# RUSSIAN EXAM – FALL QUARTER 2005

## ТЕОРЕМА РИМАНА — РОХА

(1)

### § 1. ЛЕММЫ О НОРМИРОВАНИЯХ

Напомним, что ***кольцом дискретного нормирования*** $\mathfrak{o}$ называется кольцо главных идеалов (и тем самым кольцо, в котором разложение на множители однозначно), имеющее единственный ненулевой простой идеал. Любая образующая $t$ этого идеала называется ***локальным параметром***. Каждый элемент $x \neq 0$ кольца $\mathfrak{o}$ представляется в виде

$$x = t^r y,$$

где $r$ — целое число $\geqslant 0$, а $y$ — единица (обратимый элемент). Значит, элементы поля частных $K$ тоже представляются в таком виде, только $r$ может быть любым целым числом. Это число называется ***порядком*** (или ***нормой***) соответствующего элемента. Если $r > 0$, то мы говорим, что $x$ имеет ***нуль*** в данном нормировании, а если $r < 0$, то ***полюс***. Мы пишем

$$r = v_{\mathfrak{o}}(x), \quad \text{или } v(x), \quad \text{или } \operatorname{ord}_{\mathfrak{o}}(x).$$

Пусть $\mathfrak{p}$ — максимальный идеал в $\mathfrak{o}$. Отображение поля $K$, которое совпадает с каноническим гомоморфизмом $\mathfrak{o} \to \mathfrak{o}/\mathfrak{p}$ на $\mathfrak{o}$, а все элементы $x \notin \mathfrak{o}$ переводит в $\infty$, называется *точкой*, отвечающей этому нормированию.

Мы примем без доказательства несколько основных результатов о нормированиях; их можно найти в моей книге „Алгебра“ [1]). А именно, пусть $E$ — конечное расширение поля $K$ и $\mathfrak{o}$ — кольцо дискретного нормирования в $K$ с максимальным идеалом $\mathfrak{p}$. Тогда в поле $E$ существует кольцо дискретного нормирования $\mathfrak{O}$ с максимальным идеалом $\mathfrak{P}$, такое, что

$$\mathfrak{o} = \mathfrak{O} \cap K \quad \text{и} \quad \mathfrak{p} = \mathfrak{P} \cap K.$$

---

[1]) Русский перевод: „Мир“, 1968. — *Прим. ред.*

Если $u$ — простой элемент кольца $\mathfrak{O}$, то $t\mathfrak{O} = (u)$. Число $e$ называется ***индексом ветвления*** $\mathfrak{O}$ над $\mathfrak{o}$ (или $\mathfrak{P}$ над $\mathfrak{p}$). Если $\Gamma_{\mathfrak{O}}$ и $\Gamma_{\mathfrak{o}}$ — группы нормирований этих колец, то $(\Gamma_{\mathfrak{O}} : \Gamma_{\mathfrak{o}}) = e$.

**Пример.** Пусть $k$ — поле, $t$ трансцендентно над $k$ и $a \in k$. Обозначим через $\mathfrak{o}$ множество рациональных функций $f(t)/g(t)$, где $f(t), g(t) \in k[t]$ и $g(a) \neq 0$. Тогда $\mathfrak{o}$ — кольцо дискретного нормирования, максимальный идеал которого состоит из функций с $f(a) = 0$. Это — типичная ситуация. В самом деле, пусть (для простоты) $k$ алгебраически замкнуто. Рассмотрим расширение $k(x)$, полученное присоединением к $k$ одного трансцендентного элемента $x$. Пусть $\mathfrak{o}$ — любое кольцо дискретного нормирования в $k(x)$, содержащее $k$. Заменив при необходимости $x$ на $1/x$, мы можем считать, что $x \in \mathfrak{o}$. Тогда $\mathfrak{p} \cap k[x] \neq 0$, поэтому идеал $\mathfrak{p} \cap k[x]$ порождается некоторым неприводимым многочленом $p(x)$, который должен быть линейным, ибо по предположению $k$ алгебраически замкнуто. Значит, $p(x) = x - a$ для некоторого $a \in k$. Тогда каноническое отображение

$$\mathfrak{o} \to \mathfrak{o}/\mathfrak{p}$$

индуцирует на многочленах отображение

$$f(x) \mapsto f(a).$$

Отсюда очевидно, что $\mathfrak{o}$ состоит из всех частных $f(x)/g(x)$, для которых $g(a) \neq 0$. Тем самым мы оказываемся в ситуации, описанной в начале примера.

