sider the cylinder as a special case of the cone, *i. e.*, a cone whose vertex is at infinity, for when $a = \text{const.}$, $b = \text{const.}$, the conditions that the line generates a cone, viz., $p = ka + k_1$, $q = kb + k_2$ become $p = \text{const.}$, $q = \text{const.}$ and the two consecutive generators actually coincide. Thus, we cannot say, that the shortest distance between two consecutive generators of a cylinder is zero, *i. e.*, that the two generators actually intersect. There is no shortest distance between two such lines; they are everywhere equally distant. Hence, to find the distance between two consecutive parallel lines, we shall have to use the formula for the distance of a point from a line. It is easily seen that, in general, this distance is an infinitesimal of the first order; it is zero only if the two consecutive lines coincide; it is infinite when $a^2 + b^2 + 1 = 0$. Hence

THEOREM IX. *The distance between two consecutive generators of a cylinder is, in general, an infinitesimal of the first order; if the generator is a minimal straight line, the distance is infinite.*

COLUMBIA UNIVERSITY.

NOTE ON THE COMMUTATOR OF TWO OPERATORS.

BY PROFESSOR G. A. MILLER.

(Read before the American Mathematical Society, April 27, 1907.)

THERE is a confusing lack of uniformity with respect to the use of the term commutator. The present note aims to exhibit this fact and to point out some of its sources in the hope that these data may tend towards greater uniformity in the use of this term and also make its various meanings less confusing to the reader.

The operation now known as the commutator of two operators was used for a long time in the development of group theory before it received a special name. It is frequently employed, in various forms, in Jordan's Traité des substitutions, and its elegant application in the study of direct products was recognized by Hölder* and others. The first paper which deals with the

*Hölder, *Math. Annalen*, vol. 34 (1889), p. 35. It should be noted that the reference 91) in Encyklopädie der mathematischen Wissenschaften, vol. 1, p. 219. should be to this article instead of to the later one in vol. 43.

important properties of the subgroups formed by the commutators of every pair of operators in a finite group appeared in the *Quarterly Journal of Mathematics* in 1896.* In this paper the commutator of s and t is represented by $sts^{-1}t^{-1}$, but no special name is assigned to the operation. Its form was suggested by the form of the alternant (Klammerausdruck) in the theory of continuous groups.

Towards the close of 1896 Frobenius reproduced some of the fundamental theorems relating to the commutator subgroup † (giving due credit both to the earlier publication and to Dedekind's unpublished work along the same line) and called the operation $s^{-1}t^{-1}st$ the commutator of t and s, following Dedekind.

Shortly after this Dedekind published an article in the *Mathematische Annalen*‡ in which he gave some of the known properties of the commutator subgroup and defined $s^{-1}t^{-1}st$ as the commutator of t and s just as Frobenius had done. About a year later $s^{-1}t^{-1}st$ was defined § as the commutator of s and t, instead of the commutator of t and s as had been done in the articles just cited, and it was observed that the interchange of s and t in $s^{-1}t^{-1}st$ gives its inverse, thus leading to two commutators of s and t if the order of these operators is not observed.

In Weber's Lehrbuch der algebra, volume 2 (1899), page 133, the second definition of commutator given above is adopted, so that Weber's commutator is the inverse of that given by Frobenius and Dedekind. Some writers say that both of the two operators $s^{-1}t^{-1}st$ and $t^{-1}s^{-1}ts$ are commutators of s and t, thus giving a double meaning to this term. This definition appears implicitly in the last article cited above and is adopted by Easton in his Constructive development of group theory, 1902, page 57 and also by De Séguier in his Groupes abstraits, 1904, page 8. A disadvantage of this definition is that the expression "commutator of s and t" may mean either one of two operators.

If the elements of the commutator $s^{-1}t^{-1}st$ are permuted in every possible manner there result eight operators which may be distinct and differ from the identity. Each of them has the

* Vol. 28, p. 266.
† Frobenius, *Berliner Sitzungsberichte*, 1896, p. 1348.
‡ Dedekind, *Math. Annalen*, vol. 48 (1897), p. 553.
§ BULLETIN, vol. 4 (1898), p. 135.

property that it is explicitly the transform of an operator multiplied by its inverse, and hence all of them have been called commutators.* Four of them are conjugate under $\{s, t\}$, while the others are the inverses of these four. Hence they have the same order and all of them occur in the commutator subgroup of the group generated by s and t. In fact they generate this subgroup. As long as we are concerned only with the properties of the commutator subgroup, it does not matter which of the eight forms considered above is regarded as the commutator of s and t. In fact, all of them may be regarded as commutators of these elements in this connection. In view of the fact that the commutator subgroup, has played the principal rôle in the discussions in which the term commutator has been employed, it is not surprising that there should have been some laxity in the definition of the term.

While the eight commutators considered above play the same rôle with respect to the commutator subgroup, they have quite different properties if considered as factors of s and t. For instance, $s^{-1}t^{-1}st$ is the factor which multiplied on the right into s $(s \cdot s^{-1}t^{-1}st)$ gives the transform of s with respect to t, but it has no such property as regards t. In fact, the product of this commutator into t will generally have an order which differs from the order of t and hence there is, in general, no operator which transforms t into itself multiplied by this commutator. From this it follows that $s^{-1}t^{-1}st$ has entirely different properties with respect to the two operators s, t and the question arises whether it would not be desirable to select for the commutator of s, t an operator whose properties with respect to s and t are more nearly alike.

