Secondary Sylow Theorems

Jakob von Raumer

November 18, 2018

Abstract

These theories extend the existent proof of the first sylow theorem (written by Florian Kammueller and L. C. Paulson) by what is often called the second, third and fourth sylow theorem. These theorems state propositions about the number of Sylow p-subgroups of a group and the fact that they are conjugate to each other. The proofs make use of an implementation of group actions and their properties.

Contents

theory *GroupAction*
imports
HOL−Algebra.Bij

HOL−Algebra.Sylow
begin

1 Group Actions

This is an implemention of group actions based on the group implementation of HOL-Algebra. An action a group G on a set M is represented by a group homomorphism between G and the group of bijections on M

1.1 Preliminaries and Definition

First, we need two theorems about singletons and sets of singletons which unfortunately are not included in the library.

theorem *singleton-intersection*:
  assumes *A*:*card A* = *1*
  assumes *B*:*card B* = *1*
  assumes *noteq*:$A \neq B$
  shows $A \cap B = \{\}$
⟨*proof*⟩

theorem *card-singleton-set*:
  assumes *cardOne*:$\forall x \in A.(card\ x = 1)$
  shows *card* $(\bigcup A)$ = *card A*
⟨*proof*⟩

Intersecting Cosets are equal:

lemma (**in** *subgroup*) *repr-independence2*:
  assumes *group*:*group G*
  assumes *U*:$U \in rcosets_G\ H$
  assumes *g*:$g \in U$
  shows $U = H\ \#>\ g$
⟨*proof*⟩

locale *group-action* = *group* +
  fixes φ *M*
  assumes *grouphom*:*group-hom G* (*BijGroup M*) φ

context *group-action*
begin

lemma *is-group-action*:*group-action G* φ *M*⟨*proof*⟩

The action of **1** has no effect:

lemma *one-is-id*:
  assumes $m \in M$
  shows $(\varphi\ \mathbf{1})\ m = m$

⟨*proof*⟩

lemma *action-closed*:
  assumes *m*:*m* ∈ *M*
  assumes *g*:*g* ∈ *carrier G*
  shows *φ g m* ∈ *M*
⟨*proof*⟩

lemma *img-in-bij*:
  assumes *g* ∈ *carrier G*
  shows (*φ g*) ∈ *Bij M*
⟨*proof*⟩

The action of *inv g* reverts the action of *g*

lemma *group-inv-rel*:
  assumes *g*:*g* ∈ *carrier G*
  assumes *mn*:*m* ∈ *M n* ∈ *M*
  assumes *phi*:(*φ g*) *n* = *m*
  shows (*φ* (*inv g*)) *m* = *n*
⟨*proof*⟩

lemma *images-are-bij*:
  assumes *g*:*g* ∈ *carrier G*
  shows *bij-betw* (*φ g*) *M M*
⟨*proof*⟩

lemma *action-mult*:
  assumes *g*:*g* ∈ *carrier G*
  assumes *h*:*h* ∈ *carrier G*
  assumes *m*:*m* ∈ *M*
  shows (*φ g*) ((*φ h*) *m*) = (*φ* (*g* ⊗ *h*)) *m*
⟨*proof*⟩

1.2 The orbit relation

The following describes the relation containing the information whether two elements of *M* lie in the same orbit of the action

definition *same-orbit-rel*
  where *same-orbit-rel* = {*p* ∈ *M* × *M*. ∃ *g* ∈ *carrier G*. (*φ g*) (*snd p*) = (*fst p*)}

Use the library about equivalence relations to define the set of orbits and the map assigning to each element of *M* its orbit

definition *orbits*
 where *orbits* = *M* // *same-orbit-rel*

definition *orbit* :: *'c* ⇒ *'c set*
  where *orbit m* = *same-orbit-rel* `` {*m*}

Next, we define a more easy-to-use characterization of an orbit.

