γ

Лекция 3

Структура коммутативного кольца

Содержание лекции:
Алгебраческая структура кольца по своей важности и фундаментальности не уступает структуре группы. В этой лекции мы опишем данную структуру и дадим определения связанным с ней объектам. Лекция является ознакомительной, но понятия вводимые в ней окажутся крайне полезными в дальнейшем.

Ключевые слова:
Согласование законов, дистрибутивность, кольцо, гомоморфизм колец, подкольцо, идеал кольца, фактор-кольцо, канонический кольцевой гомоморфизм, класс вычетов, делитель нуля, область целостности, нильпотент, обратимый элемент, главный идеал, поле.

Авторы курса:

Трифанов А.И. Москаленко М.А.

Ссылка на ресурсы:
`mathdep.ifmo.ru/geolin`

3.1 Согласование внутренних законов

Пусть на множестве M задано два всюду определенных закона композиции, обозначаемых через $\circ$ и $*$. Закон композиции $\circ$ называется **дистрибутивным слева** относительно закона $*$, если для любых элементов $x, y, z \in M$ имеет место равенство

$$x \circ (y * z) = (x \circ y) * (x \circ z)\,.$$

Соответственно, **дистрибутивность справа** означает выполнение следующего равенства:

$$\forall x, y, z \in M \quad (y * z) \circ x = (y \circ x) * (z \circ x)\,.$$

Закон, дистрибутивный и справа и слева называется **двояко дистрибутивным**.

Пример 3.1. Пусть на множестве M задано два всюду определенных закона композиции, обозначаемых через $\circ$ и $*$, причем $\circ$ наделяет M структурой группы. Если в M существует *нейтральный элемент* e относительно $*$ и $\circ$ двояко дистрибутивен относительно $*$, тогда элемент e является *поглощающим* относительно закона $\circ$.
Действительно, пусть $x, y \in M$, рассмотрим композицию

$$x \circ y = x \circ (e * y) = (x \circ e) * (x \circ y) = e * (x \circ y).$$

Вообще говоря, из выведенного равенства не следует, что $(x \circ e) = e$, так как не доказано свойство всеобщности - мы показали лишь, что это верно для подмножества M_z композиций вида $z = x \circ y$. Чтобы $M_z = M$ достаточно потребовать существования групповой структуры на M относительно закона $\circ$.

3.2 Кольца и гомоморфизмы колец

Nota bene На протяжении всего раздела под кольцом R мы будем понимать ассоциативное и коммутативное кольцо с единицей.

Кольцом R называется множество замкнутое относительно двух согласованно заданных на нем бинарных операций, удовлетворяющих следующим аксиомам:

A1. Ассоциативность сложения:

$$\forall x, y, z \in R \quad (x + y) + z = x + (y + z);$$

A2. Существование нуля:

$$\exists\, 0 \in R : \quad x + 0 = x = 0 + x \quad \forall x \in R$$

A3. Существование противоположного:

$$\forall x \in R \quad \exists\, (-x) : \quad x + (-1) = 0 = (-x) + x.$$

M1. Асоциативность умножения:

$$\forall x, y, z \in R \quad (xy)z = x(yz);$$

M2. Существование единицы:

$$\exists\, 1 \in R : \quad 1 \cdot x = x = x \cdot 1, \quad \forall x \in R;$$

M3. Коммутативность:

$$\forall x, y \in R \quad x \cdot y = y \cdot x;$$

D1. Дистрибутивность слева:

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

D2. Дистрибутивность справа:

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

Пример 3.2. Примеры колец:

1. Нулевое кольцо:

$$R : \quad 0 = 1 \quad \Rightarrow \quad \forall x \in R \quad x = 1 \cdot x = 0 \cdot x = 0;$$

2. Целые числа:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots, \pm m, \dots\};$$

3. Кольцо доичных дробей:

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{m}{2^n}: \quad m \neq 2 \cdot k, \quad k \in \mathbb{Z}\right\}$$

4. Пифагорово кольцо:

$$\mathbb{Z}[\sqrt{2}] = \left\{x + \sqrt{2}y: \quad x, y \in \mathbb{Z}\right\} \tag{3.1}$$

5. Гауссово кольцо:

$$\mathbb{Z}[i] = \left\{x + iy: \quad x, y \in \mathbb{Z}, \quad i^2 = -1\right\};$$

6. Кольцо многочленов над Z от одного или нескольких параметров:

$$\mathbb{Z}[x] = \left\{\sum a_j x^j: \quad a_j \in \mathbb{Z}\right\}, \quad \mathbb{Z}[x_1, x_2, \dots, x_n] = \left\{\sum a_{j_1, j_2, \dots, j_n} x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}\right\}$$

7. Кольцо матриц - пример некоммутативного кольца.

