Глава 1

Локализация.

1.1 Лекция 1.

1.1.1 История вопроса.

Изучение автоморфизмов классических групп началось работой Шрайера и Ван-дер-Вардена [15] в 1928 г. Были описаны автоморфизмы группы PSL_n ($n \geqslant 3$) над произвольным полем.

Дьедонне [10] (1951) и Рикарт [14] (1950) ввели метод инволюций, с помощью которого были описаны автоморфизмы группы GL_n ($n \geqslant 3$) над телом.

Первый шаг в построении теории автоморфизмов над кольцами, а именно, для группы GL_n ($n \geqslant 3$) над кольцом целых чисел, сделали Хуа Логен и Райнер [12] (1951), после них появилось несколько работ по коммутативным областям главных идеалов.

Методы отмечавшихся выше работ основывались в наибольшей степени на изучении инволюций в соответствующих линейных группах.

О'Мира [13] в 1976 году придумал совершенно иной (геометрический) метод, не использующий инволюций, с помощью него удалось описать автоморфизмы группы GL_n ($n \geqslant 3$) над областями целостности.

В 1982 г. В.М. Петечук [6] описал автоморфизмы групп GL, SL ($n \geqslant 4$) над произвольными коммутативными кольцами. Если $n = 3$, то автоморфизмы данных линейных групп не всегда стандартны. Они оказываются стандартными, если в кольце обратима двойка, либо рассматриваемое кольцо является областью целостности, либо это полупростое кольцо.

Изоморфизмы групп $\mathrm{GL}_n(R)$ и $\mathrm{GL}_m(S)$ над произвольными ассоциативными кольцами с обратимой двойкой при $n, m \geqslant 3$ были описаны в 1981 году И.З. Голубчиком и А.В. Михалевым [2] и независимо Е.И. Зельмановым [5]. В 1997 году И.З. Голубчик описал изоморфизмы между этими группами при $n, m \geqslant 4$, но для произвольных ассоциативных колец с единицей [3].

Основная задача данных лекций — доказательство результата В.М. Петечука [6] об автоморфизмах линейных групп над произвольными коммутативными кольцами.

1.1.2 Основные понятия и формулировки теорем.

Пусть R — коммутативное кольцо с 1, R^* — группа обратимых элементов кольца R.

Пусть V — свободный R-модуль ранга n. Общая линейная группа $\mathrm{GL}(V)$ — это группа обратимых R-линейных отображений R-модуля V в себя. Она содержится в $\mathrm{End}\, V$ — кольце всех R-линейных отображений R-модуля V в себя. Если зафиксировать базис R-модуля V, то $\mathrm{GL}(V)$ можно отождествить с $\mathrm{GL}_n(R)$ — группой обратимых матриц степени n над R. Специальная линейная группа $\mathrm{SL}_n(R)$ — это подгруппа группы GL_n, состоящая из матриц с определителем 1.

Пусть E_n — единичная матрица размера $n \times n$, E_{ij} — стандартная матричная единица, т. е. матрица, у которой на месте (i, j) стоит 1, а на остальных местах нули, $t_{ij}(\lambda) = E_n + \lambda E_{ij}$ $(i \neq j,\ \lambda \in R)$ — *элементарная трансвекция.*

Группу, порожденную всеми элементарными трансвекциями, обозначим через $E_n(R)$.

Группа $E_n(R)$ всегда обладает некоторым набором автоморфизмов, считающихся стандартными:

1) i_g — *внутренний автоморфизм*, порожденный подходящей $\mathrm{GL}_n(S)$, где S — подходящее расширение кольца R.

2) $\overline{\delta}$ — *кольцевой автоморфизм*:

$$\overline{\delta} : A = (a_{ij}) \mapsto (\delta(a_{ij})),$$

где δ — некоторый автоморфизм кольца R.

3) Λ_e — *контрградиентный* автоморфизм

$$\Lambda_e : A \mapsto (A^T)^{-1} e + A(1 - e),$$

где e — идемпотент кольца R.

Группы $\mathrm{SL}_n(R)$, $\mathrm{GL}_n(R)$, кроме автоморфизмов, перечисленных в пунктах 1)–3), обладают еще автоморфизмом $\overline{\gamma}$, который называется *гомотетией* или *центральным автоморфизмом*:

4) если γ — некоторый гомоморфизм группы $\mathrm{SL}_n(R)$, $\mathrm{GL}_n(R)$ в центр этой группы, то

$$\overline{\gamma} : A \mapsto \gamma(A)A.$$

Автоморфизм, являющийся произведением автоморфизмов 1)–4) (для группы $E_n(R)$ — произведением автоморфизмов 1)–3)), называется *стандартным.*

Основной темой этого семестра будет являться доказательство следующих двух основных теорем:

Теорема 1.1. *Любой автоморфизм группы $E_n(R)$, где R — произвольное коммутативное кольцо с единицей, $n \geqslant 4$, стандартен.*

Теорема 1.2. *Любой автоморфизм группы $\mathrm{GL}_n(R)$, $\mathrm{SL}_n(R)$, $\mathrm{GL}_n(R)'$, $\mathrm{SL}_n(R)'$, где R — произвольное коммутативное кольцо с единицей, $n \geqslant 4$, стандартен.*

Для того, чтобы доказать теорему 1.1, нам нужно будет пройти следующие три важных темы:

1) Локализации колец по простым и максимальным идеалам, их свойства; вложение произвольного коммутативного кольца в прямое произведение своих локализаций по максимальным идеалам.

2) Описание изоморфизмов между группами SL_n и PSL_n над полями при $n \geqslant 4$.

3) Описание подгрупп в группе $\mathrm{GL}_n(R)$, нормализуемых группой $E_n(R)$.

Мы начнем с локализации. Более подробное изложение (с бóльшим числом упражнений) можно найти в книге [1].

1.1.3 Кольца частных по мультипликативным системам.

Процедура, с помощью которой по кольцу $\mathbb{Z}$ строится поле $\mathbb{Q}$ (с вложением $\mathbb{Z}$ в $\mathbb{Q}$) естественным образом распространяется на любое коммутативное кольцо без делителей нуля A. В результате получается *поле частных* кольца A. Конструкция состоит в том, чтобы рассматривать упорядоченные пары (дроби) $\frac{a}{s}$, где $a, s \in A$, $s \neq 0$, считая две пары $\frac{a}{s}$ и $\frac{b}{t}$ эквивалентными, если $at - bs = 0$.

Однако такая конструкция работает только если у кольца A нет делителей нуля, так как в ином случае не получается транзитивность отношения:

$$\frac{a}{s} \sim \frac{b}{t} \text{ и } \frac{b}{t} \sim \frac{c}{u} \Longleftrightarrow at = bs \text{ и } bu = tc \Longrightarrow (au - sc)bt = 0,$$

что не дает $au - sc = 0$ в общем случае.

Однако конструкция обобщается следующим образом.

Определение 1.1. Пусть A — коммутативное кольцо. Подмножество $S \subset A$ называется *мультипликативно замкнутым* подмножеством в A, если $1 \in S$ и S замкнуто относительно умножения.

Введем отношение эквивалентности $\sim$ на множестве пар $A \times S$ следующим образом:

$$\frac{a}{s} \sim \frac{b}{t} \Longleftrightarrow \exists u \in S : \ (at - bs)u = 0.$$

Это отношения очевидно является рефлексивным и симметричным. Чтобы показать транзитивность, предположим

$$\frac{a}{s} \sim \frac{b}{t} \text{ и } \frac{b}{t} \sim \frac{c}{u},$$

откуда

$$\exists v, w \in S\, (at - bs)v = (bu - tc)w = 0, \text{ т. е. } \begin{cases} atv = bsv, \\ tcw = buw \end{cases}$$

Домножая первое равенство на uw, а второе — на sv, получим, что правые части равенств равны. Из этого следует, что равны и левые, т. е.

$$autvw = cstvw \Longrightarrow (au - cs)tvw = 0.$$

Так как $tvw \in S$, то $\frac{a}{s} \sim \frac{c}{u}$, транзитивность доказана.

Таким образом, мы получили отношение эквивалентности. Теперь через $\frac{a}{s}$ мы будем означать весь класс эквивалентности для пары (a, s), а через $S^{-1}R$ — множество всех классов эквивалентности. Введем на $S^{-1}R$ структуру кольца, положив

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Для доказательства корректности этого определения достаточно показать, что результаты сложения и умножения не зависят от выбора представителей (оставим это в качестве упражнения).

Легко увидеть, что полученное множество с операциями сложения и умножения является коммутативным кольцом с единицей. Также у нас имеется кольцевой гомоморфизм $f : A \to S^{-1}A$, определенный как $f(x) = \frac{x}{1}$. В общем случае гомоморфизм f не является инъективным.

Определение 1.2. Кольцо $S^{-1}A$ называется *кольцом частных для A по отношению к S.*

Имеет место универсальное свойство:

Предложение 1.1. *Пусть $g : A \to B$ кольцевой гомоморфизм такой, что $g(s)$ обратим в кольце B для любого $s \in S$. Тогда существует и единственен кольцевой гомоморфизм $h : S^{-1}A \to B$ такой, что $g = h \circ f$.*

Доказательство. 1) *Единственность.* Если h удовлетворяет условиям, то

$$h\left(\frac{a}{1}\right) = hf(a) = g(a) \text{ для всех } a \in A.$$

Следовательно, если $s \in S$, то

$$h\left(\frac{1}{s}\right) = h\left(\left(\frac{s}{1}\right)^{-1}\right) = h\left(\frac{s}{1}\right)^{-1} = g(s)^{-1} \Longrightarrow h\left(\frac{a}{s}\right) = h\left(\frac{a}{1}\right) h\left(\frac{1}{s}\right) = g(a)g(s)^{-1},$$

откуда следует, что отображение h однозначно определено.

2) *Существование.* Положим

$$h\left(\frac{a}{s}\right) := g(a)g(s)^{-1}.$$

Тогда понятно, что h — кольцевой гомоморфизм, если доказать, что h корректно определено.

Предположим, что $\frac{a}{s} = \frac{a'}{s'}$, тогда существует $t \in S$ такое, что $(as' - a's)t = 0$, откуда

$$(g(a)g(s') - g(a')g(s))g(t) = 0.$$

Так как $g(t)$ обратим, то

$$g(a)g(s)^{-1} = g(a')g(s')^{-1}.$$

□

Кольцо $S^{-1}A$ и гомоморфизм $f : A \to S^{-1}A$ обладают следующими очевидными свойствами:

1) Для любого $s \in S$ элемент $f(s)$ обратим в $S^{-1}A$.

2) Если $f(a) = 0$, то $as = 0$ для некоторого $s \in S$.

3) Любой элемент из $S^{-1}A$ имеет вид $f(a)f(s)^{-1}$ для некоторого $a \in A$ и некоторого $s \in S$.

Обратно, эти три условия определяют кольцо $S^{-1}A$ с точностью до изоморфизма. Именно, имеет место

Следствие 1.1. *Если $g : A \to B$ — кольцевой гомоморфизм такой, что*

(1) *для любого $s \in S$ элемент $g(s)$ обратим в B;*

(2) *если $g(a) = 0$, то $as = 0$ для некоторого $s \in S$;*

(3) *любой элемент из B имеет вид $g(a)g(s)^{-1}$ для некоторого $a \in A$ и некоторого $s \in S$;*

то существует и единственен изоморфизм $h : S^{-1}A \to B$ такой, что $g = h \circ f$.

Доказательство. По предложению 1.1 нам надо показать, что гомоморфизм $h : S^{-1}A \to B$, определенный формулой $h(\frac{a}{s}) = g(a)g(s)^{-1}$, является изоморфизмом.

По свойству (3) он сюръективен. Чтобы доказать инъективность h, посмотрим на его ядро: если $h(\frac{a}{s}) = 0$, то $g(a) = 0$, по свойству (2) $at = 0$ для некоторого $t \in S$, откуда $\frac{a}{s} \sim \frac{0}{1}$, $\frac{a}{s} = 0$ в $S^{-1}A$. □

1.1.4 Важные примеры колец частных.

Пример 1.1. Пусть $\mathfrak{p}$ — простой идеал в A. Тогда множество $S = A \setminus \mathfrak{p}$ мультипликативно замкнуто (это равносильно определению простого идеала). Будем обозначать кольцо частных $S^{-1}A$ в этом случае через $A_{\mathfrak{p}}$. Элементы $\frac{a}{s}$, $a \in \mathfrak{p}$. образуют идеал $\mathfrak{M}$ в $A_{\mathfrak{p}}$. Если $\frac{b}{t} \notin \mathfrak{M}$, то $b \in S$, поэтому $\frac{b}{t}$ обратим в $A_{\mathfrak{p}}$. Значит, идеал $\mathfrak{M}$ состоит из всех необратимых элементов кольца $A_{\mathfrak{p}}$, т. е. $\mathfrak{M}$ — наибольший идеал этого кольца, а $A_{\mathfrak{p}}$ — локальное кольцо.

Процесс перехода от кольца A к кольцу $A_{\mathfrak{p}}$ называется *локализацией по* $\mathfrak{p}$.

Пример 1.2. Кольцо $S^{-1}A$ является нулевым тогда и только тогда, когда $0 \in S$.

Пример 1.3. Пусть $f \in A$ и $S = \{f^n\}_{n \geqslant 0}$. Мы обозначаем кольцо $S^{-1}A$ через A_f в этом случае.

Пример 1.4. Пусть $\mathfrak{A}$ — идеал кольца A, $S = 1 + \mathfrak{A} = \{1 + x \mid x \in \mathfrak{A}\}$. Ясно, что множество S мультипликативно замкнуто.

1.1.5 Перенесение конструкции кольца частных на модули.

Конструкцию $S^{-1}A$ можно перенести и на A-модуль M.

Определим отношение $\sim$ на $M \times S$ следующим образом:

$$(m, s) \sim (m', s') \Longleftrightarrow \exists t \in S : t(sm' - s'm) = 0.$$

Как и выше, легко доказать, что это отношение эквивалентности. Пусть m/s обозначает класс эквивалентности пары (m, s), $S^{-1}M$ — множество всех таких дробей — превращается в модуль $S^{-1}M$ с помощью естественных операций сложения и скалярного умножения. Как и в примере 1.1, мы будем писать $M_{\mathfrak{p}}$ вместо $S^{-1}M$ для $S = A \setminus \mathfrak{p}$, где $\mathfrak{p}$ — простой идеал кольца A.

1.1.6 Упражнения.

1. Докажите, что при $n \geqslant 3$ у группы $E_n(R)$ не может быть нетривиальных центральных автоморфизмов.

2. Докажите, что если коммутативное кольцо R содержит обратимый элемент α такой, что $\alpha^2 - 1$ также обратим, то у группы $E_2(R)$ не может быть нетривиальных центральных автоморфизмов. Верно ли это для произвольного коммутативного кольца R?

3. Приведите пример коммутативного кольца R, для которого:
a) группы $\mathrm{SL}_2(R)$ и $\mathrm{SL}_2(R)'$ не совпадают;
b) группы $\mathrm{GL}_2(R)'$ и $\mathrm{SL}_2(R)$ не совпадают;
c) группы $\mathrm{SL}_n(R)$ и $\mathrm{SL}_n(R)'$, $n \geqslant 3$, не совпадают;
d) группы $\mathrm{GL}_n(R)'$ и $\mathrm{SL}_n(R)$, $n \geqslant 3$, не совпадают.

4. Приведите пример коммутативного кольца R и нестандартного автоморфизма группы $\mathrm{SL}_2(R)$.

5. Докажите, что любой максимальный идеал является простым.

6. Проверьте, что операции сложения и умножения в кольце частных $S^{-1}A$ заданы корректно.

7. Пусть $A = \mathbb{Z}$, $\mathfrak{p} = p\mathbb{Z}$ (p — простое). Чему тогда изоморфно кольцо $A_{\mathfrak{p}}$? Если $f \in \mathbb{Z}$, $f \neq 0$, то чему изоморфно кольцо A_f (см. пример 1.3)?

8. Пусть S — мультипликативно замкнутое подмножество кольца A, M — конечно порожденный A-модуль. Докажите, что $S^{-1}M = 0$ тогда и только тогда, когда существует $s \in S$ такое, что $sM = 0$.

9. Пусть A — коммутативное кольцо, S и T — его мультипликативно замкнутые подмножества, U — это образ множества T в кольце $S^{-1}A$. Докажите, что кольца $(ST)^{-1}A$ и $U^{-1}(S^{-1}A)$ изоморфны.

1.2 Лекция 2.

Пусть $u : M \to N$ — гомоморфизм A-модулей. Тогда появляется возможность определить гомоморфизм $S^{-1}A$-модулей

$$S^{-1}u : S^{-1}M \to S^{-1}N$$

как

$$\frac{m}{s} \overset{S^{-1}}{\mapsto} \frac{u(m)}{s}.$$

Тогда $S^{-1}(v \circ u) = (S^{-1}v) \circ (S^{-1}u)$.

