Алгебраическая геометрия 1 — 14.10.2013, Лекция 6

Поля

Чтобы двигаться дальше, понадобятся некоторые понятия из теории полей. Напомним

Определение 1. Поле L – *конечное расширение* поля k, если $\mathsf{k} \subset L$ и L – конечномерное векторное пространство над k. Размерность этого векторного пространства называется *степенью* расширения и обозначается $[L : \mathsf{k}]$.

Предложение 2. *Если расширения полей $\mathsf{k} \subset L$ и $L \subset M$ конечны, то и расширение $\mathsf{k} \subset M$ конечно, при этом $[L : \mathsf{k}] \cdot [M : L] = [M : \mathsf{k}]$.*

Доказательство. Пусть $e_1, \ldots, e_n$ – базис L над k, а $f_1, \ldots, f_m$ – базис M над L. Тогда все произведения $e_i f_j$ образуют базис M над k. Действительно, если $x \in M$ произвольный, то $x = \sum_j \alpha_j f_j$, где $\alpha_j \in L$, значит $\alpha_j = \sum_i \beta_{ij} e_i$, получаем $x = \sum_j \sum_i \beta_{ij} e_i f_j$, где $\beta_{ij} \in \mathsf{k}$. Покажем, что $e_i f_j$ линейно независимы. Если $\sum_j \sum_i \beta_{ij} e_i f_j = 0$, то все $\sum_i \beta_{ij} e_i = 0$ т.к. f_j линейно независимы и значит все $\beta_{ij} = 0$ т.к. e_i линейно независимы. □

Определение 3. Пусть $\mathsf{k} \subset L$ – расширение полей и $\alpha \in L$. Элемент α называется *алгебраическим* над k, если существует ненулевой многочлен $f \in \mathsf{k}[x]$ такой, что $f(\alpha) = 0$. Иначе α называется *трансцендентным.*

Для любого элемента $\alpha \in L$ многочлены $f \in \mathsf{k}[x]$ такие, что $f(\alpha) = 0$, образуют идеал в $\mathsf{k}[x]$. Этот идеал, как и все идеалы в кольце $\mathsf{k}[x]$, главный. Если α алгебраический, то этот идеал ненулевой.

Определение 4. Порождающий этот идеал многочлен называется *минимальным* многочленом алгебраического элемента, обозначим его f_α.

Имеется гомоморфизм колец $\mathsf{k}[x] \to L$, переводящий x в α. Его ядро – (f_α), поэтому подкольцо $\mathsf{k}[\alpha]$ в L, порождённое α, изоморфно $\mathsf{k}[x]/(f_\alpha)$. Это подкольцо не имеет делителей нуля, поэтому многочлен f_α неприводим.

Предложение 5. *Подкольцо $\mathsf{k}[\alpha] \subset L$ является полем, причём это поле – конечное расширение k, его степень равна степени многочлена f_α.*

Доказательство. Идеал (f_α) в кольце главных идеалов $\mathsf{k}[x]$ порождён неприводимым многочленом, значит он максимален. Иначе, для любого $g \in \mathsf{k}[x], g \not\vdots f_\alpha$, многочлены f_α и g взамно просты. Поэтому существуют многочлены $u, v \in \mathsf{k}[x]$ для которых $f_\alpha u + gv = 1$. Подставляя α, получим $g(\alpha)v(\alpha) = 1$, значит $v(\alpha)$ – обратный к $g(\alpha)$. Базисом $\mathsf{k}[\alpha] = \mathsf{k}[x]/(f_\alpha)$ над k будут образы $1, x, x^2, \ldots, x^{\deg f_\alpha - 1}$. По модулю f_α через них выражаются все многочлены, а линейных соотношений на них нет, т.к. в (f_α) нет многочленов степени меньше $\deg f_\alpha$. □

Поле $k[\alpha]$ называется *полем, порождённым элементом* α над k. *Степенью* $\deg \alpha$ элемента α над k называется $[\mathsf{k}[\alpha] : \mathsf{k}] = \deg f_\alpha$.

Задача 1. У алгебраически замкнутых полей нет конечных расширений, кроме тривиального.

Задача 2. Покажите, что элементы a) $\sqrt{2} + \sqrt{7}$, b) $\sqrt[3]{2} + \sqrt{3}$, c) $\sqrt{2} + \sqrt[4]{-2}$ алгебраичны над $\mathbb{Q}$. Найдите их степени.

Задача 3. a) , b) , c) Найдите их минимальные многочлены.

Задача 4. Найдите степени элементов a) $u^2+1, 1/(u+1)$ в расширении $\mathbb{C}(u^3) \subset \mathbb{C}(u)$; b) $u+v, uv$ в расширении $\mathbb{C}(u^3, v^3) \subset \mathbb{C}(u, v)$.
Задача 5. a), b) Найдите их минимальные многочлены.

