Независимый Московский Университет

Алгебра – II

Второй курс, осенний семестр 1999/2000 г.
Лекции 2,3

Аксиома выбора и её следствия.

Определение 1. Множество M называется *частично упорядоченным*, если на нём задано отношение '$\leqslant$', являющееся рефлексивным, транзитивным и антисимметричным. Если любые два элемента частично упорядоченного множества сравнимы, то оно называется *линейно упорядоченным*, или *цепью*. Линейно упорядоченное множество, в котором каждое непустое подмножество имеет наименьший элемент, называется *вполне упорядоченным*. *Отрезком* вполне упорядоченного множества M называется любое его подмножество, содержащее вместе с каждым своим элементом все меньшие него элементы множества M.

Упражнение 1. Пусть M — вполне упорядоченное множество. Доказать, что любой его отрезок либо совпадает с M, либо имеет вид $M_a = \{x \in M \mid x < a\}$ для некоторого $a \in M$.

Утверждения об элементах вполне упорядоченного множества можно доказывать, используя *трансфинитную индукцию*. А именно, предположим, что наименьший элемент непустого вполне упорядоченного множества M обладает некоторым свойством $\mathcal{E}$, и для любого элемента $x \in M$ из того, что все строго меньшие x элементы множества M обладают свойством $\mathcal{E}$, следует, что и x им обладает. (Заметим, впрочем, что первое условие является частным случаем второго. Действительно, для наименьшего элемента множества M верно, что все меньшие него обладают свойством $\mathcal{E}$.) Тогда все элементы множества M обладают этим свойством. Действительно, если множество $x \in M$, не обладающих свойством $\mathcal{E}$, непусто, то оно содержит наименьший элемент. Но, по нашим предположениям, для него свойство $\mathcal{E}$ должно выполняться.

Кроме доказательств по индукции, вполне упорядоченное множество позволяет проводить *построение по индукции*.

Теорема 1. *Пусть заданы два множества M и S, причём множество M вполне упорядочено. Предположим, что для любого $a \in M$ задана функция $\Phi_a : S^{M_a} \to S$ (сопостовляющая каждой функции $\psi : M_a \to S$ некоторый элемент $\Phi(\psi) \in S$). Тогда существует единственная функция $\varphi : M \to S$, удовлетворяющая рекуррентному соотношению $\varphi(a) = \Phi(\varphi|_{M_a})$ (то есть условию, позволяющему по значениям функции φ на всех $x < a$ однозначно определить $\varphi(a)$).*

Доказательство. Докажем сначала единственность. Пусть существуют две такие функции. Из совпадения этих функций для всех $x < a$ следует, что их значения совпадают и в точке a (в силу однозначности рекуррентного соотношения). По трансфинитной индукции мы получаем, что эти функции равны.

Докажем теперь существование такой функции φ. Скажем, что элемент $a \in M$ допускает построение искомой функции, если на множестве $M_a \cup \{a\} = \{x \in M \mid x \leqslant a\}$ существует функция φ_a, удовлетворяющая рекуррентному соотношению $\varphi_a(x) = \Phi(\varphi|_{M_x})$ для всех $x \leqslant a$. Если a и b допускают построение искомой функции и, к примеру, $a < b$, то $\varphi_a(x) = \varphi_b(x)$ для любого $x \leqslant a$ (в силу единственности функции φ_a). Поэтому, если все элементы множества M, строго меньшие b, допускают построение искомой функции, то и b его допускает (действительно, на всех элементах $a \in M_b$ мы полагаем $\varphi_b(a) = \varphi_a(a)$, а для определения $\varphi_b(b)$ пользуемся рекуррентным соотношением). По трансфинитной индукции отсюда следует, что все элементы множества M допускают построение искомой функции. □

Теорема 2. *Следующие четыре утверждения эквивалентны:*

Аксиома выбора. *Для любого множества M существует «функция выбора» $\varphi : 2^M \setminus \{\varnothing\} \to M$, сопоставляющая каждому непустому подмножеству $A \subseteq M$ некоторый его элемент $\varphi(A) \in A$.*

Теорема Цермело. *Любое множество M можно вполне упорядочить.*

Теорема Хаусдорфа. *Любая цепь частично упорядоченного множества M содержится в некоторой максимальной (по включению) цепи.*

Лемма Цорна. *Если любая цепь частично упорядоченного множества M имеет верхнюю границу, то любой немаксимальный элемент множества M меньше некоторого максимального элемента.*

Доказательство. Докажем, что из аксиомы выбора следует теорема Цермело.

Зафиксируем функцию выбора $\varphi : 2^M \setminus \{\varnothing\} \to M$. Назовем подмножество $A \subseteq M$ *отмеченным*, если оно может быть вполне упорядочено так, что $a = \varphi(M \setminus A_a)$ для всякого $a \in A$ (через A_a обозначен отрезок вполне упорядоченного множества A, состоящий из всех элементов, меньших a).

Пусть A, B — отмеченные подмножества и пусть C — объединение всех подмножеств множества $A \cap B$, являющихся отрезками в каждом из вполне упорядоченных множеств A и B. Ясно, что C тоже является отрезком и в A и в B. Если $A \neq C \neq B$, то, по определению отмеченных множеств, множество $C \cup \{\varphi(M \setminus C)\}$ также является отрезком и в A и в B, причём оно строго содержит C, чего быть не может. Поэтому из любых двух отмеченных множеств одно обязательно является отрезком другого. Отсюда следует, что объединение всех отмеченных множеств тоже является отмеченным. Обозначим его через N. Если $N \neq M$, то $N \cup \{\varphi(M \setminus N)\}$ также является отмеченным, в противоречии с определением N. Поэтому $N = M$, то есть множество M можно вполне упорядочить.

