Арунова Маргарита БПМИ2011

Определение. *Кольцо* – множество R, на котором заданы две бинарные операции «+» и «·» (*сложение* и *умножение*), удовлетворяющее следующим условиям (аксиомам кольца):

(а) $(R, +)$ – абелева группа (*аддитивная группа* кольца R)

(б) $\forall a, b \in R$ выполнено:

- $a(b+c) = ab + ac$ (*левая дистрибутивность*)
- $(a+b)c = ac + bc$ (*правая дистрибутивность*)

(в) $\forall a, b, c \in R: \ a(bc) = (ab)c$ (*ассоциативность умножения*)

(г) существует элемент $1 \in R$ (*единица*), такой что $\forall a \in R: \ 1 \cdot a = a \cdot 1 = a$

Замечание. Для всякого кольца R справедливы следующие утверждения:

(а) $\forall a \in R: \ 0 \cdot a = a \cdot 0 = 0$

(б) если $|R| > 1$, то $1 \neq 0$

Определение. Кольцо R называется *коммутативным*, если $ab = ba$ для всех $a, b \in R$.

Определение. Элемент $a \in R$ называется *обратимым*, если для него существует обратный элемент, то есть такой $b \in R$, то $ab = ba = 1$.

Определение. Элемент $a \in R$ называется *левым* (соответственно *правым*) делителем нуля, если $a \neq 0$ и найдётся такой $b \in R$, $b \neq 0$, что $ab = 0$ (соответственно $ba = 0$).

Определение. Элемент $a \in R$ называется *нильпотентным* (или *нильпотент*), если $a \neq 0$ и существует такой $n \in \mathbb{N}$, , что $a^n = 0$.

Замечание. Выполнены следующие утверждения:

(а) все обратимые элементы в R образуют группу по умножению

(б) если R – коммутативно, то все левые и правые делители нуля в R – это одно и то же, поэтому они называются просто *делители нуля*

(в) все делители нуля необратимы

(г) всякий нильпотент является делителем нуля

Определение. Подмножество S кольца R называется *подкольцом*, если для всех $a, b \in S$ выполнено $a + b \in S$ (условие замкнутости S относительно операции в R) и S само является кольцом относительно тех же операций.

Определение. *Полем* называется коммутативное кольцо R, в котором $0 \neq 1$ и всякий ненулевой элемент обратим.

Определение. *Подполем* кольца R называется подкольцо, которое является полем.

Замечание. В поле нет делителей нуля, так как всякий делителей нуля необратим.

Определение. Подмножество I кольца R называется (*двусторонним*) идеалом, если выполнены следующие два условия:

(а) I – подгруппа по сложению

(б) для всех $a \in I$ и $r \in R$ выполнено $ra \in I$ и $ar \in I$

Обозначение: $I \lhd R$

Определение. Несобственные идеалы кольца R – это $I = R$ и $I = \{0\}$. Остальные идеалы являются собственными.

Замечание. В поле нет собственных идеалов.

Пусть R – коммутативное кольцо. Для каждого $a \in R$ рассмотрим множество $(a) = \{ra \mid r \in R\}$.

Определение. Идеал $I \lhd R$ называется главным, если существует такое $a \in R$, что $I = (a)$.

Пусть S – произвольное множество. Рассмотрим $(S) = \{r_1s_1 + \ldots + r_ks_k \mid r_i \in R,\ s_i \in R,\ k \in \mathbb{N}\}$.

Определение. (S) называется идеалом, порождаемым подмножеством S.

Замечание. Пусть $a \in R$ и $(a) \lhd R$ – порождаемый им главный идеал. Верно следующее

(а) $(a) = R \Leftrightarrow a$ – обратим

(б) $(a) = \{0\} \Leftrightarrow a = 0$

Пусть R – кольцо, а I – идеал в R. Рассмотрим факторгруппу $(R/I, +)$. Её элементы – смежные классы по идеалу I, то есть множества $a + I$, $a \in R$. Введём на R/I операцию умножения, полагая $(a + I) \cdot (b + I) = ab + I$ для всех $ab \in R$.

Определение. Кольцо R/I называется *факторкольцом* кольца R по идеалу I.

Определение. Отображение $\varphi : R \to Q$ называется *гомоморфизмом* колец, если выполняется $\varphi(a + b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$ для всех $a, b \in R$

Определение. *Ядро* гомоморфизма φ – это множество $\ker\varphi = \{r \in R \mid \varphi(r) = 0\}$.

