

Supplement

to

Comparing two formal languages for mathematics: Weak Type Theory and Mizar

Gijs Geleijnse

May 2004

In this supplement, we present our full Mizar formalization of the first chapter of *Grundlagen*. This work is separated in an axioms file: L0 and the main article L1. For the CML text by Landau, we refer to Appendix A of our thesis.

Our work on the translation of the fragment of *The Theory of Groups* into Mizar can be found from page 58. The CML text by Hall can be found in Appendix D of our thesis.

The abstract of the Mizar article on group theory will appear in the *Journal of Formalized Mathematics*. Moreover, this article (GROUP_8) will be added to the MML.

A large part of this work has been done in Białystok. We thank the members of the Mizar group for their assistance.

We have used Mizar version 6.4.02 and MML version 3.64.803 (November 2003).

1 Chapter 1 of *Grundlagen* in Mizar

1.1 The axioms article: L0

```
environ
vocabulary L0, FUNCT_1, ARYTM, ARYTM_1, RELAT_1, ARYTM_3, TARSKI, BOOLE,
  ORDINAL1, ORDINAL2;
notation SUBSET_1, FUNCT_1, FUNCT_2, ARYTM_3, RELAT_1, NUMBERS,
  TARSKI, XBOOLE_0, ORDINAL1, ORDINAL2, ARYTM_0, XCMPLX_0, XREAL_0, NAT_1;
constructors ORDINAL1, FUNCT_2, ARYTM_0, XREAL_0, XCMPLX_0, TARSKI, ARYTM_3,
  ORDINAL2, NAT_1;
clusters XBOOLE_0, RELSET_1, NUMBERS, XREAL_0, ARYTM_3, NAT_1, ORDINAL2;
requirements NUMERALS, REAL, SUBSET, BOOLE, ARITHM;
theorems XBOOLE_0, RELAT_1, SUBSET_1, ZFMISC_1, CARD_2, ORDINAL2, TARSKI,
```

```

CARD_5,ORDINAL1,NAT_1,CARD_1;
definitions TARSKI, XBOOLE_0;
schemes INT_2;

begin

definition
  func NatZahl -> non empty set equals
  :defNZ: NAT \ {0};
  correctness
  proof
    one is non empty natural; then
    one in omega by ORDINAL2:def 21; then
    one in NAT;
    then C: 1 in NAT by CARD_2:20;
    0 <> 1;
    then not(1 in {0}) by TARSKI:def 1;
    then 1 in NAT \ {0} by C, XBOOLE_0:def 4;
    hence thesis;
  end;
end;

definition
  let x be set;
  func x ' equals
  :defPR: succ x;
  correctness;
end;

theorem ax1:
  1 in NatZahl
proof
  one is non empty natural; then
  one in omega by ORDINAL2:def 21; then
  one in NAT;
  then C: 1 in NAT by CARD_2:20;
  0 <> 1;
  then not(1 in {0}) by TARSKI:def 1;
  then 1 in NAT \ {0} by C, XBOOLE_0:def 4;
  hence 1 in NatZahl by defNZ;
end;

theorem ax2:
for k being set st k in NatZahl holds k ' in NatZahl
proof

let k be set;
assume B: k in NatZahl;

```

```

then k in NAT by defNZ, XBOOLE_0:def 4;
then reconsider k as Nat;
k ' = succ k by defPR;
then C: k ' = k +1 by CARD_1:52;
then k ' <> 0 by NAT_1:21;
then k ' in NAT & not k ' in {0} by TARSKI:def 1, C;
then k ' in NatZahl by XBOOLE_0:def 4, defNZ;
hence thesis;
end;

```

```

theorem ax3:
for k being set st k in NatZahl holds k ' <> 1
proof
  let k be set;
  assume l: k in NatZahl;
  assume b: k ' = 1;
  k in succ k by ORDINAL1:10;
  then k in 1 by b,defPR; then
  k in {0} by CARD_5:1; then
  not k in NAT \ {0} by XBOOLE_0:def 4;
  then not k in NatZahl by defNZ;
  hence contradiction by l;
end;

```

```

theorem ax4:
for k,y being set holds k ' = y ' implies k=y
proof
  let k,y be set;
  assume k ' = y '; then
  succ k = y ' by defPR; then
  succ k = succ y by defPR;
  hence thesis by ORDINAL1:12;
end;

```

```

theorem ax5:
for M being set st M c= NatZahl holds
(1 in M & for k being set holds (k in M implies k ' in M)) implies NatZahl c= M
proof
  let M be set; assume a: M c= NatZahl;
  assume that
  b: 1 in M and
  c: for k being set holds (k in M implies k ' in M);
  defpred P[set] means $1 in M;
  a1: P[1] by b;
  b1: for x being Nat st x >= 1 & P[x] holds P[x+1]
  proof
    let x be Nat;
    assume x >= 1 & P[x];

```

```

        then P[x ' ] by c;
        then P[succ x] by defPR;
        hence P[x+1] by CARD_1:52;
    end;
f: for x being Nat st x>=1 holds P[x] from Ind1(a1,b1);
thus NatZahl c= M
proof
    let a be set; assume a in NatZahl; then
    a in NAT \ {0} by defNZ; then
n:   a in NAT & not a in {0} by XBOOLE_0:def 4; then
    reconsider n=a as Nat;
    per cases;
    suppose n=0;
    hence thesis by n,TARSKI:def 1;
    suppose n<>0; then
    n > 0 by NAT_1:19; then
o:   n >= 0+1 by NAT_1:38;
    hence a in M by f;
    end;
end;
end;

```

1.2 The main article: L1

environ

```

vocabulary TARSKI, LO, FUNCT_1, ORDINAL2, L1;
notation LO, TARSKI, FUNCT_1;
constructors LO, TARSKI, FUNCT_1;
theorems LO, TARSKI;
definitions TARSKI;
schemes XBOOLE_0;

```

begin

```

reserve x,y,z for set;

```

```

for x, y st x in NatZahl & y in NatZahl holds
x = y or x <> y;

```

```

for x being set st
x in NatZahl
holds x = x;

```

```

for x,y being set st

```

```
x in NatZahl & y in NatZahl
holds
x = y implies y = x;
```

```
for x,y,z being set st
x in NatZahl & y in NatZahl & z in NatZahl
holds x = y & y = z implies x = z;
```

:: page 26

```
reserve a,b,c,d,e,f,g,h,i for set;
```

```
for x, y st x in NatZahl &
y in NatZahl holds
x = y implies x ' = y ';
```

:: page 27

```
:: Satz 1
theorem satz1:
for x,y st x in NatZahl & y in NatZahl holds
x <> y implies x ' <> y '
proof
let x,y be set such that x in NatZahl & y in NatZahl;
assume that A0: x<>y and A1: x ' = y ' ;
x = y by A1,L0:4;
then contradiction by A0;
hence thesis;
end;
```

```
:: Satz 2
theorem satz2:
for x st x in NatZahl holds
x ' <> x
proof
let x such that B0: x in NatZahl;
defpred P[set] means $1 ' <> $1;
consider M being set such that C0: for x being set holds
x in M iff x in NatZahl & P[x] from Separation;
```

```
A0: M c= NatZahl
```

```

proof
  let A be set;
  assume A in M;
  hence thesis by C0;
end;

A1: x ' <> 1 by L0:3, B0;
then A2: 1 ' <> 1 by L0:1, L0:3;
1 ' <> 1 iff 1 in M by C0, L0:1;
then A3: 1 in M by A2;

for x holds x in M implies x ' in M
proof
  let x be set such that C2: x in M;
  R: x in M iff x ' <> x by C0, C2;
  then C3: x ' <> x by C2;
  D0: x in NatZahl by A0, C2, TARSKI:def 3;
  then Q0: x ' in NatZahl by L0:2;
  then (x ') ' <> x ' by D0, C3, satz1;
  then Q1: (x ') ' <> x ' by C3, satz1;
  (x ') ' <> x ' iff x ' in M by C0, Q0;
  then C6: x ' in M by Q1;
  hence x ' in M by C2;
end;
then NatZahl c= M by A0, A3, L0:5;
then x in M by B0, TARSKI:def 3;
hence x <> x ' by C0;
end;

```

:: Satz 3

```

theorem satz3:
for x being set st x in NatZahl holds
x <> 1 implies
ex u being set st u in NatZahl &
x = u '
proof
let x be set such that C0: x in NatZahl;
defpred P[set] means $1 = 1 or (ex u being set st u in NatZahl & $1 = u ');
consider M being set such that A0: for x being set holds
x in M iff x in NatZahl & P[x] from Separation;

```

```

C: M c= NatZahl
proof
  let A be set;
  assume A in M;
  hence thesis by A0;
end;

```

```

1 in NatZahl by L0:1;
then CC: 1 in M by A0;

for x being set holds x in M implies x ' in M
  proof
    let x being set such that
      B0: x in M;
      BB: x in NatZahl by A0, B0;
      then B1: x ' in NatZahl by L0:2;
      ex u being set st u in NatZahl & x ' = u '
        proof
          take u = x;

          BBB: u in NatZahl by BB;
          x ' = u ' ;
          hence thesis by BBB;
        end;
      hence x ' in M by A0, B1 ;

    end;

then NatZahl c= M by C, CC, L0:5;
then x in M by C0, TARSKI:def 3;
hence x <> 1 implies (ex u being set st u in NatZahl & x = u ') by A0;
end;

```

.....: Satz 4

```

theorem satz4a:
for x being set st x in NatZahl holds
for f, g being Function st
  f.1 = x ' & g.1 = x ' &
  (for y being set st y in NatZahl holds
    f.(y ') = (f.y) ' &
    g.(y ') = (g.y) ') holds
  for y being set st y in NatZahl holds f.y = g.y

```

proof

let x be set such that F: x in NatZahl;

let a,b be Function such that

B: a.1 = x ' & b.1 = x '&
(for y being set st y in NatZahl holds
a.(y ') = (a.y) ' &
b.(y ') = (b.y) ');

for y being set st y in NatZahl holds a.y = b.y
proof

defpred P[set] means a.\$1 = b.\$1;
consider M being set such that A0: for y being set holds
y in M iff y in NatZahl & P[y] from Separation;

A1: M c= NatZahl
proof
let A be set;
assume A in M;
hence thesis by A0;
end;

A2: a.1 = b.1 by B;
1 in NatZahl by L0:1;
then A3: 1 in M by A0, A2;

for y being set holds y in M implies y ' in M
proof

let y be set such that R0: y in M;
R1: y in NatZahl by R0, A0;
a.y = b.y by R0, A0;
then R2: (a.y) ' = (b.y) ' by L0:2;
R3: a.(y ') = (a.y) ' by B, R1;
b.(y ') = (b.y) ' by B, R1;
then R4: b.(y ') = a.(y ') by R2, R3;
y ' in NatZahl by R1, L0:2;
then y ' in M by R4,A0 ;
hence thesis;
end;

then Q0: NatZahl c= M by A3, A1, L0:5;
then Q1: for y being set st y in NatZahl holds
y in M by Q0, TARSKI:def 3;
Q2: for y being set st y in NatZahl holds y in M iff a.y = b.y by A0;
for y being set st y in NatZahl holds a.y = b.y

```

    proof
    let y be set such that Q3: y in NatZahl;
    y in M by Q3, Q1;
    then a.y = b.y by Q2, Q3;
    hence thesis;
    end;

```

```

    hence thesis;
  end;

```

```

hence thesis;
end;

```

```

::::::::::::::::::::::::::::::::::::

```

```

theorem satz4b:
for x being set st x in NatZahl holds
ex f being Function st
f.1 = x ' &
for y being set st y in NatZahl holds
f.(y ') = (f.y) '
proof
let x such that B: x in NatZahl;
defpred P[set] means ex f being Function st
f.1 = $1 ' & for y being set st y in NatZahl holds
f.(y ') = (f.y) ';
consider M being set such that A:
for x being set holds x in M iff
x in NatZahl & P[x] from Separation;

```

```

C: M c= NatZahl
proof
let A be set;
assume A in M;
hence thesis by A;
end;

```

```

D:1 in M
proof
D0: 1 in NatZahl by L0:1;
::ex f being Function st f.1 = 1 ' &
::for y st y in NatZahl holds f.(y ') = (f.y) ';
:: "take f = ' "

```

```

    consider f being Function such that
    D1: for y st y in NatZahl holds f.y = y ' ;
::> *4
    D2: f.1 = 1 ' by D1,D0;
    for y st y in NatZahl holds f.(y ') = (f.y)';
::> *4

    hence thesis by D0, D2, A;
end; :: 1 in M

E: for x being set holds x in M implies x ' in M
proof
let x be set such that EE: x in M;
x in NatZahl by EE, A, TARSKI:def 3;
then EEO: x ' in NatZahl by L0:2;
ex f being Function st f.1 = x ' &
(for y st y in NatZahl holds f.(y ') = (f.y)') by EE, A;
then consider f being Function such that EE1:
f.1 = x ' & for y st y in NatZahl holds f.(y ') = (f.y) ' ;

ex g being Function st g.1 = x ' ' &
for y st y in NatZahl holds g.(y ') = (g.y) ' ;
::> *4
    ::proof
    ::take g = f ' ;

    then x ' in M by A, EEO;
    hence thesis;
end; :: x in M implies x ' in M

then NatZahl c= M by L0:5, D, C;
then x in M by B, TARSKI:def 3;
then ex f being Function st f.1 = x ' &
for y being set st y in NatZahl holds
f.(y ') = (f.y) ' by A;
hence thesis;
end; :: end of proof of 4B

definition
let x, y be set such
that x in NatZahl & y in NatZahl;
func x + y -> set means
:defPL: it in NatZahl &
ex f being Function st
it=f.y &
f.1 = x ' &

```

```
(for y being set st y in NatZahl holds
  f.(y ') = (f.y) ' );
```

```
existence;
::> *4
uniqueness;
::> *4
end;
```

```
theorem lem0:
for x st x in NatZahl holds x + 1 = x '
proof
let x such that A: x in NatZahl;
1 in NatZahl by L0:1;
then (x + 1) in NatZahl &
ex f being Function st
(x + 1)=f.1 &
f.1 = x ' &
(for y being set st y in NatZahl holds
  f.(y ') = (f.y) ' ) by A, defPL;
then (x + 1) = x ' ;
hence thesis;
end;
```

```
theorem lem1:
for x,y st x in NatZahl & y in NatZahl holds
(x + y ') = (x + y) '
proof
let x, y such that A: x in NatZahl & y in NatZahl;
AA: (x + y) in NatZahl &
ex f being Function st
(x + y) = f.y &
f.1 = x ' &
for y being set st y in NatZahl holds
f.(y ') = (f.y) ' by A, defPL;
```

```
then consider f being Function such that
B: (x + y) = f.y &
f.1 = x ' &
for y being set st y in NatZahl holds
f.(y ') = (f.y) ' ;
```

```

C0: (x + y) ' = (f.y) ' by B;
C1: (f.y) ' = f.(y ') by B, A;
C2: y ' in NatZahl by A, L0:2;
(x + y) ' in NatZahl by AA, L0:2;
then f.(y ') = x + (y ') by A, C1, B, C2, defPL;
then x + y ' = (x + y) ' by C0, C1;
hence thesis;
end;

```

theorem lem0a:

```

  for y st y in NatZahl holds
    1 + y = y '

```

proof

```

  let y such that A: y in NatZahl;

```

```

  defpred P[set] means 1 + $1 = $1 ' ;

```

```

  consider M being set such that B: for y being set holds
  y in M iff y in NatZahl & P[y] from Separation;

```

```

  C: M c= NatZahl

```

proof

```

  let A be set;

```

```

  assume A in M;

```

```

  hence thesis by B;

```

end;

```

  D: 1 in M

```

proof

```

  1 + 1 = 1 ' by lem0, defPL, L0:1;

```

```

  then 1 in M by B, L0:1;

```

```

  hence thesis by B;

```

end;

```

  E: for y being set holds y in M implies y ' in M

```

proof

```

  let y be set such that E0: y in M;

```

```

  y in M by E0;

```

```

  then E4: y in NatZahl by C, TARSKI:def 3;

```

```

  then E5: y ' in NatZahl by L0:2;

```

```

  E2: 1 + y = y ' by E0, A, B;

```

```

  then E3: 1 + y ' = (1 + y) ' by lem1, L0:1, E4;

```

```

  E6: (y ') ' = (1 + y) ' by E2;

```

```

  then E1: 1 + y ' = (y ') ' by E3;

```

```

  then y ' in M by E1, B, L0:2, E5;

```

```

  hence thesis;

```

end;

```

then NatZahl c= M by C, D,L0:5;
then y in M by A, TARSKI:def 3;
hence thesis by B, A;

end;

theorem lem1a:
  for x, y st x in NatZahl & y in NatZahl holds
    x ' + y = (x + y) '
proof
  let x, y such that A: x in NatZahl & y in NatZahl;

  defpred P[set] means x ' + $1 = (x + $1) ' ;
  consider M being set such that B: for y being set holds
    y in M iff y in NatZahl & P[y] from Separation;

  C: M c= NatZahl
  proof
    let A be set;
    assume A in M;
    hence thesis by B;
  end;

  D: 1 in M
  proof
    D0: x in NatZahl by A;
    then D1: x ' in NatZahl by L0:2;
    then D2: x ' + 1 = (x ') ' by lem0;
    (x ') ' = (x + 1) ' by A, L0:1,lem0;
    then x ' + 1 = (x + 1) ' by D2;
    hence thesis by B, L0:1;
  end;

  E: for y being set holds y in M implies y ' in M
  proof
    let y be set such that E0: y in M;
    y in M by E0;
    then E1: y in NatZahl by C, TARSKI:def 3;
    then E2: y ' in NatZahl by L0:2;
    E22: x ' in NatZahl by A, L0:2;
    E3: x ' + y = (x + y) ' by E0, B;
    E4: x ' + y ' = (x ' + y ') ' by lem1, E1, E22;
    E5: (x ' + y ') ' = (x + y ') ' by E3;
    (x + y ') ' = (x + y ') ' by lem1, A, E1;
    then x ' + y ' = (x + y ') ' by E3, E4, E5;
    hence thesis by E2, B;
  end;

