The Jordan-Hölder Theorem

Jakob von Raumer

March 17, 2025

Abstract

This submission contains theories that lead to a formalization of the proof of the Jordan-Hölder theorem about composition series of finite groups. The theories formalize the notions of isomorphism classes of groups, simple groups, normal series, composition series, maximal normal subgroups. Furthermore, they provide proofs of the second isomorphism theorem for groups, the characterization theorem for maximal normal subgroups as well as many useful lemmas about normal subgroups and factor groups. The formalization is based on the work work in my first AFP submission [vR14] while the proof of the Jordan-Hölder theorem itself is inspired by course notes of Stuart Rankin [Ran05].

Contents

theory *MaximalNormalSubgroups*
imports *HOL−Algebra.Algebra*
begin

1 Facts about maximal normal subgroups

A maximal normal subgroup of G is a normal subgroup which is not contained in other any proper normal subgroup of G.

locale *max-normal-subgroup* = *normal* +

assumes *proper*: $H \neq$ *carrier* G
assumes *max-normal*: $\bigwedge J.\ J \lhd G \Longrightarrow J \neq H \Longrightarrow J \neq$ *carrier* $G \Longrightarrow \neg\ (H \subseteq J)$

Another characterization of maximal normal subgroups: The factor group is simple.

theorem (**in** *normal*) *max-normal-simple-quotient*:
assumes *finite*: *finite* (*carrier* G)
shows *max-normal-subgroup* H G = *simple-group* (G *Mod* H)
⟨*proof*⟩

end

theory *CompositionSeries*
imports
MaximalNormalSubgroups Secondary-Sylow.SndSylow
begin

hide-const (**open**) *Divisibility.prime*

2 Normal series and Composition series

2.1 Preliminaries

A subgroup which is unique in cardinality is normal:

lemma (**in** *group*) *unique-sizes-subgrp-normal*:
assumes *fin*: *finite* (*carrier* G)
assumes $\exists!Q.\ Q \in$ *subgroups-of-size* q
shows (*THE* $Q.\ Q \in$ *subgroups-of-size* q) $\lhd G$
⟨*proof*⟩

A group whose order is the product of two distinct primes p and q where $p < q$ has a unique subgroup of size q:

lemma (**in** *group*) *pq-order-unique-subgrp*:
assumes *finite*: *finite* (*carrier* G)
assumes *orderG*: *order* $G = q * p$
assumes *primep*: *prime* p **and** *primeq*: *prime* q **and** *pq*: $p < q$
shows $\exists!Q.\ Q \in$ (*subgroups-of-size* q)
⟨*proof*⟩

... And this unique subgroup is normal.

corollary (**in** *group*) *pq-order-subgrp-normal*:
assumes *finite*: *finite* (*carrier* G)
assumes *orderG*: *order* $G = q * p$
assumes *primep*: *prime* p **and** *primeq*: *prime* q **and** *pq*: $p < q$
shows (*THE* $Q.\ Q \in$ *subgroups-of-size* q) $\lhd G$

⟨*proof*⟩

The trivial subgroup is normal in every group.

lemma (**in** *group*) *trivial-subgroup-is-normal*:
  shows $\{\mathbf{1}\} \lhd G$
⟨*proof*⟩

2.2 Normal Series

We define a normal series as a locale which fixes one group G and a list $\mathfrak{G}$ of subsets of G's carrier. This list must begin with the trivial subgroup, end with the carrier of the group itself and each of the list items must be a normal subgroup of its successor.

locale *normal-series* = *group* +
  fixes $\mathfrak{G}$
  assumes *notempty*: $\mathfrak{G} \neq []$
  assumes *hd*: $hd\ \mathfrak{G} = \{\mathbf{1}\}$
  assumes *last*: $last\ \mathfrak{G} = carrier\ G$
  assumes *normal*: $\bigwedge i.\ i + 1 < length\ \mathfrak{G} \Longrightarrow (\mathfrak{G}\ !\ i) \lhd G(\!|carrier := \mathfrak{G}\ !\ (i + 1)|\!)$

lemma (**in** *normal-series*) *is-normal-series*: *normal-series* $G\ \mathfrak{G}$ ⟨*proof*⟩

For every group there is a "trivial" normal series consisting only of the group itself and its trivial subgroup.

