1 Булевы операции

1.1. Для любых X, Y и Z имеют место следующие равенства:

1а. $(X \cup Y) \cup Z = X \cup (Y \cup Z)$;

1б. $(X \cap Y) \cap Z = X \cap (Y \cap Z)$;

2а. $X \cup Y = Y \cup X$;

2б. $X \cap Y = Y \cap X$;

3а. $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$;

3б. $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$;

4а. $X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$;

4б. $X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$;

5. $X \setminus (X \setminus Y) = X \cap Y$.

2 Эквивалентности и частичные порядки

Определим *упорядоченную пару* X_1 и X_2 как

$$(X_1, X_2) \;:=\; \{\{X_1\}, \{X_1, X_2\}\}.$$

Нетрудно понять, что такие пары обладают следующим свойством:

$$(X_1, X_2) \;=\; (Y_1, Y_2) \quad \text{тогда и только тогда, когда} \quad X_1 = Y_1 \;\text{ и }\; X_2 = Y_2. \tag{$\star$}$$

Далее, для любых X и Y выражение

$$\begin{aligned} X \times Y \;&:= \{(x, y) \mid x \in X \wedge y \in Y\} \\ &= \{u \mid \exists x\, \exists y\, (u = (x, y) \wedge x \in X \wedge y \in Y)\} \\ &= \{u \in \mathcal{P}(\mathcal{P}(X \cup Y)) \mid \exists x\, \exists y\, (u = (x, y) \wedge x \in X \wedge y \in Y)\} \end{aligned}$$

задаёт множество, которое называют *прямым* (или *декартовым*) *произведением* X и Y. Под *бинарными* (или *двухместными*) *отношениями на* X понимают произвольные подмножества $X \times X$. Бинарное отношение R на X называют:

- *рефлексивным*, если $\forall x\, (x \in X \to xRx)$;
- *иррефлексивным*, если $\neg \exists x\, (x \in X \wedge xRx)$;
- *транзитивным*, если $\forall x\, \forall y\, \forall z\, ((xRy \wedge yRz) \to xRz)$;
- *симметричным*, если $\forall x\, \forall y\, (xRy \to yRx)$;
- *антисимметричным*, если $\forall x\, \forall y\, ((xRy \wedge yRx) \to x = y)$.

(Здесь для удобства мы пишем xRy вместо $(x, y) \in R$.) Говорят, что R является:

- *предпорядком* на X, если R рефлексивно и транзитивно;
- *строгим частичным порядком* на X, если R иррефлексивно и транзитивно;
- *частичным порядком* на X, если R рефлексивно, антисимметрично и транзитивно;
- *эквивалентностью* на X, если R рефлексивно, симметрично и транзитивно.

Данные базовые понятия играют весьма важную роль в математике.

Пусть $\approx$ — эквивалентность на X. Для каждого $x \in X$ под *классом эквивалентности* x *по* $\approx$ понимается множество

$$[x]_{\approx} \;:=\; \{u \in X \mid x \approx u\}.$$

Фактор-множество X *по* $\approx$ определяется как

$$X_{/\approx} \;:=\; \{[x]_{\approx} \mid x \in X\},$$

т.е. как множество всех классов эквивалентности элементов X по $\approx$.

Для отношений эквивалентности имеется простая характеризация. Чтобы её сформулировать, давайте введём пару вспомогательных понятий. Будем называть Y (*взаимно*, или *попарно*) *дизъюнктным*, если оно удовлетворяет условию

$$\forall u \, \forall v \, ((u \in Y \wedge v \in Y \wedge u \neq v) \to u \cap v = \varnothing).$$

Будем говорить, что Y является *разбиением* X, если Y дизъюнктно, $\varnothing \notin Y$ и $\bigcup Y = X$. Очевидно, элементы всякого разбиения X обязаны быть подмножествами X.

