ГРУППЫ И ИХ ОБОБЩЕНИЯ: ПОЛУГРУППЫ И КВАЗИГРУППЫ

Определение группы

Группой $(G, *)$ называется множество G с определенной на нем бинарной операцией $*$, удовлетворяющей следующим трем аксиомам:

1. $\forall a, b, c \in G,\ (a * b) * c = a * (b * c)$ (ассоциативность)
2. $\exists e \in G :\ \forall a \in G,\ a * e = e * a = a$ (существование *единицы*)
3. $\forall a \in G,\ \exists\ x \in G :\ \ a * x = x * a = e$ (существование *обратного элемента* $x = a^{-1}$)

Полугруппы, квазигруппы, моноиды и лупы

Полугруппой $(G, *)$ называется непустое множество G с определенной на нем бинарной операцией $*$, удовлетворяющей аксиоме ассоциативности:

$$\forall a, b, c \in G,\ (a * b) * c = a * (b * c).$$

Квазигруппой $(G, *)$ называется непустое множество G с определенной на нем бинарной операцией $*$, удовлетворяющей следующим двум аксиомам:

1. $\forall a, b \in G,\ \exists! x \in G :\ a * x = b$ (левое деление)
2. $\forall a, b \in G,\ \exists! y \in G :\ y * a = b$ (правое деление)

Полугруппа с единицей называется *моноидом.*

Квазигруппа с единицей называется *лупой*

Полугруппа и квазигруппа=группа.

Очевидно: любая группа является и моноидом, и лупой (в группе $a*x=b \Leftrightarrow x=a^{-1}*b$ и $y*a=b \Leftrightarrow y=b*a^{-1}$).

Теорема 1. Пусть G — непустое множество с определенной на нем бинарной операцией $*$. Тогда следующие условия эквивалентны:

1. $(G,*)$ — группа;
2. $(G,*)$ — моноид и лупа;
3. $(G,*)$ — моноид и квазигруппа;
4. $(G,*)$ — полугруппа и лупа;
5. $(G,*)$ — полугруппа и квазигруппа.

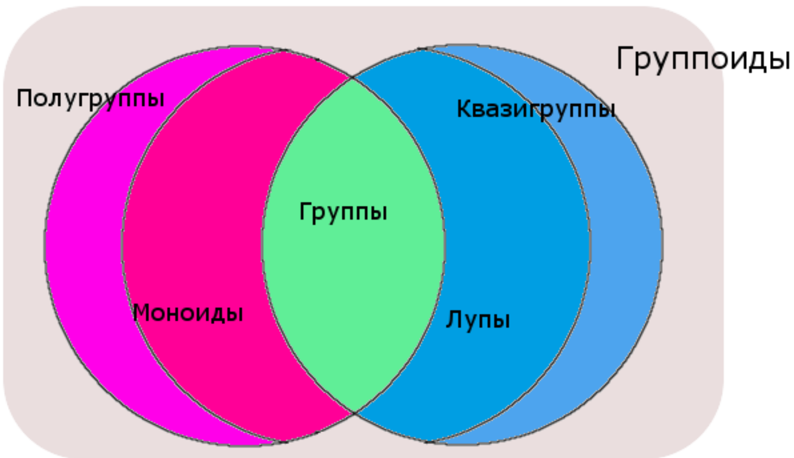
Доказательство

Пусть $(G,*)$ — полугруппа и квазигруппа. Докажем существование единицы. Зафиксируем $g \in G$ и найдем элемент $e \in G$, такой, что $e*g=g$. Тогда $(g*e)*g=g*(e*g)=g*g$, и из единственности решения уравнения $y*g=g*g$ получаем $g*e=g$. Теперь для любого $a \in G$ имеем $(a*e)*g=a*(e*g)=a*g$, и из единственности решения уравнения $y*g=a*g$ получаем $g*e=g$. Аналогично проверяется, что $e*a=a$, т.е. e — единица. Пусть теперь $x*a=e$ и $a*y=e$. Тогда

$$x=x*e=x*(a*y)=(x*a)*y=e*y=y,$$

т.е. $x=y=a^{-1}$. $\square$

Иллюстрация



Латинские квадраты

Квадратом над конечным множеством M из n элементов назовем произвольную матрицу L размера $n \times n$ с элементами из M. Строки и столбцы матрицы L мы будем нумеровать элементами из M и обозначать через $L[x, y]$ элемент из строки x и столбца y матрицы L. *Латинским квадратом* называется квадрат над конечным множеством M, в каждом столбце и каждой строке которого содержатся все элементы из M. Любой квадрат L над M можно рассматривать как таблицу бинарной операции $*$ на M, считая, что $L[x, y] = x * y$.

