Regular Paper

有限可換群の基本定理の形式化について

On the Formalizations of Basic Theorem for Finite Commutative Group

岡崎 裕之 [1,◕], 山崎　浩 [1,◕], 師玉 康成 [1,*]
Hiroyuki Okazaki[1,◕], Hiroshi Yamazaki[1,◕], Yasunari Shidama[1,*]

1 信州大学工学部, 長野県長野市若里 4-17-1

1 Faculty of Engineering, Shinshu University. 4-17-1 Wakasato, Nagano, Japan

◕These authors contributed equally to this work.
* Corresponding Author: shidama@cs.shinshu-u.ac.jp

Proof checked by Mizar Version: 8.1.11 and MML Version: 5.65.1394
Received: April 16, 2021, Accepted: TBA, Published: TBA

Abstract

In this paper, we formalized some theorems concerning the product of cyclic groups. In this article, we present the generalized formalization of [1]. First, we formalize that every finite commutative group which order is composite number is isomorphic to a direct product of finite commutative groups which orders are relative prime. Next, we formalize finite direct products of finite commutative groups.

1　はじめに

有限可換群の基本定理の形式化について報告する．有限可換群の議論は代数学分野で重要な基礎であり，暗号理論等，情報工学分野でも重要な道具になっている．この報告は，有限可換群 G には，その位数の素因数分解列に現れる素数因数の累乗を位数とする可換部分群の族が与えられ，G はこの族の直積に分解されることの形式化について述べている．

2　有限可換族の直積分解

2.1　形式化の方針

基本的な形式化の方針は，先ず，有限可換群 G の位数 $card\, G$ が互いに素な自然数 h, k の積で表されるとき，G の部分群でそれぞれの位数が h, k である H, K が存在し，G が

H, K の直積に分解されることを示す以下の補題 [GROUP_17 - Th.16] の形式化を行い，ついで，G の位数 $card\ G$ の素因数分解

$$card\ G = {p_1}^{n_1} \cdot {p_2}^{n_2} \cdots {p_l}^{n_l}$$

によって, この補題を繰り返し適用し，G が部分群の列

$$H_1, H_2, \cdots H_l$$

の直積に分解することを示すというものである．

Listing 1. GROUP_17 - Th.16

```
theorem :: GROUP_17:16
  for G being finite commutative Group,
  h,k be Nat
  st card G = h*k & h,k are_coprime holds
  ex H,K being strict finite Subgroup of G st
  the carrier of H = {x where x is Element of G: x|^h = 1_G} &
  the carrier of K = {x where x is Element of G: x|^k = 1_G} &
  H is normal & K is normal
  &
  (for x be Element of G holds
  ex a,b be Element of G st a in H & b in K & x = a*b)
  &
  (the carrier of H) /\ (the carrier of K) = {1_G};
```

ここで，素因数列

$$p_1, p_2, \cdots, p_l$$

は G の位数 $card\ G$ によって決まるが，長さ l も，出現する素因数 p_i も，位数 $card\ G$ によって変化し，この列に添え字を付して表すと，今後この定理を利用するたびに，その素数が何であるかを記述しなくてはならず煩雑化が予想される．そのため，位数 $card\ G$ の素因数分解列中に現れる素数そのものを添え字として使う形式化を試みた．その結果，最終的に以下の形式化 [GROUP_17 - Th.34] が得られた．

Listing 2. GROUP_17 - Th.34

```
theorem :: GROUP_17:34
  for G being strict finite commutative Group
  st card G > 1
  holds
   ex I be non empty finite set,
   F be associative Group-like commutative multMagma-Family of I,
   HFG be Homomorphism of product F ,G
   st I = support (prime_factorization card G )
        & (for p be Element of I holds
             F.p is strict finite commutative Group
             &
             F.p is Subgroup of G
             &
             card (F.p) = (prime_factorization card G ).p )
   &
   (for p,q be Element of I st p <> q holds
        (the carrier of (F.p) ) /\ (the carrier of (F.q) ) ={1_G})
   &
   HFG is bijective
   &
   for x be (the carrier of G)-valued total I -defined Function
   st for p be Element of I holds x.p in F.p
   holds x in product F & HFG.x =Product x;
```

上記は G の部分群の直積との G 同型を与える定理であるが，これを使えば G の部分群による直積分解は以下 [GROUP_17 - Th.35] のように得られる．