Докажем, что из теоремы Цермело следует теорема Хаусдорфа.

Пусть A — некоторая цепь в M. По теореме Цермело множество $N = M \setminus A$ можно считать вполне упорядоченным (эта упорядоченность никак не связана с частичной упорядоченностью множества M). Построим с помощью трансфинитной индукции по множеству N некоторое его подмножество K, состоящее из элементов, которые мы назовём «допустимыми»(построение подмножества по индукции — это то же самое, что построение функции из M в $\{0, 1\}$; подмножество — это прообраз единицы). Назовём элемент $x \in N$ допустимым, если он сравним со всеми элементами цепи A и со всеми допустимыми элементами множества N, меньшими x. Тогда, очевидно, множество $A \cup K$ является максимальной цепью в M.

Лемма Цорна сразу следует из теоремы Хаусдорфа. Действительно, каждый элемент $a \in M$ можно рассматривать как одноэлементную цепь; по теореме Хаусдорфа эта цепь содержится в некоторой максимальной цепи; верхняя граница b этой максимальной цепи будет, очевидно, максимальным элементом множества M; если $a \neq b$, то $a < b$.

Выведем, наконец, аксиому выбора из леммы Цорна.

Пусть M — непустое множество. Рассмотрим множество $\mathfrak{M}$, элементами которого являются все «частичные функции выбора» $\varphi : \mathcal{C} \to M$, где $\mathcal{C}$ — некоторое множество непустых подмножеств множества M, а $\varphi(C) \in C$ для любого $C \in \mathcal{C}$. Множество $\mathfrak{M}$ частично упорядочено: мы считаем $\varphi_1 \leqslant \varphi_2$, если область определения $\mathcal{C}_1$ функции φ_1 является подмножеством области определения $\mathcal{C}_2$ функции φ_2, и $\varphi_2|_{\mathcal{C}_1} = \varphi_1$.

Для $\mathfrak{M}$ условия леммы Цорна, очевидно, выполнены: для любой цепи в нём его верхней границей будет функция на объединении областей определения функций, входящих в цепь, совпадающая с ними на их областях определения. Пусть a — некоторый элемент множества M и $\varphi_a : \{a\} \mapsto a$ — частичная функция выбора, заданная на множестве $\mathcal{C}_0 = \{\{a\}\}$. По лемме Цорна существует φ — максимальный элемент множества $\mathfrak{M}$, больший φ_0.

Если есть хотя бы одно непустое множество A, не принадлежащее области определения $\mathcal{C}$ функции φ, то функция на множестве $\mathcal{C} \cup \{A\}$, равная φ на $\mathcal{C}$ и сопоставляющая множеству A некоторый его элемент, строго больше φ, что невозможно в силу его максимальности. Поэтому φ — искомая функция выбора. □

Не обсуждая, насколько очевидна аксиома выбора и эквивалентные ей утверждения, мы, следуя установившейся традиции, будем их свободно использовать.

Аксиоматика зависимости.

Определение 2. *Матроидом* называется множество E вместе с отображением s множества 2^E всех подмножеств множества E в себя, удоветворяющим условиям:

(S1): Если $X \subseteq E$, то $X \subseteq s(X)$.

(S2): Если $X \subseteq E$, то $s(s(X)) = s(X)$.

(S3): Если $X \subseteq Y \subseteq E$, то $s(X) \subseteq s(Y)$.

(S4): Если $X \subseteq E$ и $x \in s(X)$, то существует конечное подмножество $X_0 \subseteq X$, такое что $x \in s(X_0)$.

(S5): Если $X \subseteq E$, $y \in s(X \cup \{x\})$ и $y \notin s(X)$, то $x \in s(X \cup \{y\})$.

Функция s обычно называется *оператором замыкания*, а множества $X \subseteq E$, для которых $s(X) = X$, называются *замкнутыми*.

Множество $A \subseteq E$, не лежащее в замыкании никакого своего собственного подмножества, называется *независимым*. Остальные подмножества множества E называются *зависимыми*. Максимальное независимое подмножество называется *базисом*.

Пример 1. Любое векторное пространство V является матроидом (оператор замыкания — это взятие линейной оболочки). Более того, любое подмножество E векторного пространства V является матроидом (замыкание множества — это пересечение его линейной оболочки с E).

Чтобы освоиться с понятием матроида, решите следующие несложные задачи. Итак, пусть (E, s) — произвольный матроид.

Упражнение 2. Доказать, что подмножество независимого множества $A \subset E$ тоже является независимым множеством.

Упражнение 3. Доказать, что независимое множество $A \subset E$ является базисом тогда и только тогда, когда $s(A) = E$.

Упражнение 4. Доказать, что любое зависимое множество $A \subset E$ содержит конечное зависимое подмножество.

Упражнение 5. Доказать, что любое зависимое множество $A \subset E$ содержит минимальное зависимое подмножество.

Упражнение 6. Доказать, что если $A \subset E$ — минимальное зависимое множество, то любой его элемент a лежит в замыкании множества $A \setminus \{a\}$.

Упражнение 7. Доказать, что если $A \subset E$ — независимое множество, и $b \in s(A)$, то $A \cup \{b\}$ содержит единственное минимальное зависимое множество.

