

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 $G = \mathrm{GL}_n(\mathbb{F})$ — группа обратимых матриц над полем $\mathbb{F}$, $H = \mathrm{SL}_n(\mathbb{F})$ — 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. □

2. Вторая лекция, 15 января 2019 г.**3. Третья лекция, 17 января 2019 г.**

3.1. Прямые произведения. Для начала напомним понятие прямого произведения групп.

ОПРЕДЕЛЕНИЕ 3.1. Группа G раскладывается в *прямое произведение* своих подгрупп $G_1, \dots, G_k$, если:

- (1) каждый элемент $g \in G$ единственным образом представляется в виде произведения $g = g_1 \dots g_k$, где $g_i \in G_i$;
- (2) $g_i g_j = g_j g_i$ при $g_i \in G_i, g_j \in G_j, i \neq j$.

Обозначение: $G = G_1 \times \dots \times G_k$.

Во-первых, из условия (1) (точнее, из единственности такого представления) следует, что $G_i \cap G_j = \{e\}$. Далее, если условие (1) выполнено, то условие (2) равносильно требованию нормальности групп G_i . Докажем это.

ЛЕММА 3.2. Пусть G_1 и G_2 — нормальные подгруппы в G , причем $G_1 \cap G_2 = \{e\}$. Тогда $g_1 g_2 = g_2 g_1$ для любых $g_1 \in G_1, g_2 \in G_2$.

ДОКАЗАТЕЛЬСТВО. Докажем, что $g_1 g_2 g_1^{-1} g_2^{-1} = e$. Действительно, $g_1 g_2 g_1^{-1} g_2^{-1} = (g_1 g_2 g_1^{-1}) g_2^{-1} \in G_2$, т.к. в силу нормальности группы G_2 имеем $g_1 g_2 g_1^{-1} \in G_2$. По той же причине $g_1 g_2 g_1^{-1} g_2^{-1} = g_1 (g_2 g_1^{-1} g_2^{-1}) \in G_1$. Значит, $g_1 g_2 g_1^{-1} g_2^{-1} \in G_1 \cap G_2$, то есть равняется единице. $\square$

Рассмотрим случай двух множителей отдельно.

ПРЕДЛОЖЕНИЕ 3.3. Группа G разлагается в прямое произведение своих подгрупп G_1 и G_2 тогда и только тогда, когда

- (1) G_1 и G_2 — нормальные подгруппы;
- (2) $G_1 \cap G_2 = \{e\}$;
- (3) $G_1 G_2 = G$, т.е. каждый элемент $g \in G$ представляется в виде $g = g_1 g_2$, где $g_1 \in G_1, g_2 \in G_2$.

ДОКАЗАТЕЛЬСТВО. Часть «только тогда» доказана выше. Пусть теперь выполнены условия 1)–3). Тогда по предыдущей лемме $g_1 g_2 = g_2 g_1$ при $g_1 \in G_1, g_2 \in G_2$. Проверим единственность такого представления. Пусть $g_1 g_2 = \tilde{g}_1 \tilde{g}_2$. Тогда $\tilde{g}_1^{-1} g_1 = g_2 \tilde{g}_2^{-1} \in G_1 \cap G_2 = \{e\}$. Поэтому $g_1 = \tilde{g}_1, g_2 = \tilde{g}_2$. $\square$

Выше мы предполагали, что группы G_i — подгруппы в одной и той же группе G . В этой ситуации иногда говорят о *внутреннем* прямом произведении. Можно, наоборот, для заданного набора групп G_i (вообще говоря, не вложенных в какую-то большую группу) построить такую группу G , которая будет раскладываться в прямое произведение своих подгрупп, изоморфных G_i .

ОПРЕДЕЛЕНИЕ 3.4. *Прямым произведением* групп $G_1, \dots, G_k$ называется множество последовательностей $(g_1, \dots, g_k)$, где $g_i \in G_i$, с покомпонентными операциями умножения и взятия обратного. Обозначение: $G_1 \times \dots \times G_k$.

Ясно, что такие операции задают на $G_1 \times \dots \times G_k$ структуру группы, единицей которой является набор $(e, \dots, e)$. Кроме того, каждая из групп G_i вкладывается в $G_1 \times \dots \times G_k$ как подгруппа: $g_i \mapsto (e, \dots, e, g_i, e, \dots, e)$, где неединичный элемент стоит на i -м месте. Тогда $G_1 \times \dots \times G_k$ есть прямое произведение своих подгрупп G_i в смысле первого определения.

ПРИМЕР 3.5. Группа ненулевых комплексных чисел $\mathbb{C}^*$ раскладывается в прямое произведение групп $\mathbb{R}_+ \times U(1)$, где $U(1)$ — группа комплексных чисел единичного модуля. Это не что иное, как представление комплексного числа в тригонометрической форме: $z = r e^{i\varphi}$ (для ненулевого числа это представление единственно).

ПРИМЕР 3.6. Каждое движение плоскости может быть представлено, причем единственным образом, в виде композиции параллельного переноса и ортогонального преобразования (сохраняющего начало координат). Однако это не прямое произведение, т.к., например, подгруппа ортогональных преобразований не является нормальной в группе всех движений (или, иначе говоря, ортогональные преобразования не коммутируют с параллельными переносами). Зато оказывается, что это является разложением в так называемое *полупрямое произведение*, о котором речь пойдёт дальше.

4. Четвертая лекция, 22 января 2019 г.

5. Пятая лекция, 29 января 2019 г.

6. Шестая лекция, 31 января 2019 г.

От абелевых групп вернемся к произвольным группам.

6.1. Автоморфизмы групп.

ОПРЕДЕЛЕНИЕ 6.1. *Автоморфизм* группы — это её изоморфизм на себя.

ПРИМЕР 6.2. Отображение $A \mapsto (A^T)^{-1}$ является автоморфизмом группы матриц.

Все автоморфизмы группы G образуют группу, обозначаемую через $\text{Aut } G$.

Любой элемент $g \in G$ задаёт автоморфизм $a(g) \in \text{Aut } G$ при помощи *сопряжения*: $a(g)x = gxg^{-1}$. Такие автоморфизмы называются *внутренними*, их множество обозначается $\text{Int } G$.

Ясно, что $\text{Int } G$ — подгруппа в $\text{Aut } G$. Эта подгруппа нормальна: для любого автоморфизма $\varphi \in \text{Aut } G$ верно, что $\varphi a(g) \varphi^{-1} = a(\varphi(g))$.

Итак, у нас имеется отображение $G \rightarrow \text{Aut } G$ (каждому элементу группы $g \in G$ сопоставляется внутренний автоморфизм $a(g) \in \text{Aut } G$). Несложно проверить, что это отображение является гомоморфизмом:

$$a(gh)x = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = a(g)a(h)x.$$

Его ядро — это центр $Z(G)$ группы G . По теореме о гомоморфизме $\text{Int } G \cong G/Z(G)$.

ПРИМЕР 6.3. При $n \geq 3$ центр симметрической группы S_n тривиален. Поэтому $\text{Int } S_n \cong S_n$. Можно доказать, что при $n \neq 6$ никаких других автоморфизмов у S_n нет, а при $n = 6$ подгруппа $\text{Int } G \subset \text{Aut } G$ имеет индекс 2.