```

```

end;

then NatZahl c= M by C, D,L0:5;
then y in M by A, TARSKI:def 3;
hence thesis by B, A;

end;

theorem lem2:
for x, y st x in NatZahl & y in NatZahl holds
x + y in NatZahl by defPL;

:: :: Satz 5

theorem satz5:
for x,y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
(x + y) + z = x + (y +z)
proof
let x,y,z such that A: x in NatZahl & y in NatZahl & z in NatZahl;

defpred P[set] means (x + y) + $1 = x + (y + $1);
consider M being set such that B: for z being set holds
z in M iff z in NatZahl & P[z] from Separation;

C: M c= NatZahl
proof
let A be set;
assume A in M;
hence thesis by B;
end;

D: 1 in M
proof
D0: x in NatZahl & x + y in NatZahl & 1 in NatZahl by A,defPL, L0:1, L0:2;
then D1: (x + y) ' in NatZahl by L0:2;
then D5: (x + y) + 1 = (x + y) ' by lem0, D0;
D2: y ' in NatZahl by A, L0:2;
then D3: x + y ' in NatZahl by A, L0:2, defPL;
then D4: (x + y) ' = x + y ' by A, lem1, D1, D2;
x + y ' = x + (y + 1) by A, lem0;
then (x + y ) + 1 = x + (y + 1) by D4, D5;
hence thesis by B, L0:1;
end;

```

```

E: for z being set holds z in M implies z ' in M
proof
let z be set such that E0: z in M;
E1: (x + y) + z = x + ( y + z) by E0, B;
E2: z in NatZahl by E0, B, TARSKI:def 3;
then E3: z ' in NatZahl by L0:2;
E4: (x + y) in NatZahl by A, defPL;
then E5: (x + y) + z ' in NatZahl by E3, defPL;
(x + y) + z in NatZahl by E4,E2,defPL;
then E7: ((x + y) + z ) ' in NatZahl by L0:2;
E8: (y + z) in NatZahl by A, defPL, E2;
then (y + z) ' in NatZahl by L0:2;
then x + (y + z) ' in NatZahl by A, defPL;
y + z ' in NatZahl by E3,A,defPL;
then x + (y + z ') in NatZahl by A, defPL;
x + y in NatZahl by A, defPL;
then E9: (x + y) + z ' = ((x + y) + z ) ' by E2, E3, lem1;
E10: ((x + y) + z ) ' =( x + (y + z)) ' by E1, L0:2;
E11: ( x + (y + z))' = x + (y + z) ' by lem1, A, E8;
E12: x + (y + z) ' = x + (y + z ') by A, lem1, E2, E3;
then (x + y) + z ' = x + (y + z ') by E9, E10, E11;
hence thesis by B, E3;
end;

then NatZahl c= M by C, D,L0:5;
then z in M by A, TARSKI:def 3;
hence thesis by B, A;

end;

```

:: :: Satz 6

```

theorem satz6:
for x,y st x in NatZahl & y in NatZahl holds
x + y = y + x
proof
let x,y such that A: x in NatZahl & y in NatZahl;

defpred P[set] means $1 + y = y + $1;
consider M being set such that B: for x being set holds
x in M iff x in NatZahl & P[x] from Separation;

C: M c= NatZahl
proof
let A be set;
assume A in M;
hence thesis by B;

```

```

end;

D: 1 in M
proof
D0: 1 + y = y ' by A, lem0a;
y + 1 = y ' by A, lem0;
then 1 + y = y + 1 by D0;
hence thesis by L0:1, B;
end;

E: for x being set holds x in M implies x ' in M
proof
let x be set such that E0: x in M;
E1: x in NatZahl by E0, C, TARSKI:def 3;
E2: x + y = y + x by E0, B;
E3: (x + y) ' = x + (y ') by A,E1, lem1;
E4: (x + y) ' = (y + x ) ' by E2;
E5: (y + x) ' = (y + x ') by lem1, A,E1;
E6: x ' + y = (x + y) ' by lem1a, A, E1;
then E7: x ' + y = y + x ' by E4,E5;
x ' in NatZahl by E1, L0:2;
hence thesis by B, E7;
end;

then NatZahl c= M by C, D,L0:5;
then x in M by A, TARSKI:def 3;
hence thesis by B, A;

end;

:: :: Satz 7

theorem satz7:
for x st x in NatZahl
for y st y in NatZahl holds
y <> x + y
proof
let x such that A: x in NatZahl;

defpred P[set] means $1 <> x + $1;
consider M being set such that B: for y being set holds
y in M iff y in NatZahl & P[y] from Separation;

C: M c= NatZahl
proof
let A be set;

```

```

    assume A in M;
    hence thesis by B;
end;

D: 1 in M
proof
D0: 1 <> x ' by A, L0:3;
x ' = x + 1 by A, lem0;
then 1 <> x + 1 by D0;
hence thesis by B, L0:1;
end;

let y such that AA: y in NatZahl;

E: for y being set holds y in M implies y ' in M
proof
let y be set such that E0: y in M;
E1: y in NatZahl by C, E0, TARSKI:def 3;
then E11: y ' in NatZahl by L0:2;
then E2: y <> x + y by B,E0;
E3: y ' <> (x + y) '
  proof
    assume y ' = (x + y)';
    then y = x + y by L0:4;
    then contradiction by E2;
    hence thesis;
  end;
(x + y) ' = x + y ' by A,E1, lem1;
then y ' <> x + y ' by E3;
hence thesis by B, E11;
end;

then NatZahl c= M by C, D,L0:5;
then y in M by AA, TARSKI:def 3;
hence thesis by B, AA;

end;

:: :: Satz 8

theorem satz8:
for x,y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
y <> z implies x + y <> x + z
proof
let x,y,z such that A: x in NatZahl & y in NatZahl & z in NatZahl;
assume AA: y <> z;

```

```

defpred P[set] means $1 + y <> $1 + z;
consider M being set such that B: for x being set holds
x in M iff x in NatZahl & P[x] from Separation;

C: M c= NatZahl
proof
  let A be set;
  assume A in M;
  hence thesis by B;
end;

D: 1 in M
proof
y <> z by AA;
then D0: y ' <> z ' by L0:4;
y ' = y + 1 & z ' = z + 1 by A, lem0;
then D1: y + 1 <> z + 1 by D0;
y + 1 = 1 + y & z + 1 = 1 + z by satz6, A, L0:1;
then 1 + y <> 1 + z by D1;
hence thesis by B, L0:1;
end;

E: for x being set holds x in M implies x ' in M
proof
let x be set such that E0: x in M;
E1: x + y <> x + z by B, E0;
E2: (x + y) ' <> (x + z) '
  proof
    assume (x + y) ' = (x + z) ' ;
    then x + y = x + z by L0:4;
    then contradiction by E1;
    hence thesis;
  end;
E3: x in NatZahl by E0, C, TARSKI:def 3;
then E33: x ' in NatZahl by L0:2;
E4: (x + y) ' = x ' + y by E3, lem1a, A;
E5: (x + z) ' = x ' + z by lem1a, E3, A;
then x ' + y <> x ' + z by E2, E4;
hence thesis by B, E33;
end;

then NatZahl c= M by C, D,L0:5;
then x in M by A, TARSKI:def 3;

hence thesis by B, A;

end;

```

reserve u,v for set;

theorem satz9a:

for x, y st x in NatZahl & y in NatZahl holds
(x = y implies for u st u in NatZahl holds x <> y + u & x + u <> y)
&
(for u st u in NatZahl holds x = y + u implies (x <> y &
for v st v in NatZahl holds x + v <> y))
&
(for v st v in NatZahl holds x + v = y implies (x <> y &
for u st u in NatZahl holds x <> y + u))
proof
let x, y such that A: x in NatZahl & y in NatZahl;

B: (x = y implies for u st u in NatZahl holds x <> y + u & x + u <> y)

proof

assume B0: x = y;

let u such that B1: u in NatZahl;

B2: x <> y + u

proof

assume B11: x = y + u;

then B12: x = x + u by B0;

u + x = x + u by satz6, B1, A;

then x = u + x by B12;

hence contradiction by B1, A, satz7;

end;

B3: x + u <> y

proof

assume B31: x + u = y;

then B32: x + u = x by B0;

x + u = u + x by B1, A, satz6;

then u + x = x by B32;

hence contradiction by A, B1, satz7;

end;

hence thesis by B2, B3;

end;

C: (for u st u in NatZahl holds x = y + u implies (x <> y &
for v st v in NatZahl holds x + v <> y))

proof

let u such that C0: u in NatZahl;

assume C1: x = y + u;

C2: x <> y

```

proof
assume C22:  $x = y$ ;
then C23:  $x = x + u$  by C1;
 $x + u = u + x$  by C0, A, satz6;
then  $x = u + x$  by C23;
hence contradiction by satz7, A, C0;
end;

C3: for  $v$  st  $v$  in NatZahl holds  $x + v <> y$ 
proof
let  $v$  such that C30:  $v$  in NatZahl;
assume C31:  $x + v = y$ ;
C32:  $x = y + u$  by C1;
C33:  $y + u = (x + v) + u$  by C31;
C34:  $(x + v) + u = x + (v + u)$  by satz5, A, C0, C30;
C35:  $v + u$  in NatZahl by C30, C0, defPL;
then  $x + (v + u) = (v + u) + x$  by satz6, A;
then  $x = (v + u) + x$  by C31, C32, C33, C34;
hence contradiction by satz7, A, C35;
end;

hence thesis by C2, C3;
end;

D: (for  $v$  st  $v$  in NatZahl holds  $x + v = y$  implies ( $x <> y$  &
for  $u$  st  $u$  in NatZahl holds  $x <> y + u$ ))
proof
let  $v$  such that D0:  $v$  in NatZahl;
assume D1:  $x + v = y$ ;

D2:  $x <> y$ 
proof
assume D20:  $x = y$ ;
 $x + v = x$  by D1, D20;
then  $x = v + x$  by A, D0, satz6;
hence contradiction by satz7, A, D0;
end;

D3: for  $u$  st  $u$  in NatZahl holds  $x <> y + u$ 
proof
let  $u$  such that D30:  $u$  in NatZahl;
assume D31:  $x = y + u$ ;
then D32:  $y + u = (x + v) + u$  by D1;
D34:  $(x + v) + u = x + (v + u)$  by satz5, A, D30, D0;
D35:  $v + u$  in NatZahl by D30, D0, defPL;
then  $x + (v + u) = (v + u) + x$  by satz6, A;
then  $x = (v + u) + x$  by D31, D32, D34, D35;
hence contradiction by satz7, A, D35;

```

```

    end;

hence thesis by D2, D3;
end;

hence thesis by B, C, D;
end;

:: :: Satz 9b, existence

theorem satz9b:
for x,y st x in NatZahl & y in NatZahl holds
x = y or
(ex u being set st u in NatZahl &
    x = y + u ) or
(ex v being set st v in NatZahl &
    y = x + v)
proof
  let x,y such that A: x in NatZahl & y in NatZahl;

  defpred P[set] means x = $1 or (ex u being set st
    u in NatZahl & x = $1 + u) or (ex v being set st v in NatZahl & $1 = x +v );
  consider M being set such that B: for y being set holds
    y in M iff y in NatZahl & P[y] from Separation;

  C: M c= NatZahl
  proof
    let A be set;
    assume A in M;
    hence thesis by B;
  end;

  D: 1 in M
  proof
  per cases;
    suppose D1: x = 1;
    hence 1 in M by B, A;
    suppose D2: x <> 1;
    then D2: ex u being set st u in NatZahl & x = u ' by A, satz3;
    D3: ex u being set st u in NatZahl & x = 1 + u
    proof
    consider u being set such that D4: u in NatZahl & x = u ' by D2;
    D5: x = u ' by D4;
    D6: u ' = u + 1 by lem0, D4;
    u + 1 = 1 + u by satz6, D4, L0:1;
  end;
  end;
end;

```

```

then x = 1 + u by D5, D6;

hence thesis by B, D4, L0:1;

end;

hence thesis by D3, B, L0:1;
hence thesis;

end;

E: for y being set holds y in M implies y ' in M
proof
let y such that E0: y in M;
E1: x = y or
(ex u being set st u in NatZahl &
    x = y + u ) or
(ex v being set st v in NatZahl &
    y = x + v) by E0, B;
per cases by E1;
suppose x = y;
then E11: x = y;
E2: y in NatZahl by E0, C, TARSKI:def 3;
then E3: y ' = y + 1 by lem0;
E4: ex v st v in NatZahl & y ' = x + v
proof
take v =1;
y ' = y + v by E3;
then y ' = x + v by E11;
hence thesis by L0:1;
end;
y ' in NatZahl by E2, L0:2;
hence y ' in M by E4, B;

suppose ex u st u in NatZahl & x = y + u;
then consider u such that EEO: u in NatZahl & x = y + u;
EE1: u = 1 implies ( x = y + 1) by EEO, L0:1;
EE2: y in NatZahl by E0, C, TARSKI:def 3;
then EE3: u = 1 implies ( x = y ' ) by A, EE1, lem0;
EE33: y ' in NatZahl by EE2, L0:2;
EE4: u = 1 implies y ' in M by A, B, EE3 ;

```

```

EE5: u <> 1 implies y ' in M
  proof
    assume EE6: u <> 1;
    x = y + u by EE0;
    ex w being set st w in NatZahl & u = w ' by EE0, satz3, EE6;
    then consider w being set such that EE7: w in NatZahl & u = w ';
    EE8: u = w + 1 by EE0, lem0, EE7;
    w + 1 = 1 + w by satz6, L0:1, EE7;
    then EE9: u = 1 + w by EE8;
    then EE10: x = y + (1 + w) by EE0;
    y + (1 + w) = (y + 1) + w by satz5, EE7, EE2, L0:1;
    then EE11: x = (y + 1) + w by EE10;
    (y + 1) + w = (y ') + w by lem0, EE2;
    then EE12: x = y ' + w by EE11;
    ex u being set st x = y ' + u & u in NatZahl
      proof
        take u = w;
        x = y ' + u & u in NatZahl by EE12, EE7;
        hence thesis;
      end;
    then y ' in M by B, EE33;
    hence thesis;
  end;

hence y ' in M by EE4, EE5;

suppose ex v st v in NatZahl & y = x + v;
then consider v such that EF0: v in NatZahl & y = x + v;
EF1: y ' = (x + v) ' by EF0;
(x + v) ' = x + v ' by lem1, A, EF0;
then EF2: y ' = x + v ' by EF1;
EFF: ex w being set st y ' = x + w & w in NatZahl
  proof
    take w = v ';
    EF3: w in NatZahl by EF0, L0:2;
    y ' = x + w by EF2;
    hence thesis by EF3;
  end;
y in NatZahl by E0, C, TARSKI:def 3;
then y ' in NatZahl by L0:2;
hence y ' in M by B, EFF;

hence thesis;
end;

then NatZahl c= M by C, D, E, L0:5;
then y in M by A, TARSKI:def 3;
hence thesis by B, A;

```

end;

:::::::::::::::::::::::::::::
:::::::::::::::::::::::::::::

:: :::::::::::::::::::::::
:: :::::::::::::::::::::::
:: :::::: Paragraph 3 ::
:: :::::::::::::::::::::::

definition
let x,y such that x in NatZahl & y in NatZahl;
pred x > y means
:def1: ex u st u in NatZahl & x = y + u;
end;

definition
let x,y;
pred x < y means
:def2: ex u st u in NatZahl & y = x + u;
end;

:: Satz 10

theorem satz10:
for x, y st x in NatZahl & y in NatZahl holds
(x = y implies (not(x > y) & not(x < y)))
&
(x < y implies (not(x = y) & not(x > y)))
&
(x > y implies (not(x = y) & not(x < y)))
&
(x = y or x > y or x < y)
proof
let x, y such that AA: x in NatZahl & y in NatZahl;

A: (x = y implies (not(x > y) & not(x < y)))

```

proof
assume A0: x = y;
( x = y implies for u st u in NatZahl
holds x <> y + u & x + u <> y) by satz9a, AA;
then A1: for u st u in NatZahl holds x <> y + u & x + u <> y by A0;
AAA: not(x > y)
  proof
  assume x > y;
  then ex u st u in NatZahl & x = y + u by def1, AA;
  then consider u such that A2: u in NatZahl & x = y + u;
  contradiction by A1, A2;
  hence thesis;
  end;

not(x < y)
  proof
  assume x < y;
  then ex u st u in NatZahl & y = x + u by def2, AA;
  then consider u such that A3: u in NatZahl & y = x + u;
  contradiction by A3, A1;
  hence thesis;
  end;

hence thesis by AAA;
end;

B: (x < y implies (not(x = y) & not(x > y)))
proof
assume x < y;

then ex u st u in NatZahl & y = x + u by def2, AA;
then consider u such that B1: u in NatZahl & y = x + u;
B2: (for v st v in NatZahl holds x + v = y implies (x <> y &
  for u st u in NatZahl holds x <> y + u)) by satz9a, AA;

BB: not(x = y)
  proof
  assume x = y;
  then contradiction by B1,B2;
  hence thesis;
  end;

BBB: not(x > y)
  proof
  assume x > y;
  then ex u st u in NatZahl & y + u = x by AA, def1;
  then consider w being set such that BBB1: w in NatZahl & y + w = x;
  y + w = x by BBB1;
  y = x + u by B1, AA;