2.1. i. Если Y — разбиение X, то

$$\mathscr{E}_Y \;:=\; \big\{(u,v) \in X^2 \mid \exists y \, (y \in Y \wedge u \in y \wedge v \in y)\big\}$$

— эквивалентность на X, причём $X_{/\mathscr{E}_Y}$ равно Y.

ii. Если $\approx$ — эквивалентность на X, то $X_{/\approx}$ — разбиение X, причём $\mathscr{E}_{X_{/\approx}}$ равно $\approx$.

Предпорядки можно превращать в частичные порядки посредством факторизации по подходящей эквивалентности:

2.2. Пусть R — предпорядок на X. Тогда

$$\mathscr{S}_R \;:=\; \big\{(u,v) \in X^2 \mid uRv \wedge vRu\big\}$$

— эквивалентность на X. Кроме того,

$$R^{\sharp} \;:=\; \Big\{\Big([u]_{\mathscr{S}_R}, [v]_{\mathscr{S}_R}\Big) \mid u \in X \wedge v \in X \wedge uRv\Big\},$$

— частичный порядок на $X_{/\mathscr{S}_R}$.

Связь же между обычными и строгими частичными порядками вполне тривиальна:

2.3. i. Если R — строгий частичный порядок на X, то $R \cup \mathrm{id}_X$ — частичный порядок на X;

ii. Если R — частичный порядок на X, то $R \setminus \mathrm{id}_X$ — строгий частичный порядок на X.

3 Отношения и функции

3.1. Пусть R — множество упорядоченных пар, т.е.

$$\forall z\,(z \in R \to \exists x\,\exists y\, z = (x, y)).$$

Тогда найдутся X и Y такие, что $R \subseteq X \times Y$.

3.2. Пусть P, Q и R — бинарные отношения на X. Тогда:

a. $P \circ (Q \circ R) = (P \circ Q) \circ R$;

b. $(P \circ Q)^{-1} = Q^{-1} \circ P^{-1}$;

c. $\mathrm{id}_X \circ P = P \circ \mathrm{id}_X = P$.

3.3. Отношение R между X и Y функционально тогда и только тогда, когда $R^{-1} \circ R \subseteq \mathrm{id}_Y$.

3.4. Если $f : X \to Y$ и $g : Y \to Z$, то $f \circ g : X \to Z$, причём $(f \circ g)(x) = g(f(x))$ для всех $x \in X$.

3.5. Пусть $f : X \to Y$. Говорят, что *на f можно сокращать справа*, если для любых $g_1 : Z_1 \to X$ и $g_2 : Z_2 \to X$,

$$g_1 \circ f \;=\; g_2 \circ f \quad \text{влечёт} \quad g_1 \;=\; g_2.$$

По аналогии, *на f можно сокращать слева*, если для любых $g_1 : Y \to Z_1$ и $g_2 : Y \to Z_2$,

$$f \circ g_1 \;=\; f \circ g_2 \quad \text{влечёт} \quad g_1 \;=\; g_2.$$

Имеют место следующие эквивалентности:

i. f инъективна тогда и только тогда, когда на f можно сокращать справа;

ii. f сюръективна тогда и только тогда, когда на f можно сокращать слева.

(Проверьте это.)

3.6. Пусть $f : X \to Y$. Под *правой обратной к f* понимают любую $g : Y \to X$ такую, что

$$f \circ g \;=\; \mathrm{id}_X.$$

По аналогии, под *левой обратной к f* понимают любую $g : Y \to X$ такую, что

$$g \circ f \;=\; \mathrm{id}_Y.$$

Имеют место следующие эквивалентности:

i. f инъективна тогда и только тогда, когда существует правая обратная к f;

ii. f сюръективна тогда и только тогда, когда существует левая обратная к f.

(Проверьте это.) Кроме того, если правая и левая обратные к f обе существуют, то они должны совпадать.

3.7. В литературе аксиома выбора иногда формулируется так:

$$\forall X\,\exists f\,(f : \mathcal{P}(X) \setminus \{\varnothing\} \to X \wedge \forall u\,(u \subseteq X \wedge u \neq \varnothing \to f(u) \in u)). \qquad (\mathsf{C}')$$

Предполагая наличие всех остальных аксиом, покажите, что C и C' выводятся друг из друга.