ПРИМЕР 6.4. Найдём группу $\text{Aut } \mathbb{Z}/n\mathbb{Z}$. Пусть $\varphi \in \text{Aut } \mathbb{Z}/n\mathbb{Z}$, $\varphi(\bar{1}) = \bar{k}$. Тогда

$$\varphi(\bar{\ell}) = \bar{k}\bar{\ell} = \bar{k} \cdot \bar{\ell},$$

где умножение понимается в смысле кольца $\mathbb{Z}/n\mathbb{Z}$. Таким образом, всякий автоморфизм группы $\mathbb{Z}/n\mathbb{Z}$ имеет вид $\varphi_k: \ell \rightarrow k\ell$. Обратно, для любого k отображение $\ell \mapsto k\ell$ является гомоморфизмом группы $\mathbb{Z}/n\mathbb{Z}$ в себя. Значит, гомоморфизм φ_k является автоморфизмом тогда и только тогда, когда k обратимо в кольце $\mathbb{Z}_n$. Поэтому $\text{Aut } \mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})^*$.

6.2. Полупрямое произведение. Понятие внутреннего автоморфизма позволяет переформулировать определение нормальной подгруппы: подгруппа нормальна тогда и только тогда, когда она инвариантна относительно всех внутренних автоморфизмов.

Пусть N — нормальная подгруппа в G , H — произвольная подгруппа. Тогда произведение $NH = \{nh : n \in N, h \in H\}$ является подгруппой. Действительно,

$$\begin{aligned}(n_1h_1)(n_2h_2) &= n_1(h_1n_2h_1^{-1})h_1h_2, \\ (nh)^{-1} &= h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1}.\end{aligned}$$

Кроме того, $NH = HN$.

ОПРЕДЕЛЕНИЕ 6.5. Говорят, что группа G разлагается в *полупрямое произведение* своих подгрупп N и H , если

- (1) N — нормальная подгруппа;
- (2) $N \cap H = \{e\}$;
- (3) $NH = G$.

Обозначение: $G = N \rtimes H$ (иногда используется другой значок: $G = N \ltimes H$).

ЗАМЕЧАНИЕ 6.6. Мнемоническое правило: острие треугольника в значке $\rtimes$ показывает на нормальную подгруппу, и это похоже на запись $N \triangleleft G$.

Как и в случае прямого произведения, свойства 2) и 3) эквивалентны тому, что каждый элемент из G единственным образом представляется в виде произведения элементов из N и H .

ПРИМЕР 6.7. $S_n = A_n \rtimes \langle (12) \rangle$.

УПРАЖНЕНИЕ 6.8. (вариация на тему предыдущего примера). Пусть известно, что $S_n = A_n \rtimes \langle \sigma \rangle$. Что можно сказать о перестановке σ ?

ПРИМЕР 6.9. $S_4 = V_4 \rtimes S_3$, где V_4 — четверная группа Клейна, а S_3 вложена в S_4 как группа перестановок, оставляющих на месте символ 4.

ПРИМЕР 6.10. $\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \rtimes \{\mathrm{diag}(\lambda, 1, \dots, 1) \mid \lambda \in K^*\}$.

6.3. «Внешнее» полупрямое произведение групп. Мы только что определили разложение группы в полупрямое произведение двух своих подгрупп (одна из которых должна быть нормальной). Можно действовать иначе: для двух групп N и H рассмотреть их *внешнее* полупрямое произведение, т.е. построить группу $G = N \rtimes H$ аналогично тому, как это делалось для прямого произведения. Отличие от прямого произведения состоит в том, что для описания полупрямого произведения необходима дополнительная информация — а именно, нужно задать для каждого элемента из H нужно задать автоморфизм $\alpha(h)$ группы N , которым h будет действовать на N . Это соответствие должно быть гомоморфизмом групп $H \rightarrow \mathrm{Aut} N$.

Итак, пусть $N \times H$ — прямое произведение N и H как множеств, т.е. множество пар (n, h) . Пусть также задан гомоморфизм $\alpha: H \rightarrow \mathrm{Aut} N$. Определим на множестве $N \times H$ умножение следующим образом:

$$(n_1, h_1)(n_2, h_2) = (n_1 \alpha(h_1)n_2, h_1 h_2).$$

Обратный элемент к (n, h) будет определяться так:

$$(n, h)^{-1} = (\alpha(h^{-1})n^{-1}, h^{-1}).$$

Тем самым на $N \times H$ будет задана структура группы, которая называется *внешним полупрямым произведением* N и H и обозначается через $N \rtimes_{\alpha} H$. При этой конструкции разным гомоморфизмам α будут соответствовать, вообще говоря, неизоморфные группы! Так, например, если α переводит каждый элемент H в тождественный автоморфизм группы N , то полученная группа будет прямым произведением групп N и H .

Обратно, если группа G раскладывается в полупрямое произведение своих подгрупп: $G = N \rtimes H$, то имеется изоморфизм групп $N \rtimes_{\alpha} H \rightarrow G$. (Как при этом будет действовать на N автоморфизм $\alpha(h)$?)

ПРИМЕР 6.11. Рассмотрим две циклические группы: $\langle a \rangle_n \cong \mathbb{Z}/n\mathbb{Z}$ и $\langle b \rangle_m \cong \mathbb{Z}/m\mathbb{Z}$. Гомоморфизм $\langle b \rangle_m \rightarrow \mathrm{Aut} \mathbb{Z}/n\mathbb{Z}$ полностью определяется тем, как действует образующая b . Как обсуждалось на прошлой лекции, $\mathrm{Aut} \mathbb{Z}/n\mathbb{Z} = (\mathbb{Z}/n\mathbb{Z})^*$, поэтому всякий автоморфизм $\mathbb{Z}/n\mathbb{Z}$ есть возведение элемента a в некоторую степень k . Таким образом, задать гомоморфизм $\langle b \rangle_m \rightarrow \mathrm{Aut} \mathbb{Z}/n\mathbb{Z}$ значит задать такое k , что $k^m \equiv 1 \pmod n$. Такое полупрямое произведение обозначается через $\langle a \rangle_n \rtimes_k \langle b \rangle_m$. Вообще говоря, при различных k эти группы могут оказаться изоморфными.

В частности, если $(\varphi(n), m) = 1$, то $k = 1$, и всякий такой гомоморфизм α тривиален, т.е. в этом случае не бывает полупрямых произведений $\mathbb{Z}/n\mathbb{Z}$ и $\mathbb{Z}/m\mathbb{Z}$, отличных от прямого произведения.

ПРИМЕР 6.12. Рассмотрим группу $\langle a \rangle_n \rtimes_{-1} \langle b \rangle_2$. Она задаётся соотношениями соотношениями $a^n = b^2 = 1$ и $bab^{-1} = a^{-1}$. Поэтому это группа самосовмещений n -угольника.

7. Седьмая лекция, 5 февраля 2019 г.

7.1. Коммутант. Пусть $x, y \in G$ — два элемента группы. Их *коммутатором* называется элемент $(x, y) = xyx^{-1}y^{-1}$. Очевидны следующие свойства коммутатора:

- (1) $(x, y) = e$ тогда и только тогда, когда x и y коммутируют.
- (2) $(x, y)^{-1} = (y, x)$ (обратный к коммутатору элемент снова является коммутатором).

