РЕДУКТИВНЫЕ ГРУППЫ НАД КОЛЬЦАМИ. ПРИЛОЖЕНИЕ

Алексей Степанов

Содержание

Здесь представлены доказательства теорем, которые слишком сложны для презентации. Их можно рассказывать на доске при наличии времени.

G – редуктивная групповая схема над кольцом K, удовлетворяющая условиям, сформулированным ниже. В частности, условия выполнены для односвязной групповой схемы Шевалле–Демазюра $G = \mathrm{G}(\Phi, \_)$, $\Phi \neq A_1$ (в этом случае $K = \mathbb{Z}$). Условие односвязности нужно не для всех результатов, но для простоты будем всегда его предполагать.

Рассмотрим категорию K-*ideal*, объектами которой являются пары (K-алгебра,идеал в ней), а морфизм из $(R, \mathfrak{q}) \to (R', \mathfrak{q}')$ – это такой гомоморфизм колец $\varphi : R \to R'$ для которого $\varphi(\mathfrak{q}) \subseteq \mathfrak{q}'$. Морфизм называется сюръективным, если он сюръективен и на кольцах, и на идеалах.

Ясно, что $G(R, \mathfrak{a})$ определяет функтор из K-*ideal* в категорию групп. Рассмотрим групповой подфунктор $E(R, \mathfrak{a}) \subseteq G(R, \mathfrak{a})$. Чтобы отличать эти 2 функтора, от функторов $E, G : K\text{-}alg \to Groups$, будем обозначать их $\check{E}$ и $\check{G}$. В настоящем миникурсе мы доказываем несколько теорем про группы $E(R, \mathfrak{a})$ и $G(R, \mathfrak{a})$ при условии, что эти функторы удовлетворяют некоторым свойствам, выписанным ниже.

1. Аффинные групповые схемы

Пусть A – K-алгебра. $\mathrm{Sp}_K A(R) := \mathrm{Hom}_{K\text{-}alg}(A, R)$ – аффинная схема.

$G : K\text{-}alg \to Groups$ – функтор, композиция которого с забывающим – аффинная схема. $A = K[G]$ – аффинная алгебра схемы G – алгебра Хопфа.

Обозначим $g = \mathrm{id}_A \in G(A)$ – общий элемент схемы G. Если $a \in G(R)$, т.е. $a : A \to R$, то $G(a)(g) = a$. Вместо $G(a)$ пишем a.

Единичный элемент группы $G(K)$ – это гомоморфизм $e_K : A \to K$ – коединица. Ядро коединицы – фундаментальный идеал $I = \mathrm{Ker}\, e_K$. Заметим, что композиция $K \to A \xrightarrow{e_K} K$ тождественна, поэтому $K[G] = K \oplus I$ (как K-модули).

Пусть $\mathfrak{q}$ – идеал в R. $G(R, \mathfrak{q}) = \mathrm{Ker}\big(G(R) \to G(R/\mathfrak{q})\big)$.

Лемма 1.1. $a \in G(R, \mathfrak{q}) \iff a(I) \subseteq \mathfrak{q}$.

2. Аксиомы

Свойство 2.1 (нормальность)**.** $E(R, \mathfrak{q}) \trianglelefteq E(R)$.

Свойство 2.2 (сюръективность)**.** Функтор $\check{E}$ сохраняет сюръективные отображения.

Свойство 2.3 (порождение)**.** Пусть $\mathfrak{a}$ и $\mathfrak{b}$ – идеалы в R. Тогда

$$E(R, \mathfrak{a})E(R, \mathfrak{b}) = E(R, \mathfrak{a} + \mathfrak{b}).$$

Если R' – подалгебра в R такая, что $R = R' + \mathfrak{a}$, то

$$E(R')E(R, \mathfrak{a}) = E(R).$$

Лемма 2.4 (Принцип расщепления). *Если композиция $R' \rightarrowtail R \xrightarrow{\varphi} R'$ тождественна, а $\mathfrak{q} = \operatorname{Ker}\varphi$, то $G(R,\mathfrak{q}) \cap E(R) = E(R,\mathfrak{q})$.*

Свойство 2.5 (Разложение Гаусса). Существует покрытие схемы G главными открытыми подсхемами $\mathcal{G}_i = \operatorname{Sp}_K A_{s_i}$, где $i = 1,\dots,\ell$, содержащимися в E, причем $s_i - \delta_{1i} \in I$.