4 Натуральные числа и индукция

4.1. Для любого $n \in \mathbb{N}$ верно $n \subseteq n + 1 \wedge \neg\exists x\, n \subsetneq x \subsetneq n + 1$.

4.2. Для любых $m, n \in \mathbb{N}$,

$$m < n \quad \text{тогда и только тогда, когда} \quad m \subsetneq n.$$

4.3. Для всех $n, m \in \mathbb{N}$ верно следующее:

i. $n \neq 0 \leftrightarrow \exists k \in \mathbb{N}\, n = k + 1$;

ii. $n + 1 = m + 1 \leftrightarrow n = m$.

4.4 (принцип Дирихле). i. Для любого $n \in \mathbb{N}$ не существует инъекции из $n + 1$ в n.

ii. Для любых $n, m \in \mathbb{N}$, если $m < n$, то не существует инъекции из n в m.

iii. Для любых $n, m \in \mathbb{N}$, если $n \neq m$, то не существует биекции между n и m.

Говорят, что X *содержит n элементов*, где $n \in \mathbb{N}$, и пишут $|X| = n$, если существует биекция между n и X. Далее, X называют *конечным*, если $|X| = n$ для некоторого $n \in \mathbb{N}$, и *бесконечным*, если оно не конечно.

Свойство «быть конечным» можно определять по-разному. Для произвольного Y обозначим

$$\mathrm{Max}\,(Y) \ := \ \{u \in Y \mid \neg\exists v\,(v \in Y \wedge u \subsetneq v)\}.$$

Элементы $\mathrm{Max}\,(Y)$ называют *$\subsetneq$-максимальными* в Y. Говорят, что X *конечно по Тарскому*, или Т-*конечно*, если оно удовлетворяет условию

$$\forall Y\,((Y \subseteq \mathcal{P}\,(X) \wedge Y \neq \varnothing) \to \mathrm{Max}\,(Y) \neq \varnothing),$$

и *бесконечно по Тарскому*, или Т-*бесконечно*, если оно не Т-конечно.

4.5. Каждое натуральное число Т-конечно.

4.6. Множество всех натуральных чисел Т-бесконечно.

4.7. Множество конечно тогда и только тогда, когда оно Т-конечно.

5 Возвратная индукция и рекурсия

5.1. Используя лишь обычную индукцию, докажите, что для любого $n \in \mathbb{N}$,

$$\forall X\,((X \subseteq n \wedge X \neq \varnothing) \to \mathrm{Min}\,(X) \neq \varnothing).$$

Выведите отсюда принцип минимального элемента.

5.2. Выведите принцип возвратной индукции из принципа минимального элемента.

Пусть $X \subseteq \mathbb{N}$ и $X \neq \varnothing$. Будем называть X *ограниченным*, если $\exists n \in \mathbb{N}\,\forall u \in X\,(u \leqslant n)$. Будем говорить, что $x \in X$ является *наибольшим* в X, если $\forall u \in X\,(u \leqslant x)$.

5.3. Если непустое множество натуральных чисел ограничено, то оно содержит наибольший элемент, причём такой элемент единственнен.

5.4. Завершите доказательство теоремы о рекурсии, т.е. проверьте, что определённое в этом доказательстве отношение f будет искомой функцией из $\mathbb{N}$ в Y.

5.5. Завершите доказательство параметризованной теоремы о рекурсии, т.е. проверьте, что определённая в этом доказательстве функция f будет искомой.

5.6. Для всех $k, m, n \in \mathbb{N}$ верно следующее:

i. $(k+m)+n=k+(m+n)$;

ii. $m+n=n+m$.

Можно продолжить в том же духе изучать свойства различных арифметических операций. Делать мы этого не будем.

5.7. Докажите теорему о возвратной рекурсии.

5.8. Докажите теорему о возвратной «классовой рекурсии».

