Семинар №6 по курсу «Основы высшей алгебры и теории кодирования»

Репеев Роман, Шиманогов Игорь

Определение 1 (Кольцо)
Кольцо — это множество M с двумя бинарными операциями сложения (обозначается $+$) и умножения (обозначается $\cdot$, иногда опускается, как это принято в формулах элементарной алгебры), для которых выполняются следующие аксиомы:

1. относительно сложения M — коммутативная группа (которая называется аддитивной группой кольца), нейтральный элемент относительно сложения называется нулём и обозначается обычно как 0

2. умножение ассоциативно

3. $a \cdot (b + c) = a \cdot b + a \cdot c$
   $(b + c) \cdot a = b \cdot a + c \cdot a$

Заметим, что определения могут отличаться в различных источниках. Мы будем пользоваться именно этим.

Пример 1
Обычные числовые системы — целые, рациональные, действительные и комплексные числа — являются кольцами относительно обычных операций сложения и умножения чисел.

Покажем, что уже можно получить из этого определения. Заметим, что вычитанием в кольце называют, очевидно, сложение с обратным.

Задача 1 (Дистрибутивность вычитания)
Докажите, что в любом кольце $a(b-c) = ab - ac, (b-c)a = ba - ca$ для любых элементов a, b, c.

Решение $a(b-c) + ac = a(b + (-c) + c) = a(b+0) = ab \Rightarrow a(b-c) = ab - ac$

Задача 2 (Свойство нуля)
Докажите, что в любом кольце $a \cdot 0 = 0 = 0 \cdot a$.

Решение $a \cdot 0 = a(b-b) = ab - ab = 0$

Рассмотрим свойства, которые можно дополнительно накладывать на кольца.

Определение 2 (Коммутативное кольцо)
Кольцо называется коммутативным, если умножение в кольце коммутативно: $xy = yx$ для любых элементов кольца.

Определение 3 (Кольцо с единицей)
Кольцо называется кольцом с единицей, если в нём есть нейтральный элемент относительно умножения. Этот элемент называется единицей и обозначается 1.

Покажем, что можно получить из этих определений.

Задача 3 (Произведение минус единиц)
Пусть R — кольцо с 1. Докажите, что $(-1) \cdot (-1) = 1$.

Решение $0 = (-1) \cdot 0 = (-1) \cdot (1 + (-1)) = (-1) + (-1) \cdot (-1)$

Задача 4 (Разность квадратов)
Докажите, что в коммутативном кольце $a^2 - b^2 = (a-b)(a+b)$.

Решение $(a-b)(a+b) = a^2 + (-b)a + ab + (-b)b = a^2 + (-b)b + a((-b)+b) = a^2 + (-b)b$

$$0 = b^2 + (-b)b = (b + (-b))b = 0 \cdot b$$

Однако в кольцах не все так гладко, как хочется. Рассмотрим такой важный недостаток колец, как наличие делителей нуля.

Определение 4 (Делитель нуля)
Элемент $a \neq 0$ кольца R называется левым делителем нуля, если существует такой $b \neq 0$,

что $ab = 0$. Аналогично, a называется правым делителем нуля, если существует такой $b \neq 0$, что $ba = 0$.

Пример 2
В кольцах матриц могут встречаться делители нуля, например:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Поэтому, логично выделить наиболее «хорошие» кольца.

Определение 5 (Область целостности)
Коммутативное кольцо с единицей и без делителей нуля называется областью целостности.

Пример 3
Кольцо, которое состоит из комплексных чисел с целыми действительной и мнимой частями, называется кольцом гауссовых чисел. Оно является областью целостности.

Определение 6 (Нильпотентный элемент)
Элемент кольца a называется *нильпотентным*, если существует $k > 0$ такое, что $a^k = 0$.

Задача 5
Доказать, что если в коммутативном кольце R элемент a нильпотентный, то для любого $r \in R$ элемент ra также нильпотентный.

Решение Пусть $a^m = 0$.
Так как кольцо коммутативно, то $(ra)^m = r^m \cdot a^m = r^m \cdot 0 = 0$.

Определим теперь гомоморфизмы колец. Очевидно, определение будет очень похоже на определение гомоморфизма групп.

Определение 7 (Гомоморфизм колец)
Отображение $\varphi : R \mapsto R'$ на кольцах $\langle R, +, \cdot \rangle$ и $\langle R', \oplus, \otimes \rangle$ назывпается *гомоморфизмом*, если выполняется сохранение операций:

1. $\varphi(r_1 + r_2) = \varphi(r_1) \oplus \varphi(r_2)$
2. $\varphi(r_1 \cdot r_2) = \varphi(r_1) \otimes \varphi(r_2)$

Биективный гомоморфизм называется *изоморфизмом*.

Определение 8 (Идеал)
(Двусторонним/левым/правым) идеалом I кольца R называется такое множество, для которого выполняются два свойства:

1. I – подгруппа аддитивной группы кольца
2. для любого $a \in R$ и любого $i \in I$ выполнено $(ai \in I, ia \in I / ai \in I / ia \in I)$.

Для коммутативных колец разницы между двусторонними, левыми и правыми идеалами нет — эти понятия совпадают.

