Abstract Algebra – I Groups (群理论)
1.14 Normal series (正规列) and Solvable groups, 1.15 Semidirect products, 1.16 Nilpotent groups

November 27, 2012

Outline

Normal series (正规列) and Jordan–Hölder Theorem (若尔当 – 赫尔德定理)

- Definition & Examples
- Commutator series (换位子序列)
- Solvable groups (可解群)

Exact sequences (正合序列) and group extensions (群扩张)

- Semidirect products (半直积)

Nilpotent groups (幂零群)

Normal series (正规列) and Jordan-Hölder Theorem (若尔当 – 赫尔德定理)

Definition

Given a group G, then a normal series (正规列) *for G is a series $G_0 = \{\mathrm{id}\} \triangleleft G_1 \triangleleft \ldots G_n = G$, i.e. every group $G_k \triangleleft G_{k+1}$, not necessarily in G.*

A composition series (合成列) *is a normal series where all factors are simple.*

Example

1. Consider the group $G = S_4$ with the normal series $\{\mathrm{id}\} \triangleleft \langle (12)(34) \rangle \triangleleft V_4 \triangleleft A_4 \triangleleft S_4$. This is a normal series of length 4. Note that the factors are all cyclic of prime order, thus it is a composition series.

Normal series (正规列) and Jordan-Hölder Theorem (若尔当 – 赫尔德定理) II

2. Consider on the other hand the normal series $\{\mathrm{id}\} \triangleleft A_5 \triangleleft S_5$. It is rather short and A_5 is not abelian. Nevertheless it is simple and the series thus a composition series.
3. Consider $\mathbb{Z}/(6)$. It has two composition series, namely $0 \triangleleft \mathbb{Z}/(2) \triangleleft \mathbb{Z}/(6)$ and $0 \triangleleft \mathbb{Z}/(3) \triangleleft \mathbb{Z}/(6)$. But the factors G_k/G_{k-1} are $(\mathbb{Z}/(2), \mathbb{Z}/(3))$ and $(\mathbb{Z}/(3), \mathbb{Z}/(2))$, respectively, thus isomorphic up to order. This happens for all composition series of a fixed group.

Theorem (Schreier)

Given any group and two finite normal series $1 = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_m = G$ *and* $1 = H_0 \triangleleft H_1 \triangleleft \ldots \triangleleft H_m = G$*, then there is a common refinement* $1 = K_0 \triangleleft K_1 \triangleleft \ldots \triangleleft K_N = G$*, i.e. there are monotone subsequences* $i_\bullet : \{0, \ldots, m\} \to \{0, \ldots, N\}$ *and* $j_\bullet : \{0, \ldots, n\} \to \{0, \ldots, N\}$ *such that* $G_l = K_{i_l}$ *and* $H_l = K_{j_l}$.

Idea of proof.

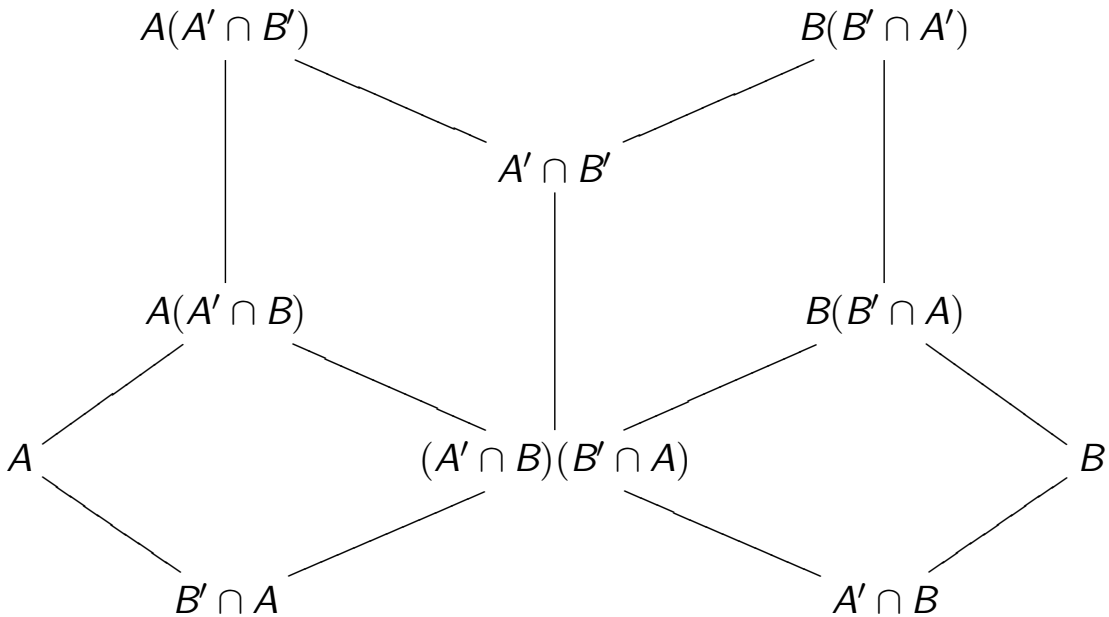
The basic idea is to define $K_{i+mj} := G_i \cap H_j$ and see if they still form a normal series. In order to prove that, you need something like the following:

