$\alpha = \gamma' + \gamma'' + \gamma''',$$

$$\beta = \gamma'\gamma'' + \gamma'\gamma''' + \gamma''\gamma''',$$

$$\gamma = \gamma'^2 + \gamma''^2 + \gamma''''^2,$$

$$\delta = \gamma'\gamma''\gamma''',$$

$$\varepsilon = \gamma'^2\gamma''^2 + \gamma'^2\gamma''''^2 + \gamma''^2\gamma''''^2,$$

on trouvera, pour le produit dont il s'agit,

$$A^3 + A^2B\alpha + A^2C\gamma + AB^2\beta + ABC(\alpha\beta - 3\delta) + AC^2\varepsilon + B^3\delta + B^2C\alpha\delta + BC^2\beta\delta + C^3\delta^2.$$

Mais faisant encore, pour abréger,

$$a = \frac{n}{2}, \quad b = \frac{mp - 4q}{4}, \quad c = \frac{p^2 - (4n - m^2)q}{8},$$

en sorte que l'équation en y soit représentée par

$$y^3 - ay^2 + by - c = 0,$$

on aura, comme on sait, par la nature des équations,

$$\alpha = a, \quad \beta = b, \quad \delta = c,$$

et de là

$$\gamma = a^2 - 2b, \quad \varepsilon = b^2 - 2ac.$$

Donc l'équation cherchée, résultant de l'élimination de y dans ces deux-ci

$$A + By + Cy^2 = 0,$$

$$y^3 - ay^2 + by - c = 0,$$

sera

$$\begin{aligned} A^3 + aA^2B + (a^2 - 2b)A^2C + bAB^2 + (ab - 3c)ABC \\ + (b^2 - 2ac)AC^2 + cB^3 + acB^2C + bcBC^2 + c^2C^3 = 0. \end{aligned}$$

Si l'on remet maintenant dans cette équation les valeurs de A, B, C et de a , b , c , on aura une équation en x qui montera au douzième degré, puisque A contient toutes les puissances de x jusqu'à la quatrième inclusivement, que B contient simplement x^2 , et que les autres quantités ne renferment point x .

Ainsi la résolution de cette équation du douzième degré sera comme ci-dessus

$$x = \frac{1}{2} \left(z - \frac{m}{2} \pm \sqrt{z^2 - mz + \frac{m^2}{4} - 4y + \frac{2my - p}{z}} \right),$$

en supposant

$$z = \pm \sqrt{2y + \frac{m^2}{4} - nk};$$

et il n'y aura point ici de racines superflues, puisque les trois valeurs de y , combinées avec les signes ambigus des deux radicaux, donneront précisément les douze racines de l'équation dont il s'agit.

Faisons à présent $k = 1$ pour avoir le cas du n° 27; donc $h = 0$, et par conséquent

$$A = X = x^4 + mx^3 + nx^2 + px + q, \quad B = 0, \quad C = 0;$$

ainsi l'équation dont il s'agit se réduira à $A^3 = 0$, c'est-à-dire à celle-ci

$$(x^4 + mx^3 + nx^2 + px + q)^3 = 0,$$

qui n'est autre chose, comme on voit, que l'équation proposée élevée au cube, de sorte qu'elle doit avoir les mêmes racines que cette dernière, mais chacune triple.

On voit par là bien clairement la raison pourquoi l'expression trouvée pour la racine d'une équation du quatrième degré renferme réellement douze racines, qui se réduisent cependant à quatre, puisque chacune d'elles en a deux autres qui lui sont égales. De plus la démonstration précédente fait voir que les racines égales ne viennent que de l'élimination de y , et nullement de l'ambiguïté des radicaux, puisque c'est l'élimination de y qui fait monter dans l'équation résultante la quantité X

au cube; d'où l'on peut conclure d'abord que, quelque valeur de y que l'on emploie dans l'expression de x , on aura toujours les mêmes quatre racines.

29. Mais, pour éclaircir encore davantage cette matière, on remarquera que, dès que la réduite en y a lieu, ce qui peut arriver de trois manières différentes à cause qu'elle a trois racines, on peut donner à la proposée la forme

$$\left(x^2 + \frac{mn}{2} + y\right)^2 - z^2 \left(x + \frac{my - p}{2z^2}\right)^2 = 0,$$

comme on l'a fait au n° 27; par où l'on voit qu'elle n'est autre chose que le produit de ces deux-ci

$$\begin{aligned} x^2 + \frac{mx}{2} + y + z \left(x + \frac{my - p}{2z^2}\right) &= 0, \\ x^2 + \frac{mx}{2} + y - z \left(x + \frac{my - p}{2z^2}\right) &= 0, \end{aligned}$$

c'est-à-dire

$$\begin{aligned} x^2 + \left(\frac{m}{2} + z\right)x + y + \frac{my - p}{2z} &= 0, \\ x^2 + \left(\frac{m}{2} - z\right)x + y - \frac{my - p}{2z} &= 0, \end{aligned}$$

de sorte que leur résolution donnera toujours les mêmes quatre racines de la proposée, quelle que soit la racine qu'on substituera à y .

Nommons maintenant a, b, c, d les quatre racines de la proposée; et il faudra que deux de ces racines soient renfermées dans l'une des deux équations précédentes, et que les deux autres le soient dans l'autre; de sorte qu'on aura, par la nature des équations,

$$\begin{aligned} a + b &= -\frac{m}{2} - z, & ab &= y + \frac{my - p}{2z}, \\ c + d &= -\frac{m}{2} + z, & cd &= y - \frac{my - p}{2z}, \end{aligned}$$

d'où l'on tire

$$z = \frac{c + d - a - b}{2}, \quad y = \frac{ab + cd}{2}.$$

Cette valeur de y nous fait voir d'abord pourquoi la réduite en y est du troisième degré. En effet il est visible que la quantité y doit avoir autant de valeurs différentes qu'on en pourra former par toutes les permutations possibles des racines a, b, c, d dans l'expression $\frac{ab + cd}{2}$; on ne peut avoir de cette manière que les trois quantités suivantes

$$\frac{ab + cd}{2}, \quad \frac{ac + bd}{2}, \quad \frac{ad + cb}{2},$$

de sorte que l'équation dont y sera la racine, devra donner chacune de ces trois quantités et, par conséquent, devra être du troisième degré.

30. On peut donc déduire de cette remarque une manière directe de parvenir à la réduite du quatrième degré, et par son moyen à la résolution générale de ce degré. Car, puisque la combinaison $ab + cd$ des quatre racines a, b, c, d est telle qu'elle n'admet que trois variations, savoir

$$ab + cd, \quad ac + bd, \quad ad + cb,$$

il s'ensuit d'abord que si l'on fait

$$ab + cd = u,$$

on aura une équation en u du troisième degré, dont les racines seront

$$ab + cd, \quad ac + bd, \quad ad + cb,$$

qui sera par conséquent de cette forme

$$u^3 - Au^2 + Bu - C = 0,$$

où l'on aura, par la nature des équations,

$$A = ab + cd + ac + bd + ad + cb,$$

$$B = (ab + cd)(ac + bd) + (ab + cd)(ad + cb) + (ac + bd)(ad + cb),$$

$$C = (ab + cd)(ac + bd)(ad + cb),$$

c'est-à-dire

$$A = ab + ac + ad + bc + bd + cd,$$

$$B = a^2(bc + bd + cd) + b^2(ac + ad + cd) + c^2(ab + ad + bd) + d^2(ab + ac + bc),$$

$$C = abcd(a^2 + b^2 + c^2 + d^2) + a^2b^2c^2 + a^2b^2d^2 + a^2c^2d^2 + b^2c^2d^2.$$

Or il est facile de voir que ces valeurs de A , B , C doivent être données par les coefficients m , n , p , q de la proposée, et cela sans aucune extraction de racines, puisqu'elles demeurent les mêmes, quelque permutation qu'on fasse entre les racines a , b , c , d de cette équation; d'où il suit que chacune d'elles ne peut avoir qu'une seule et même valeur. En effet, ayant

$$\begin{aligned} -m &= a + b + c + d, \\ n &= ab + ac + ad + bc + bd + cd, \\ -p &= abc + abd + acd + bcd, \\ q &= abcd, \end{aligned}$$

on aura d'abord

$$A = n;$$

ensuite, pour trouver B , on observera que

$$a(bc + bd + cd) = -p - bcd,$$

et de même

$$b(ac + ad + cd) = -p - acd,$$

et ainsi des autres, de sorte qu'on aura

$$B = (a + b + c + d)(-p) - 4abcd,$$

c'est-à-dire

$$B = mp - 4q.$$

Enfin, pour avoir C , on remarquera que

$$a^2 + b^2 + c^2 + d^2 = m^2 - 2n;$$

en sorte que la partie $abcd(a^2 + b^2 + c^2 + d^2)$ deviendra $(m^2 - 2n)q$; et, pour avoir l'autre partie, on fera le carré de p et l'on en déduira

$$\begin{aligned} a^2b^2c^2 + a^2b^2d^2 + a^2c^2d^2 + b^2c^2d^2 &= p^2 - 2abcd(ab + ac + bc + ad + bd + cd) \\ &= p^2 - 2nq, \end{aligned}$$

de sorte que l'on aura

$$C = (m^2 - 4n)q + p^2.$$

Moyennant quoi notre réduite sera

$$u^3 - nu^2 + (mp - 4q)u - (m^2 - 4n)q - p^2 = 0,$$

qui est la même que celle en y du n° 27, en supposant $u = 2y$.

31. Voyons maintenant comment, en connaissant une des valeurs de u , on pourra trouver les quatre racines a, b, c, d . Puisque

$$u = ab + cd \quad \text{et} \quad abcd = q,$$

il est clair que les deux quantités ab et cd seront les racines de cette équation du second degré

$$t^2 - ut + q = 0,$$

de sorte qu'en nommant t' et t'' ces deux racines on connaîtra les deux produits

$$ab = t' \quad \text{et} \quad cd = t'';$$

de plus on a

$$-p = ab(c + d) + cd(a + b) = t'(c + d) + t''(a + b),$$

et comme

$$a + b + c + d = -m,$$

on aura

$$a + b = \frac{p - mt'}{t' - t''}, \quad c + d = \frac{p - mt''}{t'' - t'},$$

donc, puisque

$$ab = t' \quad \text{et} \quad cd = t'',$$

il est clair que a et b seront les racines de cette équation du second degré

$$x^2 - \frac{p - mt'}{t' - t''} x + t' = 0,$$

et que c et d seront celles de l'équation

$$x^2 - \frac{p - mt''}{t'' - t'} x + t'' = 0.$$

On voit par là qu'il suffit de connaître une des racines de la réduite en u pour avoir les quatre racines a, b, c, d de la proposée, et que chacune des racines de cette réduite donnera toujours les mêmes quatre racines a, b, c, d ; car si, au lieu de prendre $u = ab + cd$, on eût pris $u = ac + bd$ ou $u = ad + bc$, il n'y eût eu d'autre changement dans nos formules sinon que b eût été changé en c ou en d , et *vice versa*.

32. On pourrait résoudre encore l'équation du quatrième degré d'une manière plus simple à l'aide de la réduite dont la racine serait (29)

$$z = \frac{c + d - a - b}{2} \quad \text{ou bien} \quad s = c + d - a - b,$$

en faisant, pour plus de simplicité, $s = 2z$. Pour savoir d'abord de quel degré et de quelle forme doit être cette équation, il n'y a qu'à faire dans la quantité $c + d - a - b$ toutes les permutations possibles entre les lettres a, b, c, d , et il en résultera les six suivantes

$$\begin{aligned} &a + b - c - d, \\ &a + c - b - d, \\ &a + d - c - b, \\ &c + d - a - b, \\ &b + d - a - c, \\ &b + c - a - d, \end{aligned}$$

qui seront donc les racines de la réduite en s , de sorte que cette réduite sera nécessairement du sixième degré; mais, comme les six quantités précédentes sont deux à deux égales et de signes contraires, il s'ensuit que la réduite ne pourra contenir que des puissances paires de l'inconnue s , en sorte qu'elle sera résoluble à la manière des équations du troisième degré.

Donc, si l'on fait $s^2 = t$, on aura une réduite en t du troisième degré et dont les trois racines seront

$$(a + b - c - d)^2, \quad (a + c - b - d)^2, \quad (a + d - b - c)^2.$$

Ainsi l'on pourra trouver cette équation en cherchant la valeur de ses coefficients, comme nous l'avons fait plus haut à l'égard de la réduite en u (30); mais, sans entreprendre un nouveau calcul pour cet objet, il suffira de remarquer que le carré de $a + b - c - d$ est

$$a^2 + b^2 + c^2 + d^2 + 2ab + 2cd - 2ac - 2ad - 2bc - 2bd;$$

mais on a

$$ab + ac + ad + bc + bd + cd = n,$$

$$a^2 + b^2 + c^2 + d^2 = m^2 - 2n;$$

donc, puisque

$$(a + b - c - d)^2 = s^2 = t,$$

on aura

$$t = m^2 - 4n + 4(ab + cd),$$

c'est-à-dire

$$t = m^2 - 4n + 4u;$$

de sorte que, pour avoir la réduite cherchée en t , il n'y aura qu'à substituer, dans celle en u du n° 30, $\frac{t - m^2 + 4n}{4}$ à la place de u ; et l'on aura celle-ci

$$t^3 - (3m^2 - 8n)t^2 + (3m^4 - 16m^2n + 16n^2 + 16mp - 64q)t - (m^3 - 4mn + 8p)^2 = 0.$$

Maintenant, si l'on suppose que t' , t'' et t''' soient les trois racines de cette équation, on aura (hypothèse)

$$(a + b - c - d)^2 = t', \quad (a + c - b - d)^2 = t'', \quad (a + d - b - c)^2 = t''';$$

d'où, en tirant la racine carrée, on aura

$$a + b - c - d = \sqrt{t'}, \quad a + c - b - d = \sqrt{t''}, \quad a + d - b - c = \sqrt{t'''};$$

combinant ces trois équations avec l'équation

$$a + b + c + d = -m,$$

on en tirera les valeurs de chacune des quatre racines a , b , c , d ; on aura donc

$$a = \frac{-m + \sqrt{t'} + \sqrt{t''} + \sqrt{t'''}}{4},$$

$$b = \frac{-m + \sqrt{t'} - \sqrt{t''} - \sqrt{t'''}}{4},$$

$$c = \frac{-m - \sqrt{t'} + \sqrt{t''} - \sqrt{t'''}}{4},$$

$$d = \frac{-m - \sqrt{t'} - \sqrt{t''} + \sqrt{t'''}}{4}.$$

De cette manière on aura donc les quatre racines de la proposée, sans être obligé de résoudre aucune autre équation que la réduite en t . Mais il se présente ici une difficulté, c'est que, comme chaque radical $\sqrt{t'}$, $\sqrt{t''}$, $\sqrt{t'''}$ peut être pris également en plus et en moins, les expressions précédentes renfermeront encore ces quatre quantités-ci

$$\frac{-m + \sqrt{t'} + \sqrt{t''} - \sqrt{t'''}}{4},$$

$$\frac{-m + \sqrt{t'} - \sqrt{t''} + \sqrt{t'''}}{4},$$

$$\frac{-m - \sqrt{t'} + \sqrt{t''} + \sqrt{t'''}}{4},$$

$$\frac{-m - \sqrt{t'} - \sqrt{t''} - \sqrt{t'''}}{4},$$

qui ne sont pas les valeurs des racines a, b, c, d , mais celles de leurs compléments à la somme

$$a + b + c + d = -m.$$

Pour résoudre cette difficulté, je remarque qu'il n'est pas nécessaire de savoir précisément quel signe on doit donner à la valeur de chacun des radicaux dont il s'agit, mais qu'il suffit de savoir si ces valeurs doivent être prises, l'une positive et les deux autres positives ou négatives, ou bien l'une négative et les deux autres positives ou négatives; car il est facile de voir que les expressions des racines a, b, c, d , trouvées ci-dessus, donneront toujours les mêmes quatre racines en changeant à la fois les signes de deux quelconques des radicaux $\sqrt{t'}$, $\sqrt{t''}$, $\sqrt{t'''}$, et conservant celui du troisième. De sorte que tout se réduit à connaître le signe que doit avoir le produit des trois valeurs de $\sqrt{t'}$, $\sqrt{t''}$, $\sqrt{t'''}$. Or, par l'équation en t , on aura

$$t' t'' t''' = (m^3 - 4mn + 8p)^2,$$

d'où l'on tire

$$m^3 - 4mn + 8p = \sqrt{t'} \sqrt{t''} \sqrt{t'''} \quad (*).$$

Donc, si l'on dénote par $\theta', \theta'', \theta'''$ les valeurs des radicaux $\sqrt{t'}, \sqrt{t''}, \sqrt{t'''}$ prises positivement, en sorte que l'on ait

$$\sqrt{t'} = \pm \theta', \quad \sqrt{t''} = \pm \theta'', \quad \sqrt{t'''} = \pm \theta''',$$

il faudra, lorsque $m^3 - 4mn + 8p$ est une quantité positive, prendre, ou

$$\sqrt{t'} = \theta' \quad \text{et} \quad \sqrt{t''} = \pm \theta'', \quad \sqrt{t'''} = \pm \theta''',$$

ou

$$\sqrt{t''} = \theta'' \quad \text{et} \quad \sqrt{t'} = \pm \theta', \quad \sqrt{t'''} = \pm \theta''',$$

ou

$$\sqrt{t'''} = \theta''' \quad \text{et} \quad \sqrt{t'} = \pm \theta', \quad \sqrt{t''} = \pm \theta'',$$

les signes ambigus devant être les mêmes pour les quantités $\theta'', \theta''',$ ou $\theta', \theta''',$ ou $\theta', \theta'',$ et l'on aura dans ce cas pour les quatre racines de la proposée les valeurs suivantes

$$\frac{-m + \theta' + \theta'' + \theta'''}{4},$$

$$\frac{-m + \theta' - \theta'' - \theta'''}{4},$$

$$\frac{-m - \theta' + \theta'' - \theta'''}{4},$$

$$\frac{-m - \theta' - \theta'' + \theta'''}{4}.$$

(*) Cette formule a été obtenue en extrayant la racine carrée des deux membres de la précédente, et celle-ci indique seulement que le produit des radicaux $\sqrt{t'}, \sqrt{t''}, \sqrt{t'''}$ est égal à $\pm (m^3 - 4mn + 8p)$. Lagrange remplace le signe ambigu \pm par $+$, mais c'est le signe $-$ qu'il fallait prendre; en effet, les radicaux $\sqrt{t'}, \sqrt{t''}, \sqrt{t'''}$ représentent les valeurs des quantités

$$a + b - c - d, \quad a + c - b - d, \quad a + d - b - c,$$

qui ont pour produit la fonction symétrique

$$(a + b + c + d)^3 - 4(a + b + c + d)(ab + ac + ad + bc + bd + cd) + 8(abc + abd + acd + bcd),$$

dont la valeur est $-m^3 + 4mn - 8p$. On a donc

$$\sqrt{t'} \sqrt{t''} \sqrt{t'''} = -m^3 + 4mn - 8p,$$

quels que soient les coefficients m, n, p , réels ou imaginaires. Cette relation détermine complètement dans tous les cas l'un des radicaux $\sqrt{t'}, \sqrt{t''}, \sqrt{t'''}$ quand les valeurs des deux autres ont été fixées.

(Note de l'Éditeur.)

Au contraire, si $m^3 - 4mn + 8p$ est une quantité négative, il faudra alors prendre, ou

$$\sqrt{t'} = -\theta' \text{ et } \sqrt{t''} = \pm\theta'', \quad \sqrt{t'''} = \pm\theta''',$$

ou

$$\sqrt{t''} = -\theta'' \text{ et } \sqrt{t'} = \pm\theta', \quad \sqrt{t'''} = \pm\theta''',$$

ou

$$\sqrt{t'''} = -\theta''' \text{ et } \sqrt{t'} = \pm\theta', \quad \sqrt{t''} = \pm\theta'';$$

ce qui donnera, pour les quatre racines cherchées, ces valeurs

$$\frac{-m + \theta' + \theta'' - \theta'''}{4},$$

$$\frac{-m + \theta' - \theta'' + \theta'''}{4},$$

$$\frac{-m - \theta' + \theta'' + \theta'''}{4},$$

$$\frac{-m - \theta' - \theta'' - \theta'''}{4}.$$

33. La méthode de Ferrari, que nous venons d'examiner, nous a conduits à décomposer l'équation du quatrième degré

$$x^4 + mx^3 + nx^2 + px + q = 0$$

en ces deux-ci du second degré (29)

$$x^2 + \left(\frac{m}{2} + z\right)x + y + \frac{my - p}{2z} = 0,$$

$$x^2 + \left(\frac{m}{2} - z\right)x + y - \frac{my - p}{2z} = 0,$$

de la résolution desquelles on peut tirer les quatre racines de la proposée, comme on l'a vu plus haut; on pourrait aussi obtenir cette décomposition d'une manière plus simple et plus directe, en supposant d'abord que l'équation proposée soit le produit de deux équations du second degré telles que

$$x^2 + fx + g = 0, \quad x^2 + hx + k = 0,$$

et déterminant ensuite les coefficients f, g, h, k par la comparaison des termes homologues; c'est ce qu'a fait Descartes, et ce qui a donné naissance à la méthode des indéterminées dont il est regardé comme l'auteur. Multipliant donc les deux équations précédentes l'une par l'autre, on aura celle-ci

$$x^4 + (f+h)x^3 + (fh+g+k)x^2 + (fk+gh)x + gk = 0,$$

laquelle étant comparée terme à terme avec la proposée

$$x^4 + mx^3 + nx^2 + px + q = 0$$

donnera les quatre équations

$$f+h=m, \quad fh+g+k=n, \quad fk+gh=p, \quad gk=q,$$

lesquelles serviront à déterminer les quatre inconnues f, g, h, k .

34. Supposons d'abord, avec Descartes, que le second terme de la proposée soit évanoui, c'est-à-dire que l'on ait $m=0$; on aura donc $f+h=0$ et par conséquent $h=-f$, de sorte que dans ce cas la proposée ne pourra venir que de la multiplication de deux équations telles que

$$x^2 + fx + g = 0, \quad x^2 - fx + k = 0,$$

et l'on aura alors pour la détermination des trois coefficients f, g, k les équations

$$g+k-f^2=n, \quad (k-g)f=p, \quad gk=q;$$

les deux premières donnent

$$g = \frac{n+f^2-\frac{p}{f}}{2}, \quad k = \frac{n+f^2+\frac{p}{f}}{2};$$

et, ces valeurs étant substituées dans la dernière, on aura

$$(n+f^2)^2 - \frac{p^2}{f^2} = 4q,$$

ou bien, en multipliant par f^2 et ordonnant les termes par rapport à f ,

$$f^6 + 2nf^4 + (n^2 - 4q)f^2 - p^2 = 0,$$

équation du sixième degré, mais qui est résoluble à la manière de celles du troisième, à cause qu'elle ne renferme que des puissances paires de l'inconnue.

Telle est la méthode de Descartes pour les équations du quatrième degré. Il est vrai que cet Auteur suppose d'abord que les équations composantes soient représentées par

$$x^2 + fx + \frac{f^2}{2} + \frac{n}{2} - \frac{p}{2f} = 0, \quad x^2 - fx + \frac{f^2}{2} + \frac{n}{2} + \frac{p}{2f} = 0,$$

ainsi qu'il résulte de la substitution des valeurs de g et de k trouvées ci-dessus; mais il est naturel de croire qu'il n'a trouvé ces formules que par une analyse semblable à celle que nous venons de donner, comme on peut le voir dans le *Commentaire* de Schooten et dans la Lettre de Hudde sur *la réduction des équations*.

35. Il est visible que la Solution précédente revient au même que celle des n°s 26 et suivants, et que les inconnues f et z expriment la même quantité dans les deux Solutions lorsque $m = 0$. Ainsi les principales remarques qu'on a faites sur la Solution de Ferrari pourront s'appliquer aussi à celle de Descartes, sans qu'il soit nécessaire d'entrer là-dessus dans un nouveau détail; mais il est bon, de plus, d'examiner en particulier le principe de cette dernière Solution et de chercher *à priori* les conséquences qui peuvent en résulter.

Ce principe consiste, comme nous venons de le voir, à supposer que l'équation proposée soit divisible par une équation du second degré telle que

$$x^2 + fx + g = 0,$$

c'est-à-dire qu'elle ait deux racines communes avec cette dernière. Ainsi l'on pourra trouver les conditions nécessaires pour cela par la méthode du n° 12. En effet, en divisant le quinôme

$$x^4 + mx^3 + nx^2 + px + q$$

par le trinôme

$$x^2 + fx + g,$$

on trouvera le quotient

$$x^2 + (m - f)x + n - g - f(m - f),$$

et le reste

$$[p - g(m - f) - f[n - g - f(m - f)]]x + q - g[n - g - f(m - f)],$$

de sorte que, pour que la division puisse se faire exactement, il faudra que le reste soit nul indépendamment de x , ce qui donnera ces deux équations

$$p - g(m - f) - f[n - g - f(m - f)] = 0,$$

$$q - g[n - g - f(m - f)] = 0,$$

au moyen desquelles on pourra déterminer f et g . La première de ces équations donnera d'abord

$$g = \frac{p - nf + mf^2 - f^3}{m - 2f},$$

et, cette valeur étant substituée dans la seconde, on aura

$$q - (n - mf + f^2) \frac{p - nf + mf^2 - f^3}{m - 2f} + \frac{(p - nf + mf^2 - f^3)^2}{(m - 2f)^2} = 0,$$

ou bien

$$(f^3 - mf^2 + nf - p)^2 - (f^3 - mf^2 + nf - p)(f^2 - mf + n)(2f - m) + q(2f - m)^2 = 0,$$

qui, étant ordonnée par rapport à f , sera en changeant les signes

$$f^6 - 3mf^5 + (3m^2 + 2n)f^4 - m(m^2 + 4n)f^3 + (2m^2n + mp + n^2 - 4q)f^2 - m(mp + n^2 - 4q)f + mnp - m^2q - p^2 = 0,$$

la même que celle qu'on tirerait des quatre équations de condition du n° 33.

Cette équation est, comme on voit, du sixième degré, ayant tous ses termes; mais en faisant $m = 0$ tous les termes qui renferment des puissances impaires de l'inconnue s'évanouissent, de sorte que l'équation devient résoluble à la manière de celles du troisième degré; c'est le cas

que nous avons déjà considéré dans le n° 34. Mais il n'est pas même nécessaire de supposer $m=0$ pour anéantir tous les termes où l'inconnue se trouve élevée à des puissances impaires; il suffit pour cela de faire disparaître le second terme en supposant, suivant la méthode connue,

$$f = l + \frac{3m}{6} = l + \frac{m}{2},$$

et l'on verra que tous les autres termes s'évanouiront en même temps, de sorte qu'on aura une équation en l qui ne renfermera que des puissances de l^2 , laquelle sera

$$l^6 - \left(\frac{3m^2}{4} - 2n \right) l^4 + \left(\frac{3m^4}{16} - m^2n + mp + n^2 - 4q \right) l^2 - \left(\frac{m^3}{8} - \frac{mn}{2} + p \right)^2 = 0,$$

équation qui est la même que la réduite en t du n° 32, en y faisant $t = 4l^2$, de sorte que, comme on a supposé dans le même numéro $t = s^2$ et $s = 2z$, on aura $l = z$; d'où l'on voit que la quantité $l = f - \frac{m}{2}$ dans les formules précédentes sera la même que la quantité z des n°s 27 et suivants, et cela sans supposer $m = 0$, ce qui sert à montrer d'autant mieux la liaison des solutions que nous venons d'examiner.

36. Voyons maintenant la raison pourquoi la méthode de Descartes conduit à une réduite du sixième degré telle que, en y faisant évanouir le second terme, tous ceux qui renferment des puissances impaires de l'inconnue s'évanouissent aussi, comme nous venons de le trouver; pour cela on considérera que, puisque l'équation du second degré $x^2 + fx + g = 0$ doit être un diviseur exact de la proposée dont les racines sont a, b, c, d , il faut nécessairement que la même équation renferme deux quelconques de ces quatre racines. Ainsi l'on aura

$$-f = a + b, \quad g = ab,$$

ou

$$-f = a + c, \quad g = ac,$$

ou

$$-f = a + d, \quad g = ad,$$

ou

$$-f = b + c, \quad g = bc,$$

ou

$$-f = b + d, \quad g = bd,$$

ou enfin

$$-f = c + d, \quad g = cd;$$

d'où l'on voit que l'équation en f doit être du sixième degré aussi bien que l'équation en g , c'est-à-dire du degré dont l'exposant sera égal au nombre des combinaisons de quatre choses prises deux à deux, nombre qu'on sait être $\frac{4 \cdot 3}{2} = 6$. On pourrait donc par ce moyen trouver directement tant l'équation en f que celle en g en cherchant la valeur de chacun de leurs coefficients, comme nous l'avons déjà pratiqué dans plusieurs occasions. Pour cela on représenterait d'abord l'équation en f par la forme générale

$$f^6 + Af^5 + Bf^4 + Cf^3 + Df^2 + Ef + F = 0,$$

et comme les racines de cette équation doivent être

$$-a - b, \quad -a - c, \quad -a - d, \quad -b - c, \quad -b - d, \quad -c - d,$$

on aurait

$$\begin{aligned} A &= a + b + a + c + a + d + b + b + c + b + d + c + d \\ &= 3(a + b + c + d) = -3m, \end{aligned}$$

$$\begin{aligned} B &= (a + b)(a + c + a + d + b + c + b + d + c + d) \\ &\quad + (a + c)(a + d + b + c + b + d + c + d) \\ &\quad + (a + d)(b + c + b + d + c + d) \\ &\quad + (b + c)(b + d + c + d) \\ &\quad + (b + d)(c + d) \\ &= 3(a^2 + b^2 + c^2 + d^2) + 8(ab + ac + ad + bc + bd + cd), \\ &= 3(m^2 - 2n) + 8n = 3m^2 + 2n, \end{aligned}$$

et ainsi de suite.

Maintenant, si l'on voulait faire évanouir le second terme de cette

équation en f , il faudrait, suivant la règle connue, augmenter toutes les racines de $\frac{A}{6}$, c'est-à-dire mettre, à la place de f , $f + \frac{A}{6}$, ce qui donnerait une transformée en l où

$$l = f + \frac{A}{6} = f + \frac{a + b + c + d}{2},$$

puisque

$$A = 3(a + b + c + d),$$

de sorte que les racines de cette transformée seraient

$$\frac{a + b + c + d}{2} - a - b,$$

$$\frac{a + b + c + d}{2} - a - c,$$

.....

c'est-à-dire

$$\frac{a + b - c - d}{2},$$

$$\frac{a + c - b - d}{2},$$

$$\frac{a + d - b - c}{2},$$

$$\frac{b + c - a - d}{2},$$

$$\frac{b + d - a - c}{2},$$

$$\frac{c + d - a - b}{2},$$

où l'on voit que chaque racine a sa compagne négative; en sorte que, si l'on en prend les carrés et qu'on regarde l^2 comme l'inconnue, elle ne pourra avoir que trois valeurs différentes, savoir

$$\left(\frac{a + b - c - d}{2} \right)^2,$$

$$\left(\frac{a + c - b - d}{2} \right)^2,$$

$$\left(\frac{a + d - b - c}{2} \right)^2,$$

d'où il s'ensuit que l'équation en l , étant ordonnée par rapport à l^2 , montera au troisième degré, c'est-à-dire qu'elle sera du sixième, ayant toutes les puissances de l'inconnue paires, comme nous l'avons trouvé plus haut par une autre voie : c'est à cette circonstance heureuse qu'on doit la résolution des équations du quatrième degré. On voit aussi par là la raison pourquoi, dans le numéro précédent, l'équation en l est la même que celle en z , car il est clair (32) que les valeurs de z sont les mêmes que celles que nous venons de trouver pour l .

37. On peut encore remarquer que, puisque l'on a

$$-m = a + b + c + d,$$

et que les valeurs de f sont

$$-a - b, \quad -a - c, \quad -a - d, \quad -b - c, \quad -b - d, \quad -c - d,$$

on aura les mêmes valeurs pour la quantité $m - f$; d'où il s'ensuit que l'équation en f doit être telle, qu'elle demeure la même en y substituant $m - f$ à la place de f ; donc, si l'on fait $f = \frac{m}{2} + l$, ce qui donne $m - f = \frac{m}{2} - l$, il faudra que la transformée en l soit telle, qu'elle demeure la même en y changeant l en $-l$; par conséquent elle ne devra renfermer que des puissances paires de l .

Or, si l'on substitue cette valeur de f dans l'expression de g du n° 35, on a

$$g = \frac{l^2}{2} + \frac{ml}{4} + \frac{4n - m^2}{8} + \frac{4nm - m^3 - 8p}{16l};$$

et les deux facteurs

$$x^2 + fx + g = 0, \quad x^2 + (m - f)x + n - g - f(m - f) = 0,$$

dans lesquels a été décomposée l'équation

$$x^4 + mx^3 + nx^2 + px + q = 0,$$

deviendront

$$x^2 + \left(\frac{m}{2} + l\right)x + \frac{l^2}{2} + \frac{ml}{4} + \frac{4n - m^2}{8} + \frac{4nm - m^3 - 8p}{16l} = 0,$$

$$x^2 + \left(\frac{m}{2} - l\right)x + \frac{l^2}{2} - \frac{ml}{4} + \frac{4n - m^2}{8} - \frac{4nm - m^3 - 8p}{16l} = 0,$$

équations qui sont les mêmes que celles du n° 29 en faisant $l = z$ et en substituant dans ces dernières à la place de y sa valeur en z , laquelle est (28)

$$y = \frac{4z^2 + 4n - m^2}{8}.$$

Les méthodes que nous venons d'analyser renferment, si je ne me trompe, toutes les méthodes connues pour la résolution des équations du quatrième degré; il en faut seulement excepter celles de MM. Tschirnaus, Euler et Bezout, lesquelles méritent un examen particulier; c'est l'objet qu'il nous reste à remplir dans cette Section.

38. Et d'abord il est clair que pour pouvoir résoudre l'équation du quatrième degré, suivant la méthode de M. Tschirnaus, il n'est pas nécessaire de faire disparaître tous les termes intermédiaires, comme dans celles du troisième, mais qu'il suffit d'y faire disparaître le second et le quatrième terme où l'inconnue se trouve élevée à des puissances impaires; car alors on aura une équation résoluble à la manière de celles du second degré. Pour cela on prendra donc, comme on a fait pour le troisième degré (10), l'équation subsidiaire

$$x^2 = bx + a + y,$$

qui contient deux indéterminées a et b ; et éliminant par son moyen l'inconnue x de l'équation proposée

$$x^4 + mx^3 + nx^2 + px + q = 0,$$

on aura (14) une transformée en y du quatrième degré, dans laquelle le coefficient de y^3 sera une fonction de a et b de la première dimension, celui de y^2 une fonction de a et b de la seconde dimension, celui de y

une fonction de a et b de la troisième dimension, etc. De sorte que, pour faire disparaître à la fois le second et le quatrième terme, il faudra déterminer les quantités a et b en sorte qu'elles satisfassent à deux équations, l'une du premier degré et l'autre du troisième, ce qui donnera une réduite en a ou en b du troisième degré; d'où l'on peut conclure que la méthode de M. Tschirnaus doit aussi réussir pour le quatrième degré: c'est ce qu'on va voir maintenant par le calcul.

39. Comme nous avons jusqu'ici fait usage des lettres a, b, c, d pour représenter les quatre racines de l'équation proposée, pour éviter toute confusion nous prendrons d'autres lettres pour les coefficients de l'équation subsidiaire, et nous représenterons cette équation ainsi

$$x^2 + fx + g + y = 0.$$

Or, puisqu'il faut, par la nature de la méthode dont il s'agit (11), que cette équation ait une racine commune avec la proposée, il n'y aura qu'à faire en sorte qu'elles aient un diviseur commun où x se trouve à la première dimension. On divisera donc d'abord le quinôme

$$x^4 + mx^3 + nx^2 + px + q$$

par le trinôme

$$x^2 + fx + g + y,$$

et faisant pour un moment $g + y = g'$, on trouvera, comme ci-dessus (35), le reste

$$[p - g'(m - 2f) - nf + mf^2 - f^3] x + q - g'(n - mf + f^2) + g'^2,$$

lequel, ne contenant que la première dimension de x , devra par conséquent être le diviseur commun des deux polynômes; ainsi il faudra que ce reste divise exactement le diviseur précédent $x^2 + fx + g'$, c'est-à-dire que la valeur de x tirée de l'équation

$$[p - g'(m - 2f) - nf + mf^2 - f^3] x + q - g'(n - mf + f^2) + g'^2 = 0$$

satisfasse aussi à l'équation

$$x^2 + fx + g' = 0.$$

On aura donc

$$x = \frac{q - g'(n - mf + f^2) + g'^2}{f^3 - mf^2 + nf - p + (m - 2f)g'},$$

et substituant cette valeur dans $x^2 + fx + g' = 0$, on aura

$$\begin{aligned} & [q - g'(n - mf + f^2) + g'^2]^2 \\ & + f[q - g'(n - mf + f^2) + g'^2][f^3 - mf^2 + nf - p + (m - 2f)g'] \\ & + g'[f^3 - mf^2 + nf - p + (m - 2f)g']^2 = 0, \end{aligned}$$

où il ne s'agira plus que de remettre $g + y$ à la place de g' et de développer les termes en les ordonnant par rapport à y .

Soient, pour abréger,

$$F = f^3 - mf^2 + nf - p,$$

$$G = f^2 - mf + n,$$

$$H = 2f - m,$$

et l'équation précédente deviendra

$$(q - Gg' + g'^2)^2 + f(q - Gg' + g'^2)(F - Hg') + g'(F - Hg')^2 = 0,$$

laquelle étant d'abord ordonnée par rapport à g' devient

$$\begin{aligned} & g'^4 - (2G + fH - H^2)g'^3 + (G^2 + 2q + fF + fGH - 2FH)g'^2 \\ & - (2qG + fqH + fFG - F^2)g' + q^2 + qfF = 0, \end{aligned}$$

et en remettant les valeurs de F , G , H ,

$$\begin{aligned} & g'^4 - (mf + 2n - m^2)g'^3 + [nf^2 - (mn - 3p)f + n^2 - 2mp + 2q]g'^2 \\ & - [pf^3 - (mp - 4q)f^2 + (np - 3mq)f - p^2 + 2nq]g' \\ & + q(f^4 - mf^3 + nf^2 - pf + q) = 0. \end{aligned}$$

Faisons maintenant

$$A = mf + 2n - m^2,$$

$$B = nf^2 - (mn - 3p)f + n^2 - 2mp + 2q,$$

$$C = pf^3 - (mp - 4q)f^2 + (np - 3mq)f - p^2 + 2nq,$$

$$D = q(f^4 - mf^3 + nf^2 - pf + q),$$

pour avoir l'équation

$$g'^4 - Ag'^3 + Bg'^2 - Cg' + D = 0,$$

et remettant maintenant $g + y$ à la place de g' , on aura, après avoir ordonné les termes par rapport à y , cette transformée

$$y^4 + (4g - A)y^3 + (6g^2 - 3gA + B)y^2 + (4g^3 - 3Ag^2 + 2Bg - C)y + g^4 - Ag^3 + Bg^2 - Cg + D = 0,$$

dans laquelle on est maître de faire évanouir deux termes à volonté en déterminant convenablement les quantités f et g .

Faisons donc évanouir, comme nous nous le sommes proposé, le second et le quatrième terme; on aura pour cet effet les équations

$$4g - A = 0, \\ 4g^3 - 3Ag^2 + 2Bg - C = 0,$$

dont la première donne

$$g = \frac{A}{4},$$

ce qui étant substitué dans la seconde, on aura, en ôtant les fractions,

$$A^3 - 4AB + 8C = 0,$$

équation qui, en remettant pour A , B , C leurs valeurs en f , montera au troisième degré, et deviendra, après avoir ordonné les termes,

$$(m^3 - 4mn + 8p)f^3 - (3m^4 - 14m^2n + 8n^2 + 2mp - 32q)f^2 + [m^5 - 16m^3n + 20m^2p + 16m(n^2 - 2q) - 16np]f - m^6 + 6m^4n - 8m^3np - 8m^2(n^2 - q) + 8mn^2p - 8p^2 = 0.$$

Ayant donc déterminé f par cette équation, l'équation en y deviendra, à cause de $g = \frac{A}{4}$,

$$y^4 - \left(\frac{3A^2}{8} - B\right)y^2 - \frac{3A^4}{256} + \frac{A^2B}{16} - \frac{AC}{4} + D = 0,$$

ou bien, en mettant à la place de C sa valeur $\frac{AB}{2} - \frac{A^3}{8}$,

$$y^4 - \left(\frac{3A^2}{8} - B\right)y^2 + \frac{5A^4}{256} - \frac{A^2B}{16} + D = 0,$$

laquelle est, comme on voit, résoluble à la manière de celles du second degré. Ainsi l'on connaîtra f et y ; après quoi on aura sur-le-champ

$$x = \frac{q - (n - mf + f^2) \left(\frac{A}{4} + y \right) + \left(\frac{A}{4} + y \right)^2}{f^3 - mf^2 + nf - p + (m - 2f) \left(\frac{A}{4} + y \right)};$$

et les quatre valeurs de y tirées de l'équation précédente donneront toujours les quatre mêmes racines de la proposée, quelle que soit la racine f qu'on emploie; ce qu'on pourrait démontrer, s'il en était besoin, d'une manière analogue à celle du n° 28.

40. Si l'on voulait savoir *à priori* pourquoi la réduite en f que nous venons de trouver ci-dessus est nécessairement du troisième degré, il faudrait chercher quelle fonction des racines a, b, c, d doit être la valeur de f . Pour cela on reprendra l'équation subsidiaire

$$x^2 + fx + g + y = 0,$$

et l'on y substituera successivement a, b, c, d à la place de x , et à la place de y les quatre racines de l'équation en y ci-dessus; mais il n'est pas nécessaire de connaître la valeur de ces dernières racines, il suffit de considérer que, comme l'équation ne contient aucune puissance impaire de y , ses racines doivent être deux à deux égales et de signes contraires; en sorte qu'on pourra les représenter par $y', -y', y'', -y''$. Faisant donc ces substitutions dans l'équation $x^2 + fx + g + y = 0$, on aura ces quatre-ci

$$a^2 + fa + g + y' = 0,$$

$$b^2 + fb + g - y' = 0,$$

$$c^2 + fc + g + y'' = 0,$$

$$d^2 + fd + g - y'' = 0;$$

d'où, chassant d'abord y' et y'' , on tire

$$a^2 + b^2 + f(a + b) + 2g = 0,$$

$$c^2 + d^2 + f(c + d) + 2g = 0,$$

et chassant ensuite g , on aura

$$f = -\frac{a^2 + b^2 - c^2 - d^2}{a + b - c - d}.$$

Or, pour avoir toutes les valeurs de f , il n'y aura qu'à faire entre les quatre racines a, b, c, d toutes les permutations possibles, et l'on n'obtiendra que ces trois valeurs différentes

$$\frac{a^2 + b^2 - c^2 - d^2}{a + b - c - d},$$

$$\frac{a^2 + c^2 - b^2 - d^2}{a + c - b - d},$$

$$\frac{a^2 + d^2 - b^2 - c^2}{a + d - b - c},$$

qui seront les racines de la réduite en y , laquelle ne pourra être par conséquent que du troisième degré. On pourrait même remonter de là à l'équation en y , comme nous l'avons déjà pratiqué plusieurs fois; et l'on trouverait la même équation qu'on a vue ci-dessus.

Au reste, pour pouvoir mieux comparer la réduite en f dont nous parlons, avec celles que nous avons trouvées plus haut d'après les solutions de Ferrari et de Descartes, on remarquera que

$$a^2 + b^2 - c^2 - d^2 = \frac{(a + b)^2 - (c + d)^2 + (a - b)^2 - (c - d)^2}{2};$$

or

$$\begin{aligned} (a + b)^2 - (c + d)^2 &= (a + b + c + d)(a + b - c - d) \\ &= -m(a + b - c - d), \end{aligned}$$

et

$$(a - b)^2 - (c - d)^2 = (a + c - b - d)(a + d - b - c);$$

mais on trouve par le calcul

$$(a + b - c - d)(a + c - b - d)(a + d - b - c) = -m^3 + 4mn - 8p,$$

donc on aura

$$a^2 + b^2 - c^2 - d^2 = \frac{1}{2} \left[-m(a + b - c - d) - \frac{m^3 - 4mn + 8p}{a + b - c - d} \right];$$

par conséquent

$$f = -\frac{a^2 + b^2 - c^2 - d^2}{a + b - c - d} = \frac{m}{2} + \frac{m^3 - 4mn + 8p}{2(a + b - c - d)^2}.$$

Or nous avons trouvé (32) que la réduite en t a pour racines les différentes valeurs de $(a + b - c - d)^2$; donc on aura, en général,

$$f = \frac{m}{2} + \frac{m^3 - 4mn + 8p}{2t},$$

d'où l'on voit que la réduite en f n'est autre chose qu'une transformation de la réduite en t du numéro cité.

41. Après avoir vu comment la méthode de Tschirnhaus peut s'appliquer aux équations du quatrième degré en faisant évanouir deux termes de la proposée, il ne sera pas inutile de voir encore ce qui en résulterait si l'on voulait faire évanouir à la fois tous les termes intermédiaires, comme on a fait pour le troisième degré.

On aurait donc trois termes à faire disparaître, savoir le second, le troisième et le quatrième, ce qui exigerait une équation subsidiaire qui contient trois indéterminées, et qui fût de cette forme

$$x^3 + fx^2 + gx + h + y = 0.$$

On éliminerait donc x par le moyen de cette équation et de la proposée

$$x^4 + mx^3 + nx^2 + px + q = 0,$$

et l'on aurait une transformée en y du quatrième degré, telle que

$$y^4 + A y^3 + B y^2 + C y + D = 0,$$

dans laquelle il faudrait supposer $A = 0$, $B = 0$, $C = 0$, pour avoir l'équation à deux termes

$$y^4 + D = 0.$$

Or, de ce que nous avons démontré, en général, dans le n° 14, il s'ensuit que A sera une fonction d'une dimension des trois indéterminées f , g , h , que B sera une fonction de deux dimensions, et C une fonction de

trois dimensions des mêmes quantités; de sorte que l'on aura, pour la détermination des inconnues f, g, h , ces trois équations

$$A = 0, \quad B = 0, \quad C = 0,$$

dont la première sera du premier degré, la seconde du second, et la troisième du troisième degré; d'où il est facile de voir qu'on aura par l'élimination une équation finale en f , ou g , ou h , qui sera du degré 1.2.3, c'est-à-dire du sixième. Il paraît donc par là que la méthode dont il s'agit ne saurait réussir, puisqu'elle conduit à une réduite d'un degré supérieur à la proposée; mais il pourrait se faire que cette réduite du sixième degré pût s'abaisser à un degré inférieur; c'est ce qu'il est bon d'examiner *à priori* avant d'entreprendre le calcul que nous venons d'indiquer.

42. Pour cet effet il faut chercher quelle fonction des racines a, b, c, d devra être l'indéterminée f , par exemple, pour que la transformée en y se réduise à la forme

$$y^4 + D = 0.$$

Or cette équation en y donne ces quatre racines (25)

$$y = \pm \sqrt[4]{-D},$$

$$y = \pm \sqrt{-1} \sqrt[4]{-D};$$

ainsi, en faisant pour plus de simplicité $\sqrt[4]{-D} = k$, il n'y aura qu'à mettre successivement dans l'équation subsidiaire

$$x^3 + fx^2 + gx + h + y = 0,$$

a, b, c, d à la place de x , et $k, -k, k\sqrt{-1}, -k\sqrt{-1}$ à la place de y , et l'on aura ces quatre-ci

$$a^3 + a^2f + ag + h + k = 0,$$

$$b^3 + b^2f + bg + h - k = 0,$$

$$c^3 + c^2f + cg + h + k\sqrt{-1} = 0,$$

$$d^3 + d^2f + dg + h - k\sqrt{-1} = 0,$$

d'où l'on pourra tirer les valeurs de f, g, h et k .

Si l'on ajoute ensemble les deux premières et les deux dernières, on aura ces deux-ci

$$a^3 + b^3 + (a^2 + b^2)f + (a + b)g + 2h = 0,$$

$$c^3 + d^3 + (c^2 + d^2)f + (c + d)g + 2h = 0,$$

qui, étant retranchées l'une de l'autre, donnent

$$a^3 + b^3 - c^3 - d^3 + (a^2 + b^2 - c^2 - d^2)f + (a + b - c - d)g = 0,$$

où il n'y a plus que deux inconnues f et g .

Qu'on retranche maintenant les deux premières l'une de l'autre, comme aussi les deux dernières, on aura ces deux-ci

$$a^3 - b^3 + (a^2 - b^2)f + (a - b)g + 2k = 0,$$

$$c^3 - d^3 + (c^2 - d^2)f + (c - d)g + 2k\sqrt{-1} = 0,$$

dont la seconde étant multipliée par $\sqrt{-1}$, et ensuite ajoutée à la première, on aura

$$a^3 - b^3 + (c^3 - d^3)\sqrt{-1} + [a^2 - b^2 + (c^2 - d^2)\sqrt{-1}]f + [a - b + (c - d)\sqrt{-1}]g = 0,$$

équation qui, étant combinée avec celle qu'on a trouvée ci-dessus, servira à déterminer f et g .

Chassant g , on aura une équation en f qui donnera

$$f = -\frac{(a^3 + b^3 - c^3 - d^3)[a - b + (c - d)\sqrt{-1}] - [a^3 - b^3 + (c^3 - d^3)\sqrt{-1}](a + b - c - d)}{(a^2 + b^2 - c^2 - d^2)[a - b + (c - d)\sqrt{-1}] - [a^2 - b^2 + (c^2 - d^2)\sqrt{-1}](a + b - c - d)},$$

d'où l'on pourra déduire facilement toutes les différentes valeurs dont la quantité f est susceptible, en faisant toutes les permutations possibles entre les quatre racines a, b, c, d . De cette manière, si l'on fait, pour abréger,

$$M = (a^3 + b^3 - c^3 - d^3)(a - b) - (a^3 - b^3)(a + b - c - d),$$

$$N = (a^3 + b^3 - c^3 - d^3)(c - d) - (c^3 - d^3)(a + b - c - d),$$

$$P = (a^2 + b^2 - c^2 - d^2)(a - b) - (a^2 - b^2)(a + b - c - d),$$

$$Q = (a^2 + b^2 - c^2 - d^2)(c - d) - (c^2 - d^2)(a + b - c - d),$$

$$\begin{aligned}
 M' &= (a^3 + c^3 - b^3 - d^3)(a - c) - (a^3 - c^3)(a + c - b - d), \\
 N' &= (a^3 + c^3 - b^3 - d^3)(b - d) - (b^3 - d^3)(a + c - b - d), \\
 P' &= (a^2 + c^2 - b^2 - d^2)(a - c) - (a^2 - c^2)(a + c - b - d), \\
 Q' &= (a^2 + c^2 - b^2 - d^2)(b - d) - (b^2 - d^2)(a + c - b - d), \\
 M'' &= (a^3 + d^3 - b^3 - c^3)(a - d) - (a^3 - d^3)(a + d - b - c), \\
 N'' &= (a^3 + d^3 - b^3 - c^3)(b - c) - (b^3 - d^3)(a + d - b - c), \\
 P'' &= (a^2 + d^2 - b^2 - c^2)(a - d) - (a^2 - d^2)(a + d - b - c), \\
 Q'' &= (a^2 + d^2 - b^2 - c^2)(b - c) - (b^2 - c^2)(a + d - b - c),
 \end{aligned}$$

on trouvera les six valeurs suivantes

$$\begin{aligned}
 &-\frac{M + N\sqrt{-1}}{P + Q\sqrt{-1}}, \quad -\frac{M - N\sqrt{-1}}{P - Q\sqrt{-1}}, \\
 &-\frac{M' + N'\sqrt{-1}}{P' + Q'\sqrt{-1}}, \quad -\frac{M' - N'\sqrt{-1}}{P' - Q'\sqrt{-1}}, \\
 &-\frac{M'' + N''\sqrt{-1}}{P'' + Q''\sqrt{-1}}, \quad -\frac{M'' - N''\sqrt{-1}}{P'' - Q''\sqrt{-1}},
 \end{aligned}$$

qui seront donc les racines de l'équation en f ; d'où l'on voit que cette équation montera en effet au sixième degré, comme nous l'avons déjà conclu par une autre voie.

43. Il s'agit maintenant de voir si cette équation du sixième degré peut s'abaisser à un degré inférieur; or c'est ce qui doit avoir lieu en effet, comme je vais le prouver, d'après la forme que je viens de trouver pour les six racines de l'équation en question. Car supposons que les deux racines

$$-\frac{M + N\sqrt{-1}}{P + Q\sqrt{-1}} \quad \text{et} \quad -\frac{M - N\sqrt{-1}}{P - Q\sqrt{-1}}$$

soient représentées par l'équation du second degré

$$f^2 + tf + u = 0,$$

on aura donc par la nature des équations

$$t = \frac{M + N\sqrt{-1}}{P + Q\sqrt{-1}} + \frac{M - N\sqrt{-1}}{P - Q\sqrt{-1}} \quad \text{et} \quad u = \frac{M + N\sqrt{-1}}{P + Q\sqrt{-1}} \times \frac{M - N\sqrt{-1}}{P - Q\sqrt{-1}},$$

c'est-à-dire

$$t = \frac{2(MP + NQ)}{P^2 + Q^2} \quad \text{et} \quad u = \frac{M^2 + N^2}{P^2 + Q^2}.$$

Or je dis que les quantités t et u ne peuvent dépendre que d'équations du troisième degré telles que

$$t^3 - Et^2 + Ft - G = 0, \\ u^3 - Hu^2 + Ku - L = 0,$$

les coefficients E, F, G, H, K, L étant des fonctions rationnelles des coefficients m, n, p, q de la proposée. De sorte que, nommant t', t'', t''' les trois racines de la première équation, et u', u'', u''' les racines correspondantes de la seconde, on aura ces trois équations en f

$$f^2 + t'f + u' = 0, \\ f^2 + t''f + u'' = 0, \\ f^2 + t'''f + u''' = 0,$$

dans lesquelles pourra se décomposer l'équation du sixième degré en f dont nous venons de parler.

Pour démontrer cette proposition, il n'y a qu'à chercher de combien de valeurs différentes sont susceptibles les quantités t et u , c'est-à-dire les fonctions

$$\frac{MP + NQ}{P^2 + Q^2} \quad \text{et} \quad \frac{M^2 + N^2}{P^2 + Q^2}$$

des racines a, b, c, d de la proposée, en supposant que l'on fasse entre ces racines toutes les permutations possibles; car il est clair que les valeurs qui en résulteront seront les racines des équations en t et en u . Pour cela je remarque d'abord que le nombre total des permutations des quatre quantités a, b, c, d , doit être, suivant les règles connues, $4 \cdot 3 \cdot 2 \cdot 1 = 24$; de sorte que, généralement parlant, les équations en t et en u devraient monter au vingt-quatrième degré. Mais il arrive ici que parmi les permutations dont il s'agit il y en a plusieurs qui redonnent les mêmes valeurs de t et u , et qui, par conséquent, doivent être rejetées.

En effet :

1° Lorsqu'on échange a en b , il est visible que les quantités N et Q demeurent les mêmes, et que les quantités M et P changent simplement de signes, de sorte que les quantités t et u doivent demeurer les mêmes; d'où il est facile de conclure que parmi les vingt-quatre valeurs de t et de u répondant aux vingt-quatre permutations des lettres a, b, c, d , il doit y en avoir douze égales à douze autres, ce qui réduit déjà le nombre des valeurs utiles de t et u à la moitié.

2° Lorsqu'on échange c en d , les quantités M et P demeurent les mêmes, et les quantités N et Q changent simplement de signe, ce qui ne produit aucun changement dans les valeurs de t et u ; donc, comme ces permutations sont indépendantes des précédentes, il s'ensuit, par une raison semblable, que les douze valeurs de t et u se réduiront à six.

3° Enfin, si l'on échange a en c et b en d à la fois, on verra aisément que les quantités M et N se changeront l'une dans l'autre en changeant de signe, et qu'il en sera de même des quantités P et Q ; mais il est clair que ces changements ne feront point varier les quantités t et u . Ainsi, comme ces nouvelles permutations sont aussi indépendantes des précédentes, on en conclura que les six valeurs de t et u se réduiront à trois, en sorte que, parmi les vingt-quatre valeurs de t et u , il ne s'en trouvera effectivement que trois différentes entre elles, dont chacune sera répétée huit fois.

Il y a encore, à la vérité, un échange qui ne produit aucune variation dans les quantités t et u : c'est celui de a en d et b en c à la fois; mais il ne doit pas entrer en ligne de compte, parce qu'il est déjà renfermé dans les précédents.

De là on peut conclure que les équations en t et u du vingt-quatrième degré ne pourront renfermer que trois racines différentes, dont chacune en aura sept autres d'égales, de sorte que ces équations ne seront autre chose que des équations du troisième degré élevées à la huitième puissance.

44. Nous venons donc de voir *à priori* que les valeurs différentes de t ne peuvent être qu'au nombre de trois, ainsi que celles de u ; or il est

facile de trouver que ces valeurs seront, pour la quantité t ,

$$\frac{2(MP + NQ)}{P^2 + Q^2}, \quad \frac{2(M'P' + N'Q')}{P'^2 + Q'^2}, \quad \frac{2(M''P'' + N''Q'')}{P''^2 + Q''^2},$$

et pour la quantité u ,

$$\frac{M^2 + N^2}{P^2 + Q^2}, \quad \frac{M'^2 + N'^2}{P'^2 + Q'^2}, \quad \frac{M''^2 + N''^2}{P''^2 + Q''^2},$$

de sorte qu'on aura (43)

$$t' = \frac{2(MP + NQ)}{P^2 + Q^2}, \quad t'' = \frac{2(M'P' + N'Q')}{P'^2 + Q'^2}, \quad t''' = \frac{2(M''P'' + N''Q'')}{P''^2 + Q''^2},$$

et

$$u' = \frac{M^2 + N^2}{P^2 + Q^2}, \quad u'' = \frac{M'^2 + N'^2}{P'^2 + Q'^2}, \quad u''' = \frac{M''^2 + N''^2}{P''^2 + Q''^2}.$$

Effectivement, si l'on met ces valeurs dans les coefficients E, F, \dots des équations en t et en u , lesquels doivent être, comme on sait, exprimés ainsi

$$E = t' + t'' + t''', \quad F = t't'' + t't''' + t''t''', \quad G = t't''t''', \\ H = u' + u'' + u''', \quad K = u'u'' + u'u''' + u''u''', \quad L = u'u''u''',$$

on aura des fonctions de a, b, c, d , qui demeureront les mêmes, quelque permutation qu'on fasse entre les quantités a, b, c, d , et qui pourront par conséquent s'exprimer par des fonctions rationnelles des coefficients m, n, p, q de la proposée dont les quantités a, b, c, d sont les racines. De sorte qu'on pourra par ce moyen trouver directement les valeurs des coefficients dont il s'agit, comme nous l'avons déjà pratiqué plusieurs fois dans le cours de ces recherches.

Au reste, dès qu'on connaîtra les trois racines t', t'', t''' de l'équation en t , on pourra par leur moyen trouver les racines correspondantes u', u'', u''' de l'équation en u , sans être obligé de résoudre aucune équation. Car si l'on prend ces trois expressions

$$u' + u'' + u''', \\ t'u' + t''u'' + t'''u''', \\ t'^2u' + t''^2u'' + t'''^2u''',$$

et qu'on y mette à la place de t' , t'' , t''' et u' , u'' , u''' leurs valeurs ci-dessus en a , b , c , d , on verra aisément que les fonctions résultant de a , b , c , d seront telles, qu'elles ne changeront point de forme, quelque permutation qu'on y fasse entre les quantités a , b , c , d , de sorte qu'elles seront toujours exprimables par des fonctions rationnelles des coefficients m , n , p , q de l'équation proposée. Ainsi l'on pourra trouver les valeurs des expressions dont il s'agit, moyennant quoi on aura trois équations par lesquelles on déterminera aisément les trois inconnues u' , u'' , u''' . (Voyez la Section quatrième.)

45. Nous étant donc assurés *à priori* que la *réduite* du sixième degré, à laquelle doit conduire la méthode en question, pourra toujours s'abaisser au troisième, voyons maintenant le procédé du calcul que cette méthode exige. On reprendra donc l'équation subsidiaire (40)

$$x^3 + fx^2 + gx + h + y = 0,$$

et l'on cherchera par la méthode ordinaire (11) les conditions nécessaires pour que cette équation ait une racine commune avec la proposée

$$x^4 + mx^3 + nx^2 + px + q = 0.$$

On divisera donc d'abord le polynôme

$$x^4 + mx^3 + nx^2 + px + q$$

par le polynôme

$$x^3 + fx^2 + gx + h',$$

en faisant pour plus de simplicité $h' = h + y$, et, abstraction faite du quotient, on aura ce reste

$$Mx^2 + N'x + P',$$

en supposant

$$M = n - g - f(m - f),$$

$$N' = p - h' - g(m - f),$$

$$P' = q - h'(m - f).$$

On divisera maintenant le quatrinôme $x^3 + fx^2 + gx + h'$ par le trinôme

$Mx^2 + N'x + P'$, et l'on aura ce nouveau reste

$$\left(g - \frac{P' + N'f}{M} + \frac{N'^2}{M^2}\right)x + h' - \frac{P'f}{M} + \frac{N'P'}{M^2} = 0;$$

qui, ne renfermant que la première puissance de x , devra par conséquent être le diviseur commun cherché. Faisant donc ce diviseur égal à zéro, on en tirera

$$x = - \frac{M^2h' - MP'f + N'P'}{M^2g - M(P' + N'f) + N'^2},$$

valeur qui, étant substituée dans l'équation

$$Mx^2 + N'x + P' = 0,$$

donnera les conditions cherchées.

Faisons maintenant

$$\begin{aligned} N &= p - h - g(m - f), \\ P &= q - h(m - f), \end{aligned}$$

et, à cause de $h' = h + y$, on aura

$$\begin{aligned} N' &= N - y, \\ P' &= P - (m - f)y; \end{aligned}$$

done, substituant ces valeurs dans l'expression de x , et supposant de plus

$$\begin{aligned} Q &= M^2h - MPf + NP, \\ R &= M^2 + (Mf - N)f - P, \\ S &= M^2g - M(P + Nf) + N^2, \\ T &= Mm - 2N, \end{aligned}$$

on aura

$$x = - \frac{Q + Ry + (m - f)y^2}{S + Ty + y^2},$$

et l'équation de condition sera

$$\begin{aligned} M[Q + Ry + (m - f)y^2]^2 + (y - N)[Q + Ry + (m - f)y^2](S + Ty + y^2) \\ + [P - (m - f)y](S + Ty + y^2) = 0, \end{aligned}$$

laquelle, étant développée et ordonnée par rapport aux puissances de y , se trouvera, après les réductions, de la forme

$$y^4 + Ay^3 + By^2 + Cy + D = 0,$$

comme nous l'avons déjà montré plus haut.

Dans cette équation en y les coefficients A, B, C, D seront des fonctions rationnelles et entières des trois indéterminées f, g, h , et les dimensions de ces indéterminées ne passeront pas le premier degré dans le coefficient A , le second degré dans le coefficient B , et ainsi de suite, conformément à ce qu'on a déjà prouvé *à priori*. Ainsi, pour réduire l'équation précédente à deux termes, on fera

$$A = 0, \quad B = 0, \quad C = 0,$$

équations d'où l'on tirera d'abord les valeurs de g et h en f , et ensuite une équation finale en f qui sera du sixième degré, mais qui sera réductible au troisième, comme on l'a démontré ci-dessus; car, en divisant cette équation par une équation du second degré telle que

$$f^2 + tf + u = 0,$$

on trouvera, pour que la division puisse se faire exactement, deux équations de condition entre t et u , à l'aide desquelles on pourra d'abord déterminer u en t , et ensuite on aura une équation finale en t qui ne sera que du troisième degré. Résolvant donc cette équation du troisième degré, on connaîtra t et de là u ; après quoi on aura f par la résolution de l'équation ci-dessus du second degré, et de là g et h par des équations linéaires. Ainsi l'on connaîtra la valeur de tous les coefficients D, Q, R, S, T .

Or l'équation en y , étant réduite à celle-ci

$$y^4 + D = 0$$

par l'évanouissement des termes intermédiaires, donnera les quatre valeurs de y

$$\pm \sqrt[4]{-D} \quad \text{et} \quad \pm \sqrt[4]{-D} \sqrt{-1},$$

lesquelles, étant substituées successivement dans l'expression de x ci-

dessus, donneront les quatre racines de la proposée. Au reste, comme ce calcul conduit à des formules assez compliquées, nous nous contenterons de l'indiquer, et nous allons plutôt chercher des moyens de le simplifier.

46. Puisque la racine x est de la forme

$$x = -\frac{Q + Ry + (m - f)y^2}{S + Ty + y^2},$$

la quantité y devant être déterminée par l'équation à deux termes

$$y^4 + D = 0,$$

il est facile de voir qu'on peut réduire l'expression de x à cette forme plus simple

$$x = a + by + cy^2 + dy^3,$$

a, b, c, d étant des coefficients dépendants de Q, R, \dots . Car si l'on multiplie d'abord le haut et le bas de la fraction

$$\frac{Q + Ry + (m - f)y^2}{S + Ty + y^2}$$

par $S - Ty + y^2$, le dénominateur de la nouvelle fraction deviendra

$$(S + y^2)^2 - T^2y^2, \text{ c'est-à-dire } S^2 + (2S - T^2)y^2 + y^4,$$

et, en mettant $-D$ à la place de y^4 ,

$$S^2 - D + (2S - T^2)y^2;$$

donc, multipliant encore tant le numérateur que le dénominateur par $S^2 - D - (2S - T^2)y^2$, le nouveau dénominateur sera

$$(S^2 - D)^2 - (2S - T^2)^2y^4,$$

ou bien, à cause de $y^4 = -D$,

$$(S^2 - D)^2 + D(2S - T^2)^2,$$

où il n'y aura plus de y . Ainsi l'on pourra faire évanouir y du dénominateur de l'expression de x en le multipliant, aussi bien que le numérateur, par

$$(S - Ty + y^2)[S^2 - D - (2S - T^2)y^2];$$

or par ce moyen le numérateur deviendra un polynôme où y montera au sixième degré; donc, en y substituant $-D$ à la place de y^4 , $-Dy$ à la place de y^5 et $-Dy^2$ à celle de y^6 , il ne s'y trouvera plus que les puissances y , y^2 et y^3 , en sorte que l'expression de x sera de la forme

$$a + by + cy^2 + dy^3.$$

Maintenant, comme la substitution des valeurs de y tirées de l'équation $y^4 + D = 0$ doit donner les quatre racines x de la proposée

$$x^4 + mx^3 + nx^2 + px + q = 0,$$

on pourra regarder cette équation comme résultant de l'élimination de y dans ces deux-ci

$$x = a + by + cy^2 + dy^3 \quad \text{et} \quad y^4 + D = 0,$$

et la comparaison des termes homologues donnera quatre équations par lesquelles on pourra déterminer quatre quelconques des cinq coefficients a , b , c , d et D , le cinquième pouvant toujours être pris à volonté.

C'est la méthode que MM. Euler et Bezout ont proposée pour la résolution des équations du quatrième degré dans les Mémoires cités ci-dessus (18).

