G.Frobenius: New Proof of Sylow's Theorem

Translated from German by Sasha Gutfraind*

April 2008

The proposition by Cauchy, that every group, whose order is divisible by a prime p contains an element of order p (*Exerc. d'analyse et de phys. math. vol.III, p.250*), was generalized here by Herr Sylow, saying that a group, whose order is divisible by ν-th power of a prime p, always contains a subgroup of order p^{ν} (*Math. Ann. vol.5*). For the symmetric group, whose elements are all the $n!$ permutations of n symbols, this proposition has already been proven since Cauchy by direct generation of subgroups, and from this lemma the validity of his proposition for any finite group is deduced. The case, that Herr Sylow assumes as known in his deduction of Cauchy's proposition, has induced Herr Netto to develop another proof for the Sylow proposition, in which he starts directly from the Cauchy lemma (*Math Ann. vol.13; Grunert's Archiv, vol.62*). However, the symmetric group, which in all of the these proofs will be brought in, is absolutely foreign to the substance of the Sylow proposition, so I have tried to find a new derivation, in which the Cauchy Lemma is not needed, and this was successful with the help of the methods, which Herr Sylow (*l.c. p.588*) has used for the exploration of the composition of groups whose order is a power of a prime.

The elements of every finite group can considered as substitutions (*this journal, vol.86, p.230*). However, I do not want to base the following proof on this notion. Let there be several elements, which have the following properties (*cf. Kronecker, Berl. Monatsber. 1870, p.882; Weber, Math. Ann. vol.20, p.302)*:

I Every two elements A and B set in the given order specify a unique third which is designated AB.

II From every of both equations $AC = BC$ or $CA = CB$ it follows that $A = B$.

*The following paper (Crelle's J. reine angew. Math. 100 (1887), 179-181) is one of the first to use the abstract formulation of a group (William C. Waterhouse, *The early proofs of Sylow's Theorem*, Archive for History of Exact Sciences **21** (1979), no. 3, 279–290. H Wussing, *The Genesis of the Abstract Group Concept*, Cambridge, MA., 1984.) In many ways, the paper is similar to modern proofs of the theorem: it uses induction, quotient groups, the group center, and the class equation, but remarkably it calls not one of them by name. Style: readers unfamiliar with fraktur letters should note that in roman script: $\mathfrak{H} = H$ and $\mathfrak{G} = G$. The now uncommon style of mathematical communication found in this article has been retained in the English translation, as much as it was possible. Corrections of any kind are very welcome: ag362@cornell.edu.

III To the operation through which A and B equates to AB, applies an associative law: $(AB)C = A(BC)$, but the commutative law $AB = BA$ is not required.

IV The number of elements is finite.

From the three first conditions it follows that there can be no more than one element E (the "chief element"), which satisfies the equation $E^2 = E$, thus constituting a group by itself. If there is also $F = F^2$ then because of I. $(E^2)F = E(F^2)$ or because of III. $EEF = EFF$ and consequently because of II. $E = F$. If A is any element, then so is $AE^2 = AE$ and $E^2A = EA$ and therefore $AE = EA = A$. It is easily found from IV that such a chief element truly exists.

Let now $\mathfrak{H}$ be a group constructed from the given elements, which has order h divisible by ν-th (or higher) power of the prime p. Then it should be shown that $\mathfrak{H}$ contains a subgroup, whose order is p^ν. To simplify the presentation I will assume that it is true for groups whose order is less than h. Those elements of $\mathfrak{H}$ which, like for example, the chief element, commute with any element of $\mathfrak{H}$, make a subgroup $\mathfrak{G}$, whose order g is a divisor of h. I now distinguish two cases:

1. g is divisible by p. Let $A, B, C \dots$ be the elements of $\mathfrak{G}$, any two of which commute with each other (by the definition of this group). Let $a, b, c, \dots$ be their orders and $\alpha, \beta, \gamma, \dots$ integer variables which range from 0 to respectively $a-1, b-1, c-1 \dots$ Then the expression $A^\alpha B^\beta C^\gamma \dots$ makes each element of $\mathfrak{G}$ as often as it makes the chief element E. Hence the product $abc\dots$ is divisible by g as well as by p, and consequently must one of its factors be divisible by p. If this factor is a, then $A^{a/p} = P$ is an element of $\mathfrak{H}$ different from E whose order is exactly p (*cf. this journal vol.86, p.223*). Consider now (*cf. Kronecker, l.c. p.884; Camille Jordan, Bull. de la soc. math de France, vol.I, p.46*) two elements of $\mathfrak{H}$ as (relatively) equal, if they differ from each other by just a power of P, then conditions I-IV are satisfied for this concept of equality as well, because every power of P commutes with every element of $\mathfrak{H}$[1], and the relatively different elements of $\mathfrak{H}$ construct a group, whose order is $\frac{h}{p} < h$, and consequently by the assumption contain a subgroup of order $p^{\nu-1}$. Let Q run through the elements of this subgroup and let λ run through the values 0 to $p-1$, then the p^ν elements $P^\lambda Q$ differ from each other completely, and comprise a group of order p^ν contained in $\mathfrak{H}$.

2. g is not divisible by p. I call two elements A and B "similar" (in reference to $\mathfrak{H}$) if there is an element H in $\mathfrak{H}$, that satisfies the equation $H^{-1}AH = B$. All elements which are completely similar (and here also pair-wise) construct a class of similar elements. Each of the g elements $A_1, A_2, \dots A_g$ of the group $\mathfrak{G}$ constructs for itself a class. If

$$A_1, \dots A_g, \;\; B_1, \dots B_m \qquad (1)$$

[1] If the elements of $\mathfrak{H}$ would not commute with this constructed group from the power of P, then condition I would not be satisfied.

is a complete system of dissimilar elements of $\mathfrak{H}$, then the elements which commute with B_μ, an element of $\mathfrak{H}$, constitute a group $\mathfrak{G}_\mu$, whose order is $g_\mu < h$. Otherwise B_μ would belong to the group $\mathfrak{G}$. Let H run through the h elements of the group $\mathfrak{H}$, and thus $H^{-1}B_\mu H$ runs through all the elements of the class represented by B_μ. Because g_μ of these h elements equal B_μ, and thus every g_μ elements equal to each other. If here h_μ is the number of distinct elements in $\mathfrak{H}$ which are similar to B_μ, then

$$g_\mu h_\mu = h \tag{2}$$

Because each element of $\mathfrak{H}$ is similar to one and only one element of (1), we have that:

$$h = g + h_1 + \ldots + h_m \tag{3}$$

Because h is divisible by p but g is not, then the numbers $h_1, \ldots h_m$ of this equation cannot all be divisible by p. If is h_μ not divisible by p, then by equation (2) the order g_μ of the group $\mathfrak{G}_\mu$ is divisible by p^ν. Since $g_\mu < h$ holds, $\mathfrak{G}_\mu$ as well as $\mathfrak{H}$ contains a subgroup of order p^ν.

Zurich, March 1884.