CHARACTERISTIC SUBGROUPS

ALEX NELSON

Abstract. We formalize in Mizar [BBG+15, BBG+18] the notion of characteristic subgroups using the definition found in Dummit and Foote [DF04], as subgroups invariant under automorphisms from its parent group. Along the way, we formalize notions of Automorphism and results concerning centralizers. Much of what we formalize may be found sprinkled throughout the literature, in particular Gorenstein [Gor80] and Isaacs [Isa08]. We show all our favorite subgroups turn out to be characteristic: the center, the derived subgroup, the commutator subgroup generated by characteristic subgroups, and the intersection of all subgroups satisfying a generic group property.

Contents

Introduction

We will begin with formalizing results concerning characteristic subgroups. In section 1 we will briefly discuss the environment part of a Mizar article. In section 2 we will formalize preliminary material, including trivial subgroups and proper subgroups. In section 6, we formalize automorphisms, then in section 7 inner automorphisms. In section 8, we formalize the notion of a characteristic subgroup, prove the center subgroup is characteristic, among other results. We conclude, in

Date: December 23, 2022.
2020 *Mathematics Subject Classification.* 20-04, 20E99.
Compiled: 2023-01-26 08:48:55-08:00.

section 10, with introducing the centralizer of a subgroup and Theorem 1.62 proves the centralizer of a characteristic subgroup is characteristic.

Mizar Article. We call a Mizar file/script an "article". While developing a Mizar article, the main body is stored in a `TEXT/` subdirectory. As I understand it, the casing of the directory matters (because there are DOS computers which have case-sensitive file systems... or something). Every Mizar article looks like:

2a ⟨*TEXT/group-22.miz* 2a⟩≡
```
⟨License for group_22.miz 2c⟩

⟨Environment for group_22.miz 3a⟩

⟨group_22.miz article body 8b⟩
```
Root chunk (not used in this document).

Vocabulary File. Each Mizar article has an associated "vocabulary file" which lists the *new* terms introduced. It's stored in a `DICT/` subdirectory. Terms are prefixed with the following:

- `R` for predicate (like `Rare_isomorphic` for a new predicate `are_isomorphic`)
- `O` for functor (e.g., `Oid` for `id`)
- `M` for mode (e.g., `MSubgroup` for `Subgroup`)
- `G` for structure (e.g., `GmultLoopStr_0` for `multLoopStr_0`)
- `U` for selectors (e.g., `Ucarrier` in `STRUCT_0` gives us a way to write `the carrier of X`)
- `V` for attributes (so `Vcharacteristic` is a new attribute "characteristic")
- `K` for left functor brackets (like `[:` in `ZFMISC_1`)
- `L` for right functor brackets (like the corresponding `:]` in `ZFMISC_1`)

Right now, we have just started, so we need an empty vocabulary file:

2b ⟨*DICT/GROUP-22.VOC* 2b⟩≡

This definition is continued in chunks 37c and 49b.
Root chunk (not used in this document).

License. The license for the MML seems to be the same for each article, I will just copy it over.

2c ⟨*License for* `group_22.miz` 2c⟩≡
```
:: Characteristic Subgroups
::  by Alex Nelson
::
:: This code can be distributed under the GNU General Public Licence
:: version 3.0 or later, or the Creative Commons Attribution-ShareAlike
:: License version 3.0 or later, subject to the binding interpretation
:: detailed in file COPYING.interpretation.
:: See COPYING.GPL and COPYING.CC-BY-SA for the full text of these
:: licenses, or see http://www.gnu.org/licenses/gpl.html and
:: http://creativecommons.org/licenses/by-sa/3.0/.
```
This code is used in chunk 2a.

1. Environment

The header, or "environment part", tells Mizar what mathematics needs to be imported from existing Mizar articles found in the MML. The idea is we can define new terms ["functors"], new predicates, or new types ["modes"], but we have to specify which articles we want to use for their definitions, results, and notations.

This is complicated and kind of a distraction. The reader can skip ahead to where we start proving theorems and defining concepts in §2.

3a ⟨*Environment for* `group_22.miz` 3a⟩≡

```
environ

 ⟨group_22.miz vocabularies 3b⟩;
 ⟨group_22.miz constructors 4d⟩;
 ⟨group_22.miz notations 5d⟩;
 ⟨group_22.miz registrations 6a⟩;
 ⟨group_22.miz requirements 8a⟩;
 ⟨group_22.miz definitions 6e⟩;
 ⟨group_22.miz equalities 7e⟩;
 ⟨group_22.miz expansions 7f⟩;
 ⟨group_22.miz theorems 7a⟩;
 ⟨group_22.miz schemes 7d⟩;
```

This code is used in chunk 2a.

Remark 1.0.1. In practice, we often just copy/paste the `environ` of an article proving results about similar topics. This is probably the easiest way to get started, but it leaves one wondering what exactly this elaborate section *does* in Mizar.

1.1. Vocabularies, Notations, Constructors.

1.1.1. *Vocabularies.* The `vocabularies` refers to the identifiers defined. As I understand it, Mizar is actually using the `vocabularies` for the user to add new tokens to the language. Then Mizar will parse the file and treat user-defined terms *as* terms. The meaning associated to them will be spelled out in the other parts of the `environ`.

For example, `Isomorphism` may be found in `RING_3`. If I wanted to define an `Isomorphism` of groups, then I must use `Isomorphism` as a token. Thus I would need to add `RING_3` to the vocabularies list. (Earlier versions of this text made me think this was a good idea, but it turned out to be a huge distraction.)

Similarly, `MOD_4` introduces the tokens `Endomorphism` and `Automorphism`, which I want to use, so I add them, too.

3b ⟨`group_22.miz` *vocabularies* 3b⟩≡

```
vocabularies MOD_4, GROUP_22, CARD_3, QC_LANG1, RLSUB_1,
  ⟨Functions and subset tokens 4a⟩,
  ⟨Group and subgroups tokens 4b⟩,
  ⟨Group conjugation and normal subgroups tokens 4c⟩
```

This code is used in chunk 3a.

Remark 1.0.2 (VOC file). For our article, we will need to define new tokens. They are placed in `./DICT/GROUP_22.VOC` (relative to whatever directory we have made our Mizar workstation). As we introduce new terms, we will check if it exists already in Mizar by running "`findvoc -w "term"`". If Mizar is unfamiliar with the

term, then nothing will be reported, and we will have to add it to our `VOC` file. Otherwise, if `term` is introduced in another article, we add it to our `vocabularies` environ directive.

We need to recognize the tokens found in rudimentary set theory, so we begin with importing the usual suspects. For `bijective` and `onto`, we need `FUNCT_2`. We will also be proving properties concerning the cardinality of subgroups, so we load `CARD_1`.

We'll also make use of the fact that the real numbers form a group, and some basics of arithmetic (the `ARYTM_` supply us with what we need).

For proving the Frattini subgroup is characteristic, we need to use `meet` from `SETFAM_1`.

For finite cyclic groups, we need `ORDINAL1` since the underlying set of $\mathbb{Z}_n$ is the ordinal n.

4a ⟨*Functions and subset tokens* 4a⟩≡
```
RELAT_1, TARSKI, FUNCT_1, ZFMISC_1, XXREAL_1, FINSEQ_1,
FINSET_1, NUMBERS, WELLORD1, SUBSET_1, XBOOLE_0, PARTFUN1,
FUNCT_2, CARD_1, ARYTM_3, CQC_SIM1, ORDINAL1, EQREL_1
```
This code is used in chunk 3b.

Characteristic subgroups requires recognizing tokens about... groups, and subgroups.

4b ⟨*Group and subgroups tokens* 4b⟩≡
```
STRUCT_0, GROUP_1, GROUP_2, GROUP_3, GROUP_4, GROUP_5,
GROUP_6, BINOP_1, BINOP_2, ALGSTR_0, REALSET1, AUTGROUP,
GR_CY_1, NATTRA_1, INT_1
```
This code is used in chunk 3b.

`NEWTON` defines the token `|^`, used as infix operator `a |^ b` which is Mizar notation for a^b. Mizar follows group theorist notation of writing $g^h = h^{-1}gh$ for conjugation. Also observe that `normal` is introduced in `PRE_TOPC`, so we need to include that, as well.

We use `WEDDWITT` since it defines the notion of a centralizer.

4c ⟨*Group conjugation and normal subgroups tokens* 4c⟩≡
```
NAT_1, INT_2, SETFAM_1, NEWTON, PRE_TOPC, GROUP_10, WEDDWITT
```
This code is used in chunk 3b.

1.1.2. *Constructors.* But the vocabularies just permits Mizar's parser to *recognize* terms. For the *meaning* of these terms, we need to import the *constructors*. But if a constructor uses *another article*'s constructors, we need to also import that other article as well.

Often we just copy the articles imported for the notations section, but in my experience it's often a strict subset of the notations. I'm lazy, so I'll just copy the constructor imports:

4d ⟨`group_22.miz` *constructors* 4d⟩≡
```
constructors ⟨Set theoretic constructors for group_22.miz 5a⟩
  ⟨Number constructors for group_22.miz 5b⟩
  ⟨Group theory constructors for group_22.miz 5c⟩
```
This code is used in chunk 3a.

5a ⟨*Set theoretic constructors for* `group_22.miz` 5a⟩≡
```
TARSKI, XBOOLE_0, ZFMISC_1, SUBSET_1, RELAT_1, FUNCT_1,
RELSET_1, PARTFUN1, FUNCT_2, FUNCOP_1, FINSEQ_1, FINSEQ_2, FINSOP_1,
```
This code is used in chunk 4d.

5b ⟨*Number constructors for* `group_22.miz` 5b⟩≡
```
CARD_1, CARD_3, NUMBERS, REAL_1, SETWISEO,
ARYTM_2, ARYTM_3, ORDINAL2, SQUARE_1,
SETFAM_1, ORDINAL1,INT_1, INT_2, PBOOLE,
XXREAL_2, XCMPLX_0, XXREAL_0, XREAL_0,  NAT_1, NAT_D,
```
This code is used in chunk 4d.

5c ⟨*Group theory constructors for* `group_22.miz` 5c⟩≡
```
BINOP_1, BINOP_2, FINSET_1, STRUCT_0, ALGSTR_0, REALSET1, MONOID_0,
GROUP_1, GROUP_2, GROUP_3, GROUP_4, GROUP_5, PRALG_1, GROUP_7, GRSOLV_1,
AUTGROUP, GROUP_9, GROUP_10, GR_CY_1, NEWTON, GROUP_6
```
This code is used in chunk 4d.

1.1.3. *Notations.* Now we need to import the functor patterns to "couple" the definitions and notations. Usually this is just the constructor list.

The basics of Tarski–Grothendieck set theory may be found in `TARSKI`. Partial functions are introduced in `PARTFUN1`. Binary operations applied to functions `FUNCOP_1` will be necessary later on. And fancy functions from sets to sets, like `Permutation`, is defined in `FUNCT_2`. There are few random odds and ends, like `NUMBERS` for subsets of complex numbers and `XXREAL_0` for the real numbers.

We also use `SETFAM_1` for `meet`, necessary when proving the Frattini subgroup is characteristic.

For the numbers notations, it's... difficult to disentangle.

The group theoretic notions are a grab bag of binary operators (`BINOP_1` and `BINOP_2`), prerequisites for algebraic structures (`STRUCT_0` and `ALGSTR_0`), primordial group theoretic articles (`REALSET1`), and the relevant group theory articles.

I'll also be using products of groups (established in `GROUP_7`) and need some helper results (`PRALG_1`).

5d ⟨`group_22.miz` *notations* 5d⟩≡
```
notations TARSKI, XBOOLE_0, SUBSET_1, XCMPLX_0, ORDINAL1, RELAT_1,
  FUNCT_1, RELSET_1, FUNCT_2, FUNCOP_1, SETWISEO, PARTFUN1,
  ZFMISC_1, CARD_1, CARD_3, INT_1, NAT_1, ARYTM_2, ARYTM_3, INT_2,
  FINSEQ_2, REAL_1, SETFAM_1, NUMBERS, MEMBERED, PBOOLE, BINOP_1,
  BINOP_2, FINSET_1, STRUCT_0, ALGSTR_0, XXREAL_0, FINSEQ_1, GROUP_1, GROUP_2,
  GROUP_3, GROUP_4, GROUP_5, REALSET1, NAT_D, GRSOLV_1,
  AUTGROUP, GROUP_9, GROUP_10, GR_CY_1, NEWTON, PRALG_1, GROUP_7, GROUP_6
```
This code is used in chunk 3a.

1.2. **Registrations, Definitions, Theorems, Schemes.**

1.2.1. *Registrations.* We often cluster adjectives together with registrations, or have one adjective imply another automatically (like how a characteristic Subgroup is

always normal). We import these using the registrations portion of the environment. For our purposes, we may need basic facts about relations (`RELAT_1`), functions and partial functions (`FUNCT_1`, `PARTFUN1`, `FUNCT_2`), relations between sets (`RELSET_1`).

6a ⟨`group_22.miz` *registrations* 6a⟩≡
```
registrations ⟨Register set theoretic clusters for group_22.miz 6b⟩,
  ⟨Register number clusters for group_22.miz 6c⟩,
  ⟨Register group theoretic clusters for group_22.miz 6d⟩
```
This code is used in chunk 3a.

The clusters we want to use from set theory are defined in the "same" scattering of places.

6b ⟨*Register set theoretic clusters for* `group_22.miz` 6b⟩≡
```
XBOOLE_0, RELAT_1, FUNCT_1, PARTFUN1, RELSET_1, FUNCT_2
```
This code is used in chunk 6a.

6c ⟨*Register number clusters for* `group_22.miz` 6c⟩≡
```
ORDINAL1, FINSET_1, FINSEQ_1, NUMBERS, NAT_1, INT_1, INT_2, XCMPLX_0,
ARYTM_3, XREAL_0, ARYTM_2, SETWISEO, CARD_1, NEWTON, FINSEQ_2
```
This code is used in chunk 6a.

We also need to register adjectives germane to group theory.

6d ⟨*Register group theoretic clusters for* `group_22.miz` 6d⟩≡
```
STRUCT_0, BINOP_1, GROUP_1, GROUP_2, GROUP_3, GROUP_6, GR_CY_1, GROUP_7
```
This code is used in chunk 6a.

1.2.2. *Definitions.* When using a definition $f := M$, we need to cite it in a proof. Specifically, automatically unfolding predicates from specific articles. If we want this to be automated, we can cite the article in the `definitions` portion of the `environ`.

6e ⟨`group_22.miz` *definitions* 6e⟩≡
```
definitions ⟨Include set theoretic definitions for group_22.miz 6f⟩,
  ⟨Group theoretic definitions for group_22.miz 6g⟩
```
This code is used in chunk 3a.

Remark 1.0.3. Kornilowicz [Kor15, see §5.1] that: "Environment directive `definitions` is used for importing two different kinds of information from the database: definitional expansions used by REASONER and expansions of terms defined by equals used by EQUALIZER."

Arguably, we want to be using basic predicates concerning subsets (`SUBSET_1`), functions (`FUNCT_1` and `FUNCT_2`), and set theory (`TARSKI`), so let's just add them.

6f ⟨*Include set theoretic definitions for* `group_22.miz` 6f⟩≡
```
TARSKI, SUBSET_1, FUNCT_1, FUNCT_2, ARYTM_2, FINSEQ_1, INT_1
```
This code is used in chunk 6e.

But we also want to use facts concerning normal subgroups (`GROUP_3`) and the automorphism group $\mathrm{Aut}(G)$ (`AUTGROUP`).

6g ⟨*Group theoretic definitions for* `group_22.miz` 6g⟩≡
```
PRALG_1, GROUP_1, GROUP_3, GROUP_4, GROUP_5, GROUP_6, AUTGROUP, NEWTON,
XXREAL_0, GROUP_7
```
This code is used in chunk 6e.

1.2.3. *Theorems.* The `vocabularies` allows Mizar's scanner and parser to *recognize* terms. The `constructors` and `notations` allows us to use the patterns and constructors for terms. But if we want to cite theorems and definitions in proofs (i.e., if we want to use the *results* of previous articles), then we need to add those cited articles to the `theorems` environment.

7a ⟨`group_22.miz` *theorems* 7a⟩≡
```
theorems
  ⟨Import set-theoretic theorems for group_22.miz 7b⟩,
  ⟨Import group-theoretic theorems for group_22.miz 7c⟩
```
This code is used in chunk 3a.

We have the usual cast of set theoretic characters. There are a large number of articles we refer to for using the real numbers.

7b ⟨*Import set-theoretic theorems for* `group_22.miz` 7b⟩≡
```
TARSKI, RELSET_1, FUNCT_1, FUNCT_2, XBOOLE_0, INT_2, SETFAM_1, FINSEQ_3,
PARTFUN1, ORDINAL1, ZFMISC_1, NAT_D, INT_1
```
This code is used in chunk 7a.

Again, we import the usual group theoretic theorems.

7c ⟨*Import group-theoretic theorems for* `group_22.miz` 7c⟩≡
```
GROUP_1, GROUP_2, GROUP_3, GROUP_4, GROUP_5, GROUP_6, STRUCT_0, GRSOLV_1,
AUTGROUP, GROUP_9, GROUP_10, GR_CY_1, XCMPLX_1
```
This code is used in chunk 7a.

1.2.4. *Schemes.* If we want to cite and use a scheme defined elsewhere, then we need the article's name cited in the `schemes` portion of the environment.

7d ⟨`group_22.miz` *schemes* 7d⟩≡
```
schemes FUNCT_2, GROUP_4, FINSEQ_1
```
This code is used in chunk 3a.

1.3. . . . and the rest.

1.3.1. *Equalities.* This seems to be introduced around 2015, the only documentation I could find was in Kornilowics [Kor15]. Expansions of terms defined by `equals` are imported by a new `environ` directive `equalities`.

7e ⟨`group_22.miz` *equalities* 7e⟩≡
```
equalities PARTFUN1, FINSET_1, BINOP_1, REALSET1, STRUCT_0, GROUP_2,
  GROUP_3, GROUP_4, GROUP_5, GROUP_6, GR_CY_1,
  ALGSTR_0, NEWTON, PRALG_1, GROUP_7
```
This code is used in chunk 3a.

1.3.2. *Expansions.* Import expansions of predicates and adjectives from the specified articles.

7f ⟨`group_22.miz` *expansions* 7f⟩≡
```
expansions TARSKI, FINSET_1, GROUP_1, GROUP_2, GROUP_6, STRUCT_0, BINOP_1,
  FUNCT_2, NEWTON, PRALG_1, GROUP_7
```
This code is used in chunk 3a.

1.3.3. *Requirements.* Within mathematics, there's a lot of implicit knowledge. Mizar automates some of that with `requirements` inclusions. For example, if we want to show `x in X` (Mizar for the primitive binary predicate $x \in X$) implies the typing relation `x is Element of X`, well, that's "obvious" to us humans, and we can make it obvious to Mizar as well using the proper requirements.

Remark 1.0.4. As I understand it (from Wiedijk's excellent "Writing a Mizar Article in 9 easy steps"), the only possibilities for the `requirements` are: `BOOLE`, `SUBSET`, `NUMERALS`, `ARITHM`, `REAL`.

8a ⟨`group_22.miz` *requirements* 8a⟩≡
```
requirements BOOLE, SUBSET, NUMERALS, ARITHM, REAL
```
This code is used in chunk 3a.

2. Article Body

The article body is where the magic happens. Now we can start making definitions, stating theorems, proving results. The basic structure of our article can be cleaved in two: first we state and prove "helper lemmas", which probably belong somewhere else, but currently are not located anywhere in the Mizar library. The second half are our results concerning characteristic subgroups.

Just to give some idea of what we're doing, we will have to define a notion of `Automorphism`. We will also have to prove a number of results concerning `Automorphisms`. After all, a characteristic subgroup is one which is left invariant under any automorphism of its parent group.

Once that has been squared away, we will define a notion of a `characteristic` subgroup. Then we will prove results right away.

8b ⟨`group_22.miz` *article body* 8b⟩≡
```
begin :: Preparatory Work
⟨Helper lemmas and registrations for group_22.miz 9a⟩

begin :: Nontrivial Groups and Subgroups
⟨Nontrivial Groups 13a⟩

begin :: Proper Subgroups
⟨Proper Subgroups 17b⟩

begin :: Automorphisms
⟨Automorphisms of Groups 22⟩

begin :: Inner Automorphisms
⟨Inner Automorphisms 36c⟩

begin :: Characteristic Subgroups
⟨Characteristic subgroups 47b⟩

begin :: Results concerning meets
⟨Meets of families of subgroups 78a⟩

begin :: Centralizer of Characteristic Subgroups is Characteristic
⟨Centralizers of Characteristic Subgroups 84⟩
```

This code is used in chunk 2a.

3. Preparatory results

There are a lot of recurring patterns which can be isolated into helper functions—err, lemmas. I'm sure many (if not all) are already present somewhere in the Mizar Mathematical Library, but I couldn't find them. I am placing them within their own "section", because if I ever submit the result to the Mizar Mathematical Library, they will either be removed (and relocated to the relevant articles) or the editors will know what I should have done instead.

9a ⟨*Helper lemmas and registrations for* `group_22.miz` 9a⟩≡

```
reserve X for set;
```

⟨*Register: the identity function is surjective and bijective* 9b⟩

⟨*Theorem: restriction of group morphism acts on elements like the original* 10a⟩

⟨*Theorem: Subgroups invariant under conjugation are normal* 10b⟩

⟨*Theorem: if f is bijective, then $(f^{-1})^{-1} = f$* 11a⟩

⟨*Theorem: if $f\colon X \to Y$ is bijective, then $f \circ f^{-1} = \mathrm{id}_Y$* 12a⟩

⟨*Theorem: $f\colon X \hookrightarrow Y$ and $x \notin A \subseteq X$ implies $f(x) \notin f(A)$* 12b⟩

This code is used in chunk 8b.

Registration 1.1. We begin by registering the identity function as being surjective and bijective. This should have been done in [Funct_2], but hey, what can you do?

9b ⟨*Register: the identity function is surjective and bijective* 9b⟩≡

```
registration
  let X;
  cluster id X -> onto;
  coherence;
end;

registration
  let X;
  cluster id X -> bijective;
  coherence;
end;
```

This code is used in chunk 9a.

Theorem 1.1 (Restriction of Group Morphisms to Subgroups)**.** *If $f\colon G_1 \to G_2$ is a group morphism and $H \leq G_1$ is a subgroup, then for any $h \in H$ we have $f(h) = f|_H(h)$.*

Remark 1.1.1. Mizar proves that, if $f\colon X \to Y$ is a set theoretic function and $A \subseteq X$ is an arbitrary subset, then $\forall a \in X$ we have $a \in A \implies f|_A(a) = f(a)$. But this doesn't generalize to morphisms, sadly, because a group is like a chocolate-covered set.

So we just prove for any pair of groups G_1 and G_2, for any subgroup $H \leq G_1$, for any group morphism $f\colon G_1 \to G_2$, and for arbitrary $h \in G_1$, we have $h \in H \implies f|_H(h) = f(h)$. The reasoning is that we can always look at the set-theoretic function $U(f)$ underlying f, then piggie-back off earlier results establishing the desired claim (Theorem [FUNCT_1:Th49], to be precise).

10a ⟨*Theorem: restriction of group morphism acts on elements like the original* 10a⟩≡

```
theorem Th1:
  for G1,G2 being Group
  for H being Subgroup of G1
  for f being Homomorphism of G1,G2
  for h being Element of G1
  st h in H
  holds (f|H).h = f.h
proof
  let G1,G2 be Group;
  let H be Subgroup of G1;
  let f be Homomorphism of G1,G2;
  let h be Element of G1;
  assume h in H;
  then (f|(the carrier of H)).h = f.h by FUNCT_1:49;
  hence (f|H).h = f.h by GRSOLV_1:def 2;
end;
```

This code is used in chunk 9a.
Defines:
Th1, never used.

Theorem 1.2. *Let $H \leq G$ be such that $\forall a \in G, a^{-1}Ha = H$. Then $H \trianglelefteq G$ is a normal subgroup.*

Remark 1.2.1. The current theorems in [GROUP_3] require H to be a *strict* subgroup, but this strictness condition is not necessary.

10b ⟨*Theorem: Subgroups invariant under conjugation are normal* 10b⟩≡

```
theorem Th2:
  for G being Group
  for H being Subgroup of G
  st (for a being Element of G holds H |^ a = the multMagma of H)
  holds H is normal Subgroup of G
proof
  let G be Group;
  let H be Subgroup of G;
  assume for a being Element of G holds H |^ a = the multMagma of H;
  hence H is normal Subgroup of G by GROUP_3:def 13;
end;
```

This code is used in chunk 9a.
Defines:
Th2, never used.

Theorem 1.3. *If $f\colon X \to Y$ is a bijective function of non-empty sets, then $(f^{-1})^{-1} = f$.*

Proof outline. Let $f\colon X \to Y$ be bijective. Then $g = f^{-1}$ is a bijective function from Y to X. And $h = g^{-1}$ is a bijective function from X to Y. Then for any $x \in X$, we have $f(x) = h(x)$. This proves the claim. □

11a ⟨*Theorem: if f is bijective, then $(f^{-1})^{-1} = f$* 11a⟩≡

```
theorem Th3:
  for X,Y being non empty set
  for f being Function of X,Y
  st f is bijective
  holds (f")" = f
proof
  let X,Y be non empty set;
  let f be Function of X,Y;
  assume A1: f is bijective;
  then A2: dom f = X & rng f = Y & f is one-to-one by FUNCT_2:def 3,def 1;
  reconsider g = f" as Function of Y,X by A2,FUNCT_2:25;
  A3: g is bijective by A1,GROUP_6:63;
  g is one-to-one & rng g = X implies g" is Function of X,Y
  by FUNCT_2:25;
  then reconsider h = g" as Function of X,Y by A3,FUNCT_2:def 3;

  for x being object st x in X holds h.x = f.x
  ⟨Proof: ∀x, x ∈ X ⟹ h(x) = f(x) 11b⟩
  then h = f;
  hence (f")" = f;
end;
```

This code is used in chunk 9a.
Defines:
Th3, never used.

Proof step (∀x ∈ X, h(x) = f(x)). Let $x \in X$ be arbitrary. Consider

$$y = f(x). \tag{3.1a}$$

Then $x = g(y)$ — i.e., $x = f^{-1}(y)$ — implies

$$h(x) = g^{-1}(x) = y. \tag{3.1b}$$

But since $y = y$ we from Eqs (3.1) prove $h(x) = f(x)$. □

11b ⟨*Proof: ∀x, x ∈ X ⟹ h(x) = f(x)* 11b⟩≡

```
proof
  let x be object;
  assume x in X;
  then reconsider x as Element of X;
  consider y being object such that
  Z1: y = f.x;
  x = g.y by A1,Z1,FUNCT_2:26;
  hence thesis by A1,Z1,FUNCT_2:26;
end;
```

This code is used in chunk 11a.

Theorem 1.4. *If $f\colon X \to Y$ is a bijective function of sets, then for any $y \in Y$ we have $f(f^{-1}(y)) = y$.*

Proof sketch. Let $f\colon X \to Y$ be bijective. Then $g\colon Y \to X$ given by $g = f^{-1}$ is bijective. Mizar knows $g^{-1}(g(y)) = y$ for $y = f(x)$. Then plugging in the definition of g and using Theorem 1.3 to transform $(f^{-1})^{-1} = f$, together gives the result. □

Remark 1.4.1. Mizar has the opposite result in its library, namely, Theorem [FUNCT_2:Th26] states that $f^{-1}(f(x)) = x$ provided f is injective.

12a ⟨*Theorem: if* $f\colon X \to Y$ *is bijective, then* $f \circ f^{-1} = \mathrm{id}_Y$ 12a⟩≡

```
theorem Th4:
  for X,Y being non empty set
  for f being Function of X,Y
  st f is bijective
  for y being Element of Y
  holds f.((f").y) = y
proof
  let X,Y be non empty set;
  let f be Function of X,Y;
  assume A1: f is bijective;
  let y be Element of Y;
  f is onto by A1;
  then reconsider g = f" as Function of Y,X by A1,FUNCT_2:25;
  y = (g").(g.y) by A1,FUNCT_2:26
   .= f.((f").y) by Th3,A1;
  hence thesis;
end;
```

This code is used in chunk 9a.
Defines:
Th4, never used.

Theorem 1.5. *Let* $f\colon X \hookrightarrow Y$ *be an injective function of non-empty sets, let* $A \subseteq X$ *be a non-empty subset, let* $x \in X$ *be any element such that* $x \notin A$*. Then* $f(x) \notin f(A)$*.*

Proof sketch. We prove that, if $f(x) \in f(A)$, then we get a contradiction with the hypothesis $x \notin A$ or f is injective. □

12b ⟨*Theorem:* $f\colon X \hookrightarrow Y$ *and* $x \notin A \subseteq X$ *implies* $f(x) \notin f(A)$ 12b⟩≡

```
theorem Th5:
  for X,Y being non empty set
  for A being non empty Subset of X
  for x being Element of X
  st not x in A
  for f being Function of X,Y
  st f is one-to-one
  holds not f.x in (f .: A)
proof
  let X,Y be non empty set;
  let A be non empty Subset of X;
  let x be Element of X;
  assume A1: not x in A;
  let f be Function of X,Y;
  assume A2: f is one-to-one;
  A3: dom f = X by FUNCT_2:def 1;
  f.x in (f .: A) iff ex a being object st a in dom f & a in A & f.x = f.a
  by FUNCT_1:def 6;
  hence f.x in (f .: A) implies contradiction by A2,A3,A1,FUNCT_1:def 4;
end;
```

This code is used in chunk 9a.

Defines:
Th5, never used.

4. Nontrivial Groups

We will be using nontrivial groups later. Recall, a group G is nontrivial if $G \neq \mathbf{1}_G$. It is defined (or *overloaded*) in [GROUP_6:def2]:

```
definition
  let G be non empty 1-sorted;
  redefine attr G is trivial means
  ::GROUP_6:Def2
  ex x being object st the carrier of G = {x};
  compatibility
  :: ...
end;
```

We register the negated version "non trivial" for groups and subgroups.

13a ⟨*Nontrivial Groups* 13a⟩≡
⟨*Register: non trivial for Group* 13b⟩
⟨*Register: trivial groups and trivial subgroups* 14a⟩
⟨*Register: non trivial for Subgroup* 14b⟩

⟨*Theorem: trivial groups look like* $\mathbf{1}$ 15b⟩

⟨*Register: nontrivial for "finite group"* 16a⟩

⟨*Theorem:* $H \leq G$*,* H *is trivial implies* $H = \mathbf{1}_G$ 16b⟩

⟨*Theorem: for* $H \leq G$ *and* $K \leq G$ *both trivial,* $H = K$ 16c⟩

⟨*Theorem:* $H \leq K$ *and* $K \leq G$*, then* $K = \mathbf{1} \implies H = \mathbf{1}$ 17a⟩
This code is used in chunk 8b.

Proposition 1.2 ([GROUP_1:Th3])**.** *The real numbers equipped with addition form a group.*

Remark 1.2.1. We will need this to prove the existence of nontrivial groups and, later, serve as an example of a nontrivial group with a proper subgroup.

Registration 1.3. We have a notion of "non trivial" groups, and at least one exists (namely, the real numbers as an Abelian group).

13b ⟨*Register: non trivial for Group* 13b⟩≡

```
registration
  cluster non trivial for Group;
  existence
  proof
    reconsider G = multMagma (# REAL, addreal #) as Group by GROUP_1:3;
    take G;
    thus not (G is trivial);
  end;
end;
```

This code is used in chunk 13a.
Defines:
`trivial`, never used.

Registration 1.4. We need to register the adjective "trivial" for groups and subgroups. *Every* group — strict or not, proper or not, hairy or bald — has a trivial subgroup. Similarly, *every* subgroup has a trivial subgroup.

14a ⟨*Register: trivial groups and trivial subgroups* 14a⟩≡

```
registration
  let G be Group;
  cluster trivial for Subgroup of G;
  existence
  proof
    take (1).G;
    thus thesis;
  end;
  let H be Subgroup of G;
  cluster trivial for Subgroup of H;
  existence
  proof
    take (1).H;
    thus thesis;
  end;
end;
```

This code is used in chunk 13a.
Defines:
`trivial`, never used.

Registration 1.5. For any non trivial group G, we can find a nontrivial subgroup $H \leq G$, namely G itself.

14b ⟨*Register: non trivial for Subgroup* 14b⟩≡

```
registration
  let G be non trivial Group;
  cluster non trivial for Subgroup of G;
  existence
  proof
    reconsider H=G as Subgroup of G by GROUP_2:54;
    the carrier of H <> {1_G};
    hence thesis;
  end;

  cluster strict non trivial for Subgroup of G;
  existence
  ⟨Proof: existence of strict nontrivial subgroup of G 15a⟩
end;
```

This code is used in chunk 13a.

Proof outline (Existence of nontrivial subgroup). We basically take the strict group underlying G as an example of a nontrivial subgroup. □

15a ⟨*Proof: existence of strict nontrivial subgroup of G* 15a⟩≡

```
proof
  set H = multMagma (#the carrier of G, the multF of G#);
  reconsider H as Group-like non empty multMagma;
  the multF of H = (the multF of G)||the carrier of H;
  then H is strict Subgroup of G & H is non trivial by GROUP_2:def 5;
  hence thesis;
end;
```

This code is used in chunk 14b.

Theorem 1.6. *A group G is trivial if $G = \mathbf{1}$.*

One direction has been proven in Theorem [GROUP_6:Th10], so we just need to prove the forward direction.

15b ⟨*Theorem: trivial groups look like* **1** 15b⟩≡

```
theorem Th6:
  for G being Group
  holds G is trivial iff the multMagma of G = (1).G
proof
  let G be Group;
  thus G is trivial implies the multMagma of G = (1).G
  proof
    assume G is trivial;
    then consider x being object such that
    A1: the carrier of G = {x};
    x = 1_G by A1, TARSKI:def 1;
    then the carrier of G = the carrier of (1).G by A1,GROUP_2:def 7;
    hence the multMagma of G = (1).G by GROUP_2:61;
  end;
  thus the multMagma of G = (1).G implies G is trivial;
  thus thesis;
end;
```

This code is used in chunk 13a.
Defines:
Th6, never used.

Lemma 1.1. *$\mathbb{Z}_2$ is a nontrivial group.*

Proof outline. The set underlying $\mathbb{Z}_2$ is [isomorphic to] the ordinal $2 = \{0, 1\}$ whereas the set underlying its trivial subgroup is the ordinal $1 = \{0\}$. These are different set, and thus must underly different groups. □

15c ⟨*Lemma: Existence of finite nontrivial groups* 15c⟩≡

```
LmFiniteNontrivial:
  not INT.Group(2) is trivial
proof
  set G = INT.Group(2);
  the carrier of (1).G = {1_G} by GROUP_2:def 7
                      .= {} \/ {0} by GR_CY_1:14
                      .= succ 0 by ORDINAL1:def 1
                      .= 1;
  then the carrier of (1).G <> the carrier of G by ORDINAL1:def 17;
  hence not INT.Group(2) is trivial by Th6;
```

```
end;
```

This code is used in chunk 16a.
Defines:
`LmFiniteNontrivial`, never used.

Registration 1.6. We can have `non trivial finite Group` as a sensible type, so we register `non trivial` as an adjective for the type `finite Group`.

16a ⟨*Register: nontrivial for "finite group"* 16a⟩≡
⟨*Lemma: Existence of finite nontrivial groups* 15c⟩

```
registration
  cluster non trivial for finite Group;
  existence by LmFiniteNontrivial;
end;
```

This code is used in chunk 13a.

Theorem 1.7. *If $H \leq G$ is trivial, then $H = \mathbf{1}$.*

Proof. *Trivial*, thanks to Theorem 1.6. □

16b ⟨*Theorem: $H \leq G$, H is trivial implies $H = \mathbf{1}_G$* 16b⟩≡

```
theorem Th7:
  for G being Group
  for H being Subgroup of G
  st H is trivial
  holds the multMagma of H = (1).G
proof
  let G be Group;
  let H be Subgroup of G;
  assume H is trivial;
  then the multMagma of H = (1).H by Th6
                          .= (1).G by GROUP_2:63;
  hence thesis;
end;
```

This code is used in chunk 13a.
Defines:
`Th7`, never used.

