A generalization of SYLOW's theorem.

By G. FROBENIUS.

Every finite group whose order is divisible by the prime p contains elements of order p. (CAUCHY, *Mémoire sur les arrangements que l'on peut former avec des lettres données*. Exercises d'analyse et de physique Mathématique, Vol. III, §. XII, p. 250.) Their number is, as I will show here, always a number of the form $(p-1)(np+1)$. From that theorem, SYLOW deduced the more general one, that a group whose order h is divisible by p^κ, must contain subgroups of order p^κ. (*Théorèmes sur les groupes de substitutions*, Math. Ann., Vol. V.) I gave a simple proof thereof in my work *Neuer Beweis des* SYLOW*'schen Satzes*, CRELLE's Journal, Vol. 100. The number of those subgroups must, as I will show here, always be $\equiv 1 \pmod p$. If p^λ is the highest power of p contained in h, the SYLOW proved this theorem only for the case that $\kappa = \lambda$. Then any two groups of order p^λ contained in $\mathfrak{H}$ are conjugate, and their number $np+1$ is a divisor of h, while for $\kappa < \lambda$ this does not hold in general. I obtain the stated results in a new way from a theorem of group theory that appears to be unnoticed thus far:

In a group of order h, the number of elements whose order divides g is divisible by the greatest common divisor of g and h.

§. 1.

If p is a prime number then any group $\mathfrak{P}$ of order p^λ has a series of invariant subgroups (chief series) $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_{\lambda-1}$ of orders $p, p^2, \ldots, p^{\lambda-1}$, each of which is contained in the subsequent one. SYLOW (loc. cit., p. 588) derives this result from the theorem:

I. *Every group of order p^λ contains an invariant element of order p.*

An invariant element of a group $\mathfrak{H}$ is an element of $\mathfrak{H}$ is permutable with every element of $\mathfrak{H}$. If $\mathfrak{P}$ contains the invariant element P of order p then the powers of P form an invariant subgroup $\mathfrak{P}_1$ of $\mathfrak{P}$ whose order is p. Likewise, $\mathfrak{P}/\mathfrak{P}_1$ has an invariant subgroup $\mathfrak{P}_2/\mathfrak{P}_1$ of order p hence $\mathfrak{P}$ has an invariant subgroup $\mathfrak{P}_2$ of order p^2 which contains $\mathfrak{P}_1$, etc. In my work *Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul*, CRELLE's Journal, Vol. 101 (§. 3, IV), I complemented that theorem with the following remark:

II. *Every group of order $p^{\lambda-1}$ contained in a group of order p^λ is an invariant subgroup.*

Other proofs for this I developed in my work *Über endliche Gruppen*, Sitzungsberichte 1895 (§. 2, III, IV, V; §. 4, II). This can be obtained from Theorem I in the following way: Let $\mathfrak{H}$ be a group of order p^λ, $\mathfrak{G}$ a subgroup of order $p^{\lambda-1}$, P an invariant element of $\mathfrak{H}$ whose order is p, and $\mathfrak{P}$ the group of the powers of P. If $\mathfrak{G}$ is divisible by $\mathfrak{P}$ then $\mathfrak{G}/\mathfrak{P}$ is an invariant subgroup of $\mathfrak{H}/\mathfrak{P}$ because on can assume Theorem II as proven for groups whose order is smaller than p^λ. Thus $\mathfrak{G}$ is an invariant subgroup of $\mathfrak{H}$. If $\mathfrak{G}$ is not divisible by $\mathfrak{P}$ then $\mathfrak{H} = \mathfrak{G}\mathfrak{P}$ meaning every element of $\mathfrak{H}$ can be brought into the form $H = GP$, where G is an element of $\mathfrak{G}$. Now, G is permutable with $\mathfrak{G}$ and P even with every element of $\mathfrak{G}$. Hence also H is permutable with $\mathfrak{G}$.

The theorem mentioned at the onset lends itself to completion in a different direction:

III. *Every invariant subgroup of order p of a group of order p^λ consists of powers of an invariant element.*

Let $\mathfrak{H}$ be a group of order p^λ, $\mathfrak{P}$ an invariant subgroup of order p. If Q is any element of $\mathfrak{H}$ and $q = p^\kappa$ is its order, then the powers of Q form a group $\mathfrak{Q}$ contained in $\mathfrak{H}$ of order q. If $\mathfrak{P}$ is a divisor of $\mathfrak{Q}$ then every element P of $\mathfrak{P}$ is a power of Q, hence permutable with Q. If $\mathfrak{P}$ is not a divisor of $\mathfrak{Q}$ then $\mathfrak{P}$ and $\mathfrak{Q}$ are relatively prime. $\mathfrak{P}$ is permutable with every element of $\mathfrak{H}$ and therefore with every element of $\mathfrak{Q}$. Thence $\mathfrak{P}\mathfrak{Q}$ is a group of order $p^{\kappa+1}$ and $\mathfrak{P}$ is an invariant subgroup of it. But by Theorem II, $\mathfrak{Q}$ is one also. Therefore P and Q are permutable in view of the Theorem:

IV. *If each of the relatively prime groups $\mathfrak{A}$ and $\mathfrak{B}$ is permutable with every element of the other, then every element of $\mathfrak{A}$ is permutable with every element of $\mathfrak{B}$.*

Indeed, if A is an element of $\mathfrak{A}$ and B is an element of $\mathfrak{B}$, then the element

$$A(BA^{-1}B^{-1}) = (ABA^{-1})B^{-1}$$

is contained in both $\mathfrak{A}$ and $\mathfrak{B}$, and is therefore the principal element E.

