1 Спуск Галуа для векторных пространств (7 марта)

Пусть L/K — расширение полей. Векторное пространство W над K можно превратить в векторное пространство $L \otimes_K W$ над L посредством тензорного умножения. При этом W вкладывается в $L \otimes_K W$: $w \mapsto 1 \otimes w$. При этом любой K-базис $\{e_i\}$ в W превращается в L-базис $\{1 \otimes e_i\}$ пространства $L \otimes_K W$. Переход от W к $L \otimes_K W$ называется **восхождением (ascent)**. Обратно, если нам дано (ненулевое) векторное пространство V над L, можно попытаться описать K-подпространства $W \leq V$ такие, что K-базис пространства W является L-базисом пространства V.

Определение 1. Пусть V — векторное пространство над L. K-подпространство W такое, что K-базис W является L-базисом V, называется K**-формой** пространства V. Переход от V к K-форме V называется **спуском**.

Примеры 1. K-форма L^n — это K^n, поскольку стандартный K-базис K^n является L-базисом в L^n. K-форма $M_n(L)$ — это $M_n(K)$. K-форма $L[x]$ — это $K[x]$. У любого векторного пространства V над L есть K-форма: можно взять любой L-базис $\{e_i\}$ в V, и его K-линейная оболочка является K-формой V.

Теорема 1. *Пусть V — векторное пространство над L, W — K-подпространство V. Следующие условия эквивалентны:*

1. *любой K-базис W является L-базисом V;*
2. *некоторый K-базис W является L-базисом V;*
3. *L-линейное отображение $L \otimes_K W \to V$, $a \otimes w \mapsto aw$ является изоморфизмом векторных пространств над L.*

Пусть теперь L/K — конечное расширение Галуа и $G = \mathrm{Gal}(L/K)$.

Определение 2. Пусть V — векторное пространство над L, $\sigma \in G$. Отображение $r \colon V \to V$ называется σ**-линейным**, если оно аддитивно и $r(av) = \sigma(a)r(v)$ для всех $a \in L$, $v \in V$.

Определение 3. G**-структурой** на L-векторном пространстве V называется набор функций $r_\sigma \colon V \to V$, $\sigma \in G$ такой, что r_σ σ-линейно, $r_1 = \mathrm{id}_V$ и $r_\sigma \circ r_{\sigma'} = r_{\sigma\sigma'}$. Если на V задана G-структура, будем говорить, что G **полулинейно действует** на V.

Примеры 2. Пусть W — векторное пространство над K. На L-пространстве $L \otimes W$ можно ввести стандарную G-структуру: $r_\sigma(a \otimes w) = \sigma(a) \otimes w$. Если $\varphi \colon V \to V'$ — изоморфизм векторных пространств над L, и на V задана G-структура, то существует единственная G-структура на V', согласованная с φ.

Лемма 1. *Пусть V — векторное пространство на L с G-структурой, V' — G-инвариантное L-подпространство (то есть, $\sigma(V') \subseteq V'$ для всех $\sigma \in G$). Тогда на фактор-пространстве V/V' можно задать G-структуру: $\sigma(v + V') = \sigma(v) + V'$.*

Доказательство. Несложно. □

Лемма 2. *Пусть A — абелева группа, $\xi_1, \ldots, \xi_n \colon A \to L^\times$ — различные гомоморфизмы групп. Пусть V — векторное пространство над L, и $v_1, \ldots, v_n \in V$. Если $\xi_1(a)v_1 + \cdots + \xi_n(a)v_n = 0$ для всех $a \in A$, то $v_1 = \cdots = v_n = 0$.*

Доказательство. Линейная независимость характеров. □

Для векторного пространства V над L с G-структурой определим множество неподвижных точек $V^G = \{v \in V \mid \sigma(v) = v \text{ для всех } \sigma \in G\}$. Очевидно, что V^G является K-подпространством V.

Лемма 3. *Пусть V — векторное пространство над L с G-структурой. Определим отображение следа $\mathrm{Tr}_G \colon V \to V$ формулой $\mathrm{Tr}_G(v) = \sum_{\sigma\in G}\sigma(v)$. Тогда $\mathrm{Tr}_G(V) \subseteq V^G$ и для любого $v \in V$, $v \neq 0$, найдется $a \in L$ такое, что $\mathrm{Tr}_G(av) \neq 0$. В частности, если $V \neq 0$, то $V^G \neq 0$.*

Доказательство. Несложно. Для второй части нужно воспользоваться леммой 2 для $A = L^\times$. □

Теперь мы можем установить соответствие между K-формами и G-структурами.