Theorem 1.8. *If $H \leq G$ and $K \leq G$ are both trivial, then $H = K$ as groups.*

Proof. If H and K are both trivial, then by Theorem 1.7 they both look like $\mathbf{1}$ and thus are equal to each other as groups. □

16c ⟨*Theorem: for $H \leq G$ and $K \leq G$ both trivial, $H = K$* 16c⟩≡

```
theorem Th8:
  for G being Group
  for H being trivial Subgroup of G
  for K being trivial Subgroup of G
  holds the multMagma of H = the multMagma of K
proof
  let G be Group;
```

```
  let H be trivial Subgroup of G;
  let K be trivial Subgroup of G;
  the multMagma of H = (1).G by Th7
                    .= the multMagma of K by Th7;
  hence thesis;
end;
```

This code is used in chunk 13a.
Defines:
Th8, never used.

Theorem 1.9. *If $H \leq K$ and $K \leq G$ and $K = \mathbf{1}_G$, then $H = \mathbf{1}_G$.*

Proof. We have $\mathbf{1} \leq H \leq \mathbf{1}$ imply $H = \mathbf{1}$. But since we didn't use strict subgroups, we need to work with their underlying sets and the fact $\{1_G\} \subseteq H \subseteq \{1_G\}$ implies $H = \{1_G\}$ by Definition [XBOOLE_0:def10]. □

17a ⟨*Theorem: $H \leq K$ and $K \leq G$, then $K = \mathbf{1} \implies H = \mathbf{1}$* 17a⟩≡

```
theorem Th9:
  for G being Group
  for K being trivial Subgroup of G
  for H being Subgroup of G
  st H is Subgroup of K
  holds H is trivial Subgroup of G
proof
  let G be Group;
  let K be trivial Subgroup of G;
  let H be Subgroup of G;
  assume A1: H is Subgroup of K;
  the carrier of H = {1_G}
  proof
    the multMagma of K = (1).G by Th7;
    then the carrier of K = {1_G} by GROUP_2:def 7;
    then B1: the carrier of H c= {1_G} by A1,GROUP_2:def 5;
    (1).G is Subgroup of H by GROUP_2:65;
    then the carrier of (1).G c= the carrier of H by GROUP_2:def 5;
    then {1_G} c= the carrier of H by GROUP_2:def 7;
    hence the carrier of H = {1_G} by B1,XBOOLE_0:def 10;
  end;
  hence H is trivial Subgroup of G;
end;
```

This code is used in chunk 13a.
Defines:
Th9, never used.

5. Proper Subgroups

When we have a [nontrivial] group G, we can discuss the notion of a proper subgroup $H < G$ in analogy to the notion of a proper subset $X \subset Y$.

17b ⟨*Proper Subgroups* 17b⟩≡
⟨*Definition: proper subgroup* 18a⟩

⟨*Theorem: $H \leq G$ is proper iff the underlying sets are different* 19c⟩

⟨*Theorem: $H \leq G$ is proper iff $G \setminus H \neq \emptyset$* 20a⟩

⟨*Register: proper subgroup for nontrivial groups* 18b⟩

⟨*Lemma: maximal subgroups are proper* 21a⟩

⟨*Register: maximal subgroups are proper* 21b⟩

⟨*Theorem: $H < K \leq G$ and $H \neq K$ implies K is nontrivial* 21c⟩

This code is used in chunk 8b.

Definition 1.1. Let G be a group. We call a subgroup $H \leq G$ **"Proper"** if $H \neq G$. We typically denote $H < G$ to reflect it is proper.

Remark 1.1.1. The implementation for Mizar is a bit quirky. I looked at how maximal subgroups were defined, because maximal subgroups are necessarily proper. Maximal subgroups were defined ([GROUP_4:def 6]) using the condition the multMagma of H <> the multMagm

18a ⟨*Definition: proper subgroup* 18a⟩≡

```
definition
  let G be Group;
  let IT be Subgroup of G;
  attr IT is proper means
  :Def1:
  the multMagma of IT <> the multMagma of G;
end;
```

This code is used in chunk 17b.
Defines:
Def10, never used.
proper, never used.

Registration 1.7. For any nontrivial group G, we can find a proper subgroup $H \leq G$, namely the trivial subgroup $H = \mathbf{1}_G$.

18b ⟨*Register: proper subgroup for nontrivial groups* 18b⟩≡

```
registration
  let G be non trivial Group;
  cluster proper for Subgroup of G;
  existence
  proof
    take (1).G;
    thus (1).G is proper;
  end;
  ⟨Cluster proper normal Subgroup 19a⟩
  ⟨Cluster strict proper normal Subgroup 19b⟩
end;
```

This code is used in chunk 17b.

Registration 1.8. For any nontrivial group G, we can find a proper *normal subgroup* $H \trianglelefteq G$, namely the trivial subgroup $H = \mathbf{1}_G$.

19a ⟨*Cluster* `proper normal Subgroup` 19a⟩≡
```
cluster proper for normal Subgroup of G;
existence
proof
  take (1).G;
  thus (1).G is proper;
end;
```
This code is used in chunk 18b.

Registration 1.9. For any nontrivial group G, we can find a strict proper *normal subgroup* $H \trianglelefteq G$, namely the trivial subgroup $H = \mathbf{1}_G$.

19b ⟨*Cluster* `strict proper normal Subgroup` 19b⟩≡
```
cluster strict proper for normal Subgroup of G;
existence
proof
  take (1).G;
  thus (1).G is strict proper;
end;
```
This code is used in chunk 18b.

Theorem 1.10. *Let $H \leq G$ be a subgroup. Then $H < G$ is proper if and only if the underlying set of G differs from the underlying set of H.*

Proof outline. The only way a group could be different, since they are magmas satisfying some properties, is either if the underlying set differs or if the group operation differs. But since we know H is a subgroup of G, we know the group operation for H is just the restricted version of the group operation for G. Thus we are forced to accept the underlying sets must be different. This argument works backwards as well as forwards. □

19c ⟨*Theorem: $H \leq G$ is proper iff the underlying sets are different* 19c⟩≡
```
reserve G for Group;
reserve H for Subgroup of G;
theorem Th10:
  H is proper iff the carrier of H <> the carrier of G
proof
  (the carrier of H c= the carrier of G) & (the multF of H =
  (the multF of G)||(the carrier of H)) by GROUP_2:def 5;
  hence thesis;
end;
```
This code is used in chunk 17b.
Defines:
`Th10`, never used.

Theorem 1.11. *Let $H \leq G$ be a subgroup. Then H is a proper subgroup if and only if the set difference is nonempty $G \setminus H \neq \emptyset$.*

Remark 1.11.1. This version, as stated, is a little sloppy. We should more precisely state the set difference of the underlying set $U(G)$ of G with the underlying set $U(H)$ of H is nonempty $U(G) \setminus U(H) \neq \emptyset$.

Proof outline. There are two sub-proofs:

(1) H is proper implies $U(G) \setminus U(H) \neq \emptyset$

(2) $U(G) \setminus U(H) \neq \emptyset$ implies H is proper. □

20a ⟨*Theorem: $H \leq G$ is proper iff $G \setminus H \neq \emptyset$* 20a⟩≡

```
reserve h,x,y for object;

theorem Th11:
  H is proper iff (the carrier of G) \ (the carrier of H) is non empty set
proof
  set UG = the carrier of G;
  set UH = the carrier of H;
  thus H is proper implies UG \ UH is non empty set
  ⟨Sub-proof: H < G ⟹ G \ H ≠ ∅ 20b⟩
  thus UG \ UH is non empty set implies H is proper
  ⟨Sub-proof: H < G ⟸ G \ H ≠ ∅ 20c⟩
  thus thesis;
end;
```

This code is used in chunk 17b.
Defines:
`Th11`, never used.

Sub-proof outline. If $H < G$ is a proper subgroup, then the underlying set $U(H)$ of H is a subset of the underlying set $U(G)$ of G — i.e., $U(H) \subseteq U(G)$ — and $U(H) \neq U(G)$. Then there is some element $g \in G$ for which $g \notin H$. Then $U(G) \setminus U(H) \neq \emptyset$. □

20b ⟨*Sub-proof: $H < G \implies G \setminus H \neq \emptyset$* 20b⟩≡

```
proof
  assume A1: H is proper;
  UH c= UG & UH <> UG by A1,Th10, GROUP_2:def 5;
  then (for x holds x in UH implies x in UG) &
  not (for x holds x in UH iff x in UG) by TARSKI:2;
  hence (the carrier of G) \ (the carrier of H) is non empty set
  by XBOOLE_0:def 5;
end;
```

This code is used in chunk 20a.

Sub-proof outline. Assume $G \setminus H \neq \emptyset$. Then there exists some $y \in G \setminus H$, i.e., $y \in G$ and $y \notin H$. But we've found an element in G that's not in H. So by the extensional notion of set equality, these are clearly different sets. Thus $H < G$ □

20c ⟨*Sub-proof: $H < G \impliedby G \setminus H \neq \emptyset$* 20c⟩≡

```
proof
  assume A1: (the carrier of G) \ (the carrier of H) is non empty set;
  set GH = UG \ UH;
  ex x st x in GH by A1, XBOOLE_0:def 1;
  hence H is proper by XBOOLE_0:def 5;
end;
```

This code is used in chunk 20a.

Lemma 1.2. *Maximal subgroups are also proper subgroups.*

The proof is literally, "Look at the definitions!"

21a ⟨*Lemma: maximal subgroups are proper* 21a⟩≡

```
Lm1:
  for G being Group
  for H being Subgroup of G
  st H is maximal
  holds H is proper by GROUP_4:def 6;
```

This code is used in chunk 17b.
Defines:
Lm1, never used.

Registration 1.10. We can now automatically take advantage of the fact that, a maximal subgroup for a nontrivial group is implicitly a proper subgroup.

21b ⟨*Register: maximal subgroups are proper* 21b⟩≡

```
registration
  let G be non trivial Group;
  cluster maximal -> proper for Subgroup of G;
  coherence by Lm1;
end;
```

This code is used in chunk 17b.

Theorem 1.12. *If $H < K$ is proper and $K \leq G$ and $H \neq K$, then K is a nontrivial group.*

Proof outline. Assume for contradiction that $K = \mathbf{1}$. Then combined with $H < K$ and $H \neq K$ implies $H = \mathbf{1}$ and this contradicts $H < K$ proper. □

21c ⟨*Theorem: $H < K \leq G$ and $H \neq K$ implies K is nontrivial* 21c⟩≡

```
theorem Th12:
  for G being non trivial Group
  for H being proper Subgroup of G
  for K being Subgroup of G
  st H is Subgroup of K & the multMagma of H <> the multMagma of K
  holds K is non trivial Subgroup of G
proof
  let G be non trivial Group;
  let H be proper Subgroup of G;
  let K be Subgroup of G;
  assume A1: H is Subgroup of K;
  assume A2: the multMagma of H <> the multMagma of K;
  not (K is non trivial Subgroup of G) implies contradiction
  proof
    assume B1: not K is non trivial Subgroup of G;
    then H is trivial Subgroup of G by A1,Th9;
    hence contradiction by A2,B1,Th8;
  end;
  hence K is non trivial Subgroup of G;
end;
```

This code is used in chunk 17b.
Defines:
Th12, never used.

6. Automorphisms

Now, we have a section for defining inner and outer group automorphisms. A *group automorphism* is just a bijective endomorphism on a group, and an *endomorphism* is a group morphism whose codomain is its domain.

Remember (§1.1.1), although we are defining new terms `Endomorphism` and `Automorphism`, we do not need to add them to our `DICT/GROUP_22.VOC` file. Why not? Because the tokens are already included from [Mod_4].

22 ⟨*Automorphisms of Groups* 22⟩≡
⟨*Definition:* `Endomorphism` 23a⟩

⟨*Reserve:* f *for* `Endomorphism` 24b⟩
⟨*Register* `bijective` *for* `Endomorphism` 23b⟩

⟨*Definition:* `Automorphism` 23c⟩
⟨*Reserve:* φ *for* `Automorphism` 23d⟩

⟨*Theorem: Endomorphisms preserve the trivial subgroup* 24a⟩

⟨*Theorem: Automorphisms map trivial subgroups to themselves* 24c⟩

⟨*Theorem: for* $\varphi \in \mathrm{Aut}(G)$ *and* $H \leq G$*, we have* $\ker(\varphi|H) \leq \ker(\varphi)$ 25b⟩

⟨*Lemma: for any* $\varphi \in \mathrm{Aut}(G)$ *and* $H \leq G$ *we have monomorphism* $\varphi|_H$ 26a⟩

⟨*Theorem:* $(\forall \varphi \in \mathrm{Aut}(G), \varphi(H) \leq H) \implies \varphi[\varphi^{-1}(H)] \leq \varphi(H)$ 26b⟩

⟨*Theorem:* $\forall \varphi \in \mathrm{Aut}(G), \varphi[\varphi^{-1}(H)] = H$ 27a⟩

⟨*Theorem:* $\varphi(H) \leq K \implies H \leq \varphi^{-1}(K)$ 29c⟩

⟨*Theorem: for any* $\varphi \in \mathrm{Aut}(G)$ *and* $H \leq G$ *we have* $H \cong \varphi(H)$ 30a⟩

⟨*Theorem: isomorphic subgroups have equal indices* 30b⟩

⟨*Theorem: Sylow p-Subgroups invariant under* $\mathrm{Aut}(G)$ 31⟩

⟨*Theorem:* $\varphi \in \mathrm{Aut}(G)$ *and* $H \leq G$ *such that* $\varphi(H) = H$ *implies* $\varphi|H \in \mathrm{Aut}(H)$ 32a⟩

⟨*Theorem:* $\varphi \in \mathrm{Aut}(G)$ *and* $H < G$ *implies* $\varphi(H) < G$ 33a⟩

⟨*Theorem: Automorphisms map maximal subgroups to maximal subgroups* 34a⟩
This code is used in chunk 8b.

Abbreviation 1.11. Let G be a group. An **"Endomorphism"** of G is a group morphism $f : G \to G$.

Remark 1.11.1. We denote the collection of endomorphisms of G as $\mathrm{End}(G)$.

Remark 1.11.2. Mizar uses the archaic word "homomorphism" instead of the more modern conventional term "morphism". I will use the two interchangeably. And, unless stated otherwise, it is understood these are group morphisms.

23a ⟨*Definition:* `Endomorphism` 23a⟩≡

```
definition
  let G;
  mode Endomorphism of G is Homomorphism of G,G;
end;
```

This code is used in chunk 22.
Defines:
`Endomorphism`, never used.

Registration 1.12. We begin by registering the attribute `bijective` for group endomorphisms. This will effectively create a subtype of `Endomorphism of G`, the aptly named `bijective Endomorphism of G`. Most of our work has been done in Theorem [GROUP_6:Th38] (which effectively states the function on the underlying set `id (the carrier of G)` is a multiplicative function and so nearly a group morphism that we can reconsider it as an `Endomorphism`), and the fact that `id X` is bijective.

23b ⟨*Register* `bijective` *for* `Endomorphism` 23b⟩≡

```
registration
  let G;
  cluster bijective for Endomorphism of G;
  existence
  proof
    reconsider i = id the carrier of G as Homomorphism of G,G by GROUP_6:38;
    i is bijective;
    hence thesis;
  end;
end;
```

This code is used in chunk 22.

Abbreviation 1.13. Let G be a group. We define an **"Automorphism"** of G to be a bijective endomorphism $f\colon G \to G$. In particular, an inverse $f^{-1}\colon G \to G$ exists and is a group morphism.

Remark 1.13.1. We denote the collection of automorphisms of G as $\mathrm{Aut}(G)$.

23c ⟨*Definition:* `Automorphism` 23c⟩≡

```
definition
  let G;
  mode Automorphism of G is bijective Endomorphism of G;
end;
```

This code is used in chunk 22.
Defines:
`Automorphism`, never used.

Reserve 1.14. We will henceforth generically use φ as an Automorphism of G unless otherwise stated. This means, for most theorems, we can omit explicitly stating, "For any automorphism φ of G, ..."; and for most proofs, we can omit the line, "Let φ be an Automorphism of G".

23d ⟨*Reserve:* φ *for* `Automorphism` 23d⟩≡

```
reserve phi for Automorphism of G;
```

This code is used in chunk 22.

Proposition 1.15. *For any automorphism $\varphi\colon G \to G$, its inverse φ^{-1} is also an automorphism.*

This is proven in Theorem [GROUP_6:Th62]. We have, for example, the following accepted by Mizar:

```
for G being Group
for phi being Automorphism of G
holds phi" is Automorphism of G by GROUP_6:62;
```

Theorem 1.13. *For any group G and endomorphism $f \in \mathrm{End}(G)$, we have the trivial subgroup $\mathbf{1} \leq G$ be preserved under f; i.e., $f(\mathbf{1}) = \mathbf{1}$.*

The proof is simply "follow your nose".

Proof. Trivial. □

24a ⟨*Theorem: Endomorphisms preserve the trivial subgroup* 24a⟩≡

```
theorem Th13:
  Image (f|(1).G) = (1).G
proof
  Image(f|(1).G) = f .: ((1).G) by GRSOLV_1:def 3
                .= (1).G by GRSOLV_1:11;
  hence thesis;
end;
```

This code is used in chunk 22.
Defines:
Th13, never used.

Reserve 1.16. Now we need to tell Mizar that f is an endomorphism of G.

24b ⟨*Reserve: f for* Endomorphism 24b⟩≡

```
reserve f for Endomorphism of G;
```

This code is used in chunk 22.

Theorem 1.14. *For any automorphism $\varphi \in \mathrm{Aut}(G)$, we have $\varphi(\mathbf{1}_G) = \mathbf{1}_G$.*

Proof outline. If ϕ is an automorphism of a group G, then the image of the trivial subgroup under ϕ is a subgroup of itself $\phi(\mathbf{1}) \leq \mathbf{1}$. We have, from Theorem 1.13, that $\phi(\mathbf{1}) = \mathbf{1}$ since ϕ (being an automorphism) is also an endomorphism. And Theorem [GROUP_2:Th54] proves that G is a subgroup of itself. □

24c ⟨*Theorem: Automorphisms map trivial subgroups to themselves* 24c⟩≡

```
:: In particular, the trivial proper subgroup (1).G of G is invariant
:: under inner automorphisms, and thus is a characteristic subgroup.
theorem Th14:
  Image(phi|(1).G) is Subgroup of (1).G
proof
  (1).G is Subgroup of (1).G by GROUP_2:54;
  hence Image(phi|(1).G) is Subgroup of (1).G by Th13;
end;
```

This code is used in chunk 22.
Defines:
Th14, never used.

Lemma 1.3. *If $H \leq \mathbf{1}_G \leq G$, then $H = \mathbf{1}$.*

Proof. Assume $H \leq \mathbf{1}_G$. We know $\mathbf{1}_G \leq H$, and taken together, the result follows. □

25a ⟨*Lemma: $H \leq G$ and $\mathbf{1} \leq H$ implies $H = \mathbf{1}$* 25a⟩≡

```
Lm2: H is Subgroup of (1).G implies the multMagma of H = the multMagma of (1).G
proof
  assume H is Subgroup of (1).G;
  then H is Subgroup of (1).G & (1).G is Subgroup of H by GROUP_2:65;
  hence thesis by GROUP_2:55;
end;
```

This code is used in chunk 26a.
Defines:
Lm2, never used.

Theorem 1.15. *Let G be a group, $H \leq G$ any subgroup, and $\varphi \in \mathrm{Aut}(G)$ any automorphism. Then* $\ker(\varphi|H) \leq \ker(\varphi)$.

Proof outline. We begin by recognizing $\ker(\varphi|_H) \leq G_1$ and $\ker(\varphi) \leq G_1$. Then any $g \in G$ such that $g \in \ker(\varphi|_H)$ is also a member of $\ker(\varphi)$. The result follows. □

25b ⟨*Theorem: for $\varphi \in \mathrm{Aut}(G)$ and $H \leq G$, we have* $\ker(\varphi|H) \leq \ker(\varphi)$ 25b⟩≡

```
theorem Th15:
  for G1,G2 being Group
  for f being Homomorphism of G1,G2
  for H being Subgroup of G1
  holds Ker(f|H) is Subgroup of Ker(f)
proof
  let G1,G2 be Group;
  let f be Homomorphism of G1,G2;
  let H be Subgroup of G1;
  A1: Ker(f|H) is Subgroup of G1 by GROUP_2:56;
  for g being Element of G1 st g in Ker(f|H) holds g in Ker(f)
  ⟨Proof: ∀g ∈ G, g ∈ ker(φ|H) ⟹ g ∈ ker(H) 25c⟩
  hence thesis by A1,GROUP_2:58;
end;
```

This code is used in chunk 22.
Defines:
Th15, never used.

Sub-proof (∀g ∈ G, g ∈ ker(φ|H) ⟹ g ∈ ker(H)). Any $g \in \ker(\varphi|_H)$ is defined to be $\varphi|_H(g) = 1_{G_2}$. But $\varphi|_H(g) = \varphi(g)$ by Theorem 1.1. So we have $\varphi(g) = 1_{G_2}$, which implies $g \in \ker(\varphi)$ by Theorem [GROUP_6:Th41]. □

25c ⟨*Proof: ∀g ∈ G, g ∈ ker(φ|H) ⟹ g ∈ ker(H)* 25c⟩≡

```
proof
  let g be Element of G1;
  assume A2: g in Ker(f|H);
  then A3: g in H by GROUP_2:40;
  (f|H).g = f.g by A2,Th1,GROUP_2:40;
  then 1_G2 = f.g by A2,A3,GROUP_6:41;
  hence g in Ker(f) by GROUP_6:41;
end;
```

This code is used in chunk 25b.

Lemma 1.4. *For any subgroup $H \leq G$ and automorphism $\varphi \in \mathrm{Aut}(G)$ of G, we have $\varphi|_H \colon H \hookrightarrow \varphi(H)$ be an injective group morphism.*

Proof sketch. Given a subgroup $H \leq G$ and automorphism $\varphi \in \mathrm{Aut}(G)$, we know $\varphi|_H \colon H \to \varphi|_H(H)$ is a group morphism. Since φ is an automorphism, it is injective, and in particular $\ker(\varphi) = \mathbf{1}_G$. Then $\ker(\varphi|_H) \leq \ker(\varphi)$ and $\mathbf{1}_G \leq \ker(\varphi|_H)$ implies $\ker(\varphi|_H)$ is trivial, and thus $\varphi|_H$ is injective. □

26a ⟨*Lemma: for any $\varphi \in \mathrm{Aut}(G)$ and $H \leq G$ we have monomorphism $\varphi|_H$* 26a⟩≡
⟨*Lemma: $H \leq G$ and $\mathbf{1} \leq H$ implies $H = \mathbf{1}$* 25a⟩
```
Lm3:
(phi|H) is Homomorphism of H,Image(phi|H) & (phi|H) is one-to-one
proof
  thus phi|H is Homomorphism of H,Image(phi|H) by GROUP_6:49;
  Ker(phi) = (1).G by GROUP_6:56;
  then Ker(phi|H) is Subgroup of (1).G by Th15;
  then Ker(phi|H) = (1).G by Lm2
                 .= (1).H by GROUP_2:63;
  hence (phi|H) is one-to-one by GROUP_6:56;
end;
```
This code is used in chunk 22.
Defines:
Lm3, never used.

Theorem 1.16. *Let $H \leq G$ be a subgroup such that $\forall \varphi \in \mathrm{Aut}(G), \varphi(H) \leq H$. Then any automorphism φ of G has an inverse which satisfies $\varphi[\varphi^{-1}(H)] \leq \varphi(H)$.*

Proof. Let $\psi = \varphi^{-1} \in \mathrm{Aut}(G)$ be an automorphism (which follows from Theorem [GROUP_6:Th62]). We have $\psi(H) = \psi|_H(H) \leq H$ since the image of a morphism is a subgroup of the codomain. Then $\phi(\psi(H)) \leq \phi(H)$. □

26b ⟨*Theorem: $(\forall \varphi \in \mathrm{Aut}(G), \varphi(H) \leq H) \implies \varphi[\varphi^{-1}(H)] \leq \varphi(H)$* 26b⟩≡
```
theorem Th16:
  (for f being Automorphism of G holds Image(f|H) is Subgroup of H) implies
  ex psi being Automorphism of G
  st psi = phi" & Image(phi|Image(psi|H)) is Subgroup of Image(phi|H)
proof
  assume A1: for f being Automorphism of G holds Image(f|H) is Subgroup of H;
  reconsider psi = phi" as Automorphism of G by GROUP_6:62;
  take psi;
  thus psi = phi";
  Image(psi|H) is Subgroup of H by A1;
  then phi .: Image(psi|H) is Subgroup of phi .: H by GRSOLV_1:12;
  then Image(phi|Image(psi|H)) is Subgroup of phi .: H by GRSOLV_1:def 3;
  hence Image(phi|Image(psi|H)) is Subgroup of Image(phi|H) by GRSOLV_1:def 3;
end;
```
This code is used in chunk 22.
Defines:
Th16, never used.

Theorem 1.17. *Let G be a group, and $H \leq G$ be a subgroup. Then for any automorphism $\varphi \in \mathrm{Aut}(G)$, we have $\varphi[\varphi^{-1}(H)] = H$.*

This is an obvious result which is usually taken for granted.

Proof outline. Let $\psi = \varphi^{-1} \in \mathrm{Aut}(G)$ (which follows from Theorem [GROUP_6:Th62]). Then we establish any group element g is a member of $\varphi(\psi(H))$ if and only if g is a member of H. The result then follows that they are equal as groups using Theorem [GROUP_2:Th60]. □

27a ⟨*Theorem:* $\forall \varphi \in \mathrm{Aut}(G), \varphi[\varphi^{-1}(H)] = H$ 27a⟩≡

```
theorem Th17:
  ex psi being Automorphism of G
  st psi = phi" & Image(phi|Image(psi|H)) = the multMagma of H
proof
  reconsider psi = phi" as Automorphism of G by GROUP_6:62;
  take psi;
  thus psi = phi";
  for g being Element of G holds g in Image(phi|Image(psi|H)) iff g in H
  ⟨Proof: ∀g ∈ G, g ∈ φ[φ⁻¹(H)] ⟺ g ∈ H 27b⟩
  hence Image(phi|Image(psi|H)) = the multMagma of H by GROUP_2:60;
end;
```

This code is used in chunk 22.
Defines:
Th17, never used.

Sub-proof ($\forall g \in G, g \in \varphi[\varphi^{-1}(H)] \implies g \in H$*).* The bones of the proof for this claim amounts to unfolding the logical structure of the claim. □

27b ⟨*Proof:* $\forall g \in G$, $g \in \varphi[\varphi^{-1}(H)] \iff g \in H$ 27b⟩≡

```
proof
  let g be Element of G;
  thus g in Image(phi|Image(psi|H)) implies g in H
  ⟨Step 1: g ∈ φ[φ⁻¹(H)] ⟹ g ∈ H 27c⟩

  thus g in H implies g in Image(phi|Image(psi|H))
  ⟨Step 2: g ∈ φ[φ⁻¹(H)] ⟸ g ∈ H 28c⟩
  thus thesis;
end;
```

This code is used in chunk 27a.

Proof step 1 ($g \in \varphi[\varphi^{-1}(H)] \implies g \in H$*).* We begin by showing, if $g \in \varphi[\varphi^{-1}(H)]$, then there is some M1: $a \in \varphi^{-1}(H)$ such that B2: $g = \varphi(a)$. And then we have, by the same line of reasoning applied to a, there is some M2: $b \in H$ such that B3: $\varphi^{-1}|_H(b) = a$. It follows that $g = \varphi(\varphi^{-1}(b))$, and by Theorem 1.4 we have $g = b$ which proves the claim. □

27c ⟨*Step 1:* $g \in \varphi[\varphi^{-1}(H)] \implies g \in H$ 27c⟩≡

```
proof
  assume g in Image(phi|Image(psi|H));
  ⟨∃a ∈ φ⁻¹(H), g = φ(a) 28a⟩
  ⟨∃b ∈ H, a = φ⁻¹(b) 28b⟩
  then b = phi.(psi.b) by Th4
        .= g by M2,B2,B3,Th1;
  hence g in H;
end;
```

This code is used in chunk 27b.

Proof sub-step 1. Showing $a \in \varphi^{-1}(H)$ and $g = \varphi(a)$ follow from basic results. □

28a ⟨$\exists a \in \varphi^{-1}(H), g = \varphi(a)$ 28a⟩≡
```
then consider a being Element of Image(psi|H) such that
B1: g = (phi|Image(psi|H)).a by GROUP_6:45;
M1: a in Image(psi|H) & a is Element of G by GROUP_2:42;
then B2: phi.a = g by B1, Th1;
```
This code is used in chunk 27c.

Proof sub-step 2. Almost the same reasoning applies to $b \in H$ satisfying $a = \varphi^{-1}(b)$. □

28b ⟨$\exists b \in H, a = \varphi^{-1}(b)$ 28b⟩≡
```
consider b being Element of H such that
B3: a = (psi|H).b
by M1,GROUP_6:45;
M2: b in H & b is Element of G by GROUP_2:42;
```
This code is used in chunk 27c.

Proof step 2 ($g \in \varphi[\varphi^{-1}(H)] \iff g \in H$). To prove $g \in H$ implies $g \in \varphi[\varphi^{-1}(H)]$, we simply let $K = \varphi^{-1}(H)$ and show $a = \varphi^{-1}|_H(g) \in K$ and then show $b = \varphi|_K(a) \in \varphi[K] = \varphi[\varphi^{-1}(H)]$. Then we have $b = \varphi(\varphi^{-1}(g)) = g$ due to φ being bijective. The result follows. □

28c ⟨*Step 2:* $g \in \varphi[\varphi^{-1}(H)] \iff g \in H$ 28c⟩≡
```
proof
  assume B1: g in H;
  set a = (psi|H).g;
  B2: a in Image(psi|H)
  ⟨Sub-step 1: a ∈ φ⁻¹(H) 28d⟩

  set K = Image(psi|H);
  set b = (phi|Image(psi|H)).a;

  B3: b in Image(phi|Image(psi|H))
  ⟨Sub-step 2: b ∈ φ[φ⁻¹(H)] 29a⟩
  thus g in Image(phi|K)
  ⟨Sub-step 3: g ∈ φ[φ⁻¹(H)] 29b⟩
end;
```
This code is used in chunk 27b.

Proof sub-step 1 ($a \in \varphi^{-1}(H)$). The first step follows by unfolding definitions. □

28d ⟨*Sub-step 1:* $a \in \varphi^{-1}(H)$ 28d⟩≡
```
proof
  g in dom(psi|H) by B1,FUNCT_2:def 1;
  then (psi|H).g in (psi|H) .: (the carrier of H) by FUNCT_1:def 6;
  hence a in Image(psi|H) by GROUP_6:def 10;
end;
```
This code is used in chunk 28c.

Proof sub-step 2 ($b \in \varphi[\varphi^{-1}(H)]$). The next step, like the first, follows from definitions. □

29a ⟨*Sub-step 2: $b \in \varphi[\varphi^{-1}(H)]$* 29a⟩≡

```
proof
  a in dom(phi|K) by B2, FUNCT_2:def 1;
  then (phi|K).a in (phi|K) .: (the carrier of K) by FUNCT_1:def 6;
  hence b in Image(phi|K) by GROUP_6:def 10;
end;
```

This code is used in chunk 28c.

Proof sub-step 3 ($g \in \varphi[\varphi^{-1}(H)]$). The last step is a little more involved, because it requires recalling $\varphi|_k(k) = \varphi(k)$ for $k \in K$, and $\varphi^{-1}|_H(h) = \varphi^{-1}(h)$ for $h \in H$. We can then combine these deductions to show $b = \varphi(\varphi^{-1}(g))$ which proves the claim. □

29b ⟨*Sub-step 3: $g \in \varphi[\varphi^{-1}(H)]$* 29b⟩≡

```
proof
  B4: psi.g = a by B1,Th1;
  a is Element of G by B2,GROUP_2:42;
  then (phi|K).a = phi.a by B2,Th1
                .= g by B4,Th4;
  hence thesis by B3;
end;
```

This code is used in chunk 28c.

Theorem 1.18. *Let $H \leq G$ and $K \leq G$ be subgroups, let $\varphi \in \mathrm{Aut}(G)$ be an automorphism of G. If $\varphi(H) \leq K$, then $H \leq \varphi^{-1}(K)$.*

Proof sketch. The argument basically applies Theorem 1.17 to φ^{-1}, then unfolds definitions. □

Remark 1.18.1. I need to work on my numbering scheme...

29c ⟨*Theorem: $\varphi(H) \leq K \implies H \leq \varphi^{-1}(K)$* 29c⟩≡

```
theorem Th18:
  for H being strict Subgroup of G
  for K being Subgroup of G
  st Image(phi|H) is Subgroup of K
  holds ex psi being Automorphism of G
  st psi = phi" & H is Subgroup of Image(psi|K)
proof
  let H be strict Subgroup of G;
  let K be Subgroup of G;
  assume A1: Image(phi|H) is Subgroup of K;
  reconsider psi = phi" as Automorphism of G by GROUP_6:62;
  take psi;
  thus psi = phi";
  consider phi0 being Automorphism of G such that
  A2: phi0 = psi" and
  A3: Image(psi|Image(phi0|H)) = the multMagma of H
  by Th17;
  A4: phi = phi0 by A2,Th3;
  psi .: Image(phi|H) is Subgroup of psi .: K by A1,GRSOLV_1:12;
```

```
    then Image(psi|Image(phi|H)) is Subgroup of psi .: K by GRSOLV_1:def 3;
    hence H is Subgroup of Image(psi|K) by A3,A4,GRSOLV_1:def 3;
  end;
```

This code is used in chunk 22.
Defines:
Th18, never used.

Theorem 1.19. *Let G be a group, $H \leq G$ be any subgroup, and $\varphi \in \mathrm{Aut}(G)$ be any automorphism. Then the image of H under φ is isomorphic to H itself, i.e., $H \cong \varphi(H)$.*

Proof outline. Let $H_2 = \varphi(H)$ be a subgroup of G. We know $\varphi|_H$ is injective by Lemma 1.4. This gives us our result. □

30a ⟨*Theorem: for any $\varphi \in \mathrm{Aut}(G)$ and $H \leq G$ we have $H \cong \varphi(H)$* 30a⟩≡

```
  theorem Th19:
    H,phi .: H are_isomorphic
  proof
    reconsider H2 = phi .: H as Subgroup of G;
    H,Image(phi|H) are_isomorphic by Lm3,GROUP_6:68;
    hence H,phi .: H are_isomorphic by GRSOLV_1:def 3;
  end;
```

This code is used in chunk 22.
Defines:
Th19, never used.

Theorem 1.20. *Let $H_1 \leq G$ and $H_2 \leq G$ be isomorphic subgroups. Suppose G is a finite group. Then $[G : H_1] = [G : H_2]$.*

30b ⟨*Theorem: isomorphic subgroups have equal indices* 30b⟩≡

```
  theorem Th20:
    for G being finite Group
    for H1,H2 being strict Subgroup of G
    st H1,H2 are_isomorphic
    holds index H1 = index H2
  proof
    let G be finite Group;
    let H1,H2 be strict Subgroup of G;
    assume A1: H1,H2 are_isomorphic;
    card H1 * index H1 = card G by GROUP_2:147
                      .= card H2 * index H2 by GROUP_2:147;
    then index H1 * card H1 = index H2 * card H1 by A1,GROUP_6:73;
    hence index H1 = index H2 by XCMPLX_1:5;
  end;
```

This code is used in chunk 22.
Defines:
Th20, never used.

