FORMALIZED MATHEMATICS
2007, Vol. **15**, No. **3**, Pages 159–165

The Sylow Theorems

Marco Riccardi
Casella Postale 49
54038 Montignoso, Italy

Summary. The goal of this article is to formalize the Sylow theorems closely following the book [4]. Accordingly, the article introduces the group operating on a set, the stabilizer, the orbits, the p-groups and the Sylow subgroups.

MML identifier: `GROUP_10`, version: `7.8.05 4.87.985`

The papers [20], [26], [18], [9], [21], [14], [11], [27], [6], [28], [7], [3], [5], [10], [1], [23], [24], [22], [16], [13], [19], [17], [2], [25], [15], [8], and [12] provide the notation and terminology for this paper.

1. Group Operating on a Set

Let S be a non empty 1-sorted structure, let E be a set, let A be an action of the carrier of S on E, and let s be an element of S. We introduce $A \frown s$ as a synonym of $A(s)$.

Let S be a non empty 1-sorted structure, let E be a set, let A be an action of the carrier of S on E, and let s be an element of S. Then $A \frown s$ is a function from E into E.

Let S be a unital non empty groupoid, let E be a set, and let A be an action of the carrier of S on E. We say that A is left-operation if and only if:

(Def. 1) $A \frown (\mathbf{1}_S) = \mathrm{id}_E$ and for all elements s_1, s_2 of S holds $A \frown (s_1 \cdot s_2) = (A \frown s_1) \cdot (A \frown s_2)$.

Let S be a unital non empty groupoid and let E be a set. Note that there exists an action of the carrier of S on E which is left-operation.

Let S be a unital non empty groupoid and let E be a set. A left operation of S on E is a left-operation action of the carrier of S on E.

ISSN 1426–2630

The scheme *ExLeftOperation* deals with a set $\mathcal{A}$, a group-like non empty groupoid $\mathcal{B}$, and a unary functor $\mathcal{F}$ yielding a function from $\mathcal{A}$ into $\mathcal{A}$, and states that:

> There exists a left operation T of $\mathcal{B}$ on $\mathcal{A}$ such that for every element s of $\mathcal{B}$ holds $T(s) = \mathcal{F}(s)$

provided the parameters meet the following requirements:

- $\mathcal{F}(\mathbf{1}_{\mathcal{B}}) = \mathrm{id}_{\mathcal{A}}$, and
- For all elements s_1, s_2 of $\mathcal{B}$ holds $\mathcal{F}(s_1 \cdot s_2) = \mathcal{F}(s_1) \cdot \mathcal{F}(s_2)$.

Next we state the proposition

(1) Let E be a non empty set, S be a group-like non empty groupoid, s be an element of S, and L_1 be a left operation of S on E. Then $L_1 \frown s$ is one-to-one.

Let S be a non empty groupoid and let s be an element of S. We introduce $\boldsymbol{\gamma}_s$ as a synonym of s^*.

Let S be a group-like associative non empty groupoid. The functor $\mathbf{\Gamma}_S$ yielding a left operation of S on the carrier of S is defined as follows:

(Def. 2) For every element s of S holds $\mathbf{\Gamma}_S(s) = \boldsymbol{\gamma}_s$.

Let E be a set and let n be a set. The functor $[E]^n$ yielding a family of subsets of E is defined by:

(Def. 3) $[E]^n = \{X; X$ ranges over subsets of E: $\overline{\overline{X}} = n\}$.

Let E be a finite set and let n be a set. One can verify that $[E]^n$ is finite.

The following two propositions are true:

(2) For every natural number n and for every non empty set E such that $\overline{\overline{n}} \leq \overline{\overline{E}}$ holds $[E]^n$ is non empty.

(3) For every non empty finite set E and for every element k of $\mathbb{N}$ and for all sets x_1, x_2 such that $x_1 \neq x_2$ holds $\mathrm{card}\,\mathrm{Choose}(E, k, x_1, x_2) = \mathrm{card}([E]^k)$.

Let E be a non empty set, let n be a natural number, let S be a group-like non empty groupoid, let s be an element of S, and let L_1 be a left operation of S on E. Let us assume that $\overline{\overline{n}} \leq \overline{\overline{E}}$. The functor $\boldsymbol{\gamma}^n_{s,L_1}$ yields a function from $[E]^n$ into $[E]^n$ and is defined by:

(Def. 4) For every element X of $[E]^n$ holds $\boldsymbol{\gamma}^n_{s,L_1}(X) = (L_1 \frown s)^\circ X$.

Let E be a non empty set, let n be a natural number, let S be a group-like non empty groupoid, and let L_1 be a left operation of S on E. Let us assume that $\overline{\overline{n}} \leq \overline{\overline{E}}$. The functor $\mathbf{\Gamma}^n_{L_1}$ yields a left operation of S on $[E]^n$ and is defined by:

(Def. 5) For every element s of S holds $\mathbf{\Gamma}^n_{L_1}(s) = \boldsymbol{\gamma}^n_{s,L_1}$.

