Логика предикатов лекция 7

Лев Дмитриевич Беклемишев
http://lpcs.math.msu.su/vml2008

lbekl@yandex.ru

20.03.2008

Теории

Опр.

Теорией сигнатуры Σ называем произвольное множество T замкнутых формул языка $\mathcal{L}_\Sigma$. Элементы $A \in T$ называем *нелогическими аксиомами* T.

Пример.

Теория отношения эквивалентности:

- $\forall x\, R(x, x)$;
- $\forall x, y\, (R(x, y) \to R(y, x))$;
- $\forall x, y, z\, (R(x, y) \wedge R(y, z) \to R(x, z))$.

Теории

Опр.

Теорией сигнатуры Σ называем произвольное множество T замкнутых формул языка $\mathcal{L}_\Sigma$. Элементы $A \in T$ называем *нелогическими аксиомами* T.

Пример.

Теория отношения эквивалентности:

- $\forall x\, R(x, x)$;
- $\forall x, y\, (R(x, y) \to R(y, x))$;
- $\forall x, y, z\, (R(x, y) \wedge R(y, z) \to R(x, z))$.

Модель теории

Опр.

Модель $(M; \Sigma)$ есть *модель теории* T (обозначение $M \vDash T$), если для любой $A \in T$ $M \vDash A$.

Пример.

R есть отношение эквивалентности на множестве M, если и только если $(M; R) \vDash T$, где T — теория отношения эквивалентности.

Модель теории

Опр.

Модель $(M; \Sigma)$ есть *модель теории* T (обозначение $M \vDash T$), если для любой $A \in T$ $M \vDash A$.

Пример.

R есть отношение эквивалентности на множестве M, если и только если $(M; R) \vDash T$, где T — теория отношения эквивалентности.

Пример.

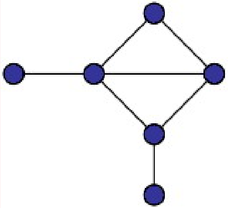
Модель $(M; <)$ есть *строгий частичный порядок*, если в $(M; <)$ истинны следующие предложения:

1. $\forall x, y, z\, (x < y \wedge y < z \rightarrow x < z)$
2. $\forall x \neg\, x < x$

Пример.

Простой граф — это модель вида $(V; E)$, где E — бинарный предикат смежности, причём отношение E симметрично и иррефлексивно:

- $\forall x \neg E(x, x)$
- $\forall x, y\, (E(x, y) \to E(y, x))$



Пример.

$(M; =, \cdot, 1)$ есть *группа*, если M есть модель следующей теории (при условии, что «$=$» в M понимается как равенство):

1. $\forall x, y, z \;\; x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $\forall x \, (1 \cdot x = x \wedge x \cdot 1 = x)$
3. $\forall x \exists y \, (x \cdot y = 1 \wedge y \cdot x = 1)$

Равенство

Пусть Σ — сигнатура, содержащая выделенный предикатный символ $=$.

Опр.

Нормальной моделью называем модель $(M; \Sigma)$, в которой $=$ интерпретируется как равенство $\{\langle x, x\rangle \mid x \in M\}$.

Опр.

Аксиомы равенства для Σ — универсальные замыкания следующих формул:

1. аксиомы отношения эквивалентности для $=$
2. $a_1 = b_1 \wedge a_2 = b_2 \wedge \dots \wedge a_n = b_n \to (P(a_1, \dots, a_n) \leftrightarrow P(b_1, \dots, b_n))$
3. $a_1 = b_1 \wedge a_2 = b_2 \wedge \dots \wedge a_n = b_n \to (f(a_1, \dots, a_n) = f(b_1, \dots, b_n))$

для всех $f \in \mathrm{Func}_\Sigma$ and $P \in \mathrm{Pred}_\Sigma$.

Предложение.

Если $(M; \Sigma)$ — нормальная модель, то в M истинны все аксиомы равенства.

Опр.

Теорией с равенством называем теорию сигнатуры Σ с равенством, содержащую все аксиомы равенства.

Предложение.

Если $(M;\Sigma)$ — нормальная модель, то в M истинны все аксиомы равенства.

Опр.

Теорией с равенством называем теорию сигнатуры Σ с равенством, содержащую все аксиомы равенства.

Теорема.

Пусть T — теория с равенством. Если T выполнима, то T имеет нормальную модель.

Доказательство.

