This conic is tangent to the curve at $t = 0$, $t = \infty$, and intersects the curve at six other points. At one of the latter points a tangent to the conic is tangent to the curve at some other point. We may summarize with this theorem: *The self-dual plane rational quintic admitting of the greatest possible number of correlations is invariant under a G_{12} consisting of collineations and correlations.*

THROOP COLLEGE,
February, 1919.

GROUPS CONTAINING A RELATIVELY LARGE NUMBER OF OPERATORS OF ORDER TWO.

BY PROFESSOR G. A. MILLER.

(Read before the American Mathematical Society March 29, 1919.)

§ 1. *Introduction.*

IT is well known that every group which contains at least one operator of order 2 must contain an odd number of such operators and that there is an infinite number of groups such that each of them contains exactly $2m + 1$ operators of order 2, where m is an arbitrary positive integer or 0. It is also known that if exactly one half of the operators of a group are of order 2 then the order of this group must be of the form $2(2m + 1)$ and it must be the dihedral or the generalized dihedral group of this order. Moreover, it has been proved that a group G of order

$$g = 2^\alpha(2m + 1)$$

cannot contain more than $2^\alpha m + 2^\alpha - 1$ operators of order 2, α being an arbitrary positive integer, and whenever G contains this number of operators of order 2 it is either the abelian group of order 2^α and of type $(1, 1, 1, \cdots)$ or it is the direct product of the abelian group of order $2^{\alpha-1}$ and of type $(1, 1, 1, \cdots)$ and the dihedral or the generalized dihedral group of order $2(2m + 1)$.*

* G. A. Miller, this BULLETIN, vol. 13 (1907), p. 235.

From these theorems it results directly that when the order of a group is given but no other restrictions are imposed on the group, it is always possible to find an integer which represents the upper limit for the number of operators of order 2 contained in a group of this order, and also to state how many groups of this order contain this number of operators of order 2. In particular, there is no group of order 1,000 which contains more than

$$2^3 \cdot 62 + 2^3 - 1 = 503$$

operators of order 2, and there are exactly three groups of order 1,000 which contain separately 503 operators of this order since there are three abelian groups of order p^3, p being a prime number.

When the number of operators of order 2 contained in G exceeds $g/2$, this excess cannot be an even number, for if it were an even number $2m$ it would result that the order of G would have to be twice an odd number. In fact, if we let $2k$ represent the number of the operators of order greater than 2 in such a group, it would follow that

$$2k + 2m + 1 = g/2.$$

Since a group whose order is twice an odd number contains a subgroup of half its order composed of its operators of odd order, it results that $m = 0$ whenever $2m$ represents the number of the operators of order 2 in excess of half the order of the group. That is, *whenever more than half of the operators of a group are of order* 2 *this excess is an odd number.* This elementary theorem will be generalized in the following section.

Let $g/2 - k$, k being a positive integer, represent the number of the operators of order 2 contained in G. When k is even, g is of the form $2(2m + 1)$ and hence G contains a subgroup of order $2m + 1$. If t represents any operator of order 2 contained in G, the product of t and an operator in this subgroup of order $2m + 1$ cannot be of order 2 unless t transforms this operator into its inverse. As all of the operators of a group must correspond to their inverses whenever more than three-fourths of them correspond to their inverses in an automorphism of the group, it results that when k is even $2m + 1 \leqq 4k$. In particular, *there is only a finite number of groups which satisfy the condition that the number of their operators of order* 2 *is equal to half the order of the group minus a given even number.*

While the number of the operators of order 2 contained in a group cannot be equal to one half of the order of the group plus a positive even number, it can be equal to one-half the order of the group minus an arbitrary positive number. In fact, there is a cyclic group such that the number of its operators of order 2 is $g/2 - k$, k being an arbitrary positive integer. The order of this cyclic group is clearly $2(k+1)$. When $k=2$ or 4 there is no other group satisfying the given condition, but when $k = 6$ there is also a non-cyclic group of order 18 which involves exactly $9 - 6 = 3$ operators of order 2, as can easily be verified.