Аналогично, пусть $\mathfrak{o} = k[[t]]$ — кольцо формальных степенных рядов от одной переменной. Это — кольцо дискретного нормирования, максимальный идеал которого порожден $t$. Любой элемент поля частных разлагается в формальный ряд

$$x = a_{-m}t^{-m} + \ldots + a_{-1}t^{-1} + a_0 + a_1 t + a_2 t^2 + \ldots$$

с коэффициентами $a_i \in k$. Точка отображает $x$ в коэффициент $a_0$, если только она не является полюсом для $x$.

Нам понадобится одна аппроксимационная теорема, обеспечивающая существование функции (т. е. элемента поля $K$) с частично предписанными нулями и полюсами. Пусть $K$ — некоторое поле, $o_1, \ldots o_n$ — конечное множество колец дискретных нормирований в нем.

**Предложение 1.** *Если $o_1$, $o_2$ — кольца дискретных нормирований с общим полем частных $K$ и $o_1 \subset o_2$, то $o_1 = o_2$.*

Доказательство. Покажем сначала, что если $p_1$, $p_2$ — соответствующие максимальные идеалы, то $p_2 \subset p_1$. Пусть $y \in p_2$. Если $y \notin p_1$, то $1/y \in o_1$, откуда $1/y \in o_2$ — противоречие. Значит, $p_2 \subset p_1$. Любая единица кольца $o_1$ тем более является единицей в $o_2$. Каждый элемент $y \in p_2$ можно записать в виде $y = \pi_1^{v_1} u$, где $u$ — некоторая единица кольца $o_1$, а $\pi_1$ — элемент порядка 1 в $p_1$. Если элемент $\pi_1$ не лежит в $p_2$, то он должен быть единицей в $o_2$, что не так. Значит, $\pi_1 \in p_2$, так что $p_1 = o_1 \pi_1$. Поэтому $p_2 = p_1$. Наконец, если $u$ — единица в $o_2$, но не в $o_1$, то $1/u \in p_1$, а это невозможно для единиц из $o_2$, чем доказательство и завершается. ■

Впредь мы будем считать, что *кольца $o_i$ $(i = 1, \ldots, n)$ различны и, значит, ни одно из них не содержится в другом.*

**Предложение 2.** *Существует элемент $y$ поля $K$, имеющий нуль в $o_1$ и полюсы в $o_j$ $(j = 2, \ldots, n)$.*

Доказательство. Применим индукцию по $n$. При $n = 2$ можно найти элементы $y \in o_2$, $y \notin o_1$ и $z \in o_1$, $z \notin o_2$, ибо наши кольца не вложены друг в друга. Тогда $z/y$ имеет нуль в $o_1$ и полюс в $o_2$, что и требовалось.

Предположим, что мы уже нашли элемент $y \in K$ с нулем в $o_1$ и полюсами в $o_2, \ldots, o_{n-1}$. Пусть еще $z$ имеет нуль в $o_1$ и полюс в $o_n$. Тогда для достаточно большого $r$ элемент $y + z^r$ удовлетворяет нашим требованиям. Действительно, для значений в точке имеем: нуль + нуль = нуль; нуль + полюс = полюс, и сумма полюсов разных порядков дает полюс. ■

## § 4. Алгебры Галуа

$S$-алгебра $A$ над полем $k$ называется алгеброй Галуа с группой $G$, если существует гомоморфизм группы $G$ в группу автоморфизмов над $k$ алгебры $A$ и $A$ обладает $G$-нормальным базисом над $k$. Таким образом, алгебра Галуа является одновременно $S$-алгеброй и $k$-модулем регулярного представления группы $G$.