Пусть $M \models T$. Предикат $=_M$ есть отношение эквивалентности на M. Положим $M' \rightleftharpoons M/{=_M}$ — множество классов эквивалентности и $\varphi : M \to M'$ сопоставляет любому $x \in M$ его класс $\varphi(x) \in M'$.

Теорема.

Пусть T — теория с равенством. Если T выполнима, то T имеет нормальную модель.

Доказательство.

Пусть $M \models T$. Предикат $=_M$ есть отношение эквивалентности на M. Положим $M' \rightleftharpoons M/{=_M}$ — множество классов эквивалентности и $\varphi : M \to M'$ сопоставляет любому $x \in M$ его класс $\varphi(x) \in M'$.

В силу аксиом равенства в M, все функции и предикаты корректно определены на M' и M' — нормальная модель.

Индукцией по построению формулы A проверяем

$$M \vDash A[x_1, \ldots, x_n] \iff M' \vDash A[\varphi(x_1), \ldots, \varphi(x_n)].$$

Отсюда следует $M' \vDash T$.

Упражнения

Упражнение

Выпишете аксиомы теории коммутативных колец с единицей в сигнатуре $=, +, -, \cdot, 0, 1$.

Упражнение

Выпишете аксиомы теории полей в той же сигнатуре.

Элементарная геометрия

Аксиоматика Тарского:

$G1.$ $ab \cong ba$

$G2.$ $ab \cong pq \land ab \cong rs \to pq \cong rs$

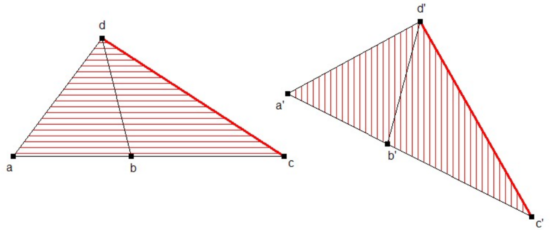
$G3.$ $ab \cong cc \to a = b$

$G4.$ $Babd \land Bbcd \to Babc$

$G5.$ $\exists x(Bqax \land ax \cong bc)$

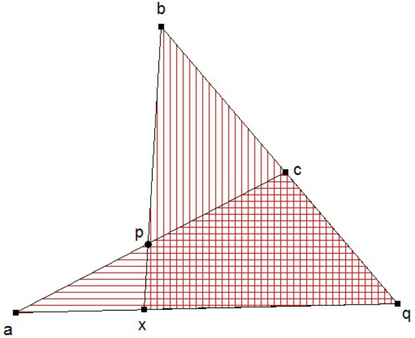
$G6.$ (пять отрезков)

$$(a \neq b \wedge Babc \wedge Ba'b'c' \wedge ab \cong a'b' \wedge bc \cong b'c' \wedge ad \cong a'd' \wedge bd \cong b'd') \rightarrow cd \cong c'd'$$



$G7.$ (аксиома Паша)

$$Bapc \wedge Bqcb \rightarrow \exists x \, (Baxq \wedge Bbpx)$$

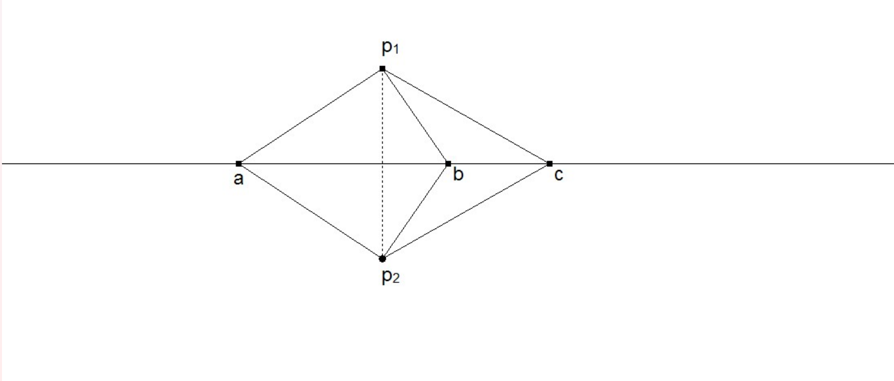


Аксиомы размерности

$G8.\ \exists x, y, z\, (\neg Bxyz \wedge \neg Byzx \wedge \neg Bzxy)$

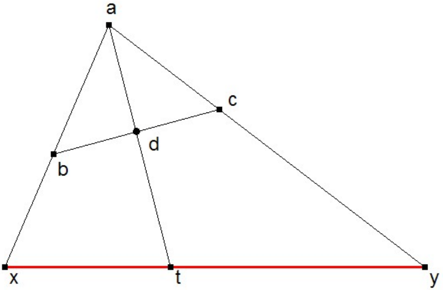
$G9.\ (dim \leq 2)$

$$(p_1 \neq p_2 \wedge ap_1 \cong ap_2 \wedge bp_1 \cong bp_2 \wedge cp_1 \cong cp_2) \longrightarrow a \in bc$$