§ 2. *Groups in Which More Than One-Half of the Operators are of Order Two.*

Whenever more than one half of the operators of G are of order 2, this excess must be an odd number, as was noted above. We shall now prove that this odd number is always of the form $2^a - 1$. When G is abelian and of type $(1, 1, 1, \cdots)$ it is evident that this condition is satisfied. In all other cases G contains a non-invariant operator s_1 of order 2. Let H_1 represent the subgroup of G composed of all the operators of G which are commutative with s_1 and let $G - H_1$ represent the totality of the operators of G which are not contained in H_1. Since each of the operators of $G - H_1$ is non-commutative with s_1 it results that at least one half of these operators have orders which exceed 2, and hence more than one half of the operators of H_1 are of order 2.

When H_1 is abelian it must be of order 2^n and of type $(1, 1, 1, \cdots)$. If it is non-abelian, it contains a non-invariant operator s_2 of order 2, and we let H_2 represent the subgroup composed of all the operators of H_1 which are commutative with s_2. The totality of operators $H_1 - H_2$ will again contain at least as many operators whose orders exceed 2 as the number of its operators of order 2, and the central of H_2 must exceed that of H_1, which, in turn, exceeds that of G. By continuing this process we must arrive at an abelian group H_m composed of all the operators of H_{m-1} which are commutative with one of its non-invariant operators s_m of order 2. The subgroup H_m has an order of the form 2^n and is of type $(1, 1, 1, \cdots)$.

Since H_m is a subgroup of G it is well known that all the operators of G may be uniquely represented as follows:

$$H_m + H_m t_2 + H_m t_3 + \cdots + H_m t_\gamma.$$

As H_m contains each of the operators $s_1, s_2, \cdots, s_m$, it is evident that at least half of the operators in each of these co-sets have orders which exceed 2. On the other hand, there is at most one of the co-sets $H_m t_2, H_m t_3, \cdots, H_m t_\gamma$ in which the number of operators whose orders exceeds 2 is larger than the number of its operators of order 2. To prove this fact it is only necessary to observe that the number of operators of order 2 in Ht_α, $2 \leqq \alpha \leqq \gamma$, is equal to the order of the subgroup of H_m composed of its operators which are commutative with t_α. If this order were less than 2^{n-1} for two values of α the number of operators of order 2 contained in G would be less than $g/2$, 2^n being the order of H_m.

If the number of operators of order 2 in each of the co-sets $H_m t_2, H_m t_3, \cdots, H_m t_\gamma$ is equal to 2^{n-1} then 2^{n-1} represents also the excess over $g/2$ of the number of the operators of order 2 contained in G. If one of these co-sets Ht_α contains more operators whose orders exceed 2 than operators of order 2 this excess is equal to the number of operators of order 2 which are both contained in H_m and commutative with t_α. Hence it has been proved that *whenever the number of the operators of order 2 contained in a group exceeds one half of the order of the group this excess must be of the form* $2^\alpha - 1$.

From the theorem which has just been proved it is easy to find the form of all the possible ratios between g and the number of operators in G whose orders exceed 2 whenever g is of the form 2^k. In fact, this number is evidently $2^{k-1} - 2^\alpha$ and hence this ratio is always of the form

$$\frac{2^k}{2^{k-1} - 2^\alpha} = \frac{2^\beta}{2^{\beta-1} - 1}.$$

Moreover, there is an infinite system of such groups for every positive integral value of $\beta > 1$.* It may also be noted that whenever one of the co-sets Ht_α, $2 \leqq \alpha \leqq \gamma$, involves more operators whose orders exceed 2 than operators of order 2, this co-set is composed of all the operators of G which are commutative with less than one half of the operators of H_m. Hence this co-set involves the inverses of all its operators and therefore each of its operators transforms H_m into itself. As one of these operators is of order 2 this co-set and H_m generate a group whose order is twice the order of H_m, and hence the order of each operator of this co-set is a divisor of 4.

* G. A. Miller, *Annals of Mathematics*, vol. 7 (1906), p. 57.

