Теория с лекций. Алгебра

Содержание

1 Алгебра

Рекомендуемая литература

1. Кострикин "Основа алгебры"(1том)
2. Винберг "Курс алгебры"
3. Лэнг "Алгебра"
4. Сборник задач по алгебре под редакцией Кострикина
5. Сборник задач Фадеева и Соминского

1.1 Кольцо

Пусть A - некоторое непустое множество. Пусть на нем даны операции: $(a, b) \to (a + b); (a, b) \to (ab); a, b \in A$
Дадим определение операциям сложения и умножения:

1. $\forall a, b, c \in A : a + (b + c) = (a + b) + c$ - ассоциативность по сложению
2. $\exists 0 \in A, \forall a \in A : a + 0 = 0 + a = a$
3. $\forall a \in A, \exists b \in A : a + b = b + a = 0$ b - противополжный a элемент
   Удостоверимся в том, что 0 - единственный:
   $$\begin{cases} a + 0 = o + a = a \\ a + 0` = 0` + a = a \\ \forall a \in A \end{cases} \leftrightarrow \begin{cases} 0` + 0 = o + 0` = 0` \\ 0 + 0` = 0` + 0 = 0 \\ \forall a \in A \end{cases} \leftrightarrow 0 = 0`$$
4. $\forall a, b \in A : a + b = b + a$ - коммутативность по сложению
5. $\forall a, b, c \in A : (a + b)c = ac + bc = bc + ac$

Множество, которое удовлетворяет этим аксиомам - кольцо в широком смысле. В нашел курсе мы будем рассматривать более частный вариант кольца, добавив еще несколько определений:

1. $\forall a, b \in A : ab = bc$ - коммутативность по умножению
2. $\forall a, b, c \in A : a(bc) = (ab)c$ - ассоциативность по умножению
3. $\forall a \in A : a * 1 = 1 * a = a$

Есть кольцо где выполняется еще одна аксиома:
$\forall a \in A, a \neq 0, \exists b \in A : ab = ba = 1$
Если выполнены все эти аксиомы, то такое множество называется полем.
Примеры колец:

1. $\mathbb{Z}$
2. A $= 0$
3. $d \in \mathbb{N}, \sqrt{d} \neq \mathbb{Z}$, образующие множества $[\sqrt{b}]\mathbb{Z}$

Примеры полей:

1. $\mathbb{Q}$
2. $\mathbb{R}$
3. $\mathbb{C}$

Если есть 2 кольца A,B, то мы можем образовать их произведение и сложение следующим образом:

1. $(a_1; b_1) + (a_2; b_2) = (a_1 + a_2; b_1 + b_2)$
2. $(a_1; b_1) * (a_2; b_2) = (a_1 * a_2; b_1 * b_2)$

Мы можем аналогично задать произведение $A_1 * A_2 .... * A_n$:
Доказательство этого утверждения проведем по индукции (в данном случае свойства ассоциативности):
База: при n =3 - доказано по аксиоме.
Переход: Есть произведение $(x_1 ... x_k)(x_{k-1} ... x_n)$.
Введем понятие левонормированного произведения: $(...(x_1 x_2) x_3) ..... x_n)$ - левонормированное произведение. Такое произведение можно раскрыть с помощью ассоциативности умножения (и привести любое произведение к такому виду).
Тогда если в левой скобки будет 1 элемент, то мы получили еще одно левонормированное проивзедение и победили.
Если же нет, то тогда рассмотрим две скобки. К правой применим свойство ассоциативности. Тогда вновь получим случай для n-1, т.е мы победили.
Аналогично для сложения.
Докажем еще одно свойство: $(-a)b = -ab$
Прибавим к обеим частям ab:
$ab + (-a)b = ab + (-ab) \leftrightarrow b(a + (-a)) =$

1.2 Понятние идеала для кольца.

Пусть I - непустое множество A, при этом $x, y \in I \rightarrow x + y \in I; x \in I, a \in A :$ $ax \in I$
Если $1 \in I \Rightarrow \forall a \in A : a \in I$
Такой идеал называется единичным.
0 - всегда принадлежит иделу, докажем это.
$x \in I \Rightarrow x * (-1) = -x \in I; x + (-x) = 0 \in I$
0 - нулевой идеал
Найдем все иделы целых чисел. Возьмем $k \in \mathbb{Z}, k\mathbb{Z}$ - это идеал. Причем

других идеалов нет.
Теорема.
Для любого идела кольца $\mathbb{Z}$ имеет вид $k\mathbb{Z}, k \in \mathbb{Z}$. Если идеал нулевой, то теорема доказана. Теперь предположим, что идеал не нулевой. Тогда в нем точно будут положительные числа. Пусть k - наименьшее положительное число в I. Тогда $k\mathbb{Z} \in I$.