Теорема 2. *Пусть V — векторное пространство над L. Существует естественная биекция между K-формами V и G-структурами на V, которая K-форме $W \subseteq V$ ставит в соответствие векторное пространство $L \otimes_K W$ со стандартной G-структурой (точнее, ее перенос на V вдоль изоморфизма), а G-структуре на V сопоставляет множество неподвижных относительно нее точек V^G.*

Доказательство. Мы приведем только [нетривиальный] кусок доказательства: докажем, что для пространства V с G-структурой K-подпространство V^G является K-формой на V. Более точно, отображение $f \colon L \otimes_K V^G \to V$, $a \otimes w \mapsto aw$, является изоморфизмом векторных пространств над L. Очевидно, что f является L-линейным отображением. Покажем, что f инъективно. Если $t \in L \otimes V^G$ таков, что $f(t) = 0$, можно записать t в виде суммы разложимых тензоров $t = \sum_i a_i \otimes w_i$. Более того, можно считать, что элементы $w_i \in V^G$ линейно независимы над K. Тогда $\sum a_i w_i = f(t) = 0$, то есть, w_i являются линейно зависимыми над L. Докажем, что такого не бывает: любая линейно независимая над K система векторов из V^G является линейно независимой над L. Предположим противное и рассмотрим минимальную нетривиальную линейную комбинацию $a_1w_1 + \dots + a_nw_n = 0$, где $a_i \in L$ и $w_i \in V^G$. Тогда $a_n \neq 0$, и после домножения на скаляр можно считать, что $a_n = 1$. Применяя к этой линейной комбинации σ, получаем $\sigma(a_1)w_1 + \dots + \sigma(a_n)w_n = 0$. Заметим, что $\sigma(a_n) = a_n = 1$ и вычтем одно равенство из другого: получим, что $(a_1 - \sigma(a_1))w_1 + \dots + (a_{n-1} - \sigma(a_{n-1})w_{n-1} = 0$. Это линейная комбинация меньшей длины, поэтому из минимальности следует, что $a_i = \sigma(a_i)$ для всех i и для всех $\sigma \in G$. Значит, все a_i лежат в K; поэтому исходные векторы были линейно зависимы над K, что противоречит нашему предположению.

Покажем теперь, что f сюръективно. Рассмотрим его образ $f(L \otimes_K V^G)$. Это L-подпространство в V, устойчивое относительно действия G. По лемме 1 на нем индуцируется G-структура. Для любого вектора $v \in V$ выполнено $\mathrm{Tr}_G(v) \in V^G \subseteq f(L \otimes_K V^G)$, откуда $\mathrm{Tr}_G(\overline{v}) = \overline{\mathrm{Tr}_G(v)} = \overline{0}$. По лемме 3 это означает, что $\overline{V} = \overline{0}$, поэтому $V = f(L \otimes V^G)$, и f сюръективно. □

В случае $K = \mathbb{R}$, $L = \mathbb{C}$ группа Галуа состоит из двух элементов: $G = \{1, c\}$, где c соответствует комплексному сопряжению. Поэтому для задания G-структуры на V достаточно задать одно c-линейное отображение $V \to V$. Сюръективность отображения $f \colon \mathbb{C} \otimes_{\mathbb{R}} V^G \to V$ легко видеть из тождества $v = \frac{v + c(v)}{2} + i\frac{v - c(v)}{2i}$. В случае произвольного расширения можно написать аналогичные формулы.

Пример 1. Пусть X — конечное множество с действием группы Галуа G. Рассмотрим пространство $V = \mathrm{Map}(X, L)$ всех отображений из X в L относительно поточечных операций. Дельта-функции δ_x ($\delta_x(x) = 1$, $\delta_x(y) = 0$ при $y \neq x$) образуют его базис. Зададим полулинейное действие G на V: для функции $f \colon X \to L$ и элемента $\sigma \in G$ определим $\sigma(f) \colon X \to L$

так, чтобы диаграмма

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\sigma"'] & L \arrow[d, "\sigma"] \\ X \arrow[r, "\sigma(f)"'] & L \end{tikzcd}$$

была коммутативна. Это означает, что $\sigma(f)(x) = \sigma(f(\sigma^{-1}(x)))$ для всех $x \in X$. Какая K-форма соответствует этой структуре? Наивный ответ $\mathrm{Map}(X, K)$ (то есть, линейная оболочка δ_x) не подходит, если только X не состоит целиком из неподвижных точек: дело в том, что $\sigma(\delta_x) = \delta_{\sigma(x)}$.

