GROUPS CONTAINING MAXIMAL SUBGROUPS OF PRIME ORDER

By G. A. Miller

Department of Mathematics, University of Illinois

Communicated May 23, 1941

A maximal subgroup of a group G is a proper subgroup of G which with any operator of G not contained in this subgroup generates G. Every operator of G which does not generate G therefore appears in at least one maximal subgroup of G. A fundamental case presents itself when this maximal subgroup is of prime order p and we begin with a study of this case. When G is abelian this case is very simple since G is then evidently either one of the two possible groups of order p^2 or the cyclic group of order pq, where p and q are distinct prime numbers. In what follows we may therefore confine our attention to the case when G is a non-abelian group which contains a maximal subgroup of prime order and this will be done unless the contrary is explicitly stated.

Suppose now that G contains a maximal subgroup of order *2* generated by the operator s. If t represents any operator of G which is not cummutative with s the two operators s and $t^{-1}st$ are both of order 2 and hence they generate the dihedral group whose order is twice the order of their product. Since s is a maximal subgroup of G this dihedral group is G itself and the order of G is twice an odd prime number since otherwise s would not generate a maximal subgroup of G. Moreover, every such dihedral group contains a maximal subgroup of order 2. Hence there results the following theorem: *A necessary and sufficient condition that a non-abelian group contains a maximal subgroup of order 2 is that it is the dihedral group whose order is twice an odd prime number.*

From the preceding paragraph it results that when G contains a maximal subgroup of order 2 it is non-invariant and G contains also another maximal subgroup of prime order which is invariant under G. The general case when G contains an invariant maximal subgroup of prime order is very simple since G then contains also a non-invariant maximal subgroup of prime order. In fact, if the former maximal subgroup is of order p the order of the latter is a divisor of p-1, where p is an odd prime number. Every prime divisor of p-1 gives rise to a group which has maximal subgroups of two distinct prime orders and we proceed to prove that this includes all the non-abelian groups which contain maximal subgroups of as many as two distinct prime orders. It was noted above that the only abelian group which contains maximal subgroups of as many as two distinct prime orders is the cyclic group of order pq, p and q being distinct prime numbers.

Suppose that G contains a non-invariant maximal subgroup of order p. If the order of G is not a power of p this subgroup must appear in a Sylow subgroup whose oıder is a power of p according to the well-known theorems that every subgroup whose order is a power of p appears in a Sylow subgroup whose order is a power of p whenever the order of the group is not a power of p, and a group whose order is a power of p cannot contain a non-invariant maximal subgroup of order p. Hence G contains Sylow subgroups of order p and as these are maximal they are transformed under G according to a primitive permutation group whose peımutations, besides the identity, which omit one letter, omit exactly one letter. Hence G contains an invariant subgroup of index p generated by its permutations of highest degree according to a well-known theorem due to G. Frobenius (1849–1917).

If this invariant subgroup is of prime order these groups come under the case considered above and hence we may confine our attention here to the case when this subgroup is of composite order. Since G is non-abelian the number of its operators of order p is equal to the order of G multiplied by $(p\text{-}1)/p$. As this is more than half the order of G when p is odd it has been proved that if a non-abelian group contains maximal subgroups of at least two distinct prime orders then the order of this group is pq, p and q being prime numbers such that p-1 is divisible by q. The given invariant subgroup of index p contained in G is a regular permutation group if G is represented on letters corresponding to the given subgroups of order p and hence its order is $1 + kp$. In particular, *a simple group of composite order cannot contain a maximal subgroup of prime order.*

It remains only to determine the possible groups which separately contain maximal subgroups of a single prime order p and in which the invariant subgroup of order $1 + kp$ is not of prime order. The tetrahedral group is an instance of such a group. In this case $p = 3$ and $k = 1$. Another instance is furnished by the group of order 56 which contains eight subgroups of order 7. In this case $p = 7$ and $k = 1$. In both of these cases the invariant subgroup of index p and of order $1 + kp$ is abelian and is composed of operators of the same order besides the identity. It is easy to see that whenever this subgroup is abelian all of its operators besides the identity are of the same order since otherwise this invariant abelian subgroup would involve a characteristic subgroup besides the identity which with a subgroup of order p contained in G would generate a proper subgroup of G. This is impossible since the subgroups of order p are maximal.

When the invariant subgroup of order $1 + kp$ contained in G is non-abelian it must coincide with its commutator subgroup since otherwise this commutator subgroup and a subgroup of order p contained in G would generate a proper subgroup of G. In particular, this invariant subgroup cannot be a solvable non-abelian group. If its order is a power of a prime number it must be abelian and hence all of its operators besides the identity must have the same order. A necessary and sufficient condition that the order of the given invariant subgroup of order $1 + kp$ is a power of a prime number is that the order of G is divisible by two and only two distinct prime numbers and a necessary and sufficient condition that this invariant subgroup is abelian is that all of its operators besides the identity are of the same order. The operators of order p contained in G appear in p-1 sets of conjugates since G contains an invariant subgroup of index p.