Напротив, произведение двух коммутаторов не обязано быть коммутатором.

Все коммутаторы порождают подгруппу в G , которая называется *коммутантом* группы G (или, реже, её *производной группой*) и обозначается через G' :

$$G' := \langle (x, y) \mid x, y \in G \rangle.$$

Ясно, что $G' = \{e\}$ тогда и только тогда, когда G абелева.

Пусть $\varphi: G \rightarrow H$ — гомоморфизм групп. Поскольку $\varphi((x, y)) = (\varphi(x), \varphi(y))$, то $\varphi(G') \subset H'$. Если φ к тому же является эпиморфизмом, то $\varphi(G') = H'$.

Теперь возьмём в качестве H саму G , а в качестве φ — какой-нибудь её внутренний автоморфизм. Получается, что $\varphi(G') = G'$. Это значит, что G' — подгруппа, инвариантная относительно всех внутренних автоморфизмов. Значит, она нормальна в G .

ТЕОРЕМА 7.1. *Всякая подгруппа $H \subset G$, содержащая G' , нормальна. При этом факторгруппа G/H абелева (в частности, G/G' тоже абелева). Обратно, если H — такая нормальная подгруппа в G , что G/H абелева, то G' содержится в H . Другими словами, G' — наименьшая нормальная подгруппа в G , факторгруппа по которой абелева.*

ДОКАЗАТЕЛЬСТВО. Пусть $H \supset G'$. Пусть $h \in H, g \in G$. Тогда

$$ghg^{-1} = ghg^{-1}h^{-1}h = (g, h) \cdot h \in G' \cdot H \subset H,$$

поэтому $H \triangleleft G$.

Далее, пусть H — нормальная подгруппа в G , и $g_1, g_2 \in G$. Докажем, что g_1H и g_2H коммутируют, т.е. G/H коммутативна, тогда и только тогда, когда $G' \subset H$.

$$(g_1H, g_2H) = g_1Hg_2Hg_1^{-1}Hg_2^{-1}H = g_1g_2g_1^{-1}g_2^{-1}H = (g_1, g_2)H.$$

Если факторгруппа G/H абелева, то $(g_1, g_2)H = eH$, т.е. $(g_1, g_2) \in H$. Обратно, если $(g_1, g_2) \in H$, то из приведенного равенства получаем, что элементы факторгруппы g_1H и g_2H коммутируют. Теорема доказана. $\square$

7.2. Коммутанты некоторых групп. Из курса прошлого семестра вам известно следующее

ПРЕДЛОЖЕНИЕ 7.2. *Группа чётных перестановок A_n порождается тройными циклами (ijk) . При $n \geq 5$ группа A_n порождается парами независимых транспозиций $(ij)(kl)$.*

ПРИМЕР 7.3. $S'_n = A_n$ при $n \geq 3$. Действительно, $S'_n \subset A_n$, т.к. группа $S_3/A_3 = \mathbb{Z}/2\mathbb{Z}$ абелева. Далее, найдём S'_3 . Эта группа содержится в A_3 . Но в A_3 нет никакой меньшей подгруппы, кроме единичной, поэтому S'_3 совпадает со всей A_3 (он отличен от $\{e\}$, т.к. S_3 некоммутативна). A_3 содержит оба 3-цикла (123) и (132) . Поэтому S'_n содержит всевозможные 3-циклы. Поэтому из предложения 7.2 следует, что $S'_n = A_n$.

ПРИМЕР 7.4. $A'_4 = V_4$, где $V_4 = \langle (ij)(kl) \rangle$ — четверная группа Клейна. Действительно, $A_4/V_4 \cong \mathbb{Z}_3$ абелева, т.е. $A'_4 \subset V_4$. Но V_4 не содержит никаких нетривиальных подгрупп, нормальных в A_4 (и вообще V_4 — единственная нормальная подгруппа в A_4 , отличная от единичной и её самой), поэтому $A'_4 = V_4$.

ПРИМЕР 7.5. Предыдущий пример показывает, что при $n \geq 5$ коммутант A'_n содержит все пары независимых транспозиций. Поэтому он совпадает со всей группой A_n .

ЗАМЕЧАНИЕ 7.6. Можно показать, что при $n \geq 5$ группа A_n проста, т.е. не содержит нетривиальных нормальных подгрупп (этот результат принадлежит Эваристу Галуа). Разумеется, для всякой неабелевой простой группы G верно, что $G' = G$.

Вычислим коммутанты групп $GL_n(K)$ и $SL_n(K)$. Для этого нам понадобится следующее утверждение.

ПРЕДЛОЖЕНИЕ 7.7. *Группа $SL_n(K)$ порождается трансвекциями $E + cE_{ij}$ при $i \neq j$, т.е. матрицами элементарных преобразований первого рода (здесь E — единичная матрица, E_{ij} — матричная единица, т.е. матрица, все элементы которой равны нулю, кроме (i, j) -го, который равен 1).*

ЗАДАЧА 7.8. Докажите предложение 7.7.

Докажем, что $GL_n(K)' = SL_n(K)' = SL_n(K)$, в предположении, что поле K содержит более трёх элементов. Во-первых, $GL_n(K)/SL_n(K)$ есть группа скалярных матриц, которая является абелевой, т.е. $GL_n(K)' \subset SL_n(K)$. Далее, можно проверить явно, что

$$\left(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & (\lambda^2 - 1)c \\ 0 & 1 \end{pmatrix}.$$

Поэтому если в K найдётся элемент λ , отличный от 0 и ± 1 , то группа $GL_n(K)'$ будет содержать все трансвекции. Поэтому она совпадает с $SL_n(K)$ в силу предыдущего предложения.

7.3. Разрешимые группы. Определим *высшие коммутанты* $G^{(i)}$ группы G по следующему правилу: $G^{(1)} = G'$, $G^{(i)} = (G^{(i-1)})'$. Получим ряд подгрупп, каждая из которых нормальна в предыдущей:

$$G = G^{(0)} \triangleright G^{(1)} \triangleright \dots \triangleright G^{(k)} \triangleright \dots$$

ОПРЕДЕЛЕНИЕ 7.9. Группа G *разрешима*, если $G^{(k)} = \{e\}$ для некоторого k .

ПРИМЕР 7.10. В предыдущем пункте мы видели, что S_4 разрешима (для неё $S_4^{(3)} = \{e\}$, т.к. $S_4^{(2)} = V_4$ абелева), а при $n \geq 5$ группа S_n уже не является разрешимой.

Справедлива следующая несложная

ТЕОРЕМА 7.11. *Пусть $H \triangleleft G$ — нормальная подгруппа. Группа G разрешима тогда и только тогда, когда H и G/H разрешимы.*

ЗАДАЧА 7.12. Докажите эту теорему.

8. Восьмая лекция, 12 февраля 2019 г.

8.1. Действия групп на множествах. Напомним несколько определений из предыдущего семестра.

ОПРЕДЕЛЕНИЕ 8.1. Говорят, что группа G действует на множестве X (обозначение: $G \curvearrowright X$, раньше ещё часто писали $G : X$), если задано отображение $G \times X \rightarrow X$, $(g, x) \mapsto y = g \circ x$, удовлетворяющее следующим требованиям: $g \circ (g' \circ x) = (gg') \circ x$, и $e \circ x = x$ для любых $g, g' \in G$ и $x \in X$.

