C. Quintics of Genus 2.

The cubic may be replaced by a triple line; the nodal curve is completed by one double directrix and one triple directrix (XV); the skew directrices may be (27) distinct or (28) coincident.

CORNELL UNIVERSITY,
January 25, 1902.

SIMPLIFIED DEFINITION OF A GROUP.

BY DR. E. V. HUNTINGTON.

(Read before the American Mathematical Society, February 22, 1902.)

UP to the present time no attempt seems to have been made to prove the independence of the postulates employed to define a group, and as a matter of fact the definition usually given contains several redundancies.* These redundancies are removed in the following note, the number of necessary postulates being reduced to three, and the independence of these three being established.

Fundamental Concepts.

A *class* of objects is determined when any condition is given such that every object in the universe must either satisfy or not satisfy the condition. Every object which satisfies the condition is said to *belong to* the class. (We shall agree to exclude the case of a class to which no element belongs.)

A class thus defined is usually called, in mathematical parlance, an *assemblage* (Menge, ensemble), every object which belongs to the class being called an *element* of the assemblage.

A *rule of combination* in an assemblage is any rule or agreement by which, when any two elements (whether the same or different) are given, in a definite order, some object (which may or may not itself belong to the assemblage †) is uniquely determined.

If the first of the two given elements is denoted by a and the second by b, then the object which they determine is denoted by $a \circ b$ (read: "a with b").

---

*See for example H. Weber, Algebra, Vol. II. (1899), pp. 3-4.

† The object determined by any two elements of the assemblage always will belong to the assemblage if postulates 1, 2, 3 are satisfied, as we prove below in 10.

When two different symbols x and y are used to represent the same object, we indicate this fact by the notation $x = y$.

Definition of a Group.

Any assemblage in which the rule of combination denoted by $\circ$ satisfies the three following postulates we shall call a *group* with respect to this rule of combination:

1. *Given any two elements a and b, there is an element x such that $a \circ x = b$.*

2. *Given any two elements a and b, there is an element y such that $y \circ a = b$.*

3. *If a, b, c, $a \circ b$, $b \circ c$, and either $(a \circ b) \circ c$ or $a \circ (b \circ c)$ are elements of the assemblage, then*

$$(a \circ b) \circ c = a \circ (b \circ c).*$$

The usual definition of a group, as given for example in Weber's Algebra, loc. cit., contains not only these three postulates, but also certain others, which we proceed now to deduce as consequences of our postulates 1, 2, 3, thus establishing the equivalence of the two definitions.

4. *Lemma. If $a \circ x = a$ then $b \circ x = b$.* (That is, if an element x, when combined with any particular element a, leaves that element unchanged, then x will have the same property when combined with any other element b.)

Proof: By 2 take y so that $y \circ a = b$; then by hypothesis, $y \circ (a \circ x) = b$. But by 3, $y \circ (a \circ x) = (y \circ a) \circ x$; therefore $b \circ x = b$.

5. *Lemma. If $y \circ a = a$ then $y \circ b = b$.*

Proof: By 1 take x so that $a \circ x = b$; then by hypothesis, $(y \circ a) \circ x = b$. But by 3, $(y \circ a) \circ x = y \circ (a \circ x)$; therefore $y \circ b = b$.

6. *If $a \circ b = a \circ b'$ then $b = b'$.*

Proof: By 1 take x so that $b' \circ x = b$; then by hypothesis, $a \circ (b' \circ x) = a \circ b'$ whence by 3, $(a \circ b') \circ x = (a \circ b')$. Therefore by 4, $b' \circ x = b'$, that is, $b = b'$.

* Postulate 3 does not demand that either of the objects $(a \circ b) \circ c$ and $a \circ (b \circ c)$ shall belong to the assemblage; if either one of them does belong, however, then the other must also.

7. *If* $a \circ b = a' \circ b$ *then* $a = a'$.

Proof: By 2 take y so that $y \circ a' = a$; then by hypothesis, $(y \circ a') \circ b = a' \circ b$, whence by 3, $y \circ (a' \circ b) = (a' \circ b)$. Therefore by 5, $y \circ a' = a'$, that is, $a = a'$.

8. *The element* x *in* 1 *is uniquely determined by* a *and* b (*by* 6).

9. *The element* y *in* 2 *is uniquely determined by* a *and* b (*by* 7).

10. *Whatever elements* a *and* b *may be,* $a \circ b$ *is also an element of the assemblage; that is, there is an element* c *such that* $a \circ b = c$.

Proof: By 1 take e so that $a \circ e = a$, (1°)

and b' so that $b \circ b' = e$; (2°)

then by 2 take c so that $c \circ b' = a$. (3°)

The element c thus determined is the element required in the theorem.

For, by 1 take β so that $a \circ \beta = c$, (4°)

and β' so that $\beta \circ \beta' = e$. (5°)

From (3°) and (4°) we have $(a \circ \beta) \circ b' = a$ and from (1°) and (5°) we have $a \circ (\beta \circ \beta') = a$, whence by 3

$$(a \circ \beta) \circ \beta' = (a \circ \beta) \circ b'.$$

Therefore by 6, $\beta' = b'$.