Заметим, что указание группы $G$ в определении алгебры Галуа необходимо, одна и та же $S$-алгебра иногда может быть наделена структурой алгебры Галуа для различных групп. Например, если $A$ — вполне распадающаяся $S$-алгебра, то ее полная группа автоморфизмов над $k$ есть вся симметрическая группа перестановок прямых слагаемых, так что $A$ можно наделить структурой алгебры Галуа для любой группы порядка, равного числу прямых слагаемых.

Нормальное расширение $A$ поля $k$ с группой Галуа $G$ является алгеброй Галуа в силу существования нормального базиса. Более общие алгебры Галуа возникают, в частности, из нормальных расширений при расширении основного поля. Точнее, пусть $A$ — нормальное расширение поля $k$ с группой $G$ и пусть $L$ — некоторое расширение поля $k$. Тогда $\bar{A} = A \otimes L$ есть алгебра над $L$ (при его естественном вложении в $\bar{A}$), операторы из $G$ естественно распространяются на $\bar{A}$ по правилу $(x \otimes c)^g = x^g \otimes c$ при $x \in A$, $c \in L$ и нормальный базис $A$ над $k$ является нормальным базисом $\bar{A}$ над $L$.

При исследовании задачи погружения оказывается целесообразным несколько ослабить требование к искомому объекту, требуя, чтобы он был не полем, но только алгеброй Галуа. Точнее, целесообразно ставить задачу о погружении данного поля $K/k$ с группой $F$ в алгебру Галуа $A$ с группой $G$, для которой $F$ является гомоморфным образом, так, чтобы $K$ совпало с алгеброй элементов $A$, инвариантных при всех автоморфизмах из ядра гомоморфизма $\varphi$: $G \to F$.

Когда решение задачи погружения является полем, будем называть такое решение собственным, а задачу погружения — разрешимой в собственном смысле.

Решение задачи погружения в алгебру Галуа допускает, аналогично решению задачи погружения в поле, широкую и узкую трактовки.

Сформулируем в виде теоремы одно свойство, вполне характеризующее алгебру Галуа, так что оно могло бы служить ее определением.

Теорема 1.4. *Пусть $A$ есть $S$-алгебра над полем $k$ и задано гомоморфное отображение группы $G$ в группу $k$-автоморфизмов алгебры $A$. Для того чтобы $A$ была алгеброй Галуа с группой $G$, необходимо и достаточно, чтобы размерность алгебры $A$ равнялась порядку группы $G$ и алгебра $G$-инвариантных элементов алгебры $A$ совпадала с полем $k$.*

Доказательство. Если $A$ — алгебра Галуа, то, очевидно, ее размерность равна порядку группы $G$. Пусть теперь $a \in A$ — образующая нормального базиса, т. е. $\{a^g\}_{g \in G}$ есть базис $A$ над $k$. Пусть $x \in A$ — инвариантный элемент, т. е. такой, что $x^g = x$ при всех $g \in G$. Выразим его через базис: $x = \sum_{g \in G} a^g x_g$ при $x_g \in k$. Тогда $x^h = \sum_g a^{gh} x_g = \sum_g a^g x_{gh^{-1}}$. Равенство $x^h = x$ равносильно системе равенств $x_g = x_{gh^{-1}}$. Так как эти равенства должны выполняться при всех $g$, $h \in G$, то $x = x_1 \sum_g a^g$, т. е. алгебра $G$-инвариантных элементов одномерна и, следовательно, совпадает с полем $k$ при его естественном вложении в $A$. Тем самым необходимость доказана.

Докажем достаточность. Пусть $S$-алгебра $A$ удовлетворяет условиям $[A : k] = (G : 1)$ и $A^G = k$.

