The non-regular transitive substitution groups whose order is the product of three unequal prime numbers.[1]

By

G. A. Miller at Paris.

We shall represent the three prime numbers by p, q, r and assume that $p > q > r$. Since the order of a transitive group is a multiple of its degree and all the groups in question contain an invariant (selfconjugate) subgroup of order p[2]) the degree of these groups must be p, pr, or pq. We shall examine all the possible groups for these three degrees in the given order.

§ 1.

The transitive groups of degree p and of order pqr.

The largest group (H) that transforms the subgroup of order p into itself transforms its substitutions according to the cyclical group of order $p-1$, for p has primitive roots. Hence it is only necessary to consider the subgroups of order qr which are contained in this cyclical group.

Since a cyclical group has one and only one subgroup corresponding to each divisor of its order, the given group of order $p-1$ has one subgroup of order qr, when $p-1$ is divisible by qr. If this condition is fulfilled, H (the metacyclic group) has one and only one subgroup of order pqr[3]). We shall represent this group by G_1. It contains $p-1$ substitutions of order p, $p(q-1)$ of order q, $p(r-1)$ of order r, and $p(qr+1-q-r)$ of order qr.

---

[1]) The regular groups of this order were determined by Cole and Glover (American Journal of Mathematics, vol. 15, pp. 215—220) and by Hölder (Mathematische Annalen, vol. 43, pp. 361—371).

[2]) Cf. Frobenius, Sitzungsberichte der Akademie zu Berlin, 1893, I, p. 343.

[3]) Cf. Netto, Substitutionentheorie, p. 151.

The number of groups of this type, which exist for a given value of p, is clearly equal to the number of pairs of unequal prime factors contained in $p-1$. Hence such groups exist always, when p is larger than 5 and $p-1$ is not a power of 2. The first value of p for which there is more than one such group is 31. In this case there are three groups. Their orders are 186, 310, and 465 respectively.

§ 2.

The transitive groups of degree pr and of order pqr.

The invariant subgroup (H_1) of order pq[1]) must be intransitive, for its order is not a multiple of its degree. Since its systems of intransitivity are permuted according to a transitive group of order r, their number must be r. H_1 may, therefore, be formed by establishing a simple isomorphism between r transitive groups of order pq. As the latter can exist only when $p-1$ is divisible by q, there can be no transitive groups of degree pr and order pqr unless this condition is satisfied. In what follows we shall suppose that it is satisfied.

If we add to H_1 a substitution (t) which merely interchanges its r systems of intransitivity, we obtain a group (G_2) of the required type. G_2 contains the cyclical group of order pr. Each one of its other substitutions transforms the substitutions of the subgroup of order p into one of the $q-1$ powers which belong to the exponent q, modulus p. Those which are not contained in H_1 are of order qr.

When $p-1$ is divisible by qr, we may construct a second group (G_3) of the required degree by using, instead of t, the substitution obtained by multiplying into t a substitution which transforms the substitutions of the subgroup of order p into some one of the $r-1$ powers which belong to the exponent r, modulus p. G_3 contains the non-cyclical transitive group of order pr. Those of its other substitutions which are not found in H_1 are of order qr.

The other groups which may be constructed in the same manner as G_3 are conjugate to it with respect to substitutions which merely interchange the systems of H_1. Hence there are two groups of degree pr and order pqr, whenever $p-1$ is divisible

[1]) Cf. Frobenius, loc. cit.

by qr, when $p-1$ is divisible by q but not by r there is only one such group, when $p-1$ is not divisible by q there is no group of this type.

The smallest set of values of p, q, r is 5, 3, 2. Since $5-1=4$ is not divisible by 3 there is no transitive group of degree 10 and order 30 [1]). The second smallest set of values is 7, 3, 2. In this case $7-1=6$ is divisible by both, 3 und 2. Hence there are two transitive groups of degree 14 and order 42. These two groups contain the following substitutions.

G_2	G_3
abcdefg . hijklmn	*abcdefg . hijklmn*
acegbdf . hjlnikm	*acegbdf . hjlnikm*
adgcfbe . hknjmil	*adgcfbe . hknjmil*
aebfcgd . hlimjnk	*aebfcgd . hlimjnk*
afdbgec . hmkinlj	*afdbgec . hmkinlj*
agfedcb . hnmlkji	*agfedcb . hnmlkji*
bce . dgf . ijl . knm	*bce . dgf . ijl . knm*
abd . cfe . hik . jml	*abd . cfe . hik . jml*
acg . bed . hjn . ilk	*acg . bed . hjn . ilk*
adc . bfg . hkj . imn	*adc . bfg . hkj . imn*
aef . bgc . hlm . inj	*aef . bgc . hlm . inj*
afb . deg . hmi . kln	*afb . deg . hmi . kln*
age . cdf . hnl . jkm	*age . cdf . hnl . jkm*
bec . dfg . ilj . kmn	*bec . dfg . ilj . kmn*
adb . cef . hki . jlm	*adb . cef . hki . jlm*
agc . bde . hnj . ikl	*agc . bde . hnj . ikl*
acd . bgf . hjk . inm	*acd . bgf . hjk . inm*
afe . bcg . hml . ijn	*afe . bcg . hml . ijn*
abf . dge . him . knl	*abf . dge . him . knl*
aeg . cfd . hln . jmk	*aeg . cfd . hln . jmk*
ah . bi . cj . dk . el . fm . gn	*ah . bn . cm . dl . ek . fj . gi*
aickemghbjdlfn	*ai . bh . cn . dm . el . fk . gj*
ajenbkfhclgidm	*aj . bi . ch . dn . em . fl . gk*
akgjfiehdncmbl	*ak . bj . ci . dh . en . fm . gl*
albmcndheifjgk	*al . bk . cj . di . eh . fn . gm*

[1]) Cf. Cole's enumeration of the transitive groups of degree 10 in Quarterly Journal of Mathematics, vol. 27, pp. 40--44.

