ЛЕКЦИЯ 13

ПОЛУПРЯМЫЕ ПРОИЗВЕДЕНИЯ

ГРУППЫ ИЗ 12 ЭЛЕМЕНТОВ

НЕМНОГО О КОЛЬЦАХ

ИДЕАЛЫ В КОЛЬЦАХ

ПОЛУПРЯМЫЕ ПРОИЗВЕДЕНИЯ ГРУПП

Ранее мы описывали ситуации, когда в группе G есть две подгруппы — N_1 и N_2, такие, что:

- N_1, N_2 обе нормальны в G;
- $N_1 \cap N_2 = \{e\}$;
- $N_1 N_2 = G$ (или $|N_1| \cdot |N_2| = |G|$).

В этом случае оказывалось, что группа G является прямым произведением $N_1 \times N_2$.

Мы сейчас обсудим чуть более общую ситуацию — когда в группе G есть две подгруппы N и H такие, что:

- N нормальна в G;
- $N \cap H = \{e\}$;
- $NH = G$ (или $|N| \cdot |H| = |G|$).

Лемма 1. *При таких условиях любой элемент g группы G однозначно представляется в виде $g = nh$, где $n \in N$, $h \in H$.*

Доказательство. Действительно, если $nh = n'h'$, то ${n'}^{-1} n = h'h^{-1}$, т. е. элемент из группы H равен элементу из группы N. Так как эти группы пересекаются только по единице, мы имеем ${n'}^{-1} n = h'h^{-1} = e$. Отсюда $n = n'$, $h = h'$. □

Лемма 2. *В описанной выше ситуации существует гомоморфизм*

$$\varphi : H \to \operatorname{Aut} N$$

из подгруппы H в группу автоморфизмов группы N такой, что для любых $g = nh$, $g' = n'h'$, $n, n' \in N$, $h, h' \in H$, выполнено

$$gg' = nhn'h' = n(\varphi(h))(n')hh'.$$

Таким образом, группа G полностью определяется подгруппами N, H и гомоморфизмом φ.

Доказательство. Действительно, пусть $g = nh$, $g' = n'h'$. Тогда

$$gg' = nhn'h' = n(hnh^{-1})hh'.$$

Так как подгруппа N нормальна в G, то $hnh^{-1} \in N$. Ясно, что для каждого $h \in H$ отображение, сопоставляющее каждому $n \in N$ элемент $hnh^{-1} \in N$, является автоморфизмом.

Это означает, что мы можем построить отображение $\varphi : H \to \operatorname{Aut} N$, сопоставляющее каждому $h \in H$ соответствующий автоморфизм. Ясно, что это отображение является гомоморфизмом. □

Лемма 3. *Если фиксированы две группы — N и H — и некоторый гомоморфизм $\varphi : H \to \operatorname{Aut} N$, то по ним однозначно (с точностью до изоморфизма) строится группа G, содержащая подгруппы, изоморфные N и H такими, что $N \lhd G$, $N \cap H = \{e\}$, $NH = G$, для всех $g = nh, g'n'h'$*

$$gg' = nhn'h' = n(\varphi(h))(n')hh'.$$

Доказательство. Сначала докажем, что такая группа всегда существует.

Действительно, группу G можно задавать как состоящую из пар (n, h), $n \in N$, $h \in H$, с законом умножения

$$g \cdot g' = (n, h)(n', h') = (n(\varphi(h))(n'), hh').$$

Нам требуется доказать, что такой закон задает группу, то есть проверить ассоциативность, существование единицы и существование обратного.