Предложение 1.2. *Операция S^{-1} точна, т. е. если последовательность*

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

точна в M, то последовательность

$$S^{-1}M' \overset{S^{-1}f}{\to} S^{-1}M \overset{S^{-1}g}{\to} S^{-1}M''$$

точна в $S^{-1}M$.

Доказательство. Так как $g \circ f = 0$, то $S^{-1}g \circ S^{-1}f = S^{-1}0 = 0$, откуда следует, что $Im(S^{-1}f) \subseteq ker\,(S^{-1}g)$.

Для доказательства обратного включения положим $m/s \in ker\,(S^{-1}g)$, тогда $\frac{g(m)}{s} = 0$ в $S^{-1}M''$, т. е. существует $t \in S$ такое, что $tg(m) = 0$ в M''. Однако $tg(m) = g(tm)$, поэтому $tm \in ker\,(g) = Im\,(f)$, поэтому $tm = f(m')$ для некоторого $m' \in M'$. Значит, в модуле $S^{-1}M$ имеет место

$$\frac{m}{s} = \frac{f(m')}{st} = (S^{-1}f)\left(\frac{m'}{st}\right) \in Im\,(S^{-1}f).$$

Следовательно, $ker\,(S^{-1}g) \subseteq Im(S^{-1}f)$, последовательность точна. □

В частности, из предложения 1.2 следует, что если M' — подмодуль M, то отображение $S^{-1}M' \to S^{-1}M$ инъективно, поэтому модуль $S^{-1}M'$ можно рассматривать как подмодуль модуля $S^{-1}M$.

Следствие 1.1. *Операция взятия частного коммутирует с операциями конечных сумм, конечных пересечений, факторов. Точнее, если N, P — подмодули A-модуля M, то*

(1) $S^{-1}(N + P) = S^{-1}N + S^{-1}P$;
(2) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$;
(3) *$S^{-1}A$-модули $S^{-1}M/S^{-1}(N)$ и $S^{-1}(M/N)$ изоморфны.*

Доказательство. Утверждение (1) следует из определений, утверждение (2) легко проверяется: если

$$\frac{y}{s} = \frac{z}{t} \quad (y \in N, z \in P, s, t \in S),$$

то $u(ty - sz) = 0$ для некоторого $u \in S$, откуда следует $w = uty = usz \in N \cap P$, поэтому

$$\frac{y}{s} = \frac{w}{stu} \in S^{-1}(N \cap P).$$

Значит, $S^{-1}N \cap S^{-1}P \subseteq S^{-1}(N \cap P)$, а обратное включение очевидно.

(3) Нужно применить S^{-1} к точной последовательности

$$0 \to N \to M \to M/N \to 0.$$

□

Теперь нам понадобится напоминание о конструкции тензорного произведения модулей. Так как эту конструкцию мы подробно изучали в прошлом семестре, то здесь будут приведены только основные формулировки. Подробные доказательства утверждений о тензорном проихведении можно найти в книге [1].

Пусть M, N,P — три A-модуля. Отображение $f : M \times N \to P$ называется A-билинейным, если для любого $x \in M$ отображение $y \mapsto f(x, y)$ из модуля N в модуль P A-линейно, а для любого $y \in N$ отображение $x \mapsto f(x, y)$ из M в P также A-линейно.

Построим A-модуль T, называемый *тензорным произведением* модулей M и N, со свойством, что A-билинейные отображения из $M \times N$ в P будут находиться в естественном взаимно-однозначном соответствии с линейными отображениями $T \to P$, для всех A-модулей P. Более точно,

Предложение 1.3. *Пусть M, N — A-модули. Тогда существует пара (T, g), состоящая из A-модуля T и билинейного отображения $g : M \times N \to T$ такого, что:*

для любого A-модуля P и любого A-билинейного отображения $f : M \times N \to P$ существует и единственно A-линейное отображение $f' : T \to P$ такое, что $f = f' \circ g$.

Кроме того, если (T, g) и (T', g') — две пары с таким свойством, то существует единственный изоморфизм $j : T \to T'$ такой, что $j \circ g = g'$.

Мы обозначаем построенный модуль T через $M \otimes N$. Образы пар $(x, y) \in M \times N$ при естественном отображении из $M \times N$ в $M \otimes N$ обозначаются через $x \otimes y$; модуль $M \times N$ порождается элементами такого вида (любой его элемент можно представить в виде $\sum_{i=1}^{n} x_i \otimes y_i$, $x_i \in M$, $y_i \in N$); также выполняются следующие свойства:

$$\begin{aligned}(x + x') \otimes y &= x \otimes y + x' \otimes y;\\ x \otimes (y + y') &= x \otimes y + x \otimes y';\\ (ax) \otimes y = x \otimes (ay) &= a(x \otimes y).\end{aligned}$$

Вернемся теперь к кольцам и модулям частных.

Предложение 1.4. *Пусть M — A-модуль. Тогда $S^{-1}A$-модули $S^{-1}M$ и $S^{-1}A \otimes_A M$ изоморфны. Более точно, существует и единственен изоморфизм*

$$f : S^{-1}A \otimes_A M \to S^{-1}M,$$

для которого

$$f\left(\frac{a}{s} \otimes m\right) = \frac{am}{s} \text{ для всех } a \in A, m \in M, s \in S. \qquad (*)$$

Доказательство. Отображение $S^{-1}A \times M \to S^{-1}M$, определенное формулой

$$\left(\frac{a}{s}, m\right) \mapsto \frac{am}{s},$$

A-билинейно, поэтому по универсальному свойству тензорного произведения индуцирует A-гомоморфизм $f : S^{-1}A \otimes_A M \to S^{-1}M$, удовлетворяющий равенству (*).

Благодаря этому равенству видно, что гомоморфизм f сюръективен. Докажем его инъективность.

Пусть $\sum\limits_i \left(\frac{a_i}{s_i}\right) \otimes m_i$ — произвольный элемент из $S^{-1}A \otimes M$. Если $s = \prod\limits_i s_i \in S$, $t_i = \prod\limits_{j \neq i} s_j$, то имеем

$$\sum_i \frac{a_i}{s_i} \otimes m_i = \sum_i \frac{a_i t_i}{s} \otimes m_i = \sum_i \frac{1}{s} \otimes a_i t_i m_i = \frac{1}{s} \otimes \sum_i a_i t_i m_i,$$

т. е. любой элемент из $S^{-1}A \otimes M$ имеет вид $\frac{1}{s} \otimes m$.

Предположим, что $f(\frac{1}{s} \otimes m) = 0$. Тогда $\frac{m}{s} = 0$, откуда $tm = 0$ для некоторого $t \in S$, поэтому

$$\frac{1}{s} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0.$$

Таким образом f инъективно, т. е. является изоморфизмом. □

Теперь вспомним определения и свойства плоского модуля (подробности снова см. в [1]).

A-Модуль N называется *плоским*, если тензорное умножение любой точной последовательности на этот модуль оставляет эту последовательность точной. Более подробные варианты определения дает следующее предложение:

Предложение 1.5. *Для A-модуля N следующие условия эквивалентны*:

(1) *модуль N — плоский*;

(2) *если $0 \to M' \to M \to M'' \to 0$ — любая точная последовательность A-модулей, то последовательность*

$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

точна;

(3) *если гомоморфизм $f : M \to M'$ инъективен, то гомоморфизм $f \otimes 1 : M \otimes N \to M' \otimes N$ инъективен*;

(4) *если гомоморфизм $f : M \to M'$ инъективен, модули M, M' конечно порождены, то гомоморфизм $f \otimes 1 : M \otimes N \to M' \otimes N$ инъективен.*

Следствие 1.2. *Модуль $S^{-1}A$ является плоским A-модулем.*

Доказательство. Это прямое следствие из предложений 1.2 и 1.4. □

Предложение 1.6. *Если M и N — A-модули, то существует единственный изоморфизм $S^{-1}A$-модулей*

$$f : S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$$

такой, что

$$f\left(\frac{m}{s} \otimes \frac{n}{t}\right) = \frac{m \otimes n}{st}.$$

В частности, если $\mathfrak{p}$ — произвольный простой идеал, то

$$M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \cong (M \otimes_A N)_{\mathfrak{p}}$$

как $A_{\mathfrak{p}}$-модули.

Доказательство. Прямая проверка. □

1.2.1 Локальные свойства.

Свойство $\mathbf{P}$ кольца A (или A-модуля M) называется *локальным*, если верно следующее:

A (или M) удовлетворяет $\mathbf{P} \iff$

$\iff A_{\mathfrak{p}}$ (или $M_{\mathfrak{p}}$) удовлетворяет $\mathbf{P}$ для любого простого идеала $\mathfrak{p}$.

Предложение 1.7. *Пусть M — A-модуль. Тогда следующие условия эквивалентны*:
(1) $M = 0$;
(2) $M_{\mathfrak{p}} = 0$ *для любого простого идеала* $\mathfrak{p}$ *из* A;
(3) $M_{\mathfrak{m}} = 0$ *для любого максимального идеала* $\mathfrak{m}$ *из* A.

Доказательство. Ясно, что (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3).

Предположим, что выполнено условие (3), но при этом $M \neq 0$. Пусть $0 \neq x \in M$, пусть $\mathfrak{a} = \operatorname{Ann} x$. Тогда $\mathfrak{a}$ — идеал в кольце A, не содержащий единицы. Значит, $\mathfrak{a}$ содержится в некотором максимальном идеале $\mathfrak{m}$.

Рассмотрим $\frac{x}{1} \in M_{\mathfrak{m}}$. Так как $M_{\mathfrak{m}} = 0$, то $\frac{x}{1} = 0$, т. е. x обнуляется некоторым элементом из $A \setminus \mathfrak{m}$, что невозможно, так как $\operatorname{Ann} x \subseteq \mathfrak{m}$. □

Предложение 1.8. *Пусть $\varphi : M \to N$ — гомоморфизм A-модулей. Тогда следующие условия эквивалентны*:
(1) *гомоморфизм φ инъективен*;
(2) *гомоморфизм $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ инъективен для любого простого идеала $\mathfrak{p}$*;
(3) *гомоморфизм $\varphi_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ инъективен для любого максимального идеала $\mathfrak{m}$.*
Слово "инъективен" можно заменить на слово "сюръективен".

Доказательство. (1) $\Longrightarrow$ (2). Так как гомоморфизм φ инъективен, то последовательность $0 \to M \to N$ точна. Значит, последовательность $0 \to M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ точна, т. е. гомоморфизм $\varphi_{\mathfrak{p}}$ инъективен.

(2) $\Longrightarrow$ (3) очевидно.

(3) $\Longrightarrow$ (1). Пусть $M' = \ker \varphi$, тогда последовательность $0 \to M' \to M \to N$ точна, поэтому последовательность $0 \to M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ точна для любого максимального идеала $\mathfrak{m}$. Следовательно, $M'_{\mathfrak{m}} \cong \ker \varphi_{\mathfrak{m}} = 0$, так как $\varphi_{\mathfrak{m}}$ инъективен. Значит, $M' = 0$ по предложению 1.7. Таким образом, гомоморфизм φ инъективен. □

Свойство модуля быть плоским является локальным свойством:

Предложение 1.9. *Для любого A-модуля M следующие утверждения эквивалентны*:
(1) M — *плоский модуль*;
(2) $M_{\mathfrak{p}}$ — *плоский $A_{\mathfrak{p}}$-модуль для любого простого идеала $\mathfrak{p}$ кольца A*;
(3) $M_{\mathfrak{m}}$ — *плоский $A_{\mathfrak{m}}$-модуль для любого максимального идеала $\mathfrak{m}$ кольца A.*

Доказательство. (1) $\Longrightarrow$ (2) по предложению 1.2.

(2) $\Longrightarrow$ (3) очевидно.

(3) $\Longrightarrow$ (1). Если $N \to P$ — гомоморфизм A-модулей, $\mathfrak{m}$ — любой максимальный идеал в A, то

$$\begin{aligned}\text{Гомоморфизм } N \to P \text{ инъективен} &\Longrightarrow \text{гомоморфизм } N_{\mathfrak{m}} \to P_{\mathfrak{m}} \text{ инъективен} \Longrightarrow \\ \Longrightarrow \text{гомоморфизм } N_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \to P_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} &\text{ инъективен по свойству плоского модуля} \Longrightarrow \\ \Longrightarrow \text{гомоморфизм } (N \otimes_A M)_{\mathfrak{m}} \to (P \otimes_A M)_{\mathfrak{m}} &\text{ инъективен} \Longrightarrow \\ \Longrightarrow \text{гомоморфизм } N \otimes_A M \to (P \otimes_A M) &\text{ инъективен по предложению 1.8.}\end{aligned}$$

Теперь утверждение следует из предложения 1.5. □

1.2.2 Вложение кольца в произведение его локализаций.

Предложение 1.10. *Любое коммутативное кольцо A с единицей можно естественно вложить в декартово произведение всех его локализаций по максимальным идеалам*

$$S = \prod_{\mathfrak{m} \text{ — макс. идеал } A} A_{\mathfrak{m}}$$

с помощью диагонального отображения, сопоставляющего каждому $a \in A$ элемент

$$\prod_{\mathfrak{m}} \left(\frac{a}{1}\right)_{\mathfrak{m}}$$

кольца S.

Доказательство. Очевидно, что данное отображение является гомоморфизмом $A \to S$. Покажем, что его ядро нулевое. Если образ элемента a является нулевым в локализации по каждому максимальному идеалу, то рассмотрим максимальный идеал $\mathfrak{m}$, содержащий аннулятор элемента a. Должно существовать $t \in A \setminus \mathfrak{m}$ такое, что $ta = 0$, что невозможно. □

1.2.3 Упражнения.

1. Коммутирует ли операция взятия частного с операциями взятия
а) бесконечных сумм;
б) бесконечных пересечений?

2. Пусть A — коммутативное кольцо. Предположим, что для любого простого идеала $\mathfrak{p}$ локальное кольцо $A_{\mathfrak{p}}$ не содержит ни одного ненулевого нильпотентного элемента. Докажите, что тогда и кольцо A не содержит ненулевых нильпотентных элементов.

3. Пусть A — коммутативное кольцо. Предположим, что для любого простого идеала $\mathfrak{p}$ локальное кольцо $A_{\mathfrak{p}}$ является областью целостности. Будет ли тогда кольцо A являться областью целостности?

4. Мультипликативно замкнутое подмножество S кольца A назовем *насыщенным*, если

$$xy \in S \Longleftrightarrow x \in S \text{ и } y \in S.$$

Докажите, что множество S насыщено тогда и только тогда, когда множество $A \setminus S$ является объединением простых идеалов.

5. Пусть M — A-модуль, $\mathfrak{a}$ — идеал в кольце A. Предположим, что $M_{\mathfrak{m}} = 0$ Для всех максимальных идеалов $\mathfrak{m}$, содержащих идеал $\mathfrak{a}$. Докажите, что тогда $M = \mathfrak{a}M$.

Глава 2

Изоморфизмы линейных групп над полями.

2.1 Лекция 3.

2.1.1 Постановка задачи.

Теперь мы хотим описать все изоморфизмы между группами $\mathrm{PSL}_n(K)$ и $\mathrm{PSL}_m(L)$ над полями K и L при $n, m \geqslant 3$. Именно,

Теорема 2.1. *Если группы* $\mathrm{PSL}_n(K)$ *и* $\mathrm{PSL}_m(L)$ *над полями* K *и* L *при* $n, m \geqslant 3$ *изоморфны, то обязательно* $n = m$, $K \cong L$, *а любой изоморфизм* Φ *между этими группами имеет вид либо*

$$\Phi = \bar{i}_g \circ \overline{\delta},$$

либо

$$\Phi = \bar{i}_g \circ \overline{\Lambda} \circ \overline{\delta},$$

где $\delta : K \to L$ *— изоморфизм колец* K *и* L, $\overline{\Lambda}$ *— контрградиентный автоморфизм группы* $\mathrm{PSL}_m(L)$, *индуцированный контрградиентным автоморфизмом группы* $\mathrm{SL}_m(L)$, $g \in \mathrm{GL}_m(L)$.

Однако нам понадобится и теорема, описывающая изоморфизмы между группами $\mathrm{PSL}_2(K)$ и $\mathrm{PSL}_2(L)$:

Теорема 2.2. *Если группы* $\mathrm{PSL}_2(K)$ *и* $\mathrm{PSL}_2(L)$ *над полями* K *и* L *изоморфны, то обязательно* $K \cong L$, *кроме случая* $K, L = \mathbb{F}_4, \mathbb{F}_5$, *а любой изоморфизм* Φ *между этими группами имеет вид* $\bar{i}_g \circ \overline{\delta}$, *где* $\delta : K \to L$ *— изоморфизм колец* K *и* L, $g \in \mathrm{GL}_2(L)$.

Если одно из полей состоит из четырех элементов, а другое — из пяти, то существует изоморфизм между $\mathrm{PSL}_2(K)$ *и* $\mathrm{PSL}_2(L)$.