Listing 3. GROUP_17 - Th.35

```
theorem :: GROUP_17:35
  for G being strict finite commutative Group st card G > 1 holds
  ex I be non empty finite set,
  F be associative Group−like commutative multMagma−Family of I st
  I = support (prime_factorization card G)
  & (for p be Element of I holds F.p is strict Subgroup of G &
  card (F.p) = (prime_factorization card G).p) &
  (for p,q be Element of I st p <> q holds
  (the carrier of (F.p)) /\ (the carrier of (F.q)) = {1_G})
  &
  (for y be Element of G
    ex x be (the carrier of G)−valued total I −defined Function
  st (for p be Element of I holds x.p in F.p) & y = Product x)
  &
  for x1,x2 be (the carrier of G)−valued total I −defined Function st
  (for p be Element of I holds x1.p in F.p) &
  (for p be Element of I holds x2.p in F.p) &
  Product x1 = Product x2 holds x1=x2;
```

2.2 有限可換群の直積分解

上の記述中に現れる

$$support\ (prime\_factorization\ card\ G)$$

は $card\ G$ の素因数全ての集合を表している．

$$prime\_factorization\ card\ G$$

は素数全ての集合から自然数への写像で，各素数 p に対して，$card\ G$ の素因数分解中に現れる p の指数を対応させる．ここで，p がその素因数分解中に現れない場合は値 0 を対応させている．f を任意の関数とするとき，$supportf$ は f の台集合を表しており，関数 f の値が 0 でない f の定義域の元の全ての集合である．

この $I = prime\_factorization\ card\ G$ によって添え字付けられた G の元の族や，部分群の族

$$\{x_p\}_{p\in I}, \{H_p\}_{p\in I}$$

について，それらの積

$$\prod_{p\in I} x_p, \quad \prod_{p\in I} H_p$$

を使って形式化を行う．後者については既存のライブラリには以下 [GROUP_7 - Def.2] で定義されている [2]．

Listing 4. GROUP_7 - Def.2

```
definition
  let I be set, F be multMagma−Family of I;
  func product F −> strict multMagma means :: GROUP_7:def 2
  the carrier of it = product
Carrier F & for f, g being Element of product Carrier F, i being set st i in I
```

```
ex Fi being non empty multMagma, h being Function st Fi = F.i & h = (the multF
  of it).(f,g) & h.i = (the multF of Fi).(f.i,g.i);
end;
```

前者に関しては，既存のライブラリには以下 [GROUP_4 - Def.2] で定義されている [3].

Listing 5. GROUP_4 - Def.2

```
definition
  let G be non empty multMagma;
  let F be FinSequence of the carrier of G;
  func Product F -> Element of G equals :: GROUP_4:def 2
  (the multF of G) "**" F;
end;
```

これは自然数の部分集合

$$Seg\ n = \{k\ where\ k\ is\ Nat : 1 \leq k \wedge k \leq n\}$$

上の関数である有限列に対しての定義 [2] であり，任意の空でない有限集合上の関数については定義されていないので，以下 [GROUP_17 - Def.1] のように新たに定義した.

Listing 6. GROUP_17 - Def.1

```
definition
  let G be non empty multMagma,
      I be finite set,
      b be (the carrier of G)-valued
         total I -defined Function;
 func Product b -> Element of G means :: GROUP_17:def 1
 ex f being FinSequence of the carrier of G
       st it = Product f & f = b*canFS(I);
end;
```

目的の定理の証明には位数 $card\ G$ の素因数分解列の長さによる帰納法を用いる．これに伴い，G の元の族 $\{x_p\}_{p\in I}$ の積

$$\prod_{p\in I} x_p$$

についても I の要素 q を一つ選び,q とそれ以外の I の要素に分け,

$$\prod_{p\in I} x_p = \prod_{p\in I\setminus\{q\}} x_p \cdot x_q$$

のように部分積に分解する必要がある．このため以下の補題を形式化した.