Упражнение 8. Доказать, что если $A \subset E$ — независимое множество, и $b \in s(A)$, то A содержит такое конечное подмножество $A^{(b)}$, что $b \in s(A^{(b)})$, причём $A^{(b)}$ содержится в любом подмножестве множества A, замыкание которого содержит b.

Упражнение 9. Доказать, что если $A \subset E$ — независимое множество, и $b \in s(A)$, то $A \setminus \{a\} \cup \{b\}$ является независимым для тех и только тех элементов $a \in A$, которые принадлежат $A^{(b)}$.

Теорема 3. *У любого матроида E существует базис. Любые два базиса матроида равномощны.*

Доказательство. Легко проверить, что для любой цепочки вложенных независимых множеств их объединение будет независимым множеством (заметьте, что здесь важна аксиома (S4)). По лемме Цорна отсюда следует, что любое независимое множество можно дополнить до базиса.

Пусть теперь A и B — любые два базиса. Докажем, что мощность A не превосходит мощности B. Разбор случая, когда $|B| < \infty$, я оставляю в качестве упражнения. Пусть B — бесконечное множество. Мы имеем $A = \bigcup_{b \in B} A^{(b)}$ (см. Упражнения 3, 8). Остается воспользоваться тем, что мощность объединения конечных множеств, индексированных бесконечным множеством B, не превосходит мощности B. Для счетных множеств это легко следует из счетности $\mathbb{N} \times \mathbb{N}$. С другой стороны, любое бесконечное множество можно представить как объединение счетных (для доказательства примените лемму Цорна). $\square$

В качестве следствия доказанной теоремы мы получаем, что понятие размерности можно обобщить на бесконечномерные пространства — размерностью пространства называется мощность любого его базиса. В частности, в счётномерном пространстве любое линейно независимое подмножество не более чем счётно. Это утверждение понадобится нам в следующем разделе.

Теорема Гильберта о нулях. Для любого идеала $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ обозначим через $V(I)$ множество всех таких наборов $(a_1, \ldots, a_n) \in \mathbb{C}^n$ (точек n-мерного комплексного пространства) что $f(a_1, \ldots, a_n) = 0$ для любого $f \in I$. Короче говоря, $V(I)$ — множество нулей идеала I.

Теорема 4 (Nullstellensatz Гильберта). *Для любого идеала I кольца многочленов $\mathbb{C}[x_1, \ldots, x_n]$ справедливы следующие два утверждения:*

(i) $V(I) = \varnothing$ тогда и только тогда, когда $1 \in I$;

(ii) если f обращается в нуль во всех точках $V(I)$, то $f^k \in I$ для некоторого $k \in \mathbb{N}$.

Доказательство. Нам понадобится одно общее утверждение:

Упражнение 10. Доказать, что любой неединичный идеал любого кольца содержится в некотором максимальном идеале.

Докажем сначала утверждение (i).

Предположим, что I — неединичный идеал в $\mathbb{C}[x_1, \ldots, x_n]$. Нам надо доказать, что множество $V(I)$ непусто. Так как каждый неединичный идеал содержится в максимальном идеале, а множество нулей меньшего идеала содержит множество нулей большего идеала, то достаточно доказать, что для любого максимального идеала $J \subset \mathbb{C}[x_1, \ldots, x_n]$ множество его нулей в $\mathbb{C}^n$ непусто.

Факторкольцо $\mathbb{C}[x_1, \ldots, x_n]/J$ является полем (в силу максимальности идеала J). Обозначим это поле через $\mathbb{F}$. Поле $\mathbb{C}$ вкладывается в кольцо многочленов $\mathbb{C}[x_1, \ldots, x_n]$, следовательно, оно гомоморфно отображается в поле $\mathbb{F}$. Любой гомоморфизм полей является вложением, поэтому мы можем считать, что поле $\mathbb{C}$ вложено в поле $\mathbb{F}$.

Идеал J имеет хотя бы один нуль в $\mathbb{F}^n$: точку $(\bar{x}_1, \ldots, \bar{x}_n)$ (через $\bar{x}_i$ обозначен образ x_i при канонической проекции $\mathbb{C}[x_1, \ldots, x_n] \to \mathbb{F}$). Поэтому нам достаточно доказать, что $\mathbb{F} = \mathbb{C}$.

Предположим, что $\mathbb{F} \neq \mathbb{C}$. Рассмотрим произвольный элемент $a \in \mathbb{F} \setminus \mathbb{C}$. Заметим, что $f(a) \neq 0$ для любого ненулевого многочлена $f \in \mathbb{C}[t]$ (так как поле $\mathbb{C}$ алгебраически замкнуто, то все корни многочлена f лежат в $\mathbb{C}$). Поэтому все элементы вида $\dfrac{1}{a-\lambda}$, где $\lambda \in \mathbb{C}$, линейно независимы над $\mathbb{C}$. Так как поле $\mathbb{C}$ несчётно, то размерность $\mathbb{F}$ над $\mathbb{C}$ тоже несчётна. В то же время алгебра $\mathbb{C}[x_1, \ldots, x_n]$ счётномерна над $\mathbb{C}$, поэтому размерность $\mathbb{F} = \mathbb{C}[x_1, \ldots, x_n]/J$ не более чем счётна. Полученное противоречие доказывает, что $\mathbb{F} = \mathbb{C}$.

Выведем теперь утверждение (ii) из утверждения (i).