I want to prove Theorem III also in a second way: If $Q^{-1}PQ = P^a$ then $Q^{-q}PQ^q = P^{a^q}$. Hence if $Q^q = E$ then $a^q \equiv 1 \pmod p$. Now $a^{p-1} \equiv 1 \pmod p$, hence as q and $p-1$ are relatively prime, also $a \equiv 1 \pmod p$ and therewith $PQ = QP$.

Thirdly and finally, the Theorem follows from the more general Theorem:

V. *Every invariant subgroup of a group $\mathfrak{H}$ of order p^λ contains an invariant element of $\mathfrak{H}$ whose order is p.*

Partition the elements of $\mathfrak{H}$ into classes of conjugate elements (conjugate with respect to $\mathfrak{H}$). If a class consists of a single element, then it is an invariant one, and conversely every invariant element of $\mathfrak{H}$ forms a class by itself. Let $\mathfrak{G}$ be an invariant subgroup of $\mathfrak{H}$ and p^κ its order. If the group $\mathfrak{G}$ contains an element of a class then it contains all its elements. Select an element $G_1, G_2, \dots, G_n$ from each of the n classes contained in $\mathfrak{G}$. If the elements of $\mathfrak{H}$ permutable with G_ν form a group of order p^{λ_ν}, then the number of elements of $\mathfrak{H}$ conjugate to G_ν, i.e. the number of elements in the class represented by G_ν, equals $p^{\lambda-\lambda_\nu}$ (CRELLE's Journal, Vol. 100, p. 181). Thence

$$p^\kappa = p^{\lambda-\lambda_1} + p^{\lambda-\lambda_2} + \cdots + p^{\lambda-\lambda_n}.$$

If G_1 is the principal element E then $\lambda = \lambda_1$. Therefore not all the last $n-1$ terms on the right hand side of this equation can be divisible by p. There must exist therefore another index $\nu > 1$ for which $\lambda_\nu = \lambda$ holds. Then G_ν is an invariant element of $\mathfrak{H}$ whose order is $p^\mu > 1$, and the $p^{\mu-1}$-th power of G_ν is an invariant element of $\mathfrak{H}$ of order p that is contained in $\mathfrak{G}$.

§. 2.

I. *If a and b are relative primes, then any element of order $a\,b$ can always, and in a unique way, be written as a product of two elements whose orders are a and b and which are permutable with each other.*

If A and B are two permutable elements whose orders a and b are relative primes, then $AB = C$ has the order ab. Conversely, let C be any element of order ab. Determining the integer numbers x and y such that $ax + by = 1$ and setting $ax = \beta$, $by = \alpha$, there holds $C = C^\alpha C^\beta$, and C^α has, since y is relatively prime to a, the order a, and C^β the order b. (CAUCHY, loc. cit., §. V, p. 179.) Let now also $C = AB$, where A and B have the orders a and b and are permutable with each other. Then $C^\alpha = A^\alpha B^\alpha$, $B^\alpha = B^{by} = E$, $A^\alpha = A^{1-\beta} = A$, thus $A = C^\alpha$ and $B = C^\beta$. Being powers of C, A and B belong to every group to which C belongs.

II. *If the order of a group is divisible by n then the number of those elements of the group whose order divides n is a multiple of n.*

Let $\mathfrak{H}$ be a group of order h and n a divisor of h. For every group whose order is $h' < h$ and for each divisor n' of h', I assume the Theorem as proven. The number of elements of $\mathfrak{H}$ whose order divides n is, if $n = h$ holds, equal to n. So if $n < h$, I can assume the theorem has been proven for every divisor of h which is $> n$. Now if p is a prime dividing $\frac{h}{n}$, then the number of elements of h whose order divides np is divisible by np, hence also by n. Let $np = p^\lambda r$, where r is not divisible by p and $\lambda \geq 1$. Let $\mathfrak{K}$ be the complex of those elements of $\mathfrak{H}$ whose order divides np but not n, hence divisible by p^λ, and let k be the order of this complex. Then it only remains to show that the number k, if it differs from zero, is divisible by n. For that purpose I prove that k is divisible by $p^{\lambda-1}$ and r.