Множество $Gx = \{y \in X \mid y = g \circ x\} \subset X$ называется *орбитой* элемента x . Множество элементов группы G , оставляющих x на месте, называется *стабилизатором* элемента x и обозначается $\text{Stab}_G x$ или G_x :

$$\text{Stab}_G x = G_x = \{g \in G \mid g \circ x = x\} \subset G.$$

Очевидно, что это подгруппа в G .

Теорема Лагранжа утверждает, что если группа G конечна, то $|G| = |Gx| \cdot |\text{Stab}_G x|$ для любого элемента $x \in X$.

Если $X = Gx$, то есть все элементы X образуют одну орбиту, действие называется *транзитивным*.

Вот пример важного *нетранзитивного* действия.

ПРИМЕР 8.2. Группа действует на себе сопряжениями: $G \curvearrowright G$, $g \circ h = ghg^{-1}$. Это действие не транзитивно, т.к. $Ge = \{e\}$. Орбита элемента h для этого действия называется его *классом сопряжённости* и обозначается через $C(h)$, а стабилизатор — *централизатором* элемента h и обозначается через $Z(h)$. Ясно, что $Z(h) = \{g \in G \mid gh = hg\}$.

Одноточечные орбиты этого действия суть в точности элементы центра $Z(G)$ (это элементы группы, коммутирующие со всеми элементами).

Для конечных групп теорема Лагранжа утверждает, что $|Z(h)| \cdot |C(h)| = |G|$. В частности, $|C(h)|$ делит $|G|$. Это нам ещё неоднократно пригодится.

8.2. p -группы. Пусть G — конечная группа. Её порядок, как известно, делится на порядок любой подгруппы в G . Можно задать обратный вопрос: для всякого ли делителя $|G|$ найдётся подгруппа $H \in G$ соответствующего порядка? Несложно понять, что ответ будет отрицательным: так, например, группа A_5 имеет порядок 60, а подгруппы порядка 30 в ней нет: если бы такая подгруппа была, она была бы нормальной, а группа A_5 , как известно, проста.

Однако в некоторых случаях — в частности, для делителей числа $|G|$, имеющих вид p^k — подгруппа соответствующего порядка всегда существует. Чтобы доказать это, подробнее изучим группы порядка p^k .

ОПРЕДЕЛЕНИЕ 8.3. Группа G называется *p -группой*, где p — простое число, если $|G| = p^k$.

ТЕОРЕМА 8.4. *Нетривиальная p -группа имеет нетривиальный центр: если $|G| = p^k$, то $Z = Z(G) \neq \{e\}$.*

ДОКАЗАТЕЛЬСТВО. $G \setminus Z$ распадается на классы сопряжённости, содержащие более одного элемента (все одноэлементные классы лежат в центре). Порядок каждого из них $|C(x)|$ делит порядок группы, значит, $|C(x)| \vdots p$. Но $|G| \vdots p$. Поэтому и порядок центра кратен p . А значит, Z нетривиален. $\square$

СЛЕДСТВИЕ 8.5. *Всякая p -группа разрешима.*

ДОКАЗАТЕЛЬСТВО. Индукция по $\log_p |G|$. База очевидна: если $|G| = p$, то $G = \mathbb{Z}/p\mathbb{Z}$. Переход: центр $Z \subset G$ является нормальной абелевой подгруппой в G , в частности, он разрешим. Но G/Z — это p -группа, но уже меньшего порядка (предположение индукции!). Из разрешимости Z и G/Z следует разрешимость G . $\square$

СЛЕДСТВИЕ 8.6. *Всякая группа порядка p^2 абелева.*

ДОКАЗАТЕЛЬСТВО. Предположим, что $|G| = p^2$ и $Z \neq G$. Тогда $|Z| = p$ и $|G/Z| = p$, то есть G/Z — циклическая группа. Пусть aZ — её порождающий элемент. Тогда любой элемент из G представим в виде $a^k z$, где $z \in Z$. Но любые два таких элемента коммутируют — противоречие. $\square$

8.3. Силоские подгруппы. Теорема Лагранжа утверждает, что порядок подгруппы делит порядок группы. Можно поставить обратный вопрос: верно ли, что для всякого числа m , делящего порядок группы G , в G найдется подгруппа порядка m ?

УПРАЖНЕНИЕ 8.7. Докажите это утверждение в предположении, что группа G абелева.

Если же группа G неабелева, это неверно. В качестве простого примера можно привести группу A_5 . Она имеет порядок 60, но при этом в ней не будет подгруппы порядка 30. Действительно, если бы она была, то она была бы нормальной (как подгруппа индекса 2). Но, как мы покажем в следующей лекции, в A_5 нет нормальных подгрупп.

Оказывается, что в некоторых ситуациях «обратная теорема Лагранжа» всё-таки верна. Одна из таких ситуаций описывается теоремами Силова.

Пусть $|G| = p^n m$, причём $(p, m) = 1$.

ОПРЕДЕЛЕНИЕ 8.8. *Силоская p -подгруппа* группы G — это любая её подгруппа порядка p^n .

ТЕОРЕМА 8.9 (первая теорема Силова). *Силоская p -подгруппа существует.*

ДОКАЗАТЕЛЬСТВО. Если группа G абелева, теорема следует из теоремы о структуре конечных абелевых групп: её силоская подгруппа — это $\text{Tors}_p G$. В общем случае воспользуемся индукцией по $|G|$.

Пусть $|G| > 1$. Рассмотрим разбиение G на классы сопряжённых элементов: $G = \bigcup C(x_i)$.

Случай 1: найдётся такой нетривиальный класс $C(x)$, число элементов в котором не делится на p . Тогда $|Z(x)| \nmid p^n$, и в $Z(x)$ по предположению индукции есть подгруппа порядка p^n — она-то и будет силоской подгруппой в G .

Случай 2: такого класса нет. Тогда $|C(x_i)| \nmid p$, и поэтому $|Z| \nmid p$ (рассуждение аналогично доказательству теоремы о нетривиальности центра p -группы). Пускай $|Z| = p^{n_0} m_0$. Выберем в Z силоскую подгруппу Z_1 : порядок Z_1 равен p^{n_0} . В G/Z_1 по предположению индукции существует подгруппа порядка p^{n-n_0} . Её полный прообраз при каноническом эпиморфизме $G \rightarrow G/Z_1$ и будет искомой силоской p -подгруппой. $\square$

ТЕОРЕМА 8.10 (вторая теорема Силова). *Всякая p -подгруппа содержится в некоторой силоской p -подгруппе. Все силоские p -подгруппы сопряжены.*

ДОКАЗАТЕЛЬСТВО. Пусть $S \subset G$ — фиксированная силоская p -подгруппа, $H \subset G$ — произвольная p -подгруппа.

