On the factorizations of the linear fractional group $LF(2, p^n)$.

By NOBORU ITÔ in Nagoya (Japan).

In the factorization theory of finite groups we refer to the following two theorems of J. SZÉP: (1) Let G admit a maximal Sylow factorization. If neither of the factors is normal, then G is simple. (2) Let H be a non-factorizable simple group. Let P be a minimal representation module of H over the prime field of characteristic p. Let G be the holomorph of P by H. Then in any factorization of G, the meet of the factors contains no normal subgroup ($\neq 1$) of either of the factors. The converse is also true[1][2][3].

Now the purpose of the present paper is to enumerate the factorizations of the linear fractional group $LF(2, p^n)$. This may be done without much difficulties, since all the subgroups of $LF(2, p^n)$ are known[4]. Some of our results, however, may be modified so as to be applied to the higher degree case.

Next, we shall give some remarks on the above theorems of J. SZÉP: (1) We show that $LF(2, p^n)$ with $p^n \equiv 3 \pmod 4$ admits a maximal Sylow factorization in which neither of the factors is normal. The only exceptionals are $LF(2, 3)$ and $LF(2, 7)$. Therefore J. SZÉP's theorem (1) is applicable to prove the simplicity of such groups. In fact, proofs on this line are, as it seems to the writer, more easily comprehensible than the other known proofs. (2) We show that $LF(2, p^n)$ with $p^n \equiv 1 \pmod 4$ admits no factorization. The only exceptionals are $LF(2, 5)$, $LF(2, 3^2)$ and $LF(2, 29)$. Therefore we may take such an $LF(2, p^n)$ as H in J. SZÉP's theorem (2).

§ 1.

Let G be a product of two proper subgroups H and K: $G = H \cdot K$. Then we say that G is factorizable and $G = H \cdot K$ is a factorization of G, where H and K are the factors of this factorization. Let H_1 and K_1 be any conjugate subgroups of H and K respectively. We can get H_1 by transforming H with a suitable element of K, and similarly with K_1. Therefore G admits also the factorization $G = H_1 \cdot K_1$. We say that this factorization of G is equivalent to the original one. Further we refer to the number of non-equivalent factorizations of G simply as the number of factorizations of G.

---

[1]) J. SZÉP, On factorisable simple groups, *these Acta*, **14** (1951), 22.

[2]) J. SZÉP, Zur Theorie der endlichen einfachen Gruppen, *these Acta*, **14** (1951), 111—112. — *Remark of the referee:* By (2) the author means the exceptional case of the theorem in the cited paper. In a previous letter to J. SZÉP the author remarked that the $\mathfrak{N}$ figuring in the proof of this theorem is, in the exceptional case of the theorem, an elementary abelian p-group.

[3]) For definitions see § 1.

[4]) Cf. L. E. DICKSON, *Linear Groups* (Leipzig, 1901), especially Chapter XII.

We introduce an order into the set of all the factorizations of G as follows. Let $G=H\cdot K$ and $G=\tilde{H}\cdot\tilde{K}$ be two factorizations of G. We say that $G=H\cdot K$ is greater than $G=\tilde{H}\cdot\tilde{K}$ if we have either $H\supsetneqq\tilde{H}$ and $K\supset\tilde{K}$ or $H\supset\tilde{H}$ and $K\supsetneqq\tilde{K}$. In this sense we use the terminologies such as a maximal factorization and a minimal factorization. A factorization is maximal if and only if both factors are maximal subgroups. If $H\cap K=1$, with a factorization $G=H\cdot K$, we call this factorization an exact factorization. Obviously an exact factorization is a minimal factorization. An exact factorization $G=H\cdot K$ such that $(H:1, K:1)=1$ we call a Sylow factorization. Then every soluble group admits, by P. HALL's theorem, just one Sylow factorization[5]). There exists, however, a group admitting more than one Sylow factorization, for instance, $LF(2, 11)$ and $LF(2, 23)$ as we show in § 3. Further we remark that these notions are easily modified to those of the factorization classes.

§ 2.

We summarize here the necessary results on subgroups of the linear fractional group $LF(2, p^n)$.[6])

(1) Let q be a prime such that $p^{2n}\equiv 1 \pmod q$ and $p^m \not\equiv 1 \pmod q$ for any $m<2n$. Assume $q\geqq 7$. Then every maximal subgroup of $LF(2, p^n)$, whose order is divisible by q, is a dihedral group D of order p^n+1 for $p>2$ and of order $2(2^n+1)$ for $p=2$. Further, all such subgroups, with a fixed q, are conjugate with one another.