lemma *orbit-char*:
assumes *m*:*m* ∈ *M*
shows *orbit m* = {*n*. ∃ *g*. *g* ∈ *carrier G* ∧ (*φ g*) *m* = *n*}
⟨*proof*⟩

lemma *same-orbit-char*:
assumes *m* ∈ *M n* ∈ *M*
shows (*m*, *n*) ∈ *same-orbit-rel* = (∃ *g* ∈ *carrier G*. ((*φ g*) *n* = *m*))
⟨*proof*⟩

Now we show that the relation we've defined is, indeed, an equivalence relation:

lemma *same-orbit-is-equiv*:
shows *equiv M same-orbit-rel*
⟨*proof*⟩

1.3 Stabilizer and fixed points

The following definition models the stabilizer of a group action:

definition *stabilizer* :: *'c* ⇒ -
where *stabilizer m* = {*g* ∈ *carrier G*. (*φ g*) *m* = *m*}

This shows that the stabilizer of *m* is a subgroup of *G*.

lemma *stabilizer-is-subgroup*:
assumes *m*:*m* ∈ *M*
shows *subgroup* (*stabilizer m*) *G*
⟨*proof*⟩

Next, we define and characterize the fixed points of a group action.

definition *fixed-points* :: *'c set*
where *fixed-points* = {*m* ∈ *M*. *carrier G* ⊆ *stabilizer m*}

lemma *fixed-point-char*:
assumes *m* ∈ *M*
shows (*m* ∈ *fixed-points*) = (∀ *g*∈*carrier G*. *φ g m* = *m*)
⟨*proof*⟩

lemma *orbit-contains-rep*:
assumes *m*:*m* ∈ *M*
shows *m* ∈ *orbit m*
⟨*proof*⟩

lemma *singleton-orbit-eq-fixed-point*:
assumes *m*:*m* ∈ *M*
shows (*card* (*orbit m*) = *1*) = (*m* ∈ *fixed-points*)
⟨*proof*⟩

1.4 The Orbit-Stabilizer Theorem

This section contains some theorems about orbits and their quotient groups. The first one is the well-known orbit-stabilizer theorem which establishes a bijection between the the quotient group of the an element's stabilizer and its orbit.

theorem *orbit-thm*:
assumes *m*:$m \in M$
assumes *rep*:$\bigwedge U.\ U \in (carrier\ (G\ Mod\ (stabilizer\ m))) \Longrightarrow rep\ U \in U$
shows *bij-betw* $(\lambda H.\ (\varphi\ (inv\ (rep\ H))\ m))\ (carrier\ (G\ Mod\ (stabilizer\ m)))\ (orbit\ m)$
⟨*proof*⟩

In the case of G being finite, the last theorem can be reduced to a statement about the cardinality of orbit and stabilizer:

corollary *orbit-size*:
assumes *fin*:*finite* $(carrier\ G)$
assumes *m*:$m \in M$
shows $order\ G = card\ (orbit\ m) * card\ (stabilizer\ m)$
⟨*proof*⟩

lemma *orbit-not-empty*:
assumes *fin*:*finite M*
assumes *A*:$A \in orbits$
shows $card\ A > 0$
⟨*proof*⟩

lemma *fin-set-imp-fin-orbits*:
assumes *finM*:*finite M*
shows *finite orbits*
⟨*proof*⟩

lemma *singleton-orbits*:
shows $\bigcup \{N \in orbits.\ card\ N = 1\} = fixed\text{-}points$
⟨*proof*⟩

If G is a p-group acting on a finite set, a given orbit is either a singleton or p divides its cardinality.

lemma *p-dvd-orbit-size*:
assumes *orderG*:$order\ G = p\ \hat{}\ a$
assumes *prime*:*prime p*
assumes *finM*:*finite M*
assumes *Norbit*:$N \in orbits$
assumes $card\ N > 1$
shows $p\ dvd\ card\ N$
⟨*proof*⟩

