than $n-1$, while the average number of elements in all the substitutions of G is $n-1$. This is impossible, as the substitutions of G which are not also in H cannot contain more than $n-1$ elements. *Hence H is transitive.* Since the average number of elements in the substitutions of G is the same as that in the substitutions of H, *the substitutions of G which are not found in H must all be of the $(n-1)$th degree.*

The theorems of §§ 75, 76 of Netto's work * are proved by the preceding paragraph. It may be well to add in regard to the given § 75 that G may be transitive while the corresponding subgroup of G is intransitive. The following group † is an instance:

1	1	$AB.CE$	$af.bj.ci.dh.eg$
$ABCDE$	$abcde.fghij$	$AC.DE$	$ag.bf.cj.di.eh$
$ACEBD$	$acebd.fhjgi$	$AD.BC$	$ah.bg.cf.dj.ei$
$ADBEC$	$adbec.figjh$	$AE.BD$	$ai.bh.cg.df.ej$
$AEDCB$	$aedcb.fjihg$	$BE.CD$	$aj.bi.ch.dg.ef$

Netto's statement: "If G is transitive in the A's, H is transitive in the x's," together with the rest of the section seems to me to imply that such a case is impossible.

LEIPZIG, *August*, 1895.

ON AN UNDEMONSTRATED THEOREM OF THE DISQUISITIONES ARITHMETICÆ.

BY DR. JAMES PIERPONT.

THE last section of the Disquisitiones Arithmeticæ contains the algebraic solution of the equations upon which the prime roots of unity depend.

$$x^p - 1 = 0, \quad (1)$$ ‡

where p is a prime. As this equation contains the factor $(x-1)$, we may consider instead the equation

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = 0. \quad (2)$$

* COLE's translation, pp. 86, 87.

† COLE, *Quarterly Journal*, vol. 27, p. 41.

‡ The algebraic solution of these equations so simple in form presented difficulties which the mathematicians of the last century were not able to surmount. When $p = 11$ one arrives at an equation of 5th degree. Vandermonde gave the solution of this equation at the close of his paper Mémoire sur la Résolution des Equations, Hist. Acad. de Paris, 1771, but it appears to have been little known.

Gauss shows how the roots of this equation may be rationally expressed in the roots of the *suite*

$$Z_1 = 0, \quad Z_2 = 0, \cdots, \tag{3}$$

whose coefficients are respectively rational in the roots of the preceding equations, the coefficients of the first being integers. The degrees of the equations (3) are precisely the prime factors of $p-1$; hence it follows that if $p-1$ contains no factors other than 2, the solution of (1) can be effected by the extraction of square roots of known quantities. Now the roots of (1) expressed in circular functions are

$$x_\kappa = \cos\frac{2\pi\kappa}{p} + i\sin\frac{2\pi\kappa}{p}, \quad \kappa = 0, 1, \cdots, p-1,$$

to which correspond in the plane representing the complex variable precisely the vertices of a regular polygon of p sides. Further, since the roots of a quadratic equation whose coefficients can be constructed geometrically, *i.e.* by rule and compass, can also be constructed geometrically, it follows that when $p-1$ is of the form 2^μ, the roots of the *suite* (3) can be constructed, and hence those of (1). Thus we are able to construct all polygons of a prime number of sides p, if $p-1$ is a power of 2. Such primes are

$$3, \quad 5, \quad 17, \quad 257, \quad 65537, \cdots.$$

Of this result Gauss remarks* that it is certainly remarkable that although the geometric construction of regular polygons of 3 and 5 sides and those immediately derivable from them, viz.

$$2^\mu, \quad 2^\mu \cdot 3, \quad 2^\mu \cdot 5, \quad 2^\mu \cdot 15,$$

was already known in Euclid's time, still in an interval of 2000 years not only no new polygons had been discovered, but geometers were unanimous in declaring no others could be constructed.

A result of this startling character could easily tempt Gauss's contemporaries to seek other constructible polygons. Against such an attempt, however, Gauss expressly warns in the following words:

"As often as $p-1$ contains other prime factors besides 2, we arrive at higher equations, namely, to one or more cubic equations, if 3 enters once or oftener as a factor of $p-1$, to equations of 5th degree if $p-1$ is divisible by 5, etc. And

* GAUSS, Disq. Arith., Art. 365.

we can prove with all rigor that these higher equations cannot be avoided or made to depend upon equations of lower degree; and although the limits of this work do not permit us to give the demonstration here, we still thought it necessary to signal this fact in order that one should not seek to construct other polygons than those given by our theory, as, for example, polygons of 7, 11, 13, 19 sides, and so employ his time in vain."

Having laid down the theory for polygons of a prime number of sides, Gauss now turns his attention to polygons of any number of sides, $n = p_1^{a_1} p_2^{a_2} \cdots p_\nu^{a_\nu}$ where $p_1, p_2, \cdots$, are the prime factors of n. These he disposes of in a very summary fashion by declaring, without any attempt of proof, that they can be constructed then and only then when

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_\nu}\right)$$

contains no other factor than 2.*

That this is a sufficient condition follows at once from an easy extension of Gauss's method as developed when n is a prime. It is, however, vastly more important to know that *only* these polygons can be geometrically constructed as thereby the theory of regular polygons, as far as their construction by rule and compass is concerned, is made complete.† That is, in a given case we can decide whether the polygon is constructable, and in case that it is, Gauss's theory gives us the necessary directions to construct it.