The same holds for $q=5$ and $q=3$ if the order of a maximal subgroup is divisible by q^2. On the contrary, if the order of a maximal subgroup is divisible by q to the first power only, then the subgroup may be one of the following three types of groups for $q=3$: (1) the tetrahedral group A_4 for $p^n\equiv 3 \pmod 8$, (2) the octahedral group S_4 for $p^n\equiv 1 \pmod 8$, and (3) the icosahedral group A_5 for $p^n\equiv\pm 1 \pmod{10}$; and it may be A_5 for $q=5$ and $p^n\equiv\pm 1 \pmod{10}$. Further, the A_4's are all conjugate with one another and the S_4's and the A_5's constitute two classes of conjugate subgroups.

(2) Assume $p>2$. Every maximal subgroup of $LF(2, p^n)$ containing a p-Sylow subgroup of $LF(2, p^n)$ is a normalizer N of the p-Sylow subgroup. They are clearly all conjugate with one another.

(3) Assume $p=2$ and $n>2$. Every maximal subgroup of $LF(2, 2^n)$, whose order is divisible by 2^{n-1}, is the normalizer N of a 2-Sylow subgroup. They are clearly all conjugate with one another.

---

5) P. HALL proved that every soluble group is representable uniquely (up to the conjugation) as a product of pairwise commutative Sylow subgroups. See P. HALL, On the Sylow systems of a soluble group, *Proc. London Math. Soc.*, **43** (1937), 316—323. This theorem can be considered as a generalization of the so-called fundamental theorem of the elementary number theory.

6) See 4).

(4) A theorem of E. GALOIS. $LF(2, p^n)$ always contains subgroups of index p^n+1, but contains subgroups of lower index only when $p^n = 2, 3, 5, 7, 3^2, 11$.

§ 3.

(1) Let us consider the linear fractional group $G = LF(2, p^n)$ other than $LF(2, 2^3)$ and $LF(2, p)$, where p is a Fermat prime: $p = 2^K - 1$. Since the order of G is $\frac{p^n(p^{2n}-1)}{2}$ for $p > 2$ and is $2^n(2^{2n}-1)$ for $p = 2$, we see, by a theorem of K. ZSIGMONDY [7]), that there exists a prime q such that $p^{2n} \equiv 1 \pmod q$ and $p^m \not\equiv 1 \pmod q$ for any $m < 2n$. Let q be the largest one among such primes. We first treat the case $q \geqq 7$.

Let us assume that G is factorizable and let $G = H \cdot K$ be a maximal factorization. Hence both H and K are maximal subgroups of G. Since the order of either H or K is divisible by q, we may assume, by symmetry, that the order of K is divisible by q. Then we have, by § 2(1), that $K = D$. Now we further assume that $p > 2$. Since the order of K is prime to p, H contains a p-Sylow subgroup of G. Therefore, by § 2(2), $H = N$. Since the orders of K and N are p^n+1 and $\frac{p^n(p^n-1)}{2}$ respectively, clearly $N \cap D = 1$. Conversely, if $N \cap D = 1$, then G admits clearly the factorization $G = N \cdot D$. Now if $\frac{p^n-1}{2}$ is odd, that is, if $p^n \equiv 3 \pmod 4$, then $\frac{p^n(p^n-1)}{2}$ and p^n+1 are relatively prime to each other. Therefore $D \cap N = 1$. Hence in this case G admits the only one factorization $G = N \cdot D$. On the other hand if $\frac{p^n-1}{2}$ is even, that is, if $p^n \equiv 1 \pmod 4$, then both $\frac{p^n-1}{2}$ and p^n+1 are even. Since all the elements of order 2 are conjugate with one another and every conjugate subgroup of N can be attained from N by the transformation with a suitable element of D, the element of order 2 of D can be assumed to be contained in N. Therefore $N \cap D > 1$. Hence in this case G admits no factorization.

(2) Now let us assume $p = 2$. Under our assumptions we have clearly $n \geqq 4$. Since the order of D is divisible by 2 only to the first power, we have, by § 2 (3), $H = N$. Since the orders of D and N are $2(2^n+1)$ and $2(2^n-1)$, G clearly admits the factorization $G = D \cdot N$, where the order of $D \cap N$ is 2. Further, let Z be the cyclic subgroup of order 2^n+1 of D. Then also $G = Z \cdot N$, where $Z \cap N = 1$. Hence in this case G admits just two factorizations: $G = D \cdot N$ and $G = Z \cdot N$.

---

7) K. ZSIGMONDY, Zur Theorie der Potenzreste, *Monatshefte für Math. und Phys.*, 3 (1892), 265—284.