Пусть $f \in \mathbb{C}[x_1, \ldots, x_n]$ обращается в нуль во всех точках $V(I) \subset \mathbb{C}^n$. Вложим $\mathbb{C}[x_1, \ldots, x_n]$ в $\mathbb{C}[x_1, \ldots, x_n, t]$ и рассмотрим в этом большем кольце идеал J, порождённый многочленами из I и ещё одним многочленом $g = 1 - t \cdot f$. Множество $V(J)$ в пространстве $\mathbb{C}^{n+1}$ с координатами $(x_1, \ldots, x_n, t)$ пусто, ибо общие нули многочленов из I имеют вид (x, t), где $x \in V(I) \subseteq \mathbb{C}^n$, а в таких точках $g = 1$. Из утверждения (i) теоремы Гильберта следует тогда, что $1 \in J$.

Это означает, что найдутся многочлены $q_0, q_1, \ldots, q_s \in \mathbb{C}[x_1, \ldots, x_n, t]$ и $f_1, \ldots, f_s \in I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ такие, что

$$q_0(x,t)(1 - tf(x)) + q_1(t,x)f_1(x) + \cdots + q_s(x,t)f_s(x) = 1.$$

Написанное равенство есть равенство в кольце многочленов $\mathbb{C}[x_1, \ldots, x_n, t]$. Если вместо переменных в него подставить элементы произвольного поля $\mathbb{F} \supset \mathbb{C}$, то получится верное равенство в поле $\mathbb{F}$. Возьмём в качестве $\mathbb{F}$ поле рациональных функций $\mathbb{C}(x_1, \ldots, x_n)$, а в качестве значений x_ν и t подставим, соответственно, сами x_ν и дробь $1/f(x)$. Получим равенство

$$q_1(\frac{1}{f(x)}, x)f_1(x) + \cdots + q_s(\frac{1}{f(x)}, t)f_s(x) = 1,$$

справедливое в поле $\mathbb{C}(x_1, \ldots, x_n)$. Все знаменатели в этом равенстве имеют вид f^d, и от них можно избавиться, умножая обе части на достаточно большую степень f^k. В результате получится равенство в кольце многочленов $\mathbb{C}[x_1, \ldots, x_n]$, выражающее f^k через $f_1, \ldots, f_s$ с полиномиальными коэффициентами. Это доказывает, что $f^k \in I$. $\square$

Упражнение 11. Доказать, что в кольце многочленов $\mathbb{C}[x_1, \ldots, x_n]$ идеал, состоящий из всех многочленов, обращающихся в нуль в некоторой точке $(a_1, \ldots, a_n) \in \mathbb{C}^n$, максимален, и что так получаются все максимальные идеалы этого кольца.

Расширения полей.

Определение 3. Пусть $\mathbb{k}$ — поле. Любое поле $\mathbb{F}$, содержащее $\mathbb{k}$ в качестве подполя, называется *расширением поля* $\mathbb{k}$. Для расширений кроме обозначения $\mathbb{k} \subseteq \mathbb{F}$ используется обозначение $\mathbb{F}/\mathbb{k}$ (не подразумевающее никакого фактор-объекта: факторполей не бывает).

Поскольку $\mathbb{k}$ является подполем своего расширения $\mathbb{F}$, то определено умножение элементов $\mathbb{k}$ на элементы $\mathbb{F}$, удовлетворяющее аксиомам ассоциативности и дистрибутивности. Тем самым, любое расширение поля $\mathbb{k}$ является векторным пространством над полем $\mathbb{k}$ (и даже алгеброй над $\mathbb{k}$).

Определение 4. Расширение $\mathbb{F}/\mathbb{k}$ называется *конечным*, если $\mathbb{F}$ является конечномерным векторным пространством над $\mathbb{k}$. Размерность $\mathbb{F}$ над $\mathbb{k}$ называется *степенью* расширения $\mathbb{F}/\mathbb{k}$ и обозначается через $[\mathbb{F} : \mathbb{k}]$.

Упражнение 12. Доказать, что если $\mathbb{k} \subseteq \mathbb{F} \subseteq \mathbb{L}$ — последовательные расширения полей, то расширение $\mathbb{L}/\mathbb{k}$ является конечным тогда и только тогда, когда $\mathbb{F}/\mathbb{k}$ и $\mathbb{L}/\mathbb{F}$ — конечные расширения; кроме того, в этом случае $[\mathbb{L} : \mathbb{k}] = [\mathbb{L} : \mathbb{F}] \cdot [\mathbb{F} : \mathbb{k}]$.

Определение 5. Пусть $\mathbb{F}$ — расширение поля $\mathbb{k}$, и $a_1, \ldots, a_k \in \mathbb{F}$. Через $\mathbb{k}(a_1, \ldots, a_k)$ обозначается *подполе поля* $\mathbb{F}$*, порожденное над* $\mathbb{k}$ *элементами* $a_1, \ldots, a_k$, то есть минимальное (по включению) подполе, содержащее $\mathbb{k}$ и элементы $a_1, \ldots, a_k$. Через $\mathbb{k}[a_1, \ldots, a_k]$ обозначается *подкольцо поля* $\mathbb{F}$*, порожденное над* $\mathbb{k}$ *элементами* $a_1, \ldots, a_k$, то есть минимальное (по включению) подкольцо, содержащее $\mathbb{k}$ и элементы $a_1, \ldots, a_k$. Иначе $\mathbb{k}(a_1, \ldots, a_k)$ можно описать как множество всех элементов поля $\mathbb{F}$, которые можно выразить в виде рациональной функции с коэффициентами из $\mathbb{k}$ от $a_1, \ldots, a_k$, а $\mathbb{k}[a_1, \ldots, a_k]$ — как множество всех элементов поля $\mathbb{F}$, которые можно выразить в виде многочлена с коэффициентами из $\mathbb{k}$ от $a_1, \ldots, a_k$. Расширение $\mathbb{F}/\mathbb{k}$ называется *конечнопорожденным*, если $\mathbb{F} = \mathbb{k}(a_1, \ldots, a_k)$ для некоторых $a_1, \ldots, a_k \in \mathbb{F}$. Если $\mathbb{F} = \mathbb{k}(a)$, то элемент a называется *примитивным элементом* расширения $\mathbb{F}/\mathbb{k}$.