Theorem 1.21. *Let G be a finite group, $p \in \mathbb{N}$ be prime. If $\varphi \in \mathrm{Aut}(G)$ is an automorphism and $P \leq G$ is a Sylow p-subgroup, then $\varphi(P)$ is a Sylow p-subgroup.*

31 ⟨*Theorem: Sylow p-Subgroups invariant under* Aut(G) 31⟩≡

```
theorem Th21:
  G is finite implies
  for p being prime Nat
  for P being strict Subgroup of G
  st P is_Sylow_p-subgroup_of_prime p
  holds Image(phi|P) is_Sylow_p-subgroup_of_prime p
proof
  assume A0: G is finite;
  let p be prime Nat;
  let P be strict Subgroup of G;
  assume A1: P is_Sylow_p-subgroup_of_prime p;
  then A2: P is p-group by GROUP_10:def 18;
  set Q = (phi .: P);
  consider r being Nat such that
  A3: card P = p |^ r
  by A2,GROUP_10:def 17;
  card Q = p |^ r by A3,Th19,GROUP_6:75;
  then A4: Q is p-group by GROUP_10:def 17;
  A5: Q = Image(phi|P) by GRSOLV_1:def 3;
  not p divides index P by A1, GROUP_10:def 18;
  then not p divides index Q by A0,Th19,Th20;
  hence Image(phi|P) is_Sylow_p-subgroup_of_prime p by A4, A5, GROUP_10:def 18;
end;
```

This code is used in chunk 22.
Defines:
Th21, never used.

Theorem 1.22. *Let $H \leq G$ be any subgroup. If $\varphi \in \mathrm{Aut}(G)$ is an automorphism such that $\varphi(H) = H$ it leaves H invariant, then its restriction to H is an automorphism $\varphi|_H \in \mathrm{Aut}(H)$.*

This result isn't surprising, but proving surjectivity was surprisingly (and agonizingly) hard.

Proof outline. Our proof consists of several steps. First, we work with the underlying function restricted to the underlying set $U(H)$ of H, and show it is a function $f|_H \colon U(H) \to U(H)$.

Next, we show $f|_H$ is bijective as a function.

Finally, we show for any $x, y \in H$ that $f|_H(xy) = f|_H(x)f|_H(y)$, which proves $f|_H$ is a group morphism. When combined with the previous step, it shows $f|_H$ is an automorphism of H. □

Remark 1.22.1. Since we only hypothesize that H is a subgroup of G, not a *strict* subgroup, we need the hypothesis to be `Image(f|H) = the multMagma of H` — i.e., the image of the group morphism restricted to H is equal to H *as a group*. We could possibly have extra structure on H (it could have topological structure, or it could be an algebraic variety, or…), but we do not care nor do we need it. We could greatly simplify the proof by demanding H be a strict subgroup, but it would equally limit the applicability of the theorem.

32a ⟨*Theorem:* $\varphi \in \mathrm{Aut}(G)$ *and* $H \leq G$ *such that* $\varphi(H) = H$ *implies* $\varphi|H \in \mathrm{Aut}(H)$ 32a⟩≡

```
theorem Th22:
  for f being Automorphism of G
  st Image(f|H) = the multMagma of H
  holds f|H is Automorphism of H
proof
  let f be Automorphism of G;
  assume A1: Image(f|H) = the multMagma of H;
  set UH = the carrier of H;
  reconsider fH=f|H as Function of UH,UH by A1,GROUP_6:49;
  A2: fH is bijective
  proof
    thus fH is one-to-one by Lm3;
    UH = rng(f|H) by A1, GROUP_6:44
      .= rng(fH);
    hence fH is onto;
  end;
  for x,y being Element of H holds fH.(x*y) = (fH.x) * (fH.y)
  proof
    let x,y be Element of H;
    fH.(x * y) = (f|H).(x * y)
               .= (f|H).x * (f|H).y by GROUP_6:def 6
               .= fH.x * fH.y by GROUP_2:43;
    hence thesis;
  end;
  hence thesis by A2,GROUP_6:def 6;
end;
```

This code is used in chunk 22.
Defines:
Th22, never used.

Proof sketch (Surjectivity). For reasons I do not adequately understand, I could not simply handle `f|H` as a `Homomorphism of H,H` (despite having established this fact).

I could not use any theorem concerning surjectivity of group morphisms, so I just "forgot" it was a morphism, proved surjectivity, then "remembered" it was a group morphism after all. □

Remark 1.22.2. I am starting to think that the claim `f is onto` is different than `f is onto Homomorphism of G1,G2`.

32b ⟨*Proof:* $\varphi|_H$ *is surjective* 32b⟩≡

```
proof
  set UH = the carrier of H;
  f|H is Function of UH,UH & rng(f|H) = the carrier of H by A1, GROUP_6:44,49;
  hence thesis by A1,GROUP_6:49,FUNCT_2:def 3;
end;
```

Root chunk (not used in this document).

Theorem 1.23. *Let* $H < G$ *be a proper subgroup. Then its image under any automorphism* $\varphi \in \mathrm{Aut}(G)$ *is another proper subgroup* $\varphi(H) < G$.

33a ⟨*Theorem:* $\varphi \in \mathrm{Aut}(G)$ *and* $H < G$ *implies* $\varphi(H) < G$ 33a⟩≡

```
theorem Th23:
  for G being non trivial Group
  for H being Subgroup of G
  for phi being Automorphism of G
  st H is proper Subgroup of G
  holds Image(phi|H) is proper Subgroup of G
proof
  let G be non trivial Group;
  let H be Subgroup of G;
  let phi be Automorphism of G;
  set UH = the carrier of H;
  set UG = the carrier of G;
  A1: phi is one-to-one & phi is onto & UH is non empty Subset of UG &
      phi is Function of UG,UG by GROUP_2:def 5;
  assume H is proper Subgroup of G;
  then UG \ UH is non empty by Th11;
  then consider x such that
  A2: x in UG \ UH by XBOOLE_0:def 1;
  A3: x in G & not x in H by A2,XBOOLE_0:def 5;
  A4: ⟨φ(x) ∉ φ(H) 33b⟩
  ⟨φ(x) ∈ G 33c⟩
  then phi .: H is proper by A4;
  hence Image(phi|H) is proper Subgroup of G by GRSOLV_1:def 3;
end;
```

This code is used in chunk 22.
Defines:
Th23, never used.

Proof step ($\varphi(x) \notin \varphi(H)$)*.* Since $x \in G$ and $x \notin H$, it follows that $\varphi(x) \notin \varphi(H)$ thanks to Theorem 1.5. We also need an extra step since φ is considered first as a function on the underlying set $U(H)$ of H, then we need to remember that this is the same as φ applied to the subgroup H. □

33b ⟨$\varphi(x) \notin \varphi(H)$ 33b⟩≡

```
not (phi.x in phi .: H)
proof
  not (phi.x in (phi .: UH)) by A1, A3, Th5;
  hence not (phi.x in (phi .: H)) by GRSOLV_1:8;
end;
```

This code is used in chunk 33a.

Proof step ($\varphi(x) \in G$)*.* We need to make explicit that $\varphi(x)$ is not just "some object", but an element of the group G. This follows from the fact $\varphi(x)$ is in the range of φ by definition of the range of a function (i.e., [FUNCT_1:def3]). Since φ is an automorphism, in particular surjective, it follows that the set underlying $\varphi(G)$ is the set underlying G, i.e., $U(G)$. Then $\varphi(x) \in G$. □

33c ⟨$\varphi(x) \in G$ 33c⟩≡

```
phi.x is Element of G
proof
  dom phi = UG & rng phi = UG by A1, FUNCT_2:def 1;
  hence phi.x is Element of G by A2, FUNCT_1:def 3;
```

```
end;
```

This code is used in chunk 33a.

Theorem 1.24. *Let G be a group, $\varphi \in \mathrm{Aut}(G)$ an arbitrary automorphism. If $H < G$ is a maximal subgroup, then $\varphi(H) < G$ is also maximal.*

Proof outline. Since $H < G$ is maximal, if $\varphi(H)$ were not maximal, there would be a subgroup $K < G$ such that $\varphi(H) < K$. In that case, $\varphi^{-1}(K) = L$ would be a proper subgroup which contains H as a proper subgroup, which is impossible. Thus $\varphi(H)$ must be maximal. □

34a ⟨*Theorem: Automorphisms map maximal subgroups to maximal subgroups* 34a⟩≡

```
theorem Th24:
  for G being non trivial Group
  for H being strict Subgroup of G
  for phi being Automorphism of G
  st H is maximal
  holds Image(phi|H) is maximal
proof
  let G be non trivial Group;
  let H be strict Subgroup of G;
  let phi be Automorphism of G;
  assume A1: H is maximal;
  A2: Image(phi|H) is proper Subgroup of G by A1,Th23;
  then P1: Image(phi|H) <> the multMagma of G by Def1;
  set UG = the carrier of G;
  set UH = the carrier of H;
  P2: for K being strict Subgroup of G
  st Image(phi|H) <> K & Image(phi|H) is Subgroup of K
  holds K = the multMagma of G
  ⟨Proof: H is maximal implies K = G 34b⟩
  thus Image(phi|H) is maximal by P1,P2,GROUP_4:def 6;
end;
```

This code is used in chunk 22.
Defines:
`Th24`, never used.

Sub-proof outline (H is maximal implies $K = G$). Let K be an arbitrary subgroup of G such that $\varphi(H) < K$. We can consider $\psi \in \mathrm{Aut}(G)$ defined by $\psi(x) = \varphi^{-1}(x)$ for all $x \in G$. Since $H < K < G$, we can find some $k \in K$ but $k \notin K$. Then $\psi(k) \in \psi(K)$. Since H is maximal, $\varphi(\psi(K)) = G$. But also $\varphi(\psi(K)) = K$. Hence $K = G$. □

34b ⟨*Proof: H is maximal implies $K = G$* 34b⟩≡

```
proof
  let K be strict Subgroup of G;
  assume B1: Image(phi|H) <> K;
  assume B2: Image(phi|H) is Subgroup of K;
  then consider psi being Automorphism of G such that
  B3: psi = phi" and
  B4: H is Subgroup of Image(psi|K)
  by Th18;
  set UK = the carrier of K;
```

```
  reconsider K as non trivial strict Subgroup of G by A2,B1,B2,Th12;
  UK \ (the carrier of Image(phi|H)) is non empty by B1,B2,Def1,Th11;
  then consider k being object such that
  B6: k in UK \ (the carrier of Image(phi|H))
  by XBOOLE_0:def 1;
  reconsider k as Element of K by B6;
  set L = Image(psi|K);
  B8: psi.k in L
  ⟨Proof: ψ(k) ∈ L 35a⟩
  B9: the multMagma of H <> L
  ⟨Proof: H ≠ L 35b⟩
  B10: Image(phi|L) = the multMagma of G
  ⟨Proof: φ(L) = G 36a⟩
  Image(phi|L) = K
  ⟨Proof: φ(L) = K 36b⟩
  hence thesis by B10;
end;
```

This code is used in chunk 34a.

Proof step ($\psi(k) \in L$). Since $k \in K$ and $L = \psi(K)$, the result follows from unfolding definitions. □

35a ⟨*Proof:* $\psi(k) \in L$ 35a⟩≡

```
proof
  C1: k in G by GROUP_2:41;
  consider l being object such that
  C2: l = psi.k;
  dom psi = the carrier of G by FUNCT_2:def 1;
  then l in psi .: (the carrier of K) by C1,C2,FUNCT_1:def 6;
  then l in the carrier of (psi .: K) by GRSOLV_1:8;
  hence psi.k in Image(psi|K) by C2,GRSOLV_1:def 3;
end;
```

This code is used in chunk 34b.

Proof step ($H \neq L$). Since $k \in K \setminus \varphi(H)$, it follows $\psi(k) \in \psi(K) \setminus H$. □

35b ⟨*Proof:* $H \neq L$ 35b⟩≡

```
proof
  set UPH = the carrier of Image(phi|H);
  C1: phi is one-to-one & phi is onto & UPH is non empty Subset of UG &
  phi is Function of UG,UG by GROUP_2:def 5;
  C2: k in G & not k in Image(phi|H) by B6, XBOOLE_0:def 5, GROUP_2:41;
  consider phi2 being Automorphism of G such that
  C3: phi2 = psi" and
  C4: Image(psi|Image(phi2|H)) = the multMagma of H
  by Th17;
  C5: phi2=phi by C3,B3, Th3;
  set UPH = the carrier of Image(phi|H);
  psi .: UPH = the carrier of (psi .: Image(phi|H)) by GRSOLV_1:8
            .= the carrier of Image(psi|Image(phi|H)) by GRSOLV_1:def 3;
  hence thesis by B8,C1,C2,C4,C5,Th5;
end;
```

This code is used in chunk 34b.

Proof step ($\varphi(L) = G$). Since $H \neq L$, and H is maximal, it follows that $L = G$. Then $\varphi(L) = \varphi(G)$ and $\varphi(G) = G$ gives the result. □

36a ⟨*Proof:* $\varphi(L) = G$ 36a⟩≡

```
proof
  L = the multMagma of G by A1,B4,B9,GROUP_4:def 6;
  then phi .: the carrier of L = phi .: UG
                               .= rng phi by RELSET_1:22
                               .= UG by FUNCT_2:def 3;
  then UG = phi .: (the carrier of L)
         .= the carrier of (phi .: L) by GRSOLV_1:8
         .= the carrier of Image(phi|L) by GRSOLV_1:def 3;
  hence thesis by GROUP_2:61;
end;
```

This code is used in chunk 34b.

Proof step ($\varphi(L) = K$). From $L = \psi(K)$, it follows $\varphi(L) = K$. □

36b ⟨*Proof:* $\varphi(L) = K$ 36b⟩≡

```
proof
  consider psi2 being Automorphism of G such that
  C1: psi2 = phi" and
  C2: Image(phi|Image(psi2|K)) = the multMagma of K
  by Th17;
  thus Image(phi|Image(psi|K)) = K by B3,C1,C2;
end;
```

This code is used in chunk 34b.

7. Inner Automorphisms

We can now organize our treatment of inner automorphisms.

36c ⟨*Inner Automorphisms* 36c⟩≡

⟨*Definition:* `inner` *for Automorphism* 37a⟩

⟨*Theorem:* `id G` *is effectively inner* 38a⟩

⟨*Register* `inner` *for* `Automorphism` 38b⟩

⟨*Theorem: Relate* `Automorphism of G` *to elements of* `Aut G` 38d⟩

⟨*Theorem:* f *in* `InnAut G` *iff* f *is* `inner Automorphism of G` 39b⟩

⟨*Theorem: inner automorphism acting on subgroup is conjugate of argument* 41a⟩

⟨*Theorem: Kernel of conjugation as endomorphism* 42b⟩

⟨*Theorem: Conjugation by fixed element is an automorphism* 43b⟩

⟨*Corollary: conjugation of given element is an* inner *automorphism* 45a⟩

⟨*Theorem: constructing inner automorphisms from group elements* 45b⟩

⟨*Theorem: inner Automorphisms fix only normal Subgroups* 46a⟩

This code is used in chunk 8b.

Definition 1.2. We call a group automorphism $f \in \mathrm{Aut}(G)$ **"inner"** if there is a group element $g \in G$ such that for all $x \in G$ we have $f(x) = x^g = g^{-1}xg$. That is, f is just conjugation by a fixed group element.

Remark 1.2.1 (Notation: $\mathrm{Inn}(G)$). We denote the set of inner automorphisms of G by $\mathrm{Inn}(G)$ and informally we know $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$. (We will prove $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$ later, I think.)

37a ⟨*Definition:* `inner` *for Automorphism* 37a⟩≡
```
definition
  let G;
  let IT be Automorphism of G;
  attr IT is inner means
  :Def2:
  ex a being Element of G st
  for x being Element of G holds IT.x = x |^ a;
end;
```
⟨*Outer as antonym of inner* 37b⟩

This code is used in chunk 36c.
Defines:
`Def2`, never used.
`inner`, never used.

Notation 1.17. We also recall that an automorphism is called **"Outer"** if it is not inner.

Mizar let's us do this with the `antonym` construct within a `notation` block.

37b ⟨*Outer as antonym of inner* 37b⟩≡
```
notation
  let G be Group, f be Automorphism of G;
  antonym f is outer for f is inner;
end;
```
This code is used in chunk 37a.
Defines:
`outer`, never used.

Vocabulary 1.18. Before rushing off to prove properties concerning inner and outer automorphisms, we should add the attributes to our vocabulary file.

37c ⟨*DICT/GROUP-22.VOC* 2b⟩+≡
```
Vinner
Vouter
```

Theorem 1.25 (Id_G is effectively inner)**.** *The identity endomorphism* Id_G *is an inner automorphism of* G*.*

We will be registering "inner" as an attribute for "Automorphism of G". This will require proving that there exists an inner Automorphism of G. I've found the trivial examples are often best for establishing the existence of such things, so we will prove `id the carrier of G` is an inner Automorphism. This uses the

fact, if $e \in G$ is the identity element, then for any $g \in G$ we have conjugation $g^e = e^{-1}ge = g$ (proven in Theorem [GROUP_3:Th19]).

38a ⟨*Theorem:* `id G` *is effectively inner* 38a⟩≡
```
theorem Th25:
  for x being Element of G holds (id the carrier of G).x = x |^ 1_G
  by GROUP_3:19;
```
This code is used in chunk 36c.
Defines:
`Th25`, never used.

Registration 1.19. Now registering `inner` for `Automorphism`.

38b ⟨*Register* `inner` *for* `Automorphism` 38b⟩≡
```
registration
  let G;
  cluster inner for Automorphism of G;
  existence
  ⟨Proof of existence of an inner Automorphism 38c⟩
end;
```
This code is used in chunk 36c.

Proof sketch (Existence of inner automorphism). The proof is a two punch knock-out. We take `id the carrier of G` to be the morphism, `1_g` the group's identity element to be the element `id the carrier of G` conjugates by, then from earlier (Theorem 1.25) we have `id the carrier of G` be inner. □

38c ⟨*Proof of existence of an inner Automorphism* 38c⟩≡
```
proof
  reconsider i = id (the carrier of G) as Automorphism of G by GROUP_6:38;
  take i;
  take 1_G;
  thus thesis by Th25;
end;
```
This code is used in chunk 38b.

Theorem 1.26 ($\varphi \in \mathrm{Aut}(G) \iff \varphi$ is `Automorphism of G`)**.** *For any φ, we have $\varphi \in \mathrm{Aut}(G)$ if and only if $\varphi\colon G \to G$ is an automorphism.*

Remark 1.26.1. Mizar has [AUTGROUP], an article which defines `Aut G` the collection of functions on the underlying set $U(G)$ of a group G. We can prove that $f \in \mathrm{Aut}(G)$ if and only if f is `Automorphism of G`.

Proof outline. Like any "iff" statement, we have two steps to this proof:

Step 1: $\varphi \in \mathrm{Aut}(g) \implies \varphi\colon G \to G$ is an Automorphism. This is involved and requires carving out a sub-proof.

Step 2: $\varphi \in \mathrm{Aut}(g) \impliedby \varphi\colon G \to G$ is an Automorphism. This follows from how $\mathrm{Aut}(G)$ is defined in `AUTGROUP:def 1`. □

38d ⟨*Theorem: Relate* `Automorphism of G` *to elements of* `Aut G` 38d⟩≡
```
theorem Th26:
  for G being strict Group, f being object
  holds (f in Aut G) iff (f is Automorphism of G)
proof
```

```
  let G be strict Group;
  let f be object;
  thus f in Aut G implies f is Automorphism of G
  ⟨Proof f ∈ Aut(G) ⟹ f is Automorphism of G 39a⟩
  thus f is Automorphism of G implies f in Aut G by AUTGROUP:def 1;
  thus thesis;
end;
```

This code is used in chunk 36c.
Defines:
Th26, never used.

Sub-proof (⟹). The forward direction is straightforward. The only subtlety is, since we didn't assume anything about φ, we should establish it's an endomorphism of G along the way. Then its membership in $\mathrm{Aut}(G)$ implies φ is bijective, and the result follows. □

39a ⟨*Proof* $f \in \mathrm{Aut}(G) \implies f$ *is* `Automorphism of G` 39a⟩≡

```
proof
  assume A1: f in Aut G;
  then reconsider f as Endomorphism of G by AUTGROUP:def 1;
  f is bijective by A1,AUTGROUP:def 1;
  hence thesis;
end;
```

This code is used in chunk 38d.

Theorem 1.27. *We have $\varphi \in \mathrm{Inn}\,\mathrm{Aut}(G)$ if and only if φ is an inner Automorphism of G.*

Proof outline. We have two steps to our proof.

Step 1: $\varphi \in \mathrm{Inn}\,\mathrm{Aut}(G)$ (in the sense of Definition [AutGroup:def4]) imply φ is an inner automorphism of G.

Step 2: φ is an inner automorphism of G implies $\varphi \in \mathrm{Inn}\,\mathrm{Aut}(G)$.

Then the result follows. □

Remark 1.27.1. We can relate the notion of an `inner Automorphism of G` with elements of `InnAut G` from [AutGroup]. The only peculiarity is that [AutGroup] requires G to be a *strict* group.

39b ⟨*Theorem: f in* `InnAut G` *iff f is* `inner Automorphism of G` 39b⟩≡
⟨*Lemma: Elements of* `InnAut G` *are automorphisms* 40c⟩

```
theorem Th27:
  for G being strict Group
  for f being object
  holds (f in InnAut G) iff (f is inner Automorphism of G)
proof
  let G be strict Group;
  let f be object;
  A1: f is Automorphism of G implies
      f is Element of Funcs (the carrier of G, the carrier of G) by FUNCT_2:9;
  thus (f in InnAut G) implies (f is inner Automorphism of G)
  ⟨Proof f is in InnAut G ⟹ (f is inner automorphism) 40a⟩
  thus (f is inner Automorphism of G) implies (f in InnAut G)
```

```
⟨Proof (f is inner automorphism) ⟹ f is in InnAut G 40b⟩
thus thesis;
end;
```

This code is used in chunk 36c.
Defines:
Th27, never used.

Proof step ($\varphi \in \operatorname{Inn}\operatorname{Aut}(G) \implies \varphi$ is inner). The proof amounts to unwinding definitions, but the subtlety is in first reconsidering φ as an Automorphism of G thanks to our handy-dandy lemma. □

40a ⟨*Proof f is in* `InnAut G` ⟹ *(f is inner automorphism)* 40a⟩≡

```
proof
  assume B1: f in InnAut G;
  then reconsider f as Automorphism of G by Lm6;
  consider a being Element of G such that
  B2: for x being Element of G holds f.x = x |^ a
  by A1,B1,AUTGROUP:def 4;
  thus thesis by Def2,B2;
end;
```

This code is used in chunk 39b.

Proof step (φ is inner $\implies \varphi \in \operatorname{Inn}\operatorname{Aut}(G)$). This is again unwinding the definitions. The same subtlety lurks here, requiring us to reconsider f as an inner automorphism of G. □

40b ⟨*Proof (f is inner automorphism)* ⟹ *f is in* `InnAut G` 40b⟩≡

```
proof
  assume f is inner Automorphism of G;
  then reconsider f as inner Automorphism of G;
  consider a being Element of G such that
  B1: for x being Element of G holds f.x = x |^ a
  by Def2;
  thus thesis by A1,B1,AUTGROUP:def 4;
end;
```

This code is used in chunk 39b.

Lemma 1.5. *Any member of the group* $\operatorname{Inn}\operatorname{Aut}(G)$ *is an Automorphism of* G.

It's relatively straightforward to show that if f is an element of `InnAut G`, then f is an `Automorphism of G`. We just unwind the definitions.

40c ⟨*Lemma: Elements of* `InnAut G` *are automorphisms* 40c⟩≡

```
Lm6:
  for G being strict Group
  for f being Element of InnAut G
  holds f is Automorphism of G
proof
  let G be strict Group;
  let f be Element of InnAut G;
  f is Element of Aut G by AUTGROUP:12;
  hence f is Automorphism of G by Th26;
end;
```

This code is used in chunk 39b.

Defines:
Lm6, never used.

Theorem 1.28. *Given any element $a \in G$, and any inner automorphism φ of G such that $\forall x \in G, f(x) = x^a = a^{-1}xa$, it follows that the image of a subgroup under f is the conjugate of that subgroup $\varphi(H) = H^a$.*

Proof. Let $\varphi \in \mathrm{End}(G)$ be defined by hypothesis as $\varphi(x) = x^a$ for some fixed $a \in G$. We have $\varphi|_H(h) = h^a$ for any $h \in H$. We show $y \in \varphi|_H(H) \iff y \in H^a$ in two sub-proofs. Then it follows that $\varphi(H) = H^a$ by Definition [GROUP_2:def6]. □

41a ⟨*Theorem: inner automorphism acting on subgroup is conjugate of argument* 41a⟩≡

```
theorem Th28:
  for a being Element of G
  for f being inner Automorphism of G
  st (for x being Element of G holds f.x = x |^ a)
  holds Image(f|H) = H |^ a
proof
  let a be Element of G,
      f be inner Automorphism of G;
  assume
A1: for x being Element of G holds f.x = x |^ a;
A2: for h being Element of G st h in H holds (f|H).h = h |^ a
  proof
    let h be Element of G;
    assume h in H;
    hence (f|H).h = f.h by Th1
                 .= h |^ a by A1;
  end;

A3: for y being Element of G st y in Image(f|H) holds y in H |^ a
  ⟨Proof ∀y ∈ G, y ∈ f(H) ⟹ y ∈ H^a 41b⟩
  for y being Element of G st y in H |^ a holds y in Image(f|H)
  ⟨Proof ∀y ∈ G, y ∈ f(H) ⟸ y ∈ H^a 42a⟩
  hence (H |^ a) = Image(f|H) by A3;
end;
```

This code is used in chunk 36c.
Defines:
Th28, never used.

Proof step 1 ($\forall y \in G, y \in f(H) \implies y \in H^a$). The forward direction amounts to unwrapping the definition of $f(h) = h^a$. Since $h \in H$, it follows $h^a \in H^a$ by Theorem [GROUP_3:Th58]. □

41b ⟨*Proof* $\forall y \in G, y \in f(H) \implies y \in H^a$ 41b⟩≡

```
proof
  let y be Element of G;
  assume y in Image(f|H);
  then consider h being Element of H such that
  B1: (f|H).h = y by GROUP_6:45;
  reconsider h as Element of G by GROUP_2:42;
  B2: h in H;
  then h |^ a = (f|H).h by A2
             .= y by B1;
```

```
    hence y in H |^ a by B2,GROUP_3:58;
  end;
```

This code is used in chunk 41a.

Proof step 2 ($\forall y \in G, y \in f(H) \iff y \in H^a$). The proof in the backwards direction begins with $y \in H^a$ must look like $y = g^a$ for some $g \in H$ by Theorem [GROUP_3:Th58], and showing $y = f(g)$, which amounts to "plug it in". □

42a ⟨*Proof* $\forall y \in G, y \in f(H) \iff y \in H^a$ 42a⟩≡

```
  proof
    let y be Element of G;
    assume y in H |^ a;
    then consider g being Element of G such that
    B1:    y=g|^a and
    B2:    g in H
    by GROUP_3:58;

    B3: (f|H).g = f.g by Th1,B2
              .= g |^ a by A1
              .= y by B1;
    thus y in Image(f|H) by B2,B3,GROUP_6:45;
  end;
```

This code is used in chunk 41a.

Theorem 1.29 (Kernel of inner automorphism is trivial)**.** *Let G be a group, $\varphi \in \mathrm{End}(G)$ be defined by $\forall x \in G, \varphi(x) = x^a$ for some fixed $a \in G$. Then $\ker(\varphi) = \mathbf{1}_G$.*

We are proving something a little more general, namely, any endomorphism $f\colon G \to G$ defined by $f(x) = x^a$ (for some fixed $a \in G$) will have a trivial kernel.

Proof outline. If $\varphi \in \mathrm{End}(G)$ is defined as $\forall x \in G, \varphi(x) = x^a$ for some fixed $a \in G$, then we will prove $\ker(\varphi) \leq \mathbf{1}_G$. We know from Theorem [GROUP_2:Th65] that $\mathbf{1}_G \leq \ker(\varphi)$. Since one is subgroup of the other (and vice-versa), we know from Theorem [GROUP_2:Th55] they must be equal as subgroups. □

42b ⟨*Theorem: Kernel of conjugation as endomorphism* 42b⟩≡

```
  theorem Th29:
    for a being Element of G
    for f being Endomorphism of G
    st (for x being Element of G holds f.x = x |^ a)
    holds Ker f = (1).G
  proof
    let a be Element of G;
    let f be Endomorphism of G;
    assume A1: for x being Element of G holds f.x = x |^ a;
    for x being Element of G holds x in Ker f implies x in (1).G
    ⟨Proof ker(f) ⊆ 1 43a⟩
    then A2: Ker f is Subgroup of (1).G by GROUP_2:58;

    A3: (1).G is Subgroup of Ker f by GROUP_2:65;
    thus Ker f = (1).G by A2,A3,GROUP_2:55;
  end;
```

This code is used in chunk 36c.

Defines:
Th29, never used.

Sub-proof ($\ker(f) \subseteq \mathbf{1}$*).* Let $x \in \ker(f)$ be arbitrary, then $f(x) = 1_G$. But this means $x = 1_G$ (according to Theorem [GROUP_3:Th18]). Thus $x \in \mathbf{1}_G$ by definition of the trivial subgroup. □

43a ⟨*Proof* $\ker(f) \subseteq \mathbf{1}$ 43a⟩≡
```
proof
  let x be Element of G;
  assume x in Ker f;
  then 1_G = f.x by GROUP_6:41
          .= x |^ a by A1;
  then x = 1_G by GROUP_3:18;
  hence x in (1).G by GROUP_2:46;
end;
```
This code is used in chunk 42b.

Theorem 1.30 (Conjugation by fixed element is an automorphism)**.** *Let G be a group, $a \in G$ a fixed element. The endomorphism $\varphi\colon G \to G$ defined by $\varphi(x) = x^a$ is, in fact, an automorphism of G.*

Proof outline. We establish φ is injective because it has a trivial kernel (thanks to Theorem 1.29 and Theorem [GROUP_6:Th56]). We then prove $\psi \in \mathrm{End}(G)$ exists such that $\varphi \circ \psi = \mathrm{id}_G$. The existence of such a ψ implies $\mathrm{rng}(\varphi) = G$, which implies φ is surjective. We then have φ, being both injective and surjective, is bijective and moreover an automorphism. □

43b ⟨*Theorem: Conjugation by fixed element is an automorphism* 43b⟩≡
```
theorem Th30:
  for a being Element of G
  for f being Endomorphism of G
  st (for x being Element of G holds f.x = x |^ a)
  holds f is Automorphism of G
proof
  let a be Element of G;
  let f be Endomorphism of G;
  assume A1: for x being Element of G holds f.x = x |^ a;
  then Ker f = (1).G by Th29;
  then A2: f is one-to-one by GROUP_6:56;
  ex fInv being Endomorphism of G st f*fInv = id (the carrier of G)
  ⟨Proof an endomorphism f^-1 exists 44a⟩

  then f is onto by FUNCT_2:18;
  hence f is Automorphism of G by A2;
end;
```
This code is used in chunk 36c.
Defines:
Th30, never used.

Sub-proof (Existence of inverse of conjugation). This is the long part of the proof, its length owing to showing every detail. We can construct $\psi(x) = x^{a^{-1}}$ as a function of the underlying set of the group. We just need to prove this is an

endomorphism (suffices to prove it respects the group binary operation), and that ψ is the inverse function of φ. □

44a ⟨*Proof an endomorphism* f^{-1} *exists* 44a⟩≡
```
proof
  deffunc F(Element of G) = ($1) |^ a";
  consider fInv be Function of the carrier of G, the carrier of G such that
  A3: for g being Element of G holds fInv.g = F(g) from FUNCT_2:sch 4;
  ⟨Establish f^-1 is an Endomorphism 44c⟩
  ⟨Establish f^-1 is the inverse function of f 44b⟩
  hence thesis;
end;
```
This code is used in chunk 43b.

Sub-proof (ψ *is inverse function of* φ*).* The proof is straightforward, simply compose the functions together and show we get the identity function. We just have to unwind a lot of definitions. □

44b ⟨*Establish* f^{-1} *is the inverse function of* f 44b⟩≡
```
for x being Element of G holds (f*fInv).x = (id the carrier of G).x
proof
  let x be Element of G;
  (f * fInv).x = f.(fInv.x) by FUNCT_2:15
              .= f.(x |^ a") by A3
              .= (x |^ a") |^ a by A1
              .= x |^ (a" * a) by GROUP_3:24
              .= x |^ 1_G by GROUP_1:def 5
              .= x by GROUP_3:19
              .= (id the carrier of G).x;
  hence thesis;
end;
then f*fInv = id the carrier of G;
```
This code is used in chunk 44a.

Sub-proof (ψ *is an endomorphism).* We need to show $\psi(x_1x_2) = \psi(x_1)\psi(x_2)$, which follows from the results of conjugation from the article [GROUP_3]. □

44c ⟨*Establish* f^{-1} *is an Endomorphism* 44c⟩≡
```
for x1,x2 being Element of G holds fInv.(x1 * x2) = fInv.x1 * fInv.x2
proof
  let x1,x2 be Element of G;
  A4: fInv.x1 = x1 |^ a" & fInv.x2 = x2 |^ a" by A3;
  fInv.(x1 * x2) = (x1 * x2) |^ a" by A3
                .= (x1 |^ a") * (x2 |^ a") by GROUP_3:23
                .= fInv.x1 * fInv.x2 by A4;
  hence thesis;
end;
then reconsider fInv as Endomorphism of G by GROUP_6:def 6;
```
This code is used in chunk 44a.

Corollary 1.31. *Given a group element $a \in G$, we can always construct an inner automorphism $f \in \mathrm{Inn}(G)$ defined by $\forall x \in G, f(x) = x^a = a^{-1}xa$ conjugation by a.*

Proof. We have shown in Theorem 1.30 that conjugation is an automorphism, and by definition it is inner. □

45a ⟨*Corollary: conjugation of given element is an* inner *automorphism* 45a⟩≡

```
theorem Th31:
  for a being Element of G
  for f being Endomorphism of G
  st (for x being Element of G holds f.x = x |^ a)
  holds f is inner Automorphism of G by Th30,Def2;
```

This code is used in chunk 36c.
Defines:
`Th31`, never used.

Theorem 1.32 (Constructing inner automorphisms)**.** *Let $a \in G$ be a group element. Then there exists an inner automorphism $\varphi \in \mathrm{Inn}(G)$ such that for any $x \in G$ we have $\varphi(x) = x^a$.*

Proof. We can show that, for any $a \in G$, we can construct a function of the underlying set of G to itself $\varphi\colon G \to G$ defined by $\forall x \in G, \varphi(x) = x^a$. We have to show this is an endomorphism, i.e., for any $x_1, x_2 \in G$ that $\varphi(x_1x_2) = \varphi(x_1)\varphi(x_2)$. The result follows thanks to Corollary 1.31. □

Remark 1.32.1 (Motivation). Given a group G and suppose we have an element $a \in G$, can we construct an inner automorphism $f \in \mathrm{Inn}(G)$ such that $\forall x \in G, f(x) = x^a$? Yes, we can do it! A wiser way to organize these results may be to first show such an f is an Endomorphism and it exists, then use that result in the proof that it's an automorphism, and so on.

45b ⟨*Theorem: constructing inner automorphisms from group elements* 45b⟩≡

```
theorem Th32:
  for a being Element of G
  holds ex f being inner Automorphism of G st (for x being Element of G
  holds f.x = x |^ a)
proof
  let a be Element of G;
  deffunc F(Element of G) = ($1) |^ a;
  consider f be Function of the carrier of G, the carrier of G such that
A1: for g being Element of G holds f.g = F(g) from FUNCT_2:sch 4;
  for x1,x2 being Element of G holds f.(x1 * x2) = f.x1 * f.x2
  proof
    let x1,x2 be Element of G;
    A2: f.x1 = x1 |^ a & f.x2 = x2 |^ a by A1;
    f.(x1 * x2) = (x1 * x2) |^ a by A1
              .= (x1 |^ a) * (x2 |^ a) by GROUP_3:23
              .= f.x1 * f.x2 by A2;
    hence thesis;
  end;
  then reconsider f as Endomorphism of G by GROUP_6:def 6;
  for x being Element of G holds f.x = x |^ a & f is inner Automorphism of G
  by A1,Th31;
  hence thesis;
```

```
  end;
```

This code is used in chunk 36c.
Defines:
  Th32, never used.