```

```

    then contradiction by B2, B1, BBB1;
    hence thesis;

    end;
  hence thesis by BB;
end;

C: (x > y implies (not(x = y) & not(x < y)))
proof
  assume x > y;
  then ex u st u in NatZahl & y + u = x by AA, def1;
  then consider u such that C0: u in NatZahl & y + u = x;
  C1: (for v st v in NatZahl holds y + v = x implies (x <> y &
    for u st u in NatZahl holds y <> x + u)) by satz9a, AA;

  CC:not(x = y)
  proof
    assume x =y;
    then contradiction by C0, C1;
    hence thesis;
  end;

  not(x < y)
  proof
    assume x < y;
    then ex o being set st o in NatZahl & y = x + o by AA, def2;
    then consider o being set such that C8: x + o = y & o in NatZahl;

    y + u = x by C0;
    then contradiction by C1, AA, C8, C0;
    hence thesis;
  end;

  hence thesis by CC;
end;

D: x = y or x < y or x > y
proof
  D0: x = y or
    (ex u being set st u in NatZahl &
      x = y + u ) or
  (ex v being set st v in NatZahl &
    y = x + v) by AA, satz9b;
  D2: x > y iff (ex u being set st u in NatZahl &
    x = y + u ) by def1, AA;
  x < y iff (ex u being set st u in NatZahl &
    y = x + u) by def2, AA;

```

```

    hence thesis by D0,D2;

    end;

hence thesis by A, B, C, D;
end;

theorem satz11:
for x, y st x in NatZahl & y in NatZahl holds x > y implies y < x
proof
let x, y such that AA: x in NatZahl & y in NatZahl;

assume A: x > y;

then ex u st u in NatZahl & x = y + u by AA, def1;
then y < x by AA, def2;
hence thesis by AA;
end;

:: Satz 12

theorem satz12:
for x, y st x in NatZahl & y in NatZahl holds x < y implies y > x
proof
let x, y such that A: x in NatZahl & y in NatZahl;
assume x < y;
then ex u st u in NatZahl & y = x + u by def2, A;
hence thesis by A, def1;
end;

definition
let x,y such that x in NatZahl & y in NatZahl;
pred x >= y means
:def3: x > y or x = y;
end;

definition
let x,y such that x in NatZahl & y in NatZahl;
pred x <= y means
:def4: x < y or x = y;
end;

:: Satz 13
theorem satz13:
for x, y st x in NatZahl & y in NatZahl holds x >= y implies y <= x

```

```

proof
let x, y such that A: x in NatZahl & y in NatZahl;
assume x >= y;
then x > y or x = y by A,def3;
then y < x or x = y by satz11, A;
hence thesis by def4, A;
end;

```

```

:: Satz 14
theorem satz14:
for x, y st x in NatZahl & y in NatZahl holds
x <= y implies y >= x
proof
let x, y such that A: x in NatZahl & y in NatZahl;
assume x <= y;
then x < y or x = y by A, def4;
then y > x or x = y by A, satz12;
hence thesis by def3, A;
end;

```

```

:: Satz 15
theorem satz15:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
x < y & y < z implies x < z
proof
let x, y, z such that A: x in NatZahl & y in NatZahl & z in NatZahl;
assume B: x < y & y < z;
then ex v st v in NatZahl & x + v = y by def2,A;
then consider v such that C: v in NatZahl & x + v = y;
ex w being set st w in NatZahl & y + w = z by def2, A, B;
then consider w being set such that D: w in NatZahl & y + w = z;

```

```

DD: z = (x + v) + w by C,D;
then E: z = x + (v + w) by A, C,D, satz5;
ex o being set st o in NatZahl & z = x + o
proof
take o = v + w;
F: z = x + o by E;
o in NatZahl by defPL, C, D;
hence thesis by F;
end;
hence thesis by def2;
end;

```

```

theorem satz15b:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
x > y & y > z implies x > z

```

```

proof
let x, y, z such that A: x in NatZahl & y in NatZahl & z in NatZahl;
assume B: x > y & y > z;
then y < x & z < y by A, satz11;
then z < x by satz15, A;
hence thesis by satz12, A;
end;

```

:: Satz 16

```

theorem satz16:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
(x <= y & y < z implies x < z) &
(x < y & y <= z implies x < z)
proof
let x,y,z such that A: x in NatZahl & y in NatZahl & z in NatZahl;

```

B: $x \leq y \ \& \ y < z$ implies $x < z$

```

proof
assume B2: x <= y & y < z;
then B1: x < y or x = y by def4, A;
per cases by B1;
  suppose x < y;
  then B3: x < y & y < z by B2;

```

```

  x < y & y < z implies x < z by A, satz15 ;
  then x < z by A,B3;
  hence thesis;

```

```

  suppose x = y;
  then x = y & y < z by B2;
  then x < z;
  hence thesis;

```

```

hence thesis;
end;

```

C: $x < y \ \& \ y \leq z$ implies $x < z$

```

proof
assume C0: x < y & y <= z;
then C1: y < z or y = z by A,def4;
per cases by C1;
  suppose y < z;
  then C3: x < y & y < z by C0;
  x < y & y < z implies x < z by A, satz15 ;
  then x < z by A,C3;
  hence thesis;

```

```

  suppose y = z;
  then x < y & y = z by C0;

```

```

    then x < z;
    hence thesis;

end;

hence thesis by B,C;
end;

:: Satz 17

theorem satz17:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
x <= y & y <= z implies x <= z
proof
let x, y, z such that A:x in NatZahl & y in NatZahl & z in NatZahl;
assume x <=y & y <=z;
then B: (x < y or x = y) & (y < z or y =z) by A, def4;
per cases by B;
  suppose x = y & y = z;
  then x = z;
  hence thesis by def4, A;
  suppose x = y & y < z;
  then x < z;
  hence thesis by def4, A;
  suppose x < y & y = z;
  then x < z;
  hence thesis by def4, A;
  suppose x < y & y < z;
  then x < z by satz15, A;
  hence thesis by def4, A;

hence thesis;
end;

:: Satz 18

theorem satz18:
for x, y st x in NatZahl & y in NatZahl holds
x + y > x
proof
let x, y such that A: x in NatZahl & y in NatZahl;
B: x + y in NatZahl by defPL, A;
ex u st u in NatZahl & (x + y) = x + u

```

```

proof
  take u = y;
  x + u = x + u & u in NatZahl by A;
  hence thesis;
end;

hence thesis by def1, A, B;
end;

:: Satz19

theorem satz19a:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl
holds
(x > y implies x + z > y + z)
proof
let x, y, z such that A: x in NatZahl & y in NatZahl & z in NatZahl;
assume x > y;
  then ex u st u in NatZahl & x = y + u by A, def1;
  then consider u such that B0: u in NatZahl & x = y + u;
  B1: x + z = (y + u) + z by B0;
  B2: (y + u) + z = (u + y) + z by A, B0, satz6;
  B3: (u + y) + z = u + (y + z) by A, B0, satz5;
  y + z in NatZahl by defPL, A;
  then u + (y + z) = (y + z) + u by B0, satz6;
  then B30: x + z = (y + z) + u by B1, B2, B3;
  B4: ex v st v in NatZahl & (x + z) = (y + z) + v
  proof
    take v = u;
    v in NatZahl & x + z = (y + z) + v by B30, B0;
    hence thesis;
  end;

  y + z in NatZahl & x + z in NatZahl by A, defPL;
hence thesis by def1, B4;
end;

theorem satz19b:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
x = y implies x + z = y + z;

theorem satz19c:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl
holds
(x < y implies x + z < y + z)
proof
let x, y, z such that A: x in NatZahl & y in NatZahl & z in NatZahl;
assume x < y;
then B: y > x by A, satz12;

```

```

y > x implies y + z > x + z by satz19a, A;
then C: y + z > x + z by B;
y + z in NatZahl & x + z in NatZahl by defPL, A;
hence thesis by C, satz11;
end;

```

```

theorem satz19:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl
holds
(x < y implies x + z < y + z)
&
(x = y implies x + z = y + z)
&
(x > y implies x + z > y + z) by satz19a, satz19b, satz19c;

```

:: :: Satz 20

```

theorem satz20a:

```

```

for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
x + z > y + z implies x > y
proof
let x, y, z such that A: x in NatZahl & y in NatZahl & z in NatZahl;
assume B: x + z > y + z;

```

```

x + z in NatZahl & y + z in NatZahl by A, defPL;
then A0: not(x + z = y + z) & not(x + z < y + z) by satz10, B;
C: ( x = y or x < y or x > y) by A, satz10;

```

```

D: not(x < y)
proof
assume x < y;
then x + z < y + z by satz19, A;
then contradiction by A0;
hence thesis;
end;

```

```

E: not(x = y)
proof
assume x = y;
then x + z = y + z by satz19, A;
then contradiction by A0;
hence thesis;
end;

```

```

hence thesis by C, D, E;
end;

```

```

theorem satz20b:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
x + z = y + z implies x = y
proof
let x, y, z such that A: x in NatZahl & y in NatZahl & z in NatZahl;
assume B: x + z = y + z;

x + z in NatZahl & y + z in NatZahl by A, defPL;
then A0: not(x + z < y + z) & not(x + z > y + z) by satz10, B;
C: ( x = y or x < y or x > y) by A, satz10;

D: not(x < y)
  proof
  assume x < y;
  then x + z < y + z by satz19, A;
  then contradiction by A0;
  hence thesis;
  end;

E: not(x > y)
  proof
  assume x > y;
  then x + z > y + z by satz19, A;
  then contradiction by A0;
  hence thesis;
  end;

hence thesis by C, D, E;
end;

```

```

theorem satz20c:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
x + z < y + z implies x < y
proof
let x, y, z such that A: x in NatZahl & y in NatZahl & z in NatZahl;
assume B: x + z < y + z;

x + z in NatZahl & y + z in NatZahl by A, defPL;
then A0: not(x + z = y + z) & not(x + z > y + z) by satz10, B;
C: ( x = y or x < y or x > y) by A, satz10;

D: not(x = y)
  proof
  assume x = y;
  then x + z = y + z by satz19, A;
  then contradiction by A0;
  hence thesis;
  end;

```

```

end;

E: not(x > y)
  proof
    assume x > y;
    then x + z > y + z by satz19, A;
    then contradiction by A0;
    hence thesis;
  end;

hence thesis by C, D, E;
end;

theorem satz20:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
(x + z < y + z implies x < y) &
(x + z = y + z implies x = y) &
(x + z > y + z implies x > y) by satz20a, satz20b, satz20c;

theorem satz21:
for u,x,y,z st u in NatZahl & x in NatZahl & y in NatZahl & z in NatZahl
holds
x > y & z > u implies x + z > y + u
proof
let u,x,y,z such that
A: u in NatZahl & x in NatZahl & y in NatZahl & z in NatZahl;
assume B: x > y & z > u;
then C: x + z > y + z by A, satz19;
z + y > u + y by A, B, satz19;
then D: y + z > u + y by A, satz6;
x + z in NatZahl & y + z in NatZahl & u + y in NatZahl by A, defPL;
then x + z > u + y by satz15b,C,D;
hence thesis by satz6, A;
end;

theorem satz22a:
for u,x,y,z st u in NatZahl & x in NatZahl & y in NatZahl & z in NatZahl
holds
x >= y & z > u implies x + z > y + u
proof
let u,x,y,z such that
A: u in NatZahl & x in NatZahl & y in NatZahl & z in NatZahl;
assume B: x >= y & z > u;
then C: x = y or x > y by A, def3;
per cases by C;
  suppose D :x = y;

```

```

    then  $z + x > u + x$  by satz19, B, A;
    then  $z + x > u + y$  by D;
    then  $x + z > u + y$  by A, satz6;
    hence thesis by A, D, satz6;
    suppose E:  $x > y$ ;
    hence thesis by A, satz21, B, E;

hence thesis;
end;

theorem satz22b:
for  $u, x, y, z$  st  $u$  in NatZahl &  $x$  in NatZahl &  $y$  in NatZahl &  $z$  in NatZahl
holds
 $x > y$  &  $z \geq u$  implies  $x + z > y + u$ 
proof
let  $u, x, y, z$  such that
A:  $u$  in NatZahl &  $x$  in NatZahl &  $y$  in NatZahl &  $z$  in NatZahl;
assume B:  $x > y$  &  $z \geq u$ ;
then C:  $z = u$  or  $z > u$  by A, def3;
per cases by C;
    suppose D :  $z = u$ ;
    then  $x + u > y + u$  by satz19, B, A;
    then  $x + z > y + u$  by D;
    hence thesis;
    suppose E:  $z > u$ ;
    hence thesis by A, satz21, B, E;

hence thesis;
end;

theorem satz23:
for  $u, x, y, z$  st  $u$  in NatZahl &  $x$  in NatZahl &  $y$  in NatZahl &  $z$  in NatZahl
holds
 $x \geq y$  &  $z \geq u$  implies  $x + z \geq y + u$ 
proof
let  $u, x, y, z$  such that
A:  $u$  in NatZahl &  $x$  in NatZahl &  $y$  in NatZahl &  $z$  in NatZahl;
assume B:  $x \geq y$  &  $z \geq u$ ;
then C:  $(x = y$  or  $x > y)$  &  $(z = u$  or  $z > u)$  by A, def3;
per cases by C;
    suppose  $x = y$  &  $z = u$ ;
    then C0:  $x + z = y + u$ ;
     $x + z$  in NatZahl &  $y + u$  in NatZahl by A, defPL;
    hence thesis by def3, C0;

    suppose  $x = y$  &  $z > u$ ;
    then  $z + x > u + y$  by A, satz19;
    then  $x + z > u + y$  by A, satz6;

```

then C1: $x + z > y + u$ by A, satz6;
 $x + z$ in NatZahl & $y + u$ in NatZahl by A, defPL;
hence thesis by def3, C1;

suppose $x > y$ & $z = u$;
then C2: $x + z > y + u$ by A, satz19;
 $x + z$ in NatZahl & $y + u$ in NatZahl by A, defPL;
hence thesis by def3, C2;

suppose $x > y$ & $z > u$;
then C3: $x + z > y + u$ by A, satz21;
 $x + z$ in NatZahl & $y + u$ in NatZahl by A, defPL;
hence thesis by def3, C3;

hence thesis;
end;

theorem satz24:
for x st x in NatZahl holds $x \geq 1$
proof
let x such that A: x in NatZahl;
 $x < 1$ implies ex u st u in NatZahl & $x = u + 1$ by A, satz3;
then C: $x = 1$ or ex u st u in NatZahl & $x = u + 1$;
per cases by C;
 suppose $x = 1$;
 hence thesis by def3, A, L0:1;
 suppose ex u st u in NatZahl & $x = u + 1$;
 then consider u such that D: u in NatZahl & $x = u + 1$;
 E: $x = u + 1$ by lem0, D, A;
 $x > 1$
 proof
 ex v st $x = 1 + v$ & v in NatZahl
 proof
 take $v = u$;
 F: $x = v + 1$ by E;
 v in NatZahl by D;
 then $x = 1 + v$ by F, satz6, L0:1;
 hence thesis by D;
 end;
 hence thesis by def1, A, L0:1;
 end;
hence thesis by def3, A, L0:1;

hence thesis;
end;

```

theorem satz25:
for x, y st x in NatZahl & y in NatZahl holds
y > x implies y >= x + 1
proof
let x, y such that A: x in NatZahl & y in NatZahl;
assume y > x;
then ex u st u in NatZahl & y = x + u by A, def1;
then consider u such that B: u in NatZahl & y = x + u;
C: y = x + u by B;
D: u >= 1 by B, satz24;
u + x >= 1 + x
  proof
    E: u = 1 or u > 1 by def3, B, L0:1, D;
    per cases by E;
      suppose F: u = 1;
      G: u + x = 1 + x by F;
      u + x in NatZahl by A,B, L0:1, defPL;
      hence thesis by def3, G;

      suppose G: u > 1;
      H: u + x > 1 + x by satz19, A, B, G, L0:1;
      u + x in NatZahl & 1 + x in NatZahl by A, B, L0:1, defPL;
      hence thesis by def3, H;
  end;

then y >= 1 + x by C, A, B, satz6;
hence thesis by L0:1, A, satz6;
end;

```

```

theorem satz26:
for x, y st x in NatZahl & y in NatZahl holds
y < x + 1 implies y <= x
proof
let x, y such that A: x in NatZahl & y in NatZahl;
assume B: y < x + 1;
C: y < x or y = x or y > x by A, satz10;

not(y > x)
proof
assume y > x;
then F :y >=x + 1 by A, satz25;
G: x + 1 in NatZahl by A, defPL, L0:1;

```

```

then  $y < x + 1$  implies  $\text{not}(y = x + 1 \text{ or } y > x + 1)$  by satz10, A;
then  $\text{not}(y = x + 1 \text{ or } y > x + 1)$  by B;
then  $\text{not}(y \geq x + 1)$  by def3,G, A;
then contradiction by F ;
hence thesis;
end;

```

```

then  $y < x$  or  $y = x$  by C;
hence thesis by A, def4;

```

```

end;

```

```

theorem lemma3:
for  $x, y$  st  $x$  in NatZahl &  $y$  in NatZahl holds
 $x \leq y$  implies  $y \geq x$ 
proof
let  $x, y$  such that A:  $x$  in NatZahl &  $y$  in NatZahl;
assume  $x \leq y$ ;
then  $x < y$  or  $x = y$  by A, def4;
then  $y > x$  or  $x = y$  by satz12, A;
hence thesis by A, def3;
end;

```

```

theorem lemma4:
for  $x, y$  st  $x$  in NatZahl &  $y$  in NatZahl holds
 $x \geq y$  implies  $y \leq x$ 
proof
let  $x, y$  such that A:  $x$  in NatZahl &  $y$  in NatZahl;
assume  $x \geq y$ ;
then  $x > y$  or  $x = y$  by A, def3;
then  $y < x$  or  $x = y$  by satz11, A;
hence thesis by A, def4;
end;

```

```

:: :: lege verzameleing definitie
definition
let  $t$  be set;
attr  $t$  is leer means
:defL:  $\text{not}(\text{ex } e \text{ being set st } e \text{ in } t)$ ;
end;

