Лекция 1

страница курса: http://gorod.bogomolov-lab.ru/ps/stud/algebra-1/2021/list.html

Множества и отображения

$$X \xrightarrow{f} Y$$

отображение сопоставляет каждому элементу $x \in X$ ровно один элемент $f(x) \in Y$.

Отображение f наз. **инъективным** (отображение "в") инъекция, вложение, мономорфизм

если у каждого $y \in Y$ не более одного прообраза, т.е. либо $\nexists x: f(x)=y$
либо $\exists! x: f(x)=y$.

Образ отображения — множество $\{y \in Y \mid \exists x: f(x)=y\}$

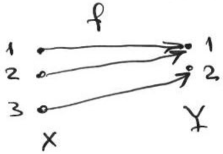
Обозначение im(f)

f наз. **сюръективным** (отображение "на") сюръекция, наложение, эпиморфизм

если образ $f = Y$, т.е. у каждого $y \in Y$ есть прообраз.

f наз. **биекцией**, изоморфизмом, взаимно-однозначным, если оно вложение и наложение.

Отображение vs слова



X как фиксированные позиции

1 1 2

слово 1 1 2 $\leftarrow \underbrace{1 \quad 2 \quad 3}_{X}$

позиции букв - это элементы множества X

а сами буквы — алфавит, которым слово написано, это множество Y.

Y^X

Все отображения $X \to Y$ обозначаются Hom(X, Y)

$||$

слова "из X букв" написанные в алфавите Y

Обз: |X| - число элементов в конечном множестве

|X| и |Y| конечны $\Rightarrow$ $|\mathrm{Hom}(X,Y)| = |Y|^{|X|}$.

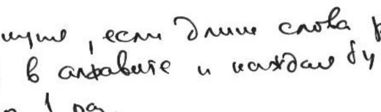
- f инъективно, если в соответствующем слове буквы не повторяются.

- f - биекция, если длина слова равна количеству букв в алфавите и каждая буква используется ровно 1 раз.

|X| - конечно, количество биекций $X \xrightarrow{\sim} X$ тоже конечно и $|\mathrm{Aut}\,X| = |X|!$

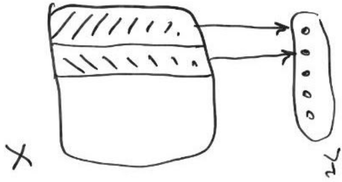
биекции $X \to X$ называют автоморфизмами
Aut(X) - множество всех биекций

$$|\mathrm{Aut}\,X|! = |X| \cdot (|X|-1) \cdot (|X|-2) \cdot \ldots$$



(Отображения vs разбиения на классы)

сюръективное отображение



X распадается в объединение непересекающихся "слоёв"

$$X = \bigsqcup_{y\in Y} f^{-1}(y)$$

слой $f^{-1}(y) = \{x\in X \mid f(x)=y\}$

$X\cup Y$ – объединение

$X\sqcup Y$ – дизъюнктное объединение, т.е. объединение непересекающихся множеств

Это наблюдение можно использовать для подсчёта числа элементов:

если все слои $f^{-1}(y)$ состоят из одного и того же числа элементов S, то

$$|X| = S\cdot|Y|$$

Пример использования: раскрытие степеней

$$(a_1+a_2+\ldots+a_m)^n = (a_1+\ldots+a_m)(a_1+\ldots+a_m)\ldots(a_1+\ldots+a_m)$$

в каждой скобке выбираем букву и составляем из них слово (n-буквенное).

