

ЛЕКЦИЯ 22

Определение 1. Идеал алгебры – это идеал I этой алгебры, как кольца, являющийся векторным подпространством.

Замечание 1. На самом деле относительно суммы и взятия противоположного идеал кольца всегда замкнут. Что может быть не выполнено – это замкнутость относительно умножения на элемент поля. Однако, если наша алгебра A с единицей, то поле F вкладывается в A путем $\lambda \mapsto \lambda \cdot 1$. При этом для любого $x \in I$, где I – идеал A как кольца, выполнено $\lambda x = (\lambda \cdot 1)x \in I$. Таким образом, любой идеал алгебры с единицей как кольца является идеалом этой алгебры как алгебры.

Если у нас есть идеал I в алгебре A , то на факторкольце можно определить операцию умножения на элемент поля посредством $\lambda \cdot (a + I) = \lambda a + I$. Легко проверить, что эта операция определена корректно и превращает факторкольцо A/I в алгебру, которую называют *факторалгеброй*.

Таким образом, $F[x]/(f)$ – алгебра над F .

Лемма 1. *Базис этой алгебры $\{1 + (f), x + (f), \dots, x^{n-1} + (f)\}$, где $n = \deg f$.*

Доказательство. Пусть $g(x) \in F[x]$. Поделим g на f с остатком: $g(x) = q(x)f(x) + r(x)$. Тогда $g + (f) = r + (f)$. Но $\deg r(x) \leq n-1$. Значит, $r(x)$ является линейной комбинацией $1, x, \dots, x^{n-1}$. Мы доказали, что $\{1 + (f), x + (f), \dots, x^{n-1} + (f)\}$ – полная система.

Докажем линейную независимость. Пусть $\sum_{i=0}^{n-1} \alpha_i(x^i + (f)) = 0$. Положим $h(x) = \sum_{i=0}^{n-1} \alpha_i x^i$. Тогда $h + (f) = 0 + (f)$. Это значит, что $h \in (f)$, то есть h делится на f , чего не может быть, так как $\deg h(x) < \deg f(x)$. \square

Замечание 2. Если мы имеем алгебру A размерности n над полем \mathbb{Z}_p , то $|A| = p^n$. В самом деле, пусть $\{e_1, \dots, e_n\}$ – базис A . Тогда $A = \{\lambda_1 e_1 + \dots + \lambda_n e_n \mid \lambda_i \in \mathbb{Z}_p\}$. Каждый коэффициент λ_i принимает p значений. Значит, всего p^n вариантов.

Пример 1. *Рассмотрим многочлен $f(x) = x^2 + x + 1$ в кольце $\mathbb{Z}_2[x]$. Проверим, что у $f(x)$ нет корней в \mathbb{Z}_2 . Действительно, $f(0) = 1$, $f(1) = 1$. Так как f – многочлен второй степени и у него нет корней, он неприводим. Значит, кольцо $\mathbb{Z}_2[x]/(x^2 + x + 1)$ является полем из 4 элементов. Построим таблицы сложения и умножения.*

+	0	1	x	x+1	·	0	1	x	x+1
0	0	1	x	x+1	0	0	0	0	0
1	1	0	x+1	x	1	0	1	x	x+1
x	x	x+1	0	1	x	0	x	x+1	1
x+1	x+1	x	1	0	x+1	0	x+1	1	x

Например, $(x + (f)) \cdot (x + (f)) = x^2 + (f) = x + 1 + (f)$.

Определение 2. Кольцо R называется *простым*, если в R нет других (двусторонних) идеалов, кроме $\{0\}$ и R .

Теорема 1. *Кольцо квадратных матриц $n \times n$ над полем является простым.*

Доказательство. Пусть I – ненулевой идеал в кольце матриц. Возьмем $A \neq 0 \in I$. Тогда найдутся i и j такие, что $a_{ij} \neq 0$. Рассмотрим $E_{ki} A E_{jl} = B \in I$. Несложно видеть, что $B = a_{ij} E_{kl}$. Так как $a_{ij} \neq 0$, получаем, $E_{kl} \in I$. Но так как числа k и l произвольные, все матричные единицы лежат в I . Но тогда для любой матрицы X имеем $X = \sum x_{ij} E_{ij} \in I$. \square

Заметим, что нетривиальные односторонние (например, левые) идеалы в кольце матриц есть. Например, множество матриц, у которых первый столбец нулевой, является левым идеалом.

Задача 1. Опишите все левые и правые идеалы в кольце матриц.