Theorem 1.33. *Let $H \leq G$ be an arbitrary subgroup. Then $\forall \varphi \in \text{Inn}(G), \varphi(H) = H$ if and only if $H \trianglelefteq G$.*

Remark 1.33.1. This is another, "Well, I guess Mizar should have this, but I can't find it, so here we go!"-type proof. The only quirk is the use of `strict Subgroup`, which is necessary because otherwise `H |^ a` is strictly speaking a `multMagma`, not a subgroup. And to assert two subgroups are equal, we need a `strict` subgroup, which requires adding a `strict` hypothesis.

Remark 1.33.2 (On `strict` hypothesis). The `strict` condition is necessary to prove $H \trianglelefteq G$ implies $\forall \varphi \in \text{Inn}(G), \varphi(H) = H$. Otherwise, we end up with the slightly peculiar situation where $\varphi(H) =$ `the multMagma of` H, which isn't terrible, but requires additional steps later on in proving "$K \leq N$ is characteristic and $N \trianglelefteq G$ is `strict` normal implies $K \trianglelefteq G$."

46a ⟨*Theorem: inner Automorphisms fix only normal Subgroups* 46a⟩≡

```
theorem Th33:
  for H being strict Subgroup of G
  holds (H is normal) iff (for f being inner Automorphism of G
                             holds Image(f|H)=H)
proof
  let H be strict Subgroup of G;
  A1: (H is normal) implies (for f being inner Automorphism of G
                               holds Image(f|H)=H)
  ⟨Proof: normal implies fixed by inner automorphisms 46b⟩
  A2: not ((for f being inner Automorphism of G holds Image(f|H)=H)
           implies H is normal)
  implies contradiction
  ⟨Proof by contradiction: fixed by inner automorphisms implies normal 47a⟩
  thus thesis by A1,A2;
end;
```

This code is used in chunk 36c.
Defines:
  Th33, never used.

Sub-proof (normal implies fixed by inner automorphisms). Assume $H \trianglelefteq G$ is a normal subgroup. Let $\varphi \in \text{Inn}(G)$ be an arbitrary inner automorphism. We have $\varphi(x) = x^a$ for some fixed $a \in G$ and for any $x \in G$. Then $\varphi(H) = H^a$ by Theorem 1.28 and $H^a = H$ by Definition [GROUP_3:def13] and definition of equality for subgroups [GROUP_2:def6]. Thus the result. □

46b ⟨*Proof: normal implies fixed by inner automorphisms* 46b⟩≡

```
proof
  assume B1: H is normal;
  let f be inner Automorphism of G;
  consider a being Element of G such that
  B2: for x being Element of G holds f.x = x |^ a
  by Def2;
```

```
    Image(f|H) = H |^ a by B2,Th28
              .= the multMagma of H by B1,GROUP_3:def 13
              .= H;
    hence Image(f|H)=H;
  end;
```

This code is used in chunk 46a.

Sub-proof (fixed by inner automorphisms implies normal). We prove by contradiction, assuming $\forall \varphi \in \mathrm{Inn}(G)$ that $\varphi(H) = H$ but assuming for contradiction that H is not a normal subgroup. We run into the situation where $\varphi(H) = H^a = H$. But a subgroup is normal if and only if $H^a = H$. Thus the contradiction. □

Remark 1.33.3 (Proof by contradiction in Mizar). Mizar's proof by contradiction is rather curious. If we want to prove $P \implies Q$ by contradiction, we assert $\neg(P \implies Q) \implies \bot$. The proof we offer is about as satisfying as any other proof by contradiction.

47a ⟨*Proof by contradiction: fixed by inner automorphisms implies normal* 47a⟩≡

```
  proof
    assume B1: for f being inner Automorphism of G holds Image(f|H)=H;
    assume not H is normal;
    then consider a being Element of G such that
    B2: H |^ a <> the multMagma of H
    by GROUP_3:def 13;
    consider f being inner Automorphism of G such that
    B3: (for x being Element of G holds f.x= x |^ a)
    by Th32;
    Image(f|H) = H |^ a by B3, Th28;
    hence contradiction by B1,B2;
  end;
```

This code is used in chunk 46a.

8. Characteristic Subgroups

We now arrive at the meat of the matter: characteristic subgroups!

47b ⟨*Characteristic subgroups* 47b⟩≡

⟨*Definition:* `characteristic` *attribute* 49a⟩

⟨*Lemma: trivial subgroup is* `characteristic` 49c⟩

⟨*Theorem: Existence of characteristic subgroups* 50a⟩

⟨*Register* `characteristic` *as attribute for Subgroup* 50b⟩
⟨*Register* `strict characteristic` *for Subgroups* 50d⟩

⟨*Theorem: characteristic subgroups are normal* 51a⟩

⟨*Register characteristic subgroups are normal* 51c⟩

⟨*Theorem: two group morphisms which coincide on subgroup have the same image* 52a⟩

⟨*Theorem: unique subgroup of order n is* `characteristic` 54a⟩

⟨*Theorem: characteristic subgroup of a normal subgroup is normal* 54b⟩

⟨*Theorem: transitivity of characteristic subgroups* 55b⟩

⟨*Theorem:* $H \leq G$ *is characteristic iff* $\forall \varphi \in \text{Aut}(G), \varphi(H) \leq H$ 56⟩

⟨*Theorem:* $Z(G)$ *is characteristic subgroup* 58a⟩

⟨*Scheme: if* $H \leq G \wedge P[H]$ *and* $\forall \varphi \in \text{Aut}(G), P[\varphi(H)]$*, then* $\bigcap\{H \leq G \mid P[H]\}$ *is* $\text{Aut}(G)$*-invariant* 60⟩

⟨*Scheme:* $\bigcap\{A \subseteq G \mid \exists H \leq G, A = H, P[H]\}$ *is characteristic* 63⟩

⟨*Theorem:* $\Phi(G)$ *is characteristic* 64⟩

⟨*Theorem:* $\forall \varphi \in G, \varphi(\text{Commutators}(G)) = \text{Commutators}(G)$ 65⟩

⟨*Theorem:* $\forall h \in H, \varphi(h) \in H$ *implies* $\varphi(H) \leq H$ 67a⟩

⟨*Theorem:* $A \subseteq G$ *s.t.* $\forall \varphi \in \text{Aut}(G), \varphi(A) = A$*, then* $\langle A \rangle$ *is characteristic* 67b⟩

⟨*Theorem: The derived subgroup is characteristic* 70a⟩

⟨*Theorem:* $H \leq G, a \in G$*,* $\varphi(aH) = \varphi(a)\varphi(H)$ 70b⟩

⟨*Theorem:* $H \leq G, a \in G$*,* $\varphi(Ha) = \varphi(H)\varphi(a)$ 71⟩

⟨*Theorem:* $N \trianglelefteq G$*,* $\varphi \in \text{Aut}(G)$ *implies* $\varphi(N) \trianglelefteq G$ 72⟩

⟨*Theorem:* $H \leq G$ *characteristic* $\iff \forall \varphi \in \text{Aut}(G) \forall x \in H, \varphi(x) \in H$ 73⟩

⟨*Theorem:* $H, K \leq G$ *characteristic implies* $H \cap K$ *characteristic* 74⟩

⟨*Theorem:* $H, K \leq G$ *characteristic implies* $\langle H, K \rangle$ *is characteristic* 75⟩

⟨*Theorem:* $H, K \leq G$ *characteristic implies* $\text{Commutators}(H, K)$ *is stable* 76a⟩

⟨*Theorem:* $H, K \leq G$ *characteristic implies* $[H, K]$ *is characteristic* 77b⟩

This code is used in chunk 8b.

Definition 1.3 (Dummit and Foote [DF04, §4.4])**.** A subgroup H of G is called **"Characteristic"** in G, usually denoted H char G, if every Automorphism of G maps H to itself; i.e., $\sigma(H) = H$ for all $\sigma \in \text{Aut}(G)$.

Remark 1.3.1. The other definition which is routinely given is that H is a characteristic subgroup of G if for any $\varphi \in \text{Aut}(G)$ we have $\varphi(H) \leq H$. We prove this later as equivalent in Theorem 1.40.

Remark 1.3.2. We need to formalize this definition to make the image equal to `the multMagma of IT` because subgroup equality is defined only for strict subgroups. If we tried just using the "obvious" definition, "`Image(f|IT) = IT`", then a neferious Mizar user could obtain inconsistent results by clever means.

49a ⟨*Definition:* `characteristic` *attribute* 49a⟩≡

```
:: Dummit and Foote, Abstract Algebra, ch.4 section 4
definition
  let G;
  let IT be Subgroup of G;
  attr IT is characteristic means
  :Def3:
  for f being Automorphism of G
  holds Image (f|IT) = the multMagma of IT;
end;
```

This code is used in chunk 47b.
Defines:
`characteristic`, never used.
`Def3`, never used.

Vocabulary 1.20. Before rushing off to prove properties concerning characteristic subgroups, we have to tell Mizar that `characteristic` is now a token that should be associated with Definition 1.3.

49b ⟨*DICT/GROUP-22.VOC* 2b⟩+≡

```
Vcharacteristic
```

Lemma 1.6. *For any group G, its trivial subgroup $\mathbf{1}$ is characteristic.*

49c ⟨*Lemma: trivial subgroup is* `characteristic` 49c⟩≡

⟨*Lemma: if $H \leq \mathbf{1}$, then $H = \mathbf{1}$* 49d⟩

```
Lm7: (1).G is characteristic
proof
  for f being Automorphism of G holds Image(f|(1).G) = (1).G
  proof
    let f be Automorphism of G;
    reconsider I = Image(f|(1).G) as Subgroup of (1).G by Th14;
    (1).G = I by Lm8;
    hence Image(f|(1).G) = (1).G;
  end;
  hence (1).G is characteristic;
end;
```

This code is used in chunk 47b.
Defines:
`Lm7`, never used.

Lemma 1.7. *For any subgroup $H \leq G$, if $\mathbf{1}_G \leq H$ and $H \leq \mathbf{1}_G$, then $H = \mathbf{1}_G$.*

Remark 1.7.1. I couldn't quite find this anywhere in the MML, so I had to prove it myself.

Remark 1.7.2 (To do). I think I prove this result several times, I should refactor my code accordingly.

49d ⟨*Lemma: if $H \leq \mathbf{1}$, then $H = \mathbf{1}$* 49d⟩≡

```
Lm8: H is Subgroup of (1).G implies the multMagma of H = the multMagma of (1).G
proof
  assume H is Subgroup of (1).G;
  then reconsider H as Subgroup of (1).G;
```

```
    H is Subgroup of (1).G & (1).G is Subgroup of H by GROUP_2:65;
    hence thesis by GROUP_2:55;
  end;
```

This code is used in chunk 49c.
Defines:
Lm8, never used.

Theorem 1.34 (Existence of a characteristic subgroup)**.** *For any group G, there exists a subgroup $H \leq G$ which is characteristic.*

Proof outline. The trivial subgroup is a subgroup of any group. And it is characteristic. Thus the result. □

50a ⟨*Theorem: Existence of characteristic subgroups* 50a⟩≡

```
theorem Th34:
  ex H st H is characteristic
proof
  take H = (1).G;
  thus H is characteristic by Lm7;
end;
```

This code is used in chunk 47b.
Defines:
Th34, never used.

Registration 1.21. Now we can instruct Mizar to recognize `characteristic` as an adjective of `Subgroup`.

50b ⟨*Register* `characteristic` *as attribute for Subgroup* 50b⟩≡

```
registration
  let G;
  cluster characteristic for Subgroup of G;
  existence by Th34;
end;
```

This definition is continued in chunk 50c.
This code is used in chunk 47b.

Reserve 1.22. We will henceforth use the symbol K to refer to characteristic subgroups of G, unless otherwise stated.

50c ⟨*Register* `characteristic` *as attribute for Subgroup* 50b⟩+≡

```
reserve K for characteristic Subgroup of G;
```

This code is used in chunk 47b.

Registration 1.23. We can also register the cluster `strict characteristic` for Subgroups, which will come handy later.

50d ⟨*Register* `strict characteristic` *for Subgroups* 50d⟩≡

```
registration
  let G be Group;
  cluster strict characteristic for Subgroup of G;
  existence
  proof
    take (1).G;
```

```
      thus thesis by Lm7;
    end;
  end;
```

This code is used in chunk 47b.

Theorem 1.35 (Characteristic subgroups are normal)**.** *Let G be a group, $K \leq G$ a subgroup. If K is a characteristic subgroup of G, then $K \trianglelefteq G$ it is also normal.*

Proof outline. We show K is invariant under conjugation, i.e., for any $a \in G$ we have $K^a = K$. Then $K \trianglelefteq G$. □

51a ⟨*Theorem: characteristic subgroups are normal* 51a⟩≡

```
theorem Th35:
  K is normal Subgroup of G
proof
  for a being Element of G holds K |^ a = the multMagma of K
  ⟨Sub-proof: characteristic subgroups invariant under conjugation 51b⟩
  hence K is normal Subgroup of G by GROUP_3:def 13;
end;
```

This code is used in chunk 47b.
Defines:
Th35, never used.

Sub-proof (characteristic subgroups invariant under conjugation). Really, proving a characteristic subgroup is normal amounts to proving invariance under conjugation. Fortunately, we have established this along the way! We just have to point to our hard work from earlier. □

51b ⟨*Sub-proof: characteristic subgroups invariant under conjugation* 51b⟩≡

```
proof
  let a be Element of G;
  consider f being inner Automorphism of G such that
  A2: for x being Element of G holds f.x = x |^ a
  by Th32;
  the multMagma of K = Image(f|K) by Def3
                    .= K |^ a by A2,Th28;
  hence thesis;
end;
```

This code is used in chunk 51a.

Registration 1.24. Now we can register this fact with Mizar, so it will be automatically accounted for in future proofs. Since we made this fact a proof, we just have to tell Mizar where to find the proof.

51c ⟨*Register characteristic subgroups are normal* 51c⟩≡

```
registration
  let G be Group;
  cluster characteristic -> normal for Subgroup of G;
  coherence by Th35;
end;
```

This code is used in chunk 47b.

Theorem 1.36. *If we have two morphisms $f\colon G_1 \to G_2$ and $g\colon H_1 \to H_2$, where $H_1 \leq G_1$ and $H_2 \leq G_2$, and if we have a common subgroup $K \leq H_1 \leq G_1$, then the image of the morphisms on this shared subgroup should coincide.*

Proof outline. Let $f\colon G_1 \to G_2$ be a group morphism, let $H_1 \leq G_1$ and $H_2 \leq G_2$ be subgroups, let $g\colon H_1 \to H_2$. If $K \leq H_1$ is a subgroup for which $g|_K = f|_K$, then $f(K) = g(K)$. □

Remark 1.36.1. The heavy lifting is done by a straightforward and intuitive result.

Initially, I had a more conservative result: let $\varphi, \psi \in \text{Aut}(G)$ and $H \leq G$, if $\forall h \in H, \varphi(h) = \psi(h)$, then $\varphi(H) = \psi(H)$. Then I realized this didn't describe the situation I was facing, so I revised it to fit. Then I realized I didn't need the hypothesis that φ and ψ were automorphisms, they could be generic morphisms.

52a ⟨*Theorem: two group morphisms which coincide on subgroup have the same image* 52a⟩≡

```
theorem Th36:
  for G1,G2 being Group
  for H1 being Subgroup of G1
  for K being Subgroup of H1
  for H2 being Subgroup of G2
  for f being Homomorphism of G1,G2
  for g being Homomorphism of H1,H2
  st (for k being Element of G1 st k in K holds f.k=g.k)
  holds Image(f|K) = Image(g|K)
proof
  let G1,G2 be Group;
  let H1 be Subgroup of G1;
  let K be Subgroup of H1;
  let H2 be Subgroup of G2;
  let f be Homomorphism of G1,G2;
  let g be Homomorphism of H1,H2;
  assume A1: for k being Element of G1 st k in K holds f.k=g.k;
  A2: Image(f|K) is strict Subgroup of G2 &
      Image(g|K) is strict Subgroup of G2 by GROUP_2:56;
  for y being object
  holds y in the carrier of Image(f|K) iff y in the carrier of Image(g|K)
  ⟨Proof: y ∈ f(K) ⟺ y ∈ g(K) 52b⟩
  hence Image(f|K) = Image(g|K) by A2,GROUP_2:59,TARSKI:2;
end;
```

This code is used in chunk 47b.
Defines:
Th36, never used.

Sub-proof (∀y, y ∈ f(K) ⟺ y ∈ g(K)). We show, for any y, that both $y \in f(K) \implies y \in g(K)$ and $y \in f(K) \impliedby y \in g(K)$. Taken together, this gives us $y \in f(K) \iff y \in g(K)$. □

52b ⟨*Proof: y ∈ f(K) ⟺ y ∈ g(K)* 52b⟩≡

```
proof
  let y be object;
  thus y in the carrier of Image(f|K) implies y in the carrier of Image(g|K)
  ⟨Proof: y ∈ f(K) ⟹ y ∈ g(K) 53a⟩
  thus y in the carrier of Image(g|K) implies y in the carrier of Image(f|K)
  ⟨Proof: y ∈ g(K) ⟹ y ∈ f(K) 53b⟩
```

```
    thus thesis;
  end;
```

This code is used in chunk 52a.

Sub-proof step 1 ($y \in f(K) \implies y \in g(K)$). We have $y \in f(K)$ if there is some $h \in K$ such that $y = f|_K(h)$. But by hypothesis, $f|_K(h) = g|_K(h)$, and thus $y = g|_k(h) \in g(K)$. □

53a ⟨*Proof:* $y \in f(K) \implies y \in g(K)$ 53a⟩≡

```
  proof
    assume y in the carrier of Image(f|K);
    then consider h being Element of K such that
    B1: (f|K).h = y
    by STRUCT_0:def 5,GROUP_6:45;
    B2: h is Element of G1 & h is Element of H1 & h in K by GROUP_2:42;
    f.h = g.h by A1,B2
       .= (g|K).h by B2, Th1;
    then (g|K).h = f.h
                .= (f|K).h by B2,Th1
                .= y by B1;
    hence y in the carrier of Image(g|K) by STRUCT_0:def 5,GROUP_6:45;
  end;
```

This code is used in chunk 52b.

Sub-proof step 2 ($y \in g(K) \implies y \in f(K)$). We have $y \in g(K)$ if there is some $h \in K$ such that $y = g|_K(h)$. But by hypothesis $g|_K(h) = f|_K(h)$, and thus $y = f|_K(h) \in f(K)$. □

53b ⟨*Proof:* $y \in g(K) \implies y \in f(K)$ 53b⟩≡

```
  proof
    assume y in the carrier of Image(g|K);
    then consider h being Element of K such that
    C1: (g|K).h = y
    by STRUCT_0:def 5,GROUP_6:45;
    C2: h is Element of H1 & h is Element of G1 & h in K by GROUP_2:42;
    g.h = f.h by A1,C2
       .= (f|K).h by C2,Th1;
    then (f|K).h = g.h
                .= (g|K).h by C2,Th1
                .= y by C1;
    hence y in the carrier of Image(f|K) by STRUCT_0:def 5,GROUP_6:45;
  end;
```

This code is used in chunk 52b.

Theorem 1.37. *If H is the unique subgroup of a given order in a group G, then H is characteristic in G.*

Proof. Let H be a subgroup of G. Assume there are no other subgroups of order $|H|$. Then for any $\varphi \in \mathrm{Aut}(G)$, we'd have $\varphi(H) = H$ since $\varphi(H)$ has the same order as H by Theorem **??**, but we assumed there is only one (namely, H). □

54a ⟨*Theorem: unique subgroup of order n is* `characteristic` 54a⟩≡

```
theorem Th37:
  for H being strict Subgroup of G
  st (for K being strict Subgroup of G
      st card K = card H
      holds H = K)
  holds H is characteristic
proof
  let H be strict Subgroup of G;
  assume A1: for K being strict Subgroup of G st card K = card H holds H = K;
  H is characteristic
  proof
    let phi be Automorphism of G;
    Image(phi|H) = phi .: H by GRSOLV_1:def 3;
    then card H = card Image(phi|H) by Th19,GROUP_6:73;
    hence Image(phi|H) = the multMagma of H by A1;
  end;
  hence thesis;
end;
```

This code is used in chunk 47b.
Defines:
`Th37`, never used.

Theorem 1.38. *If $K \leq H$ is characteristic, and if $H \trianglelefteq G$ is normal, then $K \trianglelefteq G$ is normal.*

This required a surprising amount of legwork, even when carving it out into a helper theorem! The "architecture" of the proof follows what we would find in a textbook. It's just that a textbook will gloss over facts about morphisms which we'd need to prove.

Proof. Let K be a characteristic subgroup of N and $N \trianglelefteq G$ be a normal subgroup. Then consider conjugation of N by any element $a \in G$. This corresponds to an inner Automorphism of G, $\varphi \in \text{Inn}(G)$, and an automorphism $\varphi|_N \in \text{Aut}(N)$ of N. But since K is characteristic in N, it follows $\varphi|_N(K) = K$. Then K, considered as a subgroup of G, must be invariant under φ and therefore a normal subgroup of G by Theorem 1.2. □

Remark 1.38.1. The `strict` hypothesis on `N` is necessary, since Definition [GROUP_2:def6] defines equality only on *strict* subgroups.

54b ⟨*Theorem: characteristic subgroup of a normal subgroup is normal* 54b⟩≡

```
theorem Th38:
  for N being strict normal Subgroup of G
  for K being characteristic Subgroup of N
  holds K is normal Subgroup of G
proof
  let N be strict normal Subgroup of G;
  let K be characteristic Subgroup of N;
  for a being Element of G holds K |^ a = the multMagma of K
  ⟨Proof: ∀a ∈ G, K^a = K 55a⟩
  hence K is normal Subgroup of G by Th2;
end;
```

This code is used in chunk 47b.
Defines:
Th38, never used.

Sub-proof ($\forall a \in G, K^a = K$). Given an arbitrary $a \in G$, we construct an inner automorphism $\varphi \in \mathrm{Inn}(G)$ defined by $\varphi(x) = x^a$. Then $\varphi(N) = N$ by Theorem 1.33 which implies $\varphi|_N \in \mathrm{Aut}(N)$ by Theorem 1.22. Viewed as an automorphism of N, $\varphi|_N =: \psi \in \mathrm{Aut}(N)$, we must have $\psi(K) = K$ by virtue of K being characteristic subgroup of N. But $\psi(K) = \varphi(K)$ due to a sub-sub-proof that $\forall k \in K, \psi(k) = \varphi(k)$. Then the result follows. □

55a ⟨*Proof: $\forall a \in G, K^a = K$* 55a⟩≡

```
proof
  let a be Element of G;
  consider g being inner Automorphism of G such that
  A1: for x being Element of G holds g.x = x |^ a
  by Th32;

  Image(g|N) = N by Th33;
  then reconsider f = g|N as Automorphism of N by Th22;
  A2: Image(f|K) = the multMagma of K by Def3;

  for k being Element of G st k in K holds f.k = g.k by Th1,GROUP_2:40;
  then Image(g|K) = the multMagma of K & Image(g|K) = K |^ a
  by A1,A2,Th28,Th36;
  hence thesis;
end;
```

This code is used in chunk 54b.

Theorem 1.39. *If $N \leq G$ is characteristic, and if $K \leq N$ is characteristic, then $K \leq G$ is characteristic.*

The proof is remarkably similar to the previous theorem. In fact, we can re-use exactly the same line of reasoning establishing $\forall k \in G,\ k \in K \implies f(k) = g(k)$.

Proof outline. For any automorphism $g \in \mathrm{Aut}(G)$ we have $g(N) = N$ by virtue of N is a characteristic subgroup of G. We can then consider $f = g|_N$ as an automorphism of N. Then $f(K) = K$ since K is a characteristic subgroup of N.

We have $\forall k \in K, f(k) = g(k)$. Thus $f(K) = g(K)$, and we have established $f(K) = K$, therefore $g(K) = K$. □

55b ⟨*Theorem: transitivity of characteristic subgroups* 55b⟩≡

```
theorem Th39:
  for N being characteristic Subgroup of G
  for K being characteristic Subgroup of N
  holds K is characteristic Subgroup of G
proof
  let N be characteristic Subgroup of G;
  let K be characteristic Subgroup of N;
  for g being Automorphism of G holds Image(g|K) = the multMagma of K
  proof
    let g be Automorphism of G;
    Image(g|N) = the multMagma of N by Def3;
```

```
    then reconsider f = g|N as Automorphism of N by Th22;
    A1: Image(f|K) = the multMagma of K by Def3;

    for k being Element of G st k in K holds f.k = g.k by Th1, GROUP_2:40;
    hence Image(g|K) = the multMagma of K by A1,Th36;
  end;
  hence K is characteristic Subgroup of G by Def3;
end;
```

This code is used in chunk 47b.
Defines:
Th39, never used.

Theorem 1.40. *Let $H \leq G$. Then H char G if and only if for any automorphism φ, we have $\varphi(H) \leq H$.*

Some texts give this as the definition for H being a characteristic subgroup, which is fine.

Proof outline. Given a subgroup $H \leq G$. We have two halfs to our proof.

We prove H is a characteristic subgroup of G implies $\forall \varphi \in \text{Aut}(G), \varphi(H) \leq H$. This uses the facts $\varphi(H) = H \leq H$. This establishes the first half of the proof.

Now, the other direction, assuming $\forall \varphi \in \text{Aut}(G), \varphi(H) \leq H$ we find H is a characteristic subgroup of G. □

56 ⟨*Theorem: $H \leq G$ is characteristic iff $\forall \varphi \in \text{Aut}(G), \varphi(H) \leq H$* 56⟩≡

```
theorem Th40:
  for G being Group
  for H being strict Subgroup of G
  holds H is characteristic Subgroup of G iff
  (for phi being Automorphism of G holds Image(phi|H) is Subgroup of H)
proof
  let G be Group;
  let H be strict Subgroup of G;
  thus H is characteristic Subgroup of G implies
       (for phi being Automorphism of G holds Image(phi|H) is Subgroup of H)
  ⟨Proof: H char G ⟹ ∀φ ∈ Aut(G), φ(H) ≤ H 57a⟩

  thus (for phi being Automorphism of G holds Image(phi|H) is Subgroup of H)
       implies H is characteristic Subgroup of G
  ⟨Proof: H char G ⟸ ∀φ ∈ Aut(G), φ(H) ≤ H 57b⟩

  thus thesis;
end;
```

This code is used in chunk 47b.
Defines:
Th40, never used.

Sub-proof (H char G $\implies$ $\forall \varphi \in \text{Aut}(G), \varphi(H) \leq H$). The proof in the forward direction boils down to the observation $H \leq H$ then applying the definition of characteristic subgroup. □

57a ⟨*Proof: H char G* $\implies \forall \varphi \in \mathrm{Aut}(G), \varphi(H) \leq H$ 57a⟩≡

```
proof
  assume B1: H is characteristic Subgroup of G;
  let phi be Automorphism of G;
  Image(phi|H) = H & H is Subgroup of H by B1,GROUP_2:54,Def3;
  hence Image(phi|H) is Subgroup of H;
end;
```

This code is used in chunk 56.

Sub-proof (H char G $\impliedby \forall \varphi \in \mathrm{Aut}(G), \varphi(H) \leq H$*).* The proof in the backward direction amounts to proving, for arbitrary automorphisms φ of G, $\varphi(H) \leq H$ and since φ is an Automorphism $H \leq \varphi^{-1}(H)$. Then for any $\varphi \in \mathrm{Aut}(G)$, we have $\varphi(H) \leq H$. Taken together, this implies $\forall \varphi \in \mathrm{Aut}(G)$, $H = \varphi(H)$.

But as discussed earlier (§**??**), subgroup equality holds only for strict subgroups. For this reason, we have the hypothesis that H is a strict subgroup of G. □

57b ⟨*Proof: H char G* $\impliedby \forall \varphi \in \mathrm{Aut}(G), \varphi(H) \leq H$ 57b⟩≡

```
proof
  assume A1: for phi being Automorphism of G
  holds Image(phi|H) is Subgroup of H;
  A2: for phi being Automorphism of G holds H is Subgroup of Image(phi|H)
  ⟨Proof: ∀φ ∈ Aut(G), H ≤ φ(H) 57c⟩
  for phi being Automorphism of G holds H = Image(phi|H)
  proof
    let phi be Automorphism of G;
    H is Subgroup of Image(phi|H) & Image(phi|H) is Subgroup of H
    by A1,A2;
    hence H = Image(phi|H) by GROUP_2:55;
  end;
  hence H is characteristic Subgroup of G by Def3;
end;
```

This code is used in chunk 56.

Sub-sub-proof ($\forall \varphi \in \mathrm{Aut}(G), H \leq \varphi(H)$*).* This is a slick argument, which is confusing until one realizes what's going on. We use the facts that, for any $\varphi, \psi \in \mathrm{Aut}(G)$,

- Hypothesis `A1`: $\psi(H) \leq H$;
- Theorem 1.16: for $\psi = \varphi^{-1}$, we have $\varphi[\psi(H)] \leq \varphi(H)$; and
- Theorem 1.17: for $\psi = \varphi^{-1}$, the underlying magmas of H and $\varphi[\psi(H)]$ are equal.

This suffices to infer $H \leq \varphi(H)$. □

57c ⟨*Proof:* $\forall \varphi \in \mathrm{Aut}(G), H \leq \varphi(H)$ 57c⟩≡

```
proof
  let phi be Automorphism of G;
  consider psi being Automorphism of G such that
  B1: psi = phi" and
  B2: Image(phi|Image(psi|H)) is Subgroup of Image(phi|H) by A1,Th16;
  consider psi2 being Automorphism of G such that
  B3: psi2 = phi" and
  B4: the multMagma of H = Image(phi|Image(psi2|H)) by Th17;
  thus H is Subgroup of Image(phi|H) by B1,B2,B3,B4;
end;
```

This code is used in chunk 57b.

Theorem 1.41. *Let G be a group. Its center $Z(G)$ is a characteristic subgroup.*

Proof outline. This is our first application of $\forall \varphi \in \text{Aut}(G), \varphi(H) \leq H$ implies H is characteristic. The bulk of the proof amounts to showing $\varphi(Z(G)) \leq Z(G)$, which requires two prior steps:

(1) for any $g \in G$ and $z \in Z(G)$, we have $\varphi(z)g = g\varphi(z)$ — i.e., $\varphi(z)$ commutes with every element of G; then
(2) $\varphi(z) \in Z(G)$ for any $z \in Z(G)$.

Then we have $\varphi(Z(G))$ be a subgroup of $Z(G)$, which let's us use the previous theorem. □

Remark 1.41.1. The `center` functor is defined in Definition [GROUP_5:def10].

58a ⟨*Theorem: $Z(G)$ is characteristic subgroup* 58a⟩≡

```
theorem Th41:
  center G is characteristic Subgroup of G
proof
  set Z = center G;
  ⟨Prove ∀φ ∈ Aut(G), φ(Z(G)) ≤ Z(G) 58b⟩

  hence Z is characteristic Subgroup of G by Th40;
end;
```

This code is used in chunk 47b.
Defines:
`Th41`, never used.

Proof branch ($\forall \varphi \in \text{Aut}(G), \varphi(Z(G)) \leq Z(G)$). The heart of the proof amounts to showing, for any Automorphism φ, that $\varphi(Z(G))$ is a subgroup of $Z(G)$. □

58b ⟨*Prove* $\forall \varphi \in \text{Aut}(G), \varphi(Z(G)) \leq Z(G)$ 58b⟩≡
⟨*Step 1:* $\forall \varphi \in \text{Aut}(G) \forall y \in G \forall z \in Z(G), \varphi(z)y = y\varphi(z)$ 58c⟩
⟨*Step 2:* $\forall \varphi \in \text{Aut}(G) \forall z \in G, z \in Z(G) \implies \varphi(z) \in Z(G)$ 59a⟩
⟨*Step 3:* $\forall \varphi \in \text{Aut}(G), \varphi(Z(G)) \leq Z(G)$ 59b⟩
This code is used in chunk 58a.

Proof step 1 ($\forall \varphi \in \text{Aut}(G) \forall y \in G \forall z \in Z(G), \varphi(z)y = y\varphi(z)$). Proving $\varphi(z)$ commutes with every element of the group is a straightforward calculation. In fact, this is usually what textbooks present, then dismiss the rest of the proof as "trivial" or "obvious". □

58c ⟨*Step 1:* $\forall \varphi \in \text{Aut}(G) \forall y \in G \forall z \in Z(G), \varphi(z)y = y\varphi(z)$ 58c⟩≡

```
A1: for y,z being Element of G st z in Z
holds (phi.z)*y = y*phi.z
proof
  let y,z be Element of G;
  assume B1: z in Z;
  set x = (phi").y;
  (phi.z)*y = (phi.z)*(phi.x) by Th4
          .= phi.(z*x) by GROUP_6:def 6
          .= phi.(x*z) by B1,GROUP_5:77
          .= (phi.x)*(phi.z) by GROUP_6:def 6
```

```
            .= y*(phi.z) by Th4;
    hence thesis;
  end;
```

This code is used in chunk 58b.

Proof step 2 ($\forall\varphi \in \mathrm{Aut}(G)\forall z \in G, z \in Z(G) \implies \varphi(z) \in Z(G)$). Establishing $z \in Z(G)$ implies $\varphi(z) \in Z(G)$ amounts to unfolding definitions. □

59a ⟨*Step 2:* $\forall\varphi \in \mathrm{Aut}(G)\forall z \in G, z \in Z(G) \implies \varphi(z) \in Z(G)$ 59a⟩≡

```
  A2: for z being Element of G st z in Z
  holds (phi|Z).z in Z
  proof
    let z be Element of G;
    assume B1: z in Z;
    then for y being Element of G holds (phi.z)*y=y*(phi.z) by A1;
    then (phi.z) in Z by GROUP_5:77;
    hence ((phi|Z).z) in Z by B1,Th1;
  end;
```

This code is used in chunk 58b.

Proof step 3 ($\forall\varphi \in \mathrm{Aut}(G), \varphi(Z(G)) \leq Z(G)$). The last step, which is the "obvious" part, infers from $\forall z \in Z(G), \varphi(z) \in Z(G)$ that $\varphi(Z(G)) \leq Z(G)$. It's also the ugliest part of the proof which could probably be cleaned up considerably. This is only due to the sub-step establishing $w \in \mathrm{rng}(\varphi|_{Z(G)}) \implies w \in Z(G)$. □

59b ⟨*Step 3:* $\forall\varphi \in \mathrm{Aut}(G), \varphi(Z(G)) \leq Z(G)$ 59b⟩≡

```
  Image(phi|Z) is Subgroup of Z
  proof
    for w being Element of G st w in rng(phi|Z) holds w in Z
    ⟨Sub-step 3.1: ∀w ∈ G, w ∈ rng(φ|Z(G)) ⟹ w ∈ Z(G) 59c⟩
    then rng(phi|Z) c= the carrier of Z by STRUCT_0:def 5;
    then the carrier of Image(phi|Z) c= the carrier of Z by GROUP_6:44;
    hence Image(phi|Z) is Subgroup of Z by GROUP_2:57;
  end;
```

This code is used in chunk 58b.

Proof sub-step 3.1 ($\forall w \in G, w \in \mathrm{rng}(\varphi|_{Z(G)}) \implies w \in Z(G)$). This substep is ugly, and I offer no apology for it. There's probably a more elegant solution, but I cannot think of one. We explicitely walkthrough showing $w \in \mathrm{rng}(\varphi|_{Z(G)})$, which means there is some z such that $z \in \mathrm{dom}(\varphi|_{Z(G)})$ and $\varphi|_{Z(G)}(z) = w$. Since $\mathrm{dom}(\varphi|_{Z(G)}) = Z(G)$, it follows $\varphi|_{Z(G)}(z) \in Z(G)$ from step 2. Thus the result follows. □

59c ⟨*Sub-step 3.1:* $\forall w \in G, w \in \mathrm{rng}(\varphi|_{Z(G)}) \implies w \in Z(G)$ 59c⟩≡

```
  proof
    let w be Element of G;
    assume w in rng(phi|Z);
    then consider z being object such that
    C1: z in dom(phi|Z) and
    C2: (phi|Z).z = w by FUNCT_1:def 3;
    reconsider z as Element of Z by C1;
    z is Element of G by GROUP_2:42;
```

```
    hence w in Z by C2,A2,STRUCT_0:def 5;
  end;
```

This code is used in chunk 59b.

