9 Формулы логики первого порядка

Дашков: Предлагаю *определить* атомарные формулы и термы без участия скобок и запятых, но *разрешить* их синонимическое употребление, где удобно: $\neg Rxyz$, $f(a, c+b, g(x))$.

Дашков: Я полагался (не сильно, впрочем) на то, что обозначения и определение значения формулы при оценке и т. п. такие как в ВШ.

10 Теория моделей I

В разд. 9 мы определи понятия *языка первого порядка* некоторой *сигнатуры*, а также *интерпретации* этой сигнатуры. Нам будет удобно переформулировать данные определения, немного сместив акценты. В самом деле, с точки зрения «обычной» математики, первичным понятием является именно «интерпретация» (кольцо целых чисел, некоторое упорядоченное множество, некоторый граф, некоторая группа или иная *структура*).

Структурой называется кортеж множеств $(M, \mathcal{F}, \mathcal{R}, \mathcal{C})$, где *носитель* M структуры непустой, для всякого $f \in \mathcal{F}$ найдется $n \in \mathbb{N}_+$, т. ч. $f\colon M^n \to M$; для всякого $R \in \mathcal{R}$ найдется $n \in \mathbb{N}_+$, т. ч. $R \subseteq M^n$; и $\mathcal{C} \subseteq M$. Пусть $(M, \mathcal{F}, \mathcal{R}, \mathcal{C})$ есть некоторая структура.

Пусть σ есть сигнатура со множеством функциональных символов Fnc, множеством предикатных символов Prd и множеством константных символов (или, *констант*) Cnst. Мы предполагаем, что названные множества попарно не пересекаются, $\mathrm{Prd} \neq \varnothing$, и все символы, кроме констант, имеют положительную валентность. Пусть отображение $\mathcal{I}\colon \mathrm{Fnc} \cup \mathrm{Prd} \cup \mathrm{Cnst} \to \mathcal{F} \cup \mathcal{R} \cup \mathcal{C}$ таково, что $\mathcal{I}(\mathrm{Fnc}) = \mathcal{F}$, $\mathcal{I}(\mathrm{Prd}) = \mathcal{R}$ и $\mathcal{I}(\mathrm{Cnst}) = \mathcal{C}$, причем если символ $f \in \mathrm{Fnc}$ имеет валентность n, то $\mathcal{I}(f)\colon M^n \to M$, и если символ $R \in \mathrm{Prd}$ имеет валентность n, то $\mathcal{I}(R) \subseteq M^n$. Тогда кортеж множеств $\mathcal{M} = (M, \mathcal{F}, \mathcal{R}, \mathcal{C}, \mathcal{I})$ называется *интерпретацией сигнатуры* σ, или *σ-структурой*. В таком случае, мы пишем $f^{\mathcal{M}}$ вместо $\mathcal{I}(f)$, $R^{\mathcal{M}}$ вместо $\mathcal{I}(R)$ и $c^{\mathcal{M}}$ вместо $\mathcal{I}(c)$. Значения функции $\mathcal{I}$ назовем *интерпретациями*, соответственно, функциональных, предикатных и константных символов сигнатуры σ. Заметим, что для задания σ-структуры достаточно указать лишь M и $\mathcal{I}$.

Скажем, что σ-структура $\mathcal{M}$ *нормальная*, если σ содержит двувалентный предикатный символ $=$ и $\mathcal{I}(=) = \{(a, a) \in M^2 \mid a \in M\}$.

Мы часто будем задавать σ-структуру просто перечисляя образующие ее множества: $(M; f^{\mathcal{M}}, \ldots; R^{\mathcal{M}}, \ldots; c^{\mathcal{M}}, \ldots)$. При этом интерпретации символов сигнатуры, или даже и сама сигнатура, если не указаны явно, должны быть ясны из контекста.

Задавая сигнатуры явно, тоже будем использовать списки (в т. ч. пустые): например, запись $(; R^{(3)}, Q^{(2)}; c, 1)$ означает сигнатуру без функциональных, но с двумя предикатными символами R и Q валентностей 3 и 2 соответственно, а также с двумя различными константами c и 1.

Когда это не вызывает неясностей, мы позволяем себе не указывать валентости, смешивать обозначение символа сигнатуры с обозначением соответствующего ему множества, обозначение структуры с обозначением ее носителя и т. п.

Пусть $\mathcal{M}$ и $\mathcal{N}$ суть две интерпретации сигнатуры σ с носителями M и N соответственно. Инъекция $\eta\colon M \to N$ называется (изоморфным) *(σ-)вложением*, если: **(1)** $\eta(f^{\mathcal{M}}(a_1, \ldots, a_n)) = f^{\mathcal{N}}(\eta(a_1), \ldots, \eta(a_n))$ для всех $f \in \mathrm{Fnc}$ и всех $a_1, \ldots, a_n \in M$, где n валентность символа f; **(2)** $(a_1, \ldots, a_n) \in R^{\mathcal{M}} \iff (\eta(a_1), \ldots, \eta(a_n)) \in R^{\mathcal{N}}$ для всех $R \in \mathrm{Prd}$ и всех $a_1, \ldots, a_n \in M$, где n валентность символа R; **(3)** $\eta(c^{\mathcal{M}}) = c^{\mathcal{N}}$ для всех $c \in \mathrm{Cnst}$.