Рассмотрим действие $S_1 \curvearrowright G/S$ на левых смежных классах по S . Число элементов любой нетривиальной H -орбиты делится на p , а число элементов в G/S равно m и поэтому на p не делится. Значит, H имеет в G/S неподвижные точки. Пусть gS — такая точка. Тогда $hgS = gS$ для любого $h \in H$, то есть $H \subset gSg^{-1}$, откуда следует первое утверждение теоремы. Если H силоская подгруппа, то из сравнения порядков групп заключаем, что $H = gSg^{-1}$. $\square$

ТЕОРЕМА 8.11 (третья теорема Силова). *Число силоских подгрупп сравнимо с 1 по модулю p .*

ДОКАЗАТЕЛЬСТВО. Пусть S — силоская подгруппа, $C(S)$ — класс подгрупп, сопряжённых S . По предыдущей теореме это и есть множество всех силоских подгрупп. При действии G на $C(S)$ сопряжениями стабилизатором каждой подгруппы $S' \in C(S)$ служит её нормализатор $N(S')$. Ограничим это действие на S . Тогда $C(S)$ как-то разобьётся на нетривиальные S -орбиты, число элементов в каждой из которых кратно p , и неподвижные

точки. Покажем, что неподвижная точка будет ровно одна — сама подгруппа S . Отсюда и будет следовать утверждение теоремы.

Пусть $S' \in C(S)$ — неподвижная точка. Это значит, что $S \subset N(S')$. Тогда S и S' — силовские подгруппы в $N(S')$, а значит, что они в ней сопряжены. Но S' — нормальная подгруппа в $N(S')$. Поэтому $S = S'$. $\square$

8.4. Применение теорем Силова.

ПРИМЕР 8.12. Пусть $|G| = n$, и p — наименьший простой делитель числа n . Покажем, что всякая подгруппа H индекса p нормальна. Действительно, рассмотрим действие H на левых смежных классах G/H . Число элементов каждой орбиты делит $|H|$, то есть оно либо равно 1, либо не меньше p . Но, поскольку $|G/H| = p$ и действие имеет неподвижную точку eH , то оно тривиально.

ПРИМЕР 8.13. Покажем, что всякая группа G порядка pq , где p и q — различные простые числа, является полупрямым произведением циклических групп порядка p и q . Пусть $p > q$. Тогда силовская p -подгруппа G_p нормальна в силу предыдущего примера. Если G_q — силовская q -подгруппа, то $G_p \cap G_q = \{e\}$, а поэтому $|G_p G_q| = pq = |G|$. Значит, $G = G_p \ltimes G_q$.

ПРИМЕР 8.14. Докажем, что каждая группа порядка 45 абелева. Действительно, пусть n_3 и n_5 — число её силовских 3-подгрупп и 5-подгрупп соответственно. Тогда $n_3 \equiv 1 \pmod 3$ и $n_3 | 5$, откуда $n_3 = 1$. Значит, имеется единственная силовская 3-подгруппа, которая тем самым нормальна. Аналогично из условий $n_5 \equiv 1 \pmod 5$ и $n_5 | 9$ получаем, что силовская 5-подгруппа нормальна и поэтому единственна. Поэтому вся группа будет прямым произведением этих двух подгрупп, следовательно, будет абелевой.

ПРИМЕР 8.15. Докажем, что не существует простых групп порядка 30. Для этого покажем, что в каждой группе G порядка 30 есть нормальная подгруппа. Рассмотрим силовские 5-подгруппы в G . Они все суть циклические подгруппы порядка 5. Ясно, что пересекаться они могут только по единице. Их число, по третьей теореме Силова, даёт остаток 1 от деления на 5. Предположим, что оно больше 1. Тогда оно может равняться только шести, что даст нам 24 элемента порядка 5 в G . Теперь посмотрим на силовские 3-подгруппы. В каждой из них два элемента порядка 3. Если силовская подгруппа не одна, то их не менее 4, что даёт ещё 8 элементов порядка 2. Но в группе всего 30 элементов, что меньше, чем $24 + 8$. Противоречие. Значит, в G есть нормальная подгруппа.

9. Девятая лекция, 14 февраля 2019 г.

Простые группы. Простота A_5 и A_n .

10. Десятая лекция, 19 февраля 2019 г.

Группы симметрий правильных многогранников.

11. Одиннадцатая лекция, 26 февраля 2019 г.

В предыдущей части курса рассматривались вопросы, связанные с делимостью, разложением на множители и т.д. в кольцах целых чисел и многочленов. Наша ближайшая задача — обобщить эти понятия на более широкий класс колец. Для начала напомним определение кольца.

11.1. Кольца, поля, идеалы.

ОПРЕДЕЛЕНИЕ 11.1. *Кольцо* (точнее, коммутативное ассоциативное кольцо с единицей — пока что мы будем рассматривать только такие) — это множество A , снабжённое двумя бинарными операциями, сложением и умножением, удовлетворяющими следующим аксиомам:

- (A1-A4): A является абелевой группой по сложению;
- (M1): умножение коммутативно: $ab = ba$ для любых $a, b \in A$;
- (M2): умножение ассоциативно: $a(bc) = (ab)c$ для любых $a, b, c \in A$;
- (M3): существование единицы: $\exists 1 \in A: \forall a \in A \ 1 \cdot a = a$;
- (D): дистрибутивность: $(a + b)c = ac + bc$

ЗАМЕЧАНИЕ 11.2. Мы не требуем того, что $1 \neq 0$. Однако если единица равна нулю, то кольцо A состоит только из нуля (докажите это!)

ЗАМЕЧАНИЕ 11.3. Если $1 \neq 0$ и выполнена аксиома существования обратного по умножению:

$$(M4): \forall a \in A \ \exists a^{-1} \in A: a \cdot a^{-1} = 1,$$

то такое кольцо называется *полем*.

В дальнейшем буквой $\mathbb{K}$ (от немецкого Körper) мы без дополнительных оговорок будем называть произвольное поле.

ОПРЕДЕЛЕНИЕ 11.4. Пусть A — произвольное кольцо. Подмножество $I \subset A$ называется *идеалом*, если выполнено следующее:

- I1: $\forall x, y \in I \ x + y \in I$;
- I2: $\forall x \in I \ -x \in I$;
- I3: $\forall x \in I, a \in A$ верно, что $ax \in I$.

Первые две аксиомы равносильны тому, что I — подгруппа в A по сложению (в частности, $0 \in I$). Обратите внимание, что в третьей аксиоме требуется замкнутость I по умножению на *все* элементы из A (а не только из I) — это очень существенное ограничение.

В частности, если $I \ni 1$, то $I = A$: единицу можно умножить на любой элемент кольца, и результат будет снова принадлежать I . По той же причине идеал, содержащий любой *обратимый* элемент, совпадает со всем кольцом.

Приведем несколько примеров идеалов.

ПРИМЕР 11.5. В любом кольце есть два тривиальных идеала: нулевой (состоящий из одного нуля) и всё кольцо. Впрочем, некоторые авторы предпочитают считать, что $I \neq A$, и всё кольцо, таким образом, идеалом не считается — но это вопрос терминологический.

ПРИМЕР 11.6. Пусть $d \in \mathbb{Z}$. Множество $(d) = \{dm \mid m \in \mathbb{Z}\} \subset \mathbb{Z}$ является идеалом в $\mathbb{Z}$. Чуть позже мы проверим, что всякий идеал в $\mathbb{Z}$ имеет такой вид.