Прежде чем доказывать сформулированные теоремы, докажем несколько полезных предложений о линейных и проективных линейных группах.

2.1.2 Простота групп $\mathrm{PSL}_n(K)$ над полями.

Определение 2.1. Группа G называется *простой*, если она неабелева и не содержит нормальных подгрупп, отличных от единичной и от нее самой.

Предложение 2.1. *Группа* $\mathrm{PSL}_2(K)$ *проста для любого поля* K*, содержащего больше трех элементов.*

Доказательство. Переформулируем это предложение на языке подгрупп группы $\mathrm{SL}_2(K)$, а не $\mathrm{PSL}_2(K)$. Простота группы $\mathrm{PSL}_2(K)$ означает, что группе $\mathrm{SL}_2(K)$ не ни одной собственной подгруппы, содержащей центр этой группы, но не совпадающей с ним.

Предположим, что группа $\mathrm{SL}_2(K)$ не удовлетворяет этому условию. Тогда она содержит нормальную подгруппу N, в которой есть хотя бы одна матрица, не являющаяся скалярной. Пусть это матрица

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Если эта матрица диагональна ($c = b = 0$), то $a \neq d$, $d = 1/a$. Ее коммутатор с матрицей $B = E + \lambda E_{1,2}$ равен

$$[A, B] = ABA^{-1}B^{-1} = \begin{pmatrix} 1 & (a^2 - 1)\lambda \\ 0 & 1 \end{pmatrix} \in N.$$

Таким образом, так как $a^2 \neq 1$, то любая матрица вида $E + \lambda E_{1,2}$ содержится в подгруппе N, то же можно сказать и о матрицах вида $E + \lambda E_{2,1}$. Над полем полученные элементарные матрицы порождают всю группу $\mathrm{SL}_2(K)$ (см. упражнение 1), что нам и требовалось.

Теперь предположим, что матрица A имела вид $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, $a \neq d$.

Тогда

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b + \alpha(d - a) \\ 0 & d \end{pmatrix} \in N.$$

Так как $d - a \neq 0$, то мы можем выбрать $\alpha = -b/(d - a)$ и таким образом прийти к предыдущему случаю.

Если матрица A имеет вид $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$, то $a = \pm 1$. Без ограничения общности предположим, что $a = 1$.

Заметим, что если сопрячь матрицу A диагональной матрицей $\mathrm{diag}\,[\alpha, 1/\alpha]$, то получится матрица $E + \alpha^2 b E_{1,2}$. Если матрицы такого вида и обратные к ним перемножать между собой, то будут получаться произвольные матрицы вида $E + (\pm\alpha_1^2 \pm \alpha_2^2 \pm \cdots \pm \alpha_k^2) b E_{1,2}$. Если характеристика поля K не равна двум, то любой элемент поля можно получить в виде сумм и разностей квадратов элементов этого поля:

$$a = \left(a + \frac{1}{2}\right)^2 - a^2 - \left(\frac{1}{2}\right)^2,$$

поэтому в группе N содержится любая матрица вида $E + \lambda E_{1,2}$, что нам и требуется.

Если характеристика поля K равна двум, то так как в поле больше двух элементов (по условию), то мы можем выбрать в нем некоторое $\alpha \in K^*$ такое, что $\alpha^2 \neq 1$. Тогда аналогично предыдущему вместе с матрицей $A = E + bE_{1,2}$ в группе N содержится и матрица $A' = E + \alpha^2 bE_{1,2}$, а также матрицы $B = E - 1/bE_{2,1}$ и $B' = E - 1/(\alpha^2 b)E_{2,1}$.

Матрицы ABA и $A'B'A'$, также содержащиеся в подгруппе N, имеют вид

$$\begin{pmatrix} 0 & b \\ -1/b & 0 \end{pmatrix} \text{ и } \begin{pmatrix} 0 & \alpha^2 b \\ 1/(\alpha^2 b) & 0 \end{pmatrix},$$

соответственно. Их произведение — это диагональная матрица вида $\operatorname{diag}[\alpha^2, 1/\alpha^2]$. Так как $\alpha \neq 1$, то и $\alpha^2 \neq 1$ (в поле характеристики два из каждого элемента можно извлечь не более одного квадратного корня (см. упражнение 2). Значит, мы снова пришли к исходной ситуации с диагональной матрицей не из центра.

Осталось предположить, что изначальная матрица $A \in N$ имеет вид

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad c \neq 0.$$

Сопрягая матрицу A матрицей $E + \frac{a}{c}E_{1,2}$, мы получим матрицу

$$A' = \begin{pmatrix} 0 & b' \\ -1/b' & d' \end{pmatrix} \in N.$$

Пусть $d' \neq 0$. Тогда рассмотрим коммутатор матрицы A' с диагональной матрицей $\operatorname{diag}[\alpha, 1/\alpha]$, где $\alpha^2 \neq 1$. Этот коммутатор лежит в подгруппе N и равен

$$\begin{pmatrix} \alpha^2 & 0 \\ \frac{d'}{b'}\left(1 - \frac{1}{\alpha^2}\right) & \frac{1}{\alpha^2} \end{pmatrix},$$

что приводит нас к одному из рассмотренных случаев.

Если $d' = 0$, то мы имеем матрицу

$$A' = \begin{pmatrix} 0 & b' \\ -1/b' & 0 \end{pmatrix},$$

а у изначальной матрицы A совпадали a и d. Рассмотрим тогда коммутатор матрицы A' с матрицей $E + E_{1,2}$, он равен

$$\begin{pmatrix} 1 & -b'^2 \\ -1 & 1 + b'^2 \end{pmatrix},$$

тогда можно будет от этого коммутатора прийти к матрице с $d' \neq 0$.

Доказательство закончено. □

Предложение 2.2. *При $n \geqslant 3$ группа $\mathrm{PSL}_n(K)$ проста для любого поля K.*

Доказательство. Как и в предыдущем предложении, нам требуется рассмотреть произвольную нескалярную матрицу из некоторой нормальной подгруппы N и доказать, что N совпадает со всей $\mathrm{SL}_n(K)$.

Для начала пусть эта матрица (снова обозначим ее через A) диагональна. Тогда на ее диагонали есть два различных элемента. Меняя местами подходящие векторы базиса, мы можем добиться того, что эти два различных элемента будут стоять на первом и втором местах. Таким образом, можно считать, что матрица A имеет вид $\mathrm{diag}\,[a_1, a_2, \ldots, a_n]$, $a_1 \neq a_2$. Рассмотрим коммутатор матрицы A и матрицы $E + \alpha E_{1,2}$, он будет равен $E + (a_1/a_2 - 1)\alpha E_{1,2}$. Таким образом, все $E + \beta E_{1,2}$, $\beta \in K$, содержатся в подгруппе N, а значит, там содержатся и все $E + \beta E_{ij}$, $\beta \in K$, $i \neq j$. Следовательно, $N = \mathrm{SL}_n(K)$.

Теперь предположим, что матрица $A = (a_{i,j})$ не является диагональной. Тогда существуют $i \neq j$ такие, что $a_{i,j} \neq 0$. Так как меняя векторы базиса, мы можем перевести индекс j в единицу, а индекс i — в двойку, то будем считать, что $a_{2,1} \neq 0$.

Заметим, что сопряжение с помощью матрицы $E + \alpha E_{i,j}$ делает с матрицей следующее: к ее строке с номером j прибавляется строка с номером i, умноженная на α, а из ее столбца с номером i вычитается столбец с номером j, умноженный на α.

Так как $a_{2,1} \neq 0$, то мы можем вычесть из каждой строки вторую строку, умноженную на подходящий коэффициент, при этом ко второму столбцу будут прибавляться остальные столбцы, умноженные на соответствующие коэффициенты. Таким образом, от матрицы $A \in N$ мы перейдем к матрице $A' \in N$, у которой в первом столбце ненулевым элементом является только $a_{2,1}$ (после подходящего сопряжения диагональной матрицей можно считать, что $a_{2,1} = 1$). Для удобства обозначений будем по-прежнему обозначать элементы матрицы A' через $a_{i,j}$.

Теперь вычтем из второго столбца первый и прибавим к первой строке вторую, получим матрицу $A'' \in N$, имеющую вид

$$A'' = \begin{pmatrix} 1 & a_{1,2} + a_{2,2} - 1 & a_{1,3} + a_{2,3} & \ldots & a_{1,n} + a_{2,n} \\ 1 & a_{2,2} - 1 & a_{2,3} & \ldots & a_{2,n} \\ 0 & a_{3,2} & a_{3,3} & \ldots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n,2} & a_{n,3} & \ldots & a_{n,n} \end{pmatrix}.$$

Домножим матрицу A'' справа на матрицу $B = {A'}^{-1} = (b_{i,j})$ (заметим, что $b_{2,2} = 0$): так как все строки матрицы A'', начиная с третьей, совпадают с теми же строками матрицы A', то при умножении A'' на B полученная матрица будет иметь строки с номерами $3, \ldots, n$, совпадающие с соответствующими строками единичной матрицы.

Во второй строке произведения на месте номер j должна стоять сумма

$$b_{1,j} + b_{2,j}(a_{2,2} - 1) + b_{3,j}a_{2,3} + \cdots + b_{n,j}a_{2,n}.$$

При этом мы знаем (так как матрица B обратна к матрице A'), что

$$b_{1,j} + b_{2,j}a_{2,2} + b_{3,j}a_{2,3} + \cdots + b_{n,j}a_{2,n} = \delta_{2,j}.$$

Значит, во второй строке произведения стоят элементы

$$-b_{2,1}, 1 - b_{2,2}, -b_{2,3}, \ldots, -b_{2,n}.$$

В первой строке произведения на месте номер j должна стоять сумма

$$b_{1,j} + b_{2,j}(a_{1,2} + a_{2,2} - 1) + b_{3,j}(a_{1,3} + a_{2,3}) + \cdots + b_{n,j}(a_{1,n} + a_{2,n}),$$

при этом

$$\begin{aligned} b_{1,j} + b_{2,j}a_{2,2} + b_{3,j}a_{2,3} + \cdots + b_{n,j}a_{2,n} &= \delta_{2,j}, \\ b_{2,j}a_{1,2} + b_{3,j}a_{1,3} + \cdots + b_{n,j}a_{1,n} &= \delta_{1,j}. \end{aligned}$$

Таким образом, в первой строке произведения стоят элементы

$$1 - b_{2,1}, 1 - b_{2,2}, -b_{2,3}, \ldots, -b_{2,n}.$$

Таким образом, в группе N содержится матрица (мы учитываем, что $b_{2,2} = 0$)

$$C = \begin{pmatrix} 1 - b_{2,1} & 1 & -b_{2,3} & \ldots & -b_{2,n} \\ -b_{2,1} & 1 & -b_{2,3} & \ldots & -b_{2,n} \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}.$$

Прибавив ко первому столбцу второй столбец и вычтя из второй строки первую, мы получим матрицу

$$C' = \begin{pmatrix} 2 - b_{2,1} & 1 & -b_{2,3} & \ldots & -b_{2,n} \\ -1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} \in N.$$

Теперь рассматриваемая матрица C' разделится на следующие случаи:

1. Все $b_{2,3}, \ldots, b_{2,n}$ равны нулю. Тогда мы имеем дело с блочно-диагональной матрицей, у которой первый блок имеет вид

$$B = \begin{pmatrix} a & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

второй блок — это единичная матрица. Понятно, что можно рассматривать только первый блок. Рассмотрим коммутатор матрицы B с матрицей $E + E_{1,3}$, он равен матрице

$$\begin{pmatrix} 1 & 0 & a - 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix},$$

которая заменой базиса приводится к элементарной матрице $E + E_{2,3}$, эта матрица уже породит всю группу $\mathrm{SL}_n(K)$.

2. Не все $b_{2,3}, \ldots, b_{2,n}$ равны нулю. В этом случае блочно-диагональной заменой базиса, тождественной в первом диагональном блоке размера 2×2, мы можем прийти к матрице, верхний левый диагональный блок которой равен

$$B = \begin{pmatrix} a & 1 & 1 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

дополнительный блок единичен.

Рассмотрим коммутатор матрицы B с той же самой матрицей $E + E_{1,3}$, снова получим матрицу

$$\begin{pmatrix} 1 & 0 & a-1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix},$$

которая снова породит всю группу $\mathrm{SL}_n(K)$. □

Пусть поле K конечно и содержит $q = p^n$ элементов. Тогда в группе $\mathrm{GL}_n(K)$ содержится $(q^n-1)(q^n-q)\ldots(q^-q^{n-1})$ элементов, в группе $\mathrm{SL}_n(K)$ — $(q^n-1)(q^n-q)\ldots(q^n-q^{n-2})q^{n-1}$ элементов, в группе $\mathrm{PSL}_n(K)$ содержится $(q^n-1)(q^n-q)\ldots(q^n-q^{n-2})q^{n-1}$ элементов для поля характеристики два, $(q^n-1)(q^n-q)\ldots(q^n-q^{n-2})q^{n-1}/2$ элементов для поля характеристики, отличной от двух.

Таким образом, в группе $\mathrm{PSL}_2(\mathbb{Z}_2)$ шесть элементов, она некоммутативна, поэтому можно легко заключить, что она изоморфна группе S_3. Ясно также, что она не может быть изоморфна никакой другой проективной линейной группе. Любой автоморфизм этой группы является внутренним (см. упражнение 3), поэтому очевидно подходит к условиям теоремы.

В группе $\mathrm{PSL}_2(\mathbb{Z}_3)$ двенадцать элементов, из которых ровно три

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ и } \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$$

имеют порядок два, остальные неединичные элементы имеют порядок три. Это означает, что силовская 2-подгруппа в этой группе нормальна и изоморфна V_4. Ясно, что существует лишь одна такая неабелева группа, она изоморфна A_4 (см. упражнение 4). Понятно также, что группа $\mathrm{PSL}_2(\mathbb{Z}_3)$ не изоморфна никакой другой проективной линейной группе. Описание автоморфизмов данной группе оставим читателю в качестве упражнения (см. упражнение 5).

2.1.3 Изоморфизмы между группами $\mathrm{PSL}_2(K)$.

Группа $\mathrm{PSL}_2(K)$ над полем K есть фактор группы $\mathrm{SL}_2(K)$ по матрицам $\pm E$ в случае, когда характеристика поля K отлична от двух, и сама группа $\mathrm{SL}_2(K)$, если характеристика поля K равна двум. Таким образом, мы можем рассматривать элементы группы $\mathrm{PSL}_2(K)$ как матрицы из $\mathrm{SL}_2(K)$ с точностью до умножения на ± 1.

Лемма 2.1. *Если группы* $\mathrm{PSL}_2(K)$ *и* $\mathrm{PSL}_2(L)$ *изоморфны, поля* K *и* L *не состоят из четырех или пяти элементов, то не может быть, что поле* K *имеет характеристику два, а поле* L *имеет характеристику* $\neq 2$.

Доказательство. Предположим, что $\operatorname{char} K = 2$, $\operatorname{char} L \neq 2$. Мы можем предполагать, что в поле K больше четырех элементов (т. е. по крайней мере восемь).

Рассмотрим элемент $Q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ в группе $\mathrm{PSL}_2(K)$. Тогда элемент $\Phi(Q)$ имеет порядок два в группе $\mathrm{PSL}_2(L)$, поэтому в каком-то базисе представляется в виде матрицы $Q' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Матрица Q обладает тем свойством, что все элементы, коммутирующие с ней, имеют порядок два, коммутируют друг с другом, а также их больше трех штук. Значит, тем же свойством должна обладать и матрица Q'. Коммутирование в группе $\mathrm{PSL}_2(L)$ означает коммутирование или антикоммутирование в группе $\mathrm{SL}_2(L)$. С матрицей Q' коммутируют матрицы

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix},$$

а антикоммутируют матрицы

$$\begin{pmatrix} c & d \\ d & -c \end{pmatrix}.$$

Матрицы первого вида имеют порядок два только при $a = 0$ (и тогда они совпадают с Q') или при $b = 0$ (и тогда они скалярны). Этот случай нам не годится. Значит, должно быть по крайней мере три матрицы второго вида. Заметим, что вместе с матрицей $\begin{pmatrix} c & d \\ d & -c \end{pmatrix}$ в группе $\mathrm{SL}_2(L)$ содержится матрица $\begin{pmatrix} d & c \\ c & -d \end{pmatrix}$. Если такие две матрицы коммутируют, то $d = \pm c$, $2c^2 = -1$. Возможных таких матриц (с точностью до умножения на -1) есть всего две. Если такие матрицы антикоммутируют, то либо $a = 0$, $b^2 = -1$, либо $a^2 = -1$, $b = 0$. Таких матриц тоже всего две. При этом матрицы первого вида не коммутируют и не антикоммутируют с матрицами второго вида, поэтому трех искомых матриц не найдется.