M. Euler fait $c = 1$, et il trouve par l'élimination des trois autres indéterminées a , b , d une réduite en D du troisième degré. M. Bezout, au contraire, fait d'abord $D = -1$, et il trouve une réduite en c du sixième degré résoluble à la manière des équations du troisième, parce qu'elle ne contient aucune puissance impaire de l'inconnue. M. Bezout fait voir en même temps que, si au lieu de chercher c on cherchait b ou d , on tomberait dans une réduite du vingt-quatrième degré, avec des exposants multiples de 4, et par conséquent résoluble à la manière des équations du sixième degré. Il fait voir de plus que si l'on cherche une réduite

dont bd soit la racine, elle ne sera que du troisième degré; et par là il démontre que la réduite en b ou en d ne renfermera que les difficultés du troisième degré, puisqu'elle pourra, à l'aide de l'équation en bd , se décomposer en trois équations du huitième degré avec des exposants multiples de 4, lesquelles seront par conséquent résolubles à la manière de celles du second.

Nous nous contentons d'indiquer ici ces résultats, puisque le lecteur peut aisément les trouver de lui-même s'il n'est pas à portée de consulter les Mémoires cités; mais nous allons chercher *à priori* la raison de ces résultats, comme nous l'avons pratiqué jusqu'ici.

47. Nommons x' , x'' , x''' , x^{iv} les quatre valeurs de x , c'est-à-dire les racines de la proposée, et les quatre valeurs de y tirées de l'équation $y^4 + D = 0$ étant $\pm \sqrt[4]{-D}$, $\pm \sqrt[4]{-D} \sqrt{-1}$, on aura, par la substitution successive de ces valeurs dans l'équation

$$x = a + by + cy^2 + dy^3,$$

ces quatre-ci

$$\begin{aligned} x' &= a + b\sqrt[4]{-D} + c\sqrt[4]{D^2} + d\sqrt[4]{-D^3}, \\ x'' &= a - b\sqrt[4]{-D} + c\sqrt[4]{D^2} - d\sqrt[4]{-D^3}, \\ x''' &= a + b\sqrt[4]{-D} \sqrt{-1} - c\sqrt[4]{D^2} - d\sqrt[4]{-D^3} \sqrt{-1}, \\ x^{iv} &= a - b\sqrt[4]{-D} \sqrt{-1} - c\sqrt[4]{D^2} + d\sqrt[4]{-D^3} \sqrt{-1}. \end{aligned}$$

Si l'on ajoute d'abord ensemble ces quatre équations on aura

$$x' + x'' + x''' + x^{iv} = 4a = -m,$$

d'où

$$a = \frac{-m}{4}.$$

Ensuite, si l'on fait deux sommes à part des deux premières et des deux dernières, on aura

$$x' + x'' = 2a + 2c\sqrt[4]{D^2},$$

$$x''' + x^{iv} = 2a - 2c\sqrt[4]{D^2},$$

d'où l'on tire

$$c\sqrt[4]{D^2} = c\sqrt{-D} = \frac{x' + x'' - x''' - x^{iv}}{4}.$$

Donc, faisant avec M. Euler $c = 1$, on aura

$$-D = \frac{(x' + x'' - x''' - x^{iv})^2}{16}.$$

Et il est facile de conclure de cette expression de D que l'équation en D sera effectivement du troisième degré, comme M. Euler l'a trouvé, car elle ne sera autre chose que la réduite en t trouvée plus haut (32), dans laquelle on mettrait $-16D$ à la place de t , puisqu'on a fait

$$t = s^2 = (a + b - c - d)^2,$$

a, b, c, d désignant dans ce numéro-là les quantités que nous dénotons maintenant par x', x'', x''', x^{iv} , c'est-à-dire les quatre racines de la proposée.

Mais si M. Euler, au lieu de supposer $c = 1$, avait supposé $b = 1$, sa réduite en D n'aurait plus été du troisième degré, mais elle serait montée au sixième.

Car, si des quatre équations ci-dessus on prend la différence des deux premières et la différence des deux dernières, on a ces deux-ci

$$x' - x'' = 2b\sqrt[4]{-D} + 2d\sqrt[4]{-D^3},$$

$$x''' - x^{iv} = [2b\sqrt[4]{-D} - 2d\sqrt[4]{-D^3}] \sqrt{-1},$$

d'où l'on tire

$$b\sqrt[4]{-D} = \frac{x' - x'' - (x''' - x^{iv})\sqrt{-1}}{4},$$

$$d\sqrt[4]{-D^3} = \frac{x' - x'' + (x''' - x^{iv})\sqrt{-1}}{4}.$$

De sorte qu'en faisant $b = 1$ et prenant les quatrièmes puissances on aura

$$-D = \left[\frac{x' - x'' - (x''' - x^{iv})\sqrt{-1}}{4} \right]^4,$$

quantité qui doit dépendre d'une équation du sixième degré, comme on le verra dans un moment.

48. Si l'on fait avec M. Bezout $D = -1$, on aura par les formules

précédentes

$$c = \frac{x' - x'' + x''' - x^{iv}}{4},$$

d'où l'on peut conclure d'abord que la réduite en c sera du sixième degré avec tous les exposants pairs, ainsi que cet Auteur l'a trouvé; car il est évident que la valeur de $-D$, dans l'hypothèse de M. Euler, est la même que celle de c^2 dans l'hypothèse présente, de sorte qu'en mettant $-c^2$ à la place de D dans la réduite de M. Euler on aura la réduite de M. Bezout en c , laquelle sera par conséquent du sixième degré, résoluble à la manière des équations du troisième. Au reste, cette réduite en c sera la même que celle en z du n° 29, en y substituant $-2c$ à la place de z .

Voyons maintenant quelle devra être la forme des réduites en b et en d , en faisant toujours avec M. Bezout $D = -1$. On aura dans cette hypothèse, par les formules du numéro précédent,

$$b = \frac{x' - x'' - (x''' - x^{iv}) \sqrt{-1}}{4},$$

$$d = \frac{x' - x'' + (x''' - x^{iv}) \sqrt{-1}}{4},$$

d'où l'on tirera toutes les valeurs de b et de d en faisant toutes les permutations possibles entre les quatre racines x' , x'' , x''' , x^{iv} , et l'on pourra juger, par le nombre et la forme de ces valeurs, du degré et de la nature des équations par lesquelles les quantités b et d doivent être déterminées.

Done :

1° L'équation en b sera la même que l'équation en d , puisque la valeur de d résulte de celle de b en échangeant entre elles les deux racines x'' , x^{iv} , de sorte que les valeurs de b et de d seront les racines d'une même équation;

2° Cette équation sera en général du degré $4.3.2.1$, c'est-à-dire du vingt-quatrième, puisqu'il y a autant de permutations possibles entre les quatre quantités x' , x'' , x''' , x^{iv} ;

3° Cette équation du vingt-quatrième degré aura tous les exposants multiples de 4, car il est facile de voir que, b étant une de ses racines,

$-b$, $b\sqrt{-1}$, et $-b\sqrt{-1}$ en seront aussi. En effet, prenant comme plus haut

$$b = \frac{x' - x'' - (x''' - x^{iv})\sqrt{-1}}{4},$$

il est visible que la quantité b deviendra $-b$ en échangeant x' en x'' et x''' en x^{iv} , qu'elle deviendra $b\sqrt{-1}$ en échangeant x' en x'' et x'' en x^{iv} , et qu'enfin elle deviendra $-b\sqrt{-1}$ en échangeant x' en x^{iv} et x'' en x''' . Donc il faudra que l'équation en b demeure la même en y prenant b négatif et en y mettant $\pm b\sqrt{-1}$ à la place de b , ce qui exige qu'elle ne contienne aucune puissance impaire de b ni aucune puissance pairement impaire. D'où il s'ensuit qu'en faisant $b^4 = v$ on aura une réduite en v du sixième degré. Et l'on remarquera que cette réduite en v sera la même que celle en $-D$ dans l'hypothèse de $b = 1$ (numéro précédent); car il est visible que la valeur de $-D$ est la même que celle de b^4 ci-dessus.

On pourrait démontrer ici, par une méthode semblable à celle dont nous avons fait usage dans le n° 42, que cette équation en v pourra se décomposer en trois équations du second degré au moyen d'une réduite du troisième; mais on peut le prouver d'une manière plus simple que voici.

Je fais le produit des quantités b et d , j'ai

$$bd = \frac{(x' - x'')^2 + (x''' - x^{iv})^2}{16};$$

or

$$\begin{aligned} (x' - x'')^2 + (x''' - x^{iv})^2 &= x'^2 + x''^2 + x'''^2 + x^{iv^2} - 2(x'x'' + x'''x^{iv}) \\ &= m^2 - 2n - 2(x'x'' + x'''x^{iv}), \end{aligned}$$

et il est clair que la quantité $x'x'' + x'''x^{iv}$ est la même que la quantité u du n° 30 que nous avons vu dépendre d'une équation du troisième degré; d'où il s'ensuit que l'équation en bd sera aussi du troisième degré. Et comme

$$bd = \frac{m^2 - 2n - 2u}{16},$$

on aura cette équation en bd , en substituant, dans l'équation en u du numéro cité, $\frac{m^2 - 2n - 16bd}{2}$ à la place de u .

Supposons maintenant que ρ' , ρ'' , ρ''' soient les racines de cette équation en bd , on aura (numéro cité)

$$\rho' = \frac{m^2 - 2n}{16} - \frac{x'x'' + x'''x^{iv}}{8} = bd,$$

$$\rho'' = \frac{m^2 - 2n}{16} - \frac{x'x''' + x''x^{iv}}{8},$$

$$\rho''' = \frac{m^2 - 2n}{16} - \frac{x'x^{iv} + x''x'''}{8};$$

or, si l'on multiplie ensemble les deux équations

$$x' - x'' = 2(b + d), \quad x''' - x^{iv} = 2(b - d)\sqrt{-1}$$

du n° 48, on a

$$x'x''' + x''x^{iv} - x''x''' - x'x^{iv} = 4(b^2 - d^2)\sqrt{-1};$$

donc

$$4(b^2 - d^2)\sqrt{-1} = 8(\rho''' - \rho''),$$

et, prenant les carrés,

$$b^4 - 2b^2d^2 + d^4 = -4(\rho''' - \rho'')^2;$$

mais on a déjà $bd = \rho'$; donc

$$b^4 + d^4 = 2\rho'^2 - 4(\rho''' - \rho'')^2,$$

et, à cause de $d = \frac{\rho'}{b}$,

$$b^4 + \frac{\rho'^4}{b^4} = 2\rho'^2 - 4(\rho''' - \rho'')^2;$$

donc

$$b^8 - 2[\rho'^2 - 2(\rho''' - \rho'')^2]b^4 + \rho'^4 = 0,$$

équation du huitième degré, résoluble à la manière de celles du deuxième, ce qui s'accorde avec le résultat de M. Bezout.

Au reste, il est à propos de remarquer, touchant la réduite en b , qu'en

représentant (25) par $1, \alpha, \alpha^2, \alpha^3$ les quatre racines de l'équation $x^4 - 1 = 0$, on aura

$$b = \frac{x' + \alpha x^{1v} + \alpha^2 x'' + \alpha^3 x'''}{4},$$

ou bien, ce qui revient au même, en échangeant x^{1v} en x'' , x'' en x''' et x''' en x^{1v} ,

$$b = \frac{x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x^{1v}}{4},$$

expression analogue à celle qu'on a trouvée pour la réduite du troisième degré (n°s 6 et 19), ce qui sert à faire voir l'analogie entre la résolution du quatrième degré déduite de cette dernière méthode et celle de la résolution des équations du troisième degré.

49. Si l'on reprend les équations du n° 46,

$$\begin{aligned} x &= a + by + cy^2 + dy^3, \\ y^4 + D &= 0, \end{aligned}$$

et qu'on y suppose $y^2 = z$, on aura ces deux-ci

$$\begin{aligned} x &= (a + cz) + (b + dz)\sqrt{z}, \\ z^2 + D &= 0, \end{aligned}$$

dont la première, étant délivrée de l'irrationnalité, devient

$$(x - a - cz)^2 - (b + dz)^2 z = 0,$$

laquelle, à cause de $z^2 = -D$, se réduira à cette forme

$$x^2 + (f + gz)x + h + kz = 0.$$

De cette manière on aura donc les deux équations

$$\begin{aligned} z^2 + D &= 0, \\ x^2 + (f + gz)x + h + kz &= 0, \end{aligned}$$

qui, par l'élimination de z , donneront une équation du quatrième degré comparable à la proposée

$$x^4 + mx^3 + nx^2 + px + q = 0;$$

de sorte que, par la comparaison des termes analogues, on pourra déterminer quatre des cinq coefficients f , g , h , k et D , le cinquième demeurant à volonté.

Cette méthode revient à la même que celle que M. Bezout a donnée à la fin de son Mémoire de 1762 *sur les équations*, et qu'il a redonnée dans le Mémoire de 1765, page 548, comme un exemple d'une méthode générale qui s'étend à toutes les équations dont le degré est marqué par un nombre composé. Dans le premier de ces endroits l'Auteur suppose d'abord $g = -1$, et il trouve une équation finale en k du troisième degré. Dans le second il fait $D = -1$, et il parvient à une équation finale en g du sixième degré avec des exposants pairs, et par conséquent résoluble à la manière des équations du troisième degré.

Pour voir la raison de ces résultats, il n'y a qu'à remarquer que, puisque $z = \pm\sqrt{-D}$, on aura ces deux équations

$$x^2 + (f + g\sqrt{-D})x + h + k\sqrt{-D} = 0,$$

$$x^2 + (f - g\sqrt{-D})x + h - k\sqrt{-D} = 0,$$

dont le produit doit donner l'équation proposée; de sorte qu'il faudra que l'une de ces équations renferme deux des racines de la proposée, et que l'autre en renferme les deux autres. Ainsi l'on aura, par la nature des équations,

$$-f - g\sqrt{-D} = x' + x'', \quad h + k\sqrt{-D} = x' x'',$$

$$-f + g\sqrt{-D} = x''' + x^{iv}, \quad h - k\sqrt{-D} = x''' x^{iv};$$

donc

$$-2g\sqrt{-D} = x' + x'' - x''' - x^{iv},$$

$$2k\sqrt{-D} = x' x'' - x''' x^{iv}.$$

Si l'on fait d'abord $g = -1$, et qu'on substitue la valeur de $\sqrt{-D}$ tirée de la première équation dans la seconde, on aura

$$k = \frac{x' x'' - x''' x^{iv}}{x' + x'' - x''' - x^{iv}};$$

et de là on peut conclure que l'équation en k ne sera que du troisième

degré; car, quelque permutation qu'on fasse entre les quatre racines x' , x'' , x''' , x^{iv} , on n'aura jamais que ces trois valeurs différentes de k ,

$$\frac{x'x'' - x'''x^{iv}}{x' + x'' - x''' - x^{iv}},$$

$$\frac{x'x''' - x''x^{iv}}{x' + x''' - x'' - x^{iv}},$$

$$\frac{x'x^{iv} - x''x'''}{x' + x^{iv} - x'' - x'''},$$

d'après lesquelles valeurs on pourrait, si l'on voulait, trouver directement l'équation même en k .

Si l'on fait $D = -1$, on aura

$$g = \frac{x^{iv} + x''' - x' - x''}{2},$$

en sorte que la quantité g sera la même que la quantité z du n° 29, et qu'on y pourra appliquer les conséquences trouvées au n° 32. Si, dans cette hypothèse de $D = -1$, on cherchait k au lieu de g , on aurait

$$k = \frac{x'x'' - x'''x^{iv}}{2},$$

et l'équation en k serait aussi du sixième degré avec tous ses exposants pairs, ses racines étant

$$\frac{x'x'' - x'''x^{iv}}{2}, \quad \frac{x'x''' - x''x^{iv}}{2}, \quad \frac{x'x^{iv} - x''x'''}{2},$$

$$\frac{x''x''' - x'x^{iv}}{2}, \quad \frac{x''x^{iv} - x'x'''}{2}, \quad \frac{x'''x^{iv} - x'x''}{2}.$$

Au reste, cette équation en k pourrait se dériver aisément de l'équation en u du n° 30; car puisque

$$k = \frac{x'x'' - x'''x^{iv}}{2} \quad \text{et} \quad u = x'x'' + x'''x^{iv}$$

(il faut se souvenir que x' , x'' , x''' , x^{iv} désignent ici les mêmes quantités

que a, b, c, d dans le numéro cité, c'est-à-dire les racines de la proposée), on aura

$$u^2 - 4k^2 = 4x'x''x'''x'''' = 4q;$$

done

$$u = 2\sqrt{q + k^2}.$$

Ainsi, si dans l'équation en u on substitue cette valeur, et qu'on fasse ensuite disparaître l'irrationnalité, on aura une équation en k du sixième degré, dont tous les exposants seront multiples de 2.

50. Nous terminerons ici notre analyse des méthodes qui concernent la résolution des équations du quatrième degré. Non-seulement nous avons rapproché ces méthodes les unes des autres, et montré leur liaison et leur dépendance mutuelle; nous avons encore, ce qui était le point principal, donné la raison *à priori* pourquoi elles conduisent, les unes à des *réduites* du troisième degré, les autres à des réduites du sixième, mais qui peuvent s'abaisser au troisième; et l'on a dû voir que cela vient en général de ce que les racines de ces *réduites* sont des fonctions des quantités x', x'', x''', x'''' , telles, qu'en faisant toutes les permutations possibles entre ces quatre quantités, elles ne peuvent recevoir que trois valeurs différentes comme la fonction $x'x'' + x'''x''''$, ou six valeurs, mais deux à deux égales et de signes contraires, comme la fonction $x' + x'' - x''' - x''''$, ou bien six valeurs telles, qu'en les partageant en trois couples et prenant la somme ou le produit des valeurs de chaque couple, ces trois sommes ou ces trois produits soient toujours les mêmes, quelque permutation qu'on fasse entre les quantités x', x'', x''', x'''' , comme la fonction trouvée au n° 42. C'est uniquement de l'existence de telles fonctions que dépend la résolution générale des équations du quatrième degré (*).

(*) La longueur déjà trop grande de ce Mémoire nous oblige d'en réserver la suite pour le volume de 1771, auquel il appartient naturellement. On y trouvera une Analyse générale des méthodes de MM. Tschirnhaus, Euler et Bezout, faite par des principes analogues à ceux que nous avons suivis jusqu'ici, et d'après laquelle on sera en état de connaître *à priori* les résultats qu'on doit attendre de l'application de ces méthodes aux équations qui passent le quatrième degré. On y trouvera aussi des remarques générales sur la résolution et la réduction des équations, lesquelles serviront à jeter un nouveau jour sur cette partie de l'Algèbre.

SECTION TROISIÈME.

DE LA RÉSOLUTION DES ÉQUATIONS DU CINQUIÈME DEGRÉ ET DES DEGRÉS ULTÉRIEURS.

Le Problème de la résolution des équations des degrés supérieurs au quatrième est un de ceux dont on n'a pas encore pu venir à bout, quoique d'ailleurs rien n'en démontre l'impossibilité. Je ne connais jusqu'à présent que deux méthodes qui paraissent donner quelque espérance de succès. Ce sont, l'une celle de M. Tschirnaus, publiée dans les *Actes de Leipsic* de 1683, et l'autre celle que MM. Euler et Bezout ont proposée presque en même temps, le premier dans les *Nouveaux Commentaires de Pétersbourg*, tome IX, et le second dans les *Mémoires de l'Académie des Sciences de Paris* pour l'année 1765. Ces méthodes ont l'avantage de donner la résolution des équations du troisième et du quatrième degré d'une manière générale et uniforme, comme on l'a vu dans les Sections précédentes, avantage qui leur est particulier, et qui peut par conséquent être un préjugé pour leur succès dans les degrés plus élevés; mais les calculs qu'elles demandent dans les équations du cinquième degré et des degrés ultérieurs sont si longs et si compliqués, que le plus intrépide calculateur peut en être rebuté. En effet, pour appliquer, par exemple, la méthode de M. Tschirnaus au cinquième degré, il faudra résoudre quatre équations qui renferment quatre inconnues, et dont la première est du premier degré, la seconde du second, et ainsi de suite; de sorte que l'équation résultante de l'élimination de trois de ces inconnues doit monter, en général, au degré dont l'exposant sera 1. 2. 3. 4, c'est-à-dire au vingt-quatrième degré. Or, indépendamment du travail immense qui sera nécessaire pour parvenir à cette équation, il est clair que quand on l'aura trouvée on n'en sera guère plus avancé, à moins qu'on ne puisse la réduire à un degré moindre que le cinquième, réduction qui, si elle est possible, ne pourra être que le fruit d'un nouveau travail plus considérable que le premier.

Suivant la méthode de M. Euler, on parviendra aussi nécessairement à

une réduite du vingt-quatrième degré; car quoique cette méthode paraisse promettre une réduite du quatrième degré seulement, par la raison qu'elle ne donne pour le troisième degré qu'une réduite du second, et pour le quatrième degré qu'une réduite du troisième; cependant M. Bezout remarque avec raison que c'est une simplification accidentelle qui, dans le quatrième degré, rabaisse la réduite de M. Euler au troisième degré, laquelle doit être, en général, du degré 2.3, c'est-à-dire du sixième, et que cette simplification n'a lieu que parce que l'exposant 4 est un nombre composé. Nous en avons donné la raison *à priori* dans la Section précédente, et nous y avons aussi fait voir que M. Euler serait nécessairement tombé dans une réduite du sixième degré s'il avait cherché à déterminer par l'élimination une des deux autres inconnues qui entrent dans ses formules. Ainsi l'on n'a d'avance aucun fondement d'attendre, pour le cinquième degré, une réduite d'un degré moindre que le vingt-quatrième, par la méthode de M. Euler; et si cette équation est susceptible de quelque réduction, ce ne sera qu'à l'aide d'un grand nombre de tentatives et de calculs très-laborieux qu'on pourra s'en assurer.

Ces inconvénients doivent avoir lieu de même dans la méthode de M. Bezout, qui ne diffère point de celle de M. Euler, si ce n'est qu'elle donne des réduites plus élevées en apparence, les exposants y étant tous des multiples de l'exposant du degré de l'équation proposée. Ainsi, dans le cinquième degré, on a, d'après la méthode de M. Bezout, une réduite du cent vingtième degré avec des exposants multiples de 5; de sorte qu'elle équivaut à une équation du vingt-quatrième degré.

Ce savant Auteur pense à la vérité que cette réduite du cent vingtième degré, regardée comme une équation du vingt-quatrième degré, ne doit renfermer que les difficultés des degrés inférieurs au cinquième, et ses raisons sont: 1^o que l'expression des racines des équations du cinquième degré ne peut renfermer d'autres radicaux que ceux de ce degré et des degrés inférieurs; 2^o que par conséquent les racines de la réduite de ce degré ne doivent renfermer que les mêmes espèces de radicaux, c'est-à-dire des radicaux cinquièmes, quatrièmes, etc.; 3^o que comme les racines de la réduite du cent vingtième degré doivent être les racines cin-

quièmes de celles d'une équation du vingt-quatrième degré, les radicaux cinquièmes seront mis en évidence par là, en sorte que les racines de cette équation du vingt-quatrième degré ne pourront plus renfermer que des radicaux inférieurs, et qu'ainsi sa résolution ne devra dépendre que des degrés inférieurs au cinquième. Mais cette conclusion, si j'ose le dire, me paraît un peu forcée, car j'avoue que je ne vois pas bien clairement ce qui pourrait empêcher que l'expression des racines de l'équation du vingt-quatrième degré dont il s'agit ne contînt encore des radicaux cinquièmes; du moins il n'est pas démontré que cela ne puisse absolument avoir lieu; ainsi il pourrait bien arriver que cette équation du vingt-quatrième degré renfermât encore toutes les difficultés de l'équation proposée du cinquième degré; auquel cas, après avoir trouvé cette équation par des calculs très-pénibles, on n'en serait que plus éloigné de la résolution de l'équation proposée.

Il résulte de ces réflexions qu'il est très-douteux que les méthodes dont nous venons de parler puissent donner la résolution complète des équations du cinquième degré, et à plus forte raison celle des degrés supérieurs; et cette incertitude, jointe à la longueur des calculs que ces méthodes exigent, doit rebuter d'avance tous ceux qui pourraient être tentés d'en faire usage pour résoudre un des Problèmes les plus célèbres et les plus importants de l'Algèbre. Aussi voyons-nous que les Auteurs mêmes de ces méthodes se sont contentés d'en faire l'application au troisième et au quatrième degré, et que personne n'a encore entrepris de pousser leur travail plus loin.

Il serait donc fort à souhaiter que l'on pût juger *à priori* du succès que l'on peut se promettre dans l'application de ces méthodes aux degrés supérieurs au quatrième; nous allons tâcher d'en donner les moyens par une analyse semblable à celle dont nous nous sommes servis jusqu'ici à l'égard des méthodes connues pour la résolution des équations du troisième et du quatrième degré.

51. Considérons en général l'équation du $\mu^{ième}$ degré

$$(a) \quad x^\mu + mx^{\mu-1} + nx^{\mu-2} + px^{\mu-3} + \dots = 0.$$

Suivant la méthode de M. Tschirnhaus on prendra une équation subsitaire, telle que

$$(b) \quad x^\mu + fx^{\mu-1} + gx^{\mu-2} + \dots + y = 0,$$

qui contient ρ indéterminées f, g, \dots avec une nouvelle inconnue y ; on éliminera par le moyen de ces deux équations l'inconnue x , et l'on aura une transformée en y qui sera du même degré μ que la proposée, et qui aura cette forme

$$(c) \quad y^\mu + A y^{\mu-1} + B y^{\mu-2} + C y^{\mu-3} + \dots = 0,$$

où les coefficients A, B, C, \dots seront des fonctions rationnelles et entières des coefficients indéterminés, f, g, \dots , et où l'on aura, en particulier, A égal à une fonction de la première dimension, B égal à une fonction de la seconde dimension, et ainsi de suite (14).

Or, ayant ρ indéterminées, on pourra par leur moyen faire évanouir, dans la transformée en y , ρ termes à volonté, ou bien établir entre ces termes telles relations qu'on voudra, dépendantes de ρ équations, et par là rendre l'équation en y résoluble, ou au moins réductible à une équation de degré inférieur. La résolution de cette équation en y donnera sur-le-champ celle de l'équation proposée en x , car nous avons démontré (11) que l'équation en y renferme les conditions nécessaires pour que les deux équations d'où l'on a éliminé x aient une racine commune; de sorte que la valeur de x ne pourra être que la racine commune aux deux équations (a) et (b), qu'on trouvera en cherchant leur plus grand commun diviseur et l'égalant à zéro.

On fera pour cela l'opération ordinaire, qu'on continuera jusqu'à ce qu'on parvienne à un reste où x ne soit plus que linéaire: ce reste sera le diviseur cherché; ou bien, ce qui revient au même, on éliminera successivement des deux équations précédentes les puissances de x , jusqu'à ce qu'on arrive à une équation qui ne renferme que la première puis-

sance de x , et il est aisé de prouver que cette équation sera de la forme

$$F + Gy + Hy^2 + \dots + Ky^\lambda + (L + My + Ny^2 + \dots + Ry^\lambda)x = 0;$$

d'où l'on aura

$$(d) \quad x = -\frac{F + Gy + Hy^2 + \dots + Ky^\lambda}{L + My + Ny^2 + \dots + Ry^\lambda},$$

λ étant égal à $\frac{\mu}{2}$ si μ est pair, et égal à $\frac{\mu-1}{2}$ si μ est impair.

De cette manière on aura donc x exprimé par une fonction rationnelle de y , de sorte que si l'on connaît toutes les μ valeurs de y , on aura par leur substitution successive les μ valeurs correspondantes de x qui seront les racines de la proposée.

52. Cette méthode est, comme on voit, très-simple et très-générale; mais la difficulté est de pouvoir déterminer les indéterminées f, g, h, \dots , en sorte que la transformée en y soit résoluble.

La supposition la plus naturelle et en même temps la plus générale qu'on puisse faire pour cet objet, c'est d'égaler à zéro les coefficients A, B, \dots de tous les termes intermédiaires; en sorte que l'équation en y se réduise à cette forme

$$y^\mu + V = 0,$$

dont on peut toujours avoir immédiatement une ou deux racines suivant que μ est impair, ou pair, et dont les autres racines ne dépendent plus que d'une équation du degré $\frac{\mu-1}{2}$ ou $\frac{\mu-2}{2}$ (21), outre qu'on peut aussi les déterminer toutes directement par la division de la circonference du cercle (23).

Il faudra donc prendre dans ce cas $\rho = \mu - 1$ pour avoir autant d'indéterminées que d'équations à remplir, et l'on tombera, en général, dans une équation finale du degré $1.2.3 \dots (\mu - 1)$, comme on l'a prouvé dans le n° 14.

Si l'exposant μ est un nombre composé, en sorte que l'on ait $\mu = \nu\varpi$, il est clair qu'on pourra, en faisant $y^\varpi = z$ et faisant disparaître tous les termes de l'équation en y dont l'exposant ne sera pas divisible par ϖ , réduire cette équation en une équation en z du degré inférieur ν . On aura

donc, dans ce cas, $\nu(\varpi - 1)$ termes à faire disparaître; par conséquent il faudra prendre $\rho = \nu(\varpi - 1)$ pour avoir autant d'indéterminées, et de ce qu'on a démontré dans le n° 14 il est facile de conclure que l'équation finale qu'on aura dans ce cas sera, en général, du degré marqué par le nombre

$$1.2.3\dots(\varpi - 1)(\varpi + 1)(\varpi + 2)\dots(2\varpi - 1)(2\varpi + 1)(2\varpi + 2)\dots(3\varpi - 1)\dots(\nu\varpi - 1),$$

c'est-à-dire du degré

$$\frac{1.2.3.4\dots(\mu - 1)}{\varpi.2\varpi.3\varpi\dots(\nu - 1)\varpi},$$

ou bien de celui-ci

$$\frac{\nu(\nu + 1)(\nu + 2)\dots(\mu - 1)}{\varpi^{\nu-1}}.$$

Tels seront donc les degrés auxquels pourront monter les réduites qu'il faudra résoudre lorsqu'on voudra faire usage de la méthode de M. Tschirnhaus; mais il peut se faire que ces réduites soient telles qu'elles puissent s'abaisser à des degrés moindres: c'est ce qu'il serait comme impossible de reconnaître *à posteriori*, c'est-à-dire par la forme même de ces réduites, mais on pourra s'en assurer *à priori* par la considération de leurs racines, regardées comme des fonctions de celles de l'équation proposée, et de l'équation transformée en y , ainsi qu'on va le voir.

53. Désignons, en général, par x' , x'' , x''' , x^{iv} , ... les μ racines de l'équation proposée

$$x^\mu + mx^{\mu-1} + nx^{\mu-2} + \dots = 0,$$

et par y' , y'' , y''' , ... les μ racines de la transformée

$$y^\mu + A y^{\mu-1} + B y^{\mu-2} + \dots + V = 0;$$

substituant successivement ces racines dans l'équation subsidiaire

$$x^\mu + fx^{\mu-1} + gx^{\mu-2} + hx^{\mu-3} + \dots + l + y = 0,$$

on aura μ équations particulières par lesquelles on pourra déterminer les coefficients indéterminés f , g , h , ...; et comme chacune des racines y' , y'' , y''' , ... peut répondre également à chacune des racines x' , x'' , x''' , ...;

il s'ensuit que les inconnues f, g, h, \dots seront susceptibles de différentes valeurs, qu'on trouvera toutes en faisant toutes les combinaisons possibles des racines x', x'', x''', \dots avec les racines y', y'', y''', \dots . C'est par le nombre et la forme de ces différentes valeurs d'une même inconnue qu'on pourra juger du degré et de la nature de l'équation par laquelle elle doit être déterminée.

54. Supposons d'abord que tous les termes intermédiaires de la transformée en y doivent disparaître, en sorte qu'elle se réduise à la forme

$$y^\mu + V = 0;$$

pour cela il faudra faire dans l'équation subsidiaire $\rho = \mu - 1$ pour avoir $\mu - 1$ indéterminées (52), et comme l'équation $y^\mu + V = 0$ donne [en supposant pour plus de simplicité

$$u = \sqrt[\mu]{-V}$$

et désignant par $1, \alpha, \alpha^2, \dots, \alpha^{\mu-1}$ les racines de l'équation $y^\mu - 1 = 0$ (24)]; les racines $u, \alpha u, \alpha^2 u, \dots, \alpha^{\mu-1} u$, on aura, en prenant ces racines pour y', y'', y''', \dots et les substituant, ainsi que les racines x', x'', x''', \dots , dans l'équation subsidiaire, on aura, dis-je, ces μ équations

$$(e) \quad \left\{ \begin{array}{l} x'^{\mu-1} + fx'^{\mu-2} + gx'^{\mu-3} + \dots + l + u = 0, \\ x''^{\mu-1} + fx''^{\mu-2} + gx''^{\mu-3} + \dots + l + \alpha u = 0, \\ x'''^{\mu-1} + fx'''^{\mu-2} + gx'''^{\mu-3} + \dots + l + \alpha^2 u = 0, \\ \dots \dots \dots \dots \dots \dots \end{array} \right.$$

par lesquelles on pourra déterminer tant la quantité u que les $\mu - 1$ quantités f, g, \dots, l .

Comme ces inconnues ne sont qu'au premier degré dans les équations précédentes, il est clair que le système de toutes ces équations ne donnera qu'une seule valeur déterminée pour chacune de ces inconnues. Or, supposons que l'on ait trouvé, par la méthode ordinaire d'élimination, la valeur de l'inconnue f (on fera les mêmes raisonnements pour chacune des autres indéterminées g, h, \dots, l), il est visible que cette valeur sera exprimée par une fonction des μ racines x', x'', x''', \dots et de la racine α . Donc, si l'on y fait toutes les permutations possibles entre les μ racines $x',$

x'', x''', \dots , on aura toutes les valeurs particulières de f qui devront être les racines de l'équation en f .

Comme le nombre des permutations qui peuvent avoir lieu entre μ choses est exprimé en général par $1.2.3\dots\mu$, il s'ensuit qu'on aura, généralement parlant, $1.2.3\dots\mu$ valeurs particulières de f ; mais, si parmi ces valeurs il s'en trouve d'égales entre elles, il est clair qu'on pourra les réduire à un plus petit nombre en faisant abstraction des valeurs égales, et nous allons faire voir qu'il n'y aura en effet que $1.2.3\dots(\mu-1)$ valeurs différentes de f .

55. Pour cela il n'est pas nécessaire de chercher l'expression de f par le moyen des équations (e); il suffit d'examiner les variations dont le système de ces équations est susceptible par les permutations des racines x', x'', x''', \dots entre elles. Pour connaître ces variations, on commencera par supposer que la racine x' demeure à sa place, c'est-à-dire que la première équation reste la même, et l'on échangera successivement entre elles, dans les autres équations, les $\mu-1$ racines $x'', x''', x'''' \dots$, ce qui donnera $1.2.3\dots(\mu-1)$ variations; ensuite on fera prendre à x' la place de x'' et *vice versa*, ou, ce qui revient au même, on mettra dans la première équation αu à la place de u , et dans la seconde u à la place de αu , et l'on fera ensuite les mêmes échanges entre les $\mu-1$ racines $x'', x''', x'''' \dots$, ce qui donnera $1.2.3\dots(\mu-1)$ nouvelles variations; on mettra encore x' à la place de x'''' , et *vice versa*, ou bien on substituera $\alpha^2 u$ à la place de u dans la première équation, et u à la place de $\alpha^2 u$ dans la troisième, et l'on fera ensuite les mêmes échanges entre les racines $x'', x''', x'''' \dots$, ce qui donnera aussi $1.2.3\dots(\mu-1)$ variations, et ainsi de suite. Par ce moyen on aura μ fois $1.2.3\dots(\mu-1)$ variations, ce qui fait le nombre total $1.2.3\dots\mu$ de toutes les variations possibles du système des équations (e).

Maintenant je remarque que dès qu'on aura trouvé les $1.2.3\dots(\mu-1)$ variations qui ont lieu tant que x' demeure à sa place, on pourra en déduire sur-le-champ toutes les autres en ne faisant que substituer successivement dans toutes les équations (e), à la place de u , les quantités

$\alpha u, \alpha^2 u, \alpha^3 u, \dots, \alpha^{\mu-1} u$; c'est de quoi il est facile de se convaincre avec un peu d'attention en observant que

$$\alpha^\mu = 1, \quad \alpha^{\mu+1} = \alpha, \quad \alpha^{\mu+2} = \alpha^2, \dots$$

Or il est visible que ces substitutions de $\alpha u, \alpha^2 u, \dots$ à la place de u ne peuvent produire aucun changement dans la valeur de f ; car, dès qu'on élimine u , il est indifférent quelle valeur on donne à cette quantité, et les résultats de l'élimination sont nécessairement indépendants de la valeur de u .

Donc il n'y aura proprement que les $1.2.3\dots(\mu-1)$ variations, qui résultent des permutations entre les $\mu-1$ racines x'', x''', \dots , qui pourront donner des valeurs différentes pour f ; de sorte que l'équation en f ne devra être que du degré $1.2.3\dots(\mu-1)$, ce qui s'accorde avec ce que l'on a dit plus haut (52).

Mais voyons encore si cette équation ne sera pas susceptible de quelque réduction. Pour cela il faut distinguer le cas où l'exposant μ de la proposée est un nombre premier, et celui où cet exposant est un nombre composé.

56. Supposons que μ soit un nombre quelconque premier, et faisant abstraction, dans le système des équations (e), de la première équation, à cause qu'on peut regarder la quantité x' comme fixe, voyons quelles sont les variations dont ce système est susceptible en vertu des permutations entre les autres racines x'', x''', \dots

Pour cela on suivra une méthode semblable à celle du numéro précédent. On regardera d'abord la quantité x'' comme fixe et on cherchera les variations résultantes des $1.2.3\dots(\mu-2)$ permutations entre les $\mu-2$ autres racines x''', x''''', \dots ; on mettra ensuite x'' à la place de x''' et réciproquement, ce qui revient au même que de mettre $\alpha^2 u$ à la place de αu dans la seconde équation, et αu à la place de $\alpha^2 u$ dans la troisième, et l'on cherchera de nouveau les $1.2.3\dots(\mu-2)$ variations provenantes des permutations des autres racines x''', x''''', \dots ; on mettra x'' à la place de x'''' et *vice versa*, ou, ce qui revient au même, on substituera $\alpha^3 u$ à la place

de αu dans la seconde équation, et αu à la place de $\alpha^3 u$ dans la quatrième, et l'on cherchera comme auparavant les $1.2.3\dots(\mu-2)$ variations provenantes des permutations entre les $\mu-2$ racines x'' , x''' , ..., et ainsi de suite. Ce procédé donnera $\mu-1$ fois $1.2.3\dots(\mu-2)$ variations, ce qui fera le nombre total des $1.2.3\dots(\mu-1)$ variations cherchées.

Or je dis que dès qu'on aura trouvé les $1.2.3\dots(\mu-2)$ variations, qui ont lieu tant que x'' demeure à sa place, et qu'on change celles des autres racines x''' , x'''' , ..., on pourra en déduire immédiatement toutes les variations résultantes des permutations entre les $\mu-1$ racines x'' , x''' , x'''' , ... en substituant successivement α^2 , α^3 , ..., $\alpha^{\mu-1}$ à la place de α dans toutes les équations (e); car par ce moyen le terme αu de la seconde équation se changera successivement en $\alpha^2 u$, $\alpha^3 u$, ..., et les termes $\alpha^2 u$, $\alpha^3 u$, ... des autres équations ne feront que s'échanger entre eux (à cause que μ est un nombre premier, comme on peut s'en convaincre par ce qui a été démontré dans le n° 24), échanges qui équivalent évidemment à ceux des racines x''' , x'''' , ... entre elles.

D'où je conclus que quand on aura trouvé par le moyen des équations (e) l'expression de f en x' , x'' , x''' , ... et α , et qu'on voudra connaître les $1.2.3\dots(\mu-1)$ valeurs de f qui résultent des permutations des racines x'' , x''' , x'''' , ... entre elles, et qui doivent être les racines de l'équation en f du degré $1.2.3\dots(\mu-1)$ (numéro précédent), il suffira de chercher les $1.2.3\dots(\mu-2)$ valeurs de f provenantes des seules permutations entre les racines x'' , x'''' , ... et d'y échanger ensuite successivement α en α^2 , α^3 , α^4 , ..., $\alpha^{\mu-1}$; ou bien, ce qui revient au même, on échangera d'abord dans l'expression de f la racine α en α^2 , α^3 , ..., $\alpha^{\mu-1}$, et ensuite on fera dans chacune de ces $\mu-1$ valeurs de f les $1.2.3\dots(\mu-2)$ permutations qui ont lieu entre les $\mu-2$ racines x'' , x'''' , ...; on aura par là les $1.2.3\dots(\mu-1)$ racines de l'équation en f .

57. Imaginons maintenant que les $\mu-1$ valeurs de f qui viennent de la substitution successive de α^2 , α^3 , ..., $\alpha^{\mu-1}$ à la place de α soient les racines de l'équation du $(\mu-1)^{ième}$ degré

$$(f) \quad f^{\mu-1} + Ff^{\mu-2} + Gf^{\mu-3} + \dots = 0,$$

et comme $1, \alpha, \alpha^2, \alpha^3, \dots$ sont les racines de l'équation $y^\mu - 1 = 0$ (hypothèse), il est clair que $\alpha, \alpha^2, \alpha^3, \dots$ seront les $\mu - 1$ racines de l'équation $\frac{y^\mu - 1}{y - 1} = 0$, savoir

$$(g) \quad y^{\mu-1} + y^{\mu-2} + y^{\mu-3} + \dots + 1 = 0.$$

Donc, si dans l'expression de f tirée des équations (e) on met, en général, y à la place de α , et qu'ensuite on élimine y par le moyen de l'équation (g), on aura nécessairement l'équation (f); d'où l'on voit que cette équation ne contiendra plus α , de sorte que les coefficients F, G, \dots ne seront que des fonctions de x', x'', x''', \dots

Or, ayant trouvé l'équation (f), il n'y aura plus qu'à faire dans les expressions des coefficients F, G, \dots toutes les permutations possibles entre les $\mu - 2$ racines $x''', x''^{\text{iv}}, \dots$, et l'on aura par là $1.2.3 \dots (\mu - 2)$ équations en f dont chacune sera du $(\mu - 1)^{\text{ième}}$ degré, et qui renfermeront par conséquent les $1.2.3 \dots (\mu - 1)$ racines de l'équation générale en f .

De là il est facile de conclure que chacun des coefficients F, G, \dots ne pourra dépendre que d'une équation du degré $1.2.3 \dots (\mu - 2)$. En effet, comme ces coefficients sont des fonctions des racines x', x'', x''', \dots , il est clair que chacun d'eux, par exemple F , devra être déterminé par une équation qui ait autant de racines que ce coefficient aura de différentes valeurs en faisant toutes les permutations possibles entre les racines x', x'', x''', \dots ; mais on a démontré plus haut (55) que les permutations de la racine x' en chacune des autres ne changent point les valeurs de f ; par conséquent elles ne changeront pas non plus celles de F, G, \dots qui sont des fonctions des racines de (f); de plus on a vu (56) qu'on peut suppléer aux permutations de la racine x'' en échangeant la racine α en $\alpha^2, \alpha^3, \dots$, de sorte que comme les valeurs de F, G, \dots sont indépendantes de α , elles ne recevront aucun changement par les permutations de x'' . Ainsi il n'y aura que les permutations des $\mu - 2$ racines $x''', x''^{\text{iv}}, \dots$ entre elles, qui donneront des valeurs différentes de F , ainsi que de G, H, \dots ; d'où il s'ensuit que le nombre de ces valeurs différentes sera simplement $1.2.3 \dots (\mu - 2)$; par conséquent chacun des coefficients

F, G, H, \dots sera donné par une équation d'un degré marqué par ce même nombre.

58. Donc la réduite en f , qu'on trouvera par la méthode de M. Tschirnhaus, et que nous avons vu devoir être, en général, du degré $1.2.3\dots(\mu-1)$, sera toujours décomposable, lorsque μ est un nombre premier, en $1.2.3\dots(\mu-2)$ équations du degré $\mu-1$, telles que l'équation (f) ci-dessus, et cela par le moyen d'une équation du degré $1.2.3\dots(\mu-2)$; car, quoique les coefficients F, G, \dots dépendent chacun d'une équation de ce dernier degré, cependant il suffira d'avoir l'équation en F , ou en G , etc., parce que les autres coefficients pourront toujours s'exprimer par des fonctions rationnelles de celui-là.

En effet, si l'on regarde l'équation (f) du degré $\mu-1$ comme un diviseur de la réduite en f du degré $1.2.3\dots(\mu-1)$, on trouvera pour cela $\mu-1$ conditions par lesquelles on pourra déterminer, en général, les $\mu-2$ coefficients G, H, \dots en F , sans aucune extraction de racines, et ces valeurs étant ensuite substituées dans l'une des équations de condition, on aura l'équation même en F , laquelle ne devra pas passer le degré $1.2.3\dots(\mu-2)$. Je dis qu'on peut déterminer, en général, les valeurs de G, H, \dots en F sans extraction de racines; cela est vrai tant qu'on ne donne à F aucune valeur particulière; mais lorsqu'on voudra substituer à la place de F les racines de l'équation en F pour avoir les valeurs correspondantes de G, H, \dots , s'il arrive que la racine substituée soit double, ou triple, ou, etc., les expressions rationnelles de G, H, \dots se trouveront en défaut, et ces quantités dépendront alors de la résolution d'une équation du second, ou du troisième, ou, etc., degré, comme nous le démontrerons plus bas (102).

On pourrait au reste trouver directement l'équation en F par le moyen de ses racines regardées comme des fonctions de x', x'', x''', \dots ; on a vu différents exemples de cette méthode dans les Sections précédentes. Et, supposant cette équation en F connue, on pourra, par son moyen, déterminer directement les valeurs de G, H, \dots par la méthode qu'on trouvera dans la Section quatrième (100).

Maintenant il est visible que l'équation en F sera toujours d'un degré plus haut que la proposée, excepté le seul cas de $\mu = 3$; car, faisant $\mu = 3$, on a

$$1 \cdot 2 \dots (\mu - 2) = 1,$$

faisant $\mu = 5$, on a

$$1 \cdot 2 \dots (\mu - 2) = 1 \cdot 2 \cdot 3 = 6,$$

faisant $\mu = 7$, on a

$$1 \cdot 2 \dots (\mu - 2) = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120,$$

et ainsi de suite; donc, à moins que cette équation ne puisse encore s'abaisser à un degré moindre que μ , la solution de M. Tschirnaus ne sera d'aucun usage; or c'est ce qui me paraît presque impossible, en général. Il est vrai que, quoique le degré $1 \cdot 2 \dots (\mu - 2)$ de l'équation dont nous parlons soit plus élevé que le degré μ de la proposée, cette équation ne renfermera pas cependant des difficultés supérieures à celles des équations du degré μ ; car, puisque ses $1 \cdot 2 \cdot 3 \dots (\mu - 2)$ racines sont des fonctions connues des μ racines x', x'', x''', \dots , il est clair qu'elles ne seront pas indépendantes les unes des autres, mais qu'il y aura entre elles des relations exprimées par un nombre d'équations égal à la différence des exposants $1 \cdot 2 \cdot 3 \dots (\mu - 2)$ et μ ; de sorte que, supposant que l'on connaisse un nombre μ de ces racines, on connaîtra aussi par leur moyen toutes les autres.

D'où il s'ensuit que l'équation en F ne pourra renfermer dans le fond que les difficultés du degré μ ; mais, par la même raison, il paraît aussi qu'elle devra toujours renfermer toutes les difficultés de ce degré, de sorte qu'on se trouvera ramené aux mêmes difficultés auxquelles la résolution générale de l'équation proposée est sujette.

59. Supposons présentement que l'exposant μ de la proposée soit un nombre composé : dans ce cas il faudra apporter quelque modification au raisonnement du n° 56, car, si dans les termes de la progression géométrique $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{\mu-1}$ on substituait indifféremment à la place de α les puissances $\alpha^2, \alpha^3, \dots, \alpha^{\mu-1}$, on ne retrouverait pas toujours les mêmes termes comme lorsque μ est un nombre premier; nous en avons donné

la raison dans le n° 24, et nous y avons démontré aussi qu'il n'y a que les puissances de α dont l'exposant est un nombre premier à μ qui, étant substituées à la place de α dans les termes $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{\mu-1}$, puissent redonner les mêmes termes, de sorte qu'il faudra restreindre à ces seules puissances de α les résultats du n° 56.

Donc, si l'on désigne, en général, par ν, ϖ, ρ, \dots tous les nombres moindres que μ et premiers à μ , dont nous supposerons que le nombre soit $\lambda - 1$, on pourra, par les substitutions de $\alpha^\nu, \alpha^\varpi, \alpha^\rho, \dots$ à la place de α dans l'expression de f , suppléer aux permutations de la racine x'' dans les racines $x^{(\nu+1)}, x^{(\varpi+1)}, x^{(\rho+1)}, \dots$; par conséquent, si l'on suppose que les λ valeurs de f qui viennent de la substitution $\alpha^\nu, \alpha^\varpi, \alpha^\rho, \dots$ à la place de α soient les racines de l'équation

$$(h) \quad f^\nu + Ff^{\lambda-1} + Gf^{\lambda-2} + \dots = 0,$$

cette équation sera un diviseur de la réduite en f , et les coefficients F, G, \dots seront donnés chacun par une équation du degré $\frac{1.2.3\dots(\mu-1)}{\lambda}$; de sorte que dans ce cas la réduite en f , trouvée par la méthode de M. Tschirnhaus, et qui est du degré $1.2.3\dots(\mu-1)$, sera résoluble en $\frac{1.2.3\dots(\mu-1)}{\lambda}$ équations, chacune du degré λ , et cela moyennant une équation du degré

$$\frac{1.2.3\dots(\mu-1)}{\lambda}.$$

Pour trouver l'équation (h) *à priori*, il n'y aura qu'à mettre y à la place de α dans l'expression de f , et ensuite éliminer y par le moyen de l'équation dont les racines seraient $\alpha, \alpha^\nu, \alpha^\varpi, \alpha^\rho, \dots$; or voici comment on pourra avoir cette équation.

60. Considérons, en général, l'équation

$$y^\mu - 1 = 0,$$

dont les racines sont $1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{\mu-1}$, et supposons que le nombre μ soit résolu dans les facteurs premiers r, s, t, \dots , dont chacun soit contenu

une ou plusieurs fois dans le nombre μ , il est facile de voir que les puissances de α , qu'il faudra exclure, pour avoir uniquement les puissances $\alpha, \alpha^r, \alpha^s, \alpha^t, \dots$ dont les exposants sont premiers à μ , il est facile de voir, dis-je, que ces puissances seront celles dont les exposants seront des multiples des nombres r, s, t, \dots ; de plus il est clair, par ce qu'on a démontré dans le n° 24, que ces mêmes puissances de α seront les racines des équations

$$y^r - 1 = 0, \quad y^s - 1 = 0, \quad y^t - 1 = 0, \dots;$$

done, si l'on fait pour plus de simplicité

$$\frac{\mu}{r} = \mu', \quad \frac{\mu}{s} = \mu'', \quad \frac{\mu}{t} = \mu''', \dots$$

et qu'on divise l'équation $y^4 - 1 = 0$ successivement par celles-ci

$$y^{\mu'} - 1 = 0, \quad y^{\mu''} - 1 = 0, \quad y^{\mu'''} - 1 = 0, \dots,$$

on aura les équations suivantes

dont la première aura pour racines toutes les puissances de α jusqu'à α^{p-1} , à l'exception de celles dont les exposants seront des multiples de r ; la seconde, toutes les puissances de α , à l'exception de celles dont les exposants seront des multiples de s ; la troisième, etc.; d'où l'on peut conclure que, si l'on cherche le plus grand commun diviseur de toutes ces équations, on aura l'équation cherchée, dont les racines seront les puissances $\alpha, \alpha^v, \alpha^w, \alpha^p, \dots$, et qui sera par conséquent de la forme

$$(i) \quad y^\lambda + \beta y^{\lambda-1} + \gamma y^{\lambda-2} + \dots + \gamma y^2 + \beta y + 1 = 0.$$

Ainsi, par exemple, si $\mu = 4$, on aura $r = 2$, $\mu' = 2$, et l'on aura cette

seule équation

$$y^2 + 1 = 0,$$

dont les racines seront α et α^3 .

Si $\mu = 6$, on aura $r = 2$, $s = 3$; donc $\mu' = 3$, $\mu'' = 2$, ce qui donnera ces deux équations

$$y^3 + 1 = 0,$$

$$y^4 + y^2 + 1 = 0,$$

dont le plus grand commun diviseur est

$$y^2 - y + 1 = 0,$$

équation dont les racines seront par conséquent α et α^5 .

Si $\mu = 8$, on aura $r = 2$; donc $\mu' = 4$, et l'on aura cette seule équation

$$y^4 + 1 = 0,$$

dont les racines seront α , α^3 , α^5 , α^7 , et ainsi de suite.

Quant à l'exposant λ , on peut le déterminer *à priori* d'après les facteurs du nombre μ , car on aura toujours

$$\lambda = \frac{\mu}{rst\ldots} (r-1)(s-1)(t-1)\ldots,$$

comme on peut le démontrer aisément en cherchant combien, parmi les nombres moindres que μ , il y en aura de premiers à μ . (*Voyez les Nouveaux Commentaires de Pétersbourg*, tome VIII.)

61. Ayant donc trouvé ainsi l'équation (*i*), on s'en servira pour éliminer y de l'expression de f , et il en résultera l'équation (*h*), dont tous les coefficients F, G, \dots seront des fonctions des racines x', x'', \dots , sans α , telles qu'elles ne seront susceptibles que de $\frac{1 \cdot 2 \cdot 3 \dots (\mu-1)}{\lambda}$ variations, par toutes les permutations possibles des racines x', x'', \dots entre elles; de sorte que chacune de ces fonctions sera donnée simplement par une équation du degré

$$\frac{1 \cdot 2 \cdot 3 \dots (\mu-1)}{\lambda},$$

comme on l'a déjà dit plus haut.

Il se peut au reste que ces équations en F , ou en G , etc., soient encore susceptibles de quelques réductions; c'est ce qui dépendra de la forme des fonctions de x' , x'' , ... par lesquelles les quantités F , G , ... seront exprimées; mais nous n'entrerons pas dans cette recherche, d'autant que dans le cas où l'exposant μ est un nombre composé on peut simplifier la Solution de M. Tschirnhaus en ne faisant évanouir que quelques-uns des termes intermédiaires de la transformée (52).

62. Nous allons donc chercher *à priori* les résultats qu'on doit avoir dans ce cas, et nous supposerons, comme dans le numéro cité, que, μ étant égal à $\nu\varpi$, tous les termes de la transformée en y dont les exposants ne seront pas divisibles par ϖ disparaissent, en sorte que, faisant $y^\varpi = z$, l'équation (c) devienne

$$z^\nu + Dz^{\nu-1} + Kz^{\nu-2} + \dots + V = 0,$$

laquelle aura par conséquent ν racines que nous dénoterons par z' , z'' , z''' , ..., $z^{(\nu)}$; et comme l'équation $y^\varpi = z$ donne

$$y = \sqrt[\varpi]{z},$$

ou bien, en dénotant par 1 , α , α^2 , ..., $\alpha^{\varpi-1}$ les ϖ racines de $y^\varpi - 1 = 0$,

$$y = \sqrt[\varpi]{z}, \quad \alpha\sqrt[\varpi]{z}, \quad \alpha^2\sqrt[\varpi]{z}, \dots, \quad \alpha^{\varpi-1}\sqrt[\varpi]{z},$$

on aura, en substituant successivement à la place de z les ν racines z' , z'' , z''' , ..., et faisant pour plus de simplicité

$$\zeta' = \sqrt[\varpi]{z'}, \quad \zeta'' = \sqrt[\varpi]{z''}, \quad \zeta''' = \sqrt[\varpi]{z'''}, \dots,$$

on aura, dis-je, ces μ valeurs de y

$$\begin{aligned} \zeta', & \quad \alpha\zeta', \quad \alpha^2\zeta', \quad \alpha^3\zeta', \dots, \quad \alpha^{\varpi-1}\zeta', \\ \zeta'', & \quad \alpha\zeta'', \quad \alpha^2\zeta'', \quad \alpha^3\zeta'', \dots, \quad \alpha^{\varpi-1}\zeta'', \\ \zeta''', & \quad \alpha\zeta''', \quad \alpha^2\zeta''', \quad \alpha^3\zeta''', \dots, \quad \alpha^{\varpi-1}\zeta''', \\ & \quad \dots \dots \dots \dots \dots \dots, \\ \zeta^{(\nu)}, & \quad \alpha\zeta^{(\nu)}, \quad \alpha^2\zeta^{(\nu)}, \quad \alpha^3\zeta^{(\nu)}, \dots, \quad \alpha^{\varpi-1}\zeta^{(\nu)}, \end{aligned}$$

qui seront celles des racines y' , y'' , y''' , ..., $y^{(\mu)}$.

Substituant donc successivement ces valeurs à la place de y dans l'équation subsidiaire (b) du n° 51, et mettant en même temps x', x'', x''', \dots à la place de x (53), on aura les μ équations suivantes

Or, comme on doit supposer dans ce cas (52)

$$\rho = \nu(\varpi - 1) = \mu - \nu$$

pour que le nombre des indéterminées f, g, \dots, l soit aussi $\mu - \nu$, il est clair que, si dans les μ équations qu'on vient de trouver on élimine d'abord les ν quantités $\zeta', \zeta'', \zeta''', \dots, \zeta^{(\nu)}$, il restera $\mu - \nu$ équations, qui serviront à déterminer les $\mu - \nu$ inconnues f, g, \dots, l .

Imaginons maintenant qu'on ait trouvé, par les règles ordinaires de l'élimination, l'expression de f (on appliquera les mêmes raisonnements aux autres indéterminées g, \dots, l); on cherchera toutes les valeurs différentes de f qui peuvent venir des permutations des μ racines x', x'', \dots entre elles, et l'on aura les racines de l'équation en f , laquelle sera par conséquent d'un degré égal au nombre de ces différentes valeurs.

Or les racines x', x'', \dots étant au nombre de μ , seront susceptibles en général de $1.2.3\dots\mu$ permutations; mais il faudra défalquer de ce

nombre les permutations qui ne produiront aucun changement dans l'expression de f .

Pour cela je remarque d'abord que si l'on suppose qu'on échange respectivement les racines x' , x'' , ..., $x^{(\varpi)}$ en $x^{(\varpi+1)}$, $x^{(\varpi+2)}$, ..., $x^{(2\varpi)}$, ou en $x^{(2\varpi+1)}$, $x^{(2\varpi+2)}$, ..., $x^{(3\varpi)}$, ou, etc., il en résultera dans les équations précédentes les mêmes changements que si l'on échangeait ζ' en ζ'' , ou en ζ''' , ou, etc.; de sorte que les permutations des quantités ζ' , ζ'' , ζ''' , ... entre elles seront équivalentes aux permutations des racines x' , $x^{(\varpi+1)}$, $x^{(2\varpi+1)}$, ... entre elles, ces permutations étant combinées avec les permutations correspondantes et simultanées des racines x'' , $x^{(\varpi+2)}$, $x^{(2\varpi+2)}$, ... entre elles, avec celles des racines x''' , $x^{(\varpi+3)}$, $x^{(2\varpi+3)}$, ... entre elles, etc.

Or, comme dans la détermination des coefficients f , g , ... on doit faire disparaître les quantités ζ' , ζ'' , ζ''' , ... par l'élimination, il sera indifférent que ces quantités soient mises les unes à la place des autres d'une manière quelconque; par conséquent il ne résultera de leurs permutations quelconques aucun changement dans les valeurs de f , g , ...; donc, puisque ces quantités étant au nombre de ν sont susceptibles de $1.2.3\dots\nu$ permutations, voilà autant de permutations entre les μ racines x' , x'' , x''' , ..., $x^{(\mu)}$ qui ne produiront aucun changement dans les valeurs de f , g , ...; d'où il s'ensuit que, dans le nombre total $1.2.3\dots\mu$ des valeurs particulières de f , chaque valeur se trouvera répétée $1.2.3\dots\nu$ fois; par conséquent il ne pourra y avoir qu'un nombre de valeurs différentes de f exprimé par

$$\frac{1.2.3\dots\mu}{1.2.3\dots\nu}$$

63. Maintenant si l'on considère les permutations des racines x' , x'' , x''' , ..., $x^{(\varpi)}$ entre elles, et qu'on considère en même temps les ϖ premières équations du n° 62, lesquelles renferment ces racines, on y pourra appliquer des raisonnements analogues à ceux du n° 55, et l'on en conclura que les échanges de la racine x' en les autres racines x'' , x''' , ..., $x^{(\varpi)}$ ne produiront aucun changement dans les valeurs de f , g , ..., puisque ces échanges donneront les mêmes résultats que l'on aurait en substituant successivement $\alpha\zeta'$, $\alpha^2\zeta'$, $\alpha^3\zeta'$, ..., $\alpha^{\varpi-1}\zeta'$ à la place de ζ' .

Donc le nombre des valeurs différentes de f ne pourra être plus grand que

$$\frac{1 \cdot 2 \cdot 3 \dots \mu}{1 \cdot 2 \cdot 3 \dots \nu} \text{ divisé par } \varpi.$$

On tirera des conclusions semblables de la considération des ϖ racines $x^{(\varpi+1)}, x^{(\varpi+2)}, x^{(\varpi+3)}, \dots, x^{(2\varpi)}$, comme aussi des racines $x^{(2\varpi+1)}, x^{(2\varpi+2)}, x^{(2\varpi+3)}, \dots, x^{(3\varpi)}$, et ainsi des autres; et comme les combinaisons de ces racines entre elles sont totalement indépendantes, il s'ensuit qu'il faudra diviser le nombre $\frac{1 \cdot 2 \cdot 3 \dots \mu}{1 \cdot 2 \cdot 3 \dots \nu}$ autant de fois par ϖ qu'il y a de ces systèmes de ϖ racines chacun, c'est-à-dire ν fois, nombre des quantités $\zeta', \zeta'', \dots, \zeta^{(\nu)}$.

Donc le nombre des valeurs différentes de f ne pourra être que

$$\frac{1 \cdot 2 \cdot 3 \dots \mu}{1 \cdot 2 \cdot 3 \dots \nu \varpi^{\nu}};$$

par conséquent l'équation en f ne devra monter qu'au degré marqué par ce même nombre.

C'est aussi ce qui s'accorde avec ce que l'on a trouvé à la fin du n° 52; en effet, il est clair que le nombre

$$\frac{1 \cdot 2 \cdot 3 \dots \mu}{1 \cdot 2 \cdot 3 \dots \nu \varpi^{\nu}}$$

se réduit d'abord à celui-ci

$$\frac{\nu(\nu+1)(\nu+2)\dots\mu}{\nu \varpi^{\nu}},$$

et ensuite, à cause de $\mu = \nu \varpi$, à celui-ci

$$\frac{\nu(\nu+1)(\nu+2)\dots(\mu-1)}{\varpi^{\nu-1}}.$$

64. La réduite en f sera donc, généralement parlant, du degré

$$\frac{\nu(\nu+1)(\nu+2)\dots(\mu-1)}{\varpi^{\nu-1}};$$

mais cette équation pourra toujours s'abaisser à un degré inférieur par des considérations semblables à celles des n°s 57 et 59. En effet, si ϖ est

un nombre premier, il est facile de prouver par des raisonnements analogues à celui du n° 56, que l'on pourra suppléer aux permutations des racines x' , $x^{(\varpi+1)}$, $x^{(2\varpi+1)}$, ... en x'' , $x^{(\varpi+2)}$, $x^{(2\varpi+2)}$, ... en x''' , $x^{(\varpi+3)}$, $x^{(2\varpi+3)}$, ... en, etc., en substituant successivement dans l'expression de f les puissances α^2 , α^3 , ..., $\alpha^{\varpi-1}$ à la place de α ; de sorte que si l'on met y au lieu de α dans l'expression de f , et qu'ensuite on élimine y par le moyen de l'équation

$$\frac{y^{\varpi} - 1}{y - 1} = 0,$$

ou bien

$$y^{\varpi-1} + y^{\varpi-2} + y^{\varpi-3} + \dots + 1 = 0,$$

on aura une équation en f telle que

$$f^{\varpi-1} + Ff^{\varpi-2} + Gf^{\varpi-3} + \dots = 0,$$

laquelle sera un diviseur de la réduite en f ; et les coefficients F , G , ... seront déterminés chacun par une équation du degré

$$\frac{\nu(\nu+1)(\nu+2)\dots(\mu-1)}{(\varpi-1)\varpi^{\nu-1}};$$

ce qui donnera autant de diviseurs de la même réduite, dont chacun sera du degré $\varpi - 1$.

Si ν n'est pas un nombre premier, alors il faudra chercher, comme dans le n° 60, l'équation dont les racines seront les puissances de α qui auront pour exposant des nombres premiers à ν en y comprenant l'unité, et, désignant cette équation par

$$y^\lambda + \beta y^{\lambda-1} + \dots + \beta y + 1 = 0,$$

on éliminera, par son moyen, y de l'expression de f ; on aura une équation en f telle que

$$f^\lambda + Ff^{\lambda-1} + Gf^{\lambda-2} + \dots = 0,$$

où chaque coefficient F , G , ... ne dépendra que d'une équation du degré

$$\frac{\nu(\nu+1)(\nu+2)\dots(\mu-1)}{\lambda\varpi^{\nu-1}};$$

de sorte que l'on aura par là autant de valeurs de F , G , ..., et par consé-

quent autant d'équations en f du degré λ , lesquelles seront les diviseurs de la réduite en f .

Soit, par exemple, $\mu = 6$:

1^o On pourra faire $\nu = 3$, $\varpi = 2$, et la réduite en f sera du degré $\frac{3 \cdot 4 \cdot 5}{2^2} = 15$; et, à cause de $\varpi - 1 = 1$, elle ne pourra plus s'abaisser par la méthode précédente.

2^o On pourra faire $\nu = 2$, $\varpi = 3$, on aura $\frac{2 \cdot 3 \cdot 4 \cdot 5}{3} = 40$ pour le degré de la réduite en f ; et comme $\varpi - 1 = 2$, on pourra résoudre cette réduite en vingt équations du second degré chacune, moyennant une équation du vingtième degré.

65. Revenons maintenant aux formules du n° 51; et il est clair que l'équation proposée (a) pourra être regardée à son tour comme le résultat de l'élimination de y faite par le moyen des équations (c) et (d). Ainsi, si l'on regarde les coefficients A, B, C, ... de l'équation en y comme donnés et les coefficients F, G, ... de l'expression de x en y comme indéterminés, on pourra, par la comparaison des termes de l'équation résultante de l'élimination de y avec ceux de la proposée, déterminer ces derniers coefficients, pourvu que leur nombre ne soit pas moindre que μ ; ce qui ne sera point à craindre tant qu'on prendra $\lambda = \frac{\mu}{2}$ ou $\frac{\mu - 1}{2}$; et si l'équation en y est prise telle qu'elle soit résoluble, ce qui peut avoir lieu d'une infinité de manières différentes, on aura la résolution complète de la proposée; mais la difficulté consistera dans la détermination des coefficients indéterminés F, G,

On facilitera cependant beaucoup cette détermination ainsi que l'élimination de y , si l'on change l'expression de x , donnée par l'équation (d), en une autre où l'inconnue y ne se trouve qu'au numérateur; c'est ce qui est toujours possible en multipliant le haut et le bas de la fraction

$$\frac{F + Gy + Hy^2 + \dots + Ky^k}{L + My + Ny^2 + \dots + Ry^r}$$

par un polynôme convenable en y , qu'on pourra trouver de la manière suivante.

