Дополнительный материал

Теорема 1. *Пусть K – расширение поля F. Рассмотрим множество $\overline{F}_K \subset K$, состоящее из всех элементов K, алгебраичных над F. Тогда $\overline{F}_K$ – поле и если $k \in K$ алгебраичен над $\overline{F}_K$, то он алгебраичен над F.*

Доказательство. Возьмем $a, b \in \overline{F}_K$. Так как a алгебраичен над F, $F \subset F(a)$ – конечное расширение. Элемент b алгебраичен над F, и следовательно, он алгебраичен и над $F(a)$. Тогда $F(a) \subset F(a)(b) = F(a, b)$ – конечное расширение. По теореме о башне расширений $F \subset F(a, b)$ – конечное расширение. Элементы $a + b, ab, -a, a^{-1}$ лежат в $F(a, b)$. Значит, все они алгебраические над F.

Пусть k удовлетворяет уравнению $a_n k^n + \ldots + a_0 = 0$, $a_i \in \overline{F}_K$. Рассмотрим $F(a_0, \ldots, a_n)$ – конечное расширение F. Получаем, что k алгебрачен над $F(a_0, \ldots, a_n)$, то есть $F(a_0, \ldots, a_n)(k)$ – конечное расширение $F(a_0, \ldots, a_n)$. По теореме о башне расширений $F(a_0, \ldots, a_n)(k) = F(a_0, \ldots, a_n, k)$ – конечное расширение F, а значит, $k \in \overline{F}_K$. □

Поле $\overline{F}_K$ называется *алгебраическим замыканием* поля F в K.

Зачастую есть необходимость вложить поле F в алгебраически замкнутое поле. Минимальное по включению такое поле называется *алгебраическим замыканием* $K = \overline{F}$ поля F. Минимальность по включению означает, что $\overline{F}_K = K$.

Как это сделать? Нужно добавить все корни всех многочленов с коэффициентами из F. Однако поскольку коэффициентов вообще говоря бесконечное количество и многочленов также бесконечное количество, то вообще говоря здесь нужны трансфинитные методы. проследим за конечным полем $\mathbb{F}_p = \mathbb{Z}_p$.

Теорема 2. *Пусть K – это объединение цепочки вложенных полей*

$$\mathbb{F}_p \subset \mathbb{F}_{p^{2!}} \subset \mathbb{F}_{p^{3!}} \subset \ldots$$

Тогда K – это алгебраическое замыкание $\overline{\mathbb{F}_p}$.

Доказательство. Пусть $f(x) = a_m x^m + \ldots + a_0$ – неприводимый многочлен над K. Тогда существует n такое, что все a_i лежат в $\mathbb{F}_{p^{n!}}$. Тогда можно рассмотреть поле $\mathbb{F}_{p^{n!}}[x]/(f) \cong \mathbb{F}_{p^{n!\cdot m}}$, в котором у f есть корень. Тогда $\mathbb{F}_{p^{n!\cdot m}} \subset \mathbb{F}_{p^{(mn)!}} \subset K$, а значит, у $f(x)$ есть корень в поле K.

С другой стороны поле K сочтоит из элементов, каждый из которых является корнем некоторого многочлена над $\mathbb{F}_p$, а значит, оно минимальное расширение $\mathbb{F}_p$ с условием алгебраической замкнутости. □

Алгебры с делением.

Определение 1. (Ассоциативное) кольцо с единицей называется *телом*, если каждый ненулевой элемент в нем обратим.

Алгебра, являющаяся телом, называется *алгеброй с делением*.

Замечание 1. Центр $Z(D)$ любого тела D – это поле. И тело D является алгеброй с делением над $Z(D)$.

Если A – алгебра с единицей над полем F, то элементы $\lambda 1 \in A$, $\lambda \in F$ образуют подполе, изоморфное F. Далее мы будем отождествлять элементы $\lambda \in F$ и $\lambda 1 \in A$.