Биективное σ-вложение $\mathcal{M} \to \mathcal{N}$ называется *(σ-)изоморфизмом*. Если последний существует, интерпретации $\mathcal{M}$ и $\mathcal{N}$ *(σ)-изоморфны* (пишем $\mathcal{M} \cong \mathcal{N}$). σ-Изоморфизм $\mathcal{M} \to \mathcal{M}$ называется *(σ-)автоморфизмом*. Множество σ-автоморфизмов σ-структуры $\mathcal{M}$ обозначим $\mathrm{Aut}(\mathcal{M})$. Если $M \subseteq N$ и инъекция $\eta\colon M \to N$, т. ч. $\eta(a) = a$ для всех $a \in M$, является вложением, то $\mathcal{M}$ есть *подстурктура* $\mathcal{N}$, а $\mathcal{N}$ есть *расширение* $\mathcal{M}$.

10.1. Пусть $\sigma = (\circ^{(2)}; =^{(2)}; 0)$. Покажите, что

а) σ-структура $(\mathbb{N}; +; =; 0)$ есть подструктура σ-структуры $(\mathbb{Z}; +; =; 0)$;

б) $(\mathbb{N}; +; =; 0)$ вкладывается в $(\mathbb{N}; \cdot; =; 1)$;

в) $(\mathbb{N}\setminus\{0\};\cdot\,;=)$ не вкладывается в $(\mathbb{N};+;=)$.

Если терм t (или формула φ) сигнатуры σ не имеет (свободных) вхождений иных переменных, кроме $u_1,\ldots,u_n$, мы пишем $t(u_1,\ldots,u_n)$ (соответственно, $\varphi(u_1,\ldots,u_n)$). Для формулы $\varphi(u_1,\ldots,u_n)$ и термов $t_1,\ldots,t_n$, мы будем писать $\varphi(t_1,\ldots,t_n)$, где имеется в виду одновременная подстановка, вместо $\varphi(t_1/u_1,\ldots,t_n/u_n)$, если это не вызывает двусмысленностей. Замкнутая, т. е. не имеющая свободных вхождений переменных, формула еще называется *предложением.* Формулы (предложения, термы) сигнатуры σ также называем *σ-формулами* (*σ-предложениями, σ-термами*).

Пусть $\mathcal{M}$ есть σ-структура. Каждому терму $t(u_1,\ldots,u_n)$ вместе с упорядоченным набором попарно различных переменных $(u_1,\ldots,u_n)$ поставим в соответствие функцию $t^{\mathcal{M}}\colon M^n\to M$ следующим образом: $t^{\mathcal{M}}(\vec{a})=[t](\pi+(u_1\mapsto a_1)+\ldots+(u_n\mapsto a_n))$ для любого набора (кортежа) $\vec{a}\in M^n$. Как известно из результатов разд. 9, значение $[t]$ терма t не зависит от переменных, кроме $u_1,\ldots,u_n$, так что оценка π может быть выбрана любой.

Для простоты будем считать, что в формулах употребляются лишь связки $\neg,\wedge$ и квантор $\exists$. Оставшиеся связки и кванторы рассматриваем как сокращения.

Формула $\varphi(u_1,\ldots,u_n)$ с упорядоченным набором попарно различных переменных $(u_1,\ldots,u_n)$ *истинна в интерпретации $\mathcal{M}$ на наборе параметров $\vec{a}\in M^n$*, если $[\varphi](\pi+(u_1\mapsto a_1)+\ldots+(u_n\mapsto a_n))=1$ в интерпретации $\mathcal{M}$. (Как и ранее, оценка π может быть выбрана любой.) Мы пишем $\mathcal{M}\models\varphi(\vec{a})$ в этом случае.

Произвольное множество σ-предложений называется *теорией в языке сигнатуры* σ. Говорят, что σ-структура $\mathcal{M}$ является *моделью* теории T, если $\mathcal{M}\models\varphi$ для всех $\varphi\in T$. Тогда пишут $\mathcal{M}\models T$. *Модель предложения* φ это модель теории $\{\varphi\}$. Теория называется *совместной* (или, *выполнимой*), если она имеет модель. *Теорией σ-структуры* $\mathcal{M}$ называется множество $\mathrm{Th}(\mathcal{M})$ σ-предложений, истинных в $\mathcal{M}$. σ-Структуры $\mathcal{M}$ и $\mathcal{N}$ *элементарно эквивалентны*, если $\mathrm{Th}(\mathcal{M})=\mathrm{Th}(\mathcal{N})$. В этом случае пишем $\mathcal{M}\equiv\mathcal{N}$.

Если рассматриваемые объекты относятся к одной сигнатуре, точный вид которой не важен, мы опускаем упоминания о ней. Если длина наборов переменных и параметров согласована, но в точности не важна, она не указывается: в частности, мы пишем $\vec{a}\in X$ вместо $\vec{a}\in X^n$ и $\xi(\vec{a})$ вместо $(\xi(a_1),\ldots,\xi(a_n))$, где $\vec{a}=(a_1,\ldots,a_n)$ и $\xi\colon X\to Y$.

10.2. Пусть $\mathcal{M}$ есть подструктура $\mathcal{N}$. Покажите, что для любого $\vec{a}\in M$, любого терма t и любой бескванторной формулы φ верно: **а)** $t^{\mathcal{M}}(\vec{a})=t^{\mathcal{N}}(\vec{a})$; **б)** $\mathcal{M}\models\varphi(\vec{a})\iff\mathcal{N}\models\varphi(\vec{a})$.