Обратно, если многочлен $f(x) \in \mathsf{k}[x]$ неприводим, то можно определить расширение поля k, полученное присоединением корня f. Рассмотрим факторкольцо $L = \mathsf{k}[x]/(f)$. Оно содержит k и является полем (т.к. идеал (f) максимален). Расширение $\mathsf{k} \subset L$ конечно, базисом L над k являются образы элементов $1, x, \ldots, x^{\deg f - 1}$. Соответственно, $[L : \mathsf{k}] = \deg f$. Элемент $[x]$ в L – корень многочлена f. Поле L – единственное с точностью до изоморфизма поле, содержащее k и порождённое над ним одним элементом, который есть корень f.

Замечание 6. Если многочлен f приводим, то поле, полученное добавлением его корня, не единственно. Например, добавляя к $\mathbb{Q}$ корень многочлена $x^4 - 4$, можно получить поля $\mathbb{Q}[\sqrt{2}]$ и $\mathbb{Q}[\sqrt{-2}]$.

Задача 6. Найдите степень поля, полученного добавлением корней многочлена x^4+4 к $\mathbb{Q}$.
Задача 7. a) Пусть $\mathsf{k} \subset L$ – расширение полей, $\alpha, \beta \in L$ – алгебраические элементы. Тогда расширение $\mathsf{k}[\alpha, \beta] \supset \mathsf{k}$ конечно и $[\mathsf{k}[\alpha, \beta] : \mathsf{k}] \leqslant \deg \alpha \cdot \deg \beta$. b) Элементы $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ алгебраичны над k.

Для трансцендентного элемента $\alpha \in L$ подкольцо $\mathsf{k}[\alpha]$ изоморфно кольцу многочленов $\mathsf{k}[x]$ и не является полем.

Предложение 7. *Если $\mathsf{k} \subset L$ – конечное расширение полей, то любой элемент $\alpha \in L$ алгебраичен над k.*

Доказательство. Степени $1, \alpha, \alpha^2, \alpha^3, \ldots$ лежат в конечномерном векторном пространстве L и потому линейно зависимы над k. Значит, есть соотношение $\sum \alpha^i c_i = 0$, где $c_i \in \mathsf{k}$, это и означает, что α алгебраичен. □

Предложение 8. *Если $\mathsf{k} \subset L$ – конечное расширение полей, и $\mathsf{k} \subset F \subset L$, где F – кольцо, то F – поле.*

Доказательство. Если F порождено над k как алгебра одним элементом, то всё было доказано раньше. Иначе возьмём $\alpha \in F \setminus \mathsf{k}$ и применим индукцию по степени $[L : \mathsf{k}]$ к расширению $\mathsf{k}[\alpha] \subset F \subset L$. □

Следствие 9. *Пусть алгебры A и B конечно порождены над полем k, $f\colon A \to B$ – гомоморфизм над k и $\mathfrak{n} \subset B$ – максимальный идеал. Тогда идеал $\mathfrak{m} = \mathfrak{n}^c \subset A$ тоже максимален и имеется цепочка вложений $\mathsf{k} \to \mathsf{k}(\mathfrak{m}) \to \mathsf{k}(\mathfrak{n})$.*

Доказательство. Рассмотрим композицию $A \xrightarrow{f} B \to B/\mathfrak{n}$. Её ядро – $\mathfrak{m}$, получаем вложение $A/\mathfrak{m} \to B/\mathfrak{n}$, также имеется вложение $\mathsf{k} \to A/\mathfrak{m}$. По предложению 8 $A/\mathfrak{m}$ – поле, значит $\mathfrak{m}$ – максимальный идеал и имеем вложения $\mathsf{k} \to \mathsf{k}(\mathfrak{m}) \to \mathsf{k}(\mathfrak{n})$. □

Таким образом, для каждой замкнутой точки $\mathfrak{m}$ спектра кольца A, конечно порождённого над полем k, имеется поле вычетов $\mathsf{k}(\mathfrak{m})$, это конечное расширение k. Чем больше это поле, тем «толще» замкнутая точка. Если поле k алгебраически замкнуто, то поля вычетов всех максимальных идеалов A совпадают с k и замкнутые точки не различаются по размеру.

Пусть имеется система полиномиальных уравнений $f_i(x_1, \dots, x_n) = 0$, где f_i – многочлены на полем k и $A = \mathsf{k}[x_1, \dots, x_n]/(f_i)$. Любое её решение $\bar{a} = (a_1, \dots, a_n) \in L^n$ над конечным расширением $L \supset \mathsf{k}$ определяет идеал $I_{\bar{a}} = \{[f] \in A \mid f(a_1, \dots, a_n) = 0\}$. Гомоморфизм вычисления

$$s\colon A \to L, \quad [f] \mapsto f(\bar{a})$$

имеет ядром $I_{\bar{a}}$, поэтому $A/I_{\bar{a}} \cong \operatorname{im} s \subset L$. Заметим, что $L \supset \operatorname{im} s \supset \mathsf{k}$. Значит, по предложению 8 $A/I_{\bar{a}}$ – поле и идеал $I_{\bar{a}}$ максимальный, его поле вычетов вложено в L.

