Независимый Московский Университет

Алгебра – I

Первый курс, весенний семестр 1998/99 г.
Лекция 4

Кольца, идеалы и факторкольца

Определение 1. *Кольцом* называется множество R с заданными на нем операциями сложения и умножения, удовлетворяющее следующим аксиомам:

1) R является абелевой группой по сложению;

2) $a(b+c) = ab + ac$ и $(a+b)c = ac + bc$ для любых $a, b, c \in R$.

R называется *ассоциативным кольцом*, если умножение в нем ассоциативно, *коммутативным кольцом* — если умножение в нем коммутативно, и *кольцом с единицей* — если в нем найдется такой элемент e, что $ae = ea = e$ для любого $a \in R$. *Полем* называется коммутативное ассоциативное кольцо с единицей, не равной нулю, в котором каждый ненулевой элемент обратим.

Мы будем рассматривать только ассоциативные кольца.

Подмножество $Q \subseteq R$ кольца R называется *подкольцом*, если оно замкнуто относительно сложения и умножения. Отметим, что подкольцо всегда является кольцом, подкольцо коммутативного кольца является коммутативным, но подкольцо кольца с единицей может не быть кольцом с единицей. Например, в кольце целых чисел $\mathbb{Z}$ любая аддитивная подгруппа (то есть подгруппа $\mathbb{Z}$, как абелевой группы по сложению) является подкольцом, но из них лишь $\mathbb{Z}$ и $\{0\}$ являются кольцами с единицей, причем у последнего единица не совпадает с единицей объемлющего кольца $\mathbb{Z}$.

Пусть R и Q — кольца. Отображение $\varphi : R \to Q$ называется *гомоморфизмом колец*, если $\varphi(a+b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$ для любых $a, b \in R$. *Ядром* гомоморфизма колец $\varphi : R \to Q$ называется $\varphi^{-1}(0)$, то есть ядро в смысле гомоморфизма абелевых групп по сложению. Очевидно, что ядро и образ гомоморфизма являются подкольцами соответственно в R и Q. Так же, как и для групп, образом гомоморфизма может быть любое подкольцо, но совсем не любое подкольцо может быть ядром гомоморфизма.

Пусть $\varphi : R \to Q$ — гомоморфизм колец, $x \in I = \operatorname{Ker}\varphi$. Тогда $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)\cdot 0 = 0$ для любого $a \in R$. Аналогично, $\varphi(xa) = 0$ для любого $a \in R$. Таким образом, $ax \in I$ и $xa \in I$ для любого $a \in R$. Это можно записать так: $RI \subseteq I$ и $IR \subseteq I$. Отметим, что если R — кольцо с единицей, то включения можно заменить на равенства: $RI = I$ и $IR = I$.

Определение 2. Пусть R — кольцо. Подкольцо $I \subseteq R$ называется *идеалом*, если $RI \subseteq I$ и $IR \subseteq I$.

Как мы только что проверили, ядро любого гомоморфизма является идеалом. Чуть позже мы убедимся и в обратном — что каждый идеал является ядром некоторого гомоморфизма.

Замечание: Если кольцо R не является коммутативным, то имеет смысл рассматривать подкольца $A \subseteq R$, удовлетворяющие одному условию: $RA \subseteq A$ — *левые идеалы*, или $AR \subseteq A$ — *правые идеалы*. В отличие от правых и левых идеалов, просто идеалы в некоммутативном кольце часто называются *двусторонними идеалами*.

Упражнение 1. Доказать, что в кольце матриц $M_n(\Bbbk)$ есть только два двусторонних идеала: $M_n(\Bbbk)$ и $\{0\}$.

Пусть I — идеал кольца R. Рассмотрим абелеву группу R/I — факторгруппу аддитивной группы поля по подгруппе I. Для каждого $a \in R$ обозначим через $\overline{a}$ смежный класс $a + I$. Положим $\overline{a}\overline{b} = \overline{ab}$. Это определение не зависит от представителей смежных классов $\overline{a}$ и $\overline{b}$. Действительно, $(a+I)(b+I) \subseteq (ab + aI + Ib + II) \subseteq (ab + I)$.