Определение. *Образ* гомоморфизма φ – это множество $\operatorname{Im}\varphi = \varphi(R) \subseteq Q$.

Замечание. $\ker\varphi$ – идеал в R, $\operatorname{Im}\varphi$ – подкольцо в Q.

Теорема (о гомоморфизме колец). $R/\ker\varphi \simeq \operatorname{Im}\varphi$.

Задание 1. Найдите все обратимые элементы, все делители нуля и все нильпотентные элементы в кольце матриц следующего вида

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Q} \right\}$$

с обычными операциями сложения и умножения.

1. Единица E в кольце R – это единичная матрица размера 2×2. Она имеет описанный вид и при умножении произвольной матрицы $A \in R$ на неё справа или слева получается A.

2. Найдём все обратимые элементы, то есть матрицы $A \in R$, для которых существуют такие A^{-1}, что $AA^{-1} = A^{-1}A = E$, где E – единица в R.

   Известно, что для матрицы A, у которой $\det A \neq 0$, существует матрица $A^{-1} = \frac{1}{\det A} \cdot \hat{A}$, такая что выполнено $AA^{-1} = A^{-1}A = E$. Значит, матрицы $A \in R$, определитель которых не равен нулю, могут быть обратимыми в R. Проверим, что для каждой невырожденной $A \in R$ матрица $A^{-1} = \frac{1}{\det A} \cdot \hat{A}$ принадлежит R.

   Рассмотрим матрицу $A \in R$ ($\det A \neq 0 \Leftrightarrow a \neq 0,\ c \neq 0$). Найдём A^{-1} по описанной формуле:

$$A^{-1} = \frac{1}{ac} \cdot \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} \frac{1}{a} & \frac{-b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix}$$

   Все коэффициенты A^{-1} лежат в $\mathbb{Q}$, так как $a, c \in \mathbb{Q} \setminus \{0\}, b \in \mathbb{Q}$, а $\mathbb{Q}$ – поле, и матрица A^{-1} имеет описанный для R вид. Получаем, что $A^{-1} \in R$, поэтому матрица $A \in R$ с ненулевым определителем является обратимой в R.

   Покажем, что вырожденные матрицы в R необратимы. Вырожденные матрицы в R имеют вид

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & d \\ 0 & c \end{pmatrix}, \begin{pmatrix} a & d \\ 0 & 0 \end{pmatrix}, \text{ где } a, b, c \in \mathbb{Q} \setminus \{0\},\ d \in \mathbb{Q}$$

   (нулевая матрица не рассматривается, так как $A \cdot 0 = 0 \cdot A = 0 \neq E$ для любой $A \in R$)

   Для первых двух матриц существует ненулевая матрица, при умножении на которую справа получается нулевая матрица, то есть матрицы первых двух видов – левые делители нуля.

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix} = 0,\ t \in \mathbb{Q} \setminus \{0\}$$

$$\begin{pmatrix} 0 & d \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix} = 0,\ t \in \mathbb{Q} \setminus \{0\}$$

   Для последней матрицы существует ненулевая матрица, при умножении на которую слева получается нулевая матрица, значит последняя матрица – правый делитель нуля.

$$\begin{pmatrix} 0 & 0 \\ 0 & t \end{pmatrix} \cdot \begin{pmatrix} a & d \\ 0 & 0 \end{pmatrix} = 0,\ t \in \mathbb{Q} \setminus \{0\}$$

   Делители нуля необратимы. Получаем, что все обратимые элементы в R – невырожденные верхнетреугольные матрицы размера 2×2 с рациональными коэффициентами.

3. Найдем все делители нуля. Делители нуля необратимы, а значит, матрицы, найденные в предыдущем пункте не являются делителями нуля в R. Таким образом, для нахождения делителей нуля можно рассматривать только вырожденные матрицы в R, то есть вида

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & d \\ 0 & c \end{pmatrix}, \begin{pmatrix} a & d \\ 0 & 0 \end{pmatrix}, \text{ где } a, b, c \in \mathbb{Q} \setminus \{0\},\ d \in \mathbb{Q}$$

(нулевая матрица не рассматривается, так как она по определению не делитель нуля)

В предыдущем пункте было показано, что первые два вида матриц – левые делители нуля, а последний вид – правый делитель нуля.