Scheme 1.1. *Let $P[-]$ be a predicate on subgroups of G for which (1) there is at least one subgroup $H \leq G$ satisfying $P[H]$ and (2) if $H \leq G$ satisfies $P[H]$, then for any automorphism $\varphi \in \mathrm{Aut}(G)$ we have $P[\varphi(H)]$.*

Let $\mathcal{F} = \{A \subseteq G \mid \exists H \leq G, P[H] \wedge A = U(H)\}$ be the family of sets underlying all subgroups of G satisfying $P[-]$. Then $\varphi(\bigcap \mathcal{F}) = \bigcap \mathcal{F}$.

Proof outline. Let $\mathcal{F} = \{A \subseteq G \mid H \leq G \wedge P[H]\}$ be the collection of sets underlying subgroups $H \leq G$ which satisfy the property $P[H]$. First, we need to prove $\mathcal{F} \neq \emptyset$. But since we have, by hypothesis, there is at least one subgroup $H \leq G$ which satisfies $P[H] \ldots$ so $\mathcal{F}$ is nonempty. Then to prove $\varphi(\bigcap \mathcal{F}) = \bigcap \mathcal{F}$, we establish $\varphi(\bigcap \mathcal{F}) \subseteq \bigcap \mathcal{F}$ and $\varphi(\bigcap \mathcal{F}) \supseteq \bigcap \mathcal{F}$. The result then follows. □

60 ⟨*Scheme: if $H \leq G \wedge P[H]$ and $\forall \varphi \in \mathrm{Aut}(G), P[\varphi(H)]$, then $\bigcap\{H \leq G \mid P[H]\}$ is $\mathrm{Aut}(G)$-invariant* 60⟩≡

```
  reserve A1,A2 for set;

  scheme :: sch 1
    CharMeet{G() -> Group, P[set]} :
    for phi being Automorphism of G()
    holds phi .: meet{A where A is Subset of G() : ex K being strict Subgroup
    of G() st A = the carrier of K & P[K]} = meet{A where A is Subset of G() :
    ex K being strict Subgroup of G() st A = the carrier of K & P[K]}
  provided
  A1: for phi being Automorphism of G()
      for H being strict Subgroup of G()
      st P[H]
      holds P[Image(phi|H)] and
  A2: ex H being strict Subgroup of G() st P[H]
  proof
    let phi be Automorphism of G();
    set UG = the carrier of G();
    set Fam = {A where A is Subset of G() : ex K being strict Subgroup
    of G() st A = the carrier of K & P[K]};
    consider H being strict Subgroup of G() such that
  A3: P[H]
    by A2;
    A4: Fam <> {}
    ⟨Proof step: $\mathcal{F} \neq \emptyset$ 61a⟩

    A5: for phi0 being Automorphism of G()
    for x being object st x in meet Fam
    holds phi0.x in meet Fam
    ⟨Proof step: $\forall \varphi_0 \in \mathrm{Aut}(G), \forall x, x \in \bigcap \mathcal{F} \implies \varphi_0(x) \in \bigcap \mathcal{F}$ 61b⟩

    for x being object st x in meet Fam
    holds x in phi .: meet Fam
    ⟨Proof step: $x \in \bigcap \mathcal{F} \implies x \in \varphi(\bigcap \mathcal{F})$ 62a⟩
    then P1: meet Fam c= phi .: meet Fam;

    for y being object st y in phi .: meet Fam
```

```
    holds y in meet Fam
    ⟨Proof step: y ∈ φ(⋂F) ⟹ y ∈ ⋂F 62b⟩
    then phi .: meet Fam c= meet Fam;
    hence thesis by P1,XBOOLE_0:def 10;
  end;
```

This code is used in chunk 47b.
Defines:
`CharMeet`, never used.

Proof step: $\mathcal{F}$ is non-empty. Since we assumed there exists a subgroup $H \leq G$ such that $P[H]$ holds, there is at least one element of $\mathcal{F}$, namely $H \in \mathcal{F}$. Hence $\bigcap \mathcal{F} \neq \emptyset$. □

61a ⟨*Proof step: $\mathcal{F} \neq \emptyset$* 61a⟩≡

```
  proof
    consider A being set such that
    B1: A = the carrier of H;
    the carrier of H is Subset of G() by GROUP_2:def 5;
    then A in Fam by A3, B1;
    hence thesis;
  end;
```

This code is used in chunk 60.

Proof step ($\forall \varphi_0 \in \mathrm{Aut}(G), \forall x, x \in \bigcap \mathcal{F} \implies \varphi_0(x) \in \bigcap \mathcal{F}$). Suppose $x \in \bigcap \mathcal{F}$. Then $\forall A \in \mathcal{F}, x \in A$. Let φ_0 be an arbitrary automorphism of G. From the hypothesis $P[H] \implies \forall \varphi \in \mathrm{Aut}(G), P[\varphi(H)]$, we apply it to $\psi = \varphi_0^{-1}$. But this means $x \in \psi(A)$. Then $\varphi_0(x) \in \varphi_0(\psi(A))$, and $\varphi_0(\psi(A)) = A$. Thus the result follows. □

61b ⟨*Proof step: $\forall \varphi_0 \in \mathrm{Aut}(G), \forall x, x \in \bigcap \mathcal{F} \implies \varphi_0(x) \in \bigcap \mathcal{F}$* 61b⟩≡

```
  proof
    let phi0 be Automorphism of G();
    let x be object;
    assume x in meet Fam;
    then B1: for A1 holds A1 in Fam implies x in A1 by SETFAM_1:def 1; :: sic
    for A being set holds A in Fam implies phi0.x in A
    proof
      let A be set;
      assume C1: A in Fam;
      consider A0 being Subset of G() such that
      C2: A0=A & ex H being strict Subgroup of G()
                 st A0 = the carrier of H & P[H]
      by C1;
      consider K being strict Subgroup of G() such that
      C3: A = the carrier of K & P[K]
      by C2;
      consider psi being Automorphism of G() such that
      C4: psi = phi0" & Image(phi0|Image(psi|K)) = the multMagma of K
      by Th17;
      x in K by C1,B1,C3;
      then C5: x in G() & dom phi0 = the carrier of G()
      by GROUP_2:40,FUNCT_2:def 1;
      P[Image(psi|K)] by C3,A1;
      then carr Image(psi|K) in Fam;
```

```
      then x in carr Image(psi|K) by B1;
      then phi0.x in phi0 .: (carr Image(psi|K)) by C5, FUNCT_1:def 6;
      then phi0.x in carr (phi0 .: Image(psi|K)) by GRSOLV_1:8;
      hence phi0.x in A by C3,C4,GRSOLV_1:def 3;
    end;
    hence thesis by A4, SETFAM_1:def 1;
  end;
```

This code is used in chunk 60.

Proof step ($x \in \bigcap \mathcal{F} \implies x \in \varphi(\bigcap \mathcal{F})$). Suppose $x \in \bigcap \mathcal{F}$. Let $\varphi \in \text{Aut}(G)$ be completely arbitrary, and $\psi = \varphi^{-1}$. From $x \in \bigcap \mathcal{F}$, it follows $\forall A \in \mathcal{F}, x \in A$. It follows from a previous step that $\forall A \in \mathcal{F}, \psi(x) \in A$. Then applying φ we find $\forall A \in \mathcal{F}, \varphi(\psi(x)) = x \in \varphi(A)$. Hence $x \in \varphi(\bigcap \mathcal{F})$. □

62a ⟨*Proof step:* $x \in \bigcap \mathcal{F} \implies x \in \varphi(\bigcap \mathcal{F})$ 62a⟩≡

```
  proof
    let x be object;
    assume B1: x in meet Fam;
    then carr H in Fam & for A1 holds A1 in Fam implies x in A1
    by A3,SETFAM_1:def 1;
    then B2: x in H;
    then B3: x is Element of G() by GROUP_2:42;
    reconsider psi = phi" as Automorphism of G() by GROUP_6:62;
    B4: dom phi = the carrier of G() by FUNCT_2:def 1;
    B5: psi.x in meet Fam by B1,A5;
    B6: phi.(psi.x) = x by B3,Th4;
    psi is bijective & x in G() by B2, GROUP_2:40;
    then psi.x in dom phi by B4, FUNCT_2:5;
    hence x in phi .: meet Fam by B6,B5,FUNCT_1:def 6;
  end;
```

This code is used in chunk 60.

Proof step ($y \in \varphi(\bigcap \mathcal{F}) \implies y \in \bigcap \mathcal{F}$). Let $\varphi \in \text{Aut}(G)$ be arbitrary. Suppose $y \in \varphi(\bigcap \mathcal{F})$. Then there is an $x \in \bigcap \mathcal{F}$ such that $y = \varphi(x)$. Then $\varphi(x) \in \bigcap \mathcal{F}$ from our first proof step. Hence $y \in \bigcap \mathcal{F}$. □

62b ⟨*Proof step:* $y \in \varphi(\bigcap \mathcal{F}) \implies y \in \bigcap \mathcal{F}$ 62b⟩≡

```
  proof
    let y be object;
    assume y in phi .: meet Fam;
    then consider x being object such that
    B1: x in dom phi & x in meet Fam & y = phi.x
    by FUNCT_1:def 6;
    thus y in meet Fam by B1,A5;
  end;
```

This code is used in chunk 60.

Scheme 1.2. *Let $P[-]$ be a predicate on subgroups of G for which (1) there is at least one subgroup $H \leq G$ satisfying $P[H]$ and (2) if $H \leq G$ satisfies $P[H]$, then for any automorphism $\varphi \in \text{Aut}(G)$ we have $P[\varphi(H)]$.*

Let $\mathcal{F} = \{A \subseteq G \mid \exists H \leq G, P[H] \wedge A = U(H)\}$ be the family of sets underlying all subgroups of G satisfying $P[-]$. There exists a subgroup $K \leq G$ whose underling set is $U(K) = \bigcap \mathcal{F}$ such that K is characteristic.

Proof outline. The proof boils down to what we would find in a textbook. For any Automorphism $\varphi \in \mathrm{Aut}(G)$, we have the collection $\mathcal{F}$ of subgroups of G satisfying $P[H]$, then we know there exists a subgroup $K \leq G$ such that its underlying set $U(K)$ is

$$U(K) := \bigcap \mathcal{F}. \tag{8.1}$$

Now to prove it is characteristic, we reason as follows:

$$\varphi(K) = \varphi(\bigcap \mathcal{F}) = \bigcap \varphi(\mathcal{F}) = \bigcap \mathcal{F} = K. \tag{8.2}$$

We take advantage of Scheme 1.1 to prove

$$\varphi(\bigcap \mathcal{F}) = \bigcap \varphi(\mathcal{F}) = \bigcap \mathcal{F}. \tag{8.3}$$

We also use the hypothesis that subgroups $H \leq G$ satisfying $P[H]$ are mapped to subgroups $\varphi(H)$ satisfying $P[\varphi(H)]$ under automorphisms $\varphi \in G$. □

63 ⟨*Scheme:* $\bigcap\{A \subseteq G \mid \exists H \leq G, A = H, P[H]\}$ *is characteristic* 63⟩≡

```
scheme :: sch 2
  MeetIsChar{G() -> Group, P[set]} :
  ex K being strict Subgroup of G() st
  the carrier of K = meet {A where A is Subset of G() :
  ex H being strict Subgroup of G() st A = the carrier of H & P[H]} &
  K is characteristic
provided
A1: for phi being Automorphism of G()
    for H being strict Subgroup of G()
    st P[H]
    holds P[Image(phi|H)] and
A2: ex H being strict Subgroup of G() st P[H]
proof
  set Fam = {A where A is Subset of G() :
              ex H being strict Subgroup of G()
              st A = the carrier of H & P[H]};

  A3: for phi being Automorphism of G()
  holds phi .: meet Fam = meet Fam from CharMeet(A1,A2);

  consider K being strict Subgroup of G() such that
  A4: the carrier of K = meet Fam
  from GROUP_4:sch 1(A2);
  take K;

  for phi being Automorphism of G()
  holds Image(phi|K) = K
  proof
    let phi be Automorphism of G();
    the carrier of Image(phi|K)
     = the carrier of phi .: K by GRSOLV_1:def 3
    .= phi .: (the carrier of K) by GRSOLV_1:8
    .= phi .: meet Fam by A4
    .= meet Fam by A3
    .= the carrier of K by A4;
    hence Image(phi|K) = K by GROUP_2:59;
```

```
    end;
    hence thesis by A4;
  end;
```

This code is used in chunk 47b.
Defines:
`MeetIsChar`, never used.

Proposition 1.25 ([GROUP_4:Th38]). *Let G be a group. Suppose G has a maximal subgroup. Then for any group element $a \in G$, we have $a \in \Phi(G)$ if and only if for every maximal subgroup $H < G$ we have $a \in H$.*

Theorem 1.42. *The Frattini subgroup $\Phi(G)$ is a characteristic subgroup of G.*

Proof outline. The proof boils down to what we would find in a textbook. We have abstracted away the argument to form Scheme 1.2, which gives us the results. □

Remark 1.42.1. Observe the key property required to prove that $\Phi(G)$ is characteristic is the observation we have a family $\mathcal{F}$ of subgroups of G for which any automorphism $\varphi \in \mathrm{Aut}(G)$ acts like a permutation of $\mathcal{F}$. If this is true, then $\bigcap \mathcal{F}$ is characteristic. We can formulate this argument as a scheme.

Remark 1.42.2. The proof is an extra step, because I believe it worth the cost to stress at a human-readable level that $K = \Phi(G)$.

64 ⟨*Theorem:* $\Phi(G)$ *is characteristic* 64⟩≡

```
  theorem Th42:
    for G being non trivial Group
    holds (ex H being strict Subgroup of G st H is maximal) implies
    Phi(G) is characteristic Subgroup of G
  proof
    let G be non trivial Group;
    defpred P[Subgroup of G] means $1 is maximal;
    assume A1: ex H being strict Subgroup of G st P[H];
    set MaxSubCarrs = {A where A is Subset of G :
                       ex H being strict Subgroup of G
                       st A = the carrier of H & P[H]};

    A2: for phi being Automorphism of G
    for H being strict Subgroup of G
    st P[H]
    holds P[Image(phi|H)] by Th24;

    consider K being strict Subgroup of G such that
    A3: the carrier of K = meet {A where A is Subset of G :
        ex H being strict Subgroup of G st A = the carrier of H & P[H]} and
    A4: K is characteristic
    from MeetIsChar(A2,A1);
    K = Phi(G) by A1,A3,GROUP_4:def 7; :: sic
    hence thesis by A4;
  end;
```

This code is used in chunk 47b.
Defines:
`Th42`, never used.

8.1. **Derived Subgroup is Characteristic.** We will denote the *set* of all commutators of elements of G by

$$\text{Commutators}(G) := \{[a,b] \in G \mid a,b \in G\}. \tag{8.4}$$

The derived subgroup is the *subgroup* generated by this

$$G' = [G,G] := \langle \text{Commutators}(G) \rangle. \tag{8.5}$$

We will prove the derived subgroup is characteristic.

Theorem 1.43. *Let G be a group, let $C = \text{Commutators}(G)$ be the set of commutators of any pair of group elements. Then for any automorphism $\varphi \in \text{Aut}(G)$, we have $\varphi(C) = C$.*

Proof outline. We will prove $\varphi(C) \subseteq C$ and $\varphi(C) \supseteq C$. □

65 ⟨*Theorem:* $\forall \varphi \in G, \varphi(\text{Commutators}(G)) = \text{Commutators}(G)$ 65⟩≡

```
theorem Th43:
  for phi being Automorphism of G
  holds phi .: commutators G = commutators G
proof
  let phi be Automorphism of G;
  for g being object
  st g in commutators G
  holds g in phi .: commutators G
  ⟨Proof: φ(Commutators(G)) ⊇ Commutators(G) 66a⟩
  then P1: commutators G c= phi .: commutators G;
  for h being object
  st h in phi .: commutators G
  holds h in commutators G
  ⟨Proof: φ(Commutators(G)) ⊆ Commutators(G) 66b⟩
  then phi .: commutators G c= commutators G;
  hence commutators G = phi .: commutators G by P1,XBOOLE_0:def 10;
end;
```

This code is used in chunk 47b.
Defines:
Th43, never used.

Proof step [$\varphi(\text{Commutators}(G)) \supseteq \text{Commutators}(G)$]. Let $g \in \text{Commutators}(G)$. Then consider $a,b \in G$ such that

$$g = [a,b] \tag{8.6}$$

by Theorem [GROUP_5:Th58]. Take $x = \varphi^{-1}(a)$ and $y = \varphi^{-1}(b)$. These are elements of G, so $[x,y] \in \text{Commutators}(G)$. Then $\varphi([x,y]) \in \varphi(\text{Commutators}(G))$ and

$$\varphi([x,y]) = [a,b] = g \tag{8.7}$$

thus $g \in \varphi(\text{Commutators}(G))$. Since we let g be arbitrary, this implies $\varphi(\text{Commutators}(G)) \supseteq \text{Commutators}(G)$ by Theorem [TARSKI:def3]. □

66a ⟨*Proof:* $\varphi(\text{Commutators}(G)) \supseteq \text{Commutators}(G)$ 66a⟩≡

```
proof
  let g be object;
  assume B1: g in commutators G;
  then reconsider g as Element of G;
  consider a,b being Element of G such that
  B2: g = [.a,b.]
  by B1, GROUP_5:58;
  reconsider psi = phi" as Automorphism of G by GROUP_6:62;
  set x = psi.a;
  set y = psi.b;
  set h = [.x,y.];
  dom phi = the carrier of G by FUNCT_2:def 1;
  then B3: h in dom phi & h in commutators G & phi.((phi").g) = g by Th4;
  psi.g = psi.([.a,b.]) by B2
       .= [.psi.a,psi.b.] by GROUP_6:34
       .= h;
  hence thesis by B3, FUNCT_1:def 6;
end;
```

This code is used in chunk 65.

Proof step ⌈$\varphi(\text{Commutators}(G)) \subseteq \text{Commutators}(G)$⌋. We consider an arbitrary $h \in \varphi(\text{Commutators}(G))$. Then there is some $g \in \text{Commutators}(G)$ such that $\varphi(g) = h$. Consider $a, b \in G$ such that

$$g = [a, b]. \tag{8.8}$$

Then by Theorem [GROUP_6:Th34],

$$\varphi([a, b]) = [\varphi(a), \varphi(b). \tag{8.9}$$

But look, this is a commutator! Combining all this together, this means $\varphi(g) \in \text{Commutators}(G)$. And since we let h be arbitrary, this means $\varphi(\text{Commutators}(G)) \subseteq \text{Commutators}(G)$ by Theorem [TARSKI:def3]. □

66b ⟨*Proof:* $\varphi(\text{Commutators}(G)) \subseteq \text{Commutators}(G)$ 66b⟩≡

```
proof
  let h be object;
  assume B1: h in phi .: commutators G;
  consider g being object such that
      g in dom phi and
  B2: g in commutators G and
  B3: h = phi.g
  by B1,FUNCT_1:def 6;
  consider a,b be Element of G such that
  B4: g = [.a,b.]
  by B2,GROUP_5:58;
  h = phi.g by B3
   .= phi.([.a,b.]) by B4
   .= [.phi.a, phi.b.] by GROUP_6:34;
  hence h in commutators G;
end;
```

This code is used in chunk 65.

Theorem 1.44. *Let $H \leq G$ be a subgroup, $\varphi \in \mathrm{Aut}(G)$ be an automorphism. If every $h \in H$ satisfies $\varphi(h) \in H$, then $\varphi(H) \leq H$.*

Proof. We have $\varphi(H) \leq H$ follow from the underlying set inclusions, and unfolding the definitions. □

67a ⟨*Theorem:* $\forall h \in H, \varphi(h) \in H$ *implies* $\varphi(H) \leq H$ 67a⟩≡

```
theorem Th44:
  for G being Group
  for phi being Automorphism of G
  for H being Subgroup of G
  st (for h being Element of H
      holds phi.h in H)
  holds Image(phi|H) is Subgroup of H
proof
  let G be Group;
  let phi be Automorphism of G;
  let H be Subgroup of G;
  assume A1: for h being Element of H holds phi.h in H;
  for y being object st y in rng(phi|H) holds y in the carrier of H
  proof
    let y be object;
    assume y in rng(phi|H);
    then consider x being object such that
    B1: x in dom(phi|H) and
    B2: y = (phi|H).x
    by FUNCT_1:def 3;
    B3: x in H by B1;
    reconsider x as Element of H by B1;
    phi.x in H & x is Element of G by A1,GROUP_2:42;
    hence y in the carrier of H by B2,B3,Th1;
  end;
  then rng(phi|H) c= the carrier of H;
  then the carrier of Image(phi|H) c= the carrier of H by GROUP_6:44;
  hence Image(phi|H) is Subgroup of H by GROUP_2:57;
end;
```

This code is used in chunk 47b.
Defines:
`Th44`, never used.

Theorem 1.45. *If $A \subseteq G$ is a nonempty subset such that, for any automorphism $\varphi \in \mathrm{Aut}(G)$ we have $\varphi(A) = A$, then the generated subgroup $\langle A \rangle$ is a characteristic subgroup.*

Proof sketch. We should recall that a generic element of $\langle A \rangle$ is given by the product of finitely many elements of A. The first thing we prove is (A_2) for any automorphism $\varphi \in \mathrm{Aut}(G)$ and for any $a \in A$, we have $\varphi(a) \in A$. Then we prove $\varphi(\langle A \rangle) = \langle A \rangle$, which establishes the result. □

67b ⟨*Theorem:* $A \subseteq G$ *s.t.* $\forall \varphi \in \mathrm{Aut}(G), \varphi(A) = A$, *then* $\langle A \rangle$ *is characteristic* 67b⟩≡

```
theorem Th45:
  for G being Group
  for A being non empty Subset of G
  st (for phi being Automorphism of G
```

```
      holds phi .: A = A)
  holds gr A is characteristic
proof
  let G be Group;
  let A be non empty Subset of G;
  assume A1: for phi being Automorphism of G holds phi .: A = A;
  A2: for phi being Automorphism of G for a being Element of A holds phi.a in A
  proof
    let phi be Automorphism of G;
    let a be Element of A;
    dom phi = the carrier of G by FUNCT_2:def 1;
    then phi.a in phi .: A by FUNCT_1:def 6;
    hence phi.a in A by A1;
  end;
  set H = gr A;
  A3: for phi being Automorphism of G holds Image(phi|H) is Subgroup of H
  proof
    let phi be Automorphism of G;
    B2: for h being Element of G st h in H holds phi.h in H
    ⟨Proof: ∀h ∈ G, h ∈ H ⟹ φ(h) ∈ H 68⟩
    for h being Element of H holds phi.h in H
    proof
      let h be Element of H;
      C1: h in H;
      h is Element of G by GROUP_2:42;
      hence phi.h in H by B2,C1;
    end;
    hence Image(phi|H) is Subgroup of H by Th44;
  end;
  thus gr A is characteristic by A3,Th40;
end;
```

This code is used in chunk 47b.
Defines:
Th45, never used.

Proof step ($\forall h \in G, h \in H \implies \varphi(h) \in H$*).* Taking two finite sequences $F^{(1)} = (a_1, \ldots, a_n)$ and $F^{(2)}_j = \varphi(F^{(1)}_j)$, we prove (C_8) that $F^{(2)}$ is a sequence of elements of A, then $\varphi(\prod_j F^{(1)}_j) = \prod_j \varphi(F^{(1)}_j) = \prod_j F^{(2)}_j$ implies $\prod_j F^{(2)}_j \in H$. □

68 ⟨*Proof:* $\forall h \in G, h \in H \implies \varphi(h) \in H$ 68⟩≡

```
proof
  let h be Element of G;
  assume h in H;
  then consider F1 being FinSequence of the carrier of G,
               I being FinSequence of INT such that
  C2: len F1 = len I and
  C3: rng F1 c= A and
  C4: Product(F1 |^ I) = h
  by GROUP_4:28;
  deffunc F(Nat) = phi.(F1/.$1);
  consider F2 being FinSequence such that
  C5: len(F2) = len F1 and
```

```
    C6: for k being Nat st k in dom F2 holds F2.k = F(k)
    from FINSEQ_1:sch 2;
    C7: dom F2 = dom F1 by C5,FINSEQ_3:29;
    C8: F2 is FinSequence of the carrier of G & rng F2 c= A
    proof
      D1: for y being object st y in rng F2 holds y in A
      proof
        let y be object;
        assume y in rng F2;
        then consider k being object such that
        E2: k in dom F2 and
        E3: y = F2.k by FUNCT_1:def 3;
        reconsider k as Element of NAT by E2;
        set x = F1.k;
        x in rng F1 by FUNCT_1:def 3, E2, C7;
        then reconsider x as Element of A by C3;
        E4: x = F1/.k by E2,C7,PARTFUN1:def 6;
        y = F(k) by E2,E3,C6
         .= phi.(F1/.k);
        hence y in A by A2,E4;
      end;
      for y being object st y in rng F2 holds y in the carrier of G
      proof
        let y be object;
        assume y in rng F2;
        then y in A by D1;
        hence y in the carrier of G;
      end;
      hence rng F2 c= the carrier of G;
      thus rng F2 c= A by D1;
    end;
    then reconsider F2 as FinSequence of the carrier of G;
    set h2 = Product(F2 |^ I);
    C9: (for k being Nat st k in dom F1
         holds F2.k = phi.(F1.k)) & len F1 = len I & len F2 = len I
    proof
      thus (for k being Nat st k in dom F1 holds F2.k = phi.(F1.k))
      proof
        let k be Nat;
        assume D1: k in dom F1;
        then k in dom F2 by C5,FINSEQ_3:29;
        then F2.k = F(k) by C6
                 .= phi.(F1/.k);
        hence F2.k = phi.(F1.k) by D1,PARTFUN1:def 6;
      end;
      thus len F1 = len I by C2;
      thus len F2 = len I by C2,C5;
    end;
    then len F2 = len I & rng F2 c= A & Product(F2 |^ I) = phi.h
    by C4,C8,GROUP_9:125;
    hence phi.h in H by GROUP_4:28;
  end;
```

This code is used in chunk 67b.

Theorem 1.46. *The derived subgroup $G' = [G, G]$ is a characteristic subgroup.*

Proof sketch. We simply use the fact that, for any automorphism (indeed, any endomorphism) $\varphi \in \mathrm{Aut}(G)$, we have $\varphi(\{[x, y] \mid x, y \in G\}) = \{[x, y] \mid x, y \in G\})$. Then from the previous theorem, we have $\varphi([G, G]) = [G, G]$. □

70a ⟨*Theorem: The derived subgroup is characteristic* 70a⟩≡
```
theorem Th46:
  G‘ is characteristic
proof
  A1: [.1_G,1_G.] in commutators G;
  for phi being Automorphism of G holds phi .: commutators G = commutators G
  by Th43;
  hence thesis by A1,Th45;
end;
```
This code is used in chunk 47b.
Defines:
`Th46`, never used.

Theorem 1.47. *If $H \leq G$ is any subgroup, $a \in G$ is any group element, and $\varphi \in \mathrm{Aut}(G)$, then $\varphi(aH) = \varphi(a)\varphi(H)$.*

Proof sketch. We prove set equality by showing $\varphi(aH) \subseteq \varphi(a)\varphi(H)$ and then $\varphi(a)\varphi(H) \subseteq \varphi(aH)$, which then proves the result. □

70b ⟨*Theorem: $H \leq G, a \in G$, $\varphi(aH) = \varphi(a)\varphi(H)$* 70b⟩≡
```
theorem Th47:
  for G1,G2 being Group
  for H being Subgroup of G1
  for a being Element of G1
  for f being Homomorphism of G1,G2
  holds f.:(a * H) = (f.a) * (f .: H)
proof
  let G1,G2 be Group;
  let H be Subgroup of G1;
  let a be Element of G1;
  let f be Homomorphism of G1,G2;
  A1: dom f = the carrier of G1 by FUNCT_2:def 1;
  for y being object st y in f.:(a * H) holds y in (f.a)*(f.:H)
  proof
    let y be object;
    assume y in f .: (a * H);
    then consider x being object such that
    B1: x in the carrier of G1 & x in (a * H) and
    B2: y = f.x
    by A1,FUNCT_1:def 6;
    consider h being Element of G1 such that
    B3: x = a*h & h in H
    by B1,GROUP_2:103;
    B4: y = f.(a*h) by B2,B3
         .= (f.a)*(f.h) by GROUP_6:def 6;
    dom f = the carrier of G1 & h in H & h in G1 by B3,FUNCT_2:def 1;
    then f.h in f.:(the carrier of H) by FUNCT_1:def 6;
    then f.h in f.:H by GRSOLV_1:8;
```

```
    hence y in (f.a) * (f .: H) by B4,GROUP_2:103;
  end;
  then A1: f.:(a * H) c= (f.a) * (f .: H);
  for y being object st y in (f.a)*(f.:H) holds y in f.:(a * H)
  proof
    let y be object;
    assume y in (f.a)*(f.:H);
    then consider g being Element of G2 such that
    B1: y = (f.a)*g and
    B2: g in (f.:H)
    by GROUP_2:103;
    g in Image(f|H) by B2,GRSOLV_1:def 3;
    then consider x being Element of H such that
    B3: g = (f|H).x
    by GROUP_6:45;
    B4: x in H & x is Element of G1 by GROUP_2:42;
    reconsider x as Element of G1 by GROUP_2:42;
    B5: y = (f.a)*g by B1
         .= (f.a)*(f.x) by B3,B4,Th1
         .= f.(a*x) by GROUP_6:def 6;
    a*x in the carrier of G1 & dom f = the carrier of G1 by FUNCT_2:def 1;
    then (a*x) in dom f & (a*x) in a*H & y=f.(a*x) by B4,B5,GROUP_2:103;
    hence y in f.:(a * H) by FUNCT_1:def 6;
  end;
  then A2: (f.a) * (f .: H) c= f.:(a * H);
  thus f.:(a * H) = (f.a) * (f .: H) by A1,A2,XBOOLE_0:def 10;
end;
```

This code is used in chunk 47b.
Defines:
Th47, never used.

Theorem 1.48. *If $H \leq G$ is any subgroup, $a \in G$ is any group element, and $\varphi \in \mathrm{Aut}(G)$, then $\varphi(Ha) = \varphi(H)\varphi(a)$.*

The proof boils down to the same steps as the previous one.

71 ⟨*Theorem:* $H \leq G, a \in G$, $\varphi(Ha) = \varphi(H)\varphi(a)$ 71⟩≡

```
theorem Th48:
  for G1,G2 being Group
  for H being Subgroup of G1
  for a being Element of G1
  for f being Homomorphism of G1,G2
  holds f.:(H * a) = (f .: H) * (f.a)
proof
  let G1,G2 be Group;
  let H be Subgroup of G1;
  let a be Element of G1;
  let f be Homomorphism of G1,G2;
  A1: dom f = the carrier of G1 by FUNCT_2:def 1;
  for y being object st y in f.:(H * a) holds y in (f.:H)*(f.a)
  proof
    let y be object;
    assume y in f .: (H * a);
    then consider x being object such that
```

```
    B1: x in the carrier of G1 & x in (H * a) and
    B2: y = f.x
    by A1,FUNCT_1:def 6;
    consider h being Element of G1 such that
    B3: x = h*a & h in H
    by B1,GROUP_2:104;
    dom f = the carrier of G1 & h in H & h in G1 by FUNCT_2:def 1, B3;
    then f.h in f.:(the carrier of H) by FUNCT_1:def 6;
    then f.h in f.:H by GRSOLV_1:8;
    then (f.h)*(f.a) in (f.:H)*(f.a) by GROUP_2:104;
    hence thesis by B2,B3,GROUP_6:def 6;
  end;
  then A2: f.:(H * a) c= (f .: H) * (f.a);
  for y being object st y in (f.:H)*(f.a) holds y in f.:(H * a)
  proof
    let y be object;
    assume y in (f.:H)*(f.a);
    then consider g being Element of G2 such that
    B1: y = g*(f.a) and
    B2: g in (f.:H)
    by GROUP_2:104;
    g in Image(f|H) by B2,GRSOLV_1:def 3;
    then consider x being Element of H such that
    B3: g = (f|H).x
    by GROUP_6:45;
    B4: x in H & x is Element of G1 by GROUP_2:42;
    reconsider x as Element of G1 by GROUP_2:42;
    B5: y = g*(f.a) by B1
         .= (f.x)*(f.a) by B3,B4,Th1
         .= f.(x*a) by GROUP_6:def 6;
    x*a in the carrier of G1 & dom f = the carrier of G1 by FUNCT_2:def 1;
    then (x*a) in dom f & (x*a) in H*a & y=f.(x*a) by B4,B5,GROUP_2:104;
    hence y in f.:(H * a) by FUNCT_1:def 6;
  end;
  then (f .: H) * (f.a) c= f.:(H * a);
  hence f.:(H * a) = (f .: H)*(f.a) by A2,XBOOLE_0:def 10;
end;
```

This code is used in chunk 47b.
Defines:
Th48, never used.

Theorem 1.49. *If $N \trianglelefteq G$, then given any automorphism $\varphi \in \mathrm{Aut}(G)$ of G we have our automorphism map N to another normal subgroup $\varphi(N) \trianglelefteq G$.*

Proof sketch. We recall $gN = Ng$ for any $g \in G$ and normal subgroup $N \trianglelefteq G$. Then

$$\varphi(g)\varphi(N) = \varphi(gN) \tag{8.10a}$$
$$= \varphi(Ng) \tag{8.10b}$$
$$= \varphi(N)\varphi(g). \qquad \square$$

72 ⟨*Theorem: $N \trianglelefteq G$, $\varphi \in \mathrm{Aut}(G)$ implies $\varphi(N) \trianglelefteq G$* 72⟩≡

```
theorem Th49:
```

```
  for G being Group
  for N being strict normal Subgroup of G
  for phi being Automorphism of G
  holds Image(phi|N) is normal Subgroup of G
proof
  let G be Group;
  let N be strict normal Subgroup of G;
  let phi be Automorphism of G;
  set H = Image(phi|N);
  for g being Element of G holds g * H = H * g
  proof
    let g be Element of G;
    set f = (phi").g;
    B1: phi.f = g by Th4;
    B2: phi .: (f * N) = (phi.f) * (phi .: N) by Th47
                      .= g * H by B1,GRSOLV_1:def 3;
    phi .: (N * f) = (phi .: N)*(phi.f) by Th48
                  .= (phi .: N)*g by Th4
                  .= H*g by GRSOLV_1:def 3;
    hence g * H = H * g by B2,GROUP_3:117;
  end;
  hence H is normal Subgroup of G by GROUP_3:117;
end;
```

This code is used in chunk 47b.
Defines:
Th49, never used.

Theorem 1.50. *Let $H \leq G$. Then H is characteristic if and only if for any automorphism $\varphi \in \mathrm{Aut}(G)$ and every $x \in H$ we have $\varphi(x) \in H$.*

Remark 1.50.1. We need to have H be a strict subgroup since the definition of a characteristic subgroup requires $\forall \varphi \in \mathrm{Aut}(G), \varphi(H) = H$. Without strictness, we cannot have subgroup equality.

Proof sketch. There are two key moments to this proof:

(1) H is characteristic implies $\forall \varphi \in \mathrm{Aut}(G), \forall x \in H, \varphi(x) \in H$;
(2) $\forall \varphi \in \mathrm{Aut}(G), \forall x \in H, \varphi(x) \in H$ implies H is characteristic.