Let S be a non empty groupoid, let s be an element of S, and let Z be a non empty set. The functor $\boldsymbol{\gamma}_{s,Z}$ yielding a function from $[\!:$ the carrier of S, $Z :\!]$ into $[\!:$ the carrier of S, $Z :\!]$ is defined by the condition (Def. 6).

(Def. 6) Let z_1 be an element of $[:$the carrier of $S,\ Z:]$. Then there exists an element z_2 of $[:$the carrier of $S,\ Z:]$ and there exist elements s_1, s_2 of S and there exists an element z of Z such that $z_2 = \boldsymbol{\gamma}_{s,Z}(z_1)$ and $s_2 = s \cdot s_1$ and $z_1 = \langle s_1, z\rangle$ and $z_2 = \langle s_2, z\rangle$.

Let S be a group-like associative non empty groupoid and let Z be a non empty set. The functor $\mathbf{\Gamma}_{S,Z}$ yields a left operation of S on $[:$the carrier of S, $Z:]$ and is defined by:

(Def. 7) For every element s of S holds $\mathbf{\Gamma}_{S,Z}(s) = \boldsymbol{\gamma}_{s,Z}$.

Let G be a group, let H, P be subgroups of G, and let h be an element of H. The functor $\boldsymbol{\gamma}_{h,P}$ yields a function from the left cosets of P into the left cosets of P and is defined by the condition (Def. 8).

(Def. 8) Let P_1 be an element of the left cosets of P. Then there exists an element P_2 of the left cosets of P and there exist subsets A_1, A_2 of G and there exists an element g of G such that $P_2 = \boldsymbol{\gamma}_{h,P}(P_1)$ and $A_2 = g \cdot A_1$ and $A_1 = P_1$ and $A_2 = P_2$ and $g = h$.

Let G be a group and let H, P be subgroups of G. The functor $\mathbf{\Gamma}_{H,P}$ yields a left operation of H on the left cosets of P and is defined as follows:

(Def. 9) For every element h of H holds $\mathbf{\Gamma}_{H,P}(h) = \boldsymbol{\gamma}_{h,P}$.

2. Stabilizer and Orbits

Let G be a group, let E be a non empty set, let T be a left operation of G on E, and let A be a subset of E. The functor T_A yields a strict subgroup of G and is defined as follows:

(Def. 10) The carrier of $T_A = \{g; g$ ranges over elements of G: $(T \frown g)^{\circ} A = A\}$.

Let G be a group, let E be a non empty set, let T be a left operation of G on E, and let x be an element of E. The functor T_x yielding a strict subgroup of G is defined by:

(Def. 11) $T_x = T_{\{x\}}$.

Let S be a unital non empty groupoid, let E be a set, let T be a left operation of S on E, and let x be an element of E. We say that x is fixed under T if and only if:

(Def. 12) For every element s of S holds $x = (T \frown s)(x)$.

Let S be a unital non empty groupoid, let E be a set, and let T be a left operation of S on E. The functor T_0 yields a subset of E and is defined by:

(Def. 13) $$T_0 = \begin{cases} \{x; x \text{ ranges over elements of } E\text{: } x \text{ is fixed under } T\}, \\ \qquad \text{if } E \text{ is non empty}, \\ \emptyset_E, \text{ otherwise.} \end{cases}$$

Let S be a unital non empty groupoid, let E be a set, let T be a left operation of S on E, and let x, y be elements of E. We say that x and y are conjugated under T if and only if:

(Def. 14) There exists an element s of S such that $y = (T \frown s)(x)$.

We now state three propositions:

(4) Let S be a unital non empty groupoid, E be a non empty set, x be an element of E, and T be a left operation of S on E. Then x and x are conjugated under T.

(5) Let G be a group, E be a non empty set, x, y be elements of E, and T be a left operation of G on E. Suppose x and y are conjugated under T. Then y and x are conjugated under T.

(6) Let S be a unital non empty groupoid, E be a non empty set, x, y, z be elements of E, and T be a left operation of S on E. Suppose x and y are conjugated under T and y and z are conjugated under T. Then x and z are conjugated under T.

Let S be a unital non empty groupoid, let E be a non empty set, let T be a left operation of S on E, and let x be an element of E. The functor $T(x)$ yields a subset of E and is defined as follows:

(Def. 15) $T(x) = \{y; y$ ranges over elements of E: x and y are conjugated under $T\}$.

One can prove the following four propositions:

(7) Let S be a unital non empty groupoid, E be a non empty set, x be an element of E, and T be a left operation of S on E. Then $T(x)$ is non empty.

(8) Let G be a group, E be a non empty set, x, y be elements of E, and T be a left operation of G on E. Then $T(x)$ misses $T(y)$ or $T(x) = T(y)$.

(9) Let S be a unital non empty groupoid, E be a non empty finite set, x be an element of E, and T be a left operation of S on E. If x is fixed under T, then $T(x) = \{x\}$.

(10) Let G be a group, E be a non empty set, a be an element of E, and T be a left operation of G on E. Then $\overline{\overline{T(a)}} = |\bullet : T_a|$.