Listing 7. GROUP_17 - Th.8–9

```
theorem :: GROUP_17:8
  for G being commutative Group,
  A,B being non empty finite set,
  FA be (the carrier of G)-valued total A -defined Function,
  FB be (the carrier of G)-valued total B -defined Function,
  FAB be (the carrier of G)-valued total A \/ B -defined Function
  st A misses B & FAB = FA +* FB holds
```

```
  Product (FAB) = (Product FA) * (Product FB);

theorem :: GROUP_17:9
  for G being non empty multMagma,
  q be set,
  z be Element of G,
  f be (the carrier of G)−valued total {q}−defined Function
  st f = q .−−> z
  holds Product f = z;
```

冒頭に述べたように，先ず補題 [GROUP_17 - Th.16] の形式化を行った．これは有限可換群 G の位数 $cardG$ が互いに素な，自然数 h, k の積で表されるとき，G の部分群でそれぞれの位数が h, k である H, K が存在し，G が H, K の直積に分解されることをを示す補題である．

このための，一般の群 G の 2 つの正規部分群 A, B について，それらの共通部分が G の単位元だけからなる場合に A, B の元が可換になること，また A, B の直積から G への同型が与えられることを表す以下の命題を形式化した．

Listing 8. GROUP_17 - Th.11–12

```
theorem :: GROUP_17:11
  for G being Group, A,B being normal Subgroup of G st
  (the carrier of A) /\ (the carrier of B) = {1_G} holds
  for a,b be Element of G st a in A & b in B holds a*b = b*a;

theorem :: GROUP_17:12
  for G being Group, A,B being normal Subgroup of G st
  (for x be Element of G holds
  ex a,b be Element of G st a in A & b in B & x = a*b)
  & (the carrier of A) /\ (the carrier of B) = {1_G} holds
  ex h being Homomorphism of product <*A,B*>,G st h is bijective
  & for a,b be Element of G st a in A & b in B
  holds h.(<*a,b*>) = a*b;
```

以上の一般的な命題の準備をもとに，有限可換群 G の要素 x で $x^m = 1_G$ となる全ての元の集合が G の可換な正規部分群になることを示す補題と，その部分群 H の位数と素因数についての補題を経由して目的の [GROUP_17 - Th.16] を形式化した．

[GROUP_17 - Th.16] からは以下の [GROUP_17 - Th.18] のように G の直積分解を与える部分群 H, K の直積と G との同型の存在定理も直ぐに従う．この定理を G の位数に関する帰納法を用いて繰り返し適用するために必要な補題 [GROUP_17:2,7] も形式化した。

Listing 9. GROUP_17 - Th.18

```
theorem :: GROUP_17:18
  for G being finite commutative Group,
  h,k be non zero Nat
  st card G = h*k & h,k are_coprime
  ex H,K being strict finite Subgroup of G st
  card H = h & card K = k &
  (the carrier of H) /\ (the carrier of K) = {1_G} &
  ex F being Homomorphism of product <*H,K*>,G
  st F is bijective
  & for a,b be Element of G st a in H & b in K
  holds F.(<*a,b*>) = a*b;
```

2.3 有限可換群の有限直積分解

冒頭に述べたように，G の位数に関する帰納法は，G の位数 $card\ G$ の素因数分解

$$card\ G = \prod_{p \in I} p^{n_p}$$

$$I = prime\_factorization\ card\ G$$

によって, この補題を繰り返し適用し，G が部分群の族

$$\{H_p\}_{pinI}$$

の直積に分解することを示すものである．

これには，上の素因数分解の結果を素因数 q とそれ以外の素因数に分け，

$$card\ G = \prod_{p \in I \setminus \{q\}} p^{n_p} \cdot q^{n_q}$$

のように 2 つの積に表し，これらを位数にもつ G の 2 つの部分群 H, K を構成する．

次に，位数

$$\prod_{p \in I \setminus \{q\}} p^{n_p}$$

をもつ G の部分群 H について，帰納法の仮定によって，その直積分解

$$\{H_p\}_{p \in \setminus \{q\}}$$

を構成し，この族に K を加えた G の部分族と G の同型を構成する手順をとった．この手順を実行するために一連の補題 [GROUP_17:19–33] を形式化し，目標とした定理 [GROUP_17 - Th.34] を得た．

3 まとめ

進行中の有限可換群の基本定理の形式化について状況を報告した．形式化数学の視点からは，有限可換群 G の位数 $card\ G$ の素因数分解中に現れる素数 p を直に G の直積分解を与える G の部分族の添え字に使ったところに従来にない形式化の特徴がある．なお，直積分解に現れた部分群 H_p は可換 p-群な部分群になる．素数 p の累乗を位数とする群は p-群と呼ばれるが，可換な p-群はいくつかの巡回群の族の直積と同型になることが知られている．

以後の形式化でこの定理を引用する際の表現の簡潔化が期待できる．有限群の議論は周知のように未解決課題もあり，精緻で深い内容を持っている．本稿の読者にはこれに興味を持たれ，筆者らへの助力やライブラリ構築に参加して頂ければ幸いである．

参考文献

[1] Arai K, Okazaki H, Shidama Y. Isomorphisms of Direct Products of Finite Cyclic Groups. Formalized Mathematics. 2012;20(**4**):343–347.

