Évariste Galois's last mathematical testament in the form of a letter to his friend Auguste Chevallier is reproduced here in English translation[1]. On May 29, 1832, in the evening before the fatal duel, Galois who was certain of his death in the duel penned this letter (along with letters of more personal character to many of his republican friends who were unaware of the duel). As Galois had wished, Chevallier got the letter published in September 1832 but the letter did not receive the attention it deserved. It was only in September 1843 that Liouville, who prepared Galois's papers for publication, announced to the Academy that Galois had solved the problem of solvability of equations by radicals. But the publication of the celebrated paper of 1831 was delayed till 1846. At the same time in a series of papers during 1844– 46 Cauchy went back to his studies on groups which he had abandoned in 1815. This helped to clarify Galois's ideas and the significance of his work began to be appreciated. Many unpublished manuscript fragments were edited and published by J Tannery in 1907. Finally, in 1961 R Bourgne and J P Azra edited a critical collection uniting all of Galois's writings – papers, letters and rough drafts of his articles.

The Last Mathematical Testament of Galois

My dear friend,

I have analysed several new ideas. One concerning the theory of equations; the other, integral functions.

In the theory of equations, I have studied as to in which cases the equations are solvable by radicals, which has provided me with an opportunity to go into this theory in depth and describe all possible transformations on an equation, even when it is not solvable by radicals.

All this can be put in three papers.

The first one is written, and, in spite of what Poisson has said, I stand by it, with the corrections that I have indicated.

The second contains rather interesting applications from the theory of equations. Here is a summary of the most important ones:

1. According to the propositions II and III of the first paper, one sees a great difference between adjoining, to an equation, one of the roots or all the roots of

[1] Translated by Anita R Singh, Foreign Languages Section and C S Yogananda, MO Cell (NBHM), Department of Mathematics, IISc, Bangalore560 012, India.

an auxiliary equation.

In both the cases, the group of the equation can be partitioned by adjunction into groups such that one can pass from one to another by a self-transformation; but the condition that these groups have the same substitutions holds only in the second case. This is called *proper decomposition.*

In other words, when a group G contains another, H, the group G can be partitioned into groups each of which is obtained by operating on the permutations in H a self-transformation, in such a way that,

$$G = H + HS + HS' + \cdot\cdot$$

And we can also partition into groups which have all similar substitutions, such that

$$G = H + TH + T'H +$$

These two types of decompositions generally do not coincide. When they do coincide the decomposition is said to be *proper.*

It is easy to see that, when the group of an equation is not susceptible to any proper decomposition, however well we might have transformed this equation, the groups of the transformed equations will always have the same number of permutations.

On the contrary, when the group of an equation is susceptible to a proper decomposition in such a way that we can decompose it into M groups of N permutations, we can resolve the given equation by means of two equations: one will have a group of M permutations and the other, one of N permutations.

Hence when we would have exhausted all possible proper decompositions on the group of an equation, we arrive at groups which can be transformed but for which the number of permutations will always be the same.

If each of these groups has a prime number of permutations then the equation will be solvable by radicals; otherwise, not.

The smallest number of permutations that an indecomposable group can have, when this number is not a prime number, is 5 $4 \cdot 3$.

2. The simplest decompositions are those which have been treated by the method of Gauss.

As these decompositions are evident, even in the present form of the group of the equation, it is needless to spend more time on this subject.

Which decompositions are feasible on an equation which cannot be simplified by the method of Gauss?

I have called equations which cannot be simplified by the method of Gauss as *primitive*; not that these equations are really indecomposable since they may even be solvable by radicals.

As a lemma to the theory of primitive equations solvable by radicals, I have dealt with in June 1830, in the *Bulletin de Ferussac*, an analysis of the imaginary numbers in the theory of numbers.

