Comments

I return to the observation that was the occasion for this digression, as it could be misunderstood. I prefer that it not be, for the point I was attempting to make is serious.

We have seen, when discussing the regular pentagon the importance, or at least the interest, of the algebraic symmetries of points that divide the circle into five equal arcs and we expect something similar for the regular heptadecagon. We have also observed, without entering into the mathematical details, that a similar interest, for similar reasons, attaches to the points that divide a lemniscate into five equal parts, although the equations here are more difficult to come by. The modern mathematical catch phrase for the symmetries is "Galois structure" or "Galois action" and the phrase, or theory, that captures the division into equal parts is "l-adic cohomology". Thus we have studied – just a little – the "Galois action on l-adic cohomology". This is part, a good part, of the context in which Wiles's proof of the Fermat theorem is carried out. So we have succeeded – again just a little – in coming into direct contact with the mathematics itself, rather than with a publicist's rendering of it. Just as the public at large is separated from the essential ideas by the popularizers, who hear and repeat the catch phrases, often without understanding their content, mathematicians, even those with some special competence, are often separated from it by the accretion of theory. Rather than returning to the specific and tangible to communicate, we resort to metaphors, which only take the abstraction one degree further.

The last entry in the diary refers, although in a manner that is cryptic enough that we cannot be entirely sure what Gauss had in mind (but Abel's paper permits a precise guess), to a second aspect of modern number theory, to congruences, thus to the study of the number of solutions of a relation

$$p \text{ divides } P(x, y, z, \ldots).$$

We may not have occasion to say much about the second topic. As Gauss suggests, the two are linked. The connection has become such a commonplace in contemporary mathematics that we forget how strange it is. It would be good, if we have the time, to return to it, to try to capture some of its wonder.

Lecture 8

The heptadecagon: beginning.

We have seventeen seventeenth roots of 1. We take them to be

$$z_k = \cos(2k\pi/17) + i\sin(2k\pi/17), \qquad k = 0, 16$$

As before $z_0 = 1$ and each of the others satisfies the equation

$$Z^{16}+Z^{15}+Z^{14}+Z^{13}+Z^{12}+\cdots+Z^6+Z^5+Z^4+Z^3+Z^2+Z^1+1 = 0$$

We take as proved that they satisfy no equation of smaller degree. This is proved pretty much as it was for the fifth roots of unity. Thus all the numbers

$$a_1z_1 + a_2z_2 + a_3z_3 + a_4z_4 + \cdots + +a_{13}z_{13} + a_{14}z_{14} + a_{16}z_{16}$$

are different. We must not forget that

$$z_1 + z_2 + z_3 + z_4 + \cdots + z_{13} + z_{14} + z_{15} + z_{16} = -1$$

Moreover we have sixteen symmetries $z_1 \to z_2$, $z_1 \to z_3$, $z_1 \to z_4$, and so on. If the symmetry takes z_1 to z_2 then it takes $z_5 = z_1^5$, for example, to $z_2^5 = (z_1^2)^5 = z_1^{10}$. It takes z_9 to $z_2^9 = z_1^{18} = z_1^1$. We call this symmetry, thought of as a reflection, ρ and ask what happens when we repeat it over and over again, as in a hall of mirrors. It is enough to trace its effect on z_1 because all the other numbers can be expressed by taking powers of z_1, multiplying them by fractions, and adding the results together. This can be done after the reflection as well as before. The result is not changed. In each line of the table on the next page, the first step is the result of the preceding line and the second is the result of then applying ρ one more time.

$$
\begin{aligned}
\rho: &\quad z_1 \to z_2 \\
\rho^2: &\quad z_1 \to z_2, \quad z_2 \to z_4 \quad \Rightarrow z_1 \to z_4 \\
\rho^3: &\quad z_1 \to z_4, \quad z_4 \to z_8 \quad \Rightarrow z_1 \to z_8 \\
\rho^4: &\quad z_1 \to z_8, \quad z_8 \to z_{16} \Rightarrow z_1 \to z_{16} \\
\rho^5: &\quad z_1 \to z_{16}, \quad z_{16} \to z_{15} \Rightarrow z_1 \to z_{15} \\
\rho^6: &\quad z_1 \to z_{15}, \quad z_{15} \to z_{13} \Rightarrow z_1 \to z_{13} \\
\rho^7: &\quad z_1 \to z_{13}, \quad z_{13} \to z_9 \Rightarrow z_1 \to z_9 \\
\rho^8: &\quad z_1 \to z_9, \quad z_9 \to z_1 \quad \Rightarrow z_1 \to z_1
\end{aligned}
$$

Thus after eight repetitions we come to the trivial symmetry. The number z_1 is reflected in itself, as are therefore all other numbers.