Легко проверить, что введенное таким образом умножение превращает R/I в кольцо. Оно называется *факторкольцом* кольца R по идеалу I. Из определения ясно, что каноническая проекция $\pi : R \to R/I$ является гомоморфизмом колец, причем $I = \operatorname{Ker} \pi$. Очевидно также, что любое факторкольцо коммутативного кольца коммутативно, а любое факторкольцо кольца с единицей является тоже кольцом с единицей.

Если $I = R$, то факторкольцо R/I изоморфно тривиальному кольцу $\{0\}$. Отсюда видно, почему требование $1 \neq 0$ не следует включать в определение кольца с единицей.

Теорема 1 (О гомоморфизмах колец). *Пусть $\varphi : R \to Q$ — произвольный гомоморфизм колец. Обозначим через I ядро этого гомоморфизма, через π — каноническую проекцию $R \to R/I$. Тогда существует единственный гомоморфизм колец $\psi : R/I \to Q$, делающий диаграмму*

$$\begin{tikzcd} R \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & Q \\ & R/I \arrow[ur, "\psi"'] & \end{tikzcd}$$

коммутативной. При этом ψ является изоморфизмом R/I на $\varphi(R)$.

Доказательство: Отображение ψ существует и единственно по теореме о факторизации отображений. По теореме о гомоморфизмах групп оно является гомоморфизмом аддитивной группы кольца R/I в аддитивную группу кольца Q. То, что ψ — гомоморфизм колец, проверяется столь же просто. Действительно, для любых $a, b \in R$ мы имеем $\psi(\overline{a}\overline{b}) = \psi(\overline{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(\overline{a})\psi(\overline{b})$. □

Далее в этой лекции мы будем рассматривать только коммутативные кольца.

Пример 1. Пусть $R = \mathbb{Z}$ — кольцо целых чисел. Подкольцо $n\mathbb{Z}$ является, очевидно, идеалом кольца $\mathbb{Z}$. Поэтому группу $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ классов вычетов по модулю n можно рассматривать как кольцо.

Название «кольцо классов вычетов» произошло из теории чисел. Два целых числа k и m называются *сравнимыми по модулю* n, если их разность делится на n. Сравнения записываются так:

$$k \equiv m \pmod n.$$

Числа, сравнимые по модулю n, называются (по отношению друг к другу) *вычетами по модулю* n. Соответственно, все числа, сравнимые с данным числом (а, следовательно, сравнимые и друг с другом), образуют *класс вычетов по модулю* n.

Кольца классов вычетов часто используются для доказательства неразрешимости уравнений в целых числах. Рассмотрим, например, уравнение $x^2 - y^2 = 154$. Пусть оно имеет решение в целых числах: $x = a$, $y = b$. Поскольку каноническая проекция $\pi : \mathbb{Z} \to \mathbb{Z}_4$ является гомоморфизмом колец, то из равенства $a^2 - b^2 = 154$ в кольце $\mathbb{Z}$ следует равенство $\overline{a}^2 - \overline{b}^2 = \overline{154}$. Однако в кольце $\mathbb{Z}_4$ лишь $\overline{0}$ и $\overline{1}$ являются квдратами, поэтому $\overline{154} = \overline{2}$ невозможно представить как разность квадратов в $\mathbb{Z}_4$. Следовательно, уравнение $x^2 - y^2 = 154$ неразрешимо в целых числах.

Теорема 2. *Пусть p — простое число. Тогда кольцо $\mathbb{Z}_p$ является полем.*

Доказательство: То, что единица в $\mathbb{Z}_p$ не равна нулю, очевидно. Пусть $k \in \mathbb{Z}$ не кратно p, то есть $\overline{k} \in (\mathbb{Z}_p \setminus \{\overline{0}\})$. Обозначим через ν_k отображение $\mathbb{Z}_p \to \mathbb{Z}_p$, задаваемое формулой $\nu_k(\overline{a}) = \overline{k}\overline{a}$. Очевидно, что это групповой гомоморфизм аддитивной группы $\mathbb{Z}_p$ в себя. Если $\overline{a} \neq \overline{0}$, то есть a не делится на p, то и произведение ka не делится на p, поэтому $\overline{k}\overline{a} \neq 0$. Следовательно, $\operatorname{Ker} \nu_k = \{\overline{0}\}$, то есть гомоморфизм ν_k инъективен. Однако инъективное отображение конечного множества в себя является биекцией. Поэтому, в частности, найдется $\overline{a} \in \mathbb{Z}_p$ такое, что $\overline{k}\overline{a} = \overline{1}$. Следовательно, все ненулевые элементы $\mathbb{Z}_p$ обратимы, то есть $\mathbb{Z}_p$ является полем. □