As a result of the last lemma the only orbits that count modulo p are the fixed points

lemma *fixed-point-congruence*:
assumes *order G* = *p* ^ *a*
assumes *prime p*
assumes *finM*:*finite M*
shows *card M mod p* = *card fixed-points mod p*
⟨*proof*⟩

We can restrict any group action to the action of a subgroup:

lemma *subgroup-action*:
assumes *H*:*subgroup H G*
shows *group-action* (*G*(|*carrier* := *H*|)) *φ M*
⟨*proof*⟩

end

1.5 Some Examples for Group Actions

lemma (**in** *group*) *right-mult-is-bij*:
assumes *h*:*h* ∈ *carrier G*
shows (λ*g* ∈ *carrier G*. *h* ⊗ *g*) ∈ *Bij* (*carrier G*)
⟨*proof*⟩

lemma (**in** *group*) *right-mult-group-action*:
shows *group-action G* (λ*h*. λ*g* ∈ *carrier G*. *h* ⊗ *g*) (*carrier G*)
⟨*proof*⟩

lemma (**in** *group*) *rcosets-closed*:
assumes *HG*:*subgroup H G*
assumes *g*:*g* ∈ *carrier G*
assumes *M*:*M* ∈ *rcosets H*
shows *M* #> *g* ∈ *rcosets H*
⟨*proof*⟩

lemma (**in** *group*) *inv-mult-on-rcosets-is-bij*:
assumes *HG*:*subgroup H G*
assumes *g*:*g* ∈ *carrier G*
shows (λ*U* ∈ *rcosets H*. *U* #> *inv g*) ∈ *Bij* (*rcosets H*)
⟨*proof*⟩

lemma (**in** *group*) *inv-mult-on-rcosets-action*:
assumes *HG*:*subgroup H G*
shows *group-action G* (λ*g*. λ*U* ∈ *rcosets H*. *U* #> *inv g*) (*rcosets H*)
⟨*proof*⟩

end

theory *SubgroupConjugation*
imports *GroupAction*
begin

2 Conjugation of Subgroups and Cosets

This theory examines properties of the conjugation of subgroups of a fixed group as a group action

2.1 Definitions and Preliminaries

We define the set of all subgroups of G which have a certain cardinality. G will act on those sets. Afterwards some theorems which are already available for right cosets are dualized into statements about left cosets.

lemma (**in** *subgroup*) *subgroup-of-subset*:
  assumes *G*:*group G*
  assumes *PH*:$H \subseteq K$
  assumes *KG*:*subgroup K G*
  shows *subgroup H* (*G*(|*carrier* := *K*|))
⟨*proof*⟩

context *group*
begin

definition *subgroups-of-size* ::*nat* ⇒ -
  where *subgroups-of-size p* = {*H*. *subgroup H G* ∧ *card H* = *p*}

lemma *lcosI*: [| *h* ∈ *H*; *H* ⊆ *carrier G*; *x* ∈ *carrier G*|] ==> *x* ⊗ *h* ∈ *x* <# *H*
  ⟨*proof*⟩

lemma *lcoset-join2*:
  assumes *H*:*subgroup H G*
  assumes *g*:*g* ∈ *H*
  shows *g* <# *H* = *H*
⟨*proof*⟩

lemma *cardeq-rcoset*:
  assumes *finite* (*carrier G*)
  assumes *M* ⊆ *carrier G*
  assumes *g* ∈ *carrier G*
  shows *card* (*M* #> *g*) = *card M*
⟨*proof*⟩

lemma *cardeq-lcoset*:
  assumes *finite* (*carrier G*)
  assumes *M*:*M* ⊆ *carrier G*

assumes *g*:*g* ∈ *carrier G*
shows *card* (*g* <# *M*) = *card M*
⟨*proof*⟩

2.2 Conjugation is a group action

We will now prove that conjugation acts on the subgroups of a certain group. A large part of this proof consists of showing that the conjugation of a subgroup with a group element is, again, a subgroup.