ПРИМЕР 11.7. Пусть $a_1, \dots, a_m \in A$ — некоторое подмножество элементов кольца. *Идеал, порожденный $a_1, \dots, a_m$* , обозначается $(a_1, \dots, a_m)$. Это минимальный по включению идеал, содержащий эти элементы. Ясно, что он имеет вид

$$(a_1, \dots, a_m) = \{a_1x_1 + \dots + a_mx_m \mid x_1, \dots, x_m \in A\}.$$

В предыдущем примере можно было взять любое подмножество в A , не обязательно конечное, и породить им идеал.

Вот ещё один пример, который оказывается очень важным в алгебраической геометрии.

ПРИМЕР 11.8. Пусть $A = \mathbb{K}[x_1, \dots, x_n]$, $S \subset \mathbb{K}^n$ — произвольное подмножество точек в n -мерном аффинном пространстве. Множество функций, равных нулю во всех точках S , образует идеал в A .

11.2. Кольца главных идеалов.

ОПРЕДЕЛЕНИЕ 11.9. Идеал вида $(a) \subset A$, т.е. порождённый одним элементом, называется *главным идеалом*.

ОПРЕДЕЛЕНИЕ 11.10. Целостное кольцо A называется *кольцом главных идеалов*, если все идеалы в нём являются главными.

ПРЕДЛОЖЕНИЕ 11.11. $\mathbb{Z}$ и $\mathbb{K}[x]$ — кольца главных идеалов.

ДОКАЗАТЕЛЬСТВО. Пусть I — ненулевой идеал в $\mathbb{Z}$. Выберем в нём наименьший положительный элемент и обозначим его через d . Докажем, что $I = (d)$. Действительно, пусть $x \in I$. Разделим x на d с остатком: $x = dq + r$. Значит, $r = x - dq$. Оба слагаемых в правой части принадлежат I , значит, $r \in I$. Но $0 \leq r < d$. Поэтому $r = 0$, и x делится на d нацело. Значит, $x \in (d)$.

Случай $\mathbb{K}[x]$ разбирается аналогично, только в качестве d надо взять элемент наименьшей степени. $\square$

УПРАЖНЕНИЕ 11.12. Докажите, что $\mathbb{Z}[x]$ и $\mathbb{K}[x, y]$ не являются кольцами главных идеалов.

11.3. Евклидовы кольца. Неформально говоря, евклидовыми называются кольца, в которых возможно деление с остатком (т.е. алгоритм Евклида).

ОПРЕДЕЛЕНИЕ 11.13. Целостное кольцо A называется *евклидовым*, если в нём существует функция *нормы*, или *высоты*,

$$n: A \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0},$$

удовлетворяющая аксиомам:

E1: $n(xy) \geq n(x)$ для любых $x, y \in A$;

E2: Для любых $x, y \in A$, где $y \neq 0$, найдутся такие $q, r \in A$, что $x = qy + r$, причём либо $n(y) > n(r)$, либо $r = 0$.

УПРАЖНЕНИЕ 11.14. Докажите, что аксиома (E1) на самом деле является избыточной: а именно, если на A существует функция, удовлетворяющая (E2), то из неё можно изготовить функцию (вообще говоря, другую), удовлетворяющую обоим аксиомам.

ПРИМЕРЫ 11.15. Кольца $\mathbb{Z}$, $\mathbb{K}[x]$, $\mathbb{K}[[x]]$ являются евклидовыми. Нормами в них являются соответственно модуль целого числа, степень многочлена и порядок нуля степенного ряда (т.е. номер первого ненулевого коэффициента).

ПРЕДЛОЖЕНИЕ 11.16. Всякое евклидово кольцо является кольцом главных идеалов.

ДОКАЗАТЕЛЬСТВО. Это доказывается аналогично предложению 11.11, при помощи выбора в идеале элемента наименьшей нормы. $\square$

ЗАМЕЧАНИЕ 11.17. Бывают (достаточно экзотические) примеры колец главных идеалов, не являющихся евклидовыми. Таким, например, является кольцо $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. Задача со звёздочкой: докажите это.

11.4. Делимость в кольцах главных идеалов. В этом разделе A — кольцо главных идеалов.

Дадим определение наибольшего общего делителя двух элементов. Привычное определение придётся модифицировать, т.к. в произвольном кольце не совсем понятно, что такое “наибольший”.

ОПРЕДЕЛЕНИЕ 11.18. Пусть $a, b \in A$. *Наибольшим общим делителем* элементов a, b (обозначение: (a, b)) называется такой элемент d , что $d \mid a$ и $d \mid b$, и при этом d делится на любой другой общий делитель элементов a и b .

При таком определении $\gcd$ неясно, что НОД двух элементов вообще существует. Однако это несложно доказать.

ПРЕДЛОЖЕНИЕ 11.19. В кольце главных идеалов у любых двух элементов $a, b \in A$ существует наибольший общий делитель, который выражается через них в виде $d = ax + by$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим идеал $(a, b) \subset A$. Он главный; пусть он порождён элементом d . Это значит, что $d = ax + by$. Докажем, что d — НОД элементов a и b . Действительно, поскольку $a, b \in (a, b) = (d)$, оба этих элемента делятся на d . Пусть e — какой-то другой общий делитель a и b . Поскольку $e \mid a$ и $e \mid b$, получаем, что $e \mid ax + by = d$, что и требовалось. $\square$

ОПРЕДЕЛЕНИЕ 11.20. Если $(a, b) = 1$, то a и b называются *взаимно простыми*.

11.5. Существование и единственность разложения на неприводимые. Введём понятие *ассоциированных* элементов. Два элемента a и b называются ассоциированными (обозначение: $a \sim b$), если $a = bs$, где s обратим. Иными словами, элементы a и b ассоциированы, если идеалы (a) и (b) совпадают.

Простое число — это такое число, которое делится на единицу и на себя. Обобщим это понятие на произвольные кольца.

ОПРЕДЕЛЕНИЕ 11.21. Необратимый ненулевой элемент p кольца A называется *неприводимым*, если его нельзя представить в виде $p = ab$, где a и b — необратимые элементы. Иными словами, всякий делитель неприводимого элемента p ассоциирован либо с 1, либо с p .

Наша ближайшая цель — доказать существование и единственность разложения элемента в произведение неприводимых в кольцах главных идеалов. Сначала докажем следующую лемму.

ЛЕММА 11.22. Пусть A — кольцо главных идеалов, элемент p прост, и $p \mid a_1 \dots a_n$. Тогда $p \mid a_i$ при некотором i .

ДОКАЗАТЕЛЬСТВО. Сначала докажем лемму при $n = 2$. Пусть $p \mid ab$. Допустим, что $p \nmid a$; покажем, что $p \mid b$. Действительно, если p не делит a , то p и a взаимно просты. Напишем линейное выражение их НОД:

$$1 = px + ay.$$

Домножим обе части равенства на b :

$$b = pbx + aby.$$

Правая часть делится на p , так как ab делится на p . Значит, b делится на p .

Случай произвольного n доказывается индукцией по числу сомножителей. $\square$

Отсюда следует единственность разложения элемента кольца главных идеалов на неприводимые множители (с точностью до ассоциированности) — аналог основной теоремы арифметики. Доказательство в этом случае также почти не отличается от случая кольца целых чисел.