Let G be a group, let E be a non empty set, and let T be a left operation of G on E. The orbits of T yields a partition of E and is defined by:

(Def. 16) The orbits of $T = \{X; X$ ranges over subsets of E: $\bigvee_{x\,:\,\text{element of } E} X = T(x)\}$.

3. p-GROUPS

Let p be a prime natural number and let G be a group. We say that G is a p-group if and only if:

(Def. 17) There exists a natural number r such that $\operatorname{ord}(G) = p^r$.

Let p be a prime natural number, let G be a group, and let P be a subgroup of G. We say that P is a p-group if and only if:

(Def. 18) There exists a finite group H such that $P = H$ and H is a p-group.

One can prove the following proposition

(11) Let E be a non empty finite set, G be a finite group, p be a prime natural number, and T be a left operation of G on E. If G is a p-group, then $\operatorname{card} T_0 \bmod p = \operatorname{card} E \bmod p$.

4. The Sylow Theorems

Let p be a prime natural number, let G be a group, and let P be a subgroup of G. We say that P is a Sylow p-subgroup if and only if:

(Def. 19) P is a p-group and $p \nmid |\bullet : P|_{\mathbb{N}}$.

We now state three propositions:

(12) For every finite group G and for every prime natural number p holds there exists a subgroup of G which is a Sylow p-subgroup.

(13) Let G be a finite group and p be a prime natural number. If $p \mid \operatorname{ord}(G)$, then there exists an element g of G such that $\operatorname{ord}(g) = p$.

(14) Let G be a finite group and p be a prime natural number. Then

(i) for every subgroup H of G such that H is a p-group there exists a subgroup P of G such that P is a Sylow p-subgroup and H is a subgroup of P, and

(ii) for all subgroups P_1, P_2 of G such that P_1 is a Sylow p-subgroup and P_2 is a Sylow p-subgroup holds P_1 and P_2 are conjugated.

Let G be a group and let p be a prime natural number. The functor $\mathsf{Syl}_p(G)$ yielding a subset of $\operatorname{SubGr} G$ is defined as follows:

(Def. 20) $\mathsf{Syl}_p(G) = \{H; H$ ranges over elements of $\operatorname{SubGr} G :$
$\bigvee_{P\,:\,\text{strict subgroup of } G} (P = H \ \wedge\ P$ is a Sylow p-subgroup$)\}$.

Let G be a finite group and let p be a prime natural number. Note that $\mathsf{Syl}_p(G)$ is non empty and finite.

Let G be a finite group, let p be a prime natural number, let H be a subgroup of G, and let h be an element of H. The functor $\boldsymbol{\gamma}_{h,p}$ yielding a function from $\mathsf{Syl}_p(G)$ into $\mathsf{Syl}_p(G)$ is defined by the condition (Def. 21).

(Def. 21) Let P_1 be an element of $\mathsf{Syl}_p(G)$. Then there exists an element P_2 of $\mathsf{Syl}_p(G)$ and there exist strict subgroups H_1, H_2 of G and there exists an element g of G such that $P_2 = \boldsymbol{\gamma}_{h,p}(P_1)$ and $P_1 = H_1$ and $P_2 = H_2$ and $h^{-1} = g$ and $H_2 = {H_1}^g$.

Let G be a finite group, let p be a prime natural number, and let H be a subgroup of G. The functor $\mathbf{\Gamma}_{H,p}$ yields a left operation of H on $\mathsf{Syl}_p(G)$ and is defined as follows:

(Def. 22) For every element h of H holds $\mathbf{\Gamma}_{H,p}(h) = \gamma_{h,p}$.

The following proposition is true

(15) For every finite group G and for every prime natural number p holds $\mathrm{card}(\mathsf{Syl}_p(G)) \bmod p = 1$ and $\mathrm{card}(\mathsf{Syl}_p(G)) \mid \mathrm{ord}(G)$.

5. Appendix

The following propositions are true:

(16) For all non empty sets X, Y holds $\overline{\overline{\{[\!: X, \{y\} :\!] : y \text{ ranges over elements of } Y\}}} = \overline{\overline{Y}}$.

(17) For all natural numbers n, m, r and for every prime natural number p such that $n = p^r \cdot m$ and $p \nmid m$ holds $\binom{n}{p^r} \bmod p \neq 0$.

(18) For every natural number n such that $n > 0$ holds $\mathrm{ord}(\mathbb{Z}_n^+) = n$.

(19) For every group G and for every non empty subset A of G and for every element g of G holds $\overline{\overline{A}} = \overline{\overline{A \cdot g}}$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Nicolas Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3.* Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, 1989.
[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[10] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[12] Artur Korniłowicz. The definition and basic properties of topological groups. *Formalized Mathematics*, 7(**2**):217–225, 1998.
[13] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[14] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[15] Karol Pąk. Cardinal numbers and finite sets. *Formalized Mathematics*, 13(**3**):399–406, 2005.
[16] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.

[17] Dariusz Surowik. Cyclic groups and some of their properties – part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.
[18] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.
[19] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[20] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[21] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[22] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(**5**):955–962, 1990.
[23] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[24] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.
[25] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.
[26] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[27] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[28] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received August 13, 2007