ЛЕКЦИЯ 4.04

АЛГЕБРЫ С ДЕЛЕНИЕМ, ТЕОРЕМЫ ФРОБЕНИУСА, КОММУТАТИВНЫЕ АЛГЕБРЫ С ДЕЛЕНИЕМ

2.7.1. АЛГЕБРЫ С ДЕЛЕНИЕМ

Одной из классических задач алгебр – это разыскание всех алгебр с делением. Несмотря на важность этой задачи она в полном объёме не решена до сих пор. Однако, если помимо существования деления, наложить ещё другие требования естественного характера, то задача становится легче. В 1878 г. немецкий математик Г.Фробениус (1849-1917) доказал следующую теорему.

Любая ассоциативная алгебра с делением изоморфна одной из трёх: алгебре действительных чисел, алгебре комплексных чисел или алгебре кватернионов.

Впоследствии был установлен более общий факт, называемый обобщённой теоремой Фробениуса..

Любая альтернативная алгебра с делением изоморфна одной из четырех алгебр: действительных чисел, комплексных чисел кватернионов или октав.

Доказательство теоремы Фробениуса опирается на ряд утверждений.

Утверждение I. ***Ассоциативная алгебра*** A ***с делением содержит единицу.***

Рассмотрим уравнение $\mathbf{xa}=\mathbf{a}$, где $\mathbf{a}-$ отличный от нуля элемент алгебры A. Так как алгебра с делением, то имеется единственное решение $\mathbf{e}$ этого уравнения, то есть $\mathbf{ea}=\mathbf{a}$. Умножая обе части этого равенства слева на $\mathbf{b}$, в силу ассоциативности алгебры получаем $\mathbf{b}(\mathbf{ea})=(\mathbf{be})\mathbf{a}=\mathbf{ba}$ или $\mathbf{be}=\mathbf{b}$.

Теперь умножим это равенство справа на $\mathbf{c}$: $(\mathbf{be})\mathbf{c}=\mathbf{b}(\mathbf{ec})=\mathbf{bc} \quad \to \quad \mathbf{ec}=\mathbf{c}$.

Эти два равенства в силу произвольности элементов $\mathbf{b}$ и $\mathbf{c}$ означают, что элемент $\mathbf{e}$ является единицей алгебры A. В дальнейшем единицу будем обозначать $\mathbf{1}$.

Утверждение II. ***Если элемент*** $\mathbf{a}\in A$ ***не пропорционален*** $\mathbf{1}$***, то совокупность*** C_a ***элементов вида*** $\alpha\mathbf{1}+\beta\mathbf{a}$ ***образует подалгебру, изоморфную алгебре комплексных чисел.***

В алгебре размерности n система из $n+1$ векторов $1,\mathbf{a}^1,\mathbf{a}^2,...,\mathbf{a}^n$ линейно зависима и некоторая степень $m\le n$ должна разлагаться по предыдущим: $\mathbf{a}^m=k_{m-1}\mathbf{a}^{m-1}+...+k_2\mathbf{a}^2+k_1\mathbf{a}+k_0\mathbf{1}$ или $\mathbf{a}^m-k_{m-1}\mathbf{a}^{m-1}-...-k_2\mathbf{a}^2-k_1\mathbf{a}-k_0\mathbf{1}=0.$ Это уравнение эквивалентно произведению многочленов первой и второй степени $P_1(\mathbf{a})P_2(\mathbf{a})...P_m(\mathbf{a})=0$, то есть имеется сомножитель равный нулю и $\mathbf{a}$ удовлетворяет уравнению первой или второй степени. Уравнение первой степени не может быть, ибо тогда $\alpha\mathbf{1}+\mathbf{a}=0$ и элемент $\mathbf{a}$ пропорционален $\mathbf{1}$, вопреки условию. Следовательно $\mathbf{a}$ удовлетворяет неразложимому квадратному уравнению, корень которого комплексное число.