So we start again, this time with σ which reflects z_1 in z_3. Thus it takes $z_3 = z_1^3$ to $z_3^3 = z_1^9$

$$
\begin{aligned}
\sigma: &\quad z_1 \to z_3 \\
\sigma^2: &\quad z_1 \to z_3, \quad z_3 \to z_9 \quad \Rightarrow z_1 \to z_9 \\
\sigma^3: &\quad z_1 \to z_9, \quad z_9 \to z_{10} \Rightarrow z_1 \to z_{10} \\
\sigma^4: &\quad z_1 \to z_{10}, \quad z_{10} \to z_{13} \Rightarrow z_1 \to z_{13} \\
\sigma^5: &\quad z_1 \to z_{13}, \quad z_{13} \to z_5 \Rightarrow z_1 \to z_5 \\
\sigma^6: &\quad z_1 \to z_5, \quad z_5 \to z_{15} \Rightarrow z_1 \to z_{15} \\
\sigma^7: &\quad z_1 \to z_{15}, \quad z_{15} \to z_{11} \Rightarrow z_1 \to z_{11} \\
\sigma^8: &\quad z_1 \to z_{11}, \quad z_{11} \to z_{16} \Rightarrow z_1 \to z_{16} \\
\sigma^9: &\quad z_1 \to z_{16}, \quad z_{16} \to z_{14} \Rightarrow z_1 \to z_{14} \\
\sigma^{10}: &\quad z_1 \to z_{14}, \quad z_{14} \to z_8 \Rightarrow z_1 \to z_8 \\
\sigma^{11}: &\quad z_1 \to z_8, \quad z_8 \to z_7 \Rightarrow z_1 \to z_7 \\
\sigma^{12}: &\quad z_1 \to z_7, \quad z_7 \to z_4 \Rightarrow z_1 \to z_4 \\
\sigma^{13}: &\quad z_1 \to z_4, \quad z_4 \to z_{12} \Rightarrow z_1 \to z_{12} \\
\sigma^{14}: &\quad z_1 \to z_{12}, \quad z_{12} \to z_2 \Rightarrow z_1 \to z_2 \\
\sigma^{15}: &\quad z_1 \to z_2, \quad z_2 \to z_6 \Rightarrow z_1 \to z_6 \\
\sigma^{16}: &\quad z_1 \to z_6, \quad z_6 \to z_1 \Rightarrow z_1 \to z_1
\end{aligned}
$$

Thus the powers of σ exhaust the symmetries and we can measure the amount of symmetry of any element

(A) $a_1z_1+a_2z_2+a_3z_3+a_4z_4+\cdots++a_{13}z_{13}+a_{14}z_{14}+a_{15}z_{15}+a_{16}z_{16}$

by the smallest power of σ under which it is invariant. For example the most symmetric are those that are their own reflections by σ and therefore by any repetition of σ. The reflection of (A) given by σ is

$$a_1z_3 + a_2z_6 + a_3z_9 + a_4z_{12} + \cdots + a_{13}z_5 + a_{14}z_8 + a_{15}z_{11} + a_{16}z_{14}$$

What happens is that it can be invariant only if all coefficients are the same. but

$$az_1 + az_2 + az_3 + \cdots = -a$$

so that if it is invariant under σ itself, it just a fraction or rational number. If it is invariant under σ^2, it must be a sum $a(8,1)+b(8,3)$ where, following Gauss and using his notation, we build the periods

$$(8,1) = z_1 + z_9 + z_{13} + z_{15} + z_{16} + z_8 + z_4 + z_2$$

and

$$(8,3) = z_3 + z_{10} + z_5 + z_{11} + z_{14} + z_7 + z_{12} + z_6$$

Since

$$(8,1) + (8,3) = 1$$

and $(8,1)^2$ has the same symmetry as $(8,1)$, we must have

$$(8,1)^2 = a(8,1) + b(8,3) = (a-b)(8,1) - b$$

Once we have calculated a and b we will be able to solve easily for $(8,1)$.