[2] Korniłowicz A. The Product of the Families of the Groups. Formalized Mathematics. 1998;7(**1**):127–134. Available from: `http://fm.mizar.org/1998-7/pdf7-1/group_7.pdf`.

[3] Trybulec WA. Lattice of Subgroups of a Group. Frattini Subgroup. Formalized Mathematics. 1991;2(**1**):41–47. Available from: `http://fm.mizar.org/1991-2/pdf2-1/group_4.pdf`.

Mizar article information

Works in Progress

GROUP_17 Isomorphisms of Direct Products of Finite Commutative Groups
by Hiroyuki Okazaki, Hiroshi Yamazaki and Yasunari Shidama

Summary: We have been working on the formalization of groups. In [1], we encoded some theorems concerning the product of cyclic groups. In this article, we present the generalized formalization of [1]. First, we show that every finite commutative group which order is composite number is isomorphic to a direct product of finite commutative groups which orders are relatively prime. Next, we describe finite direct products of finite commutative groups.

Listing 10. GROUP_17 - abstract

```
:: Isomorphisms of Direct Products of Finite Commutative Groups
:: by Hiroyuki Okazaki , Hiroshi Yamazaki and Yasunari Shidama

environ

 vocabularies FINSEQ_1, FUNCT_1, RELAT_1, RLVECT_2, CARD_3, TARSKI, BINOP_1,
      GROUP_1, XXREAL_0, GROUP_2, CARD_1, FUNCT_4, GROUP_6, GROUP_7, FUNCOP_1,
      ALGSTR_0, PARTFUN1, FUNCT_2, SUBSET_1, XBOOLE_0, STRUCT_0, NAT_1,
      ORDINAL4, PRE_TOPC, ARYTM_1, ARYTM_3, FINSET_1, INT_2, ZFMISC_1, PBOOLE,
      NEWTON, INT_1, NAT_3, REAL_1, PRE_POLY, XCMPLX_0, UPROOTS, INT_7;
 notations TARSKI, XBOOLE_0, ZFMISC_1, SUBSET_1, RELAT_1, FUNCT_1, ORDINAL1,
      RELSET_1, PARTFUN1, FUNCT_2, DOMAIN_1, FUNCOP_1, FUNCT_4, FINSET_1,
      CARD_1, PBOOLE, CARD_3, NUMBERS, XCMPLX_0, XXREAL_0, XREAL_0, NAT_1,
      INT_1, INT_2, BINOP_1, FINSEQ_1, NEWTON, PRE_POLY, NAT_3, STRUCT_0,
      ALGSTR_0, GROUP_1, GROUP_2, GROUP_3, GROUP_4, GROUP_6, PRALG_1, GROUP_7,
      INT_7;
 constructors BINOP_1, REALSET1, GROUP_6, MONOID_0, PRALG_1, GROUP_4, CARD_2,
      GROUP_7, RELSET_1, WELLORD2, NAT_D, INT_7, RECDEF_1, NAT_3, FINSOP_1;
 registrations XBOOLE_0, XREAL_0, STRUCT_0, GROUP_2, MONOID_0, FUNCT_2, CARD_1,
      CARD_3, GROUP_7, GROUP_3, RELSET_1, FINSEQ_1, INT_1, AOFA_000, GR_CY_1,
      FINSET_1, NAT_3, RELAT_1, FUNCT_1, MEMBERED, FUNCOP_1, NEWTON, VALUED_0,
      PRE_POLY, PBOOLE, INT_7, GROUP_6, ORDINAL1;
 requirements NUMERALS, SUBSET, ARITHM, BOOLE;


begin :: Preliminaries

theorem :: GROUP_17:1
  for A,B,A1,B1 be set st A misses B
  & A1 c= A & B1 c= B & A1 \/ B1 = A \/ B holds
  A1 = A & B1 = B;

theorem :: GROUP_17:2
  for H,K be non empty finite set holds
  card product (<* H, K *>) = card(H)*card(K);
```

```
theorem :: GROUP_17:3
  for ps,pt,f be bag of SetPrimes,
  q being Nat
  st (support ps) misses (support pt) & f = ps + pt & q in (support ps) holds
  ps.q = f.q;

theorem :: GROUP_17:4
  for ps,pt,f be bag of SetPrimes,
  q being Nat
  st (support ps) misses (support pt) & f = ps + pt & q in (support pt) holds
  pt.q = f.q;

theorem :: GROUP_17:5
  for h be non zero Nat, q being Prime
  st not q,h are_coprime holds
  q divides h;

theorem :: GROUP_17:6
  for h,s be non zero Nat
  st for q being Prime st q in support (prime_factorization s)
  holds not q,h are_coprime holds
  support (prime_factorization s) c= support (prime_factorization h);

theorem :: GROUP_17:7
  for h,k,s,t be non zero Nat
  st h,k are_coprime & s * t = h * k
  & (for q being Prime st q in support prime_factorization s