I partition the elements of $\mathfrak{K}$ into systems by assigning two elements to the same system if each is a power of the other. All elements of a system have the same order m. Their number is $\phi(m)$. A system is completely determined by each of its elements A, it is formed by the elements A^{μ} where μ runs through the $\phi(m)$ numbers which are $< m$ and relatively prime to m. If A is an element of the complex $\mathfrak{K}$ then all the elements of the system represented by A belong to the complex $\mathfrak{K}$. Then the order m of A is divisible by p^{λ}, hence also $\phi(m)$ by $p^{\lambda-1}$. Since the number of elements of each system, into which $\mathfrak{K}$ is decomposed, is divisible by $p^{\lambda-1}$, so must k be divisible by $p^{\lambda-1}$.

To show secondly that k is also divisible by r, I partition again the elements of $\mathfrak{K}$ into systems, but of a different kind, yet still such that the cardinality of elements of each system is divisible by r. Every element of $\mathfrak{K}$ can, and in a unique way at that, be represented as a product of an element P of order p^{λ} and a with it permutable element Q whose order divides r. Conversely, every product PQ so obtained belongs to the complex $\mathfrak{K}$.

Let P be some element of order p^{λ}. All elements of $\mathfrak{K}$ that are permutable with P form a group $\mathfrak{Q}$ whose order q is divisible by p^{λ}. The powers of P form a group $\mathfrak{P}$ of order p^{λ} which is an invariant subgroup of $\mathfrak{Q}$. The elements Q of $\mathfrak{Q}$ that satisfy the equation $Y^r = E$ are identical to those that satisfy the equation $Y^t = E$, where t is the greatest common divisor of q and r. The first issue is to determine the number of those elements.

Every element of $\mathfrak{Q}$ can, and in a unique way at that, be represented as a product of an element A whose order is a power of p and a with it permutable element B whose order is not divisible by p.

If the t-th power of AB belongs to the group $\mathfrak{P}$ then

$$(AB)^t = A^t B^t = P^s, \quad \text{hence} \quad A^t = P^s, \quad B^t = E,$$

because also this element can be decomposed in the given fashion in a single way. Thus A^t belongs to $\mathfrak{P}$, hence also A itself because t is not divisible by p. The order of the group $\mathfrak{Q}/\mathfrak{P}$ is $\frac{q}{p^{\lambda}} < h$. The number of (complex) elements of this group that satisfy the equation $Y^t = R$ is therefore a multiple of t, say tu. If $\mathfrak{P}AB$ is such an element then, as A belongs to $\mathfrak{P}$, $\mathfrak{P}A = \mathfrak{P}$, hence $\mathfrak{P}AB = \mathfrak{P}B$. Since B, as an element of $\mathfrak{Q}$, is permutable with P, the complex $\mathfrak{P}B$ contains only one element whose order divides t, namely B itself, whilst the order of every other element of $\mathfrak{P}B$ is divisible by p. Let

$$\mathfrak{P}\mathfrak{B} + \mathfrak{P}B_1 + \mathfrak{P}B_2 + \cdots$$

be the tu distinct (complex) elements of the group $\mathfrak{Q}/\mathfrak{P}$ whose t-th power is contained in $\mathfrak{P}$, then this complex contains all those elements of $\mathfrak{Q}$ whose t-th power (absolutely) equals E. However, only the elements $B, B_1, B_2, \cdots$ have this property. Thus $\mathfrak{Q}$ contains exactly tu elements that satisfy the equation $Y^t = E$, or there are, if P is a certain element of order p^λ, exactly tu elements that are permutable with P and whose order divides r.

The number of elements of $\mathfrak{H}$ permutable with P is q. The number of elements $P, P_1, P_2, \cdots$ of $\mathfrak{H}$ that are conjugate to P with respect to $\mathfrak{H}$ is therefore $\frac{h}{q}$. Then there are exactly tu elements Q_1 in $\mathfrak{H}$ that are permutable with P_1 and whose order divides r. Taking each of the $\frac{h}{q}$ elements $P, P_1, P_2, \cdots$ successively as X and each time as Y the tu elements permutable with X and satisfy the equation $Y^r = E$, one obtains the system $\mathfrak{K}'$ of

$$k' = \frac{h}{q}\, tu$$

distinct elements XY of the complex $\mathfrak{K}$. Now h is divisible by both q and r hence also by their least common multiple $\frac{qr}{t}$. Thus k' is divisible by r. The system $\mathfrak{K}'$ is completely determined by each of its elements. Two distinct systems among $\mathfrak{K}', \mathfrak{K}'', \cdots$ have no element in common. Their order $k', k'', \cdots$ are all divisible by r. Thus also $k = k' + k'' + \cdots$ is divisible by r.

The number of elements of a group that satisfy the equation $X^n = E$ is mn, the integer number m is > 0 because $X = E$ always satisfies that equation.

