

Алгебра, первый курс, третий модуль

Е. Ю. Смирнов

Аннотация. Записки лекций по алгебре для первого курса факультета математики ВШЭ, программа «математика», весна 2018/19 учебного года.

1. Первая лекция, 10 января 2019 г.

1.1. Напоминание: группы, подгруппы... В прошлом модуле уже рассматривалось понятие группы. Напомним его:

ОПРЕДЕЛЕНИЕ 1.1. *Группа* — это множество G , на котором введена бинарная операция $G \times G \rightarrow G$, $(g_1, g_2) \mapsto g_1 \cdot g_2$, обладающая следующими свойствами:

- (1) ассоциативность: $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ для любых элементов $g_1, g_2, g_3 \in G$;
- (2) существование единицы: существует такой элемент $e \in G$, для которого $g \cdot e = e \cdot g = g$ для любого $g \in G$;
- (3) существование обратного: для любого элемента $g \in G$ найдется такой элемент $g^{-1} \in G$, для которого $g \cdot g^{-1} = g^{-1} \cdot g = e$.

Эту операцию мы обычно будем называть *умножением*. Знак умножения часто будет просто опускаться. Впрочем, иногда мы будем говорить об *аддитивных* группах, операцией в которых является сложение, которое мы, как обычно, будем обозначать знаком «плюс». В этом случае мы обычно будем говорить не об обратном, а о противоположном элементе, а нейтральный элемент называется не единицей, а нулем.

ОПРЕДЕЛЕНИЕ 1.2. Если в группе G выполнено условие $g_1 \cdot g_2 = g_2 \cdot g_1$ для любых $g_1, g_2 \in G$, то G называется *коммутативной*, или *абелевой* группой.

ПРИМЕР 1.3. *Тривиальная* группа: множество из одного элемента $\{e\}$ с однозначно определенной операцией является группой.

ПРИМЕР 1.4. Пусть R — произвольное кольцо. Тогда с ним связаны его *аддитивная группа* $(R, +)$, состоящая из всех элементов R с операцией сложения, и *мультипликативная группа* $(R^\times, \cdot)$, состоящая из всех *обратимых* элементов из R с операцией умножения. Например, если $R = \mathbb{F}$ — это поле, то $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$, однако для произвольного кольца это, конечно, уже не так.

ПРИМЕР 1.5. Множество биекций $\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ образует группу, которая называется *группой перестановок* и обозначается через S_n .

ПРИМЕР 1.6. Пусть $M \subset \mathbb{R}^n$ — множество в евклидовом пространстве, $\text{Sym } M$ — множество всевозможных движений пространства $\mathbb{R}^n$, переводящих M в себя. Тогда $\text{Sym } M$ является группой, которая называется *группой симметрий* множества M .

Предыдущий пример показывает, что некоторые группы оказываются вложенными в другие, большие группы. Это мотивирует следующее определение:

Вы используете эти записки на свой страх и риск. Никто не гарантирует, что их текст полностью соответствует содержанию лекций. Тем более не гарантируется отсутствие в этом тексте ошибок. Впрочем, о найденных ошибках лучше сообщать автору.

ОПРЕДЕЛЕНИЕ 1.7. Подмножество $H \subset G$ называется *подгруппой* в группе G , если выполнены следующие условия:

- (1) $h_1 h_2 \in H$ для любых $h_1, h_2 \in H$ (замкнутость относительно умножения);
- (2) $h^{-1} \in H$ для любого $h \in H$ (замкнутость относительно взятия обратного);
- (3) $e \in H$.

Ясно, что последнее условие равносильно непустоте H .

ПРИМЕР 1.8. Множество $n\mathbb{Z}$ всех чисел, кратных некоторому натуральному числу n , является подгруппой в (аддитивной) группе $\mathbb{Z}$.

Этот пример важен для нас, т.к. мы можем рассматривать множество $\mathbb{Z}/n\mathbb{Z}$ остатков по модулю n , которые тоже образуют группу (и даже кольцо, хотя это нам сейчас неважно). Постараемся обобщить на произвольную группу и подгруппу понятие «множества остатков». Это понятие — *смежные классы по подгруппе* — уже встречалось в предыдущем модуле.

