Note di Matematica **22,** n. 1, 2003, 83–87.

Sylow's Theorem and the arithmetic of binomial coefficients

Marco Barlotti
Dipartimento di Matematica per le Decisioni, Università di Firenze
marco.barlotti@dmd.unifi.it

Virgilio Pannone
Dipartimento di Matematica "U. Dini", Università di Firenze
pannone@math.unifi.it

Received: 23/6/2003; accepted: 23/6/2003.

Abstract. We present a result on the existence and the number of subgroups of any given prime-power order containing an arbitrarily fixed subgroup in a finite group (see also [2]). Our proof is an extension of Krull's generalization ([1], 1961) of Sylow's theorem, which leads us to consider a new concept (the *conditioned binomial coefficient*) of independent combinatorial interest.

Keywords: Sylow's Theorem, Binomial Coefficients.

MSC 2000 classification: 20D20.

dedicated to prof. Adriano Barlotti on the occasion of his 80th birthday

1 Prerequisites

All the groups considered in this paper are finite. The terminology and the notations we use are standard, and can be found, e. g., in [2]. We recall, for later reference, some elementary facts on the behaviour of a subset U of a finite group acting on it by right-multiplication. Let G be a group. If U is a subgroup of G and $g \in G$,

$$Ug = U \iff g \in U.$$

If U is just a subset of G, neither implication is true. Thus we are naturally led to define and study the set

$$R(U) := \{\, g \in G \mid Ug = U \,\}.$$

It is immediate to check that, for any $U \subseteq G$, $R(U)$ is a subgroup of G; we call it the *stabilizer of U under right-multiplication by elements of G* (or, briefly, the *right-stabilizer of U*). Since $U \cdot R(U) = U$, U is union of left cosets of $R(U)$ whence $|R(U)|$ divides $|U|$.

1 Remark. Le G be a group. For any subset U of G such that $1_G \in U$, the following statements are equivalent:

(i) U is a subgroup of G

(ii) $R(U) = U$

(iii) $|R(U)| = |U|$

2 Remark. Let G be a group. For any subset U of G, $|\{Ug \mid g \in G\}| = |G : R(U)|$.

We will also need two results on binomial coefficients. The first one can be obtained by straightforward computation, while the second one is proved in [1].

3 Remark. Let a,b be positive integers such that b divides a. Then

$$\binom{a}{b} = \frac{a}{b} \cdot \binom{a-1}{b-1}$$

4 Remark. Let p be a prime, s a positive integer and g a positive integer divisible by p^s. Then

$$\binom{g-1}{p^s-1} \equiv 1 \mod p$$

2 The main theorem

We want to prove

5 Theorem. *Let G be a finite group, p a prime dividing $|G|$, H a p-subgroup of G. Let $|H| = p^h$ and let k be a positive integer such that $h < k$ and p^k divides $|G|$. Denote by $S_H(p^k)$ the set of all the p-subgroups of G of order p^k which contain H. Then*

$$|S_H(p^k)| \equiv 1 \mod p.$$

We set some notation. Denote by $F_H(p^k)$ the collection of all the subsets of G having cardinality p^k and containing exactly p^{k-h} right cosets of H. For any two subsets U_1, U_2 of G, define $U_1 \sim U_2$ if and only if $U_2 = U_1 g$ for some $g \in G$.

Since G is a group, $\sim$ is an equivalence relation in any set of subsets of G; in particular, $\sim$ is an equivalence relation in $F_H(p^k)$, and thus $F_H(p^k)$ is partitioned into equivalence classes $\Theta_1, \Theta_2, \ldots, \Theta_t$. Therefore we can write

$$|F_H(p^k)| = |\Theta_1| + |\Theta_2| + \cdots + |\Theta_t| \tag{1}$$

We note that the subgroups of G which have order p^k and contain H are exactly the subgroups of G belonging to $F_H(p^k)$. Indeed, let K be a subgroup belonging to $F_H(p^k)$: then its order is p^k and it contains p^{k-h} right cosets of H; these are a partition of K, so in particular 1_G must belong to one of these right cosets, which must be H itself, whence $H \subseteq K$. On the other hand, any subgroup K of G of order p^k containing H will contain exactly p^{k-h} right cosets of H, hence will belong to $F_H(p^k)$.

6 Lemma. *Let $\Theta \subseteq F_H(p^k)$ be an equivalence class of $\sim$. Then*

(a) For any $U \in \Theta$, $\Theta = \{\, Ug \mid g \in G \,\}$

(b) For any $U \in \Theta$, $|\Theta| = |G : R(U)|$

(c) For any $U_1, U_2 \in \Theta$, $R(U_1)$ is conjugate to $R(U_2)$; in particular, $|R(U_1)| = |R(U_2)|$

(d) There exists $U_0 \in \Theta$ such that $1_G \in U_0$

(e) For any $U \in \Theta$, $|\Theta| = \frac{|G|}{p^k} \cdot \frac{p^k}{|R(U)|}$ with $\frac{|G|}{p^k}$ and $\frac{p^k}{|R(U)|}$ integers.

(f) For any $U \in \Theta$, $\frac{p^k}{|R(U)|} = 1$ if and only if Θ contains a subgroup.