Возьмем $x \in \mathbb{Z}$. Докажем, что $x \vdots k$.
Поделим x на k с остатком. $x = kq + r \Rightarrow r = x - kq; r \in I$. Но r меньше k, противоречие! Так что r $= 0$.
Теорема доказана
Ненулевое кольцо - область целостности/область/целостное кольцо, если $\forall a, b \neq 0 : ab \neq 0$
Если $ab = 0 \Rightarrow a = 0 \vee b = 0$
Приме. $\mathbb{Z}$, любое поле.
Область целостности, в котором $\forall$ идеал главный называется кольцом главных идеалов. Идеал главный, если он имеет вид $(a), a \in A$. Поля можно охарактеризовать как кольца имеющие 2 главных идела (0) и (1). Фактор кольцо по классу.
A - кольцо, I - идел в A.
A/I - фактор кольцо по иделу I.
$x \in A, x + I = \{x + i, i \in I\}$ - класс эл-та x относ I
$\{x + I, x \in A\}$ - мн-во всех классовю.
Пример. Любые два класса либо не пересекаются, либо совпадают.
$c \in (x + I) \cup (y + I); c = x + i_1 = y + i_2, i_3 = x - y = i_1 - i_2 \in I$ Пусть C_1, C_2 - два класса. Докажем, что:
$C_1 + C_2 = (x_1 + x_2) + I = (y_1 + y_2) + I;$
$C_1 = x_1 + I = y_1 + I; C_2 = x_2 + I = y_2 + I$
$(y_1 + y_2) - (x_1 + x_2) = (y_1 - x_1) + (y_2 - x_2) \in I$
$C_1C_2 = x_1x_2 + I = y_1y_2 + I;$
$y_1y_2 - x_1x_2 \in I; y_1y_2 - x_1x_2 = y_1(y_2 - x_2) - y_2(y_1 - x_2) \in I$
$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, ...(n - 1) + n\mathbb{Z}\}, n$ классов,$n \in \mathbb{Z}, n \neq 0, n > 0$
Изоморфизм колец.
Гомоморфизм колец - пусть A и B - 2 кольца, f:$A \to B$
f - гомоморфизм колец, если выполнены следующие равенства:

1. $\forall a_1, a_2 : f(a_1 + a_2) = f(a_1) + f(a_2)$
2. $\forall a_1, a_2 : f(a_1a_2) = f(a_1)f(a_2)$
3. $f(1_a) = 1_b$

$f(0) = f(0) + f(0) \Leftrightarrow f(0) = 0$
$f(1) = f(1 * 1) = f(1) * f(1) = 1 \Rightarrow f(1) = 1$
Пример когда это свойство не выполнено: $\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$
Мономорфизм, это гомоморфизм: $\forall a_1, a_2 \in A : f(a_1) = f(a_2) \Rightarrow a_1 = a_2$
Элиморфизм: $\forall b \in B; \exists a \in A : f(a) = b$
Изоморфизм - аналог биекции.

Операции над множествами.
1) Пересечение: I_i - идеал в A, $\cap I_i$ - идеал в A.
2) Произведение конечного числа идеалов - есть идеал.
3) Сумма конечного числа идеалов - есть идеал.
$\Sigma I_i = \{\Sigma(\alpha_1 + \alpha_2 + ... + \alpha_n)\}$, где $\forall \alpha_i \in I_j$
Сумма идеалов - это наименьший по включению идеал, содержащий все идеалы I_i.
Произведение:$\sqcap I_i = \{\Sigma x_1 x_2 ... x_k; x_i \in I_i\}$
Идеалы I и J - взаимнопросты, если: I+J =(1)
Пример: A - целые числа, и $(9), (8) : 1 = (-1) * 8 + 9 * 1$

1.3 Китайская теорема об остатках (КТО)