The result follows immediately. □

73 ⟨*Theorem: $H \leq G$ characteristic $\iff \forall \varphi \in \mathrm{Aut}(G) \forall x \in H, \varphi(x) \in H$* 73⟩≡

```
theorem Th50:
  for G being Group
  for H being strict Subgroup of G
  holds H is characteristic iff
        (for phi being Automorphism of G
         for x being Element of G
         st x in H
         holds phi.x in H)
proof
  let G be Group;
  let H be strict Subgroup of G;
  thus H is characteristic implies (for phi being Automorphism of G
                                    for x being Element of G
                                    st x in H
```

```
                                        holds phi.x in H)
    proof
      assume B1: H is characteristic;
      let phi be Automorphism of G;
      let x be Element of G;
      assume B2: x in H;
      B3: H = Image(phi|H) by B1
           .= phi .: H by GRSOLV_1:def 3;
      dom phi = the carrier of G by FUNCT_2:def 1;
      then phi.x in phi .: (the carrier of H) by B2,FUNCT_1:def 6;
      hence thesis by B3,GRSOLV_1:8;
    end;
    thus (for phi being Automorphism of G
          for x being Element of G
          st x in H
          holds phi.x in H)
         implies H is characteristic
    proof
      assume B1: for phi being Automorphism of G
                 for x being Element of G st x in H holds phi.x in H;
      for phi being Automorphism of G holds Image(phi|H) is Subgroup of H
      proof
        let phi be Automorphism of G;
        for x being Element of H holds phi.x in H
        proof
          let x be Element of H;
          reconsider g=x as Element of G by GROUP_2:42;
          g in H;
          hence thesis by B1;
        end;
        hence Image(phi|H) is Subgroup of H by Th44;
      end;
      hence H is characteristic by Th40;
    end;
  end;
```

This code is used in chunk 47b.
Defines:
Th50, never used.

Theorem 1.51. *If $H \leq G$ and $K \leq G$ are strict characteristic subgroups, then $H \cap K$ is a characteristic subgroup.*

Remark 1.51.1. Although we don't use this result in this article, it is important in other settings.

Proof sketch. For any $x \in H \cap K$ and automorphism $\varphi \in \mathrm{Aut}(G)$, we have $\varphi(x) \in H$ and $\varphi(x) \in K$, hence $\varphi(x) \in H \cap K$. Since x was arbitrary, this establishes $\varphi(H \cap K) \leq H \cap K$, which implies $H \cap K$ is characteristic. □

74 ⟨*Theorem: $H, K \leq G$ characteristic implies $H \cap K$ characteristic* 74⟩≡

```
  theorem Th51:
    for G being Group
    for H,K being strict characteristic Subgroup of G
    holds H /\ K is characteristic Subgroup of G
```

```
proof
  let G be Group;
  let H,K be strict characteristic Subgroup of G;
  for phi being Automorphism of G
  for x being Element of G st x in H /\ K
  holds phi.x in H /\ K
  proof
    let phi be Automorphism of G;
    let x be Element of G;
    assume x in H /\ K;
    then B1: x in H & x in K by GROUP_2:82;
    then B2: phi.x in H by Th50;
    phi.x in K by B1,Th50;
    hence phi.x in H /\ K by B2, GROUP_2:82;
  end;
  hence H /\ K is characteristic Subgroup of G by Th50;
end;
```

This code is used in chunk 47b.
Defines:
Th51, never used.

Theorem 1.52. *If $H \leq G$ and $K \leq G$ are characteristic subgroups, then $\langle H, K\rangle$ is a characteristic subgroup of G.*

Remark 1.52.1. More generally, if $\{K_i\}_{i\in I}$ is any family of characteristic subgroups of G, then their join $\langle K_i\rangle_{i\in I}$.

Proof sketch. This amounts to showing the product of subsets $U(H)U(K)$ is stable under automorphisms of G, then it generates a characteristic subgroup of G. □

75 ⟨*Theorem: $H, K \leq G$ characteristic implies $\langle H, K\rangle$ is characteristic* 75⟩≡

```
theorem Th52:
  for G being Group
  for H,K being strict characteristic Subgroup of G
  holds H "\/" K is characteristic Subgroup of G
proof
  let G be Group;
  let H,K be strict characteristic Subgroup of G;

  for phi being Automorphism of G
  for g being Element of G st g in H "\/" K
  holds phi.g in H "\/" K
  proof
    let phi be Automorphism of G;
    let g be Element of G;
    assume g in H "\/" K;
    then g in H*K by GROUP_4:53;
    then consider h, k being Element of G such that
    B1: g = h*k and
    B2: h in carr H and
    B3: k in carr K;
    h in H by B2;
    then B4: phi.h in H by Th50;
    k in K by B3;
```

```
      then phi.k in K by Th50;
      then phi.h * phi.k in carr H*carr K by B4;
      then phi.g in H*K by B1,GROUP_6:def 6;
      hence phi.g in H "\/" K by GROUP_4:53;
    end;

    hence H "\/" K is characteristic Subgroup of G by Th50;
  end;
```

This code is used in chunk 47b.
Defines:
Th52, never used.

Theorem 1.53. *If $H \leq G$ and $K \leq G$ are characteristic, then the set of commutators $\{[h,k] \in G \mid h \in H, k \in K\}$ is invariant under automorphisms of G.*

Proof outline. We prove equality by showing $\text{Commutators}(H,K) \subseteq \varphi(\text{Commutators}(H,K))$ and $\text{Commutators}(H,K) \supseteq \varphi(\text{Commutators}(H,K))$, which proves equality. □

76a ⟨*Theorem:* $H, K \leq G$ *characteristic implies* $\text{Commutators}(H,K)$ *is stable* 76a⟩≡

```
  theorem Th53:
    for G being Group
    for H,K being strict characteristic Subgroup of G
    for phi being Automorphism of G
    holds phi .: commutators(H,K) = commutators(H,K)
  proof
    let G be Group;
    let H,K be strict characteristic Subgroup of G;
    let phi be Automorphism of G;
    A1: dom phi = the carrier of G by FUNCT_2:def 1;

    for x being object st x in commutators(H,K) holds x in phi .: commutators(H,K)
    ⟨Proof: Commutators(H,K) ⊆ φ(Commutators(H,K)) 76b⟩
    then A2: commutators(H,K) c= phi .: commutators(H,K);

    for y being object st y in phi .: commutators(H,K) holds y in commutators(H,K)
    ⟨Proof: Commutators(H,K) ⊇ φ(Commutators(H,K)) 77a⟩
    then phi .: commutators(H,K) c= commutators(H,K);
    hence phi .: commutators(H,K) = commutators(H,K) by A2,XBOOLE_0:def 10;
  end;
```

This code is used in chunk 47b.
Defines:
Th53, never used.

Proof step ($\text{Commutators}(H,K) \subseteq \varphi(\text{Commutators}(H,K))$*).* We show $x \in \text{Commutators}(H,K)$ looks like $x = [h,k]$ for some $h \in H$ and $k \in K$. But then given an automorphism $\varphi \in \text{Aut}(G)$, we can find $a = \varphi^{-1}(h) \in H$ and $b = \varphi^{-1}(k) \in K$ since H and K are characteristic subgroups. Then $[a,b] \in [H,K]$ and moreover $\varphi([a,b]) = [h,k]$ which proves the claim. □

76b ⟨*Proof:* $\text{Commutators}(H,K) \subseteq \varphi(\text{Commutators}(H,K))$ 76b⟩≡

```
  proof
    let x be object;
    assume B0: x in commutators(H,K);
```

```
    then reconsider g=x as Element of G;
    consider h,k being Element of G such that
    B1: x = [.h,k.] and
    B2: h in H & k in K by B0,GROUP_5:52;
    reconsider psi = phi" as Automorphism of G by GROUP_6:62;
    set a = psi.h;
    set b = psi.k;
    B3: a in H & b in K by B2,Th50;
    B4: psi.x = psi.([.h,k.]) by B1
             .= [.psi.h,psi.k.] by GROUP_6:34
             .= [.a,b.];
    B5: phi.([. a,b .]) = phi.(psi.x) by B4
                        .= g by Th4;
    [. a, b .] in commutators(H,K) by B3;
    hence x in phi .: commutators(H,K) by B5,A1,FUNCT_1:def 6;
  end;
```

This code is used in chunk 76a.

*Proof step (*Commutators$(H, K) \supseteq \varphi($Commutators$(H, K))$*).* We begin with $y \in \varphi(\text{Commutators}(H, K))$, which means there is some $x \in \text{Commutators}(H, K)$ such that $y = \varphi(x)$. Then there is some $h \in H$, $k \in K$ such that $x = [h, k]$. Since H and K are characteristic subgroups, $\varphi(h) \in H$ and $\varphi(k) \in K$. Then $\varphi(x) = [\varphi(h), \varphi(k)] \in \text{Commutators}(H, K)$ which proves the claim. □

77a ⟨*Proof:* Commutators$(H, K) \supseteq \varphi($Commutators$(H, K))$ 77a⟩≡

```
  proof
    let y be object;
    assume y in phi .: commutators(H,K);
    then consider x being object such that
    B2: x in dom phi & x in commutators(H,K) & y = phi.x
    by FUNCT_1:def 6;
    consider h,k being Element of G such that
    B3: x = [.h,k.] and
    B4: h in H & k in K by B2,GROUP_5:52;
    B5: phi.h in H & phi.k in K by B4,Th50;
    phi.x = phi.([. h,k .]) by B3
         .= [. phi.h, phi.k .] by GROUP_6:34;
    hence y in commutators(H,K) by B2,B5;
  end;
```

This code is used in chunk 76a.

Theorem 1.54. *If $H \leq G$ and $K \leq G$ are characteristic, then the commutator subgroup $[H, K]$ is a characteristic subgroup.*

Proof sketch. We use the fact $\varphi([H, K]) = [\varphi(H), \varphi(K)]$, then since H and K are characteristic the result follows immediately. □

77b ⟨*Theorem: $H, K \leq G$ characteristic implies $[H, K]$ is characteristic* 77b⟩≡

```
  theorem Th54:
    for G being Group
    for H,K being strict characteristic Subgroup of G
    holds [.H,K.] is characteristic Subgroup of G
  proof
```

```
    let G be Group;
    let H,K be strict characteristic Subgroup of G;
    set A = commutators(H,K);
    reconsider A as non empty Subset of G by GROUP_5:53;
    for phi being Automorphism of G holds phi .: A = A by Th53;
    hence [.H,K.] is characteristic Subgroup of G by Th45;
  end;
```

This code is used in chunk 47b.
Defines:
`Th54`, never used.

9. Meets of Families of Subgroups

78a ⟨*Meets of families of subgroups* 78a⟩≡
⟨*Scheme:* $\bigcap \mathcal{F}$ *is minimal* 78b⟩

⟨*Theorem:* $H_1 \leq H_2 \leq G$ *and* $a \in G$ *implies* ${H_1}^a \leq {H_2}^a$ 79⟩

⟨*Scheme:* $\bigcap\{N \trianglelefteq G \mid P[N]\} \trianglelefteq G$ 80⟩

⟨*Theorem: Meet of family of normal subgroups is normal* 82⟩

This code is used in chunk 8b.

Scheme 1.3. *If we have some group G and some family of subgroups defined by some unary predicate $\mathcal{F} = \{H \leq G \mid P[H]\}$, then there exists a group obtained by their meet $H_{min} = \bigcap \mathcal{F}$ such that for any $K \leq G$ satisfying $P[K]$ has a subgroup $H \leq K$.*

Proof outline. There are two steps to this proof: first, we prove that $\bigcap \mathcal{F}$ really is a group (thanks to [Group_4:sch1]. Second, we prove that $\bigcap \mathcal{F}$ really is minimal. This is because for any $K \leq G$ satisfying $P[K]$, we have its underlying set $U(K)$ contain the underlying set of $\bigcap \mathcal{F}$. Thus K must contain the meet as a subgroup, establishing $\bigcap \mathcal{F}$ is minimal. □

78b ⟨*Scheme:* $\bigcap \mathcal{F}$ *is minimal* 78b⟩≡

```
scheme :: sch3
  MeetIsMinimal{G() -> Group, P[set]} :
  ex H being strict Subgroup of G() st
  the carrier of H = meet {A where A is Subset of G() :
                           ex K being strict Subgroup of G()
                           st A = the carrier of K & P[K]} &
  (for K being strict Subgroup of G() st P[K] holds H is Subgroup of K)
provided
A1: ex H being strict Subgroup of G() st P[H]
proof
  set Fam = {A where A is Subset of G() : ex H being strict Subgroup of G()
                                          st A = the carrier of H & P[H]};
  consider H being strict Subgroup of G() such that
A2: the carrier of H = meet {A where A is Subset of G() :
                             ex K being strict Subgroup of G()
                             st A = the carrier of K & P[K]}
  from GROUP_4:sch 1(A1);
```

```
    take H;
    for K being strict Subgroup of G() st P[K] holds H is Subgroup of K
    proof
      let K be strict Subgroup of G();
      assume P[K];
      then carr K in Fam;
      hence H is Subgroup of K by A2,GROUP_2:57,SETFAM_1:3;
    end;
    hence thesis by A2;
  end;
```

This code is used in chunk 78a.
Defines:
`MeetIsMinimal`, never used.

Theorem 1.55. *Let G be a group, let $H_1 \leq G$ and $H_2 \leq G$ be subgroups. If $H_1 \leq H_2$ and $a \in G$ is an arbitrary element, then the conjugates-by-a are subgroups too: ${H_1}^a \leq {H_2}^a$.*

Proof outline. The key to this proof amounts to observing any $h \in G$ such that $h \in {H_1}^a$, we find $h \in {H_2}^a$. We can claim this by having $g \in G$ such that $h = g^a$. But then $g \in H_1$ and moreover $g \in H_2$, which implies $h \in {H_2}^a$. Then the result follows from Theorem [GROUP_2:Th57]. □

79 ⟨*Theorem: $H_1 \leq H_2 \leq G$ and $a \in G$ implies ${H_1}^a \leq {H_2}^a$* 79⟩≡

```
  theorem Th55:
    for G being Group
    for H1,H2 being Subgroup of G
    st H1 is Subgroup of H2
    for a being Element of G
    holds H1 |^ a is Subgroup of H2 |^ a
  proof
    let G be Group;
    let H1,H2 be Subgroup of G;
    assume A1: H1 is Subgroup of H2;
    let a be Element of G;
    for h being Element of G st h in H1 |^ a holds h in H2 |^ a
    proof
      let h be Element of G;
      assume h in H1 |^ a;
      then consider g being Element of G such that
      B1: h = g |^ a & g in H1
      by GROUP_3:58;
      g in H2 by A1,B1,GROUP_2:40;
      hence thesis by B1,GROUP_3:58;
    end;
    hence H1 |^ a is Subgroup of H2 |^ a by GROUP_2:58;
  end;
```

This code is used in chunk 78a.
Defines:
`Th55`, never used.

Scheme 1.4. *Let G be a group, $P[-]$ an arbitrary unary predicate. If $\mathcal{F} = \{N \trianglelefteq G \mid P[N]\}$ is a family of normal subgroup of G satisfying $P[N]$, then their meet $\bigcap \mathcal{F}$ is a normal subgroup of G.*

80 ⟨*Scheme:* $\bigcap\{N \trianglelefteq G \mid P[N]\} \trianglelefteq G$ 80⟩≡

```
scheme :: sch4
  MeetOfNormsIsNormal{G() -> Group, P[set]} :
  for H being strict Subgroup of G()
  st the carrier of H = meet {A where A is Subset of G() :
                              ex N being strict Subgroup of G()
                              st A = the carrier of N & N is normal & P[N]}
  holds H is strict normal Subgroup of G()
provided
A1: ex H being strict normal Subgroup of G() st P[H]
proof
  defpred IsNorm[Subgroup of G()] means $1 is normal Subgroup of G();
  set Fam = {A where A is Subset of G() : ex N being strict Subgroup of G()
                                          st A = the carrier of N &
                                             N is normal & P[N]};
  let H be strict Subgroup of G();
  assume A2: the carrier of H = meet Fam;
  A3: Fam <> {}
  proof
    consider N being strict normal Subgroup of G() such that
    B1: P[N]
    by A1;
    carr N in Fam by B1;
    hence thesis;
  end;
  A4: for N being strict normal Subgroup of G() st P[N] holds H is Subgroup of N
  proof
    let N be strict normal Subgroup of G();
    assume P[N];
    then carr N in Fam;
    hence H is Subgroup of N by A2,GROUP_2:57,SETFAM_1:3;
  end;
  A5: for N being strict normal Subgroup of G() st carr N in Fam holds P[N]
  proof
    let N be strict normal Subgroup of G();
    assume B1: carr N in Fam;
    consider A being Subset of G() such that
    B2: A = carr N;
    consider A0 being Subset of G() such that
    B3: A = A0 and
    B4: ex H0 being strict Subgroup of G()
        st A0 = the carrier of H0 & H0 is normal & P[H0]
    by B1,B2;
    consider H0 being strict Subgroup of G() such that
    B5: A0 = the carrier of H0 & H0 is normal & P[H0]
    by B4;
    thus P[N] by B2,B3,B5,GROUP_2:59;
  end;
  A6: for a being Element of G()
  for N being strict normal Subgroup of G() st carr N in Fam
  holds H |^ a is Subgroup of N
  proof
    let a be Element of G();
```

```
  let N be strict normal Subgroup of G();
  assume carr N in Fam;
  then H is Subgroup of N by A4,A5;
  then H |^ a is Subgroup of N |^ a by Th55;
  hence H |^ a is Subgroup of N by GROUP_3:def 13;
end;
A7: for a being Element of G()
for N being strict normal Subgroup of G() st carr N in Fam
holds carr(H |^ a) c= carr N
proof
  let a be Element of G();
  let N be strict normal Subgroup of G();
  assume carr N in Fam;
  then H |^ a is Subgroup of N by A6;
  hence carr(H |^ a) c= carr N by GROUP_2:def 5;
end;

for a being Element of G() holds H |^ a is Subgroup of H
proof
  let a be Element of G();
  B1: for A being Subset of G() st A in Fam holds carr(H |^ a) c= A
  proof
    let A be Subset of G();
    assume A in Fam;
    then consider A0 being Subset of G() such that
    C1: A = A0 and
    C2: ex H0 being strict Subgroup of G()
        st A0 = the carrier of H0 & H0 is normal & P[H0];
    consider H0 being strict Subgroup of G() such that
    C3: A0 = the carrier of H0 & H0 is normal & P[H0]
    by C2;
    reconsider H0 as strict normal Subgroup of G() by C3;
    carr H0 in Fam by C3;
    hence carr(H |^ a) c= A by A7,C1,C3;
  end;
  for x being object st x in carr (H |^ a) holds x in meet Fam
  proof
    let x be object;
    assume C1: x in carr(H |^ a);
    for A being set st A in Fam holds x in A
    proof
      let A be set;
      assume C2: A in Fam;
      then consider A0 being Subset of G() such that
      C3: A0 = A and
          ex H0 being strict Subgroup of G()
          st A0 = the carrier of H0 & H0 is normal & P[H0];
      carr(H |^ a) c= A0 by C2,C3,B1;
      hence thesis by C1,C3;
    end;
    hence thesis by A3,SETFAM_1:def 1;
  end;
  then carr (H |^ a) c= meet Fam;
```

```
    hence thesis by A2,GROUP_2:57;
  end;
  hence thesis by GROUP_3:122;
end;
```

This code is used in chunk 78a.
Defines:
`MeetOfNormsIsNormal`, never used.

Theorem 1.56. *Let G be a group, $\mathcal{X}$ be a finite collection of normal subgroups of G. If $\mathcal{X} \neq \emptyset$, then there exists a normal subgroup $N \trianglelefteq G$ such that $N = \bigcap \mathcal{X}$.*

Remark 1.56.1. Note, unlike the previous scheme, this is a theorem and can be used in conjunction with other theorems in justifying a claim.

82 ⟨*Theorem: Meet of family of normal subgroups is normal* 82⟩≡

```
theorem Th56:
  for G being Group
  for X being finite set
  st X <> {} & (for A being Element of X
                ex N being strict normal Subgroup of G
                st A = the carrier of N)
  ex N being strict normal Subgroup of G
  st the carrier of N = meet X
proof
  let G be Group;
  let X be finite set;
  assume A1: X <> {};
  assume A2: for A being Element of X
             ex N being strict normal Subgroup of G
             st A = the carrier of N;
  defpred P[Group] means $1 is normal Subgroup of G & the carrier of $1 in X;
  set Fam = {A where A is Subset of G : ex N being strict Subgroup of G
                                        st A = the carrier of N & P[N]};
  set Fam2 = {A where A is Subset of G : ex N being strict Subgroup of G
                                         st A = the carrier of N &
                                         N is normal & P[N]};
  A3: ex H being strict Subgroup of G st P[H]
  proof
    consider A being object such that
    B1: A in X by A1,XBOOLE_0:def 1;
    reconsider A as Element of X by B1;
    consider H being strict normal Subgroup of G such that
    B2: A = the carrier of H
    by A2;
    take H;
    thus P[H] by B1,B2;
  end;

  consider N being strict Subgroup of G such that
  A4: the carrier of N = meet Fam
  from GROUP_4:sch 1(A3);

  for A being object holds A in Fam iff A in Fam2
  proof
```

```
  let A be object;
  thus A in Fam implies A in Fam2
  proof
    assume A in Fam;
    then consider A0 being Subset of G such that
    B1: A = A0 and
    B2: ex N being strict Subgroup of G st A0 = the carrier of N & P[N];

    consider N being strict Subgroup of G such that
    B3: A0 = the carrier of N & P[N]
    by B2;
    thus A in Fam2 by B1,B3;
  end;
  thus A in Fam2 implies A in Fam
  proof
    assume A in Fam2;
    then consider A0 being Subset of G such that
    B1: A = A0 &
        ex N being strict Subgroup of G
        st A0 = the carrier of N & N is normal & P[N];
    thus A in Fam by B1;
  end;
end;
then A5: Fam = Fam2 by TARSKI:2;

A6: ex H being strict normal Subgroup of G st P[H] by A3;
for H being strict Subgroup of G st the carrier of H = meet Fam2
holds H is strict normal Subgroup of G
from MeetOfNormsIsNormal(A6);
then reconsider N as strict normal Subgroup of G by A4,A5;
take N;

for A being object holds A in Fam iff A in X
proof
  let A be object;
  thus A in Fam implies A in X
  proof
    assume A in Fam;
    then consider A0 being Subset of G such that
    B1: A = A0 &
        ex N being strict Subgroup of G st A0 = the carrier of N & P[N];
    thus thesis by B1;
  end;
  thus A in X implies A in Fam
  proof
    assume B1: A in X;
    then consider N being strict normal Subgroup of G such that
    B2: A = the carrier of N
    by A2;
    A is Subset of G by B2,GROUP_2:def 5;
    hence A in Fam by B1,B2;
  end;
end;
```

```
    hence the carrier of N = meet X by A4,TARSKI:2;
  end;
```

This code is used in chunk 78a.
Defines:
`Th56`, never used.

10. Centralizers of Characteristic Subgroups

84 ⟨*Centralizers of Characteristic Subgroups* 84⟩≡
⟨*Definition: Centralizer of Subset* 85⟩

⟨*Theorem:* $A \subseteq G$ *and* $g \in G$*, have* $g \in C_G(A) \iff (\forall a \in A, ga = ag)$ 88a⟩

⟨*Theorem:* $A \subseteq B \subseteq G \implies C_G(B) \leq C_G(A)$ 88b⟩

⟨*Definition: Centralizer of Subgroup* 89a⟩

⟨*Theorem: carrier of* $C_G(H) = \{b \in G \mid \forall a \in H, ba = ab\}$ 89b⟩

⟨*Theorem: Let* $g \in G$*. Then* $g \in C_G(H) \iff \forall h \in H, gh = hg$ 91a⟩

⟨*Theorem:* $A \subseteq G \implies A \subseteq C_G(C_G(A))$ 91b⟩

⟨*Theorem: Centralizer of characteristic subgroups is characteristic* 92⟩

⟨*Definition:* $\forall a \in G$*,* $\{a\} \subseteq G$ 93a⟩

⟨*Theorem:* $\{x\} = \{y\} \iff x = y$ 93c⟩

⟨*Definition: Normalizer of group element* 93b⟩

⟨*Theorem:* $h \in N_G(a) \iff a^h = a$ 94a⟩

⟨*Theorem:* $A \subseteq G$*,* $C_G(A) = \bigcap_{a \in A} N_G(a)$ 94b⟩

⟨*Theorem:* $|H_1 \cap H_2| = |H_1| = |H_2| \implies H_1 = H_2$ 96⟩

⟨*Theorem:* $\forall a, b, c \in \mathbb{N}, c \neq 0 \wedge c|a \wedge c|b \implies a|b$ 97a⟩

⟨*Theorem:* $a, b, c \in \mathbb{N}, b|c \wedge \gcd(ab, c) = 1 \implies b = 1$ 97b⟩

⟨*Theorem:* $G_1/N_1 \cong G_2/N_2 \implies |N_2| \cdot |G_1| = |N_1| \cdot |G_2|$ 98a⟩

⟨*Theorem:* $K, N \trianglelefteq G \implies |KN| \cdot |K \cap N| = |K| \cdot |N|$ 98b⟩

⟨*Theorem:* $N \trianglelefteq G$ *with* $|N|$ *and* $[G : N]$ *coprime implies* N *is characteristic* 99⟩

⟨*Theorem:* $f_2(f_1(A)) = (f_2 \circ f_1)(A)$ *for group morphisms* 100⟩

⟨*Theorem:* $\varphi \in \mathrm{Aut}(G)$*,* $\varphi(N) = N$*,* $\exists \sigma \in \mathrm{Aut}(G/N), \sigma(xN) = \varphi(x)N$ 101⟩

⟨*Theorem:* H *char* G *and* $H \leq K \leq G$*, then* $H \trianglelefteq K$ 105⟩

⟨*Theorem:* $H \leq K \leq G$, H *char* G, K/H *char* G/H *implies* K *is characteristic* 106⟩

⟨*Theorem:* $H \leq G$, $H \leq C_G(H) \iff H$ *is commutative* 109⟩

⟨*Theorem:* $C_G(G) = Z(G)$ 110⟩

⟨*Theorem:* $N \trianglelefteq G \implies C_G(H) \trianglelefteq G$ 111⟩

⟨*Theorem:* $\forall h \in H, n \in N_G(H), n^{-1}hn \in H$ 112a⟩

⟨*Theorem:* $\forall H \leq G, H \leq N_G(H)$ 112b⟩

⟨*Lemma:* $C_G(H) \leq N_G(H)$ 114a⟩

⟨*Theorem:* $C_G(H) \trianglelefteq N_G(H)$ 115⟩

This code is used in chunk 8b.

Definition 1.4. Let G be a group, let $A \subseteq G$ be a subset of G. We define the **"Centralizer"** of A to be the subgroup of G given by

$$C_G(A) = \{g \in G \mid \forall a \in A, ag = ga\}. \tag{10.1}$$

Remark 1.4.1. We not only need to prove the existence of centralizers, but also the uniqueness (since we speak of *the* centralizer of A).

Remark 1.4.2. Note that [WeddWitt] defines the centralizer of a group *element*, but nothing further (well, nothing further about group centralizers).

Proof sketch of existence. Basically, we have four steps to proving the existence of a centralizer subgroup $C_G(A)$:

(1) it contains the identity element $1_G \in C_G(A)$;
(2) its carrier is a subset of G, $C_G(A) \subseteq G$;
(3) it is closed under the group operation;
(4) it is closed under inversion.

Then from these claims, it follows $C_G(A)$ is a subgroup. □

Proof sketch of uniqueness. Suppose we have two subgroups $H_1 \leq G$ and $H_2 \leq G$ satisfying the definition of being a centralizer of A. Then $H_1 = H_2$ since they contain the same elements. □

85 ⟨*Definition: Centralizer of Subset* 85⟩≡

```
definition
  let G be Group;
  let A be Subset of G;
  func Centralizer A -> strict Subgroup of G means
  :Def4:
  the carrier of it = { b where b is Element of G :
                        for a being Element of G st a in A holds a*b = b*a };
  existence
  proof
    set Car = {b where b is Element of G :
               for a being Element of G st a in A holds a*b = b*a };
    C1: 1_G in Car
    ⟨Proof: 1_G ∈ C_G(A) 86b⟩
```

```
    for x being object st x in Car holds x in the carrier of G
    ⟨Proof: ∀x, x ∈ C_G(A) ⟹ x ∈ G 86a⟩
    then C2: Car is Subset of G by TARSKI:def 3;

    C3: for g1,g2 being Element of G st g1 in Car & g2 in Car
    holds g1*g2 in Car
    ⟨Proof: C_G(A) closed under multiplication 87a⟩

    C4: for g being Element of G st g in Car holds g" in Car
    ⟨Proof: ∀g ∈ C_G(A), g^-1 ∈ C_G(A) 87b⟩

    thus thesis by C1,C2,C3,C4,GROUP_2:52;
  end;
  uniqueness
  proof
    let H1,H2 be strict Subgroup of G such that
A1: the carrier of H1 = {b where b is Element of G : for a being Element of G
                                                     st a in A
                                                     holds a*b = b*a } and
A2: the carrier of H2 = {b where b is Element of G : for a being Element of G
                                                     st a in A
                                                     holds a*b = b*a };
    for g being Element of G holds g in H1 iff g in H2 by A1,A2;
    hence thesis;
  end;
end;
```

This code is used in chunk 84.
Defines:
`Centralizer`, never used.
`Def4`, never used.

86a ⟨*Proof:* $\forall x, x \in C_G(A) \implies x \in G$ 86a⟩≡

```
proof
  let x be object;
  assume x in Car;
  then ex g being Element of G
       st (x = g) & (for a being Element of G st a in A holds a*g = g*a);
  hence thesis;
end;
```

This code is used in chunk 85.

86b ⟨*Proof:* $1_G \in C_G(A)$ 86b⟩≡

```
proof
  for a being Element of G st a in A holds 1_G*a = a*1_G
  proof
    let a be Element of G;
    assume a in A;
    1_G*a = a by GROUP_1:def 4
        .= a*1_G by GROUP_1:def 4;
    hence thesis;
  end;
```

```
    hence thesis;
  end;
```

This code is used in chunk 85.

87a ⟨*Proof:* $C_G(A)$ *closed under multiplication* 87a⟩≡

```
  proof
    let g1,g2 be Element of G;
    assume B1: g1 in Car;
    assume B2: g2 in Car;
    B3: ex z1 being Element of G st (z1 = g1) & (for a being Element of G
    st a in A holds a*z1 = z1*a) by B1;
    B4: ex z2 being Element of G st (z2 = g2) & (for a being Element of G
    st a in A holds a*z2 = z2*a) by B2;
    for a being Element of G st a in A holds a*(g1*g2)=(g1*g2)*a
    proof
      let a be Element of G;
      assume Z1: a in A;
      a*(g1*g2) = (a*g1)*g2 by GROUP_1:def 3
               .= (g1*a)*g2 by Z1,B3
               .= g1*(a*g2) by GROUP_1:def 3
               .= g1*(g2*a) by Z1,B4
               .= g1*g2*a by GROUP_1:def 3;
      hence thesis;
    end;
    hence thesis;
  end;
```

This code is used in chunk 85.

87b ⟨*Proof:* $\forall g \in C_G(A), g^{-1} \in C_G(A)$ 87b⟩≡

```
  proof
    let g be Element of G;
    assume g in Car;
    then Z1: ex z1 being Element of G st (z1 = g) & (for a being
    Element of G st a in A holds z1*a=a*z1);
    for a being Element of G st a in A holds g" * a = a * g"
    proof
      let a be Element of G;
      assume a in A;
      then g" * ((a*g) * g") = g" * ((g*a) * g") by Z1
                           .= (g" * (g * a)) * g" by GROUP_1:def 3
                           .= ((g" * g) * a) * g"  by GROUP_1:def 3
                           .= (1_G * a) * g"  by GROUP_1:def 5
                           .= a * g"  by GROUP_1:def 4;
      hence g" * a = a * g" by GROUP_3:1;
    end;
    hence thesis;
  end;
```

This code is used in chunk 85.

Theorem 1.57. *Let G be a group, $A \subseteq G$ be any subset, $g \in G$ be any group element. We have $g \in C_G(A)$ if and only if for any $a \in A$, $ag = ga$.*

Remark 1.57.1. This allows us to use the fact that $g \in C_G(A)$ and $a \in A$ implies $ag = ga$.

88a ⟨*Theorem:* $A \subseteq G$ *and* $g \in G$*, have* $g \in C_G(A) \iff (\forall a \in A, ga = ag)$ 88a⟩≡

```
theorem Th57:
  for G being Group
  for A being Subset of G
  for g being Element of G
  holds (for a being Element of G st a in A holds g*a = a*g) iff
        g is Element of Centralizer A
proof
  let G be Group;
  let A be Subset of G;
  let g be Element of G;
A1: the carrier of Centralizer A = {b where b is Element of G : for a
  being Element of G st a in A holds b*a=a*b} by Def4;
  hereby
    assume for a being Element of G st a in A holds g*a = a*g;
    then g in the carrier of Centralizer A by A1;
    hence g is Element of Centralizer A;
  end;
  assume g is Element of Centralizer A;
  then g in the carrier of Centralizer A;
  then ex b being Element of G st (b = g) & (for a being Element of G st a in A
  holds b*a = a*b) by A1;
  hence thesis;
end;
```

This code is used in chunk 84.
Defines:
Th57, never used.

Theorem 1.58. *Let* G *be a group, let* $A \subseteq B \subseteq G$ *be subsets. Then* $C_G(B) \leq C_G(A)$.

88b ⟨*Theorem:* $A \subseteq B \subseteq G \implies C_G(B) \leq C_G(A)$ 88b⟩≡

```
theorem Th58:
  for G being Group
  for A,B being Subset of G
  st A c= B
  holds Centralizer B is Subgroup of Centralizer A
proof
  let G be Group;
  let A,B be Subset of G;
  assume A1: A c= B;
  for g being Element of G st g in Centralizer B
  holds g in Centralizer A
  proof
    let g be Element of G;
    assume g in Centralizer B;
    then for a being Element of G st a in A
    holds g*a = a*g by A1,Th57;
    then g is Element of Centralizer A by Th57;
    hence thesis;
  end;
  hence Centralizer B is Subgroup of Centralizer A by GROUP_2:58;
end;
```

This code is used in chunk 84.
Defines:
Th58, never used.

Definition 1.5. Let G be a group, $H \leq G$ be a subgroup. We define the **"Centralizer"** of H is the subgroup whose underlying set is

$$C_G(H) = \{g \in G \mid \forall h \in H, hg = gh\}. \tag{10.2}$$

Remark 1.5.1. This basically amounts to Definition 1.4 applied to the underlying set of a subgroup of G. The proofs of existence and uniqueness carry over.

Remark 1.5.2. We also follow Mizar's example in Definition [GROUP_3:def15] of the normalizer of $H \leq G$, based off the Definition [GROUP_3:def14] of the normalizer for a subset $A \subseteq G$. Consequently we only need a `correctness;` assertion. This is briefly mentioned at the very end of §2 of "Mizar in a nutshell".

89a ⟨*Definition: Centralizer of Subgroup* 89a⟩≡

```
definition
  let G be Group;
  let H be Subgroup of G;
  func Centralizer H -> strict Subgroup of G means
  :Def5:
  it = Centralizer carr H;
  correctness;
end;
```

This code is used in chunk 84.
Defines:
Def5, never used.

Theorem 1.59. *Let $H \leq G$. Then the set underlying $C_G(H)$ is precisely $\{b \in G \mid \forall a \in H, ba = ab\}$.*

Remark 1.59.1. This may seem silly and redundant, but we need to explicitly spell out what the underlying set of the centralizer for a subgroup *is*, if we want to use it later.