Квадрат L является латинским тогда и только тогда, когда $(M, *)$ — *квазигруппа*, т.е.

$$\forall \quad a, b \in M \quad \exists!\ x, y \in M : a * x = b \quad \& \quad y * a = b.$$

Пример

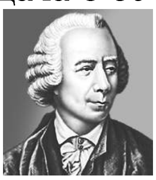
Латинский квадрат

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

есть таблица операции $x * y = 2x + y$ в абелевой группе $\mathbb{Z}_5$.

Впервые латинские квадраты (4-го порядка) были опубликованы в книге «Шамс аль Маариф» («Книга о Солнце Гнозиса»), написанной Ахмадом аль-Буни в Египте приблизительно в 1200 году.

Задача о 36 офицерах



Л. Эйлер (1707 – 1783) сформулировал следующую задачу (Euler L. Recherches sur une nouvelle espèce de quarrés magiques. — Middelburg, 1782):

“Этот вопрос касается совокупности 36 офицеров шести разных званий, взятых из шести разных полков, которых выстраивают в каре таким образом, чтобы в каждом ряду, как по горизонтали, так и по вертикали, находилось шесть офицеров различных званий и из разных полков. Однако после всех трудов, затраченных на решение этой задачи, я вынужден был признать, что такое размещение абсолютно невозможно, хотя и не удалось дать строгого доказательства этому.”

Задача о 9 офицерах (греко-латинский квадрат)

Пусть a, b, c обозначают полки — уланский, драгунский, гусарский, α, β, γ обозначают звания — корнет, штабс-ротмистр, ротмистр. Пара $a\alpha$ обозначает улана-корнета и т.д., до пары $c\gamma$, которая обозначает гусара-ротмистра.

Решение

$a\alpha$	$b\gamma$	$c\beta$
$b\beta$	$c\alpha$	$a\gamma$
$c\gamma$	$a\beta$	$b\alpha$

a	b	c
b	c	a
c	a	b

α	γ	β
β	α	γ
γ	β	α

Ортогональные латинские квадраты

Квадраты L и L' над множеством M называются *ортогональными*, если отображение $(x, y) \mapsto (L[x, y], L'[x, y])$ биективно на $M \times M$. Иными словами, любая пара элементов из M единственный раз встречается в одинаково расположенных клетках этих квадратов.

В терминах операций: квадраты L и L', заданные, соответственно, операциями $*$ и $\circ$ на множестве M, ортогональны тогда и только тогда, когда

$$\forall \quad a, b \in M \quad \exists!\ x, y \in M : x * y = a \quad \& \quad x \circ y = b.$$

Наглядное представление

0	2	4	1	3
1	3	0	2	4
2	4	1	3	0
3	0	2	4	1
4	1	3	0	2

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

00	21	42	13	34
12	33	04	20	41
24	40	11	32	03
31	02	23	44	10
43	14	30	01	22

Гипотеза Эйлера

Л.Эйлер доказал существование пар ортогональных латинских квадратов любого нечётного порядка и любого “чётно-чётного” (т.е. кратного 4) порядка (мы дадим алгебраическое доказательство для квадратов нечётного порядка, использующее группы).

Он также предположил, что ортогональных латинских квадратов “чётно-нечётного” порядка (т.е. порядка вида $n = 4k + 2,\ k = 0, 1, 2, \dots$) не существует.

Для $n = 2$ это очевидно.

Для $n = 6$ это доказано только спустя 100 с лишним лет Г.Тарри (1900).

Однако уже при $n = 10$ пары ортогональных латинских квадратов порядка n существуют (R. C. Bose, S. S. Shrikhande and E. T. Parker, 1960, для построения использовался компьютер). Способ “ручного” построения таких пар предложил Чжу Ле (1982).