The calculation is somewhat lengthy because $(8,1)\times(8,1)$ contains sixty-four terms. Let's see what can be done.

	z_1	z_9	z_{13}	z_{15}	z_{16}	z_8	z_4	z_2
z_1	z_2	z_{10}	z_{14}	z_{16}	1	z_9	z_5	z_3
z_9	z_{10}	z_1	z_5	z_7	z_8	1	z_{13}	z_{11}
z_{13}	z_{14}	z_5	z_9	z_{11}	z_{12}	z_4	1	z_5
z_{15}	z_{16}	z_7	z_{11}	z_{13}	z_{14}	z_6	z_2	1
z_{16}	1	z_8	z_{12}	z_{14}	z_{15}	z_7	z_3	z_1
z_8	z_9	1	z_4	z_6	z_7	z_{16}	z_{12}	z_{10}
z_4	z_5	z_{13}	1	z_2	z_3	z_{12}	z_8	z_6
z_2	z_3	z_{11}	z_{15}	1	z_1	z_{10}	z_6	z_4

The result is

$$3(8,1)+4(8,3)+8=-(8,1)+4$$

Thus

$$(8,1)^2+(8,1)-4=0$$

and

$$(8,1)=\frac{-1\pm\sqrt{17}}{2}$$

To decide which sign to take, we calculate both sides approximately. The left side is 1.56155. With the positive sign the right side gives the same approximation. Thus

$$(8,1)=\frac{-1+\sqrt{17}}{2}$$

$$z_9\times z_{13}=z_{22}=z_5 \qquad z_9^9\times z_1^{13}=z_1^{22}=z_1^5$$

The next step is to look at those elements that are not changed by σ^4 These are all of the form:

$$a(4,1) + b(4,3) + c(4,9) + d(4,10)$$

Here

$$\begin{aligned}(4,1) &= z_1 + z_{13} + z_{16} + z_4\\ (4,3) &= z_3 + z_5 + z_{14} + z_{12}\\ (4,9) &= z_9 + z_{15} + z_8 + z_2 = (8,1) - (4,1)\\ (4,10) &= z_{10} + z_{11} + z_7 + z_6\end{aligned}$$

I could calculate both $(4,1) \times (4,1)$ and $(4,1) \times (4,9)$. The point is that every number that is fixed by σ^4 will be of the form

$$a(4,1) + b(4,3) + c(4,9) + d(4,10)$$

The four basic numbers of this form are $(4,1)$, $(8,1)$,

$$1 = -(8,1) - (8,3)$$

and $(4,1) \times (8,1)$. Since $(4,1)^2$ must also be a number of this form, we will have

$$(4,1)^2 = a(4,1) + b,$$

with $a = c(8,1) + d$, $d = e(8,1) + f$, so that a and b are numbers that we know we can construct with ruler and compass. Since

$$(4,1) = \frac{a \pm \sqrt{a^2 + 4b}}{2},$$

it too can be constructed.

A simpler way to proceed is to observe that $(4,1)$ and $(4,9)$ satisfy the equation

$$0 = (Z - (4,1))(Z - (4,9)) = Z^2 - ((4,1) + (4,9))Z + (4,1)(4,9)$$

which equals

$$Z^2 - (8,1)Z + (4,1)(4,9).$$

Using this, it is enough to calculate $(4,1)(4,9)$ in which there are only sixteen terms.

$$\begin{array}{ccccc} & z_1 & z_{13} & z_{16} & z_4 \\ \\ z_9 & z_{10} & z_5 & z_8 & z_{13} \\ z_{15} & z_{16} & z_3 & z_6 & z_{11} \\ z_8 & z_9 & z_4 & z_7 & z_{12} \\ z_2 & z_3 & z_{15} & z_1 & z_6 \end{array}$$

The sum of all these numbers is -1. Thus

$$(4,1)^2 - (8,1)(4,1) - 1 = 0$$

and

$$(4,1) = \frac{(8,1) \pm \sqrt{(8,1)^2 + 4}}{2}$$

Since $(8,1)^2 = -(8,1)+4$, the expression under the square root is $8-(8,1)$. We find that

$$\frac{(8,1) + \sqrt{8-(8,1)}}{2} = \frac{\frac{-1+\sqrt{17}}{2} + \sqrt{\frac{17-\sqrt{17}}{2}}}{2} \sim 2.04948 \sim (4,1)$$

and this determines the sign.

Notice that

$$\frac{(8,1) - \sqrt{8-(8,1)}}{2} \sim -.487928.$$

So there is no ambiguity!

The next step is to find an expression for the period

$$(2,1) = z_1 + z_{16}$$

invariant under σ^8.