Two of the eight commutators $(s^{-1}t^{-1}st,\ t^{-1}sts^{-1},\ sts^{-1}t^{-1},\ ts^{-1}t^{-1}s,\ t^{-1}s^{-1}ts,\ st^{-1}s^{-1}t,\ tst^{-1}s^{-1},\ s^{-1}tst^{-1})$ which are obtained by permuting the elements of $s^{-1}t^{-1}st$ are such that the products obtained by multiplying them into s or t will be of the same order as s or t respectively. Two others will not change the order of s, but will generally change the order of t, if used

*BULLETIN, vol. 5 (1899), p. 239. The general definition of a commutator is "the product of the transform of an operator and its inverse." On this point all authors agree. The disagreements relate to the definition of a commutator by means of its elements. When we speak of the commutators of a group it is assumed that the elements of the commutators are also found in the group and hence it may happen that only a small number of its operators are commutators. Since every operator of a group may be represented by a positive substitution and all positive substitutions are commutators, it follows that every possible operator is a commutator of some elements.

as factors with s or t, while two others will not change the order of t but will change the order of s. The remaining two will, in general, change the order of both t and s if they are multiplied into these operators respectively. From this standpoint it does not appear desirable to call either $ts^{-1}t^{-1}s$ or $st^{-1}s^{-1}t$ a commutator of s and t. That is, if we regard the commutator as a factor which must be multiplied into an operator in order to obtain its conjugate (and this is a very useful concept) neither of the two operators $ts^{-1}t^{-1}s$, $st^{-1}s^{-1}t$ is a commutator of s or t since we cannot generally transform s or t into themselves multiplied by one of these two operators. From this point of view $s^{-1}t^{-1}st$ and $tst^{-1}s^{-1}$ are commutators of s but not of t, $t^{-1}s^{-1}ts$ and $sts^{-1}t^{-1}$ are commutators of t but not of s, while $t^{-1}sts^{-1}$ and $s^{-1}tst^{-1}$ are commutators of both s and t.

From the preceding paragraph it follows that for some important uses of the commutator it would appear desirable to call $t^{-1}sts^{-1}$ the commutator of s and t, and $s^{-1}tst^{-1}$ the commutator of t and s, while $s^{-1}t^{-1}st$ and $t^{-1}s^{-1}ts$ might be called the commutators of s with respect to t and of t with respect to s respectively. Although the main objects of this note are to call attention to the history and the nature of the commutator, yet the reasons given above seem to demand a new definition of the term and we shall hereafter call $t^{-1}sts^{-1}$ *the commutator of* s *and* t. If this is done the eight commutators mentioned at the beginning of the preceding paragraph are respectively the commutators of t^{-1} and s, s and t, t and s^{-1}, s^{-1} and t^{-1}, s^{-1} and t, t^{-1} and s^{-1}, s and t^{-1}, t and s. These eight commutators are conjugate under the octic group.

It is well known that every simple isomorphism of a group G with itself may be obtained by transforming all of its operators by some operator in its holomorph. In such an isomorphism each operator corresponds to itself multiplied by some operator of G. If G involves s and t, and if we transform G by t, the operator which corresponds to s may be obtained by multiplying s on the left by the commutator of s and t. By multiplying t on the right by the same commutator we obtain its transform with respect to s^{-1}. As in many instances (such as finding the operators of G which transform a function into one of its conjugates) it is desirable to employ left hand multiplication, the advantages of the last definition of commutator become apparent. In conclusion it may be said that it seems very desirable that the term commutator should

be completely defined by giving its elements in order. That is, the expression 'commutator of s and t' should not have a double meaning. For the most important applications which have been made of commutators any one of the given definitions seems just as good as any other, but there are applications in which the last definition seems to be the most convenient. It may be added that the definition of commutator in the Encyklopädie der Mathematischen Wissenschaften, Volume I 1, page 210, is rendered meaningless by typographical errors.

A THEOREM IN THE THEORY OF NUMBERS.

BY PROFESSOR D. N. LEHMER.

(Read before the San Francisco Section of the American Mathematical Society, December 19, 1903.)

LAGRANGE has shown that if the indeterminate equation $x^2 - Ry^2 = \pm D$ is resolvable in integers, D being less than $\sqrt{R}$, and x and y being relative primes, then D is a denominator of a complete quotient in the expansion of $\sqrt{R}$ in a continued fraction. (For a proof of this theorem, see Chrystal's Algebra II, page 451.) Making use of this result, we may prove the following interesting theorem, which is sometimes very effective in finding the factors of large numbers.

If R is the product of two factors which differ by less than $2\sqrt[4]{R}$, these two factors may be found directly from the expansion of $\sqrt{R}$ in a continued fraction.

Let the two factors be p and q, so that $R = pq$. Then $R = [\frac{1}{2}(p+q)]^2 - [\frac{1}{2}(p-q)]^2$, and the equation $x^2 - Ry^2 = [\frac{1}{2}(p-q)]^2$ is resolvable in integers. If now $[\frac{1}{2}(p-q)]^2$ is less than $\sqrt{R}$, then by the theorem quoted above, there will be a denominator of a complete quotient in the expansion of $\sqrt{R}$ equal to $[\frac{1}{2}(p-q)]^2$. Since $[\frac{1}{2}(p-q)]^2 < \sqrt{R}$, then $p - q < 2\sqrt[4]{R}$. Moreover the values of the indeterminates in the equation $x^2 - Ry^2 = \pm D$, are furnished by the numerator and denominator of the convergent which immediately precedes the complete quotient having D for a denominator. Hence it follows that the expansion of $\sqrt{R}$ need not be carried farther than is sufficient to make the numerator of the convergent as