III. *If the order of a group $\mathfrak{H}$ is divisible by n then the elements of $\mathfrak{H}$ whose order divides n generate a characteristic subgroup of $\mathfrak{H}$ whose order is divisible by n.*

Let $\mathfrak{R}$ be the complex of elements of $\mathfrak{H}$ that satisfy the equation $X^n = E$. If X is an element of $\mathfrak{R}$ and R is any element permutable* with $\mathfrak{H}$ then $R^{-1}XR$ is also an element of $\mathfrak{R}$. Thus $R^{-1}\mathfrak{R}R = \mathfrak{R}$. Let the complex $\mathfrak{R}$ generate a group $\mathfrak{G}$ of order g. Then also $R^{-1}\mathfrak{G}R = \mathfrak{G}$, so that $\mathfrak{G}$ is a characteristic subgroup of $\mathfrak{H}$.

If q^μ is the highest power of a prime q that divides n then q^μ also divides h. Thus $\mathfrak{H}$ contains a group $\mathfrak{Q}$ of order q^μ. Now $\mathfrak{R}$ is divisible by $\mathfrak{Q}$, hence also $\mathfrak{G}$, and consequently g is divisible by q^μ. Since this holds for every prime q that divides n, g is divisible by n.

On the relation of the complex $\mathfrak{R}$ to the group $\mathfrak{G}$ I further note the following: I considered in *Über endliche Gruppen*, §. 1 the powers $\mathfrak{R}, \mathfrak{R}^2, \mathfrak{R}^3, \cdots$ of a complex $\mathfrak{R}$. If in that sequence $\mathfrak{R}^{r+s}$ is the first one that equals one of the foregoing ones $\mathfrak{R}^r$, then $\mathfrak{R}^\rho = \mathfrak{R}^\sigma$ if and only if $\rho \equiv \sigma \pmod{s}$ and ρ and σ are both $\geq r$. Let t be the number uniquely defined by the conditions $t \equiv 0 \pmod{s}$ and $r \leq t < r+s$.

*tn: cf. Frobenius, *Über endliche Gruppen*, SB. Akad. Berlin, 1895 (I), http://dx.doi.org/10.3931/e-rara-18846

Then $\mathfrak{R}^t$ is the only group contained in that sequence of powers. If $\mathfrak{R}$ contains the principal element E then $\mathfrak{R}^{\rho+1}$ is divisible by $\mathfrak{R}^{\rho}$. Hence $\mathfrak{G} = \mathfrak{R}^t$ is divisible by $\mathfrak{R}$. If N is an element of the group $\mathfrak{G}$ then $\mathfrak{G}N = \mathfrak{G}$. More generally then, if $\mathfrak{R}$ is a complex of elements contained in $\mathfrak{G}$ then $\mathfrak{G}\mathfrak{R} = \mathfrak{G}$. Therefore $\mathfrak{R}^{t+1} = \mathfrak{R}^t$, hence $s = 1$ and $t = r$. Consequently, $\mathfrak{R}^r = \mathfrak{R}^{r+1}$ is the first one in the sequence of powers of $\mathfrak{R}$ that equals the subsequent one, and this is the group generated by the complex $\mathfrak{R}$.

IV. *If the order of a group $\mathfrak{H}$ is divisible by the two relatively prime numbers r and s, if there exists in $\mathfrak{H}$ exactly r elements A whose order divides r and exactly s elements B whose order divides s, then each of the r elements A is permutable with each of the s elements B and there exist in $\mathfrak{H}$ exactly rs elements whose order divides rs, namely the rs distinct elements $AB = BA$.*

Indeed, every element C of $\mathfrak{H}$ whose order divides rs can be written as a product of two with each other permutable elements A and B whose orders divide r and s. Now $\mathfrak{H}$ contains no more than r elements A and no more than s elements B. Were it not the case that each of the r elements A is permutable with each of the s elements B and furthermore that the rs elements AB are all distinct, then $\mathfrak{H}$ would contain less than rs elements C. But this contradicts Theorem II.

§. 3.

If the order h of a group $\mathfrak{H}$ divisible by the prime p then $\mathfrak{H}$ contains elements of order p, namely $mp-1$ many, because there exist mp elements in $\mathfrak{H}$ whose order divides p. From this theorem of CAUCHY, SYLOW derived the more general one, that any group whose order is divisible by p^{κ} possesses a subgroup of order p^{κ}. In his proof he draws on the language of the theory of substitutions. If one wants to avoid this, one should apply the procedure that I used in my work *Über endliche Gruppen* in the proof of Theorems V and VII, §. 2.