  holds not q,h are_coprime)
  & (for q being Prime st q in support prime_factorization t
  holds not q,k are_coprime)
  holds
  s = h & t = k;

definition
  let G be non empty multMagma,
  I be finite set,
  b be (the carrier of G)-valued total I -defined Function;
  func Product b -> Element of G means
:: GROUP_17:def 1
  ex f being FinSequence of G st it = Product f & f = b*canFS(I);
end;

theorem :: GROUP_17:8
  for G being commutative Group,
  A,B being non empty finite set,
  FA be (the carrier of G)-valued total A -defined Function,
  FB be (the carrier of G)-valued total B -defined Function,
  FAB be (the carrier of G)-valued total A \/ B -defined Function
  st A misses B & FAB = FA +* FB holds
  Product (FAB) = (Product FA) * (Product FB);

theorem :: GROUP_17:9
  for G being non empty multMagma,
  q be set,
  z be Element of G,
  f be (the carrier of G)-valued total {q}-defined Function
  st f = q .--> z
  holds Product f = z;

begin :: Direct Product of Finite Commutative Groups

theorem :: GROUP_17:10
  for X,Y being non empty multMagma holds
  the carrier of product <*X,Y*>
  = product <* the carrier of X,the carrier of Y *>;

theorem :: GROUP_17:11
  for G being Group, A,B being normal Subgroup of G st
```

```
  (the carrier of A) /\ (the carrier of B) = {1_G} holds
  for a,b be Element of G st a in A & b in B holds a*b = b*a;

theorem :: GROUP_17:12
  for G being Group, A,B being normal Subgroup of G st
  (for x be Element of G holds
  ex a,b be Element of G st a in A & b in B & x = a*b)
  & (the carrier of A) /\ (the carrier of B) = {1_G} holds
  ex h being Homomorphism of product <*A,B*>,G st h is bijective
  & for a,b be Element of G st a in A & b in B
  holds h.(<*a,b*>) = a*b;

theorem :: GROUP_17:13
  for G being finite commutative Group,
  m be Nat,
  A be Subset of G
  st A ={x where x is Element of G: x|^m = 1_G}
  holds
  A <> {}
  &
  (for g1,g2 be Element of G
  st g1 in A & g2 in A holds g1 * g2 in A) &
  for g be Element of G st g in A holds g" in A;

theorem :: GROUP_17:14
  for G being finite commutative Group,
  m be Nat,
  A be Subset of G
  st A ={x where x is Element of G: x|^m = 1_G} holds
  ex H being strict finite Subgroup of G
  st the carrier of H = A & H is commutative normal;

theorem :: GROUP_17:15
  for G being finite commutative Group,
  m be Nat,
  H being finite Subgroup of G
  st the carrier of H = {x where x is Element of G: x|^m = 1_G} holds
  for q being Prime st q in support prime_factorization card H
  holds not q,m are_coprime;

theorem :: GROUP_17:16
  for G being finite commutative Group,
  h,k be Nat
  st card G = h*k & h,k are_coprime holds
  ex H,K being strict finite Subgroup of G st
  the carrier of H = {x where x is Element of G: x|^h = 1_G} &
  the carrier of K = {x where x is Element of G: x|^k = 1_G} &
  H is normal & K is normal
  &
  (for x be Element of G holds
  ex a,b be Element of G st a in H & b in K & x = a*b)
  &
  (the carrier of H) /\ (the carrier of K) = {1_G};

theorem :: GROUP_17:17
  for H,K be finite Group holds
  card product (<* H, K *>) = card(H)*card(K);

theorem :: GROUP_17:18
  for G being finite commutative Group,
  h,k be non zero Nat
  st card G = h*k & h,k are_coprime
  ex H,K being strict finite Subgroup of G st
  card H = h & card K = k &
  (the carrier of H) /\ (the carrier of K) = {1_G} &
  ex F being Homomorphism of product <*H,K*>,G
  st F is bijective
  & for a,b be Element of G st a in H & b in K
  holds F.(<*a,b*>) = a*b;
```