Lemma (butterfly $\sim$, Zassenhaus, 蝴蝶引理)

If $A \triangleleft A' \subset G$ and $B \triangleleft B' \subset G$, then $A(A' \cap B)$, $A(A' \cap B')$, $B(B' \cap A)$ and $B(B' \cap A')$ are subgroups of G, $A(A' \cap B) \triangleleft A(A' \cap B')$ and $B(B' \cap A) \triangleleft B(B' \cap A')$, and

$$A(A' \cap B')/A(A' \cap B) \cong B(B' \cap A')/B(B' \cap A).$$

The subgroup inclusion pattern is



Normal series (正规列) and Jordan-Hölder Theorem (若尔当 – 赫尔德定理) IV

Given a group of *finite length* (i.e. every non-repeating series of (normal) subgroups is finite, e.g. when G is finite itself), we can construct a composition series just by starting from any normal series and trying to refine it whereever one of its factors is not yet simple.

Given any composition series $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$, we call $F_k := G_{k+1}/G_k$ the factors of G (w.r.t. this composition series).

As the Example 1.1.2-3 shows, these composition series are not unique. However Schreier's theorem states that they are contained in a joint refinement. The conclusion is the Jordan–Hölder Theorem that claims that the factors are unique (depending only on G):

Normal series (正规列) and Jordan-Hölder Theorem (若尔当 – 赫尔德定理) V

Corollary (Jordan–Hölder)

Given two composition series $\{\mathrm{id}\} \triangleleft G_1 \triangleleft \ldots \triangleleft G_m = G$ *and* $\{\mathrm{id}\} \triangleleft H_1 \triangleleft \ldots \triangleleft H_n = G$ *of the same group* G*, then there is a bijection between the factors such that corresponding factors are isomorphic. (In particular* $m = n$*.)*

Idea of proof.

Schreier's theorem states, that there is a joint refinement. On the other hand each series is already maximally refined. Therefore we will just insert a couple of trivial factors $F_i = 1$ and the non-trivial factors are the same in each composition series (i.e. there is a bijection between them).

□

Normal series (正规列) and Jordan-Hölder Theorem (若尔当 – 赫尔德定理) VI

We therefore see that finite groups are built of simple groups. A first step in a classification/ complete understanding of all finite groups is thus to understand the simple groups. This has indeed be achieved[1] and leads to 18 infinite series of simple groups together with 26 exceptions of simple groups. Some of the infinite series are:

- C_p for $p \in \mathbb{P}$ a prime (the only abelian ones),
- A_n for $n \geq 5$ (alternating groups),
- $\mathrm{PSL}_n(F)$ for $n \geq 3$ and F a finite field,
- ....

[1] Gorenstein et al, **1994**, ~ 2100 pages

Commutator series (换位子序列)

An effective means to compute a composition series is the commutator series (换位子序列):

Definition

Given a group G, then the commutator (整流子) *of two elements $a, b \in G$ is $[a, b] := aba^{-1}b^{-1}$. The* commutator subgroup (换位子群) *of G is $G' := [G, G] := \langle [a, b] : a, b \in G \rangle$.*
The commutator series (换位子序列) *or* derived series (导出列) *$D^\bullet G$ of a group G is the series $\mathrm{D}^0 G := G$, $\mathrm{D}^{n+1} G := [\mathrm{D}^n G, \mathrm{D}^n G]$*

Proposition

Given a group G, then G' is a normal subgroup. Every group homomorphism $\phi\colon G \to A$ into an abelian group factors (uniquely) through $\pi\colon G \to G/G'$.

Commutator series (换位子序列) II

Proof.