Another proof is obtained by partitioning the $mp-1$ elements P of order p contained in $\mathfrak{H}$ into classes of conjugate elements. If the elements of $\mathfrak{H}$ permutable with P form a group $\mathfrak{G}$ of order g, then the number of elements conjugate to P is $\frac{h}{g}$. Thus

$$mp-1 = \sum \frac{h}{g}$$

where the sum is to be extended over the different classes into which the elements P are segregated. From this equation it follows that not all the summands $\frac{h}{g}$ are divisible by p. Let p^{λ} be the highest power of p contained in h, and let $\kappa \leq \lambda$. If

$\frac{h}{g}$ is not divisible by p then g is divisible by p^λ. The powers of P form a group $\mathfrak{P}$ of order p, which is an invariant subgroup of $\mathfrak{G}$. The order of the group $\mathfrak{G}/\mathfrak{P}$ is $\frac{g}{p} < h$. For this group we may therefore assume the theorems which we wish to prove for $\mathfrak{H}$ as known. Thus it contains a group $\mathfrak{P}_\kappa/\mathfrak{P}$ of order $p^{\kappa-1}$, and in the case that $\kappa < \lambda$, a group $\mathfrak{P}_{\kappa+1}/\mathfrak{P}$ of order p^κ that is divisible by $\mathfrak{P}_\kappa/\mathfrak{P}$. Consequently, $\mathfrak{H}$ contains the group $\mathfrak{P}_\kappa$ of order p^κ and the group $\mathfrak{P}_{\kappa+1}$ of order $p^{\kappa+1}$ that is divisible by $\mathfrak{P}_\kappa$.

§. 4.

I. *If the order of a group is divisible by the κ-th power of the prime p then the number of groups of order p^κ contained therein is a number of the form $np+1$.*

Let r_κ denote the number of groups of order p^κ contained in $\mathfrak{H}$. Then the number of elements of $\mathfrak{H}$ whose order is p equals $r_1(p-1)$. As shown above, this number has the form $mp-1$. Thus

$$r_1 \equiv 1 \pmod{p}. \tag{1.}$$

Let $r_{\kappa-1} = r$, $r_\kappa = s$, and let

$$\mathfrak{A}_1, \mathfrak{A}_2, \cdots, \mathfrak{A}_r \tag{2.}$$

be the r groups of order $p^{\kappa-1}$ contained in $\mathfrak{H}$ and

$$\mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_s \tag{3.}$$

the s groups of order p^κ. Suppose the group $\mathfrak{A}_\rho$ is contained in a_ρ of the groups (3.). Suppose the group $\mathfrak{B}_\sigma$ is divisible by b_σ of the groups (2.). Then

$$a_1 + a_2 + \cdots + a_r = b_1 + b_2 + \cdots + b_s \tag{4.}$$

is the number of distinct pairs of groups $\mathfrak{A}_\rho, \mathfrak{B}_\sigma$ for which $\mathfrak{A}_\rho$ is contained in $\mathfrak{B}_\sigma$.

Let $\mathfrak{A}$ be one of the groups (2.). Of the groups (3.) let $\mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_a$ be those which are divisible by $\mathfrak{A}$. By §. 3, $a > 0$, and by Theorem II, §. 1, $\mathfrak{A}$ is an invariant subgroup of each of these a groups, hence also of their least common multiple $\mathfrak{G}$. Therefore the group $\mathfrak{G}/\mathfrak{A}$ contains the a groups $\mathfrak{B}_1/\mathfrak{A}, \mathfrak{B}_2/\mathfrak{A}, \cdots, \mathfrak{B}_a/\mathfrak{A}$ of order p and none further. Indeed, if $\mathfrak{B}/\mathfrak{A}$ is a group of order p contained in $\mathfrak{G}/\mathfrak{A}$ then $\mathfrak{B}$ is a group of order p^κ divisible by $\mathfrak{A}$. By formula (1.) there holds $a \equiv 1 \pmod{p}$. Thus

$$a_\rho \equiv 1, \quad a_1 + a_2 + \cdots + a_r \equiv r \pmod{p}. \tag{5.}$$

Now I need the Lemma:

The number of groups of order $p^{\lambda-1}$ which are contained in a group of order p^λ is $\equiv 1 \pmod p$.

I suppose this Lemma is already proven for groups of order p^κ if $\kappa < \lambda$. Then, if in the above expansion $\kappa < \lambda$ then

$$b_\sigma \equiv 1, \quad b_1 + b_2 + \cdots + b_s \equiv s \pmod p. \tag{6.}$$

Therefore $r \equiv s$ or $r_{\kappa-1} \equiv r_\kappa \pmod p$, and since this congruence holds for each value $\kappa < \lambda$, it is

$$1 \equiv r_1 \equiv r_2 \equiv \cdots \equiv r_{\lambda-1} \pmod p.$$

Applying this result to a group $\mathfrak{H}$ whose order is p^λ, it is therefore $r_{\lambda-1} \equiv 1 \pmod p$ for such a group, and with this, the above Lemma is proven also for groups of order p^λ, if it holds for groups of order $p^\kappa < p^\lambda$, it is therefore generally valid. For each value κ consequently, $r_\kappa \equiv r_{\kappa-1}$ and therefore $r_\kappa \equiv 1 \pmod p$.

In exactly the same way one proves the more general Theorem:

II. *If the order of a group $\mathfrak{H}$ divisible by the κ-th power of the prime p, if $\vartheta \le \kappa$ and $\mathfrak{P}$ is a group of order p^ϑ contained in $\mathfrak{H}$, then the number of groups of order p^κ contained in $\mathfrak{H}$ that are divisible by $\mathfrak{P}$ is a number of the form $np+1$.*

§. 5.