- *Ассоциативность.*

$$\begin{gathered}((n_1, h_1) \cdot (n_2, h_2)) \cdot (n_3, h_3) = (n_1(\varphi(h_1))(n_2), h_1h_2) \cdot (n_3, h_3) = \\ = (n_1(\varphi(h_1))(n_2)(\varphi(h_1h_2))(n_3), h_1h_2h_3) = \\ = (n_1(\varphi(h_1))(n_2(\varphi(h_2))(n_3)), h_1h_2h_3) = \\ = (n_1, h_1) \cdot (n_2(\varphi(h_2))(n_3), h_2h_3) = (n_1, h_1) \cdot ((n_2, h_2) \cdot (n_3, h_3)).\end{gathered}$$

- *Нейтральный элемент.*

$$(e_N, e_H) \cdot (n, h) = (e_N(\varphi(e_H))(n), e_Hh) = (n, h).$$

С другой стороны,

$$(n, h) \cdot (e_N, e_H) = (n(\varphi(h))(e_N), he_H) = (ne_N, h) = (n, h).$$

- *Наличие обратного.*

$$((\varphi^{-1}(h))(n^{-1}), h^{-1}) \cdot (n, h) =$$
$$= ((\varphi^{-1}(h))(n^{-1})(\varphi(h^{-1}))(n), h^{-1}h) = ((\varphi(h^{-1}))(nn^{-1}), e_H) =$$
$$= ((\varphi(h^{-1}))(e_N), e_H) = (e_N, e_H).$$

С другой стороны,

$$(n, h) \cdot ((\varphi^{-1}(h))(n^{-1}), h^{-1}) =$$
$$= (n \cdot (\varphi(h))(\varphi^{-1}(h))(n^{-1}), hh^{-1}) = (nn^{-1}, e_H) = (e_N, e_H).$$

Очевидно, что N вкладывается в построенную группу G с помощью вложения

$$n \mapsto (n, e_H),$$

являющегося инъективным гомоморфизмом:

$$n_1 \cdot n_2 \mapsto (n_1 \cdot n_2, e_H) = (n_1(\varphi(e_H))(n_2), e_H \cdot e_H) = (n_1, e_H) \cdot (n_2, e_H).$$

Также совершенно очевидно, что образ группы N нормален в G:

$$(n_1, h_1) \cdot (n, e_H) \cdot (n_1, h_1)^{-1} = (n_1, h_1) \cdot (n, e_H) \cdot (*, h_1^{-1}) = (*, e_H).$$

Остальные свойства полупрямого произведения еще более очевидны.

Таким образом, искомое полупрямое произведение всегда существует.

Очевидно, что построенная группа единственна с точностью до изоморфизма, так как ее таблица умножения (как мы видели выше) задается однозначно.

□

ГРУППЫ ИЗ 12 ЭЛЕМЕНТОВ

Теперь поставим задачу найти все группы из 12 элементов.

В группе из 12 элементов число n_2 силовских 2-подгрупп (из четырех элементов) может быть равно единице или трем, а число n_3 силовских 3-подгрупп (из трех элементов) — одному или четырем. Случай $1:1$ означает, что обе подгруппы нормальны, то есть группа G есть прямое произведение своих силовских подгрупп. Так как группы из трех и четырех элементов — абелевы, то мы получи в результате абелеву группу, т.е. одну из двух: $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \simeq \mathbb{Z}_{12}$ или $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$.

Пусть теперь группа не является прямым произведением. Для начала предположим, что $n_2 = 3$, $n_3 = 4$.

В этом случае мы имеем четыре группы из трех элементов, пересекающиеся только по единичному. Таким образом, элементов порядка три должно быть восемь штук. Остается всего 4 элемента, которые могут образовать не более одной группы порядка четыре. Значит, такой случай невозможен.

Остается четыре случая:

- нормальна подгруппа порядка три (изоморфная $\mathbb{Z}_3$), а подгруппа порядка четыре изоморфна $\mathbb{Z}_4$;
- нормальна подгруппа порядка три (изоморфная $\mathbb{Z}_3$), а подгруппа порядка четыре изоморфна $\mathbf{V}_4$;
- нормальна подгруппа порядка четыре, изоморфная $\mathbb{Z}_4$;

• нормальна подгруппа порядка четыре, изоморфная $\mathbf{V}_4$.