Определение 6. Пусть $\mathbb{F}$ — расширение поля $\mathbb{k}$. Элемент $a \in \mathbb{F}$ называется *алгебраическим над* $\mathbb{k}$, если $f(a) = 0$ для некоторого ненулевого многочлена $f(x) \in \mathbb{k}[x]$. Ненулевой многочлен минимальной степени из $\mathbb{k}[x]$ со старшим коэффициентом 1, аннулирующий алгебраический элемент $a \in \mathbb{F}$, называется *минимальным многочленом* этого элемента. Расширение $\mathbb{F}/\mathbb{k}$ называется *алгебраическим*, если любой элемент $a \in \mathbb{F}$ алгебраичен над $\mathbb{k}$. Поле $\mathbb{k}$ называется *алгебраически замкнутым в расширении* $\mathbb{F}$, если любой элемент поля $\mathbb{F}$, алгебраический над $\mathbb{k}$, принадлежит $\mathbb{k}$.

Ясно, что все многочлены, аннулирующие алгебраический элемент $a \in \mathbb{F}$, образуют идеал I_a кольца $\mathbb{k}[x]$. Стандартные рассуждения, использующие евклидовость этого кольца, доказывают, что идеал I_a порожден минимальным многочленом элемента a.

Упражнение 13. Доказать, что минимальный многочлен любого алгебраического над $\Bbbk$ элемента a расширения $\mathbb{F}/\Bbbk$ является неприводимым.

Теорема 5. *Если расширение* $\mathbb{F}/\Bbbk$ *является алгебраическим, то* $\Bbbk(a_1,\ldots,a_k)=\Bbbk[a_1,\ldots,a_k]$ *для любых* $a_1,\ldots,a_k\in\mathbb{F}$.

Доказательство. Пусть $k=1$, то есть мы порождаем расширение одним элементом $a_1=a$, и пусть $f(x)\in\Bbbk[x]$ — минимальный многочлен элемента a. Мы уже знаем, что многочлен $f(x)$ неприводим. Но тогда $\Bbbk[x]/(f(x))$ и, следовательно, $\Bbbk[a]$ является полем. Поэтому $\Bbbk(a)=\Bbbk[a]$.

Доказательство для любого k получается из приведенного выше рассуждения с помощью индукции по k. $\square$

Теорема 6. *Расширение* $\mathbb{F}/\Bbbk$ *является конечным тогда и только тогда, когда оно является одновременно алгебраическим и конечнопорожденным.*

Доказательство. То, что конечное расширение $\mathbb{F}/\Bbbk$ является конечнопорожденным, не должно вызывать сомнений. Докажем, что оно является алгебраическим. Пусть $a\in\mathbb{F}$ и $\dim_{\Bbbk}\mathbb{F}=n$. Рассмотрим элементы $1,a,a^2,\ldots,a^n$. Их количество больше размерности $\mathbb{F}$, поэтому существует нетривиальная линейная зависимость $\sum\limits_{k=0}^{n}\mu_n a^n=0$, то есть $f(x)=\sum\limits_{k=0}^{n}\mu_n x^n$ — ненулевой многочлен, аннулирующий a.

Пусть, наоборот, расширение $\mathbb{F}/\Bbbk$ является одновременно алгебраическим и конечнопорожденным. Тогда оно конечнопорождено как кольцо (согласно теореме 5). Если $\mathbb{F}=\Bbbk[a]$ для некоторого элемента $a\in\mathbb{F}$ (который является алгебраическим над $\Bbbk$), то $\mathbb{F}\cong\Bbbk[x]/(f(x))$, где $f(x)$ — минимальный многочлен элемента a. Поэтому $\mathbb{F}$ конечномерно над $\Bbbk$. Общий случай сводится к этому с помощью индукции по числу образующих. $\square$

Следствие 6.1. *Пусть* $\mathbb{F}$ *— произвольное расширение поля* $\Bbbk$. *Элемент* $a\in\mathbb{F}$ *алгебраичен над* $\Bbbk$ *тогда и только тогда, когда поле* $\Bbbk(a)$ *является конечномерным векторным пространством над* $\Bbbk$.

Следствие 6.2. *Пусть* $\mathbb{F}$ *— произвольное расширение поля* $\Bbbk$. *Множество элементов поля* $\mathbb{F}$, *алгебраических над* $\Bbbk$, *образует подполе поля* $\mathbb{F}$, *алгебраически замкнутое в* $\mathbb{F}$.

Доказательство. Если a,b — алгебраические над $\Bbbk$ элементы поля $\mathbb{F}$, то поле $\Bbbk(a,b)$ является, очевидно, конечномерным векторным пространством над $\Bbbk$. Поэтому все его элементы, в частности $a-b$ и a/b (при $b\neq 0$), являются алгебраическими. Поэтому множество $\mathbb{L}$ элементов поля $\mathbb{F}$, алгебраических над $\Bbbk$, является подполем поля $\mathbb{F}$.