Формула вида $\forall\vec{x}\,\psi$ называется *универсальной*, если формула ψ бескванорная (т. е. несколько кванторов всеобщности предшествуют бескванторной формуле). Аналогично, формула вида $\exists\vec{x}\,\psi$ называется *экзистенциальной.*

10.3. Пусть $\mathcal{M}$ есть подструктура структуры $\mathcal{N}$. Покажите, что для любой формулы $\varphi(\vec{u})$ и любого $\vec{a}\in M$: **а)** если φ экзистенциальная, $\mathcal{M}\models\varphi(\vec{a})\implies\mathcal{N}\models\varphi(\vec{a})$; **б)** если φ универсальная, $\mathcal{N}\models\varphi(\vec{a})\implies\mathcal{M}\models\varphi(\vec{a})$.

10.4. Покажите, что для любых σ-структур $\mathcal{M}$, $\mathcal{N}$ и $\mathcal{N}'$: **а)** $\mathcal{M}\cong\mathcal{M}$; **б)** если $\mathcal{M}\cong\mathcal{N}$, то $\mathcal{N}\cong\mathcal{M}$; **в)** если $\mathcal{M}\cong\mathcal{N}$ и $\mathcal{N}\cong\mathcal{N}'$, то $\mathcal{M}\cong\mathcal{N}$.

10.5. Пусть $\eta\colon\mathcal{M}\to\mathcal{N}$ есть изоморфизм. Покажите, что: **а)** для любой формулы $\varphi(\vec{u})$ и любого $\vec{a}\in M$ равносильны $\mathcal{M}\models\varphi(\vec{a})$ и $\mathcal{N}\models\varphi(\eta(\vec{a}))$; **б)** $\mathcal{M}\equiv\mathcal{N}$.

10.6. Покажите, что: **а)** $(\mathbb{R};+;=)\cong(\mathbb{R}_+;\cdot\,;=)$; **б)** линейные порядки $\mathbb{R}\mathbb{Q}$ и $\mathbb{Q}\mathbb{R}$ не изоморфны; **в)** линейные порядки $\mathbb{R}$ и $\mathbb{R}+\mathbb{R}$ не изоморфны; **г)** аддитивная группа (т. е. интерпретация сигнатуры $(+^{(2)},-^{(1)};=;0)$) рациональных чисел $\mathcal{Q}^+$ и группа $\mathcal{Q}^+\oplus\mathcal{Q}^+$ не изоморфны.[1]

10.1 Мощности

Мощностью[2] $|\mathcal{M}|$ структуры $\mathcal{M}$ считается мощность ее носителя M. *Мощностью* $|\sigma|$ сигнатуры σ считается мощность множества $\mathrm{Fnc}_\sigma\cup\mathrm{Prd}_\sigma\cup\mathrm{Cnst}_\sigma$.

10.7. Покажите, что любое множество попарно элементарно неэквивалентных σ-структур имеет мощность не более $2^{\max(|\sigma|,\aleph_0)}$.

[1] *Внешняя прямая сумма* $G\oplus H$ аддитивных коммутативных групп G и H есть множество $G\times H$ с операцией $+$, т. ч. $(g,h)+(g',h')=(g+_G g',h+_H h')$.

[2] Читатель, не знакомый с формальным определением мощности (скажем, как ординала, не равномощного никакому меньшему), может рассуждать в терминах равномощных множеств. Символ $\aleph_0$ обозначает мощность счетного множества.

10.8. Покажите, что если сигнатура σ бесконечна, то найдется множество попарно элементарно неэквивалентных σ-структур, имеющее мощность $2^{|\sigma|}$.

10.9. Покажите, что если сигнатура σ содержит двувалентный предикатный символ, то найдется множество попарно элементарно неэквивалентных σ-структур, имеющее мощность $2^{\aleph_0}$.

10.10. Пусть мощность κ бесконечная. Покажите, что любое множество попарно неизоморфных σ-структур мощности κ имеет мощность не более $2^{\max(|\sigma|,\kappa)}$.

10.11. Покажите, что для любой интерпретации $\mathcal{M}$ и любой мощности $\kappa > |\mathcal{M}|$ найдется интерпретация $\mathcal{N}$, т. ч. $\mathcal{M} \equiv \mathcal{N}$ и $|\mathcal{N}| = \kappa$.

10.12. **а)** Для каждого $n \in \mathbb{N}$ укажите сигнатуру σ, не содержащую ничего, кроме одновалентных предикатных символов, и выполнимое σ-предложение φ, любая модель которого имеет мощность не меньше n. **б)** Найдите наименьшее возможное число предикатных символов в такой сигнатуре. **в)** Докажите, что для любой сигнатуры из одного двувалентного предикатного символа и для любого $n \in \mathbb{N}$ найдется выполнимое предложение φ, любая модель которого имеет мощность не меньше n.

10.13. Разрешимость монадической логики. Пусть сигнатура σ не содержит ничего, кроме одновалентных предикатных символов. **а)** Докажите, что алгоритмически разрешима *проблема выполнимости*: по σ-предложению φ выяснить, есть ли у φ модель. **б)** Можно ли проверить σ-предложение φ на общезначимость?

Назовем *(конечным) спектром* предложения φ сигнатуры с равенством σ множество

$$\mathrm{Sp}(\varphi) = \{n \in \mathbb{N}_+ \mid \text{существует нормальная } \sigma\text{-структура } \mathcal{M}, \text{ т. ч. } \mathcal{M} \models \varphi \text{ и } |\mathcal{M}| = n\}.$$

10.14. Укажите предложение φ, т. ч. $\mathrm{Sp}(\varphi) = X$, если: **а)** $X = \varnothing$; **б)** X одноточечное; **в)** X конечное или коконечное подмножество $\mathbb{N}_+$.