Proof outline. There are two steps to the proof. First, we prove $C_G(H) \subseteq \{b \in G \mid \forall a \in H, ba = ab\}$. Next we prove $\{b \in G \mid \forall a \in H, ba = ab\} \subseteq C_G(H)$. The result follows. □

89b ⟨*Theorem: carrier of* $C_G(H) = \{b \in G \mid \forall a \in H, ba = ab\}$ 89b⟩≡

```
theorem Th59:
  for G being Group
  for H being Subgroup of G
  holds the carrier of Centralizer H = {b where b is Element of G : for a
  being Element of G st a in H holds b*a=a*b}
proof
  let G be Group;
  let H be Subgroup of G;
  set A = carr H;
  set Car = {b where b is Element of G : for a being Element of G st a in H
                                         holds b*a=a*b};

  A1: the carrier of Centralizer A = {b where b is Element of G : for a
```

```
    being Element of G st a in A holds b*a=a*b} by Def4;
    for x being object st x in Car holds x in the carrier of Centralizer H
    proof
      let x be object;
      assume B1: x in Car;
      ex b being Element of G
      st (x = b) & (for a being Element of G st a in carr(H) holds b*a=a*b)
      proof
        consider b being Element of G such that
        B2: x = b and
        B3: for a being Element of G st a in H holds b*a=a*b
        by B1;
        for a being Element of G st a in carr H holds b*a=a*b
        proof
          let a be Element of G;
          assume a in carr H;
          then a in H;
          hence b*a=a*b by B3;
        end;
        hence thesis by B2;
      end;
      then x in the carrier of Centralizer carr H by A1;
      hence thesis by Def5;
    end;
    then A3: Car c= the carrier of Centralizer H;

    for x being object st x in the carrier of Centralizer H holds x in Car
    proof
      let x be object;
      assume x in the carrier of Centralizer H;
      then B1: x in the carrier of Centralizer carr H by Def5;
      ex b being Element of G
      st (x=b) & (for a being Element of G st a in H holds b*a=a*b)
      proof
        consider b being Element of G such that
        Z1: x = b  & (for a being Element of G st a in carr H holds b*a=a*b)
        by A1,B1;
        for a being Element of G st a in H holds b*a=a*b by Z1;
        hence thesis by Z1;
      end;
      hence x in Car;
    end;
    then the carrier of Centralizer H c= Car;
    hence thesis by A3,XBOOLE_0:def 10;
  end;
```

This code is used in chunk 84.
Defines:
Th59, never used.

Theorem 1.60. *Let $H \leq G$ and $g \in G$. Then $g \in C_G(H)$ if and only if for any $a \in H$ we have $ga = ag$.*

Proof sketch. This boils down to relying on previous results for the centralizer of the set underlying H. □

91a ⟨*Theorem: Let* $g \in G$. *Then* $g \in C_G(H) \iff \forall h \in H, gh = hg$ 91a⟩≡

```
theorem Th60:
  for G being Group
  for H being Subgroup of G
  for g being Element of G
  holds (for a being Element of G st a in H holds g*a = a*g) iff
        g is Element of Centralizer H
proof
  let G be Group;
  let H be Subgroup of G;
  let g be Element of G;
A1: the carrier of Centralizer H = {b where b is Element of G : for a
  being Element of G st a in H holds b*a=a*b} by Th59;
  hereby
    assume for a being Element of G st a in H holds g*a = a*g;
    then g in the carrier of Centralizer H by A1;
    hence g is Element of Centralizer H;
  end;
  assume g is Element of Centralizer H;
  then g in the carrier of Centralizer H;
  then ex b being Element of G st (b = g) & (for a being Element of G st a in H
  holds b*a = a*b) by A1;
  hence thesis;
end;
```

This code is used in chunk 84.
Defines:
Th60, never used.

Theorem 1.61. *Let* $A \subseteq G$ *be a subset of a group. Then* $A \subseteq C_G(C_G(A))$.

91b ⟨*Theorem:* $A \subseteq G \implies A \subseteq C_G(C_G(A))$ 91b⟩≡

```
theorem Th61:
  for G being Group
  for A being Subset of G
  holds A is Subset of Centralizer (Centralizer A)
proof
  let G be Group;
  let A be Subset of G;
  set H = Centralizer A;
  for g being object
  st g in A
  holds g in the carrier of Centralizer H
  proof
    let g be object;
    assume B1: g in A;
    then reconsider g as Element of G;
    for h being Element of G st h in H
    holds g*h = h*g by B1,Th57;
    then g is Element of Centralizer H by Th60;
    hence thesis;
  end;
```

```
    then A c= the carrier of Centralizer H;
    hence A is Subset of Centralizer H;
  end;
```

This code is used in chunk 84.
Defines:
Th61, never used.

Theorem 1.62. *Let G be a group, let $K \leq G$ be a characteristic subgroup. Then its centralizer $C_G(K)$ is a characteristic subgroup.*

92 ⟨*Theorem: Centralizer of characteristic subgroups is characteristic* 92⟩≡

```
  theorem Th62:
    for G being Group
    for K being strict characteristic Subgroup of G
    holds (Centralizer K) is characteristic Subgroup of G
  proof
    let G be Group;
    let K be strict characteristic Subgroup of G;
    for phi being Automorphism of G
    for x being Element of G
    st x in Centralizer K
    holds phi.x in Centralizer K
    proof
      let phi be Automorphism of G;
      let x be Element of G;
      assume B1: x in Centralizer K;
      set y = phi.x;
      reconsider psi = phi" as Automorphism of G by GROUP_6:62;
      for k being Element of G st k in K holds y*k = k*y
      proof
        let k be Element of G;
        assume C1: k in K;
        set j = psi.k;
        phi.(x*j) = phi.(j*x) by B1,C1,Th50,Th60
                  .= phi.j * phi.x by GROUP_6:def 6;
        then y * phi.(psi.k) = phi.(psi.k) * y by GROUP_6:def 6
                             .= k * y by Th4;
        hence y * k = k * y by Th4;
      end;
      then y is Element of Centralizer K by Th60;
      hence thesis;
    end;
    hence Centralizer K is characteristic Subgroup of G by Th50;
  end;
```

This code is used in chunk 84.
Defines:
Th62, never used.

Abbreviation 1.26. Let G be a group, let $a \in G$ be any group element. Then the singleton $\{a\}$ is a subset of G.

Remark 1.5.3. Singletons in Mizar seem to be just a "generic set", so this claim is really a *redefinition* of a singleton set to narrow its type to `Subset of G`. This is

necessary for defining the normalizer of a group element (or the centralizer for a group element).

93a ⟨*Definition:* $\forall a \in G$, $\{a\} \subseteq G$ 93a⟩≡

```
definition
  let G be Group;
  let a be Element of G;
  redefine func {a} -> Subset of G;
  coherence
  proof
    for x being object st x in {a}
    holds x in the carrier of G
    proof
      let x be object;
      assume x in {a};
      then x = a by TARSKI:def 1;
      hence thesis;
    end;
    then {a} c= the carrier of G;
    hence {a} is Subset of G;
  end;
end;
```

This code is used in chunk 84.

Abbreviation 1.27. Let G be a group, let $a \in G$. The **"Normalizer of a"** is the strict subgroup of G given by $N_G(\{a\})$.

93b ⟨*Definition: Normalizer of group element* 93b⟩≡

```
definition
  let G be Group;
  let a be Element of G;
  func Normalizer a -> strict Subgroup of G equals
  Normalizer{a};
  correctness;
end;
```

This code is used in chunk 84.

Theorem 1.63. *For any x, y we have $\{x\} = \{y\}$ if and only if $x = y$.*

93c ⟨*Theorem:* $\{x\} = \{y\} \iff x = y$ 93c⟩≡

```
theorem Th63:
  for x,y being object
  holds {x} = {y} iff x = y by ZFMISC_1:3;
```

This code is used in chunk 84.
Defines:
Th63, never used.

Theorem 1.64. *Let G be a group, $a \in G$ an arbitrary group element. We have $x \in N_G(a)$ if and only if there is some $h \in G$ such that $x = h$ and conjugates $a = a^h$.*

94a ⟨*Theorem:* $h \in N_G(a) \iff a^h = a$ 94a⟩≡

```
theorem Th64:
  for G being Group
  for a,x being Element of G
  holds x in Normalizer a iff ex h being Element of G st x = h & a |^ h = a
proof
  let G be Group;
  let a,x be Element of G;
  A1: x in Normalizer{a} iff ex h being Element of G st x = h & {a} |^ h = {a}
  by GROUP_3:129;
  {a} |^ x = {a} |^ {x}
          .= {a |^ x} by GROUP_3:37;
  then x in Normalizer{a} iff a |^ x = a by A1,Th63;
  hence thesis;
end;
```

This code is used in chunk 84.
Defines:
`Th64`, never used.

Theorem 1.65. *Let G be a group and $A \subseteq G$. Then $C_G(A) = \bigcap_{a \in A} N_G(a)$.*

Proof outline. We prove this in two steps. Step one $C_G(A) \subseteq \bigcap_{a \in A} N_G(a)$. Step two $\bigcap_{a \in A} N_G(a) \subseteq C_G(A)$. □

94b ⟨*Theorem:* $A \subseteq G$, $C_G(A) = \bigcap_{a \in A} N_G(a)$ 94b⟩≡

```
theorem Th65:
  for G being Group
  for A being non empty Subset of G
  holds the carrier of Centralizer A = meet {B where B is Subset of G :
  ex H being strict Subgroup of G st B = the carrier of H &
  (ex a being Element of G st a in A & H = Normalizer a)}
proof
  let G be Group;
  let A be non empty Subset of G;
  defpred P[strict Subgroup of G] means (ex a being Element of G
                                          st a in A & $1 = Normalizer a);
  set Fam = {B where B is Subset of G :
  ex H being strict Subgroup of G st B = the carrier of H & P[H]};
  A1: Fam <> {}
  proof
    consider a being object such that
    B1: a in A
    by XBOOLE_0:def 1;
    reconsider a as Element of G by B1;
    consider H being strict Subgroup of G such that
    B2: H = Normalizer a;
    carr H in Fam by B1,B2;
    hence thesis;
  end;
  for x being object st x in the carrier of Centralizer A
  holds x in meet Fam
  ⟨Proof: $\forall x, x \in C_G(A) \implies x \in \bigcap_a N_G(a)$ 95a⟩
  then A2: the carrier of Centralizer A c= meet Fam;
```

```
    for x being object st x in meet Fam
    holds x in the carrier of Centralizer A
    ⟨Proof: ∀x, x ∈ ⋂_a N_G(a) ⟹ x ∈ C_G(A) 95b⟩
    then meet Fam c= the carrier of Centralizer A;
    hence thesis by A2, XBOOLE_0:def 10;
  end;
```

This code is used in chunk 84.
Defines:
Th65, never used.

95a ⟨Proof: ∀x, x ∈ C_G(A) ⟹ x ∈ ⋂_a N_G(a) 95a⟩≡

```
  proof
    let x be object;
    assume B1: x in the carrier of Centralizer A;
    then x in Centralizer A;
    then x in G by GROUP_2:40;
    then reconsider g = x as Element of G;
    for X being set st X in Fam
    holds x in X
    proof
      let X be set;
      assume X in Fam;
      then consider B being Subset of G such that
      C1: B = X and
      C2: ex H being strict Subgroup of G
          st B = the carrier of H &
             (ex a being Element of G st a in A & H = Normalizer a);
      consider H being strict Subgroup of G, a being Element of G such that
      C3: B = the carrier of H & a in A & H = Normalizer a by C2;
      C4: a |^ g = g" * a * g
                .= g" * (a * g) by GROUP_1:def 3
                .= g" * (g * a) by B1,C3,Th57
                .= (g" * g) * a by GROUP_1:def 3
                .= (1_G) * a by GROUP_1:def 5
                .= a by GROUP_1:def 4;
      {a} |^ g = {a} |^ {g}
              .= {a |^ g} by GROUP_3:37
              .= {a} by C4;
      then g in Normalizer a by GROUP_3:129;
      hence x in X by C1,C3;
    end;
    hence x in meet Fam by A1,SETFAM_1:def 1;
  end;
```

This code is used in chunk 94b.

95b ⟨Proof: ∀x, x ∈ ⋂_a N_G(a) ⟹ x ∈ C_G(A) 95b⟩≡

```
  proof
    let x be object;
    assume B1: x in meet Fam;
    B2: ex H being strict Subgroup of G st P[H]
    proof
      consider X being object such that
      C1: X in Fam by A1, XBOOLE_0:def 1;
```

```
    consider B being Subset of G such that
    C2: B = X & ex H being strict Subgroup of G st B = the carrier of H & P[H]
    by C1;
    thus thesis by C2;
  end;

  consider K being strict Subgroup of G such that
  B3: the carrier of K = meet Fam
  from GROUP_4:sch 1(B2);

  reconsider g = x as Element of G by B1,B3,GROUP_2:42;
  B4: for a being Element of G st a in A
  holds g in Normalizer a
  proof
    let a be Element of G;
    assume a in A;
    then carr Normalizer a in Fam;
    hence g in Normalizer a by B1,SETFAM_1:def 1;
  end;
  for a being Element of G st a in A holds g*a = a*g
  proof
    let a be Element of G;
    assume a in A;
    then g in Normalizer a by B4;
    then consider h being Element of G such that
    C1: g = h & a |^ h = a
    by Th64;
    C2: a = g" * a * g by C1
         .= g" * (a * g) by GROUP_1:def 3;
    g * a = g * (g" * (a * g)) by C2
         .= (g * g") * (a * g) by GROUP_1:def 3
         .= 1_G * (a * g) by GROUP_1:def 5
         .= a * g by GROUP_1:def 4;
    hence g*a = a*g;
  end;

  then g is Element of Centralizer A by Th57;
  hence thesis;
end;
```

This code is used in chunk 94b.

Theorem 1.66. *If $H_1 \leq G$ and $H_2 \leq G$ are subgroups such that $|H_1 \cap H_2| = |H_1|$ and $|H_1 \cap H_2| = |H_2|$, then $H_1 = H_2$.*

96 ⟨*Theorem:* $|H_1 \cap H_2| = |H_1| = |H_2| \implies H_1 = H_2$ 96⟩≡

```
theorem Th66:
  for G being finite Group
  for H1,H2 being strict Subgroup of G
  st card(H1 /\ H2) = card H1 & card(H1 /\ H2) = card H2
  holds H1 = H2
proof
  let G be finite Group;
  let H1,H2 be strict Subgroup of G;
```

```
    assume A1: card(H1 /\ H2) = card H1;
    assume A2: card(H1 /\ H2) = card H2;
    A3: H1 /\ H2 = H1
    proof
      reconsider H12 = H1 /\ H2 as strict Subgroup of H1 by GROUP_2:88;
      multMagma(# the carrier of H12, the multF of H12 #)
      = multMagma(# the carrier of H1, the multF of H1 #) by A1,GROUP_2:73;
      hence thesis;
    end;
    H1 /\ H2 = H2
    proof
      reconsider H12 = H1 /\ H2 as strict Subgroup of H2 by GROUP_2:88;
      multMagma(# the carrier of H12, the multF of H12 #)
      = multMagma(# the carrier of H2, the multF of H2 #) by A2,GROUP_2:73;
      hence thesis;
    end;
    hence thesis by A3;
  end;
```

This code is used in chunk 84.
Defines:
Th66, never used.

Theorem 1.67. *For any natural numbers a, b, c with $c \neq 0$. If $c|a$ and $c|b$, then $a|b$.*

97a ⟨*Theorem:* $\forall a, b, c \in \mathbb{N}, c \neq 0 \wedge c|a \wedge c|b \implies a|b$ 97a⟩≡

```
  theorem Th67:
    for a,b,c being Nat
    st c <> 0 & c*a divides c*b
    holds a divides b
  proof
    let a,b,c be Nat;
    assume A1: c <> 0;
    assume c*a divides c*b;
    then consider q being Integer such that
    A2: c*b = c*a*q by INT_1:def 3;
    take q;
    b*c = a*q*c by A2;
    hence thesis by A1,XCMPLX_1:5;
  end;
```

This code is used in chunk 84.
Defines:
Th67, never used.

Theorem 1.68. *For any natural numbers $a, b, c \in \mathbb{N}$ with $b|c$ and $\gcd(ab, c) = 1$, we have $b = 1$.*

97b ⟨*Theorem:* $a, b, c \in \mathbb{N}, b|c \wedge \gcd(ab, c) = 1 \implies b = 1$ 97b⟩≡

```
  theorem Th68:
    for a,b,c being Nat
    st b<>0 & b divides c & a*b,c are_coprime
    holds b=1
  proof
    let a,b,c be Nat;
```

```
    assume b<>0;
    assume A1: b divides c;
    assume A2: a*b,c are_coprime;
    b divides a*b by INT_1:def 3;
    then b divides (a*b gcd c) by A1,INT_2:22;
    then b divides 1 by A2, INT_2:def 3;
    hence b=1 by INT_2:13;
  end;
```

This code is used in chunk 84.
Defines:
Th68, never used.

Theorem 1.69. *If $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$ and $G_1/N_1 \cong G_2/N_2$, then $|N_2| \cdot |G_1| = |N_1| \cdot |G_2|$.*

98a ⟨*Theorem:* $G_1/N_1 \cong G_2/N_2 \implies |N_2| \cdot |G_1| = |N_1| \cdot |G_2|$ 98a⟩≡

```
  theorem Th69:
    for G1,G2 being finite Group
    for N1 being normal Subgroup of G1
    for N2 being normal Subgroup of G2
    st G1./.N1, G2./.N2 are_isomorphic
    holds card(N2)*card(G1)=card(N1)*card(G2)
  proof
    let G1,G2 be finite Group;
    let N1 be normal Subgroup of G1;
    let N2 be normal Subgroup of G2;
    assume G1./.N1, G2./.N2 are_isomorphic;
    then A1: card(G1./.N1) = card(G2./.N2) by GROUP_6:73
                          .= index N2 by GROUP_6:27;
    set k = index N1;
    A2: card(G1) = card(N1) * index(N1) by GROUP_2:147
                .= card(N1) * k;
    card(G2) = card(N2) * index(N2) by GROUP_2:147
            .= card(N2) * k by A1,GROUP_6:27;
    then card(N1)*card(G2) = card(N1)*card(N2)*k
                          .= card(N2)*card(N1)*k
                          .= card(N2)*(card(N1)*k)
                          .= card(N2)*card(G1) by A2;
    hence thesis;
  end;
```

This code is used in chunk 84.
Defines:
Th69, never used.

Theorem 1.70. *Let G be a finite group. If $K \trianglelefteq G$ and $N \trianglelefteq G$ are such that $|K| = |N|$, then $|K \cap N| \cdot |KN| = |K| \cdot |N|$.*

98b ⟨*Theorem:* $K, N \trianglelefteq G \implies |KN| \cdot |K \cap N| = |K| \cdot |N|$ 98b⟩≡

```
  theorem Th70:
    for G being finite Group
    for K,N being strict normal Subgroup of G
    for m,d being Nat
    st m = card N & m = card K & d = card(K /\ N)
    holds d*card(N "\/" K) = m*m
```

```
proof
  let G be finite Group;
  let K,N be strict normal Subgroup of G;
  let m,d be Nat;
  assume A1: m = card N;
  assume A2: m = card K;
  assume A3: d = card(K /\ N);
  reconsider B=K as Subgroup of G;
  A4: N is Subgroup of B "\/" N by GROUP_4:60;
  (B "\/" N)./.(B "\/" N,N)‘*‘, B./.(B /\ N) are_isomorphic by GROUP_6:81;
  then d*card(B "\/" N) = card(B) * card((B "\/" N,N)‘*‘) by A3,Th69
                       .= card(B)*card(N) by A4,GROUP_6:def 1
                       .= card(B)*m by A1
                       .= m*m by A2;
  hence d*card(N "\/" K) = m*m;
end;
```

This code is used in chunk 84.
Defines:
Th70, never used.

Theorem 1.71 ([Gor80, Th2.1.3]). *Let G be a finite group, $N \trianglelefteq G$. If $\gcd(|N|, [G : N]) = 1$, then N is a characteristic subgroup of G.*

99 ⟨*Theorem: $N \trianglelefteq G$ with $|N|$ and $[G : N]$ coprime implies N is characteristic* 99⟩≡

```
theorem Th71:
  for G being finite Group
  for N being strict normal Subgroup of G
  st card N, index N are_coprime
  holds N is characteristic Subgroup of G
proof
  let G be finite Group;
  let N be strict normal Subgroup of G;
  assume A1: card N, index N are_coprime;
  consider m being Nat such that
  A2: m = card N;
  consider n being Nat such that
  A3: n = index N;
  A4: card G = m*n by A2,A3,GROUP_2:147;
  A5: for phi being Automorphism of G holds Image(phi|N) = N
  proof
    let phi be Automorphism of G;
    set K = Image(phi|N);
    reconsider K as strict normal Subgroup of G by Th49;
    K = phi .: N by GRSOLV_1:def 3;
    then B1: card K = card N by Th19,GROUP_6:73;
    set d = card(N /\ K);
    d divides m
    proof
      N /\ K is Subgroup of N by GROUP_2:88;
      hence thesis by A2,GROUP_2:148;
    end;
    then consider q being Nat such that
    B2: m = d*q by NAT_D:def 3;
```

```
    B3: q<>0 by A2,B2;
    card(N "\/" K) = m*q
    proof
      K /\ N = N /\ K
      proof
        carr(K /\ N) = (carr K) /\ (carr N) by GROUP_2:def 10
                    .= carr(N) /\ carr(K)
                    .= carr(N /\ K) by GROUP_2:def 10;
        hence thesis by GROUP_2:59;
      end;
      then d*card(N "\/" K) = m*(d*q) by A2,B1,B2,Th70
                          .= m*d*q
                          .= d*m*q
                          .= d*(m*q);
      hence card(N "\/" K) = m*q by XCMPLX_1:5;
    end;
    then q divides n by A2,A4,Th67,GROUP_2:148;
    then q=1 by A1,A2,A3,B2,B3,Th68;
    hence Image(phi|N) = N by A2,B1,B2,Th66;
  end;
  thus N is characteristic Subgroup of G by A5,Def3;
end;
```

This code is used in chunk 84.
Defines:
`Th71`, never used.

Theorem 1.72. *Let $f_1 \colon G_1 \to G_2$, $f_2 \colon G_2 \to G_3$ be group morphisms. If $A \subseteq G_1$, then $f_2(f_1(A)) = (f_2 \circ f_1)(A)$.*

100 ⟨*Theorem: $f_2(f_1(A)) = (f_2 \circ f_1)(A)$ for group morphisms* 100⟩≡

```
theorem Th72:
  for G1,G2,G3 being Group
  for f1 being Homomorphism of G1,G2
  for f2 being Homomorphism of G2,G3
  for A being Subgroup of G1
  holds the multMagma of f2 .: (f1 .: A) = the multMagma of ((f2 * f1) .: A)
proof
  let G1,G2,G3 be Group;
  let f1 be Homomorphism of G1,G2;
  let f2 be Homomorphism of G2,G3;
  let A be Subgroup of G1;
  for z being Element of G3
  holds z in f2 .: (f1 .: A) iff z in (f2 * f1) .: A
  proof
    let z be Element of G3;
    thus z in f2 .: (f1 .: A) implies z in (f2 * f1) .: A
    proof
      assume z in f2 .: (f1 .: A);
      then z in f2 .: (the carrier of f1 .: A) by GRSOLV_1:8;
      then consider y being object such that
      A2: y in dom f2 and
      A3: y in the carrier of (f1 .: A) and
      A4: z = f2.y by FUNCT_1:def 6;
```

```
      y in f1 .: (the carrier of A) by A3,GRSOLV_1:8;
      then consider x being object such that
      A5: x in dom f1 & x in the carrier of A & y = f1.x by FUNCT_1:def 6;
      A6: x in dom(f2 * f1) by A2,A5,FUNCT_1:11;
      then x in the carrier of A & z = (f2 * f1).x by A4,A5,FUNCT_1:12;
      then z in (f2 * f1) .: the carrier of A by A6,FUNCT_1:def 6;
      hence thesis by GRSOLV_1:8;
    end;

    thus z in (f2 * f1) .: A implies z in f2 .: (f1 .: A)
    proof
      assume z in (f2 * f1) .: A;
      then z in (f2 * f1) .: the carrier of A by GRSOLV_1:8;
      then consider x being object such that
      A2: x in dom (f2 * f1) & x in the carrier of A & z = (f2 * f1).x
      by FUNCT_1:def 6;
      A3: x in dom f1 & f1.x in dom f2 by A2,FUNCT_1:11;

      set y = f1.x;
      x in dom f1 & x in the carrier of A & y = f1.x by A2,FUNCT_1:11;
      then A5: y in f1 .: (the carrier of A) by FUNCT_1:def 6;
      z = (f2 * f1).x by A2
       .= f2.(f1.x) by A2,FUNCT_1:12
       .= f2.y;
      then z in f2 .: (f1 .: (the carrier of A)) by A3,A5,FUNCT_1:def 6;
      then z in f2 .: (the carrier of (f1 .: A)) by GRSOLV_1:8;
      hence z in f2 .: (f1 .: A) by GRSOLV_1:8;
    end;

  end;

  hence the multMagma of f2 .: (f1 .: A) = the multMagma of ((f2 * f1) .: A)
  by GROUP_2:60;
end;
```

This code is used in chunk 84.
Defines:
Th72, never used.

Theorem 1.73. *Let $N \trianglelefteq G$, $\varphi \in \mathrm{Aut}(G)$ such that $\varphi(N) = N$. (N need not be characteristic.) Then there exists an automorphism $\sigma \in \mathrm{Aut}(G/N)$ such that for any $x \in G$, $\sigma(xN) = \varphi(x)N$.*

101 ⟨*Theorem:* $\varphi \in \mathrm{Aut}(G)$, $\varphi(N) = N$, $\exists \sigma \in \mathrm{Aut}(G/N), \sigma(xN) = \varphi(x)N$ 101⟩≡

```
theorem Th73:
  for G being Group
  for N being strict normal Subgroup of G
  for phi being Automorphism of G
  st Image(phi|N) = N
  ex sigma being Automorphism of G./.N
  st (for x being Element of G holds sigma.(x*N) = (phi.x)*N)
proof
  let G be Group;
  let N be strict normal Subgroup of G;
```

```
let phi be Automorphism of G;
assume A1: Image(phi|N) = N;
defpred P[set,set] means ex a being Element of G st $1 = a*N & $2 = (phi.a)*N;
A2: for x being Element of G./.N ex y being Element of G./.N st P[x,y]
proof
  let x be Element of G./.N;
  x in Cosets N;
  then consider a being Element of G such that
  B1: x = a*N by GROUP_2:def 15;
  (phi.a)*N in Cosets N by GROUP_2:def 15;
  then consider y being Element of G./.N such that
  B2: y = (phi.a)*N;
  take y;
  thus P[x,y] by B1,B2;
end;

consider sigma being Function of G./.N, G./.N such that
A3: for x being Element of G./.N holds P[x, sigma.x]
from FUNCT_2:sch 3(A2);

A4: for a being Element of G holds sigma.(a*N) = (phi.a)*N
proof
  let a be Element of G;
  a*N in Cosets N by GROUP_2:def 15;
  then consider x being Element of G./.N such that
  B1: x = a*N;

  consider b being Element of G such that
  B2: x = b*N & sigma.x = (phi.b)*N by A3;
  consider n being Element of G such that
  B3: n = b" * a & n in N by B1,B2,GROUP_2:114;

  B4: b*n = b*(b" * a) by B3
         .= (b * b") * a by GROUP_1:def 3
         .= 1_G * a by GROUP_1:def 5
         .= a by GROUP_1:def 4;

  dom phi = the carrier of G & n in N by B3, FUNCT_2:def 1;
  then phi.n in phi .: (the carrier of N) by FUNCT_1:def 6;
  then phi.n in the carrier of (phi .: N) by GRSOLV_1:8;
  then B5: phi.n in N by A1,GRSOLV_1:def 3;
  phi.a * N = phi.(b * n) * N by B4
           .= (phi.b * phi.n) * N by GROUP_6:def 6
           .= phi.b * (phi.n * N) by GROUP_2:105
           .= phi.b * N by B5, GROUP_2:113
           .= sigma.x by B2;
  hence thesis by B1;
end;

for x,y being Element of G./.N holds sigma.(x*y) = sigma.x * sigma.y
proof
  let x,y be Element of G./.N;
  consider a being Element of G such that
```

```
  B1: x = a*N & sigma.x = (phi.a)*N by A3;
  consider b being Element of G such that
  B2: y = b*N & sigma.y = (phi.b)*N by A3;
  B3: for g1,g2 being Element of G holds (g1*N)*(g2*N) = g1*g2*N
  proof
    let g1,g2 be Element of G;
    (g1*N)*(g2*N) = (g1 * N) * (N * g2) by GROUP_3:117
                .= g1 * N * N * g2 by GROUP_3:11
                .= g1 * (N*N) * g2 by GROUP_4:45
                .= g1 * N * g2 by GROUP_2:76
                .= g1 * (N * g2) by GROUP_2:106
                .= g1 * (g2 * N) by GROUP_3:117
                .= g1 * g2 * N by GROUP_2:105;
    hence thesis;
  end;

  B4: x * y = @x * @y by GROUP_6:def 3
           .= (a * N) * (b * N) by B1,B2
           .= a * b * N by B3;

  B5: (sigma.x) * (sigma.y) = phi.(a*b) * N
  proof
    sigma.x * sigma.y = @(sigma.x) * @(sigma.y) by GROUP_6:def 3
                    .= ((phi.a)*N) * ((phi.b) * N) by B1,B2
                    .= (phi.a) * (phi.b) * N by B3
                    .= phi.(a*b) * N by GROUP_6:def 6;
    hence thesis;
  end;
  sigma.(x * y) = sigma.(a * b * N) by B4
              .= phi.(a*b) * N by A4
              .= sigma.x * sigma.y by B5;
  hence sigma.(x*y) = sigma.x * sigma.y;
end;

then reconsider sigma as Homomorphism of G./.N, G./.N by GROUP_6:def 6;
sigma is bijective
proof
  B1: for x being Element of G holds x*N in Ker sigma iff x in N
  proof
    let x be Element of G;
    reconsider z = x*N as Element of G./.N by GROUP_2:def 15;
    C1: (phi").(phi.x) = x by FUNCT_2:26;
    thus x*N in Ker sigma implies x in N
    proof
      assume (x*N) in Ker sigma;
      then sigma.z = 1_(G./.N) by GROUP_6:41;
      then D1: sigma.(x*N) = 1_(G./.N)
                          .= carr N by GROUP_6:24;
      (phi.x)*N = sigma.(x*N) by A4
               .= carr N by D1;
      then phi.x in Image(phi|N) by A1,GROUP_2:113;
      then D2: phi.x in phi .: N by GRSOLV_1:def 3;
      consider psi being Automorphism of G such that
```

```
    D3: psi = phi" and
        Image(phi|Image(psi|N)) = the multMagma of N
    by Th17;
    reconsider i = id the carrier of G as Automorphism of G by GROUP_6:38;
    the carrier of G <> {} & phi is onto;
    then D4: psi * phi = id the carrier of G by D3,FUNCT_2:29;
    dom psi = the carrier of G by FUNCT_2:def 1;
    then psi.(phi.x) in psi .: (the carrier of (phi .: N))
    by D2,FUNCT_1:def 6;
    then psi.(phi.x) in the carrier of (psi .: (phi .: N)) by GRSOLV_1:8;
    then x in i .: N by C1,D3,D4,Th72;
    then D5: x in (id the carrier of G) .: (the carrier of N) by GRSOLV_1:8;
    the carrier of N is Subset of the carrier of G by GROUP_2:def 5;
    hence x in N by D5,FUNCT_1:92;
  end;
  thus x in N implies x*N in Ker sigma
  proof
    assume x in N;
    then D1: x * N = carr N by GROUP_2:113
                  .= 1_(G./.N) by GROUP_6:24;
    then sigma.(x*N) = 1_(G./.N) by GROUP_6:31;
    hence x*N in Ker sigma by D1,GROUP_6:41;
  end;
end;
for x being Element of G./.N holds x in Ker sigma iff x in (1).(G./.N)
proof
  let x be Element of G./.N;
  thus x in Ker sigma implies x in (1).(G./.N)
  proof
    assume C1: x in Ker sigma;
    x in G./.N;
    then consider g being Element of G such that
    C2: x = g*N by GROUP_2:def 15;
    g*N = carr N by B1,C1,C2,GROUP_2:113;
    then g*N = 1_(G./.N) by GROUP_6:24;
    then g*N in {1_(G./.N)} by TARSKI:def 1;
    hence x in (1).(G./.N) by C2,GROUP_2:def 7;
  end;
  thus x in (1).(G./.N) implies x in Ker sigma
  proof
    assume x in (1).(G./.N);
    then x in {1_(G./.N)} by GROUP_2:def 7;
    then x = 1_(G./.N) by TARSKI:def 1;
    then sigma.x = 1_(G./.N) by GROUP_6:31;
    hence x in Ker sigma by GROUP_6:41;
  end;
end;

then Ker sigma = (1).(G./.N);
hence sigma is one-to-one by GROUP_6:56;

for y being Element of G./.N holds y in Image sigma
proof
```

```
      let y be Element of G./.N;
      y in G./.N;
      then consider b being Element of G such that
      C1: y = b*N by GROUP_2:def 15;
      reconsider psi = phi" as Automorphism of G by GROUP_6:62;
      consider a being Element of G such that
      C2: a = psi.b;
      a*N in G./.N by GROUP_2:def 15;
      then consider x being Element of G./.N such that
      C3: x = a*N;
      C4: phi.a = phi.((phi").b) by C2
               .= b by Th4;
      sigma.x = sigma.(a*N) by C3
             .= (phi.a)*N by A4
             .= b*N by C4
             .= y by C1;
      hence y in Image sigma by GROUP_6:45;
    end;
    hence sigma is onto by GROUP_2:62,GROUP_6:57;
  end;
  then reconsider sigma as Automorphism of G./.N;
  take sigma;
  let x be Element of G;
  thus sigma.(x*N) = (phi.x)*N by A4;
end;
```

This code is used in chunk 84.
Defines:
Th73, never used.

Theorem 1.74. *Let G be a finite group $H \leq K \leq G$ and H be a characteristic subgroup. Then H is a normal subgroup of K.*

105 ⟨*Theorem: H char G and $H \leq K \leq G$, then $H \trianglelefteq K$* 105⟩≡

```
theorem Th74:
  for G being finite Group
  for H being strict characteristic Subgroup of G
  for K being strict Subgroup of G
  st H is Subgroup of K
  holds H is normal Subgroup of K
proof
  let G be finite Group;
  let H be strict characteristic Subgroup of G;
  let K be strict Subgroup of G;
  assume A1: H is Subgroup of K;
  A2: for g being Element of G
  holds g in Ker (nat_hom H) iff g in H by GROUP_6:43;

  reconsider R = Ker ((nat_hom H)|K) as strict Subgroup of K;

  A3: for k being Element of K
  holds k in H iff k in Ker ((nat_hom H)|K)
  proof
    let k be Element of K;
```

```
      reconsider g=k as Element of G by GROUP_2:42;
      B1: g in K;
      thus k in H implies k in Ker ((nat_hom H)|K)
      proof
        assume C1: k in H;
        C2: g in K;
        (nat_hom H).g = 1_(G./.H) by A2,C1,GROUP_6:41;
        then ((nat_hom H)|K).g = 1_(G./.H) by C2,Th1;
        hence k in Ker ((nat_hom H)|K) by GROUP_6:41;
      end;
      thus k in Ker ((nat_hom H)|K) implies k in H
      proof
        assume C1: k in Ker ((nat_hom H)|K);
        ((nat_hom H)|K).g = (nat_hom H).g by B1,Th1;
        then (nat_hom H).g = 1_(G./.H) by C1,GROUP_6:41;
        then g in Ker (nat_hom H) by GROUP_6:41;
        hence k in H by GROUP_6:43;
      end;

    end;
    reconsider H1=H as strict Subgroup of K by A1;
    the multMagma of R = the multMagma of H1 by A3,GROUP_2:60;
    hence thesis;
  end;
```

This code is used in chunk 84.
Defines:
Th74, never used.