Следствие 2.6. *Если $\mathfrak{q}$ содержится в радикале Джекобсона кольца R, то $G(R,\mathfrak{q}) \leqslant E(R)$.*

Если R локальное кольцо, то $G(R) = E(R)$.

Заметим, что условие $\operatorname{Sp}_K A_{s_i} \leqslant E$ равносильно условию $\lambda_{s_i}(g) \in E(A_{s_i})$.

Свойство 2.7 (существование представления). Существует точное представление $\pi : G \to \mathrm{GL}_n$.

Для групп Шевалле имеет место и широко используется следующий принцип, называемый леммой Квиллена, Q-аксиомой или dilation principle.

Лемма 2.8 (стандартное избавление от знаменателей). *Пусть G – группа Шевалле с системой корней ранга $\geqslant 2$. Пусть S – мультипликативное подмножество в R, а $a \in G(R[t], tR[t])$. Предположим, что $\lambda_S(a) \in E(R_S[t])$. Тогда существует $s \in S$ такое, что $a(st) \in E(R[t], tR[t])$.*

В групп Шевалле этот принцип работает, потому что кольцо многочленов – это аффинная алгебра корневой подгруппы $X_\alpha \cong \mathbb{G}_a$. У нас нет никаких корневых подгрупп, поэтому необходимо усилить этот принцип.

Свойство 2.9 (избавление от знаменателей). Пусть R – кольцо, S – мультипликативное подмножество в R, $t \in R$ и $a \in G(R, tR)$. Предположим, что $\lambda_S(a) \in E(R_S, tR_S)$. Тогда существует $s \in S$ такой, что $\rho_r(a) \in E\big(R/(t-sr)R\big)$ для любого $r \in R$, где $\rho_r : R \to R/(t-sr)R$ – гомоморфизм редукции по модулю $t - sr$.

3. Нормальность элементарной подгруппы

Лемма 3.1 (Нормальность элементарной подгруппы). $[G(R,\mathfrak{q}), E(R)] \leqslant E(R,\mathfrak{q})$*, в частности $E(R) \trianglelefteq G(R)$.*

Доказательство. Пусть $a \in E(R)$. Рассмотрим кольцо $B = A \otimes R[t_1,\dots,t_\ell]/(t_1 + \dots + t_\ell - 1)$ (по умолчанию все тензорные произведения берутся над базовым кольцом K). Конечно, B – это просто кольцо многочленов над $A \otimes R$ от $\ell - 1$ переменной, но мы хотим рассматривать его как кольцо многочленов от t_i для всех $i = 1,\dots,\ell$. Образы элементов $a \in E(R)$ и $g \in G(A)$ в $G(B)$ будем обозначать теми же буквами.

По свойству “порождение” существуют элементы $a_i \in E(B, t_iB)$ такие, что $a = a_1 \dots a_\ell$. Возьмем $s_1,\dots,s_\ell$ из свойства “разложение Гаусса”. Так как $\lambda_{s_i}(g) \in E(B_{s_i})$, то для элемента $[g, a_i]$ выполнены условия свойства “стандартное избавление от знаменателей”. Поэтому существует $m_i \in \mathbb{N}$ такое, что $\varepsilon_i\big([g,a_i]\big) \in E(B)$, где ε_i гомоморфизм $B \to B$ тождественный на $A \otimes R$ и на всех t_j при $j \neq i, (i+1) \mod n$, и отображающий t_i в $s_i^{m_i} t_i$.