G' is a subgroup, because we permit finite products of commutators and $[a,b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b,a]$ for all $a, b \in G$. Moreover G' is invariant under conjugation, because

$$x[a,b]x^{-1} = xaba^{-1}b^{-1}x^{-1} = (xax^{-1})(xbx^{-1})(xax^{-1})^{-1}(xbx^{-1})^{-1}$$

for all $x \in G$. Therefore $G' \triangleleft G$. Let now $\phi\colon G \to A$ be any homomorphism into any abelian group A. Then obviously $0 = \phi(aba^{-1}b^{-1})$ and thus $aba^{-1}b^{-1} \in \ker\phi$. Therefore $G' \subset \ker\phi$ and thus ϕ factors (uniquely) through $\pi\colon G \to G/G'$. □

If some derivation $\mathrm{D}^n G = 1$ is trivial, then this is indeed a normal series. We have just shown that the factors D^{n-1}/D^n are all abelian.

Examples

1. Starting with the group S_4 we observe $D^0 = S_4$, $D^1 = A_4$?, $D^2 = V_4$?, and $D^3 = 1$, i.e. S_4 is solvable.
2. For S_5 on the other hand, we find $D^0 = S_5$, $D^1 = A_5$, $D^2 = A_5 = D^3 = \ldots$, thus the commutator series stops here (and never reaches 1, this is called non-solvable).

Exercise

a. Show that D_4 has a normal series where one of the components is not a normal subgroup of D_4.

b. Given normal series for $N \triangleleft G$ and G/N. Show that these can be pieced together to give a normal series of the group G.

c. Let $\{\mathrm{id}\} \triangleleft G_1 \triangleleft G_2 \triangleleft \ldots \triangleleft G_n = G$ be a normal series. Explain how normal series of each factor G_k/G_{k-1} give a refinement of this normal series. What is needed to obtain a composition series?

d. Given composition series of $N \triangleleft G$ and G/N. How can you obtain a composition series for the group G?

Exercise

If G has a composition series, then every normal subgroup $N \triangleleft G$ and every quotient G/N (by a normal subgroup) has a composition series.

Hint: Show how N appears in a composition series.

Exercise

Find all composition series of

a. A_4,

b. D_4,

c. D_5.

Exercise

Show that all abelian groups of order n have the same simple factors.

Exercise

Show that the simple factors of D_n are all abelian. (This means that D_n is solvable.)

Exercise

Let G be a group of order n and m the length of each of its composition series.

a. Show that a group of order $n = p^m$ where $p \in \mathbb{P}$ is a prime and $m \in \mathbb{N}_+$ a positive integer has a composition series of length m.

b. Show that $m \leq \log_2 n$.

c. Show that equality $m = \log_2 n$ is possible for arbitrary high values of n.

Exercise

What can you say if $DG = G$ for a group G?

Hint: Consider $D(A_5 \times A_5)$ and note that this direct product is not simple.

Solvable groups (可解群)

We call a group G solvable (可解群) if the derived series terminates in 1. Given finite abelian factors, we can refine them to be cyclic of prime order. Conversely, if G is not solvable, then it has some non-abelian factor in every normal series, including every truncation of the derived series (filled with 1 on the left end). Therefore the full derived series cannot end in 1.

Proposition

The derived series of a group ends in 1 *iff every composition series has only abelian factors.* □

Solvable groups (可解群) II

Proposition

The class of solvable groups is closed under the following operations:

1. *Subgroup, i.e. if G is solvable, then so is every subgroup $H \subset G$.*
2. *Quotient, i.e. if G is solvable and $N \triangleleft G$ a normal subgroup, then also G/N is solvable.*
3. *Composition, i.e. if $N \triangleleft G$ is solvable and G/N is solvable, then so is G.*

Examples

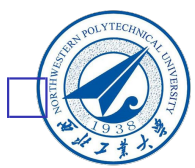
Remember that a p-group is a group G where every element $g \in G$ has order some integer power of the given $p \in \mathbb{P}$. In particular every finite p-group has order a power of p.

Proposition

Every finite p-group is solvable.

Proof.

Let G denote the group in question and $|G| = p^n$ for some $n \in \mathbb{N}$. If $n \leq 1$ then G is cyclic and thus solvable. For $n \geq 2$ we note that there is a subgroup $N \subset G$ of order p^{n-1} which is normal in G (because it is either unique or G is a direct product of several p groups each of which is normal in G). But then an induction shows that N as well as $G/N \cong \mathbb{Z}/(p)$ are both solvable and by the last proposition so is G.



Examples II

Further examples of (finite) solvable groups arise from the following property:

Proposition

Given a group G of order $p^m q$ where $p, q \in \mathbb{P}$ are primes and $m \in \mathbb{N}$ is an integer, then G is solvable.

Examples III

Proof.