Матрица первого вида не только левый, но и правый делитель:

$$\begin{pmatrix} 0 & t \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = 0,\ t \in \mathbb{Q} \setminus \{0\}$$

Покажем, что матрица второго вида также правый делитель нуля. Для описанной матрицы рассмотрим следующую ненулевую матрицу:

$$\begin{pmatrix} -c & d \\ 0 & 0 \end{pmatrix} \in R$$

При умножении матриц второго вида на эту матриц слева, получим нулевую матрицу:

$$\begin{pmatrix} -c & d \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & -cd + dc \\ 0 & 0 \end{pmatrix} = 0$$

Аналогично покажем, что матрицы третьего вида также и левые делители нуля. Для этого рассмотрим следующую ненулевую матрицу матрицу

$$\begin{pmatrix} 0 & -d \\ 0 & a \end{pmatrix} \in R$$

При умножении матриц второго вида на эту матриц справа, получим нулевую матрицу:

$$\begin{pmatrix} a & d \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -d \\ 0 & a \end{pmatrix} = \begin{pmatrix} 0 & -ad + da \\ 0 & 0 \end{pmatrix} = 0$$

Таким образом все ненулевые вырожденные матрицы в R являются делителями нуля (и правыми, и левыми).

4. Найдём все нильпотентные элементы в R. Нильпотентами могут быть только делители нуля (всякий нильпотент – делитель нуля), поэтому будем рассматривать только делители нуля – матрицы видов

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & d \\ 0 & c \end{pmatrix}, \begin{pmatrix} a & d \\ 0 & 0 \end{pmatrix}, \text{ где } a, b, c \in \mathbb{Q} \setminus \{0\},\ d \in \mathbb{Q}$$

Матрицы первого вида – нильпотенты. При возведении таких матриц во вторую степень получаем:

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}^2 = 0$$

Докажем, что матрицы второго и третьего вида не являются нильпотентами. Для этого покажем, что при любом натуральном n матрицы описанных видов, возведённые в степень n, не равны нулю.

Для второго вида имеем:

$$\begin{pmatrix} 0 & d \\ 0 & c \end{pmatrix}^n = \begin{pmatrix} 0 & d \\ 0 & c \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 0 & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & dc \\ 0 & c^2 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 0 & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} 0 & dc^2 \\ 0 & c^3 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} 0 & d \\ 0 & c \end{pmatrix} =$$
$$= \begin{pmatrix} 0 & dc^{n-1} \\ 0 & c^n \end{pmatrix} = 0$$

Последнее равенство выполняется тогда и только тогда, когда $c = 0$, а $d \in \mathbb{Q}$, но значение c не может быть равным нулю, так как $c \in \mathbb{Q} \setminus \{0\}$.

Для третьего вида имеем:

$$\begin{pmatrix} a & d \\ 0 & 0 \end{pmatrix}^n = \begin{pmatrix} a & d \\ 0 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} a & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a^2 & ad \\ 0 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} a & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a^3 & a^2 d \\ 0 & 0 \end{pmatrix} \cdot \ldots \cdot \begin{pmatrix} a & d \\ 0 & 0 \end{pmatrix} =$$
$$= \begin{pmatrix} a^n & a^{n-1}d \\ 0 & 0 \end{pmatrix} = 0$$

Последнее равенство выполняется тогда и только тогда, когда $a = 0$, а $d \in \mathbb{Q}$, но значение a не может быть равным нулю, так как $a \in \mathbb{Q} \setminus \{0\}$.

Получаем, что нильпотентами являются только матрицы первого вида (заметим, что случаи для второго и третьего вида сводились также к первому виду).

Ответ: – обратимые элементы:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \ a \in \mathbb{Q} \setminus \{0\}, \ b \in \mathbb{Q}, \ c \in \mathbb{Q} \setminus \{0\}$$

– делители нуля:

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & d \\ 0 & c \end{pmatrix}, \begin{pmatrix} a & d \\ 0 & 0 \end{pmatrix}, \ \text{где } a, b, c \in \mathbb{Q} \setminus \{0\}, \ d \in \mathbb{Q}$$

– нильпотентные элементы:

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \ b \in \mathbb{Q} \setminus \{0\}$$

Задание 2. Докажите, что идеал $(x+2, y)$ в кольце $\mathbb{R}[x,y]$ не является главным.

1. Предположим противное, пусть описанный идеал главный, то есть
$$(x+2, y) = \{f_1(x+2) + f_2 y \mid f_1, f_2 \in \mathbb{R}[x,y]\} = (f), \text{ где } f \in \mathbb{R}[x,y]$$

2. Идеалу $(x+2, y)$ принадлежат многочлены вида $x+2$, y. Легко в этом убедится, подставив в описанную формулу $f_1(x+2) + f_2 y$ многочлены $f_1 = 1$, $f_2 = 0$ и $f_1 = 0$, $f_2 = 1$.