We consider also

$$(2,13) = z_{13} + z_4$$

because $(2,1) + (2,13) = (4,1)$. Thus with any luck, we can calculate $(2,1)$ if we can calculate $(2,1) \times (2,13)$. It is given by the table

	z_1	z_{16}
z_{13}	z_{14}	z_{12}
z_4	z_5	z_3

This gives $(4,3)$, which we have not yet calculated. There are two possibilities: to express $(4,3)$ as $a(4,1) + b$ with $a = c(8,1) + d$, $b = e(8,1) + f$, where c, d, e, f are ordinary fractions, or to calculate $(4,3)$ as we calculated $(4,1)$. The second method is easier.

First of all,

$$(4,3) + (4,10) = (8,3) = \frac{-1 - \sqrt{17}}{2}$$

We calculate $(4,3) \times (4,10)$ in the usual way

$$\begin{array}{ccccc} & z_3 & z_5 & z_{14} & z_{12} \\ \\ z_{10} & z_{13} & z_{15} & z_7 & z_5 \\ z_{11} & z_{14} & z_{16} & z_8 & z_6 \\ z_7 & z_{10} & z_{12} & z_4 & z_2 \\ z_6 & z_9 & z_{11} & z_3 & z_1 \end{array}$$

The sum is -1, so that

$$(4,3)^2 - (8,3)(4,3) - 1 = 0$$

Thus

$$(4,3) = \frac{(8,3) \pm \sqrt{(8,3)^2 + 4}}{2} = \frac{(8,3) \pm \sqrt{8 - (8,3)}}{2},$$

so that the expression for $(4,3)$ is exactly the same as that for $(4,1)$, except that $(8,3)$ replaces $(8,1)$.

$$(4,3) = \frac{(8,3) \pm \sqrt{(8,3)^2 + 4}}{2}$$

We still have to check the sign numerically. It is positive.

$$(4,3) \sim .344151 \sim \frac{(8,3) + \sqrt{8 - (8,3)}}{2}$$

Thus

$$(4,3) = \frac{\frac{-1-\sqrt{17}}{2} + \sqrt{\frac{17+\sqrt{17}}{2}}}{2}.$$

We return to $(2,1)$, which we know satisfies the equation

$$Z^2 - (4,1)Z + (4,3) = 0$$

Thus

$$(2,1) = \frac{(4,1) + \sqrt{(4,1)^2 - 4(4,3)}}{2}$$

The expression under the square-root sign is

$$\left(\frac{\frac{-1+\sqrt{17}}{2} + \sqrt{\frac{17-\sqrt{17}}{2}}}{2} \right)^2 - 4\frac{\frac{-1-\sqrt{17}}{2} + \sqrt{\frac{17+\sqrt{17}}{2}}}{2}.$$

Since

$$\left(\frac{-1+\sqrt{17}}{2} \right)^2 = \frac{9-\sqrt{17}}{2},$$

the first square is equal to

$$\frac{13-\sqrt{17}}{4} + \frac{(-1+\sqrt{17})\sqrt{\frac{17-\sqrt{17}}{2}}}{4}$$

All together, we have

$$\frac{17+3\sqrt{17}}{4} + \frac{(-1+\sqrt{17})\sqrt{\frac{17-\sqrt{17}}{2}}}{4} - 2\sqrt{\frac{17+\sqrt{17}}{2}}$$

Since

$$\frac{(4,1)}{2} = \frac{-1}{8} + \frac{\sqrt{17}}{8} + \frac{\sqrt{34-2\sqrt{17}}}{8},$$

we find that $(2,1)$ is equal to

$$\tfrac{-1}{8} + \tfrac{\sqrt{17}}{8} + \tfrac{\sqrt{34-2\sqrt{17}}}{8} \pm \tfrac{\sqrt{68+12\sqrt{17}-16\sqrt{34+2\sqrt{17}}-2(1-\sqrt{17})\sqrt{34-2\sqrt{17}}}}{8}$$

This is the form to be found in Klein's lectures.

Of course the sign has to be discovered by numerical approximation. We find that, with the plus sign both $(2,1)$ and this expression are about 1.86494.