Следовательно, образа $\Phi(Q)$ в группе $\mathrm{PSL}_2(L)$ не может существовать, поэтому такого изоморфизма нет. □

Теперь предположим, что поля K и L имеют характеристику, отличную от двух.

Рассмотрим некоторую матрицу $A \in \mathrm{SL}_2(K)$, обладающую свойством

$$Pr_1(A) := A^2 \neq \pm E \wedge \exists X \ \big(X^2 \neq \pm E \wedge XA \neq \pm AX \wedge (XAX^{-1})A = \pm A(XAX^{-1})\big).$$

Лемма 2.2. *Матрица, удовлетворяющая свойству* Pr_1, *над полем характеристики* $\neq 2$ *в некотором базисе имеет вид*

$$\pm \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

кроме полей $\mathbb{Z}_3$, $\mathbb{Z}_5$.

Доказательство. Пусть матрица A в некотором базисе имеет искомый вид $\pm(E + E_{1,2})$ и пусть характеристика поля отлична от двух. Тогда рассмотрим в этом базисе матрицу $X = \operatorname{diag}[\alpha, 1/\alpha]$, где $\alpha^2 \neq \pm 1$ (во всех полях, кроме перечисленных, такие элементы α есть). Данная матрица удовлетворяет условиям $X^2 \neq \pm E$, $XA \neq \pm AX$, матрица XAX^{-1} имеет вид $E + \alpha^2 E_{1,2}$, т е. коммутирует с A.

Пусть теперь матрица A ни в каком базисе не имеет вид $\pm(E + E_{1,2})$. Значит, она диагонализируема над каким-то расширением рассматриваемого поля K. Если матрица A удовлетворяла свойству Pr_1 над полем K, то она будет удовлетворять ему и над расширением данного поля. Таким образом, можем считать, что матрица A диагональна и удовлетворяет свойству Pr_1. По условию у матрицы A элементы на диагонали различны. Значит, она коммутирует только с диагональными матрицами, а "антикоммутирует" только с матрицами вида $\begin{pmatrix} 0 & \alpha \\ -1/\alpha & 0 \end{pmatrix}$, и только в случае, если квадрат ее собственного значения равен -1. Если квадрат ее собственного значения равен -1, то она имеет порядок два в группе $\mathrm{PSL}_2(K)$, чего не может быть по условию. Значит, матрица XAX^{-1} диагональна. Тогда подходящей матрицей X может быть лишь мономиальная матрица (матрица, у которой в каждой строке и в каждом столбце есть ровно по одному ненулевому значению), но она обязательно либо диагональна (и тогда коммутирует с A), либо побочно-диагональна (и тогда в квадрате скалярна). Значит, для такой A условие Pr_1 выполняться не может.

Лемма доказана. □

Лемма 2.3. *Над полем характеристики два любая матрица $A \in SL_2(K)$ порядка два в некотором базисе имеет вид*

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Доказательство. Так как матрица A имеет порядок два, то она не может быть скалярной. Значит, существует вектор v_1 такой, что Av_1 линейно независим с v_1. Тогда вектор $v_2 = Av_1 + v_1$ также линейно независим с v_1. Рассмотрим матрицу A в базисе $\{v_2, v_1\}$. Заметим, что так как $A^2 = E$, то $A(Av_1) = v_1$, поэтому $A(v_2) = v_2$. Кроме того, $Av_1 = v_2 + v_1$, откуда получаем искомый вид матрицы. □

Лемма 2.4. *Над полем из пяти элементов любая матрица $A \in \mathrm{PSL}_2(\mathbb{Z}_5)$ порядка пять в некотором базисе имеет вид*

$$\pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Доказательство. Если некоторая матрица A порядка пять ни в каком базисе не имеет искомый вид, то она должна иметь два различных собственных значения, $\alpha, 1/\alpha$ такие, что $\alpha^5 = \pm 1$. Однако в поле характеристики пять $\alpha^5 \pm 1 = (\alpha \pm 1)^5$, поэтому $\alpha = \pm 1$, что невозможно. □

Лемма 2.5. *Для любого изоморфизма $\Phi : \mathrm{PSL}_2(K) \to \mathrm{PSL}_2(L)$, где $|K|, |L| > 3$, исключен случай, когда поля K, L — это пара полей $\mathbb{F}_4$, $\mathbb{F}_5$, матрица $\Phi(\overline{E + E_{1,2}})$ имеет в некотором базисе пространства L^2 вид $\overline{E + E_{1,2}}$.*

Доказательство. Если характеристика полей равна двум, то результат следует из леммы 2.3.

Пусть характеристики полей отличны от двух. Если $K = L = \mathbb{F}_5$, то результат следует из леммы 2.4.

Теперь мы можем считать, что $|K|, |L| > 5$.

По лемме 2.2 матрицы, которые в некотором базисе имеют вид $E + E_{1,2}$, и только они, удовлетворяют формуле Pr_1. В проективной группе данная формула превратится в формулу

$$\overline{Pr_1}(\overline{A}) = \overline{A}^2 \neq E \wedge \exists \overline{X}\ \overline{X}^2 \neq E \wedge \overline{X} \neq E \wedge \overline{XA} \neq \overline{AX} \wedge\ \wedge (\overline{XAX}^{-1})\overline{A} = \overline{A}(\overline{XAX}^{-1}).$$

Значит, матрица $\Phi(\overline{E + E_{1,2}})$ удовлетворяет формуле $\overline{Pr_1}$, т. е. любой ее представитель удовлетворяет формуле Pr_1, а поэтому является в некотором базисе матрицей $\pm(E + E_{1,2})$. □

Теперь мы можем считать, что после замены базиса $\Phi(E + E_{1,2}) = E + E_{1,2}$.

2.1.4 Упражнения.

1. Докажите, что над полем K матрицы $E + \lambda E_{i,j}$, $\lambda \in K$, $1 \leqslant i \neq j \leqslant n$, порождают всю специальную линейную группу $\mathrm{SL}_n(K)$.

2. Докажите, что над полем характеристики два из каждого элемента можно извлечь не более одного квадратного корня.

3. Докажите, что любой автоморфизм группы S_3 является внутренним.

4. Докажите, что группа $\mathrm{PSL}_2(\mathbb{Z}_3)$ изоморфна группе A_4.

5. Найдите все автоморфизмы группы $\mathrm{PSL}_2(\mathbb{Z}_3) \cong A_4$.

6. Докажите, что простая группа порядка 60 обязательно изоморфна группе A_5.

2.2 Лекция 4.

2.2.1 Изоморфизмы между группами $\mathrm{PSL}_2(K)$ и $\mathrm{PSL}_2(L)$ — окончание.

Напомним, что мы считаем, что две группы $\mathrm{PSL}_2(K)$ и $\mathrm{PSL}_2(L)$ изоморфны, $|K|, |L| > 3$, поля K, L не являются парой полей $\mathbb{F}_4$, $\mathbb{F}_5$, изоморфизм Φ таков, что $\Phi(\overline{E + E_{1,2}}) = \overline{E + E_{1,2}}$.

Лемма 2.6. *В предыдущих предположениях существует матрица* $g \in \mathrm{GL}_2(L)$ *такая, что для изоморфизма* $\Phi' = \overline{i_g} \circ \Phi$ *выполнены условия* $\Phi'(\overline{E + E_{1,2}}) = \overline{E + E_{1,2}}$ *и*

$$\Phi'\left(\pm\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right) = \pm\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = Q.$$

Доказательство. Заметим, что $\overline{Q}^2 = E$. Пусть $\Phi(Q) = \begin{pmatrix}a & b\\ c & d\end{pmatrix} = Q'$. Тогда $c(a+d) = b(a+d) = 0$. Если $a + d \neq 0$, то $b = c = 0$, $a^2 = d^2 = 1$, т. е. $a = \pm 1$, $d = \pm 1$, а из $ad = 1$ получим $a = d$, т. е. матрица Q' скалярна, чего не может быть. Значит, $a + d = 0$. Тогда $d = -a$, $a^2 + bc = -1$.

Воспользуемся теперь соотношением

$$Q(E + E_{1,2})Q = (E - E_{1,2})Q(E - E_{1,2}).$$

Из него получим следующие уравнения:

$$\begin{cases} a(a+c) + bc = a - c, \\ c(a+c+d) = c, \\ a(b+d) + bd = b - a - d + c, \\ c(b+d) + d^2 = d - c. \end{cases}$$

В нашем предположении $a + d = 0$, поэтому из второго уравнения $c^2 = c$. Значит, либо $c = 0$, либо $c = 1$. Если $c = 0$, то $a^2 = a$ и $a^2 = -1$, чего не может быть. Значит, $c = 1$. В этом случае $a^2 + b = -1$, т. е. $b = -1 - a^2$. Таким образом, матрица Q' имеет вид

$$\begin{pmatrix}a & -1 - a^2\\ 1 & -a\end{pmatrix}.$$

Произведем замену базиса с помощью матрицы $E + aE_{1,2}$. Такая замена не изменит матрицу $E + E_{1,2}$, а матрица Q' при этом станет равной Q.

Таким образом, лемма доказана. □

Теперь мы можем предполагать, что $\Phi'(\overline{E + E_{1,2}}) = \overline{E + E_{1,2}}$, $\Phi'(\overline{Q}) = \overline{Q}$.

Лемма 2.7. *В предыдущих предположениях для любого* $\alpha \in K$ *существует* $\beta \in L$ *такое, что*

$$\Phi'(\overline{E + \alpha E_{1,2}}) = \overline{E + \beta E_{1,2}}.$$

Доказательство. Матрицы вида $\pm(E + \alpha E_{1,2})$ коммутируют с матрицей $E + E_{1,2}$. Докажем, что никакие другие матрицы с ней не коммутируют и не "антикоммутируют".

Действительно, если какая-то матрица "антикоммутирует" с $E + E_{1,2}$, то матрицы $E + E_{1,2}$ и $-(E + E_{1,2})$ сопряжены, чего не может быть. Если $E + E_{1,2}$ коммутирует с некоторой матрицей $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, то прямым подсчетам получаем $c = 0$ и $a = d$, откуда $a = d = \pm 1$. Лемма доказана. □

Лемма 2.8. *Отображение $\rho : \alpha \mapsto \beta$ является изоморфизмов между полями K и L.*

Доказательство. Очевидно, что отображение ρ инъективно и сюръективно. Отображение ρ аддитивно, так как $E + \rho(\alpha_1 + \alpha_2)E_{1,2} = \Phi'(E + (\alpha_1 + \alpha_2)E_{1,2}) = \Phi'((E + \alpha_1 E_{1,2})(E + \alpha_2 E_{1,2})) = (E + \rho(\alpha_1)E_{1,2})(E + \rho(\alpha_2)E_{1,2}) = E + (\rho(\alpha_1) + \rho(\alpha_2))E_{1,2}$.

Докажем мультипликативность рассматриваемого отображения.

Докажем сначала, что диагональные матрицы при изоморфизме Φ' переходят в диагональные.

Действительно, диагональные матрицы характеризуются двумя свойствами:

1. $QDQ^{-1} = D^{-1}$.

2. $D(E + E_{1,2})D^{-1} = E + aE_{1,2}$.

Именно поэтому диагональные переходят в диагональные.

Теперь покажем, что матрицы вида

$$\begin{pmatrix} 0 & a \\ -1/a & 0 \end{pmatrix}$$

переходят в матрицы того же вида.

Действительно, это матрицы вида DQ, где D — диагональные.

Покажем, что $\Phi'(E - \alpha^{-1}E_{2,1}) = E - \rho(\alpha)^{-1}E_{2,1}$. Ясно, что $\Phi'(E - \alpha^{-1}E_{2,1}) = E + \beta E_{2,1}$. Воспользуемся теперь тем, что $(E+\alpha E_{1,2})(E-\alpha^{-1}E_{2,1})(E+\alpha E_{1,2})$ — это матрица вида DQ. Тогда из соотношения получаем, что $1+\beta\rho(\alpha) = 0$, откуда $\beta = -\rho(\alpha)^{-1}$, что и требовалось.

Теперь $\Phi'(\operatorname{diag}[\alpha\beta, 1/(\alpha\beta)]) = \Phi'(\operatorname{diag}[\alpha, 1/\alpha])\Phi'(\operatorname{diag}[\beta, 1/\beta])$. Если $\Phi'(\operatorname{diag}[\alpha, 1/\alpha]) = \operatorname{diag}[\alpha', 1/\alpha']$, то так как $\Phi'(\operatorname{diag}[\alpha, 1/\alpha]) = \Phi'\left(\begin{pmatrix} 0 & \alpha \\ -1/\alpha & 0 \end{pmatrix} Q\right) = \Phi'((E + \alpha E_{1,2})(E - \alpha^{-1}E_{2,1})(E + \alpha E_{1,2}))Q = \operatorname{diag}[\rho(\alpha), \rho(\alpha)^{-1}]$.

Таким образом, отображение ρ мультипликативно, т. е. является изоморфизмом. □

Теперь мы видим, что изоморфизм Φ' является кольцевым, т.е. композиция изначального изоморфизма Φ с некоторым внутренним автоморфизмом группы $\mathrm{PSL}_2(L)$ — это кольцевой изоморфизм. Значит, изначальный изоморфизм имел искомый вид. Теорема 2.2 доказана.

Теперь нам нужно описать некоторый изоморфизм между группами $\mathrm{PSL}_2(\mathbb{F}_4)$ и $\mathrm{PSL}_2(\mathbb{F}_5)$.

2.2.2 Изоморфизм между группами $\mathrm{PSL}_2(\mathbb{F}_4)$ и $\mathrm{PSL}_2(\mathbb{F}_5)$.

Предложение 2.3. *Группы $\mathrm{PSL}_2(\mathbb{F}_4)$ и $\mathrm{PSL}_2(\mathbb{F}_5)$ — это изоморфные группы порядка 60 (и они изоморфны группе A_5 четных подстановок порядка 5).*

Доказательство. Мы установим изоморфизм между каждой из рассматриваемых групп и группой A_5.

1) Сначала рассмотрим группу $\mathrm{PSL}_2(\mathbb{F}_4)$. Двумерное пространство над полем $\mathbb{F}_4$ содержит всего пять прямых ($\langle e_1\rangle, \langle e_2\rangle, \langle e_1 + e_2\rangle, \langle e_1 + ae_2\rangle, \langle e_1 + be_2\rangle$, где a, b неединичные и ненулевые элемента поля $\mathbb{F}_4$). Любой элемент $A \in \mathrm{PSL}_2(\mathbb{F}_4)$ — Это некоторая перестановка данных прямых. Таким образом, возникает гомоморфизм из рассматриваемой группы

в группу S_5. Очевидно, что ядро гомоморфизма тривиально, так как только скалярные матрицы оставляют на месте все прямые пространства. Значит, это вложение группы из 60 элементов в группу S_5. Однако в S_5 существует только одна подгруппа из 60 элементов — это A_5.

2) Теперь рассмотрим группу $\mathrm{PSL}_2(\mathbb{F}_5)$. Рассмотрим $P^1(V)$ — множество прямых пространства $V = \mathbb{F}_5^2$. Из тех же соображений, что и выше, их шесть штук. Если даны различные прямые $P, Q, R, S \in P^1(V)$, то мы будем говорить, что пара P, Q *гармонически связана* с парой R, S, если в пространстве V существуют такие векторы p, q, что

$$P = \mathbb{F}_5 p, \qquad Q = \mathbb{F}_5 q,$$
$$S = \mathbb{F}_5 (p - q), \qquad R = \mathbb{F}_5 (p + q).$$

Легко проверить, что пара P, Q гармонически связана с парой R, S тогда и только тогда, когда существует преобразование $\sigma \in \mathrm{PSL}_2(\mathbb{F}_5)$, переставляющее P с Q, а R — с S.

Разбиением множества $P^1(V)$ назовем, как обычно, разложение этого множества на непересекающиеся подмножества. *Гармоническим разбиением* назовем разбиение $P^1(V)$ на три подмножества по два элемента такие, что любые два из этих подмножеств гармонически связаны. Из определений немедленно следует, что для любых трех различных прямых P, Q, L существует единственная четвертая прямая K, отличная от первых трех и такая, что пара P, Q гармонически связана с парой L, K. Поэтому, если два гармонических разбиения имеют общее подмножество (элемент разбиения), то они совпадают. В частности, существует не более пяти гармонических разбиений. С другой стороны, фиксируя прямую P и заставляя прямую Q пробегать остальные точки, получим по крайней мере пять разбиений. Таким образом, существует ровно пять гармонических разбиений, назовем их $\mathcal{H}_1, \ldots, \mathcal{H}_5$. Рассмотрим произвольный элемент $\sigma \in \mathrm{PSL}_2(\mathbb{F}_5)$. Для каждого гармонического разбиения

$$\mathcal{H} = \{L_1, L_2 \mid L_3, L_4 \mid L_5, L_6\}$$

разбиение

$$\{\sigma L_1, \sigma L_2 \mid \sigma L_3, \sigma L_4 \mid \sigma L_5, \sigma L_6\}$$

снова гармоническое, обозначим его через $\sigma\mathcal{H}$.