Типичное подобное слагаемое равно

$$a_1^{k_1}a_2^{k_2}\ldots a_m^{k_m}, \left[\begin{array}{l} 0\le k_i\le n \\ k_1+k_2+\ldots+k_m=n \end{array}\right.$$

оно войдёт с коэфф-том который обозначаем

$$? = \binom{n}{k_1 k_2 \ldots k_m} =$$ количеству n-буквенных слов, которые можно составить из k_1 букв a_1, k_2 букв a_2

k_m букв a_m

Сделаем все буквы разными, пометив буквы

a_1 верхними индексами $1, 2, \dots, k_1$

a_2 " " $1, 2, \dots, k_2$

$$\underbrace{a_1 a_1 \dots a_1}_{k_1} \underbrace{a_2 \dots a_2}_{k_2} \dots \underbrace{a_m \dots a_m}_{k_m}$$

$\downarrow$ все буквы сделаем разными.

$$a_1^{(1)} a_1^{(2)} \dots a_1^{(k_1)} a_2^{(1)} \dots a_2^{(k_2)}$$

X $|X| = n!$

n-буквенных слов, составленных из разных букв
$a_1^{(1)} a_1^{(2)} \dots a_1^{(k_1)}$
$a_2^{(1)} \dots a_2^{(k_2)}$
– – –
(всего ровно n букв)

$$\xrightarrow[\text{стирает номер}]{f}$$

Y

n буквенные слова, составленные из k_1 букв a_1 (одинак.)
k_2 букв a_2 (один.)
⋮
k_m букв a_m (одина.

разные буквы $\xrightarrow[\text{верхние номера}]{\text{стираем}}$ в котором буквы повторяются

в него перейдет $k_1!\, k_2! \dots k_m!$ слов, отличающихся различными расстановками верхних номеров над одинаковыми буквами $\longrightarrow$ $a_1 \dots a_1 a_2 \dots a_2 \dots a_m \dots a_m$

мультиномиальный коэф-т $\binom{n}{k_1 \dots k_m} = \frac{n!}{k_1!\, k_2! \dots k_m!}$

Пример: бином $(a+b)^n = \sum\limits_{k=0}^{n} \underbrace{\binom{n}{k, n-k}}_{\shortparallel} a^k b^{n-k}$

биномиальный коэф-т $\rightarrow \binom{n}{k} = \frac{n!}{k!\,(n-k)!}$

$$= \frac{\overbrace{n(n-1)\cdots}^{k}}{\underbrace{k(k-1)\cdots}_{k}}$$

Организовать разбиение множества X на непересекающиеся подмножества — это то же самое, что задать на X отношение эквивалентности

отношение (бинарное отношение) — это подмножество $R \subset X \times X$ ← декартово произведение

$$\shortparallel$$

$$\{(x_1, x_2) \mid x_1, x_2 \in X\}$$

$(x_1, x_1) \in R$ x_1 и x_2 наз. соотносящимися посредством отношения R

$x_1 \underset{R}{\sim} x_2$

$$\boxed{X \xrightarrow{f} Y \text{ сюръективное}}$$

$$\Big\downarrow$$

отношение $x_1 \sim x_2 \Leftrightarrow f(x_1) = f(x_2)$

x_1 и x_2 лежат в одном слое

лежат лежат в одном подмножестве разбиения

У этого отношения есть 3 свойства:

(1) $\forall x \in X \quad x \sim x$ ($(x,x) \in R$, R содержит диагональ $\Delta \subset X \times X$)

"рефлексивность"

$$\Delta = \{(x,x) \mid x \in X\}$$

(2) "симметричность"

$x_1 \sim x_2 \Rightarrow x_2 \sim x_1$ ($(x_1,x_2) \in R \Rightarrow (x_2,x_1) \in R$

R симметрично отн. диагонали Δ)

(3) "транзитивность"

$x_1 \sim x_2$ и $x_2 \sim x_3 \Rightarrow x_1 \sim x_3$

$$\left.\begin{matrix}(x_1,x_2) \in R \\ (x_2,x_3) \in R\end{matrix}\right\} \Rightarrow (x_1,x_3) \in R.$$

$R \subset X \times X$ наз. отношением эквивалентности, если R рефлексивно, симметрично и транзитивно.

Примеры: Пусть $X = \mathbb{Z}$ – целые числа.

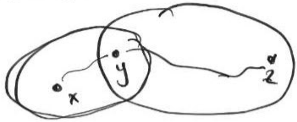
$x_1 \sim x_2$ если $x_1 - x_2$ делится на 7.

