Алгебраические объекты

Кольцо (*моноид в категории абелевых групп*) – это:
1. абелева группа $(+, 0)$
2. $a(b+c) = ab + ac$ – дистрибутивность слева и, аналогично, справа
3. $a(bc) = (ab)c$ – ассоциативность умножения
4. $\exists 1 : a1 = 1a = a$ – единица

- Кольцо коммутативно, если умножение коммутативно
- Кольцо называется Integral domain, если нет делителей нуля

Поле – это integral domain коммутативное кольцо:
1. $0 \neq 1$
2. $\forall a : a \neq 0 : \exists a^{-1} : aa^{-1} = 1$

Упражнение. Найти integral domain коммутативное кольцо с $0 = 1$.

Коммутативные кольца

Из простейших: $\mathbb{Z}$.

Тут стоит добавить, что в современной математике работают со спектрами, а не с кольцами типа $\mathbb{Z}$. Последние содержат в себе очень много нерешенных проблем, но проблемы в спектрах куда глубже и хранят *все тайны мироздания*.

А еще $\mathbb{Z}$ уникальна тем, что это инициальный объект в категории `Ring`.

Можем проверить, что $\mathbb{Z}/n\mathbb{Z}$ тоже кольцо. А еще, что это поле. Но когда? Когда n – простое.

Утверждается, что для $n = p^2$ мы можем построить еще какое-нибудь поле, отличное от классического. Например, проделаем это для $n = 4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Это таблица Кэли для сложения. Довольно симметрично, давайте на ее основе, сохраняя дистрибутивности, сделаем аналогичную для умножения

$\star$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Тоже получилось интересно. Теперь попробуем построить изоморфизм в комплексные числа, кватернионы.

$M_n(\mathbb{R})$ – кольцо матриц размерностью $n \times n$, элементы которых $\in \mathbb{R}$. Тогда можем построить изоморфизм из подмножества $M_2(\mathbb{R})$:

$$a + ib = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

Сложение понятно как, умножение проверяется (на то, что это поле). Теперь давайте какое-то подмножество $M_2(\mathbb{C})$:

$$\begin{pmatrix} z & -\tilde{d} \\ d & \tilde{z} \end{pmatrix}$$

И если раскрыть, то получатся уже кватернионы, вот как-то так (в качестве упражнения можно это проверить: только это будет уже будет просто телом, а не полем).

Групповые кольца

$\mathbb{Z}$ – кольцо, G – группа, тогда групповым кольцом называется множество конечных формальных сумм вида $\sum n_i g_i$ и обозначается это как $\mathbb{Z}[G]$.

Чем они интересны? А тем, что позволяет линеаризовывать группы. Что мы еще знаем полезного? А то, что $\mathbb{Z}[\mathbb{Z}]$ изоморфно кольцу полиномов Лорана $\mathbb{Z}\left[t, t^{-1}\right]$.

Что с делителями нуля? Ну миру известно, что если есть кручение ($\exists g \in G : \exists n : g^n = 1$), то существует делитель нуля.

А если нет? Это, вообще говоря, нерешенная проблема.

Подгруппы (продолжение)

Давайте поговорим про индексы подгрупп. G/H – классы эквивалентности, где $a \sim b \Leftrightarrow ab^{-1} \in H$.

Тогда индексом подгруппы называется $|G : H|$ такой, что $|G : H| \cdot |H| = |G|$. Почему так вообще можно и почему так? Ответы на это есть в предыдущем конспекте.

Что тут интересного? Ну если $|G| \in \mathbb{P}$, то любая подгруппа это или $\{e\}$, или сама G. А что еще интересного? Можно прочитать про группы Силова (подгруппы порядка степени простого числа).

Проверено, что $|G : H| = 2 \Rightarrow H$– нормальная подгруппа (представим $H \sqcup Hb^{-1} = G$ и проверим). Еще проверено, что $\Rightarrow \forall g \in G : g^2 \in H$.

Упражнение. Убедиться, что МТФ следствие из теоремы Лагранжа.

Коммутант (продолжение)

В качестве хорошего упражнения было проверено, что коммутант $[G, G]$ – нормальная подгруппа (решение Никиты Галимуллина в 2 множителя):

1. надо проверить, что $x[a, b]x^{-1}$ – произведение коммутаторов
2. $[xa, b][b, x] = xaba^{-1}x^{-1}b^{-1}bxb^{-1}x^{-1} = xaba^{-1}b^{-1}x^{-1} = x[a, b]x^{-1}$
3. проверили