Ясно, что разные гармонические разбиения переходят в разные, поэтому σ индуцирует перестановку на множестве из пяти гармонических разбиений. Таким образом, мы снова получаем гомоморфизм из нашей группы $\mathrm{PSL}_2(\mathbb{F}_5)$ в группу S_5. Ясно, что ядро этого гомоморфизма не может совпадать со всей группой, так как существуют элементы $\sigma \in \mathrm{PSL}_2(\mathbb{F}_5)$, индуцирующие нетривиальную перестановку прямых. Так как рассматриваемая группа проста, то ядро тривиально, поэтому образ снова является группой A_5.

Предложение доказано. □

2.2.3 Инволюции в группе $\mathrm{PSL}_n(K)$ при $\mathrm{char}\, K \neq 2$.

В этом пункте мы будем считать, что характеристика поля не равна двум. Нас будет интересовать, как устроены в проективных линейных группах инволюции (элементы порядка два), а также коммутанты их централизаторов.

Лемма 2.9. *В группе* $\mathrm{PSL}_2(K)$ *над любым полем* K *коммутант централизатора любой инволюции коммутативен.*

Доказательство. Мы уже знаем, что любая инволюция в группе $\mathrm{PSL}_2(K)$ в некотором базисе имеет вид

$$Q = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

В группе $\mathrm{SL}_2(K)$ такая матрица коммутирует с матрицами

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

и антикоммутирует с матрицами

$$\begin{pmatrix} c & d \\ d & -c \end{pmatrix}.$$

Понятно, что коммутатор двух матриц, коммутирующих или антикоммутирующих с матрицей Q, будет коммутировать с этой матрицей. Значит, коммутант централизатора состоит из матриц первого вида, которые коммутируют между собой. □

Лемма 2.10. *Если* n *нечетно,* $\mathrm{char}\, K \neq 2$*, то любая инволюция группы* $\mathrm{PSL}_n(K)$ *имеет в группе* $\mathrm{SL}_n(K)$ *представителя, который в некотором базисе имеет вид*

$$\mathrm{diag}\,[\pm 1, \pm 1, \ldots, \pm 1].$$

Доказательство. Рассмотрим произвольный представитель A в группе $\mathrm{SL}_n(K)$ инволюции $\overline{A}$. Это матрица, в квадрате дающая скалярную матрицу λE, $\lambda^n = 1$. Очевидно, что эта матрица диагонализируема в каком-то расширении поля K, так как никакая жорданова клетка размера, большего 1×1, не может в квадрате давать диагональную матрицу (над полем характеристики $\neq 2$). Ее собственные значения (также в расширении поля K) равны $\pm\sqrt{\lambda}$. Таким образом, определитель матрицы A равен $\pm\lambda^{[n/2]}\sqrt{\lambda}$. Так как этот определитель содержится в поле K, то $\sqrt{\lambda} \in K$. Значит, вместе с матрицей A представителем для $\overline{A}$ является матрица $A' = \sqrt{\lambda}^{-1} A$, собственные значения которой равны ± 1. Значит. в некотором базиса матрица A' имеет искомый вид. □

Лемма 2.11. *Если* $n = 2k$ *четно,* $\mathrm{char}\, K \neq 2$*, то любая инволюция группы* $\mathrm{PSL}_n(K)$ *имеет в группе* $\mathrm{SL}_n(K)$ *либо представителя, который в некотором базисе имеет вид* $\mathrm{diag}\,[\pm 1, \pm 1, \ldots, \pm 1]$*, либо вид*

$$\begin{pmatrix} 0 & \lambda & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & \lambda & \ldots & 0 & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 0 & \lambda \\ 0 & 0 & 0 & 0 & \ldots & 1 & 0 \end{pmatrix}.$$

Доказательство. Аналогично предыдущей лемме в некотором расширении поля K матрица A, представляющая инволюцию $\overline{A}$ группы $\mathrm{PSL}_{2k}(K)$ в некотором базисе имеет вид $\mathrm{diag}\,[\pm\sqrt{\lambda},\dots,\pm\sqrt{\lambda}]$, $\lambda^{2k}=1$. Ясно, что если $\sqrt{\lambda}\in K$, то можно считать, что элемент $\overline{A}$ также представляет и матрица $A'=\mathrm{diag}\,[\pm1,\dots,\pm1]$.

Предположим теперь, что $\sqrt{\lambda}\notin K$. Тогда над полем K у матрицы A нет ни одного собственного вектора, а в квадрате она равна λE. Рассмотрим любой ее вектор e_1. Мы знаем, что Ae_1 линейно независим от e_1. Возьмем Ae_1 за e_2. Тогда очевидно, что $Ae_2=\lambda e_1$. Теперь рассмотрим любой вектор e_3, линейно независимый от векторов e_1,e_2. Вектор $e_4=Ae_3$ линейно независим от e_1,e_2,e_3, так как если $Ae_3=ae_1+be_2+ce_3$, то $\lambda e_3=A^2e_3=ae_2+\lambda be_1+ace_1+bce_2+c^2e_3$. Это означает $c^2=\lambda$, что невозможно. Значит, векторы e_1,e_2,e_3,e_4 линейно независимы, при этом $Ae_4=\lambda e_3$. Продолжая процедуру дальше, мы придем к искомому виду матрицы A. □

Лемма 2.12. *При* $\mathrm{char}\,K\neq2$ *фактор по центру коммутанта централизатора инволюции*

$$\mathrm{diag}\,[\underbrace{1,\dots,1}_{p},\underbrace{-1,\dots,-1}_{q}]$$

в группе $\mathrm{PSL}_{p+q}(K)$ *изоморфен прямому произведению* $\mathrm{PSL}_p(K)\times\mathrm{PSL}_q(K)$.

Доказательство. Как мы уже знаем, коммутирование в группе $\mathrm{PSL}_n(K)$ означает коммутирование или антикоммутирование в группе $\mathrm{SL}_n(K)$ соответствующих представителей. С инволюцией $\mathrm{diag}\,[\underbrace{1,\dots,1}_{p},\underbrace{-1,\dots,-1}_{q}]$ коммутируют блочно-диагональные матрицы, у которых первый блок имеет размер $p\times p$, а второй — $q\times q$. С этой же инволюцией могут антикоммутировать какие-то матрицы, только если $p=q$. Тогда это матрицы вида $\begin{pmatrix}0&A_1\\A_2&0\end{pmatrix}$, где A_1,A_2 — произвольные невырожденные матрицы размера $p\times p$ с произведением определителей $(-1)^p$. Ясно, что когда мы возьмем коммутатор любых двух матриц, каждая которая коммутирует или антикоммутирует с нашей инволюцией, то этот коммутатор обязательно будет коммутировать с ней. Значит, он точно содержится в группе матриц вида $\begin{pmatrix}A_1&0\\0&A_2\end{pmatrix}$, $A_1\in\mathrm{GL}_p(K)$, $A_2\in\mathrm{GL}_q(K)$, $\det A_1\det A_2=1$. Понятно, что коммутант группы таких матриц состоит из матриц того же вида, где $A_1\in\mathrm{GL}_p(K)'$, $A_2\in\mathrm{GL}_q(K)'$. Если $K\neq\mathbb{Z}_2$ (а оно не равно по условию), то $\mathrm{GL}_m(K)'=\mathrm{SL}_m(K)$ для всех $m\geqslant1$. Таким образом, мы получим группу матриц вида $\begin{pmatrix}A_1&0\\0&A_2\end{pmatrix}$, $A_1\in\mathrm{SL}_p(K)$, $A_2\in\mathrm{SL}_q(K)$. Ясно, что фактор по центру такой группы изоморфен $\mathrm{PSL}_p(K)\times\mathrm{PSL}_q(K)$. □

Заметим, что коммутант централизатора "нестандартной" инволюции вида $Q_0=\begin{pmatrix}0&\lambda E\\E&0\end{pmatrix}$ может быть различным. Матрицы, коммутирующие с Q_0, имеют вид $\begin{pmatrix}A&\lambda B\\B&A\end{pmatrix}$, а матрицы, антикоммутирующие с Q_0, — вид $\begin{pmatrix}A&\lambda B\\-B&-A\end{pmatrix}$, коммутант содержится в подгруппе, состоящей из матриц первого вида, однако сложно описать его точно. Однако ясно, что

коммутант централизатора не будет коммутативен, потому что в нем содержатся все матрицы вида $\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$, $\det A = 1$.

Лемма 2.13. *Если* $\operatorname{char} K \neq 2$, *то для проективных линейных групп порядка два, и только для них, коммутант централизатора любой инволюции коммутативен.*

Доказательство. То, что коммутант централизатора любой инволюции коммутативен для групп порядка два, было доказано в лемме 2.9. Мы только что показали, что во всех остальных случаях он не может быть коммутативен. □

Лемма 2.14. *Прямое произведение групп* $\mathrm{PSL}_p(K) \times \mathrm{PSL}_q(K)$ *над любым полем* K *единственным способом можно представить в виде прямого произведения.*

Доказательство. Обозначим группу $\mathrm{PSL}_p(K)$ за G_1, а $\mathrm{PSL}_q(K)$ — за G_2. Пусть $G = G_1 \times G_2 = H_1 \times H_2$. Рассмотрим коммутант $G_{1,1} = [G_1, H_1]$ (подгруппу, порожденную коммутаторами $[g, h]$, $g \in G_1$, $h \in H_1$). Так как обе подгруппы G_1, H_1 нормальны в группе G, То каждый коммутатор содержится и в G_1, и в G_2, поэтому $G_{1,1} \subset G_1 \cap H_1$. При этом, очевидно, подгруппа $G_{1,1}$ нормальна в G. Точно так же подгруппа $G_{1,2} = [G_1, H_2]$ лежит в пересечении $G_1 \cap H_2$ и нормальна в G.

Таким образом, в группе G_1 содержатся две нормальные подгруппы, пересекающиеся только по единичному элементу.

Пусть $G_{1,1} = \{e\}$. Это означает, что подгруппы G_1 и H_1 коммутируют. Так как центр группы G_1 тривиален, то $H_1 \subset G_2$. Ясно, что в этом случае $G_{1,2} \neq \{e\}$, поэтому либо $G_{1,2} = G_1$, либо $K = \mathbb{Z}_3$, $p = 2$, $|G_{1,2}| = 4$.

В первом случае $G_1 \subset H_2$, $H_1 \subset G_2$. Если $H_1 \neq G_2$, то это тоже означает, что $K = \mathbb{Z}_3$, $q = 2$, $|H_1| = 4$, Тогда получается, что группа G есть прямое произведение двух подгрупп, одна из которых абелева, что означает наличие нетривиального центра. Получаем противоречие. Значит, в этом случае $H_1 = G_2$, $H_2 = G_1$.

Теперь предположим, что $K = \mathbb{Z}_3$, $p = q = 2$, $H_1 \subset G_2$, $|G_{1,2}| = 4$.

Если $H_1 = G_2$, то очевидно, что $H_2 = G_1$, что и требовалось.

Если $|H_1| = 4$, то снова у группы G получается нетривиальный центр. Противоречие. □

2.2.4 Упражнения.

1. Найдите все автоморфизмы поля из 4 элементов; из p элементов; из p^2 элементов; из 8 элементов; из 27 элементов.

2. Докажите, что простая группа из 168 элементов единственна и изоморфна $\mathrm{PSL}_3(\mathbb{Z}_2)$.

3. Сколько прямых существует в n-мерном линейном пространстве над полем из q элементов?

4. Если предположить, что изоморфизм между $\mathrm{PSL}_2(\mathbb{F}_7)$ и $\mathrm{PSL}_3(\mathbb{F}_2)$ существует, то в какую матрицу при этом изоморфизме может перейти матрица

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{F}_7)?$$

5. Найдите коммутант централизатора нестандартной инволюции $Q_0 = \begin{pmatrix} 0 & \lambda E \\ E & 0 \end{pmatrix}$ в группе $\mathrm{PSL}_4(\mathbb{F}_3)$, в группе $\mathrm{PSL}_4(\mathbb{F}_5)$, в группе $\mathrm{PSL}_4(\mathbb{R})$.

6. Какое условие нужно наложить на группы G_1 и G_2, чтобы их прямое произведение $G = G_1 \times G_2$ единственным образом представлялось в виде прямого произведения?

2.3 Лекция 5.

2.3.1 Различение размерностей при $\mathrm{char}\, K \neq 2$.

Чтобы точно различать размерности групп $\mathrm{PSL}_n(K)$, нам нужно узнать, как устроен коммутант централизатора единственной "нестандартной" инволюции $\varepsilon_{\lambda,k} \sim \begin{pmatrix} 0 & \lambda E_k \\ E_k & 0 \end{pmatrix}$. Для этого запишем ее в более удобном виде

$$\varepsilon_{\lambda,k} = \mathrm{diag}\left[\begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & \lambda \\ 1 & 0 \end{pmatrix}\right].$$

Заметим, что мы уже доказывали, что если $\sqrt{\lambda} \in K$, то эта инволюция приводится к стандартному виду, поэтому можем считать, что $\sqrt{\lambda} \notin K$.

Лемма 2.15. *Коммутант централизатора инволюции $\varepsilon_{\lambda,k}$ при $\sqrt{\lambda} \notin K$ изоморфен группе $\mathrm{SL}_k(\widetilde{K})$, где $\widetilde{K}$ — это поле, состоящее из матриц*

$$\begin{pmatrix} a & \lambda b \\ b & a \end{pmatrix}, \quad a, b \in K.$$

Доказательство. Для начала покажем, что $\widetilde{K}$ действительно является полем.

Ясно, что множество $\widetilde{K}$ замкнуто относительно сложения. Замкнутость относительно умножения и его коммутативность следует из формулы

$$\begin{pmatrix} a_1 & \lambda b_1 \\ -b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & \lambda b_2 \\ -b_2 & a_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 - \lambda b_1b_2 & \lambda(a_1b_2 + b_1a_2) \\ a_1b_2 + b_1a_2 & a_1a_2 - \lambda b_1b_2 \end{pmatrix};$$

существование обратного элемента при $a, b \neq 0$ следует из того, что определитель данной матрицы равен $a^2 - \lambda b^2$, что не может быть равно нулю при $\sqrt{\lambda} \notin K$.

Ясно, что любая матрица из коммутанта централизатора инволюции $\varepsilon_{\lambda,k}$ коммутирует с $\varepsilon_{lambda,k}$, поэтому обязательно имеет вид

$$A = (A_{i,j}), \quad \forall i, j = 1, \ldots, k \; A_{i,j} = \begin{pmatrix} a_{i,j} & \lambda b_{i,j} \\ b_{i,j} & a_{i,j} \end{pmatrix}.$$

С другой стороны, любая матрицы такого вида лежит в централизаторе матрицы A. Это означает, что нам достаточно показать, что коммутант группа таких матриц совпадает с этой группой.

Видно, что эта группа изоморфна $\mathrm{SL}_k(\widetilde{K})$. Так как группа $\mathrm{SL}_k(\widetilde{K})$ совпадает со своим коммутантом, потому что в поле $\widetilde{K}$ содержится $|K|^2$ элементов, что больше трех, то утверждение леммы доказано. □

Теперь мы хотим показать, что если характеристики полей отличны от двух, а соответствующие проективные группы изоморфны, то их размерности совпадают.

Лемма 2.16. *Для любого $n \geqslant 2$ существует предложение φ_n языка первого порядка теории групп, которое истинно во всех группах $\mathrm{PSL}_n(K)$ и ложно во всех группах $\mathrm{PSL}_m(K)$, $m \neq n$, для всех полей K характеристики, отличной от двух.*

Доказательство. Будем доказывать данное утверждение по индукции.

По лемме 2.13 для проективных линейных групп порядка два, и только для них, коммутант централизатора любой инволюции коммутативен (при условии на характеристику поля, конечно).

Данное утверждение выражается предложением первого порядка, которое мы обозначим через φ_2 (см. упражнение 1).

Если проективная группа имеет порядок три, то в ней для любой инволюции (они все в некотором базисе имеют вид $\varepsilon_3 = \mathrm{diag}\,[1, -1, -1]$) фактор по центру коммутанта ее централизатора изоморфен проективной группе порядка два над тем же полем (т. е. удовлетворяет предложению φ_2). Ясно из описания всех инволюций и коммутантов их централизаторов, что в группах бóльших порядков существуют и другие инволюции (вообще инволюция с таким свойством может существовать только теоретически в группе $\mathrm{PSL}_4(K)$).

Если проективная группа имеет порядок четыре, то в ней существует инволюция $\varepsilon_4 = \mathrm{diag}\,[1, 1, -1, -1]$, фактор по центру коммутанта централизатора которой есть прямое произведение двух групп, удовлетворяющих предложению φ_2. Ясно, что это не может быть возможно для групп других порядков.

Теперь перейдем к шагу (точнее, шагам) индукции. Предположим, что искомые предложения уже построены для всех порядков, меньших некоторого $2k + 1$.