ТЕОРЕМА 11.23. Пусть A — кольцо главных идеалов, $a \in A$ — необратимый элемент, причём

$$a = p_1 \dots p_n = q_1 \dots q_m,$$

где p_i, q_i неприводимые. Тогда $n = m$, причём $q_1, \dots, q_m$ можно перенумеровать так, что каждый из q_i станет ассоциированным с соответствующим p_i .

ДОКАЗАТЕЛЬСТВО. Пусть $n \leq m$. Докажем теорему индукцией по n . База: при $n = 1$ доказывать нечего.

Переход. Поскольку $p_1 \mid q_1 \dots q_m$, в силу предыдущей леммы p_1 делит некоторый q_i . Без ограничения общности будем считать, что $i = 1$. Поскольку q_1 также неприводим,

получаем, что $p_1 \tilde{q}_1$. Стало быть, обе части равенства $p_1 \dots p_n = q_1 \dots q_m$ можно сократить на p_1 и получить равенство $p_2 \dots p_n = sq_2 \dots q_m$, где s обратим. Мы свели теорему к случаю $n - 1$ сомножителя, а для него она верна по предположению индукции. $\square$

Теперь докажем *существование* разложения элемента в произведение неприводимых. Это утверждение, которое в $\mathbb{Z}$ очевидно, в случае произвольного кольца главных идеалов приходится доказывать. Кроме того, бывают кольца (не являющиеся кольцами главных идеалов), в которых разложения элемента в произведение неприводимых не существует.

ТЕОРЕМА 11.24. *В кольце главных идеалов каждый ненулевой необратимый элемент может быть разложен на неприводимые множители.*

ДОКАЗАТЕЛЬСТВО. Пусть это не так, и существуют элементы, которые не раскладываются в произведение неприводимых. Назовём их *плохими*. Пусть a_0 — плохой элемент. Тогда он раскладывается в произведение двух необратимых элементов (иначе он был бы простым), причём хотя бы один из сомножителей обязан также быть плохим. Пусть $a_0 = a_1 b_1$, и a_1 плохой. То же самое верно про a_1 : он раскладывается в произведение $a_2 b_2$, где a_2 плохой, и так далее до бесконечности. Мы получили бесконечный ряд элементов

$$a_0, a_1, \dots, a_n, \dots,$$

где $a_i \mid a_{i-1}$. Поэтому имеет место бесконечная строго возрастающая цепочка идеалов

$$(a_0) \subset (a_1) \subset \dots \subset (a_n) \subset \dots$$

Докажем, что в кольце главных идеалов такой цепочки быть не может. Рассмотрим объединение всех идеалов цепочки: $I = \bigcup_{i=0}^{\infty} (a_i)$. Это тоже идеал (почему?). Пусть $I = (d)$ (ведь A — кольцо главных идеалов!). Тогда элемент d лежит в каком-то из (a_n) для некоторого n . Стало быть, $(a_n) = (a_{n+1}) = I$ — противоречие с тем, что цепочка строго возрастает. Стало быть, всякий элемент разлагается на неприводимые множители. $\square$

ЗАМЕЧАНИЕ 11.25. Это же рассуждение проходит для существенно более широкого класса колец: так называемых *нётеровых колец*, в которых каждый идеал конечно порождён. Поэтому в нётеровых кольцах имеет место существование разложения в произведение неприводимых — а вот единственности там может и не быть.

ОПРЕДЕЛЕНИЕ 11.26. Целостное кольцо, в котором каждый ненулевой необратимый элемент разлагается в произведение неприводимых, причём единственным (в смысле теоремы 11.24) образом, называется *факториальным*.

Это определение позволяет объединить теоремы 11.24 и 11.23:

ТЕОРЕМА 11.27. *Всякое кольцо главных идеалов факториально.*

12. Двенадцатая лекция, 28 февраля 2019 г.

12.1. Факторкольца. Ранее мы рассматривали конструкцию факторгруппы по нормальной подгруппе. Для колец есть её непосредственный аналог: факторкольцо по идеалу.

Пусть A — произвольное коммутативное кольцо, $I \subset A$ — идеал. Определим на множестве элементов из A следующее отношение: будем говорить, что $x \equiv y \pmod I$, если $x - y \in I$. Ясно, что это отношение эквивалентности. Классы эквивалентности — это множества вида $x + I = \{x + a \mid a \in I\}$. Иногда мы также будем обозначать класс $x + I$ через $[x]$. Обозначим множество этих классов через A/I .

На классах эквивалентности из A/I можно определить операции сложения и умножения:

$$(x + I) + (y + I) = (x + y) + I; \quad (x + I)(y + I) = xy + I.$$

ПРЕДЛОЖЕНИЕ 12.1. *Заданные таким образом операции определены корректно, т.е. сумма и произведение классов не зависят от выбора их представителей.*

ДОКАЗАТЕЛЬСТВО. Проверим корректность умножения: пусть $x \equiv x' \pmod I$ и $y \equiv y' \pmod I$. Тогда $x' = x + a$, $y' = y + b$, где $a, b \in I$. Поэтому

$$x'y' = (x + a)(y + b) = xy + ay + xb + ab \equiv xy \pmod I,$$

поскольку ay , xb и ab лежат в I . Корректность сложения проверяется аналогично. $\square$

Таким образом, на A/I вводятся операции сложения и умножения, что задаёт на нём структуру кольца. Полученное кольцо называется *факторкольцом* кольца A по идеалу I .

Ясно, что нулём и единицей в A/I являются $0 + I$ и $1 + I$ соответственно.

УПРАЖНЕНИЕ 12.2. Докажите утверждение, обратное к предыдущему предложению: пусть $I \subset A$ — абелева подгруппа по сложению, причем операция умножения, заданная на классах эквивалентности из A/I , определена корректно. Покажите, что I — идеал в A .

12.2. Гомоморфизмы.

ОПРЕДЕЛЕНИЕ 12.3. Пусть A, B — два произвольных кольца. Отображение $f: A \rightarrow B$ называется *гомоморфизмом*, если оно сохраняет операции: а именно,

$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y).$$

Пусть A, B — два произвольных кольца. Отображение $f: A \rightarrow B$ называется *гомоморфизмом*, если оно сохраняет операции: а именно,

$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y).$$

ЗАМЕЧАНИЕ 12.4. В определении мы *не требуем*, чтобы единица переходила в единицу. Так, например, вложение $A \rightarrow A \oplus A$, $a \mapsto (a, 0)$ — гомоморфизм, хотя единицу в единицу он не переводит.

УПРАЖНЕНИЕ 12.5. Докажите, что $\text{Im } f \subset B$ — подкольцо в B , а $\text{Ker } f \subset A$ — идеал в A .

Говорят, что гомоморфизм инъективен/сюръективен/биективен, если он инъективен/сюръективен/биективен как отображение множеств. Такие гомоморфизмы ещё называют соответственно *мономорфизмами*, *эпиморфизмами* и *изоморфизмами*.

ПРИМЕР 12.6. Важный пример гомоморфизма — отображение факторизации $\pi: A \rightarrow A/I$, $\pi(a) = a + I$, где I — произвольный идеал в кольце A . Ясно, что π — эпиморфизм.

Следующая теорема утверждает, что всякий эпиморфизм является отображением факторизации по некоторому идеалу. Аналоги этой теоремы для факторгрупп и факторпространств уже разбирались ранее.