10.15. Укажите предложение φ, т. ч. $\mathrm{Sp}(\varphi) = X$, если: **а)** $X = \{n \in \mathbb{N}_+ \mid n \equiv r \pmod m\}$ для некоторых $m > 1$ и r; **б)** X есть множество всех составных чисел; **в)** $X = \{n^2 \mid n \in \mathbb{N}_+\}$; **г)** $X = \{2^n \mid n \in \mathbb{N}\}$.

10.16. Пусть σ-структуры $\mathcal{M}$ и $\mathcal{N}$ нормальные, $\mathcal{M} \equiv \mathcal{N}$ и $\mathcal{M}$ конечна. Покажите, что тогда $\mathcal{M} \cong \mathcal{N}$.

10.2 Выразимость и автоморфизмы

Предикат[5] $X \subseteq M^n$ *выразим* (или, *определим*) в интерпретации $\mathcal{M}$ сигнатуры σ, если существует σ-формула $\varphi(u_1, \dots, u_n)$, т. ч. для всех $\vec{a} \in M^n$

$$\vec{a} \in X \iff \mathcal{M} \models \varphi(\vec{a}).$$

Полезно более общее понятие. Пусть $A \subseteq M^m$. Предикат $X \subseteq M^n$ *A-выразим* (или, *выразим над A*) в $\mathcal{M}$, если существует σ-формула $\varphi(u_1, \dots, u_n, w_1, \dots, w_m)$ и набор параметров $\vec{b} \in A^m$, т. ч. для всех $\vec{a} \in M^n$

$$\vec{a} \in X \iff \mathcal{M} \models \varphi(\vec{a}, \vec{b}).$$

Аналогично, функция $g\colon M^n \to M^m$ *(A-)выразима* в $\mathcal{M}$, если в $\mathcal{M}$ (A-)выразим ее график $\Gamma_g = \{(\vec{a}, \vec{a}') \in M^{n+m} \mid g(\vec{a}) = \vec{a}'\}$. Элемент $a \in M$ *(A-)выразим*, если (A-)выразим предикат $\{a\}$.

10.17. Пусть структура $\mathcal{M} = (M; <, =)$ есть строгий частичный порядок. Покажите, что выразимы предикаты: **а)** множество наименьших элементов; **б)** множество минимальных элементов; **в)** $\{(a_1, \dots, a_n) \in M^n \mid \{a_i\}_{i=1}^n$ есть n-элементная цепь$\}$; **г)** $\{(a_1, a_2) \in M^2 \mid a_2$ непосредственно следует за $a_1\}$.

10.18. Решетка подмножеств. В структуре $(\mathcal{P}(U); \subseteq)$, где $\mathcal{P}(U)$ множество всех подмножеств некоторого множества U, выразите предикаты и функции: **а)** $\{\varnothing\}$; **б)** $\{U\}$;

[5] Как обычно, мы отождествляем предикат как «свойство» набора «индивидов» из M с подмножеством наборов, этим свойством обладающих.

в) $\{(a,a) \mid a \in \mathcal{P}(U)\}$; **г)** $(a_1,a_2) \mapsto a_1 \cap a_2$; **д)** $(a_1,a_2) \mapsto a_1 \cup a_2$; **е)** $a \mapsto U \setminus a$; **ж)** $\{a \in \mathcal{P}(U) \mid |a| = 1\}$; **з)** $\{a \in \mathcal{P}(U) \mid |a| = n+1\}$. **и)** Покажите, что если множество $d \in \mathcal{P}(U)$ конечно или коконечно, то предикат $\{d\}$ выразим над множеством одноэлементных подмножеств множества U.

10.19. Делимость. В структуре $(\mathbb{N}; |)$, где $m \mid n$ означает, что число m является делителем числа n, выразите предикаты: **а)** числа a_1 и a_2 совпадают; **б)** $\{0\}$ и $\{1\}$; **в)** множество простых чисел; **г)** a_2 является степенью простого числа a_1; **д)** a_1 и a_2 взаимно просты; **е)** a_3 есть наибольший, в смысле естественного порядка, общий делитель чисел a_1 и a_2; **ж)** a_3 есть наименьшее, в смысле естественного порядка, положительное общее кратное чисел a_1 и a_2; **з)** a_3 является наибольшей степенью простого числа a_1, делящей a_2; **и)** множество чисел, свободных от квадратов; **к)** a_2 является n-ой степенью простого числа a_1 (для всевозможных $n \in \mathbb{N}$).

10.20 (*Дж. Робинсон*[6]). Выразите сложение натуральных чисел в структуре $(\mathbb{N}; S, \cdot\,; =)$, где S означает функцию $n \mapsto n+1$, а $\cdot$ означает умножение.

Теорема 10.1 (Дирихле об арифметической прогрессии[7]). *Если числа $a, d \in \mathbb{N}_+$ взаимно просты, то для любого $N \in \mathbb{N}$ найдется $k > N$, т. ч. число $a + kd$ простое.*

10.21 (*Дж. Робинсон*[8]). В структуре $(\mathbb{N}; S; |)$ выразите предикаты и функции: **а)** $a_1 \equiv 1 \pmod{a_2}$; **б)** положительные числа a_1 и a_2 взаимно просты и $a_3 = a_1a_2$; **в)** умножение натуральных чисел; **г)** сложение натуральных чисел.