Утверждение III. ***Если элементы*** $\mathbf{a}\in A,\quad \mathbf{b}\in A$ ***не принадлежат одной подалгебре*** C_a***, то совокупность*** $Q_{a,b}$ ***элементов вида*** $\alpha\mathbf{1}+\beta\mathbf{a}+\gamma\mathbf{b}+\delta\mathbf{ab}$ ***образует подалгебру, изоморфную алгебре кватернионов. Если кроме того элементы*** $\mathbf{a}$ ***и*** $\mathbf{b}$ ***такие, что*** $\mathbf{a}^2=-1,\quad \mathbf{b}^2=-1$***, то*** $\mathbf{ab}+\mathbf{ba}=\lambda\mathbf{1}$***, где*** $\lambda-$ ***действительное число.***

Если $\mathbf{a}^2=-1,\quad \mathbf{b}^2=-1$ то $\mathbf{a}$ и $\mathbf{b}$ не содержат слагаемых кратных $\mathbf{1}$.

Квадраты элементов $(\mathbf{a}+\mathbf{b})^2$ и $(\mathbf{a}+2\mathbf{b})^2$ должны разлагаться соответственно по $\mathbf{1},(\mathbf{a}+\mathbf{b})$ и $\mathbf{1},(\mathbf{a}+2\mathbf{b})$, то есть

$$(\mathbf{a}+\mathbf{b})^2 = -2\cdot\mathbf{1}+(\mathbf{ab}+\mathbf{ba}) = p\mathbf{1}+q(\mathbf{a}+\mathbf{b}),$$
$$(\mathbf{a}+2\mathbf{b})^2 = -5\cdot\mathbf{1}+2(\mathbf{ab}+\mathbf{ba}) = p'\mathbf{1}+q'(\mathbf{a}+2\mathbf{b}).$$

Из этих равенств имеем $(2+p)\mathbf{1}+q(\mathbf{a}+\mathbf{b}) = (\mathbf{ab}+\mathbf{ba}) = (5+p')\mathbf{1}+q'(\mathbf{a}+2\mathbf{b})$ или $(3+p'-p)\mathbf{1}+(q'-q)\mathbf{a}+(2q'-q)\mathbf{b}=0$, то есть $\mathbf{a}$ и $\mathbf{b}$ есть элементы одной подалгебры C_a. Это исключено условием и в разложениях $q=q'=0$.

Итак, $\mathbf{ab}+\mathbf{ba}=\lambda\mathbf{1}$.

Из элементов $\mathbf{a}=\mathbf{e}_1$ и $\mathbf{b}$ можно сформировать элемент $\mathbf{e}_2=\dfrac{\lambda\mathbf{a}+2\mathbf{b}}{\sqrt{4-\lambda^2}}$

так что $\mathbf{e}_1{}^2=-\mathbf{1},\quad \mathbf{e}_2{}^2=-\mathbf{1},\quad (\mathbf{e}_1\mathbf{e}_2)^2=-\mathbf{1}$.

Действительно $$\mathbf{e}_2{}^2=\left(\frac{\lambda\mathbf{a}+2\mathbf{b}}{\sqrt{4-\lambda^2}}\right)^2=\frac{-(\lambda^2+4)\mathbf{1}+2\lambda(\mathbf{ab}+\mathbf{ab})}{4-\lambda^2}=-\mathbf{1};$$

Заметим, что $$\mathbf{e}_1\mathbf{e}_2+\mathbf{e}_2\mathbf{e}_1=\frac{\mathbf{a}(\lambda\mathbf{a}+2\mathbf{b})+(\lambda\mathbf{a}+2\mathbf{b})\mathbf{a}}{\sqrt{4-\lambda^2}}=\frac{-2\lambda\cdot\mathbf{1}+2(\mathbf{ab}+\mathbf{ab})}{\sqrt{4-\lambda^2}}=0,$$

и на основании этого факта
$$(\mathbf{e}_1\mathbf{e}_2)^2=(\mathbf{e}_1\mathbf{e}_2)(\mathbf{e}_1\mathbf{e}_2)=(\mathbf{e}_1\mathbf{e}_2)(-\mathbf{e}_2\mathbf{e}_1)=-(\mathbf{e}_1\mathbf{e}_2{}^2)\mathbf{e}_1=\mathbf{e}_1{}^2=-\mathbf{1}.$$

