Алгебра. ПИ. Семинар 15.
Полугруппа, моноид, группа.

Весна 2026. Медведь Никита Юрьевич

1 Задачи для семинара

1.1 Бинарные операции

Обсуждение 1 (Определение бинарной операции и разговор о корректности)**.** *Бинарная операция* на множестве M — это отображение, которое берёт пару элементов множества M (может быть одинаковых, может быть разных, например $2+2$ ничем не хуже, чем $2+3$) и из них получает ещё один (возможно равный одному из них, как в примере $0+2=2$, а возможно какой-то другой). Формально можно говорить об отображении из $M \times M$ в M. Также иногда говорят *алгебраическая операция* или, чтобы подчеркнуть, что всё происходит внутри некоторого множества, *внутренняя операция* (редкий термин).

Иногда встречаются ситуации, когда нам кажется, что задана бинарная операция, но на самом деле что-то не так. Сейчас мы приведём несколько примеров.

Упражнение 2 (Пример 1)**.** $(\mathbb{R}, :)$.

Пояснение: операцию деления чисел мы знаем со школы, но с формальной точки зрения это не совсем операция — ну или не совсем чисел. Ведь на ноль делить нельзя, поэтому не для любой пары определён результат. Однако, на множестве $\mathbb{R} \setminus \{0\}$ эта операция *корректно определена*. Обратите внимание, что затруднение не математического характера, а скорее лингвистического — нас нахально обманули, сославшись на то, что некие слова «деление вещественных чисел» являются операцией (да еще и общеизвестной), а на самом деле никакой операции нет. Тем не менее, для удобства записи мы обычно подобную ситуацию обозначаем словами «операция некорректна» (хотя если операции нет, то кто некорректен-то?).

Упражнение 3 (Пример 2)**.** $(\mathbb{R} \setminus \{0\}, +)$.

Пояснение: нам может казаться, что тут описана операция, но на самом деле это не так. Для пары $(+1, -1)$ результат операции не принадлежит множеству. Такая ситуация часто возникает, когда мы пытаемся операцию, определённую на некотором множестве ($\mathbb{R}$ в данном случае) пытаются ограничить на какое-то его подмножество. Однако, замечу, что такая попытка может быть и успешной: например, на подмножество $\mathbb{Z}$ эта же операция успешно ограничивается. Мы к этому ещё вернёмся.

Упражнение 4 (Пример 3)**.** Пусть M — множество $\{\bar{0}, \bar{1}, \bar{2}\}$ остатков по модулю 3. В качестве операции рассмотрим $a * b = a^b$.

Пояснение: ну а тут-то что не так? Тут тоже есть обман, и тоже в некотором роде нематематический. С чего это мы решили, что понимаем, что означает выражение a^b? Для чисел (особенно натуральных) это хорошо понятно, а для остатков не очень. Можно попробовать воспользоваться той же конструкцией, что для сложения и умножения остатков: считать, что мы берем любого представителя x для a и y для b, находим степень x^y, а потом рассматриваем соответствующий остаток. Однако, легко видеть, что эта конструкция обречена: например, для $\bar{2}^{\bar{2}}$ можно рассмотреть 2^2 или 5^5, но $2^2 = 4 \equiv 1$, $5^5 = 3125 \equiv 2$.

Более того, еще хуже было бы, если бы представители были например 2^{-4}. Можно искусственно рассмотреть только положительных представителей, но этот акт капитуляции уже намекает, что ничего не получится.

В первых двух примерах мы смогли «подправить» операцию так, чтобы смысл появился. Но здесь это по сути невозможно. *(Никакого доказательства невозможности не будет, потому*

что для этого нужно было бы как-то строго определить, что такое «подправить» и «смысл появился».)