We propose now in the *first part* of this paper to show that the condition which Gauss gave as necessary is in fact such. The demonstration, resting as it does on only the most *elementary algebraic* notions, is thought will be of interest as filling up a *lacuna* which all readers of the Disquisitiones must have felt. In the *second part* we shall establish a general algebraical theorem from which follows at once the correctness of Gauss's statement ‡ made in regard to the number and degree of the equations entering into the solution of (1).

We make, then, a further application to establish a criterion regarding the construction of regular polygons by *rational* conic sections.

---

* *Ibid.* Art. 366.

† This is the character of all Gauss's works. Compare his letter to Schumacher, Nov. 21, 1825, which contains the following passage: "Der Wunsch den ich immer bei meinen Arbeiten gehabt habe, ihnen eine solche Vollendung zu geben *ut nihil amplius desiderari possit* . . ."

‡ Put in their precise form. As we prove Gauss's criterion, it is not necessary to investigate these equations; it is, however, interesting to show that Gauss's assertions in this respect are correct.

I.

To show that the condition given by Gauss is necessary, we observe in the first place that if a quantity x can be constructed by rule and compass, it is rational in the roots of a *suite* of quadratic equations.

$$X_1 = 0,\ X_2 = 0, \cdots, \tag{4}$$

whose coefficients are respectively rational in the roots of the preceding equations, while those of $X_1 = 0$ are integers. This is simply shown by remarking that to each right line or circle which enters into the construction of x corresponds an equation respectively of the type

$$\frac{x}{a} + \frac{y}{b} = 1, \tag{5}$$

$$(x-a)^2 + (y-b)^2 = c^2,$$

where a, b, c are quantities which can be geometrically constructed. The solution of a succession of such equations leads to a *suite* of the type (4). Having established this analytical condition for the constructibility of a quantity, we proceed to show that a polygon of $m = p^a$ sides (p being a prime) cannot be constructed unless

$$\phi(m) = p^{a-1}(p-1)$$

is a power of 2. To do this we need only to show that the roots of

$$x^m - 1 = 0 \tag{6}$$

are not rational in a *suite* of the type (4). Instead, however, of considering (6) we consider the equivalent equation

$$F(x) = x^{(p-1)p^{a-1}} + x^{(p-2)p^{a-1}} + \cdots + x^{p^{a-1}} + 1 = 0, \tag{7}$$

whose roots are the $\phi(m)$ primitive mth roots of unity. Kronecker has shown* that $F(x)$ is irreducible, *i.e.* it is impossible to break $F(x)$ into two rational integral polynomials $\chi(x)$, $\psi(x)$ with rational coefficients.

For suppose $$F(x) = \chi(x)\psi(x),$$

then the coefficients of χ, ψ are not only rational but integers. As $F(1) = p$, one of the polynomials $\chi(1)$, for example, $= \pm 1$.

---

*KRONECKER, Werke, vol. 1, p. 101. Kronecker proves here the irreducibility of $F(x)$ when m is a prime p; remarks, however, that the method is applicable to the above case.

Form now the product

$$P(x) = \chi(x)\,\chi(x^2)\cdots\chi(x^{m-1}).$$

As $P(x)$ is divisible by $F(x)$, we have

$$\frac{P(x)}{F(x)} = q(x),$$

whose coefficients are evidently integers. Hence $q(1)$ is an integer, which is impossible, since

$$q(1) = \frac{P(1)}{F(1)} = \frac{\pm 1}{p}.$$

Suppose now the roots of F are rational in a *suite* as (4); proceed to enlarge the domain $R(1)$* in which $F(x)$ is irreducible by successively adjoining the roots of the equations (4), which we denote respectively by

$$y_1,\ y_1';\ y_2,\ y_2';\ \cdots.$$

At some moment $F(x)$ breaks up into rational factors, say on adjoining y_κ, we can then write

$$F(x) = F_1(x,\ y_\kappa)\,F_2(x,\ y_\kappa)\cdots F_s(x,\ y_\kappa),$$

where $F_1, F_2\cdots$ are rational polynomials having their coefficients rational in y_κ and preceding irrationalities. Let F_i be of lowest degree λ; then $m \geqq s\lambda$; further, the coefficients of

$$\Phi(x) = F_i(x,\ y_\kappa)\,F_i(x,\ y_\kappa'),$$

being symmetric in the roots of $X_\kappa = 0$, are rational in $R(y_1 y_2\cdots y_{\kappa-1})$ in which domain $F(x)$ is irreducible. As $\Phi = 0$ is satisfied by at least one root of $F = 0$, Φ is divisible by F, and hence the degree of Φ, that is 2λ, $\leqq m \leqq s\lambda$, whence

$$s \gtreqless 2, \text{ or as } s > 1, \text{ we have } s = 2.$$

That is, when $F(x)$ becomes reducible, it breaks up into two factors of equal degree. As the same reasoning is applicable to $F_i(x,\ y_\kappa)$, etc., we conclude that it is impossible to break