(g) If Θ contains a subgroup, it contains only one.

Proof. Statement (a) follows from the fact that $|Ug| = |U|$, so whenever $U \in F_H(p^k)$ then also $Ug \in F_H(p^k)$. By Remark 2 and statement (a) there follows (b).

To prove (c), let $U_2 = U_1 g$ with $g \in G$; then it is easy to check that $R(U_2) = g^{-1}R(U_1)g$.

To prove (d), take any $U \in \Theta$ and any $g \in U$ and observe that $1_G = gg^{-1} \in Ug^{-1} \in \Theta$.

To prove (e), note that p^k divides $|G|$ and $p^k = |U|$, then remember that $|R(U)|$ divides $|U|$.

To prove (f), suppose at first that $|R(U)| = p^k$ and choose, by statement (d), $U_0 \in \Theta$ such that $1_G \in U_0$: since, by statement (c), $|R(U_0)| = |R(U)| = p^k = |U_0|$, by Remark 1 U_0 is a subgroup of G; conversely, suppose that Θ contains a subgroup U_0: since $|R(U)| = |R(U_0)|$ by statement (c), and $|R(U_0)| = |U_0|$ ($= p^k$) by Remark 1, we conclude that $p^k = |R(U)|$.

Finally, statement (g) is obvious because if Θ contains a subgroup L then the elements of Θ are exactly the right cosets of L. This concludes the proof of Lemma 6. $\boxed{QED}$

By statement (e) of Lemma 6, (1) can be rewritten as

$$|F_H(p^k)| = \frac{|G|}{p^k} \cdot \left(\frac{p^k}{|R(U_1)|} + \frac{p^k}{|R(U_2)|} + \cdots + \frac{p^k}{|R(U_t)|} \right) \tag{2}$$

where $U_1, U_2, \ldots, U_t$ are any representatives of the classes $\Theta_1, \Theta_2, \ldots, \Theta_t$. By statements (f) and (g) of Lemma 6, (2) can be rewritten as

$$|F_H(p^k)| = \frac{|G|}{p^k} \cdot \left(|S_H(p^k)| + \frac{p^k}{|R(U_{i_1})|} + \frac{p^k}{|R(U_{i_2})|} + \cdots + \frac{p^k}{|R(U_{i_z})|} \right) \qquad (3)$$

where $S_H(p^k)$ is the number of subgroups of G of order p^k containing H, the sets $U_{i_1}, U_{i_2}, \ldots, U_{i_z}$ are representatives of those classes which do not contain subgroups, and the integers $\frac{p^k}{|R(U_{i_j})|}$ are different from 1.

We now examine the left side of (3). Since the right cosets of H are a partition of the set G into subsets all having cardinality p^h, the number of subsets of G of cardinality p^k containing exactly p^{k-h} components of the partition is equal to the number of choices of p^{k-h} components out of $|G|/p^h$ components. Thus, by Remark 3,

$$|F_H(p^k)| = \binom{\frac{|G|}{p^h}}{p^{k-h}} = \frac{|G|}{p^k} \cdot \binom{\frac{|G|}{p^h} - 1}{p^{k-h} - 1}$$

So (3) can be rewritten as

$$\binom{\frac{|G|}{p^h} - 1}{p^{k-h} - 1} = |S_H(p^k)| + \frac{p^k}{|R(U_{i_1})|} + \frac{p^k}{|R(U_{i_2})|} + \cdots + \frac{p^k}{|R(U_{i_z})|} \qquad (4)$$

Now, the left side of (4) is congruent to 1 modulo p by Remark 4; all the summands on the right side except $S_H(p^k)$ (being divisors of p^k different from 1) are congruent to 0 modulo p; so we can conclude that $|S_H(p^k)| \equiv 1 \mod p$ and Theorem 5 is proved.

3 The conditioned binomial coefficient

In the proof of Theorem 5 we used the collection $F_H(p^k)$ of all the subsets of G having cardinality p^k and containing exactly p^{k-h} right cosets of H. It seems equally natural to work with the family of the subsets of G which have order p^k and contain at least one right coset of H; one can also prove Theorem 5 using this family, provided he has the necessary knowledge of the arithmetical properties of its cardinality. Thus we are led to make the following general definition:

7 Definition. Let a,b,c be positive integers such that $a \geq b \geq c$ and a a multiple of c. Let A be a set of cardinality a partitioned into subsets all of cardinality c. We call *Conditioned Binomial Coefficient* determined by a,b and c, and denote by

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

the number of subsets of A of cardinality b containing at least one component of the partition.

8 Note (Open question). Let a,b,c be positive integers such that c divides b and b divides a. Give a direct proof that

(1) $\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \dfrac{a}{b}\, m \quad \text{with } m \in \mathbb{N}.$

(2) If b is a power of a prime p, then $m \equiv 1 \mod p$.

References

[1] W. Krull: *Über die p-Untergruppen*, Archiv der Math. **12** (1961) p. 1–6.

[2] M. Suzuki: Group Theory I, Springer-Verlag (Berlin, 1982) [English translation of Gunron, Iwanami Shoten (Tokyo, 1977)].

[3] V. Pannone: *A rounded off proof of Sylow's Theorem*, seminar notes typewritten by P. Santaniello (2000).