10.22. Элементарная геометрия плоскости. Рассмотрим структуру $\mathcal{G} = (\mathbb{R}^2; \equiv, B)$, интерпретирующую сигнатуру из двух предикатных символов $\equiv^{(4)}$ и $B^{(3)}$, т. ч. $ab \equiv cd$ значит, что отрезки ab и cd имеют равную длину, а $Babc$ значит, что точка b лежит на отрезке ac. Покажите, что выразимы следующие предикаты: **а)** точки a_1 и a_2 совпадают; **б)** точки a_1, a_2 и a_3 лежат на одной прямой; **в)** отрезок a_1a_2 короче отрезка a_3a_4; **г)** отрезки a_1a_2 и a_3a_4 суть основания невырожденной трапеции; **д)** точка a_4 принадлежит медиане невырожденного треугольника $a_1a_2a_3$, опущенной из a_1; **е)** точка a_4 принадлежит невырожденному треугольнику $a_1a_2a_3$ или его внутренности; **ж)** точка a_1 есть вершина прямого угла, на сторонах которого лежат отличные от нее точки a_2 и a_3; **з)** точки a_1, a_2, a_3 лежат на одной невырожденной окружности; **и)** точка a_4 принадлежит биссектрисе невырожденного треугольника $a_1a_2a_3$, опущенной из a_1. **к)** Покажите, что предикаты из пунктов б), ж) и в), а также предикат $B^{\mathcal{G}}$ выражаются формулами без символа B. **л)** Покажите, что предикаты из пунктов а) и д) выражаются формулами без символа $\equiv$.

10.23. Покажите, что в поле вещественных чисел $\mathcal{R} = (\mathbb{R}; +, -, \cdot\,; =; 0, 1)$: **а)** выразимо отношение естественного порядка; **б)** A-выразимо множество $d(X)$ предельных точек всякого A-выразимого множества X;[9] **в)** выразимо каждое рациональное число; **г)** выразимо каждое алгебраическое число. **д)** Пусть каждый элемент множества X выразим. Всегда ли $d(X)$ выразимо?

Теорема 10.2 (Лагранжа о четырех квадратах[10]). *Для всякого $n \in \mathbb{N}$ найдутся $a, b, c, d \in \mathbb{N}$, т. ч. $n = a^2 + b^2 + c^2 + d^2$.*

Теорема 10.3 (Дж. Робинсон[11]). *В поле рациональных чисел $\mathcal{Q}$ выразимо множество $\mathbb{Z}$.*

10.24. Покажите, что в поле $\mathcal{Q}$ выразим естественный порядок на множестве $\mathbb{Q}$.

Пусть R есть некоторое поле, либо кольцо $\mathbb{Z}$. Многочлен $p \in R[X]$ называется *неприводимым над* R если для любых $q, r \in R[X]$ из $p = qr$ следует, что один из многочленов q или r

[6] Robinson J. Definability and decision problems in arithmetic. *The Journal of Symbolic Logic*, 14(2):98–114, 1949.

[7] См. Гельфанд А. О., Линник Ю. В. Элементарные методы в аналитической теории чисел. М.: Физматгиз, 1962. С. 61.

[8] Robinson J. Op. cit.

[9] По определению, $d(X)$ есть множество точек $\mathbb{R}$, в чьей всякой проколотой окрестности есть точка из X; в частности, если X есть множество значений сходящейся последовательности, $d(X)$ состоит из предела этой последовательности.

[10] См. Тихомиров В. М. Великие математики прошлого и их великие теоремы. *Сер.: «Библиотека “Математическое просвещение”». Вып. 1,* 2-е изд., М.: МЦНМО, 2003. С. 11.

[11] Robinson J. Op. cit.

обратим (т. е. делит 1) в $R[X]$, но сам p необратим. Например, многочлен $2X + 4$ неприводим над $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$, но не над $\mathbb{Z}$. Многочлен $p \in \mathbb{Z}[X]$ называется *примитивным*, если наибольший общий делитель его коэффициентов равен 1.

10.25 (*Р. Робинсон*[12]). Пусть K есть поле нулевой характеристики (т. е. никакая конечная сумма его единиц не равна нулю). Покажите, что тогда в кольце $K[X]$ выразимы множества: **а)** K; **б)** множество неприводимых многочленов; **в)** множество многочленов степени n для каждого $n \in \mathbb{N}$; **г)** $\mathbb{N}^K = \{0^K, 1^K, 1^K + 1^K, 1^K + 1^K + 1^K, \ldots\}$.

Теорема 10.4 (лемма Гаусса[13]). *Если многочлен $p \in \mathbb{Z}[X]$ неприводим над $\mathbb{Z}$ и $\deg p > 0$, то p неприводим над $\mathbb{Q}$.*

10.26. В кольце $\mathbb{Z}[X]$ выразите: **а)** множество неприводимых многочленов; **б)** множество $\mathbb{N}$; **в)** множество многочленов степени n для каждого $n \in \mathbb{N}$.

10.27. Квантор укорачивает формулу. Для каждого $n \in \mathbb{N}_+$ в произвольной нормальной интерпретации $\mathcal{M}$ сигнатуры σ выразите предикат X_n формулой φ_n, т. ч. $|\varphi_n| = O(F(n))$,[14] если: **а)** $\sigma = (f^{(1)}; =^{(2)};)$, $X_n = \{(a, f_n^{\mathcal{M}}(a) \mid a \in M\}$, где $f_1^{\mathcal{M}}(d) = f^{\mathcal{M}}(d)$ и $f_{m+1}^{\mathcal{M}}(d) = f^{\mathcal{M}}(f_m^{\mathcal{M}}(d))$, $F(n) = \log_2 n$; **б)** $\sigma = (; =^{(2)};)$, $X_n = \{(a_1, \ldots, a_n) \mid$ все a_i попарно различны$\}$ и $F(n) = n$.