A - кольцо, $n > 2, I_1, I_2, ... I_n$ - идеалы кольца, такие что:
$\forall i, j i \neq j : I_i + I_j = (1)$
Тогда существует изоморфизм колец $a / \cap I_i = (A/I_1) \times (A/I_2) \times ...$
Устроенный следующим образом:
Класс элемента $a`(mod \cup I_i) = a`(mod I_1) a`(mod I_2)...$
Проверим, что такое отображение взаимнооднозначно:
1) Корректность: если классы одинаковы $a + \cap I = a` + \cap I \Leftrightarrow a - a` = \cap I \in I$, откуда класс по модулю I_i совпадает с классом по модулю $\cap I_i$.
Проверим на гомоморфизм:
f - гомоморфизм. $a`(mod \cap I_i), b`(mod \cap I_i) : f(a` + b`) = f(a`) + f(b`)$.
По определению отношения: $f(a` + b`) = f(a` + b`(mod I_1), ... a` + b`(mod I_n))$
$f(a`) + f(b`) = (a`(mod I_1), a`(mod I_2), ... + b`(mod I_1), b`(mod I_2)....)$ - что то же самое.
Аналогично для проивзведения и единичного элемента.
Проверим, что если $a \to a`, b \to b`, a` = b` \Rightarrow a = b$
Откуда наш гомоморфизм - мономорфизм.
$(a`(mod I_1), a`(mod I_2)....) = (b`(mod I_1), b`(mod I_2), ...)$
$A \to A/I, a \to a`(mod I)$
Равенство покомпонентно, откуда получим:
$a - b \in I_1, I_2, ... \Leftrightarrow a - b \in \cap I_i \Rightarrow a`(mod \cap I_i) = b`(mod \cap I_i)$
Теперь начнем доказательство КТО по индукции:
n=2: $I_1 + I_2 = (1), A/I_1 \cap I_2 \simeq A/I_1 \times A/I_2$ Берём любую пару из п.ч.: $b`(mod I_1); c`(mod I_2)$
$a \in A : a - b \in I_1, a - c \in I_2$
$a = b + i_1 = c + i_2 \Leftrightarrow b - c = i_2 - i_1; i_1 \in I_1, i_2 \in I_2$
$I_1 + I_2 = (1); x_1 + x_2 = 1 \Leftrightarrow (b - c)(x_1 + x_2) = (b - c); x_1 \in I_1; x_2 \in I_2$
$x_1(b - c) + x_2(b - c) = (b - c)$
Тогда выберем $i_1 = x_1(b - c); i_2 = x_2(b - c)$
Лемма.
Пусть $I_1, I_2 ... I_n$ - идеалы, такие что $I_1 + I_i = (1), \forall i \geq 2$ Тогда $I_1 + \cap I_i = (1)$
Доказательство:
$x_2, x_3 .... x_n \in I_1, y_i \in I_i : x_i + y_i = 1$
$\sqcap (x_i + y_i) = y_2 y_3 ... y_n \in \cap I_i + (x_2 * y_1 ... + ... x_n y_2 ...) \in I_1 = 1$

Откуда по лемме: $A/\cap I_i \simeq A/I_i \times A/\cap I_i$ Идуктивный переход очевиден.

1.4 Понятие простого и максимального идеала

Простой идеал - это такой идеал, что: $I \neq (1); \forall x, y : xy \in I \Rightarrow x \in I \vee y \in I$
Максимальный идеал - это такой идеал, что: $I \neq (1); I \in J; I \neq J \Rightarrow J = (1)$
Опишем их в конце целых чисел.
Теорема.
$\forall I_{max}-$ простой. Доказательство.
$x, y \notin I \Rightarrow xy \notin I$
$I \subsetneq I + (x) \Rightarrow I + (x) = (1); I + (y) = (1)$
$i_1 + ax = 1$
$i_2 + by = 1, a, b \in A$
$i_1 i_2 + by i_1 + ax i_2 + abxy = 1(\alpha)$
Если $xy \in I$. Но тогда $\alpha \in I \Rightarrow 1 \in I \Rightarrow I = (1)$
Противоречие, значит $xy \notin I$
Если $A = \mathbb{Z}; (a)$ - максимальные идеалы. Если $a \neq 0$ - то идеал не максимальный. $a \neq 1$ - не максимальный.
$a \geq 2$

1. Если a - составное, то a = bc, где b,c≠1. Значит идеал не максимальный $(a) \subsetneq (b)$

2. a - простое; a = p. Тогда идеал максимальный. $(p) \subset I \subset \mathbb{Z}$

Чтобы доказать, что он максимальный, нужно доказать, что он не совпадает с $x \in I; x \neq kp$;

$(p) \subset (p) + (x); (x) + (p) = (b) \Rightarrow p \vdots b; x \vdots b \Rightarrow b = p \wedge b = 1$

Если b=1, то доказано. Если b=p: $(x) \vdots p$- что противоречит условию.
Предложение.
$I \subset A$
1)I - простое $\Leftrightarrow A/I$ - целостное. 2) I - макс A/I - поле.