Так как набор $s_1,\dots,s_\ell$ унимодулярен в A, то набор $s_1^{m_1},\dots,s_\ell^{m_\ell}$ тоже унимодулярен, т. е. существуют $r_1,\dots,r_\ell \in A$ такие, что

$$r_1 s_1^{m_1} + \dots + r_\ell s_\ell^{m_\ell} = 1.$$

Зададим гомоморфизм $\varepsilon : B \to A \otimes R$ следующим образом: $\varepsilon(t_i) = r_i s_i^{m_i}$, а на $A \otimes R$ он действует тождественно. Ясно, что ε пропускается через любой из ε_i, поэтому $\varepsilon\big([g,a_i]\big) \in E(A \otimes R)$. Следовательно, $[g,a] = \varepsilon\big([g,a]\big) \in E(A \otimes R)$.

С другой стороны, $[g,a] \in G(A \otimes R, I \otimes R)$, а $A \otimes R = K \otimes R \oplus I \otimes R$. По принципу расщепления $[g,a] \in E(A \otimes R, I \otimes R)$. Пусть теперь $b \in G(R, \mathfrak{q})$. Применяя гомоморфизм $b \mathbin{\overline{\otimes}} \mathrm{id} : A \otimes R \to R$ к последнему включению, получаем $[b,a] \in E(R, \mathfrak{q})$ (здесь и далее $\overline{\otimes}$ обозначает композицию тензорного произведения гомоморфизмов с умножением). □

4. Расширенная элементарная группа

Пусть ℓ – количество главных открытых подсхем, которыми покрывается G по свойству "разложение Гаусса".

Определение 4.1 (расширенная элементарная группа)**.**

$$\widetilde{E}(R, \mathfrak{q}) = \bigcap_{(r_1, \ldots, r_\ell) \in \mathrm{Um}_\ell(R)} \prod_{i=1}^{\ell} G(R, r_i \mathfrak{q}).$$

Лемма 4.2. $E(R, \mathfrak{q}) \leqslant \widetilde{E}(R, \mathfrak{q})$.

Доказательство. $E(R, \mathfrak{q}) = \prod_{i=1}^{\ell} E(R, r_i \mathfrak{q}) \leqslant \prod_{i=1}^{\ell} G(R, r_i \mathfrak{q})$. □

Лемма 4.3. *Пусть $\mathfrak{a}$ и $\mathfrak{b}$ – идеалы кольца R. Тогда $[G(R, \mathfrak{a}), G(R, \mathfrak{b})] \subseteq G(R, \mathfrak{a}\mathfrak{b})$.*

Доказательство. Заметим, что

$$A \otimes_K A = (K \oplus I) \otimes_K (K \oplus I) = K \oplus I \otimes_K K \oplus K \otimes_K I \oplus I \otimes_K I.$$

Поэтому $(A \otimes_K I) \cap (I \otimes_K A) = I \otimes_K I$. Существует два естественных отображения кольца A в $A \otimes_K A$. Обозначим через g_1 и g_2 образы общего элемента $g \in G(A)$ в $G(A \otimes_K A)$ под действием этих отображений. Так как $g_1 \in G(A \otimes_K A, I \otimes_K A)$, а $g_2 \in G(A \otimes_K A, A \otimes_K I)$, то

$$[g_1, g_2] \in G\big(A \otimes_K A, I \otimes_K A\big) \cap G\big(A \otimes_K A, A \otimes_K I\big) = \\ G\big(A \otimes_K A, (I \otimes_K A) \cap (A \otimes_K I)\big) = G\big(A \otimes_K A, I \otimes_K I\big).$$

Пусть теперь $a \in G(R, \mathfrak{a})$, а $b \in G(R, \mathfrak{b})$. Тогда гомоморфизм $a \mathbin{\overline{\otimes}} b : A \otimes_K A \to R$ отображает $I \otimes_K A$ в $\mathfrak{a}$, а $A \otimes_K I$ в $\mathfrak{b}$. Индуцированный гомоморфизм групп $a \mathbin{\overline{\otimes}} b : G(A \otimes_K A) \to G(R)$ отображает g_1 в a, а g_2 в b. Поэтому $[a,b] = (a \mathbin{\overline{\otimes}} b)\big([g_1, g_2]\big) \in (a \mathbin{\overline{\otimes}} b)\big(G(A \otimes_K A, I \otimes_K I)\big) \leqslant G(R, \mathfrak{a}\mathfrak{b})$. □