$G10.$ (аксиома Евклида)

$$Badt \wedge Bbdc \wedge a \neq d \rightarrow$$
$$\exists x, y\, (Babx \wedge Bacy \wedge Bytx)$$



G11. (схема аксиом непрерывности)

$$\exists u \forall x, y\, (C[a/x] \wedge D[a/y] \to Buxy) \to \exists v \forall x, y\, (C[a/x] \wedge D[a/y] \to Bxvy)$$

Здесь x, y, u, v не входят в C, D.

G11′. (аксиома непрерывности 2-го порядка)

$$\forall X, Y\, (\exists u \forall x, y\, (x \in X \wedge y \in Y \to Buxy) \to \exists v \forall x, y\, (x \in X \wedge y \in Y \to Bxvy))$$

Теорема Тарского о полноте

Теорема.

Для любого предложения A языка элементарной геометрии, если $(\mathbb{R}^2; =, B, \cong) \vDash A$, то A логически следует из аксиом $G1 - G11$.

Теорема.

Существует алгоритм проверки формулы A на выполнимость в $\mathbb{R}^2$.

Исчисление предикатов

Исчисление предикатов сигнатуры Σ задаётся след. аксиомами и правилами вывода.

Аксиомы:

$A1.$ аксиомы исчисления высказываний,

$A2.$ $\forall x A[a/x] \to A[a/t]$,

$A3.$ $A[a/t] \to \exists x A[a/x]$.

Здесь A — любая формула сигнатуры Σ и t — любой терм (x не входит в A).

Правила вывода:

$$R1.\ \frac{A \quad A \to B}{B} \ (\textit{modus ponens})$$

$$R2.\ \frac{A \to B}{A \to \forall x B[a/x]}$$

$$R3.\ \frac{B \to A}{\exists x B[a/x] \to A}$$

Здесь a не входит в A (и x не входит в B).

Правила R2 и R3 называются *правилами Бернайса*.

Выводимость

Опр.

Выводом в исчислении предикатов называется конечная последовательность формул, каждая из которых либо является аксиомой, либо получается из предыдущих формул по одному из правил вывода $R1 - R3$.

Пример.

$$\forall x A[a/x] \to A \qquad (A2)$$
$$\forall x A[a/x] \to \forall y A[a/y] \qquad (R2)$$

Выводимость

Опр.

Выводом в исчислении предикатов называется конечная последовательность формул, каждая из которых либо является аксиомой, либо получается из предыдущих формул по одному из правил вывода $R1 - R3$.

Пример.

$$\begin{array}{ll} \forall x A[a/x] \to A & (A2) \\ \forall x A[a/x] \to \forall y A[a/y] & (R2) \end{array}$$

Опр.

Формула A называется *выводимой* в исчислении предикатов или *теоремой* исчисления предикатов (обозначение $\vdash A$), если существует вывод, в котором последняя формула есть A.

Пример.

$\vdash \forall x A[a/x] \to \forall y A[a/y]$ для любой формулы A.

Выводы в теории

Опр.

Выводом в теории T называется конечная последовательность формул, каждая из которых либо принадлежит множеству T, либо является логической аксиомой вида $A1 - A3$, либо получается из предыдущих формул по одному из правил вывода $R1 - R3$.

Доказуемость, опровержимость

Опр.

Формула A называется *выводимой (доказуемой) в теории T* или *теоремой T* (обозначение $T \vdash A$), если существует вывод в T, в котором последняя формула есть A.

Опр.

Формула A *опровержима* в T, если $T \vdash \neg A$.

Опр.

Формула A *независима* от T, если $T \nvdash A$ и $T \nvdash \neg A$.

Доказуемость, опровержимость

Опр.

Формула A называется *выводимой (доказуемой) в теории T* или *теоремой T* (обозначение $T \vdash A$), если существует вывод в T, в котором последняя формула есть A.

