Ten Formal Proof Sketches

Freek Wiedijk

Radboud University Nijmegen

Abstract. This note collects the formal proof sketches that I have done.

1 Algebra: Irrationality of $\sqrt{2}$

1.1 Source

G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers.* 4th edition, Clarendon Press, Oxford, 1960. Pages 39–40.

1.2 Informal Proof

THEOREM 43 (PYTHAGORAS' THEOREM). $\sqrt{2}$ *is irrational.*

The traditional proof ascribed to Pythagoras runs as follows. If $\sqrt{2}$ is rational, then the equation

$$a^2 = 2b^2 \tag{4.3.1}$$

is soluble in integers a, b with $(a, b) = 1$. Hence a^2 is even, and therefore a is even. If $a = 2c$, then $4c^2 = 2b^2$, $2c^2 = b^2$, and b is also even, contrary to the hypothesis that $(a, b) = 1$.

1.3 Formal Proof Sketch: Informal Layout

THEOREM Th43: sqrt 2 *is irrational* :: PYTHAGORAS' THEOREM

PROOF assume sqrt 2 is rational; consider a, b such that

4_3_1: $$a\hat{}2 = 2 * b\hat{}2$$

and a, b are_relative_prime; $a\hat{}2$ is even; a is even; consider c such that $a = 2 * c$; $4 * c\hat{}2 = 2 * b\hat{}2$; $2 * c\hat{}2 = b\hat{}2$; b is even; thus contradiction; END;

1.4 Formal Proof Sketch: Formal Layout

```
theorem Th43: sqrt 2 is irrational
proof
 assume sqrt 2 is rational;
 consider a,b such that
4_3_1: a^2 = 2*b^2 and
  a,b are_relative_prime;                                          *4
```

```
 a^2 is even;                                               *4
 a is even;                                                 *4
 consider c such that a = 2*c;                              *4
 4*c^2 = 2*b^2;                                             *4
 2*c^2 = b^2;                                               *4
 b is even;                                                 *4
 thus contradiction;                                        *1
end;
```

1.5 Formal Proof

```
theorem Th43: sqrt 2 is irrational
proof
 assume sqrt 2 is rational;
 then consider a,b such that
A1: b <> 0 and
A2: sqrt 2 = a/b and
A3: a,b are_relative_prime by Def1;
A4: b^2 <> 0 by A1,SQUARE_1:73;
 2 = (a/b)^2 by A2,SQUARE_1:def 4
  .= a^2/b^2 by SQUARE_1:69;
 then
4_3_1: a^2 = 2*b^2 by A4,REAL_1:43;
 a^2 is even by 4_3_1,ABIAN:def 1;
 then
A5: a is even by PYTHTRIP:2;
 then consider c such that
A6: a = 2*c by ABIAN:def 1;
A7: 4*c^2 = (2*2)*c^2
  .= 2^2*c^2 by SQUARE_1:def 3
  .= 2*b^2 by A6,4_3_1,SQUARE_1:68;
 2*(2*c^2) = (2*2)*c^2 by AXIOMS:16
  .= 2*b^2 by A7;
 then 2*c^2 = b^2 by REAL_1:9;
 then b^2 is even by ABIAN:def 1;
 then b is even by PYTHTRIP:2;
 then 2 divides a & 2 divides b by A5,Def2;
 then
A8: 2 divides a gcd b by INT_2:33;
 a gcd b = 1 by A3,INT_2:def 4;
 hence contradiction by A8,INT_2:17;
end;
```

1.6 Mizar Version

6.1.11 – 3.33.722

2 Algebra: Infinity of Primes

2.1 Source

The slides of a talk by Herman Geuvers, *Formalizing an intuitionistic proof of the Fundamental Theorem of Algebra.*

2.2 Informal Proof

Theorem There are infinitely many primes:
for every number n there exists a prime $p > n$

Proof [after Euclid]
Given n. Consider $k = n! + 1$, where $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$.
Let p be a prime that divides k.
For this number p we have $p > n$: otherwise $p \leq n$;
but then p divides $n!$,
so p cannot divide $k = n! + 1$,
contradicting the choice of p. QED

2.3 Formal Proof Sketch: Informal Layout

theorem $\{n : n$ is prime$\}$ is infinite proof
for n ex p st p is prime & $p > n$

proof :: [after Euclid]
let n; set $k = n! + 1$;
consider p such that p is prime & p divides k;
take p; thus p is prime; thus $p > n$ proof assume $p <= n$;
p divides $n!$;
not p divides $n! + 1$;
thus contradiction; end; end; thus thesis; end;

2.4 Formal Proof Sketch: Formal Layout

```
theorem {n: n is prime} is infinite
proof
 for n ex p st p is prime & p > n
 proof
  let n;
  set k = n! + 1;
  consider p such that p is prime & p divides k;                        *4
  take p;
  thus p is prime;                                                       *4
  thus p > n
  proof
   assume p <= n;
```

```
   p divides n!;                                                    *4
   not p divides n! + 1;                                            *4
   thus contradiction;                                              *1
  end;
 end;
 thus thesis;                                                       *4
end;
```

2.5 Formal Proof

```
theorem {p: p is prime} is infinite
proof
A1: for n ex p st p is prime & p > n
 proof
  let n;
  set k = n! + 1;
  n! > 0 by NEWTON:23;
  then n! >= 0 + 1 by NAT_1:38;
  then k >= 1 + 1 by REAL_1:55;
  then consider p such that
A2: p is prime & p divides k by INT_2:48;
  take p;
  thus p is prime by A2;
  assume
A3: p <= n;
  p <> 0 by A2,INT_2:def 5;
  then
A4: p divides n! by A3,NAT_LAT:16;
  p > 1 by A2,INT_2:def 5;
  then not p divides 1 by NAT_1:54;
  hence contradiction by A2,A4,NAT_1:57;
 end;
 thus thesis from Unbounded(A1);
end;
```

2.6 Mizar Version

6.1.11 – 3.33.722

3 Algebra: Image of Left Unit Element

3.1 Source

Rob Nederpelt, *Weak Type Theory: A formal language for mathematics.* Computer Science Report 02-05, Eindhoven University of Technology, Department of Math. and Comp. Sc., May 2002. Page 42.

3.2 Informal Proof

THEOREM. Let G be a set with a binary operation $\cdot$ and left unit element e. Let H be a set with binary operation $*$ and assume that ϕ is a homomorphism of G onto H. Then H has a left unit element as well.

