Алгебра. ПИ. Семинар 16.
Подгруппы. Порядок. Изоморфизм.

Весна 2026. Медведь Никита Юрьевич

1 Задачи для семинара

Обсуждение 1 (Мультипликативная нотация)**.** Как видим, группы могут быть очень и очень разными множествами с разными операциями. Далее мы планируем рассматривать разные утверждения вида «пусть дана произвольная группа G с операцией…» Возникает вопрос, как обозначить произвольную операцию. Довольно логично использовать какой-нибудь редкий значок, часто используют $a \circ b$ или $a * b$, но я буду придерживаться другой традиции, при которой произвольную операцию обозначают так же, как умножение: при помощи точки $a \cdot b$ или опуская точку ab.

Одно из удобств такой нотации в том, что мы «бесплатно» получаем обозначение для $\underbrace{a \cdot a \cdot \dots \cdot a}_{n}$ — в качестве обозначения можно взять a^n. Обратите внимание, что скобки здесь в длинном произведении не нужны, потому что по свойству ассоциативности где бы мы их ни поставили, будет получаться одинаковый результат. Отсюда легко вывести базовые свойства вроде $a^n \cdot a^m = a^{n+m}$; я пропущу их доказательство, но мы будем смело пользоваться тем, что все обычные свойства степеней сохраняются. Обратный элемент принято обозначать a^{-1} по той же причине: этот *значок* подразумевает не степень, а специальное отдельное действие над элементом, но после того как мы его ввели, очень удобно немедленно договориться, что -1-я степень любого элемента будет равна его обратному. Так мы можем ввести отрицательные степени; обратите внимание, что возникают естественные вопросы вроде равны ли $(a^{-1})^2$ и $(a^2)^{-1}$, несложно проверить, что да.

Мы будем обозначать степень через a^n и обратный элемент через a^{-1}, но иногда встречаются ситуации, когда операция — это сложение (чисел, матриц, функций…) В этих случаях мы будем делать исключение и обозначать их na и $-a$ соответственно.

Обсуждение 2 (Порядок элемента)**.** Пусть у вас есть, например, подстановка. Вы можете помнить, что если возвести её в степень, равную НОКу длин всех циклов, то «всё сократится» и получится тождественная подстановка id. Можно заметить, что в этом поведении есть нечто похожее на ситуацию с остатками, известную вам из дискретной математики — если a взаимно просто с m, и начать a возводить в степень по модулю m, то рано или поздно (по теореме Эйлера не позже, чем на $\varphi(m)$-том шаге) получится нейтральный элемент — остаток 1. Менее интересная аналогия — если в группе остатков $\mathbb{Z}_m$ по сложению начать какой-то остаток складывать сам с собой, то тоже рано или поздно получится остаток 0, ведь это заведомо случится, если сложить m раз.

Эти и некоторые другие примеры наталкивают на следующее определение: *порядком* элемента a группы G называется *минимальная натуральная* степень n такая, что $a^n = e$. Это обозначают $\operatorname{ord} a = n$, а если нужно подчеркнуть, в какой группе дело происходит, то $\operatorname{ord}_G a = n$.

Заметим, что такого n может вообще не существовать. Например, в группе $\mathbb{Z}$ если взять какое-нибудь ненулевое число и начать с собой складывать: $4 + 4 + 4 + 4 + 4 + \dots$, то ноль всё никак не получается и не получается. В такой ситуации мы говорим, что порядок бесконечен: $\operatorname{ord}_{\mathbb{Z}} 4 = \infty$.

Упражнение 3 (Пример вычисления)**.** Найдите порядки элементов в группе $\mathbb{Z}_{12}$.

Задача 4 (К 56.7а)**.** Доказать, что в любой группе элементы x и yxy^{-1} имеют одинаковый порядок.

Задача 5 (К 56.11). Найти порядок элемента x^k, если порядок элемента x равен m.

Обсуждение 6 (Подгруппы, циклические подгруппы). Понятие подгруппы, обозначение $H \subseteq G$. Как проверить, является ли подмножество подгруппой? Проверить, что замкнуто относительно операции и относительно взятия обратного; всё остальное следует автоматически.

Примеры подгрупп по сути обсуждались многие в прошлый раз:

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C},$$

$$\{1, -1\} \subseteq \mathbb{Q}^\times \subseteq \mathbb{R}^\times \subseteq \mathbb{C}^\times,$$

$$A_n \subseteq S_n,$$

$$n\mathbb{Z} \subseteq \mathbb{Z},$$

$$SL_n \subseteq GL_n.$$

Обсуждаем конструкцию циклической подгруппы и связь с порядком элемента.

Упражнение 7. Пример: циклические подгруппы в S_3. Циклические подгруппы в $\mathbb{Z}_6$.

Обсуждение 8 (Изоморфизм). Обсуждаем понятие изоморфных групп. Метафора переклеивания ярлычков, метафора присвоения имён.

Задача 9 (К56.26). Построить изоморфизм между $\mathbb{Z}_n$ и $(\sqrt[n]{1}, \cdot)$.

Задача 10 (a la К55.25в). Построить изоморфизм между группой движений треугольника и симметрической группой S_3.