Тогда предложение φ_{2k+1} должно описывать все возможные факторы по центру коммутантов централизаторов инволюций соответствующей группы. Именно, мы знаем, что все эти факторы изоморфны $\mathrm{PSL}_{2k}(K)$, $\mathrm{PSL}_{2k-1}(K) \times \mathrm{PSL}_2(K)$, …, $\mathrm{PSL}_k(K) \times \mathrm{PSL}_{k+1}(K)$. Ясно, что ни в каких проективных группах другой размерности нет ровно такого набора факторов по центру коммутантов централизаторов инволюций.

В предложении φ_{2k+2} достаточно написать, что существует инволюция (например, $\varepsilon_{2k+2} = \mathrm{diag}\,[-1, -1, 1, 1, \ldots, 1]$), фактор по центру коммутанта централизатора которой есть прямое произведение проективных групп порядка два и $2k$. □

Отсюда очевидно следует, что проективные группы разных порядков над полями характеристики, отличной от двух, не могут быть изоморфны.

Кроме того, мы видим, что все типы инволюций можно охарактеризовать с помощью формул первого порядка (см. упражнение 1), поэтому они должны при изоморфизме переходить в инволюции того же типа.

Опишем изоморфизмы между группами $\mathrm{PSL}_3(K)$ и $\mathrm{PSL}_3(L)$.

2.3.2 Группы $\mathrm{PSL}_3(K)$ и $\mathrm{PSL}_3(L)$ при $\mathrm{char}\, K, L \neq 2$.

Ясно, что мы можем считать, что $\Phi(\mathrm{diag}[-1,-1,1]) = \mathrm{diag}[-1,-1,1] = \varepsilon$ после подходящей замены базиса в пространстве L^3. Коммутант централизатора данной инволюции тоже должен перейти в коммутант централизатора при изоморфизме, поэтому можно считать, что изоморфизм Φ индуцирует изоморфизм $\widetilde{\Phi}$ между группами $\mathrm{SL}_2(K)$ и $\mathrm{SL}_2(L)$. Заметим, что из соображения количества элементов в группах не могло быть такого, что одно из полей есть $\mathbb{F}_4$, а другое — $\mathbb{F}_5$. Значит, поля K и L изоморфны,а изоморфизм $\widetilde{\Phi}$ между группами $\mathrm{SL}_2(K)$ и $\mathrm{SL}_2(L)$ стандартен, т. е. имеет вид $\widetilde{\Phi} = i_g \circ \rho$, $\rho : K \to L$ — кольцевой изоморфизм, $g = \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$, $A \in \mathrm{GL}_3(L)$. Ясно, что оба изоморфизм и автоморфизм в композиции являются одновременно изоморфизмом и автоморфизмом для групп порядка три. Значит, мы можем рассмотреть отображение $\Phi' = \rho^{-1} \circ i_{g^{-1}} \circ \Phi$, которое является уже автоморфизмом группы $\mathrm{PSL}_n(K)$, под действием которого матрицы вида

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad ad - bc = 1, \tag{$*$}$$

переходят сами в себя.

Рассмотрим матрицы A, коммутирующие с инволюцией ε, и удовлетворяющие следующим двум свойствам:

1. $A(E + E_{1,2})A^{-1}$ коммутирует с $E + E_{1,2}$;
2. QAQ^{-1} коммутирует с A.

Ясно, что диагональные матрицы удовлетворяют этим двум условиям. Если матрица A удовлетворяет этим двум условиям, то из коммутирования с ε она должна иметь вид

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & f \end{pmatrix},$$

далее из условия 1 у нее $c = 0$, а тогда из условия 2 $b = 0$.

Значит, мы смогли охарактеризовать диагональные матрицы, поэтому при нашем автоморфизме Φ' диагональные матрицы перейдут в диагональные. Таким образом,

$$\Phi'(\mathrm{diag}[1,-1,-1]) = \mathrm{diag}[1,-1,-1] \text{ или } \mathrm{diag}[-1,1,-1].$$

Во втором случае домножим автоморфизм Φ' сначала на i_Q — сопряжение матрицей $Q = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, а затем на контрградиентный автоморфизм. После этого мы придем к авто-

морфизму Φ'', который каждую матрицу вида $(*)$ переводит в себя, а также $\Phi''(\operatorname{diag}[1,-1,-1]) = \operatorname{diag}[1,-1,-1]$.

Рассмотрим образ матрицы

$$Q_{2,3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}.$$

Матрица $Q_{2,3}$ коммутирует с матрицей $\operatorname{diag}[1,-1,-1]$ и даже лежит в коммутанте ее централизатора, поэтому

$$\Phi''(Q_{2,3}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}.$$

Кроме того, $Q_{2,3}\operatorname{diag}[-1,-1,1] = \operatorname{diag}[-1,1,-1]Q_{2,3}$, откуда $a = d = 0$. Значит, $c = -b^{-1}$. Домножим теперь автоморфизм Φ'' на замену базиса, в которой первые два вектора не изменятся, а последний вектор умножится на b. После такой замены получим новый автоморфизм Φ''', под действием которого матрицы вида

$$\begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}, \quad A \in \mathrm{SL}_2(K),$$

по-прежнему будут переходить в себя, $\Phi'''(\operatorname{diag}[1,-1,-1]) = \operatorname{diag}[1,-1,-1]$, $\Phi'''(Q_{2,3}) = Q_{2,3}$.

Из последнего равенства следует, что $\Phi(E + aE_{1,3}) = E + aE_{1,3}$, аналогично, $\Phi(E + aE_{i,j}) = E + aE_{i,j}$ для всех $i, j = 1, \ldots, 3$, $i \neq j$.

Так как эти матрицы порождают всю группу $\mathrm{SL}_3(K)$, а их классы — всю группу $\mathrm{PSL}_3(K)$, то изоморфизм Φ''' оказывается тождественным.

Значит, домножив изначальный изоморфизм Φ на различные замены базиса, контрградиентный (может быть) автоморфизм и кольцевой изоморфизм, мы получили тождественный автоморфизм, т. е. изначальный изоморфизм был стандартен.

Теорема для размерности три доказана.

2.3.3 Группы $\mathrm{PSL}_4(K)$ и $\mathrm{PSL}_4(L)$ при $\operatorname{char} K, L \neq 2$.

Как мы видим из леммы 2.15, если $i = \sqrt{-1} \in K$, то инволюция $\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ диагонализируема над полем K с видом $\operatorname{diag}[i,i,-i,-i]$, такая инволюция эквивалентна в группе $\mathrm{PSL}_4(K)$ инволюции $\operatorname{diag}[1,1,-1,-1]$. С другой стороны, если $i \notin K$, то стандартную инволюцию $\operatorname{diag}[1,1,-1,-1]$ можно отличить от нестандартной с помощью формул про коммутанты их централизаторов, поэтому мы можем считать, что при изоморфизме Φ инволюция $\operatorname{diag}[1,1,-1,-1] \in \mathrm{PSL}_4(K)$ переходит в такую же инволюцию в группе $\mathrm{PSL}_4(L)$.

Тогда ясно, что матрицы вида $\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$, $A_1, A_2 \in \mathrm{SL}_2(K)$ должны переходить в матрицы того же самого вида. Так как мы уже показывали, что прямое произведение $\mathrm{PSL}_2(K) \times \mathrm{PSL}_2(K)$ можно представить в виде нетривиального прямого произведения лишь одним способом, то матрицы вида $\begin{pmatrix} A & 0 \\ 0 & E \end{pmatrix}$ при изоморфизме переходят либо в матрицы того же вида, либо в матрицы вида $\begin{pmatrix} E & 0 \\ 0 & B \end{pmatrix}$. Во втором случае после замены базиса с помощью матрицы $\begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix}$ мы придем к ситуации, когда

$$\Phi \begin{pmatrix} A & 0 \\ 0 & E \end{pmatrix} = \begin{pmatrix} \Phi_1(A) & 0 \\ 0 & E \end{pmatrix}, \quad \Phi \begin{pmatrix} E & 0 \\ 0 & A \end{pmatrix} = \begin{pmatrix} E & 0 \\ 0 & \Phi_2(A) \end{pmatrix}.$$

Таким образом, мы получаем два изоморфизма $\Phi_1, \Phi_2 : \mathrm{PSL}_2(K) \to \mathrm{PSL}_2(L)$. Так как из соображений порядка пара полей K, L не могла быть парой $\mathbb{F}_4, \mathbb{F}_5$, то $K \cong L$, а оба изоморфизма являются композициями кольцевых изоморфизмов и замен базиса, причем для первого замена базиса происходит для векторов e_1, e_2, а для второго — для векторов e_3, e_4. Заменив все векторы базиса, мы придем к изоморфизму Φ', который каждую матрицу $\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$, $A_1, A_2 \in \mathrm{SL}_2(K)$ отображает в $\begin{pmatrix} \overline{\rho}_1(A_1) & 0 \\ 0 & \overline{\rho}_2(A_2) \end{pmatrix}$, где $\rho_1, \rho_2 : K \to L$ — изоморфизмы полей K и L.

Рассмотрим образ инволюции

$$Q_4 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Это матрица, коммутирующая с матрицами

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ и } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

и, кроме того не лежащая в коммутанте централизатора исходной инволюции, но лежащая в ее централизаторе. Это означает, что ее образ также коммутирует с двумя выписанными матрицами и при этом должен иметь вид $\begin{pmatrix} 0 & B \\ \pm B^{-1} & 0 \end{pmatrix}$. Значит, B скалярна, а при этом ее определитель равен единице, поэтому она либо совпадает с Q_4, либо имеет вид $\begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}$.

В любом из этих случаев, так как Q_4 коммутировала со всеми матрицами $\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$, $A \in \mathrm{SL}_2(K)$, то ее образ коммутирует со всеми матрицами вида $\begin{pmatrix} \rho_1(A) & 0 \\ 0 & \rho_2(A) \end{pmatrix}$, $A \in \mathrm{SL}_2(K)$,

что означает, что для любой матрицы $A \in \mathrm{SL}_2(K)$ имеет место $\rho_1(A) = \rho_2(A)$. Значит, кольцевые изоморфизмы ρ_1 и ρ_2 совпадают, поэтому мы можем (как и в случае матриц 3×3 рассмотреть композицию изоморфизма Φ' с кольцевым изоморфизмом $\rho_1^{-1} : L \to K$. Эта композиция (обозначим ее через Φ'') будет автоморфизмом группы $\mathrm{PSL}_4(K)$, тождественно действующим на матрицах $\mathrm{diag}\,[A, B]$, $A, B \in \mathrm{SL}_2(K)$, а также переводящим матрицу Q_4 либо в себя, либо в себя, умноженную на изначально рассматриваемую инволюцию.

Рассмотрим теперь произвольную инволюцию ε', которая коммутирует с матрицей $\mathrm{diag}\,[1, 1, -1, -1]$, с матрицей $\begin{pmatrix} Q & 0 \\ 0 & Q \end{pmatrix}$, с матрицей Q_4, а также удовлетворяет соотношениям $\varepsilon'(E + E_{1,2} + E_{3,4})\varepsilon' = (E + E_{1,2} + E_{3,4})^{-1}$ и $\varepsilon'(E + E_{1,2} - E_{3,4})\varepsilon' = (E + E_{1,2} - E_{3,4})^{-1}$ (естественно, все коммутирование рассматривается в группе $\mathrm{PSL}_4(K)$, т. е. это коммутирование или антикоммутирование матриц).

Из того, что ε' коммутирует с матрицей $\mathrm{diag}\,[1, 1, -1, -1]$, следует, что это либо блочно-диагональная матрица, либо матрица вида $\begin{pmatrix} 0 & A \\ \pm A^{-1} & 0 \end{pmatrix}$, $A, B \in \mathrm{GL}_2(K)$. Рассмотрим сначала второй случай.

Из коммутирования с матрицей $\begin{pmatrix} Q & 0 \\ 0 & Q \end{pmatrix}$ мы получим, что $QAQ^{-1} = \pm A$, откуда $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ или $\begin{pmatrix} a & b \\ b & -a \end{pmatrix}$. Теперь из первого из оставшихся соотношений получим

$$\pm A \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix},$$

а из второго —

$$\pm A \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} A^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

что показывает, что таких матриц не существует.

Остается первый случай, в котором легко получаем, что матрица ε' имеет один из видов: $\pm\,\mathrm{diag}\,[1, -1, 1, -1]$ или $\pm\,\mathrm{diag}\,[1, -1, -1, 1]$. Пусть теперь

$$\Phi''(\,\mathrm{diag}\,[1, -1, 1, -1]) = \,\mathrm{diag}\,[1, -1, -1, 1].$$

Однако вспомним, что первая из матриц лежит в коммутанте централизатора матрицы Q_4, а вторая — нет (только в самом централизаторе). Таким образом, это невозможно, т. е. $\Phi''(\,\mathrm{diag}\,[1, -1, 1, -1]) = \,\mathrm{diag}\,[1, -1, 1, -1]$. Соответственно, $\Phi''(\,\mathrm{diag}\,[1, -1, -1, 1]) = \mathrm{diag}\,[1, -1, -1, 1]$.

Теперь нам будет интересен образ матрицы

$$Q_{2,3} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Это матрица A со следующими свойствами:

1. $A^2 = \,\mathrm{diag}\,[1, -1, -1, 1]$;

2. A лежит в коммутанте централизатора инволюции $\operatorname{diag}[1,-1,-1,1]$;
3. $A\operatorname{diag}[1,1,-1,-1] = \operatorname{diag}[1,-1,1,-1]A$.

Из первого свойства сразу видим, что

$$A = \begin{pmatrix} a & 0 & 0 & b \\ 0 & c & d & 0 \\ 0 & f & g & 0 \\ e & 0 & 0 & h \end{pmatrix}.$$

Из третьего свойства либо $a = h = d = f = 0$, либо $b = e = c = g = 0$. В первом случае рассмотрим композицию автоморфизма Φ'' с заменой базиса матрицей $\begin{pmatrix} Q & 0 \\ 0 & Q \end{pmatrix}$ и контраградиентным автоморфизм. После этого все рассмотренные выше матрицы будут иметь прежние образы, а матрица A в любом случае будет иметь $b = e = c = g = 0$. Будем по-прежнему обозначать полученный автоморфизм через Φ''' (чтобы не писать слишком много штрихов). Из первого свойства видим, что Значит, $a, h = \pm 1$, $df = -1$. Произведем теперь замену базиса с помощью матрицы $\operatorname{diag}[1,1,d,d]$. Тогда образы матриц, рассматриваемых выше, не изменятся, а матрица A будет иметь (из соображений определителя) искомый вид $\pm Q_{2,3}$. Таким образом, $\Phi'''(Q_{2,3}) = Q_{2,3}$. После этого понятно, что $\Phi'''(E + \alpha E_{1,3}) = \Phi'''(Q_{2,3}(E + \alpha E_{1,2})Q_{2,3}^{-1}) = E + \alpha E_{1,3}$. Аналогично переходят в себя все остальные элементарные матрицы, поэтому автоморфизм Φ''' является тождественным.

Теорема доказана для $n = 4$.

2.3.4 Группы $\mathrm{PSL}_{2m+1}(K)$ и $\mathrm{PSL}_{2m+1}(L)$ при $\operatorname{char} K, L \neq 2$.

Ясно, что теперь теорему можно доказывать по индукции по размеру матриц. Пусть она доказана для всех $n \leqslant 2k$ и мы хотим доказать ее для размерности $2k+1$. Тогда рассмотрим инволюцию $\varepsilon_1 = \operatorname{diag}[1,-1,\ldots,-1]$, фактор по центру коммутанта централизатора которой есть PSL_{2k}. Ясно, что после подходящей замены базиса, применения (если потребуется) контраградиентного автоморфизма и кольцевого изоморфизма мы можем считать, что рассматривается автоморфизм Φ' группы $\mathrm{PSL}_{2k+1}(K)$, при котором для любой матрицы

$$X = \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}, \quad A \in \mathrm{SL}_{2k}(K),$$

имеет место $\Phi'(\overline{X}) = \overline{X}$.

Для начала посмотрим на образ инволюции $\varepsilon_2 = \operatorname{diag}[-1,1,-1,\ldots,-1]$. Это инволюция ε', коммутирующая со всеми матрицами вида $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & B \end{pmatrix}$, $B \in \mathrm{SL}_{2k-1}(K)$. Ясно, что тогда ε' обязательно имеет вид $\operatorname{diag}[A, \lambda E]$, $A \in \mathrm{GL}_2(K)$, $A^2 = \lambda^2 E$, $\lambda^{2k+1} = \pm 1$. С другой стороны, инволюция ε' коммутирует с исходной инволюцией ε_1, поэтому матрица A должна быть диагональна. Значит, ε' имеет вид $\operatorname{diag}[\pm\lambda, \pm\lambda, \lambda, \ldots, \lambda]$. Ясно, что матрица не скалярна, поэтому хотя бы одно из первых двух собственных значений должно иметь

знак минус. Добавим условие, что фактор по центру коммутанта такой инволюции есть $\mathrm{PSL}_{2k}(K)$, тогда обязательно $\varepsilon' = \mathrm{diag}\,[\lambda, -\lambda, \lambda, \ldots, \lambda]$, т. е. инволюция ε' эквивалентна исходной инволюции ε_2.