В первом случае мы получаем полупрямое произведение группы $\mathbb{Z}_3$ на группу $\mathbb{Z}_4$, т.е. группа $\mathbb{Z}_4$ действует сопряжениями на группу $\mathbb{Z}_3$. Значит, требуется построить (нетривиальный) гомоморфизм группы $\mathbb{Z}_4$ в группу автоморфизмов группы $\mathbb{Z}_3$.

Группа автоморфизмов группы $\mathbb{Z}_3$ изоморфна $\mathbb{Z}_2$ (единственным нетривиальным автоморфизмом является перестановка элементов 1 и 2 в $\mathbb{Z}_3$).

Именно в этот автоморфизм может отобразиться образующий из $\mathbb{Z}_4$.

Таким образом, группа G в данном случае задается следующими образующими и соотношениями:

$$a, b; \qquad a^3 = b^4 = e, \quad bab^{-1} = a^{-1}.$$

Названия у данной группы нет, ее центр состоит из двух элементов: $\{b^2, e\}$, коммутант порождается элементом a.

Во втором случае мы получаем полупрямое произведение группы $\mathbb{Z}_3$ на группу $\mathbf{V}_4$, т.е. группа $\mathbf{V}_4$ действует сопряжениями на группу $\mathbb{Z}_3$. Значит, требуется построить (нетривиальный) гомоморфизм группы $\mathbf{V}_4$ в группу автоморфизмов группы $\mathbb{Z}_3$.

Если обозначить образующий группы $\mathbb{Z}_3$ за a, нетривиальный автоморфизм этой группы - за ξ, образующие группы $\mathbf{V}_4$ — за b и c, то видим, что каждая из образующих b и c отображается либо в ξ, либо в e.

Пусть b отображается в ξ. Тогда если c отображается вξ, то bc отображается в e, а если c отображается в e, то bc отображается в ξ. Оба такие гомоморфизмы дадут в результате изоморфные

группы, так как замена местами c и bc — это автоморфизм группы $\mathbf{V}_4$.

Значит, рассмотрим гомоморфизм

$$b \mapsto \xi, \quad c \mapsto e.$$

Он задаст группу G в виде образующих и соотношений:

$$a, b, c; \qquad a^3 = b^2 = c^2 = e, \quad bc = cb \quad ac = ca, \quad bab^{-1} = a^{-1}.$$

Сразу видно, что подгруппа (порядка два), порожденная элементом c, коммутирует со всеми остальными образующими, т.е. выделяется прямым слагаемым.

Образующие b и a порождают группу $\mathbf{D}_3 = \mathbf{S}_3$. Таким образом, мы получаем группу $\mathbf{D}_3 \oplus \mathbb{Z}_2 = \mathbf{D}_6$.

Во третьем случае мы получаем полупрямое произведение группы $\mathbb{Z}_4$ на группу $\mathbb{Z}_3$, т.е. группа $\mathbb{Z}_3$ действует сопряжениями на группу $\mathbb{Z}_4$. Значит, требуется построить (нетривиальный) гомоморфизм группы $\mathbb{Z}_3$ в группу автоморфизмов группы $\mathbb{Z}_4$.

У группы $\mathbb{Z}_4$ есть (как и у $\mathbb{Z}_3$) лишь один нетривиальный автоморфизм, при котором 1 и 3 меняются местами. Этот автоморфизм имеет порядок два.

Однако мы не можем построить нетривиальный гомоморфизм из группы $\mathbb{Z}_3$ в группу $\mathbb{Z}_2$, поэтому никакого нетривиального полупрямого произведения не может возникнуть.

Во последнем случае мы имеем полупрямое произведение группы $\mathbf{V}_4$ на группу $\mathbb{Z}_3$, т.е. группа $\mathbb{Z}_3$ действует сопряжениями на группу $\mathbf{V}_4$. Значит, требуется построить (нетривиальный) гомоморфизм группы $\mathbb{Z}_3$ в группу автоморфизмов группы $\mathbf{V}_4$.