Gauss's form is

$$\frac{-1}{8}+\frac{\sqrt{17}}{8}+\frac{\sqrt{34-2\sqrt{17}}}{8}+\frac{\sqrt{68+12\sqrt{17}-8\sqrt{34+2\sqrt{17}}-4\sqrt{34-2\sqrt{17}}}}{8}$$

It is obtained from Klein's by means of the square root of the identity

$$16(34+2\sqrt{17})=(18+2\sqrt{17})(34-2\sqrt{17})=(1+\sqrt{17})^2(34-2\sqrt{37})$$

This means

$$16\times 34=18\times 34-4\times 17 \qquad 16\times 2=2\times 34-18\times 2$$

We have now established that $(2,1)=z_1+z_{16}$ can be found by repeatedly extracting roots. Recall that

$$z_1=\cos(2\pi/17)+i\sin(2\pi/17)$$

and that

$$z_{16}=\cos(32\pi/17)+i\sin(32\pi/17)=\cos(2\pi/17)-i\sin(2\pi/17).$$

Thus

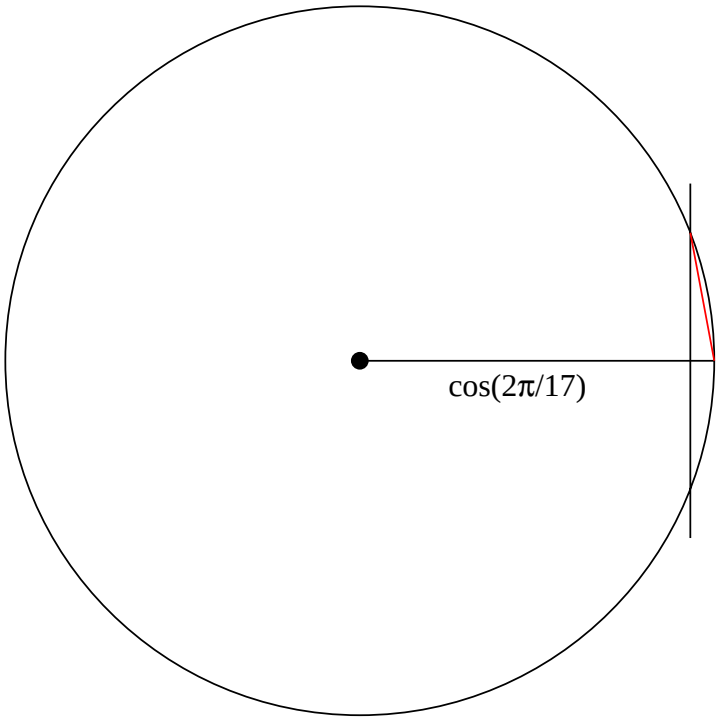
$$(2,1)=2\cos(2\pi/17),$$

so that $\cos(2\pi/17)$ can be found by repeatedly extracting square roots. Since z_1 is a root of

$$0=(Z-z_1)(Z-z_{16})=Z^2-(2,1)Z+1,$$

it can be found by extracting one more square root.

Of course, once $a=\cos(2\pi/17)$ is found, the usual way to construct z_1 is by erecting a perpendicular to the axis of abscissas at $(a,0)$ and intersecting it with the circle $x^2+y^2=1$.


cos(2π/17)

Final remark

The algebraic analysis shows how we are to proceed geometrically to construct successively the following numbers:

1) (8,1) and (8,3);

2) (4,1) and (4,3);

3) (2,1).

The numbers at each stage are obtained from those at the preceding stage by solving a quadratic equation – thus in effect by extracting a square root. Once we show how to solve in general a quadratic equation with given coefficients, we can proceed efficiently step by step. This is done in Klein's *Famous problems of elementary geometry*. It is clearly best to take the steps one at a time and not to represent them all together, but time is brief. So I present them to you all together as Klein finally does, although he also gives each step as well as describing an efficient way for solving a quadratic equation with known coefficients.