G_2	G_3
amdiglchfkbnej	*am . bl . ck . dj . ei . fh . gn*
anfldjbhgmekci	*an . bm . cl . dk . ej . fi . gh*
ah . bjeicl . dnfkgm	*ah . bmenck . diflgj*
aidhbk . cmejfl . gn	*aigkcl . bngjeh . fm*
ajghcn . bldiek . fm	*ajfnei . bhcmgl . dk*
akchdj . bmgifn . el	*akejgm . bi . cnfhdl*
alfhem . bncigj . dk	*aldmbj . chekfi . gn*
ambhfi . cj . dlgken	*amcidn . bkghfj . el*
anehgl . bi . ckfjdm	*anblfk . cj . dhgiem*
ah . blciej . dmgkfn	*ah . bkcnem . djglfi*
akbhdi . clfjem . gn	*akflbn . cj . dmeigh*
anchgj . bkeidl . fm	*andicm . bjfhgk . el*
ajdhck . bnfigm . el	*ajbmdl . cifkeh . gn*
amehfl . bjgicn . dk	*amgjek . bi . cldhfn*
aifhbm . cj . dnekgl	*aienfj . blgmch . dk*
alghen . bi . cmdjfk	*alckgi . bhejdn . fm*

§ 3.

The transitive groups of degree pq and of order pqr.

The invariant subgroup of order pq must be transitive. If it is non-cyclical the largest group (H^1) that is commutative to it must be of order $p^2q\ (p-1)$. We can readily prove that the order of H^1 does not exceed $p^2q\ (p-1)$, for H^1 cannot transform a substitution of order q in the given invariant subgroup (H_2) into more than p positions. Another substitution belonging to the same division of H_2 with respect to its invariant subgroup of order p can then be transformed into no more than $p-1$ positions. As there are just pq substitutions that are commutative to all the substitutions of H_2[1]) and the two given substitutions generate H_2 the given statement is proved.

It is also easy to see that the order of H^1 cannot be less than $p^2q\ (p-1)$, for the substitutions of order p which are commutative to all the substitutions of H_2 combined with H_2 generate a group of order p^2q. If we combine with this group a substitution of order $p-1$ which transforms the substitutions

[1]) Jordan, Traité des Substitutions, § 75.

of order p in H_2 into a power which belongs to exponent $p-1$ with respect to modulus p and does not interchange the cycles of these substitutions, we obtain a group of order $p^2q\ (p-1)$ that contains H_2 as an invariant subgroup. This group must, therefore, be H^1.

The groups in question must be subgroups of H^1 and correspond to a group of order r in the group which is isomorphic to H^1 with respect to the given invariant subgroup of order pq. The order of this isomorphic group is $p\,(p-1)$. We have proved that it is isomorphic to a cyclical group of order $p-1$ with respect to its invariant subgroup of order p. Hence there is one and only one group of the required type, whenever $p-1$ is divisible by qr. We shall denote this group by G_4.

G_4 contains an intransitive invariant subgroup of order pr which may be constructed by establishing a simple isomorphism between q transitive groups of degree p and order pr. Its other substitutions not found in H_2 are all of order qr. It remains only to examine the case when the invariant subgroup of order pq is cyclical.

The substitutions of these groups, which are not contained in the given invariant subgroup of order pq (*Hcyc.*), must transform the substitutions of *Hcyv.* into powers which belong to the exponent r, modulus p. To each group correspond $r-1$ different powers. Since the congruence

$$x^r \equiv 1 \pmod{pq}\,,\ p > q > r$$

has one root, when neither $p-1$ nor $q-1$ is divisible by r, r roots, when either $p-1$ or $q-1$ is divisible by r, r^2 roots, when both $p-1$ and $q-1$ are divisible by r [1]), and since the root unity clearly does not correspond to a group; there is one group of the required type, when either $p-1$ or $q-1$ is divisible by r, and there are $r+1$ groups, when both $p-1$ and $q-1$ are divisible by r.

These groups are generated by *Hcyc.* and substitutions of order r which transform any substitution of order pq in *Hcyc.* into one of the required powers. The substitutions of order r may

[1]) Cf. Gauss, Disquisitiones arithmeticae, Sectio III, Art. 92.

easily be found by writing the substitutions of order pq over their required powers in such a way as to make at least one letter correspond to itself. The transforming substitutions found in this way will be of a degree which is less than pq and their rth power must be found in *Hcyc*. This power must, therefore, be unity.

Summary:

Degree.	No. of Groups.	Conditions.
p	1	$p-1$ divisible by qr.
pr	2	$p-1$ divisible by qr.
	1	$p-1$ divisible by q but not by r.
pq	$r+2$	$p-1$ divisible by qr and $q-1$ divisible by r,
	$r+1$	$p-1$ divisible by r but not by q and $q-1$ divisible by r,
	2	$p-1$ divisible by qr and $q-1$ not divisible by r,
	1	$p-1$ divisible by r but not by q and $q-1$ not divisible by r, or $p-1$ not divisible by r and $q-1$ divisible by r.

Paris, July 1896.