PROOF. Take $e' = \phi(e)$. Let $h \in H$. There is $g \in G$ such that $\phi(g) = h$. Then

$$e' * h = \phi(e) * \phi(g) = \phi(e \cdot g) = \phi(g) = h,$$

hence e' is left unit element of H. □

3.3 Formal Proof Sketch: Informal Layout

let G, H be non empty HGrStr; let e be Element of G such that e is_left_unit_of G; let *phi* be map of G, H such that *phi* is_homomorphism G, H and *phi* is onto; thus ex e' being Element of H st e' is_left_unit_of H

PROOF take $e' = phi.e$; now let h be Element of H; consider g being Element of G such that $phi.g = h$; thus

$$e' * h = phi.e * phi.g \mathrel{.=} phi.(e * g) \mathrel{.=} phi.g \mathrel{.=} h;$$

end; hence e' is_left_unit_of H; END;

3.4 Formal Proof Sketch: Formal Layout

```
 let G,H be non empty HGrStr;
 let e be Element of G such that e is_left_unit_of G;
 let phi be map of G,H such that
  phi is_homomorphism G,H and phi is onto;
 thus ex e' being Element of H st e' is_left_unit_of H
proof
 take e' = phi.e;
 now
  let h be Element of H;
  consider g being Element of G such that phi.g = h;                  *4
  thus e' * h = phi.e * phi.g .= phi.(e * g) .= phi.g .= h;           *4 *4 *4 *4
 end;
 hence e' is_left_unit_of H;                                          *4
end;
```

3.5 Formal Proof

```
 let G,H be non empty HGrStr;
 let e be Element of G such that
H1: e is_left_unit_of G;
 let phi be map of G,H such that
H2: phi is_homomorphism G,H and
```

```
H3: phi is onto;
 thus ex e' being Element of H st e' is_left_unit_of H
proof
 take e' = phi.e;
 now
  let h be Element of H;
  consider g being Element of G such that
A1: phi.g = h by H3,Th1;
  thus e' * h = phi.(e * g) by A1,H2,Def2
   .= h by A1,H1,Def1;
 end;
 hence e' is_left_unit_of H by Def1;
end;
```

3.6 Mizar Version

6.1.11 – 3.33.722

4 Algebra: Lagrange's Theorem

4.1 Source

B.L. van der Waerden, *Algebra*. 5th edition, Springer-Verlag, Berlin, 1966. Page 26.

4.2 Informal Proof

Zwei Nebenklassen $a\mathfrak{g}$, $b\mathfrak{g}$ können sehr wohl gleich sein, ohne daß $a = b$ ist. Immer dann nämlich, wenn $a^{-1}b$ in $\mathfrak{g}$ liegt, gilt

$$b\mathfrak{g} = aa^{-1}b\mathfrak{g} = a(a^{-1}b\mathfrak{g}) = a\mathfrak{g}.$$

Zwei *verschiedene* Nebenklassen haben kein Element gemeinsam. Denn wenn die Nebenklassen $a\mathfrak{g}$ und $b\mathfrak{g}$ ein Element gemein haben, etwa

$$ag_1 = bg_2,$$

so folgt

$$g_1g_2^{-1} = a^{-1}b.$$

so daß $a^{-1}b$ in $\mathfrak{g}$ liegt; nach dem Vorigen sind also $a\mathfrak{g}$ und $b\mathfrak{g}$ identisch.

Jedes Element a gehört einer Nebenklasse an, nämlich der Nebenklasse $a\mathfrak{g}$. Diese enthält ja sicher das Element $ae = a$. Nach dem eben Bewiesenen gehört das Element a auch *nur* einer Nebenklasse an. Wir können demnach jedes Element a als *Repräsentanten* der a enthaltenden Nebenklass $a\mathfrak{g}$ ansehen.

Nach dem vorhergehenden bilden die Nebenklassen eine *Klasseneinteilung* der Gruppe $\mathfrak{G}$. Jedes Element gehört einer und nur einer Klasse an.

Je zwei Nebenklassen sind gleichmächtig. Denn durch $a\mathfrak{g} \to b\mathfrak{g}$ ist eine eineindeutige Abbildung von $a\mathfrak{g}$ auf $b\mathfrak{g}$ definiert.

Die Nebenklassen sind, mit Ausnahme von $\mathfrak{g}$ selbst, *keine* Gruppen; denn eine Gruppe müßte das Einselelement enthalten.

Die Anzahl der verschiedenen Nebenklassen einer Untergruppe $\mathfrak{g}$ in $\mathfrak{G}$ heißt der *Index* von $\mathfrak{g}$ in $\mathfrak{G}$. Der Index kann endlich oder unendlich sein.

Ist N die als (endlich angenommene) Ordnung von $\mathfrak{G}$, n die von $\mathfrak{g}$, j der Index, so gilt die Relation

$$N = jn; \tag{2}$$

denn $\mathfrak{G}$ ist ja in j Klassen eingeteilt, deren jede n Elemente enthält.

Man kann für endliche Gruppen aus (2) den Index j berechnen:

$$j = \frac{N}{n}$$

Folge. *Die Ordnung einer Untergruppe einer endlichen Gruppe ist ein Teiler der Ordnung der Gesamtgruppe.*

4.3 Formal Proof Sketch: Informal Layout

now let a,b; assume $a\hat{\ }^{-1} * b$ in G; thus

$$b * G = a * a\hat{\ }^{-1} * b * G. = a * (a\hat{\ }^{-1} * b * G). = a * G; \qquad \textit{end;}$$

for a, b st $a * G <> b * G$ holds $(a * G) \mathbin{/\backslash} (b * G) = \{\}$
proof let a,b; now assume $(a * G) \mathbin{/\backslash} (b * G) <> \{\}$; consider g_1, g_2 such that

$$a * g_1 = b * g_2;$$

$$g_1 * g_2\hat{\ }^{-1} = a\hat{\ }^{-1} * b;$$

$a\hat{\ }^{-1} * b$ in G; thus $a * G = b * G$; end; thus thesis; end;

for a holds a in $a * G$ proof let a; $a * e(G) = a$; thus thesis; end;

$\{a * G : a \text{ in } H\}$ is a˙partition of H;

for a, b holds card$(a{*}G)$ = card$(b{*}G)$ proof let a, b; consider f being Function of $a * G, b * G$ such that for g holds $f.(a * g) = b * g$; f is bijective; thus thesis; end;

set 'Index' = card$\{a * G : a \text{ in } H\}$;

now let N such that $N =$ card H; let n such that $n =$ card G; let j such that $j =$ 'Index'; thus

