Лекции курса «Алгебра», лектор Р. С. Авдеев

ФКН НИУ ВШЭ, 1-й курс ОП ПМИ, 4-й модуль, 2015/2016 учебный год

Лекция 7

Факторкольца. Теорема о гомоморфизме колец. Евклидовы кольца, кольца главных идеалов и факториальные кольца.

Вернёмся к случаю произвольного кольца R. Поскольку любой идеал I является подгруппой абелевой группы $(R, +)$, мы можем рассмотреть факторгруппу R/I. Введём на ней умножение по формуле

$$(a + I)(b + I) := ab + I.$$

Покажем, что это определение корректно. Пусть элементы $a', b' \in R$ таковы, что $a'+I = a+I$ и $b'+I = b+I$. Проверим, что $a'b' + I = ab + I$. Заметим, что $a' = a + x$ и $b' = b + y$ для некоторых $x, y \in I$. Тогда

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

поскольку $ay, xb, xy \in I$ в силу определения идеала.

Упражнение 1. Проверьте, что множество R/I является кольцом относительно имеющейся там операции сложения и только что введённой операции умножения.

Определение 1. Кольцо R/I называется *факторкольцом* кольца R по идеалу I.

Пример. $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

Пусть $\varphi\colon R \to R'$ — гомоморфизм колец. Тогда определены его ядро $\operatorname{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\}$ и образ $\operatorname{Im}\varphi = \{\varphi(r) \mid r \in R\} \subseteq R'$.

Лемма 1. *Ядро* $\operatorname{Ker}\varphi$ *является идеалом в* R.

Доказательство. Так как φ — гомоморфизм абелевых групп, то $\operatorname{Ker}\varphi$ является подгруппой в R по сложению. Покажем теперь, что $ra \in \operatorname{Ker}\varphi$ и $ar \in \operatorname{Ker}\varphi$ для произвольных элементов $a \in \operatorname{Ker}\varphi$ и $r \in R$. Имеем $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$, откуда $ra \in \operatorname{Ker}\varphi$. Аналогично получаем $ar \in \operatorname{Ker}\varphi$. $\square$

Упражнение 2. Проверьте, $\operatorname{Im}\varphi$ — подкольцо в R'.

Теорема о гомоморфизме для колец. Пусть $\varphi\colon R \to R'$ – гомоморфизм колец. Тогда имеет место изоморфизм

$$R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi.$$

Доказательство. Положим для краткости $I = \operatorname{Ker}\varphi$ и рассмотрим отображение

$$\pi\colon R/I \to \operatorname{Im}\varphi, \quad a + I \mapsto \varphi(a).$$

Из доказательства теоремы о гомоморфизме для групп следует, что отображение π корректно определено и является изоморфизмом абелевых групп (по сложению). Покажем, что π — изоморфизм колец. Для этого остаётся проверить, что π сохраняет операцию умножения:

$$\pi((a + I)(b + I)) = \pi(ab + I) = \varphi(ab) = \varphi(a)\varphi(b) = \pi(a + I)\pi(b + I).$$

$\square$

Пример 1.

(a) Пусть $R = \mathcal{F}(M, \mathbb{R})$. Зафиксируем произвольную точку $m_0 \in M$ и рассмотрим гомоморфизм $\varphi\colon R \to \mathbb{R}$, $f \mapsto f(m_0)$. Ясно, что гомоморфизм φ сюръективен. Его ядром является идеал I всех функций, обращающихся в нуль в точке m_0. По теореме о гомоморфизме получаем $R/I \cong \mathbb{R}$.

(b) Рассмотрим отображение $\varphi\colon \mathbb{R}[x] \to \mathbb{C}$, $f \mapsto f(i)$. Очевидно, что φ — гомоморфизм, причем сюръективный. Если функция принадлежит ядру φ, то есть $f(i) = 0$, то $(x - i) \mid f$ в кольце $\mathbb{C}[x]$. Но и сопряженный к корню также будет являться корнем многочлена, так что дополнительно $(x + i) \mid f$. Итого, получаем, что $f \in (x - i)(x + i) = (x^2 + 1)$ и, соответственно, $\operatorname{Ker}\varphi \subseteq (x^2 + 1)$. В обратную сторону включение тем более очевидно. Далее, по теореме о гомоморфизме получаем $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Далее в этой лекции всюду предполагается, что R — коммутативное кольцо без делителей нуля.