```

```

theorem satz27:
for N being set st N c= NatZahl & not(N is leer) holds
ex n being set st n in N & (for m being set st (m in N) holds n <=
m)
proof
let N be set such that A: N c= NatZahl & not(N is leer);

assume not( ex n being set st n in N &
for m being set st m in N holds n <= m);

then TA: for n being set holds not( n in N &
for m being set st m in N holds n <= m);

::then TAA: for n being set st n in N holds
::not(for m being set st m in N holds n <= m);

defpred P[set] means for n being set st n in N holds $1 <=n ;
consider M being set such that B: for x being set holds
x in M iff x in NatZahl & P[x] from Separation;

C:M c= NatZahl
proof
let A be set;
assume A in M;
hence thesis by B;
end;

D: 1 in M
proof

DD: for x st x in NatZahl holds 1 <= x
proof
let x such that DD0: x in NatZahl;
x >= 1 by satz24, DD0;
then x > 1 or x = 1 by L0:1, DD0, def3;
then 1 < x or 1 = x by satz11, DD0, L0:1;
hence thesis by def4, DD0, L0:1;
end;

for x st x in N holds 1 <=x
proof
let x such that D0: x in N;
x in NatZahl by A, D0, TARSKI:def 3;
then 1 <= x by DD;
hence thesis;

```

```

    end;
  hence thesis by L0:1, B;
end; :: 1 in M

not(N is leer) by A;
then ex n being set st n in N by defL;
then consider n being set such that Q: n in N;
QQ: n in NatZahl by Q, A, TARSKI:def 3;

AA: not(for x st x in NatZahl holds x in M)
  proof
    assume AA1: for x st x in NatZahl holds x in M;
      :: to be proved: contradiction
    for y st y in N holds not(y + 1 in M)
      proof
        let y such that T0: y in N;
        assume y + 1 in M;
        then T2: y + 1 in NatZahl &
        for n being set st n in N holds y + 1 <=n by B;
        T3: y in NatZahl by T0,A, TARSKI:def 3; then
        T4: y ' in NatZahl by L0:2;
        T1: y + 1 <= y by T0,T2;
        T5: not( y + 1 <= y)
          proof
            y ' <= y by T1, lem0,T2,T3;
            then Y: y ' = y or y ' < y by T3,T4, def4;
            Z: not(y ' = y) by T3,T4, satz2;
            not(y ' < y)
              proof
                assume y ' < y;
                then V: y + 1 < y by lem0, T2,T3;
                y + 1 > y by T3,T1, L0:1, satz18;
                then not(y + 1 < y) by satz10, T3,T2;
                then contradiction by V;
                hence thesis;
              end; then
            contradiction by Y,Z;
            hence thesis;
          end; then
        contradiction by T1;
        hence thesis;
      end;
    then
    T: not(n+1) in M by Q;
    n + 1 in NatZahl by QQ, L0:1,defPL; then
    n + 1 in M by AA1;
    hence contradiction by T;
  end;

```

```

(for m being set st m in M holds m ' in M) implies
for n being set st n in NatZahl holds n in M
  proof
    assume for m being set st m in M holds m ' in M;
    then NatZahl c= M by L0:5, B, C, D;

    then for n being set st n in NatZahl holds n in M by TARSKI:def 3;
    hence thesis;
  end;

then ex m being set st m in M & not(m ') in M by AA;
then consider m being set such that AA0: m in M & not(m ') in M;

m in N & for n being set st n in N holds m <= n
  proof
    AB: for n being set st n in N holds m <= n by B, AA0;
    m in N
      proof
        assume ACB: not(m in N);
        :: then ACA: (for o being set st o in N holds m <= o) by TAA;
        BBB: for o being set st o in N holds m < o
          proof
            let o be set such that AC: o in N;
            AD: m <= o by AC, AB;
            AE: o in NatZahl by A, AC, TARSKI:def 3;
            AF: m in NatZahl by AA0, B, TARSKI:def 3;
            then AG: m = o or m < o by def4, AD, AE;
            not(m = o)
              proof
                o in N & not(m in N) by AC, ACB;
                hence thesis;
              end;
            end;
            hence thesis by AG;
          end;
        :: for n being set st n in N holds m < n) ;
        GA: for n being set st n in N holds m ' <= n
          proof
            let n be set such that GA1: n in N;
            GB: m < n by BBB, GA1;
            GC: m in NatZahl by AA0, B, TARSKI:def 3;
            then GD: m ' in NatZahl by L0:2;
            GE: n in NatZahl by A, TARSKI:def 3, GA1;
            then n > m by GB, GC, satz12;
            then n >= m + 1 by GC, GE, satz25;
          end;
        end;
      end;
  end;

```

```

        then n >= m ' by lem0, GC;
        hence thesis by lemma4, GD, GE;
    end;
    m in NatZahl by AA0, B, TARSKI:def 3;
    then m ' in NatZahl by L0:2;
    then m ' in M by B, GA;

    then contradiction by AA0;
    hence thesis;
    end;
    hence thesis by AB;
    end;

```

```

then contradiction by TA;
hence thesis;

end;

```

```

:: satz 28, a, b..

```

```

definition
let x, y be set such that x in NatZahl & y in NatZahl;
func x * y -> set means
: defT: it in NatZahl &
ex f being Function st
it=f.y &
f.1 = x &
(for y being set st y in NatZahl holds
    f.(y ') = (f.y) + x );
existence;
::> *4
uniqueness;
::> *4
end;

```

```

theorem lem5:
for x being set st x in NatZahl
holds x * 1 = x
proof
let x be set such that A: x in NatZahl;
ex f being Function st
x * 1 = f.1 &

```

```

f.1 = x & (for y being set st y in NatZahl holds
  f.(y ') = (f.y) + x) by A, L0:1, defT;
hence thesis by A, defT, L0:1;
end;

theorem lem6:
for x, y being set st x in NatZahl & y in NatZahl
holds x * (y ') = (x * y) + x
proof
  let x,y such that A: x in NatZahl & y in NatZahl;
  B: y ' in NatZahl by A, L0:2;
  then
    ex f being Function st
      x * (y ) = f.(y ) & f.1 = x &
      for y st y in NatZahl holds f.(y ') = (f.y) + x by A, defT;

    then consider f being Function such that
      C: x * (y ) = f.(y ) & f.1 = x &
      for y st y in NatZahl holds f.(y ') = (f.y) + x;
      C0: f.(y ') = (x * y) + x by C, A, B;
      f.y = x * y by C;

    ex g being Function st
      x * (y ') = g.(y ') & g.1 = x &
      for y st y in NatZahl holds g.(y ') = (g.y) + x by A, B, defT;

    then consider g being Function such that
      D: x * (y ') = g.(y ') & g.1 = x &
      for y st y in NatZahl holds g.(y ') = (g.y) + x;

      C1: g.(y ') = x * (y ') by D;
      C2: for z st z in NatZahl holds f.z = g.z
      proof
        let z such that PP: z in NatZahl;
        defpred P[set] means f.$1 = g.$1;
        consider M being set such that Q: for y being set holds
          y in M iff y in NatZahl & P[y] from Separation;

        QC: M c= NatZahl
        proof
          let A be set;
          assume A in M;
          hence thesis by Q;
        end;

        QD: 1 in M
        proof
          QD1: f.1 = x by C;
          g.1 = x by D;

```

hence thesis by QD1, Q, L0:1;
end;

QE: for y holds y in M implies y ' in M
proof

let y;
assume QE1: y in M;
then QE0: f.y = g.y by Q;
R: y in NatZahl by QE1, Q, TARSKI:def 3;
then f.(y ') = (f.y) + x by C;
then QE5: f.(y ') = (g.y) + x by QE0;
g.(y ') = (g.y) + x by D, R;
then QE6: g.(y ') = f.(y ') by QE5;
y ' in NatZahl by R, L0:2;
hence thesis by Q, QE6;
end;

then NatZahl c= M by QC, QD,L0:5;
then z in M by PP, TARSKI:def 3;
hence thesis by Q, A;

end;
then g.(y ') = f.(y ') by B;
then x * (y ') = (x * y) + x by C0, C1, C2;
hence thesis;
end;

theorem lem5a:

for x st x in NatZahl holds

$1 * x = x$

proof

let x such that A: x in NatZahl;

defpred P[set] means $1 * \$1 = \1 ;

consider M being set such that B: for x being set holds
x in M iff x in NatZahl & P[x] from Separation;

C: M c= NatZahl

proof

let A be set;
assume A in M;
hence thesis by B;

end;

```

D: 1 in M
proof
  1 * 1 = 1 by lem5, L0:1;

hence thesis by L0:1, B;
end;

E: for x being set holds x in M implies x ' in M
proof
let x such that E0: x in M;
E1: 1 * x = x by E0, B;
E2: x in NatZahl by E0, B, TARSKI:def 3;
then E3: x ' in NatZahl by L0:2;
then E4: x ' = x + 1 by lem0, E2;
E5: x + 1 = (1 * x) + 1 by E1;
(1 * x) + 1 = 1 * (x ') by lem6, L0:1, E2;
then 1 * (x ') = x ' by E4, E5;
hence thesis by E3, B;
end;

then NatZahl c= M by C, D,L0:5;
then x in M by A, TARSKI:def 3;
hence thesis by B, A;

end;

theorem lem6a:
for x, y st x in NatZahl & y in NatZahl holds
(x ') * y = (x * y) + y
proof
let x, y such that A: x in NatZahl & y in NatZahl;

defpred P[set] means (x ') * $1 = (x * $1) + $1;
consider M being set such that B: for y being set holds
y in M iff y in NatZahl & P[y] from Separation;

C: M c= NatZahl
proof
let A be set;
assume A in M;
hence thesis by B;
end;

D: 1 in M

```

```

proof
x ' in NatZahl by A, L0:2;
then D0: (x ') * 1 = x ' by lem5;
D1: x ' = x + 1 by A, lem0;
x + 1 = (x * 1) + 1 by lem5, A;
hence thesis by L0:1, B, D0, D1 ;
end;

E: for y being set holds y in M implies y ' in M
proof
let y such that E0: y in M;
E1: x ' * y = (x * y) + y by E0, B;
E2: y in NatZahl by E0, B, TARSKI:def 3;
E3: x ' in NatZahl by L0:2, A;

then E4: (x ') * (y ') = (x ' * y ) + (x ') by lem6, E2;
E5: (x ' * y ) + (x ') = ((x * y) + y) + (x ') by E1, E2,A;
E6: x * y in NatZahl & x ' in NatZahl & y in NatZahl by A, E2, defT, E3;
then E7: ((x * y) + y ) + (x ') = (x * y) + (y + (x ')) by satz5;
E8: (x * y) + (y + (x ')) = (x * y) + (x ' + y) by satz6, E6;
E9: (x * y) + (x ' + y) = (x * y) + (x + y) ' by A, E2, lem1a;
E10: (x * y) + (x + y) ' = (x * y) + (x + y ') by A, E2, lem1;
EE: y ' in NatZahl by E2, L0:2;
then E11: (x * y) + (x + y ') = ((x * y) + x ) + (y ') by A, E6, satz5;
((x * y) + x) + (y ') = (x * (y ')) + (y ') by lem6, A, E2;
then (x ') * (y ') = (x * (y ')) + (y ') by E4, E5, E6, E7, E8, E9, E10, E11;
hence thesis by EE, B;
end;

then NatZahl c= M by C, D,L0:5;
then y in M by A, TARSKI:def 3;
hence thesis by B, A;

end;

```

```

theorem satz29:
for x,y st x in NatZahl & y in NatZahl holds
x * y = y * x
proof
let x,y such that A: x in NatZahl & y in NatZahl;

defpred P[set] means $1 * y = y * $1;
consider M being set such that B: for x being set holds
x in M iff x in NatZahl & P[x] from Separation;

```

```

C: M c= NatZahl
  proof
    let A be set;
    assume A in M;
    hence thesis by B;
  end;

D: 1 in M
  proof

D0: y * 1 = y by lem5, A, L0:1;
1 * y = y by lem5a, A, L0:1;

  hence thesis by D0, L0:1, B;
  end;

E: for x being set holds x in M implies x ' in M
  proof
  let x;
  assume E0: x in M;
  then E1: x * y = y * x by B;
  then E2: (x * y) + y = (y * x) + y;
  EE: x in NatZahl by E0, B, TARSKI:def 3;
  then EEE: x ' in NatZahl by L0:2;
  E3: (y * x) + y = (y * (x ')) by lem6, A, EE;
  (x ' * y) = (x * y) + y by lem6a, A, EE;
  then x ' * y = y * (x ') by E3, EEE, E2;
  hence thesis by EEE, B;
  end;

  then NatZahl c= M by C, D,L0:5;
  then x in M by A, TARSKI:def 3;
  hence thesis by B, A;

end;

theorem satz30:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
x * (y + z) = (x * y) + (x * z)
proof
  let x,y,z such that A: x in NatZahl & y in NatZahl & z in NatZahl;

  defpred P[set] means x * (y + $1) = (x * y) + (x * $1);
  consider M being set such that B: for z being set holds
  z in M iff z in NatZahl & P[z] from Separation;

```

```

C: M c= NatZahl
proof
  let A be set;
  assume A in M;
  hence thesis by B;
end;

D: 1 in M
proof
D0:  $x * (y + 1) = x * (y ')$  by lem0, A;
D1:  $x * (y ') = (x * y) + x$  by lem6, A;
 $(x * y) + x = (x * y) + (x * 1)$  by lem5, A;
hence thesis by B, D0, D1, L0:1;
end;

E: for z being set holds z in M implies z ' in M
proof
let z such that E0: z in M;
E1:  $x * (y + z) = (x * y) + (x * z)$  by B, E0;
E2: z in NatZahl by E0, B, TARSKI:def 3;
then E3: z ' in NatZahl by L0:2;
E4:  $x * (y + (z ')) = x * ((y + z) ')$  by A, E2, lem1;
E5:  $y + z$  in NatZahl by A, E2, defPL;
E6:  $x * ((y + z) ') = (x * (y + z)) + x$  by E5, A, lem6;
E7:  $(x * (y + z)) + x = ((x * y) + (x * z)) + x$  by E1;
 $x * y$  in NatZahl &  $x * z$  in NatZahl &  $x$  in NatZahl by A, defT, E2;
then E8:  $((x * y) + (x * z)) + x = (x * y) + ((x * z) + x)$  by satz5;
E9:  $(x * y) + ((x * z) + x) = (x * y) + (x * (z '))$  by lem6, A, E2;
 $x * (y + (z ')) = (x * y) + (x * (z '))$  by E4, E6, E7, E8, E9;
hence thesis by B, E3;
end;

then NatZahl c= M by C, D,L0:5;
then z in M by A, TARSKI:def 3;
hence thesis by B, A;

end;

theorem satz31:
for x,y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
 $(x * y) * z = x * (y * z)$ 
proof
let x,y,z such that A: x in NatZahl & y in NatZahl & z in NatZahl;

defpred P[set] means  $(x * y) * $1 = x * (y * $1)$ ;
consider M being set such that B: for z being set holds

```

```

z in M iff z in NatZahl & P[z] from Separation;

C: M c= NatZahl
proof
  let A be set;
  assume A in M;
  hence thesis by B;
end;

D: 1 in M
proof
  x * y in NatZahl by defT, A;
  then DD: (x * y) * 1 = x * y by lem5;
  x * y = x * (y * 1) by A, lem5;
  hence thesis by DD, L0:1, B;
end;

E: for z being set holds z in M implies z ' in M
proof
  let z such that E0: z in M;
  E1: (x * y) * z = x * (y * z) by E0, B;
  E2: z in NatZahl by E0, B, TARSKI:def 3;
  then E3: z ' in NatZahl by L0:2;
  E4: (x * y) * (z ') = (x * y) * (z + 1) by lem0, E2;
  E5: x * y in NatZahl by A, defT;
  F: (x * y) * (z + 1) = (x * y) * z + (x * y) * 1 by L0:1, satz30, E2, E5;
  G: (x * y) * z + (x * y) * 1 = (x * y) * z + (x * y) by lem5, E5;
  H: (x * y) * z + (x * y) = x * (y * z) + (x * y) by E1;
  y * z in NatZahl by A, E2, defT;
  then I: x * (y * z) + (x * y) = x * ((y * z) + y) by satz30, A;
  x * ((y * z) + y) = x * (y * (z ')) by lem6, A, E2;
  then (x * y) * (z ') = x * (y * (z ')) by E4, F,G,H,I;
  hence thesis by B, E3;
end;

then NatZahl c= M by C, D,L0:5;
then z in M by A, TARSKI:def 3;
hence thesis by B, A;

end;

theorem satz32a:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
x > y implies x * z > y * z
proof
let x, y, z such that A: x in NatZahl & y in NatZahl & z in NatZahl;

```

```

assume B: x > y ;
then ex u st u in NatZahl & x = y + u by A, def1;
then consider u such that C: u in NatZahl & x = y + u;
x * z = (y + u) * z by C;
y + u in NatZahl by C, A, defPL;
then (y + u) * z = z * (y + u) by satz29, A;
z * (y + u) = (z * y) + (z * u) by satz30, C, A;
then E: z * x = (z * y) + (z * u) by C;
R: ex v st x * z = (y * z) + v & v in NatZahl
  proof
    take v = z * u;
    z * x = (z * y) + v by E;
    then x * z = (z * y) + v by satz29, A;
    then RR: x * z = (y * z) + v by satz29, A;
    v in NatZahl by C, A, defT;
    hence thesis by RR;
  end;

x * z in NatZahl & y * z in NatZahl by A, defT;
hence thesis by def1, R;
end;

theorem satz32b:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
x = y implies x * z = y * z;

theorem satz32c:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
x < y implies x * z < y * z
proof
let x, y, z such that A: x in NatZahl & y in NatZahl & z in NatZahl;
assume B: x < y ;
then y > x by A, satz12;
then T: y * z > x * z by satz32a, A;
y * z in NatZahl & x * z in NatZahl by A, defT;
hence thesis by A, satz11, T;
end;

theorem satz32:
for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
(x < y implies x * z < y * z) &
(x = y implies x * z = y * z) &
(x > y implies x * z > y * z) by satz32a, satz32b, satz32c;

theorem satz33:

```

```

for x, y, z st x in NatZahl & y in NatZahl & z in NatZahl holds
(x * z > y * z implies x > y ) &
(x * z = y * z implies x = y ) &
(x * z < y * z implies x < y )
proof
let x, y, z such that A: x in NatZahl & y in NatZahl & z in NatZahl;

B: (x * z > y * z implies x > y )
  proof
    assume B0: x * z > y * z;
    x * z in NatZahl & y * z in NatZahl by A, defT;
    then B2: not(x * z = y * z) & not(x * z < y * z) by satz10, B0;
    B3: x > y or x =y or x < y by A, satz10;
    B4: not(x = y)
      proof
        assume x = y;
        then x * z = y * z by satz32, A;
        then contradiction by B2;
        hence thesis;
      end;

    not(x < y)
      proof
        assume x < y;
        then x * z < y * z by satz32, A;
        then contradiction by B2;
        hence thesis;
      end;

    hence thesis by B3, B4;
  end;

C: (x * z = y * z implies x = y )
  proof
    assume C0: x * z = y * z;
    x * z in NatZahl & y * z in NatZahl by defT, A;
    then C2: not(x * z < y * z) & not(x * z > y * z) by satz10, C0;
    C3: x = y or x < y or x > y by satz10, A;
    C4: not(x < y)
      proof
        assume x < y;
        then x * z < y * z by A, satz32;
        then contradiction by C2;
        hence thesis;
      end;

    end;
  end;

```

```

not(x > y)
proof
  assume x > y;
  then x * z > y * z by A, satz32;
  then contradiction by C2;
  hence thesis;
end;

hence thesis by C3, C4;
end;

D: (x * z < y * z implies x < y )
proof
  assume D0: x * z < y * z;
  x * z in NatZahl & y * z in NatZahl by defT, A;
  then D2: not(x * z = y * z) & not(x * z > y * z) by satz10, D0;
  D3: x = y or x < y or x > y by satz10, A;

  D4: not(x =y)
  proof
    assume x = y;
    then x * z = y * z by satz32, A;
    then contradiction by D2;
    hence thesis;
  end;

  not(x > y)
  proof
    assume x > y;
    then x * z > y * z by satz32, A;
    then contradiction by D2;
    hence thesis;
  end;

  hence thesis by D3, D4;
end;

hence thesis by B, C, D;
end;

theorem satz34:
for x, y, z, u st x in NatZahl & y in NatZahl & z in NatZahl & u in NatZahl
holds

```

```

x > y & z > u implies x * z > y * u
proof
let x, y, z, u such that
A: x in NatZahl & y in NatZahl & z in NatZahl & u in NatZahl;
assume B: x > y & z > u;
then x * z > y * z by A, satz32;
then C: x * z > z * y by A, satz29;
z * y > u * y by B, satz32, A;
then D: z * y > y * u by A, satz29;
x * z in NatZahl & z * y in NatZahl & y * u in NatZahl by A, defT;
then x * z > y * u by C, D, satz15b;
hence thesis;
end;

```

```

theorem satz35:
for x, y, z, u st x in NatZahl & y in NatZahl & z in NatZahl & u in NatZahl
holds
(x >= y & z > u implies x * z > y * u)
&
(x > y & z >= u implies x * z > y * u)
proof
let x, y, z, u such that
A: x in NatZahl & y in NatZahl & z in NatZahl & u in NatZahl;

B: (x >= y & z > u implies x * z > y * u)
proof
assume B0: x >= y & z > u;
then B1: x > y or x = y by def3, A;
per cases by B1;
  suppose x > y;
  hence thesis by B0, A, satz34;
  suppose B3: x = y;
  z * x > u * x by B0, A, satz32;
  then z * x > u * y by B3;
  then x * z > u * y by A, satz29;
  hence thesis by satz29, A;

hence thesis;
end;

```

```

C: (x > y & z >= u implies x * z > y * u)
proof
assume C0: x > y & z >= u;
then C1: z = u or z > u by def3, A;
per cases by C1;
  suppose z > u;
  hence thesis by C0, A, satz34;

```

suppose $z = u$;
hence thesis by C0, A, satz32;

hence thesis;
end;

hence thesis by B, C;
end;

theorem satz36:
for x, y, z, u st x in NatZahl & y in NatZahl & z in NatZahl & u in NatZahl
holds

$(x \geq y \ \& \ z \geq u \text{ implies } x * z \geq y * u)$

proof

let x, y, z, u such that

A: x in NatZahl & y in NatZahl & z in NatZahl & u in NatZahl;

assume B: $x \geq y \ \& \ z \geq u$;

then C: $(x = y \ \& \ z = u)$ or

$(x > y \ \& \ z = u)$ or

$(x = y \ \& \ z > u)$ or

$(x > y \ \& \ z > u)$ by A, def3;

D: $x * z$ in NatZahl & $y * u$ in NatZahl by A, defT;

per cases by C;

suppose $x = y \ \& \ z = u$;

then E: $x * z = y * u$;

hence thesis by D, def3;

suppose $x > y \ \& \ z = u$;

then E: $x * z > y * u$ by satz32, A;

hence thesis by def3, D;

suppose $x = y \ \& \ z > u$;

then $z * x > u * y$ by satz32, A;

then $x * z > u * y$ by A, satz29;

then $x * z > y * u$ by A, satz29;

hence thesis by D, def3;

suppose $x > y \ \& \ z > u$;

then $x * z > y * u$ by satz34, A;

hence thesis by D, def3;

hence thesis;
end;

```

reserve n,m for set;

theorem satz27_2:
for N being set st N c= NatZahl & not(N is leer) holds
ex n st n in N & (for m st (m in N) holds n <=
m)
proof
let N be set such that A: N c= NatZahl & not(N is leer);

defpred P[set] means for y st y in N holds $1 <= y;
consider M being set such that B: for z being set holds
z in M iff z in NatZahl & P[z] from Separation;

C: M c= NatZahl
proof
let A be set;
assume A in M;
hence thesis by B;
end;

D: 1 in M
proof
for x st x in N holds 1 <= x
proof
let x such that D1: x in N;
D2: x in NatZahl by D1, A, TARSKI:def 3; then
x >= 1 by satz24; then
x > 1 or x = 1 by L0:1, D2, def3; then
1 < x or 1 = x by satz11, D2, L0:1;
hence thesis by def4, D2, L0:1;
end;

hence thesis by B, L0:1;
end;

ex n st n in N by A, defL; then
consider n such that F: n in N;

EE: not(for x st x in NatZahl holds x in M)
proof
assume E2: for x st x in NatZahl holds x in M;
for y st y in N holds not(y + 1 in M)
proof
let y such that E0: y in N;
E2: y in NatZahl by A, TARSKI:def 3, E0; then

```

```

E4:      y + 1 in NatZahl by L0:1, defPL;
        not(y + 1 in M)
          proof
            assume y + 1 in M; then
            for z st z in N holds y + 1 <= z by B; then
E1:      y + 1 <= y by E0;
        not(y + 1 <= y)
          proof
            assume y + 1 <= y ; then
E3:      y + 1 = y or y + 1 < y by def4, E2,E4;
        y + 1 > y by satz18, L0:1, E2; then
        not(y + 1 < y) by E2,E4, satz10; then
        y + 1 = y by E3; then
        y ' = y by lem0, E2;
        hence contradiction by satz2, E2;
        end;
        hence contradiction by E1;
        end; :: not(y+1 in M)
        hence thesis;
        end; ::(for y st y in N..)
then E22: not(n + 1 in M) by F;
n + 1 in NatZahl
  proof
    n in NatZahl by F, A, TARSKI:def 3;
    hence thesis by defPL, L0:1;
    end;
  hence contradiction by E2, E22;
end;

ex m st m in M & not(m+1 in M)
  proof
    assume not(ex m st m in M & not(m+1 in M)); then
F0: for m st m in M holds m + 1 in M;
F:   for m st m in M holds m ' in M
      proof
        let m such that F1: m in M;
F2:  m in NatZahl by F1, C, TARSKI:def 3;
        m + 1 in M by F1,F0; then
        m ' in M by lem0, F2;
        hence thesis;
        end;
      for x st x in NatZahl holds x in M
        proof
          let x such that F3: x in NatZahl;
          for m holds m in M implies m ' in M by F; then
          M c= NatZahl &
          (1 in M & for k being set
           holds (k in M implies k ' in M)) by C,D,B; then

```

```

    NatZahl c= M by L0:5;
    hence thesis by F3, TARSKI:def 3;
    end;

    hence contradiction by EE;
    end;

    then consider m such that
    J: m in M & not(m +1 in M);

H:  for n st n in N holds m <= n by J,B;

K:  m in N
    proof
        assume HH: not m in N;
H4:  m in NatZahl by J,C, TARSKI:def 3; then
H44: m + 1 in NatZahl by L0:1, defPL;
H7:  for n st n in N holds m < n
        proof
            let n such that H1: n in N;
H5:  m <= n by H1, B, J;
H2:  n in NatZahl by A, TARSKI:def 3, H1; then
H6:  m = n or m < n by H4, H2, def4, H5;
            not(m = n)
            proof
                n in N & not(m in N) by HH, H1;
                hence thesis;
            end;
            hence thesis by H6;
        end;
    for n st n in N holds m + 1 <= n
        proof
            let n such that H1: n in N;
H2:  n in NatZahl by TARSKI:def 3, H1, A;
            m < n by H7, H1; then
            n > m by H7, satz12, H2,H4; then
            n >= m + 1 by H4, H2, satz25;
            hence thesis by H44,H2,satz13;
        end;

    then m + 1 in M by B, H44;
    hence contradiction by J;
    end;

    take m;

    thus thesis by H,K;

```

end; :: proof

::>

::> 4: This inference is not accepted

2 Group_8

environ

```
vocabulary CARD_1, REALSET1, GROUP_2, BOOLE, GRAPH_1, GROUP_6,
INT_1, GR_CY_1, NAT_1,
    ARYTM_1, ARYTM_3, ABSVALUE, GROUP_1, FINSET_1, GROUP_4, VECTSP_1,
    PBOOLE, TARSKI,
    RELAT_1, FINSEQ_1, FUNCT_1, QC_LANG1, WELLORD1, FILTER_0, GROUP_5,
    MATRIX_2,
    GROUP_3, POWER, GROUP_8, SETFAM_1, BINOP_1, LATTICES;
notation XBOOLE_0, CARD_1, TARSKI, ZFMISC_1, SUBSET_1, XCMPLX_0, XREAL_0,
RELAT_1, FUNCT_1, FUNCT_2, PBOOLE,
    ABIAN, BINOP_1, INT_1, NAT_1, RLVECT_1, FINSET_1, GROUP_1, GROUP_2,
    STRUCT_0, SETFAM_1,
    VECTSP_1, GROUP_3, GROUP_4, GROUP_5, GROUP_6, GR_CY_1, FINSEQ_1,
    NEWTON, INT_2;
constructors REAL_1, BINOP_1, NAT_1, GROUP_4, GROUP_5, GR_CY_1,
    NAT_LAT, MEMBERED, PREPOWER, SETFAM_1, IRRAT_1, ARYTM_3, DOMAIN_1,
    ZFMISC_1, MCART_1, PBOOLE, ABIAN, WELLORD2, GROUP_6, REALSET1;
clusters INT_1, GR_CY_1, STRUCT_0, XREAL_0, GROUP_2, FINSEQ_1, RELSET_1,
    GROUP_1, MEMBERED, GROUP_3, SETFAM_1, FINSET_1, ABIAN, REALSET1;
theorems GROUP_2, GR_CY_1, GR_CY_2, NAT_LAT, NAT_1, GROUP_3, TARSKI, XBOOLE_0,
GROUP_1, RLVECT_1, CARD_1 , GROUP_6
    , CARD_2, GROUP_5, NAT_2, ALTCAT_1, VECTSP_1, PBOOLE, FUNCT_2, GROUP_4,
    INT_2, CARD_5, XCMPLX_1, AFINSQ_1,
    INT_1, AXIOMS, REAL_2, ABIAN, REAL_1, BOOLE, FINSET_1, XCMPLX_0, FINSEQ_1,
    FUNCT_1, ARYTM_3, EULER_2, PYTHTRIP,
    REALSET1, RELSET_1;
requirements REAL, NUMERALS, SUBSET, BOOLE, ARITHM;
definitions TARSKI, XBOOLE_0, NAT_1, FUNCT_1, WELLORD2, GROUP_1, GROUP_6;
schemes SETFAM_1, GROUP_2, NAT_1, PRVECT_1, FINSEQ_1, FUNCT_2;
```

begin

```
reserve G,P for strict Group;
reserve q for Element of the carrier of P;
reserve a,b,x,y,z for Element of the carrier of G;
reserve H,H1,H2,K for strict Subgroup of G;
reserve L for strict Subgroup of P;
```

```

reserve h for Element of the carrier of H;
reserve k for Element of the carrier of K;
reserve h1 for Element of the carrier of H1;
reserve p,n,m,i,j,s for Nat;
reserve A for Subset of the carrier of G;
reserve xx for set;

```

```

theorem lemmaToTh4_1_1:
  p is prime & ord G = p & G is finite implies
  ex a st ord a = p
proof
assume A: p is prime & ord G = p & G is finite;

  then E: G is finite & ord G = p & p is prime by A;
  (G is finite & ord (G) = p & p is prime)
  implies G is cyclic Group by GR_CY_1:45;
  then N: G is cyclic Group by E;
  then ex a st ord a = ord G by GR_CY_1:43, A;
  then ex a st ord a = p by A;
  hence thesis;
end;

```

```

theorem lemmaA:
for a1,a2 being Element of the carrier of H
for b1,b2 being Element of the carrier of G st a1 = b1 & a2 = b2
holds a1*a2 = b1*b2
proof
let a1,a2 be Element of the carrier of H;
H is Subgroup of G;
then B: the carrier of H c= the carrier of G by GROUP_2:def 5;
then C: a1 is Element of the carrier of G by GROUP_2:def 5, TARSKI:def 3;
D: a2 is Element of the carrier of G by GROUP_2:def 5, TARSKI:def 3, B;

```

```

let b1,b2 be Element of the carrier of G such that A: a1 = b1 & a2 = b2;

```

```

dom the mult of G = [:the carrier of G, the carrier of G:] by FUNCT_2:def 1;
then
C: the mult of G is ManySortedSet of [:the carrier of G, the carrier of G:]
by PBOOLE:def 3;

```

```

B2: the mult of H =
      (the mult of G) | [:the carrier of H ,the carrier of H :]
      by GROUP_2:def 5;

```

```

D: a1 in the carrier of H & a2 in the carrier of H;

a1*a2 = (the mult of H).(a1,a2) by VECTSP_1:def 10
      . = (the mult of G).(b1,b2) by A,B,B2, C, ALTCAT_1:7
      . = b1*b2 by VECTSP_1:def 10;
then a1 * a2 = b1 * b2 by A;
hence thesis;
end;

```

```

theorem lemmaB:
for a being Element of the carrier of H
for b being Element of the carrier of G st a = b
for n being Nat
  holds a|^n = b|^n
proof
  let a be Element of the carrier of H;
  let b be Element of the carrier of G such that A: a = b;
  let n be Nat;

```

```

defpred P[Nat] means a|^$1 = b|^$1;
Q: P[0]
proof
Q0: a|^0 = 1.H by GROUP_1:43;
Q1: b|^0 = 1.G by GROUP_1:43;
  1.H = 1.G by GROUP_2:53;
  then a|^0 = b|^0 by Q0,Q1;
hence thesis;
end;

```

```

R: for k being Nat st P[k] holds P[k + 1]
proof
  let k be Nat such that R0: P[k];
  R1: a|^k = b|^k by R0;
  R2: a|^ (k + 1) = (a|^k) * a by GROUP_1:49;
  R3: b|^ (k + 1) = (b|^k) * b by GROUP_1:49;
  b|^k = a|^k & a = b by R1,A;
  then a|^k * a = b|^k * b by lemmaA;
  then b|^ (k + 1) = (a|^k) * a by R3;
  then b|^ (k+1) = a|^ (k + 1) by R2;
  then P[k+1];
hence thesis;
end;

```

```

for k being Nat holds P[k] from Ind(Q,R);
then P[n];
hence thesis;
end;

```

```

theorem lemmaB0:
for a being Element of the carrier of H
for b being Element of the carrier of G st a = b
for i being Integer
  holds  $a|^i = b|^i$ 
proof
let a be Element of the carrier of H;
let b be Element of the carrier of G such that A:  $a = b$ ;
let i be Integer;
ex k being Nat st  $i = k$  or  $i = -k$  by INT_1:8; then
consider k being Nat such that B:  $i = k$  or  $i = -k$ ;
per cases by B;
  suppose C:  $i = k$ ; then
     $a|^k = b|^k$  by lemmaB, A;
    hence thesis by C;
  suppose D:  $i = -k$ ;
     $a^|k = b^|k$  by A, GROUP_2:57; then
     $a|^k = b|^k$  by lemmaB; then
     $(a|^k)^| = (b|^k)^|$  by GROUP_1:72; then
     $(a|^k)^| = (b|^k)^|$  by GROUP_1:72; then
     $a|^k = (b|^k)^|$  by GROUP_1:71; then
     $a|^k = b|^k$  by GROUP_1:71;
    hence thesis by D;
hence thesis;
end;

```

```

theorem lemmaC:
for a being Element of the carrier of H
for b being Element of the carrier of G st  $a = b$  & G is finite
  holds  $\text{ord } a = \text{ord } b$ 

```

```

proof
let a be Element of the carrier of H;
let b be Element of the carrier of G such that A:  $a = b$  & G is finite;
H is Subgroup of G;
H is finite by GROUP_2:48, A;
then B:  $\text{not}(a \text{ is\_of\_order\_0}) \ \& \ \text{not}(b \text{ is\_of\_order\_0})$  by A, GR_CY_1:26;
then C:  $a|^{\text{ord } a} = 1.H$  by GROUP_1:def 11;
D:  $b|^{\text{ord } b} = 1.G$  by GROUP_1:def 11, B;
E: for n being Nat holds  $a|^n = b|^n$  by A, lemmaB;
 $1.H = 1.G$  by GROUP_2:53;
then F:  $a|^{\text{ord } a} = b|^{\text{ord } b}$  by C, D;
 $a|^{\text{ord } a} = b|^{\text{ord } a}$  by E;
then  $b|^{\text{ord } a} = b|^{\text{ord } b}$  by F;
then  $b|^{\text{ord } a} = 1.G$  by D;
then F:  $\text{ord } b$  divides  $\text{ord } a$  by GROUP_1:86;