Теперь можем установить, что множество Q_{e_1,e_2} элементов вида $\alpha\mathbf{1}+\beta\mathbf{e}_1+\gamma\mathbf{e}_2+\delta\mathbf{e}_1\mathbf{e}_2$ совпадающее с множеством $Q_{a,b}$ есть подалгебра алгебры A. Для этого достаточно убедиться в том, что произведение любых двух элементов из четвёрки $1,\mathbf{e}_1,\mathbf{e}_2,(\mathbf{e}_1\mathbf{e}_2)$ разлагается по тем же четырём элементам. Кроме очевидных следует рассмотреть следующие:
$$\mathbf{e}_1(\mathbf{e}_1\mathbf{e}_2)=\mathbf{e}_1{}^2\mathbf{e}_2=-\mathbf{e}_2,\quad (\mathbf{e}_1\mathbf{e}_2)\mathbf{e}_1=-(\mathbf{e}_2\mathbf{e}_1)\mathbf{e}_1=-\mathbf{e}_2\mathbf{e}_1{}^2=\mathbf{e}_2,$$
$$\mathbf{e}_2(\mathbf{e}_1\mathbf{e}_2)=-\mathbf{e}_2(\mathbf{e}_2\mathbf{e}_1)=-\mathbf{e}_2{}^2\mathbf{e}_1=\mathbf{e}_1,\quad (\mathbf{e}_1\mathbf{e}_2)\mathbf{e}_2=\mathbf{e}_1\mathbf{e}_2{}^2=-\mathbf{e}_1.$$

Итак, множество Q_{e_1,e_2} является подалгеброй. Поскольку, как следует из предыдущего, таблица умножения элементов четвёрки $\mathbf{1},\mathbf{e}_1,\mathbf{e}_2,(\mathbf{e}_1\mathbf{e}_2)=\mathbf{e}_3$ совпадает с таблицей умножения кватернионных единиц, для установления изоморфизма этой подалгебры алгебре кватернионов следует убедиться только в том, что четвёрка элементов $\mathbf{1},\mathbf{e}_1,\mathbf{e}_2,(\mathbf{e}_1\mathbf{e}_2)$ образует базис, то есть не один из её элементов не разлагается по *предшедствующим*.

Поскольку элементы $\mathbf{e}_1,\mathbf{e}_2$ не принадлежат одной подалгебре C_a, то элемент $\mathbf{e}_2$ не разлагается по $\mathbf{1},\mathbf{e}_1$. Не разложимость $(\mathbf{e}_1\mathbf{e}_2)$ по $\mathbf{1},\mathbf{e}_1,\mathbf{e}_2$ означает невозможность равенства $(\mathbf{e}_1\mathbf{e}_2)=p\mathbf{e}_2+q\mathbf{e}_1+r\mathbf{1}$, где $p\neq 0,\quad q\neq 0$.

Если $p=0$, то, умножив слева равенство на $\mathbf{e}_1$, получим $-\mathbf{e}_2=-q\mathbf{1}+r\mathbf{e}_1$, что невозможно в силу неразложимости $\mathbf{e}_2$ по $\mathbf{1},\mathbf{e}_1$. Поскольку $p\neq 0$ умножение слева равенства на $\mathbf{e}_1$ даёт $-\mathbf{e}_2=p(\mathbf{e}_1\mathbf{e}_2)-q\mathbf{1}+r\mathbf{e}_1$ или $(\mathbf{e}_1\mathbf{e}_2)=-\dfrac{1}{p}\mathbf{e}_2-\dfrac{r}{p}\mathbf{e}_1+\dfrac{q}{p}\mathbf{1}$. Вычитая из этого равенства исходное, получаем $\left(p+\dfrac{1}{p}\right)\mathbf{e}_2+\left(q+\dfrac{r}{p}\right)\mathbf{e}_1+\left(r-\dfrac{q}{p}\right)\mathbf{1}=0$. Все коэффициенты должны быть равны нулю, однако это невозможно ни при каком действительном p. Итак, четвёрка элементов $\mathbf{1},\mathbf{e}_1,\mathbf{e}_2,(\mathbf{e}_1\mathbf{e}_2)=\mathbf{e}_3$ образует базис подалгебры Q_{e_1,e_2}. Утверждение III справедливо.