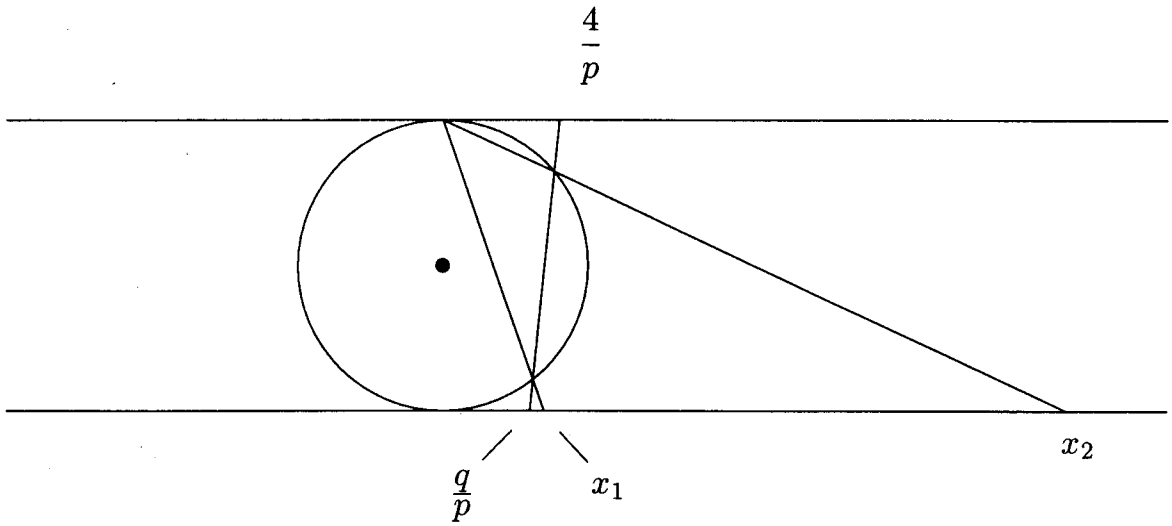
In addition to Klein, you might want to consult a text in a recent issue of the *Mathematical Intelligencer* that Robert Feinberg drew to my attention. It can be found in the mathematics library and in the common room in the mathematics building.

Christian Gottlieb, *The simple and straightforward construction of the* 257-*gon*, Math. Int., vol. 21, No.1, 1999

Observe that 257 is a prime and that

$$257 - 1 = 256 = 16^2 = 2^8 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2,$$

so that eight steps are required and not just four to arrive at the final result. In addition, the individual calculations will be longer as will the final formulas.



$$x^2 - px + q = 0$$

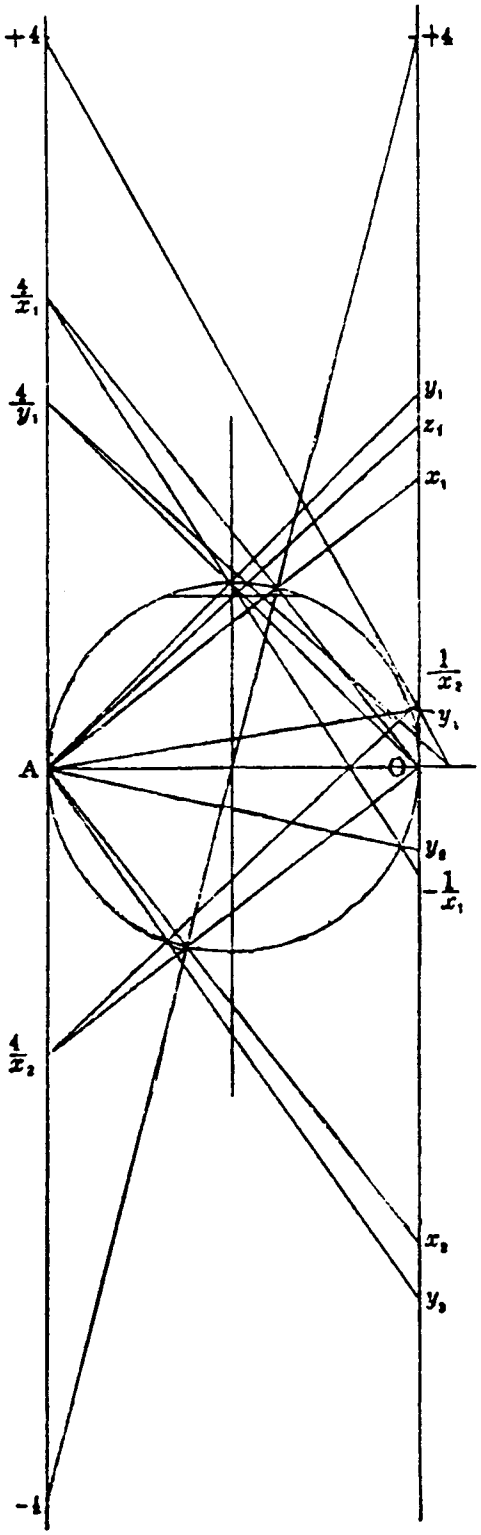

+4
+4
$\frac{4}{x_1}$
$\frac{4}{y_1}$
y_1
z_1
x_1
$\frac{1}{x_2}$
y_2
A
O
y_2
$-\frac{1}{x_1}$
$\frac{4}{x_2}$
x_2
y_2
-4

FIG. 9.