Лемма 1. *Пусть A – (ассоциативная) алгебра с единицей размерности n над полем F. Тогда каждый элемент $a \in A$ удовлетворяет некоторому уравнению $f(a) = 0$, где*

многочлен $f(x) \in F[x]$ степени не больше n. Выберем многочлен $\mu_a(x)$ минимальной степени такой, что $\mu_a(a) = 0$. Элемент a обратим тогда и только тогда, когда $\mu_a(0) \neq 0$. Если A без делителей нуля, то $\mu_a(x)$ неприводим над F и любой аннулирующий a многочлен $f(x)$ делится на $\mu_a(x)$. Алгебра A в этом случае является алгеброй с делением. Если при этом F алгебраически замкнуто, то $A = F$.

Доказательство. Элементы $1, a, a^2, \ldots, a^n$ линейно зависимы над F, значит существуют не все нулевые c_i такие, что $\sum c_i a^i = 0$, что дает аннулирующий многочлен. Если $\mu_a(0) \neq 0$, то $0 \neq -c_0 = c_1 a + \ldots + c_k a^k = a(c_1 + \ldots + c_k a^{k-1})$. Если же $\mu_a(0) = 0$, то $a(c_1 + \ldots + c_k a^{k-1}) = 0$, то есть a – делитель нуля.

Как видно из последнего рассуждения, A либо алгебра с делением, либо допускает делители нуля. Если F алгебраически замкнуто, то неприводимый многочлен μ_a линеен. □

Следствие 1. *Над полем $\mathbb{C}$ существует только одна алгебра с делением – это одномерная алгебра .*

Доказательство. Так как $\mathbb{C}$ алгебраически замкнуто, многочлен μ_a линеен, а значит, $a \in \mathbb{C}$ для любого $a \in A$. □

Теорема 3 (Теорема Фробениуса)**.** *Над полем $\mathbb{R}$ существует только 3 конечномерные ассоциативные алгебры с делением: $\mathbb{R}$, $\mathbb{C}$ и $\mathbb{H}$.*

Доказательство. Пусть $a \in A$, тогда μ_a – неприводимый над $\mathbb{R}$ многочлен. То есть либо $\mu_a(x) = x - \alpha$, тогда $a \in \mathbb{R}$, либо $\mu_a(x) = x^2 - 2\alpha x + \beta$, где $\alpha^2 < \beta$. Тогда положим $b = a - \alpha$, имеем $\mu_b(x) = x^2 + (\beta - \alpha^2)$. То есть в любом случае $a = \alpha + y$, где $y = 0$, либо $y^2 = \gamma < 0$.

Лемма 2. *Подмножество $A' = \{u \in A \mid u^2 \in \mathbb{R}, u^2 \leq 0\}$ является векторным подпространством.*

Доказательство. Ясно, что A' замкнуто относительно умножения на константу. Действительно при $\alpha \in \mathbb{R}$, $u \in A$ имеем $(\alpha u)^2 = (\alpha u)(\alpha u) = \alpha^2 u^2 \in \mathbb{R}_{\leq 0}$. Последнее равенство верно так как A – алгебра над $\mathbb{R}$.

Надо доказать, что если $u, v \in A'$, то $u + v \in A'$. Для пропорциональных u и v это ясно, поэтому далее считаем, что u и v не пропорциональны. Сначала проверим, что не может быть верным равенство $u = \alpha v + \beta$, где $\alpha, \beta \in \mathbb{R}$. Действительно иначе имеем $\gamma = u^2 = (\alpha v + \beta)^2 = \alpha^2 v^2 + 2\alpha\beta v + \beta^2 \in \mathbb{R}$. Так как $v \notin \mathbb{R}$, имеем $\alpha\beta = 0$. То есть либо $\alpha = 0$ и u вещественное (чего не может быть), либо $\beta = 0$ и векторы u и v пропорциональны, что не так.

Итак, u, v и 1 линейно независимы.