Теперь можно приступить к доказательству теоремы Фробениуса.

2.7.2. ТЕОРЕМА ФРОБЕНИУСА

Пусть A – ассоциативная алгебра с делением. Она согласно утверждению I содержит единицу. Элементы вида $k\mathbf{1}$ образуют подалгебру D, изоморфную алгебре действительных чисел. Если D не совпадает со всей алгеброй A, то, согласно утверждению II, в A содержится подалгебра C_a, изоморфная алгебре комплесных чисел. Если C_a не совпадает со всей алгеброй A, то, согласно утверждению III, в A содержится подалгебра $Q_{a,b}$, изоморфная алгебре кватернионов. Предположим , что $Q_{a,b}$ не совпадает со всей алгеброй A, то есть существует элемент $\mathbf{c}$, не принадлежащий $Q_{a,b}$, тогда это предположение приведёт к ряду противоречий, которые означают совпадение $Q_{a,b}$ со всей алгеброй A либо, что алгебра A не может быть алгеброй с делением.

В алгебре кватернионов выберем базис $\mathbf{1},\mathbf{i}.\mathbf{j},\mathbf{k}$ со стандартно таблицей умножения, а элемент $\mathbf{c}$ представим в виде $\mathbf{c} = p\mathbf{1} + q\mathbf{e}$, где $\mathbf{e}^2 = -1$ ($\mathbf{e}$ есть мнимая единица комплексной алгебры C_a). Используя ассоциативность алгебры A и по свойству III соотношения $\mathbf{ie} + \mathbf{ei} = \lambda\mathbf{1}$, $\mathbf{je} + \mathbf{ej} = \lambda'\mathbf{1}$, $\mathbf{ke} + \mathbf{ek} = \lambda''\mathbf{1}$ получаем $\mathbf{ie} = (\mathbf{jk})\mathbf{e} = \mathbf{j}(\mathbf{ke}) = \mathbf{j}(-\mathbf{ek} + \lambda''\mathbf{1}) = -(\mathbf{je})\mathbf{k} + \lambda''\mathbf{j} = -(-\mathbf{ej} + \lambda'\mathbf{1})\mathbf{k} + \lambda''\mathbf{j} =$ $= \mathbf{ei} - \lambda'\mathbf{k} + \lambda''\mathbf{j}$ и следовательно $\mathbf{ie} - \mathbf{ei} = \lambda''\mathbf{j} - \lambda'\mathbf{k}$. С другой стороны $\mathbf{ie} + \mathbf{ei} = \lambda\mathbf{1}$. Складывая эти равенства, находим что элемент $2\mathbf{ie} = \lambda\mathbf{1} + \lambda''\mathbf{j} - \lambda'\mathbf{k}$ есть элемент из $Q_{a,b}$. Следовательно элемент $\mathbf{ic} = \mathbf{i}(p\mathbf{1} + q\mathbf{e})$ есть также элемент из $Q_{a,b}$. Кроме того очевидно, что умножение $\mathbf{i}$ на элемент из $Q_{a,b}$ даёт элемент из $Q_{a,b}$. Итак, умножение $\mathbf{i}$ на любой элемент из A даёт элемент из $Q_{a,b}$.

Это невозможно, если A есть алгебра с делением, поскольку уравнение $\mathbf{ix} = \mathbf{c}$ неразрешимо если $\mathbf{c}$ не принадлежит $Q_{a,b}$. Либо $Q_{a,b}$ совпадает со всей алгеброй A. Теорема доказана.