Квадраты, построенные методом Чжу Ле

0	2	4	6	9	8	7	5	3	1
7	3	5	0	2	9	8	1	6	4
8	7	6	1	3	5	9	4	2	0
9	8	7	2	4	6	1	0	5	3
4	9	8	7	5	0	2	3	1	6
5	0	9	8	7	1	3	6	4	2
6	1	3	9	8	7	4	2	0	5
1	4	0	3	6	2	5	7	8	9
2	5	1	4	0	3	6	8	9	7
3	6	2	5	1	4	0	9	7	8

0	7	8	9	4	5	6	1	2	3
2	3	7	8	9	0	1	4	5	6
4	5	6	7	8	9	3	0	1	2
6	0	1	2	7	8	9	3	4	5
9	2	3	4	5	7	8	6	0	1
8	9	5	6	0	1	7	2	3	4
7	8	9	1	2	3	4	5	6	0
5	1	4	0	3	6	2	7	8	9
3	6	2	5	1	4	0	9	7	8
1	4	0	3	6	2	5	8	9	7

Построение ортогональных латинских квадратов нечётного порядка

Пусть n — нечётное число, $n > 1$. Рассмотрим группу $G = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ с операцией сложения. Один латинский квадрат определим с помощью операции в этой группе.

Определим на множестве G *новую* операцию: $x * y = 2x + y$, второй квадрат определим с помощью этой операции.

Пример ($n = 5$)

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

Покажем, что второй квадрат — латинский, и что он ортогонален первому.

Доказательство

Покажем, что $(G, *)$ — квазигруппа. Действительно, существование и единственность решения уравнения $a * x = b$ очевидна: $a * x = b \Leftrightarrow 2a + x = b \Leftrightarrow x = b - 2a$.

Существование и единственность решения уравнения $y * a = b$ проверяется так: $y * a = b \Leftrightarrow 2y + a = b \Leftrightarrow 2y = b - a$. По теореме Лагранжа в группе $(G, +)$ нет элементов порядка 2, следовательно, отображение $x \mapsto 2x$ — биекция. Значит, можно получить значение y, применяя обратное отображение к элементу $b - a$.

Теперь проверим, что данные квадраты ортогональны. Для этого обычным образом для любых $a, b \in G$ решим систему уравнений $\begin{cases} x + y = a \\ 2x + y = b \end{cases}$. Из первого уравнения $y = a - x$, из второго $2x + a - x = b \Leftrightarrow x = b - a$, откуда $y = 2a - b$.

Применение латинских квадратов к планированию экспериментов

А. Е. Малых, В. И. Данилова (2010),
http://vestnik.psu.ru/files/articles/199_38700.p

Рональд Фишер, проводивший с 1919 г. серию работ на Рочемстедской агробиологической станции в Англии, в 30-е гг. применил латинские квадраты в сельскохозяйственных экспериментах для учета различий в плодородии почв.

Например: нужно провести эксперимент по сравнению урожайности n сортов пшеницы. Для этого отведен участок земли, но нет уверенности в том, что плодородие почвы на нем однородно. Для уменьшения ошибки поле разбивают на n^2 одинаковых участков и засевают сорта пшеницы, занумерованные числами от 1 до n, в соответствии с наугад выбранным латинским квадратом порядка n. Такое расположение устранит влияние на урожайность неоднородности плодородия почвы.

Использование множеств попарно ортогональных латинских квадратов дает возможность увеличить число факторов. Например, проводится эксперимент по проверке действия n видов удобрений на n сортов пшеницы. Выращивая пшеницу различных сортов в соответствии с латинским квадратом A и распределяя удобрения, используя ортогональный квадрату A латинский квадрат B, получают схему эксперимента, дающую возможность проверить влияние каждого фактора (сорт пшеницы и вид удобрения), т.е. провести *факторный анализ.*

Прямое произведение квазигрупп и теорема Мак Нейша

Определение 1. Пусть $(G, *)$ и $(H, \circ)$ — две квазигруппы. Определим на декартовом произведении $G \times H$ операцию

$$(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \circ h_2).$$

Полученная *квазигруппа* называется *прямым произведением* квазигрупп G и H.

Аналогично можно определить прямое произведение групп, полугрупп и т.д.

Теорема 2 (MacNeish 1922)**.** Если квазигруппы G_1, G_2 определяют ортогональные латинские квадраты порядка n, а H_1, H_2 — порядка m, то $G_1 \times H_1, G_2 \times H_2$ определяют ортогональные латинские квадраты порядка mn.