Пусть элемент $a\in\mathbb{F}$ алгебраический над полем $\mathbb{L}$. Тогда он удовлетворяет уравнению $\sum_{k=0}^{n}b_k a^k=0$, где $b_k\in\mathbb{L}$. Ясно, что $\tilde{\mathbb{L}}=\Bbbk(b_0,\ldots,b_n)$ — конечное расширение поля $\Bbbk$. Но a алгебраичен над $\tilde{\mathbb{L}}$, поэтому $\tilde{\mathbb{L}}(a)$ — конечное расширение поля $\tilde{\mathbb{L}}$ и, следовательно, конечное расширение поля $\Bbbk$. Отсюда a алгебраичен над $\Bbbk$, то есть $a \in \mathbb{L}$. $\square$

Замечание. Для расширения $\mathbb{Q} \subseteq \mathbb{C}$ мы получаем, что множество $\bar{\mathbb{Q}}$ алгебраических чисел, то есть элементов поля $\mathbb{C}$, алгебраических над $\mathbb{Q}$, является счётным алгебраически замкнутым подполем поля $\mathbb{C}$. Счётность следует из того, что многочленов над $\mathbb{Q}$ счётное множество, а каждый многочлен имеет конечное множество корней.

Пусть $\mathbb{F}$ — произвольное расширение поля $\Bbbk$ и E — произвольное подмножество поля $\mathbb{F}$. Для любого подмножества $A \subseteq E$ обозначим через $s(A)$ пересечение E с алгебраическим замыканием поля $\Bbbk(A)$ в $\mathbb{F}$. Назовем s *оператором алгебраического замыкания*.

Упражнение 14. Доказать, что (E, s) — матроид.

Подмножество $A \subseteq E$ называется *алгебраически независимым*, если оно является независимым в матроиде (E, s). В противном случае множество A называется *алгебраически зависимым*.

Упражнение 15. Доказать, что множество $A \subseteq E \subseteq \mathbb{F}$ является алгебраически зависимым тогда и только тогда, когда для некоторых попарно различных элементов $a_1, \ldots, a_n \in A$ и для некоторого ненулевого многочлена $f \in \Bbbk[x_1, \ldots, x_n]$ в поле $\mathbb{F}$ выполнено равенство $f(a_1, \ldots, a_n) = 0$.

Упражнение 16. Доказать, что для любого алгебраически независимого подмножества $A \subseteq E \subseteq \mathbb{F}$ подкольцо $\Bbbk[A] \subseteq \mathbb{F}$ (соответственно подполе $\Bbbk(A) \subseteq \mathbb{F}$) изоморфно кольцу многочленов (соответственно полю рациональных функций) от элементов множества A, рассматриваемых как независимые переменные.

Базис матроида $(\mathbb{F}, s)$ называется *базисом трансцендентности* $\mathbb{F}$ над $\Bbbk$. Мощность любого базиса трансцендентности называется *степенью трансцендентности* $\mathbb{F}$ над $\Bbbk$.

Пример 2. Степень трансцендентности поля $\mathbb{C}$ над $\mathbb{Q}$ бесконечна (даже несчётна). Действительно, кольцо многочленов от конечного или счётного числа переменных над счётным полем счётно. Поэтому и поле рациональных функций от конечного или счётного числа переменных над счётным полем счётно. Алгебраическое замыкание счётного поля в любом расширении тоже счётно. Поэтому если бы степень трансцендентности $\mathbb{C}$ над $\mathbb{Q}$ была бы конечной или счётной, то и поле $\mathbb{C}$ было бы счётным множеством, что, как известно, не так.

Выведем из этого ещё одно доказательство теоремы Гильберта о нулях. Нам надо доказать, что у любого идеала I в кольце $\mathbb{C}[x_1, \ldots, x_n]$ есть нуль в $\mathbb{C}^n$. Пусть идеал I порождён многочленами $f_1, \ldots, f_m$ (мы пользуемся нётеровостью кольца многочленов). Нуль идеала I — это то же самое, что общий нуль многочленов $f_1, \ldots, f_m$. Пусть $\Bbbk$ — подполе поля $\mathbb{C}$, порождённое коэффициентами этих многочленов. Ясно, что оно имеет конечную степень трансцендентности над $\mathbb{Q}$ (оно конечно порождено, а базис трансцендентности можно выбрать из множества образующих); в то же время степень трансцендентности поля $\mathbb{C}$ над $\Bbbk$ бесконечна. Рассмотрим идеал $I_0 \subseteq \Bbbk[x_1, \ldots, x_n]$, порождённый многочленами $f_1, \ldots, f_m$, рассматриваемыми теперь как многочлены над $\Bbbk$. Он содержится в некотором максимальном идеале; обозначим этот максимальный идеал через J_0. Ясно, что многочлены $f_1, \ldots, f_m$ имеют общий нуль в $\mathbb{F}^n$, где поле $\mathbb{F} = \Bbbk[x_1, \ldots, x_n]/J_0$. Поле $\mathbb{F}$ мы считаем расширением поля $\Bbbk$ (которое вложено в $\mathbb{F}$ как образ многочленов нулевой степени). Докажем, что существует вложение $\varphi : \mathbb{F} \to \mathbb{C}$, тождественное на $\Bbbk$ (то есть переводящее все элементы поля $\Bbbk$ в себя).