   Если идеал является главным и порождается многочленом f, то многочлены $x+2$ и y, лежащие в этом идеале делятся на f в силу того, что $x+2 = g_1 f \in (f)$, $y = g_2 f \in (f)$, где $g_1, g_2 \in \mathbb{R}[x,y]$. Так как f делит многочлены первой степени $\deg f \leqslant 1$.

3. Пусть f имеет степень 1. Так как f делит y, этот многочлен имеет вид $f = Cy$, где $C \in \mathbb{R}$. Но f также делит $x+2$, при этом $x+2 \not\vdots\ Cy$. Таким образом, f не может иметь степень равную 1, значит, $\deg f = 0$.

4. Многочлен f имеет нулевую степень, значит f – константа, $f = C$ и $C \in \mathbb{R}$. Заметим, что $C \neq 0$, так как иначе $(0) = \{0\} \neq (x+2, y)$. Получаем, что элемент f – обратим (существует ему обратный: $f^{-1} = \frac{1}{C}$), а это означает, что $(f) = \mathbb{R}[x,y]$.

5. Получаем противоречие с тем, что $(x+2, y) \neq \mathbb{R}[x,y] = (f)$. Утверждение $(x+2, y) \neq \mathbb{R}[x,y]$ нетрудно доказать, показав, что элемент $1 \in \mathbb{R}[x,y]$ не лежит в $(x+2, y)$.

   Если $1 \in (x+2, y)$, то $1 = f_1(x+2) + f_2 y$, где $f_1, f_2 \in \mathbb{R}[x,y]$. Если последнее равенство выполняется, то оно верно при каждом значении $x, y \in \mathbb{R}$. Но при взятии значения этого многочлена в точке $x = -2$, $y = 0$, получим $1 = f_1 \cdot 0 + f_2 \cdot 0 = 0$ – противоречие.

6. Таким образом, $(x+2, y)$ не представляется в виде (f), $f \in \mathbb{R}[x,y]$, то есть не является главным идеалом в кольце $\mathbb{R}[x,y]$.

Задание 3. При помощи теоремы о гомоморфизме для колец установите следующий изоморфизм $\mathbb{C}[x]/(x^2-x) \simeq \mathbb{C}\oplus\mathbb{C}$, где $\mathbb{C}\oplus\mathbb{C} = \{(z_1, z_2) \mid z_1, z_2 \in \mathbb{C}\}$ – кольцо с покомпонентными операциями сложения и умножения.

1. Найдём 0 в $\mathbb{C}\oplus\mathbb{C}$ – это нейтральный элемент в абелевой группе $(\mathbb{C}\oplus\mathbb{C}, +)$, где «$+$» – операция покомпонентного сложения. Нулём является элемент $(0,0)$. Действительно для любого элемента $(z_1, z_2) \in \mathbb{C}\oplus\mathbb{C}$ выполнено
$$(z_1, z_2) + (0,0) = (z_1+0, z_2+0) = (0+z_1, 0+z_2) = (0,0) + (z_1, z_2) = (z_1, z_2)$$

2. Рассмотрим отображение $\varphi : \mathbb{C}[x] \to \mathbb{C}\oplus\mathbb{C},\ f \mapsto \big(f(0), f(1)\big)$. Покажем, что это отображение – гомоморфизм, то есть удовлетворяет следующим равенствам:
$$\varphi(f+g) = \varphi(f) + \varphi(g) \qquad\qquad \varphi(f\cdot g) = \varphi(f)\cdot\varphi(g)$$
   – Докажем первое равенство:
$$\varphi(f+g) = \big((f+g)(0), (f+g)(1)\big) = \big(f(0)+g(0), f(1)+g(1)\big) = \\ = \big(f(0), f(1)\big) + \big(g(0), g(1)\big) = \varphi(f) + \varphi(g)$$
   – Докажем второе равенство:
$$\varphi(f\cdot g) = \big((f\cdot g)(0), (f\cdot g)(1)\big) = \big(f(0)\cdot g(0), f(1)\cdot g(1)\big) = \\ = \big(f(0), f(1)\big)\cdot\big(g(0), g(1)\big) = \varphi(f)\cdot\varphi(g)$$
   Таким образом, φ – гомоморфизм.