```

```

a |^ ord b = b |^ ord b by E;
then a |^ (ord b) = 1.G by D;
then a |^ (ord b) = 1.H by GROUP_2:53;
then G: ord a divides ord b by GROUP_1:86;
hence thesis by F,G, NAT_1:52;
end;

```

```

theorem lemma0:
for h being Element of the carrier of G st
  h in H holds H * h c= the carrier of H
proof
let h be Element of the carrier of G such that A: h in H;
A1: for a being set holds a in H * h implies a in the carrier of H
proof
  let a be set;
  assume a in H * h;
  then ex g being Element of the carrier of G
    st a = g * h & g in H by GROUP_2:126;
  then consider g being Element of the carrier of G
    such that C: a = g * h & g in H;
  g * h in H by C,A, GROUP_2:59;
  then g * h in the carrier of H by RLVECT_1:def 1;
  then a in the carrier of H by C;
  hence thesis;
end;
hence thesis by TARSKI:def 3, A;
end;

```

```

theorem lemma_1_5_4_0:
for a st a <> 1.G holds gr {a} <> (1).G
proof
let a such that A: a <> 1.G;
assume B: gr {a} = (1).G;
C: the carrier of (1).G = {1.G} by GROUP_2:def 7;
{a} c= the carrier of gr {a} by GROUP_4:def 5;
then {a} c= the carrier of (1).G by B;
then {a} c= {1.G} by C;
then D: xx in {a} implies xx in {1.G} by TARSKI:def 3;
a = 1.G
proof
  S: xx in {a} iff xx = a by TARSKI:def 1;

```

```

T: xx in {1.G} iff xx = 1.G by TARSKI:def 1;
xx = a implies xx = 1.G
  proof
    assume xx = a;
    then xx in {a} by S;
    then xx in {1.G} by D;
    hence thesis by T;
  end;
  hence thesis;
end;
then contradiction by A;
hence thesis;
end;

```

```

theorem lemmaH:
for m being Integer holds (1.G) |^ m = 1.G
proof
let m be Integer;
ex k being Nat st m = k or m = -k by INT_1:8; then
consider k being Nat such that A: m = k or m = - k;
per cases by A;
  suppose m = k;
  hence thesis by GROUP_1:42;
  suppose C: m = -k;
  (1.G) |^ -k = (1.G) |^ (- k)
    . = ((1.G) |^ k)" by GROUP_1:70
    . = (1.G)" |^ k by GROUP_1:72
    . = (1.G) |^ k by GROUP_1:16
    . = 1.G by GROUP_1:42; then
  (1.G) |^ -k = 1.G;
  hence thesis by C;

```

```

hence thesis;
end;

```

```

theorem lemmaG:
for m being Integer holds a |^ (m * ord a) = 1.G
proof
let m be Integer;
A: a is_not_of_order_0 or a is_of_order_0;
per cases by A;
  suppose a is_of_order_0; then
  ord a = 0 by GROUP_1:def 11; then
  m * (ord a) = 0; then

```

```

    a |^ (m * ord a) = 1.G by GROUP_1:43;
    hence thesis;
    suppose a is_not_of_order_0; then
C: a |^ ord a = 1.G by GROUP_1:def 11;
    (1.G) |^ m = 1.G by lemmaH; then
    (a |^ ord a) |^ m = 1.G by C; then
    a |^ ((ord a) * m) = 1.G by GROUP_1:67;
    hence thesis;

```

```

hence thesis;
end;

```

```

theorem lemmaF:
for a st a is_not_of_order_0
for m being Integer holds a |^ m = a |^(m mod ord a)
proof
let a such that A: a is_not_of_order_0;
let m be Integer;
ord a <> 0 by A, GROUP_1:def 11; then
m mod ord a = m - (m div ord a) * ord a by INT_1:def 8; then
a |^(m mod ord a) = a |^ (m - (m div ord a) * ord a)
    . = a |^ (m - 1 * (m div ord a) * ord a)
    . = a |^ (m + - 1 * (m div ord a) * ord a) by XCMPLX_0:def 8
    . = (a|^m) * a |^(-(m div ord a) * ord a) by GROUP_1:63
    . = (a|^m) * a |^((- (m div ord a)) * ord a) by XCMPLX_1:175
    . = (a|^m) * 1.G by lemmaG
    . = (a|^m) by GROUP_1:def 4;
hence thesis;
end;

```

```

theorem lemma_1_5_4_1:
b is_not_of_order_0 implies gr {b} is finite
proof
assume A: b is_not_of_order_0;
then not(for n holds b |^ n = 1.G implies n = 0) by GROUP_1:def 10;
b |^ ord b = 1.G by A, GROUP_1:def 11;
ord b <> 0 by A, GROUP_1:def 11; then
A3: ord b > 0 by NAT_1:19;

```

```

deffunc B(Nat) = b |^ $1;
consider f being FinSequence such that
C: len f = ord b & for i being Nat st i in Seg ord b holds
f.i = B(i) from SeqLambda;
C': dom f = Seg ord b by C,FINSEQ_1:def 3;
the carrier of gr {b} c= rng f
proof
let x be set;

```

```

    assume x in the carrier of gr {b}; then
AA: x in gr {b} by RLVECT_1:def 1; then
  x in G by GROUP_2:49; then
  reconsider a = x as Element of the carrier of G by RLVECT_1:def 1;
  consider m being Integer such that
B: a = b|^m by AA,GR_CY_1:25;
  set k = m mod ord b;
  ord b >= 0 by NAT_1:18; then
  k >= 0 by GR_CY_2:2; then
  reconsider k as Nat by INT_1:16;
D: a = b|^k by lemmaF, B, A;
  per cases;
  suppose
C0: k = 0;
    ord b >= 0+1 & ord b <= ord b by A3,NAT_1:38; then
D1: ord b in Seg ord b by FINSEQ_1:3;
    a = 1.G by D,C0,GROUP_1:43
    .= b|^ord b by A,GROUP_1:def 11
    .= f.ord b by C,D1;

    hence x in rng f by D1,C',FUNCT_1:def 5;
    suppose k <> 0; then
    k > 0 & k < ord b by A3,GR_CY_2:3,NAT_1:19; then
    k >= 0+1 & k <= ord b by NAT_1:38; then
D2:k in Seg ord b by FINSEQ_1:3; then
    a = f.k by C,D;

    hence x in rng f by D2,C',FUNCT_1:def 5;
  end;
hence the carrier of gr {b} is finite by FINSET_1:13;
end;

```

```

theorem lemma_1_5_4_3:
b is_of_order_0 implies b" is_of_order_0
proof
assume b is_of_order_0;
then A: b|^n = 1.G implies n = 0 by GROUP_1:def 10;
b" is_of_order_0
proof
  b"|^n = 1.G implies n = 0
  proof
    assume b"|^n = 1.G;
    then (b|^n)" = 1.G by GROUP_1:51;
    then (b|^n)" = (1.G)" by GROUP_1:16;
    then b|^n = 1.G by GROUP_1:17;
    hence thesis by A;
  end;
hence thesis by GROUP_1:def 10;

```

```

    end;
  hence thesis;
end;

```

```

theorem lemma_1_5_4_4:
  b is_of_order_0 iff
  for n being Integer holds b |^n = 1.G implies n = 0
  proof
  A: b is_of_order_0 implies for n being Integer holds b |^n = 1.G implies n = 0
    proof
      assume B: b is_of_order_0;
      then Q: for m being Nat holds b |^m = 1.G
        implies m = 0 by GROUP_1:def 10;
      P: for m being Nat holds b |^-m = 1.G implies m = 0
        proof
          let m;
          assume E: b |^-m = 1.G;
          D: b |^-m = (b |^m)" by GROUP_1:71;
          (b |^m)" = b" |^m by GROUP_1:72; then
          F: b" |^m = 1.G by D,E;
          b" is_of_order_0 by B, lemma_1_5_4_3; then
          for m being Nat holds (b") |^m = 1.G
            implies m = 0 by GROUP_1:def 10;
          hence thesis by F;
        end;
      end;
    for n being Integer holds b |^n = 1.G implies n = 0
      proof
        let n be Integer;
        assume S: b |^n = 1.G;
        ex k being Nat st n = k or n = -k by INT_1:8; then
        consider k being Nat such that R: n = k or n = -k;
        per cases by R;
          suppose T: n = k;
          then b |^k = 1.G by S;
          then k = 0 by Q;
          hence thesis by T;
          suppose Z: n = -k;
          then b |^-k = 1.G by S;
          then k = 0 by P;
          then -k = 0;
          hence thesis by Z;
        end;
      hence thesis;
    end;
  hence thesis;
end;
end;
end;
(for n being Integer holds b |^n = 1.G implies n = 0) implies b is_of_order_0
  proof

```

```

        assume for n being Integer holds  $b|^n = 1.G$  implies  $n = 0$ ;
        then for n being Nat holds  $b|^n = 1.G$  implies  $n = 0$ ;
        hence thesis by GROUP_1:def 10;
    end;
hence thesis by A;
end;

```

```

theorem theorem_1_5_4:
for G st ex a st a <> 1.G holds
(for H holds H = G or H = (1).G) iff
G is cyclic Group & G is finite & ex p being Nat st ord G = p & p is prime
proof
let G such that A: ex a st a <> 1.G;
consider b such that B: b <> 1.G by A;
D: (for H holds H = G or H = (1).G) implies
G is cyclic Group & G is finite & ex p being Nat st ord G = p & p is prime
proof
    assume D0: for H holds H = G or H = (1).G;
    D1: gr {b} is cyclic Group by GR_CY_2:10;
    H1: b in gr {b} by GR_CY_2:8;
    then gr {b} <> (1).G by B, lemma_1_5_4_0;
    then G0: gr {b} = G by D0;
    then R3: G is cyclic Group by D1;
    Ord gr {b} = Ord G by G0;
    D5: b is_not_of_order_0
    proof
        assume G4: b is_of_order_0;
        then
        FF:  $b|^2 \neq 1.G$  by GROUP_1:def 10;
        then G1:  $\text{gr}\{b|^2\} \neq (1).G$  by lemma_1_5_4_0;
        G2:  $\text{gr}\{b|^2\} \neq G$ 
        proof
            H0: b in G by H1, G0;
            not(b in  $\text{gr}\{b|^2\}$ )
            proof
                assume b in  $\text{gr}\{b|^2\}$ ;
                then ex j1 being Integer
                st  $b = (b|^2)^{|j1}$  by GR_CY_1:25;
                then consider j1 being Integer
                such that VA:  $b = (b|^2)^{|j1}$  ;
                 $b = b|^{\text{2 * j1}}$  by VA, GROUP_1:67;
                then VB:  $b^{|j1} * (b|^{\text{2 * j1}}) = 1.G$ 
                by GROUP_1:def 5;
                 $b|^{\text{-1}} = b^{|j1}$  by GROUP_1:62;
                then  $(b|^{\text{-1}}) * (b|^{\text{2 * j1}}) = 1.G$  by VB;
                then VD:  $b|^{\text{-1 + (2 * j1)}} = 1.G$ 
            end
        end
    end
end

```

```

        by GROUP_1:63;
    then VE:  $-1 + (2 * j1) = 0$ 
        by lemma_1_5_4_4, G4;
     $-1 + (2 * j1) <> 0$ 
    proof
        assume  $-1 + (2 * j1) = 0$ ; then
         $2 * j1 = 1$  by XCMLX_1:136; then
         $2 = 1$  or  $2 = -1$  by INT_1:22;
        then contradiction;
        hence thesis;
    end;
    then contradiction by VE;
    hence thesis;
end;
    hence thesis by H0;
end;
then contradiction by G1,G2, D0;
hence thesis;
end; :: ord b is finite
then ex n being Nat st  $n = \text{ord } b \ \& \ b \text{ is\_not\_of\_order\_0}$ ;
then consider n being Nat such that RR:  $n = \text{ord } b \ \& \ b \text{ is\_not\_of\_order\_0}$ ;
gr {b} is finite by lemma_1_5_4_1, D5;
then R2: G is finite by G0 ;
RRR:  $\text{ord } G = \text{ord } \text{gr}\{b\}$  by G0;
R0:  $\text{ord } b = \text{ord } \text{gr}\{b\}$  by R2, GR_CY_1:27;
then RR3:  $\text{ord } G = n$  by RR, RRR;
R1: n is prime
proof
    assume TA: not(n is prime);
    ex u,v being Nat st  $u > 1 \ \& \ v > 1 \ \& \ n = u * v$ 
    proof
        not( $n > 1$  & for m being Nat holds
            m divides n implies  $m = 1$  or  $m = n$ )
        by TA, INT_2:def 5;
    then  $n \leq 1$  or
        ex m being Nat st
            not(m divides n implies  $m=1$  or  $m = n$ );
    then TC:  $n \leq 1$  or
        ex m being Nat st  $m <> 1 \ \& \ m <> n \ \& \ (m \text{ divides } n)$ ;
    TT:  $n > 1$ 
    proof
        YA:  $n = \text{ord } G$  by RR3;
        then YB:  $n \geq 1$  by GROUP_1:90, R2;
        ord b  $<> 1$ 
        proof
            assume ord b = 1;
            then b = 1.G by GROUP_1:85;
            hence contradiction by B;
        end;
    end;
end;

```

```

then ord G <> 1 by RRR, RO;
then XA: n <> 1 by YA;
n > 1
  proof
    assume n <=1;
    then n < 1 by XA, REAL_1:def 5;
    hence contradiction by YB;
  end;
  hence thesis by YB;
end;
then ex m being Nat
  st m <> 1 & m <> n & m divides n by TC;
then consider m being Nat
  such that YD: m <> 1 & m <> n & m divides n;
ex o being Nat st n = m * o by NAT_1:def 3, YD;
then consider o being Nat such that YE: n = m * o;
take u = m;
take v = o;
YY: u > 1
  proof
    u <> 0
      proof
        assume u = 0;
        then 0 divides n by YD;
        then n = 0 * (n div 0) by NAT_1:49;
        then n = 0;
        hence contradiction by TT;
      end;
    then 0 < u by NAT_1:19;
    then 0 + 1 <= u by INT_1:20;
    then YYY: 1 <= u;
    u <> 1 by YD;
    hence thesis by YYY, REAL_1:def 5;
  end;
YX: v > 1
  proof
    XA: v <> 0
      proof
        assume v = 0;
        then n = u * 0 by YE;
        then n = 0;
        hence contradiction by TT;
      end;
    then 0 < v by NAT_1:19;
    then 0 + 1 <= v by INT_1:20;
    then XA1: 1 <= v;
    v <> 1
      proof
        assume v = 1;

```

```

        then n = u * 1 by YE;
        then n = u;
        hence contradiction by YD;
    end;
    hence thesis by XA1, REAL_1:def 5;
end;
n = v * u by YE;
hence thesis by YY, YX;
end;
then consider u, v being Nat such that F3: u > 1 & v > 1 & n = u * v;
R4: ord (b |^v) = u
proof
  RM: G is finite & G= gr {b} &
    ord G = n & n = v * u implies ord(b|^v) = u by GR_CY_2:14;
  G is finite & G= gr{b} & ord G = n & n = v * u by F3, R2, RR3, G0;
  hence thesis by RM;
end;
ord gr {b |^v} = ord (b|^v) by GR_CY_1:27, R2;
then R5: ord gr {b |^v } = u by R4;
u <> n
  proof
    assume RN: u = n;
    n = u * v by F3;
    then RM: n = n * v by RN;
    u > 0 & v > 0 by F3, AXIOMS:22; then
    n > 0 by F3, REAL_2:122; then
    n <> 0;
    then v = 1 by F3, XCMLX_1:7, RM;
    then contradiction by F3;
    hence thesis;
  end;
then R6: gr {b |^v} <> G by R5, RR3;
gr {b |^v } <> (1).G
  proof
    assume O1: gr {b |^v } = (1).G;
    O0: ord gr {b |^v} = u by R5;
    ord (1).G = 1 by GROUP_2:81;
    then ord gr {b |^v} >ord(1).G by F3, O0;
    then contradiction by O1;
    hence thesis;
  end;
then contradiction by D0, R6;
hence thesis;
end;
ex p being Nat st ord G = p & p is prime
  proof
    take p = n;
    thus thesis by R1, RR3 ;
  end;

```

```

    hence thesis by R2, R3;
  end;
:::..... :: <=
E: G is cyclic Group & G is finite & ord G = p & p is prime
  implies (for H holds H = G or H =(1).G)
  proof
    assume E0: G is cyclic Group & G is finite & ord G = p & p is prime;
    let H;
    EF: ord G = ord H * index H by GROUP_2:177, E0;
    FF: ord H divides ord G
      proof
        ex t being Nat st ord G = ord H * t
          proof
            take t = index H;
            thus thesis by EF;
          end;
        hence thesis by NAT_1:def 3;
      end;
    ord G is prime by E0;
    then for n holds n divides ord G implies n = 1 or n = ord G by INT_2:def 5;
    then EG: ord H divides ord G implies (ord H = ord G or ord H = 1);
    then EH: ord H = ord G or ord H = 1 by FF;
    per cases by EH;
      suppose ord H = ord G;
      then H = G by E0, GROUP_2:85;
      hence thesis;
      suppose EI: ord H = 1;
      EJ: H is finite by GROUP_2:48, E0;
      EK: H is finite & ord H = 1 implies H = (1).G by GROUP_2:82;
      EL: H is finite & ord H = 1 by EI, EJ;
      H = (1).G by EK, EL;
      hence thesis;
    hence thesis;
  end;
hence thesis by D,E;
end;

```

```

theorem lemmaE:
z in x * A * y iff ex a being Element of the carrier of G
  st z = x * a * y & a in A
proof
A: z in x * A * y implies
  ex a being Element of the carrier of G st
    z = x * a * y & a in A
  proof
    assume z in x * A * y;
    then ex b being Element of the carrier of G st
      z = b * y & b in x * A by GROUP_2:34;
  end;
end;