Множество классов вычетов по простому модулю p, рассматриваемое как поле, а не как абелева группа, обычно обозначают через $\mathbb{F}_p$. Вообще, под $\mathbb{F}_q$ понимают конечное поле, состоящее из q элементов. Такие поля бывают не для всех q, а лишь для $q = p^n$, где p — простое, а n — произвольное натуральное число. К этому мы еще вернемся.

Пример 2. Рассмотрим кольцо многочленов $R = \mathbb{R}[x]$, и рассмотрим в нем подмножество I, состоящее из многочленов, делящихся на x^2+1. Очевидно, что I является идеалом. Рассмотрим факторкольцо $A = R/I$. Поскольку каждый многочлен $f(x) \in R$ сравним по модулю x^2+1 с единственным линейным многочленом от x (остатком при делении $f(x)$ на x^2+1), то любой элемент кольца A однозначно записывается в виде $(a\overline{1} + b\overline{x})$, где $a, b \in \mathbb{R}$.

Умножение в кольце A устроено так: $(a\overline{1}+b\overline{x})(c\overline{1}+d\overline{x}) = (ac-bd)\overline{1}+(ad+bc)\overline{x})$. Отсюда видно, что существует изоморфизм $A \xrightarrow{\sim} \mathbb{C}$, переводящий $\overline{1}$ в 1, а $\overline{x}$ — в i.

Пример 3. Рассмотрим теперь кольцо многочленов $R = \mathbb{F}_3[x]$. Элементы поля $\mathbb{F}_3$ мы будем обозначать через 0, 1 и -1, безо всяких черточек сверху. Обозначим через I идеал в R, состоящий из всех многочленов, делящихся на x^2+1. Как и в предыдущем примере, легко проверить, что любой элемент факторкольца $A = R/I$ однозначно записывается в виде $(a\overline{1}+b\overline{x})$, где $a, b \in \mathbb{F}_3$. Докажем, что A является полем.

Рассмотрим $\overline{f} = a\overline{1} + b\overline{x} \in A$. Мы имеем $(a\overline{1} + b\overline{x})(a\overline{1} - b\overline{x}) = a^2 + b^2$. Однако в поле $\mathbb{F}_3$ квадрат любого ненулевого элемента равен 1, поэтому $a^2 + b^2 = 0$ тогда и только тогда, когда и $a = 0$, и $b = 0$. Поэтому для любого ненулевого $\overline{f} = a\overline{1} + b\overline{x}$ существует обратный

$$(\overline{f})^{-1} = \frac{a}{a^2+b^2}\overline{1} - \frac{b}{a^2+b^2}\overline{x}.$$

Итак, A является полем. Поскольку аддитивная группа кольца A изоморфна $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, то число элементов A равно 9. Таким образом, мы построили поле $\mathbb{F}_9$.

Теория делимости в кольцах главных идеалов

Далее слово «кольцо» будет обозначать коммутативное ассоциативное кольцо с единицей.

Определение 3. Пусть R — произвольное кольцо. Элемент $a \in R$ называется *обратимым*, если он имеет обратный по умножению. Ненулевой элемент $d \in R$ называется *делителем нуля*, если существует ненулевой элемент $c \in R$ такой, что $cd = 0$.

Легко видеть, что произведение обратимых элементов обратимо, то есть обратимые элементы кольца R образуют группу по умножению. Эта группа обозначается через R^*. Делитель нуля не может быть обратим. Действительно, пусть d обратим и $cd = 0$. Тогда $c = cd \cdot d^{-1} = 0$, то есть d не является делителем нуля.

Упражнение 2. Пусть $R = \mathbb{Z}_{12}$. Проверьте, что элементы $\overline{1}$, $\overline{5}$, $\overline{7}$ и $\overline{11}$ являются обратимыми, а остальные ненулевые элементы кольца R являются делителями нуля. Является ли группа R^* циклической?

Определение 4. Кольцо R называется *целостностным*, или *областью целостности*, если в нем нет делителей нуля и $1 \neq 0$.