(3) Next we treat the case $q=5$. We can, however, by § 2 (1), assume that q divides $p^{2n}-1$ to the first power only and that $p^m \not\equiv 1 \pmod q$ for any $m < 2n$. Since at least one of the three numbers $p-1, p^2-1$ and p^4-1 is divisible by 5, we clearly have that $n \leqq 2$. More precisely if $p \equiv 4 \pmod 5$, then $n=1$, and if $p \equiv 2$ or $3 \pmod 5$, then $n=2$. Further, by a celebrated theorem of E. GALOIS and by § 2 (1), we have only to consider $LF(2, p)$ for $p \leqq 59$ and $p \equiv 4 \pmod 5$, and $LF(2, p^2)$ for $p^2 \leqq 59$ and $p \equiv 2$ or $3 \pmod 5$. Under our assumptions $LF(2, 2^2)$, $LF(2, 3^2)$, $LF(2, 19)$ and $LF(2, 29)$ only can enter into our consideration. Let us first consider $LF(2, 19)$ and $LF(2, 29)$. At any rate, since $19 \equiv 3 \pmod 4$, $LF(2, 19)$ admits the factorization $LF(2, 19) = N \cdot D$, and since $29 \equiv 1 \pmod 4$, $LF(2, 29)$ does not admit such a factorization. Now let us assume that $LF(2, 19)$ and $LF(2, 29)$ admit the following factorizations: $LF(2, 19) = N \cdot A_5$ and $LF(2, 29) = N \cdot A_5$, where A_5 is the icosahedral group. We must have that the order of $N \cap A_5$ is 3 for $LF(2, 19)$ and is 2 for $LF(2, 29)$. Now since these actually hold good for $N \cap A_5$, $LF(2, 19)$ and $LF(2, 29)$ admit actually such factorizations. Since a 3-Sylow subgroup of $LF(2, 19)$ is cyclic, we clearly have that $LF(2, 19) = N \cdot A_5$ is a minimal factorization. On the other hand, let S be the subgroup of order $29 \cdot 7$ of N. Then clearly $LF(2, 29)$ admits the factorization: $LF(2, 29) = S \cdot A_5$ where $S \cap A_5 = 1$. Since A_5's constitute just two classes of conjugate subgroups in both $LF(2, 19)$ and $LF(2, 29)$, we have that $LF(2, 19)$ admits just three factorizations $LF(2, 19) = N \cdot D$ and two $LF(2, 19) = N \cdot A_5$, and that $LF(2, 29)$ admits just four factorizations: two $LF(2, 29) = N \cdot A_5$ and two $LF(2, 29) = S \cdot A_5$.

(4) Secondly let us consider $LF(2, 3^2)$ and $LF(2, 2^2)$. We remark that these are isomorphic to A_6 and A_5 respectively, where A_n is the alternation group of degree n. Now maximal subgroups, of $LF(2, 3^2)$, whose orders are divisible by 3 are N, S_4, and A_5, where S_4 is the octahedral group. Since $3^2 \equiv 1 \pmod 4$, $LF(2, 3^2)$ admits no factorization of the form $LF(2, 3) = H \cdot D$, where H is one of the three groups N, S_4 and A_5. Therefore we clearly have, by § 2 (1), that $K = A_5$. Since a 2-Sylow subgroup of N is cyclic, the order of $N \cap A_5$ is 6. Therefore $LF(2, 3^2)$ admits the factorization $LF(2, 3) = N \cdot A_5$. Since a subgroup of index 6 of A_5 is D, and since all the elements of order 2 of $LF(2, 3^2)$ are conjugate with one another, and since N contains no subgroup of order 12, the factorization $LF(2, 3^2) = N \cdot A_5$ is minimal. Next we consider the case that the $H = S_4 \cdot S_4$'s constitute just two classes of conjugate subgroups in $LF(2, 3^2)$ which we represent by $S_4^{(1)}$ and $S_4^{(2)}$ respectively. Similarly the A_5's constitute just two classes of conjugate subgroups in $LF(2, 3^2)$, which we represent by $A_5^{(1)}$ and $A_5^{(2)}$ respectively. Thereby we can assume, as we easily see, that the order of $S_4^{(i)} \cap A_5^{(i)}$ is 4 for $i=1, 2$ and the order of $S_4^{(i)} \cap A_5^{(j)}$ is 12 for $i, j = 1, 2$ and $i \neq j$. Therefore $LF(2, 3^2)$ admits the factorization $LF(2, 3^2) = S_4^{(i)} \cdot A_5^{(i)}$ for $i = 1, 2$ and does not admit the factorization $LF(2, 3^2) = S_4^{(i)} \cdot A_5^{(j)}$ for $i, j = 1, 2$ and $i \neq j$. Now let $A_4^{(i)}$ be the tetrahedral subgroup