2.7.3. ОБОЩЁННАЯ ТЕОРЕМА ФРОБЕНИУСА

Обратимся к доказательству обобщённой теоремы Фробениуса.
Сначала дадим другое определение альтернативной алгебры. *Алгебра A называется альтернативной, если любое произведение, составленное из произвольных её элементов* $\mathbf{a}$ *и* $\mathbf{b}$*, не зависит от способа расстановки скобок.* Например, $(\mathbf{ab})\mathbf{b} = \mathbf{a}(\mathbf{bb})$, $(\mathbf{ab})(\mathbf{ba}) = (\mathbf{a}(\mathbf{bb}))\mathbf{a}$ и т.д. Это второе определение ассоциативности эквивалентно первому, которое состоит в выполнении тождеств $(\mathbf{ab})\mathbf{b} = \mathbf{a}(\mathbf{bb})$, $\mathbf{b}(\mathbf{ba}) = (\mathbf{bb})\mathbf{a}$ (теорема Артина). Таким образом, ***если алгебра A с делением такова, что любое произведение, составленное из двух произвольных её элементов, не зависит от расстановки скобок, то алгебра A изоморфна одной из четырёх алгебр: действительных чисел, комплексных чисел, кватернионов или октав.***

Утверждения I, II, III о свойствах ассоциативной алгебры с делением остаются справедливыми и в случае альтернативной алгебры с делением. Например, утверждение I о единице алгебры: решение уравнений $\mathbf{xa} = \mathbf{a}$, $\mathbf{bx} = \mathbf{b}$ $\mathbf{x} = \mathbf{e}$ обладает свойством

$$\mathbf{ea} = \mathbf{a} \quad \to \quad \mathbf{e}(\mathbf{ea}) = (\mathbf{ee})\mathbf{a} = \mathbf{ea} \quad \to \quad \mathbf{ee} = \mathbf{e},$$

$$\mathbf{be} = \mathbf{b} \quad \to \quad (\mathbf{be})\mathbf{e} = \mathbf{b}(\mathbf{ee}) = \mathbf{be} \quad \to \quad \mathbf{ee} = \mathbf{e},$$

то есть решение есть единица алгебры.

Далее аналогичное доказательство: если рассматриваемая альтернативная алгебра A не исчерпывается подалгеброй $Q_{a,b}$, то в ней содержится подалгебра, изоморфная алгебре октав; подалгебра же октав совпадает со всей алгеброй.

Однако, есть и другой путь. Можно показать, что алгебра A является нормированной. Тогда по теореме Гурвица будем иметь совпадение подалгебры октав со всей алгеброй.

Любые элементы $\mathbf{a}$ и $\widetilde{\mathbf{a}}$, как сопряжённые в комплексной алгебре, удовлетворяют условиям $\mathbf{a}+\widetilde{\mathbf{a}}=k\cdot\mathbf{1},\quad \mathbf{a}\widetilde{\mathbf{a}}=k\cdot\mathbf{1}$, где $k-$ действительное число.

Любые элементы $\mathbf{b}$ и $\widetilde{\mathbf{b}}$, как сопряжённые в алгебре кватернионов, удовлетворяют аналогичным условиям $\mathbf{b}+\widetilde{\mathbf{b}}=k\cdot\mathbf{1},\quad \mathbf{b}\widetilde{\mathbf{b}}=k\cdot\mathbf{1}$.

Пусть $\mathbf{a}=\mathbf{b}$, тогда разность соответствующих равенств даёт $\widetilde{\mathbf{a}}-\widetilde{\mathbf{b}}=k\cdot\mathbf{1},\quad \mathbf{a}\left(\widetilde{\mathbf{a}}-\widetilde{\mathbf{b}}\right)=k\cdot\mathbf{1}$. Если $\widetilde{\mathbf{a}}\neq\widetilde{\mathbf{b}}$, то из этих равенств вытекает, что элемент $\mathbf{a}$ пропорционален $\mathbf{1}$, что противоречит предположению. Таким образом, *элемент сопряжённый* $\mathbf{a}=\mathbf{b}$*, один и тот же, независимо от того, рассматриваем ли мы его как элемент комплексной подалгебры или же как элемент какой-либо подалгебры кватернионов.*

То же самое относится и к модулю элементов $\mathbf{a}=\mathbf{b}$ поскольку $|\mathbf{a}|^2=\mathbf{a}\widetilde{\mathbf{a}},\quad |\mathbf{b}|^2=\mathbf{b}\widetilde{\mathbf{b}}$.