The Lemma used in §. 4 can be also proven in the following way by relying on the Theorem: Every group $\mathfrak{H}$ of order p^λ has a subgroup $\mathfrak{A}$ of order $p^{\lambda-1}$ and such a subgroup is always an invariant one. Let $\mathfrak{A}$ and $\mathfrak{B}$ be two distinct subgroups of order $p^{\lambda-1}$ contained in $\mathfrak{H}$ and let $\mathfrak{D}$ be their greatest common divisor. Since $\mathfrak{A}$ and $\mathfrak{B}$ are invariant subgroups of $\mathfrak{H}$, so is $\mathfrak{D}$ one, and since $\mathfrak{H}$ is the least common multiple of $\mathfrak{A}$ and $\mathfrak{B}$, $\mathfrak{D}$ has order $p^{\lambda-2}$. Thus $\mathfrak{H}/\mathfrak{D}$ is a group of order p^2. Any such group has, depending on whether it is a cyclic group or not, 1 or $p+1$ subgroups of order p, thus in our case $p+1$, since $\mathfrak{A}/\mathfrak{D}$ and $\mathfrak{B}/\mathfrak{D}$ are two distinct groups of this type. Therefore $\mathfrak{H}$ contains exactly $p+1$ distinct groups of order $p^{\lambda-1}$ that are divisible by $\mathfrak{D}$.

The group $\mathfrak{H}$ always contains a group $\mathfrak{A}$ of order $p^{\lambda-1}$. If it contains yet another one, then $\mathfrak{H}$ has an invariant subgroup $\mathfrak{D}$ of order $p^{\lambda-2}$ which is contained in $\mathfrak{A}$ and for which the group $\mathfrak{H}/\mathfrak{D}$ is not a cyclic one. Let $\mathfrak{D}_1, \mathfrak{D}_2, \cdots, \mathfrak{D}_n$ be all the groups of this kind. The there exist in $\mathfrak{H}$ besides $\mathfrak{A}$ other p groups of order $p^{\lambda-1}$ divisible by $\mathfrak{D}_1$

$$\mathfrak{A}_1, \mathfrak{A}_2, \cdots, \mathfrak{A}_p \tag{1.}$$

and likewise p groups that are divisible by $\mathfrak{D}_2$

$$\mathfrak{A}_{p+1}, \mathfrak{A}_{p+2}, \cdots, \mathfrak{A}_{2p}, \tag{2.}$$

etc., and finally p groups divisible by $\mathfrak{D}_n$

$$\mathfrak{A}_{(n-1)p+1}, \mathfrak{A}_{(n-1)p+2}, \cdots, \mathfrak{A}_{np+1}. \tag{3.}$$

The $np+1$ groups $\mathfrak{A}, \mathfrak{A}_1, \cdots, \mathfrak{A}_{np}$ are all the groups of order $p^{\lambda-1}$ contained in $\mathfrak{H}$ since each such group $\mathfrak{B}$ has to have in common with $\mathfrak{A}$ a certain divisor $\mathfrak{D}$ which is one of the n groups $\mathfrak{D}_1, \mathfrak{D}_2, \cdots, \mathfrak{D}_n$. They are furthermore all distinct. Indeed, if $\mathfrak{A}_1 = \mathfrak{A}_{p+1}$ was true then $\mathfrak{A}_1$ would be divisible by both groups $\mathfrak{D}_1$ and $\mathfrak{D}_2$, hence also by their least common multiple $\mathfrak{A}$. If $\mathfrak{P}$ is a group of order p^{ϑ} contained in $\mathfrak{H}$ then one can subject all the groups considered above to the condition of being divisible by $\mathfrak{P}$. If conversely $\mathfrak{H}$ is an invariant subgroup of a group $\mathfrak{P}$ of order p^{ϑ} then one can require that they all be invariant subgroups of $\mathfrak{P}$.

With the help of Theorem V, §.1 it is easy to prove that the number of groups of order $p^{\lambda-1}$ that are contained in a group of order p^{λ} equals 1 only if $\mathfrak{H}$ is a cyclic group.

I. *The number of invariant subgroups of order p^{κ} contained in a group of order p^{λ} is a number of the form $np+1$.*

Let $\mathfrak{H}$ be a group of order h, let p^{λ} be the highest power of p contained in h, let $\kappa \leq \lambda$ and $\mathfrak{P}_{\kappa}$ any group of order p^{κ} contained in $\mathfrak{H}$. Each group $\mathfrak{P}_{\kappa}$ is contained in $np+1$ groups, hence at least one. I divide the groups $\mathfrak{P}_{\kappa}$ into two kinds. For a group of the first kind there exists a group $\mathfrak{P}_{\lambda}$ of which $\mathfrak{P}_{\kappa}$ is an invariant subgroup, for a group of the second kind no such group exists. The number of elements of $\mathfrak{H}$ permutable with $\mathfrak{P}_{\kappa}$ is divisible by p^{λ} in the first case, and in the second case it is not. The number of groups conjugate to $\mathfrak{P}_{\kappa}$ is therefore divisible by p in the second case, in the first one it is not. Hence diving the groups $\mathfrak{P}_{\kappa}$ into classes of conjugate groups one recognizes that the number of groups $\mathfrak{P}_{\kappa}$ of the second kind is divisible by p. Consequently the number of groups $\mathfrak{P}_{\kappa}$ of the first kind is $\equiv 1 \pmod{p}$.