Действительно, пусть $\bar{x}_1, \ldots, \bar{x}_n$ — образы переменных $x_1, \ldots, x_n$ при канонической проекции $\Bbbk[x_1, \ldots, x_n] \to \mathbb{F}$. Мы можем считать, что $\bar{x}_1, \ldots, \bar{x}_k$ алгебраически независимы над $\Bbbk$, а $\bar{x}_{k+1}, \ldots, \bar{x}_n$ алгебраичны над $\Bbbk(\bar{x}_1, \ldots, \bar{x}_k)$. Так как степень транцендентности поля $\mathbb{C}$ над $\Bbbk$ бесконечна, то в нём найдутся алгебраически независимые над $\Bbbk$ элементы $a_1, \ldots, a_k$. Положим $\varphi(\bar{x}_j) = a_j$ для $j = 1, \ldots, k$. Ясно, что таким образом получится изоморфизм подполя $\Bbbk(\bar{x}_1, \ldots, \bar{x}_k) \subseteq \mathbb{F}$ на подполе $\Bbbk(a_1, \ldots a_k) \subseteq \mathbb{C}$.

Далее, пусть $f(x)$ — минимальный многочлен элемента $\bar{x}_{k+1}$ над полем $\Bbbk(\bar{x}_1, \ldots, \bar{x}_k)$. Применим φ к его коэффициентам и обозначим полученный многочлен из $\mathbb{C}[x]$ через $f^{\varphi}(x)$. Так как поле $\mathbb{C}$ алгебраически замкнуто, то многочлен $f^{\varphi}(x)$ имеет комплексный корень. Обозначим его через a_{k+1} и положим $\varphi(\bar{x}_{k+1}) = a_{k+1}$. Ясно, что таким образом получается изоморфизм подполя $\Bbbk(\bar{x}_1, \ldots, \bar{x}_{k+1}) \subseteq \mathbb{F}$ на подполе $\Bbbk(a_1, \ldots a_{k+1}) \subseteq \mathbb{C}$. Продолжая этот процесс, мы получим искомое вложение поля $\mathbb{F}$ в поле $\mathbb{C}$.

Теперь заметим, что $(\varphi(\bar{x}_1), \ldots, \varphi(\bar{x}_n)) \in \mathbb{C}^n$ является общим нулём многочленов $f_1, \ldots, f_m$.

Поле разложения многочлена и алгебраическое замыкание поля.

Теорема 7. *Пусть* $f(x)$ *— неприводимый многочлен степени* n *над полем* $\Bbbk$. *Тогда существует расширение* $\mathbb{F}/\Bbbk$ *степени* n, *в котором многочлен* $f(x)$ *имеет корень.*

Доказательство. Факторкольцо $\tilde{\mathbb{F}} = \Bbbk[x]/(f(x))$ является полем. Поле $\Bbbk$ естественно вкладывается в него как образ многочленов нулевой степени. Обозначим это вложение через $\varkappa : \Bbbk \to \tilde{\mathbb{F}}$. Заменим каждый элемент вида $\varkappa(a)$ на a, где $a \in \Bbbk$. Другими словами, рассмотрим множество $\mathbb{F} = (\tilde{\mathbb{F}} \setminus \varkappa(\Bbbk)) \sqcup \Bbbk$ и введем на нем операции сложения и умножения, унаследованные из операций в поле $\tilde{\mathbb{F}}$. Ясно, что $\mathbb{F}$ — расширение поля $\Bbbk$ степени n. При этом образ x при канонической проекции $\Bbbk[x] \to \Bbbk[x]/(f(x))$ является корнем многочлена $f(x)$. $\square$

Эта конструкция называется *присоединением корня многочлена* $f(x)$.

Теорема 8. *Пусть* $f(x)$ *— многочлен над полем* $\Bbbk$. *Тогда существует конечное расширение* $\mathbb{F}/\Bbbk$, *над которым многочлен* $f(x)$ *раскладывается на линейные множители, причем* $\mathbb{F} = \Bbbk(x_1, \dots, x_n)$, *где* $x_1, \dots, x_n$ *— всевозможные корни многочлена* $f(x)$.

Доказательство. Если над полем $\Bbbk$ многочлен $f(x)$ не раскладывается на линейные множители, то присоединяем корень какого-нибудь его неприводимого сомножителя. Если над полученным полем $\Bbbk_1$ многочлен $f(x)$ не раскладывается на линейные множители, то присоединяем корень какого-нибудь его неприводимого сомножителя в $\Bbbk_1[x]$ и получаем поле $\Bbbk_2$, и так далее. С каждым шагом число корней многочлена $f(x)$ увеличивается, поэтому за конечное число шагов мы придем к полю, над которым многочлен $f(x)$ раскладывается на линейные множители. Ясно, что полученное таким образом поле $\mathbb{F}$ порождено корнями многочлена $f(x)$. ☐

Поле $\mathbb{F}$, удовлетворяющее условиям теоремы 8, называется *полем разложения многочлена* $f(x)$.

Теорема 9. *Пусть* $\varphi : \Bbbk \xrightarrow{\sim} \tilde{\Bbbk}$ *— изоморфизм полей,* $f(x) \in \Bbbk[x]$ *— неприводимый многочлен, а* $\tilde{f}(x) \in \tilde{\Bbbk}[x]$ *— многочлен, в который превращается* $f(x)$ *при применении к его коэффициентам изоморфизма* φ. *Предположим, что в некотором расширении поля* $\Bbbk$ *выбран элемент* a, *минимальным многочленом которого является* $f(x)$, *а в некотором расширении поля* $\tilde{\Bbbk}$ *выбран элемент* $\tilde{a}$, *минимальным многочленом которого является* $\tilde{f}(x)$. *Тогда существует изоморфизм* $\psi : \Bbbk(a) \to \tilde{\Bbbk}(\tilde{a})$, *совпадающий с* φ *на* $\Bbbk$, *и такой, что* $\psi(a) = \tilde{a}$.