Следствие 4.4. *Пусть $\mathfrak{a}$ и $\mathfrak{b}$ – идеалы кольца R. Тогда $[\widetilde{E}(R, \mathfrak{a}), G(R, \mathfrak{b})]$ содержится в $\widetilde{E}(R, \mathfrak{a}\mathfrak{b})$.*

5. Ключевая конструкция

Лемма 5.1. *Существует кольцо $D = D_G$ и элементы $t \in D$ и $f \in G(D, tD)$, удовлетворяющие следующему версальному свойству.*

Для любого кольца R и элементов $r \in R$ и $h \in G(R, rR)$ существует гомоморфизм $\theta : D \to R$ такой, что $\theta(t) = r$ и $\theta(f) = h$.

Конструкция.

$$\begin{tikzcd} K[z_{ij}] = K[M_n] \arrow[r, "\varphi"] \arrow[d, "\pi^*"'] & K[t, y_{ij}] \arrow[d, "\xi"'] \\ A \arrow[r, "f"] & D \end{tikzcd}$$

где $\varphi(z) = e + ty$, т. е. $\varphi(z_{ij}) = \delta_{ij} + t y_{ij}$. □

Будем обозначать через t и y_{ij} их канонические образы в D. Пусть Y – идеал в D, порожденный всеми y_{ij}.

6. Версальный элемент расширенной элементарной группы

Пусть $D^{(k)}$ обозначает кольцо изоморфное D, порожденное элементами $t^{(k)}$ и $y_{ij}^{(k)}$ вместо t и y_{ij} (где $1 \leqslant i, j \leqslant n$). Аналогично будем писать $f^{(k)} \in G(D^{(k)})$ вместо $f \in G(D)$. Положим

$$U = \bigotimes_{k=1}^{\ell} D^{(k)} \text{ и } u = f^{(1)} \cdots f^{(\ell)} \in G(U).$$

Обозначим через $\widetilde{Y}$ идеал в U, порожденный всеми $y_{ij}^{(k)}$.

Лемма 6.1. *Для любого кольца R, унимодулярной последовательности $r_1, \ldots, r_\ell \in R$ и элемента $b \in \widetilde{E}(R, \mathfrak{q})$ существует гомоморфизм $\eta : U \to R$ такой, что $\eta(u) = b$, $\eta(t^{(i)}) = r_i$ для всех $i = 1, \ldots, \ell$ и $\eta(\widetilde{Y}) \subseteq \mathfrak{q}$.*

Лемма 6.2. *Идеал Y является расщепляющим в D.*

Идеал $\widetilde{Y}$ является расщепляющим в U.

Пусть R – кольцо, а $s \in R$. Обозначим через Y' идеал $(Y \otimes_K R)/(t - s)$ кольца $(D \otimes_K R)/(t - s)$. Тогда $(D \otimes_K R)/(t - s) = R \oplus Y'$ как аддитивные группы.

7. Усиленные коммутационные формулы и длина коммутаторов

Пусть S подфунктор в $\check{E}$ такой, что $S(R, \mathfrak{q})$ порождает $E(R, \mathfrak{q})$ для любого кольца R и идеала $\mathfrak{q}$ в R. Тогда S называется функториальным порождающим множеством для $\check{E}$.

Теорема 7.1 (усиленные коммутационные формулы и длина коммутаторов)**.** $[G(R, \mathfrak{q}), \widetilde{E}(R)] \leqslant E(R, \mathfrak{q})$ *и* $[G(R), \widetilde{E}(R, \widetilde{q})] \leqslant E(R, \mathfrak{q})$.

Более того, существует константа $L \in \mathbb{N}$, зависящая только от G, такая, что для любого кольца R, идеала $\mathfrak{q}$ в R, $b \in G(R)$ и $a \in \widetilde{E}(R, \mathfrak{q})$ (или $b \in G(R, \mathfrak{q})$ и $a \in \widetilde{E}(R)$) длина коммутатора $[a, b]$ относительно $\mathcal{S}(R, \mathfrak{q})$ не превосходит L.