Элементы $u + v$ и $u - v$ не лежат в $\mathbb{R}$, а значит, минимальные многочлены этих элементов квадратичны. То есть существуют $p, q, r, s \in \mathbb{R}$ такие, что $(u + v)^2 = p(u + v) + q$, $(u - v)^2 = r(u - v) + s$. Будем использовать обозначения $u^2 = \gamma, v^2 = \delta \in \mathbb{R}_{\leq 0}$. Тогда

$\gamma + uv + vu + \delta = p(u + v) + q$,

$\gamma - uv - vu + \delta = r(u - v) + s$.

Сложим эти равенства. Получим $2\gamma + 2\delta = p(u + v) + r(u - v) + q + s$, то есть $(p + r)u + (p - r)v + (q + s - 2\gamma - 2\delta) = 0$. Так как $\{1, u, v\}$ – линейно независимая система, получаем $p = r = 0$. Таким образом, $(u + v)^2 = q \in \mathbb{R}$. Но $u + v \notin \mathbb{R}$. Если $q \geq 0$, то $q = l^2$ и $(u + v - l)(u + v + l) = 0$. Значит, $q < 0$, то есть $u + v \in A'$.

Лемма доказана. □

Из сказанного до леммы получаем, что $A = \mathbb{R} + A'$. Так как $\mathbb{R} \cap A' = \{0\}$, поскольку квадрат любого ненулевого элемента в $\mathbb{R}$ положителен, а в A' – отрицателен. Поэтому $A = \mathbb{R} \oplus A'$.

Если $A' = \{0\}$, то $A = \mathbb{R}$.

Иначе можно заметить, что $q(x) = -x^2 \in \mathbb{R}_{\geq 0}$ – квадратичная положительно определенная функция на A'. В самом деле $q(\lambda x) = (\lambda x)(\lambda x) = \lambda^2 x^2 = \lambda^2 q(x)$ при $\lambda \in \mathbb{R}$. И $q(x) = 0$, значит, $x^2 = 0$, то есть $x = 0$.

Рассмотрим полярную к q симметрическую билинейную форму (скалярное произведение на A')

$$f(x, y) = \frac{q(x+y) - q(x) - q(y)}{2} = \frac{-(x+y)^2 + x^2 + y^2}{2} = -\frac{xy + yx}{2}.$$

Пусть i – вектор из A' длины 1. Имеем $i^2 = -q(i) = -1$. Если $A' = \langle i \rangle$, то $A = \mathbb{R}[i] \cong \mathbb{C}$.

Пусть теперь $\mathbb{R}[i] \subsetneq A$, то есть $A' \neq \mathbb{R}i$. Тогда можно выбрать $j \in A'$, $f(i, j) = 0$, $q(j) = 1$. Получаем $j^2 = -1$ и $ij + ji = 0$. Положим $k = ij$. Тогда

$$k^2 = ijij = i(ji)j = i(-ij)j = -i^2 j^2 = -1.$$

Кроме того

$$ik = iij = -j, \qquad ki = iji = i(-k) = j, \qquad kj = ijj = -i, \qquad jk = jij = (-k)j = i.$$

Таким образом, $f(i, k) = f(j, k) = 0$, то есть $\{i, j, k\}$ – линейно независимая система в A'. Значит, $\{1, i, j, k\}$ – линейно независимая система в A. Умножение в $\langle 1, i, j, k \rangle$ совпадает с умножением в $\mathbb{H}$. Если $A' = \langle i, j, k \rangle$, то теорема доказана.

Пусть теперь $A' \neq \langle i, j, k \rangle$. Тогда существует $l \neq 0 \in A'$ такой, что

$$f(i, l) = f(j, l) = f(k, l) = 0.$$

То есть $il = -li$, $jl = -lj$, $kl = -lk$. Но тогда

$$lk = l(ij) = (li)j = -(il)j = -i(lj) = i(jl) = (ij)l = kl.$$

Получаем $lk = -lk$, то есть $lk = 0$, что дает делители нуля в A. Противоречие.

□