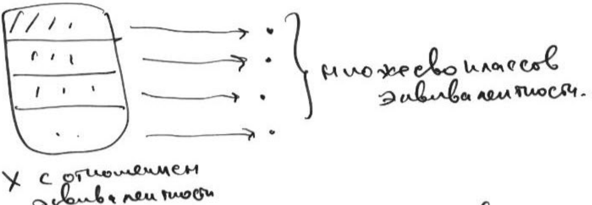
$\boxed{x_1-x_2 \vdots 7}$ $x_2-x_3 \vdots 7$ $x_1-x_3=(x_1-x_2)+(x_1-x_3)$

$\vdots 7$

$\Leftarrow$ (у x_1 и x_2 одинаковый остаток mod 7.)

Факт: если объединить в одно подмножество все элементы эквивалентные данному, то получится разбиение на непересекающиеся подмножества.




множество классов эквивалентности.
X с отношением эквивалентности

$$\begin{tikzcd}
\mathbb{Z} \arrow[r] & \mathbb{Z}/(7) \\
x \arrow[r, mapsto] & {[x]}
\end{tikzcd}$$

← множество классов целых чисел, дающих одинаковый остаток от деления на 7

↑ множество всех чисел с тем же остатком от деления на 7, что и x.

$\boxed{\mathbb{Z}/(7) \quad 0,1,2,3,4,5,6}$

$[0]\ [1]\ [2]\ [3]\ [4]\ [5]\ \underset{[-1]}{\overset{}{[6]}}$

$[6] = [-1]$

$$\boxed{[6^{2020}] = [6]^{2020} = [-1]^{2020} = [(-1)^{2020}] = [1]}$$

6^{2020} имеет остаток 1 от деления на 7.

На $\mathbb{Z}/(7)$ имеется умножение и сложение

по правилам: $[x]\cdot[y]=[xy]$ Некорректное определение

(*) $[x]+[y]=[x+y]$

Почему эти правила не зависят от способа записи класса?

$[x_1]=[x_2]$, т.е. $x_1-x_2 \vdots 7$ $\quad x_1=x_2+7k$

$[y_1]=[y_2]$, т.е. $y_1-y_2 \vdots 7$ $\quad y_1=y_2+7m$

почему $[x_1+y_1]\overset{?}{=}[x_2+y_2]$

$[x_1y_1]\overset{?}{=}[x_2y_2]$

если это не так, то правила (*) бессмысленны

$$x_1+y_1=x_2+7k+y_2+7m=x_2+y_2+7(k+m)$$

$$x_1y_1=(x_2+7k)(y_2+7m)=x_2y_2+\underbrace{7ky_2+7mx_2+49km}_{7\cdot\ldots}$$

$R\subset X\times X$ называется частичным порядком

если оно (1) рефлексивно, т.е. $x\underset{R}{\sim}x$

(2) кососимметрично, т.е. $x\underset{R}{\sim}y,\ y\underset{R}{\sim}x \Rightarrow x=y$

(3) транзитивно, т.е. $x\underset{R}{\sim}y,\ y\underset{R}{\sim}z \Rightarrow$ $\Rightarrow x\underset{R}{\sim}z$

Пример: 1) Отношение $\leqslant$ на $\mathbb{Z}$

$x\leqslant y$ и $y\leqslant x \Rightarrow y=x$.

2) отношение делимости на $\mathbb{Z}$

$x \mid y$ x делит y

$y \vdots x$ y делится на x.

3) отношение $\subseteq$ на множестве всех подмножеств данного множества.

$A \subseteq M$ и $B \subseteq M$

отношение $A \subseteq B$ нестрогое включение

в отношении (1) $\leq$ на $\mathbb{Z}$. любые два элемента сравнимы, т.е. $\forall a, b$ либо $a \leq b$ либо $b \leq a$ выполнено.

в отношениях $\underset{(2)}{\text{делимости}}$ и $\underset{(3)}{\text{включения}}$

бывают несравнимые элементы

бывают числа a и b : $a \nmid b$ и $b \nmid a$

бывают подмножества $A, B \subseteq M$:

$A \nsubseteq B$ и $B \nsubseteq A$.