Пример 4. Кольца $\mathbb{Z}$, $\Bbbk[x]$, а также любое поле $\Bbbk$ являются областями целостности.

Определение 5. Область целостности R называется *евклидовым кольцом*, если на $R \setminus \{0\}$ существует такая функция δ со значениями в множестве $\mathbb{N}$ натуральных чисел (мы будем называть $\delta(a)$ *нормой* a), что

1) $\delta(ab) \geqslant \delta(a)$ для любых $a, b \in R \setminus \{0\}$.

2) Для любых $a \in R$ и $b \in R \setminus \{0\}$ найдутся $q, r \in R$ такие, что $a = qb + r$, причем либо $r = 0$, либо $\delta(r) < \delta(b)$ (деление с остатком).

Пример 5. Кольцо целых чисел является евклидовым относительно нормы $\delta(a) = |a|$. Кольцо многочленов над полем является евклидовым относительно нормы $\delta(f) = \deg f + 1$.

Определение 6. Элемент $k \in R$ называется *делителем* элемента $a \in R$, если $a = ck$ для некоторого $c \in R$. Элемент $d \in R$ называется *наибольшим общим делителем* элементов $a, b \in R$, если d является их общим делителем (то есть делителем как a, так и b), и любой общий делитель a и b является также делителем d. То, что d является наибольшим общим делителем a и b, записывают так: $d = (a, b)$.

Утверждение 1. *Пусть кольцо R евклидово и $d \in R \setminus \{0\}$.*

1) Предположим, что $\delta(da) = \delta(a)$ для некоторого $a \in R \setminus \{0\}$. Тогда элемент d обратим.

2) Элемент d обратим тогда и только тогда, когда $\delta(d) = \delta(1)$.

Доказательство: 1) Разделим a на da с остатком: $a = qda + r$, где $r = 0$ или $\delta(r) < \delta(a)$. Мы имеем $r = (1 - qd)a$, поэтому неравенство $\delta(r) < \delta(a)$ невозможно, следовательно, $r = 0$. Поскольку R — область целостности, отсюда следует, что $1 - qd = 0$, то есть $qd = 1$ и d обратим.

2) Из определения евклидова кольца очевидно, что для любого $a \in R \setminus \{0\}$ выполнено неравенство $\delta(a) \geqslant \delta(1)$. Поэтому, если $\delta(d) = \delta(1)$, то 1 делится на d без остатка, то есть d обратим. С другой стороны, если d обратим, то $\delta(1) = \delta(dd^{-1}) \geqslant \delta(d)$, поэтому $\delta(d) = \delta(1)$. □

Определение 7. Идеал I в кольце R называется *главным*, если найдется такой элемент $a \in R$, что $I = aR$. Главный идеал aR обозначается также через (a). Кольцо R называется *кольцом главных идеалов*, если оно является областью целостности и любой идеал в нем — главный.

Теория делимости в кольцах главных идеалов опирается на следующий очевидный факт:

Утверждение 2. *Элемент a делится на элемент b тогда и только тогда, когда $(a) \subseteq (b)$.*

Утверждение 3. *Если кольцо R евклидово, то оно является кольцом главных идеалов.*

Доказательство: Пусть I — некоторый идеал в евклидовом кольце R. Если он равен $\{0\}$, то он главный: $I = (0)$. В противном случае рассмотрим непустое множество натуральных чисел $D = \{\delta(x) \mid x \in I, x \neq 0\}$. Любое непустое множество натуральных чисел имеет минимальный элемент. Пусть $b \in I$ таково, что $\delta(b) = \min(D)$. Рассмотрим произвольный элемент $a \in I$. Поделим его на b с остатком: $a = qb + r$, где либо $r = 0$, либо $\delta(r) < \delta(b)$. Однако $r = a - qb \in I$, поэтому $r = 0$, то есть $a = qb$. Следовательно, $I \subseteq (b)$. С другой стороны, I — идеал и $b \in I$, поэтому $(b) \subseteq I$. Таким образом $I = (b)$ — главный идеал. $\square$

Утверждение 4. *Пусть R — кольцо главных идеалов. Тогда для любых $a, b \in R$ существует их наибольший общий делитель (a, b).*