Самоортогональные латинские квадраты

Определение 2. Латинский квадрат L называется *самоортогональным,* если транспонированный к L латинский квадрат ортогонален к L.

Теорема 3 (Brayton, Coppersmith, Hoffman 1974)**.** Для любого $n \neq 2, 3, 6$ существует самоортогональный латинский квадрат порядка n.

Мотивировка: составление расписания смешанного турнира по теннису для n супружеских пар таким образом, чтобы:

- каждый джентльмен сыграл по одному разу против каждого джентльмена;
- каждая дама сыграла по одному разу против каждой дамы;

- каждый джентльмен сыграл по одному разу против каждой дамы, кроме своей жены;
- каждый джентльмен сыграл по одному разу в паре с каждой дамой, кроме своей жены.

Пример расписания турнира

Участники
Mr&Mrs Brown
Mr&Mrs Fox
Mr&Mrs Jones
Mr&Mrs Smith

0	3	1	2
2	1	3	0
3	0	2	1
1	2	0	3

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

00	32	13	21
23	11	30	02
31	03	22	10
12	20	01	33

Mr Brown, Mrs Smith	—	Mr Fox, Mrs Jones
Mr Brown, Mrs Fox	—	Mr Jones, Mrs Smith
Mr Brown, Mrs Jones	—	Mr Smith, Mrs Fox
Mr Fox, Mrs Smith	—	Mr Jones, Mrs Brown
Mr Fox, Mrs Brown	—	Mr Smith, Mrs Jones
Mr Jones, Mrs Fox	—	Mr Smith, Mrs Brown

Рекурсивно дифференцируемые квазигруппы

Определение 3. Квазигруппа $(L, \cdot)$ называется *рекурсивно дифференцируемой*, если операция $x * y = y \cdot (x \cdot y)$ задает на L структуру квазигруппы (и тогда эта квазигруппа автоматически ортогональна L).

Теорема 4 (Коусело, Гонсалес, Марков, Нечаев 1998)**.** Для любого $n \neq 2, 6, 14?, 18?, 26?, 42?$ существует рекурсивно дифференцируемая квазигруппа порядка n.

Теорема 5 (Марков, Нечаев, Скаженик, Тверитинов 2008)**.** Существует рекурсивно дифференцируемая квазигруппа порядка 42.

Список литературы

[1] G. Tarry. Le problème des 36 officiérs // C.R. Assoc. France Av. Sci. 1900. Vol.29, n. 2. P.170–203

[2] R. C. Bose, S. S. Shrikhande and E. T. Parker, Further results on the construction of mutually orthogonal latin squares and falsity of Euler's conjecture, Canadian J. Math. 12 (1960), 189–203.

[3] Zhu Lie, A short disproof of Euler's conjecture concerning orthogonal Latin squares, Ars Combinatoria, 14 (1982), 47–55).

[4] А. Е. Малых, В. И. Данилова, Об историческом процессе развития теории латинских квадратов и некоторых их приложениях. Вестник пермского университета, N4 (2010), 95–104

[5] H. F. MacNeish, Euler squares, Ann. Math., 23 (1922), 211–227.

[6] R. K. Brayton, D. Coppersmith, A. J. Hoffman, Self orthogonal Latin Squares for all Orders $n \neq 2, 3, 6$. Bull. Amer. Math. Soc., 80 (1974), 116–119.

[7] Е. Коусело, С. Гонсалес, В. Марков, А. Нечаев, Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы, Дискр. мат., 10 (1998), no. 2, 3–29.

[8] В. Т. Марков, А. А. Нечаев, С. С. Скаженик, Е. О. Тверитинов, Псевдогеометрии с кластерами и пример рекурсивного $[4, 2, 3]_{42}$-кода. Фундаментальная и прикладная математика, т. 14, no. 4 (2008), 563–571.

Литература для более глубокого изучения теории полугрупп и квазигрупп

[1] А. Клиффорд, Г. Престон, Алгебраическая теория полугрупп, т. 1,2. Москва, “Мир”, 1972.

[2] В. Д. Белоусов, Основы теории квазигрупп и луп, Москва, “Наука”, 1967.

[3] И. И. Валуцэ, В. Д. Белоусов, Г. Б. Белявская, Квазигруппы и латинские квадраты, Кишинев, “Штиинца”, 1983.