Итак, для любых двух элементов алгебры A имеем $\widetilde{\mathbf{a}+\mathbf{b}}=\widetilde{\mathbf{a}}+\widetilde{\mathbf{b}},\quad \widetilde{\mathbf{ab}}=\widetilde{\mathbf{b}}\widetilde{\mathbf{a}}$, то есть элемент сопряжённый $\mathbf{a}\widetilde{\mathbf{b}}$ равен $\mathbf{b}\widetilde{\mathbf{a}}$ и $\mathbf{a}\widetilde{\mathbf{b}}+\mathbf{b}\widetilde{\mathbf{a}}=k\cdot\mathbf{1}$.

Определим в алгебре A скалярное произведение $(\mathbf{a},\mathbf{b})$ равенством $\mathbf{a}\widetilde{\mathbf{b}}+\mathbf{b}\widetilde{\mathbf{a}}=2(\mathbf{a},\mathbf{b})\cdot\mathbf{1}$, которое обладает всеми свойствами скалярного произведения:

- $(\mathbf{a},\mathbf{a})>0,$ если $\mathbf{a}\neq 0$, и $(0,0)=0$;
- $(\mathbf{a},\mathbf{b})=(\mathbf{b},\mathbf{a})$;
- $(\mathbf{a},k\mathbf{b})=k(\mathbf{a},\mathbf{b})$;
- $(\mathbf{a},\mathbf{b}_1+\mathbf{b}_2)=(\mathbf{a},\mathbf{b}_1)+(\mathbf{a},\mathbf{b}_2)$.

Из определения скалярного произведения имеем

$$2(\mathbf{a},\mathbf{a})\cdot\mathbf{1}=\mathbf{a}\widetilde{\mathbf{a}}+\mathbf{a}\widetilde{\mathbf{a}}=2\|\mathbf{a}\|\cdot\mathbf{1}=2|\mathbf{a}|^2\cdot\mathbf{1},$$

то есть норма элемента $\mathbf{a}$ в алгебре A совпадает с квадратом модуля как у комплексных чисел и кватернионов. Поскольку алгебры комплексных чисел и алгебры кватернионов являются нормированными алгебрами, то $(\mathbf{ab},\mathbf{ab})=(\mathbf{a},\mathbf{a})(\mathbf{b},\mathbf{b})$, но это равенство означает нормированность алгебры A. Тогда по теореме Гурвица алгебра A изоморфна одной из четырёх «стандартных» алгебр.

2.8. КОММУТАТИВНЫЕ АЛГЕБРЫ С ДЕЛЕНИЕМ

Введём обозначение $A(\alpha,\beta,\gamma)$ для коммутативной алгебры размерности 2 с таблицей умножения

$$\mathbf{k}_1\circ\mathbf{k}_1=\alpha\,\mathbf{k}_1+\beta\,\mathbf{k}_2,\quad \mathbf{k}_1\circ\mathbf{k}_2=\beta\,\mathbf{k}_1+\gamma\,\mathbf{k}_2,\quad \mathbf{k}_2\circ\mathbf{k}_2=-\alpha\,\mathbf{k}_1-\beta\,\mathbf{k}_2,$$

где числа α,β,γ удовлетворяют условиям $\alpha\gamma-\beta^2=\pm1;\quad \beta\geq 0;\quad \alpha\geq 0,$ если $\alpha=0$, то $\gamma\geq 0$.

Имеет место факт: ***Любая коммутативная алгебра с делением имеет размерность не выше 2 и изоморфна одной из алгебр*** $A(\alpha,\beta,\gamma)$***. Все алгебры*** $A(\alpha,\beta,\gamma)$ ***суть алгебры с делением и никакие две из них не изоморфны друг другу.***