On supposera

$$z = L + M\gamma + N\gamma^2 + \dots + R\gamma^k,$$

et comme γ est déterminé par l'équation

$$\gamma^{\mu} + A\gamma^{\mu-1} + B\gamma^{\mu-2} + \dots = 0,$$

on éliminera γ par le moyen de cette équation, ce qui donnera une équation en z du degré μ qu'on pourra représenter ainsi

$$z^{\mu} + \alpha z^{\mu-1} + \beta z^{\mu-2} + \gamma z^{\mu-3} + \dots - \omega = 0,$$

où les coefficients $\alpha, \beta, \gamma, \dots, \omega$ seront par conséquent des fonctions continues des A, B, C, \dots et L, M, N, \dots

Ainsi l'on aura

$$z(z^{\mu-1} + \alpha z^{\mu-2} + \beta z^{\mu-3} + \dots) = \omega,$$

d'où l'on voit que la quantité z deviendra égale à ω , et par conséquent indépendante de γ , étant multipliée par le polynôme

$$z^{\mu-1} + \alpha z^{\mu-2} + \beta z^{\mu-3} + \dots$$

De sorte que si l'on remet dans ce polynôme, à la place de z , sa valeur en γ , on aura le polynôme cherché, dans lequel on pourra, si l'on veut, n'admettre que des puissances de γ moindres que γ^{μ} , parce qu'au moyen de l'équation

$$\gamma^{\mu} + A\gamma^{\mu-1} + \dots = 0$$

on pourra toujours faire rentrer les puissances de γ supérieures à γ^{μ} dans la classe des inférieures.

De cette manière on pourra donc ramener l'équation (d) à la forme

$$(k) \quad x = a + b\gamma + c\gamma^2 + \dots + k\gamma^{\mu-1},$$

de sorte qu'on pourra toujours regarder l'équation proposée (a)

$$x^{\mu} + mx^{\mu-1} + nx^{\mu-2} + \dots = 0,$$

comme la résultante de l'élimination de y , faite par le moyen de l'équation (c)

$$y^\mu + A y^{\mu-1} + B y^{\mu-2} + \dots + V = 0,$$

et de l'équation (k). On supposera donc les coefficients a, b, c, \dots, k , dont le nombre est μ , indéterminés, et l'équation provenante de l'élimination de y étant comparée terme à terme avec la proposée donnera μ conditions qui serviront à déterminer les quantités a, b, c, \dots .

Si l'on réduit l'équation en y à deux termes tels que

$$y^\mu + V = 0,$$

la méthode précédente reviendra à celle de MM. Euler et Bezout, dont nous avons déjà fait mention plusieurs fois dans le cours de ce Mémoire.

Le détail où nous venons d'entrer sert à rapprocher cette méthode de celle de M. Tschirnhaus, et à montrer leur analogie et dépendance mutuelle.

66. Comme tout se réduit à déterminer les inconnues a, b, c, \dots, k dont le nombre est μ , par la comparaison des termes de la proposée avec ceux de la résultante de l'élimination de y , nous remarquerons d'abord à l'égard de cette dernière, qu'elle sera nécessairement exprimée par une fonction rationnelle et entière des quantités a, b, c, \dots, k et x , où ces quantités rempliront partout le même nombre de dimensions μ , comme on peut aisément le conclure de la théorie d'élimination donnée dans le n° 13; d'où il s'ensuit qu'en ordonnant cette équation par rapport à x les coefficients de tous ces termes se trouveront être des fonctions rationnelles, entières et homogènes des quantités a, b, c, \dots, k , et dont les dimensions seront 0, 1, 2, 3, ... pour les puissances $x^\mu, x^{\mu-1}, x^{\mu-2}, \dots$

Ainsi le premier terme x^μ n'aura d'autre coefficient que l'unité, le second terme $x^{\mu-1}$ aura pour coefficient une quantité de la forme

$$\alpha a + \beta b + \gamma c + \dots,$$

α, β, γ étant des coefficients numériques, le troisième terme $x^{\mu-2}$ aura

pour coefficient une quantité de la forme

$$\alpha a^2 + \beta ab + \gamma b^2 + \delta ac + \dots,$$

et ainsi des autres.

Égalant donc le coefficient du second terme à m , celui du troisième terme à n , et ainsi de suite, on aura μ équations entre les μ inconnues a, b, c, \dots, k , dont la première sera du premier degré seulement, la seconde, du second degré, la troisième, du troisième, et ainsi des autres; de sorte qu'en éliminant ces inconnues à l'exception d'une seule quelconque, on aura, en général, pour la détermination de celle-ci une équation finale du degré marqué par $1.2.3 \dots \mu$; ce qui est contraire au sentiment de M. Euler, mais ce qui s'accorde avec ce que M. Bezout a trouvé par induction.

67. Pour confirmer davantage cette conclusion sur le degré des équations en a , ou b , ou c, \dots , et pour voir en même temps dans quel cas ces équations sont susceptibles de simplification, nous allons chercher *à priori* l'expression des quantités a, b, c, \dots en x', x'', x''', \dots , racines de la proposée.

Faisons, comme dans le n° 54, $\sqrt[\mu]{-V} = u$, et désignant par $1, \alpha, \beta, \gamma, \dots$ les μ racines de l'équation

$$y^\mu - 1 = 0,$$

on aura $u, \alpha u, \beta u, \gamma u, \dots$ pour les μ racines de l'équation

$$y^\mu + V = 0;$$

donc, substituant successivement ces racines dans l'équation (k) du n° 65 à la place de y , et mettant en même temps les racines x', x'', x''', \dots à la place de x , on aura les μ équations suivantes

$$\begin{aligned} x' &= a + bu + cu^2 + du^3 + \dots + ku^{\mu-1}, \\ x'' &= a + \alpha bu + \alpha^2 cu^2 + \alpha^3 du^3 + \dots + \alpha^{\mu-1} ku^{\mu-1}, \\ x''' &= a + \beta bu + \beta^2 cu^2 + \beta^3 du^3 + \dots + \beta^{\mu-1} ku^{\mu-1}, \\ x^{\mu} &= a + \gamma bu + \gamma^2 cu^2 + \gamma^3 du^3 + \dots + \gamma^{\mu-1} ku^{\mu-1}, \\ &\dots \end{aligned}$$

par lesquelles on pourra déterminer les μ racines inconnues a, b, c, \dots

Cette détermination n'a aucune difficulté; car puisque $\alpha, \beta, \gamma, \dots$ sont les racines de l'équation $y^k - 1 = 0$, laquelle manque de tous ses termes intermédiaires, on aura, comme on sait,

c'est-à-dire que la somme de toutes les racines élevées chacune à une même puissance quelconque sera toujours nulle lorsque l'exposant de la puissance ne sera pas divisible par μ ; et à l'égard des puissances dont l'exposant sera multiple de μ , il est visible, par l'équation même $y^\mu - 1 = 0$, qu'on aura $x^\mu = 1$, $x^{2\mu} = 1, \dots$, et ainsi des autres racines.

Donc, si l'on ajoute ensemble les μ équations du numéro précédent, après les avoir multipliées respectivement par les μ racines correspondantes $1, \alpha, \beta, \dots$ élevées successivement aux puissances $\mu^{i\text{ème}}$, $(\mu - 1)^{i\text{ème}}$, $(\mu - 2)^{i\text{ème}}$, ..., jusqu'à la première inclusivement, on aura sur-le-champ

$$\begin{aligned}
 \mu.a &= x' + x'' + x''' + x^{iv} + \dots, \\
 \mu.ub &= x' + \alpha^{\mu-1}x'' + \beta^{\mu-1}x''' + \gamma^{\mu-1}x^{iv} + \dots, \\
 \mu.u^2c &= x' + \alpha^{\mu-2}x'' + \beta^{\mu-2}x''' + \gamma^{\mu-2}x^{iv} + \dots, \\
 \mu.u^3d &= x' + \alpha^{\mu-3}x'' + \beta^{\mu-3}x''' + \gamma^{\mu-3}x^{iv} + \dots, \\
 &\dots
 \end{aligned}$$

On voit d'abord que la quantité a doit être donnée par une équation linéaire, puisqu'elle conserve la même valeur, quelque permutation qu'on fasse entre les racines x', x'', \dots ; en effet, à cause de

$$x' + x'' + x''' + \dots = -m,$$

on aura $a = -\frac{m}{\mu}$.

Quant aux autres quantités ub, u^2c, u^3d, \dots , chacune d'elles dépendra, en général, d'une équation d'un degré égal au nombre de toutes les permutations possibles entre les μ racines x', x'', x''', \dots , nombre qui est, comme on sait, marqué par $1 \cdot 2 \cdot 3 \dots \mu$; car à chacune de ces permuta-

tions il répondra une valeur différente des quantités ub , u^2c , u^3d , ...; mais ces valeurs peuvent avoir entre elles des relations telles, que l'équation dont elles seront les racines puisse s'abaisser à un degré inférieur; c'est ce que nous allons examiner.

68. Pour cela nous remarquerons d'abord que, comme la quantité u demeure indéterminée, on pourra lui donner telle valeur qu'on voudra; la supposition la plus simple est de faire, avec M. Bezout, $u = 1$, et par conséquent

$$V = -u^{\mu} = -1;$$

nous adopterons donc cette hypothèse et nous supposerons en même temps

$$k = \frac{a'}{\mu}, \quad h = \frac{a''}{\mu}, \dots, \quad b = \frac{a^{(\mu-1)}}{\mu},$$

ce qui donnera ces formules plus simples

$$\begin{aligned} a' &= x' + \alpha x'' + \beta x''' + \gamma x^{(4)} + \dots, \\ a'' &= x' + \alpha^2 x'' + \beta^2 x''' + \gamma^2 x^{(4)} + \dots, \\ a''' &= x' + \alpha^3 x'' + \beta^3 x''' + \gamma^3 x^{(4)} + \dots, \\ &\dots \dots \dots \dots \dots \dots, \\ a^{(\mu-1)} &= x' + \alpha^{\mu-1} x'' + \beta^{\mu-1} x''' + \gamma^{\mu-1} x^{(4)} + \dots \end{aligned}$$

Considérons l'expression de la quantité a' , et comme les racines de l'équation $y^{\mu} - 1 = 0$, que nous avons désignées par $1, \alpha, \beta, \gamma, \dots$, peuvent s'exprimer (24) par $1, \alpha, \alpha^2, \alpha^3, \dots$, on aura $\beta = \alpha^2, \gamma = \alpha^3, \dots$; de sorte que l'on aura

$$a' = x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x^{(4)} + \dots + \alpha^{\mu-1} x^{(\mu)},$$

et pour avoir les valeurs des autres quantités a'', a''', \dots , il n'y aura qu'à mettre, dans cette expression de a' , à la place de α , ses puissances $\alpha^2, \alpha^3, \dots$. D'où, et de ce qui a été démontré plus haut (56), on peut d'abord conclure que, lorsque l'exposant μ de l'équation proposée est un nombre premier, les quantités a', a'', a''', \dots seront les racines d'une même équa-

tion; mais il n'en sera pas ainsi lorsque μ sera un nombre composé; c'est pourquoi il faudra, dans la suite, distinguer les deux cas, où μ est un nombre premier et où il n'est pas premier.

69. Supposons, en général,

$$t = x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x'''' + \dots + \alpha^{\mu-1} x^{(\mu)},$$

et voyons quelle doit être la nature de l'équation en t . Pour cela on cherchera toutes les valeurs particulières de t qui résultent des $1.2.3\dots\mu$ permutations dont les μ racines x', x'', \dots sont susceptibles; et dans cette recherche on suivra une méthode analogue à celle du n° 55; ainsi l'on regardera d'abord la quantité x' comme fixe, et l'on fera varier la position des $\mu - 1$ autres quantités, lesquelles étant susceptibles de $1.2.3\dots(\mu - 1)$ permutations donneront autant de valeurs particulières de t , que nous dénoterons par t', t'', t''', \dots ; maintenant on fera varier, dans l'expression de chacune de ces valeurs, la position de la quantité x' en la mettant successivement à la place de x'', x''', \dots , ce qui donnera les $1.2.3\dots\mu$ valeurs cherchées qui devront être les racines de l'équation en t .

Or on verra aisément que pour avoir toutes ces valeurs il n'y aura qu'à multiplier successivement chacune des valeurs t', t'', t''', \dots par $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{\mu-1}$; de sorte que les racines de l'équation en t seront exprimées ainsi

$$\begin{aligned} t', & \quad \alpha t', \quad \alpha^2 t', \quad \alpha^3 t', \dots, \quad \alpha^{\mu-1} t', \\ t'', & \quad \alpha t'', \quad \alpha^2 t'', \quad \alpha^3 t'', \dots, \quad \alpha^{\mu-1} t'', \\ t''', & \quad \alpha t''', \quad \alpha^2 t''', \quad \alpha^3 t''', \dots, \quad \alpha^{\mu-1} t''', \\ & \quad \dots \dots \dots \dots \dots \dots \dots \end{aligned}$$

d'où il est facile de conclure que l'équation en t ne renfermera que des puissances de t dont les exposants seront multiples de μ .

De là il s'ensuit donc qu'en faisant $t^\mu = \theta$, en sorte que l'on ait

$$\theta = (x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x'''' + \dots)^\mu,$$

on aura une équation en θ du degré $1.2.3\dots(\mu - 1)$, dont les racines

seront les valeurs de θ qui viennent des permutations des $\mu - 1$ racines x'', x''', \dots en faisant abstraction de la racine x' .

Cette conclusion a lieu quel que soit le nombre μ . Examinons maintenant à part les deux cas où μ est un nombre premier ou non.

70. Supposons d'abord que l'exposant μ soit un nombre premier, et nous remarquerons que pour trouver toutes les valeurs de θ il suffira de chercher celles qui viennent des permutations des $\mu - 2$ racines x'' , x''', \dots entre elles, et dont le nombre est par conséquent $1.2.3\dots(\mu - 2)$, et de substituer successivement, dans l'expression de chacune de ces valeurs, α^2 , $\alpha^3, \dots, \alpha^{\mu-1}$ à la place de α ; c'est de quoi on peut se convaincre par un raisonnement analogue à celui du n° 56.

D'où il s'ensuit (57) que, si l'on suppose que les $\mu - 1$ valeurs de θ qui répondent aux substitutions de α^2 , $\alpha^3, \dots, \alpha^{\mu-1}$ à la place de α dans l'expression précédente de θ soient les racines de cette équation du $(\mu - 1)^{i\text{ème}}$ degré

$$\theta^{\mu-1} - T\theta^{\mu-2} + U\theta^{\mu-3} - X\theta^{\mu-4} + \dots = 0,$$

les coefficients T, U, X, \dots seront donnés chacun par une équation du degré $1.2.3\dots(\mu - 2)$; de sorte que l'équation en θ du degré $1.2.3\dots(\mu - 1)$ sera décomposable en $1.2.3\dots(\mu - 2)$ équations du $(\mu - 1)^{i\text{ème}}$ degré chacune, au moyen d'une équation du degré $1.2.3\dots(\mu - 2)$, car, ayant trouvé l'un des coefficients T, U, X, \dots par la résolution d'une équation de ce degré, il sera aisément d'avoir tous les autres.

71. Puisque les $\mu - 1$ racines de l'équation

$$\theta^{\mu-1} - T\theta^{\mu-2} + U\theta^{\mu-3} - X\theta^{\mu-4} + \dots = 0$$

sont les valeurs de θ , c'est-à-dire de

$$(x' + \alpha x'' + \alpha^2 x''' + \dots)^\mu,$$

que l'on aurait en supposant que α devint successivement $\alpha^2, \alpha^3, \dots, \alpha^{\mu-1}$, il s'ensuit de ce qui a été dit dans le n° 68 que les racines de cette équa-

tion exprimeront justement les valeurs des quantités a', a'', a''', \dots élevées à la puissance μ .

Done, si l'on dénote ces racines par $\theta', \theta'', \theta''', \dots, \theta^{(\mu-1)}$, on aura

$$b = \frac{\sqrt[\mu]{\theta'}}{\mu}, \quad c = \frac{\sqrt[\mu]{\theta''}}{\mu}, \quad d = \frac{\sqrt[\mu]{\theta'''}}{\mu}, \dots$$

Maintenant, pour trouver avec facilité l'équation dont il s'agit, on élèvera le polynôme

$$x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x'''' + \dots$$

à la puissance μ , et, faisant attention que $\alpha^\mu = 1, \alpha^{\mu-1} = \alpha, \dots$, on aura pour θ une expression de cette forme

$$\theta = \xi + \alpha \xi' + \alpha^2 \xi'' + \alpha^3 \xi''' + \dots + \alpha^{\mu-1} \xi^{(\mu-1)},$$

où ξ, ξ', ξ'', \dots seront des fonctions des racines x', x'', x''', \dots sans α ; on changera α en y et ensuite on éliminera y par le moyen de l'équation (g) du n° 57; mais, si l'on ne veut pas employer la voie ordinaire de l'élimination, on s'y prendra de la manière suivante.

72. Puisque $\beta = \alpha^2, \gamma = \alpha^3, \dots$ (68), on aura

$$\begin{aligned} \theta' &= \xi + \alpha \xi' + \alpha^2 \xi'' + \alpha^3 \xi''' + \dots + \alpha^{\mu-1} \xi^{(\mu-1)}, \\ \theta'' &= \xi + \beta \xi' + \beta^2 \xi'' + \beta^3 \xi''' + \dots + \beta^{\mu-1} \xi^{(\mu-1)}, \\ \theta''' &= \xi + \gamma \xi' + \gamma^2 \xi'' + \gamma^3 \xi''' + \dots + \gamma^{\mu-1} \xi^{(\mu-1)}, \\ &\dots \end{aligned}$$

$\alpha, \beta, \gamma, \dots$ étant avec 1 les racines de l'équation $y^\mu - 1 = 0$.

Connaissant donc ainsi les racines de l'équation en θ , on pourra déterminer par leur moyen les valeurs des coefficients T, U, X, ...; car on aura, comme on sait,

$$T = \theta' + \theta'' + \theta''' + \dots,$$

$$U = \theta' \theta'' + \theta' \theta''' + \dots,$$

.....

On facilitera beaucoup cette détermination si l'on cherche la somme

des puissances premières, secondes, troisièmes, etc., jusqu'aux μ ^{èmes}, des racines $\theta', \theta'', \theta''', \dots$, et pour cela il sera utile de faire entrer dans le calcul la quantité

$$\theta^0 = \xi + \xi' + \xi'' + \xi''' + \dots + \xi^{(\mu-1)};$$

en sorte que les quantités $\theta^0, \theta', \theta'', \dots$ répondent aux racines $1, \alpha, \beta, \dots$ de l'équation $y^\mu - 1 = 0$.

Or, si l'on élève successivement le polynôme

$$\xi + \alpha\xi' + \alpha^2\xi'' + \alpha^3\xi''' + \dots + \alpha^{\mu-1}\xi^{(\mu-1)}$$

aux puissances seconde, troisième, etc., et qu'on dénote par $\xi_2, \xi_3, \xi_4, \dots$, les termes de ces puissances qui ne seront point affectés de α , après avoir substitué partout 1 à la place de α^μ , α à la place de $\alpha^{\mu+1}$ et ainsi de suite; il est facile de voir, par les propriétés des quantités $1, \alpha, \beta, \gamma, \dots$ (67), que les sommes des puissances premières, secondes, troisièmes, etc., des quantités $\theta^0, \theta', \theta'', \dots$ se réduiront à $\mu\xi, \mu\xi_2, \mu\xi_3, \dots$

Or

$$\theta^0 = \xi + \xi' + \xi'' + \xi''' + \dots + \xi^{(\mu-1)} = [x' + x'' + x''' + \dots + x^{(\mu-1)}]^\mu = (-m)^\mu;$$

donc, si l'on retranche respectivement des quantités $\mu\xi, \mu\xi_2, \mu\xi_3, \dots$ les puissances première, seconde, troisième, etc., de $(-m)^\mu$, les restes

$$\mu\xi - (-m)^\mu, \quad \mu\xi_2 - (-m)^{2\mu}, \quad \mu\xi_3 - (-m)^{3\mu}, \dots$$

seront les sommes des $\mu - 1$ racines $\theta', \theta'', \theta''', \dots$ de leurs carrés, de leurs cubes, etc., de sorte qu'on aura, par les formules connues,

$$T = \mu\xi - (-m)^\mu,$$

$$U = \frac{T[\mu\xi - (-m)^\mu]}{2} - \frac{\mu\xi_2 - (-m)^{2\mu}}{2},$$

$$X = \frac{U[\mu\xi - (-m)^\mu]}{3} - \frac{T(\mu\xi_2 - (-m)^{2\mu})}{3} + \frac{\mu\xi_3 - (-m)^{3\mu}}{3},$$

.....

73. Maintenant, si l'on fait dans les expressions des quantités T, U, X, ... toutes les permutations possibles entre les racines x', x'', x''', \dots ,

on ne trouvera pour chacune de ces quantités que $1.2.3\dots(\mu-2)$ valeurs différentes, lesquelles viendront uniquement des permutations entre les $\mu-2$ racines x''', x''', \dots ; ainsi l'on aura autant d'équations en θ , telles que

$$\theta^{\mu-1} - T\theta^{\mu-2} + U\theta^{\mu-3} - \dots = 0,$$

lesquelles étant multipliées ensemble donneront une équation en θ du degré $1.2.3\dots(\mu-1)$, et dont tous les coefficients seront déterminables par des fonctions rationnelles des coefficients m, n, p, \dots de l'équation proposée.

Cette équation en θ étant ainsi trouvée, si on la divise par une équation du degré $\mu-1$ telle que la précédente, on aura $\mu-1$ équations de condition entre les quantités T, U, X, \dots par lesquelles on pourra déterminer, par exemple, les valeurs de U, X, \dots en T , et l'on parviendra ensuite à une équation finale en T qui ne pourra monter qu'au degré $1.2.3\dots(\mu-2)$.

En effet, puisque la quantité T n'est susceptible que de $1.2.3\dots(\mu-2)$ valeurs différentes, si l'on appelle ces valeurs $T', T'', T''', \dots, T^{(\nu)}$, en supposant, pour abréger,

$$\nu = 1.2.3\dots(\mu-2),$$

on aura une équation en T , telle que

$$T^\nu - \varpi T^{\nu-1} + \rho T^{\nu-2} - \sigma T^{\nu-3} + \dots = 0,$$

dont les racines seront T', T'', T''', \dots , en sorte qu'on pourra, si l'on veut, déterminer *à priori* les valeurs des coefficients $\varpi, \rho, \sigma, \dots$ d'après celles des racines T', T'', \dots

De cette manière on aura donc l'équation en T directement et sans recourir à l'équation en θ du degré $\nu(\mu-1)$; et l'on pourra trouver aussi, indépendamment de cette dernière équation, les valeurs des autres coefficients U, X, \dots en T , comme nous le démontrerons plus bas dans la Section quatrième.

Concluons de tout ce qui précède que la méthode de MM. Euler et Bezout conduit nécessairement à une réduite du degré $1.2.3\dots(\mu-1)$,

laquelle, quand l'exposant μ de la proposée est un nombre premier, doit être décomposable en $1.2.3\dots(\mu-2)$ facteurs du $(\mu-1)^{i\text{ème}}$ degré chacun.

Ce résultat s'accorde, comme on voit, avec celui que l'on aurait par la méthode de M. Tschirnhaus; ainsi l'on y pourra appliquer des remarques semblables à celles que nous avons faites dans le n° 58.

74. Pour éclaircir la théorie précédente par un exemple, prenons l'équation du cinquième degré

$$x^5 + mx^4 + nx^3 + px^2 + qx + r = 0,$$

dont les racines soient désignées par x', x'', x''', x'''' , x''''' .

On supposera donc

$$x = a + by + cy^2 + dy^3 + ey^4,$$

et l'on regardera l'équation proposée comme le résultat de celle-ci et de l'équation à deux termes

$$y^5 + V = 0,$$

ou bien, en faisant, comme dans le n° 68, $V = -1$,

$$y^5 - 1 = 0.$$

MM. Euler et Bezout ont donné dans leurs Mémoires sur ce sujet l'équation finale, qui doit résulter de l'élimination de y dans le cas de $m=0$ et de $a=0$, et dont la comparaison avec la proposée fournit les quatre équations nécessaires pour la détermination des coefficients b, c, d, e ; mais ces savants Auteurs n'ont point donné le résultat qui doit provenir de ces quatre équations par l'élimination de trois quelconques des quatre inconnues qu'elles renferment, et cela à cause du travail immense que cette élimination demande. La méthode précédente fournit les moyens de trouver ce résultat *à priori*, et nous allons en donner un essai.

On aura d'abord (67)

$$a = -\frac{m}{5},$$

et ensuite (71)

$$b = \frac{\sqrt[5]{\theta'}}{5}, \quad c = \frac{\sqrt[5]{\theta''}}{5}, \quad d = \frac{\sqrt[5]{\theta'''}}{5}, \quad e = \frac{\sqrt[5]{\theta^{iv}}}{5},$$

$\theta', \theta'', \theta''', \theta^{iv}$ étant les quatre racines de l'équation

$$\theta^4 - T\theta^3 + U\theta^2 - X\theta + Y = 0,$$

laquelle sera un diviseur de l'équation du vingt-quatrième degré qu'on doit trouver pour la valeur de θ .

Maintenant, pour avoir la valeur des coefficients T, U, \dots , il faudra éléver le polynôme

$$x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x^{iv} + \alpha^4 x^v$$

à la cinquième puissance, ce qui donnera, à cause de $\alpha^5 = 1$, cet autre polynôme

$$\xi + \alpha \xi' + \alpha^2 \xi'' + \alpha^3 \xi''' + \alpha^4 \xi^{iv},$$

où

$$\begin{aligned} \xi = & x'^5 + x''^5 + x'''^5 + x^{iv^5} + x^v^5 + 120 x' x'' x''' x^{iv} x^v \\ & + 20 [x'^3 (x'' x^v + x''' x^{iv}) + x''^3 (x' x''' + x^{iv} x^v) + x'''^3 (x' x^v + x'' x^{iv}) \\ & \quad + x^{iv^3} (x' x'' + x''' x^v) + x^v^3 (x' x^{iv} + x'' x''')] \\ & + 30 [x' (x''^2 x^v^2 + x'''^2 x^{iv^2}) + x'' (x'^2 x'''^2 + x^{iv^2} x^v^2) + x''' (x'^2 x^v^2 + x''^2 x^{iv^2}) \\ & \quad + x^{iv} (x'^2 x''^2 + x'''^2 x^v^2) + x^v (x'^2 x^{iv^2} + x''^2 x'''^2)], \end{aligned}$$

$$\xi' = 5 (x'^4 x'' + x''^4 x''' + x'''^4 x^{iv} + x^{iv^4} x^v + x^v^4 x'),$$

.....

Et l'on aura d'abord

$$T = 5\xi + m^5.$$

Or, en considérant l'expression de ξ , on voit que les termes

$$x'^5 + x''^5 + x'''^5 + x^{iv^5} + x^v^5 + 120 x' x'' x''' x^{iv} x^v$$

peuvent s'exprimer immédiatement par les coefficients m, n, \dots de l'équation proposée; et il est facile de trouver que la valeur de ces termes sera

$$-m^5 + 5m^3n - 5m^2p + 5m(q - n^2) + 5np - 125r.$$

Donc, si l'on fait pour plus de simplicité

$$\begin{aligned} z = 2 & [x'^3(x''x^v + x'''x^{iv}) + x''^3(x'x''' + x^{iv}x^v) + x'''^3(x''x^{iv} + x'x^v) \\ & + x^{iv}^3(x'''x^v + x'x'') + x^v^3(x'x^{iv} + x''x''')] \\ & + 3[x'(x''^2x^{v2} + x'''^2x^{iv2}) + x''(x'^2x'''^2 + x^{iv2}x^{v2}) + x'''(x''^2x^{iv2} + x'^2x^{v2}) \\ & + x^{iv}(x'''^2x^{v2} + x'^2x''^2) + x^v(x'^2x^{iv2} + x''^2x'''^2)], \end{aligned}$$

on aura

$$T = 50z - 4m^5 + 25[m^3n - m^2p + m(q - n^2) + np - 25r],$$

et l'on trouvera que la quantité z ne sera susceptible que des six valeurs suivantes, que nous désignerons par z' , z'' , z''' , z^{iv} , z^v , z^{vi} :

$$\begin{aligned} z' = 2 & [x'^3(x''x^v + x'''x^{iv}) + x''^3(x'x''' + x^{iv}x^v) + x'''^3(x''x^{iv} + x'x^v) \\ & + x^{iv}^3(x'''x^v + x'x'') + x^v^3(x'x^{iv} + x''x''')] \\ & + 3[x'(x''^2x^{v2} + x'''^2x^{iv2}) + x''(x'^2x'''^2 + x^{iv2}x^{v2}) + x'''(x''^2x^{iv2} + x'^2x^{v2}) \\ & + x^{iv}(x'''^2x^{v2} + x'^2x''^2) + x^v(x'^2x^{iv2} + x''^2x'''^2)], \end{aligned}$$

$$\begin{aligned} z'' = 2 & [x'^3(x''x^{iv} + x'''x^v) + x''^3(x'x''' + x^{iv}x^v) + x'''^3(x''x^v + x'x^{iv}) \\ & + x^v^3(x'''x^{iv} + x'x'') + x^{iv}^3(x'x^v + x''x''')] \\ & + 3[x'(x''^2x^{iv2} + x'''^2x^{v2}) + x''(x'^2x'''^2 + x^{iv2}x^{v2}) + x'''(x''^2x^{v2} + x'^2x^{iv2}) \\ & + x^v(x'''^2x^{iv2} + x'^2x''^2) + x^{iv}(x'^2x^{v2} + x''^2x'''^2)], \end{aligned}$$

$$\begin{aligned} z''' = 2 & [x'^3(x''x^v + x'''x^{iv}) + x''^3(x'x^{iv} + x'''x^v) + x^{iv}^3(x''x''' + x'x^v) \\ & + x'''^3(x^{iv}x^v + x'x'') + x^v^3(x'x''' + x''x^{iv})] \\ & + 3[x'(x''^2x^{v2} + x'''^2x^{iv2}) + x''(x'^2x^{iv2} + x'''^2x^{v2}) + x^{iv}(x''^2x^{v2} + x'^2x^{iv2}) \\ & + x'''(x^{iv2}x^{v2} + x'^2x''^2) + x^v(x'^2x^{v2} + x''^2x^{iv2})], \end{aligned}$$

$$\begin{aligned} z^{iv} = 2 & [x'^3(x''x''' + x^{iv}x^v) + x''^3(x'x^{iv} + x'''x^v) + x^{iv}^3(x''x^v + x'x''')] \\ & + x^v^3(x'''x^{iv} + x'x'') + x'''^3(x'x^v + x''x^{iv})] \\ & + 3[x'(x''^2x'''^2 + x^{iv2}x^{v2}) + x''(x'^2x^{iv2} + x'''^2x^{v2}) + x^{iv}(x''^2x^{v2} + x'^2x'''^2) \\ & + x^v(x'''^2x^{iv2} + x'^2x''^2) + x'''(x'^2x^{v2} + x''^2x^{iv2})], \end{aligned}$$

$$\begin{aligned} z^v = 2 & [x'^3(x''x''' + x^{iv}x^v) + x''^3(x'x^v + x'''x^{iv}) + x^v^3(x''x^{iv} + x'x''')] \\ & + x^{iv}^3(x'''x^v + x'x'') + x'''^3(x'x^{iv} + x''x^v)] \\ & + 3[x'(x''^2x'''^2 + x^{iv2}x^{v2}) + x''(x'^2x^{v2} + x'''^2x^{iv2}) + x^v(x''^2x^{iv2} + x'^2x'''^2) \\ & + x^{iv}(x'''^2x^{v2} + x'^2x''^2) + x'''(x'^2x^{iv2} + x''^2x^{v2})], \end{aligned}$$

$$\begin{aligned}
z^{v_1} = & 2[x'^3(x''x^{iv} + x'''x^v) + x''^3(x'x^v + x'''x^{iv}) + x^{v_3}(x''x''' + x'x^{iv}) \\
& + x'''^3(x^{iv}x^v + x'x'') + x^{iv_3}(x'x''' + x''x^v)] \\
& + 3[x'(x''^2x^{iv_2} + x'''^2x^{v_2}) + x''(x'^2x^{v_2} + x'''^2x^{iv_2}) + x^v(x''^2x'''^2 + x'^2x^{iv_2}) \\
& + x'''(x^{iv_2}x^{v_2} + x'^2x''^2) + x^{iv}(x'^2x'''^2 + x''^2x^{v_2})].
\end{aligned}$$

En effet, si l'on fait dans ces formules telles permutations que l'on voudra entre les racines x' , x'' , x''' , ..., on verra toujours renaitre les mêmes formules; d'où il s'ensuit que les six quantités z' , z'' , z''' , ... seront nécessairement les racines d'une équation du sixième degré, telle que

$$z^6 - Az^5 + Bz^4 - Cz^3 + Dz^2 - Ez + F = 0,$$

dont les coefficients A , B , ... pourront par conséquent se déterminer par les règles connues.

On aura, par exemple,

$$A = z' + z'' + z''' + z^{iv} + z^v + z^{vi};$$

c'est-à-dire

$$\begin{aligned}
A = & 4x'^3(x''x''' + x''x^{iv} + x''x^v + x'''x^{iv} + x'''x^v + x^{iv}x^v) \\
& + 4x''^3(x'x''' + x'x^{iv} + x'x^v + x'''x^{iv} + x'''x^v + x^{iv}x^v) \\
& + 4x'''^3(x'x'' + x'x^{iv} + x'x^v + x''x^{iv} + x''x^v + x^{iv}x^v) \\
& + 4x^{iv_3}(x'x'' + x'x''' + x'x^v + x''x''' + x''x^v + x'''x^v) \\
& + 4x^{v_3}(x'x'' + x'x''' + x'x^{iv} + x''x''' + x''x^{iv} + x'''x^{iv}) \\
& + 6x'[(x''x''')^2 + (x''x^{iv})^2 + (x''x^v)^2 + (x'''x^{iv})^2 + (x'''x^v)^2 + (x^{iv}x^v)^2] \\
& + 6x''[(x'x''')^2 + (x'x^{iv})^2 + (x'x^v)^2 + (x'''x^{iv})^2 + (x'''x^v)^2 + (x^{iv}x^v)^2] \\
& + 6x'''[(x'x'')^2 + (x'x^{iv})^2 + (x'x^v)^2 + (x''x^{iv})^2 + (x''x^v)^2 + (x^{iv}x^v)^2] \\
& + 6x^{iv}[(x'x'')^2 + (x'x''')^2 + (x'x^v)^2 + (x''x''')^2 + (x''x^v)^2 + (x'''x^v)^2] \\
& + 6x^v[(x'x'')^2 + (x'x''')^2 + (x'x^{iv})^2 + (x''x''')^2 + (x''x^{iv})^2 + (x'''x^{iv})^2].
\end{aligned}$$

Or on a dans l'équation proposée

$$-m = x' + x'' + x''' + x^{iv} + x^v,$$

$$n = x'x'' + x'x''' + x'x^{iv} + x'x^v + x''x''' + x''x^{iv} + x''x^v + x'''x^{iv} + x'''x^v + x^{iv}x^v;$$

donc les cinq premiers membres de la valeur de A deviendront

$$\begin{aligned}
 & 4n(x'^3 + x''^3 + x'''^3 + x^{1v3} + x^{v3}) \\
 & + 4m(x'^4 + x''^4 + x'''^4 + x^{1v4} + x^{v4}) + 4(x'^5 + x''^5 + x'''^5 + x^{1v5} + x^{v5}) \\
 & = 4n(-m^3 + 3mn - 3p) + 4m(m^4 - 4m^2n + 4mp - 4q + 2n^2) \\
 & + 4[-m^5 + 5m^3n - 5m^2p + 5m(q - n^2) - 5r + 5np].
 \end{aligned}$$

Pour trouver la valeur des cinq derniers membres de la quantité A, il faudra commencer par chercher celle de la quantité

$$\begin{aligned}
 & (x'x'')^2 + (x'x''')^2 + (x'x^{1v})^2 + (x'x^{v})^2 + (x''x''')^2 \\
 & + (x''x^{1v})^2 + (x''x^{v})^2 + (x'''x^{1v})^2 + (x'''x^{v})^2 + (x^{1v}x^{v})^2,
 \end{aligned}$$

que nous désignerons, pour abréger, par l ; or, si l'on carre la valeur de n , on aura

$$\begin{aligned}
 n^2 & = l + 2n(x'^2 + x''^2 + x'''^2 + x^{1v2} + x^{v2}) \\
 & + 2m(x'^3 + x''^3 + x'''^3 + x^{1v3} + x^{v3}) \\
 & + 2(x'^4 + x''^4 + x'''^4 + x^{1v4} + x^{v4}) \\
 & = l + 2n(m^2 - 2n) + 2m(-m^3 + 3mn - 3p) \\
 & + 2(m^4 - 4m^2n + 4mp - 4q + 2n^2),
 \end{aligned}$$

d'où

$$\begin{aligned}
 l & = n^2 - 2n(m^2 - 2n) - 2m(-m^3 + 3mn - 3p) \\
 & - 2(m^4 - 4m^2n + 4mp - 4q + 2n^2);
 \end{aligned}$$

maintenant il est facile de trouver que la valeur des cinq derniers membres de A sera exprimée par

$$\begin{aligned}
 & 6l(x' + x'' + x''' + x^{1v} + x^{v}) \\
 & - 6(m^2 - 2n)(x'^3 + x''^3 + x'''^3 + x^{1v3} + x^{v3}) + 6(x'^5 + x''^5 + x'''^5 + x^{1v5} + x^{v5}) \\
 & = -6lm - 6(m^2 - 2n)(-m^3 + 3mn - 3p) \\
 & + 6[-m^5 + 5m^3n - 5m^2p + 5m(q - n^2) - 5r + 5np];
 \end{aligned}$$

de sorte qu'en rassemblant toutes ces quantités on aura enfin

$$\begin{aligned} A = & -6mn(3n - 2m^2) + 2(8n + 3m^2)(-m^3 + 3mn - 3p) \\ & + 16m(m^4 - 4m^2n + 4mp - 4q + 2n^2) \\ & + 10[-m^5 + 5m^3n - 5m^2p + 5m(q - n^2) - 5r + 5np]. \end{aligned}$$

On pourra trouver d'une manière semblable la valeur de chacun des autres coefficients B, C, ... de l'équation z , et l'on en abrégera beaucoup le calcul si l'on fait usage des règles données par M. Cramer à la fin de son *Introduction à l'Analyse des lignes courbes*, pour calculer la somme des produits des racines d'une équation quelconque, prises deux à deux, ou trois à trois, ou, etc., et élevées chacune à une puissance quelconque donnée; mais nous n'entrerons point ici dans ce détail qui, outre qu'il exigerait des calculs très-longs, ne saurait d'ailleurs jeter aucune lumière sur la résolution des équations du cinquième degré; car comme la réduite en z est du sixième degré, elle ne sera pas résoluble à moins qu'elle ne puisse s'abaisser à un degré inférieur au cinquième; or c'est ce qui ne me paraît guère possible d'après la forme des racines z' , z'' , ... de cette équation.

75. Nous avons supposé depuis le n° 70 jusqu'ici, que l'exposant μ de l'équation proposée était un nombre premier; voyons maintenant ce qui doit arriver lorsque μ sera un nombre composé.

Dans ce cas il est facile de prouver par des raisonnements analogues à ceux du n° 59 que les conclusions du numéro cité et des numéros suivants n'auront lieu que tant qu'on ne substituera à la place de α que les puissances α^ν , α^ϖ , α^ρ , ..., dont les exposants ν , ϖ , ρ , ... sont des nombres premiers à μ ; d'où il s'ensuit :

1° Qu'en désignant par λ — 1 le nombre des exposants ν , ϖ , ρ , ... dont il s'agit, l'équation en θ , qui est généralement du degré 1.2.3...(μ — 1), sera décomposable en $\frac{1.2.3...(\mu-1)}{\lambda}$ équations, chacune du degré λ , et telle que

$$\theta^\lambda - T\theta^{\lambda-1} + U\theta^{\lambda-2} - X\theta^{\lambda-3} + \dots = 0,$$

les coefficients T, U, X, \dots étant donnés chacun par une équation du degré $\frac{1 \cdot 2 \cdot 3 \dots (\mu - 1)}{\lambda}$.

2° Que les λ racines de cette équation en θ étant désignées par $\theta', \theta'', \theta''', \dots$, les quantités $\frac{\sqrt[\mu]{\theta'}}{\mu}, \frac{\sqrt[\mu]{\theta''}}{\mu}, \frac{\sqrt[\mu]{\theta'''}}{\mu}, \dots$ exprimeront les valeurs de ceux des coefficients k, h, g, \dots, c, b dont le rang, à commencer par k , sera marqué par les nombres $1, \nu, \varpi, \rho, \dots$ premiers à μ ; de sorte que tous ces coefficients seront donnés par une même équation.

3° Que pour appliquer la méthode du n° 71 à la recherche des coefficients T, V, X, \dots , il ne faudra pas se servir de l'équation (g) du n° 57 pour éliminer γ , mais de l'équation (i) qu'on trouvera par la méthode du n° 60, et dont les racines seront $\alpha, \alpha^\nu, \alpha^\varpi, \alpha^\rho, \dots$; que, par conséquent, si l'on veut faire usage de la méthode du n° 72 pour trouver les coefficients dont il s'agit, il faudra d'abord chercher d'après l'équation (i) les sommes des racines $\alpha, \alpha^\nu, \alpha^\varpi, \alpha^\rho, \dots$, de leurs carrés, de leurs cubes, etc., qu'on dénotera par S', S'', S''', \dots ; ensuite ayant élevé successivement le polynôme

$$\xi + \alpha \xi' + \alpha^2 \xi'' + \alpha^3 \xi''' + \dots + \alpha^{\mu-1} \xi^{(\mu-1)}$$

aux puissances deuxième, troisième, etc., et représentant ces puissances par

$$\xi_2 + \alpha \xi'_2 + \alpha^2 \xi''_2 + \alpha^3 \xi'''_2 + \dots,$$

$$\xi_3 + \alpha \xi'_3 + \alpha^2 \xi''_3 + \alpha^3 \xi'''_3 + \dots,$$

.....,

on aura les quantités

$$\lambda \xi + S' \xi' + S'' \xi'' + S''' \xi''' + \dots,$$

$$\lambda \xi_2 + S' \xi'_2 + S'' \xi''_2 + S''' \xi'''_2 + \dots,$$

$$\lambda \xi_3 + S' \xi'_3 + S'' \xi''_3 + S''' \xi'''_3 + \dots,$$

.....

pour les sommes des racines $\theta', \theta'', \theta''', \dots$ élevées aux puissances première, deuxième, troisième, etc., d'où il s'ensuit qu'on aura enfin par

les formules connues

$$T = \lambda \xi + S' \xi' + S'' \xi'' + S''' \xi''' + \dots,$$

$$U = \frac{1}{2} T (\lambda \xi + S' \xi' + S'' \xi'' + \dots) - \frac{1}{2} (\lambda \xi_2 + S' \xi'_2 + S'' \xi''_2 + \dots),$$

$$X = \frac{1}{3} U (\lambda \xi + S' \xi' + S'' \xi'' + \dots) - \frac{1}{3} T (\lambda \xi_2 + S' \xi'_2 + S'' \xi''_2 + \dots)$$

$$+ \frac{1}{3} (\lambda \xi_3 + S' \xi'_3 + S'' \xi''_3 + \dots),$$

.....

76. Pour trouver maintenant les valeurs des autres coefficients qui, dans la série k, h, g, \dots, c, b occupent des places marquées par des nombres commensurables à μ , supposons, en général, $\mu = \nu \varpi$, et que l'on cherche ceux des coefficients dont il s'agit dont l'exposant du rang sera multiple de ν ; il est facile de voir par ce qui a été dit dans le n° 68, que si l'on exprime, pour plus de simplicité, ces coefficients par

$$\frac{a^{(\nu)}}{\mu}, \quad \frac{a^{(2\nu)}}{\mu}, \quad \frac{a^{(3\nu)}}{\mu}, \dots,$$

et qu'on fasse $\alpha^\nu = \omega$, on aura

$$a^{(\nu)} = x' + \omega x'' + \omega^2 x''' + \omega^3 x^{(4\nu)} + \dots + \omega^{\mu-1} x^{(\mu)},$$

et, pour avoir les autres quantités $a^{(2\nu)}, a^{(3\nu)}, \dots$, il n'y aura qu'à changer successivement ω en $\omega^2, \omega^3, \dots$

Soit, à l'imitation de ce qui a été fait dans le n° 69,

$$t = x' + \omega x'' + \omega^2 x''' + \omega^3 x^{(4\nu)} + \dots + \omega^{\mu-1} x^{(\mu)},$$

et cherchons de même quelle doit être la nature de l'équation en t .

Pour cet effet on remarquera d'abord que, puisque $\omega = \alpha^\nu$, on aura

$$\omega^\nu = \alpha^{\nu\nu} = \alpha^\mu = 1;$$

et de là

$$\omega^{\nu+1} = \omega, \quad \omega^{\nu+2} = \omega^2, \dots$$

En général, puisque $1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{\mu-1}$ sont les racines de l'équation

$y^{\varpi} - 1 = 0$, les puissances $1, \omega, \omega^2, \omega^3, \dots, \omega^{\varpi-1}$ seront les racines de l'équation $y^{\varpi} - 1 = 0$ (24).

Faisant donc rentrer les puissances de ω plus hautes que $\omega^{\sigma-1}$ dans la classe des inférieures, l'expression de t deviendra de cette forme

$$t = z' + \omega z'' + \omega^2 z''' + \omega^3 z^{iv} + \dots + \omega^{\sigma-1} z^{(\sigma)},$$

en supposant

77. En considérant maintenant l'équation en t dans toute sa généralité, il est clair qu'elle devrait être du degré $1.2.3\dots\mu$, puisqu'il y a autant de permutations possibles entre les μ racines x', x'', x''', \dots , et dont chacune doit donner une valeur particulière de t ; mais si parmi ces valeurs il y en a d'égales, on pourra en faire abstraction et abaisser par là l'équation en t à un moindre degré; or c'est précisément ce qui a lieu dans le cas présent.

En effet, il est visible que la quantité z' demeurera toujours la même, quelque permutation qu'on fasse entre les ν racines $x', x^{(\varpi+1)}, x^{(2\varpi+1)}, \dots$; donc, puisque ν choses admettent $1.2.3.\dots.\nu$ permutations, il s'ensuit d'abord que les $1.2.3.\dots.\nu$ valeurs de t seront telles que chacune se trouvera répétée $1.2.3.\dots.\nu$ fois; en sorte que parmi ces valeurs il ne pourra y en avoir que $\frac{1.2.3.\dots.\nu}{1.2.3.\dots.\nu}$ de différentes entre elles.

Considérons ensuite la quantité z'' , on prouvera de la même manière que chacune de ces dernières valeurs devra aussi se trouver répétée $1.2.3\dots\nu$ fois, ce qui réduira le nombre des valeurs différentes de t à $\frac{1.2.3\dots\nu}{(1.2.3\dots\nu)^2}$.

En continuant le même raisonnement à l'égard des autres quantités z'' , z^{IV} , ..., $z^{(\infty)}$, on en conclura enfin que le nombre des valeurs différentes

de t ne sera que $\frac{1 \cdot 2 \cdot 3 \dots \mu}{(\nu \cdot 2 \cdot 3 \dots \nu)^\omega}$; de sorte que l'équation en t ne montera qu'au degré $\frac{1 \cdot 2 \cdot 3 \dots \mu}{(\nu \cdot 2 \cdot 3 \dots \nu)^\omega}$.

78. Cela posé, si l'on compare maintenant l'expression précédente de t avec celle du n° 69, on verra aisément qu'elle est susceptible de remarques semblables, relativement aux permutations des quantités z' , z'' , z''' , ... entre elles; d'où l'on conclura :

1° Qu'en supposant ω égal à un nombre premier, l'équation en t ne renfermera que des puissances de t dont les exposants soient multiples de ω ; de sorte qu'en faisant $t^\omega = \theta$, on aura une équation en θ du degré

$$\frac{1 \cdot 2 \cdot 3 \dots \mu}{\omega(\nu \cdot 2 \cdot 3 \dots \nu)^\omega};$$

2° Que cette équation sera toujours décomposable en $\frac{1 \cdot 2 \cdot 3 \dots \mu}{(\omega - 1)\omega(\nu \cdot 2 \cdot 3 \dots \nu)^\omega}$ équations de la forme

$$\theta^{\omega-1} - T\theta^{\omega-2} + U\theta^{\omega-3} - X\theta^{\omega-4} + \dots = 0,$$

où les coefficients T , U , ... ne dépendront que d'une équation du degré

$$\frac{1 \cdot 2 \cdot 3 \dots \mu}{(\omega - 1)\omega(\nu \cdot 2 \cdot 3 \dots \nu)^\omega};$$

3° Que, si l'on désigne par θ' , θ'' , θ''' , ... les $\omega - 1$ racines de l'équation précédente, les quantités

$$\frac{\sqrt[\omega]{\theta'}}{\mu}, \quad \frac{\sqrt[\omega]{\theta''}}{\mu}, \quad \frac{\sqrt[\omega]{\theta'''}}{\mu}, \dots, \quad \frac{\sqrt[\omega]{\theta^{(\omega-1)}}}{\mu}$$

seront les valeurs de ceux des coefficients k , h , g , ..., c , b qui occupent dans cette série les places $\nu^{i\text{ème}}$, $(2\nu)^{i\text{ème}}$, $(3\nu)^{i\text{ème}}$, ... jusqu'à la $(\mu - \nu)^{i\text{ème}}$ inclusivement, ou, ce qui revient au même (à cause que le nombre de tous les coefficients a , b , c , ..., k est μ), des coefficients qui occupent les mêmes places dans la série a , b , c , ..., k ;

4° Que, pour trouver les valeurs des coefficients T , U , X , ..., on pourra se servir pareillement des méthodes des n°s 71 et 72, en ayant seulement attention de mettre partout l'exposant ω à la place de l'exposant μ ;

5° Que, si ϖ n'est pas un nombre premier, il faudra apporter aux conclusions précédentes des modifications relatives à la nature du nombre ϖ et qu'on trouvera aisément par des considérations semblables à celles qui ont fait l'objet du n° 75.

79. On voit donc, d'après ce qui précède, que, lorsque l'exposant μ de l'équation proposée est un nombre composé, les coefficients b, c, d, \dots ne peuvent pas être les racines d'une même équation, comme cela a lieu dans le cas où l'exposant μ est un nombre premier, mais que ces coefficients dépendent alors d'équations différentes suivant que leurs places dans la série a, b, c, d, \dots sont marquées par des nombres dont les plus grandes mesures avec le nombre μ sont différentes.

Cependant il ne sera pas nécessaire de chercher et de résoudre toutes ces différentes équations; car les coefficients dont il s'agit dépendent mutuellement les uns des autres, en sorte que dès que l'on aura trouvé la valeur d'un de ces coefficients on pourra en déduire aisément celles de tous les autres. En effet, si l'on suppose que l'on élimine y de l'équation (k) du n° 65 par le moyen de l'équation $y^\mu - 1 = 0$, et qu'on compare ensuite l'équation résultante terme à terme avec la proposée, on aura autant d'équations qu'il y a de coefficients indéterminés a, b, c, \dots , par lesquelles on pourra déterminer chacun de ces coefficients: or, à l'exception du premier coefficient a qui se trouvera donné par une équation où il n'y aura point d'autres inconnues, tous les autres coefficients inconnus b, c, \dots se trouveront mêlés entre eux, de manière que par la méthode ordinaire d'élimination on pourra déterminer la valeur de chacune de ces inconnues par une autre quelconque d'entre elles; sur quoi on fera des remarques semblables à celles du n° 58.

80. M. Bezout, dans le dessein de simplifier et de faciliter l'usage de sa méthode lorsque l'exposant de l'équation proposée est un nombre composé, a donné une seconde méthode qui parait en quelque manière plus générale que la première, mais qui revient cependant à la même dans le fond, comme nous l'allons faire voir.

Suivant cette méthode, si l'exposant μ de l'équation proposée est re-

présenté par le produit $\nu\varpi$ des deux nombres ν et ϖ , on prendra deux équations de cette forme

Et éliminant y on aura une équation finale en x du degré $\nu\varpi$ qu'on comparera terme à terme avec la proposée; ce qui donnera $\nu\varpi$ équations particulières entre les coefficients $a, b, c, \dots, a', b', c', \dots$, dont le nombre est aussi $\nu\varpi$; de sorte qu'on pourra par là déterminer chacun de ces coefficients.

Or, comme l'équation $y^\pi - 1 = 0$ donne π valeurs de y , on aura, par la substitution successive de ces valeurs, autant d'équations en x , chacune du degré ν ; d'où l'on tirera $\mu\nu$ valeurs de x , qui seront les racines de l'équation proposée.

Il est clair, par la théorie de l'élimination exposée dans le n° 13, que l'équation résultante de l'élimination de y dans les deux équations ci-dessus ne sera autre chose que le produit de toutes les équations (l) que l'on aurait en y mettant à la place de y les ϖ racines de l'équation $y^\varpi - 1 = 0$; d'où l'on voit que l'esprit de cette méthode consiste à décomposer l'équation proposée du degré ϖ en ϖ équations, chacune du $y^{i\text{ème}}$ degré, et cela moyennant une équation du degré ϖ , de la forme $y^\varpi - 1 = 0$.

Toute la difficulté consiste dans la détermination des coefficients inconnus $a, b, c, \dots, a', b', c', \dots$; c'est pourquoi il est bon de rechercher *à priori* quelle doit être la nature des équations par lesquelles ces quantités doivent se déterminer.

81. Supposons donc que l'équation proposée du degré $\mu = \nu \varpi$, et

donc les racines sont x', x'', x''', \dots , soit le produit de ϖ équations telles que

il faudra que chacune de ces équations renferme ν racines de la proposée; de sorte qu'en partageant la totalité des μ . racines $x', x'', x''', \dots, x^{(\mu)}$ en τ systèmes de ν racines chacun, et tels par exemple que

on aura par la nature des équations z' égal à la somme, u' égal à la somme des produits deux à deux, v' égal à la somme des produits trois à trois, etc., des racines x' , $x^{(\varpi+1)}$, $x^{(2\varpi+1)}$, ..., $x^{(\mu-\varpi+1)}$; de même on aura z'' égal à la somme, u'' égal à la somme des produits deux à deux, v'' égal à la somme des produits trois à trois, etc., des racines x'' , $x^{(\varpi+2)}$, $x^{(2\varpi+2)}$, ..., $x^{(\mu-\varpi+2)}$, et ainsi de suite.

Or, si l'on désigne par $\iota, \omega, \varphi, \psi, \dots$ les ϖ racines de l'équation $y^\varpi - 1 = 0$, on aura (numéro précédent)

et de même

et ainsi de suite.

Done, puisque par la nature de l'équation $y^{\varpi} - 1 = 0$ qui manque de tous les termes intermédiaires on a

$$\begin{aligned}1 + \omega + \varphi + \psi + \dots &= 0, \\1 + \omega^2 + \varphi^2 + \psi^2 + \dots &= 0, \\1 + \omega^3 + \varphi^3 + \psi^3 + \dots &= 0, \\&\dots \dots \dots \dots \dots \dots \dots\end{aligned}$$

on pourra déterminer les valeurs des quantités $a, b, c, \dots, k, a', b', c', \dots, k', a'', b'', c'', \dots, k''$, ... par une méthode semblable à celle du n° 67; et il viendra

ensuite

et ainsi de suite.

82. Examinons les valeurs des quantités a, b, c, \dots, k , et il est d'abord clair que la valeur de ϖa sera égale à la somme de toutes les racines $x', x'', x''', \dots, x^{(\mu)}$; de sorte que l'on aura $\varpi a = -m$; et par conséquent

$$a = -\frac{m}{\pi}.$$

Ensuite, si l'on met $\omega^2, \omega^3, \dots$ à la place de φ, ψ, \dots , en sorte que les racines de l'équation $y^\omega - 1 = 0$ soient représentées par $1, \omega, \omega^2, \omega^3, \dots, \omega^{\omega-1}$ (24), on aura

$$\varpi k = z' + \omega z'' + \omega^2 z''' + \omega^3 z^{(4)} + \dots + \omega^{w-1} z^{(w)},$$

et pour avoir les valeurs des quantités $\varpi h, \varpi g, \dots$ il n'y aura qu'à changer successivement, dans cette expression, la racine ω en $\omega^2, \omega^3, \dots$

Or l'expression précédente de ϖk est la même que celle de la quan-

tité $a^{(v)}$ ou t du n° 76; par conséquent celles de ϖh , $\varpi g, \dots$ seront aussi les mêmes que celles des quantités $a^{(2v)}$, $a^{(3v)}, \dots$ du même numéro; d'où il est facile de conclure que les coefficients a, b, c, d, \dots de l'équation (l) du n° 80, étant multipliés par ϖ , seront respectivement égaux à ceux des coefficients a, b, c, \dots de l'équation (k) du n° 65, qui occuperont dans la série a, b, c, \dots , les places marquées par les nombres $1, v, 2v, 3v, \dots, \mu - v$, chacun de ces coefficients étant multiplié par μ .

Ainsi l'on pourra appliquer sur-le-champ aux coefficients a, b, c, \dots de la formule ci-dessus les mêmes conclusions des n°s 76 et suivants.

83. Quant aux autres coefficients $a', b', c', \dots, a'', b'', c'', \dots$ de la même formule (l) on pourra, si l'on veut, les faire dépendre des précédents, ou simplement d'un quelconque d'entre eux, par des considérations semblables à celles du n° 79; on peut aussi déterminer *à priori*, d'après les formules du n° 81, le degré et la forme de l'équation d'où chacun de ces coefficients doit dépendre immédiatement.

Pour cet effet il suffira de remarquer que les quantités u', u'', u''', \dots sont analogues aux quantités correspondantes z', z'', z''', \dots en ce que ces quantités sont des fonctions des mêmes racines, lesquelles ont la propriété de demeurer les mêmes, quelques permutations qu'on fasse entre ces racines; il en est de même des quantités v', v'', v''', \dots ; d'où il s'ensuit que l'on pourra appliquer aux coefficients $b', c', d', \dots, b'', c'', d'', \dots$ des raisonnements et des conclusions semblables à celles qui ont lieu pour les coefficients b, c, d, \dots .

Mais à l'égard des coefficients a', a'', \dots il faudra les considérer à part, et après avoir prouvé par des raisonnements analogues à ceux du n° 77 que chacune de ces quantités ne pourra avoir que $\frac{1.2.3.\dots\mu}{(1.2.3.\dots v)^\varpi}$ valeurs différentes, on remarquera que ces quantités ne souffrant aucun changement par les permutations des quantités $u', u'', u''', \dots, u^{(\varpi)}$, ou $v', v'', v''', \dots, v^{(\varpi)}$, ou, etc., entre elles, il faudra encore diviser le nombre $\frac{1.2.3.\dots\mu}{(1.2.3.\dots v)^\varpi}$ par $1.2.3.\dots\varpi$ pour avoir celles des valeurs différentes de chacun des coefficients a', a'', \dots ; d'où il s'ensuit que chacun de ces mêmes

coefficients devra être déterminé par une équation particulière du degré

$$\frac{1 \cdot 2 \cdot 3 \cdots \mu}{1 \cdot 2 \cdot 3 \cdots \varpi (1 \cdot 2 \cdot 3 \cdots \nu)^\varpi}.$$

84. Supposons que l'équation proposée soit d'un degré pair, et prenons $\varpi = 2$, en sorte que l'on ait $\mu = 2\nu$; dans ce cas l'équation $y^\varpi - 1 = 0$ deviendra

$$y^2 - 1 = 0,$$

laquelle donne les deux racines

$$y = 1 \quad \text{et} \quad y = -1;$$

et il faudra, suivant la méthode précédente, que l'équation proposée

$$x^{2\nu} + mx^{2\nu-1} + nx^{2\nu-2} + px^{2\nu-3} + \dots = 0$$

soit formée du produit de ces deux-ci

$$\begin{aligned} x^\nu - (a + b)x^{\nu-1} + (a' + b')x^{\nu-2} - (a'' + b'')x^{\nu-3} + \dots &= 0, \\ x^\nu - (a - b)x^{\nu-1} + (a' - b')x^{\nu-2} - (a'' - b'')x^{\nu-3} + \dots &= 0. \end{aligned}$$

Ainsi l'on aura

$$a = -\frac{m}{2} \quad \text{et} \quad b = \frac{z' - z''}{2},$$

où

$$\begin{aligned} z' &= x' + x'' + x^v + \dots + x^{(2\nu-1)}, \\ z'' &= x'' + x^{v_1} + x^{v_2} + \dots + x^{(2\nu)}. \end{aligned}$$

Et l'on trouvera que l'équation en b sera du degré

$$\frac{1 \cdot 2 \cdot 3 \cdots 2\nu}{(1 \cdot 2 \cdot 3 \cdots \nu)^2}, \quad \text{c'est-à-dire} \quad \frac{(\nu + 1)(\nu + 2)(\nu + 3) \cdots 2\nu}{1 \cdot 2 \cdot 3 \cdots \nu},$$

avec tous les exposants pairs.

Donc, si l'on suppose que l'équation proposée ait un diviseur du degré ν et tel que

$$x^\nu + m'x^{\nu-1} + n'x^{\nu-2} + p'x^{\nu-3} + \dots = 0,$$

on trouvera pour m' une équation du degré

$$\frac{(\nu+1)(\nu+2)(\nu+3)\dots(2\nu)}{1.2.3\dots\nu},$$

ce qui s'accorde avec ce que l'on sait d'ailleurs, puisque ce nombre exprime celui des combinaisons de 2ν choses prises ν à ν .

Et comme en faisant

$$-m' = a + b = -\frac{m}{2} + b$$

on doit avoir une équation en b qui n'ait que des puissances paires, il s'ensuit que l'équation en m' sera telle que, si l'on y fait disparaître le second terme, tous les termes alternatifs disparaîtront en même temps, comme nous l'avons vu par rapport aux équations du quatrième degré (35).

85. Si l'équation proposée est du sixième degré, en sorte que $\nu = 3$, et qu'on fasse $4b^2 = \theta$, on aura une équation en θ du degré

$$\frac{4.5.6}{2 \times 1 \cdot 2 \cdot 3} = 10.$$

M. Bezout pense que cette équation pourra se décomposer en deux équations, au moyen d'une équation du second degré : c'est de quoi je doute fort; en effet, les racines de l'équation en θ seront représentées par ces dix quantités, lesquelles renferment toutes les valeurs de $(z' - z'')^2$ qui peuvent résulter des permutations entre les six racines x', x'', x''', \dots

$$\begin{aligned} & (x' + x'' + x''' - x^{iv} - x^v - x^{vi})^2, \\ & (x' + x'' + x^{iv} - x''' - x^v - x^{vi})^2, \\ & (x' + x'' + x^v - x^{iv} - x''' - x^{vi})^2, \\ & (x' + x'' + x^{vi} - x^{iv} - x^v - x''')^2, \\ & (x' + x^{iv} + x''' - x'' - x^v - x^{vi})^2, \\ & (x' + x^v + x''' - x^{iv} - x'' - x^{vi})^2, \\ & (x' + x^{vi} + x''' - x^{iv} - x^v - x'')^2, \\ & (x' + x^{iv} + x^v - x'' - x''' - x^{vi})^2, \\ & (x' + x^{iv} + x^{vi} - x'' - x''' - x^v)^2, \\ & (x' + x^v + x^{vi} - x'' - x''' - x^{iv})^2. \end{aligned}$$

Or, si l'on suppose que les deux facteurs de l'équation dont il s'agit soient représentés par

$$\begin{aligned}\theta^5 - f\theta^4 + g\theta^3 - h\theta^2 + i\theta - k &= 0, \\ \theta^5 - f'\theta^4 + g'\theta^3 - h'\theta^2 + i'\theta - k' &= 0,\end{aligned}$$

il faudra que f soit égale à la somme de cinq des dix quantités précédentes, et que f' soit égale à la somme des cinq autres; et pour que les coefficients f et f' ne soient affectés que de radicaux du second degré, il faudra que ces deux coefficients soient les racines d'une équation du second degré telle que

$$y^2 - My + N = 0,$$

M et N étant des fonctions rationnelles des coefficients m, n, p, \dots de l'équation proposée; on aura donc

$$M = f + f' \quad \text{et} \quad N = ff';$$

de sorte que tant la somme que le produit des deux quantités f et f' devront être des fonctions rationnelles de m, n, p, \dots et par conséquent des fonctions des racines x', x'', x''', \dots telles, qu'elles ne changent point de valeur, quelque permutation qu'on fasse entre ces racines; or cette condition a bien lieu à l'égard de la somme $f + f'$, qui est égale à la somme de toutes les dix quantités ci-dessus; mais il n'en est pas de même à l'égard du produit ff' ; car on peut s'assurer facilement que, de quelque manière qu'on partage la somme des dix racines précédentes en deux sommes partielles de cinq racines chacune, le produit de ces deux sommes partielles n'aura jamais la propriété de demeurer invariable dans toutes les permutations qu'on pourra faire des racines x', x'', x''', \dots entre elles.

On pourrait dire qu'il ne serait peut-être pas nécessaire que les deux quantités f et f' fussent les racines d'une même équation du second degré, et que l'une de ces quantités pourrait dépendre d'une équation et l'autre d'une autre; mais pour détruire cette exception il suffit de considérer que, supposant f déterminée par une équation du second degré

telle que

$$f^2 - Mf + N = 0,$$

les deux racines de cette équation seront nécessairement égales chacune à la somme de cinq quelconques des dix quantités précédentes; et il faudra que ces deux sommes ajoutées ensemble produisent une quantité M qui ait la propriété de demeurer la même, quelque permutation qu'on fasse entre les racines x', x'', x''', \dots ; ce qui ne saurait avoir lieu à moins que les deux sommes dont nous parlons ne renferment toutes les dix quantités en question; par conséquent, l'une étant la somme de cinq de ces quantités, l'autre devra être nécessairement celle des cinq autres.

SECTION QUATRIÈME.

CONCLUSION DES RÉFLEXIONS PRÉCÉDENTES, AVEC QUELQUES REMARQUES GÉNÉRALES SUR LA TRANSFORMATION DES ÉQUATIONS, ET SUR LEUR RÉDUCTION OU ABAISSEMENT A UN MOINDRE DEGRÉ.

86. On a dû voir par l'analyse que nous venons de donner des principales méthodes connues pour la résolution des équations, que ces méthodes se réduisent toutes à un même principe général, savoir à trouver des fonctions des racines de l'équation proposée, lesquelles soient telles : 1^o que l'équation ou les équations par lesquelles elles seront données, c'est-à-dire dont elles seront les racines (équations qu'on nomme communément les *réduites*), se trouvent d'un degré moindre que celui de la proposée, ou soient au moins décomposables en d'autres équations d'un degré moindre que celui-là; 2^o que l'on puisse en déduire aisément les valeurs des racines cherchées.

L'art de résoudre les équations consiste donc à découvrir des fonctions des racines, qui aient les propriétés que nous venons d'énoncer; mais est-il toujours possible de trouver de telles fonctions, pour les équations d'un degré quelconque, c'est-à-dire pour tel nombre de racines qu'on voudra? C'est sur quoi il paraît très-difficile de pouvoir prononcer en général.

A l'égard des équations qui ne passent pas le quatrième degré, les fonctions les plus simples qui donnent leur résolution peuvent être représentées par la formule générale

$$x' + yx'' + y^2x''' + \dots + y^{\mu-1}x^{(\mu)},$$

$x', x'', x''', \dots, x^{(\mu)}$ étant les racines de l'équation proposée, qu'on suppose être du degré μ , et y étant une racine quelconque autre que l'unité de l'équation

$$y^\mu - 1 = 0,$$

c'est-à-dire une racine quelconque de l'équation

$$y^{\mu-1} + y^{\mu-2} + y^{\mu-3} + \dots + 1 = 0,$$

comme il résulte de tout ce qu'on a exposé dans les deux premières Sections, touchant la résolution des équations du troisième et du quatrième degré.