'2': $$N = j * n; \qquad \textit{end;}$$

thus *card G divides card H*;

4.4 Formal Proof Sketch: Formal Layout

```
now
 let a,b;
 assume a^-1*b in G;
 thus b*G = a*a^-1*b*G .= a*(a^-1*b*G) .= a*G;                   *4 *4 *4
end;
for a,b st a*G <> b*G holds (a*G) /\ (b*G) = {}
proof
 let a,b;
 now
  assume (a*G) /\ (b*G) <> {};
  consider g1,g2 such that a*g1 = b*g2;                          *4
  g1*g2^-1 = a^-1*b;                                             *4
  a^-1*b in G;                                                   *4
  thus a*G = b*G;                                                *4
 end;
 thus thesis;                                                    *4
end;
for a holds a in a*G
proof
 let a;
 a*e(G) = a;                                                     *4
 thus thesis;                                                    *4
end;
{a*G : a in H} is a_partition of H;                              *4
for a,b holds card(a*G) = card(b*G)
proof
 let a,b;
 consider f being Function of a*G,b*G such that
  for g holds f.(a*g) = b*g;                                     *4
 f is bijective;                                                 *4
 thus thesis;                                                    *4
end;
set 'Index' = card {a*G : a in H};
now
 let N such that N = card H;
 let n such that n = card G;
 let j such that j = 'Index';
 thus
'2': N = j*n;                                                    *4
end;
thus card G divides card H;                                      *4
```

4.5 Formal Proof

```
A1: now
 let a,b;
 assume
A2: a^-1*b in G;
```

```
 thus b*G = e(H)*b*G by GROUP_1:def 5
  .= a*a^-1*b*G by GROUP_1:def 6
  .= a*(a^-1*b)*G by GROUP_1:def 4
  .= a*(a^-1*b*G) by GROUP_2:127
  .= a*(carr G) by A2,GROUP_2:136
  .= a*G by GROUP_2:def 13;
end;
A3: for a,b st a*G <> b*G holds (a*G) /\ (b*G) = {}
proof
 let a,b;
 now
  assume (a*G) /\ (b*G) <> {};
  then consider x such that
A4: x in (a*G) /\ (b*G) by XBOOLE_0:7;
A5: x in a*G & x in b*G by A4,XBOOLE_0:def 4;
  consider g1 such that
A6: x = a*g1 by A5,Th5;
  consider g2 such that
A7: x = b*g2 by A5,Th5;
  set g1G = g1;
  set g2G = g2;
  reconsider g1 as Element of H by GROUP_2:51;
  reconsider g2 as Element of H by GROUP_2:51;
A8: a*g1 = a*g1G by Th2
   .= b*g2 by A6,A7,Th2;
  g1G*g2G^-1 = g1*g2G^-1 by Th3
   .= g1*g2^-1 by Th2,GROUP_2:57
   .= e(H)*g1*g2^-1 by GROUP_1:def 5
   .= a^-1*a*g1*g2^-1 by GROUP_1:def 6
   .= a^-1*(a*g1)*g2^-1 by GROUP_1:def 4
   .= a^-1*(b*g2*g2^-1) by A8,GROUP_1:def 4
   .= a^-1*(b*(g2*g2^-1)) by GROUP_1:def 4
   .= a^-1*(b*e(H)) by GROUP_1:def 6
   .= a^-1*b by GROUP_1:def 5;
  then a^-1*b in G by STRUCT_0:def 5;
  hence a*G = b*G by A1;
 end;
 hence thesis;
end;
A9: for a holds a in a*G
proof
 let a;
 a*e(G) = a*e(H) by Th2,GROUP_2:53
  .= a by GROUP_1:def 5;
 hence thesis;
end;
set X = {a*G : a in H};
X c= bool the carrier of H
proof
 let A;
```

```
 assume A in X;
 then consider a such that
A10: A = a*G & a in H;
 thus A in bool the carrier of H by A10,ZFMISC_1:def 1;
end;
then reconsider X as Subset-Family of H;
A11: X is a_partition of the carrier of H
proof
 thus union X = the carrier of H
 proof
  thus union X c= the carrier of H;
  let x;
  assume
A12: x in the carrier of H;
  then reconsider a = x as Element of H;
  x in H by A12,STRUCT_0:def 5;
  then a in a*G & a*G in X by A9;
  hence x in union X by TARSKI:def 4;
 end;
 let A be Subset of the carrier of H;
 assume A in X;
 then consider a such that
A13: A = a*G & a in H;
 thus A <> {} by A13;
 let B be Subset of the carrier of H;
 assume B in X;
 then consider b such that
A14: B = b*G & b in H;
 assume A <> B;
 then A /\ B = {} by A3,A13,A14;
 hence A misses B by XBOOLE_0:def 7;
end;
then reconsider X as a_partition of H;
{a*G : a in H} is a_partition of H by A11;
A15: for a,b holds card(a*G) = card(b*G)
proof
 let a,b;
 defpred P[Element of a*G,Element of b*G] means
  for g st $1 = a*g holds $2 = b*g;
A16: now
  let x be Element of a*G;
  consider g such that
A17: x = a*g by Th5;
  reconsider y = b*g as Element of b*G;
  take y;
  thus P[x,y] by A17,Th4;
 end;
 consider f being Function of a*G,b*G such that
A18: for x being Element of a*G holds P[x,f.x qua Element of b*G]
   from FUNCT_2:sch 3(A16);
```

```
 for g holds f.(a*g) = b*g by A18;
 f is bijective
 proof
  hereby
   let x,x' be Element of a*G;
   consider g such that
A19: x = a*g by Th5;
   consider g' such that
A20: x' = a*g' by Th5;
A21: f.x = b*g & f.x' = b*g' by A19,A20,A18;
   assume f.x = f.x';
   hence x = x' by A19,A20,A21,Th4;
  end;
  let y be Element of b*G;
  consider g such that
A22: y = b*g by Th5;
  take a*g;
  thus thesis by A18,A22;
 end;
 hence thesis by EUCLID_7:3;
end;
set 'Index' = card {a*G : a in H};
'Index' = card X;
then reconsider 'Index' as natural number;
now
 let N such that
A23: N = card H;
 let n such that
A24: n = card G;
 let j such that
A25: j = 'Index';
A26: card H = card the carrier of H by STRUCT_0:def 17;
 now
  let A;
  assume A in X;
  then consider a such that
A27: A = a*G & a in H;
  e(H)*G = carr(G) by GROUP_2:132
   .= the carrier of G by GROUP_2:def 9;
  then card(e(H)*G) = card G by STRUCT_0:def 17;
  hence card A = n by A15,A24,A27;
 end;
 hence N = j*n by A23,A25,A26,Th1;
end;
then card H = 'Index'*card G;
hence card G divides card H by INT_1:def 9;
```

4.6 Mizar Version

7.11.01 – 4.117.1046

5 Analysis: successor has no fixed point

5.1 Source

Fairouz Kamareddine, Manuel Maarek and J.B. Wells, *MathLang: experience-driven development of a new mathematical language,* draft. Page 11.