Задача 11 (К55.25а). Привести пример плоской геометрической фигуры, группа движений которой изоморфна $\mathbb{Z}_2$.

Задача 12 (К55.25б). Привести пример плоской геометрической фигуры, группа движений которой изоморфна $\mathbb{Z}_3$.

Задача 13 (К55.25г). Привести пример плоской геометрической фигуры, группа движений которой изоморфна $\mathbb{V}_4$.

Задача 14 (a la К55.36а). Найти в группе матриц $\mathrm{GL}_3(\mathbb{R})$ подгруппу, изоморфную $\mathbb{Z}_3$.

2 Домашнее задание

Задача 1 (+1 внимательность). Какой порядок элемента «ЖЫШЫ» в моноиде слов с операцией конкатенации?

Замечание: вас может смутить, что порядок элемента определялся для групп, но мы нигде обратимостью не пользовались, поэтому то же определение работает и для моноидов.

Задача 2 (К 56.7б, +1 внимательность, +1 чувство прекрасного). Доказать, что в любой группе элементы ab и ba имеют одинаковый порядок.

Подсказка: напрямую почему-то (относительно) плохо доказывается, но легко сводится к пункту а.

Задача 3 (К 56.13, +1 знания). Найти число элементов порядка p^m в группе $\mathbb{Z}_{p^n}$, где p — простое число, а $0 < m \leqslant n$.

Подсказка: найдите сначала число элементов, которые в степени p^m дают нейтральный элемент, потом разберитесь, у каких из них порядок p^m, а у каких меньше; не запутайтесь в аддитивной нотации.

Упражнение 4 (K56.1а, +1 знания). Доказать, что пересечение любого набора подгрупп является подгруппой.

Если сложно для любого набора, докажите хотя бы для любого конечного набора (для этого достаточно доказать для двух подгрупп, далее по индукции).

Упражнение 5 (K56.1б, +1 знания). Доказать, что объединение двух подгрупп является подгруппой только если одна из подгрупп содержится в другой.

Упражнение 6 (K56.16г, +1 внимательность). Найти все циклические подгруппы в циклической группе $\mathbb{Z}_{125}$.

Замечание: на самом деле это в данном случае все подгруппы, других нет. Это будет следовать из теории на лекциях.

Задача 7 (K56.27, +1 внимательность, +1 знания). Какие из следующих циклических подгрупп $\langle g \rangle \subseteq G$, порождённых элементом g, изоморфны?

а) $G = \mathbb{C}^*, g = -\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$;

б) $G = \mathrm{GL}_2(\mathbb{C}), g = \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}$;

в) $G = S_6, g = (32651)$;

г) $G = \mathbb{C}^*, g = 2 - i$;

д) $G = \mathbb{R}^*, g = 10$;

е) $G = \mathbb{C}^*, g = \cos\frac{6\pi}{5} + i \sin\frac{6\pi}{5}$;

ж) $G = \mathbb{Z}, g = 3$?

Подсказка: циклические подгруппы изоморфны тогда и только тогда, когда в них одинаковое количество элементов.

Задача 8 (K56.23, +1 внимательность, +2 знания, +1 чувство прекрасного). Рассмотрим мультипликативную группу вычетов $\mathbb{Z}_{15}^*$, то есть множество остатков по модулю 15, взаимно простых с 15, с операцией умножения остатков. Исследуйте, является ли она циклической (любые нужные вычисления можно делать с калькулятором, хотя при оптимальных действиях это не понадобится).

Задача 9 (по мотивам K56.23, +1 внимательность, +2 знания, +1 чувство прекрасного). Рассмотрим мультипликативную группу вычетов $\mathbb{Z}_{14}^*$, то есть множество остатков по модулю 14, взаимно простых с 14, с операцией умножения остатков. Исследуйте, является ли она циклической (любые нужные вычисления можно делать с калькулятором, хотя при оптимальных действиях это не понадобится).

2.1 Дополнительные задачи повышенной сложности (не оцениваются)

Задача 10 (+1 знания, +2 чувство прекрасного, +1 грубая сила). Найдите изоморфизм между группами $\mathbb{Z}_{15}^*$ и $\mathbb{Z}_{16}^*$.

Комментарий: я думал поставить эту задачу в основную часть, но всё-таки она чуть сложнее, чем мы обычно делаем. Её можно решать многими разными способами; в зависимости от того, насколько хорошо вы понимаете устройство этих групп, будет отличаться, как много вы делаете «вручную», а как много «получается автоматически».

Задача 11 (К56.5, +2 знания, +2 чувство прекрасного, +2 храбрость, +1 внимательность). Доказать, что:

а) элемент $\frac{3}{5} + \frac{4}{5}i$ группы $\mathbb{C}^*$ имеет бесконечный порядок;

б) число $\frac{1}{\pi}\operatorname{arctg}\frac{4}{3}$ иррационально.

Указание 1: если вам хочется использовать лемму Кронекера, она же «лемма о кузнечике» или «лемма о кентавре» — прочтите сначала пункт б. Вы пытаетесь использовать его утверждение без доказательства, так делать нехорошо. Указание 2: рассмотрите число $(3+4i)^n$ и попробуйте определить остатки его вещественной и мнимой части по модулю 5.