1.5 Евклидовы кольца

A - целостное, $\exists f(A\{0\}) \Rightarrow \mathbb{Z}_0^+$;
$a \to ||a||; \forall a, b \in A, b \neq 0 : \exists q, r \in A : a = bq + r, r = 0 \vee r \neq 0; ||r|| < ||b||$
Пример.
A - кольцо целых чисел, ||b||=|b|.
Иногда в опр включают ||ab||≥||a||
Теорема.
∀ евклидова кольца - является кольцом главных идеалов.
Доказательство:
Пусть I - ненулевой идеал; $a \in I$:
$||a|| = min||i||; i \in I`\{\}$
Возьмем $i \in I; i = aq + r$ r - остаток при делении a на b.

$r \neq 0 : r = i - aq \in I; ||r|| \leq ||a||$ - противоречие.
$I \subset (a) \Rightarrow I = (a)$
Пример.
$A = \frac{a+b\sqrt{-19}}{2}; a, b \in \mathbb{Z}; a \equiv b(mod 2)$
Кольцо главных идеалов, но не евкидово.

1.6 Факториальное кольцо

А - область целостности. а - обратимый, если $\exists b \in A : ab = 1; a \in A$ - неразложимый элемент, если:
1) а - необратимый
2) $a = bc \Leftarrow b \vee a$ - обратимые.
(а) - простой, тогда а - неразлодимый элемент.
$a = bc \in (a) \Rightarrow b \in (a) \vee c \in (a)$
$b = ad \Rightarrow a = adc; a(1 - dc) = 0; cd = 1 \Rightarrow c-$обратимо
Опр.
Область целостности А - факториальное кольцо, если $\forall a \neq 0 \in A$:
1) Существует разложение $a = up_1p_2..., p_i$ -неразложимые, u - обратимое.
2) Если существует 2 разложения: $a = up_1p_2...p_n = vq_1q_2...q_m$, тогда n=m;
Существует взаимнооднозначное отображение $(1, 2, ..., n) \rightarrow (1, 2, ...m)$
Теорема.
Любое кольцо главных идеалов - факториальное.
$(x, y) \subset k[x, y]$
$\exists$ разложение$0 \neq a; a = up_1p_2...p_n$ Доказательство.
Предположим для элемента а такого разложения не существует.
$(a) \subset (a_1) \subset ... \subset (a_n), a_i \in A$
—
Лемма.
Такая цепочка со временем стабилизируется, т.е. начиная с некоторого i все они совпадают.
$\exists n : (a_n) = (a_{n+1}) = ...$
Доказательство.
$\cup(a_k)$ - идеал.
$x, y \in \cup(a_i)$, будем считать, что они принадлежит одному идеалу.
$x \in (a_k); y \in (a_s), k \in s \Rightarrow x, y \in (a_i) \Rightarrow x + y \in (a_i)$
Любой идеал главный $\Rightarrow \cup(a_i) = (b) \Rightarrow b \in (a_k) \Rightarrow (b) \subset (a_k) \subset (b) \Rightarrow (b) = (a_k)$
Получили, что: $(a) \subset (a_1) \subset .... \subset (a_k) = (a_{k+1}) = ...$
—
Вернемся к док-ву.
а - неразложимый, значит он представим в виде bc, где b,c -необратимы, и один из них неразложим.
Пусть b - неразложим.
Сравним главные идеалы а и b: $(a) \subsetneq (b)$. Иначе получили бы a=adc, откуда получили бы, что c - обратимый.

Построим идеал строго больший а. Тогда мы аналогично смогли бы построить $(a) \subsetneq (a_1) \subsetneq ...$, что противоречит лемме.
Докажем, что разложение единственно.
$a = up_1p_2...p_n = vq_1q_2...q_m$
Проведем индукцию по количеству элементов в правой части.
База: m=0 - очевидно.
m>0: $q_m \Rightarrow up_1p_2...p_n \in (q_m)$
Докажем, что (p_m) - простой.
Пусть π неразложимый элемент элемент $\Rightarrow (\pi)$- простой.
Проверим: пусть $xy \in (\pi); (\pi; x); x \notin \pi = (a)$
$\pi \vdots a \Rightarrow \pi = ab, \pi-$ неразложимый$\Rightarrow a \vee b$ - обратимы.
Если b - обратимо, то $(\pi) = (a) \Rightarrow (\pi, x) = (a)$ противоречие
Если a - обратиый, то $(a) = (1) \Rightarrow (\pi, x) = (1)$
$\alpha\pi + \beta x = 1/ * y \Leftrightarrow \alpha y\pi + \beta xy = y \Rightarrow y \in \pi$
Что и требовалось$\Rightarrow p_n \in (q_m)$
$p_n = q_m * u_m$.
Получаем результат (Евклидовы кольца)$\subset$(Кольца главных идеалов)$\subset$(факториальные кольца)