Обсуждение 5 (Великие цели и ассоциативность)**.** В чем цель рассмотрения столь абстрактного определения? Представьте, что некто Иванов столь проникся алгебраическими структурами, что изучал их 20 лет и доказал некую мощную «теорему Иванова», которая звучит примерно так: "для любой алгебраической структуры $(M, *)$ выполнено свойство А и свойство Ы". Казалось бы, кому какое дело до такой теоремы. Но оказывается, что дальше (лет через 5-10, как водится) может прийти специалист по, например, вещественным числам и сказать: "Ба! Я как раз не знаю, как доказать свойство Ы для сложения вещественных чисел — а это частный случай данной теоремы. Вот спасибо, порадовали." А может с таким же случаем заглянуть специалист по матрицам, или по многочленам, или физик с тензорными полями (что бы это ни значило). Итак, основная (в некотором роде) цель алгебры — доказывать различные теоремы в максимальной общности, не для одной конкретной структуры, а сразу для большого множества структур.

Увы, таких теорем, насколько я понимаю, более-менее не бывает. Ведь операции могут быть настолько какими угодно, что бóльшая их часть совершенно бессмысленны и у них явно нет никаких общих свойств. Поэтому мы хотим изучать не класс произвольных операций, а какой-то более ограниченный — операции, чем-то похожие на те, которые встречаются в известных нам примерах. Если вспомнить известные нам уже примеры (операции в поле, операции с матрицами, с многочленами, умножение подстановок) — то даже у них операции заметно разные. Например, совершенно естественное свойство $f(a, b) = f(b, a)$ (коммутативность) есть у некоторых из них, но нету у умножения матриц, у умножения подстановок. Но вот свойство *ассоциативности* есть у них у всех. Для всех перечисленных сложений $(a + b) + c = a + (b + c)$, а для всех перечисленных умножений (включая умножение подстановок, которое не очень-то умножение) выполнено $(ab)c = a(bc)$.

Обсуждение 6 (Полугруппы)**.** Итак, для краткости множествам с ассоциативной операцией дано отдельное название — они называются *полугруппы.* Сейчас мы рассмотрим задачи «определить, является ли *** полугруппой». К сожалению, снова возникает вопрос «а как вообще мы будем такое доказывать?» Если вы им еще не задались, можете подумать например, как бы доказать ассоциативность операции сложения банальных натуральных чисел $\mathbb{N}$. Подумав несколько минут вы, вероятно, столкнетесь с проблемой, что для начала иметь бы хотя бы какое-то... *определение* сложения натуральных чисел, а то как с ними работать? Да и хуже того — определение самих натуральных чисел не помешало бы. Возможно, некоторые из вас знают, что дело это гиблое. Грамотное определение натуральных чисел и операций над ними может занимать пару-тройку лекций. Это не входит в наши планы. Поэтому мы воспользуемся методом, который «обладает теми же преимуществами, которыми обладает воровство перед честным трудом» (Б.Рассел). Мы будем считать, что все «естественные» свойства чисел (натуральных, целых, рациональных, вещественных) мы уже откуда-то знаем и будем их использовать без доказательства. Более того, для матриц, комплексных чисел, подстановок мы тоже будем не доказывать свойства заново, а ссылаться, что мы их уже доказывали.

Упражнение 7. Пусть M — множество (произвольных) функций из $\mathbb{R}$ в $\mathbb{R}$ с операцией композиции функций. Докажите, что это полугруппа.

Решение. Давайте вспомним определение композиции (а заодно договоримся, что оно справа налево, а то бывают разные договоренности). По определению $f \circ g$ это такая функция, что из элемента x она сначала делает $g(x)$, а потом из этого $f(g(x))$. Это естественно записать как $(f \circ g)(x) = f(g(x))$. Обратите пожалуйста внимание — это не «очевидно», «следует из свойств композиции» и проч. — это определение композиции.
Давайте начнем решать задачу. Нас просят доказать, что $(f \circ g) \circ h = f \circ (g \circ h)$ для любых функций

f, g, h. Доказать, что функция в левой части равна функции в правой части...А что значит «функции равны»? Это значит — делают одно и то же. Давайте возьмём и представим, будто бы мы подставили в обе части произвольный элемент x и проверим, получается ли одно и то же.[1] В левой части мы получаем $((f \circ g) \circ h)(x)$. Если применить определение композиции, получаем $(f \circ g)(h(x))$. Теперь можно воспринимать $h(x)$ как единое целое, и применить определение композиции к $f \circ g$. Получим $f(g(h(x)))$. Аналогично, для правой части имеем $(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$.