Как мы помним, группа автоморфизм группы $\mathbf{V}_4$ изоморфна $\mathbf{S}_3$ (можно произвольным образом переставить три неединичных элемента), поэтому нетривиальный гомоморфизм из $\mathbb{Z}_3$ можно устроить, переведя образующий этой группы (обозначим его через a) в "цикл длины три".

В виде образующих и соотношений это будет означать следующее:

$$a, b, c; \qquad a^3 = b^2 = c^2 = e,$$
$$bc = cb, \quad aba^{-1} = c, \quad aca^{-1} = bc, \quad a(bc)a^{-1} = b.$$

Легко доказать, что эта группа изоморфна $\mathbf{A}_4$ ($a \mapsto (123)$, $b \mapsto (12)(34)$, $c \mapsto (14)(23)$).

Таким образом, мы доказали следующую теорему:

Теорема 1 (классификация групп из 12 элементов)**.** *Любая группа из* 12 *элементов изоморфна одной из следующих*:

1) $\mathbb{Z}_12$;
2) $\mathbb{Z}_2 \oplus \mathbb{Z}_6$;
3) $\langle a, b \mid a^3 = b^4 = e,\ bab^{-1} = a^{-1} \rangle$;
4) $\mathbf{D}_6$;
5) $\mathbf{A}_4$.

Никакие две из перечисленных выше групп не изоморфны друг другу.

ОПРЕДЕЛЕНИЕ КОЛЬЦА

Определение 1. Множество R с операциями сложения $+$ и умножения $\cdot$ называется *кольцом*, если относительно сложения это множество является абелевой группой, а сложение с умножением связывает закон дистрибутивности

$$\forall x, y, z \in R \quad x \cdot (y + z) = xy + xz, \quad (x + y)z = xz + yz.$$

Если операция умножения обладает свойством ассоциативности, то кольцо называется *ассоциативным*. В основном, мы будем рассматривать ассоциативные кольца.

Если в кольце R содержится нейтральный по умножению элемент (единица 1), то кольцо называется *кольцом с единицей*.

Если операция умножения в кольце R коммутативна, то кольцо называется *коммутативным*.

Определение 2. Ассоциативное кольцо с единицей, в котором каждый ненулевой элемент имеет обратный (т.е. множество $R \setminus \{0\}$ с операцией умножения является группой) называется *телом*.

Определение 3. Коммутативное тело называется *полем*.

ПРИМЕРЫ КОЛЕЦ

1. Любое из привычных нам полей $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ является кольцом.

2. Самый распространенный пример кольца, не являющегося полем, — кольцо целых чисел $\mathbb{Z}$.

3. Если R — коммутативное ассоциативное кольцо с единицей (поле), то $R[x]$ — кольцо многочленов над R от одной переменной, $R[x_1, x_2, \ldots, x_n]$ — кольцо многочленов над R от многих (коммутирующих переменных). Также можно рассмотреть кольцо многочленов от n некоммутирующих переменных $x_1, \ldots, x_n$. Чтобы не путать его с обычным кольцом многочленов, будем обозначать его через $R\langle x_1, x_2, \ldots, x_n\rangle$.

4. Примером кольца, благодаря которому кольца именно так именуются, является кольцо вычетов по модулю n — $\mathbb{Z}_n$. Данное кольцо состоит из остатков $\{0, 1, 2, \ldots, n-1\}$ от деления на n, операции сложения и умножения проводятся по модулю n. Ясно, что при составном n такое кольцо не будет являться полем:

Если бы кольцо $\mathbb{Z}_n = \mathbb{Z}_{km}$ являлось полем, то в нем были бы делители нуля k и m, а в поле не может быть делителей нуля.

