Структура кольца

Содержание

§1. Два закона композиции на множестве

NtB 1.1. Пусть на множестве M задано два всюду определенных закона композиции, которые мы обозначим через $\circ$ и $*$.

Опр. 1.1. Закон композиции $\circ$ называется **дистрибутивным слева** относительно закона $*$, если для любых элементов $x, y, z \in M$ имеет место равенство

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

NtB 1.2. Соответственно, **дистрибутивность справа** означает выполнение следующего равенства:

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

Если закон дистрибутивен и слева и справа, то он называется **двояко дистрибутивным**.

Пример 1.1. Если в M существует *нейтральный элемент* e относительно $*$ и $\circ$ двояко дистрибутивен относительно $*$, тогда элемент e является *поглощающим* относительно закона $\circ$:

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

NtB 1.3. 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 $\circ$.

Опр. 1.2. Кольцом R называется множество замкнутое относительно двух согласованно заданных на нем бинарных операций (обычно обозначаемых через $+$ и $\cdot$), удовлетворяющих следующим требованиям:

- R - абелева группа относительно $''+''$ (0 - нейтральный элемент);
- R - коммутативный моноид относительно $''\cdot''$ (1 - нейтральный элемент);
- Законы $+$ и $\cdot$ согласованы ($''\cdot''$ дистрибутивен относительно $''+''$):

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

§2. Примеры колец

Пример 2.1. Примеры колец:

(а) Нулевое кольцо:

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

(б) Целые числа:

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

(в) Пифагорово кольцо:

$$\mathbb{Z}[\sqrt{2}] = \left\{ x + \sqrt{2}y : \quad x, y \in \mathbb{Z} \right\}. \tag{1}$$

(г) Кольцо $\mathbb{Z}_m$ вычетов по модулю $m \in \mathbb{Z}$:

$$x \equiv y \mod m, \quad y \in \{0, 1, \ldots, m-1\}.$$

§3. Кольцо многочленов

Опр. 3.1. Многочленом от одной переменной с коэффициентами из кольца R будем называть формальную бесконечную сумму следующего вида:

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots,$$

где отличны от нуля только *некоторые* **коэффициенты** $a_0, a_1, a_2, \ldots \in R$, а x является **формальной переменной**.

NtB 3.1. Операции на множестве многочленов $R[x]$ определяются стандартно и *индуцируют* на нем структуру кольца, при этом

$$\theta(x) = 0, \quad 1(x) = 1.$$

Делимость многочленов

Опр. 3.2. Говорят, что многочлен $p(x)$ **делится на многочлен** $q(x)$ (пишут $p \vdots q$), если существует такой многочлен $g(x)$, что $p(x) = g(x) \cdot q(x)$.

Лемма 3.1. *Свойства делимости многочленов:*

- *если* $p(x) \vdots q(x)$ *и* $q(x) \vdots r(x)$, *тогда* $p(x) \vdots r(x)$;
- *пусть* $p(x), q(x) \vdots g(x)$, *тогда*

$$\forall a(x), b(x) \in R[x] \quad a(x)p(x) + b(x)q(x) \vdots g(x)$$

Опр. 3.3. Два многочлена $p(x)$ и $q(x)$ называются **ассоциированными**, если $p(x) = \alpha \cdot q(x)$, где $\alpha \in R$, $\alpha \neq 0$.

NtB 3.2. Тот факт, что $p(x)$ и $q(x)$ ассоциированы обозначают $p(x) \sim q(x)$.

Лемма 3.2. *Пусть* $p(x) \vdots q(x)$ *и* $q(x) \vdots p(x)$, *тогда* $p(x) \sim q(x)$.

Степень многочлена

Опр. 3.4. Степенью $\deg(p)$ многочлена $p \in R[t]$ называется максимальный номер его ненулевого коэффициента. Если $\deg p = n \in \mathbb{N}_0$ то коэффициент a_n называется **старшим коэффициентом** многочлена p.

NtB 3.3. Для нулевого многочлена $\theta(t)$ положим $\deg(\theta) = -\infty$.

Лемма 3.3. *Пусть* $p, q \in R[x]$ *тогда имеют место следующие свойства:*

$$\deg(pq) = \deg(p) + \deg(q), \quad \deg(p+q) \leqslant \max\{\deg(p), \deg(q)\}.$$

Лемма 3.4. *Свойства степени при делении многочленов:*

- *если* $f \vdots g, \quad f, g \neq 0 \quad \Rightarrow \quad \deg(f) \geqslant \deg(g)$;
- *если* $f \vdots g, \quad \deg(f) = \deg(g) \quad \Rightarrow \quad f \sim g$.

Лемма 3.5. *Пусть* $p, q \in R[x]$, *причем* $q \neq 0$, *тогда существуют единственные* $g, r \in R[x]$, *такие что*

$$p(x) = g(x)q(x) + r(x), \quad \deg(r) < \deg(q).$$

Опр. 3.5. Многочлен $r(x) \in R[x]$ называется **остатком от деления** многочлена $p(x)$ на многочлен $q(x)$.

Корень многочлена

Опр. 3.6. Корнем многочлена $p(x) \in R[x]$ кратности m называется число $x_0 \in R$, такое что

$$p(x) \vdots (x - x_0)^m, \quad p(x) \nvdots (x - x_0)^{m+1}.$$

Теорема 3.1. *Остаток от деления* $p(x) \in R[x]$ *на* $(x - x_0)$ *равен* $f(\alpha)$

Доказательство. По теореме от делении с остатком имеем:

$$p(x) = (x - x_0)g(x) + r(x), \quad \deg(r) \leqslant \deg(x - x_0) = 1$$

Следовательно, $r(x) = r \in R$ и

$$p(x_0) = 0 \cdot g(x) + r = r.$$

□

NtB 3.4. Если x_0 - корень многочлена $p(x)$ тогда $p(x_0) = 0$.