Theorem 1.75 (Gorenstein [Gor80, Th2.1.2(iv)]). *Let G be a finite group, H a characteristic subgroup of G, and $H \leq K \leq G$. If K/H is a characteristic subgroup of G/H, then K is a characteristic subgroup of G.*

106 ⟨*Theorem: $H \leq K \leq G$, H char G, K/H char G/H implies K is characteristic* 106⟩≡

```
  :: Gorenstein, Finite Groups, Theorem 2.1.2 (iv)
  theorem Th75:
    for G being finite Group
    for H being strict characteristic Subgroup of G
    for K being strict Subgroup of G
    st H is Subgroup of K &
    K./.(K,H)‘*‘ is characteristic Subgroup of G./.H
    holds K is characteristic Subgroup of G
  proof
    let G be finite Group;
    let H be strict characteristic Subgroup of G;
    let K be strict Subgroup of G;
    assume A1: H is Subgroup of K;
    assume A2: K./.(K,H)‘*‘ is characteristic Subgroup of G./.H;
    A3: (K,H)‘*‘ = H by A1,GROUP_6:def 1;
    for phi being Automorphism of G
    for k being Element of G st k in K
    holds phi.k in K
    proof
      let phi be Automorphism of G;
```

```
let k be Element of G;
assume B1: k in K;
Image(phi|H) = H by Def3;
then consider sigma being Automorphism of G./.H such that
B2: for x being Element of G holds sigma.(x*H) = (phi.x)*H
by Th73;
consider J being strict characteristic Subgroup of G./.H such that
B3: J = (K./.(K,H)‘*‘) by A2;

B4: for k1 being Element of G st k1*H in J holds k1 in K
proof
  let k1 be Element of G;
  assume C1: k1*H in J;
  C2: k1*H = k1*(carr H)
          .= k1*(K,H)‘*‘ by A1,GROUP_6:def 1;
  set x = k1*(K,H)‘*‘;
  consider a being Element of K such that
  C3: x = a*(K,H)‘*‘ by B3,C1,C2,GROUP_2:def 15;

  reconsider a1 = a as Element of G by GROUP_2:42;
  C4: a1 in K;
  for j1 being object holds j1 in a*(K,H)‘*‘ iff j1 in a1*H
  proof
    let j1 be object;
    thus j1 in a*(K,H)‘*‘ implies j1 in a1*H
    proof
      assume j1 in a*(K,H)‘*‘;
      then consider g1 being Element of K such that
      D1: j1 = a*g1 & g1 in (K,H)‘*‘ by GROUP_2:103;
      reconsider g=g1 as Element of G by GROUP_2:42;
      D2: j1 = a1*g by D1,GROUP_2:43;
      g in H by D1,A1,GROUP_6:def 1;
      hence j1 in a1*H by D2,GROUP_2:103;
    end;

    thus j1 in a1*H implies j1 in a*(K,H)‘*‘
    proof
      assume j1 in a1*H;
      then consider g1 being Element of G such that
      D1: j1 = a1*g1 & g1 in H by GROUP_2:103;
      reconsider g=g1 as Element of K by A1,D1,GROUP_2:42;
      D2: j1 = a*g by D1,GROUP_2:43;
      g in (K,H)‘*‘ by D1,A1, GROUP_6:def 1;
      hence j1 in a*(K,H)‘*‘ by D2,GROUP_2:103;
    end;

  end;
  then a1*H = x by TARSKI:2,C3
           .= k1*H by C2;
  then (a1") * k1 in H by GROUP_2:114;
  then C5: (a1") * k1 in K by A1,GROUP_2:41;
  a1 * ((a1") * k1) = (a1 * a1") * k1 by GROUP_1:def 3
                   .= 1_G * k1 by GROUP_1:def 5
```

```
                    .= k1 by GROUP_1:def 4;
    hence k1 in K by C4,C5,GROUP_2:50;
  end;

  B5: for k1 being Element of G holds k1 in K iff k1*H in J
  proof
    let k1 be Element of G;
    thus k1 in K implies k1*H in J
    proof
      assume k1 in K;
      then reconsider k2=k1 as Element of K;
      C1: k2*((K,H)‘*‘) in J by B3, GROUP_2:def 15;
      for x being object holds x in k2*carr((K,H)‘*‘) iff x in k1*carr(H)
      proof
        let x be object;
        thus x in k2*carr((K,H)‘*‘) implies x in k1*carr(H)
        proof
          assume E1: x in k2*carr((K,H)‘*‘);
          x in k2*((K,H)‘*‘) iff
          ex g being Element of K st (x = k2*g & g in (K,H)‘*‘)
          by GROUP_2:103;
          then consider huh being Element of K such that
          E2: x = k2*huh & huh in (K,H)‘*‘ by E1;
          E3: huh in H by A1,E2,GROUP_6:def 1;
          reconsider huh2=huh as Element of G by GROUP_2:42;
          set x2 = k1*huh2;
          x = k1*huh2 by E2,GROUP_2:43;
          hence thesis by E3,GROUP_2:27;
        end;
        assume x in k1*carr(H);
        then consider h1 being Element of G such that
        D1: x = k1*h1 & h1 in carr(H) by GROUP_2:27;
        reconsider h2=h1 as Element of K by A1,D1,GROUP_2:42;
        reconsider H1=H as normal Subgroup of K by A3;
        D2: the carrier of H = the carrier of ((K,H)‘*‘) by A1,GROUP_6:def 1;
        k2*h2 in k2*carr(H1) by D1,GROUP_2:27;
        hence x in k2*carr((K,H)‘*‘) by D1,D2,GROUP_2:43;
      end;

      then k2*carr(((K,H)‘*‘)) = k1*carr(H) by TARSKI:2
                              .= k1*H;
      hence k1*H in J by C1;
    end;
    thus k1*H in J implies k1 in K by B4;
  end;
  then k*H in J by B1;
  then reconsider kH = k*H as Element of G./.H by GROUP_2:42;
  sigma.(kH) in J by Th50,B1,B5;
  then sigma.(k*H) in J & sigma.(k*H) = (phi.k)*H by B2;
  hence phi.k in K by B4;
end;

hence K is characteristic Subgroup of G by Th50;
```

```
  end;
```

This code is used in chunk 84.
Defines:
  Th75, never used.

Theorem 1.76. *Let $H \leq G$. Then $H \leq C_G(H)$ if and only if H is a commutative group.*

109 ⟨*Theorem: $H \leq G$, $H \leq C_G(H) \iff H$ is commutative* 109⟩≡

```
theorem Th76:
  for G being Group
  for H being Subgroup of G
  holds H is Subgroup of Centralizer H iff H is commutative Group
proof
  let G be Group;
  let H be Subgroup of G;
  thus H is Subgroup of Centralizer H implies H is commutative Group
  proof
    assume A1: H is Subgroup of Centralizer H;
    A2: for g,h being Element of G st g in H & h in H holds g*h=h*g
    proof
      let g,h be Element of G;
      assume B1: g in H;
      assume B2: h in H;
      g in Centralizer H by B1,A1,GROUP_2:40;
      hence g*h=h*g by B2,Th60;
    end;
    for g,h being Element of H holds g*h=h*g
    proof
      let g,h be Element of H;
      B1: g in H & h in H;
      reconsider g1=g, h1=h as Element of G by GROUP_2:42;
      g*h = g1*h1 by GROUP_2:43
         .= h1*g1 by A2,B1
         .= h*g by GROUP_2:43;
      hence thesis;
    end;
    hence thesis by GROUP_1:def 12;
  end;

  thus H is commutative Group implies H is Subgroup of Centralizer H
  proof
    assume A1: H is commutative Group;
    A2: for g,h being Element of G st g in H & h in H holds g*h=h*g
    proof
      let g,h be Element of G;
      assume B1: g in H;
      assume B2: h in H;
      reconsider g1=g,h1=h as Element of H by B1,B2;
      g*h = g1*h1 by GROUP_2:43
         .= h1*g1 by A1,GROUP_1:def 12
         .= h*g by GROUP_2:43;
      hence g*h=h*g;
```

```
    end;
    for g being Element of G st g in H holds g in Centralizer H
    proof
      let g be Element of G;
      assume B1: g in H;
      for a being Element of G st a in H holds g*a = a*g by B1,A2;
      then g is Element of Centralizer H by Th60;
      hence g in Centralizer H;
    end;
    hence thesis by GROUP_2:58;
  end;
end;
```

This code is used in chunk 84.
Defines:
Th76, never used.

Theorem 1.77. *For any group G, $C_G(G) = Z(G)$.*

110 ⟨*Theorem:* $C_G(G) = Z(G)$ 110⟩≡

```
theorem Th77:
  for G being Group
  holds Centralizer (Omega).G = center G
proof
  let G be Group;
  for g being Element of G holds g in Centralizer (Omega).G iff g in center G
  proof
    let g be Element of G;
    thus g in Centralizer (Omega).G implies g in center G
    proof
      assume A1: g in Centralizer (Omega).G;
      for a being Element of G holds g*a = a*g
      proof
        let a be Element of G;
        a in (Omega).G;
        hence g*a = a*g by A1,Th60;
      end;
      hence g in center G by GROUP_5:77;
    end;

    thus g in center G implies g in Centralizer (Omega).G
    proof
      assume g in center G;
      then for b being Element of G st b in (Omega).G holds g*b = b*g
      by GROUP_5:77;
      then g is Element of Centralizer (Omega).G by Th60;
      hence thesis;
    end;

  end;
  hence Centralizer (Omega).G = center G;
end;
```

This code is used in chunk 84.
Defines:
Th77, never used.

Theorem 1.78. *Let $N \trianglelefteq G$ be a subgroup. Then $C_G(N) \trianglelefteq G$.*

111 ⟨*Theorem:* $N \trianglelefteq G \implies C_G(H) \trianglelefteq G$ 111⟩≡

```
theorem Th78:
  for G being Group
  for N being normal Subgroup of G
  holds Centralizer N is normal Subgroup of G
proof
  let G be Group;
  let N be normal Subgroup of G;

  A1: for g,n being Element of G st n in N holds n |^ g in N
  proof
    let g,n be Element of G;
    assume B1: n in N;
    B2: the multMagma of N = the multMagma of (N |^ g) by GROUP_3:def 13;
    n |^ g in N |^ g by B1,GROUP_3:58;
    hence thesis by B2;
  end;

  A2: for g,x,n being Element of G st x in Centralizer N & n in N
  holds (x |^ g)*n = n*(x |^ g)
  proof
    let g,x,n be Element of G;
    assume B1: x in Centralizer N;
    assume B2: n in N;
    consider n2 being Element of G such that
    B3: n2 = g * n * g";
    B4: n2 = n |^ g" by B3;
    then (x * n2) |^ g = (n2 * x) |^ g by B1,B2,A1,Th60
                      .= (n2 |^ g) * (x |^ g) by GROUP_3:23;
    then (x |^ g) * (n2 |^ g) = (n2 |^ g) * (x |^ g) by GROUP_3:23
                              .= n * (x |^ g) by B4,GROUP_3:25;
    hence (x |^ g) * n = n * (x |^ g) by B4,GROUP_3:25;
  end;

  A3: for g,z being Element of G st z in Centralizer N
  holds z |^ g in Centralizer N
  proof
    let g,z be Element of G;
    assume z in Centralizer N;
    then for n being Element of G st n in N holds
    (z |^ g)*n = n*(z |^ g) by A2;
    then (z |^ g) is Element of Centralizer N by Th60;
    hence z |^ g in Centralizer N;
  end;


  for g being Element of G holds (Centralizer N) |^ g = Centralizer N
  proof
    let g be Element of G;
    for z being Element of G
    holds z in (Centralizer N) |^ g iff z in (Centralizer N)
```

```
    proof
      let z be Element of G;
      hereby
        assume z in (Centralizer N) |^ g;
        then (z |^ g") in ((Centralizer N) |^ g) |^ g" by GROUP_3:58;
        then (z |^ g") in Centralizer N by GROUP_3:62;
        then (z |^ g") |^ g in Centralizer N by A3;
        hence z in (Centralizer N) by GROUP_3:25;
      end;
      assume z in (Centralizer N);
      then (z |^ g") |^ g in (Centralizer N) |^ g by A3,GROUP_3:58;
      hence z in (Centralizer N) |^ g by GROUP_3:25;
    end;

    hence (Centralizer N) |^ g = Centralizer N;
  end;
  hence Centralizer N is normal Subgroup of G by GROUP_3:def 13;
end;
```

This code is used in chunk 84.
Defines:
Th78, never used.

Theorem 1.79. *Let $H \leq G$, $h \in H$ and $n \in N_G(H)$. Then $h^n = n^{-1}hn \in H$.*

112a ⟨*Theorem:* $\forall h \in H, n \in N_G(H), n^{-1}hn \in H$ 112a⟩≡

```
theorem Th79:
  for G being Group
  for H being Subgroup of G
  for h,n being Element of G
  st h in H & n in Normalizer H
  holds h |^ n in H
proof
  let G be Group;
  let H be Subgroup of G;
  let h,n be Element of G;
  assume A1: h in H;
  assume n in Normalizer H;
  then consider g being Element of G such that
  A2: n" = g & (carr H) |^ g = carr H by GROUP_2:51,GROUP_3:129;
  consider h1 being Element of G such that
  A3: h = h1 |^ g & h1 in carr H by A1,A2,GROUP_3:41;
  h |^ n = (h1 |^ (n")) |^ n by A2,A3
        .= h1 by GROUP_3:25;
  hence h |^ n in H by A3;
end;
```

This code is used in chunk 84.
Defines:
Th79, never used.

Theorem 1.80. *For any subgroup $H \leq G$, we have $H \leq N_G(H)$.*

112b ⟨*Theorem:* $\forall H \leq G, H \leq N_G(H)$ 112b⟩≡

```
theorem Th80:
  for G being Group
```

```
  for H being Subgroup of G
  holds H is Subgroup of Normalizer H
proof
  let G be Group;
  let H be Subgroup of G;
  A1: for g being Element of G st g in H
  for x being Element of G st x in (carr H) |^ g holds x in carr H
  proof
    let g be Element of G;
    assume B1: g in H;
    let x be Element of G;
    assume x in (carr H) |^ g;
    then consider h being Element of G such that
    B2: x = h |^ g & h in carr H by GROUP_3:41;
    B3: h in H by B2;
    g" in H by B1,GROUP_2:51;
    then g" * h in H by B3, GROUP_2:50;
    then x in H by B1,B2, GROUP_2:50;
    hence x in carr H;
  end;

  for g being Element of G st g in H holds g in Normalizer H
  proof
    let g be Element of G;
    assume B1: g in H;
    for x being Element of G st x in carr H holds x in (carr H) |^ g
    proof
      let x be Element of G;
      thus x in carr H implies x in (carr H) |^ g
      proof
        assume x in carr H;
        then C1: x in H;
        set h = x |^ g";
        g" in H by B1,GROUP_2:51;
        then x * g" in H by C1,GROUP_2:50;
        then g * (x * g") in H by B1,GROUP_2:50;
        then C2: h in (carr H) by GROUP_1:def 3;
        C3: h |^ g = (x |^ g") |^ g
                  .= x by GROUP_3:25;
        thus x in (carr H) |^ g by C2,C3,GROUP_3:41;
      end;
    end;
    then (carr H) |^ g c= carr H & carr H c= (carr H) |^ g by A1,B1;
    then (carr H) |^ g = carr H by XBOOLE_0:def 10;
    hence g in Normalizer H by GROUP_3:129;
  end;

  hence H is Subgroup of Normalizer H by GROUP_2:58;
end;
```

This code is used in chunk 84.

Defines:

Th80, never used.

Lemma 1.8. *Let $H \leq G$ be a subgroup. Then $C_G(H) \leq N_G(H)$.*

Proof sketch. We find every $g \in C_G(H)$ also lives in $g \in N_G(H)$. The result follows immediately. □

114a ⟨*Lemma:* $C_G(H) \leq N_G(H)$ 114a⟩≡

```
Lm8:
  for G being Group
  for H being Subgroup of G
  holds Centralizer H is strict Subgroup of Normalizer H
proof
  let G be Group;
  let H be Subgroup of G;
  set Z = Centralizer H;
  for g being Element of G st g in Centralizer H holds g in Normalizer H
  ⟨Proof: ∀g ∈ G, g ∈ C_G(H) ⟹ g ∈ N_G(H) 114b⟩
  hence Centralizer H is strict Subgroup of Normalizer H by GROUP_2:58;
end;
```

This code is used in chunk 84.
Defines:
Lm8, never used.

Proof step (∀g ∈ G, g ∈ $C_G(H)$ ⟹ g ∈ $N_G(H)$). We will show, for any arbitrary $g \in C_G(H)$, that $H^g = H$. This implies $g \in N_G(H)$ by definition of the normalizer. □

114b ⟨*Proof:* ∀g ∈ G, g ∈ $C_G(H)$ ⟹ g ∈ $N_G(H)$ 114b⟩≡

```
proof
  let g be Element of G;
  assume A1: g in Centralizer H;
  A2: for a being Element of G st a in H holds a = (g")*a*g
  proof
    let a be Element of G;
    assume a in H;
    then g" * (a * g) = g" * (g*a) by A1,Th60
                    .= (g" * g)*a by GROUP_1:def 3
                    .= (1_G)*a by GROUP_1:def 5
                    .= a by GROUP_1:def 4;
    hence a = (g")*a*g by GROUP_1:def 3;
  end;

  for a being Element of G holds a in H iff a in (H |^ g)
  proof
    let a be Element of G;
    thus a in H implies a in H |^ g
    proof
      assume B1: a in H;
      then a = a |^ g by A2;
      hence a in H |^ g by B1, GROUP_3:58;
    end;
    thus a in H |^ g implies a in H
    proof
      assume a in H |^ g;
      then consider h being Element of G such that
```

```
      B1: a = h |^ g & h in H
      by GROUP_3:58;
      thus a in H by A2,B1;
    end;
  end;
  then the multMagma of H = the multMagma of (H |^ g) by GROUP_2:60;
  then carr H = carr(H) |^ g by GROUP_3:def 6;
  hence g in Normalizer H by GROUP_3:129;
end;
```

This code is used in chunk 114a.

Theorem 1.81. *Let $H \leq G$. Then $C_G(H) \trianglelefteq N_G(H)$.*

Proof sketch. We will show (B_4), for arbitrary $z \in C_G(H)$ and $n \in N_G(H)$, that $z^n = n^{-1}zn$ commutes with any $h \in H$. This implies (B_5) that $z^n \in C_G(H)$ and thus $C_G(H) \leq n^{-1}C_G(H)n$. It follows that $C_G(H) \trianglelefteq N_G(H)$. □

115 ⟨*Theorem:* $C_G(H) \trianglelefteq N_G(H)$ 115⟩≡

```
theorem Th81:
  for G being Group
  for H being Subgroup of G
  holds Centralizer H is strict normal Subgroup of Normalizer H
proof
  let G be Group;
  let H be Subgroup of G;

  (Centralizer H) is normal Subgroup of Normalizer H
  proof
    reconsider Z=Centralizer H as strict Subgroup of Normalizer H by Lm8;
    set N = Normalizer H;

    B60: for z being Element of N
    holds (for n being Element of N st n in H holds z*n = n*z) iff
          z is Element of Z
    ⟨Proof: ∀z ∈ N_G(H), (∀n ∈ N_G(H), n ∈ H ⟹ zn = nz) ⟺ z ∈ C_G(H) 118⟩


    B1: for z,n,h being Element of N
    st z in Z & n in N & h in H
    holds h |^ (z |^ n) = h
    proof
      let z,n,h be Element of N;
      assume C1: z in Z;
      assume n in N;
      assume C2: h in H;
      C3: h |^ (z |^ n) = (z |^ n)" * h * (z |^ n)
      .= (z" |^ n) * h * (z |^ n) by GROUP_3:26
      .= (n" * z" * n) * h * (n" * z * n)
      .= ((n" * z") * n) * h * (n" * (z * n)) by GROUP_1:def 3
      .= ((n" * z") * n) * (h * (n" * (z * n))) by GROUP_1:def 3
      .= (n" * z") * (n * (h * (n" * (z * n)))) by GROUP_1:def 3
      .= (n" * z") * (n * h * (n" * (z * n))) by GROUP_1:def 3
      .= (n" * z") * ((n * h) * (n" * (z * n)))
```

```
.= (n" * z") * (((n * h) * n") * (z * n)) by GROUP_1:def 3
.= (n" * z") * ((n * h) * n") * (z * n) by GROUP_1:def 3
.= (n" * z") * (n * h * n") * (z * n);

C4: for a,b being Element of G
holds a in N & b in H & b in N implies a*b*a" in H & a*b*a" in N
proof
  let a,b be Element of G;
  assume D1: a in N;
  assume D2: b in H;
  assume D3: b in N;
  D4: a*b in N by D1,D3,GROUP_2:50;
  D5: a" in N & b in H by D1,D2,GROUP_2:51;
  then b |^ a" in H by Th79;
  hence a*b*a" in H;
  thus a*b*a" in N by D4,D5,GROUP_2:50;
end;

n * h * n" in H
proof
  reconsider h1=h,n1=n as Element of G by GROUP_2:42;
  n1" = n" by GROUP_2:48;
  then h1*n1" = h*n" by GROUP_2:43;
  then n1*(h1*n1") = n*(h*n") by GROUP_2:43
                  .= n*h*n" by GROUP_1:def 3;
  then D1: n1*h1*n1" = n*h*n" by GROUP_1:def 3;
  h1 in N & n1 in N & h1 in H by C2;
  hence thesis by C4,D1;
end;
then consider h2 being Element of N such that
C5: n * h * n" = h2 & h2 in H;

z*h2 = h2*z by B60,C1,C5;
then (z" * z) * h2 = z" * (h2 * z) by GROUP_1:def 3
                  .= (z" * h2) * z by GROUP_1:def 3;
then (z" * h2) * z = (z" * z) * h2
                  .= 1_N * h2 by GROUP_1:def 5
                  .= h2 by GROUP_1:def 4;
then C6: h2 * z" = ((z" * h2) * z) * z"
                .= (z" * h2) * (z * z") by GROUP_1:def 3
                .= (z" * h2) * 1_N by GROUP_1:def 5
                .= z" * h2 by GROUP_1:def 4;
h |^ (z |^ n) = (n" * z") * (n * h * n") * (z * n) by C3
             .= (n" * z") * h2 * (z * n) by C5
             .= (n" * z") * (h2 * (z * n)) by GROUP_1:def 3
             .= n" * (z" * (h2 * (z * n))) by GROUP_1:def 3
             .= n" * ((z" * h2) * (z * n)) by GROUP_1:def 3
             .= n" * ((h2 * z") * (z * n)) by C6
             .= n" * (h2 * (z" * (z * n))) by GROUP_1:def 3
             .= n" * (h2 * ((z" * z) * n)) by GROUP_1:def 3
             .= n" * (h2 * (1_N * n)) by GROUP_1:def 5
             .= n" * (h2 * n) by GROUP_1:def 4
             .= n" * h2 * n by GROUP_1:def 3
```

```
                .= h2 |^ n
                .= (n * h * n") |^ n by C5
                .= (h |^ n") |^ n
                .= h by GROUP_3:25;
      hence h |^ (z |^ n) = h;
    end;


    B2: for z,n,h being Element of N
    st z in Z & h in H
    holds (z |^ n)*h = h*(z |^ n)
    proof
      let z,n,h be Element of N;
      assume C1: z in Z;
      assume C2: h in H;
      n in N;
      then h |^ (z |^ n) = h by C1,C2,B1;
      hence (z |^ n)*h = h*(z |^ n) by GROUP_3:22;
    end;


    B3: for n being Element of N
    for z being Element of N st z in Z holds (z |^ n) in Z
    proof
      let n be Element of N;
      let z be Element of N;
      assume C1: z in Z;
      set g = z |^ n;
      for h being Element of N st h in H holds g*h = h*g by C1,B2;
      then g is Element of Z by B60;
      hence thesis;
    end;

    for n being Element of Normalizer H
    holds Z is Subgroup of Z |^ n
    proof
      let n be Element of Normalizer H;
      for z being Element of N st z in Z holds z in Z |^ n
      proof
        let z be Element of N;
        assume z in Z;
        then (z |^ n") |^ n in (Z |^ n) by B3,GROUP_3:58;
        hence z in Z |^ n by GROUP_3:25;
      end;

      hence Z is Subgroup of Z |^ n by GROUP_2:58;
    end;
    hence thesis by GROUP_3:121;
  end;
  hence thesis;
end;
```

This code is used in chunk 84.
Defines:

`Th81`, never used.

Proof step (B_{60}). We prove the analogous result from theorem 60, but when restricting quantifiers to the normalizer. □

118 ⟨*Proof:* $\forall z \in N_G(H), (\forall n \in N_G(H), n \in H \implies zn = nz) \iff z \in C_G(H)$ 118⟩≡

```
proof
  let z be Element of N;
  reconsider z1=z as Element of G by GROUP_2:42;

  C1: z is Element of Z implies (for n being Element of N st n in H
                                  holds z*n = n*z)
  proof
    assume D1: z is Element of Z;
    let n be Element of N;
    assume D2: n in H;
    reconsider n1=n as Element of G by GROUP_2:42;
    z1*n1 = n1*z1 by D1,D2,Th60
         .= n*z by GROUP_2:43;
    hence z*n = n*z by GROUP_2:43;
  end;
  not (z is Element of Z) implies not (for n being Element of N st n in H
  holds z*n = n*z)
  proof
    assume not z is Element of Z;
    then consider g being Element of G such that
    D1: g in H & g*z1 <> z1 * g by Th60;
    H is Subgroup of Normalizer H by Th80;
    then g in Normalizer H by D1, GROUP_2:41;
    then reconsider n=g as Element of N;
    D2: g*z1 = n*z by GROUP_2:43;
    take n;
    thus thesis by D1,D2,GROUP_2:43;
  end;
  hence (for n being Element of N st n in H holds z*n = n*z) implies
  z is Element of Z;

  thus z is Element of Z implies (for n being Element of N st n in H
  holds z*n = n*z) by C1;
end;
```

This code is used in chunk 115.

References

[BBG+15] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pak, and Josef Urban, *Mizar: State-of-the-art and beyond*, International Conference on Intelligent Computer Mathematics, Springer, 2015, pp. 261–279.

[BBG+18] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk, *The role of the mizar mathematical library for interactive proof development in mizar*, Journal of Automated Reasoning **61** (2018), no. 1, 9–32.

[DF04] David S Dummit and Richard M Foote, *Abstract Algebra*, Third ed., Wiley and Sons, 2004.

[Gor80] Daniel Gorenstein, *Finite Groups*, Second ed., Chelsea Publishing Company, 1980.
[Isa08] I. Martin Isaacs, *Finite Group Theory*, Graduate Studies in Mathematics, vol. 92, American Mathematical Society, 2008.
[Kor15] Artur Korniłowicz, *Definitional expansions in Mizar*, Journal of Automated Reasoning **55** (2015), no. 3, 257–268.

MML Bibliography

[ALGSTR_0] Mizar Library Committee, *Basic Algebraic Structures*, Eprint: http://mizar.org/version/current/html/algstr_0.html, 2007.
[AUTGROUP] Artur Korniłowicz, *On the Group of Inner Automorphisms*, Formaliz.Math. **5** (1996), no. 1, 43–45, Eprint: http://fm.mizar.org/1996-5/pdf5-1/autgroup.pdf.
[BIRKHOFF] ———, *Birkhoff Theorem for Many Sorted Algebras*, Formaliz.Math. **6** (1997), no. 3, 389–395, Eprint: http://fm.mizar.org/1997-6/pdf6-3/birkhoff.pdf.
[CARD_3] Grzegorz Bancerek, *König's Theorem*, Formaliz.Math. **1** (1990), no. 3, 589–593, Eprint: http://fm.mizar.org/1990-1/pdf1-3/card_3.pdf.
[CAT_1] Czesław Byliński, *Introduction to Categories and Functors*, Formaliz.Math. **1** (1990), no. 2, 409–420, Eprint: http://fm.mizar.org/1990-1/pdf1-2/cat_1.pdf.
[CAT_8] Marco Riccardi, *Exponential Objects*, Formaliz.Math. **23** (2015), no. 4, 351–369.
[CAYLEY] Artur Korniłowicz, *Cayley's Theorem*, Formaliz.Math. **19** (2011), no. 4, 223–225.
[FINSEQ_1] Grzegorz Bancerek and Krzysztof Hryniewiecki, *Segments of Natural Numbers and Finite Sequences*, Formaliz.Math. **1** (1990), no. 1, 107–114, Eprint: http://fm.mizar.org/1990-1/pdf1-1/finseq_1.pdf.
[FINSOP_1] Wojciech A. Trybulec, *Binary Operations on Finite Sequences*, Formaliz.Math. **1** (1990), no. 1, 979–981, Eprint: http://fm.mizar.org/1990-1/pdf1-5/finsop_1.pdf.
[FUNCOP_1] Andrzej Trybulec, *Binary Operations Applied to Functions*, Formaliz.Math. **1** (1990), no. 2, 329–334, Eprint: http://fm.mizar.org/1990-1/pdf1-2/funcop_1.pdf.
[FUNCT_1] Czesław Byliński, *Functions and Their Basic Properties*, Formaliz.Math. **1** (1990), no. 1, 55–65, Eprint: http://fm.mizar.org/1990-1/pdf1-1/funct_1.pdf.
[FUNCT_2] ———, *Functions from a Set to a Set*, Formaliz.Math. **1** (1990), no. 1, 153–164, Eprint: http://fm.mizar.org/1990-1/pdf1-1/funct_2.pdf.
[GR_CY_1] Dariusz Surowik, *Cyclic Groups and Some of Their Properties – Part I*, Formaliz.Math. **2** (1991), no. 5, 623–627, Eprint: http://fm.mizar.org/1991-2/pdf2-5/gr_cy_1.pdf.
[GRNILP_1] Dailu Li, Xiquan Liang, and Yanhong Men, *Nilpotent groups*, Formaliz.Math. **18** (2010), no. **1**, 53–56.
[GROUP_1] Wojciech A. Trybulec, *Groups*, Formaliz.Math. **1** (1990), no. 5, 821–827, Eprint: http://fm.mizar.org/1990-1/pdf1-5/group_1.pdf.
[GROUP_2] ———, *Subgroup and Cosets of Subgroups*, Formaliz.Math. **1** (1990), no. 5, 855–864, Eprint: http://fm.mizar.org/1990-1/pdf1-5/group_2.pdf.
[GROUP_3] Wojciech A Trybulec, *Classes of conjugation. normal subgroups*, Formaliz.Math. **1** (1990), no. 5, 955–962, Eprint: http://fm.mizar.org/fm/1990-1/pdf1-5/group_3.pdf.
[GROUP_4] Wojciech A. Trybulec, *Lattice of Subgroups of a Group. Frattini Subgroup*, Formaliz.Math. **2** (1991), no. 1, 41–47, Eprint: http://fm.mizar.org/1991-2/pdf2-1/group_4.pdf.
[GROUP_5] Wojciech A Trybulec, *Commutator and Center of a Group*, Formaliz.Math. **2** (1991), no. 4, 461–466, Eprint: https://fm.mizar.org/1991-2/pdf2-4/group_5.pdf.
[GROUP_6] Wojciech A Trybulec and Michał J Trybulec, *Homomorphisms and Isomorphisms of Groups. Quotient Group*, Formaliz.Math. **2** (1991), no. 4, 573–578, Eprint: https://fm.mizar.org/1991-2/pdf2-4/group_6.pdf.
[GROUP_7] Artur Korniłowicz, *The Product of the Families of the Groups*, Formaliz.Math. **7** (1998), no. 1, 127–134, Eprint: http://fm.mizar.org/1998-7/pdf7-1/group_7.pdf.
[GROUP_8] Gijs Geleijnse and Grzegorz Bancerek, *Properties of Groups*, Formaliz.Math. **12** (2004), no. 3, 347–350, Eprint: https://fm.mizar.org/2004-12/pdf12-3/group_8.pdf.
[GROUP_9] Marco Riccardi, *The Jordan-Hölder Theorem*, Formaliz.Math. **15** (2007), no. 2, 35–51, Eprint: https://fm.mizar.org/2007-15/pdf15-2/group_9.pdf.
[GROUP_10] ———, *The Sylow Theorems*, Formaliz.Math. **15** (2007), no. 3, 159–165, Eprint: https://fm.mizar.org/2007-15/pdf15-3/group_10.pdf.
[GROUP_12] Hiroyuki Okazaki, Kenichi Arai, and Yasunari Shidama, *Normal Subgroup of Product of Groups*, Formaliz.Math. **19** (2011), no. 1, 23–26.

[Group_17] Hiroyuki Okazaki, Hiroshi Yamazaki, and Yasunari Shidama, *Isomorphisms of Direct Products of Finite Commutative Groups*, Formaliz.Math. **21** (2013), no. 1, 65–74.

[Group_19] Kazuhisa Nakasho, Hiroshi Yamazaki, Hiroyuki Okazaki, and Yasunari Shidama, *Definition and Properties of Direct Sum Decomposition of Groups*, Formaliz.Math. **23** (2015), no. 1, 15–27.

[Group_20] Kazuhisa Nakasho, Hiroyuki Okazaki, Hiroshi Yamazaki, and Yasunari Shidama, *Equivalent Expressions of Direct Sum Decomposition of Groups*, Formaliz.Math. **23** (2015), no. 1, 67–73.

[Group_21] Kazuhisa Nakasho, Hiroshi Yamazaki, Hiroyuki Okazaki, and Yasunari Shidama, *Conservation Rules of Direct Sum Decomposition of Groups*, Formaliz.Math. **24** (2016), no. 1, 81–94.

[Int_2] Rafał Kwiatek and Grzegorz Zwara, *The divisibility of integers and integer relatively primes*, Formaliz.Math. **1** (1990), no. **5**, 829–832.

[Int_3] Christoph Schwarzweller, *The Ring of Integers, Euclidean Rings and Modulo Integers*, Formaliz.Math. **8** (1999), no. 1, 29–34, Eprint: http://fm.mizar.org/1999-8/pdf8-1/int_3.pdf.

[Mod_2] Michał Muzalewski, *Rings and Modules–Part II*, Formaliz.Math. **2** (1991), no. 4, 579–585, Eprint: https://fm.mizar.org/fm/1991-2/pdf2-4/mod_2.pdf.

[Mod_4] ———, *Opposite Rings, Modules and their Morphisms*, Formaliz.Math. **3** (1992), no. 1, 57–65, Eprint: http://fm.mizar.org/1992-3/pdf3-1/mod_4.pdf.

[Nat_3] Artur Korniłowicz and Piotr Rudnicki, *Fundamental Theorem of Arithmetic*, Formaliz.Math. **12** (2004), no. **2**, 179–186, Eprint http://fm.mizar.org/2004-12/pdf12-2/nat_3.pdf.

[PBoole] Andrzej Trybulec, *Many sorted Sets*, Formaliz.Math. **4** (1993), no. 1, 15–22, Eprint http://fm.mizar.org/1993-4/pdf4-1/pboole.pdf.

[Pralg_3] Mariusz Giero, *More on Products of Many Sorted Algebras*, Formaliz.Math. **5** (1996), no. 4, 621–626.

[Tarski] Andrzej Trybulec, *Tarski Grothendieck set theory*, Formaliz.Math. **1** (1990), no. 1, 9–11, Eprint: http://fm.mizar.org/1990-1/pdf1-1/tarski.pdf.

[VectSp_1] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski, *Abelian Groups, Fields and Vector Spaces*, Formaliz.Math. **1** (1990), no. 2, 335–342, Eprint: http://fm.mizar.org/1990-1/pdf1-2/vectsp_1.pdf.

[WeddWitt] Broderic Arneson, Matthias Baaz, and Piotr Rudnicki, *Witt's Proof of the Wedderburn Theorem*, Formaliz.Math. **12** (2003), 69–75, Eprint: https://fm.mizar.org/2004-12/pdf12-1/weddwitt.pdf.

[XBoole_0] Mizar Library Committee, *Boolean Properties of Sets - Definitions*, Encyclopedia of Mathematics in Mizar (2002), Eprint: http://mizar.org/JFM/EMM/xboole_0.html.

[Xxreal_1] Andrzej Trybulec, Yatsuka Nakamura, Artur Korniłowicz, and Adam Grabowski, *Basic Properties of Extended Real Numbers*, Eprint: http://mizar.org/version/current/html/xxreal_1.html, 2007.

Index

Mizar Index

Email address: pqnelson@gmail.com
URL: https://pqnelson.github.io