Пусть сигнатура σ содержится в сигнатуре σ'. Если σ'-структура $\mathcal{M}'$ и σ-структура $\mathcal{M}$ таковы, что $M' = M$ и $\mathcal{I}' |_{\mathrm{Fnc}_\sigma \cup \mathrm{Prd}_\sigma \cup \mathrm{Cnst}_\sigma} = \mathcal{I}$, то $\mathcal{M}'$ называется *(σ'-)обогащением* $\mathcal{M}$, а $\mathcal{M}$, соответственно, *(σ-)обеднением* $\mathcal{M}'$. Например, аддитивная группа целых чисел есть $(+, -; =; 0)$-обеднение кольца целых чисел.

10.28. Обогащение определениями (дефинициальное расширение). Пусть σ'-структура $\mathcal{M}'$ является обогащением σ-структуры $\mathcal{M}$, причем для некоторого $A \subseteq M$ и всех добавленных символов f, R, c в $\mathcal{M}$ над множеством A выразимы $f^{\mathcal{M}'}, R^{\mathcal{M}'}, c^{\mathcal{M}'}$. Покажите, что если $B \supseteq A$, то множества B-выразимых предикатов, функций и элементов в структурах $\mathcal{M}$ и $\mathcal{M}'$ соответственно совпадают. (В частности, если $A = \varnothing$, множества выразимых предикатов (функций, элементов) совпадают.)

Более того, существует алгоритм, подходящий для всех σ' и $\mathcal{M}'$, который по σ'-формуле φ' и параметрам для предиката X, а также σ-формулам и параметрам для всех новых символов, входящих в φ', вычисляет σ-формулу φ и параметры для X.

Этот результат показывает, что в решениях ряда предшествующих задач к сигнатуре можно добавить и использовать символы для уже выраженных предикатов, функций и элементов.

10.29. Устранение функций и констант. Пусть сигнатура σ содержит равенство, σ' состоит из попарно различных символов $R_f^{(n+1)}$ для каждого $f^{(n)} \in \mathrm{Fnc}_\sigma$, $R_c^{(1)}$ для каждого $c \in \mathrm{Cnst}_\sigma$ и всех символов из Prd_σ, а сигнатура σ'' является «объединением» сигнатур σ и σ'. Для произвольной нормальной σ-структуры $\mathcal{M}$ рассмотрим ее σ''-обогащение $\mathcal{M}''$, т. ч. $R_f^{\mathcal{M}''} = \Gamma_{f^{\mathcal{M}}}$ и $R_c^{\mathcal{M}''} = \{c^{\mathcal{M}}\}$, а затем σ'-обеднение $\mathcal{M}'$ структуры $\mathcal{M}''$. Покажите, что для всякого A множества предикатов (функций, элементов), A-выразимых в структурах $\mathcal{M}$, $\mathcal{M}''$ и $\mathcal{M}'$, совпадают.

10.30. Пусть в структуре $\mathcal{M}$ функции $h\colon M^n \to M^m$ и $g\colon M^k \to M^n$, а также множество $X \subseteq M^n$ выразимы над A. Покажите, что: **а)** A-выразима функция $h \circ g$; **б)** A-выразимо множество $h(X)$; **в)** если h инъекция, A-выразима функция h^{-1}.

10.31. Покажите, что следующие структуры не являются элементарно эквивалентными: **а)** линейно упорядоченные множества $\mathbb{N}$ и $\mathbb{N} + \mathbb{N}$; **б)** аддитивные группы $\mathcal{Z}^+$ и $\mathcal{Z}^+ \oplus \mathcal{Z}^+$; **в)** аддитивные группы $\mathcal{Z}^n$ и $\mathcal{Z}^m$ при $n > m$ (полагаем $\mathcal{Z}^1 = \mathcal{Z}^+$ и $\mathcal{Z}^{n+1} = \mathcal{Z}^n \oplus \mathcal{Z}^+$ для всех $n \in \mathbb{N}_+$); **г)** частично упорядоченные множества $(\mathbb{N}; |)$ и $(\mathcal{P}(U), \subseteq)$ для какого бы то ни было U.

[12] См. Jensen Ch., Lenzing H. Model Theoretic Algebra with particular emphasis on Fields, Rings, Modules. *Algebra, Logic and Applications Series. Vol. 2,* Gordon and Breach Science Publishers, 1989. P. 36.

[13] См. Кострикин А. И. Введение в алгебру. Часть I. Основы алгебры. 2-е изд., М.: Физматлит, 2001. С. 199.

[14] *Длина* $|\varphi|$ формулы φ есть число всех символов в ней. $G(n) = O(F(n))$ значит, что найдутся $N, C \in \mathbb{N}$, т. ч. $G(n) \leqslant CF(n)$ для всех $n \geqslant N$.

10.32. Автоморфизм сохраняет выразимые предикаты. Пусть $\eta \in \mathrm{Aut}(\mathcal{M})$, причем для некоторого $A \subseteq M$ и всех $b \in A$ верно $\eta(b) = b$. Тогда для любых A-выразимых в $\mathcal{M}$ предиката X, функции g и элемента d верно $\vec{a} \in X \iff \eta(\vec{a}) \in X$, $\eta(g(\vec{a})) = g(\eta(\vec{a}))$ и $\eta(d) = d$ при всех $\vec{a} \in M$.