Упражнение 8. Докажите, что $(\mathbb{Z}_n, +)$ — полугруппа. ($\mathbb{Z}_n$ — неформально говоря множество остатков по модулю n, более формальное определение будет дано после обсуждения факторгрупп.)

Решение. Во-первых, требуется показать, что данная операция корректна. Вообще говоря, это следует из общих свойств факторизации, но до этого мы доберемся потом. Давайте разберемся «в лоб». Итак, пусть есть остатки $\overline{x}$ и $\overline{y}$, представленные числами x и y. Результат операции $\overline{x} + \overline{y}$ определяется так: берем число $x + y$ и рассматриваем его остаток $\overline{x+y}$. Что может пойти не так? Вдруг если мы рассмотрим два числа a и b такие, что $\overline{x} = \overline{a}$, $\overline{y} = \overline{b}$, то результат сложения, посчитанный как $\overline{a+b}$, будет отличаться от $\overline{x+y}$. Это будет автоматически означать, что наше определение сложения бессмысленно (см., например, упражнение 4). К счастью, проверка тривиальна. Раз $\overline{x} = \overline{a}$, мы имеем $x = a + nk$ для некоторого k. Аналогично, $y = b + nm$ для некоторого m. Тогда $x + y = a + b + n(k + m)$, откуда $\overline{x+y} = \overline{a+b}$, что и требовалось доказать.
Во-вторых, требуется показать, что данная операция ассоциативна. Но это автоматически следует из ассоциативности сложения целых чисел; в таких случаях говорят «наследуется» (ср. наследование в ООП), «спускается на фактор» (станет яснее после обсуждения факторгрупп) или «пропускается через фактор». Мы встретимся ещё с другими такими же ситуациями.

Задача 9 (К54.3 частично)**.** На множестве M определена операция по правилу $x \circ y = x$ («поглощение»). Доказать, что $(M, \circ)$ — полугруппа.

Обсуждение 10 (Нейтральный элемент и моноиды)**.** Каждый помнит, что при действиях с числами особую роль играли 0 при сложении и 1 при умножении (надо сказать, 0 при умножении тоже играет особую роль, но пока что про это мы надолго забудем). Более того, внимательный человек может заметить, что эта роль в некотором роде одна и та же. Эту роль можно сформулировать так: это такой особый элемент, что при применении операции с ним и еще каким-то элементом он не изменяет этот элемент ($0 + a = a, 1 \times b = b$).

Вы легко вспомните из предыдущего материала, что у нас есть и другие примеры таких элементов для некоторых множеств с операциями: нулевая матрица для матриц с операцией сложения, единичная матрица для матриц с операцией умножения, тождественная подстановка для подстановок с операцией умножения подстановок...Именно это мотивирует нас на определение: пусть есть множество M с операцией $\circ$, элемент $e \in M$ называется *нейтральным элементом* если для любого $a \in M$ выполнено $a \circ e = e \circ a = a$.

Надо заметить, что это условие для некоммутативной операции, вообще говоря, распадается на два: $a \circ e = a$ и $e \circ a = a$. Когда выполнено только одно из них, говорят о «правом нейтральном» и «левом нейтральном» элементе соответственно. Чуть далее в примере 14 мы рассмотрим примеры односторонних нейтральных, не являющихся обычными нейтральными элементами. Тем не менее, мы их особенно рассматривать не будем, ограничиваясь обычными двусторонними нейтральными элементами, определёнными в предыдущем абзаце.

[1] Внимательный читатель может заметить, что такое же доказательство уже было при доказательстве ассоциативности произведения подстановок. Действительно, произведение подстановок — это композиция соответствующих функций, так что мы просто повторяем уже пройденное.

Если рассматривать только двусторонние нейтральные, то известна особенно приятная теорема, что если нейтральный элемент и есть, то только один. Ее доказательство столь простое и показательное, что хотя оно и есть в лекциях (и каждом учебнике), я всё равно его повторю: пусть есть два нейтральных элемента e_1 и e_2, тогда $e_1 \circ e_2 = e_2$, так как e_1 нейтральный, но $e_1 \circ e_2 = e_1$, так как e_2 нейтральный. Таким образом, $e_1 = e_2$.