Quoted from: Edmund Landau, *Foundations of Analysis.* Translated by F. Steinhardt, Chelsea, 1951.

5.2 Informal Proof

Theorem 2

$$x' \neq x$$

Proof Let $\mathfrak{M}$ be the set of all x for which this holds true.

I) By Axiom 1 and Axiom 3,

$$1' \neq 1;$$

therefore 1 belongs to $\mathfrak{M}$.

II) If x belongs to $\mathfrak{M}$, then

$$x' \neq x,$$

and hence by Theorem 1,

$$(x')' \neq x',$$

so that x' belongs to $\mathfrak{M}$.

By Axiom 5, $\mathfrak{M}$ therefore contains all the natural numbers, i.e. we have for each x that

$$x' \neq x.$$

5.3 Formal Proof Sketch: Informal Layout

Theorem_2:

$$x\ ' <> x$$

proof set $\mathfrak{M} = \{y : y\ ' <> y\}$;

I: now

$$1\ ' <> 1$$

by Axiom_1, Axiom_3; hence 1 in $\mathfrak{M}$; *end;*

II: now let x; assume x in $\mathfrak{M}$; then

$$x\ ' <> x;$$

then

$$(x\ ')' <> x\ '$$

by Theorem_1; hence $x\ '$ in $\mathfrak{M}$; *end;*

for x holds x in $\mathfrak{M}$ by Axiom_5; hence

$$x\ ' <> x;$$ *end;*

5.4 Formal Proof Sketch: Formal Layout

```
Theorem_2: x ' <> x
proof
 set M = {y : y ' <> y};
I: now
  1 ' <> 1 by Axiom_1, Axiom_3;
  hence 1 in M;                                        *4
 end;
II: now let x;
  assume x in M;
  then x ' <> x;                                       *4
  then (x ')' <> x ' by Theorem_1;
  hence x ' in M;
 end;
 for x holds x in M by Axiom_5;                        *4
 hence x ' <> x;                                       *4
end;
```

5.5 Formal Proof

```
Theorem_2: x ' <> x
proof
 set M = {y : y ' <> y};
I: now
  1 ' <> 1 by Axiom_3;
  hence 1 in M by Axiom_1;
 end;
 now let x;
  assume x in M;
  then ex y st x = y & y ' <> y;
  then (x ')' <> x ' by Axiom_4;
  hence x ' in M;
 end;
 then x in M by I,Axiom_5;
 then ex y st x = y & y ' <> y;
 hence x ' <> x;
end;
```

5.6 Mizar Version

6.4.01 – 3.60.795

6 Analysis: successor has no fixed point

6.1 Source

A message *Formal verification* on the FOM mailing list by Lasse Rempe-Gillen ⟨L.Rempe@liverpool.ac.uk⟩, dated 21 October 2014 and with Message-ID ⟨675123965B518F43B235C5FCB5D565DCBF14577E@CHEXMBX1.livad.liv.ac.uk⟩.

6.2 Informal Proof

Let f be a real-valued function on the real line, such that $f(x) > x$ for all x. Let x_0 be a real number, and define the sequence (x_n) recursively by $x_{n+1} := f(x_n)$. Then x_n diverges to infinity.

A standard proof might go along the following steps: 1) By assumption, the sequence is strictly increasing; 2) hence the sequence either diverges to infinity or has a finite limit; 3) by continuity, any finite limit would have to be a fixed point of f, hence the latter cannot occur.

6.3 Formal Proof Sketch: Informal Layout

now let f be continuous Function of REAL,REAL; assume for x holds $f.(x) > x$; let x_0 be Element of REAL; set x = recursively_iterate*(f,x_0); $x_{.(n+1)} = f.(x_{.n})$; thus x is divergent_to+infty*

proof x is increasing; x is divergent_to+infty or x is convergent; x is convergent implies $f.(\lim x) = \lim x$; x is not convergent; thus thesis; end; *end;*

6.4 Formal Proof Sketch: Formal Layout

```
now
  let f be continuous Function of REAL,REAL;
  assume for x holds f.(x) > x;
  let x0 be Element of REAL;
  set x = recursively_iterate(f,x0);
  x.(n + 1) = f.(x.n);                                            *4
  thus x is divergent_to+infty
  proof
    x is increasing;                                              *4
    x is divergent_to+infty or x is convergent;                   *4
    x is convergent implies f.(lim x) = lim x;                    *4
    x is not convergent;                                          *4
    thus thesis;                                                  *4
  end;
end;
```

6.5 Formal Proof

```
now
  let f be continuous Function of REAL,REAL;
  assume
A1: for x holds f.(x) > x;
  let x0 be Element of REAL;
  set x = recursively_iterate(f,x0);
A2: x.(n + 1) = f.(x.n) by Def1;
  thus x is divergent_to+infty
  proof
```

```
    now let n;
      x.(n + 1) = f.(x.n) by A2;
      hence x.(n + 1) > x.n by A1;
    end;
    then
A3:   x is increasing by SEQM_3:def 6;
    then x is bounded_above implies x is convergent;
    then
A4:   x is divergent_to+infty or x is convergent by A3,LIMFUNC1:31;
    x is convergent implies f.(lim x) = lim x
    proof
      assume
A5:     x is convergent;
A6:   dom f = REAL by PARTFUN1:def 2;
A7:   rng x c= dom f by A6,RELAT_1:def 19;
A8:   now let n;
        reconsider m = n as Element of NAT by ORDINAL1:def 12;
        x.(m + 1) = f.(x.m) by A2
          .= (f /* x).m by A7,FUNCT_2:108;
        hence x.(n + 1) = (f /* x).n;
      end;
      f is_continuous_in lim x by A6,XREAL_0:def 1,FCONT_1:def 2;
      hence f.(lim x) = lim (f /* x) by A5,A7,FCONT_1:def 1
        .= lim (x ^\ 1) by A8,NAT_1:def 3
        .= lim x by A5,SEQ_4:22;
    end;
    then x is not convergent by A1;
    hence thesis by A4;
  end;
end;
```

6.6 Mizar Version

8.1.02 – 5.22.1191

7 Linear Algebra: Linear Independence

7.1 Source

Jean Gallier, *Basics of Algebra and Analysis For Computer Science.* Published at <http://www.cis.upenn.edu/~jean/gbook.html>, University of Pennsylvania, 2001. Page 16.