1.2. Смежные классы. Пусть G — некоторая группа, H — подгруппа в ней. Введем на G следующее отношение эквивалентности: будем говорить, что $g_1 \sim g_2 \pmod H$, если $g_1^{-1}g_2 \in H$.

УПРАЖНЕНИЕ 1.9. Проверьте, что это действительно отношение эквивалентности.

Как и в случае любого отношения эквивалентности, возникает разбиение группы G на классы эквивалентности. Ясно, что класс, содержащий элемент g , будет состоять из всевозможных элементов вида gh , где $h \in H$. Поэтому мы будем обозначать его gH .

Эти классы называются *левыми смежными классами* (по-английски *left cosets*). В частности, сама подгруппа H тоже является левым смежным классом; далее, любые два смежных класса состоят из одинакового числа элементов и либо не пересекаются, либо совпадают. Множество левых смежных классов будем обозначать через G/H . Их число называется *индексом* группы G по подгруппе H .

Отсюда получается уже известная вам

ТЕОРЕМА 1.10 (Лагранж). Пусть G — конечная группа, $H \subset G$ — подгруппа. Тогда $|G| = |H| \cdot |G/H|$. В частности, порядок и индекс подгруппы делят порядок группы.

Заметим, что в нашем определении отношения эквивалентности был произвол: вместо этого мы могли бы объявить эквивалентными такие элементы g_1, g_2 , для которых $g_1 g_2^{-1} \in H$. Это дало бы нам разбиение на *правые смежные классы* вида $Hg = \{hg \mid h \in H\}$.

Ясно, что $H = eH = He$ является и левым, и правым смежным классом. Далее, если группа G коммутативна, то левые смежные классы, очевидно, совпадают с правыми. Однако, как мы увидим, в общем случае это может быть не так.

ПРИМЕР 1.11. Пусть $G = \text{GL}_n(\mathbb{F})$ — группа обратимых матриц над полем $\mathbb{F}$, $H = \text{SL}_n(\mathbb{F})$ — подгруппа матриц с определителем 1. Тогда левые и правые смежные классы совпадают и состоят из матриц с фиксированным определителем; в таком случае множество смежных классов можно отождествить с $\mathbb{F}^\times$. Заметим, что в этом случае группа некоммутативна, но левые и правые смежные классы всё равно совпадают.

ПРИМЕР 1.12. Пусть $G = S_n$, $H = \{\sigma : \sigma(n) = n\} \simeq S_{n-1}$ — подгруппа перестановок, оставляющих на месте последний элемент. Тогда две перестановки лежат в одном левом смежном классе, если

$$\sigma_1^{-1} \sigma_2(n) = n \quad \Leftrightarrow \quad \sigma_1(n) = \sigma_2(n).$$

Условие принадлежности одному правому смежному классу выглядит как

$$\sigma_1 \sigma_2^{-1}(n) = n \quad \Leftrightarrow \quad \sigma_1^{-1}(n) = \sigma_2^{-1}(n).$$

Ясно, что при $n \geq 3$ это *разные* условия, и левые смежные классы не совпадают с правыми.

1.3. Нормальные подгруппы. Факторгруппа.

ОПРЕДЕЛЕНИЕ 1.13. Подгруппа $H \subset G$ называется *нормальной*, если ее левые смежные классы совпадают с правыми: $gH = Hg$ для любого $g \in G$. Обозначение: $H \triangleleft G$.

Ясно, что это эквивалентно тому, что подгруппа H инвариантна относительно *сопряжений*: $g^{-1}Hg = H$ для любого элемента $g \in G$.

УПРАЖНЕНИЕ 1.14. Что происходит с подгруппой из примера 1.12 при ее сопряжениях различными перестановками?