Пусть A и B - кольца. **Гомоморфизмом колец** называется отображение $f: \quad A \to B$, со следующими свойствами:

- сохранение сложения:

$$\forall x, y \in R \quad f(x + y) = f(x) + f(y);$$

- сохранение умножения:

$$\forall x, y \in R \quad f(xy) = f(x) \cdot f(y);$$

- сохранение единицы:

$$f(1_A) = 1_B.$$

Подмножество $S \subset R$ называется **подкольцом** кольца R, если оно является абелевой подгруппой R и содержит единицу R.

Nota bene Вложение - кольцевой гомоморфизм:

$$S < R \quad \Rightarrow \quad S \hookrightarrow R;$$

Лемма 3.1. *Пусть A, B, C - кольца и*

$$f: A \to B, \quad g: B \to C,$$

- кольцевые гомоморфизмы, тогда $g \circ f: A \to C$ - кольцевой гомоморфизм.

3.3 Идеалы и фактор-кольца

Иделалом J в кольце R называется аддитивная подгруппа со свойством

$$RJ \subset J \quad (\forall x \in R, \quad \forall y \in J \quad xy \in J).$$

Пример 3.3. Найдем идеалы в кольце $\mathbb{Z}$. Пусть m - наименьшее положительное число, лежащее в идеале $J \triangleleft \mathbb{Z}$. Тогда $(m) = m \cdot \mathbb{Z}$. Других идеалов в кольце $\mathbb{Z}$ содержащих элемент m нет. Действительно, пусть

$$z \in J = m \cdot \mathbb{Z} \quad \Rightarrow \quad z = m \cdot u + r, \quad r \in J, \quad r < m \quad \Rightarrow \quad r = \min(J).$$

Лемма 3.2. *Пусть $J \triangleleft R$, тогда следующее отношение является отношением эквивалентности на R:*

$$x \sim y \quad \Leftrightarrow \quad x - y \in J.$$

►
Утверждение следует из прямой проверки свойств:

R. $x - x = 0 \in J \quad \Rightarrow \quad x \sim x;$

S. $x \sim y \quad \Rightarrow \quad x - y \in J \quad \Rightarrow \quad y - x = -(x - y) \in J \quad \Rightarrow \quad x \sim y;$

T. $x \sim y, \quad y \sim z \quad \Rightarrow \quad x - z = (x - y) + (y - z) \in J \quad \Rightarrow \quad x \sim z.$

◄

Nota bene Фактор-множество R/J состоит из классов эквивалентности вида

$$\bar{x} = x + J.$$

Лемма 3.3. *Фактор-множество R/J, наделенное операциями, индуцированными из R имеет структуру кольца:*

$$\bar{x} + \bar{y} = \overline{x + y}, \quad \bar{x} \cdot \bar{y} = \overline{x \cdot y}, \quad \bar{0} = J.$$

►
Проверяем непосредственно свойства операций:

1. $\bar{x} + \bar{y} = (x + J) + (y + J) = (x + y) + J = \overline{x + y},$
2. $\bar{x} \cdot \bar{y} = (x + J) \cdot (y + J) = xy + J = \overline{xy},$
3. $\bar{0} \cdot \bar{x} = J \cdot (x + J) = J = \bar{0}.$

◄

Множество R/J называется **фактор-кольцом** кольца R по идеалу J. Отображение $\varphi : R \to R/J$, действующее как

$$x \mapsto \bar{x} = x + J,$$

является гомоморфизмом, который называется **каноническим**.