6 Равномощность

6.1. Для любых X, Y и Z верно следующее:

i. $|X \times Y| = |Y \times X|$;

ii. $|(X \times Y) \times Z| = |X \times (Y \times Z)|$;

iii. если $|X| = |Y|$, то $|X \times Z| = |Y \times Z|$.

6.2. Для любых X, Y и Z верно $\left|Z^{X \times Y}\right| = \left|\left(Z^Y\right)^X\right|$.

6.3. Для любых X, Y и Z верно следующее:

i. если $X \subseteq Y$, то $|X| \leqslant |Y|$;

ii. если $|X| \leqslant |Y|$, то $|X \times Z| \leqslant |Y \times Z|$;

iii. если $Y \neq \varnothing$, то $|X| \leqslant |X \times Y|$.

6.4. Для любых X, Y и Z верно следующее:

i. если $|X| \leqslant |Y|$, то $\left|X^Z\right| \leqslant \left|Y^Z\right|$;

ii. если $|X| \leqslant |Y|$, то $\left|Z^X\right| \leqslant \left|Z^Y\right|$;

iii. если $Y \neq \varnothing$, то $|X| \leqslant \left|X^Y\right|$.

6.5. Пусть $|X| \leqslant |Y|$ и $X \neq \varnothing$. Тогда существует сюрьекция из Y на X.

6.6 (в ZFC). Пусть существует сюрьекция из Y на X. Тогда $|X| \leqslant |Y|$.

7 Счётные множества

7.1. Дайте убедительное (хотя и неформальное) обоснование счётности следующих множеств:

i. множество всех целых чисел;

ii. множество всех рациональных чисел;

iii. множество всех периодических дробей;

iv. множество всех полиномов с целыми коэффициентами;

v. множество всех полиномов с рациональными коэффициентами;

vi. множество всех вещественных алгебраических чисел.[†]

(Хотя последний пункт подразумевает доказательство, в котором используется аксиома выбора, тут это не принципиально.)

Говорят, что X *бесконечно по Дедекинду*, или D-*бесконечно*, если X равномощно некоторому своему собственному подмножеству. В противном случае его называют *конечным по Дедекинду*, или D-*конечным*.

7.2. Если множество конечно, то оно D-конечно.

7.3 (в ZFC). Если множество бесконечно, то оно D-бесконечно.

7.4. Пусть $f : X \to \mathbb{R}$. Предположим также, что

$$\left\{\sum\nolimits_{s\in S} f(s) \mid S \subseteq X \text{ и } S \text{ конечно}\right\}$$

ограничено, т.е. существует $N \in \mathbb{N}$ такое, что для любого конечного $S \subseteq X$,

$$\left|\sum\nolimits_{s\in S} f(s)\right| \leqslant N.$$

Тогда $\{x \in X \mid f(x) \neq 0\}$ не более чем счётно.

8 Континуальные множества

Будем называть X *континуальным*, если оно равномощно $2^{\mathbb{N}}$.

Факт. $\mathbb{R}$ континуально. [На практике был дан набросок доказательства.]

Из этого факта нетрудно вывести следующее:

8.1. $\mathbb{R} \times \mathbb{R}$, $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ и т.д. континуальны.

8.2. $\mathbb{R}^*$ континуально.

Используя «диагональную конструкцию» и явную сюрьекцию из $\mathbb{N}$ на множество всех вещественных алгебраических чисел, мы можем определить вполне конкретное трансцендентное число.[‡] По мощности же таких чисел столько же, сколько и вещественных:

8.3. Множество всех трансцендентных чисел континуально.

Напоследок отметим одно свойство, связанное с «вычитанием» из континуума:

8.4 (в ZFC). Пусть $X \cup Y = \mathbb{R}$. Тогда хотя бы одно из X и Y континуально.

[†]Здесь и далее мы будем свободно пользоваться базовыми результатами из области алгебры и анализа (включая обычные свойства вещественных чисел).

[‡]Безусловно, куда более красивыми трансцендентными числами являются π или e, но их транцендентность существенно сложнее доказать.