Опр.

Формула A *опровержима* в T, если $T \vdash \neg A$.

Опр.

Формула A *независима* от T, если $T \nvdash A$ и $T \nvdash \neg A$.

Доказуемость, опровержимость

Опр.

Формула A называется *выводимой (доказуемой) в теории* T или *теоремой* T (обозначение $T \vdash A$), если существует вывод в T, в котором последняя формула есть A.

Опр.

Формула A *опровержима* в T, если $T \vdash \neg A$.

Опр.

Формула A *независима* от T, если $T \nvdash A$ и $T \nvdash \neg A$.

Свойства выводимости

- Если $T \subseteq U$ и $T \vdash A$, то $U \vdash A$ (*монотонность*).
- Если $T \vdash A$, то существует такое конечное множество $T_0 \subseteq T$, что $T_0 \vdash A$ (*компактность*).
- Если $T \vdash A$ и для каждой аксиомы $B \in T$ имеет место $U \vdash B$, то $U \vdash A$ (*транзитивность*).

Свойства выводимости

- Если $T \subseteq U$ и $T \vdash A$, то $U \vdash A$ (*монотонность*).
- Если $T \vdash A$, то существует такое конечное множество $T_0 \subseteq T$, что $T_0 \vdash A$ (*компактность*).
- Если $T \vdash A$ и для каждой аксиомы $B \in T$ имеет место $U \vdash B$, то $U \vdash A$ (*транзитивность*).

Свойства выводимости

- Если $T \subseteq U$ и $T \vdash A$, то $U \vdash A$ (*монотонность*).
- Если $T \vdash A$, то существует такое конечное множество $T_0 \subseteq T$, что $T_0 \vdash A$ (*компактность*).
- Если $T \vdash A$ и для каждой аксиомы $B \in T$ имеет место $U \vdash B$, то $U \vdash A$ (*транзитивность*).

Эквивалентность теорий

Пусть T, U — теории сигнатуры Σ.

Опр.

U содержит T, если для любой $A \in T$ $U \vdash A$ (обозначение $U \vdash T$).

Опр.

T и U (дедуктивно) эквивалентны, если $T \vdash U$ и $U \vdash T$ (обозначение $T \equiv U$).

Эквивалентность теорий

Пусть T, U — теории сигнатуры Σ.

Опр.

U содержит T, если для любой $A \in T$ $U \vdash A$ (обозначение $U \vdash T$).

Опр.

T и U *(дедуктивно) эквивалентны*, если $T \vdash U$ и $U \vdash T$ (обозначение $T \equiv U$).

Теорема о тавтологии

Предложение.

Если $A(P_1, \ldots, P_n)$ выводима в исчислении высказываний, то для любых формул $C_1, \ldots, C_n$ сигнатуры Σ формула $A[P_1/C_1, \ldots, P_n/C_n]$ выводима в исчислении предикатов.

Доказательство.

Индукция по построению вывода формулы A.

Теорема о дедукции

Теорема.

Для любой теории T и замкнутой формулы A

$$T, A \vdash B \iff T \vdash A \to B.$$

Доказательство.

Индукция по длине вывода $T, A \vdash B$. Разбираем лишь новые случаи, относящиеся к правилам $R2$ и $R3$.

Теорема о дедукции

Теорема.

Для любой теории T и замкнутой формулы A

$$T, A \vdash B \iff T \vdash A \to B.$$

Доказательство.

Индукция по длине вывода $T, A \vdash B$. Разбираем лишь новые случаи, относящиеся к правилам $R2$ и $R3$.

Допустим $B = (C \to \forall x D[a/x])$ получена из $C \to D$ по $R2$. По пр. индукции

$$T \vdash A \to (C \to D).$$

Надо построить вывод

$$T \vdash A \to (C \to \forall x D[a/x]).$$

Рассмотрим тавтологию

$$(P \to (Q \to R)) \leftrightarrow (P \wedge Q \to R).$$

Подставляя A вместо P, C вместо Q и D вместо R получаем, что формула

$$(A \to (C \to D)) \leftrightarrow (A \wedge C \to D)$$

выводима в исчислении предикатов.

Таким образом, вывод $A \to (C \to D)$ в T можно продолжить:

$A \to (C \to D)$

$(A \to (C \to D)) \to (A \wedge C \to D)$ (тавтология)

$(A \wedge C) \to D$ (MP)

$(A \wedge C) \to \forall x D[a/x]$ (R2, A замкнута)

$A \to (C \to \forall x D[a/x])$ (аналогично)

Правило $R3$ рассматривается аналогично.