Обратно, пусть $\mathfrak{m} \subset A$ – максимальный идеал и его поле вычетов вкладывается в L: $\sigma\colon A/\mathfrak{m} \to L$. Тогда $\mathfrak{m}$ имеет вид $I_{\bar{a}}$ для некоторого решения системы $\bar{a} \in L^n$. Действительно, пусть $\sigma([x_i]) = a_i \in L$, эти a_i дают решение системы, так как

$$f_i(a_1, \dots, a_n) = f_i(\sigma([x_1]), \dots, \sigma([x_n])) = \sigma(f_i([x_1], \dots, [x_n]) = \sigma([f_i]) = 0.$$

Пусть теперь многочлен $f \in \mathsf{k}[x_1, \dots, x_n]$ обращается в ноль в $\bar{a} = (a_1, \dots, a_n)$. Тогда $\sigma([f(x_1, \dots, x_n)]) = f(\sigma([x_1, \dots, x_n])) = f(a_1, \dots, a_n) = 0$, и так как σ вложение, то $[f] = 0$ и значит $f \in \mathfrak{m}$. Т.е. $I_{\bar{a}} \subset \mathfrak{m}$ и из-за максимальности $I_{\bar{a}} = \mathfrak{m}$.

Тем самым, доказано

Предложение 10. *Пусть $f_i \in \mathsf{k}[x_1, \dots, x_n]$ – многочлены. Решения системы уравнений $f_i(x_1, \dots, x_n) = 0$ в поле L соответствуют вложениям полей вычетов $\mathsf{k}(\mathfrak{m}) \to L$ максимальных идеалов $\mathfrak{m}$ кольца $\mathsf{k}[x_1, \dots, x_n]/(f_i)$.*

Таким образом одно кольцо $\mathsf{k}[x_1, \dots, x_n]/(f_i)$ хранит информацию о решениях системы уравнений над всевозможными расширениями поля k.

Вернёмся теперь к теореме о нулях.

Теорема 11 (алгебраическая версия теоремы Гильберта о нулях)**.** *Пусть A – конечно порождённая алгебра над полем k, сама являющаяся полем. Тогда A – конечное расширение поля k.*

Пример 12.

1. Пусть $A = \mathsf{k}[x]$. Тогда A конечно порождена над k как алгебра, но A – не поле. Теорема неприменима, и A – не конечномерное пространство над k.
2. Пусть $A = \mathsf{k}(x)$. Тогда A – поле и A конечно порождено над k как поле. Но A не конечно порождена как алгебра. Теорема неприменима, и A – не конечномерное пространство над k.

Доказательство. Рассмотрим частный случай: A порождена над k одним элементом x. Тогда если x алгебраический над k, то расширение конечно, т.к. можно выбрать базис над k из степеней x. Если же x трансцендентен над k, то $A \cong \mathsf{k}(x)$, а это не конечно порождённая алгебра над k.

В общем случае идея та же. Пусть $x_1, \dots, x_n$ порождают A над k. Тогда с точностью до перенумерации можно считать, что $x_1, \dots, x_m$ алгебраически независимы над k, а $x_{m+1}, \dots, x_n$ алгебраичны над полем $F = \mathsf{k}(x_1, \dots, x_m)$. Тогда поле A – конечное расширение F, так как порождено конечным числом алгебраических элементов. Пусть $e_1, \dots, e_d$ – базис A как векторного пространства над F. Выразим порождающие: $x_i = \sum c_{ij} e_j$, $c_{ij} \in F$. Выразим произведения: $e_i e_j = \sum c_{ijk} e_k$, $c_{ijk} \in F$. Любой элемент в A – многочлен от x_i с коэффициентами в k. Подставим в него вместо x_i их выражения через e_j, потом последовательно будем заменять произведения $e_i e_j$ на их выражение через e_k. Получим, что любой элемент a в A записывается единственным образом как линейная комбинация e_i, где коэффициенты – многочлены от c_{ij} и c_{ijk}:

$$a = \sum e_p \lambda_p, \quad \lambda_p \in \mathsf{k}[c_{ij}, c_{ijk}].$$

Элементы c_{ij} и c_{ijk} – рациональные функции от $x_1, \dots, x_m$. В знаменателях в них участвует конечное число неприводимых многочленов. Следовательно, в выражении всех элементов $a = \sum e_p \lambda_p$ в знаменателях λ_p встречается лишь конечное число неприводимых многочленов. Пусть $f \in \mathsf{k}[x_1, \dots, x_m]$ – неприводимый многочлен, которого там нет. Рассмотрим элемент e_1/f и получим противоречие, если только $m > 0$. Следовательно, $m = 0$, $F = \mathsf{k}$ и A – конечномерное пространство над k. $\square$