We may assume that $p \neq q$. Let S be a p-Sylow subgroup of G. If $S \lhd G$, then we are done, because the last proposition shows that S is solvable and the last factor G/S is cyclic.

Let thus S not be normal in G. This means in particular that $S \subset N_G(S) \subsetneq G$, i.e. the normalizer of S (in G) is strictly smaller than G. Since $(G : S) = q$ a prime, this implies $N_G(S) = S$ and the number of p-Sylow subgroups in G is $n_p = (G : N_G(S)) = q$. Since the p-Sylow subgroups intersect trivially, i.e. $S \cap T = \{\mathrm{id}\}$ for any two of them, there are at least $q(p^m - 1)$ elements of order some positive power of p. That leaves only q elements in G of order some power of q and therefore there is only one q-Sylow subgroup $Q \subset G$ which must therefore be normal. But then $Q \cong \mathbb{Z}/(q)$ as well as G/Q of order p^m are solvable and thus G is solvable. □

Examples IV

Remark

An even stronger result is is Burnside's $p^m q^n$-Theorem which states that every group of order $p^m q^n$ where $p, q \in \mathbb{P}$ and $m, n \in \mathbb{N}$ integers is solvable. To prove that you need, e.g. some strong ring theory which will however be beyond the reach of this course.

Theorem (Feit–Thompson[2])

Given a finite group of odd order, then it is solvable.

[2] a longer part of the 2100 page book collection

Group extensions (群扩张)

The harder question is how to reconstruct an arbitrary group from its composition factors. The elementary step is the second part of the following definition.

Definition

A sequence of group homomorphisms $\cdots \to G_{n-1} \xrightarrow{\phi_{n-1}} G_n \xrightarrow{\phi_n} G_{n+1} \to \ldots$ *is called* exact (正合序列) *if at every group* $\ker \phi_n = \operatorname{im} \phi_{n-1}$.
An exact sequence $1 \to N \to G \to Q \to 1$ *is called* short exact sequence (短正合序列) *or* extension (群扩张) *of the group* Q *by* N.

Example

0a The beginning $1 \to S \to G$ means that S is embedded into G, i.e. a subgroup (up to isomorphism),
0b The ending $G \to H \to 1$ means that G maps surjectively onto H.

Examples

1. Both together $1 \to G \to H \to 1$ mean that $G \cong H$, i.e. the two groups are isomorphic.
2. Consider the sequence $1 \to C_2 \to G \to C_2 \to 1$ and let us ask how many inequivalent groups G exist here. Since $N = C_2 = Q$ are of order 2 each, $|G| = 4$ and thus G is abelian. But for abelian groups the classification is easy. The candidates are C_4 and $C_2 \times C_2$ and by inspection both are possible group extensions.

Semidirect products (半直积)

Definition

Given a short exact sequence of groups $1 \to N \hookrightarrow G \twoheadrightarrow Q \to 1$ *where in addition we have an (injective) group homomorphism* $s\colon Q \to G$ *that is a right-inverse of the projection* $\pi\colon G \twoheadrightarrow Q$ *(*$\pi \circ s = \mathrm{Id}_Q$*). This is called a* semidirect product*.*

Proposition

The above situation is called a right-splitting (右分裂) *of the short exact sequence. This is equivalent to the following so called* left-splitting (左分裂)*: There is a surjective map* $p\colon G \to N$ *that is a left-inverse of the embedding* $N \to G$ *(*$p \circ e = \mathrm{Id}_N$ *where* $e\colon N \hookrightarrow G$*).*

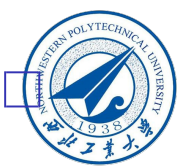
Semidirect products (半直积) II

Note that p may in general fail to be a group homomorphism, namely p is a group homomorphism iff $Q \triangleleft G$, i.e. $G = N \times Q$ a direct product.

Proof.

Let $e\colon N \hookrightarrow G$ and $\pi\colon G \twoheadrightarrow Q$ denote the maps in the short exact sequence. Given a right-splitting $s\colon Q \to G$, then for every $g \in G$, we can construct the element $\hat{g} := g \cdot s(\pi(g))^{-1}$. Since s and π are group homomorphisms, we observe $\pi(\hat{g}) = \pi(g) \cdot \pi(g)^{-1} = \mathrm{id} \in Q$ and thus there is an element $n \in N$ such that $e(n) = \hat{g}$. Again π and s group homomorphisms implies that $\ker \pi = \{\hat{g} : g \in G\} \triangleleft G$ is a subgroup which is isomorphic to N via e and maps $n \mapsto \hat{g}$. Therefore $p = e^{-1} \circ m(\mathrm{id}, s \circ \pi)\colon G \twoheadrightarrow N : g \mapsto n$ is a fiberwise surjective map.