Положим сначала, что $A$ вполне распадается: $A = \sum_{i=1}^{n} \oplus e_i k$. Здесь в силу первого условия $n = (G : 1)$ и $e_i$ — компоненты единицы в прямом разложении. Пусть $e_1 = e_1'$ — одна из них и пусть $e_1', e_2', \ldots, e_m'$ — попарно различные элементы, получающиеся из $e_1$ посредством применения автоморфизмов из $G$. Все $e_i'$ являются минимальными идемпотентами, так что они входят в множество $e_1, \ldots, e_n$. В силу ортогональности их сумма $e_1' + \ldots + e_m'$ есть идемпотент, отличный от 0, и она инвариантна при применении автоморфизмов из $G$. В силу второго условия $e_1' + \ldots + e_m' \in k$ и в силу идемпотентности $e_1' + \ldots + e_m' = 1$. Поэтому $m = n$, так что все идемпотенты, получающиеся из $e_1$ применением автоморфизмов из $G$, попарно различны и их множество совпадает с множеством $e_1, \ldots, e_n$ базисных идемпотен-

тов. Итак, в алгебре $A$ существует нормальный базис $\{e_1^g\}$, $g \in G$.

Обратимся теперь к рассмотрению общего случая. Пусть $S$-алгебра $A$ удовлетворяет условиям теоремы. Умножим ее тензорно на расширение $L$ поля $k$, содержащее поля разложения всех компонент алгебры. Тогда алгебра $\tilde{A} = A \otimes L$ вполне распадается над полем $L$ (при его естественном вложении в $A \otimes L$). Автоморфизмы из группы $G$ естественно распространяются на $\tilde{A}$ по правилу $(a \otimes y)^g = a^g \otimes y$ при $a \in A$, $y \in L$. Алгебра $G$-инвариантных элементов алгебры $\tilde{A}$ равна основному для $\tilde{A}$ полю $L$, ибо условие инвариантности формулируется в виде системы линейных однородных уравнений относительно координат в базисе $\tilde{A}$ относительно $L$, за который можно взять любой базис $A$ относительно $k$, а размерность пространства решений такой системы не изменяется при расширении поля от $k$ до $L$, т. е. остается равной 1. Размерность же $\tilde{A}$ над $L$, очевидно, равна $[A : k] = (G : 1)$. Поэтому распадающаяся над $L$ алгебра $\tilde{A}$ удовлетворяет условиям теоремы и в силу доказанного выше в ней существует $G$-нормальный базис над $L$. Поэтому представление над $L$ группы $G$ в $G$-модуле $\tilde{A}$ эквивалентно регулярному. В силу известной теоремы теории представлений [29], гласящей, что если два представления, реализующиеся в поле $k$, эквивалентны в расширении $L$ поля, то они эквивалентны и в $k$, представление группы $G$ в алгебре $A$ как в $G$-модуле эквивалентно регулярному, т. е. в алгебре $A$ существует нормальный базис для группы $G$. Теорема доказана полностью.

При доказательстве теоремы была существенно использована мультипликативная структура алгебры. Легко видеть, что $G$-модуль, размерность которого равна порядку группы $G$, и подмодуль инвариантов одномерен, не обязан быть модулем регулярного представления.

Попутно доказана теорема о существовании нормального базиса в нормальном расширении поля, ибо для нормального расширения условия теоремы выполнены.

## § 5. Стандартное задание алгебры Галуа

Пусть $G$ — конечная группа, $H$ — ее подгруппа и $M$ — пространство над полем $k$, являющееся правым $H$-модулем. Пусть $k[G]$ — групповое кольцо группы $G$, рассматриваемое как правый $G$-модуль и как левый $H$-модуль.