9 Упорядоченные множества

Пусть дано л.у.м. $\mathfrak{A} = \langle A, \leqslant \rangle$. Будем называть $S \subseteq A$ *начальным сегментом* $\mathfrak{A}$, если для любых $a_1, a_2 \in A$,

$$a_1 \leqslant a_2 \quad \text{и} \quad a_2 \in S \quad \Longrightarrow \quad a_1 \in S.$$

(На лекции это определение было дано для в.у.м., но можно и для л.у.м.)

9.1. Пусть $\langle A, \leqslant \rangle$ — л.у.м.

i. Если S — начальный сегмент $\langle A, \leqslant \rangle$, а T — начальный сегмент $\langle S, \leqslant_S \rangle$, то T — начальный сегмент $\langle A, \leqslant \rangle$.

ii. Если $S \subseteq A$, а T — начальный сегмент $\langle A, \leqslant \rangle$, то $S \cap T$ — начальный сегмент $\langle S, \leqslant_S \rangle$.

[Здесь $\leqslant_S$ обозначает $\leqslant \cap\, S \times S$.]

9.2. Пусть $\mathfrak{A}$ — л.у.м.

i. Если S и T — начальные сегменты $\mathfrak{A}$, то $S \subseteq T$ или $T \subseteq S$.

ii. Если $\mathscr{S}$ — некоторое множество начальных сегментов $\mathfrak{A}$, то $\bigcup \mathscr{S}$ и $\bigcap \mathscr{S}$ окажутся начальными сегментами $\mathfrak{A}$.

Альтернативное определение в.у.м. даёт:

9.3. Для всякого ч.у.м. $\langle A, \leqslant \rangle$ следующие условия эквивалентны:

i. $\leqslant$ — полный порядок на A;

ii. в каждом непустом подмножестве A есть наименьший элемент.

[Таким образом, (ii) гарантирует линейность $\leqslant$.]

9.4 (в ZFC). Ч.у.м. $\langle A, \leqslant \rangle$ фундировано тогда и только тогда, когда не существует инъективной функции f из $\mathbb{N}$ в A такой, что $f(n+1) < f(n)$ для всех $n \in \mathbb{N}$.

9.5. Гомоморфизм f из ч.у.м. $\mathfrak{A}$ в ч.у.м. $\mathfrak{B}$ является изоморфизмом тогда и только тогда, когда существует гомоморфизм g из $\mathfrak{B}$ в $\mathfrak{A}$ такой, что

$$f \circ g \;=\; \mathrm{id}_A \quad \text{и} \quad g \circ f \;=\; \mathrm{id}_B.$$

[Иными словами, изоморфизмы суть «гомоморфизмы, обратимые в классе гомоморфизмов».]

Следующие два упражнения, несмотря на всю тривиальность формулировок, отнюдь не лишены смысла, поскольку их строгие решения содержат идеи, полезные при доказательстве результатов о бесконечных множествах.

9.6. Всякое ч.у.м. с конечным носителем фундировано. [Постараться решить строго.]

9.7. Пусть $\mathfrak{A} = \langle A, \leqslant \rangle$ — ч.у.м., причём A конечно. Тогда для каждого $a \in A$ существует максимальный в $\mathfrak{A}$ элемент a' такой, что $a \leqslant a'$. [Постараться решить строго.]

Следующее упражнение не столь очевидно, хотя и похоже на предыдущие два.

9.8. Пусть $\mathfrak{A} = \langle A, \leqslant \rangle$ — ч.у.м., причём A конечно. Тогда существует линейный порядок $\preccurlyeq$ на A такой, что $\leqslant \subseteq \preccurlyeq$.

Далее мы поговорим о характеризации с точностью до изоморфизма.

9.9. Пусть $\mathfrak{A} = \langle A, \leqslant_A \rangle$ — в.у.м., удовлетворяющий следующим условиям:

a. в $\mathfrak{A}$ есть наименьший элемент, но нет наибольшего;

b. в каждом непустом подмножестве A, имеющем верхнюю грань, есть наибольший элемент.