Опр.

Теория T *противоречива*, если существует A такая, что $T \vdash A$ и $T \vdash \neg A$. В противном случае теория T называется *непротиворечивой*.

Следствие.

$T \cup \{A\}$ противоречива $\iff T \vdash \neg A$.

Опр.

Теория T *противоречива*, если существует A такая, что $T \vdash A$ и $T \vdash \neg A$. В противном случае теория T называется *непротиворечивой*.

Следствие.

$T \cup \{A\}$ противоречива $\iff T \vdash \neg A$.

Теорема о корректности исчисления предикатов

Теорема.

Если $M \vDash T$ *и* $T \vdash A$, *то* $M \vDash A$.

Доказательство.

Индукция по длине вывода A в T.

Следствие.

Если $\vdash A$, то A общезначима.

Теорема о корректности исчисления предикатов

Теорема.

Если $M \models T$ и $T \vdash A$, то $M \models A$.

Доказательство.

Индукция по длине вывода A в T.

Следствие.

Если $\vdash A$, то A общезначима.

Доказательства непротиворечивости

Следствие.
Если теория T имеет модель, то T непротиворечива.

Следствие.
Следующие теории непротиворечивы:

- исчисление предикатов (пустая теория);
- теория отношения эквивалентности;
- теория групп;
- элементарная геометрия.

Доказательства независимости

Следствие.
Если существует модель M теории T для которой $M \not\models A$, то $T \nvdash A$.

Пример.
Модель Пуанкаре $\mathbf{H}^2$ показывает, что аксиома Евклида независима от остальных аксиом элементарной геометрии.

Теорема Гёделя о полноте

Теорема.

1. *Всякая непротиворечивая теория* T *выполнима, то есть имеет модель* $M \models T$.
2. *Если* $T \nvdash A$, *то найдётся модель* $M \models T$ *для которой* $M \not\models A$.
3. $T \models A$ *влечёт* $T \vdash A$.

Покажем равносильность этих утверждений.

$(1 \Rightarrow 2)$: Если $T \nvdash A$, то по теореме о дедукции $T \cup \{\neg A\}$ непротиворечива. Следовательно, $T \cup \{\neg A\}$ имеет модель M.

$(2 \Rightarrow 3)$: очевидно.

$(3 \Rightarrow 1)$: Возьмём $A = (B \wedge \neg B)$. Тогда $T \nvdash A$, следовательно $T \not\models A$ и у теории T должна быть модель (опровергающая A).

Покажем равносильность этих утверждений.

$(1 \Rightarrow 2)$: Если $T \nvdash A$, то по теореме о дедукции $T \cup \{\neg A\}$ непротиворечива. Следовательно, $T \cup \{\neg A\}$ имеет модель M.

$(2 \Rightarrow 3)$: очевидно.

$(3 \Rightarrow 1)$: Возьмём $A = (B \wedge \neg B)$. Тогда $T \nvdash A$, следовательно $T \nvDash A$ и у теории T должна быть модель (опровергающая A).

Покажем равносильность этих утверждений.

$(1 \Rightarrow 2)$: Если $T \nvdash A$, то по теореме о дедукции $T \cup \{\neg A\}$ непротиворечива. Следовательно, $T \cup \{\neg A\}$ имеет модель M.

$(2 \Rightarrow 3)$: очевидно.

$(3 \Rightarrow 1)$: Возьмём $A = (B \wedge \neg B)$. Тогда $T \nvdash A$, следовательно $T \not\models A$ и у теории T должна быть модель (опровергающая A).

Покажем равносильность этих утверждений.

$(1 \Rightarrow 2)$: Если $T \nvdash A$, то по теореме о дедукции $T \cup \{\neg A\}$ непротиворечива. Следовательно, $T \cup \{\neg A\}$ имеет модель M.

$(2 \Rightarrow 3)$: очевидно.

$(3 \Rightarrow 1)$: Возьмём $A = (B \wedge \neg B)$. Тогда $T \nvdash A$, следовательно $T \nvDash A$ и у теории T должна быть модель (опровергающая A).

Теорема Мальцева о компактности

Теорема.