ТЕОРЕМА 12.7 (о гомоморфизме колец). Пусть $f: A \rightarrow B$ — гомоморфизм колец. Тогда $\text{Im } f \simeq A/\text{Ker } f$. Более точно, отображение $\varphi: \text{Im } f \rightarrow A/\text{Ker } f$, при котором $b = f(a) \in \text{Im } f$ отображается в $\pi(a) = a + \text{Ker } f$, есть изоморфизм.

ДОКАЗАТЕЛЬСТВО. Из теоремы о гомоморфизме групп следует, что отображение φ является изоморфизмом абелевых групп. Осталось проверить, что оно сохраняет умножение. Действительно, пусть $f(x) = u$, $f(y) = v$. Тогда $f(xy) = uv$, и

$$\varphi(uv) = \pi(xy) = \pi(x)\pi(y) = \varphi(u)\varphi(v),$$

что и требовалось. $\square$

ПРИМЕР 12.8. Рассмотрим отображение

$$\varphi: \mathbb{K}[x] \rightarrow \mathbb{K}, \quad f(x) \mapsto f(a)$$

вычисления значения многочлена в точке a . Ясно, что это гомоморфизм, причём сюръективный (значение многочлена в данной точке может быть любым). При этом по теореме Безу ядро φ есть

$$\text{Ker } \varphi = \{f \in \mathbb{K}[x] \mid f(a) = 0\} = (x - a).$$

Значит, $\mathbb{K}[x]/(x - a) \cong \mathbb{K}$.

ПРИМЕР 12.9. Рассмотрим теперь отображение вычисления значения *вещественного* многочлена в точке i :

$$\mathbb{R}[x] \rightarrow \mathbb{C}, \quad f(x) \mapsto f(i).$$

Это гомоморфизм, причем также сюръективный (проверьте это!). Кроме того, если $f(i) = 0$, то $f(-i) = f(\bar{i}) = \overline{f(i)} = 0$, поэтому $f(x) : (x - i)(x + i) = x^2 + 1$. Значит,

$$\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}.$$

УПРАЖНЕНИЕ 12.10. Чему изоморфно факторкольцо $\mathbb{R}[x]/(x^2 + px + q)$? (ответ зависит от знака дискриминанта квадратного трёхчлена).

12.3. Китайская теорема об остатках. Сначала напомним понятие прямой суммы колец.

ОПРЕДЕЛЕНИЕ 12.11. *Прямая сумма* $A \oplus B$ колец A и B — это кольцо, элементами которого являются пары (a, b) , где $a \in A$, $b \in B$, а сложение и умножение задаются покомпонентно.

Заметим, что подкольца $\{(a, 0)\} \cong A$ и $\{(0, b)\} \cong B$ являются идеалами в $A \oplus B$.

Вернёмся к кольцам главных идеалов. В них также имеет место аналог китайской теоремы об остатках, который очень просто формулируется и доказывается с помощью понятия факторкольца.

ТЕОРЕМА 12.12 (Китайская теорема об остатках). Пусть A — кольцо главных идеалов, элементы $u, v \in A$ взаимно просты. Тогда

$$A/(uv) \simeq A/(u) \oplus A/(v).$$

ДОКАЗАТЕЛЬСТВО. Поскольку u и v взаимно просты, через них можно линейно выразить единицу:

$$1 = au + bv.$$

Рассмотрим гомоморфизм

$$f: A \rightarrow A/(u) \oplus A/(v), \quad f(x) = (x + (u), x + (v)).$$

Тогда $f(bv) = f(1 - au) = (1, 0)$, $f(au) = f(1 - bv) = (0, 1)$. Следовательно, гомоморфизм f сюръективен. Очевидно, что его ядро — это идеал (uv) . Поэтому требуемое утверждение следует из теоремы о гомоморфизме колец. $\square$

12.4. Максимальные и простые идеалы.

ОПРЕДЕЛЕНИЕ 12.13. Идеал $\mathfrak{m} \subset A$ называется максимальным, если он не содержится ни в каком большем идеале (не совпадающем со всем кольцом).

ОПРЕДЕЛЕНИЕ 12.14. Идеал $\mathfrak{p} \subset A$ называется простым, если для любых двух элементов $a, b \in A$, таких, что $ab \in \mathfrak{p}$, верно, что либо $a \in \mathfrak{p}$, либо $b \in \mathfrak{p}$.

ПРИМЕР 12.15. Простые идеалы в $\mathbb{Z}$ — это идеалы вида (p) , где p простое. Они же являются и максимальными (проверьте это!).

ПРЕДЛОЖЕНИЕ 12.16. 1) Идеал $\mathfrak{p}$ прост тогда и только тогда, когда $A/\mathfrak{p}$ — область целостности.

2) Идеал $\mathfrak{m}$ максимален тогда и только тогда, когда $A/\mathfrak{m}$ — поле.

ДОКАЗАТЕЛЬСТВО. 1) Пусть $\mathfrak{p}$ прост, $ab \in \mathfrak{p}$. Значит, a или b лежат в $\mathfrak{p}$. Рассмотрим их образы при отображении факторизации $A \rightarrow A/\mathfrak{p}$. Получим, что из $[ab] = [0]$ следует, что $[a] = [0]$ или $[b] = [0]$, что и означает, что $A/\mathfrak{p}$ целостное. Обратное утверждение доказывается точно так же.

2) Пусть $\mathfrak{m}$ максимален. Докажем, что всякий ненулевой элемент $[a] \in A/\mathfrak{m}$ обратим. Действительно, $a \notin \mathfrak{m}$. Рассмотрим идеал $a + \mathfrak{m} = \{ax + m \mid x \in A, m \in \mathfrak{m}\}$. Этот идеал содержит $\mathfrak{m}$ и не совпадает с ним (поскольку содержит ещё и a), значит, он совпадает со всем кольцом. Поэтому $1 = ax + m$ для некоторых $x \in A, m \in \mathfrak{m}$. Получаем, что в $A/\mathfrak{m}$ элемент $[x]$ есть $[a]^{-1}$, так как $[1] = [a][x] + [m] = [a][x]$. Обратное утверждение доказывается аналогично (проделайте это!). $\square$

СЛЕДСТВИЕ 12.17. Всякий максимальный идеал прост.

УПРАЖНЕНИЕ 12.18. Приведите пример простого, но не максимального идеала.

Оказывается, что в кольцах главных идеалов верно и обратное к следствию 12.17. Это вытекает из следующей теоремы.

ТЕОРЕМА 12.19. Пусть A — кольцо главных идеалов, $u \in A$ — необратимый элемент. Тогда $A/(u)$ является полем тогда и только тогда, когда u прост.

ДОКАЗАТЕЛЬСТВО. Пусть u не прост: $u = vw$, где v и w необратимы. Тогда в $A/(u)$ получаем: $[v][w] = [u] = [0]$, причём $[v] \neq [0]$ и $[w] \neq [0]$ — значит, $A/(u)$ не область целостности, и тем более не поле.

Обратно, пусть u прост. Это значит, что для любого $x \notin (u)$ верно, что $(x, u) = 1$, следовательно, найдутся a и b , для которых $ax + bu = 1$. Значит, в $A/(u)$ получаем, что $[a][x] = [1]$, т.е. $[a]$ обратим. $\square$

E-mail address: esmirnov@hse.ru