lemma *conjugation-subgroup*:
assumes *HG*:*subgroup H G*
assumes *gG*:*g* ∈ *carrier G*
shows *subgroup* (*g* <# (*H* #> *inv g*)) *G*
⟨*proof*⟩

definition *conjugation-action*::*nat* ⇒ -
where *conjugation-action p* = (λ*g*∈*carrier G*. λ*P*∈*subgroups-of-size p*. *g* <# (*P* #> *inv g*))

lemma *conjugation-is-size-invariant*:
assumes *fin*:*finite* (*carrier G*)
assumes *P*:*P* ∈ *subgroups-of-size p*
assumes *g*:*g* ∈ *carrier G*
shows *conjugation-action p g P* ∈ *subgroups-of-size p*
⟨*proof*⟩

lemma *conjugation-is-Bij*:
assumes *fin*:*finite* (*carrier G*)
assumes *g*:*g* ∈ *carrier G*
shows *conjugation-action p g* ∈ *Bij* (*subgroups-of-size p*)
⟨*proof*⟩

lemma *lr-coset-assoc*:
assumes *g*:*g* ∈ *carrier G*
assumes *h*:*h* ∈ *carrier G*
assumes *P*:*P* ⊆ *carrier G*
shows *g* <# (*P* #> *h*) = (*g* <# *P*) #> *h*
⟨*proof*⟩

theorem *acts-on-subsets*:
assumes *fin*:*finite* (*carrier G*)
shows *group-action G* (*conjugation-action p*) (*subgroups-of-size p*)
⟨*proof*⟩

2.3 Properties of the Conjugation Action

lemma *stabilizer-contains-P*:
assumes *fin*:*finite* (*carrier G*)
assumes *P*:*P* ∈ *subgroups-of-size p*

shows $P \subseteq$ *group-action.stabilizer* G (*conjugation-action* p) P
⟨*proof*⟩

corollary *stabilizer-supergrp-P*:
assumes *fin*:*finite* (*carrier* G)
assumes P:$P \in$ *subgroups-of-size* p
shows *subgroup* P (G⦇*carrier* := *group-action.stabilizer* G (*conjugation-action* p) P⦈)
⟨*proof*⟩

lemma (**in** *group*) *P-fixed-point-of-P-conj*:
assumes *fin*:*finite* (*carrier* G)
assumes P:$P \in$ *subgroups-of-size* p
shows $P \in$ *group-action.fixed-points* (G⦇*carrier* := P⦈) (*conjugation-action* p) (*subgroups-of-size* p)
⟨*proof*⟩

lemma *conj-wo-inv*:
assumes QG:*subgroup* Q G
assumes PG:*subgroup* P G
assumes g:$g \in$ *carrier* G
assumes *conj*:*inv* g <# (Q #> g) = P
shows Q #> g = g <# P
⟨*proof*⟩

end

end

theory *SndSylow*
imports *SubgroupConjugation*
begin

no-notation *Multiset.subset-mset* (**infix** <# *50*)

3 The Secondary Sylow Theorems

3.1 Preliminaries

lemma *singletonI*:
assumes $\bigwedge x.\ x \in A \Longrightarrow x = y$
assumes $y \in A$
shows $A = \{y\}$
⟨*proof*⟩

context *group*
begin

lemma *set-mult-inclusion*:
assumes *H*:*subgroup H G*
assumes *Q*:*P* ⊆ *carrier G*
assumes *PQ*:*H* <#> *P* ⊆ *H*
shows *P* ⊆ *H*
⟨*proof*⟩

lemma *card-subgrp-dvd*:
assumes *subgroup H G*
shows *card H dvd order G*
⟨*proof*⟩

lemma *subgroup-finite*:
assumes *subgroup*:*subgroup H G*
assumes *finite*:*finite* (*carrier G*)
shows *finite H*
⟨*proof*⟩

end

3.2 Extending the Sylow Locale

This locale extends the originale *sylow* locale by adding the constraint that the p must not divide the remainder m, i.e. p^a is the maximal size of a p-subgroup of G.