```

```

then consider b such that
C:  $z = b * y$  &  $b$  in  $x * A$ ;
ex u being Element of the carrier of G st
       $b = x * u$  &  $u$  in A by GROUP_2:33, C; then
consider u being Element of the carrier of G such that
D:  $b = x * u$  &  $u$  in A;
take a = u;
 $z = x * u * y$  by D, C;
hence thesis by D;
end;
(ex a being Element of the carrier of G st  $z = x * a * y$  & a in A)
      implies  $z$  in  $x * A * y$ 
proof
  assume ex a being Element of the carrier of G st
     $z = x * a * y$  & a in A; then
  consider a being Element of the carrier of G such that
  M:  $z = x * a * y$  & a in A;
  ex h being Element of the carrier of G st  $z = h * y$  & h in  $x * A$ 
    proof
      take  $h = x * a$ ;
      N:  $z = h * y$  by M;
      ex a being Element of the carrier of G st
         $h = x * a$  & a in A by M; then
        h in  $x * A$  by GROUP_2:33;
        hence thesis by N;
      end;
    hence thesis by GROUP_2:34;
  end;
hence thesis by A;
end;

```

```

theorem lemma_1_6_1:
for A being non empty Subset of G holds
for x holds
Card A = Card ( $x * A * x$ )
proof
let A be non empty Subset of G;
let x;
set B =  $x * A * x$ ;
C: A is non empty & B is non empty
  proof consider a being Element of A;
     $x * a * x$  in B by lemmaE;
    hence thesis ;
  end;
then reconsider B as non empty Subset of G;

deffunc F(Element of the carrier of G) =  $x * \$1 * x$ ;

```

```

consider f being Function of A, the carrier of G such that
D: for a being Element of A holds f.a = F(a) from LambdaD;
E: dom f = A by C,FUNCT_2:def 1;
F:rng f = B
proof
T:  rng f c= B
  proof
    let s be set; assume s in rng f; then
    consider a being set such that
    E1:  a in A & s = f.a by E,FUNCT_1:def 5;
    reconsider a as Element of A by E1;
    s = F(a) by D,E1;
    hence thesis by lemmaE;
  end;
B c= rng f
  proof
    let s be set;
    assume FF: s in B; then
    consider a being Element of the carrier of G such that
T1:  s = x" * a * x & a in A by lemmaE;
    ex x st x in dom f & s = f.x
      proof
        take x = a;
        thus thesis by T1, D, E;
      end;
    then
    s in rng f by FUNCT_1:def 5;
    hence thesis;
  end;
hence thesis by T, XBOOLE_0:def 10;
end; then
reconsider f as Function of A,B by E,FUNCT_2:4;

deffunc FF(Element of the carrier of G) = x*$1*x";
consider g being Function of B, the carrier of G such that
D': for b being Element of B holds g.b = FF(b) from LambdaD;
E': dom g = B by C,FUNCT_2:def 1;
F':rng g = A
proof
T':  rng g c= A
  proof
    let s be set; assume s in rng g; then
    consider a being set such that
    E1':  a in B & s = g.a by E',FUNCT_1:def 5;
    reconsider a as Element of B by E1';
    s = FF(a) by D',E1'; then
    E2': s = x * a * x" by D;
    consider c being Element of the carrier of G such that
    E3': a = x" * c * x & c in A by lemmaE, E1';
  end;
end;

```

```

s = x * (x" * c * x) * x" by E2',E3'
.= x * (x" * c) * x * x" by VECTSP_1:def 16
.= x * x" * c * x * x" by VECTSP_1:def 16
.= (x * x") * c * x * x" by VECTSP_1:def 16
.= (x * x") * c * (x * x") by VECTSP_1:def 16
.= 1.G * c * (x * x") by GROUP_1:def 5
.= 1.G * c * 1.G by GROUP_1:def 5
.= 1.G * c by GROUP_1:def 4
.= c by GROUP_1:def 4;
hence thesis by E3';
end;
A c= rng g
proof
let s be set;
assume G': s in A; reconsider s as Element of A by G';
ex b being Element of the carrier of G st
b = x" * s * x;
then
consider b being Element of the carrier of G such that
H': b = x" * s * x;
I': b in B by H', lemmaE;
ex u being set st u in dom g & s = g.u
proof
take u = b;
J': u in dom g by E', I'; then
g.u = x * u * x" by D',E'
.= x * (x" * s * x) * x" by H'
.= x * (x" * s) * x * x" by VECTSP_1:def 16
.= x * x" * s * x * x" by VECTSP_1:def 16
.= x * x" * s * x * x" by VECTSP_1:def 16
.= (x * x") * s * x * x" by VECTSP_1:def 16
.= (x * x") * s * (x * x") by VECTSP_1:def 16
.= 1.G * s * (x * x") by GROUP_1:def 5
.= 1.G * s * 1.G by GROUP_1:def 5
.= 1.G * s by GROUP_1:def 4
.= s by GROUP_1:def 4;
hence thesis by J';
end;

then
s in rng g by FUNCT_1:def 5;
hence thesis;
end;

hence thesis by T', XBOOLE_0:def 10;
end; then
reconsider g as Function of B,A by E',FUNCT_2:4;

G:for a,b being Element of A st f.a = f.b holds a = b

```

```

proof
  let a,b be Element of A such that G0: f.a = f.b;
  G1: a in A & b in A;
  f.a in B & f.b in B; then
  H0: g.(f.a) = g.(f.b) by G0;
  G0: x" * a * x in B by G1, lemmaE;
  G2: x" * b * x in B by G1, lemmaE;
  g.(f.a) = g.(x" * a * x) by D
    . = x * (x" * a * x) * x" by D', G0
    . = x * (x" * a) * x * x" by VECTSP_1:def 16
    . = x * x" * a * x * x" by VECTSP_1:def 16
    . = (x * x") * a * x * x" by VECTSP_1:def 16
    . = (x * x") * a * (x * x") by VECTSP_1:def 16
    . = 1.G * a * (x * x") by GROUP_1:def 5
    . = a * (x * x") by GROUP_1:def 4
    . = a * 1.G by GROUP_1:def 5
    . = a by GROUP_1:def 4; then
  H1: g.(f.a) = a;
  g.(f.b) = g.(x" * b * x) by D
    . = x * (x" * b * x) * x" by D', G2
    . = x * (x" * b) * x * x" by VECTSP_1:def 16
    . = x * x" * b * x * x" by VECTSP_1:def 16
    . = (x * x") * b * x * x" by VECTSP_1:def 16
    . = (x * x") * b * (x * x") by VECTSP_1:def 16
    . = 1.G * b * (x * x") by GROUP_1:def 5
    . = b * (x * x") by GROUP_1:def 4
    . = b * 1.G by GROUP_1:def 5
    . = b by GROUP_1:def 4; then
  g.(f.b) = b;

  hence thesis by H0, H1;
end;

```

```

A,B are_equipotent
proof take f;
  thus thesis by C,E,F,G,GROUP_6:1;
end;
hence thesis by CARD_1:21;
end;

```

```

definition let G, H, K;
func Double_Cosets (H, K) -> Subset-Family of the carrier of G means
:Def0: A in it iff ex a st A = H * a * K;
existence
proof
  defpred P[set] means ex a st $1 = H * a * K;
  ex F being Subset-Family of the carrier of G st

```

```

    for A being Subset of the carrier of G holds
      A in F iff P[A] from SubFamEx;
    hence thesis;
  end;
uniqueness
  proof let F1,F2 be Subset-Family of the carrier of G;
    defpred P[set] means ex a st $1 = H * a * K;
    assume A3: for A holds A in F1 iff P[A];
    assume A4: for A holds A in F2 iff P[A];
    thus thesis from SubFamComp(A3,A4);
  end;
end;

theorem lemmaD:
z in H * x * K iff ex g,h being Element of the carrier of G st
  z = g * x * h & g in H & h in K
proof
X: z in H * x * K implies ex g,h being Element of the carrier of G st
  z = g * x * h & g in H & h in K
proof
assume z in H * x * K;
  then z in (H * x) * K;
  then ex g1,g2 being Element of the carrier of G st
    z = g1 * g2 & g1 in H * x & g2 in K by GROUP_2:114;
  then consider g1, g2 being Element of the carrier of G such that
C:      z = g1 * g2 & g1 in H * x & g2 in K;
  g1 in H * x by C;
  then ex h1 being Element of the carrier of G st
    g1 = h1 * x & h1 in H by GROUP_2:126;
  then consider h1 being Element of the carrier of G such that
D:      g1 = h1 * x & h1 in H;
  ex g,h being Element of the carrier of G st
    z = g * x * h & g in H & h in K
  proof
    take g = h1;
    take h = g2;
    E: g in H & h in K by C,D;
    z = g1 * h by C;
    then z = g * x * h by D;
    hence thesis by E;
  end;
  hence thesis;
end;
Y: (ex g,h being Element of the carrier of G
  st z = g * x * h & g in H & h in K) implies z in H * x * K
proof
  assume (ex g,h being Element of the carrier of G st

```

```

      z = g * x * h & g in H & h in K);
then consider g,h being Element of the carrier of G such that
H:      z = g * x * h & g in H & h in K;
      ex g1, g2 being Element of the carrier of G st
      z = g1 * g2 & g1 in H * x & g2 in K
      proof
      set g2 = h;
      set g1 = g * x;
I: z = g1 * g2 by H;
J: g2 in K by H;
      g1 in H * x
      proof
      ex h1 being Element of the carrier of G st
      g1 = h1 * x & h1 in H
      proof
      take h1 = g;
      thus thesis by H;
      end; :: ex h1
      hence thesis by GROUP_2:126;
      end; :: g1 in H * x
      then
      z = g1 * g2 & g1 in H * x & g2 in K by I,J;
      hence thesis;
      end;
      then z in H * x * K by GROUP_2:114;
      hence thesis;
      end;
hence thesis by X, Y;
end;

```

reserve a for set;

```

theorem lemma1_7_1:
for H, K holds H * x * K = H * y * K or
not ex z st z in H * x * K & z in H * y * K
proof
let H, K;
per cases;
  suppose not ex z st z in H * x * K & z in H * y * K;
  hence thesis;
  suppose ex z st z in H * x * K & z in H * y * K;
  then consider z such that A: z in H * x * K & z in H * y * K;
  ex h1, k1 being Element of the carrier of G st
    z = h1 * x * k1 & h1 in H & k1 in K by A, lemmaD; then
  consider h1, k1 being Element of the carrier of G such that B:
    z = h1 * x * k1 & h1 in H & k1 in K;
  ex h2, k2 being Element of the carrier of G st
    z = h2 * y * k2 & h2 in H & k2 in K by A, lemmaD; then

```

```

consider h2, k2 being Element of the carrier of G such that C:
z = h2 * y * k2 & h2 in H & k2 in K;
h1 * x * k1 in H * y * K by A,B,C;
h2 * y * k2 in H * x * K by A,B,C;
D: H * x * K = H * y * K
  proof
    a in H * x * K implies a in H * y * K
      proof
        assume a in H * x * K;
        then ex g,h being Element of the carrier of G st
          a = g * x * h & g in H & h in K by lemmaD;
        then consider h,k
          being Element of the carrier of G such that
            a = h * x * k & h in H & k in K;
        ex c,d being Element of the carrier of G st
          a = c * y * d & c in H & d in K
          proof
            h = h * 1.G by GROUP_1:def 4; then
            F: h * x * k = h * 1.G * x * 1.G * k by GROUP_1:def 4;
            1.G = h1" * h1 by GROUP_1:def 5; then
            h * x * k = h * (h1" * h1) * x * (k1 * k1") * k
              by F, GROUP_1:def 5
            .= h * (h1" * h1) * x * k1 * k1" * k
              by VECTSP_1:def 16
            .= h * h1" * h1 * x * k1 * k1" * k
              by VECTSP_1:def 16
            .= h * h1" * (h1 * x) * k1 * k1" * k
              by VECTSP_1:def 16
            .= h * h1" * (h1 * x * k1) * k1" * k
              by VECTSP_1:def 16
            .= h * h1" * (h2 * y * k2) * k1" * k
              by B,C
            .= h * h1" * (h2 * y) * k2 * k1" * k
              by VECTSP_1:def 16
            .= h * h1" * h2 * y * k2 * k1" * k
              by VECTSP_1:def 16
            .= (h * h1") * h2 * y * k2 * k1" * k
              by VECTSP_1:def 16
            .= (h * h1" * h2) * y * k2 * k1" * k
              by VECTSP_1:def 16
            .= (h * h1" * h2) * y * (k2 * k1") * k
              by VECTSP_1:def 16
            .= (h * h1" * h2) * y * (k2 * k1" * k)
              by VECTSP_1:def 16; then
            I: h * x * k = (h * h1" * h2) * y * (k2 * k1" * k);
            take c = h * h1" * h2;
            take d = k2 * k1" * k;
            h * x * k = c * y * d by I; then
            J: a = c * y * d by E;

```

```

K: h * h1" * h2 in H
  proof
    h in H & h1" in H by B,E, GROUP_2:60; then
      h * h1" in H by GROUP_2:59;
      hence thesis by GROUP_2:59,C ;
    end;
L: k2 * k1" * k in K
  proof
    k2 in K & k1" in K by B,C, GROUP_2:60; then
      k2 * k1" in K by GROUP_2:59;
      hence thesis by GROUP_2:59, E;
    end;
  hence thesis by J, K;
  end;
  hence thesis by lemmaD;
end;
  hence thesis by TARSKI:def 3;
  end;
H * y * K c= H * x * K
  proof
    a in H * y * K implies a in H * x * K
      proof
        assume a in H * y * K;
        then ex g,h being Element of the carrier of G st
          a = g * y * h & g in H & h in K by lemmaD;
        then consider h,k being Element of the carrier of G
          such that E: a = h * y * k & h in H & k in K;
        ex c,d being Element of the carrier of G st
          a = c * x * d & c in H & d in K
          proof
            h = h * 1.G by GROUP_1:def 4; then
            F: h * y * k = h * 1.G * y * 1.G * k by GROUP_1:def 4;
            1.G = h2" * h2 by GROUP_1:def 5; then
            h * y * k = h * (h2" * h2) * y * (k2 * k2") * k
              by F, GROUP_1:def 5
            .= h * (h2" * h2) * y * k2 * k2" * k
              by VECTSP_1:def 16
            .= h * h2" * h2 * y * k2 * k2" * k
              by VECTSP_1:def 16
            .= h * h2" * (h2 * y) * k2 * k2" * k
              by VECTSP_1:def 16
            .= h * h2" * (h2 * y * k2) * k2" * k
              by VECTSP_1:def 16
            .= h * h2" * (h1 * x * k1) * k2" * k by B,C
            .= h * h2" * (h1 * x) * k1 * k2" * k
              by VECTSP_1:def 16
            .= h * h2" * h1 * x * k1 * k2" * k
              by VECTSP_1:def 16
            .= (h * h2") * h1 * x * k1 * k2" * k
          end
      end
    end
  end

```

```

                                by VECTSP_1:def 16
.= (h * h2" * h1) * x * k1 * k2" * k
                                by VECTSP_1:def 16
.= (h * h2" * h1) * x * (k1 * k2") * k
                                by VECTSP_1:def 16
.= (h * h2" * h1) * x * (k1 * k2" * k)
                                by VECTSP_1:def 16; then
I: h * y * k = (h * h2" * h1) * x * (k1 * k2" * k);
  take c = h * h2" * h1;
  take d = k1 * k2" * k;
  h * y * k = c * x * d by I; then
J: a = c * x * d by E;
K: h * h2" * h1 in H
  proof
    h in H & h2" in H by C,E, GROUP_2:60; then
    h * h2" in H by GROUP_2:59;
    hence thesis by GROUP_2:59,B ;
  end;
L: k1 * k2" * k in K
  proof
    k1 in K & k2" in K by B,C, GROUP_2:60; then
    k1 * k2" in K by GROUP_2:59;
    hence thesis by GROUP_2:59, E;
  end;
  hence thesis by J, K;
  end;
  hence thesis by lemmaD;
  end;
  hence thesis by TARSKI:def 3;
  end; then
H * x * K c= H * y * K & H * y * K c= H * x * K by D;
hence thesis by XBOOLE_0:def 10;
end;

```

```

reserve C for strict Subgroup of G;
reserve B, A for strict Subgroup of G;
reserve D for strict Subgroup of A;
reserve E for strict Subgroup of B;

```

```

definition
  let G,A;
  cluster Left_Cosets A -> non empty;
  coherence by GROUP_2:165;
end;

```

```

definition

```

```

let G;
let H be Subgroup of G;
redefine func index H;
synonym G/H;
end;

theorem theorem_1_5_5:
G = A "\/" B & D = A /\ B & G is finite implies
  G/B >= A/D  :: index B >= index D
proof
  assume A: G = A "\/" B & D = A /\ B & G is finite; then
    reconsider LCB = Left_Cosets B as finite non empty set by GROUP_2:164;
B1: A is finite by A, GROUP_2:48; then
    reconsider LCD = Left_Cosets D as finite non empty set by GROUP_2:164;
    reconsider DD = D as Subgroup of G;
B2: now let x,y be Element of G;
    let x',y' be Element of A such that
F1:  x' = x & y' = y;
F2:  y'" = y" by F1,GROUP_2:57;
F3:  y'"*x' in A by RLVECT_1:def 1;
    x*B = y*B iff y"*x in B by GROUP_2:137; then
    x*B = y*B iff y'"*x' in B by F1,F2,GROUP_2:52; then
    x*B = y*B iff y'"*x' in D by A,F3,GROUP_2:99;
    hence x*B = y*B iff x'*D = y'*D by GROUP_2:137;
  end;
  defpred P[set, set] means
    ex a being Element of G, a' being Element of A st
      a = a' & $2 = a*B & $1 = a'*D;
S: for x being Element of LCD ex y being Element of LCB st P[x,y]
  proof
    let x be Element of LCD;
    x in LCD; then x is Subset of A; then
    consider a' being Element of A such that
S1:  x = a'*D by B1,GROUP_2:def 15;
    reconsider a = a' as Element of G by GROUP_2:51;
    a*B in LCB by GROUP_2:def 15; then
    reconsider y = a*B as Element of LCB;
    take y,a,a'; thus thesis by S1;
  end;
  consider F being Function of LCD, LCB such that
T: for a being Element of LCD holds P[a,F.a] from FuncExD(S);
T1: dom F = LCD & rng F c= LCB by FUNCT_2:def 1,RELSET_1:12;
I1: index D = card LCD by GROUP_2:def 18;
I2: index B = card LCB by GROUP_2:def 18;
  F is one-to-one
  proof
    let x1,x2 be set;
    assume x1 in dom F & x2 in dom F; then