3. Найдём ядро этого гомоморфизма, то есть такие многочлены $f \in \mathbb{C}[x]$, что $\varphi(f) = (0,0)$. Если $f(x)$ лежит в ядре φ, то $f(0) = 0$, $f(1) = 0$. Это означает, что многочлен обращается в 0 при $x = 0$ и $x = 1$ и по следствию теоремы Безу делится на многочлен x и $x-1$.
   Получаем, что если $f \in \ker\varphi$, то $f \,\vdots\, x$ и $f \,\vdots\, x-1$, то есть на $f \,\vdots\, x^2-x$. Многочлены, делящиеся на x^2-x, имеют вид $f(x) = g(x)(x^2-x)$, $g(x) \in \mathbb{C}[x]$. Все такие многочлены лежат в главном идеале (x^2-x) кольца $\mathbb{C}[x]$. Каждый многочлен описанного идеала лежит в ядре, так как в точках $x = 0$ и $x = 1$ он обращается в ноль.
   Таким образом, $\ker\varphi = (x^2-x)$.

4. Найдём образ гомоморфизма. Покажем, φ – сюръекция, то есть $\operatorname{Im}\varphi = \mathbb{C}\oplus\mathbb{C}$. Для каждого элемента $(z_1, z_2) \in \mathbb{C}\oplus\mathbb{C}$ рассмотрим в $\mathbb{C}[x]$ многочлен $f(x) = -z_1(x-1) + z_2 x$. Нетрудно убедиться в выполнении следующих равенств:
$$f(0) = -z_1\cdot(-1) + z_2\cdot 0 = z_1 \\ f(1) = -z_1\cdot 0 + z_2\cdot 1 = z_2$$
   Получаем, что $\varphi(f) = (z_1, z_2)$. Значит φ – сюръективен и $\operatorname{Im}\varphi = \mathbb{C}\oplus\mathbb{C}$.

5. По теореме о гомоморфизме колец имеем:
$$\mathbb{C}[x]/\ker\varphi \simeq \operatorname{Im}\varphi \ \Leftrightarrow\ \mathbb{C}[x]/(x^2-x) \simeq \mathbb{C}\oplus\mathbb{C}$$

Задание 4. Пусть R – коммутативное кольцо и $I \lhd R$. Докажите, что факторкольцо R/I является полем тогда и только тогда, когда идеал $I \neq R$ и I не содержится ни в каком собственном идеале кольца R.

1. Докажем следующее утверждение для факторколец: в R/I элемент $a + I = 0 + I \Leftrightarrow a \in I$.
   - Если элемент $a+I$ – нулевой, то есть он равен множеству $0+I$, то он состоит только элементов идеала, причём из всех.

     Предположим противное, пусть $a \notin I$. Элемент a будет также лежать в $a + I$: его можно получить, «сложив» a с нейтральным элементом в $(I, +)$. Но тогда $a + I \neq 0 + I$, так как в $0 + I$ все элементы из I, а $a \in a + I$ не лежит в I.
   - Если элемент $a \in I$, то смежный класс $a + I$ состоит только из элементов принадлежащих I. Действительно, I – подгруппа по сложению, а значит при «сложении» a и элементов из I получается элемент из I. Каждый $x \in I$ можно получить сложив a с элементом $x - a \in I$. Таким образом, $a + I = 0 + I$.

2. Пусть R/I – поле. Докажем, что идеал $I \neq R$ и I не содержится ни в одном собственном идеале кольца R.
   - Если $I = R$, то $R/I = R/R = R$. Но не всякое коммутативное кольцо – поле (чтобы коммутативное кольцо было полем должно выполняться $0 \neq 1$ и всякий ненулевой элемент в кольце обратим). Далее будем считать, что $I \neq R$.
   - Предположим противное: пусть I содержится в каком-то собственном идеале I' кольца R.
   - Возьмём такой элемент $x \in R$, что $x \in I'$ и $x \notin I$. Элемент $x + I$ ненулевой в факторкольце, так как иначе $x + I = 0 + I \Leftrightarrow x \in I$, а это противоречит выбору x. В силу того, что $x + I$ ненулевой элемент, существует обратный ему элемент в факторкольце, являющимся полем, то есть такой $y + I$, где $y \in R$, что выполняется

     $$(x + I)(y + I) = xy + I = yx + I = (y + I)(x + I) = 1 + I$$
   - Выражение $xy + I = 1 + I$ означает, что $xy - 1 = a \in I$. Покажем, что $1 = xy - a$ лежит в I'. Элемент $xy \in I'$, так как $x \in I'$, $y \in R$ и I' – идеал. Элемент $a \in I'$, так как $a \in I \subset I'$. Рассматриваемое множество I' – подгруппа по сложению $\Rightarrow$ $1 = xy - a \in I'$.