Доказательство. Ясно, что требуемый изоморфизм определяется формулой $\sum \mu_k a^k \mapsto \sum \varphi(\mu_k)\tilde{a}^k$, где $\mu_k \in \Bbbk$. То, что это определение корректно, проверьте сами. ☐

Следствие 9.1. *Поле разложения любого многочлена определено однозначно с точностью до изоморфизма.*

Определение 7. Поле $\Bbbk$ называется *алгебраически замкнутым*, если любой многочлен раскладывается над ним на линейные множители.

Определение 8. Пусть $\Bbbk$ — произвольное поле. *Алгебраическим замыканием* поля $\Bbbk$ называется его алгебраическое расширение, являющееся алгебраически замкнутым полем. Алгебраическое замыкание поля $\Bbbk$ обычно обозначается через $\bar{\Bbbk}$.

Теорема 10. *У любого поля есть алгебраическое замыкание.*

Доказательство. Пусть $\Bbbk$ — произвольное поле. Рассмотрим множество Σ всех неприводимых многочленов из $\Bbbk[x]$ со старшим коэффициентом 1. Для каждого многочлена $f(x) \in \Sigma$ введём свою независимую переменную x_f и обозначим через A кольцо многочленов над $\Bbbk$ от всех x_f. Рассмотрим в кольце A идеал I, порождённый всеми многочленами вида $f(x_f)$ для $f(x) \in \Sigma$.

Докажем, прежде всего, что $I \neq A$. Действительно, если $I = A$, то имеет место равенство вида

$$\sum_{i=1}^{n} g_i f_i(x_{f_i}) = 1 \tag{1}$$

для некоторых ненулевых многочленов $g_i \in A$. Рассмотрим подмножество $\Sigma_0 \subseteq \Sigma$ тех $f \in \Sigma$, для которых x_f входит в равенство (1). Ясно, что Σ_0 — конечное множество (в отличие от Σ: доказательство Евклида бесконечности множества простых чисел проходит без изменений для кольца многочленов). Рассмотрим подкольцо A_0 кольца A, порожденное x_f для $f \in \Sigma_0$, и обозначим через I_0 идеал в A_0, порожденный многочленами $f(x_f)$ для $f \in \Sigma_0$. Обозначим через $\mathbb{L}$ поле разложения многочлена $\prod_{f\in\Sigma_0} f(x)$. Для любого многочлена $f \in \Sigma_0$ в поле $\mathbb{L}$ найдётся его корень a_f. Рассмотрим гомоморфизм ($\Bbbk$-алгебр) кольца A_0 в поле $\mathbb{L}$, переводящий x_f в a_f для любого $f \in \Sigma_0$. Этот гомоморфизм переводит 1 в 1, а ядро его содержит идеал I_0. Поэтому равенство (1) не может иметь место.

Воспользуемся теперь тем, что любой неединичный идеал любого кольца содержится в некотором максимальном идеале (факт, доказываемый применением леммы Цорна к множеству неединичных идеалов кольца, упорядоченных по включению). Обозначим через J максимальный идеал кольца A, содержащий идеал I. Положим $\Bbbk_1 = A/J$. По построению, каждый неприводимый многочлен из $\Bbbk[x]$ имеет корень в $\Bbbk_1$. Отметим, кстати, что поле $\Bbbk_1$ является алгебраическим расширением поля $\Bbbk$ (так как оно порождено образами переменных x_f, являющимися алгебраическими над $\Bbbk$).

Применем теперь такую же процедуру к полю $\Bbbk_1$. Полученное поле обозначим через $\Bbbk_2$. Поле $\Bbbk_2$ является вновь алгебраическим расширением поля $\Bbbk$ (так как элемент, алгебраичный над алгебраическим расширением поля, алгебраичен и над исходным полем). Продолжая этот процесс, получаем цепочку вложенных полей $\Bbbk \subseteq \Bbbk_1 \subseteq \Bbbk_2 \subseteq \ldots$. Обозначим через $\bar{\Bbbk}$ объединение всех этих полей. Ясно, что это алгебраическое расширение поля $\Bbbk$.

Любой неприводимый многочлен $f \in \Bbbk[x]$ раскладывается на линейные множители уже над $\Bbbk_k$, где $k = \deg f$, поэтому и над $\bar{\Bbbk}$. Пусть $h \in \bar{\Bbbk}[x]$ — неприводимый многочлен, и пусть $\mathbb{F}$ — поле, получающееся из $\bar{\Bbbk}$ присоединением корня b этого многочлена. Но тогда b алгебраичен и над $\Bbbk$. Пусть f — минимальный многочлен b над $\Bbbk$. Так как f раскладывается на линейные множители в $\bar{\Bbbk}[x]$, то $b \in \bar{\Bbbk}$, то есть $\deg h = 1$. Поэтому поле $\bar{\Bbbk}$ алгебраически замкнуто. $\square$

Упражнение 17. Доказать, что алгебраическое замыкание поля $\Bbbk$ единственно с точностью до изоморфизма, тождественного на $\Bbbk$.