lemma (**in** *group*) *trivial-normal-series*:
  shows *normal-series* G $[\{\mathbf{1}\}, carrier\ G]$
⟨*proof*⟩

We can also show that the normal series presented above is the only such with a length of two:

lemma (**in** *normal-series*) *length-two-unique*:
  assumes $length\ \mathfrak{G} = 2$
  shows $\mathfrak{G} = [\{\mathbf{1}\}, carrier\ G]$
⟨*proof*⟩

We can construct new normal series by expanding existing ones: If we append the carrier of a group G to a normal series for a normal subgroup $H \lhd G$ we receive a normal series for G.

lemma (**in** *group*) *normal-series-extend*:
  assumes *normal*: *normal-series* $(G(\!|carrier := H|\!))\ \mathfrak{H}$
  assumes *HG*: $H \lhd G$
  shows *normal-series* G $(\mathfrak{H} @ [carrier\ G])$
⟨*proof*⟩

All entries of a normal series for G are subgroups of G.

lemma (**in** *normal-series*) *normal-series-subgroups*:

shows $i < \mathit{length}\ \mathfrak{G} \Longrightarrow \mathit{subgroup}\ (\mathfrak{G}\ !\ i)\ G$
⟨*proof*⟩

The second to last entry of a normal series is a normal subgroup of G.

lemma (**in** *normal-series*) *normal-series-snd-to-last*:
shows $\mathfrak{G}\ !\ (\mathit{length}\ \mathfrak{G} - 2) \lhd G$
⟨*proof*⟩

Just like the expansion of normal series, every prefix of a normal series is again a normal series.

lemma (**in** *normal-series*) *normal-series-prefix-closed*:
assumes $i \leq \mathit{length}\ \mathfrak{G}$ **and** $0 < i$
shows $\mathit{normal\text{-}series}\ (G(\!|\mathit{carrier} := \mathfrak{G}\ !\ (i - 1)|\!))\ (\mathit{take}\ i\ \mathfrak{G})$
⟨*proof*⟩

If a group's order is the product of two distinct primes p and q, where $p < q$, we can construct a normal series using the only subgroup of size q.

lemma (**in** *group*) *pq-order-normal-series*:
assumes *finite*: *finite* (*carrier G*)
assumes *orderG*: *order G* = *q* ∗ *p*
assumes *primep*: *prime p* **and** *primeq*: *prime q* **and** *pq*: *p* < *q*
shows *normal-series G* [{**1**}, (*THE H*. *H* ∈ *subgroups-of-size q*), *carrier G*]
⟨*proof*⟩

The following defines the list of all quotient groups of the normal series:

definition (**in** *normal-series*) *quotients*
where *quotients* = *map* (λ*i*. *G*(|*carrier* := 𝔊 ! (*i* + 1)|) *Mod* 𝔊 ! *i*) [0..<((*length* 𝔊) − 1)]

The list of quotient groups has one less entry than the series itself:

lemma (**in** *normal-series*) *quotients-length*:
shows *length quotients* + 1 = *length* 𝔊
⟨*proof*⟩

lemma (**in** *normal-series*) *last-quotient*:
assumes *length* 𝔊 > 1
shows *last quotients* = *G Mod* 𝔊 ! (*length* 𝔊 − 1 − 1)
⟨*proof*⟩

The next lemma transports the constituting properties of a normal series along an isomorphism of groups.

lemma (**in** *normal-series*) *normal-series-iso*:
assumes *H*: *group H*
assumes *iso*: Ψ ∈ *iso G H*
shows *normal-series H* (*map* (*image* Ψ) 𝔊)
⟨*proof*⟩

2.3 Composition Series

A composition series is a normal series where all consecutive factor groups are simple:

locale *composition-series* = *normal-series* +
  assumes *simplefact*: $\bigwedge i.\ i + 1 <$ *length* $\mathfrak{G} \Longrightarrow$ *simple-group* (G(|*carrier* := $\mathfrak{G}$! (i + *1*)|) *Mod* $\mathfrak{G}$! i)

lemma (**in** *composition-series*) *is-composition-series*:
  shows *composition-series* G $\mathfrak{G}$
⟨*proof*⟩

A composition series for a group G has length one if and only if G is the trivial group.