10.33. Выразимое замыкание. В нормальной σ-структуре $\mathcal{M}$ *выразимым замыканием* $\mathrm{dcl}(A)$ множества $A \subseteq M$ назовем множество выразимых над A элементов M. Покажите, что: **а)** $A \subseteq \mathrm{dcl}(A)$; **б)** если $A \subseteq B$, то $\mathrm{dcl}(A) \subseteq \mathrm{dcl}(B)$; **в)** $\mathrm{dcl}(A) = \mathrm{dcl}(\mathrm{dcl}(A))$; **г)** если $a \in \mathrm{dcl}(A)$, то существует конечное $A' \subseteq A$, т. ч. $a \in \mathrm{dcl}(A')$; **д)** $a \in \mathrm{dcl}(A)$ равносильно существованию выразимой функции $g\colon M^n \to M$ и набора $\vec{b} \in A^n$, т. ч. $g(\vec{b}) = a$.

10.34. Алгебраическое замыкание. В нормальной σ-структуре $\mathcal{M}$ *алгебраическим замыканием* $\mathrm{acl}(A)$ множества $A \subseteq M$ назовем объединение всевозможных выразимых над A конечных подмножеств M. Покажите, что **а)** $\mathrm{dcl}(A) \subseteq \mathrm{acl}(A)$; **б)** $A \subseteq \mathrm{acl}(A)$; **в)** если $A \subseteq B$, то $\mathrm{acl}(A) \subseteq \mathrm{acl}(B)$; **г)** $\mathrm{acl}(A) = \mathrm{acl}(\mathrm{acl}(A))$; **д)** если $a \in \mathrm{acl}(A)$, то существует конечное $A' \subseteq A$, т. ч. $a \in \mathrm{acl}(A')$; **е)** если $a \in \mathrm{acl}(A)$, то найдется конечное множество $Z \subseteq M$, т. ч. для любого $\eta \in \mathrm{Aut}(\mathcal{M})$, при котором $\eta(b) = b$ для всех $b \in A$, выполнено $\eta(a) \in Z$.

10.35. Укажите конечную сигнатуру σ и ее интерпретацию $\mathcal{M}$, т. ч. **а)** каждый элемент M выразим; **б)** ровно $n > 1$ элементов M невыразимы. Существуют ли такие σ и $\mathcal{M}$ при $n = 1$?

10.36. Покажите, что в структуре $\mathcal{G}$ не выразимы предикаты: **а)** X, если $\varnothing \subsetneq X \subsetneq \mathbb{R}$; **б)** $|ab| = 1$; **в)** вершины треугольника abc идут по часовой стрелке. **г)** Покажите, что в $(;B;)$-обеднении структуры $\mathcal{G}$ не выразим предикат $\equiv^{\mathcal{G}}$.

10.37. Исследуйте структуры:

а) для аддитивной группы $\mathcal{Z}^+$ целых чисел вычислите $\mathrm{Aut}(\mathcal{Z}^+)$ и покажите, что естественный порядок целых чисел не выразим;

б) для аддитивной группы $\mathcal{Q}^+$ рациональных чисел вычислите $\mathrm{Aut}(\mathcal{Q}^+)$ и покажите, что функция возведения в куб не выразима;

в) для аддитивной группы $\mathcal{Q}^+_<$ рациональных чисел с естественным порядком вычислите $\mathrm{Aut}(\mathcal{Q}^+_<)$ и $\mathrm{dcl}(\varnothing)$;

г) для упорядочения $(\mathbb{N}, |)$ вычислите $\mathrm{Aut}(\mathbb{N}, |)$, $\mathrm{dcl}(\varnothing)$ и $\mathrm{acl}(\varnothing)$, а также покажите, что естественный порядок и сложение натуральных чисел не выразимы;

д) для мультипликативной группы $\mathcal{Q}^\times_*$ ненулевых рациональных чисел вычислите $\mathrm{dcl}(\varnothing)$ и покажите, что $|\mathrm{Aut}(\mathcal{Q}^\times_*)| = 2^{\aleph_0}$, а множества $\mathbb{Z} \setminus \{0\}$, $\mathbb{Q}_+$ и естественный порядок на $\mathbb{Q} \setminus \{0\}$ не выразимы;

е) для группы $\mathbb{Z}_n$ чисел $\{0, 1, \ldots, n-1\}$ со сложением по модулю $n \geqslant 2$ вычислите $\mathrm{Aut}(\mathbb{Z}_n)$ и $\mathrm{dcl}(\varnothing)$;

ж) для поля $\mathcal{R}$ вычислите $\mathrm{Aut}(\mathcal{R})$ и докажите, что $\mathrm{acl}(A) = \mathrm{dcl}(A)$ при любом $A \subseteq \mathbb{R}$.

10.38. Для произвольного множества U и структуры $\mathcal{M} = (\mathcal{P}(U), \subseteq)$ вычислите: **а)** $\mathrm{Aut}(\mathcal{M})$; **б)** $\mathrm{dcl}(\varnothing)$; **в)** $\mathrm{acl}(\varnothing)$. **г)** Покажите, что если выразимое семейство $S \subseteq \mathcal{P}(U)$ содержит непустое множество, то $\bigcup S = U$.