Then (5°) becomes $\beta \circ b' = e$,

whence by (2°) $\beta \circ b' = b \circ b'$.

Therefore by 7, $\beta = b$; hence by (4°) $a \circ b = c$ as desired.

We can now justify our definition of a group as follows: our postulates 1 and 2, combined with theorems 8 and 9, are equivalent to postulate 4 in Weber's definition, and our postulate 3 to his 2. Weber's postulate 1 appears here as theorem 10, and his postulate 3 is contained in our theorems 6 and 7. Hence the two definitions are strictly equivalent.

A simple example of a group is the assemblage of all integral numbers, positive, negative, and zero, with $a \circ b = a + b$. Another example is the assemblage of positive rational numbers, with $a \circ b = a \times b$.

Independence of Postulates 1, 2, 3.

The independence of the postulates 1, 2, 3 can be readily established by the method now commonly used in such cases.

Thus, the assemblage of positive integers, with the rule of combination $a \circ b = a$, satisfies 2 and 3, but not 1. Hence 1 is not a consequence of 2 and 3.

Again, the assemblage of positive integers, with $a \circ b = b$, satisfies 1 and 3, but not 2. Hence 2 is not a consequence of 1 and 3.

Finally, the assemblage of positive rational fractions, with $a \circ b = a/b$, satisfies 1 and 2, but not 3. Hence 3 is not a consequence of 1 and 2.*

Finite Groups.

A *finite group* is a group which contains only a finite number of elements. If the number of elements is n, the group is said to be of the nth *degree.*

A simple example of a group of the nth degree can be constructed as follows: take the assemblage of the positive integers from 1 to n and let

$$\begin{aligned} a \circ b &= a + b \quad \text{when} \quad a + b \leqq n, \\ &= a + b - n \quad \text{when} \quad a + b > n. \end{aligned}$$

First Definition of a Finite Group.

If we wish to restrict our definition to groups of the nth degree, we may add to the postulates 1, 2, 3 the following:

11. *The assemblage shall contain only n elements.*

The postulates 1, 2, 3, 11 will then be independent of each other when $n > 2$.

Thus, to prove the independence of 1, take the assemblage of the first n positive integers ($n > 1$), with $a \circ b = a$, and to prove the independence of 2 take the same assemblage, with $a \circ b = b$.

To prove the independence of 3, take the assemblage of the first n positive integers ($n > 2$), with the rule of combination defined as follows:

$$\begin{aligned} a \circ b &= a + b \quad \text{when} \quad a + b \leqq n, \\ &= a + b - n \quad \text{when} \quad a + b > n \end{aligned}$$

except that

$$a \circ b = 2 \quad \text{when} \quad a + b = 1 \text{ or } n + 1,$$

and

$$a \circ b = 1 \quad \text{when} \quad a + b = 2 \text{ or } n + 2.$$

*Since each of the three systems here mentioned satisfies 10, we see that no one of the postulates 1, 2, 3 can be deduced from the other two, even with the aid of 10.

This assemblage does not satisfy 3, since $(1 \circ 1) \circ 2 = 1 \circ 2 = 3$, while $1 \circ (1 \circ 2) = 1 \circ 3 = 4$ when $n > 3$, and $= 2$ when $n = 3$.

To prove the independence of 11, consider any infinite group, such as either of the examples mentioned above.*

It should be noticed that the proof of 10 can be made much simpler when we are able to use 11. Thus, let a be any fixed element, and let c_k run through the whole assemblage. Then for every element c_k there is an element b_k such that $a \circ b_k = c_k$, by 1; and all these b's are different elements, by 6; that is, b_k also runs through the whole assemblage. Hence $a \circ b$ is always an element of the assemblage, for the given element a. Similarly for every other element a.

Second Definition of a Finite Group.

We have just shown that a finite group may be defined by a set of *four* postulates, each independent of the other three. The definition usually given, as for example by Weber, loc. cit., includes *five* postulates, viz., the propositions here numbered 10, 6, 7, 3 and 11.† It is interesting to notice, in conclusion, that these five also form a set of independent postulates when $n > 2$.

Thus, to prove the independence of 10, consider the assemblage of the first n positive integers with $a \circ b = a + b$.

To prove the independence of 6 and 7 consider the assemblage of the first n positive integers ($n > 1$), with $a \circ b = a$ and $a \circ b = b$ respectively.

And to prove the independence of 3 and 11 consider the assemblages already used for the same purpose in the preceding paragraph.

HARVARD UNIVERSITY, CAMBRIDGE, MASS.

* Since each of the four systems here considered satisfies 10, we see that no one of the postulates 1, 2, 3, 11 can be deduced from the other three, even with the aid of 10.

† The propositions 1 and 2 being readily deduced from these as theorems.