Quant à celle des équations du second degré dont nous avons jusqu'à présent fait abstraction, il est visible qu'elle se rapporte aussi au même principe; car en faisant $\mu = 2$, on aura la fonction $x' + yx''$; et l'équation $y + 1 = 0$ donnant $y = -1$, cette fonction deviendra $x' - x''$, c'est-à-dire la différence des deux racines; or l'art de résoudre les équations du second degré consiste uniquement à faire évanouir le second terme pour avoir une réduite qui, ne contenant que le carré de l'inconnue, soit résoluble par la simple extraction de la racine carrée; et comme l'évanouissement du second terme dans une équation quelconque exige qu'on diminue les racines du coefficient de ce terme pris avec un signe contraire, et divisé par l'exposant du degré de l'équation, c'est-à-dire de la somme de toutes les racines divisée par le nombre de ces racines, il s'ensuit que la réduite du second degré aura pour racines les différences entre les racines de la proposée, divisées par 2, ou bien ces différences mêmes, en supposant qu'on augmente les racines de la réduite dans la raison de 1 à 2, ce qui ne change rien à la nature de cette équation.

Il semble donc qu'on pourrait conclure de là par induction que toute

équation, de quelque degré qu'elle soit, sera aussi résoluble à l'aide d'une réduite dont les racines soient représentées par la même formule

$$x' + yx'' + y^2x''' + y^3x^{\text{iv}} + \dots$$

Mais, d'après ce que nous avons démontré dans la Section précédente à l'occasion des méthodes de MM. Euler et Bezout, lesquelles conduisent directement à de pareilles réduites, on a, ce semble, lieu de se convaincre d'avance que cette conclusion se trouvera en défaut dès le cinquième degré; d'où il s'ensuit que, si la résolution algébrique des équations des degrés supérieurs au quatrième n'est pas impossible, elle doit dépendre de quelques fonctions des racines, différentes de la précédente.

87. Comme jusqu'ici nous n'avons fait que chercher ces sortes de fonctions *à posteriori* et d'après les méthodes connues pour la résolution des équations, il est nécessaire de faire voir maintenant comment il faudrait s'y prendre pour les trouver *à priori* et sans supposer d'autres principes que ceux qui suivent immédiatement de la nature même des équations: c'est l'objet que je me propose principalement dans cette Section.

Je donnerai d'abord des règles directes et générales pour déterminer le degré et la nature de l'équation d'où une fonction quelconque proposée des racines d'une équation de degré donné devra dépendre; quoique cette matière ait déjà été traitée par d'habiles Géomètres, je crois qu'elle peut l'être encore d'une manière plus directe et plus générale, surtout dans le point de vue où nous l'envisageons ici, relativement à la résolution générale des équations.

Je ferai voir ensuite quelles sont les conditions nécessaires pour que l'équation dont il s'agit puisse admettre la résolution en supposant uniquement celle des équations des degrés inférieurs à celui de l'équation proposée; et je donnerai à cette occasion les vrais principes et, pour ainsi dire, la métaphysique de la résolution des équations du troisième et du quatrième degré.

Je traiterai enfin en peu de mots de la réduction des équations qui peuvent se décomposer en d'autres plus simples à cause de quelque rela-

tion particulière qu'il y a entre leurs racines, et je montrerai par quelques exemples comment on peut découvrir ces relations, et abaisser par là les équations proposées à des degrés moindres.

88. Nous ne considérerons ici que des fonctions rationnelles, et nous désignerons ces fonctions en général par la caractéristique f .

Ainsi $f[(x)]$ signifiera une fonction quelconque rationnelle de x ; $f[(x)(y)]$ signifiera une fonction quelconque rationnelle de x et y ; $f[(x)(y)(z)]$, une fonction quelconque rationnelle de x , y , z , et ainsi des autres.

Si dans une fonction donnée $f[(x)(y)]$ on a $y = x$, en sorte qu'il en résulte une simple fonction de x , au lieu de dénoter cette fonction par $f[(x)(x)]$, nous la désignerons pour plus de simplicité par $f[(x)^2]$; pareillement, si dans la fonction donnée $f[(x)(y)(z)]$ on fait $y = x$, on dénotera la fonction résultante de x et z par $f[(x)^2(z)]$, et, si l'on fait en même temps $x = y = z$, on aura une simple fonction de x qu'on désignera par $f[(x)^3]$, et ainsi des autres.

De plus, lorsqu'on voudra représenter une fonction de x et y , par exemple, telle qu'elle demeure la même en échangeant x en y , c'est-à-dire une fonction $f[(x)(y)]$ telle, que l'on ait $f[(x)(y)] = f[(y)(x)]$, nous la désignerons simplement par $f[(x, y)]$. De même on désignera par $f[(x, y, z)]$ toute fonction de x , y et z telle, qu'elle ne change point en échangeant les quantités x , y , z entre elles d'une manière quelconque. Ainsi $f[(x, y)(z)]$ dénotera une fonction rationnelle de x , y , z telle, qu'elle demeure la même en échangeant x en y sans toucher à la quantité z , et ainsi de suite.

Mais si l'on avait une fonction de x , y , z et u telle, qu'elle demeurât la même en échangeant à la fois x en z et y en u , on la dénoterait par $f[(x)(y), (z)(u)]$; et si cette fonction demeurait aussi la même en échangeant simplement x en y , ou z en u , on la désignerait alors par $f[(x, y), (z, u)]$.

Enfin, si l'on a plusieurs fonctions des mêmes quantités, on appellera fonctions *semblables* celles qui varient en même temps ou demeurent les

mêmes lorsqu'on y fait les mêmes permutations entre les quantités dont elles sont composées, de manière qu'elles puissent être désignées d'une manière analogue. Ainsi prenant les caractéristiques f et φ pour désigner des fonctions différentes, les fonctions $f[(x)(y)]$ et $\varphi[(x)(y)]$ seront semblables, ainsi que les fonctions $f[(x, y)]$, $\varphi[(x, y)]$, et ainsi des autres.

89. Nous supposerons, comme dans la Section précédente, que l'équation proposée soit représentée généralement par

$$x^\mu + mx^{\mu-1} + nx^{\mu-2} + px^{\mu-3} + \dots = 0,$$

et que ses racines, qui doivent être au nombre de μ , soient désignées par x' , x'' , x''' , x^{IV} , ..., $x^{(\mu)}$.

Ainsi l'on aura, par la nature des équations,

$$\begin{aligned} -m &= x' + x'' + x''' + x^{IV} + \dots, \\ n &= x'x'' + x'x''' + x''x''' + x'x^{IV} + x''x^{IV} + x'''x^{IV} + \dots, \\ -p &= x'x''x''' + x'x''x^{IV} + x'x'''x^{IV} + x''x'''x^{IV} + \dots, \\ &\dots \dots \dots \dots \dots \dots \end{aligned}$$

Et il est clair que ces fonctions de x' , x'' , x''' , x^{IV} , ..., par lesquelles sont exprimées les quantités m , n , p , ..., seront nécessairement toutes de la forme $f[(x', x'', x''', x^{IV}, \dots)]$, et que par conséquent ces fonctions seront toutes semblables, ce qui est une propriété fondamentale des équations.

90. Cela posé, pour commencer par les cas les plus simples, supposons que l'équation proposée ne soit que du second degré, et qu'on demande l'équation par laquelle devra être déterminée la fonction $f[(x')(x'')]$.

Je fais $t = f[(x')(x'')]$ en sorte que t soit l'inconnue de l'équation cherchée, et comme x' et x'' sont déterminées l'une et l'autre par la même équation

$$x^2 + mx + n = 0,$$

je mets, pour plus de généralité, x à la place de x' et y à la place de x'' ;

j'aurai ainsi l'équation

$$t - f[(x)(y)] = 0,$$

d'où il s'agira de chasser x et y par le moyen des deux équations

$$x^2 + mx + n = 0,$$

$$y^2 + my + n = 0.$$

Soit

$$t - f[(x)(y)] = X;$$

on chassera d'abord x de l'équation $X = 0$ par le moyen de l'équation $x^2 + mx + n = 0$, ce qui donnera une équation que je désignerai par $Y = 0$, et dans laquelle Y sera une fonction rationnelle des quantités t , m , n et y . On chassera ensuite y de cette dernière équation par le moyen de l'autre équation $y^2 + my + n = 0$, et l'on aura l'équation finale $T = 0$, où T sera une fonction rationnelle de t , m et n .

Je remarque maintenant que puisque les racines de l'équation

$$x^2 + mx + n = 0$$

sont x' et x'' , si l'on désigne par X' et X'' les valeurs de X qui viennent de la substitution de ces racines à la place de x , on aura (par ce qui a été démontré dans le n° 13 de la Section I)

$$Y = X'X''.$$

Et de même, à cause que x' et x'' sont aussi les racines de l'équation $y^2 + my + n = 0$, si l'on désigne par Y' et Y'' les valeurs de Y qui résulteront de la substitution de x' et x'' à la place de y , on aura

$$T = Y'Y''.$$

Or on a

$$X' = t - f[(x')(y)],$$

$$X'' = t - f[(x'')(y)];$$

donc

$$Y = [t - f[(x')(y)]] \times [t - f[(x'')(y)]],$$

et de là

$$Y' = [t - f[(x')(x')]] \times [t - f[(x'')(x')]],$$

$$Y'' = [t - f[(x')(x'')]] \times [t - f[(x'')(x'')]],$$

donc on aura

$$T = [t - f[(x')(x'')]] \times [t - f[(x'')(x')]] \times [t - f[(x')^2]] \times [t - f[(x'')^2]].$$

Or, si l'on considère la fonction $f[(x)^2]$ et qu'on fasse $t - f[(x)^2] = \xi$; qu'on élimine ensuite x de l'équation $\xi = 0$, par le moyen de l'équation $x^2 + mx + n = 0$, on aura l'équation $\theta = 0$, où θ sera une fonction rationnelle de t et de m, n . Et désignant par ξ' et ξ'' les valeurs de ξ qui résultent de la substitution de x', x'' à la place de x , on aura

$$\theta = \xi' \xi''.$$

Mais on a

$$\begin{aligned}\xi' &= t - f[(x')^2], \\ \xi'' &= t - f[(x'')^2];\end{aligned}$$

donc

$$\theta = [t - f[(x')^2]] \times [t - f[(x'')^2]].$$

Faisons

$$\Theta = [t - f[(x')(x'')]] \times [t - f[(x'')(x')]],$$

et l'on aura $T = \Theta \theta$, et par conséquent $\Theta = \frac{T}{\theta}$; de sorte que, comme T et θ sont des fonctions rationnelles de t, m et n , il est clair que Θ sera aussi une fonction rationnelle de t, m, n .

Ainsi l'équation $T = 0$ pourra se décomposer en ces deux-ci $\theta = 0$ et $\Theta = 0$; et comme la première est celle qui donne la valeur de $f[(x)^2]$, il s'ensuit que la détermination de la fonction proposée $f[(x')(x'')]$ dépendra uniquement de l'autre équation $\Theta = 0$.

Donc, pour trouver cette équation $\Theta = 0$ qui résout le Problème, il n'y aura qu'à éliminer des équations

$$\begin{aligned}t - f[(x)(y)] &= 0, \\ t - f[(x)^2] &= 0,\end{aligned}$$

les inconnues x et y par le moyen des équations

$$\begin{aligned}x^2 + mx + n &= 0, \\ y^2 + my + n &= 0,\end{aligned}$$

et désignant par $T = 0$ et $\theta = 0$ les équations résultantes on aura sur-le-champ $\Theta = \frac{T}{\theta}$.

91. On voit par l'expression de Θ que l'équation $\Theta = 0$, qui doit servir à déterminer la valeur de la fonction $f[(x')(x'')]$, est du second degré, et que ses deux racines sont $f[(x')(x'')]$ et $f[(x'')(x')]$. En effet, comme les racines x' et x'' sont déterminées de la même manière par l'équation $x^2 + mx + n = 0$, il est clair que les deux fonctions $f[(x')(x'')]$ et $f[(x'')(x')]$, qui ne diffèrent entre elles que par l'échange mutuel des racines x' , x'' , devront être aussi déterminées par une même équation.

Si la fonction $f[(x')(x'')]$ était de la forme $f[(x', x'')]$, en sorte que l'on eût (88)

$$f[(x')(x'')] = f[(x'')(x')],$$

alors on aurait

$$\Theta = [t - f[(x', x'')]]^2;$$

par conséquent l'équation $\Theta = 0$ deviendra simplement

$$t - f[(x', x'')] = 0;$$

d'où l'on voit que la fonction dont il s'agit sera déterminée dans ce cas par une équation linéaire; par conséquent elle sera donnée par une expression rationnelle en m et n .

92. Qu'on demande maintenant l'équation par laquelle devra être déterminée la fonction $f[(x')(x'')(x''')]$, en supposant que x' , x'' , x''' soient les racines de l'équation du troisième degré

$$x^3 + mx^2 + nx + p = 0.$$

Prenant, comme ci-dessus, t pour l'inconnue de cette équation, et mettant x , y , z à la place de x' , x'' , x''' , j'aurai l'équation

$$t - f[(x)(y)(z)] = 0,$$

d'où il s'agira d'éliminer successivement x , y , z par le moyen des trois

équations

$$\begin{aligned}x^3 + mx^2 + nx + p &= 0, \\y^3 + my^2 + ny + p &= 0, \\z^3 + mz^2 + nz + p &= 0.\end{aligned}$$

Soit

$$t - f[(x)(y)(z)] = X;$$

qu'on élimine d'abord de l'équation $X = 0$ la quantité x par le moyen de l'équation en x , on aura une seconde équation que je désignerai par $Y = 0$, et où Y sera une fonction rationnelle de t, y, z , et des coefficients m, n, p . Qu'on élimine ensuite y de l'équation $Y = 0$ par le moyen de l'équation en y , on aura une troisième équation, que je désignerai par $Z = 0$, et où Z sera une fonction rationnelle de t, z et des coefficients m, n, p . Qu'on élimine enfin de cette équation $Z = 0$ la quantité z , par le moyen de l'équation en z , on aura une équation finale, qu'on pourra désigner par $T = 0$, et où T sera une fonction rationnelle de t, m, n, p .

Or, puisque les racines de l'équation en x sont x', x'', x''' , si l'on désigne par X', X'', X''' les valeurs de X qui résultent des substitutions de ces racines à la place de x , on aura, par le n° 13,

$$Y = X' X'' X'''.$$

De même, puisque les racines de l'équation en y sont aussi x', x'', x''' , si l'on dénote par Y', Y'', Y''' les valeurs de Y qui résultent des substitutions de ces racines à la place de y , on aura par la même raison

$$Z = Y' Y'' Y'''.$$

Enfin, comme l'équation en z a aussi les mêmes racines x', x'', x''' , dénotant par Z', Z'', Z''' les valeurs de Z qui résultent de leurs substitutions à la place de z , on aura

$$T = Z' Z'' Z'''.$$

Mais il est clair qu'on aura

$$\begin{aligned}X' &= t - f[(x')(y)(z)], \\X'' &= t - f[(x'')(y)(z)], \\X''' &= t - f[(x''')(y)(z)].\end{aligned}$$

Donc

$$Y = [t - f[(x')(y)(z)]] \times [t - f[(x'')(y)(z)]] \times [t - f[(x''')(y)(z)]],$$

De là on aura

$$Y' = [t - f[(x')(x')(z)]] \times [t - f[(x'')(x')(z)]] \times [t - f[(x''')(x')(z)]],$$

$$Y'' = [t - f[(x')(x'')(z)]] \times [t - f[(x'')(x'')(z)]] \times [t - f[(x''')(x'')(z)]],$$

$$Y''' = [t - f[(x')(x''')(z)]] \times [t - f[(x'')(x''')(z)]] \times [t - f[(x''')(x''')(z)]].$$

Donc

$$Z = [t - f[(x')(x'')(z)]] \times [t - f[(x')(x''')(z)]] \times [t - f[(x'')(x''')(z)]]$$

$$\times [t - f[(x'')(x')(z)]] \times [t - f[(x''')(x')(z)]] \times [t - f[(x''')(x'')(z)]]$$

$$\times [t - f[(x')^2(z)]] \times [t - f[(x'')^2(z)]] \times [t - f[(x''')^2(z)]].$$

Donc

$$Z' = [t - f[(x')(x'')(x')]] \times [t - f[(x')(x''')(x')]] \times [t - f[(x'')(x''')(x')]]$$

$$\times [t - f[(x'')(x')^2]] \times [t - f[(x''')(x')^2]] \times [t - f[(x''')(x'')(x')]]$$

$$\times [t - f[(x')^3]] \times [t - f[(x'')^2(x')]] \times [t - f[(x''')^2(x')]],$$

$$Z'' = [t - f[(x')(x'')^2]] \times [t - f[(x')(x''')(x'')]] \times [t - f[(x'')(x''')(x'')]]$$

$$\times [t - f[(x'')(x')(x'')]] \times [t - f[(x''')(x')(x'')]] \times [t - f[(x''')(x'')^2]]$$

$$\times [t - f[(x')^2(x'')]] \times [t - f[(x'')^3]] \times [t - f[(x''')^2(x'')]],$$

$$Z''' = [t - f[(x')(x'')(x''')]] \times [t - f[(x')(x''')^2]] \times [t - f[(x'')(x''')^2]]$$

$$\times [t - f[(x'')(x')(x''')]] \times [t - f[(x''')(x')(x''')]] \times [t - f[(x''')(x'')(x''')]]$$

$$\times [t - f[(x')^2(x''')]] \times [t - f[(x'')^2(x''')]] \times [t - f[(x''')^3]].$$

Donc enfin, si l'on multiplie ces trois quantités ensemble, et qu'on fasse,

pour abréger,

$$\Theta = [t - f[(x')(x'')(x''')]] \times [t - f[(x'')(x')(x''')]] \times [t - f[(x''')(x'')(x')]] \\ \times [t - f[(x')(x''')(x'')]] \times [t - f[(x''')(x')(x'')]] \times [t - f[(x'')(x''')(x')]],$$

$$\theta = [t - f[(x')^3]] \times [t - f[(x'')^3]] \times [t - f[(x''')^3]],$$

$$\theta_1 = [t - f[(x')^2(x'')]] \times [t - f[(x'')^2(x')]] \times [t - f[(x''')^2(x'')]] \\ \times [t - f[(x')^2(x''')]] \times [t - f[(x''')^2(x')]] \times [t - f[(x'')^2(x''')]],$$

$$\theta_2 = [t - f[(x')(x'')^2]] \times [t - f[(x'')(x')^2]] \times [t - f[(x''')(x'')^2]] \\ \times [t - f[(x')(x''')^2]] \times [t - f[(x''')^2(x')]] \times [t - f[(x'')(x''')^2]],$$

$$\theta_3 = [t - f[(x')(x'')(x')]] \times [t - f[(x'')(x')(x'')]] \times [t - f[(x''')(x'')(x''')]] \\ \times [t - f[(x')(x''')(x')]] \times [t - f[(x''')(x')(x''')]] \times [t - f[(x'')(x''')(x'')]],$$

on aura

$$T = \Theta \theta \theta_1 \theta_2 \theta_3.$$

Maintenant je remarque que, si l'on suppose

$$t - f[(x)^3] = 0,$$

et qu'on élimine x par le moyen de l'équation en x ,

$$x^3 + mx^2 + nx + p = 0,$$

on trouvera, comme dans le numéro précédent, l'équation finale $\theta = 0$, de sorte que θ sera nécessairement une fonction rationnelle de t et des coefficients m, n, p .

On trouvera, par les mêmes principes, que si l'on fait

$$t - f[(x)^2(y)] = 0,$$

et qu'on élimine successivement x et y par le moyen des deux équations en x et en y , savoir

$$x^3 + mx^2 + nx + p = 0,$$

$$y^3 + my^2 + ny + p = 0,$$

on aura, pour équation finale, $\theta\theta_1=0$, où la quantité $\theta\theta_1$ sera par conséquent une fonction rationnelle de t, m, n, p ; et comme θ en est une aussi, il s'ensuit que θ_1 sera de même une fonction rationnelle de t et de m, n, p .

Pareillement, si l'on fait

$$t - f[(x)(y)^2] = 0$$

et qu'on élimine x et y par les mêmes équations, on trouvera cette équation finale $\theta\theta_2=0$, dans laquelle la quantité $\theta\theta_2$ sera donc une fonction rationnelle de t, m, n, p ; de sorte que la quantité θ_2 en sera une aussi.

Enfin, si l'on fait

$$t - f[(x)(y)(x)] = 0,$$

et qu'on élimine de même x et y , on trouvera pour équation finale $\theta\theta_3=0$; de sorte que la quantité $\theta\theta_3$ sera une fonction rationnelle de t, m, n, p , et par conséquent la quantité θ_3 en sera aussi une.

Donc, puisque les quantités $\theta, \theta_1, \theta_2, \theta_3$ sont chacune des fonctions rationnelles de t et des coefficients m, n, p , il s'ensuit que l'équation

$$T=0, \text{ savoir } \Theta\theta\theta_1\theta_2\theta_3=0,$$

pourra se décomposer en celles-ci

$$\theta=0, \quad \theta_1=0, \quad \theta_2=0, \quad \theta_3=0 \quad \text{et} \quad \Theta=0;$$

de sorte que la quantité Θ sera aussi une fonction rationnelle de t, m, n, p .

Or il est facile de voir que les équations

$$\theta=0, \quad \theta_1=0, \quad \theta_2=0, \quad \theta_3=0$$

sont toutes étrangères à la question proposée, c'est-à-dire à la détermination de la fonction $f[(x')(x'')(x''')]$; car ces équations, comme il paraît par les expressions des quantités $\theta, \theta_1, \theta_2, \theta_3$, ont pour racines des fonctions de x', x'', x''' d'une forme différente de la proposée; ainsi il ne restera que l'équation $\Theta=0$, qui renfermera par conséquent toutes les racines utiles à la solution du Problème.

93. Pour trouver donc cette équation $\Theta = 0$, il n'y aura qu'à éliminer des cinq équations

$$\begin{aligned} t - f[(x)(y)(z)] &= 0, \\ t - f[(x)^2(y)] &= 0, \\ t - f[(x)(y)^2] &= 0, \\ t - f[(x)(y)(x)] &= 0, \\ t - f[(x)^3] &= 0, \end{aligned}$$

les inconnues x, y, z par le moyen des équations

$$\begin{aligned} x^3 + mx^2 + nx + p &= 0, \\ y^3 + my^2 + ny + p &= 0, \\ z^3 + mz^2 + nz + p &= 0; \end{aligned}$$

et, désignant les équations finales résultantes par

$$T = 0, \quad T_1 = 0, \quad T_2 = 0, \quad T_3 = 0, \quad \theta = 0,$$

on aura

$$T_1 = \theta \theta_1, \quad T_2 = \theta \theta_2, \quad T_3 = \theta \theta_3, \quad T = \Theta \theta \theta_1 \theta_2 \theta_3;$$

par conséquent

$$\Theta = \frac{T \theta^2}{T_1 T_2 T_3}.$$

Cette méthode au reste serait extrêmement longue et pénible dans la pratique, et elle le deviendrait de plus en plus, à mesure que l'équation proposée serait d'un degré plus haut; aussi ne l'ai-je donnée ici que parce qu'elle sert à faire connaître, d'une manière directe et indépendante de toute considération étrangère, la nature de l'équation cherchée $\Theta = 0$.

94. En effet il est visible, par l'expression de Θ donnée ci-dessus (92), que la réduite $\Theta = 0$ sera du sixième degré, ayant pour racines les fonctions

$$\begin{aligned} f[(x')(x'')(x''')], \quad f[(x'')(x')(x''')], \quad f[(x''')(x'')(x')], \\ f[(x')(x''')(x'')], \quad f[(x''')(x')(x'')], \quad f[(x'')(x''')(x')], \end{aligned}$$

lesquelles sont toutes semblables, et dérivent l'une de l'autre par de

simples permutations entre les quantités $x', x'', x''';$ il est clair en effet que, comme ces quantités sont toutes déterminées de la même manière par l'équation

$$x^3 + mx^2 + nx + p = 0,$$

dont elles sont les racines, l'équation qui donnera la valeur d'une fonction quelconque des mêmes quantités devra donner également les autres fonctions qui viendront de toutes les permutations possibles entre elles. Cette proposition paraît même assez évidente par elle-même pour n'avoir pas besoin de démonstration; mais on ne voit pas aussi évidemment, ce me semble, que l'équation dont il s'agit ne devra contenir d'autres racines que les différentes fonctions qui viendront des permutations entre les racines de la proposée; c'est-à-dire qu'en supposant cette équation formée du produit des facteurs simples

$$t - f[(x')(x'')(x''')], \quad t - f[(x'')(x')(x''')], \dots,$$

chacun des coefficients pourra toujours s'exprimer par une fonction rationnelle des coefficients m, n, \dots de l'équation proposée; or c'est sur quoi notre démonstration ne laisse aucun doute, puisque l'on a vu que la quantité Θ , qui est égale à ce produit, est toujours nécessairement une fonction rationnelle de t, m, n, \dots

95. Si l'équation proposée était d'un degré plus haut, en sorte qu'elle eût quatre ou un plus grand nombre de racines $x', x'', x''', x^{iv}, \dots$, on pourrait trouver de même l'équation $\Theta = 0$, qui servirait à déterminer la fonction $f[(x')(x'')(x''')(x^{iv})\dots]$; et l'on verrait que la quantité Θ serait le produit d'autant de facteurs simples tels que

$$\begin{aligned} & t - f[(x')(x'')(x''')(x^{iv})\dots], \\ & t - f[(x'')(x')(x''')(x^{iv})\dots], \\ & t - f[(x''')(x'')(x')(x^{iv})\dots], \\ & t - f[(x'')(x''')(x')(x^{iv})\dots], \\ & \dots \dots \dots \end{aligned}$$

qu'il y a de permutations possibles entre les racines $x', x'', x''', x^{iv}, \dots$; de sorte que, si l'équation proposée est du degré μ , le nombre des fac-

teurs simples de la quantité Θ , et par conséquent le nombre des racines de l'équation $\Theta = 0$ sera marqué par $1.2.3\dots\mu$, puisque ce nombre est celui de toutes les permutations dont μ choses sont susceptibles; et les racines de cette équation seront les différentes fonctions dans lesquelles la fonction proposée $f[(x')(x'')(x''')\dots]$ pourra se changer par les permutations des racines x', x'', x''', \dots entre elles.

96. Or, pour trouver toutes ces différentes fonctions par ordre et sans en omettre aucune, on échangera d'abord, dans la fonction proposée, x'' en x' et *vice versa*; on aura ainsi deux fonctions; ensuite on échangera successivement dans ces deux-ci x''' en x' , en x'' , et l'on aura six fonctions; puis dans ces six on échangera successivement x^{iv} en x' , en x'' , en x''' et l'on aura vingt-quatre fonctions, et ainsi de suite, jusqu'à ce que l'on ait épuisé toutes les racines x', x'', x''', \dots

D'où l'on voit clairement que le nombre des fonctions différentes doit croître suivant les produits des nombres naturels

$$1, \quad 1.2, \quad 1.2.3, \quad 1.2.3.4, \quad \dots, \quad 1.2.3.4.5\dots\mu.$$

Ayant toutes ces fonctions on aura donc les racines de l'équation $\Theta = 0$; de sorte que, si on la représente par

$$t^w - M t^{w-1} + N t^{w-2} - P t^{w-3} + \dots = 0,$$

on aura $w = 1.2.3.4\dots\mu$; et le coefficient M sera égal à la somme de toutes les fonctions trouvées, le coefficient N égal à la somme de tous les produits de ces fonctions multipliées deux à deux, le coefficient P égal à la somme de tous les produits des mêmes fonctions multipliées trois à trois, et ainsi de suite.

Et comme nous avons démontré ci-dessus que l'expression de Θ doit être nécessairement une fonction rationnelle de t et des coefficients m, n, p, \dots de l'équation proposée, il s'ensuit que les quantités M, N, P, \dots seront nécessairement des fonctions rationnelles de m, n, p, \dots qu'on pourra trouver directement, comme nous l'avons pratiqué dans les Sections précédentes. *Voyez là-dessus, outre l'Ouvrage de M. Cramer que nous avons déjà cité, encore celui de M. Waring, qui a pour titre *Medi-**

tationes algebraïcæ, Ouvrage rempli d'excellentes recherches sur les équations.

97. Quoique l'équation $\Theta = 0$ doive être, en général, du degré $1.2.3 \dots \mu = \varpi$, qui est égal au nombre des permutations dont les μ racines x', x'', x''', \dots sont susceptibles, cependant s'il arrive que la fonction soit telle, qu'elle ne reçoive aucun changement par quelqu'une ou quelques-unes de ces permutations, alors l'équation dont il s'agit s'abaissera nécessairement à un degré moindre.

Car supposons, par exemple, que la fonction $f[(x')(x'')(x''')(x^{iv})\dots]$ soit telle, qu'elle conserve la même valeur en échangeant x' en x'' , x'' en x''' , et x''' en x' , en sorte que l'on ait

$$f[(x')(x'')(x''')(x^{iv})\dots] = f[(x'')(x''')(x')(x^{iv})\dots],$$

il est clair que l'équation $\Theta = 0$ aura déjà deux racines égales; mais je vais prouver que dans cette hypothèse toutes les autres racines seront aussi égales deux à deux. En effet, considérons une racine quelconque de la même équation, laquelle soit représentée par la fonction

$$f[(x^{iv})(x''')(x')(x'')\dots],$$

comme celle-ci dérive de la fonction

$$f[(x')(x'')(x''')(x^{iv})\dots],$$

en échangeant x' en x^{iv} , x'' en x''' , x''' en x' , x^{iv} en x'' , il s'ensuit qu'elle devra garder aussi la même valeur en y changeant x^{iv} en x''' , x''' en x' et x' en x^{iv} ; de sorte qu'on aura aussi

$$f[(x^{iv})(x''')(x')(x'')\dots] = f[(x''')(x')(x^{iv})(x'')\dots].$$

Donc, dans ce cas, la quantité Θ sera égale à un carré θ^2 , et par conséquent l'équation $\Theta = 0$ se réduira à celle-ci $\theta = 0$, dont la dimension sera $\frac{\varpi}{2}$.

On démontrera de la même manière que, si la fonction

$$f[(x')(x'')(x''')(x^{iv})\dots]$$

est de sa propre nature telle, qu'elle conserve la même valeur en faisant deux, ou trois, ou un plus grand nombre de permutations différentes entre les racines $x', x'', x''', x^{iv}, \dots$, les racines de l'équation $\Theta = 0$ seront égales trois à trois, ou quatre à quatre, ou, etc.; en sorte que la quantité Θ sera égale à un cube θ^3 , ou à un carré-carré θ^4 , ou, etc., et que par conséquent l'équation $\Theta = 0$ se réduira à celle-ci $\theta = 0$, dont le degré sera égal à $\frac{\varpi}{3}$, ou égal à $\frac{\varpi}{4}$, ou, etc.

98. Done, si la fonction proposée est de la forme

$$f[(x', x'')(x''')(x^{iv})\dots]$$

qui a la propriété de demeurer la même en échangeant x' en x'' (88), toutes les racines de l'équation $\Theta = 0$ seront égales deux à deux; de sorte que cette équation s'abaissera au degré $\frac{1.2.3\dots\mu}{2}$.

De même la fonction

$$f[(x', x'')(x''')(x^{iv})(x^v)\dots]$$

devant demeurer la même, quelque permutation qu'on y fasse entre les trois racines x', x'', x''' , il s'ensuit que l'équation $\Theta = 0$ aura toutes ses racines égales $1.2.3$ à $1.2.3$; de sorte qu'elle s'abaissera au degré $\frac{1.2.3\dots\mu}{1.2.3}$.

Et la fonction

$$f[(x', x'')(x''')(x^{iv})(x^v)\dots],$$

qui doit demeurer la même, quelque permutation qu'on fasse entre les deux racines x', x'' , ainsi qu'entre les deux x''', x^{iv} , donnera une équation $\Theta = 0$ où les racines seront toutes égales 1.2×1.2 à 1.2×1.2 ; de sorte qu'elle s'abaissera au degré $\frac{1.2.3\dots\mu}{1.2 \times 1.2}$.

En général, la fonction

$$f[(x', x'')(x''')(x^{(a)})(x^{(a+1)}, x^{(a+2)}, x^{(a+3)}, \dots, x^{(a+\beta)})(x^{(a+\beta+1)}, \dots)\dots]$$

donnera une équation $\Theta = 0$, où la quantité Θ sera une puissance qui

aura pour exposant le nombre $1.2.3\dots\alpha \times 1.2.3\dots\beta \times 1.2.3\dots$, de manière que cette équation s'abaissera au degré $\frac{1.2.3.4\dots\mu}{1.2.3\dots\alpha \times 1.2.3\dots\beta \times 1.2.3\dots}$.

On voit par là que toute fonction de la forme

$$f[(x', x'', x''', \dots, x^{(\mu)})],$$

qui aura la propriété de demeurer la même, quelque permutation qu'on fasse entre les racines $x', x'', x''', \dots, x^{(\mu)}$ de l'équation proposée, devra dépendre seulement d'une équation du degré $\frac{1.2.3\dots\mu}{1.2.3\dots\mu} = 1$, c'est-à-dire du premier degré; de sorte qu'elle devra être déterminable algébriquement et rationnellement par les coefficients m, n, p, \dots de la proposée; théorème que nous avons déjà supposé dans les Sections précédentes comme évident par soi-même, mais dont la démonstration rigoureuse dépend des principes établis ci-dessus.

On peut aussi conclure de ce qui précède que, si l'on a une fonction quelconque qui ne contienne qu'un nombre λ des μ racines x', x'', x''', \dots , en sorte qu'elle soit représentée par

$$f[(x')(x'')(x''')\dots(x^{(\lambda)})],$$

elle conduira simplement à une équation du degré $\frac{1.2.3.4\dots\mu}{1.2.3\dots(\mu-\lambda)}$; car il est clair qu'on peut regarder la fonction proposée comme étant de la forme

$$f[(x')(x'')(x''')\dots(x^{(\lambda)})(x^{(\lambda+1)}, x^{(\lambda+2)}, \dots, x^{(\mu)})],$$

en supposant, ce qui est permis, que les racines $x^{(\lambda+1)}, x^{(\lambda+2)}, \dots, x^{(\mu)}$ y soient multipliées par des coefficients égaux à zéro ou élevées à des exposants égaux à zéro.

Donc la fonction

$$f[(x', x'')(x''', x^{(\lambda)}, x^{(\lambda+1)}, \dots, x^{(\mu)})]$$

conduira à une équation du degré $\frac{1.2.3\dots\mu}{1.2 \times 1.2.3\dots(\mu-\lambda)}$, et ainsi des autres.

Et la fonction

$$f[(x', x'')(x''', \dots, x^{(\lambda)})]$$

conduira à une équation du degré

$$\frac{1 \cdot 2 \cdot 3 \cdots \mu}{1 \cdot 2 \cdot 3 \cdots \lambda \times 1 \cdot 2 \cdot 3 \cdots (\mu - \lambda)} = \frac{\mu(\mu - 1)(\mu - 2) \cdots (\mu - \lambda + 1)}{1 \cdot 2 \cdot 3 \cdots \lambda}.$$

Ainsi, si l'on voulait abaisser, en général, l'équation proposée du degré μ à une équation d'un degré inférieur λ , telle que

$$x^\lambda + ax^{\lambda-1} + bx^{\lambda-2} + \cdots = 0,$$

laquelle eût toutes ses racines communes avec la proposée, c'est-à-dire dont les racines fussent $x', x'', x''', \dots, x^{(\lambda)}$, on tomberait nécessairement dans une équation du degré

$$\frac{\mu(\mu - 1)(\mu - 2) \cdots (\mu - \lambda + 1)}{1 \cdot 2 \cdot 3 \cdots \lambda}$$

pour la détermination de chaque coefficient a, b, c, \dots ; car ces coefficients seraient nécessairement des fonctions de la forme

$$f[(x', x'', x''', \dots, x^{(\lambda)})],$$

comme on l'a fait remarquer dans le n° 89. C'est aussi une proposition connue depuis longtemps, mais qu'on n'avait pas encore, ce me semble, démontrée en toute rigueur.

Or, comme en prenant λ moindre que μ le nombre

$$\frac{\mu(\mu - 1)(\mu - 2) \cdots (\mu - \lambda + 1)}{1 \cdot 2 \cdot 3 \cdots \lambda}$$

ne peut jamais être plus petit que μ , il s'ensuit que l'on ne peut rien se promettre de ces sortes de réductions pour la résolution générale des équations.

99. De tout ce que nous venons de démontrer il s'ensuit donc, en général : 1° que toutes les fonctions *semblables* des racines x', x'', x''', \dots d'une même équation sont nécessairement données par des équations du même degré; 2° que ce degré sera toujours égal au nombre $1 \cdot 2 \cdot 3 \cdots \mu$ (μ étant le degré de l'équation donnée), ou à un sous-multiple de ce

nombre; 3^o que pour trouver directement l'équation la plus simple $\theta = 0$ par laquelle devra être déterminée une fonction quelconque donnée de x', x'', x''', \dots , il n'y aura qu'à chercher toutes les différentes valeurs que cette fonction peut recevoir par les permutations des quantités x', x'', x''', \dots entre elles, et, prenant ces valeurs pour les racines de l'équation cherchée, on déterminera par leur moyen les coefficients de cette équation suivant les méthodes connues et employées déjà plusieurs fois dans ce Mémoire.

100. Or, dès qu'on aura trouvé, soit par la résolution de l'équation $\theta = 0$ ou autrement, la valeur d'une fonction donnée des racines x', x'', x''', \dots , je dis qu'on pourra trouver aussi la valeur d'une autre fonction quelconque des mêmes racines, et cela, généralement parlant, par le moyen d'une équation simplement linéaire, à l'exception de quelques cas particuliers qui exigent une équation du second degré, ou du troisième, etc. Ce Problème me paraît un des plus importants de la théorie des équations, et la Solution générale que nous allons en donner servira à jeter un nouveau jour sur cette partie de l'Algèbre.

Nous commencerons par supposer, pour plus de simplicité, que les deux fonctions proposées, dont les valeurs sont l'une connue et l'autre inconnue, soient *semblables*, suivant la définition que nous avons donnée de ce terme dans le n° 88, et nous désignerons, en général, par t la première de ces deux fonctions et par y la seconde; nous désignerons de plus par $t', t'', t''', \dots, t^{(\varpi)}$ les différentes valeurs de t qui proviennent de toutes les permutations possibles entre les racines x', x'', x''', \dots , et pareillement par $y', y'', y''', \dots, y^{(\varpi)}$ les différentes valeurs de la fonction y provenantes des mêmes permutations; car, les deux fonctions t et y étant supposées semblables, il s'ensuit que le nombre des valeurs différentes dont elles seront susceptibles par toutes les permutations possibles entre x', x'', x''', \dots sera le même pour l'une et pour l'autre, et que ces valeurs seront dues aux mêmes permutations dans les deux fonctions.

Ainsi les quantités $t', t'', t''', \dots, t^{(\varpi)}$ seront les racines de l'équation en t , qui sera par conséquent du degré ϖ , et les quantités y', y'', y''', \dots ,

$y^{(\varpi)}$ seront pareillement les racines de l'équation en y , laquelle sera du même degré ϖ . On pourra donc trouver ces équations en t et en y par les méthodes exposées plus haut; mais nous n'aurons besoin que d'avoir l'équation en t , que nous représenterons, en général, par

$$1 + At + Bt^2 + Ct^3 + \dots + Kt^\varpi = 0,$$

ou plus simplement par $\theta = 0$, en supposant

$$\theta = 1 + At + Bt^2 + Ct^3 + \dots + Kt^\varpi,$$

où les coefficients A, B, C, \dots seront des fonctions connues des coefficients m, n, p, \dots de l'équation proposée en x dont les racines sont x', x'', x''', \dots

Cela posé, qu'on considère en général la fonction $t^\lambda y$, il est visible que les différentes valeurs de cette fonction résultantes de toutes les permutations possibles entre les racines x', x'', x''', \dots seront $t'^\lambda y', t''^\lambda y'', t'''^\lambda y''', \dots, t^{(\varpi)^\lambda} y^{(\varpi)}$; de sorte qu'en prenant la somme de toutes ces valeurs on aura la fonction

$$t'^\lambda y' + t''^\lambda y'' + t'''^\lambda y''' + \dots + t^{(\varpi)^\lambda} y^{(\varpi)},$$

laquelle aura la propriété de demeurer invariable, quelque permutation qu'on y fasse entre les racines x', x'', x''', \dots , et par conséquent pourra s'exprimer algébriquement et rationnellement par les coefficients m, n, p, \dots (98).

Qu'on cherche donc les valeurs de cette fonction pour les exposants $\lambda = 0, 1, 2, 3, \dots, \varpi - 1$, et qu'on les dénote par les quantités $M, M_1, M_2, M_3, \dots, M_{(\varpi-1)}$, on aura les ϖ équations suivantes

$$\begin{aligned} y' + y'' + y''' + \dots + y^{(\varpi)} &= M, \\ t' y' + t'' y'' + t''' y''' + \dots + t^{(\varpi)} y^{(\varpi)} &= M_1, \\ t'^2 y' + t''^2 y'' + t'''^2 y''' + \dots + t^{(\varpi)2} y^{(\varpi)} &= M_2, \\ t'^3 y' + t''^3 y'' + t'''^3 y''' + \dots + t^{(\varpi)3} y^{(\varpi)} &= M_3, \\ \dots & \\ t'^{\varpi-1} y' + t''^{\varpi-1} y'' + t'''^{\varpi-1} y''' + \dots + t^{(\varpi)\varpi-1} y^{(\varpi)} &= M_{(\varpi-1)}; \end{aligned}$$

où les termes $M, M_1, M_2, \dots, M_{(\sigma-1)}$ seront des quantités connues en m, n, p, \dots

Il s'agit maintenant de tirer de ces ϖ équations, par la voie de l'élimination, les valeurs des ϖ inconnues $y', y'', y''', \dots, y^{(\varpi)}$; or, si l'on suivait pour cela la méthode ordinaire, on tomberait dans des expressions fort compliquées et qui auraient d'ailleurs l'inconvénient de renfermer à la fois toutes les quantités t', t'', t''', \dots ; il faudra donc employer une autre méthode, et voici celle qui m'a paru la plus propre.

Je prends un nombre $\varpi - 1$ de quantités indéterminées que je désigne par $N_1, N_2, N_3, \dots, N_{(\varpi-1)}$, et je multiplie respectivement par ces quantités toutes les équations précédentes, excepté la première; après quoi je les ajoute ensemble, ce qui me donne cette équation unique

Supposons, en général,

$$T = 1 + N_1 t + N_2 t^2 + N_3 t^3 + \dots + N_{(w-1)} t^{w-1},$$

et désignons par T' , T'' , T''' , ..., $T^{(\sigma)}$ les valeurs particulières de T , que l'on aura en faisant successivement $t = t'$, t'' , t''' , ..., $t^{(\sigma)}$; il est clair que l'équation précédente se réduira à cette forme très-simple

$$T' y' + T'' y'' + T''' y''' + \dots + T^{(\pi)} y^{(\pi)} \\ = M + M_1 N_1 + M_2 N_2 + M_3 N_3 + \dots + M_{(\pi-1)} N_{(\pi-1)}.$$

Maintenant, pour trouver la valeur d'une quelconque des inconnues y', y'', y''', \dots , comme de $y^{(p)}$, il est clair qu'il n'y aura qu'à faire évanouir les coefficients de toutes les autres inconnues, à l'exception de celle-ci, et l'on aura sur-le-champ

$$\gamma^{(e)} = \frac{M + M_1 N_1 + M_2 N_2 + M_3 N_3 + \dots + M_{(\sigma-1)} N_{(\sigma-1)}}{T^{(e)}}.$$

Et les équations

$$T' = 0, \quad T'' = 0, \quad T''' = 0, \dots, \quad T^{(\varpi)} = 0,$$

à l'exception de $T^{(\rho)} = 0$, serviront à déterminer les $\varpi - 1$ indéterminées $N_1, N_2, N_3, \dots, N_{(\varpi-1)}$.

En effet, pour que toutes ces équations particulières aient lieu à la fois, il est visible qu'il faudra que l'équation générale $T = 0$ ait pour racines les quantités $t', t'', t''', \dots, t^{(\varpi)}$, à l'exception seulement de $t^{(\rho)}$; donc, si l'on multiplie le polynôme T , dont le terme tout connu est l'unité, par le facteur $1 - \frac{t}{t^{(\rho)}}$, on aura le polynôme $T \left(1 - \frac{t}{t^{(\rho)}} \right)$, qui étant égalé à zéro aura pour racines toutes les quantités $t', t'', t''', \dots, t^{(\varpi)}$; mais ces racines sont déjà celles de l'équation $\theta = 0$; donc, puisque le terme tout connu, tant du polynôme $T \left(1 - \frac{t}{t^{(\rho)}} \right)$ que du polynôme θ , est égal à l'unité, il s'ensuit qu'on aura l'équation

$$T \left(1 - \frac{t}{t^{(\rho)}} \right) = \theta,$$

ou bien

$$1 + \left(N_1 - \frac{1}{t^{(\rho)}} \right) t + \left(N_2 - \frac{N_1}{t^{(\rho)}} \right) t^2 + \left(N_3 - \frac{N_2}{t^{(\rho)}} \right) t^3 + \dots = 1 + At + Bt^2 + Ct^3 + \dots,$$

d'où, à cause que cette équation doit être identique, on tire

$$N_1 - \frac{1}{t^{(\rho)}} = A, \quad N_2 - \frac{N_1}{t^{(\rho)}} = B, \quad N_3 - \frac{N_2}{t^{(\rho)}} = C, \dots,$$

et de là

$$N_1 = A + \frac{1}{t^{(\rho)}},$$

$$N_2 = B + \frac{A}{t^{(\rho)}} + \frac{1}{t^{(\rho)2}},$$

$$N_3 = C + \frac{B}{t^{(\rho)}} + \frac{A}{t^{(\rho)2}} + \frac{1}{t^{(\rho)3}},$$

.....

Maintenant, pour trouver la valeur de la quantité $T^{(\rho)}$, on remarquera

que l'on a, en général,

$$T = \frac{\theta}{1 - \frac{t}{t^{(p)}}},$$

de sorte qu'il n'y aura qu'à faire dans cette expression $t = t^{(p)}$; mais, comme cette supposition fait évanouir en même temps le numérateur θ , parce que $t^{(p)}$ est une des racines de l'équation $\theta = 0$, et le dénominateur $1 - \frac{t}{t^{(p)}}$, il faudra, suivant la règle connue, prendre à la place de ces quantités leurs différences; ainsi l'on aura, en faisant varier t , la fraction $-t \frac{d\theta}{dt} : \frac{1}{t^{(p)}}$; ainsi, la valeur de $T^{(p)}$ sera égale à ce que devient la quantité $-t \frac{d\theta}{dt}$ lorsqu'on y met $t^{(p)}$ à la place de t , ce qu'on peut désigner ainsi

$$T^{(p)} = \left(-t \frac{d\theta}{dt} \right)^{(p)},$$

ou bien, en substituant la valeur de θ et changeant, après la différentiation, t en $t^{(p)}$,

$$T^{(p)} = -At^{(p)} - 2Bt^{(p)2} - 3Ct^{(p)3} - \dots$$

Il n'y aura donc plus qu'à substituer cette valeur de $T^{(p)}$, ainsi que celles de N_1, N_2, N_3, \dots , trouvées ci-dessus, dans l'expression générale de $y^{(p)}$, donnée plus haut, et l'on aura la valeur de la fonction $y^{(p)}$ exprimée uniquement par celle de la fonction correspondante donnée $t^{(p)}$ et par les coefficients m, n, p, \dots de l'équation proposée.

Toute la difficulté se réduit donc à trouver tant les coefficients A, B, C, \dots de l'équation en t

$$1 + At + Bt^2 + Ct^3 + \dots = 0,$$

que les quantités M, M_1, M_2, M_3, \dots ; c'est à quoi l'on peut parvenir par différentes méthodes, comme on l'a vu plus haut; l'essentiel consiste à remarquer que toutes ces quantités seront toujours exprimables algébriquement par les seuls coefficients m, n, p, \dots de l'équation proposée; ce que nous avons démontré *à priori* avec toute la rigueur possible.

Ces quantités étant donc trouvées, si l'on fait, pour plus de simplicité,

$$P = M_1 + AM_2 + BM_3 + CM_4 + \dots,$$

$$Q = M_1 + AM_2 + BM_3 + \dots,$$

$$R = M_2 + AM_3 + \dots,$$

$$\dots \dots \dots \dots \dots$$

on aura, pour la valeur d'une y quelconque,

$$y = -\frac{\frac{P}{t} + \frac{Q}{t^2} + \frac{R}{t^3} + \frac{S}{t^4} + \dots}{A + 2Bt + 3Ct^2 + 4Dt^3 + \dots},$$

en prenant pour t la fonction correspondante à la fonction y .

101. Il est évident que cette solution servira toujours, quelle que soit la valeur donnée de t , pourvu qu'elle ne rende pas nul le dénominateur

$$A + 2Bt + 3Ct^2 + \dots = \frac{d\theta}{dt};$$

or, comme la valeur de t doit déjà être une racine de l'équation $\theta = 0$, il s'ensuit que le cas de $\frac{d\theta}{dt} = 0$ n'aura lieu que lorsque cette valeur sera une racine multiple de la même équation $\theta = 0$.

Pour trouver ce qui doit arriver dans ce cas-là, supposons que t' soit la valeur donnée de t , laquelle répond à la valeur cherchée y' de y , et que dans la suite des valeurs t' , t'' , t''' , ..., $t^{(\infty)}$, il s'en trouve une autre comme t'' qui soit égale à t' , en sorte que la valeur donnée t' soit une racine double de l'équation $\theta = 0$; considérant d'abord les valeurs t' et t'' comme inégales, on aura

$$y' = -\frac{\frac{P}{t'} + \frac{Q}{t'^2} + \frac{R}{t'^3} + \dots}{A + 2Bt' + 3Ct'^2 + 4Dt'^3 + \dots},$$

$$y'' = -\frac{\frac{P}{t''} + \frac{Q}{t''^2} + \frac{R}{t''^3} + \dots}{A + 2Bt'' + 3Ct''^2 + 4Dt''^3 + \dots};$$

et, comme

$$1 + At + Bt^2 + Ct^3 + \dots = \theta = \left(1 - \frac{t}{t'}\right) \left(1 - \frac{t}{t''}\right) \left(1 - \frac{t}{t'''}\right) \dots,$$

on aura, en différentiant et faisant successivement $t = t'$, $t = t''$,

$$A + 2Bt' + 3Ct'^2 + \dots = -\frac{1}{t'} \left(1 - \frac{t'}{t''}\right) \left(1 - \frac{t'}{t'''}\right) \left(1 - \frac{t'}{t^{iv}}\right) \dots,$$

$$A + 2Bt'' + 3Ct''^2 + \dots = -\frac{1}{t''} \left(1 - \frac{t''}{t'}\right) \left(1 - \frac{t''}{t'''}\right) \left(1 - \frac{t''}{t^{iv}}\right) \dots,$$

où l'on voit que dans le cas de $t' = t''$ ces deux quantités seront nulles.

Supposons pour un moment que $t'' = t' + \omega$, ω étant une quantité infiniment petite, on aura, en négligeant les infiniment petits du second ordre,

$$A + 2Bt' + 3Ct'^2 + \dots = -\frac{\omega}{t'^2} \left(1 - \frac{t'}{t''}\right) \left(1 - \frac{t'}{t^{iv}}\right) \dots,$$

$$A + 2Bt'' + 3Ct''^2 + \dots = +\frac{\omega}{t'^2} \left(1 - \frac{t'}{t''}\right) \left(1 - \frac{t'}{t^{iv}}\right) \dots$$

Donc faisant, pour abréger,

$$\Pi = \frac{1}{t'^2} \left(1 - \frac{t'}{t''}\right) \left(1 - \frac{t'}{t^{iv}}\right) \dots,$$

on aura

$$y' = \frac{\frac{P}{t'} + \frac{Q}{t'^2} + \frac{R}{t'^3} + \dots}{\omega \Pi}, \quad y'' = -\frac{\frac{P}{t''} + \frac{Q}{t''^2} + \frac{R}{t''^3} + \dots}{\omega \Pi};$$

mais

$$\begin{aligned} \frac{P}{t''} + \frac{Q}{t''^2} + \frac{R}{t''^3} + \dots &= \frac{P}{t'} + \frac{Q}{t'^2} + \frac{R}{t'^3} + \dots + \omega \frac{d \left(\frac{P}{t'} + \frac{Q}{t'^2} + \frac{R}{t'^3} + \dots \right)}{dt'} \\ &= \frac{P}{t'} + \frac{Q}{t'^2} + \frac{R}{t'^3} + \dots + \omega \left(\frac{P}{t'^2} + \frac{2Q}{t'^3} + \frac{3R}{t'^4} + \dots \right); \end{aligned}$$

donc on aura

$$y'' = -y' + \frac{\frac{P}{t'^2} + \frac{2Q}{t'^3} + \frac{3R}{t'^4} + \dots}{\Pi},$$

et de là

$$y' + y'' = \frac{\frac{P}{t'^2} + \frac{2Q}{t'^3} + \frac{3R}{t'^4} + \dots}{\Pi}.$$

Mais, puisque

$$\theta = \left(1 - \frac{t}{t'}\right) \left(1 - \frac{t}{t''}\right) \left(1 - \frac{t}{t'''}\right) \left(1 - \frac{t}{t^{iv}}\right) \cdots = \left(1 - \frac{t}{t'}\right)^2 \left(1 - \frac{t}{t''}\right) \left(1 - \frac{t}{t^{iv}}\right) \cdots,$$

il est facile de voir qu'on aura, lorsque $t = t'$,

$$\frac{1}{2} \frac{d^2\theta}{dt^2} = \frac{1}{t'^2} \left(1 - \frac{t}{t''}\right) \left(1 - \frac{t}{t^{iv}}\right) \cdots = \text{II};$$

par conséquent

$$\text{II} = \frac{2B + 2 \cdot 3Ct' + 3 \cdot 4Dt'^2 + \dots}{2}$$

Donc

$$\frac{y' + y''}{2} = \frac{\frac{P}{t'^2} + \frac{2Q}{t'^3} + \frac{3R}{t'^4} + \dots}{2B + 2 \cdot 3Ct' + 3 \cdot 4Dt'^2 + \dots}.$$

Ainsi, dans ce cas, la formule ne donnera pas la valeur de chacune des inconnues y' , y'' , qui répondent aux racines égales t' , t'' , mais seulement celle de leur somme $y' + y''$, et l'on voit, tant par l'expression précédente que par l'analyse d'où elle résulte, que la valeur de la moitié de cette somme résultera de l'expression générale de y du numéro précédent, en prenant, à la place du numérateur et du dénominateur, leurs différentielles divisées par dt .

On trouvera de la même manière que, lorsque la valeur donnée de t sera une racine triple de l'équation $\theta = 0$, en sorte que l'on ait, par exemple, $t' = t'' = t'''$, alors on ne pourra pas avoir en particulier chacune des fonctions correspondantes y' , y'' , y''' , mais seulement leur somme $y' + y'' + y'''$; et l'expression générale de y donnera le tiers de cette somme en prenant, à la place du numérateur et du dénominateur de cette expression, leurs différentielles secondes divisées par dt^2 , et ainsi de suite.

102. En général, si en substituant la valeur connue de t dans le dénominateur de l'expression générale de y du n° 101, on trouve que ce dénominateur devient nul, alors on le différentiera autant de fois de suite qu'il sera nécessaire pour qu'il ne devienne plus zéro par la même sub-

stitution, en traitant toujours les différences premières dt comme constantes; on différentiera ensuite un pareil nombre de fois le numérateur, et la nouvelle fraction qu'on aura de cette manière exprimera la somme d'autant de valeurs particulières de y qu'il y aura d'unités dans le nombre des différentiations augmenté de l'unité, cette somme étant divisée par le nombre des valeurs de y ; et ces valeurs seront celles qui répondent aux valeurs égales de t , dont le nombre, comme on sait, est toujours égal à celui des différentielles successives de θ qui s'évanouissent en même temps, augmenté de l'unité.

On connaîtra donc ainsi la somme de ces différentes valeurs de y ; or, on pourra trouver de même la somme de leurs carrés, de leurs cubes, etc., car il n'y aura pour cela qu'à faire un nouveau calcul en prenant, à la place de la fonction y , son carré y^2 , et ensuite le cube y^3 , etc.; de là on tirera, par les formules connues, les valeurs des produits deux à deux, trois à trois, etc., des valeurs de y ; de sorte qu'on connaîtra tous les coefficients de l'équation dont ces valeurs seront les racines; et il faudra ensuite résoudre cette équation pour avoir chacune des valeurs cherchées en particulier.

D'où il s'ensuit que lorsque, parmi les valeurs t', t'', t''', \dots de la fonction t , il s'en trouve deux ou plusieurs qui sont égales entre elles, celles des valeurs y', y'', y''', \dots qui répondent aux valeurs égales de t ne pourront pas être données simplement par une fonction rationnelle de t et des coefficients m, n, p, \dots de l'équation proposée; mais elles le seront par une équation d'un degré égal au nombre de ces valeurs égales, et dont tous les coefficients seront eux-mêmes exprimés rationnellement en t et en m, n, p, \dots

C'est ce qui est d'ailleurs bien naturel et conforme aux principes de l'Analyse. Car, puisqu'il y a différentes valeurs de y qui répondent à une même valeur de t , il est clair que chacune de ces valeurs de y dépendra de la même manière de la valeur correspondante de t , et qu'ainsi ces valeurs ne pourront être que les racines d'une même équation, dont les coefficients seront donnés en t par des expressions rationnelles.

Supposons, par exemple, qu'ayant une équation d'un degré quel-

conque μ , telle que

$$x^\mu + mx^{\mu-1} + nx^{\mu-2} + px^{\mu-3} + \dots = 0,$$

on veuille en trouver une autre d'un degré moindre λ , telle que

$$x^\lambda + ax^{\lambda-1} + bx^{\lambda-2} + cx^{\lambda-3} + \dots = 0,$$

qui ait toutes ses racines communes avec celle-là, c'est-à-dire qui en soit un diviseur; on sait que les coefficients a, b, c, \dots seront tous des fonctions *semblables* des racines de la proposée, et qui seront susceptibles d'un nombre

$$\frac{\mu(\mu-1)(\mu-2)\dots(\mu-\lambda+1)}{1 \cdot 2 \cdot 3 \dots \lambda}$$

de variations, en sorte que chacun de ces coefficients sera nécessairement donné en m, n, p, \dots par une équation d'un degré égal à ce même nombre (n°s 89 et 98). Or, dès qu'on connaîtra la valeur d'un quelconque de ces coefficients, on pourra, à l'aide du Problème que nous venons de résoudre, trouver la valeur de chacun des autres coefficients; et il s'ensuit de notre solution que si la valeur du coefficient supposé connu est une racine simple de l'équation d'où dépend la détermination de ce coefficient, tous les autres pourront être exprimés rationnellement par celui-là; mais si la valeur du coefficient connu est une racine double, ou triple, ou, etc., de la même équation, alors chacun des autres coefficients ne pourra être donné par celui-là que par le moyen d'une équation du second, ou du troisième, ou, etc., degré.

Pour confirmer *à posteriori* ce que nous venons de trouver *à priori*, prenons l'équation du quatrième degré

$$x^4 + mx^3 + nx^2 + px + q = 0,$$

et supposons, comme dans le n° 35 (Section II), qu'elle soit divisible par celle-ci du second degré

$$x^2 + fx + g = 0;$$

on parviendra, ainsi qu'on l'a déjà vu, aux deux équations de conditions

$$p - g(m-f) - f[n - g - f(m-f)] = 0,$$

$$q - g[n - g - f(m-f)] = 0,$$

dont la première donne d'abord

$$g = \frac{p - nf + mf^2 - f^3}{m - 2f};$$

ainsi, ayant g exprimé rationnellement en f , il suffira de trouver la valeur de f pour avoir celle de g sans aucune extraction de racines. Cependant, s'il arrive que la valeur de f soit égale à $\frac{m}{2}$ et qu'on ait en même temps

$p = \frac{mn}{2} - \frac{m^3}{8}$, cette valeur de f donnera $g = 0$; et il faudra alors, pour connaître la valeur de g , avoir recours à l'autre équation où g monte au second degré, et qui est

$$g^2 - (n - mf + f^2)g + q = 0;$$

de sorte qu'en mettant $\frac{m}{2}$ à la place de f on aura celle-ci

$$g^2 - \left(n - \frac{m^2}{4}\right)g + q = 0,$$

par la résolution de laquelle il faudra donc déterminer g . Or je dis que le cas dont il s'agit est celui où la valeur $\frac{m}{2}$ de f sera une racine double de l'équation en f .

Pour le prouver nous remarquerons que cette équation en f doit venir de la substitution de la valeur de g tirée de la première équation, dans la seconde; ainsi faisant, pour abréger,

$$p - nf + mf^2 - f^3 = P, \quad m - 2f = Q,$$

en sorte que $g = \frac{P}{Q}$, on aura, pour l'équation en f , celle-ci

$$P^2 - (n - mf + f^2)PQ + qQ^2 = 0,$$

laquelle étant développée montera au sixième degré et se trouvera la même que celle du numéro cité 35; or il est visible que, lorsque $p = \frac{mn}{2} - \frac{m^3}{8}$, une des racines de cette équation sera égale à $\frac{m}{2}$, parce qu'en faisant $f = \frac{m}{2}$ on aura en même temps $P = 0$ et $Q = 0$; et comme ces deux conditions détruisent, non-seulement tous les termes de l'équation dont il s'agit, mais aussi ceux de sa différentielle qui sera

$$2PdP - (2fdf - mdf) PQ - (n - mf + f^2)(PdQ + QdP) + 2qQdQ = 0,$$

il s'ensuit que la racine $f = \frac{m}{2}$ sera une racine double de la même équation.

103. Nous avons supposé jusqu'ici que les deux fonctions t et y étaient semblables; considérons maintenant le Problème dans toute sa généralité en supposant que ces fonctions soient d'une forme quelconque.

Qu'on fasse successivement dans l'une et l'autre fonction toutes les permutations possibles entre les racines x' , x'' , x''' , ... dont elles sont composées, en n'ayant cependant aucun égard à celles de ces permutations qui redonneraient à la fois les mêmes valeurs de t et de y , et il en résultera un égal nombre ϖ de valeurs correspondantes de t et de y , que l'on désignera, comme dans le n° 100, par t' , t'' , t''' , ..., $t^{(\varpi)}$, et par y' , y'' , y''' , ..., $y^{(\varpi)}$. Dans le cas où les deux fonctions t et y sont semblables, les valeurs t' , t'' , t''' , ..., $t^{(\varpi)}$ seront toutes exprimées d'une manière différente, et seront les racines de l'équation la plus simple $\theta = 0$ qui servira à déterminer la fonction t en m , n , p , ..., et il en sera de même des valeurs y' , y'' , y''' , ..., $y^{(\varpi)}$; ce qui n'empêche cependant pas que quelques-unes des valeurs de t ou de y ne puissent être égales entre elles, comme dans le cas que nous avons examiné dans le n° 102; il s'agit ici uniquement de la forme de ces valeurs et non de leur quantité absolue. Au contraire, lorsque les fonctions t et y ne seront pas semblables, il arrivera nécessairement que parmi les valeurs t' , t'' , t''' , ..., $t^{(\varpi)}$, ou y' , y'' , y''' , ..., $y^{(\varpi)}$ il y en aura qui seront les mêmes, en sorte que le nombre des valeurs différentes de t ou de y sera moindre que ϖ , et il est facile de conclure de ce que nous avons démontré dans le n° 97 que ce nombre

ne pourra être qu'un sous-multiple de ϖ . Or il y a ici deux cas à considérer, suivant que le nombre des valeurs différentes de la fonction donnée t sera égal à ϖ ou à un sous-multiple de ϖ .

1° Supposons que les valeurs $t', t'', t''', \dots, t^{(\varpi)}$ de la fonction t soient toutes différentes, c'est-à-dire représentées d'une manière différente; en ce cas il est clair que l'équation $\theta = 0$ aura nécessairement pour racines toutes ces différentes valeurs, en sorte qu'elle sera essentiellement du degré ϖ , quelles que soient d'ailleurs les valeurs de la fonction cherchée y ; ainsi la solution du n° 100 s'appliquera également à ce cas.

2° Supposons que parmi les valeurs $t', t'', t''', \dots, t^{(\varpi)}$ il n'y en ait qu'un nombre ρ de différentes, ρ étant un facteur de ϖ , en sorte que $\varpi = \rho \sigma$; en ce cas, si $\theta = 0$ est l'équation dont ces différentes valeurs sont les racines, il s'ensuit de ce qu'on a démontré dans le n° 97 que l'équation qui aura toutes les valeurs $t', t'', t''', \dots, t^{(\varpi)}$ pour racines sera $\theta^\sigma = 0$; en sorte que chacune de ses racines en aura $\sigma - 1$ autres qui lui seront égales. On pourra donc encore appliquer à ce cas la solution générale du n° 100, pourvu qu'on prenne $\theta^\sigma = 0$ pour l'équation en t , c'est-à-dire qu'on fasse

$$1 + At + Bt^2 + Ct^3 + \dots = \theta^\sigma;$$

mais, à cause que chaque racine de cette équation est une racine égale, il faudra modifier la solution par les règles données dans le n° 102 pour le cas des racines égales; et au lieu de trouver la valeur de chaque y répondante à chaque t , on ne trouvera plus que la valeur de la somme de toutes les y qui répondront aux valeurs égales de t ; or, comme chacune des valeurs différentes de t se trouve répétée σ fois dans la série $t', t'', t''', \dots, t^{(\varpi)}$, et que d'ailleurs à chacune des valeurs de cette série il répond une valeur de la série $y', y'', y''', \dots, y^{(\varpi)}$, en sorte que les mêmes valeurs de t et de y ne se trouvent pas deux fois dans les mêmes séries à des places correspondantes, il s'ensuit qu'à chaque valeur différente de t il répondra σ valeurs différentes y , et qu'ainsi en connaissant une valeur de t on ne pourra connaître que la somme des σ valeurs différentes de y qui y répondent.

De là et du n° 103 on conclura donc que, dans ce cas, chaque valeur de y ne pourra être donnée en t qu'au moyen d'une équation du degré σ laquelle renfermera à la fois toutes les valeurs de y répondantes à une même valeur de t .

Au reste on peut simplifier beaucoup la solution du cas dont il s'agit en le ramenant à celui des fonctions semblables; car il est visible que si à la valeur t' , par exemple, répondent les valeurs $y', y'', y''', \dots, y^{(\sigma)}$, toute fonction de la forme $f[(y', y'', y''', \dots, y^{(\sigma)})]$ sera telle, qu'elle n'admettra plus que ρ valeurs différentes comme la fonction t' , et qu'ainsi ces deux fonctions seront des fonctions semblables des racines x', x'', x''', \dots . Par conséquent, en prenant à la place de la fonction y une fonction quelconque de la forme $f[(y', y'', y''', \dots, y^{(\sigma)})]$, on trouvera directement la valeur de cette fonction en t par la solution du n° 100, en employant simplement l'équation $\theta = 0$, qui n'aura pour racines que les ρ différentes valeurs de t . Ainsi l'on pourra connaître par ce moyen tous les coefficients de l'équation dont les valeurs $y', y'', y''', \dots, y^{(\sigma)}$ seront les racines, puisque chacun de ces coefficients est nécessairement une fonction de la même forme $f[(y', y'', y''', \dots, y^{(\sigma)})]$ (89).