One will find enclosed proof of the following theorems:

1. For a primitive equation to be solvable by radicals it should be of degree p^ν, p being prime.

2. All the permutations of such an equation are of the form

$$x_{k,l,m,\ldots} \mid x_{ak+bl+cm+\ldots+h, a'k+b'l+c'm+\ldots+h', a''k+\ldots,\ldots},$$

$k, l, m, .$ being ν indices, which, each taking p values, denote all the roots. The indices are taken modulo p; that is to say, the roots will be the same when a multiple of p is added to an index.

The group which we obtain by operating all the substitutions of this linear form contains, in all,

$$p^\nu(p^\nu - 1)(p^\nu - p)\cdots(p^\nu - p^{\nu-1})$$

permutations.

It is far from being true that in this generality, the equations which they represent will be solvable by radicals.

The condition that I have indicated in the *Bulletin de Ferussac* for an equation to be solvable by radicals is very restricted; there are a few exceptions, but there are.

The last application of the theory of equations is related to the modular equation of elliptic functions.

We show that the group of the equation which has for roots the sine of the amplitude of $p^2 - 1$ divisions of a period is:

$$x_{k\cdot l} \quad x_{ak+bl|ck+dl};$$

consequently the corresponding modular equation has for its group

$$x_{\frac{k}{l}}, \quad x_{\frac{ak+bl}{ck+dl}},$$

in which k/l can take the $p+1$ values

$$\infty, 0, 1, 2, . \quad , p-1.$$

Thus, by agreeing that k can be infinity, we can simply write

$$x_k, \; x_{\frac{ak+b}{ck+d}}.$$

By giving to a, b, c, d all their values, we obtain $(p+1)p(p-1)$ permutations.

Now this group is decomposable *properly* into two groups, for which the substitutions are

$$x_k, \; x_{\frac{ak+b}{ck+d}},$$

$ad - bc$ being a quadratic residue of p.

The group thus simplified is of

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

permutations.

But it is easy to see that it is not possible to properly decompose it further, unless $p = 2$ or $p = 3$.

Thus, in whatever manner we transform the equation, its group will always have the same number of permutations.

But it is curious to know if the degree can be reduced.

And firstly it cannot be reduced to less than p, since an equation of degree less than p cannot have p as a factor of the number of permutations in its group.

Therefore, let us see if the equation of degree $p+1$, for which the roots x_k are got by giving to k all its values including infinity and for which the group has for substitutions

$$x_k, \; x_{\frac{ak+b}{ck+d}},$$

$ad - bc$ being a square, can be reduced to degree p.

But for this, the group should decompose (improperly, it is understood) into p groups of $(p+1)(p-1)/2$ permutations each.

Let 0 and ∞ be two letters related in one of these groups. The substitutions which do not permute 0 and ∞ will be of the form

$$x_k,\ x_{m^2k}.$$

Hence if M is the letter associated to 1, the letter associated to m^2 will be m^2M. When M is a square, we have therefore $M^2 = 1$. But this simplification is possible only for $p = 5$.

For $p = 7$ we find a group of $(p+1)(p-1)/2$ permutations, where

$$\infty \quad 1 \quad 2 \quad 4$$

are respectively related to

$$0 \quad 3 \quad 6 \quad 5.$$

This group has its substitutions of the form

$$x_k, x_{a\frac{k-b}{k-c}},$$

b being the letter corresponding to c, and a a letter which is a residue or non-residue according as c.

For $p = 11$, the same substitutions take place with the same notations,

$$\infty \quad 1 \quad 3 \quad 4 \quad 5 \quad 9$$

are respectively related to

$$0 \quad 2 \quad 6 \quad 8 \quad 10 \quad 7.$$

Thus, for the case of $p = 5, 7, 11$, the modular equation is reduced to degree p.

In all rigor, this reduction is not possible in the higher cases.

The third paper concerns the integrals.

We know that a sum of terms of the same elliptic function is always reduced to a single term plus algebraic or logarithmic quantities.

There are no other functions for which this property holds.

But very similar properties hold if we substitute everywhere, integrals of algebraic functions.

We treat at the same time all the integrals for which the differential is a function of the variable and of a similar irrational function of the variable, whether this irrational is or is not a radical, whether it may be expressible or not expressible by radicals.