of $S_4^{(i)}$ for $i=1,2$. Since clearly the order of $A_4^{(i)} \cap A_5^{(i)}$ is 4 for $i=1,2$, we have that $LF(2,3^2)$ does not admit the factorization $LF(2,3^2)=A_4^{(i)}\cdot A_5^{(i)}$ for $i=1,2$. Therefore $LF(2,3^2)=S_4^{(i)}\cdot A_5^{(i)}$ for $i=1,2$ is a minimal factorization, where $S_4^{(i)} \cap A_5^{(i)}$ is of order 4. Finally we consider the case $H=A_5^{(1)}$ and $K=A_5^{(2)}$. Then we easily see that the order of $A_5^{(1)} \cap A_5^{(2)}$ is 10. Therefore $LF(2,3^2)$ admits the factorization $LF(2,3^2)=A_5^{(1)}\cdot A_5^{(2)}$. Further let $A_4^{(i)}$ be a tetrahedral subgroup of $A_5^{(i)}$ for $i=1,2$. Then, since clearly the order of $A_4^{(1)} \cap A_5^{(2)}$ and $A_4^{(2)} \cap A_5^{(1)}$ is 2, $LF(2,3^2)$ admits the factorizations $LF(2,3^2)=$ $=A_4^{(1)}\cdot A_5^{(2)}$ and $LF(2,3)=A_5^{(1)}\cdot A_4^{(2)}$ where $A_4^{(1)} \cap A_5^{(2)}$ and $A_5^{(1)} \cap A_4^{(2)}$ are of order 2. These factorizations are clearly minimal factorizations. In altogether, $LF(2,3^2)$ admits just seven factorizations: two $LF(2,3^2)=N\cdot A_5$, two $LF(2,3^2)=S_4\cdot A_5$, $LF(2,3^2)=A_5\cdot A_5$ and two $LF(2,3^2)=A_4\cdot A_5$. Now the case of $LF(2,2^2)$ is rather evident. We immediately have the following result: $LF(2,2^2)$ admits just two factorizations: $LF(2,2^2)=N\cdot D$ and $LF(2,2^2)=Z\cdot N$.

(5) Next we treat again the case $q=3$. We can, as in the case $q=5$, assume, by § 2 (1), that q divides $p^{2n}-1$ to the first power only and that $p^m \not\equiv 1 \pmod q$ for any $m<2n$. Since at least one of two numbers $p-1$ and p^2-1 is divisible by 3, clearly $n=1$ and $p\equiv 2 \pmod 3$. Moreover, by the theorem of E. GALOIS and by § 2 (1), we have only to consider $LF(2,p)$ for $p<59$. Under our assumptions $LF(2,2)$, $LF(2,5)$ $LF(2,11)$ and $LF(2,23)$ only can enter into our consideration. Clearly $LF(2,2)$ admits just one factorization $LF(2,2)=N\cdot Z$, where Z is the 3-Sylow subgroup. Since $LF(2,5)$ $\sim LF(2,2^2)\simeq A_5$, we have first trivially that $LF(2,5)$ admits just two factorization: $LF(2,5)=D\cdot N$ and $LF(2,5)=Z\cdot N$. Let us next consider $LF(2,11)$. At any rate, since $11\equiv 3 \pmod 4$, $LF(2,11)$ admits the factorization $LF(2,11)=N\cdot D$. Further naturally $H=N$. Now, since clearly $N\cap A_4=1$, we see that $LF(2,11)$ admits the following factorizations: $LF(2,11)=N\cdot A_4$ and $LF(2,11)=N\cdot A_5$. Now let Z be the 11-Sylow subgroup of N. Since again we clearly have that $Z\cap A_5=1$, $LF(2,11)$ admits the factorization $LF(2,11)=Z\cdot A_5$. We remark here that the A_5's constitute just two classes of conjugate subgroups in $LF(2,11)$. Thus we see that $LF(2,11)$ admits just six factorization: $LF(2,11)=N\cdot D$, $LF(2,11)=N\cdot A_4$, two $LF(2,11)=N\cdot A_5$ and two $LF(2,11)=Z\cdot A_5$. Finally let us consider $LF(2,23)$. At any rate, since $23\equiv 3 \pmod 4$, $LF(2,23)$ admits the factorization $LF(2,23)=N\cdot D$. Further we have naturally that $H=N$. Now since clearly $N\cap S_4=1$, we see that $LF(2,23)$ admits the factorization $LF(2,23)=N\cdot S_4$ where $N\cap S_4=1$. Since the S_4's constitute just two classes of conjugate subgroups in $LF(2,23)$, we have that $LF(2,23)$ admits just three factorizations $LF(2,23)=N\cdot D$ and two factorizations $LF(2,23)=N\cdot S_4$.