lemma (**in** *composition-series*) *composition-series-length-one*:
  shows (*length* $\mathfrak{G}$ = *1*) = ($\mathfrak{G}$ = [{**1**}])
⟨*proof*⟩

lemma (**in** *composition-series*) *composition-series-triv-group*:
  shows (*carrier* G = {**1**}) = ($\mathfrak{G}$ = [{**1**}])
⟨*proof*⟩

The inner elements of a composition series may not consist of the trivial subgroup or the group itself.

lemma (**in** *composition-series*) *inner-elements-not-triv*:
  assumes $i + 1 <$ *length* $\mathfrak{G}$
  assumes $i > 0$
  shows $\mathfrak{G}$! $i \neq$ {**1**}
⟨*proof*⟩

A composition series of a simple group always is its trivial one.

lemma (**in** *composition-series*) *composition-series-simple-group*:
  shows (*simple-group* G) = ($\mathfrak{G}$ = [{**1**}, *carrier* G])
⟨*proof*⟩

Two consecutive elements in a composition series are distinct.

lemma (**in** *composition-series*) *entries-distinct*:
  assumes *finite*: *finite* (*carrier* G)
  assumes i: $i + 1 <$ *length* $\mathfrak{G}$
  shows $\mathfrak{G}$! $i \neq$ $\mathfrak{G}$! (i + *1*)
⟨*proof*⟩

The normal series for groups of order $p * q$ is even a composition series:

lemma (**in** *group*) *pq-order-composition-series*:
  assumes *finite*: *finite* (*carrier* G)
  assumes *orderG*: *order* $G = q * p$
  assumes *primep*: *prime* p **and** *primeq*: *prime* q **and** *pq*: $p < q$

shows *composition-series G* [{**1**}, (*THE H*. *H* ∈ *subgroups-of-size q*), *carrier G*]
⟨*proof*⟩

Prefixes of composition series are also composition series.

lemma (**in** *composition-series*) *composition-series-prefix-closed*:
assumes *i* ≤ *length* 𝔊 **and** *0* < *i*
shows *composition-series* (*G*(|*carrier* := 𝔊 ! (*i* − *1*)|)) (*take i* 𝔊)
⟨*proof*⟩

The second element in a composition series is simple group.

lemma (**in** *composition-series*) *composition-series-snd-simple*:
assumes *2* ≤ *length* 𝔊
shows *simple-group* (*G*(|*carrier* := 𝔊 ! *1*|))
⟨*proof*⟩

As a stronger way to state the previous lemma: An entry of a composition series is simple if and only if it is the second one.

lemma (**in** *composition-series*) *composition-snd-simple-iff*:
assumes *i* < *length* 𝔊
shows (*simple-group* (*G*(|*carrier* := 𝔊 ! *i*|))) = (*i* = *1*)
⟨*proof*⟩

The second to last entry of a normal series is not only a normal subgroup but actually even a *maximal* normal subgroup.

lemma (**in** *composition-series*) *snd-to-last-max-normal*:
assumes *finite*: *finite* (*carrier G*)
assumes *length*: *length* 𝔊 > *1*
shows *max-normal-subgroup* (𝔊 ! (*length* 𝔊 − *2*)) *G*
⟨*proof*⟩

For the next lemma we need a few facts about removing adjacent duplicates.

lemma *remdups-adj-obtain-adjacency*:
assumes *i* + *1* < *length* (*remdups-adj xs*) *length xs* > *0*
obtains *j* **where** *j* + *1* < *length xs*
(*remdups-adj xs*) ! *i* = *xs* ! *j* (*remdups-adj xs*) ! (*i* + *1*) = *xs* ! (*j* + *1*)
⟨*proof*⟩

lemma *hd-remdups-adj*[*simp*]: *hd* (*remdups-adj xs*) = *hd xs*
⟨*proof*⟩

lemma *remdups-adj-adjacent*:
Suc i < *length* (*remdups-adj xs*) ⟹ *remdups-adj xs* ! *i* ≠ *remdups-adj xs* ! *Suc i*
⟨*proof*⟩

Intersecting each entry of a composition series with a normal subgroup of *G* and removing all adjacent duplicates yields another composition series.