Пример 3.4. Элементами фактор-кольца $\mathbb{Z}/(m) \triangleq \mathbb{Z}/m\mathbb{Z}$ являются *классы вычетов по модулю* m:

$$\begin{aligned} \bar{0} &= \{x \in \mathbb{Z} : \quad x = 0 \mod (m)\}, \\ \bar{1} &= \{x \in \mathbb{Z} : \quad x = 1 \mod (m)\}, \\ &\cdots\cdots\cdots \\ \overline{m-1} &= \{x \in \mathbb{Z} : \quad x = (m-1) \mod (m)\}. \end{aligned}$$

Лемма 3.4. *Пусть $f : A \to B$ - гомоморфизм колец, тогда*

$$\ker f \trianglelefteq A, \quad \operatorname{Im} f \leq B$$
$$A/\ker f \simeq \operatorname{Im} f.$$

►
Покажем, что $\ker f$ - идеал в кольце A:

$$x \in \ker f \quad \Rightarrow \quad f(x) = 0 \quad \Rightarrow \quad \forall y \in A \quad f(xy) = f(x)f(y) = 0 \quad \Rightarrow \quad xy \in \ker f.$$

То, что $\operatorname{Im} f$ - подкольцо в B следует из определения кольцевого гомоморфизма. Последнее утверждение следует из биективности и линейности отображения:

$$(x + \ker f) \mapsto f(x).$$

◄

3.4 Делители нуля. Нильпотенты

Делителем нуля в кольце R называется всякий элемент $x \neq 0$, такой что

$$\exists\, y \neq 0 : \quad xy = 0.$$

Пример 3.5. В кольце $\mathbb{Z}/6\mathbb{Z}$ делителями нуля являются элементы $\bar{2}$ и $\bar{3}$.

Областью целостности называется кольцо, в котором нет делителей нуля.

Пример 3.6. Областями целостности являются кольца $\mathbb{Z}$ и $\mathbb{Z}/p\mathbb{Z}$, где p - простое.

Элемент $z \neq 0$ называется **нильпотентом**, если

$$\exists n \in \mathbb{N}: \quad z^n = 0.$$

Nota bene Всякий нильпотент является делителем нуля. Обратное верно не всегда.

3.5 Обратимые элементы. Поле

Обратимым элементом кольца называется всякий элемент $u \in R$ такой что

$$\exists\, v \in R \quad u \cdot v = 1$$

Nota bene В паре u, v оба элемента являются обратимыми.

Лемма 3.5. *Множество обратимых элементов кольца R образует мультипликативную группу, обозначаемую R^*.*

Идеал вида $(x) = x \cdot R, x \in R$ называется **главным идеалом** кольца R.

Лемма 3.6. *Имеет место эквивалентность:*

$$x \in R^* \quad \Leftrightarrow \quad (x) = (1) \triangleq R.$$

Полем называется ненулевое кольцо, в котором каждый ненулевой элемент обратим.

Лемма 3.7. *Всякое поле K является областью целостности.*

▶
Пусть $x, y \in K$ такие что $xy = 0$. По определению K имеем

$$\exists\, u, v : ux = 1, \quad yv = 1.$$

Откуда сразу получаем:

$$1 = (ux) \cdot (yv) = u \cdot (xy) \cdot v = 0.$$

◀

Nota bene Обратное, вообще говоря не верно: $\mathbb{Z}$ - область целостности, но не поле.

Теорема 3.1. *Пусть R - ненулевое кольцо, тогда следующие утверждения равносильны:*

(1) *R - поле;*

(2) *в R нет идеалов, кроме (0) и (1);*

(3) *любой гомоморфизм R в ненулевое кольцо инъективен.*

►
Докажем соответствующие импликации:

- $(1) \Rightarrow (2)$:
  Пусть $J \trianglelefteq R$ и $x \in J$, тогда $(1) = (x) \subseteq J \quad \Rightarrow \quad J = (1)$.

- $(2) \Rightarrow (3)$:
  Пусть $f : R \to B$ - кольцевой гомоморфизм. Тогда

$$\ker f \trianglelefteq R, \quad \ker R \neq R \quad \Rightarrow \quad \ker f = 0,$$

  откуда следует инъективность.

- $(3) \Rightarrow (1)$
  Пусть $x \notin R^*$, тогда

$$(x) \neq (1) \quad \Rightarrow \quad B = R/(x) \neq 0, \quad \varphi : R \to R/(x)$$

  Из инъективности канонического отображения φ следует, что $(x) = 0$ и $x = 0$.

◄