Оказывается, что на множестве левых (они же правые) смежных классов по нормальной подгруппе существует корректно определенная операция умножения, которая наделяет множество G/H структурой группы:

ТЕОРЕМА 1.15. *Отношение сравнимости по модулю подгруппы H согласовано с умножением тогда и только тогда, когда H нормальна в G .*

ДОКАЗАТЕЛЬСТВО. Возьмем какие-нибудь элементы $g_1, g_2 \in G$. Для каждого из них возьмем по сравнимому с ними элементу; они имеют вид g_1h_1 и g_2h_2 соответственно при некоторых $h_1, h_2 \in H$. Согласованность с умножением означает, что элемент g_1g_2 сравним с элементом $(g_1h_1)(g_2h_2)$ по модулю H . Это значит, что

$$(g_1g_2)^{-1}(g_1h_1)(g_2h_2) = g_2^{-1}g_1^{-1}g_1h_1g_2h_2 = g_2^{-1}h_1g_2h_2 \in H.$$

Это равносильно тому, что $g_2^{-1}h_1g_2 \in H$ при любых $g_2 \in G, h_1 \in H$. А это и есть условие того, что подгруппа H нормальна. $\square$

Тем самым, если подгруппа H нормальна, на множестве смежных классов G/H возникают операции умножения и взятия обратного, определенные так:

$$(g_1H)(g_2H) = g_1g_2H; \quad (gH)^{-1} = g^{-1}H.$$

Это задает на G/H структуру группы. Единицей этой группы является элемент $eH = H$. Эта группа называется *факторгруппой* группы G по (нормальной) подгруппе H .

ПРИМЕР 1.16. В примере 1.11 факторгруппа $GL_n(\mathbb{F})/SL_n(\mathbb{F})$ изоморфна мультипликативной группе поля $\mathbb{F}^\times$.

1.4. Гомоморфизмы групп. Ещё одна причина, по которой нормальные подгруппы имеет смысл рассматривать, состоит в том, что они возникают как *ядра гомоморфизмов групп*.

Напомним определение гомоморфизма.

ОПРЕДЕЛЕНИЕ 1.17. Отображение $\varphi: G \rightarrow H$ называется *гомоморфизмом групп*, если $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ для любых $g_1, g_2 \in G$.

УПРАЖНЕНИЕ 1.18. Проверьте, что при гомоморфизме $\varphi(e) = e$ и $\varphi(g)^{-1} = \varphi(g^{-1})$.

У гомоморфизма, как обычно, можно рассмотреть его *образ* (теоретико-множественный) и *ядро*: множество элементов из G , которые переходят в $e \in H$.

ОПРЕДЕЛЕНИЕ 1.19. *Ядро* гомоморфизма φ — это множество элементов $\text{Ker } \varphi \subset G$, определенное так:

$$\text{Ker } \varphi = \{g \in G \mid \varphi(g) = e\}.$$

ОПРЕДЕЛЕНИЕ 1.20. *Образ* гомоморфизма φ — это множество элементов

$$\text{Im } \varphi = \{\varphi(g) \mid g \in G\}.$$

ПРЕДЛОЖЕНИЕ 1.21. *Образ гомоморфизма $\text{Im } \varphi \subset H$ является подгруппой в H . Ядро гомоморфизма $\text{Ker } \varphi \subset G$ является нормальной подгруппой в G .*

ДОКАЗАТЕЛЬСТВО. Проверим, что ядро — нормальная подгруппа, оставив утверждение об образе читателю в качестве упражнения. Сначала проверим, что это подгруппа. Пусть $g_1, g_2 \in \text{Ker } \varphi$. Это значит, что $\varphi(g_1) = \varphi(g_2) = e$. Но тогда $\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2) = e$, то есть $g_1 g_2 \in \text{Ker } \varphi$. Аналогично проверяется, что $\text{Ker } \varphi$ замкнуто относительно взятия обратного. То есть $\text{Ker } \varphi$ — подгруппа.

Проверим, что эта подгруппа нормальна. Пусть $g \in \text{Ker } \varphi$, $a \in G$. Тогда

$$\varphi(a^{-1}ga) = \varphi(a)^{-1}\varphi(g)\varphi(a) = \varphi(a)^{-1}e\varphi(a) = e,$$

то есть $a^{-1}ga \in \text{Ker } \varphi$, что и требовалось. □

E-mail address: `esmirnov@hse.ru`