lemma (**in** *composition-series*) *intersect-normal*:

assumes *finite*: *finite* (*carrier G*)
assumes *KG*: $K \lhd G$
shows *composition-series* ($G(\!|carrier := K|\!)$) (*remdups-adj* (*map* ($\lambda H.\ K \cap H$) $\mathfrak{G}$))
⟨*proof*⟩

lemma (**in** *group*) *composition-series-extend*:
assumes *composition-series* ($G(\!|carrier := H|\!)$) $\mathfrak{H}$
assumes *simple-group* (*G Mod H*) $H \lhd G$
shows *composition-series G* ($\mathfrak{H}$ @ [*carrier G*])
⟨*proof*⟩

lemma (**in** *composition-series*) *entries-mono*:
assumes $i \leq j$ $j <$ *length* $\mathfrak{G}$
shows $\mathfrak{G}$! $i \subseteq \mathfrak{G}$! j
⟨*proof*⟩

end

theory *GroupIsoClasses*
imports
HOL−Algebra.Coset
begin

3 Isomorphism Classes of Groups

We construct a quotient type for isomorphism classes of groups.

typedef *'a group* = {*G* :: *'a monoid. group G*}
⟨*proof*⟩

definition *group-iso-rel* :: *'a group* ⇒ *'a group* ⇒ *bool*
where *group-iso-rel G H* = (∃ φ. $\varphi \in$ *iso* (*Rep-group G*) (*Rep-group H*))

quotient-type *'a group-iso-class* = *'a group* / *group-iso-rel*
morphisms *Rep-group-iso Abs-group-iso*
⟨*proof*⟩

This assigns to a given group the group isomorphism class

definition (**in** *group*) *iso-class* :: *'a group-iso-class*
where *iso-class* = *Abs-group-iso* (*Abs-group* (*monoid.truncate G*))

Two isomorphic groups do indeed have the same isomorphism class:

lemma *iso-classes-iff*:
assumes *group G*
assumes *group H*
shows (∃ φ. $\varphi \in$ *iso G H*) = (*group.iso-class G* = *group.iso-class H*)
⟨*proof*⟩

end

theory *JordanHolder*
imports
CompositionSeries
MaximalNormalSubgroups
HOL−Library.Multiset
GroupIsoClasses
begin

4 The Jordan-Hölder Theorem

locale *jordan-hoelder* = *group*
+ *comp*$\mathfrak{H}$*?*: *composition-series* G $\mathfrak{H}$
+ *comp*$\mathfrak{G}$*?*: *composition-series* G $\mathfrak{G}$ **for** $\mathfrak{H}$ **and** $\mathfrak{G}$
+ **assumes** *finite*: *finite* (*carrier* G)

Before we finally start the actual proof of the theorem, one last lemma: Cancelling the last entry of a normal series results in a normal series with quotients being all but the last of the original ones.

lemma (**in** *normal-series*) *quotients-butlast*:
assumes *length* $\mathfrak{G} > 1$
shows *butlast quotients* = *normal-series.quotients* (G(|*carrier* := $\mathfrak{G}$! (*length* $\mathfrak{G}$ − 1 − 1)|)) (*take* (*length* $\mathfrak{G}$ − 1) $\mathfrak{G}$)
⟨*proof*⟩

The main part of the Jordan Hölder theorem is its statement about the uniqueness of a composition series. Here, uniqueness up to reordering and isomorphism is modelled by stating that the multisets of isomorphism classes of all quotients are equal.

theorem *jordan-hoelder-multisets*:
assumes *group* G
assumes *finite* (*carrier* G)
assumes *composition-series* G $\mathfrak{G}$
assumes *composition-series* G $\mathfrak{H}$
shows *mset* (*map group.iso-class* (*normal-series.quotients* G $\mathfrak{G}$))
= *mset* (*map group.iso-class* (*normal-series.quotients* G $\mathfrak{H}$))
⟨*proof*⟩

As a corollary, we see that the composition series of a fixed group all have the same length.

corollary (**in** *jordan-hoelder*) *jordan-hoelder-size*:
shows *length* $\mathfrak{G}$ = *length* $\mathfrak{H}$
⟨*proof*⟩

end

References

[Ran05] Stuart Rankin. The jordan-hölder theorem, 2005.

[vR14] Jakob von Raumer. Secondary sylow theorems. *Archive of Formal Proofs*, January 2014. http://isa-afp.org/entries/Secondary_Sylow.shtml, Formal proof development.