1.7 Разложение простых на сумму квадратов

Задача. Выяснить какие $p = a^2 + b^2$ и в каких случаях оно единственно?
Предложение.
Кольцо $\mathbb{Z}[i] = \{a + bi\}, a, b \in \mathbb{Z}; i = \sqrt{-1}$, евклидово относительно $||u + iv|| = u^2 + v^2$
$a + bi; c + di \neq 0 \in \mathbb{Z}[i];$
$(a + bi) \neq k(c + di), k \in \mathbb{Z}$
Рассмотрим комплексное число:
$\frac{a+bi}{c+di} = \alpha + \beta i$. Т.к. $a, b, c, d \in \mathbb{Z} \Rightarrow \alpha, \beta \in \mathbb{Q};$
$|\alpha - |\alpha| \leq 0; |\alpha|$- тут, это окрукгление, т.е.$\alpha \in [m; m + 1] \Rightarrow \exists u : |u - \alpha| \leq 0,5$.
Аналогично определим v для β.
$a + bi = (\alpha + \beta i)(c + di) = (c + di)(u + vi) + (c + di)((\alpha - u) + (\beta - u)i)$
$||(c + di)((\alpha - u) + (\beta - v)i))|| = ||c + di|| * ||(\alpha - u) + (\beta - v)i|| =$
$= (c^2 + d^2)((\alpha - u)^2 + (\beta - v)^2) \leq (c^2 + d^2) * \frac{1}{2} = \frac{||c+di||}{2} < ||c + di||$
Откуда получаем,что кольцо евклидово, и из вышедоказанного, что оно факториальное.
Возьмем произвольное число вида 4k+1=p и посмотрим будет ли оно простым в кольце.
p - простое. $p\mathbb{Z} = (p) - max$ идеал
$\mathbb{Z}/p\mathbb{Z}$- поле. Докажем это:
Вощьмем ненулевой остаток такой, что при домножении на него получаются ненулевые и попарно различные остатки. То что они не нулевые следует из факториальности.
Берем $\overline{k_1 a} = k_2\overline{a} \Leftrightarrow \overline{a}(\overline{k_1} - \overline{k_2}) \vdots p \Leftarrow k_1 - k_2 \vdots p \Leftarrow k_1 = k_2$
—

Докажем теорему Вильсона.

p - простое $\Rightarrow (p-1)!+1 \vdots p$
Возьмем $p \geq 5 \overline{a} \in \{\overline{2}, ..., \overline{p-2}\} = P_k$
$\overline{a} - \overline{b} = \overline{1}$; Выкинем такую пару остатков a и b. Проделаем эту итерацию так, что в итоге получится:
$P_k = \cup(a_i; b_i) \Rightarrow \sqcap \overline{a_i} = \overline{1}; \overline{p-1} = \overline{-1}$

$\sqcap \, \overline{a_i} = 1 * (-1) = -1 \Rightarrow (p-1)! + 1 \vdots p.$
—
Пусть p = 4k+1; Разделим его остатки следующим образом: $\overline{(1)}, ..\overline{(\frac{p-1}{2})}, ..., -\overline{(\frac{p-1}{2})}$
При перемножении получим 1, т.к. их количество четное. По т.Вильсона:

$(\frac{p-1}{2})! + 1 \vdots p$

Пусть $(\frac{p-1}{2})! = x; x^2 + 1 \vdots p$

Мы нашли x удовлетворяющее условию $(x-i)(x+i) \vdots p \in \mathbb{Z}[i] \Rightarrow p$ неразложимое
Пусть:
$p = (a+bi)(+ di)$
$p = (a-bi)(c-di)$
$p^2 = (a^2+b^2)(c^2+d^2) \Leftrightarrow (a^2+b^2 = p) \vee (c^2+d^2 = p)$. Т.к. не один из множетелей не равен 1, иначе p был бы обратимым. Т.е. получили, что и хотели:
$p = a^2 + b^2 = c^2$
Проверим единственность представления.
$p = (a+bi)(a-bi) = (c+di)(c-di)$ где множители неразложимы.
Пусть $a+bi$ раскладывается в 2 необратимых элемента, тогда анологично получаем:
$a^2 + b^2 = (r^2+s^2)(\overline{r^2} + \overline{s^2})$ - противоречие.
Значит, получаем, что: $(a+bi) = (c \pm di) * u, u \in \{\pm 1; \pm i\}$