Лемма 1 (Пересечение идеалов)
Пересечение идеалов — это идеал.

Пример 4
Возьмём кольцо целых чисел $\mathbb{Z}$. Выберем в нем фиксированный элемент n, и рассмотрим все его кратные, то есть множество $n\mathbb{Z} = \{rn : r \in \mathbb{Z}\}$. Это множество – идеал, что легко проверить из определения. На самом деле, других идеалов там и нет, но доказывать мы это, конечно, не будем.

Определение 9 (Главный идеал)
Пусть S — подмножество кольца R. Идеал, порождённый множеством S (обозначается (S)), — это пересечение всех идеалов, содержащих S.
Идеал называется главным, если он порождён одним элементом. Обозначается идеал как (a).

Замечание 1
Главный идеал, порожденный элементом a можно записать в виде

$$(a) = \{ra + na \mid r \in R, n \in \mathbb{N}\}$$

Если в кольце есть единица, эта запись упрощается:

$$(a) = \{ra \mid r \in R\}$$

Пример 5
Казалось бы, идеал $(12, 15)$ *не главный. Но это не так.* $(12, 15) = (3)$

Определение 10 (Кольцо главных идеалов)
Кольцо, в котором все идеалы, отличные от самого кольца, — главные, называется кольцом главных идеалов.

Определение 11 (Класс вычетов)
Классами вычетов по модулю идеала I называются смежные классы по I как аддитивной подгруппе кольца.

Пример 6
Вычеты по идеалу $n\mathbb{Z}$ в кольце $\mathbb{Z}$:

$$\begin{aligned} 0 + n\mathbb{Z} &= \{rn \mid r \in \mathbb{Z}\} = \overline{0} \\ 1 + n\mathbb{Z} &= \{1 + rn \mid r \in \mathbb{Z}\} = \overline{1} \\ &\dots \\ (n-1) + n\mathbb{Z} &= \{(n-1) + rn \mid r \in \mathbb{Z}\} = \overline{(n-1)} \end{aligned}$$

Будем далее рассматривать только двусторонние идеалы. Для них мы получим, что классы вычетов также образуют кольцо.

Определение 12 (Сравнимые элементы)
Два элемента a и b называются *сравнимыми по модулю идеала I*, если они находятся в одном классе вычетов, то есть $a = r + i_1,\ b = r + i_2$, где $r_1, r_2 \in I$.
В этом случае пишут $a \equiv b \mod I$ или просто $a \equiv b$.

Утверждение 1
$a \equiv b \mod I \Longleftrightarrow a - b \in I$.

Доказательство Если $a = r + i_1,\ b = r + i_2$, то $a - b = i_1 - i_2 \in I$.
Обратно, если $a - b = i \in I$, то $a = i + b \in b + I \Rightarrow a \equiv b$.

Утверждение 2
Если $a_1 \equiv a_2$ и $b_1 \equiv b_2$, то $a_1 + b_1 \equiv a_2 + b_2$, $a_1b_1 \equiv a_2b_2$.

Доказательство
1) $a_1 - a_2 \in I$, $b_1 - b_2 \in I \Rightarrow (a_1 + b_1) - (a_2 + b_2) \in I$
2) $a_1b_1 - a_2b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2 \in I$
Здесь мы использовали, что идеал двусторонний.

На основе этих утверждений можно утверждать о корректности следуеющего определения.

Определение 13 (Факторкольцо)
Факторцольцом или *кольцом классов вычетов* по двустороннему идеалу I называется множество классов вычетов $R/I = \{\overline{r} = r + I \mid r \in R\}$ с определенными на нем операциями

$$\overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}$$

$$\overline{r_1} \cdot \overline{r_2} = \overline{r_1 r_2}$$

Определение 14
Ядром гомоморфизма называют прообраз **нуля**

$$\text{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\}$$

Утверждение 3
Ядро любого гомоморфизма является двусторонним идеалом.

Для факторколец существует теорема аналогичная такой для групп.

Теорема 1 (О гомоморфизме колец)
Пусть $\varphi : \ R_1 \mapsto R_2$ — гомоморфизм колец. Тогда факторкольцо по модулю ядра гомоморфизма изоморфно гомоморфному образу кольца:

$$R_1/\mathrm{Ker}\varphi \cong \varphi(R_1)$$

$$(a) = \{ra \mid r \in R\}$$

Задача 6 (Вторая теорема о гомоморфизме?)
Пусть A подкольцо R, а B идеал в R. Докажите, что $A/(A \cap B) \cong (A + B)/B$.

Решение То что $A \cap B$ — идеал, а $(A + B)$ — подкольцо достаточно очевидно. Перейдем непосредственно к доказательству утверждения. Рассмотрим гомоморфизм $f : A \to R/B$, который каждому элементу ставит его класс вычетов $f(a) = a + B$. Несложно заметить, в ядре находятся те элементы A, которые сами лежат в B: $\mathrm{Ker}f = A \cap B$. С образом все немного сложнее.

$$\mathrm{Im}f = \{f(a)|a \in A\} = \{a + B|a \in A\} = \{a + b + B|a \in A, b \in B\} = (A + B)/B$$

Используя теорему о гомоморфизме колец получаем нужное утверждение.