II. *If $\mathfrak{H}$ is a group of order p^{λ} and $\mathfrak{G}$ is an invariant subgroup of $\mathfrak{H}$ whose order is divisible by p^{κ} then the number of groups of order p^{κ} contained in $\mathfrak{G}$ that are invariant subgroups of $\mathfrak{H}$ is a number of the form $np+1$.*

Also here let more generally p^{λ} be the highest power of the prime p that divides the order h of $\mathfrak{H}$. Let $\mathfrak{G}$ be an invariant subgroup of $\mathfrak{H}$ whose order g is divisible by p^{κ}. The number of all groups $\mathfrak{P}_{\kappa}$ of order p^{κ} contained in $\mathfrak{G}$ is $\equiv 1 \pmod{p}$. I divide them into groups of the first and the second kind (with respect to $\mathfrak{H}$) and further into classes of conjugate groups. If $\mathfrak{G}$ is divisible by $\mathfrak{P}_\kappa$ then $\mathfrak{G}$ is also divisible by every group conjugate to $\mathfrak{P}_\kappa$. Therefrom the claim follows in the same way as above. One can also easily prove it directly by means of the method used in §. 4:

Let the order of $\mathfrak{H}$ be $h = p^\lambda$. By Theorem V, §.1 the group $\mathfrak{G}$ contains elements of order p that are invariant elements of $\mathfrak{H}$. They form, together with the principal element, a group. If p^α is its order then $p^\alpha - 1$ is the number of those elements. By Theorem III, §.1 every invariant subgroup of $\mathfrak{H}$ whose order is p consists of the powers of such an element. Therefore there exist in $\mathfrak{G}$ $r = \frac{p^\alpha-1}{p-1}$ groups of order p that are invariant subgroups of $\mathfrak{H}$. This number is

$$r \equiv 1 \pmod{p}. \tag{4.}$$

Let

$$\mathfrak{A}_1, \mathfrak{A}_2, \cdots, \mathfrak{A}_r \tag{5.}$$

be those r groups and let

$$\mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_s \tag{6.}$$

be the s groups of order p^κ contained in $\mathfrak{G}$ that are invariant subgroups of $\mathfrak{H}$. Let $\mathfrak{B}$ be one of the groups (6.). Among the groups (5.) let $\mathfrak{A}_1, \mathfrak{A}_2, \cdots, \mathfrak{A}_b$ be those contained in $\mathfrak{B}$. By (4.) is then $b \equiv 1 \pmod{p}$. Let $\mathfrak{A}$ be one of the groups (5.). Among the groups (6.) let $\mathfrak{B}_1, \mathfrak{B}_2, \cdots, \mathfrak{B}_a$ be those divisible by $\mathfrak{A}$. Then $\mathfrak{B}_1/\mathfrak{A}, \mathfrak{B}_2/\mathfrak{A}, \cdots, \mathfrak{B}_a/\mathfrak{A}$ are the groups of order $p^{\kappa-1}$ contained in $\mathfrak{G}/\mathfrak{A}$ that are invariant subgroups of $\mathfrak{H}/\mathfrak{A}$. By the method of induction is therefore $a \equiv 1 \pmod{p}$. Resorting to the same notation as in §. 4 there holds

$$1 \equiv r \equiv a_1 + a_2 + \cdots + a_r \equiv b_1 + b_2 + \cdots + b_s \equiv s \pmod{p}.$$

I add a few remarks on the number of groups $\mathfrak{P}_\kappa$ of the first kind that are conjugate to a particular one, and on the number of classes of conjugate groups into which the groups $\mathfrak{P}_\kappa$ are partitioned.

Let $\mathfrak{P}$ be a group of order p^λ contained in $\mathfrak{P}$ and $\mathfrak{Q}$ an invariant subgroup of $\mathfrak{P}$ of order p^κ. The elements of $\mathfrak{H}$ permutable with $\mathfrak{P}(\mathfrak{Q})$ form a group of $\mathfrak{P}'(\mathfrak{Q}')$ of order $p'(q')$. Let the greatest common divisor of $\mathfrak{P}'$ and $\mathfrak{Q}'$ be the group $\mathfrak{R}$ of order r. The groups $\mathfrak{P}'$, $\mathfrak{Q}'$ and $\mathfrak{R}$ are divisible by $\mathfrak{P}$. Let p^δ be the order of the largest common divisor of $\mathfrak{P}$ and a group conjugate with respect to $\mathfrak{H}$ that is selected in such a way that δ is a maximum. Then (*Über endliche Gruppen*, §. 2, VIII)