locale *snd-sylow* = *sylow* +
assumes *pNotDvdm*:¬ (*p dvd m*)

context *snd-sylow*
begin

lemma *pa-not-zero*: *p* ^ *a* ≠ *0*
⟨*proof*⟩

lemma *sylow-greater-zero*:
shows *card* (*subgroups-of-size* (*p* ^ *a*)) > *0*
⟨*proof*⟩

lemma *is-snd-sylow*: *snd-sylow G p a m* ⟨*proof*⟩

3.3 Every p-group is Contained in a conjugate of a p-Sylow-Group

lemma *ex-conj-sylow-group*:
assumes *H*:*H* ∈ *subgroups-of-size* (*p* ^ *b*)
assumes *Psize*:*P* ∈ *subgroups-of-size* (*p* ^ *a*)
obtains *g* **where** *g* ∈ *carrier G H* ⊆ *g* <# (*P* #> *inv g*)
⟨*proof*⟩

3.4 Every p-Group is Contained in a p-Sylow-Group

theorem *sylow-contained-in-sylow-group*:
assumes H:$H \in$ *subgroups-of-size* $(p \hat{} b)$
obtains S **where** $H \subseteq S$ **and** $S \in$ *subgroups-of-size* $(p \hat{} a)$
⟨*proof*⟩

3.5 p-Sylow-Groups are conjugates of each other

theorem *sylow-conjugate*:
assumes P:$P \in$ *subgroups-of-size* $(p \hat{} a)$
assumes Q:$Q \in$ *subgroups-of-size* $(p \hat{} a)$
obtains g **where** $g \in$ *carrier* G $Q = g <\# (P \#> inv\ g)$
⟨*proof*⟩

corollary *sylow-conj-orbit-rel*:
assumes P:$P \in$ *subgroups-of-size* $(p \hat{} a)$
assumes Q:$Q \in$ *subgroups-of-size* $(p \hat{} a)$
shows $(P,Q) \in$ *group-action.same-orbit-rel* G (*conjugation-action* $(p \hat{} a)$) (*subgroups-of-size* $(p \hat{} a)$)
⟨*proof*⟩

3.6 Counting Sylow-Groups

The number of sylow groups is the orbit size of one of them:

theorem *num-eq-card-orbit*:
assumes P:$P \in$ *subgroups-of-size* $(p \hat{} a)$
shows *subgroups-of-size* $(p \hat{} a) =$ *group-action.orbit* G (*conjugation-action* $(p \hat{} a)$) (*subgroups-of-size* $(p \hat{} a)$) P
⟨*proof*⟩

theorem *num-sylow-normalizer*:
assumes *Psize*:$P \in$ *subgroups-of-size* $(p \hat{} a)$
shows *card* $(rcosets_{G(\!|carrier := group\text{-}action.stabilizer\ G\ (conjugation\text{-}action\ (p \hat{} a))\ P|\!)} P) * p \hat{} a =$ *card* (*group-action.stabilizer* G (*conjugation-action* $(p \hat{} a)$) P)
⟨*proof*⟩

theorem (**in** *snd-sylow*) *num-sylow-dvd-remainder*:
shows *card* (*subgroups-of-size* $(p \hat{} a)$) *dvd* m
⟨*proof*⟩

We can restrict this locale to refer to a subgroup of order at least p^a:

lemma (**in** *snd-sylow*) *restrict-locale*:
assumes *subgrp*:*subgroup* P G
assumes *card*:$p \hat{} a$ *dvd card* P
shows *snd-sylow* $(G(\!|carrier := P|\!))$ p a $((card\ P)\ div\ (p \hat{} a))$
⟨*proof*⟩

theorem (**in** *snd-sylow*) *p-sylow-mod-p*:

shows *card* (*subgroups-of-size* (*p* ^ *a*)) *mod p* = *1*
⟨*proof*⟩

end

end