7.2 Informal Proof

Lemma 2.1. *Given a linearly independent family $(u_i)_{i\in I}$ of elements of a vector space E, if $v \in E$ is not a linear combination of $(u_i)_{i\in I}$, then the family $(u_i)_{i\in I}\cup_k$*

(v) obtained by adding v to the family $(u_i)_{i\in I}$ is linearly independent (where $k \notin I$).

Proof. Assume that $\mu v + \sum_{i\in I} \lambda_i u_i = 0$, for any family $(\lambda_i)_{i\in I}$ of scalars in K. If $\mu \neq 0$, then μ has an inverse (because K is a field), and thus we have $v = -\sum_{i\in I}(\mu^{-1}\lambda_i)u_i$, showing that v is a linear combination of $(u_i)_{i\in I}$ and contradicting the hypothesis. Thus, $\mu = 0$. But then, we have $\sum_{i\in I} \lambda_i u_i = 0$, and since the family $(u_i)_{i\in I}$ is linearly independent, we have $\lambda_i = 0$ for all $i \in I$. □

7.3 Formal Proof Sketch: Informal Layout

theorem Lem21: *u is linearly-independent* & *not v in* Lin(u) *implies* u \/ $\{v\}$ *is linearly-independent*

proof assume u is linearly-independent & not v in Lin(u); assume u \/ $\{v\}$ is linearly-dependent; consider m being Element of K, l being Linear_Combination of u such that $m * v + \mathrm{Sum}(l) = 0.E$; now assume $m <> 0.K$; $v = -m" * \mathrm{Sum}(l)$; v in Lin(u); thus contradiction; end; $m = 0.K$; Sum(l) $= 0.E$; Carrier(l) $= \{\}$; thus contradiction; *end;*

7.4 Formal Proof Sketch: Formal Layout

```
theorem Lem21:
 u is linearly-independent & not v in Lin(u) implies
  u \/ {v} is linearly-independent
proof
 assume u is linearly-independent & not v in Lin(u);
 assume u \/ {v} is linearly-dependent;
 consider m being Element of K,
  l being Linear_Combination of u such that
   m*v + Sum(l) = 0.E;                                    *4
 now
  assume m <> 0.K;
  v = -m"*Sum(l);                                         *4
  v in Lin(u);                                            *4
  thus contradiction;                                     *1
 end;
 m = 0.K;                                                 *4
 Sum(l) = 0.E;                                            *4
 Carrier(l) = {};                                         *4
 thus contradiction;                                      *1
end;
```

7.5 Formal Proof

```
theorem Lem21:
 u is linearly-independent & not v in Lin(u) implies
```

```
  u \/ {v} is linearly-independent
proof
 assume
A1: u is linearly-independent & not v in Lin(u);
 given l' being Linear_Combination of u \/ {v} such that
A2: Sum(l') = 0.E & Carrier(l') <> {};
 consider m' being Linear_Combination of {v},
  l being Linear_Combination of u such that
A3: l' = m' + l by Th2;
 set m = m'.v;
A4: m*v + Sum(l) = Sum(m') + Sum(l) by VECTSP_6:43
  .= 0.E by A2,A3,VECTSP_6:77;
A5: now
  assume
A6: m <> 0.K;
  m*v = -Sum(l) by A4,RLVECT_1:def 10;
  then v = m"*(-Sum(l)) by A6,VECTSP_1:67
   .= -m"*Sum(l) by VECTSP_1:69;
  then
A7: v = (-m")*Sum(l) by VECTSP_1:68;
  Sum(l) in Lin(u) by VECTSP_7:12;
  hence contradiction by A1,A7,VECTSP_4:29;
 end;
 Sum(l) = 0.E + Sum(l) by VECTSP_1:7
  .= 0.E by A4,A5,VECTSP_1:59;
 then
A8: Carrier(l) = {} by A1,VECTSP_7:def 1;
 now
  let x be set;
A9: Carrier(m') c= {v} by VECTSP_6:def 7;
  not v in Carrier(m') by A5,VECTSP_6:20;
  hence not x in Carrier(m') by A9,TARSKI:def 1;
 end;
 then Carrier(m') = {} by BOOLE:def 1;
 then Carrier(l) \/ Carrier(m') = {} by A8;
 then Carrier(l') c= {} by A3,VECTSP_6:51;
 hence contradiction by A2,BOOLE:30;
end;
```

7.6 Mizar Version

6.1.11 – 3.33.722

8 Mathematical Logic: Newman's Lemma

8.1 Source

Henk Barendregt, *The Lambda Calculus: Its Syntax and Semantics.* North Holland, 1984. Page 58.

8.2 Informal Proof

3.1.25. PROPOSITION. *For notions of reduction one has*

$$\mathrm{SN} \wedge \mathrm{WCR} \Rightarrow \mathrm{CR}$$

PROOF. By SN each term R-reduces to an R-nf. It suffices to show that this R-nf is unique. Call M *ambiguous* if M R-reduces to two distinct R-nf's. For such M one has $M \to_R M'$ with M' ambiguous (use WCR, see figure 3.3). Hence by SN ambiguous terms do not exist.

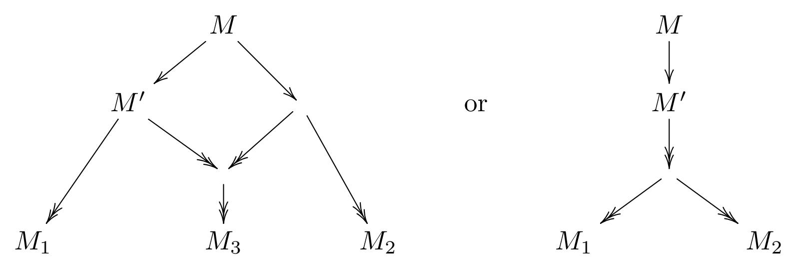

FIG. 3.3.