Remark. Obviously the factorizations of $LF(2,11)$: $LF(2,11)=$ $=N\cdot D=N\cdot A_4=Z\cdot A_5^{(1)}=Z\cdot A_5^{(2)}$ and those of $LF(2,23)$: $LF(2,23)=N\cdot D=$ $=N\cdot S_4^{(1)}=N\cdot S_4^{(2)}$ are all Sylow factorizations. Clearly D and A_4 in $LF(2,11)$, or D and S_4 in $LF(2, 23)$, are not isomorphic with each other. Similarly $A_5^{(1)}$ and $A_5^{(2)}$ in $LF(2, 11)$, or $S_4^{(1)}$ and $S_4^{(2)}$ in $LF(2, 23)$ are not conjugate with each other. This shows the Sylow structure theory of P. HALL on soluble groups certainly fails to hold for general finite groups. It may be of interest to find a general method of constructing groups in which the Sylow structure theory does not hold.

Let us lastly consider $LF(2, 2^3)$ and $LF(2, p)$ for $p = 2^k - 1$ $(k \geqq 2)$. Since a 3-Sylow subgroup of $LF(2, 2^3)$ is cyclic, we may assume, by a theorem of H. WIELANDT[8]), that either H or K, say H, by symmetry, contains a 3-Sylow subgroup of $LF(2, 2^3)$. Therefore, as before, we have that $H = D$. Then, since the order of K must be divisible by 2^3, we have, by § 2 (3), that $K = N$. Hence $LF(2, 2^3)$ admits just two factorizations: $LF(2, 2^3) = N \cdot D$ and $LF(2, 2^3) = N \cdot Z$, where Z is the cyclic subgroups of order 9 of K. In other words $LF(2, 2^3)$ admits the same factorizations as $LF(2, 2^n)$ for $n \geqq 4$. Now we treat $LF(2, 3)$. Since $LF(2, 3)$ is isomorphic to the tetrahedral group, we see immediately that $LF(2, 3)$ admits the only one factorization $LF(2,3) = N \cdot D$, where N is a 3-Sylow subgroup and H is the 2-Sylow subgroup of $LF(2, 3)$. So, consider $LF(2, p)$ for $p = 2^k - 1$ $(k \geqq 3)$. At any rate we have, by § 2 (2), that $H = N$. Since the order of N is odd, K clearly contains a 2-Sylow subgroup of $LF(2, p)$. Now let us assume that $k \geqq 4$. Then by § 2 (1), a 2-Sylow subgroup of $LF(2, p)$ is maximal. Clearly it is a dihedral group. Therefore $K = D$. Hence we have that $LF(2, p)$ for $p = 2^k - 1$ $(k \geqq 4)$ admits the only one factorization $LF(2, p) = N \cdot D$, where K is a 2-Sylow subgroup. Finally treat $LF(2, 7)$. Here we have, by § 2 (1), that $LF(2, 7)$ contains as a maximal subgroup the octahedral group S_4. Therefore we have that $K = S_4$. Let Z and D be the 7-Sylow subgroup and a 2-Sylow subgroup of N and S_4 respectively. Since cleary $Z \cap S_4 = 1$ and $N \cap D = 1$, and since S_4's constitute just two classes of conjugate subgroups in $LF(2, 7)$, we have that $LF(2, 7)$ admits just five factorizations: two $LF(2, 7) = N \cdot S_4$, two $LF(2, 7) = Z \cdot S_4$ and $LF(2, 7) = N \cdot D$.

Remark. Thus we see that there exists a simple group with a nilpotent maximal subgroup; $LF(2, p)$ for $p = 2^k - 1$ and $k \geqq 4$ is such one. Naturally such a group is not nilpotent-factorizable, since, otherwise, it must be soluble[9]). It may be of interest to seek for a simple group with a maximal p-Sylow subgroup for $p > 2$.

MATHEMATICAL INSTITUTE
NAGOYA UNIVERSITY.

(Received December 20, 1952.)

[8]) H. WIELANDT, Über das Produkt paarweise vertauschbarer nilpotenter Gruppen, *Math. Zeitschrift*, **55** (1951), 1—7.

[9]) Cf. N. Itô, Remarks on factorizable groups, *these Acta*, **14** (1951), 83—84.