Лемма 2. *Левый (правый) идеал в кольце с единицей, содержащий обратимый элемент совпадает со всем кольцом.*

Доказательство. Пусть $I \triangleleft R$ – левый идеал некоторого кольца и пусть $a \in I$ – обратимый элемент. Тогда $a^{-1}a = 1 \in I$. Но тогда для любого $r \in R$ имеем $r = r1 \in I$. \square

Предложение 1. *Коммутативное (ассоциативное) кольцо с единицей является простым тогда и только тогда, когда это поле.*

Доказательство. Пусть R – поле. Тогда любой ненулевой идеал содержит обратимый элемент, и следовательно, совпадает с R .

Пусть теперь R – простое коммутативное кольцо. Рассмотрим $r \neq 0 \in R$. Тогда можно рассмотреть идеал (r) . Так как в этом идеале содержится $r \neq 0$, это ненулевой идеал. Значит, $(r) = R$. Тогда $1 \in (r)$, что означает $1 = xr$. \square

Далее мы рассматриваем только коммутативные кольца.

Определение 3. Коммутативное кольцо с единицей называется *областью целостности* или, что то же самое *целостным кольцом*, если в нем нет делителей нуля.

Определение 4. Идеал I в кольце R называется *простым*, если из того, что $ab \in I$ следует, что $a \in I$ или $b \in I$.

Пример 2. Идеал (n) в кольце \mathbb{Z} является простым тогда и только тогда, когда число n простое.

Предложение 2. *Факторкольцо R/I не имеет делителей нуля тогда и только тогда, когда I – простой идеал.*

Доказательство. Пусть $a + I$ и $b + I$ – ненулевые смежные классы. Это значит, что $a, b \notin I$. Тогда $(a + I)(b + I) = 0$ равносильно $ab \in I$. Но существование таких a и b , что $a, b \notin I$, а $ab \in I$ равносильно тому, что идеал I не простой. \square

Определение 5. Идеал I в кольце R называется *максимальным*, если не существует идеала $J \triangleleft R$ такого, что $I \subsetneq J \subsetneq R$.

Лемма 3. *Пусть $\psi: R \rightarrow S$ – гомоморфизм колец. Пусть J – идеал в S . Тогда полный прообраз $\psi^{-1}(J)$ – это идеал в R .*

Доказательство. Пусть $a, b \in \psi^{-1}(J)$. Тогда $\psi(a + b) = \psi(a) + \psi(b) \in J$ и $\psi(-a) = -\psi(a) \in J$, то есть $a + b \in \psi^{-1}(J)$ и $-a \in \psi^{-1}(J)$. Кроме того $\psi(ra) = \psi(r)\psi(a) \in J$, $\psi(ar) = \psi(a)\psi(r) \in J$, то есть $ra, ar \in \psi^{-1}(J)$. \square

Лемма 4. *Пусть $\psi: R \rightarrow S$ – сюръективный гомоморфизм колец. И пусть I – идеал в R . Тогда $\psi(I)$ – идеал в S .*

Доказательство. Пусть $a = \psi(x)$, $b = \psi(y)$, где $x, y \in I$. Тогда $x + y \in I$ и $\psi(x + y) = a + b \in \psi(I)$. И $-a = \psi(-x) \in \psi(I)$. Для любого $s \in S$ имеем $s = \psi(r)$ для некоторого $r \in R$. Тогда $sa = \psi(rx) \in \psi(I)$. \square

Теорема 2. Пусть R – коммутативное кольцо с единицей. Факторкольцо R/I – поле тогда и только тогда, когда I – максимальный идеал.

Доказательство. Рассмотрим канонический гомоморфизм (колец) $\pi_I: R \rightarrow R/I$, $\text{Ker } \pi_I = I$. Существование собственного идеала J такого, что $I \subsetneq J \subsetneq R$ равносильно существованию промежуточного идеала $\{0\} \subsetneq L \subsetneq R/I$ такого, что $\pi_I^{-1}(L) = J$. Но существование такого L равносильно тому, что R/I – не поле. \square

Определение 6. Пусть R – область целостности, не являющаяся полем. Тогда R называется *евклидовым кольцом*, если задана функция (*евклидова норма*) $N: R \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$ такая, что

- 1) $N(ab) \geq N(a)$ для любых $a, b \in R \setminus \{0\}$
- 2) для любых $a, b \in R$, $b \neq 0$ возможно "деление с остатком" то есть существуют такие $q, r \in R$, что $a = bq + r$, причем либо $N(r) < N(b)$, либо $r = 0$.

Пример 3. 1) $R = \mathbb{Z}$, $N(a) = |a|$.