```

```

    reconsider z1 = x1, z2 = x2 as Element of LCD by T1;
    consider a being Element of G, a' being Element of A such that
I3: a = a' & F.z1 = a*B & z1 = a'*D by T;
    consider b being Element of G, b' being Element of A such that
I4: b = b' & F.z2 = b*B & z2 = b'*D by T;
    thus thesis by B2,I3,I4;
end; then
index D c= index B by T1,I1,I2,CARD_1:26;
hence thesis by CARD_1:56;
end;

```

```

theorem lemmaL:
G is finite implies index H > 0
proof
assume B: G is finite; then
A: ord G >= 1 by GROUP_1:90;
ord G = ord H * index H by GROUP_2:177, B; then
C: ord H * index H >= 1 by A;
index H <> 0
proof
assume index H = 0; then
ord H * index H = ord H * 0 . = 0;
hence contradiction by C;
end;
hence thesis by NAT_1:19;
end;

```

```

theorem theorem1_5_6:
for G being strict Group st G is finite
for C being strict Subgroup of G
for A,B being strict Subgroup of C st C = A "\/" B
for D being strict Subgroup of A st D = A /\ B
for E being strict Subgroup of B st E = A /\ B
for F being strict Subgroup of C st F = A /\ B
holds
Left_Cosets(B) is finite &
Left_Cosets(A) is finite & index A, index B are_relative_prime
implies index B = index D & index A = index E
proof
let G such that A0: G is finite;
let C be strict Subgroup of G;
let A,B be strict Subgroup of C such that A1: C = A "\/" B;

```

```

let D be strict Subgroup of A such that A2:  $D = A \wedge B$ ;
let E be strict Subgroup of B such that A3:  $E = A \wedge B$ ;
let F be strict Subgroup of C such that A4:  $F = A \wedge B$ ;
assume A5: Left_Cosets(B) is finite &
  Left_Cosets(A) is finite & index A, index B are_relative_prime;
A6: C is finite &  $F = E \wedge F = D$  by A0, A2, A4, A3, GROUP_2:48; then
A7: index F = index E * index B by GROUP_2:179;
index F = index D * index A by A6, GROUP_2:179; then
B0: index E * index B = index D * index A by A7;
B1: index B divides (index A * index D) by NAT_1:def 3, B0;
B11: (index B qua Integer) divides
      ((index A qua Integer) * (index D qua Integer))
      proof
        ex i3 being Integer st
          (index A qua Integer) * (index D qua Integer) =
            (index B qua Integer) * i3
            proof
              take i3 = index E;
              thus thesis by B0;
            end;
          hence thesis by INT_1:def 9;
        end;
B2: index A, (index B qua Integer) are_relative_prime by A5, EULER_2:1; then
B3: (index A qua Integer), (index B qua Integer) are_relative_prime
      by EULER_2:1; then
B33:(index B qua Integer) divides (index D qua Integer) by INT_2:40, B11;
B34: index B is Nat & index D is Nat; then
B35:(index B qua Integer) divides index D by B33;
B36: index B divides (index D qua Integer) by B34, B33;
B4: index B divides index D
      proof
        ex n being Nat st index D = (index B) * n
          proof
            consider i being Integer such that
              index D = (index B qua Integer) * i by INT_1:def 9, B35;
            BA: index B = index B qua Integer;
            0 <= i
              proof
                assume 0 > i; then
                  BG: 0 >= i;
                  BBO: C is finite by A0, GROUP_2:48; then
                    index B > 0 by lemmaL; then
                      BH: index B >= 0;
                      A is finite by BBO, GROUP_2:48; then
                        BI: index D > 0 by lemmaL;
                        (index B) * i <= 0 by BG, BH, REAL_2:123; then
                          index D <= 0 by BA, BB;
                          hence contradiction by BI;

```

```

        end;
    then reconsider i as Nat by INT_1:16;
    take n = i;
    index D = (index B) * n by BB, BA;
    hence thesis;
end;
hence thesis by NAT_1:def 3;
end;

B5: C/B >= A/D by theorem_1_5_5, A6, A1, A2;
D0: index B = index D
proof
  assume D1: index B <> index D;
  A is finite
  proof
    DD: C is Subgroup of G;
    A is Subgroup of C; then
    A is Subgroup of G by DD;
    hence thesis by A0, GROUP_2:48;
  end;
then
index D > 0 by lemmaL;
then
index B <= index D by NAT_1:54, B4; then
index B < index D by D1, REAL_1:def 5;
hence contradiction by B5;
end;

B3: index A divides index B * index E by NAT_1:def 3, B0;
B31: (index A qua Integer) divides
((index B qua Integer) * (index E qua Integer))
proof
  ex i3 being Integer st
  (index B qua Integer) * (index E qua Integer) =
  (index A qua Integer) * i3
  proof
    take i3 = index D;
    thus thesis by B0;
  end;
  hence thesis by INT_1:def 9;
end;

index B, index A are_relative_prime
proof
  index A, index B are_relative_prime by A5; then
  for k being Nat st k divides index A & k divides index B holds
    k =1 by PYTHTRIP:def 1; then
  for k being Nat st k divides index B & k divides index A holds k=1;
end;

```

```

    hence thesis by PYHTRIP:def 1;
  end; then
(index B qua Integer), (index A qua Integer) are_relative_prime
    by EULER_2:1; then
B440: (index A qua Integer) divides (index E qua Integer)
    by INT_2:40, B31; then
BBY: (index A qua Integer) divides index E;
B44: index A divides index E
  proof
    ex n being Nat st index E = (index A) * n
      proof
        consider i being Integer such that
BA:      index E = (index A qua Integer) * i by INT_1:def 9, BBY;
BB:      index A = index A qua Integer;
        0 <= i
          proof
            assume 0 > i; then
            BG: 0 >= i;
            BBO: C is finite by A0, GROUP_2:48; then
            index A > 0 by lemmaL; then
            BH: index A >= 0;
            B is finite by BBO, GROUP_2:48; then
            BI: index E > 0 by lemmaL;
            (index A) * i <= 0 by BG, BH, REAL_2:123; then
            index E <= 0 by BA, BB;
            hence contradiction by BI;
            end;
          then reconsider i as Nat by INT_1:16;
          take n = i;
          index E = (index A) * n by BB, BA;
          hence thesis;
        end;
      hence thesis by NAT_1:def 3;
    end;
end;

```

```

B6: index A >= index E
  proof
    E0: C = B "\/" A by A1, GROUP_4:74;
    E = B /\ A by A3, GROUP_2:def 10;
    hence thesis by A6, theorem_1_5_5, E0;
  end;

```

```

index A = index E
  proof
    assume D11: index A <> index E;
    B is finite
      proof

```

```

        DD: C is Subgroup of G;
           B is Subgroup of C; then
           B is Subgroup of G by DD;
           hence thesis by A0, GROUP_2:48;
        end;

    then
    index E > 0 by lemmaL;
    then
    index A <= index E by NAT_1:54, B44; then
    index A < index E by D11, REAL_1:def 5;
    hence contradiction by B6;
    end;
hence thesis by D0;
end;

theorem lemmaK:
for a being Element of the carrier of G holds a in H implies
for j being Integer holds a |^ j in H
proof
let a be Element of the carrier of G;
assume A: a in H;
let j be Integer;
ex k being Nat st j = k or j = -k by INT_1:8; then
consider k being Nat such that
B: j = k or j = - k;
per cases by B;
  suppose S: j =k;
  defpred P[Nat] means a |^ $1 in H;
  Q: P[0]
  proof
    a |^0 = 1.G by GROUP_1:43;
    hence thesis by GROUP_2:55 ;
  end;
  R: for n being Nat st P[n] holds P[n + 1]
  proof
    let n be Nat such that R0: P[n];
    a |^ n in H by R0; then
    (a |^ n) * a in H by A, GROUP_2:59;
    hence thesis by GROUP_1:49;
  end;
for n being Nat holds P[n] from Ind(Q,R);
then P[k];
hence thesis by S;
suppose L: j = - k;
defpred PP[Nat] means a |^ (- $1) in H;
QQ: PP[0]
  proof
    a |^0 = 1.G by GROUP_1:43;

```

```

    hence thesis by GROUP_2:55 ;
  end;
RR: for n being Nat st PP[n] holds PP[n +1 ]
  proof
    let n be Nat such that Y0: PP[n];
    a" in H by A, GROUP_2:60; then
    a |(-n) * a" in H by Y0, GROUP_2:59; then
    a |(-n) * a |(-1) in H by GROUP_1:62; then
    a |(- n + (- 1)) in H by GROUP_1:63;
    then a |(- n + - 1) in H; then
    a |((-n) + - 1) in H; then
    a |(- 1 * (n + 1)) in H by XCMLPX_1:140;

    hence thesis;
  end;
for n being Nat holds PP[n] from Ind(QQ,RR); then
PP[k]; then a |(- k) in H;
hence thesis by L;

hence thesis;
end;

reserve a for Element of the carrier of G;

theorem lemmaZ:
for G being strict Group st G <> (1).G
ex b being Element of the carrier of G st b <> 1.G
proof
let G be strict Group such that A: G <> (1).G;
assume not(ex b being Element of the carrier of G st b <> 1.G); then
B: for b being Element of the carrier of G holds b = 1.G;
G is trivial
  proof
    for x,y being Element of the carrier of G holds x = y
      proof
        let x,y be Element of the carrier of G;
        D: x = 1.G by B;
        y = 1.G by B;
        hence thesis by D;
      end;
    hence thesis by REALSET1:def 20;
  end; then
G = (1).G by GROUP_6:13;

```

hence contradiction by A;
 end;

```

theorem lemmaJJ:
for G being strict Group
for a being Element of the carrier of G st G = gr{a} & G <> (1).G
for H being strict Subgroup of G st H <> (1).G holds
ex k being Nat st 0 < k & a |^k in H
proof
let G be strict Group;
let a be Element of the carrier of G such that A: G = gr{a} & G <> (1).G;
let H be strict Subgroup of G such that B: H <> (1).G;
B0: H <> (1).H by GROUP_2:75, B; then
ex b being Element of the carrier of H st b <> 1.H by lemmaZ; then

consider b being Element of the carrier of H such that
C: b <> 1.H;
D:b in G by GROUP_2:50; then
reconsider b as Element of the carrier of G by RLVECT_1:def 1;
ex c being Element of the carrier of H st c <> 1.H by B0, lemmaZ; then consider
c being Element of the carrier of H such that M: c <> 1.H;
M0: c in H by RLVECT_1:def 1; then
c in G by GROUP_2:49; then
reconsider c as Element of the carrier of G by RLVECT_1:def 1;
MM: c in gr{a} by M0,A, GROUP_2:49;
ex j being Integer st c = a |^j & j <> 0
proof
  assume not(ex j being Integer st c = a |^j & j <> 0); then
  MB: for j being Integer st c = a |^j holds j = 0;
  ex i being Integer st c = a |^i by MM, GR_CY_1:25; then
  consider i being Integer such that
  MA: c = a |^ i;
  MC: i = 0 by MA, MB;
  a |^i <> 1.H by M, MA; then
  a |^i <> 1.G by GROUP_2:53; then
  i <> 0 by GROUP_1:59;
  hence contradiction by MC;
end; then consider j being Integer
such that N: c = a |^ j & j <> 0;
ex n being Nat st j = n or j = -n by INT_1:8; then consider n being Nat
such that O: j = n or j = -n;
per cases by O;
  suppose P: j = n;
  M1: c = a |^ n by N, P;
  n <> 0 by N, P; then

```

```

S: 0 < n by NAT_1:19;
a |^ n in H by M0, M1;
hence thesis by S;
suppose R: j = - n;
T0: c = a |^ -n by R,N;
n <> 0 by R,N; then
S0: 0 < n by NAT_1:19;
a |^ -n in H by T0, M0; then
(a |^ n)" in H by GROUP_1:71; then
(a |^ n)"" in H by GROUP_2:60; then
a |^ n in H by GROUP_1:19;
hence thesis by S0;
hence thesis;
end;

```

```

theorem lemmaJ:
for G being strict cyclic Group st G <> (1).G
for H being strict Subgroup of G st H <> (1).G holds
H is cyclic Group
proof
let G be strict cyclic Group such that AA0: G <> (1).G;
let H be strict Subgroup of G such that AA: H <> (1).G;
ex a being Element of the carrier of G st
  the HGrStr of G = gr {a} by GR_CY_1:def 9; then
consider b being Element of the carrier of G such that
A: the HGrStr of G = gr{b};

b in G by GR_CY_2:8, A;
ex i being Integer st b |^ i in H
proof
take i=0;
b |^ 0 = 1.G by GROUP_1:43;
hence thesis by GROUP_2:55;
end;
then consider i being Integer such that
A3: b |^ i in H;

ex m being Nat st 0 < m & b |^m in H & for j being Nat st
0 < j & b |^j in H holds m <= j
proof
defpred P[Nat] means 0 < $1 & b |^$1 in H;
DD: ex k being Nat st P[k] by lemmaJJ, AA, A, AA0;
ex m being Nat st P[m] & for j being Nat st P[j] holds m <= j
from Min(DD);
hence thesis;
end;

```

```

then
consider m being Nat such that
A8:  $0 < m$  &  $b \mid^m$  in H & for j being Nat st  $0 < j$  &  $b \mid^j$  in H holds  $m \leq j$ ;

set c =  $b \mid^m$ ;
reconsider c as Element of the carrier of H by RLVECT_1:def 1, A8;
RR:  $c = b \mid^m$ ;
RR3: c is Element of the carrier of G by GROUP_2:50, RLVECT_1:def 1;
RRR: for a being Element of the carrier of H holds
ex i being Integer st  $a = c \mid^i$ 
  proof
    let a be Element of the carrier of H;
    ex k being Nat st  $i = k$  or  $i = -k$  by INT_1:8; then
    consider k being Nat such that
AA4:  $i = k$  or  $i = -k$ ;
A4:  $b \mid^k$  in H
  proof
    per cases by AA4;
    suppose  $i = k$ ;
    hence thesis by A3;
    suppose  $i = -k$ ; then
     $b \mid^{-k}$  in H by A3; then
    ( $b \mid^k$ )" in H by GROUP_1:70; then
    ( $b \mid^k$ )" " in H by GROUP_2:60;
    hence thesis by GROUP_1:19;
    hence thesis;
  end;

  end;

ex t being Integer st  $b \mid^t$  in H &  $b \mid^t = a$ 
  proof

    C0: a in G by GROUP_2:50; then
    CC: a in  $\text{gr}\{b\}$  by A;
    a is Element of the carrier of G
      by RLVECT_1:def 1, C0; then
    ex j1 being Integer st  $a = b \mid^{j1}$ 
      by GR_CY_1:25, CC; then consider j1 being Integer
    such that C1:  $a = b \mid^{j1}$ ;
     $b \mid^{j1}$  in H by RLVECT_1:def 1, C1;
    hence thesis by C1;
  end;

then consider t being Integer such that A9:  $b \mid^t$  in H &  $b \mid^t = a$ ;
ex r,s being Integer st  $0 \leq s$  &  $s < m$  &  $t = m * r + s$ 

proof
  take  $r = t \text{ div } m$ ;

```

```

    take s = t mod m;
    Y1: t = r * m + s by GR_CY_2:4, A8;
    m >= 0 by NAT_1:18; then
    Y2: t mod m >= 0 by GR_CY_2:2;
    t mod m < m by GR_CY_2:3, A8;
    hence thesis by Y1,Y2;
    hence thesis;
end; then consider r,s being Integer such that W0:
0 <= s & s < m & t = m * r + s;
reconsider s as Nat by INT_1:16, W0;

    Y4: b |^ t = b |^ (m * r + s) by W0
.= b |^(m * r) * (b |^ s) by GROUP_1:63
.= ((b |^ m)|^ r) * (b |^ s) by GROUP_1:67;
Y3: (b |^ m) |^ r in H by lemmaK, A8;
X0: b |^ s in H
proof
  set u = b |^ t;
  set v = (b |^ m) |^ r;
  Y5: u = v * b |^ s & u in H & v in H by Y3, Y4, A9; then
  Y6: v" * u = v" * (v * b |^ s)
  .= v" * v * b |^ s by VECTSP_1:def 16
  .= (v" * v) * b |^ s by VECTSP_1:def 16
  .= 1.G * b |^ s by GROUP_1:def 5
  .= b |^ s by GROUP_1:def 4;
  v" in H by GROUP_2:60, Y5; then
  v" * u in H by GROUP_2:59, Y5;
  hence thesis by Y6;
end;

    b |^ s = 1.G
proof
  s = 0
proof
  assume s <> 0; then
  s > 0 by NAT_1:19; then
  m <= s by A8, X0;
  hence contradiction by W0;
  end;
  hence thesis by GROUP_1:43 ;
end; then
    b |^ t = ((b |^ m) |^ r) * 1.G by Y4
  .= (b |^ m) |^ r by GROUP_1:def 4;
  then
    b |^ t = (b |^ m) |^ r; then
  A10: a = (b |^ m) |^ r by A9;
  RA: b |^ m = c by RR; then
    b |^ m is Element of the carrier of G by GROUP_2:50, RLVECT_1:def 1; then

```

```
(b |^m)|^ r = (c) |^ r by RR3, RA, lemmaB0;  
hence thesis by A10;  
end;  
H = gr{c} by GR_CY_2:11, RRR; then  
H is cyclic Group by GR_CY_2:10;  
hence thesis;  
end;
```