8.3 Formal Proof Sketch: Informal Layout

THEOREM 3_1_25:

$$R \text{ is SN } \& \ R \text{ is WCR implies } R \text{ is CR}$$

PROOF assume that R is SN and R is WCR; for M ex M_1 st M reduces_to M_1; (for M, M_1, M_2 st M reduces_to M_1 & M reduces_to M_2 holds $M_1 = M_2$) implies R is CR; defpred ambiguous[Term of R] means ex M_1, M_2 st \$1 reduces_to M_1 & \$1 reduces_to M_2 & M_1 <> M_2; now now let M such that ambiguous[M]; thus ex M' st M ---> M' & ambiguous[M']

> PROOF consider M_1, M_2 such that M -->> M_1 & M -->> M_2 & M_1 <> M_2; per cases; suppose not ex M' st M ---> M' & M' -->> M_1 & M' -->> M_2; consider M' such that M ---> M' & M' -->> M_1; consider M'' such that M ---> M'' & M'' -->> M_2; consider M''' such that M' -->> M''' & M'' -->> M'''; consider M_3 such that M''' -->> M_3; take M'; thus thesis; suppose ex M' st M ---> M' & M' -->> M_1 & M' -->> M_2; consider M' such that M ---> M' & M' -->> M_1 & M' -->> M_2; take M'; thus thesis; END;

END; thus not ex M st ambiguous[M]; END; thus thesis; END;

8.4 Formal Proof Sketch: Formal Layout

```
theorem 3_1_25:
 R is SN & R is WCR implies R is CR
proof
 assume that R is SN and R is WCR;
 for M ex M1 st M reduces_to M1;                                        *4
 (for M,M1,M2 st M reduces_to M1 & M reduces_to M2 holds M1 = M2)
  implies R is CR;                                                      *4
 defpred ambiguous[Term of R] means
  ex M1,M2 st $1 reduces_to M1 & $1 reduces_to M2 & M1 <> M2;
 now
  now
   let M such that ambiguous[M];
   thus ex M' st M ---> M' & ambiguous[M']
   proof :: begin fig 3.3
    consider M1,M2 such that M -->> M1 & M -->> M2 & M1 <> M2;          *4
    per cases;
    suppose not ex M' st M ---> M' & M' -->> M1 & M' -->> M2;
     consider M' such that M ---> M' & M' -->> M1;                      *4
     consider M'' such that M ---> M'' & M'' -->> M2;                   *4
     consider M''' such that M' -->> M''' & M'' -->> M''';              *4
     consider M3 such that M''' -->> M3;                                *4
     take M';
     thus thesis;                                                       *4,4
    suppose ex M' st M ---> M' & M' -->> M1 & M' -->> M2;
     consider M' such that M ---> M' & M' -->> M1 & M' -->> M2;         *4
     take M';
     thus thesis;                                                       *4,4
   end; :: end fig 3.3
  end;
  thus not ex M st ambiguous[M];                                        *4
 end;
 thus thesis;                                                           *4
end;
```

8.5 Formal Proof

```
theorem 3_1_25:
 R is SN & R is WCR implies R is CR
proof
 assume that
A1: R is SN and
A2: R is WCR;
A3: R is WN by A1,Th9;
 then for M ex M1 st M reduces_to M1 by Def10;
A4: (for M,M1,M2 st M reduces_to M1 & M reduces_to M2 holds M1 = M2)
  implies R is CR
 proof
  assume
```

```
A5: for M,M1,M2 st M reduces_to M1 & M reduces_to M2 holds M1 = M2;
  let M,M',M'';
  assume
A6: M -->> M' & M -->> M'';
  consider M1 such that
A7: M' -->> M1 by A3,Def10;
  consider M2 such that
A8: M'' -->> M2 by A3,Def10;
  M -->> M1 & M -->> M2 by A6,A7,A8,Th6;
  then M' -->> M1 & M'' -->> M1 by A5,A7,A8;
  hence thesis;
 end;
 defpred ambiguous[Term of R] means
  ex M1,M2 st $1 reduces_to M1 & $1 reduces_to M2 & M1 <> M2;
A9: now
A10: now
   let M such that
A11: ambiguous[M];
   thus ex M' st M ---> M' & ambiguous[M']
   proof :: begin fig 3.3
    consider M1,M2 such that
A12: M -->> M1 & M -->> M2 & M1 <> M2 by A11;
    per cases;
    suppose
A13:  not ex M' st M ---> M' & M' -->> M1 & M' -->> M2;
     M1 is_nf & M2 is_nf by Def9;
     then
A14:  M <> M1 & M <> M2 by A12,Th8;
     then consider M' such that
A15:  M ---> M' & M' -->> M1 by A12,Th7;
     consider M'' such that
A16:  M ---> M'' & M'' -->> M2 by A12,A14,Th7;
     consider M''' such that
A17:  M' -->> M''' & M'' -->> M''' by A2,A15,A16,Def11;
     consider M3 such that
A18:  M''' -->> M3 by A3,Def10;
     take M';
     M' -->> M3 & M'' -->> M3 by A17,A18,Th6;
     then M' -->> M1 & M' -->> M3 & M1 <> M3 by A13,A15,A16;
     hence thesis by A15;
    suppose ex M' st M ---> M' & M' -->> M1 & M' -->> M2;
     then consider M' such that
A19:  M ---> M' & M' -->> M1 & M' -->> M2;
     take M';
     thus thesis by A12,A19;
   end; :: end fig 3.3
  end;
  thus not ex M st ambiguous[M] from SN_induction1(A1,A10);
 end;
 thus thesis by A4,A9;
```

```
end;
```

8.6 Mizar Version

6.1.11 – 3.33.722

9 Mathematical Logic: Diaconescu's Theorem

9.1 Source

Michael Beeson, *Foundations of Constructive Mathematics.* Springer-Verlag, 1985.