Определение 2. Говорят, что элемент $b \in R$ *делит* элемент $a \in R$ (b — *делитель* a, a *делится* на b; пишут $b \,|\, a$) если существует элемент $c \in R$, для которого $a = bc$.

Определение 3. Два элемента $a, b \in R$ называются *ассоциированными*, если $a = bc$ для некоторого обратимого элемента c кольца R.

Замечание 1. Легко видеть, что отношение ассоциированности является отношением эквивалентности на кольце R.

Определение 4. Кольцо R без делителей нуля, не являющееся полем, называется *евклидовым*, если существует функция
$$N\colon R \setminus \{0\} \to \mathbb{Z}_{\geqslant 0}$$
(называемая *нормой*), удовлетворяющая следующим условиям:

1) $N(ab) \geqslant N(a)$ для всех $a, b \in R \setminus \{0\}$;

2) для любых $a, b \in R$, $b \neq 0$, существуют такие $q, r \in R$, что $a = qb + r$ и либо $r = 0$, либо $N(r) < N(b)$.

Неформально говоря, условие 2) означает возможность «деления с остатком» в кольце R.

Примеры евклидовых колец:

1) $\mathbb{Z}$ с нормой $N(a) = |a|$;

2) $K[x]$ (где K — произвольное поле) с нормой $N(f) = \deg f$.

Лемма 2. *Пусть R — евклидово кольцо и $a, b \in R \setminus \{0\}$. Равенство $N(ab) = N(a)$ выполнено тогда и только тогда, когда b обратим.*

Доказательство. Если b обратим, то $N(a) \leqslant N(ab) \leqslant N(abb^{-1}) = N(a)$, откуда $N(ab) = N(a)$.

Пусть теперь $N(ab) = N(a)$. Разделим a на ab с остатком: $a = qab + r$, где либо $r = 0$, либо $N(r) < N(ab)$. Если $r \neq 0$, то с учётом равенства $r = a(1 - qb)$ имеем $N(a) \leqslant N(a(1 - qb)) = N(r) < N(ab) = N(a)$ — противоречие. Значит, $r = 0$ и $a = qab$, откуда $a(1 - qb) = 0$. Так как в R нет делителей нуля и $a \neq 0$, то $1 - qb = 0$, откуда $qb = 1$, т. е. b обратим. $\square$

Определение 5. Кольцо R называется *кольцом главных идеалов*, если всякий идеал в R является главным.

Теорема 1. *Всякое евклидово кольцо R является кольцом главных идеалов.*

Доказательство. Пусть I — произвольный идеал в R. Если $I = \{0\}$, то $I = (0)$ и поэтому I является главным. Далее считаем, что $I \neq \{0\}$. Пусть $a \in I \setminus \{0\}$ — элемент с наименьшей нормой. Тогда главный идеал (a) содержится в I. Предположим, что какой-то элемент $b \in I$ не лежит в (a), т. е. не делится на a. Тогда разделим b на a с остатком: $b = qa + r$, где $r \neq 0$ и $N(r) < N(a)$. Так как $r = b - aq$, то $r \in I$, что в силу неравенства $N(r) < N(a)$ противоречит нашему выбору элемента a. $\square$

Определение 6. *Наибольшим общим делителем* элементов a и b кольца R называется их общий делитель, который делится на любой другой их общий делитель. Он обозначается (a, b).

Замечание 2. Если наибольший общий делитель двух элементов $a, b \in R$ существует, то он определён однозначно с точностью до ассоциированности, т. е. умножения на обратимый элемент кольца R.

Теорема 2. *Пусть R — евклидово кольцо и a, b — произвольные элементы. Тогда:*

(1) *существует наибольший общий делитель (a, b);*

(2) *существуют такие элементы $u, v \in R$, что $(a, b) = ua + vb$.*

Доказательство.
Способ 1: утверждение (1) получается применением (прямого хода) алгоритма Евклида, а утверждение (2) — применением обратного хода в алгоритме Евклида.

Способ 2: рассмотрим идеал $I = (a, b)$. Так как R — кольцо главных идеалов, то существует такой элемент $d \in R$, что $I = (d)$ и существуют $x, y \in R$ такие, что
$$d = ax + dy. \qquad (*)$$
Покажем, что $d = (a, b)$. Для начала, так как a и b лежат в идеале $I = (d)$, то они оба делятся на d, то есть d является одним из их делителей. А из равенства $(*)$ ясно, что любой другой общий делитель a и b будет также делиться на d. Итого, d — наибольший общий делитель. $\square$

Определение 7. Ненулевой необратимый элемент p кольца R называется *простым*, если он не может быть представлен в виде $p = ab$, где $a, b \in R$ — необратимые элементы.