# ИЗ ПРЕДИСЛОВИЯ АВТОРОВ

В течение последнего десятилетия методы алгебраической топологии, интенсивно вторгаясь в область чистой алгебры, привели, можно сказать, к ряду внутренних революций в этой области математики. В настоящей книге ставится цель изложить алгебраический аспект этих методов с единой точки зрения и заложить тем самым основы вполне самостоятельной теории.

Вторжение методов алгебраической топологии в алгебру происходило в трех направлениях — через теории когомологий групп, алгебр Ли и ассоциативных алгебр. Эти три теории, несмотря на наличие далеко идущего параллелизма, долгое время развивались независимо друг от друга. Мы излагаем здесь единую теорию когомологий (а также и гомологий), включающую в себя все три упомянутые теории; каждая из этих трех теорий получается из общей теории соответствующей специализацией.

Такая унификация обладает всеми обычными преимуществами. Три различных доказательства заменяются одним. Кроме того, общая теория позволяет обнаружить некоторые не известные до сих пор взаимосвязи; при этом каждая из трех теорий обогащается двумя другими.

Эта единая теория способна охватить гораздо более широкую область, отнюдь не исчерпывающуюся указанными выше тремя случаями. Например, оказывается, что теорема Гильберта о цепях сизигий в кольце многочленов от $n$ переменных (а также и другие аналогичные теоремы) по существу является некоторой теоремой теории гомологий.

Начальным толчком, побудившим, в частности, нас к этим исследованиям, послужила следующая топологическая задача. Около тридцати лет назад Кюннет получил некоторые соотношения между группами гомологий прямого произведения и группами гомологий сомножителей в форме числовых соотношений между их числами Бетти и коэффициентами кручения. Интересовавшая нас задача состояла в том, чтобы усилить его результаты, представив их в инвариантной теоретико-групповой форме. Эта задача немедленно сводится к чисто алгебраической проблеме вычисления групп гомологий тензорного произведения двух (алгебраических) комплексов. Оказывается, что выражение для групп гомологий тензорного

произведения двух комплексов содержит не только тензорное произведение групп гомологий сомножителей, но также и некоторое другое их произведение, которое мы называем *периодическим*. Периодическое умножение является некоторой новой операцией, определяемой с помощью операции тензорного умножения. Нашей исходной точкой явилось замечание о том, что процесс построения периодического умножения из тензорного допускает обобщение, применимое к весьма широкому классу функторов. В частности, путем многократного повторения этого процесса можно из одного данного функтора получить целую последовательность новых функторов. Получающаяся при этом последовательность обладает многими формальными свойствами, известными из теории гомологий. Опишем этот процесс более подробно.

Пусть $\Lambda$ — произвольное кольцо, $A$ — некоторый $\Lambda$-модуль, на котором $\Lambda$-операторы действуют справа (т. е. правый $\Lambda$-модуль) и $C$ — некоторый левый $\Lambda$-модуль. Основной операцией является построение тензорного произведения $A \otimes_\Lambda C$, т. е. абелевой группы, порожденной парами $a \otimes c$, подчиняющимися двум дистрибутивным законам и соотношению $a\lambda \otimes c = a \otimes \lambda c$. Для многих вопросов очень важно изучить свойства этой операции по отношению к обычным алгебраическим понятиям: гомоморфизмам, подмодулям, фактормодулям и т. д.

Это изучение существенно облегчается при использовании метода диаграмм. Последовательность $\Lambda$-модулей и $\Lambda$-гомоморфизмов

$$A_m \longrightarrow A_{m+1} \longrightarrow \ldots \longrightarrow A_n, \qquad m+1 < n,$$

мы будем называть *точной последовательностью*, если для любой пары последовательных гомоморфизмов образ первого гомоморфизма совпадает с ядром второго. Мы будем, в частности, рассматривать точные последовательности вида

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0. \tag{1}$$

В такой точной последовательности модуль $A'$ можно рассматривать как подмодуль модуля $A$, а модуль $A''$ — как фактормодуль модуля $A$ по подмодулю $A'$.