Доказательство: Идеал $(a) + (b)$ — главный. Пусть $(a) + (b) = (d)$. Тогда $a = \alpha d$ и $b = \beta d$ для некоторых $\alpha, \beta \in I$, то есть d является общим делителем a и b. С другой стороны, для любого k, являющегося общим делителем a и b, элементы a и b лежат в (k), поэтому $(d) = (a) + (b) \subseteq (k)$, то есть k является делителем d. Следовательно, $d = (a, b)$. $\square$

Как мы видели на прошлой лекции, факторкольцо $\mathbb{Z}/p\mathbb{Z}$ является полем, если p — простое число. Прежде, чем установить подобную взаимосвязь для произвольного кольца главных идеалов, исследуем в общем виде вопрос: при каких условиях на идеал $I \subseteq R$ факторкольцо R/I является полем?

Определение 8. Идеал I в кольце R называется *максимальным*, если он не равен всему R, а любой строго содержащий I идеал совпадает с R.

Утверждение 5. *1) Идеал I совпадает со всем кольцом тогда и только тогда, когда он содержит единицу.*

2) Факторкольцо R/I является полем тогда и только тогда, когда идеал I максимален.

Доказательство:

1). Ясно, что если I совпадает с R, то он содержит единицу. Пусть наоборот, $1 \in I$. Тогда, поскольку I — идеал, $R \cdot 1 \subseteq I$, но $R \cdot 1 = R$, поэтому $I = R$.

2). Пусть идеал I максимален. Тогда $1 \neq 0$ в факторкольце R/I, поскольку $I \neq R$. Рассмотрим произвольный элемент $a \in R \setminus I$. Идеал $J = aR + I$ строго содержит I, поэтому $J = R$, то есть найдется $b \in R$ такой, что $1 \in ab + I$. Это означает, что образ элемента a при канонической проекции $R \to R/I$ обратим. Поэтому R/I — поле.

В обратную сторону, пусть R/I — поле. Тогда $1 \neq 0$ в R/I, поэтому $I \neq R$. Пусть идеал $J \subseteq R$ строго содержит I. Выберем $a \in J \setminus I$. Образ элемента

a при канонической проекции $R \to R/I$ обратим, поэтому найдется $b \in R$ такой, что $1 \in ab + I$. Это означает, что $aR + I = R$, поэтому тем более $J = R$. Следовательно, идеал I максимален. $\square$

Определение 9. Пусть R — произвольное кольцо. Необратимый элемент $p \in R$ называется *простым* или *неприводимым*, если из разложения $p = ab$ следует, что либо a, либо b обратим.

Теорема 3. *Пусть R — кольцо главных идеалов. Элемент $p \in R$ является неприводимым тогда и только тогда, когда $R/(p)$ — поле.*

Доказательство: По утверждению 5 достаточно проверить, что идеал (p) максимален тогда и только тогда, когда p неприводим.

Пусть идеал (p) максимален. Тогда $(p) \neq R$, поэтому p не является обратимым. Предположим, что $p = ab$, причем b — не обратим. Тогда $(b) \neq R$, но $(p) \subseteq (b)$, поэтому $(p) = (b)$ из максимальности (p). Это означает, что найдется $c \in R$ такое, что $b = cp$. Получаем $p = acp$, то есть $(1 - ac)p = 0$. Поскольку R — область целостности, $ac = 1$ и a обратим. Следовательно, p неприводим.

С другой стороны, если p неприводим, то $1 \notin (p)$, то есть $(p) \neq R$. Далее, пусть идеал J строго содержит (p). Поскольку R — кольцо главных идеалов, то существует $a \in R$ такое, что $J = (a)$. Раз $(p) \subset (a)$, то $p = ab$ для некоторого $b \in R$. При этом b не обратим, иначе идеал (p) совпадал бы с (a). Следовательно, a обратим, и $(a) = R$. Таким образом, идеал (p) максимален. $\square$

Определение 10. Область целостности R называется *факториальным кольцом*, если любой ненулевой и необратимый элемент $a \in R$ однозначно разлагается в произведение неприводимых, то есть существуют такие неприводимые элементы $p_i \in R$ $(i = 1, \ldots, k)$, что $a = p_1 p_2 \ldots p_k$, и для любого другого разложения на неприводимые множители $a = q_1 q_2 \ldots q_m$ можно утверждать, что $k = m$ и для некоторой перестановки $\sigma \in S_n$ выполнены равенства $p_i = \varepsilon_i q_{\sigma(i)}$ $(i = 1, \ldots, k)$, где элементы ε_i обратимы.