Множества просто с нейтральным элементом нас редко интересуют (так сложилось само собой!), нам обычно хочется, чтобы при этом они также были полугруппами. Такие множества с операцией называют «моноиды».

Упражнение 11. В качестве M возьмем множество слов в некотором алфавите $\mathfrak{A}$. Слово — это конечная последовательность элементов некоторого множества (которое мы и называем алфавитом); элементы могут повторяться, порядок букв важен. Например, если алфавит — это кириллица, то в множестве M будут такие замечательные слова, как «А», «Б», «В», «ЫШГУЦИ», «ЪЪЪЪЪЪЪ» и проч. Также в множество слов принято включать так называемое «пустое слово», которое обычно обозначают Λ. Это слово, не содержащее букв вообще. Определенные таким образом слова — по сути то же, что строки в программировании; пустое слово соответствует строке ''. Из программирования же вы наверняка знакомы и с естественной операцией со словами — конкатенацией (иногда называемой сложением строк). Эта операция состоит в том, что одна строка приписывается к другой, например БУТЕР+БРОД=БУТЕРБРОД. Так вот, пустое слово Λ является нейтральным элементом для этой операции, причем двусторонним (несмотря на некоммутативность операции).

Упражнение 12. Рассмотрим полугруппу натуральных чисел (не с нуля, а нормальных, с единицы) с операцией сложения. Это не моноид. Действительно, если бы было такое e, что для любого a выполнено $a + e = a$, то $e = 0$, но это не элемент множества натуральных чисел. А вот множество натуральных чисел с операцией умножения — вполне себе моноид (но совсем другой!).

Обсуждение 13 (Обратимость)**.** У сложения и умножения чисел (давайте на минутку забудем уточнить, что мы имеем в виду под «числами») есть и еще одно интересное общее свойство — если некто, например, прибавил к некоему неизвестному числу x некое известное число a, можно по числам $x+a$ и a найти число x. Это хорошо известное вам вычитание; вы его знаете так давно, что особенно о нём даже и не задумываетесь. Особенно удобным представляется то, что вычитание можно описать через сложение: вычитание числа a это просто сложение со специальным числом $-a$. То же самое мы имеем и с умножением (умножение на $\frac{1}{a}$). Обобщение этих ситуаций приводит к идее определения элемента, *обратного к* данному элементу a. Самое естественное определение такое: пусть дан моноид M с операцией $\circ$ и нейтральным элементом e, тогда элемент b называют обратным к элементу a, если $a \circ b = e$ и $b \circ a = e$.

Замечание: аналогично ситуации с нейтральным, мы можем рассматривать отдельно правые обратные и левые нейтральные элементы. Мы не будем углубляться в эту тему.

С предыдущими свойствами все было просто: практически все интересные нам множества с операциями обладали этими свойствами. К сожалению, с обратимостью все не так. Нередко бывает, что ни у каких элементов нет обратного (например, для $(\mathbb{N}, +)$), или у большинства нет (например, для $(\mathbb{Z}, \times)$ обратный есть только у ± 1), или у большинства есть, но у некоторых нет (например, для $(\mathbb{R}, \times)$ обратный элемент есть у всех, кроме 0, ведь не бывает такого b, что $0 \times b = 1$). Тем не менее, случай, когда у **всех** элементов есть обратный, представляет для нас особый интерес и мы хотим изучить этот случай отдельно.

Задача 14 (К54.2)**.** Пусть S — полугруппа матриц $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$ с операцией умножения матриц.

Найти левые и правые нейтральные элементы, а также элементы, обратимые слева или справа относительно этих нейтральных.

Обсуждение 15 (Группы; К55.1абв)**.** Определение: моноид, в котором у каждого элемента есть обратный, называется *группой*.