Теперь рассмотрим матрицу

$$Q_{1,2} = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & E_{2k-1} \end{pmatrix}.$$

Пусть ее образ есть Q'. Тогда Q' коммутирует с со всеми матрицами $\mathrm{diag}\,[1, 1, A]$, $A \in \mathrm{SL}_{2k-1}(K)$, ее квадрат равен инволюции $\mathrm{diag}\,[-1, -1, 1, 1, \ldots, 1] = \varepsilon_1\varepsilon_2$. Значит, она имеет вид $\mathrm{diag}\,[A, \lambda E]$, $A \in \mathrm{GL}_2(K)$, $A^2 = -\lambda^2 E$, $\lambda^{2k+1} = \pm 1$. Дополнительно имеем $Q' \,\mathrm{diag}\,[1, -1, -1, \ldots, -1] = \mathrm{diag}\,[-1, 1, -1, \ldots, -1]Q'$, откуда ясно, что матрица A имеет ненулевой лишь побочную диагональ. После того, как мы подходящим образом растянем первый вектор базиса, получим, что $Q' \sim Q_{1,2}$. Значит, все элементарные матрицы отображаются тождественно, т. е. автоморфизм Φ' тождественен.

2.3.5 Группы $\mathrm{PSL}_{2m}(K)$ и $\mathrm{PSL}_{2m}(L)$ при $\mathrm{char}\, K, L \neq 2$.

Продолжая индукцию и рассуждения, аналогичные предыдущим, мы придем к той же самой ситуации. В данном случае надо будет рассматривать инволюцию $\mathrm{diag}\,[-1, -1, 1, \ldots, 1]$, после чего показывать, что инволюция $\mathrm{diag}\,[1, -1, -1, 1, \ldots, 1]$ также перейдет в себя, а далее (с помощью растяжения первых двух элементов базиса) переводить в себя матрицу $Q_{2,3} = E - E_{2,2} - E_{3,3} + E_{2,3} - E_{3,2}$.

2.3.6 Группы $\mathrm{PSL}_n(K)$ и $\mathrm{PSL}_m(L)$ при $\mathrm{char}\, K = 2$ и $\mathrm{char}\, L \neq 2$.

Если в поле K бесконечно много элементов, то в группе $\mathrm{PSL}_n(K)$ существует бесконечно много попарно коммутирующих инволюций — это всевозможные элементы вида $E + \alpha E_{1,2}$, $\alpha \in K$. С другой стороны, в группе $\mathrm{PSL}_m(L)$ не может найтись бескнечного числа попарно коммутирующих инволюций, так как они все должны быть диагональны в одном базисе (расширения поля), т. е. их не может быть более $m2^{m-1}$ (с учетом единичного определителя).

Таким образом, мы можем заведомо считать, что если $\mathrm{PSL}_n(K) \cong \mathrm{PSL}_m(L)$, то обязательно оба поля конечны. Пусть $|K| = 2^k$, $|L| = p^l$, $p > 2$.

Теперь рассмотрим множество $\{E + \alpha_1 E_{1,2} + \alpha_2 E_{1,3} + \cdots + \alpha_{n-1} E_{1,n} \mid \alpha_1, \ldots, \alpha_{n-1} \in K\}$ инволюций в группе $\mathrm{PSL}_n(K)$. Ясно, что это максимальное множество попарно коммутирующих инволюций (если некоторая матрица $A = (a_{ij})$ коммутирует со всеми этими инволюциями, то она коммутирует со всеми $E_{1,i}$, $i \neq 1$. Это означает $\sum_{j=1}^{n} a_{i,j} E_{1,j} = \sum_{k=1}^{n} a_{k,1} E_{k,i}$ для любого $i \neq 1$. Ясно, это означает, что $a_{1,1} = a_{i,i}$ для всех $i \neq 1$, кроме того, $a_{i,j} = 0$ для всех $i \neq j$, $i \neq 1$. Это и означает, что других инволюций не добавится.)

При этом заметим, что все рассматриваемые инволюции имеют жорданову форму $E + E_{1,2}$, т. е. сопряжены между собой. Значит, в группе $\mathrm{PSL}_n(K)$ существует максимальное множество инволюций, при этом состоящее только из сопряженных друг другу инволюций.

Ясно, что такое свойство не может выполняться в группе $\mathrm{PSL}_m(L)$, так как все инволюции там будут иметь в каком-то базисе диагональный вид (и их попарные произведения будут иметь разные жордановы формы).

Исключением могут служить только размерности два, три или четыре, в которых инволюции имеют только один вид.

Однако в размерности три попарно коммутирующих сопряженных инволюций всего три (с единицей их четыре), поэтому должно быть $|K| \cdot (n-1) = 4$, что не получается просто из перебора.

В размерности два максимально сопряженных инволюций может быть четыре в случае $\sqrt{-1} = i \in L$, тогда можно рассмотреть матрицы $\mathrm{diag}\,[i, -i]$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Ясно, что больше коммутирующих сопряженных инволюций в этом множестве не будет, поэтому снова $|K| \cdot (n-1) = 4$. Прямой проверкой получим, что возможна ситуация $\mathrm{PSL}_3(\mathbb{F}_2)$, а больше никаких.

Рассмотрение размерности четыре оставим в качестве упражнения (см. упражнение!!!).

2.3.7 Упражнения.

1. Выразите все свойства, описываемые в лемме 2.16, в виде формул первого порядка.

Определение 2.2. Две группы (два кольца) G и H называются *элементарно эквивалентными*, если для любого предложения φ (формулы без свободных переменных) языка теории групп (теории колец) φ истинно в группе (кольце) G тогда и только тогда, когда оно истинно в H.

2. Докажите, что если две группы конечны, то их элементарная эквивалентность равносильна изоморфности.

3. Приведите пример а) двух групп, б) двух колец, в) двух полей, которые были бы элементарно эквивалентны, но не изоморфны друг другу.

4. Докажите, что если поля K, L имеют характеристику отличную от двух, то группы $\mathrm{PSL}_n(K)$ и $\mathrm{PSL}_m(L)$ не могут быть элементарно эквивалентны.

5. Подробно проведите описание изоморфизмов между группами $\mathrm{PSL}_{2n}(K)$ и $\mathrm{PSL}_{2n}(L)$, где $n > 2$, $\mathrm{char}\, K, L \neq 2$.

6. Покажите строго, что группа $\mathrm{PSL}_4(L)$, $\mathrm{char}\, L \neq 2$, не может быть изоморфна группе $\mathrm{PSL}_n(K)$, $\mathrm{char}\, K = 2$.

7*. Докажите, что если для полей K, L характеристики, отличной от двух, группы $\mathrm{PSL}_n(K)$ и $\mathrm{PSL}_m(L)$ элементарно эквивалентны, то $n = m$ и поля K и L элементарно эквивалентны.

2.4 Лекция 6.

2.4.1 Группы $\mathrm{PSL}_n(K)$ и $\mathrm{PSL}_m(L)$ при $\mathrm{char}\, K, L = 2$.

В этом параграфе всегда поля L и K имеют характеристику два.

Лемма 2.17. *В группе $\mathrm{PSL}_n(K)$ любой элемент порядка 2^{n-1} в некотором базисе имеет вид*

$$E_{\max} = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

(одна жорданова клетка размера $n \times n$ со значением 1). Элементов порядка 2^n в рассматриваемой группе не существует.

Доказательство. Если некоторый элемент $\overline{A}$ имеет порядок 2^{n-1}, то в группе $\mathrm{SL}_n(K)$ любой его представитель A обладает свойством $A^{2^n} = \lambda E$, $\lambda^n = 1$. В любом случае все собственные значения оператора A совпадают и равны $\mu = \sqrt[2^{n-1}]{\lambda}$ (таких корней не более одного). Ясно, что мы можем предполагать n нечетным (так как если $\lambda^{2k} = 1$, то $\lambda^k = 1$). В этом случае мы можем найти такие p и q, что $2^{n-1} \cdot p = n \cdot q + 1$. Таким образом, $\mu = \lambda^p$, поэтому $\mu \in K$. Значит, матрицу A можно привести к жордановой форме прямо над полем K. Будем считать, что матрица A уже имеет жорданову форму, а после деления матрицы на μ все ее собственные значения равны 1. После этого мы видим, что порядок такой матрицы равен 2^{k-1}, где k — размер максимальной ее клетки. Отсюда очевидно следуют оба утверждения леммы. □

Теперь мы можем быть уверены, что если $\mathrm{PSL}_n(K) \cong \mathrm{PSL}_m(L)$, то $n = m$.

Лемма 2.18. *При изоморфизме $\Phi : \mathrm{PSL}_n(K) \to \mathrm{PSL}_n(L)$ матрица $E + E_{1,2}$ переходит в матрицу, которая в некотором базисе имеет тот же вид.*

Доказательство. Утверждение леммы очевидно следует из того, что матрицы с жордановой формой $E + E_{1,2}$, и только они, являются 2^{n-2}-ми степенями матриц порядка 2^{n-1}. □

Назовем матрицы, сопряженные к $E + E_{1,2}$, *элементарными трансвекциями*.

Как устроена каждая такая трансвекция A? Для A существует разложение пространства $V = V_0 \oplus l_0$ и прямая $l_1 \in V_0$, такие, что на подпространстве V_0 оператор A действует тождественно, а к вектору $v_0 \in l_0$ он прибавляет вектор $v_1 \in l_1$. Заметим, что вектор v_1 и подпространство V_0 определены однозначно, а вот прямую l_0 можно выбирать произвольно вне V_0.

Лемма 2.19. *Две трансвекции σ и σ' (с соответствующими l_0, V_0, l_1 и l'_0, V'_0, l'_1) коммутируют тогда и только тогда, когда либо либо $V_0 = V'_0$, либо $l_0, l_1 \in V'_0$, $l'_0, l'_1 \in V_0$.*

Доказательство. Если $v_0 \in V_0$, то $\sigma' \circ \sigma(v_0) = \sigma'(v_0) = \sigma(\sigma'(v_0))$. Значит, $\sigma'(v_0) \in V_0$, т. е. подпространство V_0 инвариантно для оператора σ'. Точно так же подпространство V_0' инвариантно для оператора σ. Значит, либо $V_0 = V_0'$, либо $l_0, l_1 \in V_0'$, $l_0', l_1' \in V_0$.

Если $V_0 = V_0'$, то для любого $v \in V_0$ имеем $\sigma\sigma'(v) = \sigma'\sigma(v) = v$, для $v_0 \in l_0$ имеем $v_0 = v_0' + u$, где $u \in V_0$, поэтому $\sigma' \circ \sigma(v_0) = \sigma'(v_0 + v_1) = \sigma'(v_0) + v_1 = \sigma'(v_0') + u + v_1 = v_0' + v_1' + u + v_1 = v + 0 + v_1 + v + 1'$. С другой стороны, $\sigma \circ \sigma'(v_0) = \sigma(v_0 + v_1') = v_0 + v_1 + v_1'$. Значит, совпадения подпространств V_0 и V_0' достаточно для коммутирования σ и σ'.

Если $l_0, l_1 \in V_0'$, $l_0', l_1' \in V_0$, то для любого вектора $v \in V_0$ имеем $\sigma'\sigma(v) = \sigma'(v) \in V_0$, поэтому $\sigma\sigma'(v) = \sigma'(v)$. Для вектора $v_0 \in l_0$ имеем $\sigma'\sigma(v_0) = \sigma'(v_0 + v_1) = v_0 + v_1 = \sigma(v_0) = \sigma\sigma'(v_0)$, так как $v_0, v_1 \in V_0'$. Значит, мы нашли необходимые и достаточные условия коммутирования. □

Условия коммутирования двух трансвекций из леммы 2.19 на самом деле равносильны более простому условию $l_1 \in V_0'$, $l_1' \in V_0$ (см. упражнение 1).

В матричной форме доказанная лемма означает, что любая трансвекция σ, коммутирующая с трансвекцией $E + E_{1,2}$, может в некотором базисе, в котором $E + E_{1,2}$ не изменится, иметь вид либо $E + \alpha E_{1,2}$ ($l_1 = l_1'$ и $V_0 = V_0'$), либо $E + E_{1,3}$ ($l_1 = l_1'$, но $V_0 \neq V_0'$), либо $E + E_{3,2}$ ($V_0 = V_0'$, но $l_1 \neq l_1'$), либо $E + E_{3,4}$ ($l_1 \neq l_1'$ и $V_0 \neq V_0'$).

Первый случай (в алгебраическом смысле) отличается от остальных тем, что σ коммутирует со всеми трансвекциями, с которыми коммутирует исходная трансвекция $E + E_{1,2}$. Четвертый случай отличается от предыдущих двух тем, что произведение трансвекции $E + E_{1,2}$ с трансвекцией σ уже само не будет трансвекцией. Отсюда следует

Лемма 2.20. *Можно так изменить базис в пространстве L^n, что при изоморфизме $\Phi : \mathrm{PSL}_n(K) \to \mathrm{PSL}_n(L)$ будет иметь место $\Phi(E + E_{1,2}) = E + E_{1,2}$ и либо $\Phi(E + E_{1,3}) = E + E_{1,3}$, либо $\Phi(E + E_{1,3}) = E + E_{3,2}$.*

Если оказалось, что $\Phi(E + E_{1,3}) = E + E_{3,2}$, то возьмем композицию изоморфизма Φ с заменой базиса с помощью матрицы $Q_{1,2} = E = E_{1,1} - E_{2,2} + E_{1,2} - E_{2,1}$ и контрградиентного автоморфизма группы $\mathrm{PSL}_n(L)$. Тогда в любом случае придем к первому случаю $\Phi(E + E_{1,2}) = E + E_{1,2}$ и $\Phi(E + E_{1,3}) = E + E_{1,3}$.

Если добавить к данным двум трансвекциям $\sigma_1 = E + E_{1,2}$ и $\sigma_2 = E + E_{1,3}$ третью трансвекцию σ_3, коммутирующую с ними и такую, что любое из произведений $\sigma_1\sigma_3$ и $\sigma_2\sigma_3$ является трансвекцией, то в некотором базисе (в котором σ_1, σ_2 имеют прежний вид) трансвекция σ_3 будет иметь вид $E + E_{1,4}$. Продолжая так далее, придем к ситуации $\Phi(E + E_{1,i}) = E + E_{1,i}$ для любого $i \neq 1$.

Лемма 2.21. *Трансвекция σ, коммутирующая со всеми $E + E_{1,i}$, $3 \leqslant i \leqslant n$, и удовлетворяющая условию $(E + E_{1,2})\sigma = \sigma(E + E_{1,2} + E_{1,3})$, в рассматриваемом базисе имеет вид $E + E_{2,3} + aE_{1,3}$.*

Доказательство. Так как трансвекция σ коммутирует со всеми $E + E_{1,i}$, $3 \leqslant i \leqslant n$, то общая вычетная прямая $\langle e_1 \rangle$ всех рассматриваемых трансвекций должна содержаться в вычетном пространстве V_0 транвекции σ, откуда следует, что $\sigma(e_1) = e_1$. С другой стороны, пересечение всех вычетных пространств трансвекций $E + E_{1,i}$, $3 \leqslant i \leqslant n$, должно содержать вычетную прямую l_1 трансвекции σ, откуда следует, что $l_1 \subset \langle e_1, e_2 \rangle$.

Таким образом, матрица σ имеет вид

$$\begin{pmatrix} 1 & a_2 & a_3 & \dots & a_n \\ 0 & 1 & b_3 & \dots & b_n \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Теперь воспользуемся соотношением $(E + E_{1,2})\sigma = \sigma(E + E_{1,2} + E_{1,3})$: с одной стороны,

$$\begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 & a_3 & \dots & a_n \\ 0 & 1 & b_3 & \dots & b_n \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_2 + 1 & a_3 + b_3 & \dots & a_n + b_n \\ 0 & 1 & b_3 & \dots & b_n \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

с другой стороны,

$$\begin{pmatrix} 1 & a_2 & a_3 & \dots & a_n \\ 0 & 1 & b_3 & \dots & b_n \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 + 1 & a_3 + 1 & \dots & a_n \\ 0 & 1 & b_3 & \dots & b_n \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Таким образом, $b_3 = 1$, $b_4 = \dots = b_n = 0$. Однако, $\sigma - E$ должна быть матрицей ранга один, поэтому $a_2 = a_4 = \dots = a_n = 0$. Лемма доказана. □

Из доказанной леммы очевидно следует, что $\Phi'(E + E_{2,3}) = E + a_2E_{1,3} + E_{2,3}$. После замены базиса с помощью матрицы $E+a_2E_{1,2}$ (данная замена базиса коммутирует со всеми матрицами $E + E_{1,i}$) получим $\Phi'(E + E_{2,3}) = E + E_{2,3}$.