С другой стороны, если n — это простое число, то кольцо $\mathbb{Z}_n$ является полем:

Чтобы это показать, нам достаточно показать, что у каждого ненулевого элемента в $\mathbb{Z}_n$ есть обратный. Действительно, пусть $m \in \mathbb{Z}_n$. Тогда числа

$$m \cdot 1, m \cdot 2, \ldots, m \cdot (n-1)$$

это различные ненулевые элементы в $\mathbb{Z}_n$, так как при $ml = mk \bmod n$ мы получаем $m(l-k)$ делится на n, что невозможно, так как n просто. Значит, среди перечисленных чисел есть единица, то есть элемент m обратим.

5. Если R — это некоторое ассоциативное кольцо с единицей, $n \geqslant 1$, то $\mathbf{M}_n(R)$ — кольцо матриц над R. При $n = 1$ оно совпадает с кольцом R, при $n \geqslant 2$ оно обязательно некоммутативно (например, $E_{12}E_{21} \neq E_{21}E_{12}$) и содержит необратимые ненулевые элементы.

6. Для любого ассоциативного кольца R с единицей можно рассмотреть кольцо *формальных степенных рядов* $R[[x]]$ от одной переменной (также по аналогии вводится кольцо

$$R[[x_1, \ldots, x_n]]$$

формальных степенных рядов от многих переменных). Каждый элемент этого кольца — формальный ряд

$$\sum_{i=0}^{\infty} r_i x^i.$$

Два ряда

$$\sum_{i=0}^{\infty} r_i x^i \text{ и } \sum_{j=0}^{\infty} s_j x^j$$

складываются почленно, а при умножении дают ряд

$$\sum_{n=0}^{\infty} u_n x^n,$$

где

$$u_n = \sum_{k=0}^{n} r_k s_{n-k}.$$

7. Если R и S — два кольца (с какими-то свойствами), то их *прямая сумма* $R \oplus S$ состоит из пар

$$R \oplus S = \{(r, s) \mid r \in R, s \in S\},$$

где сложение умножение определяются покомпонентно.

Аналогично вводится *прямая сумма* произвольного конечного числа колец. Прямая сумма бесконечного числа колец определяется как множество последовательностей (может быть, несчетных) элементов соответствующих колец, где лишь конечное число отлично от нуля. Заметим, что даже если исходные кольца все были кольцами с единицей, то такая прямая сумма единицы не содержит.

Прямое произведение бесконечного числа колец состоит из произвольных последовательностей элементов, где каждый элемент принадлежит соответствующему кольцу. Ясно, что для конечного числа колец прямая сумма и прямое произведение дают одно и то же.

Если кольца изначально все были коммутативны, то их прямое произведение тоже коммутативно. Если все кольца имели единицы, то единицей прямого произведения является последовательность, состоящая из всех единиц соответствующих колец.

ДЕЛИТЕЛИ НУЛЯ, НИЛЬПОТЕНТНЫЕ, ОБРАТИМЫЕ ЭЛЕМЕНТЫ

Определение 4. Элемент $r \neq 0$ ассоциативного кольца R (не обязательно с единицей) называется *левым делителем нуля*, если существует $0 \neq s \in R$ такой, что $rs = 0$. Аналогично вводятся *правый* и двусторонний делители нуля.

1. В поле нет делителей нуля: если $rs = 0$ и $r \neq 0$, то существует обратный элемент $1/r$. Тогда $1/r \cdot rs = 1/r \cdot 0$, откуда $s = 1/r \cdot 0$. Однако $x + x \cdot 0 = x(1 + 0) = x \cdot 1 = x$ откуда , $x \cdot 0 = 0$. Значит, $s = 0$, т.е. в поле нет делителей нуля.

2. В кольце целых чисел нет делителей нуля.

3. Если в кольце R не было делителей нуля, то и в кольце многочленов (от любого числа переменных) над R нет делителей нуля.