     Получаем, что единица лежит в идеале I', но если $1 \in I'$, то $I' = R$. Это противоречит тому, что I' – собственный идеал.

3. Пусть теперь $I \neq R$ и I не содержится ни в каком собственном идеале кольца R. Докажем, что R/I – поле.
   - Возьмём произвольный ненулевой элемент $x + I$ факторкольца R/I. Так как $x + I$ ненулевой, $x \notin I$. Покажем, что для этого элемента существует обратный в R/I.
   - Для данного x рассмотрим множество $I' = \{a + rx \mid a \in I, r \in R\}$. Нетрудно убедиться, что I целиком содержится в I', причём не совпадает с ним ($x \in I'$, но $x \notin I$). Для каждого $a \in I$ рассмотрим элемент в I' равный $a + rx$ при $r = 0 \in R$, тогда получим, что $a \in I'$.

- Докажем, что $I^{'}$ – идеал. Для этого проверим условия, которым должен удовлетворять идеал. Покажем, что $I^{'}$ – подгруппа по сложению.
  - В $I^{'}$ есть нейтральный элемент равный $0 \in R$:
  $$0 + (a + rx) = (a + rx) + 0 = a + rx$$
  - Для каждого $a + rx$ и каждого $a^{'} + r^{'}x$:
  $$(a + rx) + (a^{'} + r^{'}x) = \underbrace{(a + a^{'})}_{\in I} + \underbrace{(r + r^{'})}_{\in R}x \in I^{'}$$
  - Для каждого $a + rx$ существует обратный по сложению $-a - rx \in I^{'}$:
  $$(a + rx) + (-a - rx) = (-a - rx) + (a + rx) = 0$$

  Покажем, что для всех $a \in I^{'}$ и $r \in R$ элементы $ra \in I^{'}$ и $ar \in I^{'}$.
  - Пусть $a = a_0 + r_0x$, где $a_0 \in I$ и $r_0 \in R$.
  - Имеем следующее в силу коммутативности R:
  $$ra = r(a_0 + r_0x) = \underbrace{r \cdot a_0}_{\in I} + \underbrace{r \cdot r_0}_{\in R}x = \underbrace{a_0 \cdot r}_{\in I} + \underbrace{r_0 \cdot r}_{\in R}x = (a_0 + r_0x)r = ar \in I^{'}$$
  Элемент $ra_0 \in I$, так как I – идеал.
- Таким образом, $I^{'}$ – идеал, содержащий в себе идеал I. Но идеал I не содержится ни в одном несобственном идеале, а это значит, что $I^{'}$ – несобственный, причём $I^{'} \neq \{0\}$. Если $I^{'} = \{0\}$, то I не существует, так как $I \subset I^{'}$. Значит, $I^{'} = R$.
- Так как $I^{'} = R$, в $I^{'}$ лежит единица, а это означает, что $1 = a + rx$ для некоторых $a \in I$ и $r \in R$. Таким образом получаем, что для рассматриваемого ненулевого элемента $x + I$ в R/I существует обратный элемент в R/I. Этот элемент – смежный класс $r + I$:
  $$(r + I)(x + I) = (x + I)(r + I) = \underbrace{(a + I)}_{=0+I} + (x + I)(r + I) = \underbrace{(a + I)}_{=0+I} + (xr + I) =$$
  $$= (a + xr) + I = 1 + I$$
  Здесь использовано то, что факторкольцо коммутативного кольца по идеалу коммутативно. Действительно, для любых $a, b \in R$ верно $(a + I)(b + I) = ab + I = ba + I = (b + I)(a + I)$.
- Покажем, что в R/I верно, что $0 + I \neq 1 + I$. Если выполняется $0 + I = 1 + I$, то $1 \in I$, а значит, $I = R \Rightarrow$ противоречие.
- Таким образом, R/I – коммутативное кольцо, в котором $0 \neq 1$ и все ненулевые элементы обратимы $\Rightarrow R/I$ – поле.

4. Получаем, что для коммутативного кольца R и $I \lhd R$ факторкольцо R/I является полем $\Leftrightarrow$ $I \neq R$ и I не содержится ни в каком собственном идеале кольца R.