We proceed to prove that whenever g is not of the form 2^α then exactly one half of the operators in each of the co-sets Ht_α, $2 \leqq \alpha \leqq \gamma$, are of order 2. If this condition were not satisfied, H_m would involve an operator s_1 which would be commutative with an operator t of odd order contained in G and would transform into its inverse an operator t' of order 4 found in the co-set in which more than half the operators would be of order 4. This follows directly from the fact that all the operators of the co-set involving t are commutative with exactly half the operators of H_m while t' is commutative with at most one fourth of the operators of this subgroup.

Let H_1 be the subgroup composed of all the operators of G which are commutative with s_1. If the product of t' and an operator t_1' of order 2 which is found in H_1 but not in H_m had an order larger than 2 then t_1' and t' would be commutative since this product would be transformed into its inverse by s_1 and hence $(t't_1')^{-1} = t'^{-1}t_1'$. Therefore, it results that t' is transformed either into itself or into its inverse by all the operators of the group generated by the operators of order 2 found in H_1 but not in H_m. These operators clearly generate H_1, since H_1 involves an operator of odd order and this operator must be contained in each of its subgroups of index 2.

Since t could not transform t' into its inverse it follows that t and t' are commutative. Their product must be transformed into its inverse by s_1 and hence we are led to the contradictory equation

$$(t't)^{-1} = tt'^{-1}.$$

As the assumptions that one of the given co-sets contains more operators of order 4 than of order 2 and that the order of G is divisible by an odd prime number led to a contradiction, we have proved that exactly half of the operators of each of these co-sets must be of order 2 whenever g is divisible by an odd prime.

It will now be proved that the subgroup of index 2 under H_m composed of all the operators of H_m which are commutative with t_α is the same for every value of α from 2 to γ. If this were not true, the subgroup formed by the operators of H_m which are commutative with t would involve an operator s_1 which would transform into its inverse an operator t_1 not found in the subgroup H_1 composed of all the operators of G which are commutative with s_1. Just as before, we may

prove that t_1 is commutative with t because it is transformed either into itself or into its inverse by all the operators of order 2 contained in H_1 but not in H_m.

Moreover, tt_1 is transformed into $t_1^{-1}t^{-1} = t^{-1}t_1^{-1}$ whenever the order of this product exceeds 2. If this order were 2, s_1 would transform $(tt_1)^2 = t^2t_1^2$ into $t^2t_1^{-2} = t^2t_1^2$. As this leads to a contradiction and as tt_1 is also transformed into tt_1^{-1} by s_1, it results that the two assumptions that G contains operators of odd order and that some of the operators of H_m which are commutative with a certain t_α are not commutative with every t_α, $2 \leqq \alpha \leqq \gamma$, are contradictory. It therefore results that *exactly half of the operators of H_m constitute the central of G whenever g is divisible by an odd prime number.*

Let K represent the central of G and suppose that g is divisible by an odd prime number. The quotient group G/K has an order which is divisible by all the odd divisors of g and at least one half of its operators are of order 2. If exactly half of these operators are of order 2, this quotient group is either the dihedral or the generalized dihedral group whose order is of the form $2(2m + 1)$. If more than one half of its operators are of order 2, we may proceed as above and find a second quotient group in which at least one half of the operators are of order 2. Hence we have established the following theorem: *If the order of a group is $2^\alpha(2m + 1)$, $m > 0$, and if more than one half of its operators are of order 2 then this group contains an invariant subgroup of order $2^{\alpha-1}$ and the corresponding quotient group is either the dihedral or the generalized dihedral group of order $2(2m + 1)$.*

The subgroup of G which corresponds to the subgroup of order $2m + 1$ in the quotient group does not involve any of the operators of H_m which transform each of the operators of G whose orders exceed 2 into their inverses, since more than one half of the operators of the former subgroup have orders greater than 2. This subgroup must be abelian since all of its operators whose orders exceed 2 correspond to their inverses in an automorphism and the products of these operators must also correspond to their inverses. It therefore results from the preceding theorem that, *if a group whose order is divisible by an odd prime number has the property that at least one half of its operators are of order 2, it is either a dihedral or a generalized dihedral group.* It also results that H_m is identical with H_1 whenever g has an odd prime factor but this is not necessarily true when g is of the form 2^α, as can easily be verified.