4. Как мы уже видели, в кольце вычетов $\mathbb{Z}_n$ есть делители нуля, если n — не просто. Этими делителями являются любые числа в $\mathbb{Z}_n$, которые не взаимно просты с n.

5. В матричном кольце делителями нуля являются все вырожденные матрицы. Действительно, если представить матрицу как линейный оператор на векторном пространстве, то вырожденные матрицы — это ровно те, у которых образом является не все пространство и (или) ядро ненулевое. Пусть оператор A действовал

на пространстве V, $\ker A = U \neq 0$, $\operatorname{Im} A = W \neq V$. Рассмотрим оператор B, образом которого является подпространство U, и оператор C, ядром которого является подпространство W.

Тогда $AB = CA = 0$, т.е. A — и правый, и левый делитель нуля.

6. Если кольцо R не имело делителей нуля, то кольцо рядов тоже не будет их содержать.

7. Прямая сумма (произведение) двух и более колец всегда содержит делители нуля — например, для элемента $(a, 0)$, $a \neq 0$, можно взять $(0, b)$, $b \neq 0$.

Определение 5. Элемент $r \neq 0$ ассоциативного кольца R (не обязательно с единицей) называется *нильпотентным*, если существует $n \in \mathbb{N}$ такое, что $r^n = 0$.

Ясно, что любой нильпотентный элемент является делителем нуля, поэтому если в кольце нет делителей нуля, то нет и нильпотентных элементов. Таким образом, из наших примеров рассмотрим только те, где встречались делители нуля.

1. Рассмотрим кольцо вычетов $\mathbb{Z}_n$, пусть $n = p_1^{k_1} \dots p_m^{k_m}$. Любой делитель нуля в этом кольце должен делиться хоть на какое-то из чисел $p_1, \dots, p_m$. Однако для того, чтобы являться нильпотентным, числу нужно делиться на все $p_1, \dots, p_m$, т.е. оно должно быть равно $p_1 p_2 \dots p_m \cdot q$. Если число n было свободно от квадратов, то нильпотентных элементов в кольце нет.

2. В матричном кольце далеко не каждая вырожденная матрица является нильпотентной. Если, например, мы рассматриваем матрицы над комплексными числами, то нильпотенными матрицами являются те и только те матрицы, у которых все собственные значения равны нулю.

3. В прямой сумме (произведении) двух и более колец нильпотентные элементы есть тогда и только тогда, когда они есть хотя бы в одном из слагаемых колец (сомножителей-колец).

Определение 6. Элемент r ассоциативного кольца R с единицей называется *обратимым слева*, если существует $s \in R$ такой, что $sr = 1$. Аналогично вводится обратимость справа. Элемент r называется *обратимым*, если он обратим слева и справа. В этом случае обратный элемент единственен.

1. В поле, как мы знаем, все ненулевые элементы обратимы.

2. В кольце целых чисел обратимы только ± 1.

3. В кольцах многочленов обратимыми могут быть только константы, так как у многочленов при умножении складываются степени. Соответственно, обратимыми элементами являются обратимые константы кольца R.

4. В кольце вычетов $\mathbb{Z}_n$ обратимыми являются все остатки, взаимно простые с n. Таким образом, в данном кольце каждый элемент либо обратим, либо является делителем нуля.

5. В матричном кольце обратимой является любая невырожденная матрица. Таким образом, как и в предыдущем примере, каждый элемент кольца является или обратимым, или делителем нуля.

6. В кольце рядов $R[[x]]$ обратимыми являются те и только те ряды, у которых обратим коэффициент при нулевой степени.

Доказательство. Пусть у ряда

$$z = \sum_{i=0}^{\infty} r_i x^i$$

r_0 необратим, но у него существует обратный ряд

$$z' = \sum_{j=0}^{\infty} s_j x^j.$$

Тогда, с одной стороны, и произведение должно быть равно ряду 1, с другой стороны, у произведения таких рядов коэффициент при нулевой степени x равен $r_0 s_0$, т.е. r_0 обратим.