begin :: *Finite Direct Products of Finite Commutative Groups*

theorem :: *GROUP_17:19*
for G **be** Group,
q **be set**,
F **be** associative Group−like multMagma−Family **of** {q},
f **being** Function **of** G,product F **st** F = q .−−> G **&**
for x **being** Element **of** G **holds** f . x = q .−−> x **holds**
f **is** Homomorphism **of** G,(product F);

theorem :: *GROUP_17:20*
for G **be** Group,
q **be set**,
F **be** associative Group−like multMagma−Family **of** {q},
f **being** Function **of** G,product F **st** F = q .−−> G **&**
for x **being** Element **of** G **holds** f . x = q .−−> x **holds**
f **is** bijective;

theorem :: *GROUP_17:21*
for q **be set**,
F **be** associative Group−like multMagma−Family **of** {q},
G **be** Group **st** F = q .−−> G **holds**
ex I **be** Homomorphism **of** G,product F **st**
I **is** bijective **&**
for x **being** Element **of** G **holds** I . x = q .−−> x;

theorem :: *GROUP_17:22*
for I0,I **be non** empty finite **set**,
F0 **be** associative Group−like multMagma−Family **of** I0,
F **be** associative Group−like multMagma−Family **of** I,
H,K **be** Group,
q **be** Element **of** I,
k **be** Element **of** K,
g **be** Function **st**
g in **the** carrier **of** product F0 **&**
not q in I0 **&** I = I0 \/ {q} **&** F = F0 +∗ (q .−−> K) **holds**
g +∗ (q .−−> k) in **the** carrier **of** product F;

theorem :: *GROUP_17:23*
for I0,I **be non** empty finite **set**,
F0 **be** associative Group−like multMagma−Family **of** I0,
F **be** associative Group−like multMagma−Family **of** I,
H,K **be** Group,
q **be** Element **of** I,
G0 **be** Function **of** H,product F0 **st**
G0 **is** Homomorphism **of** H,product F0
& G0 **is** bijective **& not** q in I0 **&** I = I0 \/ {q} **&** F = F0 +∗ (q .−−> K) **holds**
for G **be** Function **of** product <∗H,K∗>,(product F) **st**
for h **be** Element **of** H,k **be** Element **of** K
holds ex g **be** Function
st g=G0.h **&** G.(<∗h,k∗>) = g +∗ (q .−−> k) **holds**
G **is** Homomorphism **of** product <∗H,K∗>,product F;