1. *Теория* T *выполнима* $\iff$ *любое конечное подмножество* $T_0 \subseteq T$ *выполнимо.*
2. $T \vDash A$ $\iff$ *существует такое конечное множество* $T_0 \subseteq T$*, что* $T_0 \vDash A$.

Нестандартные модели арифметики

Пример.

Пусть $(\mathbb{N}; =, S, +, \cdot, 0)$ — стандартная модель арифметики и $Th(\mathbb{N})$ есть множество *всех* истинных в $\mathbb{N}$ предложений.

Добавим к сигнатуре новую константу c и рассмотрим теорию

$$T \rightleftharpoons Th(\mathbb{N}) \cup \{\neg c = 0, \neg c = S0, \neg c = SS0, \dots\}.$$

Терм $\bar{n} \rightleftharpoons SS\ldots S0$ (n раз) называем *нумералом*. Нумералы служат именами натуральных чисел.

Утверждение.

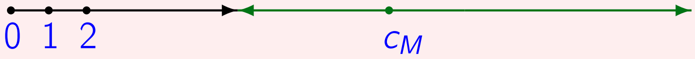
Каждая конечная подтеория $T_0 \subseteq T$ выполнима.

Доказательство.

T_0 содержит лишь кончное число аксиом вида $c \neq \bar{n}_1$, ..., $c \neq \bar{n}_k$. Интерпретируем константу c в стандартной модели как любое число $m > n_1, \ldots, n_k$.

По теореме о компактности существует (нормальная) модель $M \vDash T$. Модель M обладает следующими свойствами:

- $\mathbb{N}$ изоморфна начальному сегменту M; вложение $\mathbb{N} \to M$ задаётся функцией $\varphi : n \longmapsto \overline{n}_M$.
- $M \vDash Th(\mathbb{N})$;
- $M \not\cong \mathbb{N}$, в частности $c_M \in M$ есть «бесконечно большое число», поскольку c_M отлично от всякого $n \in \mathbb{N}$.

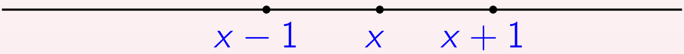


Порядок на модели $\mathbb{M}$

Формула $a < b \rightleftharpoons \exists x\,(x \neq 0 \wedge a + x = b)$ определяет порядок в $\mathbb{N}$. Для данной формулы в $\mathbb{N}$ выполнены аксиомы строгого линейного порядка и следующие предложения:

- $\forall x\,(0 < x \vee 0 = x)$;
- $\forall x \exists y\,(x < y \wedge \forall z\,(z < y \to z = x \vee z < x))$;
- $\forall y\,(y \neq 0 \to \exists x\,(x < y \wedge \forall z\,(z < y \to$
  $\to z = x \vee z < x)))$.

Следовательно, те же аксиомы выполнены и в M. Поэтому предикат $<_M$ на M представляет собой строгий линейный порядок с наименьшим элементом 0. При этом каждый элемент имеет последователя, и каждый элемент, кроме 0, имеет непосредственного предшественника.



Опр.

Элементы $x, y \in M$ *близки*, если для некоторого $n \in \mathbb{N}$ выполнено $y = SS \dots S(x)$ или $x = SS \dots S(y)$ (n символов S).

Классы эквивалентности по отношению близости называем *галактиками*.

Утверждение.

Если G — галактика в M, $G \neq \mathbb{N}$, то порядок $(G, <_M)$ изоморфен $(\mathbb{Z}, <)$.

Пусть $\mathcal{G}$ есть множество всех галактик в M, отличных от $\mathbb{N}$. Определим $G_1 <_M G_2$, если для любых $x \in G_1$, $y \in G_2$ $x <_M y$.

Теорема.

Порядок $(\mathcal{G}, <_M)$ *есть плотный порядок без наибольшего и наименьшего элементов.*

Доказательство.

Если $G_1 < G_2$, возьмём чётные $x_1 \in G_1$ и $x_2 \in G_2$ и рассмотрим $y = (x_1 + x_2)/2$ (функция $g(x) = x/2$ определима в $\mathbb{N}$, а значит и в M).

Если $y \in G_1$, то $(x_1 + x_2)/2 = x + \bar{n}$ для некоторого $n \in \mathbb{N}$. Тогда $2x_1 + 2\bar{n} = x_1 + x_2$, откуда $x_1 + 2\bar{n} = x_2$, то есть $x_2 \in G_1$.

Аналогично показываем $y \notin G_2$.