Тогда $\langle A, \leqslant_A \rangle$ изоморфно $\langle \mathbb{N}, \leqslant \rangle$, где $\leqslant$ — естественный порядок на $\mathbb{N}$.

Ч.у.м. $\mathfrak{A} = \langle A, \leqslant_A \rangle$ называют *плотным*, если

$$\forall a_1 \in A\, \forall a_2 \in A\, (a_1 <_A a_2 \to \exists a_{1.5} \in A\, (a_1 <_A a_{1.5} <_A a_2)).$$

Под ч.у.м. *без концов* понимается произвольное ч.у.м., в котором нет ни наибольшего, ни наименьшего элементов.

9.10. Пусть $\mathfrak{A} = \langle A, \leqslant_A \rangle$ и $\mathfrak{B} = \langle B, \leqslant_B \rangle$ — два плотных л.у.м. без концов, причём A и B счётны. Тогда $\mathfrak{A}$ и $\mathfrak{B}$ изоморфны. [Решение см. тут.]

9.11. С точностью до изоморфизма существует ровно четыре плотных л.у.м. со счётными носителями.

9.12. Постройте два плотных л.у.м. без концов с континуальными носителями, которые не изоморфны.

10 Ординалы и кардиналы

10.1. Докажите, что сложение и умножение на Ord ассоциативны.

10.2. Докажите, что ни сложение, ни умножение на Ord не коммутативно.

10.3. Аккуратно докажите теорему о классовой трансфинитной рекурсии.

10.4. Докажите, что сложение и умножение на Card ассоциативны и коммутативны.

10.5 (в ZFC). Докажите, что Card не является множеством.

11 Лемма Цорна [Здесь всё в ZFC!]

11.1. У всякого векторного пространства есть базис.

11.2. Пусть $\mathfrak{A} = \langle A, \leqslant \rangle$ — ч.у.м. Тогда сущ. линейный порядок $\preccurlyeq$ на A такой, что $\leqslant \subseteq \preccurlyeq$.

Набросок решения. Рассмотрим

$$X \;:=\; \text{множество всех частичных порядков на } A.$$

Обозначим через $\preccurlyeq$ порядок по включаению на S, т.е. для любых $R_1, R_2 \in X$,

$$R_1 \;\preccurlyeq\; R_2 \quad\Longleftrightarrow\quad R_1 \;\subseteq\; R_2.$$

Легко убедиться, что объединение произвольной цепи частичных порядков на A является частичным порядком на A. Значит, ч.у.м. $\langle X, \preccurlyeq \rangle$ удовлетворяет условиям (следствия) леммы Цорна.

Пусть $\leqslant'$ — это максимальный в $\langle X, \preccurlyeq \rangle$ элемент такой, что $\leqslant \subseteq \leqslant'$. Предположим, что $\leqslant'$ не линейный, т.е. для некоторых $c_1, c_2 \in A$ мы имеем

$$c_1 \not\leqslant' c_2 \quad \text{и} \quad c_1 \not\leqslant' c_2.$$

Определим бинарное отношение $\leqslant''$ на A по правилу

$$a_1 \leqslant'' a_2 \quad :\Longleftrightarrow \quad a_1 \leqslant' a_2 \text{ или } (a_1 \leqslant' c_1 \text{ и } c_2 \leqslant' a_2).$$

Нетрудно убедиться, что $\leqslant''$ будет частичным порядком на A. Однако $\leqslant''$ строго больше $\leqslant'$ в $\langle X, \preccurlyeq \rangle$ — противоречие. □

Цепь S в ч.у.м. $\mathfrak{A}$ называют *максимальной*, если S максимальна по включению среди всех цепей в $\mathfrak{A}$, т.е. не существует цепи S' в $\mathfrak{A}$ такой, что $S \subsetneq S'$.

11.3 (принцип максимума Хаусдорфа). Пусть $\mathfrak{A} = \langle A, \leqslant \rangle$ — ч.у.м. Тогда для каждой цепи S в $\mathfrak{A}$ найдётся максимальная цепь S' в $\mathfrak{A}$ такая, что $S \subseteq S'$.