Напротив, пусть у ряда

$$z = \sum_{i=0}^{\infty} r_i x^i$$

коэффициент r_0 обратим. Будем искать обратный ряд в общем виде

$$z' = \sum_{j=0}^{\infty} s_j x^j.$$

Тогда мы получим систему уравнений:

$$\begin{cases} 1 & = r_0 s_0, \\ 0 & = r_0 s_1 + r_1 s_0, \\ 0 & = r_0 s_2 + r_1 s_1 + r_2 s_0, \\ \dots & = \dots\dots\dots, \\ 0 & = r_0 s_n + r_1 s_{n-1} + \dots + r_{n-1} s_1 + r_n s_0, \\ \dots & = \dots\dots\dots \end{cases}$$

Мы видим, что $s_0 = r_0^{-1}$ (существует и однозначно определено), $s_1 = (-r_1 s_0) r_0^{-1}$ (также существует и однозначно определено), $s_2 = (-r_1 s_1 - r_2 s_0) r_0^{-1}$, $\dots$, $s_n = (-r_1 s_{n-1} - \dots - r_n s_0) r_0^{-1}$,$\dots$

Таким образом, каждый коэффициент s_i однозначно определяется по коэффициентам r_j и предыдущим коэффициентам $s_0, \dots, s_{i-1}$. Значит, ряд z был обратим. $\square$

7. В прямом произведении любого количества колец с единицей обратимыми являются те и только те элементы, каждая компонента которых обратима в соответствующем кольце.

ИДЕАЛЫ В КОЛЬЦАХ

Идеал в кольце — это аналог нормальной подгруппы в группе.

Определение 7. Идеалом кольца R называется подмножество I этого кольца, которое по сложению является его подгруппой, а по умножению удовлетворяет свойству

$$\forall r \in R \forall a \in I \; ra \in I, ar \in I.$$

Идеал I также называется *двухсторонним идеалом кольца.*

При этом левым идеалом кольца R называется его аддитивная подгруппа I, удовлетворяющая лишь свойству

$$\forall r \in R \forall a \in I \; ra \in I.$$

Аналогично вводится и понятие правого идеала кольца.

1. Понятно, что в кольце всегда есть два тривиальных идеала — $\{0\}$ и все кольцо.

В полях нет нетривиальных идеалов, так как любой ненулевой элемент поля, если он лежит в некотором идеале, будучи умноженным на подходящий элемент поля, дает любой заведомо выбранный элемент этого поля.

2. В кольце целых чисел все идеалы имеют вид $n\mathbb{Z}$ (порождаются одним элементом $n \in \mathbb{Z}$). Таким идеалы (порожденные одним элементом) называются *главными.*

Действительно, рассмотрим некоторый ненулевой идеал I кольца $\mathbb{Z}$ и его минимальный положительный элемент d. Если каждый элемент идеала делится на d, то перед нами идеал $d\mathbb{Z}$.

Если существует элемент $a \in I$, который не делится на d, то разделим a на d с остатком, получив

$$a = qd + r, \quad 0 < d < r.$$

Так как $d \in I$, то $qd \in I$, а значит, $r = a - qd \in I$. Получаем противоречие в выбором d.

Кольцо, в котором все идеалы главные, называется *кольцом главных идеалов*.

3. Кольцо многочленов от одной переменной над полем является кольцом главных идеалов (доказательство полностью аналогично доказательству для целых чисел). Кольцо многочленов над кольцом уже не обязательно является кольцом главных идеалов: в кольце $\mathbb{Z}[x]$ можно взять идеал, состоящих из многочленов с четным совободным членом. Докажите, что он не является главным.

Докажите также, что кольцо многочленов над полем от нескольких переменных тоже не является кольцом главным идеалов.

4. В кольце $\mathbb{Z}_n$ также все идеалы главные, так как вместе с любыми элементами m, k идеал всегда содержит их НОД.