Есть набор общеизвестных групп, которые и вам хорошо бы знать. Обычно для них есть обозначения, в которых операция опускается, потому что она и так ясна из объяснения, о каком множестве идет речь (хотя вообще говоря можно придумать много других операций на том же множестве). Во-первых, это $\mathbb{Z} = (\mathbb{Z}, +), \mathbb{Q} = (\mathbb{Q}, +), \mathbb{R} = (\mathbb{R}, +)$ и $\mathbb{C} = (\mathbb{C}, +)$. Во-вторых, это множества чисел с операцией умножения, из которых искусственно удалили ноль, после чего все оставшиеся числа становятся обратимыми: $\mathbb{Q}^\times = (\mathbb{Q}\setminus\{0\}, \times), \mathbb{R}^\times = (\mathbb{R}\setminus\{0\}, \times), \mathbb{C}^\times = (\mathbb{C}\setminus\{0\}, \times)$. В-третьих, это группа остатков: $\mathbb{Z}_n = (\mathbb{Z}_n, +)$ (множество остатков по модулю n с операцией сложения остатков) и мультипликативная группа остатков: $(\mathbb{Z}_n)^\times$, которая устроена так — берут множество всех остатков, взаимно простых с n и операцию умножения.

Упражнение 16 (К55.1г)**.** Является ли группой $(n\mathbb{Z}, +)$?

Упражнение 17 (К55.1е)**.** Является ли группой множество степеней данного вещественного $a \neq 0$ относительно умножения?

Упражнение 18 (К55.1ж)**.** Является ли группой множество всех корней фиксированной степени n из 1 относительно умножения?

Упражнение 19 (К55.1и)**.** Является ли группой множество комплексных чисел с фиксированным модулем r относительно умножения?

Спойлер: ответ зависит от r.

Задача 20 (К55.5б)**.** Образует ли группу относительно композиции множество всех инъективных отображений множества $\{1, 2, \ldots, n\}$?

Задача 21 (К55.5д)**.** Образует ли группу множество всех чётных подстановок (на множестве из n элементов)?

Задача 22 (К55.6а)**.** Образует ли группу множество симметричных матриц (фиксированного порядка $n \times n$) относительно сложения матриц?

2 Домашнее задание

Задача 1 (Из головы 1, +1 внимательность)**.** Зададим на множестве $\mathbb{R}$ операцию $*$ по следующему правилу: $a * b = \ln(a + b)$. Корректно ли задана данная операция?

Задача 2 (Из головы 2, +1 внимательность)**.** Зададим на множестве $\mathbb{R}_{>0}$ положительных чисел операцию $*$ по следующему правилу: $a * b = \ln(a + b)$. Корректно ли задана данная операция?

Задача 3 (Из головы 3, +1 внимательность)**.** Зададим на множестве $\mathbb{R}$ операцию $*$ по следующему правилу: $a * b = \sqrt{a^2 + b^2}$. Корректно ли задана данная операция?

Упражнение 4 (К54.1а. +1 внимательность)**.** Ассоциативна ли операция $*$ на множестве M, если $M = \mathbb{N}, x * y = x^y$?

Замечание: в нашем курсе через $\mathbb{N}$ обозначается множество натуральных чисел, начинающееся с единицы.

Упражнение 5 (К54.1б. +1 внимательность)**.** Ассоциативна ли операция $*$ на множестве M, если $M = \mathbb{N}, x * y = \text{НОД}(x, y)$?

Упражнение 6 (К54.1в. +1 внимательность). Ассоциативна ли операция $*$ на множестве M, если $M = \mathbb{N}, x * y = 2xy$?

Упражнение 7 (К54.1г. +1 внимательность). Ассоциативна ли операция $*$ на множестве M, если $M = \mathbb{Z}, x * y = x - y$?

Упражнение 8 (К54.1д. +1 внимательность). Ассоциативна ли операция $*$ на множестве M, если $M = \mathbb{Z}, x * y = x^2 + y^2$?

Упражнение 9 (К54.1е. +1 внимательность). Ассоциативна ли операция $*$ на множестве M, если $M = \mathbb{R}, x * y = \sin x \cdot \sin y$?

Задача 10 (Из головы 4, +1 внимательность). Ассоциативна ли операция $\circ$ на множестве M, если $M = \{(ij) \mid i, j \in \{1, 2, \ldots, n\}, i \neq j\}$ — множество транспозиций, $x \circ y$ — композиция подстановок (умножение подстановок)?