104. Donc :

1° Si l'on a deux fonctions quelconques t et y des racines x', x'', x''', \dots de l'équation

$$x^{\mu} + mx^{\mu-1} + nx^{\mu-2} + \dots = 0,$$

et que ces fonctions soient telles, que toutes les permutations entre les racines x', x'', x''', \dots , qui feront varier la fonction y , fassent varier aussi en même temps la fonction t , on pourra, généralement parlant, avoir la valeur de y en t et en m, n, p, \dots , par une expression rationnelle, de manière que connaissant une valeur de t on connaîtra aussi immédiatement la valeur correspondante de y ; nous disons *généralement parlant*, car s'il arrive que la valeur connue de t soit une racine double, ou triple, etc., de l'équation en t , alors la valeur correspondante de y dépendra d'une équation carrée, ou cubique, etc., dont tous les coefficients seront des fonctions rationnelles de t et de m, n, p, \dots .

2° Si les fonctions t et y sont telles, que la fonction t conserve la même valeur par des permutations qui font varier la fonction y , alors on ne pourra trouver la valeur de y en t et en m, n, p, \dots qu'au moyen d'une équation du second degré, si à une même valeur de t répondent deux valeurs différentes de y , ou du troisième degré, si à une même valeur de t répondent trois valeurs différentes de y , et ainsi de suite. Les coefficients de ces équations en y seront, généralement parlant, des fonctions rationnelles de t et de m, n, p, \dots , en sorte qu'étant donnée une valeur de t , on aura y par la simple résolution d'une équation du second ou du troisième degré, etc.; mais s'il arrive que la valeur connue de t soit une racine double ou triple, etc., de l'équation en t , alors les coefficients des équations dont il s'agit dépendront encore eux-mêmes d'une équation du second ou du troisième degré, etc.

De là on peut déduire les conditions nécessaires pour pouvoir déterminer les valeurs mêmes des racines x', x'', x''', \dots , au moyen de celles d'une fonction quelconque de ces racines; car il n'y aura pour cela qu'à prendre la simple racine x à la place de la fonction y , et appliquer à ce cas les conclusions précédentes.

105. Voyons maintenant l'application qu'on peut faire des principes établis jusqu'ici, à la résolution générale des équations; nous commencerons par examiner le cas où il n'y a que trois racines $x', x'', x''',$ c'est-à-dire où l'équation proposée est du troisième degré.

Dans ce cas, si l'on considère la fonction générale $f[(x')(x'')(x''')]$, on trouvera qu'elle doit dépendre d'une équation du degré 1.2.3, dont les six racines seront

$$\begin{aligned} f[(x')(x'')(x''')], \quad f[(x'')(x')(x''')], \\ f[(x''')(x'')(x')], \quad f[(x'')(x''')(x')], \\ f[(x')(x''')(x'')], \quad f[(x''')(x')(x'')]. \end{aligned}$$

Maintenant, pour pouvoir abaisser cette équation à un degré moindre que celui de la proposée, il est clair qu'il n'y a d'autre moyen que de faire en sorte que ses racines soient égales, trois à trois; auquel cas elle

se réduira au second degré. Pour cela on supposera que la fonction proposée soit telle, que l'on ait

$$f[(x')(x'')(x''')] = f[(x'')(x''')(x')],$$

indépendamment de toute relation entre les racines x' , x'' , x''' , c'est-à-dire que cette fonction demeure la même en y changeant x' en x'' , x'' en x''' , et x''' en x' ; et l'on aura par la même raison

$$f[(x'')(x''')(x')] = f[(x''')(x')(x'')],$$

et ensuite

$$f[(x''')(x')(x'')] = f[(x')(x'')(x''')];$$

d'où l'on voit que ces trois fonctions

$$f[(x')(x'')(x''')], \quad f[(x'')(x''')(x')], \quad f[(x''')(x')(x'')]$$

seront nécessairement égales, et qu'il n'y aura que ces trois-ci qui puissent l'être en vertu de la condition supposée; par conséquent les trois autres fonctions

$$f[(x'')(x')(x''')], \quad f[(x')(x''')(x'')], \quad f[(x''')(x'')(x')]$$

seront aussi égales; de sorte que (98) l'équation dont il s'agit s'abaissera au degré $\frac{1+2+3}{3} = 2$.

Or, pour trouver, en général, la forme de la fonction proposée, qu'on prenne une autre fonction quelconque représentée par $\varphi[(x')(x'')(x''')]$; qu'on désigne, pour abréger, par y' , y'' , y''' les trois fonctions

$$\varphi[(x')(x'')(x''')], \quad \varphi[(x'')(x''')(x')], \quad \varphi[(x''')(x')(x'')],$$

qui répondent aux trois premières fonctions égales ci-dessus, et par z' , z'' , z''' , les trois fonctions

$$\varphi[(x'')(x')(x''')], \quad \varphi[(x')(x''')(x'')], \quad \varphi[(x''')(x'')(x')],$$

qui répondent aux trois autres fonctions égales; il est clair qu'on pourra exprimer toute fonction de x' , x'' , x''' par une fonction quelconque de y' , y'' , y''' , ou de z' , z'' , z''' , puisque la caractéristique φ dénote une fonction indéterminée quelconque. Ainsi l'on pourra représenter, en général, la

fonction $f[(x')(x'')(x''')]$ par celle-ci $f[(y')(y'')(y''')]$; or il faut, par les conditions du Problème, que cette fonction demeure la même en y échangeant x' en x'' , x'' en x''' et x''' en x' ; donc, puisque par ces échanges les trois quantités y' , y'' , y''' ne font que se changer l'une dans l'autre, il s'ensuit que la fonction $f[(y')(y'')(y''')]$ doit être telle qu'elle demeure la même, quelque permutation qu'on y fasse entre les trois quantités y' , y'' , y''' , et par conséquent qu'elle soit de la forme $f[(y', y'', y''')]$.

Toute fonction donc de la forme

$$f[(y', y'', y''')]$$

aura les propriétés requises, et ne dépendra par conséquent que d'une équation du second degré. En effet, il est facile de voir que, quelques permutations qu'on fasse entre les trois racines x' , x'' , x''' , les trois quantités y' , y'' , y''' ne peuvent que s'échanger entre elles, ou dans les trois quantités analogues z' , z'' , z''' ; d'où il s'ensuit que la fonction

$$f[(y', y'', y''')]$$

ne peut que demeurer la même ou se changer dans la fonction

$$f[(z', z'', z''')],$$

et qu'ainsi ces deux fonctions ne peuvent qu'être les racines d'une même équation du second degré.

Regardons maintenant ces fonctions comme connues, et la difficulté se réduira à trouver par leur moyen les valeurs de chacune des quantités y' , y'' , y''' et z' , z'' , z''' . Or, comme les fonctions dont il s'agit sont de nature à demeurer les mêmes, quelque échange qu'on fasse entre les quantités y' , y'' , y''' , ainsi qu'entre les quantités z' , z'' , z''' , il s'ensuit de ce qui a été démontré ci-dessus, que les trois quantités y' , y'' , y''' seront les racines d'une équation du troisième degré, et les trois quantités z' , z'' , z''' les racines d'une autre équation du troisième degré. Qu'on représente ces équations par celles-ci

$$y^3 - ay^2 + by - c = 0,$$

$$z^3 - fz^2 + gz - h = 0,$$

et, comme les coefficients a , b , c sont des fonctions de la forme $f[(y', y'', y''')]$, et les coefficients f , g , h des fonctions analogues de la forme $f[(z', z'', z''')]$, il résulte de ce qui précède que les coefficients correspondants α et f seront les racines d'une même équation du second degré, dont les coefficients seront donnés en m , n , p , et il en sera de même des coefficients b , g et c , h ; sur quoi il est bon de remarquer que dès qu'on aura trouvé les valeurs de α et f , on pourra, par leur moyen, trouver immédiatement celles de b , g et c , h , par la méthode du n° 100.

Puis donc que les équations en y et z sont l'une et l'autre du troisième degré, il faut tâcher de les ramener à une forme qui en permette la résolution; car, d'un côté, on ne saurait les résoudre, en général, au moins on est censé ne savoir pas les résoudre, puisque la résolution des équations de ce degré est précisément ce qui fait l'objet de cette recherche; de l'autre, on ne peut pas employer la méthode du n° 99 pour abaisser ces équations à un degré inférieur, à cause que l'exposant 3 est un nombre premier qui n'a point de diviseur.

Or, comme la résolution des équations à deux termes est toujours possible, il conviendra de réduire les équations dont il s'agit à cet état; ainsi nous supposerons que l'équation en y devienne

$$y^3 - c = 0,$$

ou, plus généralement, de la forme

$$(y + k)^3 - l = 0;$$

et, pour trouver les conditions nécessaires pour cela, il n'y aura qu'à remarquer qu'en prenant 1 , α , α^2 pour dénoter les racines cubiques de l'unité, on aura

$$y' + k = \sqrt[3]{l}, \quad y'' + k = \alpha \sqrt[3]{l}, \quad y''' + k = \alpha^2 \sqrt[3]{l},$$

d'où l'on tire, à cause de $\alpha^3 = 1$,

$$y' + k = \alpha^2(y'' + k) = \alpha(y''' + k).$$

Ainsi, il faudra que la fonction de x' , x'' , x''' , qu'on a désignée par la

caractéristique φ , soit telle qu'on ait, indépendamment de toute relation entre les racines x' , x'' , x''' ,

$$\varphi[(x')(x'')(x''')] + k = \alpha^2 [\varphi[(x'')(x''')(x')]] + k = \alpha [\varphi[(x''')(x')(x'')]] + k.$$

Et alors on aura aussi, en échangeant x' en x'' ,

$$\varphi[(x'')(x')(x''')] + k = \alpha^2 [\varphi[(x')(x''')(x'')]] + k = \alpha [\varphi[(x''')(x'')(x')]] + k;$$

c'est-à-dire

$$z' + k = \alpha^2 (z'' + k) = \alpha (z''' + k),$$

moyennant quoi l'équation en z se réduira aussi à la forme

$$(z + k)^3 - l' = 0.$$

Or, en comparant l'équation

$$(y + k)^3 - l = 0$$

avec l'équation

$$y^3 - ay^2 + by - c = 0,$$

on a

$$c = l - k^3;$$

et par conséquent, à cause de

$$l = (y + k)^3 = (y' + k)^3$$

(puisque on est maître de substituer, à la place de y , une quelconque de ses racines),

$$c = (y' + k)^3 - k^3;$$

on trouvera de même

$$h = (z' + k)^3 - k^3.$$

De sorte que ces deux quantités

$$[\varphi[(x')(x'')(x''')] + k]^3 - k^3 \quad \text{et} \quad [\varphi[(x'')(x'')(x'')] + k]^3 - k^3$$

seront les racines d'une équation du second degré, qu'on pourra par conséquent regarder comme la *réduite* générale du troisième degré.

Par la résolution de cette équation on connaîtra donc les valeurs des

deux fonctions $\varphi[(x')(x'')(x''')]$ et $\varphi[(x'')(x')(x''')]$, et l'on aura celles des quatre autres fonctions dérivées de celles-ci, par le moyen des équations de condition ci-dessus. Or, ces fonctions étant connues, on pourra en déduire les valeurs de chacune des trois racines x', x'', x''' (104).

106. Voilà donc le principe de la résolution des équations du troisième degré présenté de la manière la plus directe et la plus générale; il est facile d'en faire des applications particulières et d'en déduire les différentes théories que nous avons données dans la Section I.

La forme la plus simple qu'on puisse donner à la fonction

$$\varphi[(x')(x'')(x''')]$$

est celle-ci

$$Ax' + Bx'' + Cx''' + D,$$

A, B, C, D étant des constantes; ainsi l'équation de condition sera

$$\begin{aligned} Ax' + Bx'' + Cx''' + D + k &= \alpha^2(Ax'' + Bx''' + Cx' + D + k) \\ &= \alpha(Ax''' + Bx' + Cx'' + D + k); \end{aligned}$$

d'où l'on tire ces équations

$$\begin{aligned} A &= \alpha^2 C = \alpha B, \\ B &= \alpha^2 A = \alpha C, \\ C &= \alpha^2 B = \alpha A, \\ D + k &= \alpha^2 (D + k) = \alpha (D + k). \end{aligned}$$

La seconde donne

$$B = \alpha^2 A, \quad C = \alpha A,$$

et ces valeurs satisfont aussi en même temps à la première et à la troisième, à cause de $\alpha^3 = 1$; quant à la quatrième, elle donnera

$$D + k = 0, \quad \text{et par conséquent} \quad D = -k;$$

ainsi la fonction proposée sera de la forme

$$A(x' + \alpha^2 x'' + \alpha x''') - k,$$

qui, en faisant $k = 0$, est précisément la même à laquelle nous avons été conduits à *posteriori* dans la Section citée (5).

107. Supposons maintenant qu'il y ait quatre racines, x' , x'' , x''' , x^{IV} , ce qui est le cas des équations du quatrième degré; et, considérant la fonction générale $f[(x')(x'')(x''')(x^{IV})]$, on trouvera qu'elle devra dépendre d'une équation du degré 1.2.3.4 dont les vingt-quatre racines seront (96) :

$$\begin{aligned}
 & f[(x')(x'')(x''')(x^{IV})], \quad f[(x'')(x')(x''')(x^{IV})], \\
 & f[(x''')(x'')(x')(x^{IV})], \quad f[(x'')(x''')(x')(x^{IV})], \\
 & f[(x')(x''')(x'')(x^{IV})], \quad f[(x''')(x')(x'')(x^{IV})], \\
 & f[(x^{IV})(x'')(x''')(x')], \quad f[(x'')(x^{IV})(x''')(x')], \\
 & f[(x''')(x'')(x^{IV})(x')], \quad f[(x'')(x''')(x^{IV})(x')], \\
 & f[(x^{IV})(x''')(x'')(x')], \quad f[(x''')(x^{IV})(x'')(x')], \\
 & f[(x')(x^{IV})(x''')(x'')], \quad f[(x^{IV})(x')(x''')(x'')], \\
 & f[(x''')(x^{IV})(x')(x'')], \quad f[(x^{IV})(x''')(x')(x'')], \\
 & f[(x')(x'')(x^{IV})(x'')], \quad f[(x'')(x')(x^{IV})(x'')], \\
 & f[(x^{IV})(x'')(x')(x'')], \quad f[(x'')(x^{IV})(x')(x'')], \\
 & f[(x')(x^{IV})(x'')(x''')], \quad f[(x'')(x^{IV})(x')(x''')], \\
 & f[(x^{IV})(x'')(x'')(x''')], \quad f[(x'')(x^{IV})(x'')(x''')].
 \end{aligned}$$

Il faudra donc tâcher d'abaisser cette équation à un degré moindre que le quatrième, c'est-à-dire au second ou au troisième degré, et il conviendra de choisir ce dernier, comme étant le plus haut qu'on puisse admettre dans cette recherche. Pour cela, il faudra donc faire en sorte que les vingt-quatre racines que nous venons de trouver soient égales huit à huit, et l'on y parviendra en comparant ces racines les unes avec les autres de toutes les manières possibles, jusqu'à ce qu'on trouve une combinaison qui donne justement huit racines égales, car alors les seize autres seront aussi égales huit à huit (97).

Supposons d'abord

$$f[(x')(x'')(x''')(x^{IV})] = f[(x'')(x')(x''')(x^{IV})],$$

en sorte que la fonction proposée soit de la forme $f[(x', x'')(x''')(x^{IV})]$, et toutes les racines deviendront égales deux à deux, de manière que l'équa-

tion ne montera plus qu'au douzième degré (98). Supposons ensuite qu'on ait aussi

$$f[(x', x'')(x''')(x^{iv})] = f[(x', x'')(x^{iv})(x''')],$$

c'est-à-dire que la forme de la fonction soit $f[(x', x'')(x''', x^{iv})]$, l'équation se réduira par là au sixième degré. Enfin, si l'on suppose encore qu'on ait

$$f[(x', x'')(x''', x^{iv})] = f[(x''', x^{iv})(x', x'')],$$

c'est-à-dire que la fonction proposée soit telle, qu'elle ne change point lorsqu'on y échange à la fois x' et x'' en x''' et x^{iv} , elle se trouvera réduite à l'état demandé, puisqu'elle n'admettra plus que ces trois variations

$$f[(x', x'')(x''', x^{iv})], \quad f[(x', x''')(x'', x^{iv})], \quad f[(x', x^{iv})(x'', x''')],$$

de sorte qu'elle ne pourra dépendre que d'une équation du troisième degré, dont ces trois fonctions seront les racines.

Pour trouver la forme générale de la fonction dont il s'agit, je prends, comme dans le n° 105, une autre fonction quelconque, désignée par $\varphi[(x')(x'')(x''')(x^{iv})]$, et je la réduis d'abord à la forme $\varphi[(x', x'')(x''', x^{iv})]$, pour qu'elle demeure la même en y , changeant x' en x'' ou x'' en x^{iv} ; supposant maintenant, pour plus de simplicité,

$$\begin{aligned} y' &= \varphi[(x', x'')(x''', x^{iv})], \\ y'' &= \varphi[(x''', x^{iv})(x', x'')], \end{aligned}$$

il est clair que toute fonction de la forme $f[(x', x'')(x''', x^{iv})]$ pourra s'exprimer par une fonction de y' et y'' ; de sorte qu'on pourra représenter, en général, la fonction cherchée par $f[(y')(y'')]$; mais il faut, par l'hypothèse, que cette fonction demeure aussi la même en y changeant à la fois x' et x'' en x''' et x^{iv} ; donc, puisque par ces permutations les deux quantités y' et y'' se changent l'une dans l'autre, il faudra que la fonction $f[(y')(y'')]$ soit de la forme $f[(y', y'')]$.

Ainsi l'expression générale de la fonction cherchée sera

$$f[(y', y'')];$$

en effet, si l'on fait

$$z' = \varphi[(x', x'')(x'', x^{iv})],$$

$$z'' = \varphi[(x'', x^{iv})(x', x'')],$$

et ensuite

$$u' = \varphi[(x', x^{iv})(x'', x''')],$$

$$u'' = \varphi[(x'', x''')(x', x^{iv})],$$

il est facile de voir qu'en faisant telle permutation qu'on voudra entre les quatre racines x', x'', x''', x^{iv} , il n'en résultera jamais que ces trois fonctions différentes

$$f[(y', y'')], \quad f[(z', z'')], \quad f[(u', u'')];$$

de sorte qu'elles seront nécessairement racines d'une même équation du troisième degré.

On pourra donc par la résolution d'une équation du troisième degré déterminer la valeur de toute fonction telle que $f[(y', y'')]$. Ainsi, si l'on suppose que les quantités y' et y'' soient les racines de cette équation du second degré

$$y^2 - ay + b = 0,$$

chacun des coefficients a et b sera donné par une équation du troisième degré, puisqu'il sera de la forme $f[(y', y'')]$; de sorte que par là on connaîtra les deux quantités y' et y'' . Or si l'on suppose, ce qui est permis, que la fonction $\varphi[(x', x'')(x'', x^{iv})]$ ne renferme que les deux racines x' et x'' , en sorte qu'elle soit simplement de la forme $\varphi[(x', x'')]$, on aura

$$y' = \varphi[(x', x'')] \quad \text{et} \quad y'' = \varphi[(x'', x^{iv})];$$

donc, si l'on prend x' et x'' pour les racines de l'équation

$$x^2 - fx + g = 0,$$

et x''', x^{iv} pour celles de l'équation

$$x^2 - hx + l = 0,$$

les valeurs des coefficients f, g, h, l ne dépendront que d'équations du

troisième et du second degré; et ces valeurs étant connues on aura celles des quatre racines cherchées par la résolution des deux équations précédentes du second degré.

Tel est le principe général auquel se rapportent la plupart des méthodes pour la résolution des équations du quatrième degré, comme on peut le voir par l'analyse que nous en avons donnée dans la Section II.

En effet, si l'on fait

$$\varphi[(x', x'')] = x' + x'' \quad \text{et} \quad f[(y', y'')] = (y' - y'')^2,$$

il en résultera la solution du n° 32, et faisant

$$\varphi[(x', x'')] = x' x'' \quad \text{et} \quad f[(y', y'')] = y' + y'',$$

il en résultera celle du n° 31, et ainsi des autres.

108. On peut encore dériver la résolution des équations du quatrième degré d'un autre principe, en faisant une combinaison différente des vingt-quatre fonctions du n° 106. Car, si l'on suppose d'abord

$$f[(x')(x'')(x''')(x^{iv})] = f[(x'')(x''')(x^{iv})(x')],$$

c'est-à-dire que la fonction demeure la même en y changeant à la fois x' en x'' , x'' en x''' , x''' en x^{iv} et x^{iv} en x' , on trouvera ensuite

$$f[(x'')(x''')(x^{iv})(x')] = f[(x''')(x^{iv})(x')(x'')],$$

et de là

$$f[(x''')(x^{iv})(x')(x'')] = f[(x^{iv})(x')(x'')(x'''')],$$

et enfin

$$f[(x^{iv})(x')(x'')(x''')] = f[(x')(x'')(x''')(x^{iv})];$$

de sorte que les fonctions

$$f[(x')(x'')(x''')(x^{iv})], \quad f[(x'')(x''')(x^{iv})(x')],$$

$$f[(x''')(x^{iv})(x')(x'')], \quad f[(x^{iv})(x')(x'')(x''')],$$

seront égales, et qu'il n'y aura que ces quatre qui le seront; d'où il s'ensuit que les quatre fonctions dont il s'agit seront égales quatre à quatre, ce qui conduira d'abord à une équation du sixième degré.

Maintenant, si l'on suppose encore cette égalité

$$f[(x')(x'')(x''')(x^{iv})] = f[(x^{iv})(x''')(x'')(x')],$$

c'est-à-dire que la même fonction reste aussi invariable en y changeant à la fois x' en x^{iv} et x'' en x''' , et *vice versa*, il en résultera encore quatre autres fonctions égales aux précédentes, savoir

$$f[(x^{iv})(x''')(x'')(x')], \quad f[(x''')(x'')(x')(x^{iv})],$$

$$f[(x'')(x')(x^{iv})(x''')], \quad f[(x')(x^{iv})(x''')(x'')],$$

moyennant quoi les vingt-quatre fonctions du numéro cité se trouveront égales huit à huit, et ne dépendront plus que d'une équation du troisième degré.

Or, en prenant une autre fonction quelconque des racines x' , x'' , x''' , x^{iv} , qu'on désignera par la caractéristique φ , et désignant par y' , y'' , y''' , y^{iv} , y^v , y^{vi} , y^{vii} , y^{viii} les huit fonctions suivantes

$$\varphi[(x')(x'')(x''')(x^{iv})], \quad \varphi[(x'')(x''')(x^{iv})(x')],$$

$$\varphi[(x''')(x^{iv})(x')(x'')], \quad \varphi[(x^{iv})(x')(x'')(x''')],$$

$$\varphi[(x^{iv})(x''')(x'')(x')], \quad \varphi[(x''')(x'')(x')(x^{iv})],$$

$$\varphi[(x'')(x')(x^{iv})(x''')], \quad \varphi[(x')(x^{iv})(x''')(x'')],$$

qui répondent, comme on voit, aux huit fonctions égales ci-dessus, on pourra représenter toute fonction, qui doit demeurer la même soit en changeant x' en x'' , x'' en x''' , x''' en x^{iv} et x^{iv} en x' , soit en changeant x' en x^{iv} et x'' en x''' , par celle-ci

$$f[(y', y'', y''', y^{iv}, y^v, y^{vi}, y^{vii}, y^{viii})];$$

car il est facile de voir que par ces échanges les quantités y' , y'' , y''' , ... ne feront que s'échanger les unes dans les autres.

Cette fonction aura donc la propriété de ne conduire qu'à une équation du troisième degré; en effet, si l'on désigne par z' , z'' , z''' , z^{iv} , z^v ,

$z^{v_1}, z^{v_2}, z^{v_3}$ ces huit fonctions-ci

$$\begin{aligned} &\varphi[(x'')(x')(x''')(x^{iv})], \quad \varphi[(x''')(x'')(x^{iv})(x')], \\ &\varphi[(x^{iv})(x''')(x')(x'')], \quad \varphi[(x')(x^{iv})(x'')(x''')], \\ &\varphi[(x''')(x^{iv})(x'')(x')], \quad \varphi[(x'')(x''')(x')(x^{iv})], \\ &\varphi[(x')(x'')(x^{iv})(x''')], \quad \varphi[(x^{iv})(x')(x''')(x'')], \end{aligned}$$

et par $u', u'', u''', u^{iv}, u^v, u^{v_1}, u^{v_2}, u^{v_3}$ ces huit autres-ci

$$\begin{aligned} &\varphi[(x''')(x')(x^{iv})(x'')], \quad \varphi[(x^{iv})(x'')(x')(x''')], \\ &\varphi[(x')(x''')(x'')(x^{iv})], \quad \varphi[(x'')(x^{iv})(x')(x''')], \\ &\varphi[(x'')(x^{iv})(x')(x''')], \quad \varphi[(x')(x''')(x^{iv})(x'')], \\ &\varphi[(x^{iv})(x'')(x''')(x')], \quad \varphi[(x''')(x')(x^{iv})(x'')], \end{aligned}$$

on verra aisément que, quelques permutations que l'on fasse entre les quatre racines x', x'', x''', x^{iv} , on n'aura jamais que ces trois fonctions différentes

$$\begin{aligned} &f[(y', y'', y''', y^{iv}, y^v, y^{v_1}, y^{v_2}, y^{v_3})], \\ &f[(z', z'', z''', z^{iv}, z^v, z^{v_1}, z^{v_2}, z^{v_3})], \\ &f[(u', u'', u''', u^{iv}, u^v, u^{v_1}, u^{v_2}, u^{v_3})], \end{aligned}$$

qui seront par conséquent racines d'une équation du troisième degré.

Ainsi, la résolution générale de ce degré étant supposée, on pourra déterminer toutes les fonctions de la forme des précédentes; mais, comme les quantités $y', y'', \dots, z', z'', \dots, u', u'', \dots$ entrent de la même manière dans ces sortes de fonctions, il est clair que leur détermination dépendra encore de trois équations, chacune du huitième degré.

Il faudra donc tâcher de nouveau de rabaisser ces équations au-dessous du quatrième degré; c'est ce qu'on obtiendra en supposant que la fonction représentée par la caractéristique φ soit telle, qu'elle demeure la même en y changeant x' en x'' , x'' en x''' , x''' en x^{iv} et x^{iv} en x' ; car alors les quatre quantités y', y'', y''', y^{iv} deviendront égales, et les quatre autres $y^v, y^{v_1}, y^{v_2}, y^{v_3}$ aussi égales; et il en sera de même des quantités correspondantes z', z'', \dots et u', u'', \dots

De cette manière les trois fonctions précédentes pourront s'exprimer simplement par les formules

$$f[(y', y^v)], \quad f[(z', z^v)], \quad f[u', u^v],$$

et les quantités $y', y^v; z', z^v; u', u^v$ seront les racines de trois équations du second degré telles que

$$y^2 - ay + b = 0,$$

$$z^2 - cz + d = 0,$$

$$u^2 - fu + g = 0,$$

où les coefficients a, c, f seront racines d'une équation du troisième degré, ainsi que les trois autres coefficients b, d, g .

Il ne reste donc qu'à trouver la forme que doit avoir la fonction φ pour que les conditions prescrites aient lieu. Pour y parvenir de la manière la plus générale, on prendra une autre fonction quelconque de x', x'', x''', x^{iv} , qu'on désignera par la caractéristique Φ : on formera, comme ci-dessus, les vingt-quatre fonctions qui répondent aux vingt-quatre permutations qu'on peut faire entre les racines x', x'', x''', x^{iv} ; et l'on désignera ces fonctions par les quantités $Y', Y'', \dots, Y^{viii}, Z', Z'', \dots, Z^{viii}, U', U'', \dots, U^{viii}$; c'est-à-dire qu'on changera dans les formules ci-dessus la caractéristique φ en Φ , et les petites lettres y, z, u dans les grandes lettres Y, Z, U . Ensuite, en prenant de nouveau la caractéristique φ pour désigner une fonction quelconque, il est facile de voir qu'on aura, en général,

$$y' = \varphi[(Y', Y'', Y''', Y^{iv})], \quad y^v = \varphi[(Y^v, Y^{v1}, Y^{v11}, Y^{v111})],$$

$$z' = \varphi[(Z', Z'', Z''', Z^{iv})], \quad z^v = \varphi[(Z^v, Z^{v1}, Z^{v11}, Z^{v111})],$$

$$u' = \varphi[(U', U'', U''', U^{iv})], \quad u^v = \varphi[(U^v, U^{v1}, U^{v11}, U^{v111})].$$

De là il est aisément de conclure que la détermination des fonctions Y', Y'', Y''', Y^{iv} dépendra maintenant d'une équation du quatrième degré, ainsi que celle des fonctions $Y^v, Y^{v1}, Y^{v11}, Y^{v111}$, et il en sera de même des autres fonctions Z', Z'', \dots, Z^{viii} et U', U'', \dots, U^{viii} , qui dépendront aussi quatre à quatre d'équations du quatrième degré.

Soit donc

$$Y^4 - AY^3 + BY^2 - CY + D = 0$$

l'équation dont les racines seraient Y' , Y'' , Y''' , Y^{IV} ; il est clair qu'on pourra la résoudre de deux manières :

1^o En faisant disparaître ses puissances impaires pour la réduire à la forme

$$Y^4 + BY^2 + D = 0.$$

qui est résoluble à la manière de celles du second degré; or pour cela il faudra que les racines Y' , Y'' , Y''' , Y^{IV} soient deux à deux égales et de signes différents, c'est-à-dire que l'on ait

$$Y' = -Y'' \quad \text{et} \quad Y''' = -Y^{IV}.$$

Ainsi il faudra, dans ce cas, que la fonction Φ soit telle, que l'on ait

$$\Phi[(x')(x'')(x''')(x^{IV})] = -\Phi[(x'')(x''')(x^{IV})(x')],$$

et

$$\Phi[(x''')(x^{IV})(x')(x'')] = -\Phi[(x^{IV})(x')(x'')(x''')];$$

c'est-à-dire qu'elle ait la propriété de devenir négative en y changeant x' en x'' , x'' en x''' , x''' en x^{IV} et x^{IV} en x' ; auquel cas on aura aussi

$$\Phi[(x'')(x''')(x^{IV})(x')] = -\Phi[(x''')(x^{IV})(x')(x'')];$$

d'où l'on voit qu'on aura en même temps

$$Y' = -Y'', \quad Y'' = -Y''', \quad Y''' = -Y^{IV};$$

c'est-à-dire

$$Y' = Y'' = -Y''' = -Y^{IV};$$

ce qui rendra l'équation en Y de cette forme

$$(Y^2 - E)^2 = 0, \quad \text{c'est-à-dire} \quad Y^2 - E = 0.$$

Et il est facile de voir que les autres équations dont les racines seront les quantités Y^v , Y^{vi} , Y^{vi} , Y^{viii} , ou Z' , Z'' , Z''' , Z^{iv} , ou, etc., se trouveront aussi par là réduites à la même forme, puisque ces racines ont entre elles

la même relation qu'ont les racines Y' , Y'' , Y''' , Y^{IV} , laquelle consiste en ce que l'une dérive de l'autre par les échanges de x' en x'' , x'' en x''' , x''' en x^{IV} et x^{IV} en x' .

Les fonctions

$$x' + x'' - x'' - x^{IV}, \quad x'x''' - x''x^{IV},$$

et d'autres semblables, auront la propriété dont il s'agit.

2^o On peut aussi rendre résoluble l'équation générale

$$Y^4 - AY^3 + BY^2 - CY + D = 0,$$

en la réduisant à deux seuls termes

$$Y^4 + D = 0;$$

auquel cas les quatre racines Y' , Y'' , Y''' , Y^{IV} seront exprimées ainsi

$$\sqrt[4]{-D}, \quad \alpha \sqrt[4]{-D}, \quad \alpha^2 \sqrt[4]{-D}, \quad \alpha^3 \sqrt[4]{-D},$$

en prenant 1 , α , α^2 , α^3 pour les quatre racines quatrièmes de l'unité; de sorte que la condition pour ce cas sera, à cause de $\alpha^4 = 1$,

$$Y' = \alpha Y'' = \alpha^2 Y''' = \alpha^3 Y^{IV},$$

c'est-à-dire qu'il faudra que la fonction Φ soit telle, qu'on ait

$$\begin{aligned} \Phi[(x')(x'')(x''')(x^{IV})] &= \alpha \Phi[(x'')(x''')(x^{IV})(x')] \\ &= \alpha^2 \Phi[(x''')(x^{IV})(x')(x'')] \\ &= \alpha^3 \Phi[(x^{IV})(x')(x'')(x''')]. \end{aligned}$$

Et alors toutes les équations du quatrième degré d'où dépendent les autres quantités Y^V , Y^{VI} , Y^{VII} , Y^{VIII} , Z' , Z'' , ... se trouveront aussi réduites au même état, par la raison énoncée ci-dessus.

Il est facile de trouver que la fonction

$$x' + \alpha x'' + \alpha^2 x''' + \alpha^3 x^{IV}$$

aura la propriété requise; d'où l'on peut conclure que l'analyse précédente contient le fondement de la méthode du n° 47.

109. Voilà, si je ne me trompe, les vrais principes de la résolution des équations et l'analyse la plus propre à y conduire; tout se réduit, comme on voit, à une espèce de calcul des combinaisons, par lequel on trouve *à priori* les résultats auxquels on doit s'attendre. Il serait à propos d'en faire l'application aux équations du cinquième degré et des degrés supérieurs; dont la résolution est jusqu'à présent inconnue; mais cette application demande un trop grand nombre de recherches et de combinaisons, dont le succès est encore d'ailleurs fort douteux, pour que nous puissions quant à présent nous livrer à ce travail; nous espérons cependant pouvoir y revenir dans un autre temps, et nous nous contenterons ici d'avoir posé les fondements d'une théorie qui nous paraît nouvelle et générale.

110. Avant de terminer cette Section, nous croyons devoir encore traiter en peu de mots de la réduction ou abaissement des équations à un moindre degré, qui a lieu lorsqu'il y a entre quelques-unes des racines de l'équation proposée quelque relation donnée. Car, quand toutes les racines d'une équation ont entre elles les mêmes rapports, l'équation est alors nécessairement et essentiellement d'un degré égal au nombre des racines, et il est impossible, généralement parlant, qu'elle puisse s'abaisser à un moindre degré. C'est ainsi, par exemple, que le Problème de la trisection de l'angle, considéré en général, est nécessairement du troisième degré, puisqu'il y a trois différentes manières d'y satisfaire, lesquelles conduisent toutes à une même équation, où les trois solutions sont également renfermées. Cependant il y a, comme on sait, des cas particuliers où l'on réussit à rabaisser ce Problème au second degré, parce qu'il y a alors un rapport particulier entre deux des racines de l'équation.

Il en est de même de tous les Problèmes et de toutes les équations. S'il y a une relation particulière entre quelques-unes des racines d'une équation quelconque, on est assuré qu'elle peut s'abaisser à un moindre degré; et si l'on connaît *à priori* cette relation, ou par la forme même de l'équation, ou par la nature du Problème qui y a conduit, on pourra toujours trouver la réduction dont elle est susceptible.

M. Hudde est, je crois, le premier qui ait traité cette matière dans la

Lettre *De reductione equationum* qui est imprimée à la suite de la *Géométrie* de Descartes. Il y fait voir comment une équation peut être abaissée à un moindre degré lorsqu'il y a entre quelques-unes de ses racines une relation telle, que leur somme, ou la somme des produits deux à deux, ou des produits trois à trois, ou, etc., est nulle ou égale à une quantité donnée; comme aussi lorsqu'elle renferme des racines égales ou des diviseurs commensurables quelconques. D'autres Géomètres se sont ensuite exercés sur cette matière et ont perfectionné et étendu plus loin les règles et les méthodes de M. Hudde (*voyez* surtout l'excellent Ouvrage de M. Waring cité ci-dessus); mais on peut encore envisager ce sujet d'une manière plus générale d'après les principes établis dans les n°s 100 et suivants.

111. Si, dans l'équation du degré μ

$$x^\mu + mx^{\mu-1} + nx^{\mu-2} + px^{\mu-3} + \dots = 0,$$

dont les racines sont $x', x'', x''', \dots, x^{(\mu)}$, on suppose qu'il y ait une relation connue entre quelques-unes de ces racines, comme entre celles-ci $x', x'', x''', \dots, x^{(\lambda)}$, λ étant plus petit que μ ; il est d'abord clair que cette relation pourra toujours s'exprimer par une équation dont le premier membre sera une fonction algébrique de $x', x'', x''', \dots, x^{(\lambda)}$; de sorte qu'on connaîtra par ce moyen la valeur d'une fonction telle que

$$f[(x')(x'')(x''')\dots(x^{(\lambda)})].$$

Or :

1° Si l'équation dont nous parlons est telle, qu'elle n'ait lieu qu'entre les racines $x', x'', x''', \dots, x^{(\lambda)}$, et même d'une seule manière, en sorte qu'elle cesse d'être vraie si l'on fait une permutation quelconque entre ces racines, alors on pourra, *généralement parlant*, déterminer la valeur de chacune des racines $x', x'', x''', \dots, x^{(\lambda)}$ en particulier sans la résolution d'aucune équation, de sorte que dans ce cas ces racines seront nécessairement toutes commensurables (104).

2° Si l'équation qui renferme la relation donnée entre les racines $x', x'', x''', \dots, x^{(\lambda)}$ n'a lieu à la vérité qu'entre ces racines, mais qu'elle sub-

siste cependant en y changeant, par exemple, x' en x'' , alors on verra par le numéro cité que les deux racines x' , x'' dépendront nécessairement d'une équation du second degré, telle que

$$x^2 - ax + b = 0,$$

dont les coefficients a et b seront commensurables.

3° De même, si l'équation en question est telle, qu'elle soit vraie aussi lorsqu'on y change x' en x'' et en x''' , les trois racines x' , x'' , x''' dépendront alors d'une équation du troisième degré, telle que

$$x^3 - ax^2 + bx - c = 0,$$

où les coefficients a , b , c seront commensurables, et ainsi de suite.

4° Si l'équation qui n'a lieu qué d'une seule manière entre les racines x' , x'' , x''' , ..., $x^{(\lambda)}$, comme dans le premier cas, a lieu aussi en même temps entre les racines $x^{(\lambda+1)}$, $x^{(\lambda+2)}$, $x^{(\lambda+3)}$, ..., $x^{(2\lambda)}$, alors, comme la fonction $f[(x')(x'')(x''') \dots (x^{(\lambda)})]$ demeure la même en y changeant x' en $x^{(\lambda+1)}$, x'' en $x^{(\lambda+2)}$, ..., il est clair que les racines x' , $x^{(\lambda+1)}$ dépendront d'une équation du second degré, comme

$$x^2 - \alpha x + \beta = 0,$$

où α et β seront commensurables; et il en sera de même des racines x'' , $x^{(\lambda+2)}$, des racines x''' , $x^{(\lambda+3)}$, et ainsi des autres.

De même, si l'équation a lieu également entre les racines x' , x'' , x''' , ..., $x^{(\lambda)}$, entre les racines $x^{(\lambda+1)}$, $x^{(\lambda+2)}$, $x^{(\lambda+3)}$, ..., $x^{(2\lambda)}$ et entre les racines $x^{(2\lambda+1)}$, $x^{(2\lambda+2)}$, $x^{(2\lambda+3)}$, ..., $x^{(3\lambda)}$, alors les racines x' , $x^{(\lambda+1)}$, $x^{(2\lambda+1)}$ dépendront d'une équation du troisième degré, telle que

$$x^3 - \alpha x^2 + \beta x - \gamma = 0,$$

où α , β , γ seront commensurables; et il en sera de même des racines x'' , $x^{(\lambda+2)}$, $x^{(2\lambda+2)}$, des racines x''' , $x^{(\lambda+3)}$, $x^{(2\lambda+3)}$, et ainsi de suite.

5° Mais si l'équation qui, comme dans le deuxième cas, a lieu de deux manières différentes entre les racines x' , x'' , x''' , ..., $x^{(\lambda)}$, avait lieu de

même entre les racines $x^{(\lambda+1)}, x^{(\lambda+2)}, x^{(\lambda+3)}, \dots, x^{(2\lambda)}$, alors on aurait pareillement pour les racines x', x'' l'équation du second degré

$$x^2 - a'x + b' = 0,$$

et de même pour les racines $x^{(\lambda+1)}, x^{(\lambda+2)}$ l'équation du second degré

$$x^2 - a''x + b'' = 0,$$

où les coefficients analogues a', a'' seraient racines d'une autre équation du second degré, telle que

$$a^2 - \alpha a + \beta = 0,$$

α et β étant commensurables; et il en serait de même des coefficients b' et b'' .

Et, si la même équation avait lieu aussi parmi les racines $x^{(2\lambda+1)}, x^{(2\lambda+2)}, x^{(2\lambda+3)}, \dots, x^{(3\lambda)}$, alors on aurait pour les racines x', x'' l'équation

$$x^2 - a'x + b' = 0,$$

pour les racines $x^{(\lambda+1)}, x^{(\lambda+2)}$ l'équation

$$x^2 - a''x + b'' = 0,$$

et pour les racines $x^{(2\lambda+1)}, x^{(2\lambda+2)}$ l'équation

$$x^2 - a'''x + b''' = 0,$$

où les coefficients a', a'', a''' seraient eux-mêmes racines de l'équation

$$a^3 - \alpha a^2 + \beta a - \gamma = 0,$$

α, β, γ étant commensurables; et il en serait de même des coefficients b', b'', b''' .

Et ainsi de suite.

6° On fera le même raisonnement sur le troisième cas, où l'on suppose que la même équation ait lieu entre les racines $x', x'', x''', \dots, x^{(\lambda)}$ en y changeant x' en x'' , en x''' ; car, si cette équation subsiste également entre les racines $x^{(\lambda+1)}, x^{(\lambda+2)}, x^{(\lambda+3)}, \dots, x^{(2\lambda)}$, alors les racines x', x'', x'''

dépendront de l'équation du troisième degré

$$x^3 - a'x^2 + b'x - c' = 0,$$

et les racines $x^{(\lambda+1)}, x^{(\lambda+2)}, x^{(\lambda+3)}$ de l'équation analogue

$$x^3 - a''x^2 + b''x - c'' = 0,$$

où les coefficients a' et a'' seront donnés par l'équation du second degré

$$a^2 - \alpha a + \beta = 0,$$

α et β étant rationnels; et il en sera ainsi des coefficients b', b'' et c', c'' .

Par la même raison, si l'équation dont il s'agit subsistait aussi entre les racines $x^{(2\lambda+1)}, x^{(2\lambda+2)}, x^{(2\lambda+3)}, \dots, x^{(3\lambda)}$, on aurait de plus pour les trois racines $x^{(2\lambda+1)}, x^{(2\lambda+2)}, x^{(2\lambda+3)}$ l'équation

$$x^3 - a'''x^2 + b'''x - c''' = 0,$$

et les coefficients a', a'', a''' seraient dans ce cas les racines de l'équation du troisième degré

$$a^3 - \alpha a^2 + \beta a - \gamma = 0,$$

α, β, γ étant rationnels; il en serait de même des coefficients b', b'', b''' et c', c'', c''' .

On voit assez par là les conséquences analogues que l'on peut tirer pour les autres cas; on doit seulement se souvenir que ces conclusions peuvent souffrir quelques exceptions dans les cas particuliers des racines égales (104).

112. Pour éclaircir ce que nous venons de dire par quelques exemples, considérons d'abord les équations qu'on appelle *réciproques*, et qui sont telles, que les coefficients des termes équidistants des extrêmes sont égaux, de cette manière

$$x^n + mx^{n-1} + nx^{n-2} + \dots + nx^2 + mx + 1 = 0;$$

il est visible, par la forme de cette équation, qu'elle demeure la même

en y mettant $\frac{1}{x}$ à la place de x ; d'où il s'ensuit que si x' en est une racine, $\frac{1}{x'}$ en sera une aussi, de sorte qu'on aura $x'x''=1$, c'est-à-dire $x'x''-1=0$; par la même raison on aura $x''x'''=1=0$, $x'''x''''=1=0$, ...

On a donc, dans ce cas, une équation entre les racines x' , x'' , qui subsiste aussi en changeant x' en x'' , et qui a lieu de même entre les racines x''', x'''' ; entre x''', x'''' , Donc, ces racines seront renfermées deux à deux dans les équations suivantes, dont le nombre sera $\frac{\mu}{2}$ ou $\frac{\mu-1}{2}$,

$$x^2 - a'x + 1 = 0,$$

$$x^2 - a''x + 1 = 0,$$

$$x^2 - a'''x + 1 = 0,$$

.....,

les coefficients a' , a'' , a''' , ... étant racines d'une même équation du degré $\frac{\mu}{2}$ ou $\frac{\mu-1}{2}$, suivant que μ sera pair ou impair, comme nous l'avons déjà démontré par une méthode particulière (22). Voyez aussi sur ce sujet, outre les *Miscellanea analytica* de M. Moivre, le tome I^{er} des *Commentaires de Bologne*, et le tome VI des anciens *Commentaires de Petersbourg*.

Au reste on peut, par les principes établis ci-dessus, rendre raison pourquoi la substitution de $y=x+\frac{1}{x}$ que nous avons employée dans le numéro cité doit conduire à une réduite du degré $\frac{\mu}{2}$ lorsque μ est pair. Car il est clair que les valeurs de y , c'est-à-dire les racines de l'équation en y seront

$$x' + \frac{1}{x'}, \quad x'' + \frac{1}{x''}, \quad x''' + \frac{1}{x'''}, \quad x'''' + \frac{1}{x''''}, \dots,$$

mais on a $x'' = \frac{1}{x'}$, $x'''' = \frac{1}{x'''}$, ..., donc ces racines seront

$$x' + \frac{1}{x'}, \quad \frac{1}{x'} + x', \quad x''' + \frac{1}{x'''}, \quad \frac{1}{x''''} + x'''', \dots,$$

et par conséquent égales deux à deux; de sorte que l'équation en y , qui devrait être naturellement du degré μ , s'abaissera d'elle-même au degré $\frac{\mu}{2}$.

On pourrait aussi employer une autre substitution qui abaisserait de même l'équation, mais en faisant disparaître toutes les puissances impaires de l'inconnue; c'est celle-ci $x = \frac{1-y}{1+y}$, laquelle donne $y = \frac{1-x}{1+x}$; car alors les racines de la transformée en y seraient

$$\frac{1-x'}{1+x'}, \quad \frac{1-x''}{1+x''}, \quad \frac{1-x'''}{1+x'''}, \quad \frac{1-x^{iv}}{1+x^{iv}}, \dots$$

c'est-à-dire (à cause de $x'' = \frac{1}{x'}$, $x^{iv} = \frac{1}{x''}$, ...)

$$\frac{1-x'}{1+x'}, \quad \frac{x'-1}{x'+1}, \quad \frac{1-x'''}{1+x'''}, \quad \frac{x'''-1}{x'''+1}, \dots$$

et par conséquent égales deux à deux, et de signes contraires.

113. Dans l'exemple précédent, c'est par la forme même de l'équation qu'on a reconnu la relation qu'il doit y avoir entre ses racines, et qui la rend susceptible de réduction; mais on peut aussi déduire cette connaissance de la nature même du Problème qu'on a à résoudre; c'est ce qu'il est bon de faire voir par quelques exemples.

Soit proposé de trouver quatre quantités en proportion continue, dont la somme soit donnée ainsi que celle de leurs carrés.

Nommant ces quantités inconnues x, y, z, u , on aura par les conditions du Problème ces quatre équations

$$xz = y^2, \quad yu = z^2, \\ x + y + z + u = a, \quad x^2 + y^2 + z^2 + u^2 = b^2,$$

a et b étant des quantités connues.

Pour éliminer plus facilement les trois inconnues y, z, u , et avoir une équation finale en x , je fais $y = rx$, et j'aurai, par les deux premières équations, $z = r^2x$, $u = r^3x$, valeurs qui, étant substituées dans les

deux dernières, donnent celles-ci

$$x(1+r+r^2+r^3)=a, \quad x^2(1+r^2+r^4+r^6)=b^2,$$

d'où il ne s'agira plus que d'éliminer r .

Pour faciliter cette élimination je multiplie la première par $1-r$, et la seconde par $1-r^2$, j'ai ainsi

$$x(1-r^4)=a(1-r), \quad x^2(1-r^8)=b^2(1-r^2),$$

et, divisant cette dernière par l'autre, j'aurai

$$x(1+r^4)=\frac{b^2(1+r)}{a};$$

de sorte qu'on aura maintenant ces deux-ci

$$x(1-r^4)=a(1-r), \quad x(1+r^4)=\frac{b^2}{a}(1+r),$$

d'où il est facile de tirer

$$r=\frac{a^2+b^2-2ax}{a^2-b^2},$$

$$r^4=\frac{2ab^2-(a^2+b^2)x}{(a^2-b^2)x}.$$

Si l'on substitue maintenant la valeur de r , que donne la première de ces équations, dans la seconde, on aura une équation finale en x qui, étant développée, montera au cinquième degré; mais si l'on substitue la même valeur de r dans l'équation primitive

$$x(1+r+r^2+r^3)=a,$$

on en aura une en x qui ne montera qu'au quatrième, et qui sera l'équation la plus simple qu'on puisse avoir pour la détermination de l'inconnue x .

Je vais prouver maintenant, sans connaître même la forme de cette équation, qu'elle doit être décomposable en deux équations du second degré, moyennant une autre équation du second degré aussi.

Pour cela, je remarque que si, au lieu de chercher l'inconnue x , on

eût cherché l'inconnue u , on serait tombé dans une équation semblable; car, faisant $z = su$, on aurait $y = s^2 u$ et $x = s^3 u$; de sorte que les équations en s et u seraient

$$u(1 + s + s^2 + s^3) = a, \quad u^2(1 + s^2 + s^4 + s^6) = b^2,$$

c'est-à-dire entièrement semblables aux équations en x et r . D'où je conclus d'abord que la valeur de l'inconnue u sera nécessairement aussi une des racines de l'équation en x trouvée ci-dessus.

Or, on a $u = r^3 x$, et, divisant la valeur de r^4 , trouvée ci-dessus, par celle de r , on a

$$r^3 = \frac{2ab^2 - (a^2 + b^2)x}{x(a^2 + b^2 - 2ax)};$$

par conséquent,

$$u = \frac{2ab^2 - (a^2 + b^2)x}{a^2 + b^2 - 2ax}.$$

Ainsi, si l'on dénote par x' , x'' , x''' , x^{IV} les quatre racines de l'équation en x dont il s'agit, ces racines seront telles, qu'on aura

$$x'' = \frac{2ab^2 - (a^2 + b^2)x'}{a^2 + b^2 - 2ax'},$$

c'est-à-dire

$$2ax'x'' - (a^2 + b^2)(x' + x'') + 2ab^2 = 0;$$

or, il n'y a pas plus de raison pour que cette équation subsiste entre les deux racines x' , x'' qu'entre les deux autres x''' , x^{IV} ; par conséquent on aura aussi

$$2ax'''x^{IV} - (a^2 + b^2)(x''' + x^{IV}) + 2ab^2 = 0.$$

Voilà donc deux équations semblables qui ont lieu entre les racines x' , x'' et x''' , x^{IV} , et qui sont de plus telles, qu'elles ne changent point en changeant x' en x'' et x''' en x^{IV} ; donc, par le n° 111, on pourra sûrement décomposer l'équation en question du quatrième degré en deux autres du second degré, telles que

$$x^2 - f'x + g' = 0,$$

$$x^2 - f''x + g'' = 0,$$

où les coefficients f' et f'' seront racines d'une équation du second degré ainsi que les coefficients g' et g'' .

Et comme ces deux équations doivent renfermer, l'une les deux racines x' , x'' , et l'autre les deux autres racines x''', x^{iv} , on aura

$$f' = x' + x'', \quad g' = x' x'', \quad f'' = x''' + x^{iv}, \quad g'' = x''' x^{iv};$$

donc on aura

$$2ag' - (a^2 + b^2)f' + 2ab^2 = 0,$$

$$2ag'' - (a^2 + b^2)f'' + 2ab^2 = 0,$$

d'où

$$g' = \frac{(a^2 + b^2)f' - 2ab^2}{2a},$$

$$g'' = \frac{(a^2 + b^2)f'' - 2ab^2}{2a}.$$

De sorte que les deux facteurs de l'équation proposée seront

$$x^2 - f'x + \frac{(a^2 + b^2)f' - 2ab^2}{2a} = 0,$$

$$x^2 - f''x + \frac{(a^2 + b^2)f'' - 2ab^2}{2a} = 0.$$

Pour le faire voir et trouver en même temps l'équation dont les racines seront f' et f'' , il faut chercher d'abord l'équation du Problème en x . Or faisant, pour abréger,

$$c = \frac{a^2 + b^2}{a^2 - b^2}, \quad e = \frac{2a}{a^2 - b^2},$$

on aura $r = c - ex$, et cette valeur, étant substituée dans l'équation

$$x(1 + r + r^2 + r^3) = a,$$

donnera, en ordonnant les termes par rapport à x , celle-ci

$$x^4 - \frac{1+3c}{e}x^3 + \frac{1+2c+3c^2}{e^2}x^2 - \frac{1+c+c^2+c^3}{e^3}x + \frac{a}{e^3} = 0.$$

Maintenant, à cause de

$$\frac{a^2 + b^2}{2a} = \frac{c}{e} \quad \text{et} \quad b^2 = \frac{c^2 - 1}{e^2},$$

les deux facteurs de cette équation seront

$$x^2 - f'x + \frac{cf'}{e} + \frac{1 - c^2}{e^2} = 0,$$

$$x^2 - f''x + \frac{cf''}{e} + \frac{1 - c^2}{e^2} = 0,$$

qui, étant multipliés l'un par l'autre, donnent

$$\begin{aligned} x^4 - (f' + f'')x^3 + \left[f'f'' + \frac{c}{e}(f' + f'') + \frac{2(1 - c^2)}{e^2} \right] x^2 \\ - \left[\frac{2c}{e}f'f'' + \frac{1 - c^2}{e^2}(f' + f'') \right] x + \frac{c^2}{e^2}f'f'' + \frac{c(1 - c^2)}{e^3}(f' + f'') + \frac{(1 - c^2)^2}{e^4} = 0. \end{aligned}$$

La comparaison des trois premiers termes de cette équation avec ceux de la précédente donne d'abord

$$\begin{aligned} f' + f'' &= \frac{1 + 3c}{e}, \\ f'f'' + \frac{c}{e}(f' + f'') + \frac{2(1 - c^2)}{e^2} &= \frac{1 + 2c + 3c^2}{e^2}, \end{aligned}$$

et par conséquent

$$f'f'' = \frac{-1 + c + 2c^2}{e^2}.$$

Et l'on trouvera que ces valeurs de $f' + f''$ et de $f'f''$ satisferont aussi à la comparaison des autres termes.

Ainsi, les quantités f' et f'' seront les racines de cette équation

$$f^2 - \frac{1 + 3c}{e}f + \frac{-1 + c + 2c^2}{e^2} = 0.$$

J'avoue qu'on peut résoudre le Problème précédent d'une manière plus simple, comme Newton l'a fait dans son *Arithmétique universelle*, où, à l'aide d'un certain choix entre les inconnues, il parvient d'abord à deux équations du second degré; mais, d'un côté, il me semble que la

solution que je viens de donner est en quelque façon plus directe et plus lumineuse, puisqu'elle fait voir la raison pourquoi l'équation du quatrième degré, à laquelle on est naturellement conduit, doit être résoluble au moyen de deux du second; et, de l'autre, la règle que Newton établit pour le choix des inconnues n'a point été démontrée par cet Auteur et ne peut l'être, si je ne me trompe, que par les principes généraux que nous avons établis ci-dessus. Mais ce n'est pas ici le lieu de nous étendre sur ce sujet.

114. On pourrait aussi, par la méthode précédente, résoudre avec la même facilité le Problème où l'on demanderait un nombre quelconque μ de quantités en proportion continue, dont la somme et celle de leurs carrés seraient données.

Car, nommant x le premier terme de la progression, et rx le second, on aura d'abord ces deux équations

$$x(1 + r + r^2 + r^3 + \dots + r^{\mu-1}) = a,$$

$$x^2(1 + r^2 + r^4 + r^6 + \dots + r^{2(\mu-1)}) = b^2,$$

qui se changent en ces deux-ci

$$x(1 - r^\mu) = a(1 - r),$$

$$x^2(1 - r^{2\mu}) = b^2(1 - r^2);$$

d'où l'on tire, comme plus haut,

$$r = \frac{a^2 - b^2 - 2ax}{a^2 - b^2},$$

$$r^\mu = \frac{2ab^2 + (a^2 + b^2)x}{(a^2 - b^2)x}.$$

La valeur de r , qu'on peut mettre, comme ci-devant, sous la forme

$$r = c - ex,$$

étant substituée dans la première équation, donnera celle-ci

$$x[1 + (c - ex) + (c - ex)^2 + (c - ex)^3 + \dots + (c - ex)^{\mu-1}] - a = 0,$$

laquelle sera, comme on voit, du degré μ .

On prouvera maintenant, par un raisonnement semblable à celui qu'on a fait plus haut, que le premier terme x et le dernier $r^{\mu-1}x$ de la progression continue devront être également racines de l'équation précédente; mais en divisant la valeur de r^μ par celle de r , on a

$$r^{\mu-1} = \frac{2ab^2 - (a^2 + b^2)x}{x(a^2 + b^2 - 2ax)},$$

donc

$$r^{\mu-1}x = \frac{2ab^2 - (a^2 + b^2)x}{a^2 + b^2 - 2ax}.$$

De là, en nommant x' , x'' , x''' , ..., $x^{(\mu)}$ les racines de l'équation précédente, on aura cette condition, entre les deux racines x' , x'' ,

$$2ax'x'' - (a^2 + b^2)(x' + x'') + 2ab^2 = 0,$$

et comme il n'y a pas plus de raison pour qu'une telle relation ait lieu entre les racines x' , x'' qu'entre les racines x''' , $x^{(iv)}$, ou x^v , $x^{(vi)}$, ou, etc., on aura de même

$$2ax''x^{(iv)} - (a^2 + b^2)(x''' + x^{(iv)}) + 2ab^2 = 0,$$

$$2ax^v x^{(vi)} - (a^2 + b^2)(x^v + x^{(vi)}) + 2ab^2 = 0,$$

.....

le nombre des équations étant $\frac{\mu}{2}$ ou $\frac{\mu-1}{2}$, suivant que μ sera pair ou impair.

D'où, et de ce qu'on a démontré dans le n° 111, il s'ensuit que l'équation du $\mu^{i\text{ème}}$ degré doit être décomposable en $\frac{\mu}{2}$ ou $\frac{\mu-1}{2}$ équations du second degré, telles que

$$x^2 - f'x + g' = 0,$$

$$x^2 - f''x + g'' = 0,$$

$$x^2 - f'''x + g''' = 0,$$

.....

dans lesquelles les coefficients f' , f'' , f''' , ... seront racines d'une même équation du degré $\frac{\mu}{2}$ ou $\frac{\mu-1}{2}$, ainsi que les coefficients g' , g'' , g''' , ...

Et comme, à cause de

$$f' = x' + x'', \quad f'' = x'' + x''' \dots, \quad g' = x' x'', \quad g'' = x'' x''' \dots,$$

on a

$$2ag' - (a^2 + b^2)f' + 2ab^2 = 0,$$

$$2ag'' - (a^2 + b^2)f'' + 2ab^2 = 0,$$

.....

on aura

$$g' = \frac{(a^2 + b^2)f' - 2ab^2}{2a},$$

$$g'' = \frac{(a^2 + b^2)f'' - 2ab^2}{2a},$$

.....

de sorte que les $\frac{\mu}{2}$ ou $\frac{\mu-1}{2}$ facteurs de l'équation dont il s'agit seront

$$x^2 - f'x + \frac{(a^2 + b^2)f' - 2ab^2}{2a} = 0,$$

$$x^2 - f''x + \frac{(a^2 + b^2)f'' - 2ab^2}{2a} = 0,$$

$$x^2 - f'''x + \frac{(a^2 + b^2)f''' - 2ab^2}{2a} = 0,$$

.....

Dans le cas où μ est un nombre pair, le produit de toutes ces équations devra donner l'équation du degré μ trouvée ci-devant; mais, dans le cas où μ est un nombre impair, il faudra y ajouter encore un facteur simple, tel que $x - h = 0$.

La multiplication faite, il n'y aura plus qu'à comparer les premiers termes de l'équation résultante avec ceux de l'équation dont nous venons de parler, et cette comparaison donnera les valeurs des quantités

$$f' + f'' + f''' + \dots, \quad f'f'' + f'f''' + f''f''' + \dots, \quad \dots,$$

qui seront les coefficients de l'équation en f ; et quant au coefficient h , dans le cas où μ est impair, il se trouvera donné par une équation linéaire.

De là il s'ensuit que le Problème proposé peut toujours se réduire à la résolution d'une équation du degré $\frac{\mu}{2}$ ou $\frac{\mu-1}{2}$.

Au reste si, au lieu de déterminer l'inconnue x , on voulait déterminer l'inconnue r , on parviendrait à une équation du genre des *réiproques*; car les deux équations

$$x(1-r^\mu) = a(1-r), \quad x^2(1-r^{2\mu}) = b^2(1-r^2)$$

donnant

$$x(1+r^\mu) = \frac{b^2}{a}(1+r),$$

on aura, en chassant x ,

$$\frac{1-r^\mu}{1+r^\mu} = \frac{a^2}{b^2} \frac{1-r}{1+r},$$

ou bien, en divisant par $1-r$,

$$\frac{1+r+r^2+r^3+\dots+r^{\mu-1}}{1+r^\mu} = \frac{a^2}{b^2} \frac{1}{1+r};$$

d'où, en multipliant en croix et faisant, pour plus de simplicité, $\frac{b^2}{a^2} = c^2$, on aura

$$(c^2-1)r^\mu + 2c^2(r^{\mu-1} + r^{\mu-2} + \dots + r) + c^2 - 1 = 0,$$

c'est-à-dire

$$r^\mu + \frac{2c^2}{c^2-1} (r^{\mu-1} + r^{\mu-2} + \dots + r) + 1 = 0,$$

équation réductible au degré $\frac{\mu}{2}$ ou $\frac{\mu-1}{2}$ par les méthodes connues.

Ce qu'il y aura de plus simple pour cela, ce sera d'employer la substitution de $r = \frac{1-\gamma}{1+\gamma}$, laquelle changera l'équation

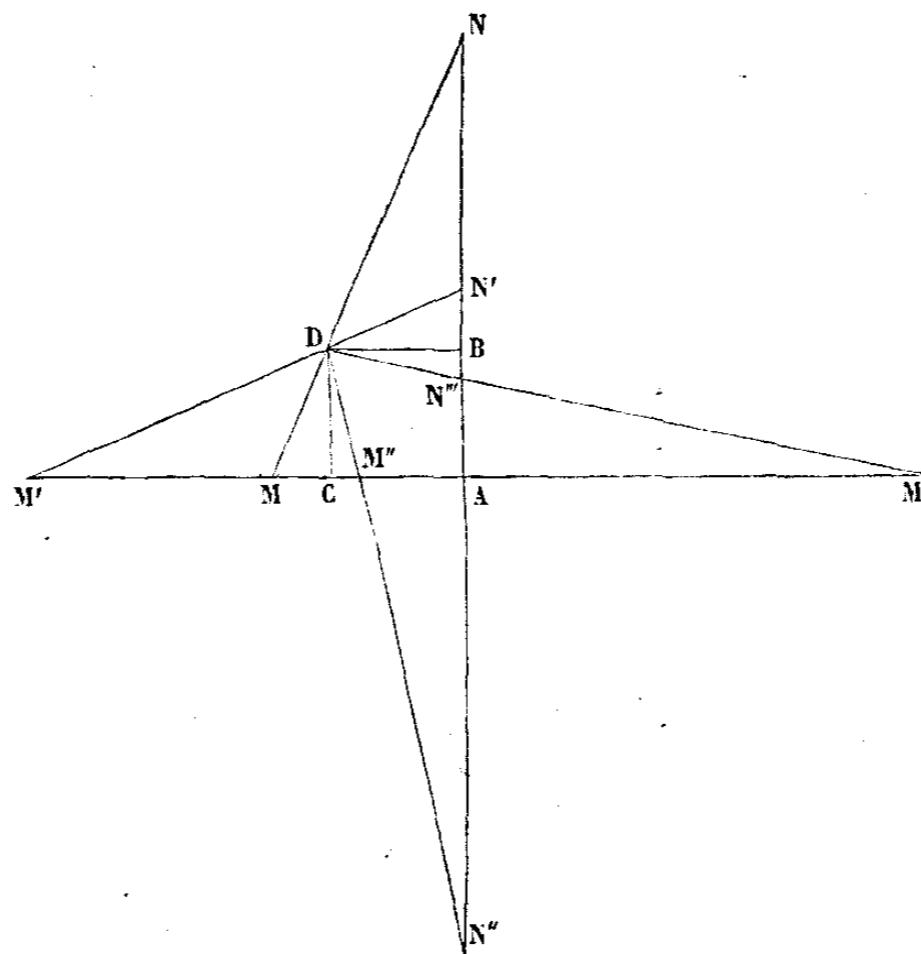
$$\frac{1-r^\mu}{1+r^\mu} = \frac{a^2}{b^2} \frac{1-r}{1+r}$$

en celle-ci

$$\frac{(1+\gamma)^\mu - (1-\gamma)^\mu}{(1+\gamma)^\mu + (1-\gamma)^\mu} = \frac{a^2\gamma}{b^2},$$

où toutes les puissances impaires de γ disparaîtront d'elles-mêmes.

115. Ajoutons encore un Exemple tiré de la Géométrie. Proposons-nous ce Problème très-connu, où il s'agit de mener par le point D du carré ACDB une ligne droite MN telle, que la partie MN de cette ligne, qui sera comprise entre les deux côtés opposés AC, AB du carré, prolongés en M, N, soit d'une grandeur donnée.



Nommant a le côté du carré et b la longueur donnée de la ligne MN, prenons, pour déterminer la position de cette ligne, l'inconnue $CM = x$; on aura donc $MD = \sqrt{x^2 + a^2}$, et les deux triangles semblables MCD, MAN donneront sur-le-champ

$$x : \sqrt{a^2 + x^2} = (a + x) : MN = (a + x) : b;$$

d'où l'on tire l'équation

$$bx = (a + x) \sqrt{a^2 + x^2};$$

laquelle, étant dégagée du radical et ordonnée par rapport à x , deviendra

$$x^4 + 2ax^3 + (2a^2 - b^2)x^2 + 2a^3x + a^4 = 0,$$

qui est, comme on voit, du quatrième degré.

Voyons maintenant si, par la nature même du Problème, on ne pourra

pas trouver quelque relation entre les racines de cette équation, qui la rende décomposable en des équations d'un degré moindre.

Pour y parvenir je remarque qu'on peut en effet mener par le point D quatre lignes qui remplissent la condition du Problème; ce sont les lignes MN , $M'N'$, $M''N''$ et $M'''N'''$; de sorte que les racines de l'équation précédente seront les lignes CM , CM' , CM'' , CM''' , dont les deux dernières sont, comme on voit, négatives.