Множество X с зафиксированным на нём частичным порядком $\leq$ наз. частично упорядоченным множеством (ЧУМ)

(poset)

Чум X наз. линейно упорядоченным или просто упорядоченным, если любые два элемента сравнимы.

Например $\mathbb{Z}, \le$ — линейно упорядочено.

Линейно упорядоченное множество X называется вполне упорядоченным, если в любом его подмножестве $Y \subseteq X$ имеется минимальный элемент y_* (т.е. такой $y_* \in Y$, что $\forall y \in Y \quad y_* \le y$).

Примеры: 1) $\mathbb{N}, \le$

2) $\mathbb{N} \sqcup \mathbb{N} \sqcup \mathbb{N} \sqcup \ldots \sqcup \mathbb{N}$

все левые строго меньше правых.

По вполне упорядоченному множеству можно вести индукцию: пусть W — вполне упорядоченно (well ordered).

и задано утверждение $\Gamma(w)$ зависящее от элементов $w \in W$. Тогда если

(1) $\Gamma(w_*)$ верно для минимального элемента $w_* \in W$

(2) Из того, что $\Gamma(w)$ верно $\forall\, w < w_0$, всегда вытекает, что $\Gamma(w)$ верно для w_0

То $\Gamma(w)$ верно $\forall w \in W$.

Пусть $\Gamma(w)$ неверно для каких-то $w \in W$
возьмём наименьшее такое w

Тогда $\Gamma(w')$ верно $\forall w' < w \Rightarrow \Gamma(w)$ верно

противоречие!

Вполне упорядоченное множество допускает рекурсивный перебор

$$[w) = [\overset{\text{мин. элемент}}{w_*}, w)$$

Для $w \in W$ обозначим $[w) :=$
$= \{w' \in W \mid w' < w\}$

начальный интервал множества W вплоть до w, исключая w.

w однозначно восстанавливается по $[w)$ как наименьший элемент дополнения
$$W \setminus [w)$$

Ключевая лемма

Рассмотрим любое ЧУМ $\underline{M}$

Обозначим через $\mathfrak{W}(M)$ множество всех подмножеств $W \subset M$, которые вполне упорядочены относительно того порядка, что есть на M.

Включим в $\mathfrak{W}(M)$ также пустое подмножество $\emptyset \subset M$.

$\mathfrak{W}(M) \neq \emptyset$

$\emptyset \in \mathfrak{W}(M)$

все конечные линейно-упорядоченные подмножества в M тоже лежат в $\mathfrak{W}(M)$.

Лемма: Не существует отображения

$$\mathfrak{W}(M) \xrightarrow{f} M$$

при котором каждое $W \in \mathfrak{W}(M)$ переходит в такой элемент $f(W)$, который строго больше всех элементов у W.

Док-во: Пусть такое f есть.

Скажем, что $W \in \mathfrak{W}(M)$ f-рекурсивно, если $\forall w \in W \quad f([w)) = w$

Например:

$f(\emptyset) \in M$

$f(\{\emptyset\})$

f-рекурсивное множество ⟶ $f(f(\{f(\emptyset), f(\{\emptyset\})\}))$

$\vdots$

Факт: если у двух f-рекурсивных множеств U и V общий начальный элемент, то либо U является начальным интервалом в V либо V является начальным интервалом в U

$$U \cap V \begin{matrix} \neq U \\ \neq V \end{matrix}$$

в U и в W есть наименьшие эл-ты
не лежащие в $U \cap V$ $u \in U$
$w \in W$

$[u)_U$ $[w)_W$ оба лежат в $U \cap V$
и равны друг другу !

$$u = f([u)) = f([w)) = w$$

Рассмотрим множество всех f-рекурсивных подмножеств с минимальным эл-том $f(\varnothing)$

Пусть U — это их объединение. — оно вполне упорядочено и f-рекурсивно.

$f(U)$ это элемент, строго больший, чем U.

$U \cup f(U)$ — это f-рекурсивное вполне упорядоченное множество, начинающееся с $f(\varnothing)$, и оно содержит U и $\neq U$.

Противоречие!