Упражнение 11 (+1 знания, +2 внимательность). Пусть есть левый нейтральный и правый нейтральный. Докажите, что это на самом деле один и тот же элемент.

Задача 12 (К54.4, +1 внимательность). Пусть M — произвольное непустое множество. На множестве M^2 определена операция по правилу $(x, y) \circ (z, t) = (x, t)$. Является ли M^2 полугруппой относительно такой операции? Существует ли в M^2 нейтральный элемент?

Подсказка: рассмотрите случай, когда в M ровно один элемент, отдельно.

Задача 13 (К55.5а, +1 внимательность, +1 знания). Образует ли группу относительно композиции множество всех отображений множества $\{1, 2, \ldots, n\}$?

Задача 14 (К55.5е, +2 внимательность, +1 знания). Образует ли группу множество всех нечётных подстановок (на множестве из n элементов) относительно операции композиции подстановок?

Задача 15 (К55.5к, +2 знания, +1 грубая сила). Образует ли группу относительно операции композиции подстановок множество подстановок (записанных в цикловой записи):

$$\{id, (12)(34), (13)(24), (14)(23)\}?$$

Задача 16 (К55.6б, +1 внимательность, +1 знания). Образует ли группу множество всех симметричных матриц порядка 2×2 относительно умножения матриц?

Задача 17 (К55.6г, +3 знания). Образует ли группу множество всех невырожденных матриц (фиксированного порядка $n \times n$) относительно умножения матриц?

Задача 18 (К54.3, +2 внимательность). На множестве M определена операция по правилу $x \circ y = x$ («поглощение»). Докажите, что $(M, \circ)$ — полугруппа. Что можно сказать о нейтральных и обратимых элементах этой полугруппы? В каких случаях она является группой?

2.1 Дополнительные задачи базового уровня (не оцениваются)

Следующие задачи просто плохо влезли в материал, но они не то чтобы сложнее предыдущих. Они все запросто могут встретиться, например, на контрольной, поэтому решить их довольно полезно.

Задача 19. Все пропущенные здесь пункты задач 55.5 и 55.6, кроме 55.6но.

Задача 20 (К55.3, +1 терпение). Доказать, что множество $2^M = \mathcal{P}(M)$ всех подмножеств непустого множества M является группой относительно операции симметрической разности подмножеств:

$$A \triangle B = (A \cap \overline{B}) \cup (B \cap \overline{A}).$$

Задача 21 (К55.5л, +2 грубая сила). Образует ли группу множество подстановок (записанных в цикловой записи):

$$\{id, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\}?$$

2.2 Дополнительные задачи повышенной сложности (не оцениваются)

Задача 22 (К55.9, +1 знания, +3 чувство прекрасного, +1 грубая сила, +2 храбрость). Пусть X — множество точек кривой $y = x^3$, пусть l — прямая, проходящая через точки $a, b \in X$ (а в случае если $a = b$, то касательная в этой точке). Пусть c — третья точка пересечения l с кривой X. Пусть m — прямая, проходящая через начало координат O и точку c (а если $c = O$, то касательная в этой точке), а d — третья точка пересечения m и X (если m касается кривой в точке O, то в качестве d возьмём саму O). Тогда определим операцию на точках кривой правилом $a \oplus b = d$.

Доказать, что $(X, \oplus)$ — коммутативная группа.

Примечание: данный сюжет связан с понятием *эллиптической кривой* (не имеет прямого отношения к эллипсу!), что в свою очередь интересно для разных разделов математики, но в частности имеет очень важные приложения в криптографии. Грубо говоря, некоторым похожим образом можно определить операцию, которая будет сложно устроена, и это по некоторым причинам полезно для нужд криптографии.

Задача 23 (К55.10, +1 знания, +2 чувство прекрасного, +2 грубая сила, +1 храбрость). Доказать, что множество функций вида

$$y = \frac{ax + b}{cx + d},$$

где $a, b, c, d \in \mathbb{R}$ и $ad - bc \neq 0$ является группой относительно операции композиции функций.