The maximal subgroups of order p contained in G are also minimal subgroups of G. It is not difficult to determine all the groups in which every subgroup which is not maximal is minimal and vice versa. It is known that if all the proper subgroups of a group are maximal then all of these subgroups are also minimal and vice versa (these PROCEEDINGS, **27,** 68 (1941)). If the order of a group is divisible by p^3 but exceeds p^3 its subgroups of order p^2 are neither maximal nor minimal and if the order of a group is not divisible by the square of a prime number but by at least three distinct prime numbers the subgroups whose orders are the product of the two largest of these prime numbers are neither maximal nor minimal when the number of these prime numbers exceeds three. When it is three these subgroups are maximal but not minimal. In this case every subgroup of G is either maximal or minimal and there is no subgroup in G which is both maximal and minimal.

Suppose that the order of G is divisible by p^2 but not by p^3 and that it contains subgroups of order p^2 but is of a larger order. These subgroups are then conjugate under G since they are Sylow subgroups. As they are maximal they are transformed under G according to a primitive permutation group which contains a regular invariant subgroup as was noted above. In the present case it must be of prime order since G would otherwise involve a proper subgroup which would include a subgroup of order p. Hence this case comes under the case considered above. If the order of a group is divisible by a higher power of p than p^3 its subgroups of order p^2 are neither maximal nor minimal but in a group of order p^3 every subgroup is either maximal or minimal. If the order of a group is divisible by p^3 but is of a larger order than p^3 its subgroups of order p^2 are neither maximal nor minimal. Hence there results the following theorem: *If the order of a group is the product of two prime numbers, equal or unequal, then each of its proper subgroups is both maximal and minimal; if this order is the product of three such prime numbers then each of the subgroups is either maximal or minimal; if this order is the product of more than three such prime numbers then it contains proper subgroups which are neither maximal nor minimal.*

It was noted above that when G contains a maximal subgroup of order 2 it is dihedral. Suppose, now, that G contains a maximal subgroup or order 3 generated by s_1 and that s_2 is in the same co-set as s_1 with respect to the invariant subgroup of order $1 + 3k$. Since s_1s_2 is of order 3 we have $(s_1s_2)^3 = (s_1s_2^{-1}\, s_1s_2)^3 = 1$. It is easy to prove that $s_1s_2s_1$ generates a cyclic group whose generators are commutative with their conjugates under s_1 and under s_2. That is, if a group contains a maximal subgroup of order 3 it contains an invariant abelian subgroup of index 3 which is either cyclic or of type 1^m. The groups which contain maximal subgroups of order 2 or of order 3 may therefore be regarded as determined, but those which contain maximal subgroups of order 2 are naturally considerably simpler than those which contain maximal subgroups of order 3.

[1] Cf. these PROCEEDINGS **27,** 212–216 (1941).

ON THE RIEMANN HYPOTHESIS IN FUNCTION-FIELDS

BY ANDRÉ WEIL

NEW SCHOOL FOR SOCIAL RESEARCH

Communicated June 11, 1941

A year ago[1] I sketched the outline of a new theory of algebraic functions of one variable over a finite field of constants, which may suitably be described as transcendental, in view of its close analogy with that portion of the classical theory of algebraic curves which depends upon the use of Abelian integrals of the first kind and of Jacobi's inversion theorem; and I indicated how this led to the solution of two outstanding problems, viz., the proof of the Riemann hypothesis for such fields, and the proof that Artin's non-abelian L-functions on such fields are polynomials. I have now found that my proof of the two last-mentioned results is independent of this "transcendental" theory, and depends only upon the algebraic theory of correspondences on algebraic curves, as due to Severi.[2]

Γ being a non-singular projective model of an algebraic curve over an algebraically closed field of constants, the variety of ordered couples (P, Q) of points on Γ has the non-singular model $\Gamma \times \Gamma$ (in a bi-projective space); correspondences are divisors on this model, additively written; they form a module $\mathfrak{C}$ on the ring Z of rational integers. Let Γ_A, Γ_B', Δ, respectively, be the loci of points (P, A), (B, P) and (P, P), on $\Gamma \times \Gamma$, A and B being fixed on Γ and P a generic point of Γ (in the precise sense defined by van der Waerden[3]). The intersection number (C, D) of C and D being defined by standard processes[4] for irreducible, non-coinciding correspondences C, D, will be defined for any C and D which have no irreducible component in common, by the condition of being linear both in C and in D. The degrees $r(C)$, $s(C)$, and the coincidence number $f(C)$