Лекция 6

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, аксиомы кольца, основные примеры колец, гомоморфизм колец, образ кольца, подкольцо, ядро кольцевого гомоморфизма.

Авторы курса:

Трифанов А.И. Москаленко М.А.

Ссылка на ресурсы:

6.1 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 6.1. 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 $M \setminus \{e\}$ относительно закона $\circ$.

Nota bene Пусть на множестве M с двумя законами композиции $\circ$ и $*$ задано отношение эквивалентности $\sim$, индуцирующее структуру фактор-множества $M/_\sim$.

Говорят что отношение эквивалентности **согласованно со структурой на** $(M, \circ, *)$, если оно согласованно с каждым из внутренних законов на M:

$$\begin{gathered}\forall x_1, x_2, y_1, y_2 \in M : \quad x_1 \sim y_1, \quad x_2 \sim y_2 \quad \Rightarrow \\ \Rightarrow \quad x_1 \circ x_2 \sim y_1 \circ y_2, \quad x_1 * x_2 \sim y_1 * y_2.\end{gathered}$$

Иными словами, если $\bar{x}$ и $\bar{y}$ - классы соответствующих элементов x и y, тогда

$$\bar{x} \circ \bar{y} = \overline{x \circ y}, \quad \bar{x} * \bar{y} = \overline{x * y},$$

где в левых частях стоят соответствующие фактор-законы.

Пример 6.2. Примеры структур с двумя внутренними законами композиции:

1. натуальные числа $(\mathbb{N}, +, \cdot)$ - структура полукольца;
2. элементы булеана $(2^M, \cup, \cap)$ - структура решетки;

6.2 Определение кольца

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 6.3. 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:

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

3. Кольцо двоичных 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:

$$\mathbb{Z}[\sqrt{2}] = \left\{x + \sqrt{2}y: \quad x, y \in \mathbb{Z}\right\} \tag{6.1}$$

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:

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

7. Кольцо матриц - пример некоммутативного кольца.

6.3 Гомоморфизмы колец

Пусть R и R' - кольца. **Гомоморфизмом колец** называется отображение $f: R \to R'$, 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:

$$f(1_R) = 1_{R'}.$$

Nota bene Таким образом, гомоморфизм колец является гомоморфизмом абелевых групп $(R, +)$ и $(R', +)$, а также мультипликативных моноидов $(R, \cdot)$ и $(R', \cdot)$.

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

Nota bene Тот факт, что S является подкольцом в R обозначают $S \leqslant R$.

Лемма 6.1. *Образ* $\operatorname{Im} f$ *гомоморфизма* $f \in \operatorname{Hom}(R, R')$ *является подкольцом в* R'*:*

$$\operatorname{Im} f \leqslant R'.$$

Лемма 6.2. *Ядро* $\ker f$ *гомоморфизма* $f \in \operatorname{Hom}(R, R')$ *имеет следующие свойства:*

1. *является нормальной подгруппой:* $\quad \ker f \trianglelefteq (R, +)$;
2. *обладает поглощением:* $\quad \forall x \in R, \quad \forall y \in \ker f \quad x \cdot y \in \ker f$.

Пример 6.4. Приведем пример подмножества L кольца R, являющееся кольцом, но при этом подкольцом R не являющееся. Пусть

$$L = \mathbb{Z}, \quad R = \mathbb{Z} \times \mathbb{Z}.$$

Имеет место вложение $\mathbb{Z} \hookrightarrow \mathbb{Z} \times \mathbb{Z}$:

$$x \mapsto (x, 0).$$

Теперь остается заметить, что образом $1_L \in \mathbb{Z}$ является $(1, 0)$, тогда как $1_R = (1, 1)$.