Доказательство. Рассмотрим кольцо $C = A \otimes U$. Образы элементов $u \in G(U)$ и $g \in G(A)$ в $G(C)$ будем обозначать теми же буквами.

Возьмем $s_1, \ldots, s_\ell$ из свойства “разложение Гаусса”. Так как $\lambda_{s_i}(g) \in E(C_{s_i})$, а $f^{(i)} \in G(C, t^{(i)}C)$, то $[g, f^{(i)}] \in G(C, t^{(i)}C)$, а $\lambda_{s_i}\big([g, f^{(i)}]\big) \in E(C_{s_i}, t^{(i)}C_{s_i})$. По свойству “избавление от знаменателей” существует $m_i \in \mathbb{N}$ такое, что $\rho_i\big([g, f^{(i)}]\big) \in E\big(C/(t^{(i)} - s_i^{m_i})\big)$, где ρ_i – гомоморфизм редукции $C \to C/(t^{(i)} - s_i^{m_i})$.

Обозначим через T идеал в $U \otimes A$, порожденный $t^{(i)} - s_i^{m_i}$ по всем $i = 1, \ldots, \ell$, а через $\rho : C \to C/T$ – гомоморфизм редукции. Так как ρ пропускается через любой из ρ_i, то $\rho\big([g, u]\big) \in E(C/T)$. Можно показать, что образы идеалов $A \otimes \widetilde{Y}$ и $I \otimes U$ являются расщепляющими в C/T. Используя принцип расщепления, получим $\rho\big([g, u]\big) \in E(C/T, \mathfrak{a})$, где $\mathfrak{a}$ является образом $A \otimes \widetilde{Y}$ или $I \otimes U$ в C/T.

По свойству “сюръективность” существуют элементы $v \in E(C, I \otimes U)$ и $v' \in E(C, A \otimes \widetilde{Y})$ такие, что

$$[g, u] \in vG(C, T) = v'G(C, T).$$

Пусть теперь $a \in \tilde{E}(R, \mathfrak{q})$, а $b \in G(R)$. Положим $r_i = b(s_i^{m_i})$. Так как набор $(r_1, \ldots, r_\ell)$ унимодулярен, то по версальному свойству элемента u существует гомомрфизм $\varphi : U \to R$ такой, что $\varphi(t^{(i)}) = r_i$, $\varphi(u) = a$, а $\varphi(\widetilde{Y}) \subseteq \mathfrak{q}$. Заметим, что $b \mathbin{\overline{\otimes}} \varphi(s_i^{m_i}) = b \mathbin{\overline{\otimes}} \varphi(t^{(i)})$, поэтому $b\overline{\otimes}\varphi(T)=0$. Подействовав гомоморфизмом $b\overline{\otimes}\varphi$ на включение $[g,u]\in v'G(C,T)$ получим

$$[b,a]=b\,\overline{\otimes}\,\varphi\big([g,u]\big)=b\,\overline{\otimes}\,\varphi(v')\in E(R,\mathfrak{q}),$$

причем длина коммутатора $[b,a]$ в образующих $S(R,\mathfrak{q})$ не превосходит длины v' в образующих $S(C,A\otimes\widetilde{Y})$. Аналогичные рассуждения с заменой v' на v работают и в случае $a\in\widetilde{E}(R)$, а $b\in G(R,\mathfrak{q})$. □

8. Мультикоммутационные формулы

Теорема 8.1. *Пусть $\mathfrak{a}_1,\dots,\mathfrak{a}_m$ – идеалы кольца R. Тогда*

$$[\widetilde{E}(R,\mathfrak{a}_1),G(R,\mathfrak{a}_2),\dots,G(R,\mathfrak{a}_m)]\leqslant[\widetilde{E}(R,\mathfrak{a}_1\dots\mathfrak{a}_{m-1}),G(R,\mathfrak{a}_m)]=:EE(R,\mathfrak{a}_1\dots\mathfrak{a}_{m-1},\mathfrak{a}_m).$$

В частности,

$$[\widetilde{E}(R,\mathfrak{a}_1),G(R,\mathfrak{a}_2),\dots,G(R)]\leqslant[\widetilde{E}(R,\mathfrak{a}_1\dots\mathfrak{a}_{m-1}),G(R)]\leqslant E(R,\mathfrak{a}_1\dots\mathfrak{a}_{m-1}).$$