Dénotons donc ces lignes par x' , x'' , x''' , x^{IV} ; et, à cause des triangles semblables MDC , DNB , on aura

$$MC : CD = DB : BN;$$

mais, puisque $M'N'$ doit être égal à MN , que $CD = DB$, il est facile de voir qu'on aura aussi $M'C = BN$; donc on aura cette proportion

$$x' : a = a : x'',$$

c'est-à-dire

$$x'x'' - a^2 = 0.$$

On pourrait d'abord conclure, par le principe de la raison suffisante, qu'une pareille relation doit aussi avoir lieu entre les deux autres racines x'' , x^{IV} ; mais, si l'on voulait s'en convaincre *à posteriori*, il n'y aurait qu'à considérer qu'à cause de $M''N'' = N''M''$ on aura nécessairement aussi $CM'' = BN''$; et qu'ensuite, à cause des triangles semblables DCM'' , DBN'' , on aura $CM'' : CD = DB : BN'' = DB : CM''$, c'est-à-dire

$$x'' : a = a : x^{IV},$$

et par conséquent

$$x''x^{IV} - a^2 = 0.$$

Puis donc qu'on a deux équations semblables, l'une entre x' , x'' , l'autre en x'' , x^{IV} , et que ces équations subsistent également en changeant x' en x'' , x'' en x^{IV} , il s'ensuit des principes établis plus haut que l'équation du quatrième degré, trouvée ci-dessus, sera nécessairement décomposable en deux équations du second degré, telles que

$$x^2 - f'x + g' = 0,$$

$$x^2 - f''x + g'' = 0,$$

où f' et f'' seront racines d'une équation du second degré, ainsi que g' et g'' ; mais, puisque $g' = x'x''$ et $g'' = x''x'''$, on aura $g' = g'' = a^2$; par conséquent les deux facteurs de l'équation dont il s'agit seront

$$x^2 - f'x + a^2 = 0,$$

$$x^2 - f''x + a^2 = 0.$$

Qu'on en fasse donc le produit, on aura

$$x^4 - (f' + f'')x^3 + (f'f'' + 2a^2)x^2 - a^2(f' + f'')x + a^4 = 0;$$

donc

$$f' + f'' = -2a, \quad f'f'' + 2a^2 = 2a^2 - b^2;$$

par conséquent

$$f'f'' = -b^2;$$

de sorte que l'équation qui aura pour racines les quantités f' et f'' sera

$$f'^2 + 2af' - b^2 = 0.$$

Au reste, il est clair que si, dans l'équation en x du quatrième degré, on fait $x = az$, on aura une équation en z du genre des *réciproques*, et dans laquelle on pourra, par conséquent, faire disparaître toutes les puissances impaires de l'inconnue en faisant $z = \frac{1-y}{1+y}$; de sorte que la substitution propre pour cet effet sera de faire d'abord $x = \frac{a(1-y)}{1+y}$.

Si l'on tire la valeur de y de cette équation, on a

$$y = \frac{a-x}{a+x} = 1 - \frac{2x}{a+x};$$

mais on a

$$\frac{x}{a+x} = \frac{\sqrt{a^2+x^2}}{b} = \frac{MD}{MN};$$

donc on aura

$$y = 1 - \frac{2MD}{MN} = \frac{MN - 2MD}{MN} = \frac{2DR}{MN} = \frac{2DR}{b},$$

supposant que R soit le point du milieu de la ligne MN . De là on voit

Exercices d'analyse et de
physique mathématique.
Tome 3 / par le baron
Augustin Cauchy

Cauchy, Augustin-Louis (1789-1857). Auteur du texte. Exercices d'analyse et de physique mathématique. Tome 3 / par le baron Augustin Cauchy. 1840-1847.

1/ Les contenus accessibles sur le site Gallica sont pour la plupart des reproductions numériques d'oeuvres tombées dans le domaine public provenant des collections de la BnF. Leur réutilisation s'inscrit dans le cadre de la loi n°78-753 du 17 juillet 1978 :

- La réutilisation non commerciale de ces contenus ou dans le cadre d'une publication académique ou scientifique est libre et gratuite dans le respect de la législation en vigueur et notamment du maintien de la mention de source des contenus telle que précisée ci-après : « Source gallica.bnf.fr / Bibliothèque nationale de France » ou « Source gallica.bnf.fr / BnF ».
- La réutilisation commerciale de ces contenus est payante et fait l'objet d'une licence. Est entendue par réutilisation commerciale la revente de contenus sous forme de produits élaborés ou de fourniture de service ou toute autre réutilisation des contenus générant directement des revenus : publication vendue (à l'exception des ouvrages académiques ou scientifiques), une exposition, une production audiovisuelle, un service ou un produit payant, un support à vocation promotionnelle etc.

[CLIQUEZ ICI POUR ACCÉDER AUX TARIFS ET À LA LICENCE](#)

2/ Les contenus de Gallica sont la propriété de la BnF au sens de l'article L.2112-1 du code général de la propriété des personnes publiques.

3/ Quelques contenus sont soumis à un régime de réutilisation particulier. Il s'agit :

- des reproductions de documents protégés par un droit d'auteur appartenant à un tiers. Ces documents ne peuvent être réutilisés, sauf dans le cadre de la copie privée, sans l'autorisation préalable du titulaire des droits.
- des reproductions de documents conservés dans les bibliothèques ou autres institutions partenaires. Ceux-ci sont signalés par la mention Source gallica.BnF.fr / Bibliothèque municipale de ... (ou autre partenaire). L'utilisateur est invité à s'informer auprès de ces bibliothèques de leurs conditions de réutilisation.

4/ Gallica constitue une base de données, dont la BnF est le producteur, protégée au sens des articles L341-1 et suivants du code de la propriété intellectuelle.

5/ Les présentes conditions d'utilisation des contenus de Gallica sont régies par la loi française. En cas de réutilisation prévue dans un autre pays, il appartient à chaque utilisateur de vérifier la conformité de son projet avec le droit de ce pays.

6/ L'utilisateur s'engage à respecter les présentes conditions d'utilisation ainsi que la législation en vigueur, notamment en matière de propriété intellectuelle. En cas de non respect de ces dispositions, il est notamment possible d'une amende prévue par la loi du 17 juillet 1978.

7/ Pour obtenir un document de Gallica en haute définition, contacter utilisation.commerciale@bnf.fr.

MÉMOIRE

SUR LES

ARRANGEMENTS QUE L'ON PEUT FORMER AVEC DES LETTRES DONNÉES,

Et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre.

se présente à la même place dans les deux termes d'une substitution donnée, cette circonstance nous indique que cette place doit pas être déplacée. Ainsi, si on échange entre elles deux lettres, on obtiendra un arrangement

§ 1^{er}. — *Considérations générales.*

Soient

x, y, z, \dots

diverses lettres, qui soient censées représenter des variables indépendantes. Si l'on numérote les places occupées par ces variables dans une certaine fonction Ω , et si l'on écrit à la suite les unes des autres ces variables x, y, z, \dots rangées d'après l'ordre de grandeur des numéros assignés aux places qu'elles occupent, on obtiendra un certain arrangement

$xyz\dots$,

et quand les variables seront déplacées, cet arrangement se trouvera remplacé par un autre, qu'il suffira de comparer au premier pour connaître la nature des déplacements. Cela posé, les diverses valeurs d'une fonction de n lettres correspondront évidemment aux divers arrangements que l'on pourra former avec ces n lettres. D'ailleurs, le nombre de ces arrangements est, comme l'on sait, représenté par le produit

$1.2.3\dots n.$

Si donc on pose, pour abréger,

$N = 1.2.3\dots n,$

N sera le nombre des valeurs diverses, égales ou distinctes, qu'une fonction de n variables acquerra successivement quand on déplacera de toutes les manières, en les substituant l'une à l'autre, les variables dont il s'agit.

On appelle *permutation* ou *substitution* l'opération qui consiste à déplacer les variables, en les substituant les unes aux autres, dans une valeur donnée de la fonction Ω , ou dans l'arrangement correspondant. Pour indiquer cette substitution, nous écrirons le nouvel arrangement qu'elle produit au-dessus du premier, et nous renfermerons le système de ces deux arrangements entre parenthèses. Ainsi, par exemple, étant donnée la fonction

$$\Omega = x + 2y + 3z,$$

où les variables x, y, z occupent respectivement la première, la seconde et la troisième place, et se succèdent en conséquence dans l'ordre indiqué par l'arrangement

$$xyz,$$

si l'on échange entre elles les variables y, z qui occupent les deux dernières places, on obtiendra une nouvelle valeur Ω' de Ω , qui sera distincte de la première, et déterminée par la formule

$$\Omega' = x + 2z + 3y.$$

D'ailleurs, le nouvel arrangement, correspondant à cette nouvelle valeur, sera

$$xzy,$$

et la substitution par laquelle on passe de la première valeur à la seconde, se trouvera représentée par la notation

$$\left(\begin{matrix} xzy \\ xyz \end{matrix} \right),$$

qui indique suffisamment de quelle manière les variables ont été déplacées. Les deux arrangements xzy, xyz , compris dans cette substitution, forment ce que nous appellerons ses *deux termes*, ou son *numérateur* et son *dénominateur*. Comme les numéros qu'on assigne aux diverses places qu'occupent les variables dans une fonction sont entièrement arbitraires, il est clair que l'arrangement correspondant à une valeur donnée de la fonction est pareillement arbitraire, et que le dénominateur d'une substitution quelconque peut être l'un quelconque des N arrangements formés avec les n variables données. On arrivera immédiatement à la même conclusion en observant qu'une substitution quelconque peut être censée indiquer un système déterminé d'opérations simples dont chacune consiste à remplacer une lettre du dénominateur par une lettre du numérateur, et que ce système d'opérations

ne variera pas si l'on échange entre elles d'une manière quelconque les lettres du dénominateur, pourvu que l'on échange entre elles, de la même manière, les lettres correspondantes du numérateur. Il en résulte qu'une substitution, relative à un système de n variables, peut être présentée sous N formes différentes dont nous indiquerons l'équivalence par le signe $=$. Ainsi, par exemple, on aura

$$\begin{pmatrix} xz\gamma \\ x\gamma z \end{pmatrix} = \begin{pmatrix} xy\gamma \\ xz\gamma \end{pmatrix} = \begin{pmatrix} yxz \\ zx\gamma \end{pmatrix} = \text{etc.}$$

Observons encore que l'on peut, sans inconvenienc, effacer toute lettre qui se présente à la même place dans les deux termes d'une substitution donnée, cette circonstance indiquant que la lettre ne doit pas être déplacée. Ainsi, en particulier, on aura

$$\begin{pmatrix} xz\gamma \\ x\gamma z \end{pmatrix} = \begin{pmatrix} z\gamma \\ \gamma z \end{pmatrix}.$$

Lorsqu'on a ainsi éliminé d'une substitution donnée toutes les lettres qu'il est possible d'effacer, cette substitution se trouve réduite à *sa plus simple expression*.

Le *produit* d'un arrangement donné $x\gamma z$ par une substitution $\begin{pmatrix} xz\gamma \\ x\gamma z \end{pmatrix}$ est le nouvel arrangement $xz\gamma$ qu'on obtient en appliquant cette substitution même à l'arrangement donné. Le *produit* de deux substitutions est la substitution nouvelle qui fournit toujours le résultat auquel conduirait l'application des deux premières, opérées l'une après l'autre, à un arrangement quelconque. Les deux substitutions données sont les deux *facteurs* du produit. Le produit d'un arrangement par une substitution ou d'une substitution par une autre s'indiquera par l'une des notations qui servent à indiquer le produit de deux quantités, le multiplicande étant placé, suivant la coutume, à la droite du multiplicateur. On trouvera ainsi, par exemple,

$$\begin{pmatrix} xz\gamma \\ x\gamma z \end{pmatrix} x\gamma z = xz\gamma,$$

et

$$\begin{pmatrix} yxuz \\ x\gamma zu \end{pmatrix} = \begin{pmatrix} yx \\ xy \end{pmatrix} \begin{pmatrix} uz \\ zu \end{pmatrix}.$$

Il y a plus; on pourra, dans le second membre de la dernière équation, échanger sans inconvenienc les deux facteurs entre eux, de sorte qu'on aura

encore

$$\begin{pmatrix} yxuz \\ xzyu \end{pmatrix} = \begin{pmatrix} uz \\ zu \end{pmatrix} \begin{pmatrix} yx \\ xy \end{pmatrix}.$$

Mais cet échange ne sera pas toujours possible, et souvent le produit de deux substitutions variera quand on échangera les deux facteurs entre eux. Ainsi, en particulier, on tronvera

$$\begin{pmatrix} yx \\ xy \end{pmatrix} \begin{pmatrix} zy \\ yz \end{pmatrix} = \begin{pmatrix} yzx \\ xyz \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} zy \\ yz \end{pmatrix} \begin{pmatrix} yx \\ xy \end{pmatrix} = \begin{pmatrix} zxz \\ xyz \end{pmatrix}.$$

Nous dirons que deux substitutions sont *permutables* entre elles, lorsque leur produit sera indépendant de l'ordre dans lequel se suivront les deux facteurs.

Rien n'empêche de représenter par de simples lettres

$$A, B, C, \dots,$$

ou par des lettres affectées d'indices

$$A_1, A_2, A_3, \dots,$$

les arrangements formés avec plusieurs variables. Alors la substitution qui aura pour termes A et B se présentera simplement sous la forme

$$\begin{pmatrix} B \\ A \end{pmatrix},$$

et l'on aura

$$\begin{pmatrix} B \\ A \end{pmatrix} A = B,$$

$$\begin{pmatrix} C \\ B \end{pmatrix} \begin{pmatrix} B \\ A \end{pmatrix} = \begin{pmatrix} C \\ A \end{pmatrix},$$

etc. . .

De plus, si, en appliquant à l'arrangement C la substitution $\begin{pmatrix} B \\ A \end{pmatrix}$, on produit l'arrangement B, on aura non-seulement

$$\begin{pmatrix} B \\ A \end{pmatrix} C = D,$$

mais encore

$$\begin{pmatrix} B \\ A \end{pmatrix} = \begin{pmatrix} D \\ C \end{pmatrix}.$$

Le nombre total des substitutions relatives au système de n variables x, y, z, \dots est évidemment égal au nombre N des arrangements que l'on peut former avec ces variables, puisqu'en prenant pour dénominateur un seul de ces arrangements, le premier par exemple, on peut prendre pour numérateur l'un quelconque d'entre eux. La substitution, dont le numérateur est le dénominateur même, peut être censée se réduire à l'unité, puisqu'on peut évidemment la remplacer par le facteur 1, dans les produits

$$\binom{A}{A} C = C,$$

$$\binom{A}{A} \binom{D}{C} = \binom{D}{C} \binom{A}{A} = \binom{D}{C}.$$

Une substitution $\binom{B}{A}$, multipliée par elle-même plusieurs fois de suite, donne pour produits successifs son *carré*, son *cube*, et généralement ses diverses *puissances*, qui sont naturellement représentées par les notations

$$\binom{B}{A}^2, \quad \binom{B}{A}^3, \dots$$

D'ailleurs, la série qui aura pour termes la substitution $\binom{B}{A}$ et ses diverses puissances, savoir,

$$\binom{B}{A}, \quad \binom{B}{A}^2, \quad \binom{B}{A}^3, \dots$$

ne pourra jamais offrir plus de N substitutions réellement distinctes. Donc, en prolongeant cette série, on verra bientôt reparaître les mêmes substitutions.

D'autre part, si l'on suppose

$$\binom{B}{A}^h = \binom{B}{A}^l,$$

h étant $< l$, alors, en faisant, pour abréger,

$$l = i + h,$$

on aura

$$\binom{B}{A}^h = \binom{B}{A}^{i+h} = \binom{B}{A}^i \binom{B}{A}^h,$$

par conséquent

$$\binom{B}{A}^i = 1,$$

i étant évidemment inférieur à l . Il y a plus; si, en supposant la valeur de i

déterminée par la formule précédente, on nomme l un nombre entier quelconque, k le quotient de la division de l par i , et j le reste de cette division, en sorte qu'on ait

$$l = ki + j,$$

j étant inférieur à i , on trouvera non-seulement

$$\left(\frac{B}{A}\right)^{ki} = \left[\left(\frac{B}{A}\right)^i\right]^k = 1^k = 1,$$

mais, en outre,

$$\left(\frac{B}{A}\right)^l = \left(\frac{B}{A}\right)^{ki} \left(\frac{B}{A}\right)^j = \left(\frac{B}{A}\right)^j;$$

et, en étendant l'avant-dernière formule au cas même où le nombre k se réduit à zéro, on aura encore

$$\left(\frac{B}{A}\right)^0 = 1.$$

En vertu des remarques que nous venons de faire, si l'on prolonge indéfiniment la série dont les divers termes sont

$$\left(\frac{B}{A}\right)^0 = 1, \quad \left(\frac{B}{A}\right), \quad \left(\frac{B}{A}\right)^2, \quad \left(\frac{B}{A}\right)^3, \text{ etc....},$$

le premier des termes qu'on verra reparaître sera précisément l'unité, et à partir de celui-ci les termes déjà trouvés se reproduiront périodiquement dans le même ordre, puisqu'on aura, par exemple,

$$1 = \left(\frac{B}{A}\right)^i = \left(\frac{B}{A}\right)^{2i} = \dots,$$

$$\left(\frac{B}{A}\right) = \left(\frac{B}{A}\right)^{i+1} = \left(\frac{B}{A}\right)^{2i+1} = \dots,$$

$$\left(\frac{B}{A}\right)^2 = \left(\frac{B}{A}\right)^{i+2} = \left(\frac{B}{A}\right)^{2i+2} = \dots,$$

etc....

Donc le nombre i des termes distincts de la série sera toujours la plus petite des valeurs entières de i pour lesquelles se vérifiera la formule

$$\left(\frac{B}{A}\right)^i = 1.$$

Le nombre i , ainsi déterminé, ou le degré de la plus petite des puissances

de $\binom{B}{A}$ équivalentes à l'unité, est ce que nous appellerons le degré ou l'ordre de la substitution $\binom{B}{A}$.

Supposons maintenant qu'une substitution réduite à sa plus simple expression se présente sous la forme

$$\begin{pmatrix} yz \dots vw \\ xy \dots uvw \end{pmatrix},$$

c'est-à-dire qu'elle ait pour objet de remplacer x par y , puis y par z, \dots , et ainsi de suite jusqu'à ce que l'on parvienne à une dernière variable w , qui devra être remplacée par la variable x de laquelle on était parti. Pour effectuer cette substitution, il suffira évidemment de ranger sur la circonference d'un cercle *indicateur*, divisée en parties égales, les diverses variables

$$x, y, z, \dots, u, v, w,$$

en plaçant la première, la seconde, la troisième, ... sur le premier, le second, le troisième, ... point de division, puis de remplacer chaque variable par celle qui la première viendra prendre sa place, lorsqu'on fera tourner dans un certain sens le cercle indicateur. Pour ce motif nous donnons à la substitution dont il s'agit le nom de *substitution circulaire*. Nous la représenterons, pour abréger, par la notation

$$(x, y, z, \dots, u, v, w);$$

et il est clair que, dans cette notation, une quelconque des variables

$$x, y, z, \dots, u, v, w$$

pourra occuper la première place. Ainsi, par exemple, on aura identiquement

$$(x, y, z) = (y, z, x) = (z, x, y).$$

Si l'on nomme i le nombre des variables comprises dans une substitution circulaire

$$(x, y, z, \dots, u, v, w),$$

alors, pour opérer cette substitution l fois de suite, ou, ce qui revient au même, pour l'élever à la puissance du degré l , il suffira évidemment de faire tourner le cercle indicateur, de manière que le point de division correspondant à chaque lettre parcoure une portion de la circonference mesurée par

le rapport $\frac{l}{i}$. Cela posé, pour ramener chaque lettre à sa place, il faudra évidemment que $\frac{l}{i}$ soit un nombre entier, et que l'on ait au moins $l = i$. Donc l'ordre d'une substitution circulaire sera précisément le nombre i des lettres qu'elle renferme.

Si, dans le cercle indicateur, on joint par une corde deux points de division correspondants à deux variables dont l'une prendrait la place de l'autre, en vertu de la substitution circulaire

$$(x, y, z, \dots, u, v, w),$$

i fois répétée, ou, ce qui revient au même, en vertu de la substitution

$$(x, y, z, \dots, u, v, w)^i,$$

le système des cordes ainsi tracées offrira évidemment ou un polygone régulier, ou un système de polygones réguliers.

Si le degré i est premier à l , c'est-à-dire au nombre qui représente l'ordre de la substitution circulaire

$$(x, y, z, \dots, u, v, w),$$

le système des cordes dont il s'agit constituera simplement un polygone régulier, qui pourra être du genre de ceux que M. Poinsot a nommés *polygones étoilés*. Mais si, les nombres i et l offrant un ou plusieurs facteurs communs, on nomme k le plus grand commun diviseur de ces deux nombres, et α le quotient de la division de i par k , alors le système des cordes tracées constituera un système de k polygones réguliers, étoilés ou non étoilés, dont chacun renfermera α côtés seulement. Donc alors aussi la substitution

$$(x, y, z, \dots, u, v, w)^i$$

sera le produit de k substitutions circulaires de l'ordre α . Si, pour fixer les idées, on pose $i = 4$, alors, en élevant à la seconde et à la troisième puissance la substitution circulaire

$$(x, y, z, u),$$

on trouvera

$$(x, y, z, u)^2 = (x, z)(y, u), \quad (x, y, z, u)^3 = (x, u, z, y).$$

Si, au contraire, l'on pose $i = 6$, alors, en élevant à diverses puissances la substitution circulaire

$$(x, y, z, u, v, w),$$

on trouvera

$$(x, y, z, u, v, w)^2 = (x, z, v)(y, u, w), \quad (x, y, z, u, v, w)^3 = (x, u)(y, v)(z, w),$$

$$(x, y, z, u, v, w)^4 = (x, v, z)(y, w, u), \quad (x, y, z, u, v, w)^5 = (x, w, v, u, z, y).$$

Soient maintenant

A et B

deux quelconques des arrangements que l'on peut former avec n variables, x, y, z, \dots . Pour substituer le second arrangement au premier, il suffira évidemment d'opérer une ou plusieurs substitutions circulaires, que l'on formera sans peine en écrivant à la suite l'une de l'autre deux variables, dont l'une sera remplacée par l'autre quand on passera du premier arrangement au second. En conséquence, la substitution $\binom{B}{A}$, réduite à sa plus simple expression, sera nécessairement, ou une substitution circulaire, ou le produit de plusieurs substitutions circulaires. On trouvera, par exemple, en supposant que $\binom{B}{A}$ renferme quatre ou cinq variables,

$$\binom{uzyx}{xyzu} = (x, u)(y, z), \quad \binom{zuwyzx}{xyzuw} = (x, z, v)(y, u).$$

Les substitutions circulaires dont une substitution quelconque $\binom{A}{B}$ sera le produit, sont ce que nous appellerons les *facteurs circulaires* de $\binom{B}{A}$. Deux quelconques d'entre elles, étant composées de lettres diverses, seront évidemment permutables. Donc, tous les facteurs circulaires de $\binom{B}{A}$ seront permutables entre eux, et représenteront des substitutions qui pourront être effectuées dans un ordre quelconque. Il y a plus : comme deux substitutions égales seront nécessairement permutables entre elles, si l'on élève $\binom{B}{A}$ à des puissances quelconques, on obtiendra de nouvelles substitutions qui seront permutables entre elles, ainsi que leurs facteurs représentés par des puissances des facteurs circulaires de $\binom{B}{A}$.

Supposons, pour fixer les idées, que les variables comprises dans les divers facteurs circulaires de $\binom{B}{A}$ soient respectivement :

dans le premier facteur..... $\alpha, \beta, \gamma, \dots$

dans le second facteur..... λ, μ, ν, \dots

dans le troisième facteur..... $\varphi, \chi, \psi, \dots$

etc. etc.

en sorte qu'on ait

$$(1) \quad \binom{B}{A} = (\alpha, \beta, \gamma, \dots) (\lambda, \mu, \nu, \dots) (\varphi, \chi, \psi, \dots) \dots$$

Alors, l étant un nombre entier quelconque, on aura encore

$$\binom{B}{A}^l = (\alpha, \beta, \gamma, \dots)^l (\lambda, \mu, \nu, \dots)^l (\varphi, \chi, \psi, \dots)^l \dots$$

et, pour que l vérifie l'équation

$$(2) \quad \binom{B}{A}^l = 1, \quad \text{il faudra qu'on ait séparément}$$

$$(3) \quad (\alpha, \beta, \gamma, \dots)^l = 1, \quad (\lambda, \mu, \nu, \dots)^l = 1, \quad (\varphi, \chi, \psi, \dots)^l = 1, \dots$$

Or, les seules valeurs de l , propres à vérifier l'équation (2), seront l'ordre i de la substitution $\binom{B}{A}$ et les multiples de i . Pareillement les valeurs de l propres à vérifier l'une quelconque des formules (3) seront l'ordre du facteur circulaire qui entre dans cette formule et les multiples de cet ordre. Cela posé, soient

$$a, b, c, \dots$$

les nombres qui représentent les ordres respectifs des substitutions circulaires

$$(\alpha, \beta, \gamma, \dots), \quad (\lambda, \mu, \nu, \dots), \quad (\varphi, \chi, \psi, \dots), \dots$$

et r le nombre des variables qui se trouvent exclues de la substitution $\binom{B}{A}$ quand elle est réduite à son expression la plus simple. Non-seulement on aura

$$(4) \quad a + b + c + \dots + r = n,$$

attendu que les divers groupes

$$\alpha, \beta, \gamma, \dots,$$

$$\lambda, \mu, \nu, \dots,$$

$$\varphi, \chi, \psi, \dots,$$

etc.,

devront renfermer en somme les $n-r$ lettres auxquelles se rapporte la substitution $\binom{B}{A}$; mais, de plus, on conclura évidemment de ce qui précède, que

l'ordre i de la substitution $\binom{B}{A}$ sera le plus petit nombre divisible à la fois par a , par b , par c , etc.

Considérons maintenant en particulier, parmi les variables x, y, z, \dots , celles qui ne sont pas déplacées par la substitution $\binom{B}{A}$, et nommons u l'une de ces dernières. Comme nous l'avons remarqué, la variable u se trouvera exclue de la substitution $\binom{B}{A}$ réduite à son expression la plus simple; mais, d'autre part, rien n'empêchera de mettre cette variable u en évidence, et de la considérer comme formant à elle seule un facteur circulaire du premier ordre, savoir, le suivant :

$$\binom{u}{u} = 1.$$

On pourra même présenter ce facteur du premier ordre sous une forme analogue à celles des facteurs circulaires

$(x, y), (x, y, z), \dots$, en écrivant simplement (u) au lieu de $\binom{u}{u}$, de même qu'on écrit $(x, y, z), \dots$ au lieu de $\binom{yx}{xy}, \binom{yzx}{xyz}, \dots$

Il suit de cette observation que, dans la formule (4), on peut regarder la lettre r comme exprimant le nombre des facteurs circulaires du premier ordre, renfermés dans la substitution $\binom{B}{A}$. Ajoutons que, dans la formule (4), deux ou plusieurs des nombres

$$a, b, c, \dots, r$$

peuvent être supposés égaux entre eux. Si l'on se place dans cette hypothèse, et si, pour plus de commodité, on suppose la substitution $\binom{B}{A}$ équivalente au produit que l'on obtient quand on multiplie entre eux

f facteurs circulaires de l'ordre a ,

g facteurs circulaires de l'ordre b ,

h facteurs circulaires de l'ordre c ,

etc., et enfin

r facteurs circulaires du premier ordre; la formule (4) se trouvera évidemment remplacée par la suivante

$$(5) \quad fa + gb + hc + \dots + r = n.$$

Une substitution quelconque $\binom{B}{A}$ sera dite *régulière*, lorsqu'elle sera, ou une substitution circulaire, ou le produit de plusieurs substitutions circulaires de même ordre. Elle sera *irrégulière* dans le cas contraire. Cela posé, l'ordre d'une substitution régulière est évidemment l'ordre de ses facteurs circulaires; de plus, toute substitution régulière est une puissance d'une certaine substitution circulaire. Ainsi, par exemple, la substitution régulière

$$(x, u) (y, v) (z, w)$$

est le cube de la substitution circulaire

$$(x, y, z, u, v, w).$$

Enfin, étant donnée une substitution régulière qui renferme plusieurs variables x, y, z, \dots , celles de ses puissances qui ne se réduiront pas à l'unité seront des substitutions régulières qui renfermeront nécessairement toutes ces variables. Au contraire, les puissances d'une substitution irrégulière seront, les unes irrégulières, les autres régulières; et celles qui seront régulières renfermeront un moindre nombre de variables. Ainsi, par exemple, la substitution irrégulière

$$(x, y, z) (u, v),$$

qui renferme les variables

$$x, y, z, u, v,$$

aura pour cinquième puissance la substitution irrégulière

$$(x, z, y) (u, v),$$

qui renfermera encore les cinq variables données; mais elle aura pour carré, pour cube et pour quatrième puissance les substitutions régulières

$$(x, z, y), (u, v), (x, y, z),$$

dont chacune renfermera deux ou trois variables seulement.

Il est bon d'observer que si, après avoir substitué à l'arrangement A un autre arrangement B, on veut revenir de l'arrangement B à l'arrangement A, cette seconde opération, inverse de la première, sera représentée, non plus par la notation $\binom{B}{A}$, mais par la notation $\binom{A}{B}$. En conséquence, il

est naturel de dire que les deux substitutions

$$\begin{pmatrix} B \\ A \end{pmatrix}, \quad \begin{pmatrix} A \\ B \end{pmatrix}$$

sont *inverses* l'une de l'autre. Cela posé, il est clair que, si la substitution $\begin{pmatrix} B \\ A \end{pmatrix}$ fait passer à la place de x une autre variable y , la substitution inverse $\begin{pmatrix} A \\ B \end{pmatrix}$ fera passer, au contraire, y à la place de x . Si la substitution $\begin{pmatrix} B \\ A \end{pmatrix}$ se réduisait à une substitution circulaire du second ordre, en sorte qu'on eût, par exemple,

$$\begin{pmatrix} B \\ A \end{pmatrix} = (x, y),$$

elle aurait pour effet unique d'échanger entre elles les deux variables x, y , et se confondrait avec la substitution inverse

$$\begin{pmatrix} A \\ B \end{pmatrix} = (y, x).$$

Ajoutons que les facteurs circulaires de $\begin{pmatrix} A \\ B \end{pmatrix}$ seront évidemment *inverses* des facteurs circulaires de $\begin{pmatrix} B \\ A \end{pmatrix}$.

§ II. — *Extension des notations adoptées dans le premier paragraphe. Substitutions semblables entre elles.*

Considérons n variables indépendantes

et soient

$$x, y, z, \dots, A, B, C, D, \text{ etc.}$$

les arrangements divers qui peuvent être formés avec ces variables. Rien n'empêchera de représenter par de simples lettres

$$P, Q, R, \dots$$

les substitutions qui consistent à remplacer ces arrangements l'un par l'autre, et de prendre, par exemple,

$$P = \begin{pmatrix} B \\ A \end{pmatrix}, \quad Q = \begin{pmatrix} D \\ C \end{pmatrix}.$$

Cela posé, les diverses puissances d'une substitution P se trouveront représentées par les notations

$$P^0 = 1, \quad P, \quad P^2, \quad P^3, \dots;$$

et si l'on nomme i l'ordre de la substitution P , c'est-à-dire la plus petite des valeurs entières de l pour lesquelles se vérifie la formule

$$(1) \quad P^l = 1;$$

alors, en désignant par k et par l des nombres entiers quelconques, on aura

$$(2) \quad P^{ki+l} = P^l.$$

En généralisant la formule (2), on est naturellement amené à considérer non-seulement des puissances positives, mais encore des puissances négatives de la substitution P . En effet, pour assigner une signification précise à la notation

$$P^{-l},$$

il suffit d'étendre, par analogie, la formule (2) au cas même où l devient négatif. Alors on trouve

$$(3) \quad P^{-l} = P^{ki-l},$$

et, en particulier,

$$(4) \quad P^{-i} = P^{i-i}.$$

Si, pour fixer les idées, on suppose $i = 6$, et

$$P = (x, y, z) (u, v),$$

on aura

$$P^{-i} = P^5 = (x, z, y) (u, v).$$

La substitution P^{-i} n'étant pas distincte de la substitution P^{i-i} , il en résulte que chacun des produits

$$PP^{-i} \quad \text{ou} \quad P^{-i}P$$

se réduit, comme on devait s'y attendre, à

$$P^i = P^0 = 1.$$

Donc, par suite, si l'on a

$$P = \begin{pmatrix} B \\ A \end{pmatrix},$$

P^{-i} sera la substitution qui, multipliée par $\begin{pmatrix} B \\ A \end{pmatrix}$, donne pour produit l'u-

nité, c'est-à-dire la substitution $\begin{pmatrix} A \\ B \end{pmatrix}$, inverse de $\begin{pmatrix} B \\ A \end{pmatrix}$. Ainsi, les notations

$$P, P^{-1}$$

désignent généralement deux substitutions *inverses* l'une de l'autre.

Ajoutons que l'inverse de la substitution P^l sera évidemment P^{-l} .

Deux substitutions étant toujours inverses l'une de l'autre, quand leur produit est l'unité, on en conclut que la substitution PQ a pour inverse $Q^{-1}P^{-1}$, et que, pareillement, la substitution P^hQ^k a pour inverse $Q^{-k}P^{-h}$.

Deux substitutions distinctes

$$P = \begin{pmatrix} B \\ A \end{pmatrix}, \quad Q = \begin{pmatrix} D \\ C \end{pmatrix}$$

seront dites *semblables* entre elles, quand elles offriront le même nombre de facteurs circulaires et le même nombre de lettres dans les facteurs circulaires correspondants, en sorte que les facteurs circulaires, comparés deux à deux, soient de même ordre.

D'après cette définition, deux substitutions circulaires de même ordre seront toujours semblables entre elles, et l'on pourra en dire autant de deux substitutions régulières qui, étant de même ordre, offriront le même nombre de facteurs circulaires. Ainsi, par exemple, la substitution circulaire de second ordre

$$(x, y)$$

sera semblable à chacune des substitutions

$$(x, z), \quad (x, u), \dots, \quad (y, z), \dots$$

La substitution du troisième ordre

$$(x, y, z)$$

sera semblable, non-seulement à son carré

$$(x, z, y),$$

mais encore à chacune des substitutions

$$(x, y, u), \quad (x, z, u), \dots, \quad (y, z, u), \dots, \quad (u, v, w), \dots$$

Ainsi encore les trois substitutions régulières, du second ordre, que l'on peut former avec quatre variables x, y, z, u , savoir :

$$(x, y)(z, u), \quad (x, z)(y, u), \quad (x, u)(y, z),$$

sont semblables l'une à l'autre.

Étant données deux substitutions P , Q semblables entre elles, on peut toujours écrire la seconde au-dessus de la première, de telle sorte que les facteurs circulaires de même ordre se correspondent deux à deux. Alors, aux diverses variables que renfermait la substitution P , correspondront, dans la substitution Q , d'autres variables qui remplaceront les premières. Cela posé, concevons que l'on présente les deux substitutions P , Q sous les formes

$$P = \begin{pmatrix} B \\ A \end{pmatrix}, \quad Q = \begin{pmatrix} D \\ C \end{pmatrix},$$

en prenant pour A un arrangement quelconque, et en nommant C celui que l'on obtient, lorsque dans l'arrangement A on remplace chaque variable par la variable correspondante, prise dans la substitution Q . Il est clair que les deux substitutions

$$P = \begin{pmatrix} B \\ A \end{pmatrix} \quad \text{et} \quad Q = \begin{pmatrix} D \\ C \end{pmatrix},$$

quand elles seront semblables l'une à l'autre, déplaceront, de la même manière, les variables qui occupaient les mêmes places dans les arrangements A et C . Donc alors, si l'on écrit l'un au-dessus de l'autre, d'une part, les arrangements A et C , d'autre part, les arrangements B et D , les variables qui se correspondront dans les arrangements A et C , se correspondront encore dans les arrangements B et D , produits, le premier, par l'application de la substitution P à l'arrangement A ; le second, par l'application de la substitution Q à l'arrangement C . Donc on aura, dans l'hypothèse admise,

$$(5) \quad \begin{pmatrix} D \\ B \end{pmatrix} = \begin{pmatrix} C \\ A \end{pmatrix}.$$

Réiproquement, si la condition (5) est remplie, les deux substitutions

$$P = \begin{pmatrix} B \\ A \end{pmatrix}, \quad Q = \begin{pmatrix} D \\ C \end{pmatrix},$$

appliquées la première à l'arrangement A , la seconde à l'arrangement C , déplaceront certainement, de la même manière, les variables qui, dans ces deux arrangements, occupaient les mêmes places. Donc, par suite, ces deux substitutions devront offrir le même nombre de facteurs circulaires, et le même nombre de lettres dans les facteurs circulaires correspondants, c'est-à-dire qu'elles seront semblables l'une à l'autre.

Il est bon d'observer que les arrangements ci-dessus désignés par les lettres A , B , C , D sont censés comprendre généralement toutes les variables que l'on considère. Donc, pour trouver les variables qui doivent se corres-

pondre dans les arrangements A et C, il est nécessaire de mettre en évidence toutes les variables, et non pas seulement celles qui se trouveraient renfermées dans les valeurs des substitutions P, Q, réduites à leurs plus simples expressions. Ainsi, par exemple, si les substitutions P, Q, formées chacune avec cinq des six variables

$$x, y, z, u, v, w,$$

se réduisent aux suivantes

$$P = (x, y, z)(u, v), \quad Q = (y, z, u)(v, w),$$

elles seront semblables l'une à l'autre. Mais, si l'on veut les présenter sous la forme

$$P = \binom{B}{A}, \quad Q = \binom{D}{C},$$

A, B, C, D étant des arrangements qui vérifient la condition (5), on devra commencer par mettre en évidence les six variables

$$x, y, z, u, v, w,$$

dans chacune des substitutions P, Q, en introduisant dans la substitution P le facteur de premier ordre (w), et, dans la substitution Q, le facteur (x). Alors, en écrivant Q au-dessus de P, de manière à faire correspondre les uns aux autres les facteurs circulaires de même ordre, on trouvera

$$Q = (y, z, u)(v, w)(x), \\ P = (x, y, z)(u, v)(w),$$

et, par suite, on pourra prendre

$$A = xyzuvw, \quad C = yzuvwx.$$

Si l'on adopte effectivement ces valeurs de A et de C, on trouvera encore

$$B = PA = yzxvuw, \quad D = QB = zuywvx,$$

et, par suite, on aura non-seulement

$$\binom{C}{A} = \binom{yzuvw}{xyzuvw} = (x, y, z, u, v, w),$$

mais aussi

$$\binom{D}{B} = \binom{zuywvx}{yzxvuw} = (y, z, u, v, w, x) = \binom{C}{A}.$$

Donc, les arrangements A, B, C, D seront, comme on devait s'y attendre, du nombre de ceux qui vérifient la formule (5).

Concevons maintenant que, les deux substitutions

$$P = \begin{pmatrix} B \\ A \end{pmatrix}, \quad Q = \begin{pmatrix} D \\ C \end{pmatrix}$$

étant semblables l'une à l'autre, et représentées à l'aide de quatre arrangements A, B, C, D , qui vérifient la condition (5), on pose

$$\begin{pmatrix} C \\ A \end{pmatrix} = R.$$

Alors on tirera de la formule (5), non-seulement

$$\begin{pmatrix} D \\ B \end{pmatrix} = \begin{pmatrix} C \\ A \end{pmatrix} = R,$$

mais aussi

$$\begin{pmatrix} B \\ D \end{pmatrix} = \begin{pmatrix} A \\ C \end{pmatrix} = R^{-1}.$$

D'ailleurs on aura identiquement

$$Q = \begin{pmatrix} D \\ C \end{pmatrix} = \begin{pmatrix} D \\ B \end{pmatrix} \begin{pmatrix} B \\ A \end{pmatrix} \begin{pmatrix} A \\ C \end{pmatrix}.$$

Donc, en égard aux formules

$$\begin{pmatrix} D \\ B \end{pmatrix} = R, \quad \begin{pmatrix} B \\ A \end{pmatrix} = P, \quad \begin{pmatrix} A \\ C \end{pmatrix} = R^{-1},$$

on aura encore

$$(6) \quad Q = R P R^{-1}.$$

Si l'on posait

$$S = R^{-1} = \begin{pmatrix} A \\ C \end{pmatrix},$$

la formule (6) deviendrait

$$(7) \quad Q = S^{-1} Q S.$$

Nous pouvons donc conclure, de ce qui précède, que P étant une substitution quelconque, toute substitution semblable à P sera de la forme

$$R P R^{-1},$$

ou, ce qui revient au même, de la forme

$$S^{-1} P S.$$

En d'autres termes, toute substitution semblable à P sera le produit de trois facteurs dont les deux extrémes seront inverses l'un de l'autre, le facteur moyen étant précisément la substitution donnée P . Réciproquement, tout produit de trois facteurs dont les deux extrémes seront deux substitutions inverses l'une de l'autre, le facteur moyen étant la substitution P , sera une substitution semblable à P .

On peut remarquer encore que de la formule (6) on tire

$$QR = RP.$$

En conséquence, deux substitutions P , Q sont semblables l'une à l'autre, lorsqu'elles vérifient une équation de la forme

$$(8) \quad QR = RP.$$

Concevons maintenant que P , Q soient deux substitutions quelconques semblables ou dissemblables. Les produits

$$PQ, \quad QP$$

seront certainement des substitutions semblables entre elles. En effet, si l'on pose

$$(9) \quad R = PQ, \quad S = QP,$$

on en conclura, d'une part,

$$P = Q^{-1} S,$$

et, par suite,

$$R = Q^{-1} SQ;$$

d'autre part,

$$Q = P^{-1} R,$$

et, par suite,

$$S = P^{-1} RP.$$

On arriverait encore à la même conclusion, en observant que des formules (9) on déduit immédiatement l'équation

$$(10) \quad RP = PS,$$

analogue à la formule (8). On peut donc énoncer la proposition suivante :

Théorème. Les deux produits que l'on peut former avec deux substitutions données, en prenant l'une ou l'autre pour multiplicande, sont deux



nouvelles substitutions, non-seulement de même ordre, mais encore semblables entre elles.

Ainsi, par exemple, si l'on multiplie, 1° (x, y) par (y, z) ; 2° (y, z) par (x, y) , on obtiendra, dans le second cas comme dans le premier, une substitution du second ordre, et l'on trouvera

$$(y, z)(x, y) = (x, z, y), \quad (x, y)(y, z) = (x, y, z).$$

§ III. — *Sur les diverses formes que peut revêtir une même substitution, et sur le nombre des substitutions semblables à une substitution donnée.*

Soit P l'une des substitutions que l'on peut former avec n variables x, y, z, \dots , et posons

$$N = 1.2.3 \dots n.$$

Si l'on présente cette substitution sous la forme d'un rapport qui ait pour termes deux des arrangements composés avec les variables x, y, z, \dots , alors, comme nous l'avons remarqué dans le § I^{er}, on pourra prendre pour dénominateur de ce rapport un quelconque de ces arrangements, et par suite, en laissant toutes les variables en évidence, on pourra présenter la substitution P sous N formes diverses. Ainsi, par exemple, si l'on prend $n = 3$, on aura $N = 6$, et la substitution du second ordre par laquelle on échangera entre elles les deux variables x, y , pourra être présentée sous l'une quelconque des six formes

$$\begin{pmatrix} yxz \\ xyz \end{pmatrix}, \quad \begin{pmatrix} yzx \\ xzy \end{pmatrix}, \quad \begin{pmatrix} xzy \\ yzx \end{pmatrix}, \quad \begin{pmatrix} xyz \\ yxz \end{pmatrix}, \quad \begin{pmatrix} zyx \\ zxy \end{pmatrix}, \quad \begin{pmatrix} zxy \\ zyx \end{pmatrix}.$$

Le nombre des formes que peut revêtir une même substitution P se trouve notablement diminué lorsqu'on l'exprime à l'aide des facteurs circulaires dont elle est le produit, et que, pour représenter chaque facteur circulaire, on écrit entre deux parenthèses les variables qu'il renferme, en les séparant par des virgules, et plaçant à la suite l'une de l'autre deux variables dont la seconde doit être substituée à la première. Alors le nombre des variables comprises dans chaque facteur circulaire indique précisément l'ordre de ce facteur, et le plus petit nombre qui soit simultanément divisible par les ordres des divers facteurs représente l'ordre i de la substitution P . Alors aussi toute variable qui reste immobile quand on effectue la substitution P , doit être censée comprise dans un facteur circulaire du premier ordre, qui renferme cette seule variable, et, par suite, un tel facteur, représenté par



l'une des notations

$$(x), (y), (z), \dots,$$

est équivalent à l'unité. Les facteurs circulaires du premier ordre disparaîtront toujours, si la substitution donnée P est réduite à son expression la plus simple. Mais ils reparaîtront nécessairement si l'on veut mettre en évidence toutes les variables. Il importe de connaître le nombre des formes différentes que peut revêtir, dans cette hypothèse, la substitution P . On y parvient aisément de la manière suivante :

Supposons, pour fixer les idées, que la substitution P , étant de l'ordre i , renferme

f facteurs circulaires de l'ordre a ;

g facteurs circulaires de l'ordre b ;

etc..., et enfin

r facteurs circulaires du premier ordre, en sorte que r exprime le nombre des variables qui restent immobiles quand on effectue la substitution P .

On aura nécessairement

$$(1) \quad af + bg + \dots + r = n.$$

Supposons encore qu'après avoir exprimé la substitution P à l'aide de ses divers facteurs circulaires, représentés chacun par une série de lettres comprises entre deux parenthèses, et séparées par des virgules, on veuille déterminer le nombre ω des formes semblables que l'on peut donner à la substitution sans déplacer les parenthèses, et, par conséquent, sans altérer les nombres de lettres comprises dans les facteurs circulaires qui occupent des rangs déterminés. Tout ce que l'on pourra faire, pour modifier la forme de la substitution P , ce sera ou de faire passer successivement à la première place, dans chaque facteur circulaire, une quelconque des lettres comprises dans ce facteur, ou d'échanger entre eux les facteurs circulaires de même ordre. Par suite, pour obtenir le nombre ω des formes, semblables entre elles, que peut revêtir la substitution P , il suffira de multiplier le produit

$$a^f b^g \dots$$

des ordres de tous les facteurs circulaires par le nombre

$$(1 \cdot 2 \dots f)(1 \cdot 2 \dots g) \dots (1 \cdot 2 \dots r)$$

des arrangements divers que l'on peut former avec ces facteurs, lorsque, sans déplacer les parenthèses qui les renferment, on se borne à échanger entre eux

de toutes les manières possibles les facteurs circulaires de même ordre. On aura donc

$$(2) \quad \omega = (1.2 \dots f)(1.2 \dots g) \dots (1.2 \dots r) a^f b^g \dots$$

Ainsi, par exemple, si l'on prend $n=5$, $a=3$, $f=1$, $r=2$, la formule (2) donnera

$$\omega = (1.2) 3 = 6.$$

Effectivement, si l'on met en évidence les cinq variables x, y, z, u, v , dans la substitution

$$(x, y, z)$$

composée avec trois de ces variables, on pourra la présenter sous la forme

$$(x, y, z)(u)(v),$$

et, sans déplacer les parenthèses, on pourra donner à cette même substitution six formes semblables, savoir :

$$(x, y, z)(u)(v), \quad (y, z, x)(u)(v), \quad (z, x, y)(u)(v), \\ (x, y, z)(v)(u), \quad (y, z, x)(v)(u), \quad (z, x, y)(v)(u).$$

Il sera maintenant facile de calculer le nombre des substitutions semblables entre elles, et à une substitution donnée P , qui peuvent être composées avec n variables

En effet, nommons

$$P, P', P'', \dots$$

ces substitutions semblables à P . Supposons d'ailleurs que l'on représente chacune d'elles par le produit de ses divers facteurs circulaires, en mettant toutes les variables en évidence, et en assignant aux parenthèses des places déterminées. Enfin, concevons que l'on donne à chacune des substitutions P, P', P'', \dots toutes les formes qu'elle peut revêtir dans cette hypothèse. Si l'on nomme ϖ le nombre total des substitutions P, P', P'', \dots , et ω le nombre des formes sous lesquelles se présentera chacune d'elles, le produit $\omega\varpi$ exprimera non-seulement le nombre total des formes que revêtiront la substitution P et les substitutions semblables à P , mais encore le nombre N des arrangements divers que l'on peut former avec n variables. Car on devra évidemment retrouver tous ces arrangements, en supprimant les virgules et

les parenthèses dans les diverses formes obtenues. On aura donc

$$(3) \quad \omega\varpi = N,$$

la valeur de N étant

$$N = 1.2 \dots n;$$

et, par suite, on aura encore

$$(4) \quad \varpi = \frac{N}{\omega}.$$

Si la substitution P renferme f facteurs circulaires de l'ordre a , g facteurs circulaires de l'ordre b , ..., enfin r facteurs circulaires du premier ordre, on aura, en vertu de la formule (2),

$$\omega = (1.2 \dots f) (1.2 \dots g) \dots (1.2 \dots r) a^f b^g \dots,$$

et par conséquent la formule (3) donnera

$$(5) \quad \varpi = \frac{N}{(1.2 \dots f) (1.2 \dots g) \dots (1.2 \dots r) \dots a^f b^g \dots}.$$

Si maintenant on désigne par

$$\Sigma\varpi$$

la somme des valeurs de ϖ correspondantes aux divers systèmes de nombres qui peuvent représenter des valeurs de a, b, c, \dots , propres à vérifier l'équation (1), ou, en d'autres termes, si l'on désigne par $\Sigma\varpi$ la somme des valeurs de ϖ correspondantes aux diverses manières de partager le nombre n en parties égales ou inégales ; alors $\Sigma\varpi$ devra être précisément le nombre total des substitutions que l'on peut former avec n lettres. On aura donc

$$(6) \quad \Sigma\varpi = N,$$

et, par suite, en égard à la formule (5),

$$(7) \quad \Sigma \frac{1}{(1.2 \dots g) (1.2 \dots h) (1.2 \dots k) \dots a^g b^h c^k \dots} = 1.$$

Cette dernière équation paraît digne de remarque. Si, pour fixer les idées, on pose $n = 5$, on trouvera

$$n = 5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1,$$

et, par suite, l'équation (7) donnera

$$\frac{1}{5} + \frac{1}{4} + \frac{1}{2} \frac{1}{3} + \frac{1}{1.2} \frac{1}{3} + \frac{1}{1.2} \frac{1}{2^2} + \frac{1}{1.2.3} \frac{1}{2} + \frac{1}{1.2.3.4.5} = 1,$$

ce qui est exact.

§ IV. — *Résolution de l'équation linéaire et symbolique par laquelle se trouvent liées l'une à l'autre deux substitutions semblables entre elles.*

Soient P , Q deux substitutions semblables entre elles, formées avec n variables

$$x, y, z, \dots,$$

ou du moins avec plusieurs de ces variables; et supposons

$$(1) \quad P = (\alpha, \beta, \gamma, \dots, \eta)(\lambda, \mu, \nu, \dots, \rho) \dots (\varphi)(\chi)(\psi) \dots,$$

$$(2) \quad Q = (\alpha', \beta', \gamma', \dots, \eta')(\lambda', \mu', \nu', \dots, \rho') \dots (\varphi')(\chi')(\psi') \dots,$$

$\alpha', \beta', \gamma', \dots, \eta'$; $\lambda', \mu', \nu', \dots, \rho'$; $\varphi', \chi', \psi', \dots$ désignant les variables qui, dans la substitution Q , ont pris les places qu'occupaient les variables $\alpha, \beta, \gamma, \dots, \eta$; $\lambda, \mu, \nu, \dots, \rho$; $\varphi, \chi, \psi, \dots$ dans la substitution P . Représentons par

A et C

les arrangements auxquels se réduisent les seconds membres des formules (1) et (2), quand on y supprime les parenthèses et les virgules placées entre les variables, en sorte qu'on ait

$$(3) \quad A = \alpha \beta \gamma \dots \eta \lambda \mu \nu \dots \rho \dots \varphi \chi \psi \dots,$$

$$(4) \quad C = \alpha' \beta' \gamma' \dots \eta' \lambda' \mu' \nu' \dots \rho' \dots \varphi' \chi' \psi' \dots$$

Enfin, soient

$$(5) \quad B = PA \quad \text{et} \quad D = QC$$

les nouveaux arrangements qu'on obtiendra en appliquant à l'arrangement A la substitution P , et à l'arrangement C la substitution Q . On trouvera

$$(6) \quad B = \beta \gamma \dots \eta \alpha \mu \nu \dots \rho \lambda \dots \varphi \chi \psi \dots,$$

$$(7) \quad D = \beta' \gamma' \dots \eta' \alpha' \mu' \nu' \dots \rho' \lambda' \dots \varphi' \chi' \psi' \dots$$

Par conséquent, les variables qui, prises deux à deux, se correspondaient mutuellement dans les arrangements A , C , se correspondront encore dans les arrangements B , D ; et cela devait être ainsi, puisque les substitutions semblables P , Q , présentées sous les formes semblables (1) et (2), ont eu précisément pour effet de déplacer de la même manière les variables semblables

ment placées dans les arrangements A et C. On aura donc

$$(8) \quad \begin{pmatrix} D \\ B \end{pmatrix} = \begin{pmatrix} C \\ A \end{pmatrix}.$$

Cela posé, faisons, pour abréger,

$$\begin{pmatrix} D \\ B \end{pmatrix} = \begin{pmatrix} C \\ A \end{pmatrix} = R.$$

On aura, par suite,

$$(9) \quad D = RB, \quad C = RA;$$

et des équations (9), jointes aux formules (5), on tirera

$$D = RPA, \quad C = QRA,$$

par conséquent

$$(10) \quad QRA = RPA,$$

et

$$(11) \quad QR = RP.$$

Réiproquement, si les substitutions P, Q sont liées entre elles par une équation semblable à la formule (11), alors, en appliquant à un arrangement quelconque A la substitution

$$QR = RP,$$

on retrouvera l'équation (10), et, en posant, pour abréger,

$$P = \begin{pmatrix} B \\ A \end{pmatrix}, \quad R = \begin{pmatrix} C \\ A \end{pmatrix}, \quad Q = \begin{pmatrix} D \\ C \end{pmatrix},$$

ou, ce qui revient au même,

$$B = PA, \quad C = RA, \quad D = QC,$$

on tirera de l'équation (10)

$$D = RB, \quad R = \begin{pmatrix} D \\ B \end{pmatrix}.$$

On aura donc alors

$$(12) \quad R = \begin{pmatrix} C \\ A \end{pmatrix} = \begin{pmatrix} D \\ B \end{pmatrix};$$

et, par suite, les substitutions

$$P = \begin{pmatrix} B \\ A \end{pmatrix}, \quad Q = \begin{pmatrix} D \\ C \end{pmatrix}$$

seront semblables l'une à l'autre, puisque, en vertu de la formule (12), elles devront déplacer de la même manière les variables qui se correspondent dans les deux termes de la substitution

Soient P, Q deux substitutions semblables à variables (C) . (A) .

Il importe d'observer que les deux membres de la formule (11) sont les produits qu'on obtient en multipliant les deux substitutions semblables P et Q par une nouvelle substitution R dont la première puissance entre, dans l'un des produits, comme multiplicande, et dans l'autre produit, comme multiplicateur. Pour obtenir cette nouvelle substitution R , il suffit d'exprimer la substitution P à l'aide de ses facteurs circulaires, en mettant toutes les variables en évidence, et d'écrire au-dessus de P la substitution Q , présentée sous une forme semblable à celle de P , puis de transformer les deux substitutions Q, P en deux arrangements C, A par la suppression des parenthèses et des virgules placées entre les variables. Ces deux arrangements C, A seront les deux termes d'une substitution R qui vérifiera la formule (11). Il y a plus : d'après ce qui a été dit ci-dessus, toute valeur de R propre à vérifier cette formule sera évidemment fournie par la comparaison des deux substitutions semblables P, Q , superposées l'une à l'autre, ainsi qu'on vient de l'expliquer. D'ailleurs, en laissant P sous la même forme, on pourra donner successivement à Q diverses formes semblables à celle de P , et semblables entre elles, dont le nombre ω sera déterminé par l'équation (2) du paragraphe précédent; et, par suite, il est clair que la substitution R admettra un nombre ω de valeurs distinctes. Donc, si l'on résout par rapport à R la formule (11), c'est-à-dire l'équation symbolique et linéaire à laquelle doit satisfaire la substitution R , on obtiendra un nombre ω de solutions diverses correspondantes aux diverses formes de la substitution Q .

Si, en supposant connues, non plus les substitutions semblables P, Q , mais l'une d'elles, P par exemple, et la substitution R , on demandait la valeur de Q déterminée par la formule (11), ou, ce qui revient au même, par la suivante

$$(13) \quad Q = RPR^{-1},$$

on remarquerait que, pour passer de la valeur de P , donnée par la formule (1), à la valeur de Q , donnée par la formule (2), il suffit de faire subir aux variables x, y, z, \dots les déplacements par lesquels on passe de la valeur de A , donnée par la formule (3), à la valeur de C , donnée par la for-

mule (4), c'est-à-dire les déplacements qui sont indiqués par la substitution R. En opérant ainsi, on obtiendrait la seule valeur de Q qui vérifie la formule (13).

Nous savons donc maintenant résoudre les deux problèmes suivants :

1^{er} *Problème.* Étant données n variables x, y, z, \dots , et deux substitutions semblables P, Q, formées avec ces variables, trouver une troisième substitution R qui soit propre à résoudre l'équation linéaire

$$RP = QR.$$

Solution. Exprimez la substitution P à l'aide de ses facteurs circulaires, en mettant toutes les variables en évidence, puis écrivez au-dessus de la substitution P la substitution Q, présentée sous une forme semblable à celle de P. Supprimez ensuite les parenthèses et les virgules placées entre les variables. Les deux substitutions Q, P seront ainsi transformées en deux arrangements qui seront propres à représenter les deux termes de la substitution R.

Corollaire. Les substitutions P, Q peuvent ne renfermer qu'une partie des variables x, y, z, \dots ; mais, pour obtenir toutes les solutions de l'équation

$$RP = QR,$$

on devra, comme nous l'avons dit, mettre toutes les variables en évidence, même celles qui ne seraient renfermées dans aucune des deux substitutions P, Q, si ces substitutions étaient réduites à leur plus simple expression. Il en résulte que, les substitutions P, Q restant les mêmes, le nombre des solutions de l'équation symbolique linéaire

$$RP = QR$$

croîtra en même temps que le nombre des variables x, y, z, \dots

Pour éclaircir ce qu'on vient de dire, supposons que les substitutions P, Q, réduites à leur plus simple expression, soient deux substitutions circulaires du second ordre, et que l'on ait

$$P = (x, y), \quad Q = (x, z).$$

Si les variables x, y, z, \dots se réduisent à trois, alors, P étant présenté sous la forme

$$(x, y) (z),$$

Q pourra être présenté sous l'une des formes semblables

$$(x, z) (y), \quad (z, x) (y),$$

et, par suite, la valeur de R devra se réduire à l'une des substitutions

$$\begin{pmatrix} xzy \\ xyz \end{pmatrix}, \quad \begin{pmatrix} zxy \\ xyz \end{pmatrix},$$

ou, ce qui revient au même, à l'une des substitutions

$$(y, z), \quad (x, z, y).$$

Si, au contraire, l'on considère quatre variables x, y, z, u , alors, P étant présenté sous la forme

$$(x, y) (z) (u),$$

Q pourra être présenté sous l'une quelconque des formes semblables

$$(x, z) (y) (u), \quad (z, x) (y) (u), \quad (x, z) (u) (y), \quad (z, x) (u) (y),$$

et, par suite, R pourra être l'une quelconque des quatre substitutions

$$\begin{pmatrix} xzyu \\ xyzu \end{pmatrix}, \quad \begin{pmatrix} zxyu \\ xyzu \end{pmatrix}, \quad \begin{pmatrix} xzuy \\ xyzu \end{pmatrix}, \quad \begin{pmatrix} zxuy \\ xyzu \end{pmatrix},$$

ou, ce qui revient au même, l'une quelconque des quatre substitutions

$$(y, z), \quad (x, z, y), \quad (y, z, u), \quad (x, z, u, y).$$

2^e Problème. Étant données n variables x, y, z, \dots , et deux substitutions semblables P, Q , formées avec ces variables, trouver la substitution Q semblable à P , et déterminée par la formule

$$Q = RPR^{-1}.$$

Solution. Exprimez la substitution P à l'aide de ses facteurs circulaires, puis effectuez dans P les déplacements de variables indiqués par la substitution R , en opérant comme si P représentait un simple arrangement.

Corollaire. Pour résoudre ce second problème, il n'est pas nécessaire de mettre toutes les variables en évidence, comme on doit le faire généralement quand il s'agit d'obtenir toutes les solutions du premier; et l'on peut se servir de substitutions réduites à leurs plus simples expressions. Si, pour fixer les idées, on prend

$$P = (x, y), \quad R = (x, z, y),$$

alors, en appliquant la règle ci-dessus établie, on trouvera, quel que soit

d'ailleurs le nombre des variables données,

$$RPR^{-1} = (z, x), \quad PRP^{-1} = (\gamma, z, x).$$

Si l'on supposait, au contraire,

$$P = (x, \gamma), \quad R = (x, z)(\gamma, u),$$

on trouverait

$$RPR^{-1} = (z, u), \quad PRP^{-1} = (\gamma, z)(x, u).$$

§ V. — *Sur les facteurs primitifs d'une substitution donnée.*

Nommons P l'une des substitutions que l'on peut former avec n variables

$$x, \gamma, z, \dots,$$

et concevons que l'ordre i de cette substitution ait été décomposé en facteurs

$$a, b, c, \dots$$

premiers entre eux; enfin, soit l un nombre entier quelconque. En vertu d'un théorème précédemment établi (page 145), on pourra toujours satisfaire à l'équivalence

$$(1) \quad i \left(\frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \dots \right) \equiv l, \quad (\text{mod. } i),$$

par des valeurs entières de $\alpha, \beta, \gamma, \dots$ D'ailleurs, i étant l'ordre de la substitution P , une équivalence de la forme

$$l \equiv l' + l'' + \dots, \quad (\text{mod. } i),$$

entraînera toujours l'équation

$$P^l = P^{l'+l''+\dots} = P^{l'} P^{l''} \dots$$

Donc la formule (1) entraînera la suivante

$$P^l = P^{\frac{i}{a}\alpha} P^{\frac{i}{b}\beta} P^{\frac{i}{c}\gamma} \dots;$$

et comme, en posant, pour abréger,

$$(2) \quad P^{\frac{i}{a}} = U, \quad P^{\frac{i}{b}} = V, \quad P^{\frac{i}{c}} = W, \dots,$$

on aura encore

$$P^{\frac{i}{a}\alpha} = U^\alpha, \quad P^{\frac{i}{b}\beta} = V^\beta, \quad P^{\frac{i}{c}\gamma} = W^\gamma, \dots$$

on tirera définitivement de la formule (1), jointe aux équations (2),

$$(3) \quad P^l = U^\alpha V^\beta W^\gamma \dots$$

Dans le cas particulier où l se réduit à l'unité, les exposants $\alpha, \beta, \gamma, \dots$ sont uniquement assujettis à vérifier l'équivalence

$$(4) \quad i \left(\frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \dots \right) \equiv 1, \quad (\text{mod. } i),$$

et la formule (3) donne

$$(5) \quad P = U^\alpha V^\beta W^\gamma \dots$$

Il est bon d'observer que, l'ordre i de la substitution P étant la plus petite valeur entière et positive de l propre à vérifier l'équation

$$P^l = 1,$$

l'ordre de la substitution

$$U = P^{\frac{i}{a}},$$

ou la plus petite valeur entière et positive de k propre à vérifier la formule

$$P^{\frac{ik}{a}} = 1,$$

sera nécessairement

$$k = \alpha.$$

Pareillement, les ordres des substitutions

$$V = P^{\frac{i}{b}}, \quad W = P^{\frac{i}{c}}, \dots$$

se trouveront représentés par les facteurs b, c, \dots du nombre i .

Concevons à présent que, p, q, r, \dots étant les facteurs premiers de i , on ait

$$(6) \quad i = p^f q^g r^h \dots$$

On pourra prendre

$$(7) \quad \alpha = p^f, \quad \beta = q^g, \quad \gamma = r^h, \dots$$

et, par suite, les nombres

p^f, q^g, r^h, \dots

exprimeront les ordres respectifs des substitutions

U, V, W, \dots

D'ailleurs, d'après ce qui a été dit à la page 161, l'ordre d'une substitution quelconque P est divisible par l'ordre de chacun des facteurs circulaires de P . Donc l'ordre p^f de la substitution U devra être divisible par l'ordre de chacun des facteurs circulaires de U . Donc, puisque les diviseurs de p^f ne pourront être que des puissances du nombre premier p , la substitution U jouira de cette propriété remarquable, que les ordres de ses divers facteurs circulaires seront tous des puissances d'un même nombre premier p . Pareillement, les ordres des divers facteurs de la substitution V , ou W , etc., seront tous des puissances du nombre premier q , ou r , ...

D'autre part, puisque U^α représente le produit de α facteurs égaux à U , que V^β représente le produit de β facteurs égaux à V, \dots , il résulte de la formule (5) que la substitution P peut être décomposée en facteurs dont chacun se confond avec l'une des puissances de P désignées par les lettres U, V, W, \dots Cela posé, les substitutions

U, V, W, \dots

joueront, par rapport à la substitution P de l'ordre i , un rôle analogue à celui que les facteurs

p^f, q^g, r^h, \dots

dont chacun est une puissance d'un nombre premier, jouent eux-mêmes par rapport au nombre entier i . On peut remarquer aussi que les substitutions U, V, W, \dots représentent des puissances de P desquelles on peut déduire toutes les autres à l'aide des formules (3) et (5). Elles offrent donc encore, pour cette raison, une certaine analogie avec certaines racines des équations binômes, savoir, avec celles qui sont désignées sous le nom de primitives, et qui, élevées à des puissances diverses, reproduisent toutes les autres racines. Pour conserver le souvenir de ces diverses analogies, nous dirons que les substitutions

U, V, W, \dots

déterminées par les formules (2), sont les *facteurs primitifs* de la substitution P .

De plus, nous appellerons *substitution primitive* celle qui n'aura d'autres facteurs primitifs qu'elle-même, ou, en d'autres termes, celle dont l'ordre sera une puissance d'un nombre premier.

Cela posé, la substitution

$$(x, y, z, u) (v, w),$$

formée avec six variables, sera une substitution primitive du quatrième ordre, représentée par le produit de deux facteurs circulaires dont les ordres 2 et 4 se réduiront à la première et à la seconde puissance du nombre premier 2.

Au contraire, la substitution circulaire

$$P = (x, y, z, u, v, w),$$

dont l'ordre est exprimé par le nombre

$$6 = 2 \cdot 3,$$

sera décomposable en facteurs primitifs, représentés chacun par l'une des substitutions régulières

$$U = P^2 = (x, z, v) (y, u, w), \quad V = P^3 = (x, u) (y, v) (z, w).$$

Effectivement, en adoptant les valeurs précédentes de U et V , on trouvera

$$U^2 V = P^7 = P;$$

et, par conséquent,

$$P = U^2 V.$$

Enfin, si l'on pose

$$P = (x, y, z) (u, v),$$

P sera une substitution du sixième ordre, que l'on pourra décomposer en facteurs primitifs représentés chacun par l'une des deux substitutions circulaires

$$U = P^2 = (x, z, y), \quad V = P^3 = (u, v),$$

et que l'on déduira encore de ces facteurs à l'aide de la formule

$$P = U^2 V.$$

§ VI. — *Sur les dérivées d'une ou de plusieurs substitutions, et sur les systèmes de substitutions conjuguées.*

Étant données une ou plusieurs substitutions qui renferment les n lettres x, y, z, \dots , ou du moins plusieurs d'entre elles, je nommerai substitutions *dérivées* toutes celles que l'on pourra déduire des substitutions données, multipliées une ou plusieurs fois les unes par les autres, ou par elles-mêmes, dans un ordre quelconque; et les substitutions données, jointes aux substitutions dérivées, formeront ce que j'appellerai un *système de substitutions conjuguées*. L'ordre de ce système sera le nombre total des substitutions qu'il présente, y compris la substitution qui offre deux termes égaux et se réduit à l'unité.

