2 Теория колец

2.1 Введение

Определение 1. *Кольцо R - множество элементов с двумя бинарными операциями, такие что:*

1. $a + b = b + a$ *(коммутативность)*
2. $(a + b) + c = a + (b + c)$ *(ассоциативность)*
3. $\exists$ *нейтральный элемент относительно сложения:*
   $a + 0 = 0 + a = a, \forall a \in R$
4. $\exists$ *противоположный остностильно сложения:*
   $-a \in R \big| (-a) + a = a + (-a) = 0$
5. *ассоциативность*
   $a(bc) = (ab)c$
6. *дистрибутивность*
   $a(b + c) = ab + ac$
   $(b + c)a = ba + ca$

Теорема 1 (Свойства колец)**.** *Пусть $a, b, c \in R$ - кольцо*

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$
4. $a(b - c) = ab - ac$
   $(b - c)a = ba - ca$

   Кроме того, если R имеет единичный элемент 1 относительно умножения, то

5. $(-1)a = -a$
6. $(-1)(-1) = 1$

Теорема 2. *Если кольцо имеет единичный элемент, то этот элемент единственен. Если для $a \in R \exists a^{-1}$, то a^{-1} - единственен.*

Определение 2. *Подмножество S кольца R называется подкольцом в R, если само является кольцом относительно операции, заданных в R.*

Теорема 3 (Признак подкольца)**.** *Непустое подмножество S кольца R является подкольцом, если S замкнуто относительно операций минус и умножить, т.е. если* $\left.\begin{matrix} a - b \\ ab \end{matrix}\right\} \in R, \forall a, b \in S$

2.2 Кольца целостности

Определение 3. *Делитель нуля* $0 \neq a \in R$ *- коммутативное кольцо* $\big|\exists 0 \neq b \in R$ *и* $ab = 0$.

Определение 4. *Кольцо целостности - коммутативное кольцо с единицей без делителей нуля.*

Теорема 4. *Пусть* $a, b, c \in R$ *- кольцо целостности. Если* $a \neq 0$ *и* $ab = ac$, *то* $b = c$.

Доказательство. Рассмотрим $ab = ac$
$ab - ac = 0$
$a(b - c) = 0$, где $a \neq 0$
$\Rightarrow b - c = 0$
$b = c$ □

Определение 5. *Поле - коммутативное кольцо с единицей, в котором любой отличный от нуля элемент обратим.*

Теорема 5. *Конечное кольцо целостности является полем.*

Доказательство. Пусть D - конечное кольцо целостности с единицей.
Рассмотрим $0 \neq a \; in D$
Докажем, что a - обратим
Если $a = 1 \Rightarrow$ очевидно
Пусть $a \neq 1$
$\left.\begin{array}{l} a, a^2, a^3, ... \\ D \text{ - конечно} \end{array}\right\} \Rightarrow \exists i > j \big| a^i = a^j$
$\Rightarrow a^i - a^j = 0$
$a^j(a^{i-j} - 1) = 0$, где $a^j \neq 0$
$a^{i-j} = 1$
$\Rightarrow a^{i-j-1}$ - обратный к a. □

Следствие 1. *Для* $\forall p$ *- простых,* $\mathbb{Z}_p$ *- поле.*

Определение 6. *Характеристика кольца* R *- наименьшее положительное целое* $n \big| n \cdot x = 0, \forall x \in R$.
Если такого n *не существует, то будем говорить, что* R *имеет характеристику 0. Обозначается* $charR = n$.