Теорема 4. *Пусть R — кольцо главных идеалов. Тогда R — факториальное кольцо.*

Доказательство: Докажем сначала существование разложения. По определению, если ненулевой элемент a необратим и не является неприводимым, то он разложим на необратимые сомножители $a = a_1 a_2$, теперь смотрим на a_1 и a_2, раскладываем те из них, которые не являются неприводимыми, и т. д. Надо лишь убедиться, что процесс оборвется. Если кольцо R евклидово, то это сразу следует из неравенств $\delta(a_1) < \delta(a)$ и $\delta(a_2) < \delta(a)$, поскольку функция δ принимает только натуральные значения. Для произвольного кольца главных идеалов рассуждение ненамного сложнее. Разложение $a = a_1 a_2$ означает, что $(a) \subset (a_1)$ (включение идеалов строгое, иначе a_2 был бы обратим).

Если бы процесс разложения мог продолжаться неограниченно, то мы получили бы бесконечную возрастающую цепочку строго вложенных друг в друга идеалов. Докажем, что это невозможно.

Пусть $(d_1) \subset (d_2) \subset \ldots$ — такая цепочка. Обозначим через D объединение идеалов (d_i). Легко видеть, что D — идеал, поэтому $D = (d)$ для некоторого $d \in D$. По определению, $d \in (d_m)$ для некоторого m. Но тогда $(d_{m+1}) \subseteq (d) \subseteq (d_m)$, то есть $(d_m) = (d_{m+1})$, в противоречии с предположением о том, что все включения строгие.

Итак, процесс разложения должен оборваться, и разложение на неприводимые множители существует. Докажем единственность.

Лемма 1. *Пусть $p_1, \ldots, p_k$ и $q_1, \ldots, q_m$ — неприводимые элементы кольца R, удовлетворяющие условию $p_1 \ldots p_k = q_1 \ldots q_m$. Тогда для некоторого $i_0 \in \{1, \ldots, m\}$ существует такой обратимый элемент $\varepsilon \in R$, что $p_1 = \varepsilon q_{i_0}$.*

Доказательство: Рассмотрим факторкольцо $R/(p_1)$. В нем $\overline{q_1} \cdot \cdots \cdot \overline{q_m} = \overline{q_1 \ldots q_m} = 0$. Поскольку $R/(p_1)$ — поле, отсюда следует, что $\overline{q_{i_0}} = 0$ для некоторого $i_0 \in \{1, \ldots, m\}$. Это значит, что $q_{i_0} = \alpha p_1$ для некоторого $\alpha \in R$. Поскольку p_1 и q_{i_0} неприводимы, отсюда следует, что α обратим, то есть для $\varepsilon = \alpha^{-1}$ мы получаем $p_1 = \varepsilon q_{i_0}$. □

С помощью леммы 1 легко доказать единственность разложения на неприводимые множители. Воспользуемся индукцией по k.

При $k = 1$ по лемме 1 существует индекс i_0 и обратимый элемент ε, для которых $p_1 = \varepsilon q_{i_0}$. Предположим, что $m > 1$. Тогда $q_{i_0}(\varepsilon - \prod_{i \neq i_0} q_i) = 0$, то есть $\prod_{i \neq i_0} q_i = \varepsilon$, что противоречит необратимости q_i. Отсюда $m = k = 1$ и $q_1 = p_1$.

Пусть теперь для $k < k_0$ утверждение теоремы выполнено и $a = p_1 \ldots p_{k_0} = q_1 \ldots q_m$ — два разложения на неприводимые множители. По лемме 1 существует индекс i_0 и обратимый элемент ε, для которых $p_1 = \varepsilon q_{i_0}$. Переставив индексы, можем считать, что $i_0 = 1$. Тогда

$$q_1\left((\varepsilon p_2)p_3 \ldots p_{k_0} - q_2 \ldots q_m\right) = 0.$$

Кольцо R — область целостности, поэтому $(\varepsilon p_2)p_3 \ldots p_{k_0} = q_2 \ldots q_m$. Доказательство завершается применением к этому равенству предположения индукции при $k = k_0 - 1$. □