theorem :: *GROUP_17:24*
for I0,I **be non** empty finite **set**,
F0 **be** associative Group−like multMagma−Family **of** I0,
F **be** associative Group−like multMagma−Family **of** I,
H,K **be** Group,
q **be** Element **of** I,
G0 **be** Function **of** H, product F0 **st**
G0 **is** Homomorphism **of** H, product F0
& G0 **is** bijective
& not q in I0 **&** I = I0 \/ {q} **&** F = F0 +∗ (q .−−> K) **holds**
for G **be** Function **of** product <∗H,K∗>, product F **st**
for h **be** Element **of** H,k **be** Element **of** K
holds ex g **be** Function
st g=G0.h **&** G.(<∗h,k∗>) = g +∗ (q .−−> k)
holds G **is** bijective;

```
theorem :: GROUP_17:25
  for q be set,
  F be multMagma–Family of {q},
  G be non empty multMagma st
  F = q .––> G holds
  for y be (the carrier of G)–valued total {q} –defined Function holds
  y in the carrier of product F & y.q in the carrier of G &
  y= q .––> y.q;

theorem :: GROUP_17:26
  for q be set,
  F be associative Group–like multMagma–Family of {q},
  G be Group st F = q .––> G holds
  ex HFG be Homomorphism of product F,G st
  HFG is bijective &
  for x be (the carrier of G)–valued total {q} –defined Function
  holds HFG.x = Product x;

theorem :: GROUP_17:27
  for I0,I be non empty finite set,
  F0 be associative Group–like multMagma–Family of I0,
  F be associative Group–like multMagma–Family of I,
  H,K be Group,
  q be Element of I,
  G0 be Homomorphism of H,(product F0) st
  not q in I0 & I = I0 \/ {q} & F = F0 +* (q .––> K) & G0 is bijective
  ex G be Homomorphism of product <*H,K*>,(product F) st
  G is bijective &
  for h be Element of H,k be Element of K
  ex g be Function st g=G0.h & G.(<*h,k*>) = g +* (q .––> k);

theorem :: GROUP_17:28
  for I0,I be non empty finite set,
  F0 be associative Group–like multMagma–Family of I0,
  F be associative Group–like multMagma–Family of I,
  H,K be Group,
  q be Element of I,
  G0 be Homomorphism of product F0, H st not q in I0 &
  I = I0 \/ {q} & F = F0 +* (q .––> K) & G0 is bijective holds
  ex G be Homomorphism of product F, product <*H,K*> st G is bijective &
  for x0 be Function,
  k be Element of K,
  h be Element of H
  st h = G0.x0 & x0 in product F0 holds
  G.(x0 +* (q .––>k)) = <* h, k *>;

theorem :: GROUP_17:29
  for I be non empty finite set,
  F be associative Group–like multMagma–Family of I,
  x be total I –defined Function
  st for p be Element of I holds x.p in F.p
  holds x in the carrier of product F;

theorem :: GROUP_17:30
  for I0,I be non empty finite set,
  F0 be associative Group–like multMagma–Family of I0,
  F be associative Group–like multMagma–Family of I,
  K be Group,
  q be Element of I,
  x be Element of product F st
  not q in I0 & I = I0 \/ {q} & F = F0 +* (q .––> K) holds
  ex x0 be total I0 –defined Function,
  k be Element of K st x0 in product F0
  & x = x0 +* (q .––> k) & for p be Element of I0 holds x0.p in F0.p;

theorem :: GROUP_17:31
  for G be Group,
  H be Subgroup of G,
```

```
  f being FinSequence of G,
  g being FinSequence of H
  st f=g
  holds Product f = Product g;

theorem :: GROUP_17:32
  for I be non empty finite set,
  G be Group,
  H be Subgroup of G,
  x be (the carrier of G)−valued total I −defined Function,
  x0 be (the carrier of H)−valued total I −defined Function
  st x=x0
  holds Product x = Product x0;

theorem :: GROUP_17:33
  for G being commutative Group,
  I0,I be non empty finite set,
  q be Element of I,
  x be (the carrier of G)−valued total I −defined Function,
  x0 be (the carrier of G)−valued total I0 −defined Function,
  k be Element of G st
  not q in I0 & I = I0 \/ {q} & x = x0 +* (q .−−> k)
  holds
  Product x = (Product x0)*k;

theorem :: GROUP_17:34
  for G being strict finite commutative Group
  st card G > 1 holds
  ex I be non empty finite set,
  F be associative Group−like commutative multMagma−Family of I,
  HFG be Homomorphism of product F,G st
  I = support (prime_factorization card G)
  & (for p be Element of I holds F.p is strict Subgroup of G &
  card (F.p) = (prime_factorization card G).p) &
  (for p,q be Element of I st p <> q holds
  (the carrier of (F.p)) /\ (the carrier of (F.q)) = {1_G}) &
  HFG is bijective &
  for x be (the carrier of G)−valued total I −defined Function
  st for p be Element of I holds x.p in F.p
  holds x in product F & HFG.x = Product x;

theorem :: GROUP_17:35
  for G being strict finite commutative Group st card G > 1 holds
  ex I be non empty finite set,
  F be associative Group−like commutative multMagma−Family of I st
  I = support (prime_factorization card G)
  & (for p be Element of I holds F.p is strict Subgroup of G &
  card (F.p) = (prime_factorization card G).p) &
  (for p,q be Element of I st p <> q holds
  (the carrier of (F.p)) /\ (the carrier of (F.q)) = {1_G})
  &
  (for y be Element of G
    ex x be (the carrier of G)−valued total I −defined Function
  st (for p be Element of I holds x.p in F.p) & y = Product x)
  &
  for x1,x2 be (the carrier of G)−valued total I −defined Function st
  (for p be Element of I holds x1.p in F.p) &
  (for p be Element of I holds x2.p in F.p) &
  Product x1 = Product x2 holds x1=x2;
```