Lorsque les substitutions données se réduisent à une seule P , les substitutions dérivées se confondent avec les puissances de P et forment un système de substitutions conjuguées qui est d'un ordre représenté par l'ordre de la substitution P .

Le système de toutes les substitutions que l'on peut former avec n lettres x, y, z, \dots est évidemment un système de substitutions conjuguées. Si l'on nomme

A, B, C, \dots

les divers arrangements qui peuvent être formés avec les n variables x, y, z, \dots , les substitutions comprises dans le système dont il s'agit seront

$$(1) \quad \binom{A}{A}, \quad \binom{B}{A}, \quad \binom{C}{A}, \dots,$$

et le nombre N de ces substitutions, ou l'ordre du système, sera déterminé par la formule

$$N = 1 \cdot 2 \cdot 3 \dots n.$$

Soit maintenant

$$(2) \quad 1, P, Q, R, \dots$$

un système quelconque de substitutions conjuguées. D'après la définition même d'un tel système, on devra toujours reproduire les mêmes substitutions, rangées seulement d'une autre manière, si on les multiplie séparément par l'une quelconque d'entre elles, ou bien encore si l'une quelconque d'entre elles est séparément multipliée par elle-même et par toutes les autres. Donc, si l'on nomme S l'une quelconque des substitutions (2), les divers termes de

la série

$$(3) \quad S, SP, SQ, SR, \dots,$$

ou bien encore de la série

$$(4) \quad S, PS, QS, RS, \dots,$$

se confondront avec les termes de la série (2) rangés dans un nouvel ordre.

Ajoutons qu'il est facile d'établir les propositions suivantes :

1^{er} *Théorème.* L'ordre d'un système de substitutions conjuguées relatives à n variables est toujours un diviseur du nombre N des arrangements que l'on peut former avec ces variables.

Démonstration. Supposons que le système donné soit celui que présente la série (2), et nommons M l'ordre de ce système. Si la série (2) se confond avec la série (1), on aura précisément $M = N$; dans le cas contraire, désignons par U, V, W, \dots des substitutions qui fassent partie de la série (1) sans appartenir à la série (2). Si l'on nomme m le nombre des termes de la série

$$(5) \quad 1, U, V, W, \dots,$$

le tableau

$$(6) \quad \left\{ \begin{array}{l} 1, P, Q, R, \dots, \\ U, UP, UQ, UR, \dots, \\ V, VP, VQ, VR, \dots, \\ W, WP, WQ, WR, \dots, \\ \text{etc.} \end{array} \right.$$

offrira m suites horizontales composées chacune de M termes, et tous les termes de chaque suite seront distincts les uns des autres. Si, d'ailleurs, deux suites horizontales différentes, par exemple la deuxième et la troisième, offraient des termes égaux, en sorte qu'on eût

$$VQ = UP,$$

on en conclurait

$$V = UPQ^{-1},$$

ou simplement

$$V = US,$$

$S = PQ^{-1}$ étant un terme de la série (2). Donc alors, dans le tableau (6), le premier terme V de la troisième suite horizontale serait déjà un des termes de la seconde. Donc tous les termes du tableau (6) seront distincts les uns

des autres, si le premier terme de chaque suite horizontale est pris en dehors des suites précédentes. Or concevons qu'en remplissant toujours cette condition, on ajoute sans cesse au tableau (6) de nouvelles suites, en faisant croître ainsi le nombre m . On ne pourra être arrêté dans cette opération qu'à l'instant où le tableau (6) renfermera les N termes compris dans la suite (1); mais alors on aura évidemment

$$(7) \quad N = mM.$$

Donc M sera un diviseur de N .

Corollaire. Il est bon d'observer qu'au tableau (6) on pourrait substituer un autre tableau de la forme

$$(8) \quad \left\{ \begin{array}{l} I, P, Q, R, \dots, \\ U, PU, QU, RU, \dots, \\ V, PV, QV, RV, \dots, \\ W, PW, QW, RW, \dots, \\ \text{etc.} \end{array} \right.$$

2^e *Théorème.* L'ordre d'un système de substitutions conjuguées est divisible par l'ordre de chacune de ces substitutions.

Démonstration. Supposons toujours que le système donné soit celui que présente la série (2). Si l'on nomme a l'ordre de la substitution P , la suite (5) devra renfermer en premier lieu les substitutions

$$(9) \quad I, P, P^2, \dots, P^{a-1}.$$

Soit d'ailleurs Q l'une des substitutions qui appartiennent à la série (2), sans faire partie de la suite (9). La suite (2) renfermera les substitutions

$$(10) \quad Q, PQ, P^2Q, \dots, P^{a-1}Q,$$

et aucune de celles-ci ne pourra se confondre avec l'une des substitutions

$$I, P, P^2, \dots, P^{a-1};$$

car si l'on avait, par exemple,

$$P^k Q = P^h,$$

on en conclurait

$$Q = P^{h-k}.$$

Soit encore R une substitution qui fasse partie de la suite (2), sans être renfermée, ni dans la suite (9), ni dans la suite (10). La suite (2) renfermera nécessairement les substitutions $R, PR, P^2R, \dots, P^{a-1}R$; et aucune de ces dernières ne sera comprise, ni dans la suite (9), ni même dans la suite (10); car, si l'on avait, par exemple,

$$P^kR = P^hQ,$$

on en conclurait

$$R = P^{h-k}Q.$$

En continuant ainsi, on partagera facilement la suite des substitutions conjuguées

en plusieurs suites,

$$(11) \quad \left\{ \begin{array}{l} I, P, P^2, \dots, P^{a-1}, \\ Q, PQ, P^2Q, \dots, P^{a-1}Q, \\ R, PR, P^2R, \dots, P^{a-1}R, \\ \text{etc.} \end{array} \right.$$

dont chacune renfermera a substitutions diverses. Donc, si l'on nomme M le nombre des substitutions conjuguées

$$I, P, Q, R, \dots,$$

ou, ce qui revient au même, l'ordre de leur système, M sera un multiple de a .

Corollaire. Il importe d'observer qu'en opérant toujours de la même manière, on pourrait intervertir l'ordre des facteurs, et substituer ainsi au tableau (11) un tableau de la forme

$$(12) \quad \left\{ \begin{array}{l} I, P, P^2, \dots, P^{a-1}, \\ Q, QP, QP^2, \dots, QP^{a-1}, \\ R, RP, RP^2, \dots, RP^{a-1}, \\ \text{etc.} \end{array} \right.$$

3^e *Théorème.* Soient

$$P, Q$$

deux substitutions, la première de l'ordre a , la seconde de l'ordre b ; et

supposons ces deux substitutions permutable entre elles, en sorte qu'on ait

$$(13) \quad QP = PQ.$$

Si d'ailleurs, h, k étant deux entiers quelconques, l'équation

$$(14) \quad P^h Q^k = 1$$

ne se vérifie jamais, excepté dans le cas où l'on a

$$(15) \quad P^h = 1, \quad Q^k = 1,$$

les deux substitutions P, Q et leurs dérivées composeront un système de substitutions conjuguées dont l'ordre sera précisément le produit ab .

Démonstration. En effet, soit S une dérivée quelconque des deux substitutions P, Q . Cette dérivée sera le produit de facteurs égaux, les uns à P , les autres à Q ; mais, en vertu de la formule (13), l'ordre dans lequel ces facteurs seront écrits pourra être interverti arbitrairement. Donc on pourra faire en sorte que chacun des facteurs égaux à P précède chacun des facteurs égaux à Q , et réduire S à la forme

$$(16) \quad S = P^h Q^k.$$

Cela posé, comme les valeurs distinctes de P^h répondront aux valeurs

$$0, 1, 2, \dots, a-1$$

de l'exposant h , et les valeurs distinctes de Q^k aux valeurs

$$0, 1, 2, \dots, b-1$$

de l'exposant k , il est clair que les valeurs distinctes de S seront toutes comprises dans le tableau

$$(17) \quad \left\{ \begin{array}{llll} 1, & P, & P^2, \dots, & P^{a-1}, \\ Q, & PQ, & P^2Q, \dots, & P^{a-1}Q, \\ Q^2, & PQ^2, & P^2Q^2, \dots, & P^{a-1}Q^2, \\ \dots & \dots & \dots & \dots \\ Q^{b-1}, & PQ^{b-1}, & P^2Q^{b-1}, \dots, & P^{a-1}Q^{b-1}. \end{array} \right.$$

Elles seront donc représentées par les divers termes de ce tableau, si ces termes sont tous inégaux entre eux. Or, c'est ce qui arrivera certainement dans l'hypothèse admise; car, si l'on suppose

$$(18) \quad P^h Q^k = P^h Q^l,$$

h, h' désignant deux nombres dont chacun soit inférieur à l'ordre a de la substitution P , et k, k' deux nombres dont chacun soit inférieur à l'ordre b de la substitution Q , l'équation (18) donnera

$$(19) \quad P^{h-h'} Q^{k-k'} = 1;$$

et puisque, dans l'hypothèse admise, la formule (14) entraîne toujours les formules (15), l'équation (19) entraînera les suivantes :

$$P^{h-h'} = 1, \quad Q^{k-k'} = 1,$$

desquelles on tirera

$$(20) \quad P^h = P^h, \quad Q^k = Q^k.$$

Donc, si les conditions (20) ne sont pas remplies, l'équation (18) ne pourra subsister, et l'on peut affirmer que deux termes distincts du tableau (17) auront des valeurs distinctes. D'ailleurs les termes de ce tableau, qui renferme a lignes verticales et b lignes horizontales, sont en nombre égal au produit ab . Donc, dans l'hypothèse admise, ce produit représentera précisément le nombre des valeurs distinctes de P , ou, ce qui revient au même, l'ordre du système des substitutions dérivées de P et de Q .

Observons au reste que, dans l'hypothèse admise, on aura identiquement

$$P^h Q^k = Q^k P^h,$$

et qu'en conséquence les substitutions (17) se confondront respectivement avec celles que renferme le tableau

$$(21) \quad \left\{ \begin{array}{llll} 1, & P, & P^2, \dots, & P^{a-1}, \\ Q, & QP, & QP^2, \dots, & QP^{a-1}, \\ Q^2, & Q^2P, & Q^2P^2, \dots, & Q^2P^{a-1}, \\ \dots & \dots & \dots & \dots \\ Q^{b-1}, & Q^{b-1}P, & Q^{b-1}P^2, \dots, & Q^{b-1}P^{a-1}. \end{array} \right.$$

Des raisonnements entièrement semblables à ceux dont nous venons de faire usage suffirraient encore pour établir les propositions suivantes :

4^e *Théorème.* Soient

$$P, Q, R, \dots$$

diverses substitutions permutables entre elles, en sorte qu'on ait

$$(22) \quad QP = PQ, \quad RP = PR, \dots, \quad RQ = QR, \dots;$$

et nommons

- a* l'ordre de la substitution P ,
- b* l'ordre de la substitution Q ,
- c* l'ordre de la substitution R ,
- etc.

Si, d'ailleurs, h, k, l, \dots étant des entiers quelconques, l'équation

$$(23) \quad P^h Q^k R^l \dots = 1$$

ne se vérifie jamais, excepté dans le cas où l'on a

$$(24) \quad P^h = 1, \quad Q^k = 1, \quad R^l = 1, \dots;$$

les substitutions P, Q, R, \dots et leurs dérivées composeront un système de substitutions conjuguées dont l'ordre sera précisément le produit $abc\dots$ des ordres des substitutions données P, Q, R, \dots

Corollaire. Il est clair que l'équation (23) entraînera toujours les équations (24), si les substitutions

réduites à leurs plus simples expressions, sont formées avec des variables diverses, en sorte que jamais deux de ces substitutions ne renferment la même variable. En effet, concevons que les substitutions

$$P, Q, R, \dots$$

soient formées, la première avec les seules variables $\alpha, \epsilon, \gamma, \dots$; la seconde avec les seules variables λ, μ, ν, \dots ; la troisième avec les seules variables $\varphi, \chi, \psi, \dots$. Ces divers systèmes de variables seront encore ceux qui serviront respectivement à former les substitutions

$$P^h, Q^k, R^l, \dots,$$

h, k, l, \dots étant des nombres entiers quelconques. Cela posé, pour appliquer à un facteur quelconque une substitution de la forme

$$S = P^h Q^k R^l \dots,$$

il suffira de faire subir aux variables $\alpha, \epsilon, \gamma, \dots$ les déplacements indiqués par la substitution P^h , aux variables λ, μ, ν, \dots les déplacements indiqués par la substitution Q^k , aux variables $\varphi, \chi, \psi, \dots$ les déplacements indiqués par la substitution R^l, \dots . Donc, pour que l'équation (23) subsiste, ou, ce

qui revient au même, pour qu'aucune des variables données ne soit déplacée par la substitution S , il sera nécessaire et il suffira que les variables $\alpha, \beta, \gamma, \dots$ ne se trouvent point déplacées par la substitution P^h , ni les variables λ, μ, ν, \dots par la substitution Q^k , ni les variables $\varphi, \chi, \psi, \dots$ par la substitution R^l, \dots , et que l'on ait en conséquence

$$P^h = 1, \quad Q^k = 1, \quad R^l = 1, \dots$$

On peut donc énoncer encore la proposition suivante :

5^e *Théorème.* Soient

$$(25) \quad P, Q, R, \dots$$

diverses substitutions formées avec des variables diverses. Non-seulement ces substitutions seront permutable entre elles, mais, de plus, étant jointes à leurs dérivées, elles fourniront un système de substitutions conjuguées, qui sera d'un ordre représenté par le produit des ordres des substitutions P, Q, R, \dots

Corollaire. Si la série (25) renferme une seule substitution de l'ordre a , une seule de l'ordre b , une seule de l'ordre c, \dots ; l'ordre du système des substitutions P, Q, R, \dots et de leurs dérivées sera le produit $abc\dots$. Si, au contraire, la série (25) renferme h substitutions de l'ordre a , k substitutions de l'ordre b , l substitutions de l'ordre c, \dots , ces diverses substitutions, jointes à leurs dérivées, composeront un système dont l'ordre sera représenté par le produit

$$a^h b^k c^l \dots$$

§ VII. — Sur les systèmes de substitutions primitives et conjuguées.

Soient P une substitution régulière qui renferme n variables x, y, z, \dots ,
 a l'ordre de cette substitution,
 b le nombre de ses facteurs circulaires;

les trois nombres a, b, n seront liés entre eux par la formule

$$n = ab.$$

Cela posé, concevons que l'on range sur a lignes horizontales distinctes, et sur b lignes verticales, les n variables comprises dans P , en plaçant à la suite l'une de l'autre, dans une même ligne horizontale, les variables qui se suivent immédiatement dans un même facteur circulaire de P . On obtiendra encore une substitution régulière Q de l'ordre n , en prenant pour facteurs

de Q , a substitutions circulaires de l'ordre b , dans chacune desquelles seraient placées, à la suite l'une de l'autre, les variables que renferme une même ligne verticale. De plus, il est clair que les deux substitutions

$$P, Q,$$

dont l'une aura pour effet unique d'échanger entre elles les lignes verticales, tandis que l'autre aura pour effet unique d'échanger entre elles les lignes horizontales, seront deux substitutions permutables entre elles, par conséquent deux substitutions dont les dérivées seront toutes comprises dans chacun des tableaux

$$(1) \quad \left\{ \begin{array}{llll} 1, & P, & P^2, \dots, & P^{a-1}, \\ Q, & QP, & QP^2, \dots, & QP^{a-1}, \\ Q^2, & Q^2P, & Q^2P^2, \dots, & Q^2P^{a-1}, \\ \dots & \dots & \dots & \dots \\ Q^{b-1}, & Q^{b-1}P, & Q^{b-1}P^2, \dots, & Q^{b-1}P^{a-1}; \end{array} \right.$$

$$(2) \quad \left\{ \begin{array}{llll} 1, & P, & P^2, \dots, & P^{a-1}, \\ Q, & PQ, & P^2Q, \dots, & P^{a-1}Q, \\ Q^2, & PQ^2, & P^2Q^2, \dots, & P^{a-2}Q^2, \\ \dots & \dots & \dots & \dots \\ Q^{b-1}, & PQ^{b-1}, & P^2Q^{b-1}, \dots, & P^{a-1}Q^{b-1}; \end{array} \right.$$

et formeront un système de substitutions conjuguées de l'ordre $n = ab$.

Si, pour fixer les idées, on pose

$$n = 4 = 2 \times 2,$$

alors, avec les quatre variables

$$x, y,$$

$$z, u,$$

rangées sur deux lignes horizontales et sur deux lignes verticales, on pourra composer les deux substitutions régulières

$$P = (x, y) (z, u) \quad \text{et} \quad Q = (x, z) (y, u),$$

qui seront permutables entre elles; et ces deux substitutions formeront, avec leurs dérivées

$$1 \quad \text{et} \quad PQ = QP,$$

un système de substitutions conjuguées

I, P,

Q, PQ

qui sera du quatrième ordre. Pareillement, si l'on pose

$$n = 6 = 3 \times 2,$$

alors, avec les six variables

$x, y, z,$

$u, v, w,$

rangées sur deux lignes horizontales et sur trois lignes verticales, on pourra composer les deux substitutions régulières

$$P = (x, y, z) (u, v, w), \quad Q = (x, u) (y, v) (z, w),$$

qui seront permutable entre elles; et ces deux substitutions formeront, avec leurs dérivées, un système de substitutions conjuguées qui sera du sixième ordre. Au reste, ce dernier système ne sera autre chose que le système des puissances de la substitution circulaire

$$(x, w, y, u, z, v),$$

dont P et Q représentent les facteurs primitifs.

Au lieu de ranger les n variables données sur a lignes horizontales et sur b lignes verticales, on pourrait représenter ces variables par une seule lettre s affectée de deux indices, et représenter même les deux systèmes d'indices par deux nouveaux systèmes de lettres

$$\alpha, \beta, \gamma, \dots, \lambda, \mu, \nu, \dots$$

Ainsi, par exemple, on pourrait représenter les six variables

$x, y, z,$

$u, v, w,$

par

$s_{\alpha, \lambda}, s_{\beta, \lambda}, s_{\gamma, \lambda},$

$s_{\alpha, \mu}, s_{\beta, \mu}, s_{\gamma, \mu};$

et alors les substitutions

$$P = (x, y, z) (u, v, w), \quad Q = (x, u) (y, v) (z, w)$$

s'offriraient sous les formes

$$P = (\alpha, \epsilon, \gamma), \quad Q = (\lambda, \mu),$$

qui rendraient sensible la propriété qu'ont ces deux substitutions d'être permutables entre elles.

Concevons maintenant que le nombre entier

$$n = abc\dots$$

soit décomposable en plusieurs facteurs a, b, c, \dots , égaux ou inégaux. Alors on pourra représenter n variables diverses

$$x, \gamma, z, \dots$$

par une seule lettre s affectée de plusieurs indices, le nombre l de ces indices étant égal au nombre des facteurs a, b, c, \dots , et représenter même les divers systèmes d'indices par divers systèmes de lettres

$$\begin{aligned} &\alpha, \epsilon, \gamma, \dots, \\ &\lambda, \mu, \nu, \dots, \\ &\varphi, \chi, \psi, \dots, \\ &\text{etc.} \end{aligned}$$

Cela posé, les substitutions P, Q, \dots qui, étant exprimées à l'aide des lettres $\alpha, \beta, \gamma, \dots, \lambda, \mu, \nu, \dots, \varphi, \chi, \psi, \dots$, se présenteront sous les formes

$$(3) \quad P = (\alpha, \epsilon, \gamma, \dots), \quad Q = (\lambda, \mu, \nu, \dots), \quad R = (\varphi, \chi, \psi, \dots), \dots,$$

seront évidemment des substitutions permutables entre elles, la première de l'ordre a , la seconde de l'ordre b , la troisième de l'ordre c, \dots ; et elles composeront, avec leurs dérivées, un système de substitutions conjuguées dont l'ordre sera

$$n = abc\dots$$

Ajoutons que, si les substitutions (3) sont exprimées à l'aide des n lettres

$$x, \gamma, z, \dots,$$

chacune d'elles sera une substitution régulière qui renfermera toutes ces lettres, P étant le produit de $\frac{n}{a}$ facteurs circulaires de l'ordre a , Q étant pareillement le produit de $\frac{n}{b}$ facteurs circulaires de l'ordre b, \dots

Dans le cas particulier où les l facteurs a, b, c, \dots deviennent égaux entre eux, on a

$$n = a^l,$$

et les substitutions

$$P, Q, R, \dots$$

forment avec leurs dérivées un système de a^l substitutions diverses qui sont toutes de l'ordre a , si a est un nombre premier, à l'exception de celle qui se réduit à l'unité.

Au reste, les propositions diverses auxquelles nous venons de parvenir peuvent encore être généralisées, ainsi que nous allons l'expliquer.

Considérons toujours un système de n variables

$$x, y, z, \dots$$

Soient d'ailleurs a un nombre entier égal ou inférieur à n , et ha un multiple de a contenu dans n . Enfin, concevons qu'avec ah variables, prises au hasard, on forme h groupes divers composés chacun de a lettres, et nommons

$$(4) \quad P_1, P_2, \dots, P_h$$

h substitutions circulaires de l'ordre a , dont chacune soit formée avec les variables comprises dans un seul groupe. Ces substitutions étant permutables entre elles, le système de ces mêmes substitutions, et de leurs dérivées, sera de l'ordre

$$a^h.$$

Ajoutons que, si a est un nombre premier, le système dont il s'agit renfermera seulement des substitutions régulières de l'ordre a , dont quelques-unes, savoir, les substitutions (4) et leurs puissances, se réduiront à des substitutions circulaires de l'ordre a .

Soient maintenant b un nombre égal ou inférieur à h , et kb un multiple de b contenu dans h . Avec plusieurs des précédents groupes que j'appellerai groupes de première espèce, on pourra composer des groupes de seconde espèce, dont chacun embrasse b groupes de première espèce, et dont le nombre soit égal à k . Cela posé, nommons

$$(5) \quad Q_1, Q_2, \dots, Q_b$$

des substitutions dont chacune consiste à permuter circulairement entre eux les b groupes de première espèce compris dans un seul groupe de seconde espèce. Chacune des substitutions (5), exprimée à l'aide des variables primitives, sera une substitution régulière équivalente au produit de a facteurs circulaires dont chacun sera de l'ordre b ; et ces substitutions seront permu-

tables, non-seulement entre elles, mais encore avec les substitutions (4). Par suite, le système des substitutions (4) et (5), et de leurs dérivées, sera de l'ordre

$$a^h b^k.$$

En continuant ainsi, on établira généralement la proposition suivante:

1^{er} *Théorème.* Considérons un système de n variables x, y, z, \dots Soient d'ailleurs a un nombre entier, égal ou inférieur à n , et $i = ha$ un multiple de a contenu dans n . Soient encore b un nombre entier, égal ou inférieur à h , et kb un multiple de b contenu dans h . Soient pareillement c un nombre entier, égal ou inférieur à k , et lc un multiple de c contenu dans k ;.... On pourra toujours former, avec i variables arbitrairement choisies, un système de substitutions conjuguées dont l'ordre sera représenté par le produit

$$a^h b^k c^l \dots$$

Corollaire. En supposant les nombres a, b, c, \dots tous égaux à un même nombre premier, p , on déduit immédiatement du théorème 1^{er} la proposition suivante:

2^e *Théorème.* Considérons un système de n variables. Soit d'ailleurs p un nombre premier égal ou inférieur à n . Soient encore $i = hp$ un multiple de p contenu dans n , kp un multiple de p contenu dans h , lp un multiple de p contenu dans k , etc. Avec i variables arbitrairement choisies, on pourra toujours former un système de substitutions conjuguées et primitives, dont l'ordre sera représenté par le produit

$$p^h p^k p^l \dots = p^{h+k+l+\dots}$$

Corollaire. Rien n'empêche d'admettre que dans le théorème précédent on désigne par hp le plus grand multiple de p contenu dans n , par kp le plus grand multiple de p contenu dans h , par lp le plus grand multiple de p contenu dans k ,.... Alors

$$p^{h+k+l+\dots}$$

se réduit (*) à la plus haute puissance de p qui divise exactement le

(*) Soit p^f la plus haute puissance de p qui divise exactement le produit

$$N = 1 \cdot 2 \cdot 3 \dots n.$$

Pour que $p^{h+k+l+\dots}$ se réduise à p^f , il sera nécessaire et il suffira que l'on ait

$$h + k + l + \dots = f.$$

Or, effectivement, on sait que l'exposant f de la plus haute puissance de p , qui divise N , est

produit

$$N = 1 \cdot 2 \cdot 3 \dots n,$$

et, par suite, on obtient, à la place du 2^e théorème, la proposition suivante :

3^e *Théorème.* Considérons un système de n variables x, y, z, \dots Soient d'ailleurs p un nombre premier, égal ou inférieur à n , i le plus grand multiple de p contenu dans n , et p^f la plus haute puissance de p qui divise exactement le produit

$$N = 1 \cdot 2 \cdot 3 \dots n.$$

Avec plusieurs des variables x, y, z, \dots choisies arbitrairement en nombre égal à i , on pourra toujours former un système de substitutions primitives conjuguées, qui sera de l'ordre p^f .

Pour montrer une application des principes que nous venons d'établir,

la somme des entiers contenus dans les fractions

$$\frac{N}{p}, \frac{N}{p^2}, \frac{N}{p^3}, \dots$$

et il est clair que, dans l'hypothèse admise, ces entiers seront précisément les nombres représentés par

$$h, k, l, \dots$$

Au reste, on peut arriver très-simplement à l'équation

$$p^{h+k+l+\dots} = p^f$$

de la manière suivante :

Soient, comme ci-dessus,

hp le plus grand multiple de p contenu dans n ,

kp le plus grand multiple de p contenu dans h ,

lp le plus grand multiple de p contenu dans k ,

etc. . .

Évidemment p^f , ou la plus haute puissance de p qui divise le produit

$$N = 1 \cdot 2 \cdot 3 \dots n,$$

sera en même temps la plus haute puissance de p qui divisera le produit

$$p \cdot 2p \cdot 3p \dots hp = 1 \cdot 2 \cdot 3 \dots hp^h.$$

Donc, par suite,

$$\frac{p^f}{p^h} = p^{f-h}$$

sera la plus haute puissance de p qui divisera le produit

$$1 \cdot 2 \cdot 3 \dots h;$$

mais kp étant le plus grand multiple de p contenu dans h , p^{f-h} sera encore la plus haute

considérons en particulier cinq variables

$$x, y, z, u, v,$$

et supposons d'ailleurs $p = 2$. On aura, dans ce cas,

$$n = 5, \quad N = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120,$$

$$i = 4 = 2p, \quad h = 2, \quad k = 1,$$

et, par suite,

$$f = h + k = 3, \quad p^f = 4 \cdot 2 = 8.$$

Donc, si l'on prend au hasard quatre des cinq variables données, on pourra toujours, avec ces quatre variables, par exemple avec x, y, z, u , former un système de substitutions régulières conjuguées, qui sera d'un ordre représenté par le nombre 8. Effectivement, partageons les quatre variables

$$x, y, z, u$$

en deux groupes

$$x, y,$$

$$z, u,$$

puissance de p qui divisera le produit

$$p \cdot 2p \cdot 3p \dots kp = 1 \cdot 2 \cdot 3 \dots kp^k.$$

Donc, par suite,

$$\frac{p^{f-h}}{p^k} = p^{f-h-k}$$

sera la plus haute puissance de p qui divisera le produit

$$1 \cdot 2 \dots k.$$

En continuant ainsi, on reconnaîtra que les plus hautes puissances de p qui diviseront les produits

$$1 \cdot 2 \cdot 3 \dots n, \quad 1 \cdot 2 \cdot 3 \dots h, \quad 1 \cdot 2 \cdot 3 \dots k, \quad 1 \cdot 2 \cdot 3 \dots l, \dots$$

sont respectivement les divers termes de la suite

$$p^f, \quad p^{f-h}, \quad p^{f-h-k}, \quad p^{f-h-k-l}, \dots$$

Or, cette même suite aura nécessairement pour dernier terme

$$p^0 = 1,$$

et comme ce dernier terme sera aussi de la forme

$$p^{f-h-k-l-\dots},$$

on aura définitivement

$$p^{f-h-k-l-\dots} = 1,$$

ou, ce qui revient au même,

$$p^f = p^{h+k+l+\dots}.$$

composés chacun de deux variables, et nommons

$$P_1 = (x, y), \quad P_2 = (z, u)$$

deux substitutions circulaires du second ordre, dont chacune soit formée avec les variables comprises dans un seul groupe. Soit, de plus,

$$Q = (x, z) (y, u)$$

la substitution qui consiste à échanger les deux groupes

$$x, y,$$

$$z, u,$$

l'un contre l'autre. Les trois substitutions

$$P_1, P_2 \text{ et } Q$$

seront permutables entre elles, et, en les joignant à leurs dérivées, on obtiendra un système de huit substitutions régulières et conjuguées, qui seront respectivement

$$1, \quad P_1, \quad P_2, \quad P_1 P_2,$$

$$Q, \quad P_1 Q, \quad P_2 Q, \quad P_1 P_2 Q,$$

ou, ce qui revient au même,

$$1, \quad (x, y), \quad (z, u), \quad (x, y) (z, u), \\ (x, z) (y, u), \quad (x, z, y, u), \quad (x, u, y, z), \quad (x, u) (y, z).$$

Concevons maintenant que les variables données

$$x, y, z, u, v, w$$

soient au nombre de six, et que l'on prenne $p = 3$. Alors on aura

$$n = 6, \quad N = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720,$$

$$i = 6 = 2p, \quad h = 2,$$

et, par suite,

$$f = h = 2, \quad p^f = 3^2 = 9.$$

Cela posé, on conclura du 3^e théorème qu'avec les six variables x, y, z, u, v, w on peut former un système de neuf substitutions régulières et conjuguées. Effectivement, partageons ces six variables en deux groupes

$$x, y, z,$$

$$u, v, w,$$

composés chacun de trois variables, et nommons

$$P_1 = (x, y, z), \quad P_2 = (u, v, w)$$

deux substitutions circulaires du troisième ordre, dont chacune soit formée avec les variables comprises dans un seul groupe. Ces deux substitutions seront permutables entre elles, et, en les joignant à leurs dérivées, on obtiendra un système de neuf substitutions régulières et conjuguées qui seront respectivement

$$1, \quad P_1, \quad P_1^2,$$

$$P_2, \quad P_1 P_2, \quad P_1^2 P_2,$$

$$P_2^2, \quad P_1 P_2^2, \quad P_1^2 P_2^2,$$

ou, ce qui revient au même,

$$1, \quad (x, y, z), \quad (x, z, y),$$

$$(u, v, w), \quad (x, y, z) (u, v, w), \quad (x, z, y) (u, v, w),$$

$$(u, w, v), \quad (x, y, z) (u, w, v), \quad (x, z, y) (u, w, v).$$

Concevons enfin que, les variables données

$$x, y, z, u, v, w$$

étant toujours au nombre de six, on prenne $p = 2$. Alors on aura non-seulement

$$n = 6, \quad N = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6,$$

mais encore

$$i = n = 6 = 3p, \quad h = 3, \quad k = 1,$$

et par suite

$$f = h + k = 4, \quad p^f = 2^4 = 16.$$

Cela posé, on conclura du 3^e théorème, qu'avec les six variables x, y, z, u, v, w on peut former seize substitutions primitives et conjuguées. Effectivement, partageons ces six variables en trois groupes

$$x, y,$$

$$z, u,$$

$$v, w,$$

et nommons

$$P_1 = (x, y), \quad P_2 = (z, u), \quad P_3 = (v, w)$$

trois substitutions circulaires du second ordre dont chacune soit formée avec les variables comprises dans un seul groupe. Soit, de plus,

$$Q = (x, z) (y, u)$$

la substitution qui consiste à échanger les deux premiers groupes
 $x, y,$
 $z, u,$
l'un contre l'autre. Les quatre substitutions

P_1, P_2, P_3 et Q

seront permutables entre elles; et, en les joignant à leurs dérivées, on obtiendra un système de seize substitutions primitives et conjuguées qui seront respectivement

$I,$	$P_1,$	$P_2,$	$P_3,$
$P_1 P_2 P_3,$	$P_2 P_3,$	$P_3 P_1,$	$P_1 P_2,$
$Q,$	$P_1 Q,$	$P_2 Q,$	$P_3 Q,$
$P_1 P_2 P_3 Q,$	$P_2 P_3 Q,$	$P_3 P_1 Q,$	$P_1 P_2 Q;$

ou, ce qui revient au même,

$I,$	$(x, y),$	$(z, u),$	$(v, w),$
$(x, y)(z, u)(v, w),$	$(z, u)(v, w),$	$(v, w)(x, y),$	$(x, y)(z, u),$
$(x, z)(y, u),$	$(x, z, y, u),$	$(x, u, y, z),$	$(x, z)(y, u)(v, w),$
$(x, u)(y, z)(v, w),$	$(x, u, y, z)(v, w),$	$(x, z, y, u)(v, w),$	$(x, u)(y, z).$

Il est bon d'observer que ce dernier système de substitutions conjuguées renferme, avec l'unité, trois substitutions circulaires du second ordre, savoir,

$(x, y), (z, u), (v, w),$

huit substitutions régulières du second ordre, savoir,

$(z, u)(v, w), (v, w)(x, y), (x, y)(z, u), (x, z)(y, u), (x, u)(y, z),$

et

$(x, y)(z, u)(v, w), (x, z)(y, u)(v, w), (x, u)(y, z)(v, w),$

deux substitutions régulières du quatrième ordre, savoir,

$(x, z, y, u), (x, u, y, z),$

dont l'une est le cube de l'autre; enfin deux substitutions primitives du quatrième ordre, savoir,

$(x, z, y, u)(v, w), (x, u, y, z)(v, w),$

dont l'une est encore le cube de l'autre.

—

§ VIII. — *Sur les diverses puissances d'une même substitution.*

Soient P une substitution quelconque, et i l'ordre de cette substitution. Les diverses puissances de P , ou, ce qui revient au même, les dérivées diverses de P , se réduiront aux divers termes de la suite

$$(1) \quad 1, P, P^2, \dots, P^{i-1},$$

dont le premier peut encore être représenté par P^0 ; et si, en nommant r un des nombres

$$(2) \quad 0, 1, 2, \dots, i-1,$$

on désigne par l un entier qui, divisé par i , donne r pour reste, la formule

$$l \equiv r, \pmod{i}$$

entraînera la suivante

$$P^l = P^r.$$

Soient maintenant

$$\mathcal{V}, \mathcal{V}', \mathcal{V}'', \dots$$

les divers facteurs circulaires de P formés avec des variables qui sont toutes distinctes les unes des autres. L'équation

$$(3) \quad P = \mathcal{V} \mathcal{V}' \mathcal{V}'' \dots$$

entraînera la suivante

$$(4) \quad P^l = \mathcal{V}^l \mathcal{V}'^l \mathcal{V}''^l \dots,$$

quel que soit l'exposant l ; et, comme les divers facteurs $\mathcal{V}^l, \mathcal{V}'^l, \mathcal{V}''^l, \dots$ de la substitution P^l sont formés avec des variables diverses, le seul cas où la substitution P^l ne déplacera aucune variable sera évidemment celui où chacun des facteurs $\mathcal{V}^l, \mathcal{V}'^l, \mathcal{V}''^l, \dots$ remplira cette même condition. En d'autres termes, pour que l'on ait

$$(5) \quad P^l = 1,$$

il sera nécessaire et il suffira que l'on ait séparément

$$(6) \quad \mathcal{V}^l = 1, \quad \mathcal{V}'^l = 1, \quad \mathcal{V}''^l = 1, \dots$$

D'ailleurs, les diverses valeurs entières et positives de l propres à vérifier la formule (3) seront l'ordre i de la substitution P et les multiples de cet ordre. Pareillement, les diverses valeurs de l propres à vérifier l'une quelconque des formules (4) seront l'ordre du facteur circulaire qui entre dans cette formule et les multiples de cet ordre. Cela posé, il est clair que la plus petite des va-



leurs positives de l propres à vérifier la formule (3) ou l'ordre i de la substitution P , devra être le plus petit nombre divisible à la fois par les ordres des divers facteurs circulaires $\mathcal{V}, \mathcal{V}, \mathcal{W}, \dots$. Ainsi se trouve rigoureusement établie la proposition que nous avons déjà indiquée page 161, et que l'on peut énoncer comme il suit :

1^{er} *Théorème.* L'ordre d'une substitution quelconque P , représentée par le produit de plusieurs facteurs circulaires

$$\mathcal{V}, \mathcal{V}, \mathcal{W}, \dots$$

est le plus petit nombre qui soit divisible par l'ordre de chacun de ces facteurs.

Soit maintenant h un nombre entier quelconque, et posons

(7)

$$S = P^h.$$

La substitution S sera l'une quelconque des dérivées de P . D'ailleurs, l'équation (7) entraînera la suivante

(8)

$$S^i = P^{hi},$$

et, par suite, la formule

(9)

$$S^i = 1$$

donnera

(10)

$$P^{hi} = 1.$$

Donc l'ordre de la substitution S , ou la plus petite des valeurs de l propres à vérifier la formule (9), sera en même temps la plus petite des valeurs de l propres à vérifier la formule (10) et, par conséquent, l'équivalence

(11)

$$hl = 0, \pmod{i};$$

ou, ce qui revient au même, la plus petite des valeurs de l qui rendront le produit hl divisible par i . Or, si l'on nomme θ le plus grand commun diviseur de h et de i , les seules valeurs de l qui rendront le produit hl divisible par i seront le rapport $\frac{i}{\theta}$ et les multiples de ce rapport. Donc l'ordre de la substitution $S = P^h$ sera précisément le rapport $\frac{i}{\theta}$, et l'on pourra énoncer encore la proposition suivante :

2^e *Théorème.* Soit P une substitution de l'ordre i . Soient, de plus, h un



nombre entier quelconque, et θ le plus grand commun diviseur des entiers h et i . L'ordre de la substitution P^h sera représenté par le rapport $\frac{i}{\theta}$.

Corollaire. Pour que $\frac{i}{\theta}$ se réduise à i , il est nécessaire et il suffit que l'on ait $\theta = 1$, c'est-à-dire que le plus grand commun diviseur de h et de i se réduise à l'unité; en d'autres termes, il est nécessaire et il suffit que h soit premier à i . D'ailleurs, lorsque cette condition se trouve remplie, h est nécessairement premier à chacun des facteurs de i , par conséquent à l'ordre de chacun des facteurs circulaires

$$\mathcal{V}, \mathcal{V}, \mathcal{W}, \dots$$

de la substitution P . Donc alors les ordres de ces divers facteurs sont respectivement égaux à ceux des substitutions

$$\mathcal{V}^h, \mathcal{V}^h, \mathcal{W}^h, \dots,$$

et la formule

$$(12) \quad P^h = \mathcal{V}^h \mathcal{V}^h \mathcal{W}^h \dots,$$

qui se déduit immédiatement de l'équation (3), fournit pour valeur de P^h une substitution semblable à la substitution P . On peut donc énoncer encore la proposition suivante :

3^e Théorème. P étant une substitution de l'ordre i , les substitutions qui seront de cet ordre, parmi les diverses puissances de P , se confondront avec les puissances dont les degrés seront premiers à i . De plus, ces substitutions seront toutes semblables à P ; en conséquence, la suite

$$1, P, P^2, \dots, P^{i-1}$$

offrira autant de termes semblables à P qu'il y a de nombres entiers inférieurs à i et premiers à i .

Corollaire. Soit θ un diviseur quelconque de i , et posons

$$(13) \quad i = \theta j.$$

En vertu du 2^e théorème, une puissance P^h de P sera de l'ordre $j = \frac{i}{\theta}$ lorsque h sera de la forme

$$(14) \quad h = \theta k,$$

k étant premier à j . Or, dans cette hypothèse, en faisant, pour abréger,

$$(15) \quad P^\theta = \Theta,$$

on trouvera

$$(16) \quad P^h = \Theta^k;$$

et comme, en vertu de la formule (15), Θ sera une substitution de l'ordre j , on conclura de la formule (16), jointe au 3^e théorème, que P^h est une substitution semblable à $P^{\theta} = \Theta$. Enfin il est clair que le nombre h déterminé par la formule (14) sera inférieur à i et premier à i , si le nombre k est inférieur à j et premier à j . Cela posé, on pourra évidemment énoncer la proposition suivante :

4^e *Théorème.* P étant une substitution de l'ordre i , θ un diviseur quelconque de i , et j la valeur entière du rapport $\frac{i}{\theta}$, les substitutions qui seront de l'ordre j , parmi les diverses puissances de P , se confondront avec les puissances dont les degrés, divisés par θ , donneront pour quotients des nombres entiers premiers à j . De plus, ces substitutions seront toutes semblables à P^{θ} ; en conséquence, la suite

$$1, P, P^2, \dots, P^{i-1}$$

offrira autant de termes semblables à P^{θ} qu'il y a de nombres entiers inférieurs à j et premiers à j .

Pour montrer une application des théorèmes qui précédent, considérons en particulier la substitution circulaire de même ordre

$$P = (x, y, z, u, v, w).$$

Dans ce cas le nombre

$$i = 6$$

aura pour diviseurs, outre l'unité, les nombres

$$2, 3, 6,$$

et les puissances distinctes de P seront

$$1, P, P^2, P^3, P^4, P^5.$$

D'ailleurs, parmi les nombres

$$0, 1, 2, 3, 4, 5,$$

qui représenteront les degrés de ces puissances, deux seulement, savoir 1 et 5, seront premiers à 6; deux autres, savoir 2 et 4, seront les produits du diviseur 2 par des facteurs 1 et 2 premiers à $3 = \frac{6}{2}$; enfin le seul nombre 3 pourra être considéré comme le produit du diviseur 3 par un facteur 1 premier à $2 = \frac{6}{3}$. Donc, en vertu des 3^e et 4^e théorèmes, parmi les cinq puis-

sances de P distinctes de l'unité, on trouvera deux substitutions circulaires du sixième ordre, savoir,

$$P \text{ et } P^5,$$

deux substitutions circulaires du troisième ordre, savoir,

$$P^2 \text{ et } P^4,$$

et une seule substitution circulaire du second ordre, savoir,

$$P^3.$$

On aura effectivement

$$\begin{aligned} P &= (x, y, z, u, v, w), & P^5 &= (x, w, v, u, z, y), \\ P^2 &= (x, z, v) (y, u, w), & P^4 &= (x, v, z) (y, w, u), \\ P^3 &= (x, u) (y, v) (z, w). \end{aligned}$$

Lorsque l'ordre de la substitution P est représenté par un nombre premier, alors, en vertu du 3^e théorème, les puissances de P distinctes de l'unité sont toutes semblables à P . Ainsi, par exemple, si l'on prend pour P la substitution régulière du deuxième ordre

$$P = (x, y, z) (u, v, w),$$

les puissances de P distinctes de l'unité, savoir,

$$P, P^2,$$

sont toutes deux des substitutions régulières du troisième ordre. On trouvera, en effet,

$$P^2 = (x, z, y) (u, w, v).$$

Pareillement, si l'on prend pour P la substitution circulaire du cinquième ordre

$$P = (x, y, z, u, v),$$

les quatre puissances de P distinctes de l'unité, savoir,

$$P, P^2, P^3, P^4,$$

seront toutes des substitutions circulaires du cinquième ordre. On aura, en effet,

$$\begin{aligned} P &= (x, y, z, u, v), & P^2 &= (x, z, v, y, u), \\ P^3 &= (x, u, y, v, z), & P^4 &= (x, v, u, z, y). \end{aligned}$$

Lorsque la substitution P est, comme dans le premier et le dernier des exemples précédents, une substitution circulaire, alors, en vertu des principes établis dans le § I (page 158), toute puissance P^h de P est le produit de

plusieurs facteurs circulaires de même ordre, et, par conséquent, une substitution régulière, dont l'ordre se confond avec $\frac{i}{\theta}$, θ étant le plus grand commun diviseur de h et de i . Ajoutons que la substitution P^h renfermera toutes les variables comprises dans la substitution circulaire P .

Si la lettre P représente, non plus une substitution circulaire, mais une substitution régulière équivalente au produit de plusieurs facteurs circulaires

$$\mathfrak{O}, \mathfrak{O}^h, \mathfrak{O}^{h'}, \dots$$

dont chacun est de l'ordre i ; alors, θ étant toujours le plus grand commun diviseur de i et de h , les divers facteurs

$$\mathfrak{O}^h, \mathfrak{O}^{h'}, \mathfrak{O}^{h''}, \dots$$

de la substitution P^h déterminée par la formule (12) renferment toutes les variables comprises dans P , et se réduisent tous à des substitutions régulières de l'ordre $\frac{i}{\theta}$. Il en résulte qu'on peut en dire autant de la substitution P^h elle-même. On peut donc énoncer encore la proposition suivante:

5^e *Théorème.* Soient P une substitution régulière de l'ordre i , et h un nombre entier quelconque. Soient encore θ le plus grand commun diviseur des nombres h , i , et j la valeur entière du rapport $\frac{i}{\theta}$. Alors P^h sera une substitution régulière de l'ordre j , dans laquelle se trouveront comprises toutes les variables que renfermait la substitution P .

Corollaire. Lorsque l'ordre i de la substitution régulière P est une puissance p^f d'un nombre premier p , les deux diviseurs de i , représentés par θ et j , se réduisent eux-mêmes à des puissances de p d'un degré inférieur ou tout au plus égal à f , et le 5^e théorème fournit la proposition suivante:

6^e *Théorème.* Nommons P une substitution régulière dont l'ordre soit une certaine puissance p^f d'un nombre premier p . Soient, de plus, h un nombre entier quelconque, et p^g la plus haute puissance de p qui divise h . La substitution P^h sera une substitution régulière de l'ordre $\frac{p^f}{p^g} = p^{f-g}$, dans laquelle se trouveront comprises toutes les variables que renfermait la substitution P .

Supposons maintenant que P représente une substitution sinon régulière, du moins primitive, c'est-à-dire une substitution régulière ou irrégulière dont l'ordre soit une puissance p^f d'un nombre premier p . Alors P sera nécessaire-

ment le produit de plusieurs substitutions régulières

$$U, V, W, \dots,$$

dont les ordres

$$p^f, p^g, \dots$$

se trouveront représentés par diverses puissances de p correspondantes à des exposants

$$f, g, \dots,$$

qui pourront être censés former une suite décroissante, f étant le plus considérable d'entre eux. D'ailleurs, si l'on désigne par h un nombre entier quelconque, l'équation

$$(17) \quad P = UVW\dots$$

entraînera la suivante

$$(18) \quad P^h = U^h V^h W^h \dots,$$

et de l'équation (18), jointe au 6^e théorème, il résulte évidemment que P^h sera, comme P , une substitution primitive. Enfin il suffira de poser, dans l'équation (18),

ou plus généralement

$$h = kp^g,$$

k étant premier à p , pour réduire à l'unité la substitution V^h , et à plus forte raison les substitutions W^h, \dots . Mais alors, en vertu des formules

$$V^h = 1, \quad W^h = 1, \text{ etc.},$$

jointes à l'équation (18), on aura

$$(19) \quad P^h = U^h.$$

Donc la puissance P^h de la substitution P sera équivalente à la puissance U^h de la substitution régulière U , et l'on conclura du 7^e théorème, que, dans l'hypothèse admise, l'ordre de la substitution P^h se réduit encore à p^{f-g} . D'autre part, comme la substitution $P^h = U^h$ comprendra toutes les variables renfermées dans U , elle sera certainement distincte de l'unité. On peut donc énoncer la proposition suivante :

7^e Théorème. Nommons P une substitution primitive dont l'ordre soit la puissance p^f d'un nombre premier p . Si l'on désigne par h un nombre entier quelconque, P^h sera encore une substitution primitive qui aura pour ordre une certaine puissance de p . Concevons maintenant que l'on décompose P en

facteurs représentés par des substitutions régulières

U, V, W, \dots

dont les ordres

p^f, p^g, \dots

forment une suite décroissante. Si l'on prend pour h , ou le second terme p^g de cette suite, ou le produit de ce second terme par un nombre k premier à p , alors P^h sera une substitution distincte de l'unité, non-seulement primitive, mais régulière et de l'ordre p^{f-g} , dans laquelle se trouveront comprises toutes les variables que renfermait le premier facteur régulier U de la substitution P .

Pour montrer une application du 7^e théorème, considérons la substitution primitive du quatrième ordre

$$P = (x, y, z, u) (v, w).$$

On aura, dans ce cas,

$$U = (x, y, z, u), \quad V = (v, w), \\ i = 4, \quad p = 2, \quad f = 2, \quad g = 1, \quad p^f = 4, \quad p^g = 2.$$

Cela posé, on obtiendra évidemment un nombre h équivalent au produit de $p^g = 2$ par un facteur premier à p , si l'on prend

$$h = 2.$$

Donc, en vertu du 8^e théorème,

$$P^2$$

sera une substitution régulière de l'ordre

$$p^{f-g} = 2.$$

On trouvera effectivement

$$P^2 = (x, z) (y, u).$$

Supposons à présent que la substitution P de l'ordre i ne soit ni régulière, ni même primitive. Alors, en nommant p l'un quelconque des facteurs premiers de i , et en posant

$$i = pl,$$

on conclura du 2^e théorème, que P^l est une substitution de l'ordre p . Donc, puisqu'une substitution dont l'ordre se réduit au nombre premier p est nécessairement régulière, on pourra énoncer la proposition suivante :

8^e *Théorème.* Soient P une substitution quelconque régulière ou irrégulière, i l'ordre de cette substitution, et p l'un quelconque des facteurs premiers de i . On pourra toujours choisir le nombre entier l de manière à faire coïncider la puissance P^l de P avec une substitution de l'ordre p .

Dans ce qui précède, nous avons généralement supposé que les exposants des puissances d'une substitution donnée P étaient positifs. Cette supposition embrasse tous les cas possibles, puisqu'on peut ajouter à un exposant quelconque un multiple quelconque de l'ordre i de la substitution donnée, et transformer ainsi un exposant négatif en un exposant positif. D'ailleurs, l étant un nombre entier quelconque, il est facile d'établir, à l'égard des substitutions de la forme

$$P^{-i} \text{ et } P^{-l},$$

les deux théorèmes que nous allons énoncer.

9^e *Théorème.* Quelle que soit la substitution P , la substitution inverse P^{-i} sera toujours semblable à P .

Démonstration. En effet, nommons i l'ordre de la substitution P . On aura

$$P^{-i} = P^{i-i};$$

et, comme le nombre $i - i$ sera premier à i , on conclura du 4^e théorème, que P^{i-i} est semblable à P .

Corollaire. Soit maintenant l un nombre entier quelconque. L'inverse de P^l , c'est-à-dire la substitution qui, étant multipliée par P^l , donnera pour produit l'unité, sera évidemment P^{-l} . Car, si l'on nomme l' un exposant positif assujetti à vérifier la condition

$$l' \equiv -l \pmod{i},$$

on aura non-seulement

$$P^l \equiv P^{-l},$$

mais encore

$$P^l P^{-l} \equiv P^{l+l'} \equiv P^0 \equiv 1,$$

et, par suite,

$$P^l P^{-l} \equiv 1.$$

Donc, en vertu du 9^e théorème, on pourra énoncer encore la proposition suivante:

10^e *Théorème.* P étant une substitution quelconque, et l un nombre entier quelconque, la puissance négative P^{-l} de P sera toujours semblable à la puissance positive P^l .

§ IX. — *Des substitutions permutables entre elles.*

Soient

P, Q

deux substitutions formées avec les n variables

x, y, z, \dots

Ces deux substitutions P, Q seront *permutables* entre elles si elles vérifient l'équation linéaire et symbolique

(1)

$$QP = PQ.$$

Donc, la substitution P étant donnée, il suffira, pour obtenir une substitution Q permutable avec P , de résoudre l'équation (1). Si, d'ailleurs, on nomme ω le nombre des formes diverses et semblables entre elles que l'on peut faire prendre à la substitution P en l'exprimant à l'aide de ses facteurs circulaires, et, mettant toutes les variables en évidence; ω sera précisément le nombre des solutions diverses de l'équation (1), ou, ce qui revient au même, le nombre des valeurs diverses de la substitution Q . Ajoutons qu'en vertu des principes établis dans le § IV, on devra, pour obtenir Q , écrire au-dessus de la substitution P la même substitution sous une seconde forme semblable à la première, puis réduire les deux formes de la substitution P à de simples arrangements en supprimant les parenthèses et les virgules placées entre les variables, et prendre ces arrangements pour les deux termes de la substitution cherchée Q .

D'autre part, ainsi que nous l'avons déjà expliqué page 171, tout ce que l'on pourra faire pour modifier la forme de la substitution P , ce sera, ou de faire passer successivement à la première place, dans chaque facteur circulaire, une quelconque des lettres comprises dans ce facteur, ou d'échanger entre eux des facteurs circulaires de même ordre. Cela posé, comme le produit de plusieurs facteurs circulaires de même ordre est ce que nous appelons une substitution *régulière*, il arrivera nécessairement de deux choses l'une. Ou P sera une substitution régulière équivalente au produit de plusieurs facteurs circulaires de même ordre qui tous seront échangés circulairement entre eux quand on passera de la première forme de P à la seconde; ou, du moins, P sera le produit de plusieurs substitutions régulières, dont chacune remplira la condition que nous venons d'indiquer.

Arrêtons-nous d'abord à la première hypothèse, et, en admettant que P se

réduise au produit de h facteurs circulaires dont chacun soit de l'ordre a , nommons

$$\mathcal{R}, s, \mathcal{C}, \dots$$

ces mêmes facteurs que nous supposerons échangés circulairement entre eux dans l'ordre indiqué par la substitution

$$(\mathcal{R}, s, \mathcal{C}, \dots).$$

Puisqu'il suffira d'opérer cet échange pour passer de la première forme de P à la seconde, il est clair que, dans ce passage, chacune des variables qui appartiennent au facteur \mathcal{R} se trouvera remplacée par une variable correspondante qui appartiendra au facteur s , puis celle-ci par une troisième variable appartenant au facteur \mathcal{C} , et ainsi de suite. Cela posé, soit α la variable qui occupait la première place dans le facteur \mathcal{R} ; désignons par β, γ, \dots les variables correspondantes tirées des facteurs s, \mathcal{C}, \dots ; enfin soit

$$(\alpha, \beta, \gamma, \dots, \lambda, \mu, \nu, \dots, \varphi, \chi, \psi, \dots)$$

le facteur circulaire qui renferme la variable α dans la substitution Q . La suite des variables

$$(2) \quad \alpha, \beta, \gamma, \dots, \lambda, \mu, \nu, \dots, \varphi, \chi, \psi, \dots$$

pourra être évidemment décomposée en plusieurs autres suites

$$(3) \quad \left\{ \begin{array}{l} \alpha, \beta, \gamma, \dots, \\ \lambda, \mu, \nu, \dots, \\ \varphi, \chi, \psi, \dots, \\ \text{etc.} \end{array} \right.$$

formées chacune avec des variables qui se succéderont dans l'ordre indiqué par la substitution

$$(\mathcal{R}, s, \mathcal{C}, \dots),$$

en sorte que, dans chacune des lignes horizontales du tableau (3), le premier terme représente une variable tirée du facteur \mathcal{R} , le second une variable tirée du facteur s , le troisième une variable tirée du facteur \mathcal{C} , etc. Or, puisque, dans le tableau (3) construit comme on vient de le dire, le nombre des colonnes verticales sera précisément le nombre h des facteurs circulaires

$$\mathcal{R}, s, \mathcal{C}, \dots,$$

il est clair que, si l'on nomme b le nombre total des termes renfermés dans ce même tableau, et θ le nombre des suites horizontales qui le composent, on aura

$$(4) \quad b = \theta h.$$

Ajoutons que le nombre b des termes compris dans le tableau (3) sera précisément l'ordre de la substitution circulaire

$$(\alpha, \beta, \gamma, \dots, \lambda, \mu, \nu, \dots, \varphi, \chi, \psi, \dots).$$

Soient maintenant

$$(5) \quad \alpha', \beta', \gamma', \dots, \lambda', \mu', \nu', \dots, \varphi', \chi', \psi', \dots$$

les variables qui, dans les facteurs circulaires

$$R, S, T, \dots,$$

ou plutôt dans les cercles indicateurs correspondants, suivent immédiatement les variables

$$\alpha, \beta, \gamma, \dots, \lambda, \mu, \nu, \dots, \varphi, \chi, \psi, \dots$$

Soient pareillement

$$(6) \quad \alpha'', \beta'', \gamma'', \dots, \lambda'', \mu'', \nu'', \dots, \varphi'', \chi'', \psi'', \dots$$

les variables qui, dans les mêmes cercles indicateurs, suivent immédiatement les variables

$$\alpha', \beta', \gamma', \dots, \lambda', \mu', \nu', \dots, \varphi', \chi', \psi', \dots$$

etc.... Chacune des suites (5), (6), ... renfermera, comme la suite (4), b termes différents, et ces termes seront encore propres à représenter les variables qui succéderont les unes aux autres, en vertu d'un facteur circulaire de la substitution Q . Cela posé, si l'on nomme

$$V, V, \Psi, \dots$$

les divers facteurs circulaires de Q , tous ces facteurs seront de même ordre, et l'on pourra supposer

$$(7) \quad \left\{ \begin{array}{l} V = (\alpha, \beta, \gamma, \dots, \lambda, \mu, \nu, \dots, \varphi, \chi, \psi, \dots), \\ V = (\alpha', \beta', \gamma', \dots, \lambda', \mu', \nu', \dots, \varphi', \chi', \psi', \dots), \\ \Psi = (\alpha'', \beta'', \gamma'', \dots, \lambda'', \mu'', \nu'', \dots, \varphi'', \chi'', \psi'', \dots), \\ \text{etc.} \end{array} \right.$$

D'autre part, les variables qui succéderont les unes aux autres, en vertu du facteur circulaire \mathcal{R} de la substitution P , seront évidemment

$$(8) \quad \alpha, \alpha', \alpha'', \dots, \lambda, \lambda', \lambda'', \dots, \varphi, \varphi', \varphi'', \dots$$

Pareillement, les variables, qui succéderont les unes aux autres dans le facteur s de la substitution P , seront

$$(9) \quad \epsilon, \epsilon', \epsilon'', \dots, \mu, \mu', \mu'', \dots, \chi, \chi', \chi'', \dots$$

De même aussi les variables, qui succéderont les unes aux autres dans le facteur \mathcal{C} de la substitution P , seront

$$(10) \quad \gamma, \gamma', \gamma'', \dots, \nu, \nu', \nu'', \dots, \psi, \psi', \psi'', \dots$$

etc.... On aura donc encore

$$(11) \quad \left\{ \begin{array}{l} \mathcal{R} = (\alpha, \alpha', \alpha'', \dots, \lambda, \lambda', \lambda'', \dots, \varphi, \varphi', \varphi'', \dots), \\ s = (\epsilon, \epsilon', \epsilon'', \dots, \mu, \mu', \mu'', \dots, \chi, \chi', \chi'', \dots), \\ \mathcal{C} = (\gamma, \gamma', \gamma'', \dots, \nu, \nu', \nu'', \dots, \psi, \psi', \psi'', \dots), \\ \text{etc.} \end{array} \right.$$

Observons d'ailleurs que, si l'on nomme k le nombre des facteurs circulaires

$$\mathcal{V}, \mathcal{V}, \mathcal{V}, \dots$$

de la substitution Q , les diverses variables comprises dans la substitution \mathcal{R} pourront être réparties entre les k suites verticales du tableau

$$(12) \quad \left\{ \begin{array}{l} \alpha, \alpha', \alpha'', \dots, \\ \lambda, \lambda', \lambda'', \dots, \\ \varphi, \varphi', \varphi'', \dots, \\ \text{etc.} \end{array} \right.$$

qui renferme, comme le tableau (3), θ lignes horizontales. Donc l'ordre a de la substitution \mathcal{R} , représenté par le nombre total des termes du tableau (12), sera

$$(13) \quad a = \theta k.$$

Remarquons à présent que, dans l'hypothèse admise, les substitutions P, Q , toutes deux régulières, seront déterminées par les formules

$$(14) \quad P = \mathcal{R} s \mathcal{C} \dots, \quad Q = \mathcal{V} \mathcal{V} \mathcal{V} \dots,$$

et que les n variables données

ce même tableau x, y, z, \dots

se confondront avec les variables comprises dans les seconds membres des formules (7), ou, ce qui revient au même, dans les seconds membres des formules (11). D'ailleurs ces mêmes variables, dont le nombre n se trouvera représenté par chacun des produits égaux

$$ah, bk, \theta hk, \dots \quad (e)$$

pourront être réparties entre les divers tableaux

$$(15) \quad \left\{ \begin{array}{l} \alpha, \beta, \gamma, \dots, \\ \alpha', \beta', \gamma', \dots, \\ \alpha'', \beta'', \gamma'', \dots, \\ \text{etc.} \end{array} \right\} \quad (a)$$

$$(16) \quad \left\{ \begin{array}{l} \lambda, \mu, \nu, \dots, \\ \lambda', \mu', \nu', \dots, \\ \lambda'', \mu'', \nu'', \dots, \\ \text{etc.} \end{array} \right\} \quad (b)$$

$$(17) \quad \left\{ \begin{array}{l} \varphi, \chi, \psi, \dots, \\ \varphi', \chi', \psi', \dots, \\ \varphi'', \chi'', \psi'', \dots, \\ \text{etc.} \end{array} \right\} \quad (c)$$

dont le nombre sera θ , et dont chacun renfermera non-seulement h lignes verticales, mais encore k lignes horizontales. Cela posé, on conclura immédiatement des formules (11), que, pour obtenir, dans l'hypothèse admise, l'un quelconque des facteurs circulaires

de la substitution P , il suffit d'écrire à la suite les unes des autres, en les plaçant entre deux parenthèses et les séparant par des virgules, les variables qui appartiennent, dans les tableaux (15), (16), (17), etc., à une ligne verticale de rang déterminé. On conclura, au contraire, des formules (7), que, pour obtenir l'un quelconque des facteurs circulaires

$$\dots \circ, \vartheta, \psi, \dots = q \quad (p)$$

de la substitution Q , il suffit d'écrire à la suite les unes des autres, en les plaçant entre deux parenthèses et les séparant par des virgules, les variables qui appartiennent, dans les tableaux (15), (16), (17), etc., à une ligne horizontale de rang déterminé.

Remarquons encore que, le nombre des lignes horizontales ou verticales comprises dans chacun des tableaux (15), (16), (17), etc., étant désigné, pour les lignes horizontales, par la lettre k , et, pour les lignes verticales, par la lettre h , on tirera immédiatement des formules (7)

$$(18) \quad \left\{ \begin{array}{l} \mathcal{V}^h = (\alpha, \lambda, \varphi, \dots) (\beta, \mu, \chi, \dots) (\gamma, \nu, \psi, \dots) \dots, \\ \mathcal{V}'^h = (\alpha', \lambda', \varphi', \dots) (\beta', \mu', \chi', \dots) (\gamma', \nu', \psi', \dots) \dots, \\ \mathcal{V}''^h = (\alpha'', \lambda'', \varphi'', \dots) (\beta'', \mu'', \chi'', \dots) (\gamma'', \nu'', \psi'', \dots) \dots, \\ \text{etc.} \end{array} \right.$$

et des formules (11)

$$(19) \quad \left\{ \begin{array}{l} \mathcal{R}^k = (\alpha, \lambda, \varphi, \dots) (\alpha', \lambda', \varphi', \dots) (\alpha'', \lambda'', \varphi'', \dots) \dots, \\ \mathcal{S}^k = (\beta, \mu, \chi, \dots) (\beta', \mu', \chi', \dots) (\beta'', \mu'', \chi'', \dots) \dots, \\ \mathcal{C}^k = (\gamma, \nu, \psi, \dots) (\gamma', \nu', \psi', \dots) (\gamma'', \nu'', \psi'', \dots) \dots, \\ \text{etc.} \end{array} \right.$$

D'autre part, les équations (14) donneront

$$(20) \quad P^k = \mathcal{R}^k \mathcal{S}^k \mathcal{C}^k \dots, \quad Q^h = \mathcal{V}^h \mathcal{V}'^h \mathcal{V}''^h \dots$$

Donc, eu égard aux formules (18), (19), chacune des substitutions P^k, Q^h sera équivalente au produit de tous les facteurs circulaires que renferme le tableau

$$(21) \quad \left\{ \begin{array}{l} (\alpha, \lambda, \varphi, \dots), (\beta, \mu, \chi, \dots), (\gamma, \nu, \psi, \dots), \\ (\alpha', \lambda', \varphi', \dots), (\beta', \mu', \chi', \dots), (\gamma', \nu', \psi', \dots), \\ (\alpha'', \lambda'', \varphi'', \dots), (\beta'', \mu'', \chi'', \dots), (\gamma'', \nu'', \psi'', \dots), \\ \text{etc.} \end{array} \right.$$

Donc, si l'on nomme Θ le produit de tous ces facteurs circulaires, on aura simultanément

$$(22) \quad P^k = \Theta, \quad Q^h = \Theta,$$

et, par suite,

$$(23) \quad P^k = Q^h.$$

De plus, θ étant précisément le nombre des variables comprises dans chaque ligne verticale du tableau (3), la valeur commune Θ de P^k et de Q^h sera évidemment une substitution régulière de l'ordre θ ; et, d'ailleurs, à la seule inspection du tableau (21), on reconnaîtra immédiatement que, pour obtenir l'un quelconque des facteurs circulaires de la substitution Θ , il suffit d'écrire à la suite les unes des autres, en les renfermant entre deux parenthèses et en les séparant par des virgules, les variables semblablement placées dans les tableaux (15), (16), (17), etc.

Remarquons enfin qu'en vertu des formules (11), un facteur quelconque de P , le facteur \mathcal{R} par exemple, renfermera une ou plusieurs des variables comprises dans chacun des facteurs circulaires de Q , et que, réciproquement, en vertu des formules (7), un facteur quelconque de Q , le facteur \mathcal{O} par exemple, renfermera une ou plusieurs variables comprises dans chacun des facteurs circulaires de P . Il est aisément d'en conclure que, dans l'hypothèse admise, on ne pourra décomposer les deux substitutions P, Q , toutes deux régulières et permutable entre elles, en facteurs qui soient distincts de ces substitutions elles-mêmes, et qui, comparés deux à deux, restent permutable entre eux. En effet, pour qu'une telle décomposition fût possible, il faudrait qu'avec une partie des variables données x, y, z, \dots , on pût former deux substitutions \mathcal{P}, \mathcal{Q} , permutable entre elles, qui eussent respectivement pour facteurs circulaires, la première un ou plusieurs des facteurs $\mathcal{R}, \mathcal{S}, \mathcal{T}, \dots$, la seconde un ou plusieurs des facteurs $\mathcal{O}, \mathcal{V}, \mathcal{W}, \dots$. Or, cette dernière supposition devra être évidemment rejetée; car, d'après la remarque énoncée, la substitution \mathcal{P} ne pourra renfermer un seul des facteurs $\mathcal{R}, \mathcal{S}, \mathcal{T}, \dots$ sans renfermer une ou plusieurs des variables comprises dans chacun des facteurs $\mathcal{O}, \mathcal{V}, \mathcal{W}, \dots$; et, si cette condition était remplie, la substitution \mathcal{Q} deviendrait nécessairement équivalente au produit de tous les facteurs $\mathcal{O}, \mathcal{V}, \mathcal{W}, \dots$. Donc alors \mathcal{Q} et \mathcal{P} renfermeraient toutes les variables données, et non plus seulement une partie de ces variables.