2) $R = F[x]$, $N(f) = \deg f$.

3) **Задача.** Докажите, что $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ – евклидово кольцо с нормой $N(z) = |z|$.

4) **Задача.** Для каких $c \in \mathbb{R}$ кольцо $\mathbb{Z}[ci] = \{a + bci \mid a, b \in \mathbb{Z}\}$ является евклидовым кольцом с нормой $N(z) = |z|$?

Определение 7. Область целостности R с единицей назовем *кольцом главных идеалов*, если любой идеал в нем главный, то есть равен (r) для некоторого $r \in R$.

Пример 4. Идеал (x, y) в $F[x, y]$ не является главным. Действительно, если $(x, y) = (f)$, то f делит и x и y . Тогда f – константа и $(f) = F[x, y]$.

Теорема 3. Евклидово кольцо является кольцом главных идеалов.

Доказательство. Пусть R – евклидово кольцо с нормой N . И пусть $I \triangleleft R$. Если $I \neq \{0\}$, рассмотрим ненулевой элемент $a \in I$ с минимальной нормой. Пусть $b \in I$. Тогда $b = aq + r$. Предположим, что $r \neq 0$. Получаем $r \in I$, $N(r) < N(a)$. Противоречие с выбором a . Значит, $r = 0$, то есть $b \in (a)$. Следовательно, $I = (a)$. \square

Определение 8. Пусть a и b – два элемента кольца главных идеалов. Рассмотрим $(a, b) = (d)$. Назовем d *наибольшим общим делителем* a и b . (НОД определен с точностью до обратимого множителя.)

Имеем $d \mid a$, $d \mid b$, $d = ua + vb$.

Определение 9. 1) Пусть R – область целостности. Необратимый элемент $r \in R$ называется *неприводимым*, если из $ab = r$ следует, что либо a , либо b обратим.

2) Два элемента $u, v \in R$ называются *ассоциированными*, если $u = cv$, где c – обратимый элемент.

3) Кольцо (область целостности) R называется *факториальным*, если любой элемент раскладывается в произведение неприводимых единственным способом с точностью до порядка и ассоциированности сомножителей.

Лемма 5. Пусть R – кольцо главных идеалов, p – неприводимый элемент. Допустим, что $p \mid ab$. Тогда либо $p \mid a$, либо $p \mid b$.

Доказательство. Пусть $s = \text{НОД}(a, p)$. Тогда $s \mid p$. Значит, либо s ассоциирован с p , либо $s = 1$. Если $s = p$, то $p \mid a$. Если же $s = 1$, то существуют $u, v \in R$ такие, что

$ua + vr = 1$. Домножим это равенство на b . Получим $uab + vrb = b$. Левая часть делится на p . Значит, и правая часть делится на p . \square

Следствие 1. Пусть R – кольцо главных идеалов, p – неприводимый элемент. Допустим, что $p \mid a_1 a_2 \dots a_k$. Тогда найдется j такой, что $p \mid a_j$.

Теорема 4. Кольцо главных идеалов факториально.

Доказательство. Существование. Пусть R – кольцо главных идеалов и $a \in R$. Если a не является неприводимым, то $a = bc$ для некоторых необратимых b и c . Тогда имеем $(a) \subsetneq (b)$ и $(a) \subsetneq (c)$. Если оба множителя неприводимы, то получено разложение. Иначе какой-то из них снова можно разложить, что даст увеличение идеала и т.д. Если разложения так и не будет, получим бесконечно возрастающую цепочку $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \dots$

Рассмотрим $I = \cup (a_i)$. Легко видеть, что I – идеал. Значит, $I = (b)$. Но $b \in \cup (a_i)$, значит, найдется j такой, что $b \in (a_j)$. Тогда $I = (a_j)$. То есть бесконечно возрастающих цепочек не может быть.

Единственность. Пусть $a = p_1 \dots p_k = q_1 \dots q_m$ – два разложения на неприводимые. Тогда $p_1 \mid q_1 \dots q_m$. Значит, существует j такое, что $p_1 \mid q_j$. Так как p_1 и q_j неприводимы, они ассоциированы. Значит, перебрасывая обратимый элемент в другой множитель и меняя нумерацию, можно считать $p_1 = q_1$.

$$p_1 p_2 \dots p_k = p_1 q_2 \dots q_m.$$

Перенесем все в одну часть.

$$p_1 (p_2 \dots p_k - q_2 \dots q_m) = 0.$$

Так как $p_1 \neq 0$ и в R нет делителей нуля, получаем $p_2 \dots p_k = q_2 \dots q_m$ и т.д. \square