Замечание 3. Простые элементы в кольце многочленов $K[x]$ над полем K принято называть *неприводимыми многочленами.*

Лемма 3. *Если простой элемент p евклидова кольца R делит произведение $a_1a_2\dots a_n$, то он делит один из сомножителей.*

Доказательство. Индукция по n. Пусть $n=2$ и предположим, что p не делит a_1. Тогда $(p,a_1)=1$ и по утверждению (2) теоремы 2 найдутся такие элементы $u,v\in R$, что $1=up+va_1$. Умножая обе части этого равенства на a_2, получаем

$$a_2 = upa_2 + va_1a_2.$$

Легко видеть, что p делит правую часть последнего равенства, поэтому p делит и левую часть, т. е. a_2.

При $n>2$ применяем предыдущее рассуждение к $(a_1\dots a_{n-1})a_n$ и пользуемся предположением индукции. □

Определение 8. Кольцо R называется *факториальным*, если всякий его ненулевой необратимый элемент «разложим на простые множители», т. е. представим в виде произведения (конечного числа) простых элементов, причём это представление единственно с точностью до перестановки множителей и ассоциированности.

Более формально единственность разложения на простые множители следует понимать так: если для элемента $a\in R$ есть два представления

$$a = p_1p_2\dots p_n = q_1q_2\dots q_m,$$

где все элементы p_i, q_j простые, то $n=m$ и существует такая подстановка $\sigma\in S_n$, что для каждого $i=1,\dots,n$ элементы p_i и $q_{\sigma(i)}$ ассоциированы.

Теорема 3. *Всякое евклидово кольцо R является факториальным.*

Доказательство состоит из двух шагов.

Шаг 1. Сначала докажем, что всякий ненулевой необратимый элемент из R разложим на простые множители. Предположим, что это не так, и среди всех элементов, не разложимых на простые множители, выберем элемент a с наименьшей нормой. Тогда a не может быть простым (иначе он разложим в произведение, состоящее из одного простого множителя), поэтому существует представление вида $a=bc$, где $b,c\in R$ — ненулевые необратимые элементы. Но тогда в силу леммы 2 имеем $N(b)<N(a)$ и $N(c)<N(a)$, поэтому элементы b и c разложимы на простые множители. Но тогда и a разложим — противоречие.

Шаг 2. Докажем теперь индукцией по n, что если для некоторого элемента $a\in R$ имеются два разложения

$$a = p_1p_2\dots p_n = q_1q_2\dots q_m,$$

где все элемнты p_i и q_j простые, то $m=n$ и после подходящей перенумерации элементов q_j окажется, что при всех $i=1,\dots,n$ элемент p_i ассоциирован с q_i.

Если $n=1$, то $a=p_1$; тогда из определения простого элемента следует, что $m=1$ и тем самым $q_1=p_1$. Пусть теперь $n>1$. Тогда элемент p_1 делит произведение $q_1q_2\dots q_m$. По лемме 3 этот элемент делит некоторый q_i, а значит, ассоциирован с ним. Выполнив перенумерацию, можно считать, что $i=1$ и $q_1=cp_1$ для некоторого обратимого элемента $c\in R$. Так как в R нет делителей нуля, то мы можем сократить на p_1, после чего получится равенство

$$p_2p_3\dots p_n = (cq_2)q_3\dots q_m$$

(заметьте, что элемент cq_2 прост!). Дальше используем предположение индукции. □

Список литературы

[1] Э. Б. Винберг. Курс алгебры. М.: Факториал Пресс, 2002 (глава 3, § 5, 10 и глава 9, § 5)
[2] А. И. Кострикин. Введение в алгебру. Основы алгебры. М.: Наука. Физматлит, 1994 (глава 5, § 2,3,4)
[3] А. И. Кострикин. Введение в алгебру. Основные структуры алгебры. М.: Наука. Физматлит, 2000 (глава 4, § 2)
[4] Сборник задач по алгебре под редакцией А. И. Кострикина. Новое издание. М.: МЦНМО, 2009 (глава 14, § 63–64)