Conversely, given $p\colon G \twoheadrightarrow N$ fiberwise surjective and a left-inverse of e, then we can for every $h \in Q$ choose the unique $g \in G$ with $\pi(g) = h$ and $p(g) = \mathrm{id} \in N$. For fixed π and h the coset class $ge(N)$ is unique and $e \circ p = \mathrm{Id}_N$. **MG: ...** Therefore $s\colon Q \to G : h \mapsto g$ is a group homomorphism. This completes the proof.



Semidirect products (半直积) III

Example

Consider the group $\mathrm{GL}_n(F)$ together with the fundamental representation on the vector space F^n. Considering the latter as abelian group, we want to find a group $G \approx \mathrm{GL}_n(F) \times F^n$ fitting into $\{0\} \to F^n \to G \to \mathrm{GL}_n(F) \to \{\mathbb{1}\}$. We choose the group law $(A, v)(B, w) := (AB, v + Aw)$. One can see easily that this is associative, has the neutral element $(\mathbb{1}, 0)$ and the inverse elements $(A, v)^{-1} = (A^{-1}, -A^{-1}v)$. Moreover F^n is invariant under the action of $Q = \mathrm{GL}_n(F)$ on G. Therefore $F^n \triangleleft G$ as well as $G/F^n \cong \mathrm{GL}_n(F)$.

Semidirect products (半直积) IV

Remark (Warning)

Remember the short exact sequence $0 \to C_2 \to C_4 \to C_2 \to 0$. Even though $C_4 \twoheadrightarrow C_2$, there is no group homomorphism inverting this projection, because C_4 is not the direct product $C_2 \times C_2$.

Q: What is the general structure of semi-direct products?

Semidirect products (半直积) IV

Remark (Warning)

Remember the short exact sequence $0 \to C_2 \to C_4 \to C_2 \to 0$. Even though $C_4 \twoheadrightarrow C_2$, there is no group homomorphism inverting this projection, because C_4 is not the direct product $C_2 \times C_2$.

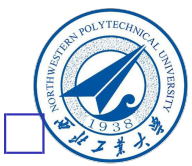
Q: What is the general structure of semi-direct products?

Corollary

A group G is a semi-direct product of the subgroups N and Q iff $N \triangleleft G$ is a normal subgroup and $NQ = G$. In particular this implies that there is a unique action $\rho\colon Q \to \mathrm{Aut}(N), \rho(q)n = qnq^{-1}$ for all $q \in Q$ and $n \in N$.

Proof.

This follows immediately from the short exact sequence ($N \triangleleft G$) and the right-splitting ($Q \subset G$ and $NQ = G$).



Exercise

Find all group extensions in the following cases

a. of $Q = C_2$ by $N = C_3$,

b. of $Q = C_3$ by $N = C_2$.

c. Which of the extensions $1 \to C_3 \to G \to C_2 \to 1$ are semi-direct products?

Exercise

Show that the D_n are semi-direct products. What is the group action?

Nilpotent groups (幂零群)

Definition

A group is nilpotent *iff its* lower central series (降/下中心列) *ends in* $\{\mathrm{id}\}$. *The lower central series is defined as*

$$G_0 := G, \quad G_{n+1} := [G, G_n]$$

where $[a, b] := aba^{-1}b^{-1}$ *for* $a, b \in G$ *is the commutator of two group elements.*

Example

Consider the Borel group $B \subset \mathrm{GL}_n(F)$ of upper triangular matrices. It is nilpotent since G_0 has the diagonal with 1s, G_1 has the first subdiagonal all 0, G_2 has the first two subdiagonals all 0, ..., the last group $G_{n-1} = \{\mathbb{1}\}$.

Proposition

A group G is nilpotent iff its upper central series (升/上中心序列) *ends in G. The upper central series is defined as*

$$Z_0 := \{\mathrm{id}\}, \quad Z_{n+1} := \{z \in G : \forall g \in G : [g, z] \in Z_n\}.$$

In particular $Z_1 = \operatorname{cent} G$

Exercise

Prove the last proposition.

Hint: Suppose G is nilpotent of length n (i.e. $G_n = 1$), show that $Z_k \supset G_{n-k}$ and thus $Z_n = G_0 = G$. In the other direction show that $Z_n = G$ implies $G_k \subset Z_{n-k}$.

Next week we will start with a new chapter: Rings and Algebras (环理论)