---

*To avoid circumlocution the author uses the terminology introduced by GALOIS; for those unfamiliar with it we add the following explanation: Let $abc\cdots$ be certain quantities; all quantities which can be derived from them by addition, subtraction, multiplication, and division, form a *domain* of rationality $R(a, b, c, \cdots)$. If α be not in R, we may enlarge R by *adjoining* it to $a, b, c, \cdots$, thus forming a new domain $R(a, b, c, \cdots \alpha)$. Thus $R(1)$ denotes all rational numbers. *It is to be remarked*, however, that while using Galois' terms, we make no use of his theory in Part I.; this would have destroyed the simplicity of the proof.

$F(x)$ into linear factors if $\phi(m)$ contains other prime factors than 2, which requires that

$$a = 1, \quad p - 1 = 2^{\mu}. \tag{8}$$

From this we conclude immediately that a polygon of

$$n = p_1^{a_1} p_2^{a_2} \cdots p_\nu^{a_\nu}$$

sides cannot be geometrically constructed unless p_κ, $\kappa = 1, 2 \cdots \nu$, satisfy the condition (8); that is,

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_\nu}\right)$$

must be a power of 2.

This shows at once the impossibility of constructing by rule and compass polygons of 7, 9, 11, 13, 14 $\cdots$ sides.

As the ancient Greek geometers frequently allowed the use of the conic sections in a geometric construction, the question naturally arises, what additional polygons can be under these new conditions constructed? This will be answered below.

II.

Incidently we proved in the preceding section that an irreducible equation of degree n cannot be solved by a *suite* (4) of quadratic equations if n contains prime factors besides 2. The equations (4) are simple Abelian equations, and the theorem just stated is a particular case of the following:

THEOREM I. — Let the roots of an irreducible algebraically solvable equation $F(x) = 0$ of degree $n = p_1^{a_1} p_2^{a_2} \cdots p_\nu^{a_\nu}$, ($p_1 p_2 \cdots$ being primes) be rational in the roots of a *suite* of simple equations

$$f_1 = 0, \quad f_2 = 0 \cdots \tag{9}$$

having the properties

1° The coefficients of $f_1 = 0$ are rational, while those of the following are respectively rational in the roots of the preceding equations.

2° The roots of no equation are rational in those of the preceding equations.

Then the *suite* (9) contains a_κ Abelian equations of degree p_κ ($\kappa = 1, 2 \cdots \nu$); should $F(x) = 0$ be itself Abelian, the *suite* (9) need contain no other equations.*

For proceed to enlarge R by the successive adjunction of the roots of (9); at a certain moment a reduction of the group

* Cf. an analogous theorem by HÖLDER, *Math. Annalen*, vol. 34, p. 26.

of $F=0$ must take place. Let it be on adjoining the roots of $f_\kappa=0$ of degree m_κ; then $f_\kappa=0$ is an Abelian equation of degree m_κ, and m_κ is a prime. If at the same time $F(x)$ becomes reducible, it breaks up into precisely m factors of equal degree. Since $F(x)$ ultimately breaks up into linear factors, it follows that (9) must contain at least a_κ Abelian equations of degree p_κ. If $F(x)=0$ is itself an irreducible Abelian equation, it need contain no more.

This theorem contains Gauss's statement in regard to the number and degree of the equations upon which the solution of (1) depends as a particular case. As another application of Theorem I., we conclude easily the following:

THEOREM II. — A polygon of n sides can then, and only then, be constructed by a series of *rational* conics* when $\phi(n)$ contains no prime factor other than 2 or 3.

For suppose $\phi(n)$ contain only such factors, then the solution of (1) depends upon a *suite*

$$Y_1=0, \quad Y_2=0,\cdots$$

of equations of the 2d or 3d degree. As the coefficients of each successive equation of this *suite* are constructible, the roots themselves are,† and hence the roots of (1). This shows that the above condition is sufficient; that it is necessary, follows from the same reasoning as employed for the circle in Part I.

We have deduced Theorem II. from Theorem I. We remark that it can be proved very simply by other considerations.

The following is a short table of constructible regular polygons of sides $\leqq 100$.

The first row indicates the polygon constructible by rule and compass, known to the Greeks; the second row indicates the polygons of this class discovered by Gauss; finally, the last row gives the *additional* polygons which can be constructed when *rational conics* can be employed.

GREEKS:	2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 30, 32, 40, 48, 60, 64, 80, 96.
GAUSS:	17, 34, 51, 68, 85.
CONICS:	7, 9, 13, 14, 18, 19, 21, 26, 27, 28, 35, 36, 37, 38, 39, 42, 45, 52, 54, 56, 57, 63, 65, 70, 72, 73, 74, 76, 78, 81, 84, 90, 91, 95, 97.

NEW HAVEN, *November*, 1895.

---

* That is, conics whose coefficients are rational in the current domain of rationality.

† Cf. DESCARTES' Geometria, edit. by v. Schooten.