9.2 Informal Proof

1.1 Theorem (Diaconescu [1975]). *The axiom of choice implies the law of excluded middle, using separation and extensionality.*

Proof. Let a formula ϕ be given; we shall derive $\phi \vee \neg\phi$. Let $A = \{n \in \mathbf{N} : n = 0 \vee (n = 1 \mathbin{\&} \phi)\}$. Let $B = \{n \in \mathbf{N} : n = 1 \vee (n = 0 \mathbin{\&} \phi)\}$. Then $\forall x \in \{A, B\}\, \exists y \in \mathbf{N}\, (y \in x)$. Suppose f is a choice function, so that $f(A) \in A$ and $f(B) \in B$. We have $f(A) = f(B) \vee f(A) \neq f(B)$, since the values are integers. If $f(A) = f(B)$ then ϕ, so $\phi \vee \neg\phi$. If $f(A) \neq f(B)$, then $\neg\phi$ can be derived: suppose ϕ. Then $A = B$ by extensionality, so $f(A) = f(B)$, contradiction. Hence in either case $\phi \vee \neg\phi$. □

9.3 Formal Proof Sketch: Informal Layout

scheme Diaconescu $\{$*phi*[]$\}$ *: axiom_of_choice implies phi*[] *or not phi*[]

proof assume axiom_of_choice; set $A = \{n : n = 0$ or $(n = 1 \mathbin{\&}$ *phi*[]$)\}$; set $B = \{n : n = 1$ or $(n = 0 \mathbin{\&}$ *phi*[]$)\}$; for x st x in $\{A, B\}$ holds ex y st y in x; consider f being choice_function such that f is extensional; $f.A$ in A & $f.B$ in B; $f.A = f.B$ or $f.A <> f.B$ by excluded_middle_on_integers; per cases; suppose $f.A = f.B$; *phi*[]; thus *phi*[] or not *phi*[]; end; suppose $f.A <> f.B$; not *phi*[] proof assume *phi*[]; $A = B$ by extensionality; $f.A = f.B$; thus contradiction; end; thus *phi*[] or not *phi*[]; end; end;

9.4 Formal Proof Sketch: Formal Layout

```
scheme Diaconescu :: 1975
 { phi[] } : axiom_of_choice implies phi[] or not phi[]
proof
 assume axiom_of_choice;
 set A = {n : n = 0 or (n = 1 & phi[])};
 set B = {n : n = 1 or (n = 0 & phi[])};
 for x st x in {A,B} holds ex y st y in x;                              *4
```

```
 consider f being choice_function such that
  f is extensional;                                                       *4
 f.A in A & f.B in B;                                                     *4,4
 f.A = f.B or f.A <> f.B by excluded_middle_on_integers;
 per cases;
 suppose f.A = f.B;
  phi[];                                                                  *4
  thus phi[] or not phi[];
 end;
 suppose f.A <> f.B;
  not phi[]
  proof
   assume phi[];
   A = B by extensionality;                                               *4
   f.A = f.B;                                                             *4
   thus contradiction;                                                    *1
  end;
  thus phi[] or not phi[];
 end;
end;
```

9.5 Formal Proof

```
scheme Diaconescu {phi[] }:
 axiom_of_choice implies phi[] or not phi[]
proof
 assume
A1: axiom_of_choice;
 set A = {n : n = 0 or (n = 1 & phi[])};
 set B = {n : n = 1 or (n = 0 & phi[])};
 deffunc F(Nat) = $1;
 defpred P[Nat] means $1 = 0 or ($1 = 1 & phi[]);
 {F(n) : P[n]} is Subset of NAT from COMPLSP1:sch 1;
 then reconsider A as Subset of NAT;
 defpred Q[Nat] means $1 = 1 or ($1 = 0 & phi[]);
 {F(n) : Q[n]} is Subset of NAT from COMPLSP1:sch 1;
 then reconsider B as Subset of NAT;
A2: for x st x in {A,B} holds ex y st y in x
 proof
  let x;
  assume x in {A,B};
  then
A3: x = A or x = B by TARSKI:def 2;
  per cases by A3;
  suppose
A4: x = A;
   take 0;
   thus thesis by A4;
  end;
  suppose
```

```
A5: x = B;
   take 1;
   thus thesis by A5;
  end;
 end;
 consider f being choice_function such that
A6: f is extensional by A1,Def3;
 A in {A,B} & B in {A,B} by TARSKI:def 2;
 then (ex y st y in A) & (ex y st y in B) by A2;
 then
A7: f.A in A & f.B in B by Def1;
A8: f.A = f.B or f.A <> f.B by excluded_middle_on_integers;
 per cases by A8;
 suppose
A9: f.A = f.B;
  set n = f.A;
A10: n in A & n in B by A7,A9;
  then
A11: ex n' st n = n' & (n' = 0 or (n' = 1 & phi[]));
  phi[]
  proof
   per cases by A11;
   suppose
A12: n = 0;
    ex n' st n = n' & (n' = 1 or (n' = 0 & phi[])) by A10;
    hence thesis by A12;
   end;
   suppose n = 1 & phi[];
    hence thesis;
   end;
  end;
  hence phi[] or not phi[];
 end;
 suppose
A13: f.A <> f.B;
  not phi[]
  proof
   assume
A14: phi[];
   now
    let y;
    hereby
     assume y in A;
     then ex n st y = n & (n = 0 or (n = 1 & phi[]));
     then y = 0 or (y = 1 & phi[]);
     then y = 1 or (y = 0 & phi[]) by A14;
     hence y in B;
    end;
    hereby
     assume y in B;
```

```
     then ex n st y = n & (n = 1 or (n = 0 & phi[]));
     then y = 1 or (y = 0 & phi[]);
     then y = 0 or (y = 1 & phi[]) by A14;
     hence y in A;
    end;
   end;
   then A = B by extensionality;
   then f.A = f.B by A6,Def2;
   hence contradiction by A13;
  end;
  hence phi[] or not phi[];
 end;
end;
```

9.6 Mizar Version

7.0.04 – 4.04.834

10 Topology: Open Intervals are Connected

10.1 Source

Paul Cairns and Jeremy Gow, *Elements of Euclidean and Metric Topology*, online undergraduate course notes from the IMP project. Project web site at `<http://www.uclic.ucl.ac.uk/imp/>`, course notes at `<http://www.uclic.ucl.ac.uk/topology/>` and the frame of this specific proof at `<http://www.uclic.ucl.ac.uk/topology/ConnectedInterval.html>`.

10.2 Informal Proof

Theorem

Open intervals are connected

GIVEN: $a, b \in \mathcal{R}$
THEN: The open interval (a, b) is connected

Proof

SKETCH:

The proof proceeds by contradiction. Suppose that (a, b) were not connected. Then there would be a pair of non-empty disjoint proper open subsets, U, V say, of (a, b) whose union would be (a, b). This implies a "gap" so we use the completeness of the real line to show that there can't be a gap. To do this, find a supremum of some interval which must be contained in U. Note that there is a small open ball about the supremum wich because U and V are open must be contained wholly within one or other of them. However, in both cases, this leads to a contradiction: if the ball is in U then the ball contains points in U exceeding the supremum; if the ball is in V then there are points in the ball also in U by definition of the supremum.