$$\frac{h}{p'} \equiv 1 \pmod{p^{\lambda-\delta}}.$$

The group $\mathfrak{R}$ consists of all the elements of $\mathfrak{Q}'$ that are permutable with $\mathfrak{P}$. With this,

$$\frac{q'}{r} \equiv 1 \pmod{p^{\lambda-\delta}}.$$

Consequently,

$$\frac{h}{q'} \equiv \frac{p'}{r} \pmod{p^{\lambda-\delta}}. \tag{7.}$$

Herein, $\frac{h}{q'}$ is the number of groups that are conjugate to $\mathfrak{Q}$ with respect to $\mathfrak{H}$ and $\frac{p'}{r}$ is the number of groups that are conjugate to $\mathfrak{Q}$ with respect to $\mathfrak{P}'$. Indeed, the group $\mathfrak{R}$ consists of all the elements of $\mathfrak{P}'$ that are permutable with $\mathfrak{Q}$. The number of groups in a certain class in $\mathfrak{H}$ is therefore congruent $\pmod{p^{\lambda-\delta}}$ to the number of groups in the corresponding class in $\mathfrak{P}'$.

Furthermore, the number of distinct classes in $\mathfrak{H}$ (into which the groups $\mathfrak{P}_\kappa$ of the first kind are partitioned) equals the number of those classes in $\mathfrak{P}'$. This follows from the Theorem:

III. *If two invariant subgroups of $\mathfrak{P}$ are conjugate with respect to $\mathfrak{H}$ then so they are with respect to $\mathfrak{P}'$.*

Let $\mathfrak{Q}$ and $\mathfrak{Q}_0$ be two invariant subgroups of $\mathfrak{P}$. If they are conjugate with respect to $\mathfrak{H}$ then there exists in $\mathfrak{H}$ such an element H that

$$H^{-1}\mathfrak{Q}_0 H = \mathfrak{Q} \tag{4.}$$

holds. Since $\mathfrak{Q}_0$ is an invariant subgroup of $\mathfrak{P}$, $H^{-1}\mathfrak{Q}_0 H = \mathfrak{Q}$ is an invariant subgroup of

$$H^{-1}\mathfrak{P}H = \mathfrak{P}_0.$$

Hence $\mathfrak{Q}'$ is divisible by $\mathfrak{P}$ and $\mathfrak{P}_0$. Consequently (*Über endliche Gruppen*, §. 2, VII) there exists in $\mathfrak{Q}'$ such an element Q that

$$Q^{-1}\mathfrak{P}_0 Q = \mathfrak{P},$$

hence

$$\mathfrak{P}HQ = HQ\mathfrak{P}$$

holds. Thus $HQ = P$ is an element of $\mathfrak{P}'$. Inserting the expression $H = PQ^{-1}$ into the equation (4.) one obtains, since Q is permutable with $\mathfrak{Q}$,

$$P^{-1}\mathfrak{Q}_0 P = Q^{-1}\mathfrak{Q}Q = \mathfrak{Q}.$$

There exists therefore in $\mathfrak{P}'$ an element P that transforms $\mathfrak{Q}_0$ into $\mathfrak{Q}$.

Partition now the groups $\mathfrak{P}_\kappa$ contained in $\mathfrak{H}$ (of the first kind) into classes of conjugate groups (with respect to $\mathfrak{H}$) and choose from each class a representative. If $\mathfrak{Q}_0$ is one, then $\mathfrak{Q}_0$ is a group of order p^κ which is contained in a certain group $\mathfrak{P}_0$ as an invariant subgroup. If $H^{-1}\mathfrak{P}_0 H = \mathfrak{P}$ then $H^{-1}\mathfrak{Q}_0 H = \mathfrak{Q}$ is an invariant subgroup of $\mathfrak{P}$. One can therefore choose the representatives of different classes in such a way that they are all invariant subgroups of a certain group $\mathfrak{P}$ of order p^λ. Each invariant subgroup of $\mathfrak{P}$ of order p^κ is then conjugate to one of these groups with respect to $\mathfrak{H}$, hence also with respect to $\mathfrak{P}'$. Let the invariant subgroups $\mathfrak{P}_\kappa$ of $\mathfrak{P}$ aggregate into s classes of groups that are conjugate with respect to $\mathfrak{P}'$. Then the groups $\mathfrak{P}_\kappa$ of the first kind of $\mathfrak{H}$ also aggregate into s classes of groups that are conjugate with respect to $\mathfrak{H}$.

Translated with minor typographical corrections from

F. G. Frobenius, "Verallgemeinerung des Sylow'schen Satzes", Sitzungsberichte der Königl. Preuß. Akad. der Wissenschaften zu Berlin, 1895 (II), 981–993.
http://dx.doi.org/10.3931/e-rara-18880

by R. Andreev, Paris (France), August 24, 2016.