Jusqu'à présent nous avons supposé, d'une part, que P était une substitution régulière, c'est-à-dire équivalente à un produit de facteurs circulaires de même ordre; d'autre part, que ces facteurs circulaires étaient tous échangés circulairement entre eux quand on passait d'une première forme de P à une seconde forme distincte de la première, afin d'obtenir, par la comparaison de ces deux formes, une substitution Q permutable avec la substitution P .

Dans le cas général où la lettre P désigne une substitution quelconque, cette substitution régulière ou irrégulière peut du moins être considérée

comme le produit de plusieurs substitutions régulières

$$\mathfrak{P}, \mathfrak{P}_1, \mathfrak{P}_2, \dots,$$

dont chacune remplit la condition que nous venons d'indiquer. Alors on a

$$(24) \quad P = \mathfrak{P} \mathfrak{P}_1 \mathfrak{P}_2 \dots;$$

et aux substitutions régulières

$$\mathfrak{Q}, \mathfrak{Q}_1, \mathfrak{Q}_2, \dots,$$

qui représentent divers facteurs de P , correspondent des facteurs de Q représentés eux-mêmes par d'autres substitutions régulières

$$\mathfrak{Q}, \mathfrak{Q}_1, \mathfrak{Q}_2, \dots,$$

de sorte qu'on a encore

$$(25) \quad Q = \mathfrak{Q} \mathfrak{Q}_1 \mathfrak{Q}_2 \dots,$$

le facteur \mathfrak{Q} étant permutable avec le facteur \mathfrak{P} , le facteur \mathfrak{Q}_1 avec le facteur \mathfrak{P}_1 , et ainsi de suite. Lorsque les facteurs $\mathfrak{P}, \mathfrak{P}_1, \mathfrak{P}_2, \dots$ se réduisent à un seul facteur \mathfrak{P} , les facteurs $\mathfrak{Q}, \mathfrak{Q}_1, \mathfrak{Q}_2, \dots$ se réduisent aussi à un seul facteur \mathfrak{Q} , et l'on se trouve ramené au cas particulier que nous avons examiné ci-dessus. Mais ce cas particulier est le seul cas où les substitutions P, Q soient permutables entre elles sans pouvoir être décomposées en facteurs plus simples qui, comparés deux à deux, restent permutables entre eux. Cela posé, il résulte des principes établis dans ce paragraphe, qu'on peut énoncer les propositions suivantes :

1^{er} *Théorème.* Soient P, Q deux substitutions permutables entre elles, mais que l'on ne puisse décomposer en facteurs plus simples qui, comparés deux à deux, restent permutables entre eux. Ces substitutions seront toutes deux régulières et de la forme de celles qu'on obtient dans le cas où, avec plusieurs systèmes de variables, on construit divers tableaux qui renferment tous un même nombre de termes compris dans un même nombre de lignes horizontales et verticales, et où, après avoir placé ces tableaux à la suite les uns des autres dans un certain ordre, on multiplie entre eux, d'une part, les facteurs circulaires dont l'un quelconque offre la série des variables qui, dans les divers tableaux, appartiennent à une ligne horizontale de rang déterminé; d'autre part, les facteurs circulaires dont l'un quelconque offre la série des variables qui, dans les divers tableaux, appartiennent à une ligne verticale de rang déterminé. Ajoutons que, dans l'hypothèse admise, les deux substi-

tutions régulières P, Q satisfont à l'équation de condition

$$P^k = Q^h,$$

h étant le nombre des facteurs circulaires de la substitution P , et k le nombre des facteurs circulaires de la substitution Q .

Corollaire 1^{er}. Concevons qu'en faisant usage des notations précédemment adoptées, on nomme

n le nombre des variables comprises dans chacune des substitutions P, Q ;

a l'ordre de la substitution régulière P ;

b l'ordre de la substitution régulière Q ;

θ le nombre des tableaux mentionnés dans le 1^{er} théorème.

Les nombres a, b, n seront liés aux nombres h, k, θ par les formules

$$(26) \quad a = \theta k, \quad b = \theta h, \quad n = \theta hk,$$

et l'ordre de la substitution $P^k = Q^h$ sera précisément le nombre θ déterminé par la formule

$$(27) \quad \theta = \frac{a}{k} = \frac{b}{h} = \frac{n}{hk} = \frac{ab}{n},$$

de laquelle on tire encore

$$(28) \quad \theta = \left(\frac{ab}{hk} \right)^{\frac{1}{2}}.$$

Corollaire 2^e. Pour montrer une application du 1^{er} théorème, supposons qu'avec les variables

$$x, y, z, u, v, w, s, t,$$

on construise les deux tableaux

$$(29) \quad \left\{ \begin{array}{l} x, y, \\ z, u, \end{array} \right.$$

et

$$(30) \quad \left\{ \begin{array}{l} v, w, \\ s, t. \end{array} \right.$$

Le facteur circulaire qui présentera, écrites à la suite l'une de l'autre, les quatre premières lignes verticales des deux tableaux, sera

$$(x, z, v, s);$$

et le facteur circulaire semblablement formé avec les quatre variables comprises dans les secondes lignes verticales des deux tableaux sera

$$(\gamma, u, w, t).$$

Au contraire, le facteur circulaire qui présentera, écrites à la suite l'une de l'autre, les quatre variables comprises dans les premières lignes horizontales des deux tableaux, sera

$$(x, \gamma, v, w),$$

et le facteur circulaire semblablement formé avec les quatre variables comprises dans les secondes lignes horizontales des deux tableaux sera

$$(z, u, s, t).$$

Cela posé, il résulte du 1^{er} théorème que, si l'on prend

$$(31) \quad P = (x, z, v, s) (\gamma, u, w, t),$$

et

$$(32) \quad Q = (x, \gamma, v, w) (z, u, s, t),$$

P, Q seront deux substitutions permutables entre elles, c'est-à-dire deux substitutions qui vérifieront la formule

$$PQ = QP,$$

ou, ce qui revient au même, la formule

$$P = QPQ^{-1}.$$

Effectivement, il suit d'une règle précédemment énoncée (page 178), que, pour obtenir le produit

$$QPQ^{-1},$$

il suffit d'exprimer la substitution P à l'aide de ses facteurs circulaires, puis d'effectuer dans P les déplacements de variables indiqués par la substitution Q , en opérant comme si P représentait un simple arrangement. Or, en écrivant, à la place de la substitution

$$P = (x, z, v, s) (\gamma, u, w, t),$$

l'arrangement

$$A = xzvsvyuwt,$$

et en appliquant à cet arrangement la substitution

$$Q = (x, y, v, w) (z, u, s, t),$$

on trouverait

$$QA = yuwtvsvxz.$$

Donc, en vertu de la règle que nous venons de rappeler, on aura

$$QPQ^{-1} = (y, u, w, t) (v, s, x, z),$$

ou, ce qui revient au même,

$$QPQ^{-1} = (x, z, v, s) (y, u, w, t) = P.$$

Ajoutons que, dans le cas présent, 2 étant tout à la fois le nombre des facteurs circulaires de P et le nombre des facteurs circulaires de Q , on aura

$$h = k = 2.$$

Donc le 1^{er} théorème donnera encore

$$P^2 = Q^2.$$

Enfin la valeur commune des deux substitutions P^2, Q^2 devra être, conformément à une remarque précédemment faite, le produit des quatre facteurs circulaires du second ordre

$$(33) \quad \left\{ \begin{array}{l} (x, v), \quad (y, w), \\ (z, s), \quad (u, t), \end{array} \right.$$

dont chacun est formé avec deux variables qui occupent la même place dans les tableaux (29) et (30). Effectivement on tirera des formules (31) et (32)

$$P^2 = Q^2 = (x, v) (y, w) (z, s) (u, t).$$

Corollaire 3^e. Si les divers tableaux formés avec les n variables que renferment les substitutions P, Q se réduisent à un seul, alors P, Q seront deux substitutions régulières du genre de celles dont nous nous sommes déjà occupés dans le § VII (page 193), et dont les propriétés deviennent évidentes quand on représente les variables qu'elles renferment à l'aide de deux espèces d'indices appliqués à une seule lettre. Alors aussi l'équation

$$\theta = 1$$

entrainera les formules

$$k = a, \quad k = b,$$

$$P^k = Q^h = 1.$$

Supposons, pour fixer les idées, qu'avec les six variables

$$x, y, z, u, v, w,$$

on construise le tableau

$$(34) \quad \left\{ \begin{array}{l} x, y, z, \\ u, v, w. \end{array} \right.$$

Alors, en prenant pour P une substitution dont chaque facteur circulaire renferme les deux variables comprises dans une même ligne verticale du tableau (34), on trouvera

$$(35) \quad P = (x, u) (y, v) (z, w).$$

Au contraire, en prenant pour Q une substitution dont chaque facteur circulaire présente, érites à la suite l'une de l'autre, les trois variables comprises dans une même ligne horizontale du tableau (34), on trouvera

$$(36) \quad Q = (x, y, z) (u, v, w).$$

Or, les substitutions P, Q , déterminées par les formules (35), (36), seront certainement permutables entre elles; car elles se réduiront au cube et au carré de la substitution du sixième ordre

$$(x, w, y, u, z, v).$$

Dé plus, le nombre k se confondant avec l'ordre $a = 2$ de la substitution P , et le nombre h avec l'ordre $b = 3$ de la substitution Q , l'équation (23) donnera

$$P^2 = Q^3 = 1.$$

Corollaire 4^e. Si la substitution P se réduit à un seul facteur circulaire, alors, tout ce que l'on pourra faire pour modifier la forme de P , ce sera de faire passer successivement à la première place l'une quelconque des variables érites à la suite l'une de l'autre dans ce même facteur. Cela posé, les deux arrangements auxquels se réduiront les deux formes assignées à P quand on supprimera les parenthèses et les virgules placées entre les variables, représenteront évidemment les deux termes d'une substitution qui sera une puissance de P . Donc la substitution Q se confondra nécessairement avec

l'une de ces puissances. Alors aussi le tableau unique, construit avec les diverses variables, ne renfermera plus qu'une seule ligne verticale.

2^e *Théorème.* Soient P, Q deux substitutions permutables entre elles et formées avec les n variables

$$x, y, z, \dots$$

Si ces deux substitutions ne sont pas de la forme indiquée dans le 1^{er} théorème, elles pourront, du moins, être décomposées en facteurs correspondants

$$\mathfrak{P}, \mathfrak{P}, \mathfrak{P}, \dots$$

$$\mathfrak{Q}, \mathfrak{Q}, \mathfrak{Q}, \dots$$

qui, pris deux à deux, seront de cette forme et, par conséquent, permutables entre eux.

Corollaire 1^{er}. Soit ω le nombre des formes diverses et semblables entre elles que l'on peut donner à la substitution P en l'exprimant à l'aide de ses facteurs circulaires, et mettant toutes les variables en évidence. ω sera précisément le nombre des solutions diverses de l'équation *symbolique et linéaire*

$$QP = PQ,$$

ré solue par rapport à Q (voir le § IV, page 176); ou, ce qui revient au même, ω sera le nombre des substitutions permutables avec P , qui pourront être formées avec les n variables x, y, z, \dots D'ailleurs, comme nous l'avons déjà remarqué, il suffira, pour obtenir une valeur de Q , d'écrire, au-dessus de la substitution P exprimée à l'aide de ses facteurs circulaires, la même substitution sous une seconde forme semblable à la première, puis de prendre pour termes de la substitution Q les deux arrangements auxquels se réduiront les deux formes de P quand on supprimera, dans ces deux formes, les parenthèses et les virgules placées entre les diverses variables. Enfin, il peut arriver que la substitution P renferme des variables immobiles qui disparaissent quand on la réduit à sa plus simple expression; et il est clair que, dans le passage d'une première forme de P à une seconde, on pourra échanger entre eux arbitrairement les facteurs circulaires du premier ordre formés avec ces variables immobiles. Il en résulte que les variables immobiles de P peuvent, dans la substitution Q , composer des facteurs circulaires quelconques. Donc, pour obtenir les diverses valeurs de Q , il suffira toujours de multiplier les diverses substitutions formées avec les variables immobiles de P , par les diverses valeurs de Q que l'on obtiendrait en laissant de côté

ces mêmes variables et en supposant la valeur de P réduite à sa plus simple expression.

Corollaire 2^e. Pour montrer une application des principes établis dans le précédent corollaire, supposons que, les variables données

$$x, y, z, u, v, w, s, t$$

étant au nombre de huit, la substitution P, réduite à sa plus simple expression, renferme seulement les six variables

$$x, y, z, u, v, w,$$

et soit déterminée par la formule

$$(35) \quad P = (x, u) (y, v) (z, w).$$

La même substitution, quand toutes les variables seront mises en évidence, pourra être présentée sous la forme

$$(37) \quad P = (x, u) (y, v) (z, w) (s) (t).$$

D'ailleurs, si on laisse de côté les deux variables immobiles s, t , le nombre des formes, semblables entre elles, sous lesquelles on pourra présenter la valeur de P fournie par l'équation (35), sera exprimé [voir la formule (2) de la page 172] par le produit

$$1 \cdot 2 \cdot 3 \cdot 2^3 = 48.$$

Donc, avec les six variables

$$x, y, z, u, v, w,$$

on pourra former 48 valeurs diverses de Q, c'est-à-dire 48 substitutions dont chacune sera permutable avec la substitution P. Au contraire, si l'on fait entrer en ligne de compte les deux variables s et t , le nombre des formes, semblables entre elles, sous lesquelles on pourra présenter la valeur de P fournie par l'équation (37), sera

$$(1 \cdot 2) (1 \cdot 2 \cdot 3 \cdot 2^3) = 2 \cdot 48 = 96.$$

Donc, avec les huit variables

$$x, y, z, u, v, w, s, t,$$

on pourra former 2×48 , ou 96 valeurs diverses de Q, c'est-à-dire 96 substitutions dont chacune sera permutable avec la substitution P. Il y a plus :

pour obtenir les 96 valeurs de Q que l'on peut former avec les huit variables diverses variables,

x, y, z, u, v, w, s, t ,

il suffira de multiplier les 48 valeurs de Q , formées avec les six variables

x, y, z, u, v, w ,

par les deux substitutions

s et (s, t) ,

qui peuvent être formées avec les variables immobiles de P ; et, à chacune des valeurs que l'on pourra obtenir par la substitution Q , en laissant de côté les deux variables s, t , correspondra une seconde valeur qui sera le produit de la première par le facteur circulaire (s, t) . Ainsi, par exemple, à la valeur de Q déterminée par l'équation (36), c'est-à-dire par la formule

$$Q = (x, y, z) (u, v, w),$$

correspondra une seconde valeur de Q déterminée par la formule

$$Q = (x, y, z) (u, v, w) (s, t),$$

et permutable, comme la première, avec la substitution P .

Avant de terminer ce paragraphe, nous allons encore établir, à l'égard des substitutions permutables entre elles, quelques propositions qui paraissent dignes d'être remarquées.

3^e *Théorème.* Désignons par

Q, R, S, \dots

diverses substitutions dont chacune soit permutable avec une substitution donnée P . Le produit de deux ou de plusieurs des substitutions Q, R, S, \dots multipliées l'une par l'autre dans un ordre quelconque, sera encore permutable avec la substitution P .

Démonstration. En effet, lorsque chacune des substitutions

Q, R, S, \dots

sera permutable avec P , on aura

$$(38) \quad QP = PQ, \quad RP = PR, \quad SP = PS, \dots,$$

ou, ce qui revient au même,

$$(39) \quad Q = PQP^{-1}, \quad R = PRP^{-1}, \quad S = PSP^{-1}, \dots$$

Or, on tirera immédiatement des équations (39)

$$(40) \quad QR = PQRP^{-1}, \quad QRS = PQRSP^{-1}, \dots,$$

ou, ce qui revient au même,

$$(41) \quad QRP = PQR, \quad QRSP = PQRS, \dots;$$

et il résulte immédiatement des formules (41), que chacun des produits

$$QR, \quad QRS, \dots,$$

formés par la multiplication de deux ou de plusieurs des substitutions

$$Q, \quad R, \quad S, \dots,$$

est permutable avec la substitution P .

Corollaire. Désignons toujours par n le nombre des variables

$$x, \quad y, \quad z, \dots$$

comprises dans la substitution P , et par ω le nombre des formes, semblables entre elles, que peut prendre P exprimé à l'aide de ces variables. ω sera le nombre total des substitutions permutables avec P qui pourront être formées avec les n variables x, y, z, \dots . Soient

$$(42) \quad 1, \quad Q_1, \quad Q_2, \dots, \quad Q_{\omega-1}$$

ces mêmes substitutions, dont l'une se réduira toujours à l'unité. En vertu du 3^e théorème, les dérivées des substitutions

$$Q_1, \quad Q_2, \dots, \quad Q_{\omega-1}$$

seront toutes permutables avec P . Donc ces dérivées seront toutes comprises dans la série (42), et cette série offrira un système de substitutions conjuguées. On peut donc énoncer encore la proposition suivante :

4^e *Théorème.* Une substitution quelconque P étant formée avec les n variables x, y, z, \dots , les diverses substitutions formées avec les mêmes variables, et permutables avec P , offriront un système de substitutions conjuguées.

Exemple. Soit

$$(43) \quad P = (x, y) (z, u).$$

Le nombre des formes, semblables entre elles, que pourra prendre la sub-

stitution P exprimée à l'aide des quatre variables x, y, z, u , sera

$$\dots - 96281 \cdot 2 \cdot 2^2 = 8. \quad (43)$$

Donc ces mêmes variables pourront former huit substitutions permutables avec P . D'ailleurs, pour obtenir ces huit substitutions, il suffira de comparer à la forme sous laquelle P se présente dans la formule (43), les huit formes, semblables entre elles, que peut acquérir P exprimé à l'aide des variables x, y, z, u . Ces huit formes, savoir,

$$(x, y) (z, u), \quad (y, x) (z, u), \quad (x, y) (u, z), \quad (y, x) (u, z), \\ (z, u) (x, y), \quad (z, u) (y, x), \quad (u, z) (x, y), \quad (u, z) (y, x),$$

se réduiront, si l'on supprime les virgules et les parenthèses, aux huit arrangements

$$xyzu, \quad yxzu, \quad xyuz, \quad yxuz, \\ zuxy, \quad zuyx, \quad uzxy, \quad uzyx.$$

Donc, en vertu de la règle énoncée à la page 177, les huit substitutions permutables avec P seront les suivantes :

$$\begin{matrix} (xyzu) \\ (xyzu) \end{matrix}, \quad \begin{matrix} (yxzu) \\ (xyzu) \end{matrix}, \quad \begin{matrix} (xyuz) \\ (xyzu) \end{matrix}, \quad \begin{matrix} (yxuz) \\ (xyzu) \end{matrix},$$

$$\begin{matrix} (zuxy) \\ (xyzu) \end{matrix}, \quad \begin{matrix} (zuyx) \\ (xyzu) \end{matrix}, \quad \begin{matrix} (uzxy) \\ (xyzu) \end{matrix}, \quad \begin{matrix} (uzyx) \\ (xyzu) \end{matrix},$$

ou, ce qui revient au même, les suivantes :

$$(44) \quad \left\{ \begin{array}{lll} 1, & (x, y), & (z, u), \quad (x, y) (z, u), \\ (x, z) (y, u), & (x, z, y, u), & (x, u, y, z), \quad (x, u) (y, z). \end{array} \right.$$

Or, il est aisé de s'assurer que, si l'on multiplie ces huit substitutions par l'une quelconque d'entre elles, les huit produits ainsi obtenus se confondront avec ces mêmes substitutions, rangées seulement dans un nouvel ordre. Donc le système des huit substitutions permutables avec P sera, conformément au 4^e théorème, un système de substitutions conjuguées.

§ X. — Sur les systèmes de substitutions permutables entre eux.

Considérons n variables

$$x, y, z, \dots,$$

et formons avec ces variables deux systèmes de substitutions conjuguées,

l'un de l'ordre α , l'autre de l'ordre b . Représentons d'ailleurs par

$$(1) \quad 1, P_1, P_2, \dots, P_{a-1} \quad (1)$$

les substitutions dont se compose le premier système, et par

$$(2) \quad 1, Q_1, Q_2, \dots, Q_{b-1} \quad (2)$$

celles dont se compose le second système. Nous dirons que les deux systèmes sont *permutables* entre eux, si tout produit de la forme

$$P_h Q_k$$

est en même temps de la forme

$$Q_k P_h.$$

Il pourra d'ailleurs arriver, ou que les indices h et k restent invariables dans le passage de la première forme à la seconde, en sorte qu'on ait

$$P_h Q_k = Q_k P_h;$$

ou que les indices h et k varient dans ce passage, en sorte qu'on ait

$$P_h Q_k = Q_{k'} P_{h'},$$

h', k' étant de nouveaux indices, liés d'une certaine manière aux nombres h et k . Dans le premier cas, l'une quelconque des substitutions (1) sera permutable avec l'une quelconque des substitutions (2). Dans le second cas, au contraire, deux substitutions de la forme P_h , Q_k , cesseront d'être généralement permutables entre elles, quoique le système des substitutions de la forme P_h soit permutable avec le système des substitutions de la forme Q_k .

Supposons maintenant que, les systèmes (1) et (2) étant permutables entre eux, on nomme S une dérivée quelconque des substitutions comprises dans les deux systèmes. Cette dérivée S sera le produit de facteurs dont chacun sera de la forme P_h ou Q_k , et l'on pourra sans altérer ce produit: 1^o échanger entre eux deux facteurs dont l'un serait de la forme P_h , l'autre de la forme Q_k , pourvu que l'on modifie convenablement les valeurs des indices h et k ; 2^o réduire deux facteurs consécutifs de la forme P_h à un seul facteur de cette forme; 3^o réduire deux facteurs consécutifs de la forme Q_k à un seul facteur de cette forme. Or il est clair qu'à l'aide de tels échanges, et de telles réductions, on pourra toujours réduire définitivement la substitution S à l'une quelconque des deux formes

$$P_h Q_k, \quad Q_k P_h.$$

On peut donc énoncer la proposition suivante:

1^{er} Théorème. Soient

$$(1) \quad 1, P_1, P_2, \dots, P_{a-1}, \quad (1)$$

et

D'ailleurs, pour ce faire, il suffit de comparer

$$(2) \quad 1, Q_1, Q_2, \dots, Q_{b-1} \quad (2)$$

deux systèmes de substitutions conjuguées, permutables entre eux, le premier de l'ordre a , le second de l'ordre b . Toute substitution S , dérivée des substitutions (1) et (2), pourra être réduite à chacune des formes

$$P_h Q_k, \quad Q_k P_h, \quad (1)$$

Corollaire. Concevons maintenant que l'on construise les deux tableaux

$$(3) \quad \left\{ \begin{array}{llll} 1, & P_1, & P_2, \dots, & P_{a-1}, \\ Q_1, & Q_1 P_1, & Q_1 P_2, \dots, & Q_1 P_{a-1}, \\ Q_2, & Q_2 P_1, & Q_2 P_2, \dots, & Q_2 P_{a-1}, \\ \dots & \dots & \dots & \dots \\ Q_{b-1}, & Q_{b-1} P_1, & Q_{b-1} P_2, \dots, & Q_{b-1} P_{a-1}; \end{array} \right.$$

$$(4) \quad \left\{ \begin{array}{llll} 1, & P_1, & P_2, \dots, & P_{a-1}, \\ Q_1, & P_1 Q_1, & P_2 Q_1, \dots, & P_{a-1} Q_1, \\ Q_2, & P_1 Q_2, & P_2 Q_2, \dots, & P_{a-1} Q_2, \\ \dots & \dots & \dots & \dots \\ Q_{b-1}, & P_1 Q_{b-1}, & P_2 Q_{b-1}, \dots, & P_{a-1} Q_{b-1}. \end{array} \right.$$

Deux termes pris au hasard, non-seulement dans une même ligne horizontale, mais encore dans deux lignes horizontales différentes du tableau (3), seront nécessairement distincts l'un de l'autre, si les séries (1) et (2) n'offrent pas de termes communs autres que l'unité. Car, si en nommant h, h' deux entiers inférieurs à a , et k, k' deux entiers inférieurs à b , on avait, par exemple,

$$(5) \quad Q_k P_h = Q_{k'} P_{h'}, \quad h \neq h', \quad k \neq k',$$

sans avoir à la fois

$$h = h' \quad \text{et} \quad k = k',$$

Considérons 2 variables

$$Q_k^{-1} Q_{k'} = P_{h'} P_h^{-1},$$

l'équation (5) entraînerait la formule

en vertu de laquelle les deux séries offriraient un terme commun qui serait distinct de l'unité. Donc, dans l'hypothèse admise, les divers termes du tableau (3), qui offrira toutes les valeurs possibles du produit

$$Q_k P_h,$$

seront distincts les uns des autres, et, par suite, les dérivées distinctes des substitutions (1) et (2) se réduiront aux termes de ce tableau. Donc le système de substitutions conjuguées, formé par ces dérivées, sera d'un ordre représenté par le nombre des termes du tableau (3), c'est-à-dire par le produit ab . On pourra d'ailleurs évidemment remplacer le tableau (3) par le tableau (4); et, par conséquent, on peut énoncer la proposition suivante :

2^e Théorème. Les mêmes choses étant posées que dans le théorème 1^{er}, les dérivées des substitutions (1) et (2) formeront un nouveau système de substitutions qui seront toutes comprises dans le tableau (3), ainsi que dans le tableau (4); et l'ordre de ce système sera le produit ab des ordres a, b des systèmes (1) et (2), si ces derniers systèmes n'offrent pas de termes communs autres que l'unité.

On peut encore démontrer facilement la proposition suivante, qui peut être considérée comme réciproque du second théorème :

3^e Théorème. Soient

$$(1) \quad 1, P_1, P_2, \dots, P_{a-1},$$

$$(2) \quad 1, Q_1, Q_2, \dots, Q_{b-1},$$

deux systèmes de substitutions conjuguées, le premier de l'ordre a , le second de l'ordre b , qui n'offrent pas de termes communs autres que l'unité. Si les dérivées de ces deux systèmes forment un nouveau système de substitutions conjuguées, dont l'ordre se réduise au produit ab , toutes ces dérivées seront comprises dans chacun des tableaux (3) et (4), et, par conséquent, les systèmes (1) et (2) seront permutables entre eux.

Démonstration. En effet, dans l'hypothèse admise, chacun des tableaux (3), (4) se composera de termes qui seront tous distincts les uns des autres, et qui seront en nombre égal à celui des dérivées des substitutions (1) et (2). Donc il renfermera toutes ces dérivées, dont chacune sera tout à la fois de la forme $Q_k P_h$, et de la forme $P_h Q_k$.

Considérons maintenant le cas particulier où les divers termes de la suite (1) se réduisent aux diverses puissances

$$(6) \quad 1, P, P^2, \dots, P^{a-1}$$

d'une substitution P dont l'ordre est représenté par la lettre a , et où pareillement les divers termes de la suite (2) se réduisent aux diverses puissances

$$(7) \quad 1, Q, Q^2, \dots, Q^{a-1}$$

d'une substitution Q dont l'ordre est représenté par la lettre b . Alors, pour que le système des substitutions (6) soit permutable avec le système des substitutions (7), il suffira que les deux suites

$$(8) \quad Q, PQ, P^2Q, \dots, P^{a-1}Q,$$

et

$$(9) \quad Q, QP, QP^2, \dots, QP^{a-1}$$

offrent les mêmes termes rangés dans le même ordre ou dans deux ordres différents. En effet, cette condition étant supposée remplie, tout produit de la forme P^hQ sera en même temps de la forme $QP^{h'}$, le nombre h' pouvant être distinct du nombre h . Donc, par suite, tout produit de la forme

$$P^hQ^2 = P^hQQ$$

sera aussi de la forme

$$QP^{h'}Q,$$

et même de la forme

$$QQP^{h''} = Q^2P^{h''},$$

h'' pouvant être distinct de h et de h' . Généralement, toute substitution de la forme

$$P^hQ^k$$

pouvant être considérée comme le produit de k facteurs égaux à Q par le multiplicateur P^h , on pourra, sans altérer cette substitution, échanger successivement le facteur P^h avec chacun des facteurs égaux à Q , pourvu que chaque fois on modifie convenablement la valeur de l'exposant h ; et lorsque, en vertu de semblables échanges, les k facteurs égaux à Q auront été déplacés de manière à précéder tous les facteurs égaux à P , la substitution

$$P^hQ^k$$

se présentera évidemment sous la forme

$$Q^kP^h.$$

On peut donc énoncer la proposition suivante:

4^e Théorème. Soient

P, Q

deux substitutions distinctes, la première de l'ordre a , la seconde de l'ordre b .
Si les deux suites

$$Q, PQ, P^2Q, \dots, P^{a-1}Q,$$

$$Q, QP, QP^2, \dots, QP^{a-1}$$

offrent précisément les mêmes termes rangés dans le même ordre ou dans deux ordres différents, alors les deux systèmes des substitutions conjuguées

$$I, P, P^2, \dots, P^{a-1},$$

et

$$I, Q, Q^2, \dots, Q^{b-1},$$

formés, l'un avec les diverses puissances de P , l'autre avec les diverses puissances de Q , seront deux systèmes permutable entre eux.

De ce dernier théorème, joint aux 1^{er} et 2^e théorèmes, on déduit immédiatement la proposition suivante :

5^e Théorème. Les mêmes choses étant posées que dans le 4^e théorème, admettons, en outre, qu'aucune des substitutions

$$P, P^2, \dots, P^{a-1}$$

ne se retrouve parmi les substitutions

$$Q, Q^2, Q^{b-1},$$

en sorte que l'équation

$$P^h = Q^k$$

ne se vérifie jamais, excepté dans le cas où l'on a

$$P^h = I, \quad Q^k = I.$$

Alors toutes les dérivées des deux substitutions P, Q seront comprises dans chacune des formes

$$P^h Q^k, \quad Q^k P^h,$$

la valeur de k devant rester la même quand on passera de la première forme à la seconde; et, par suite, ces dérivées offriront un système de substitutions conjuguées dont l'ordre sera le produit ab .

Corollaire. Dans l'hypothèse admise, les diverses dérivées des substitu-

tions P, Q se confondront évidemment avec les divers termes du tableau

$$(10) \quad \left\{ \begin{array}{llll} I, & P, & P^2, \dots, & P^{a-1}, \\ Q, & PQ, & P^2Q, \dots, & P^{a-1}Q, \\ Q^2, & PQ^2, & P^2Q^2, \dots, & P^{a-1}Q^2, \\ \dots & \dots & \dots & \dots \\ Q^{b-1}, & PQ^{b-1}, & P^2Q^{b-1}, \dots, & P^{a-1}Q^{b-1}, \end{array} \right.$$

et aussi avec les divers termes du tableau

$$(11) \quad \left\{ \begin{array}{llll} I, & P, & P^2, \dots, & P^{a-1}, \\ Q, & QP, & QP^2, \dots, & QP^{a-1}, \\ Q^2, & Q^2P, & Q^2P^2, \dots, & Q^2P^{a-1}, \\ \dots & \dots & \dots & \dots \\ Q^{b-1}, & Q^{b-1}P, & Q^{b-1}P^2, \dots, & Q^{b-1}P^{a-1}, \end{array} \right.$$

§ XI. — Des substitutions arithmétiques et des substitutions géométriques.

Considérons n variables

$$x, y, z, \dots$$

Supposons, d'ailleurs, que l'on représente ces diverses variables par une même lettre n successivement affectée des indices

$$0, 1, 2, \dots, n-1;$$

et, en conséquence, à la place de

$$x, y, z, \dots$$

écrivons

$$(1) \quad x_0, x_1, x_2, \dots, x_{n-1}.$$

Enfin concevons que l'on regarde comme pouvant être indifféremment remplacés l'un par l'autre deux indices, dont la différence se réduit à un multiple de n ; en sorte qu'on ait, pour toute valeur entière positive ou même négative de l ,

$$\begin{aligned} x_l &= x_{l+n} = x_{l+2n} = \dots \\ &= x_{l-n} = x_{l-2n} = \dots \end{aligned}$$

Pour reproduire la suite (1), ou du moins les termes de cette suite rangés dans un nouvel ordre, il suffira d'ajouter aux indices de ces divers termes une

même quantité h , ou bien encore de multiplier ces indices par un même nombre r premier à n . Dans le premier cas, à la place de la série (1), on obtiendra la suivante

$$(2) \quad x_h, x_{h+1}, x_{h+2}, \dots, x_{h+n-1}.$$

Dans le second cas, au contraire, la série (1) sera remplacée par celle-ci

$$(3) \quad x_0, x_r, x_{2r}, \dots, x_{(n-1)r}.$$

Il est bon d'observer qu'un terme x_l de la série (1) correspond le terme x_{l+h} de la série (2), et que le *rapport arithmétique* des indices $l+h, l$,

qui affectent la lettre x dans ces deux termes, se réduit précisément à la constante h . Au contraire, au terme x_l de la série (1) correspond le terme x_{rl} de la série (3), et le *rapport géométrique* des indices

$$rl, l$$

qui affectent la lettre x dans ces deux termes, se réduit précisément à la constante r . Pour ce motif, en supposant, comme ci-dessus, que les variables données sont représentées par une seule lettre successivement affectée des indices

$$0, 1, 2, \dots, n-1,$$

nous appellerons *substitution arithmétique* la substitution qui consiste à remplacer chaque terme de la série (1) par le terme correspondant de la série (2), et nous appellerons, au contraire, *substitution géométrique* la substitution qui consiste à remplacer chaque terme de la série (1) par le terme correspondant de la série (3). Cela posé, la substitution arithmétique la plus simple sera la substitution circulaire

$$(4) \quad P = (x_0, x_1, x_2, \dots, x_{n-1}),$$

qui consiste à remplacer généralement x_l par x_{l+1} , et il suffira évidemment d'élever celle-ci à la puissance du degré h pour obtenir la substitution qui consiste à remplacer généralement x_l par x_{l+h} . Ainsi, la valeur de P étant déterminée par la formule (4), chaque terme de la série (1) se trouvera remplacé par le terme correspondant de la série (2) en vertu de la substitution circulaire ou régulière P^h .

Soit maintenant Q la progression géométrique qui consiste à remplacer



généralement le terme x_l de la série (1) par le terme correspondant x_{rl} de la série (3), en sorte qu'on ait

$$(5) \quad Q = \begin{pmatrix} x_0 x_r x_{2r} \dots x_{(n-1)r} \\ x_0 x_1 x_2 \dots x_{n-1} \end{pmatrix}.$$

Alors, k étant un nombre entier quelconque, la substitution Q^k sera celle qui consiste à remplacer la variable x_l par la variable $x_{r^k l}$; et, par suite, pour que l'on ait identiquement

$$(6) \quad Q^k = 1,$$

il faudra que l'on ait, quel que soit l ,

$$(7) \quad r^k l \equiv l, \pmod{n}.$$

D'ailleurs, r étant, par hypothèse, premier à n , la formule (7), que l'on peut écrire comme il suit:

$$(r^k - 1)l \equiv 0 \pmod{n},$$

donnera

$$r^k - 1 \equiv 0, \pmod{n},$$

ou, ce qui revient au même,

$$(8) \quad r^k \equiv 1, \quad (\text{mod. } n).$$

Donc l'équation (6) entraînera toujours la formule (8); et l'ordre i de la substitution géométrique Q , c'est-à-dire la plus petite des valeurs de k , pour lesquelles se vérifiera l'équation (6), sera en même temps la plus petite des valeurs de k pour lesquelles se vérifiera la formule (8).

n étant un nombre entier quelconque, et *r* l'un des nombres premiers à *n*, l'exposant *k* de la puissance à laquelle il faut éléver la *base r* pour obtenir un nombre équivalent, suivant le module *n*, à un reste donné, est ce qu'on nomme l'*indice* de ce reste. Cela posé, le nombre *i*, ou la plus petite des valeurs de *k* pour lesquelles se vérifie la formule (8), n'est évidemment autre chose que le plus petit des indices de l'unité. Ce même nombre *i* est encore celui qui indique combien l'on peut obtenir de restes différents en divisant par *n* les termes de la progression géométrique

$$1, \ r, \ r^2, \ r^3, \dots,$$

et qui, pour cette raison, a été désigné, dans un précédent Mémoire, sous le nom d'*indicateur*. En conséquence, on peut énoncer la proposition suivante :

1^{er} *Théorème.* n étant un nombre entier quelconque, et r étant l'un des nombres premiers à n , l'ordre de la substitution géométrique Q , déterminée par la formule (8), se confond avec l'indicateur i relatif à la base r .

Concevons à présent que, h, k étant deux nombres entiers quelconques, on forme, avec les variables

$$x_0, x_1, x_2, \dots, x_{n-1},$$

les trois substitutions

$$P^h, Q^k \text{ et } Q^k P^h.$$

Ces substitutions consisteront évidemment, la première à remplacer l'indice l d'une variable quelconque par l'indice $l+h$, la deuxième à remplacer l'indice l par l'indice $r^k l$, et la troisième à remplacer l'indice l par l'indice

$$r^k(l+h).$$

Au contraire, h' étant un entier distinct de h , la substitution

$$P^{h'} Q^k$$

consisterait à remplacer l'indice l d'une variable quelconque par l'indice

$$h' + r^k l.$$

Donc on aura généralement

$$(9) \quad Q^k P^h = P^{h'} Q^k,$$

si l'on a

$$h' + r^k l = r^k(l+h),$$

ou, ce qui revient au même, si l'on a

$$h' = r^k h.$$

Mais alors l'équation (9) donnera

$$Q^k P^h = P^{r^k h} Q^k,$$

et il est d'ailleurs facile de s'assurer que cette dernière formule s'étend à des valeurs entières quelconques non-seulement positives, mais encore négatives de h . On peut donc énoncer généralement la proposition suivante :

2^e *Théorème.* Représentons n variables distinctes par une même lettre x successivement affectée des indices

$$0, 1, 2, \dots, n-1,$$

et concevons que l'on regarde comme pouvant être indifféremment remplacés l'un par l'autre deux indices dont la différence se réduit à un multiple de n . Soit d'ailleurs r un nombre entier, premier à n . Enfin soient

$$P, Q$$

deux substitutions, l'une arithmétique, l'autre géométrique, déterminées par les formules (4) et (5), c'est-à-dire deux substitutions qui consistent, la première à remplacer l'indice l d'une variable quelconque par l'indice $l + 1$, la seconde à remplacer l'indice l par l'indice rl . Alors on aura, pour des valeurs entières quelconques de h , et pour des valeurs entières et positives de k ,

$$(10) \quad Q^k P^h = P^{rh} Q^k.$$

Corollaire 1^{er}. Poser l'équation (10), c'est dire que l'équation (9), savoir,

$$Q^k P^h = P^{h'} Q^k,$$

subsiste quand les exposants h, h' vérifient la condition

$$h' = r^k h.$$

D'ailleurs, de cette dernière formule, combinée avec l'équation

$$r^i \equiv 1, \quad (\text{mod. } n),$$

on tire, en supposant $k < i$,

$$r^i h' \equiv r^k h \quad (\text{mod. } n),$$

ou, ce qui revient au même,

$$h \equiv r^{i-k} h' \quad (\text{mod. } n),$$

et plus généralement, en désignant par i' un multiple de i supérieur à k ,

$$h \equiv r^{i'-k} h', \quad (\text{mod. } n).$$

Donc, poser l'équation (10), c'est dire encore que l'équation (9) subsiste quand les exposants h, h' vérifient la condition

$$h = r^{i'-k} h'.$$

Il résulte de ces observations qu'on peut, dans la formule (9), choisir arbitrairement l'un quelconque des exposants h, h' . Il en résulte aussi que tout produit de la forme

$$Q^k P^h$$

est en même temps de la forme

$$P^h Q^k,$$

et réciproquement, la valeur de l'exposant h devant seule varier quand on passe d'une forme à l'autre. Donc, en vertu de l'équation (9), les diverses puissances de P , savoir,

$$(11) \quad 1, P, P^2, \dots, P^{n-1},$$

offrent un système de substitutions permutable avec le système des substitutions

$$(12) \quad 1, Q, Q^2, \dots, Q^{i-1},$$

qui représentent les diverses puissances de Q .

Corollaire 2^e. Il est bon d'observer encore que la substitution arithmétique P et celles de ses puissances qui ne se réduisent pas à l'unité, déplacent les n variables données

$$x_0, x_1, x_2, \dots, x_{n-1}.$$

Au contraire, la substitution géométrique Q , déterminée par la formule (5), ou, ce qui revient au même, par la suivante

$$(13) \quad Q = \begin{pmatrix} x_0 x_2 \dots x_{\frac{n-1}{2}} \\ x_1 x_3 \dots x_{\frac{n-1}{2}} \end{pmatrix},$$

laisse immobiles la variable x_0 quand n est un nombre impair, et les deux variables $x_0, x_{\frac{n}{2}}$ quand n est un nombre pair. La même propriété devant évidemment appartenir à celles des puissances de Q qui diffèrent de l'unité, il est clair que les deux substitutions

$$P, Q$$

ne pourront jamais vérifier la formule

$$P^h = Q^k,$$

excepté dans le cas où l'on aura

$$P^h = 1, \quad Q^k = 1.$$

Corollaire 3^e. Les deux corollaires précédents, joints au 3^e théorème du § X, entraînent évidemment la proposition suivante :

3^e Théorème. Les mêmes choses étant posées que dans le 2^e théorème,

les dérivées des deux substitutions P, Q seront toutes comprises sous chacune des deux formes

$$P^h Q^k, \quad Q^k P^h,$$

et composeront un système de substitutions conjuguées qui sera d'un ordre représenté par le produit

$$ni,$$

i étant l'indicateur correspondant à la base r , c'est-à-dire la plus petite des valeurs de k propres à vérifier la formule (8).

Nota. On arriverait encore aux mêmes conclusions en observant qu'il suffit de poser $k = 1$ dans l'équation (10) pour obtenir la formule

$$(14) \quad QP^h = P^{rh} Q.$$

Or, il résulte de cette dernière formule que les deux suites

$$Q, \quad PQ, \quad P^2 Q, \dots, \quad P^{n-1} Q,$$

$$Q, \quad QP, \quad Q^2 P, \dots, \quad QP^{n-1}$$

offrent les mêmes termes, rangés seulement dans deux ordres différents. Cela posé, il est clair que le 3^e théorème sera une conséquence immédiate du 5^e théorème du § X.

Soit maintenant a un diviseur de n , distinct de l'unité; et posons

$$(15) \quad \nu = \frac{n}{a},$$

$$(16) \quad R = P^a.$$

R sera précisément la substitution arithmétique qui consiste à remplacer x_l par $x_{l+\frac{n}{a}}$, ou, ce qui revient au même, par x_{l+a} . D'ailleurs on tirera de l'équation (10), en y remplaçant h par ah , et ayant égard à la formule (16),

$$(17) \quad Q^k R^h = R^{rh} Q^k.$$

Enfin, comme la substitution R et ses puissances d'un degré inférieur à ν déplaceront toutes les variables données, tandis que la substitution Q et ses puissances d'un degré inférieur à i laissent immobile au moins la variable x_0 , il est clair que les deux suites

$$1, \quad P, \quad P^2, \dots, \quad P^{n-1},$$

$$1, \quad Q, \quad Q^2, \dots, \quad Q^{i-1}$$

n'offriront pas de termes communs autres que l'unité. Cela posé, des raisonnements semblables à ceux dont nous avons fait usage pour établir le 3^e théorème suffiront pour déduire de la formule (17) la proposition suivante :

4^e *Théorème.* Les mêmes choses étant posées que dans le 2^e théorème, nommons v un diviseur de n distinct de l'unité, et soit R la substitution arithmétique qui consiste à remplacer généralement x_i par x_{i+v} . Les dérivées des deux substitutions R , Q seront toutes comprises sous chacune des deux formes

$$Q^k R^h, \quad R^h Q^k,$$

et composeront un système de substitutions conjuguées qui sera d'un ordre représenté par le produit

$$v i.$$

Appliquons maintenant les théorèmes que nous venons d'établir à quelques exemples.

Supposons d'abord $n = 7$, $r = 3$. Alors les deux substitutions P , Q , déterminées par les formules

$$(18) \quad P = (x_0, x_1, x_2, x_3, x_4, x_5, x_6),$$

$$(19) \quad Q = (x_1, x_3, x_2, x_6, x_4, x_5),$$

seront, la première du septième ordre, la seconde du sixième ordre. On aura donc $i = 6$; et, en effet, le nombre 7 étant pris pour module, 6 sera l'indicateur correspondant à la base $r = 3$, puisque, dans la progression géométrique

$$3, 3^2, 3^3, 3^4, 3^5, 3^6, \dots,$$

3^6 sera le premier terme qui, divisé par 7, donne pour reste l'unité. Cela posé, on conclura du 3^e théorème, que les substitutions arithmétique et géométrique P , Q , déterminées par les formules (18), (19), composent, avec leurs dérivées, un système dont l'ordre est représenté par le produit

$$6 \cdot 7 = 42.$$

Supposons en second lieu $n = 7$, $r = 2$. Alors la substitution géométrique Q , déterminée, non plus par la formule (19), mais par la suivante

$$(20) \quad Q = (x_1, x_2, x_4) (x_3, x_6, x_5),$$

sera du troisième ordre. On aura donc $i = 3$; et, en effet, le nombre 7 étant pris pour module, 3 sera l'indicateur correspondant à la base 2, puis-

que, dans la progression géométrique

$$2, 2^2, 2^3, \dots$$

$2^3 = 8$ sera le premier terme qui, divisé par 7, donne pour reste l'unité. Cela posé, on conclura du 3^e théorème, que les substitutions arithmétique et géométrique P, Q, déterminées par les formules (18) et (20), composent, avec leurs dérivées, un système dont l'ordre est représenté par le produit

$$3 \times 7 = 21.$$

Supposons encore $n = 9$, $r = 2$. Alors les deux substitutions P, Q, déterminées par les formules

$$(21) \quad P = (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8),$$

$$(22) \quad Q = (x_1, x_2, x_4, x_8, x_5) (x_3, x_6),$$

seront, la première du neuvième ordre, la seconde du sixième ordre. On aura donc $i = 6$; et, en effet, le nombre 9 étant pris pour module, 6 sera l'indicateur correspondant à la base 2, puisque, dans la progression géométrique

$$2, 2^2, 2^3, 2^4, 2^5, 2^6, \dots$$

$2^6 = 64$ sera le premier terme qui, divisé par 9, donne pour reste l'unité. Cela posé, on conclura du 3^e théorème, que les deux substitutions arithmétique et géométrique P, Q, déterminées par les formules (21) et (22), composent, avec leurs dérivées, un système dont l'ordre est représenté par le produit

$$6 \cdot 9 = 54.$$

Supposons enfin qu'à la substitution Q, déterminée par la formule (22), on joigne, non plus la substitution P, déterminée par la formule (21), mais la substitution R, dont la valeur est fournie par l'équation

$$(23) \quad R = P^3,$$

ou, ce qui revient au même, par la suivante

$$(24) \quad R = (x_0, x_3, x_6) (x_1, x_4, x_7) (x_2, x_5, x_8).$$

Alors R sera une substitution arithmétique de l'ordre

$$\frac{n}{3} = 3,$$

et l'on conclura du 4^e théorème que les substitutions arithmétique et géomé-

trique Q , R , déterminées par les formules (22) et (24), composent, avec leurs dérivées, un système dont l'ordre est représenté par le produit

$$3 \cdot 9 = 27.$$

Pour un module quelconque n , l'indicateur i dépend de la base r , et devient un *maximum* quand cette base r est une *racine primitive* correspondante au module n . Si l'on nomme I cet indicateur maximum, chacun des indicateurs qui correspondront aux diverses bases représentées par les divers nombres premiers à n sera égal à I ou à un diviseur de I . D'ailleurs, si l'on suppose

$$n = p^f q^g \dots,$$

p et q étant les facteurs premiers de n , l'indicateur maximum I sera le plus petit nombre entier divisible à la fois par chacun des produits

$$p^{f-1} (p-1), \quad q^{g-1} (q-1), \dots,$$

l'un de ces produits, savoir, celui qui répondra au facteur 2, devant être remplacé par sa moitié quand n sera pair et divisible par 8.

Si n se réduit à une puissance d'un nombre premier et impair p , en sorte qu'on ait

$$n = p^f,$$

on trouvera

$$I = p^{f-1} (p-1) = n \left(1 - \frac{1}{p}\right).$$

Si n se réduit à un nombre premier p , on aura simplement

$$I = n - 1.$$

Eu égard aux remarques qu'on vient de faire, les 3^e et 4^e théorèmes entraîneront évidemment les propositions suivantes :

5^e *Théorème.* Les mêmes choses étant posées que dans le 2^e théorème, si l'on nomme r une des racines primitives correspondantes au module n , et I l'indicateur maximum relatif à ce module, c'est-à-dire le plus petit des indices de l'unité correspondants à la base r , la substitution géométrique Q , qui aura pour objet de remplacer généralement x_l par x_{rl} , sera de l'ordre I . Alors aussi les dérivées des deux substitutions P , Q seront toutes comprises sous chacune des deux formes

$$Q^k P^h, \quad P^h Q^k,$$

et composeront un système dont l'ordre sera représenté par le produit

$$nI.$$

Corollaire. Si n est un nombre premier, on aura simplement Q suivant

$$1 = n - 1,$$

et, par suite, les dérivées des deux substitutions

P, Q

composeront un système dont l'ordre sera représenté par le produit

$$n(n - 1).$$

6^e Théorème. Les mêmes choses étant posées que dans le 5^e théorème, soit v un diviseur de n autre que l'unité, et nommons R la substitution arithmétique qui consiste à remplacer généralement x_l par x_{l+v} . Les dérivées des deux substitutions Q, R seront toutes comprises sous chacune des deux formes

$Q^k R^h, R^h Q^k,$

et composeront un système dont l'ordre sera exprimé par le produit

$v I.$

Au lieu de représenter les diverses variables par une même lettre successivement accompagnée d'indices divers, on pourrait continuer à les représenter par différentes lettres

x, y, z, \dots

puis assigner à chaque variable un numéro propre à indiquer, ou le rang qu'elle occupe dans la série de ces lettres écrites à la suite l'une de l'autre, suivant un ordre déterminé, ou, mieux encore, ce même rang diminué de l'unité. Alors la substitution désignée par Q dans les théorèmes précédents serait celle qui consiste à remplacer la variable correspondante au numéro l par la variable correspondante au numéro rl , ou plutôt au numéro équivalent au reste de la division du produit rl par le nombre l .

Supposons, pour fixer les idées, $n = 5$; alors cinq variables représentées par les lettres

x, y, z, u, v pourront être censées correspondre aux numéros

0, 1, 2, 3, 4.

Alors aussi, en multipliant les quatre derniers numéros par le facteur r , on

obtiendra les produits

$$r, 2r, 3r, 4r;$$

et, si l'on pose $r=2$, ces produits, divisés par 5, donneront pour restes

$$2, 4, 1, 3.$$

Ainsi, dans cette hypothèse, la substitution désignée par Q aura pour effet de substituer aux variables dont les numéros étaient

$$1, 2, 3, 4, 9 \quad (8a)$$

les variables dont les numéros sont

$$2, 4, 1, 3, \quad Q^2 = 9Q \quad (8b)$$

c'est-à-dire de substituer aux variables

$$\gamma, z, u, v$$

les variables

$$z, v, \gamma, u. \quad (8c)$$

On aura donc

$$Q = (\gamma, z, v, u). \quad (8d)$$

Cela posé, on conclura du 2^e théorème, que les dérivées des deux substitutions

$$(25) \quad P = (x, \gamma, z, u, v), \quad Q = (\gamma, z, v, u)$$

sont toutes comprises sous chacune des formes

$$P^h Q^k, \quad Q^k P^h,$$

et que l'ordre du système de ces dérivées est égal au produit

$$5 \cdot 4 = 20$$

des nombres 5 et 4 qui représentent les ordres des substitutions P et Q . Effectivement les dérivées des substitutions P, Q dont les valeurs sont données par les formules (25) se réduiront aux vingt substitutions comprises dans le tableau

$$(26) \quad \left\{ \begin{array}{l} 1, \quad P, \quad P^2, \quad P^3, \quad P^4, \\ Q, \quad QP, \quad QP^2, \quad QP^3, \quad QP^4, \\ Q^2, \quad Q^2P, \quad Q^2P^2, \quad Q^2P^3, \quad Q^2P^4, \\ Q^3, \quad Q^3P, \quad Q^3P^2, \quad Q^3P^3, \quad Q^3P^4, \end{array} \right.$$

ou, ce qui revient au même, dans le suivant :

$$(27) \quad \left\{ \begin{array}{l} 1, \quad (x, y, z, u, v), (x, z, v, y, u), (x, u, y, v, z), (x, v, u, z, y), \\ (y, z, v, u), (v, x, z, y), (z, u, x, v), (x, y, u, z), (u, v, y, x), \\ (y, v) (z, u), (u, y) (v, x), (x, u) (y, z), (z, x) (u, v), (v, z) (x, y), \\ (y, x, v, z), (z, v, x, u), (u, x, y, v), (v, y, z, x), (x, z, u, y), \end{array} \right.$$

Ajoutons qu'en vertu de la formule (10), on aura généralement

$$(28) \quad Q^k P^h = P^{2k} Q^h,$$

et, par suite,

$$(29) \quad \left\{ \begin{array}{l} QP = P^2 Q, \quad QP^2 = P^4 Q, \quad QP^3 = PQ, \quad QP^4 = P^3 Q, \\ Q^2 P = P^4 Q^2, \quad Q^2 P^2 = P^3 Q^2, \quad Q^2 P^3 = P^2 Q^2, \quad Q^2 P^4 = PQ^2, \\ Q^3 P = P^3 Q^3, \quad Q^3 P^2 = PQ^3, \quad Q^3 P^3 = P^4 Q^3, \quad Q^3 P^4 = P^2 Q^3. \end{array} \right.$$

§ XII. — *Sur diverses propriétés remarquables des systèmes de substitutions conjuguées.*

Considérons n variables

$$x, y, z, \dots$$

Le nombre total N des arrangements, ou bien encore des substitutions que l'on pourra former avec ces variables, sera représenté par le produit

$$N = 1 \cdot 2 \cdot 3 \dots n;$$

et l'un quelconque des systèmes de substitutions conjuguées formés avec ces mêmes variables, sera toujours d'un ordre exprimé par un diviseur de N . De plus, ces systèmes jouiront encore de diverses propriétés remarquables dont quelques-unes ont été déjà établies dans le § VI. Je vais maintenant en démontrer quelques autres, qui se trouvent exprimées par les théorèmes suivants.

1^{er} *Théorème.* Formons avec n variables

$$x, y, z, \dots$$

deux systèmes de substitutions conjuguées; et soient

$$(1) \quad 1, P_1, P_2, \dots, P_{a-1},$$

$$(2) \quad 1, Q_1, Q_2, \dots, Q_{b-1},$$

ces deux systèmes, le premier de l'ordre a , le second de l'ordre b . Soit d'ail-

leurs I le nombre des substitutions R pour lesquelles se vérifient des équations symboliques et linéaires de la forme

$$(3) \quad RP_h = Q_k R,$$

h étant l'un quelconque des entiers

$$1, 2, \dots, a-1,$$

et k l'un quelconque des entiers

$$1, 2, \dots, b-1.$$

Le nombre I , divisé par le produit ab , fournira le même reste que le nombre

$$N = 1 \cdot 2 \cdot 3 \dots n,$$

et l'on aura, en conséquence,

$$(4) \quad I = N \pmod{ab}.$$

Démonstration. Faisons, pour abréger,

$$(5) \quad J = N - I.$$

Parmi les substitutions que l'on pourra former avec x, y, z, \dots , celles pour lesquelles ne se vérifieront jamais des équations semblables à la formule (3) seront en nombre égal à J . Nommons U l'une de ces dernières substitutions.

Les divers termes du tableau

$$(6) \quad \left\{ \begin{array}{llll} U, & UP_1, & UP_2, \dots, & UP_{a-1}, \\ Q_1 U, & Q_1 UP_1, & Q_1 UP_2, \dots, & Q_1 UP_{a-1}, \\ Q_2 U, & Q_2 UP_1, & Q_2 UP_2, \dots, & Q_2 UP_{a-1}, \\ \dots & \dots & \dots & \dots \\ Q_{b-1} U, & Q_{b-1} UP_1, & Q_{b-1} UP_2, \dots, & Q_{b-1} UP_{a-1} \end{array} \right.$$

seront tous inégaux entre eux. Car, si l'on avait

$$Q_k UP_h = Q_{k'} UP_{h'},$$

et, par suite,

$$(7) \quad UP_h P_h^{-1} = Q_k^{-1} Q_{k'} U,$$

sans avoir en même temps

$$P_h = P_{h'} \quad \text{et} \quad Q_k = Q_{k'},$$

on réduirait l'équation (5) à la forme

$$(8) \quad U^{\mathcal{Q}} = \mathcal{Q}U,$$

en posant

$$\mathcal{Q} = P_h P_{h'}^{-1}, \quad \mathcal{Q} = Q_{h'}^{-1} Q_h.$$

Mais alors, des deux substitutions \mathcal{Q}, \mathcal{Q} , dont l'une au moins serait distincte de l'unité, la première représenterait encore un terme de la série (1), et la seconde un terme de la série (2). Donc la formule (7) ou (8), considérée comme propre à déterminer U , serait semblable à l'équation (3), et la substitution U se réduirait, contre l'hypothèse admise, à l'une des valeurs de R .

Soit maintenant V une substitution nouvelle qui, étant formée avec les variables x, y, z, \dots , ne se réduise ni à l'une des valeurs de R , ni à aucune des substitutions comprises dans le tableau (6). Les divers termes du tableau

$$(9) \quad \left\{ \begin{array}{llll} V, & VP_1, & VP_2, \dots, & VP_{a-1}, \\ Q_1 V, & Q_1 VP_1, & Q_1 VP_2, \dots, & Q_1 VP_{a-1}, \\ Q_2 V, & Q_2 VP_1, & Q_2 VP_2, \dots, & Q_2 VP_{a-1}, \\ \dots & \dots & \dots & \dots \\ Q_{b-1} V, & Q_{b-1} VP_1, & Q_{b-1} VP_2, \dots, & Q_{b-1} VP_{a-1} \end{array} \right.$$

seront encore tous inégaux entre eux, et même ils seront distincts de tous ceux que renferme le tableau (6); car, si l'on avait

$$Q_h UP_h = Q_{h'} VP_{h'},$$

on en conclurait

$$(10) \quad V = Q_{h'}^{-1} Q_h UP_h P_{h'}^{-1};$$

puis, en posant, pour abréger,

$$\mathcal{Q} = P_h P_{h'}^{-1}, \quad \mathcal{Q} = Q_{h'}^{-1} Q_h,$$

on réduirait l'équation (9) à la formule

$$(11) \quad V = \mathcal{Q}U\mathcal{Q};$$

et, comme les deux produits \mathcal{Q}, \mathcal{Q} représenteraient encore, le premier un terme de la série (1), le second un terme de la série (2), il est clair qu'en vertu de la formule (11), V se réduirait, contre l'hypothèse admise, à l'un des termes renfermés dans le tableau (6).

En continuant de la sorte, on répartira les J substitutions, pour lesquelles ne se vérifieront jamais des équations semblables à la formule (3), entre plu-

sieurs tableaux que l'on déduira successivement du tableau (6), en remplaçant dans celui-ci la substitution U , qui représente le premier terme, par une autre substitution V , ou W , etc. D'ailleurs, les termes qui se trouveront renfermés dans chaque tableau, en nombre équivalent au produit ab , seront tous inégaux entre eux. Il y a plus : les termes que comprendra le système des divers tableaux seront encore tous distincts les uns des autres, si l'on a soin de prendre pour premier terme de chaque nouveau tableau une substitution non comprise dans les tableaux déjà formés. Cette condition étant supposée remplie, le nombre total des termes compris dans les divers tableaux sera nécessairement le nombre représenté par J . Donc le nombre J ou $N - I$ sera un multiple du nombre des termes renfermés dans chaque tableau, c'est-à-dire du produit ab . Donc les nombres I et N , divisés par le produit ab , fourniront le même reste.

Corollaire. Si les deux systèmes de substitutions conjuguées, mentionnés dans le 1^{er} théorème, se réduisent à un seul, alors, à la place de ce théorème, on obtiendra la proposition suivante :

2^e *Théorème.* Soit a l'ordre d'un système de substitutions conjuguées

$$1, P_1, P_2, \dots, P_{a-1},$$

formées avec les n variables

$$x, y, z, \dots;$$

et nommons I le nombre des substitutions R pour lesquelles se vérifient des équations de la forme

$$(12) \quad RP_h = P_k R,$$

h, k étant des nombres entiers égaux ou inégaux, pris dans la suite

$$0, 1, 2, \dots, a-1.$$

Le nombre I , divisé par le carré de a , fournira le même reste que le produit

$$N = 1 \cdot 2 \cdot 3 \cdots n,$$

en sorte qu'on aura

$$(13) \quad I \equiv N, \pmod{a^2}.$$

Corollaire. Si a^2 surpassé N , la formule (13) donnera nécessairement

$$(14) \quad I = N,$$

et, par suite, une substitution quelconque R sera du nombre de celles pour lesquelles peut se vérifier l'équation (12).

Revenons maintenant à la formule (3). Cette formule exprime évidemment que les deux substitutions

$$P_h, Q_k,$$

dont la première est l'un des termes qui suivent l'unité dans la série (1), et la seconde l'un des termes qui suivent l'unité dans la série (2), sont semblables l'une à l'autre. Donc il sera impossible de satisfaire à l'équation (3) si aucune des substitutions

$$P_1, P_2, \dots, P_{a-1}$$

n'est semblable à l'une des substitutions

$$Q_1, Q_2, \dots, Q_{b-1}.$$

Donc alors on aura

$$I = 0,$$

et la formule (4), réduite à celle-ci

$$(15) \quad N \equiv 0, \pmod{ab},$$

exprimera que le nombre N est divisible par le produit ab . En conséquence, on peut énoncer la proposition suivante :

3^e *Théorème.* Formons avec n variables

$$x, y, z, \dots$$

deux systèmes de substitutions conjuguées, et supposons que ces deux systèmes étant, le premier de l'ordre a , le second de l'ordre b , renferment, outre l'unité, d'une part, les substitutions

$$(16) \quad P_1, P_2, \dots, P_{a-1},$$

d'autre part, les substitutions

$$(17) \quad Q_1, Q_2, \dots, Q_{b-1}.$$

Si aucune des substitutions (16) n'est semblable à l'une des substitutions (17), le nombre

$$N = 1 \cdot 2 \cdot 3 \dots n$$

sera divisible par le produit ab .

Le théorème que nous venons d'énoncer entraîne encore évidemment la proposition suivante :

4^e Théorème. Soient $1, P_1, P_2, \dots, P_{a-1}$, et

$$1, Q_1, Q_2, \dots, Q_{b-1}$$

deux systèmes de substitutions conjuguées, le premier de l'ordre a , le second de l'ordre b , formés l'un et l'autre avec les n variables

$$x, y, z, \dots$$

Si le produit ab n'est pas un diviseur du nombre

$$N = 1 \cdot 2 \cdot 3 \dots n,$$

alors, des substitutions

$$P_1, P_2, \dots, P_{a-1},$$

une ou plusieurs seront semblables à une ou plusieurs des substitutions

$$Q_1, Q_2, \dots, Q_{b-1}.$$

Corollaire 1^{er}. Soient maintenant p un nombre premier, égal ou inférieur à n , et p^f la plus haute puissance de p qui divise le produit

$$N = 1 \cdot 2 \cdot 3 \dots n.$$

D'après ce qui a été dit dans le § VII (page 196), on pourra former avec les n variables x, y, z, \dots un système de substitutions primitives et conjuguées qui sera de l'ordre p^f ; et rien n'empêchera de supposer que l'on prend ces mêmes substitutions pour termes de la suite

$$1, Q_1, Q_2, \dots, Q_{b-1}.$$

Or, dans cette hypothèse, b étant égal à p^f , le produit ab ne pourra diviser N si a est divisible par p ; et, d'ailleurs, chacune des substitutions

$$Q_1, Q_2, \dots, Q_{b-1},$$

étant une substitution primitive dont l'ordre sera représenté par l'un des nombres

$$p, p^2, \dots, p^f,$$

aura pour dérivées d'autres termes de la suite

$$1, Q_1, Q_2, \dots, Q_{b-1},$$

parmi lesquels (*voir le 8^e théorème du § VIII*) on trouvera au moins une substitution régulière de l'ordre p . Donc, en vertu du 4^e théorème, si l'ordre α du système de substitutions

$$1, P_1, P_2, \dots, P_{\alpha-1}$$

est divisible par le nombre premier p , l'une au moins des substitutions

$$P_1, P_2, \dots, P_{\alpha-1}$$

sera régulière et de l'ordre p .

Corollaire 2^e. Si l'on représente par des lettres diverses

$$P, Q, R, \dots$$

les substitutions qui, dans le 4^e théorème, sont désignées à l'aide d'une seule lettre P successivement affectée des indices

$$1, 2, 3, \dots, \alpha - 1,$$

et si, d'ailleurs, on nomme M l'ordre du système des substitutions conjuguées

$$1, P, Q, R, \dots,$$

alors la proposition établie dans le corollaire 1^{er} sera réduite à celle dont voici l'énoncé.

5^e Théorème. Soit M l'ordre du système des substitutions conjuguées (18) $1, P, Q, R, \dots$

formées avec les n variables x, y, z, \dots ; et nommons p un nombre premier égal ou inférieur à n . Si M est divisible par p , l'une au moins des substitutions

P, Q, R, \dots sera une substitution régulière de l'ordre p .

Corollaire. Lorsque le nombre premier p devient supérieur à $\frac{n}{2}$, une substitution régulière et de l'ordre p , formée avec les n variables x, y, z, \dots , ne peut être qu'une substitution circulaire. Donc le 7^e théorème entraîne encore la proposition suivante :

6^e Théorème. Soit M l'ordre du système des substitutions conjuguées

$$1, P, Q, R, \dots,$$

formées avec les n variables x, y, z, \dots , et nommons p un nombre premier égal ou inférieur à n , mais supérieur à $\frac{n}{2}$. Si M est divisible par p , l'une au moins des substitutions

P, Q, R, \dots

sera une substitution circulaire de l'ordre p .

Pour montrer une application du 6^e théorème, supposons que, n étant égal à 5, les variables données soient

x, y, z, u, v .

Au module 5 correspondront, d'une part, les racines primitives 2 et 3, d'autre part, l'indicateur *maximum*

$$n - 1 = 4,$$

dont les diviseurs

$$1, 2, 4$$

représenteront les divers indicateurs correspondants à des bases quelconques; et l'on conclura du troisième des théorèmes démontrés dans le § XI, qu'avec cinq variables on peut former non-seulement une substitution circulaire du cinquième ordre, mais encore un système de substitutions conjuguées dont l'ordre soit représenté par le produit

$$5 \times 2 = 10,$$

ou par le produit

$$5 \times 4 = 20.$$

Ainsi, en particulier, on pourra former, avec les cinq variables x, y, z, u, v , le système du vingtième ordre que composent les substitutions écrites dans le tableau (27) de la page 244. Cela posé, il résultera immédiatement du 6^e théorème, que tout système du dixième ou du vingtième ordre, formé avec les cinq variables x, y, z, u, v , comprendra, comme le système dont il est ici question, des substitutions régulières dont les ordres seront représentés par les facteurs premiers des nombres 10 et 20, c'est-à-dire des substitutions circulaires du cinquième ordre et des substitutions régulières du deuxième ordre.

D'après ce qu'on a vu dans le § VI (2^e théorème), l'ordre M d'un système de substitutions conjuguées

$1, P, Q, R, \dots$

est divisible par l'ordre de chacune des substitutions P, Q, R, \dots , et en con-