We find that the number of distinct periods of the most general integral related to a given irrational is always an even number.

Letting $2n$ be this number we have the following theorem:

An arbitrary sum of terms reduces to n terms, plus algebraic and logarithmic quantities.

The functions of the first kind are those for which the algebraic and logarithmic part is zero.

There are n distinct ones.

The functions of the second kind are those for which the complementary part is purely algebraic.

There are n distinct ones.

We can suppose that the differentials of other functions are never infinity but once for $x = a$, and moreover, that their complementary part is reduced to only one logarithm, $\log P$, P being an algebraic quantity. By denoting these functions by $\Pi\,(x, a)$ we have the theorem

$$\Pi\,(x, a) - \Pi\,(a, x) = \Sigma \phi a \psi x,$$

ϕa and ψx being functions of the first and second kind.

We deduce from this, by calling $\Pi(a)$ and ψ the periods of $\Pi\,(x, a)$ and ψx related to a similar revolution of x,

$$\Pi(a) = \Sigma \psi \times \phi a.$$

Thus the periods of functions of the third kind are always expressible as a function of first and second kind.

We can also deduce theorems analogous to the theorems of Legendre

$$FE' + EF' - FF' = \frac{\pi}{2}.$$

The reduction of functions of the third kind to definite integrals, which is the most beautiful discovery of Jacobi, is not practicable outside the case of elliptic functions.

The multiplication of integral functions by a natural number is always possible, as addition, by means of an equation of degree n whose roots are the values to be substituted in the integral for reducing the terms.

The equation which gives the division of periods into p equal parts is of degree $p^{2n} - 1$. Its group has in all

$$(p^{2n} - 1)(p^{2n} - p)(p^{2n} - p^{2n-1})$$

permutations.

The equation which gives the division of a sum of n terms into p equal parts is of degree p^{2n}. It is solvable by radicals.

On the transformation. We can, at first, by following the reasoning analogous to those Abel has put in his last paper, prove that if, in a similar relation between the integrals, we have the two functions

$$\int \Phi\,(x, X)dx, \quad \int \Psi\,(y, Y)dy,$$

the last integral having $2n$ periods, one will be allowed to suppose that y and Y are expressible by means of a single equation of degree n as a function of x and of X

According to this we can suppose that the transformations constantly take place between two integrals only, since one will obviously have, by taking an arbitrary rational function of y and of Y

$$\sum \int f(y, Y)dy = \int F(x, X)dx + \text{an alg. and log quantity.}$$

It is likely that on this equation there will be obvious reductions in the case where for the integrals of one and of the other, it is not likely that both of them have the same number of periods.

Thus we can only compare integrals both of which have the same number of periods.

We will prove that the smallest degree of irrationality of two similar integrals cannot be greater for one than for the other.

We will then show that we can always transform a given integral into another in which a period of the first is divisible by the prime number p, and the other $2n-1$ remain the same.

Hence what remains to compare is only integrals where the periods are the same on both sides and consequently such that the n terms of one express themselves without another equation but just one of degree n, by means of those of the other and conversely. Here we do not know anything.

You know, dear Auguste, that these subjects are not the only ones that I have explored. My principal meditations, for some time now, were directed on the application of the theory of ambiguity to transcendental analysis. It was to see, a priori, in a relation between transcendental quantities or functions, what exchanges can be done, what quantities we could substitute to the given quantities, without changing the relation. This makes one recognise immediately lots of expressions that one could look for. But I don't have the time, and my ideas are not yet well developed in this area, which is immense.

You will get this Letter printed in the *Revue encyclopedique.*

I have often dared in my life to advance propositions about which I was not sure, but all that I have written down has been in my mind for over an year, and it would not be too much in my interest to make mistakes so that one suspects me of having announced theorems of which I would not have a complete proof.

You make a public request to Jacobi and Gauss to give their opinion, not as to the truth but as to the importance of these theorems.

After this, I hope there will be people who will profit by deciphering all this mess.

I embrace you effusively.

E. Galois

29 May 1832.