10.39. Для кольца $\mathbb{Z}[X]$ вычислите: **а)** $\mathrm{Aut}(\mathbb{Z}[X])$; **б)** $\mathrm{acl}(\varnothing)$ и $\mathrm{dcl}(\varnothing)$. **в)** Покажите, что множество многочленов с единичным старшим коэффициентом не выразимо.

Множество $L \subseteq \mathbb{R}$ назовем *линейно независимым* (над полем $\mathcal{Q}$), если для любых конечных наборов $h_1, \ldots, h_k \in L$ и $q_1, \ldots, q_k \in \mathbb{Q}$ из $\sum_{i=1}^k q_i h_i = 0$ следует $q_1 = \ldots = q_k = 0$.

Теорема 10.5 (о базисе Гамеля[16]). *Для всякого линейно независимого множества $L \subseteq \mathbb{R}$ существует линейно независимое множество $H \subseteq \mathbb{R}$, называемое* базисом Гамеля *(линейного пространства $\mathbb{R}$ над полем $\mathcal{Q}$), такое что $L \subseteq H$ и для всякого $\alpha \in \mathbb{R}$ найдутся конечные наборы $h_1, \ldots, h_k \in H$ и $q_1, \ldots, q_k \in \mathbb{Q}$ со свойством $\sum_{i=1}^k q_i h_i = \alpha$.*

[16] Верещагин Н. К., Шень А. Лекции по математической логике и теории алгоритмов. Начала теории множеств. 4-е изд., М.: МЦНМО, 2012. С. 69.

10.40. Рассмотрим аддитивную группу $\mathcal{R}^+$ и ее обогащение $\mathcal{R}_1^+$ константой 1. **а)** Найдите все подмножества $\mathbb{R}$, выразимые в $\mathcal{R}^+$. **б)** Вычислите $\mathrm{dcl}(\varnothing)$ для $\mathcal{R}_1^+$. **в)** Докажите, что $\mathcal{R}^+ \cong \mathcal{R}^+ \oplus \mathcal{R}^+$.

10.41. Нормальную интерпретацию G сигнатуры $(;E^{(2)},=^{(2)};)$ назовем *графом*, если отношение E^G симметрично и антирефлексивно. Найдите предложение φ данной сигнатуры, т. ч. для любого графа G имеет место $G \models \varphi$ тогда и только тогда, когда в $(;E;)$-обеднении структуры G выразим предикат $=^G$.

10.42. Покажите, что в структуре $(\mathbb{N};S;=)$ элемент 0 не выражается никакой бескванторной формулой.

10.43. Покажите, что: **а)** в группе $\mathcal{Z}^+$ множество четных чисел не выражается никакой универсальной формулой; **б)** для кольца $\mathcal{Z}$ такая формула существует.

10.3 Интерпретируемость структур

10.44. Пусть K и L суть поля нулевой характеристики, причем $K[X] \equiv L[X]$. Покажите, что $K \equiv L$.

10.4 Стандартная интерпретация арифметики

Стандартной интерпретацией сигнатуры языка арифметики $(S^{(1)},+^{(2)},\cdot^{(2)};=^{(2)};0)$ считают нормальную структуру $(\mathbb{N};S,+,\cdot;=;0)$, где фигурируют обычные сложение и умножение натуральных чисел, функция «последователь» $S\colon n \mapsto n+1$ и число $0 \in \mathbb{N}$. Саму эту структуру (не вполне аккуратно) обозначают $\mathbb{N}$.

10.45. Покажите, что для любого $A \subseteq \mathbb{N}$, если предикат $X \subseteq \mathbb{N}^n$ является A-выразимым в $\mathbb{N}$, то X выразим.

10.46. Покажите, что в поле $\mathcal{R}$ выразимо основание натурального логарифма e, если обогатить эту структуру: **а)** предикатом $\mathbb{N}$; **б)** предикатом $\mathbb{Q}$. **в)** Докажите то же для числа π.

10.5 Игры Фрайссе–Эренфойхта

10.6 Элиминация кванторов

11 Исчисление предикатов

Фиксируем сигнатуру Σ. Исчисление предикатов ИП допускает следующие аксиомы:

(A1) – (A11) из исчисления предикатов;

(A12) $\forall\xi\varphi \to \varphi(t/\xi)$;

(A13) $\varphi(t/\xi) \to \varphi$.

В аксиомах (A12) и (A13) t означает произвольный терм в сигнатуре Σ, ξ — произвольную предметную переменную, и дополнительно требуется, чтобы подстановка $\varphi(t/\xi)$ была *корректна*, то есть никакая свободна переменная терма t не входит свободно в φ и не попадает под действие квантора по ней.

Исчисление ИП имеет *правило вывода* Modus Ponens и два *правила Бернайса*:

$$\frac{\varphi, \varphi \to \psi}{\psi}\ \text{(MP)}, \qquad \frac{\varphi \to \psi}{\varphi \to \forall\xi\psi}\ (\text{B}_\forall), \qquad \frac{\psi \to \varphi}{\exists\xi\psi \to \varphi}\ (\text{B}_\exists).$$

В правилах Бернайса дополнительно требуется, чтобы ξ не было параметром φ. Вывод из посылок в ИП определяется так же, как и в ИВ. *Лемма о дедукции* для исчисления предикатов утверждает, что для любой замкнутой формулы φ, множества замкнутых формул Γ и произвольной формулы ψ, $\Gamma \vdash_{PC} \varphi \to \psi$ равносильно $\Gamma \cup \{\varphi\} \vdash_{PC} \psi$.