Хорошо известно, что представления группы G (над полем K) тесно связаны с групповой алгеброй $K[G]$. Аналогично, G-структуры на векторном пространстве связаны с действием некоторой алгебры, которую мы сейчас построим. Пусть $C(G) = \oplus_{\sigma\in G} Le_\sigma$ — L-векторное пространство с базисом, индексированным элементами группы G. Определим умножение в $C(G)$ правилами $e_\sigma c = \sigma(c)e_\sigma$ и $e_\sigma e_\tau = e_{\sigma\tau}$ для $\sigma, \tau \in G$ и $c \in L$. При этом $C(G)$ становится ассоциативной алгеброй над K (но не над L!) с единицей e_1, которая не является коммутативной при $L \neq K$. Нетрудно понять, что задание G-структуры на векторном пространстве V эквивалентно заданию структуры $C(G)$-модуля на V. При этом утверждение о существовании K-формы в любом пространстве превращается в тот факт, что любой $C(G)$-модуль раскладывается в прямую сумму модулей, изоморфных L (с естественной структурой $C(G)$-модуля).

Пусть теперь $V = L[x_1, \dots, x_n]$ и G действует на коэффициентах многочленов из V; это определяет G-структуру на V. Ее K-форма $W = V^G = K[x_1, \dots, x_n]$. Если $I \trianglelefteq V$, то $I^G = I \cap K[x_1, \dots, x_n] \trianglelefteq K[x_1, \dots, x_n]$. Будем говорить, что I **определен над** K, если он порождается (как идеал) некоторым подмножеством $K[x_1, \dots, x_n]$.

Теорема 3. *Для идеала $I \trianglelefteq L[x_1, \dots, x_n]$ равносильны:*

1. *I определен над K;*
2. *$\sigma(I) \subseteq I$ для всех $\sigma \in G$.*
3. *$\sigma(I) = I$ для всех $\sigma \in G$.*

Для контраста посмотрим на расширение $\mathbb{F}_p(\sqrt[p]{t})/\mathbb{F}_p(t)$, не являющееся расширением Галуа. Пусть $I = (x - \sqrt[p]{t}) \trianglelefteq L[x]$; тогда $\sigma(I) = I$ для всех $\sigma \in \mathrm{Aut}_K(L) = \{e\}$, но I не определен над K. В этом случае $I \cap K[x] = (x^p - t)$, поэтому идеал в $L[x]$, порожденный $I \cap K[x]$, строго меньше I.

Пусть V — векторное пространство над L с G-структурой. Отображение $c\colon G \to V$ называется **1-коциклом** на V, если $c(\sigma\tau) = c(\sigma) + \sigma(c(\tau))$ для всех $\sigma, tau \in G$.

Например, для фиксированного $v \in V$ функция $c_v\colon G \to V$, $\sigma \mapsto \sigma(v) - v$, является 1-коциклом. Теорема Гильберта 90 (в аддитивной форме) утверждает, что все 1-коциклы $c\colon G \to L$ имеют такой вид. Можно обобщить эту теорему до коциклов в векторных пространствах с G-структурой:

Теорема 4. *Пусть V — векторное пространство над L с G-структурой. Любой 1-коцикл на V имеет вид c_v для некоторого $v \in V$.*

Мы пронаблюдали простейший случай соответствия, который неформально можно описать так:

Теорема 5 (Мета-теорема 1). *Пусть L/K — конечное расширение Галуа с группой Галуа $G = \mathrm{Gal}(L/K)$. Тогда существует эквивалентность между категорией L-объектов с действием группы G (и G-эквивариантных морфизмов над L в качестве морфизмов) и категорией объектов над K (и морфизмов над K). При этом объекту над L с действием G сопоставляется объект неподвижных точек относительно этого действия; в обратную сторону соответствие устанавливается посредством расширения скаляров.*

Теорема 6 (Мета-теорема 2). *В условиях Мета-теоремы 1 существует биекция между множеством скрученных форм объекта V и множеством $H^1(G, \mathrm{Aut}_L(V_L))$. Здесь V — объект над K, и его скрученной формой называется объект V' над K, который при расширении скаляров становится изоморфным объекту V посредством некоторого изоморфизма $\varphi\colon V_L \to V'_L$. Эта биекция сопоставляет объекту V' коцикл $\varphi^{-1} \cdot {}^{\sigma}\varphi$, а обратная к ней сопоставляет коциклу $c \in Z^1(G, \mathrm{Aut}(V_L))$ объект $V' = ({}_cV_L)^G$ (или фактор $({}_cV_L)/G$) со следующим действием группы Галуа G: $\sigma(x) = c_\sigma {}^{\sigma}x$.*