10.3 Formal Proof Sketch: Informal Layout

theorem

$(.a, b.)$ is connected

proof

assume $(.a, b.)$ is not connected; consider U, V being non empty open Subset of REAL, u, v such that U /\ V = {} & U \/ $V = (.a, b.)$ & u in U & v in V & $u < v$; reconsider $X = \{x : (.u, x.)$ c= $U\}$ as Subset of REAL; set $s = \sup X$; per cases; suppose s in U; consider e such that $e > 0$ & Ball(s, e) c= U; ex x st x in Ball(s, e) & $x > s$; thus contradiction; suppose s in V; consider e such that $e > 0$ & Ball(s, e) c= V; ex x st x in Ball(s, e) & x in U; thus contradiction;

END;

10.4 Formal Proof Sketch: Formal Layout

```
theorem (.a,b.) is connected
proof
 assume (.a,b.) is not connected;
 consider U,V being non empty open Subset of REAL, u,v such that
  U /\ V = {} & U \/ V = (.a,b.) & u in U & v in V & u < v;              *4
 reconsider X = { x : (.u,x.) c= U } as Subset of REAL;                  *4
 set s = sup X;
 per cases;                                                              *4
 suppose s in U;
  consider e such that e > 0 & Ball(s,e) c= U;                           *4
  ex x st x in Ball(s,e) & x > s;                                        *4
  thus contradiction;                                                    *1
 suppose s in V;
  consider e such that e > 0 & Ball(s,e) c= V;                           *4
  ex x st x in Ball(s,e) & x in U;                                       *4
  thus contradiction;                                                    *1
end;
```

10.5 Formal Proof

```
theorem (.a,b.) is connected
proof
 assume (.a,b.) is not connected;
 then consider U,V being non empty open Subset of REAL such that
A1: U /\ V = {} & U \/ V = (.a,b.) by Def8;
 consider u such that
A2: u in U by Def1;
 consider v such that
A3: v in V by Def1;
 ex U,V being non empty open Subset of REAL, u,v st
  U /\ V = {} & U \/ V = (.a,b.) & u in U & v in V & u < v
 proof
```

```
  per cases by AXIOMS:21;
  suppose
A4: u < v;
   take U,V,u,v;
   thus thesis by A1,A2,A3,A4;
  suppose
A5: u > v;
   take V,U,v,u;
   thus thesis by A1,A2,A3,A5;
  suppose u = v;
   hence thesis by A1,A2,A3,XBOOLE_0:def 3;
 end;
 then consider U,V being non empty open Subset of REAL, u,v such that
A6: U /\ V = {} & U \/ V = (.a,b.) & u in U & v in V & u < v;
 { x : (.u,x.) c= U } c= REAL from Fr_Set0;
 then reconsider X = { x : (.u,x.) c= U } as Subset of REAL;
 (.u,u.) = {} by RCOMP_1:12;
 then (.u,u.) c= U by XBOOLE_1:2;
 then
A7: u in X;
A8: for x st x in X holds x <= v
 proof
  let x;
  assume
A9: x in X & v < x;
A10: v in (.u,x.) by A6,A9,JORDAN6:45;
  ex x' st x = x' & (.u,x'.) c= U by A9;
  hence thesis by A6,A10,XBOOLE_0:def 3;
 end;
 for x being real number st x in X holds x <= v by A8;
 then reconsider X as non empty bounded_above Subset of REAL
  by A7,SEQ_4:def 1;
 set s = sup X;
 U c= (.a,b.) & V c= (.a,b.) by A6,XBOOLE_1:7;
 then a < u & u <= s & s <= v & v < b
  by A6,A7,A8,JORDAN6:45,SEQ_4:def 4,PSCOMP_1:10;
 then a < s & s < b by AXIOMS:22;
 then
A11: s in (.a,b.) by JORDAN6:45;
 per cases by A6,A11,XBOOLE_0:def 2;
 suppose s in U;
  then consider e such that
A12: e > 0 & Ball(s,e) c= U by Def7;
  ex x st x in Ball(s,e) & x > s
  proof
   take x = s + e/2;
   thus x in Ball(s,e) by A12,Th2;
   e/2 > 0 by A12,SEQ_2:3;
   hence thesis by REAL_1:69;
  end;
```

```
  then consider x such that
A13: x in Ball(s,e) & x > s;
  (.u,x.) c= U
  proof
   let y be set;
   assume
A14: y in (.u,x.);
   then reconsider y as Real;
A15: u < y & y < x by A14,JORDAN6:45;
   per cases;
   suppose y < s;
    then consider y' such that
A16: y' in X & y < y' & y' <= s by Def9;
    y in (.u,y'.) & ex y'' st y' = y'' & (.u,y''.) c= U
     by A15,A16,JORDAN6:45;
    hence thesis;
   suppose y >= s;
    then s in Ball(s,e) & x in Ball(s,e) & s <= y & y <= x
     by A12,A13,A14,Th1,JORDAN6:45;
    then y in Ball(s,e) by Th4;
    hence thesis by A12;
  end;
  then x in X;
  hence contradiction by A13,SEQ_4:def 4;
 suppose s in V;
  then consider e such that
A17: e > 0 & Ball(s,e) c= V by Def7;
  ex x st x in Ball(s,e) & x in U
  proof
   per cases;
   suppose
A18: u < s - e/2;
    take x = s - e/2;
    thus x in Ball(s,e) by A17,Th3;
    e/2 > 0 by A17,SEQ_2:3;
    then x < s by REAL_2:174;
    then consider x' such that
A19: x' in X & x < x' & x' <= s by Def9;
    x in (.u,x'.) & ex x'' st x' = x'' & (.u,x''.) c= U
     by A18,A19,JORDAN6:45;
    hence thesis;
   suppose
A20: s - e/2 <= u;
    take u;
    s - e/2 in Ball(s,e) & s in Ball(s,e) & s - e/2 <= u & u <= s
     by A7,A17,A20,Th1,Th3,SEQ_4:def 4;
    hence thesis by A6,Th4;
  end;
  hence contradiction by A6,A17,XBOOLE_0:def 3;
end;
```

10.6 Mizar Version

6.3.02 – 3.44.763

11 Missing Subjects

- Calculus
- Combinatorics
- Complex Variables
- Differential Equations
- Geometry
- Integration
- Probability Theory