Теорема 8.2 (обобщение нильпотентности K_1)**.** *Если R – нетерово кольцо, размерность пространства максимальных идеалов которого не превосходит d, то для любых идеалов $\mathfrak{a}_0,\dots,\mathfrak{a}_d$ кольца R*

$$[G(R,\mathfrak{a}_1),G(R,\mathfrak{a}_2),\dots,G(R,\mathfrak{a}_m)]\leqslant EE(R,\mathfrak{a}_1\dots\mathfrak{a}_{m-1},\mathfrak{a}_m).$$

9. Нормальное строение

Приведем версию теоремы о нормальном строении групп Шевалле при условии обратимости структурных констант. Естественно, для доказательства этого результата уже не достаточно приведенных аксиом. Пусть $G=\mathrm{G}(\Phi,\_)$ – групповая схема Шевалле–Демазюра с приведенной неприводимой системой корней $\Phi\neq A_1$. Обозначим через $C(R,\mathfrak{q})$ прообраз центра при гомоморфизме редукции $R\to R/\mathfrak{q}$.

Теорема 9.1. *Предположим, что 2 обратима в R, если $\Phi=B_n,C_n,F_4$, и 6 обратима в случае $\Phi=G_2$. Тогда для любой подгруппы $H\leqslant G(R)$, нормализуемой $E(R)$, существует единственный идеал $\mathfrak{q}$ кольца R такой, что*

$$E(R,\mathfrak{q})\leqslant H\leqslant C(R,\mathfrak{q}).$$

Для $\alpha\in\Phi$ положим $\mathfrak{q}_\alpha(H)=\{t\in R\,|\,x_\alpha(t)\in H\}$.

Лемма 9.2 (вычисление уровня)**.** $\mathfrak{q}(H):=\mathfrak{q}_\alpha(H)$ *не зависит от корня $\alpha\in\Phi$ и является идеалом в R.*

Лемма 9.3 (основная редукция)**.** *Предположим, что любая нецентральная подгруппа в $G(\bar{R})$, нормализуемая $E(\bar{R})$ над любым факторкольцом $\bar{R}$ кольца R содержит нетривиальный корневой унипотентный элемент. Тогда нормальное строение группы $G(R)$ стандартно.*

Лемма 9.4 (извлечение унипотента из клетки Гаусса)**.** *Если H содержит нецентральный элемент из клетки Гаусса (в частности, из $G(R,\operatorname{Rad}R)$) то она содержит нетривиальный корневой унипотентный элемент.*

Следствие 9.5 (стандартность над полем)**.** *Если R поле, то либо H содержится в центре, либо содержит $E(R)$.*

Лемма 9.6 (извлечение унипотента из общего элемента)**.** *Пусть H_g – наименьшая подгруппа $G(A)$, нормализуемая $E(A)$ и содержащая общий элемент g схемы G, а $S=V\big(\mathfrak{q}(H_g)\big)$. Тогда $S(R)\not\supseteq E(R)$ для любого кольца R.*

Доказательство теоремы о нормальном строении. Предпложим, что H не содержит нетривиальных корневых унипотентов. Условие $h(S) \neq 0$ для какого-то $h \in H$ противоречит предположению.

Следовательно, $H \subseteq S(R)$. При редукции по любому максимальному идеалу $\overline{H} := \rho_{\mathfrak{m}}(H) \subseteq S(R/\mathfrak{m})$. Следовательно, $\overline{H} \not\supseteq E(R/\mathfrak{m})$. По следствию "стандартность над полем" $[\overline{H}, E(R/\mathfrak{m})] = \{e\}$.

Таким образом, $[H, E(R)] \leqslant G(R, \operatorname{Rad} R)$. По следствию "извлечение унипотента из клетки Гаусса" $[H, E(R)]$ лежит в центре. Так как $E(R)$ совпадает со своим коммутантом, а ее централизатор совпадает с центром $G(R)$, то теория групп говорит, что H содержится в центре $G(R)$. $\square$