Тензорно умножив каждый член некоторой точной последовательности правых $\Lambda$-модулей на фиксированный левый $\Lambda$-модуль $C$, мы, вообще говоря, не получим точной последовательности. При таком умножении точность сохраняется лишь частично. Например, в случае последовательности (1) точной всегда будет лишь последовательность

$$A' \otimes_\Lambda C \longrightarrow A \otimes_\Lambda C \longrightarrow A'' \otimes_\Lambda C \longrightarrow 0. \tag{2}$$

Функторы, обладающие этим свойством, мы будем называть *точными справа функторами*.

Ядро $K$ левого гомоморфизма последовательности (2) в общем случае отлично от нуля. Если модуль $A$ свободен, то можно показать, что это ядро зависит (с точностью до естественного изоморфизма)

только от модулей $A''$ и $C$, и мы называем его периодическим произведением $\mathrm{Tor}_1^\Lambda(A'', C)$ модулей $A''$ и $C$. В случае произвольного модуля $A$ имеет место естественный гомоморфизм

$$\mathrm{Tor}_1^\Lambda(A'', C) \longrightarrow A' \otimes_\Lambda C,$$

образ которого совпадает с ядром $K$. Продолжая это построение, мы получим бесконечную точную последовательность

$$(3) \quad \ldots \longrightarrow \mathrm{Tor}_{n+1}^\Lambda(A'', C) \longrightarrow \mathrm{Tor}_n^\Lambda(A', C) \longrightarrow \longrightarrow \mathrm{Tor}_n^\Lambda(A, C) \longrightarrow \mathrm{Tor}_n^\Lambda(A'', C) \longrightarrow \ldots,$$

заканчивающуюся справа последовательностью (2); при этом считается, что

$$(4) \qquad \mathrm{Tor}_0^\Lambda(A, C) = A \otimes_\Lambda C.$$

Гомоморфизмы точной последовательности (3), связывающие модули с индексами $n+1$ и $n$, называются *связывающими гомоморфизмами*.

При определении модуля $\mathrm{Tor}(A'', C)$ условие, что модуль $A$ свободен, излишне стеснительно. Достаточно, чтобы модуль $A$ был *проективным*, т. е. чтобы любой гомоморфизм модуля $A$ в произвольный фактормодуль $B/B'$ допускал разложение в сквозное отображение $A \to B \to B/B'$.

Описанное индуктивное построение точной последовательности (3) довольно громоздко и не имеет четко выраженной связи с теорией гомологий. Этот недостаток устраняется следующим образом. Для произвольного модуля $A$ рассматривается точная последовательность

$$\ldots \longrightarrow A_n \longrightarrow A_{n-1} \longrightarrow \ldots \longrightarrow A_1 \longrightarrow A_0 \longrightarrow A \longrightarrow 0,$$

каждый член $A_i$ $(i = 0, 1, 2, \ldots)$ которой является проективным модулем; такая последовательность называется *проективной резольвентой* модуля $A$. Тензорно умножая эту резольвенту на модуль $C$, мы получим некоторую, вообще говоря, неточную последовательность

$$(5) \qquad \ldots \longrightarrow A_n \otimes_\Lambda C \longrightarrow \ldots \longrightarrow A_0 \otimes_\Lambda C.$$

Однако эта последовательность будет комплексом (т. е. композиция любых двух последовательных гомоморфизмов этой последовательности равна нулю). Оказывается, что $n$-я группа гомологий комплекса (5) совпадает с группой $\mathrm{Tor}_n^\Lambda(A, C)$. С точки зрения этого определения функтора Tor точная последовательность (3) является гомологической последовательностью, соответствующей точной последовательности комплексов

$$0 \longrightarrow X' \otimes_\Lambda C \longrightarrow X \otimes_\Lambda C \longrightarrow X'' \otimes_\Lambda C \longrightarrow 0,$$

где $X'$, $X$, $X''$ — произвольные проективные резольвенты модулей $A'$, $A$, $A''$ соответственно.