Точно так же легко показать, что $\Phi'(E + E_{3,4}) = E + E_{3,4} + \alpha E_{1,4}$ (так как матрица $E + E_{3,4}$ является трансвекцией, коммутирует со всеми $E + E_{1,i}$, кроме $E + E_{1,3}$, и плюс к этому удовлетворяет соотношению $(E + E_{1,3})(E + E_{3,4}) = (E + E_{3,4})(E + E_{1,3} + E_{1,4})$). После этого добавим замену базиса с помощью матрицы $E + \alpha E_{1,3}$ (коммутирующей со всеми $E + E_{1,i}$ и с $E_{2,3}$), получим $\Phi'(E + E_{3,4}) = E + E_{3,4}$. Так мы можем в результате, домножая изоморфизм Φ' на замены базиса в пространстве L^n, прийти к изоморфизму Φ'', для которого $\Phi''(E+E_{1,i}) = E_{1,i}$, $2 \leqslant i \leqslant n$, $\Phi''(E+E_{i,i+1}) = E+E_{i,i+1}$, $1 \leqslant i < n$. Благодаря тому, что $[E + E_{i,j}, E + E_{j,k}] = E + E_{i,k}$ для всех $i, j, k = 1, \dots, n$, получим

$$\Phi''(E + E_{i,j}) = E + E_{i,j} \text{ для всех } 1 \leqslant i < j \leqslant n.$$

Рассмотрим теперь образ трансвекции вида $E + E_{i,j}$, где $i > j$.

Сначала возьмем трансвекцию $E + E_{2,1}$. Пусть $\Phi''(E + E_{2,1}) = \sigma$.

Вычетной прямой l_1 для трансвекции σ является прямая, лежащая в пересечении всех вычетных подпространств всех трансвекций, коммутирующих с σ. Мы знаем, что

с трансвекцией σ коммутируют все матрицы $E + E_{i,j}$, $i < j$, $i \neq 1$, $j \neq 2$. Таковыми являются по крайней мере все матрицы $E + E_{2,3}$, $E + E_{2,4}$, $\ldots$, $E + E_{2,n}$ и $E + E_{3,4}$, $\ldots$, $E + E_{3,n}$. Их вычетными пространствами являются $\langle e_1, e_2, e_4, \ldots, e_n\rangle$, $\langle e_1, e_2, e_3, , e_5 \ldots, e_n\rangle$, $\ldots$, $\langle e_1, e_2, e_3, e_4, \ldots, e_{n-1}\rangle$. Таким образом, пересечением вычетных пространств является плоскость $\langle e_1, e_2\rangle$, поэтому прямая l_1 должна содержаться в этой плоскости. Вычетное пространство трансвекции σ должно содержать все вычетные прямые матриц $E + E_{2,3}$, $E + E_{3,4}$, $\ldots$, $E + E_{n-1,n}$, т. е. все векторы $e_2, e_3, \ldots, e_{n-1}$.

Таким образом,

$$\sigma = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & a_n \\ b_1 & 1 & 0 & \ldots & 0 & b_n \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}.$$

Однако из того, что ранг оператора $\sigma - E$ единичен, сразу получим $a_n = 0$.

Воспользовавшись соотношением $(E + E_{2,1})(E + E_{1,3}) = (E + E_{1,3})(E + E_{2,1})(E + E_{2,3})$, получим

$$(E + b_1E_{2,1} + b_nE_{2,n})(E + E_{1,3}) = (E + E_{1,3})(E + b_1E_{2,1} + b_nE_{2,n})(E + E_{2,3}),$$

откуда $b_1 = 1$. Заметим, что у нас еще осталась одна замена базиса, коммутирующая со всеми матрицами $E + E_{i,j}$, $1 \leqslant i < j \leqslant n$. Именно, это замена базиса с помощью матрицы вида $E + \alpha E_{1,n}$. Произведем замену базиса матрицей $E + b_nE_{1,n}$, получим $\Phi''(E + E_{2,1}) = E + E_{2,1}$.

Ясно, что остается доказать только, что $\Phi''(E + E_{i+1,i}) = E + E_{i+1,i}$ для всех $2 \leqslant i < n$, так как остальные элементарные матрицы вида $E + E_{i,j}$ будут коммутаторами уже найденных.

Действительно, рассмотрим $\sigma' = \Phi''(E + E_{3,2})$. Вычетная прямая данной трансвекции содержится в пересечении вычетных пространств трансвекций $E + E_{1,2}$, $E + E_{1,4}$, $E + E_{1,5}$, $\ldots$, $E + E_{1,n}$. Это, соответственно, гиперплоскости $\langle e_1, e_3, \ldots, e_n\rangle$, $\langle e_1, e_2, e_3, e_5, \ldots, e_n\rangle$, $\langle e_1, e_2, e_3, e_4, e_6, \ldots, e_n\rangle$, $\ldots$, $e_1, e_2, \ldots, e_{n-1}\rangle$, их пересечение есть $\langle e_1, e_3\rangle$. С другой стороны, вычетное пространство трансвекции σ' содержит прямые $\langle e_1\rangle$, $\langle e_3\rangle$, $\langle e_4\rangle$, $\ldots$, $\langle e_{n-1}\rangle$, поэтому $\sigma' = E + a_2E_{1,2} + b_2E_{3,2} + a_nE_{1,n} + b_nE_{3,n}$.

Снова воспользуемся соотношением $(E + E_{1,3})(E + E_{3,2}) = (E + E_{3,2})(E + E_{1,2} + E_{1,3})$, которое для образа дает $(E+E_{1,3})(E+a_2E_{1,2}+b_2E_{3,2}+a_nE_{1,n}+b_nE_{3,n}) = (E+a_2E_{1,2}+b_2E_{3,2}+a_nE_{1,n} + b_nE_{3,n})(E + E_{1,2} + E_{1,3})$, из чего следует $b_2 = 1$ и $b_n = 0$. Так как оператор $\sigma' - E$ имеет единичный ранг, то $a_n = 0$. Таким образом, $\sigma' = E + a_2E_{1,2} + E_{3,2}$. Предположим, что $a_2 = ne0$.

Заметим, что коммутатор $[E + E_{3,2}, E + E_{2,1}] = E + E_{3,1}$ является элементарной трансвекцией. Значит, и коммутатор $[\sigma', E+E_{2,1}]$ является элементарной трансвекцией. Прямым подсчетом получим, что его след равен $a_2^2 + n$, хотя должен быть равен n. Значит, $a_2 = 0$.

Таким образом, при изоморфизме Φ'' все матрицы $E + E_{i,j}$, $i \neq j$ переходят в себя.

Аналогично случаю $\operatorname{char} K \neq 3$ легко показать, что тогда изоморфизм Φ'' является кольцевым (см. упражнение 2).

Теорема доказана.

2.4.2 Упражнения.

1. Докажите, что условия коммутирования двух трансвекций из леммы 2.19 равносильны условию $l_1 \in V_0'$, $l_1' \in V_0$.

2. Докажите, что если изоморфизм $\Phi : \mathrm{PSL}_n(K) \to \mathrm{PSL}_m(L)$ таков, что $\Phi(E + E_{i,j}) = E + E_{i,j}$ для любых $1 \leqslant i, j \leqslant n$, $i \neq j$, то Φ — кольцевой изоморфизм.

3. Останутся ли все рассуждения этого параграфа верными, если поля K и L заменить на тела K и L?

4. Какого наименьшего числа элементарных матриц $E + E_{i,j}$, $i \neq j$, достаточно, чтобы породить (с помощью различных групповых операций) все элементарные матрицы $E+E_{i,j}$, $i \neq j$?

5. Для данной трансвекции $\sigma \in \mathrm{SL}_n(K)$ найдите все матрицы $A \in \mathrm{SL}_n(K)$, удовлетворяющие условию

$$\forall B \in \mathrm{SL}_n(K)\ (B\sigma = \sigma B \Leftrightarrow AB = BA).$$

Глава 3

Нормальная структура линейных групп над коммутативными кольцами.

3.1 Лекция 7.

3.1.1 Формулировка основной теоремы.

Главными объектами для рассмотрения в этой главе будут
— коммутативное кольцо R с единицей,
— общая линейная группа $\mathrm{GL}_n(R)$,
— элементарная подгруппа $E_n(R) = \langle E + rE_{i,j} \mid i \neq j, r \in R \rangle$,
— ее подгруппа $E_I = E_n(R, I) = \langle E + rE_{i,j} \mid i \neq j, r \in I \rangle$ для произвольного идеала I кольца R.

Заметим, что для любого идеала I кольца R естественное отображение $R \to R/I$ индуцирует гомоморфизм

$$\lambda_I : \mathrm{GL}_n(R) \to \mathrm{GL}_n(R/I).$$

Если I — собственный идеал кольца R, то ядро гомоморфизма θ_I является нецентральной нормальной подгруппой группы $\mathrm{GL}_n(R)$, не содержащей группу $\mathrm{SL}_n(R)$.

Обозначим прообраз центра группы $\mathrm{GL}_n(R/I)$ при гомоморфизме λ_I через Z_I.

Через Q_I обозначим нормальное замыкание группы E_I в $E_n(R)$ (наименьшую нормальную подгруппу в $E_n(R)$, содержащую E_I).

Основным результатом этой главы является

Теорема 3.1. *Пусть $n \geqslant 4$. Если подгруппа $\mathcal{H}$ группы $\mathrm{GL}_n(R)$ нормализуется подгруппой $E_n(R)$, то*

$$Q_I \leqslant \mathcal{H} \leqslant Z_I$$

для некоторого однозначно определенного идеала I кольца R.

Данная теорема (и даже гораздо более сильное утверждение, которое мы сейчас не будем формулировать) доказана в работе [16].

3.1.2 Основные леммы.

Определение 3.1. Если $A \in \mathrm{GL}_n(R)$, то *уровнем* $J(A)$ матрицы A назовем идеал кольца R, порожденный всеми $a_{i,j}$, $i \neq j$, и $a_{i,i} - a_{j,j}$. Если $\mathcal{H}$ — подгруппа в $\mathrm{GL}_n(R)$, то уровнем $J(\mathcal{H})$ этой подгруппы назовем сумму идеалов $\sum\limits_{A \in \mathcal{H}} J(\mathcal{H})$.

Лемма 3.1. *Для каждой матрицы $A \in \mathrm{GL}_n(R)$ идеал $J(A)$ является наименьшим идеалом I кольца R, для которого $A \in Z_I$. Благодаря этому свойству $J(BAB^{-1}) = J(A^{-1}) = J(A)$ для любых $A, B \in \mathrm{GL}_n(R)$.*

Доказательство. Очевидно. □

Лемма 3.2. *Если $i \neq j$, $r, s \in R$, то*

$$(E + rE_{i,j})^{-1} = E - rE_{i,j},$$
$$(E + rE_{i,j})(E + sE_{i,j}) = E + (r+s)E_{i,j}.$$

Таким образом, если идеал I в R порождается как аддитивная подгруппа в R элементами множества X, то

$$E_I = \langle E + xE_{i,j} \mid x \in X, i \neq j \rangle.$$

Кроме того, если i, j, k различны, $r, s \in R$, то

$$[E + rE_{i,j}, E + sE_{j,k}] = E + rsE_{i,k}.$$

Доказательство. Очевидная проверка. □

Следующая лемма является основной в доказательстве теоремы.

Лемма 3.3. *Пусть $\mathcal{H}$ — подгруппа группы $\mathrm{GL}_n(R)$, нормализуемая группой $E_n(R)$, $n \geqslant 4$. Обозначим через $J_2(\mathcal{H})$ сумму всех идеалов $J(A)$, где матрицы $A \in \mathcal{H}$ отличаются от единичной матрицы не более, чем в двух столбцах. Тогда $J(\mathcal{H}) = J_2(\mathcal{H})$.*

Доказательство. Очевидно, что $J_2(\mathcal{H}) \subseteq J(\mathcal{H})$. Докажем обратное включение.

Пусть $A \in \mathcal{H}$. Обозначим матрицу A^{-1} через B и рассмотрим $n-1$ уравнение от $n-1$ переменной $x_1, x_3, \ldots, x_n$:

$$\begin{cases} \sum\limits_{r \neq 2} b_{i,r} x_r = 0 \quad (i > 2), \\ \sum\limits_{r \neq 2} b_{2,r} x_r = a_{2,1}. \end{cases} \tag{3.1}$$

Матрица M коэффициентов рассматриваемой системы — это матрица, полученная из матрицы B вычеркиванием первой строки и второго столбца.

Покажем, что система уравнений (3.1) имеет решение

$$x_i = -(\det A)M_{2,i} \quad (i = 1, 3, \ldots, n),$$

где $M_{2,i}$ — это алгебраические дополнения элементов $m_{2,i}$ матрицы M с нумерацией строк и столбцов, унаследованной от матрицы B.

Действительно, благодаря фальшивому разложению, если $i > 2$, то

$$\sum_{r\neq 2} m_{i,r}M_{2,r} = 0,$$

а из разложения по второй строке (соответственно, в матрице M это первая строка)

$$\sum_{r\neq 2} m_{2,r}M_{2,r} = \det M.$$

Однако элемент $-\det M$ является алгебраическим дополнением к элементу $b_{1,2}$ матрицы B, по формуле обратной матрицы $a_{2,1} = -\det M/\det B$, откуда $\det M = -a_{2,1}(\det B) = -a_{2,1}/\det A$, что и требовалось.

Рассмотрим

$$C = E + \sum_{r\neq 2} x_r E_{r,2} = \prod_{r\neq 2}(E + x_r E_{r,2}).$$

Тогда $C \in E_n(R)$, а группа $\mathcal{H}$ содержит элемент

$$D = [A, C] = B\left(E - \sum_{r\neq 2} x_r E_{r,2}\right) A\left(E + \sum_{r\neq 2} x_r E_{r,2}\right) = \\ = E + \sum_{s\neq 2} x_s E_{s,2} - \sum_{r\neq 2} x_r B E_{r,2} A - \sum_{r,s\neq 2} x_r x_s B E_{r,2} A E_{s,2}.$$

Рассмотрим

$$\sum_{r\neq 2} x_r B E_{r,2} = \sum_{r\neq 2} x_r \left(\sum_{i,j} b_{i,j} E_{i,j} E_{r,2}\right) = \sum_{r\neq 2} x_r \left(\sum_{i=1}^{n} b_{i,r} E_{i,2}\right) = \sum_{i=1}^{n} \left(\sum_{r\neq 2} x_r b_{i,r}\right) E_{i,2}.$$

Так как по (3.1) имеет место $\sum\limits_{r\neq 2} x_r b_{i,r} = 0$ при $i > 2$, то $(D - E)_{i,j} = x_i \delta_{2,j}$ для $i > 2$, поэтому

$$(D - E)_{i,j} = 0 \text{ для } i > 2 \text{ и } j \neq 2. \tag{3.2}$$

Теперь пусть $J'(D)$ обозначает идеал кольца R, порожденный элементами $(D - E)_{2,j}$, $j = 1, 2, \ldots, n$. В силу того, что $d_{3,3} = 1$, получим $J'(D) \subseteq J(D)$. Однако напрямую из формулы (для расписывания удобнее отдельно взять $j = 2$ и $j \neq 2$) имеем

$$(D - E)_{2,j} = -a_{2,1}\left(a_{2,j} + \sum_{s\neq 2} x_s a_{2,s}\delta_{2,j}\right),$$

поэтому $a_{2,1}a_{2,j} \in J'(D)$ для всех $j \neq 2$, следовательно, $a_{2,1}x_s a_{2,s} \in J'(D)$ для всех $s \neq 0$, т. е. $a_{2,1}\sum\limits_{s\neq 2} x_s a_{2,s} \in J'(D)$, и в результате $a_{2,1}a_{2,j} \in J'(D)$ для всех j. Так как

$$a_{2,1} = a_{2,1} \cdot 1 = a_{2,1}\sum_{j=1}^{n} a_{2,j}b_{j,2},$$

то $a_{2,1} \in J'(D)$.

Выберем теперь различные целые числа $r, s \leqslant n$, $s > 2$, и матрицу $T = D^{-1}$.

Матрица

$$F_{r,s} = [D, E + E_{r,s}] = E + E_{r,s} - TE_{r,s}D - TE_{r,s}DE_{r,s}$$

лежит в рассматриваемой группе $\mathcal{H}$.

Найдем $(F_{r,s} - E)_{i,j}$. Рассматриваемый коэффициент равен

$$\delta_{i,r}\delta_{j,s} - t_{i,r}d_{s,j} - t_{i,r}d_{s,r}\delta_{s,j}.$$

Так как при $s > 2$, $j \neq 2$, $d_{s,j} = \delta_{s,j}$, то

$$(F_{r,s} - E)_{i,j} = -\delta_{j,s}(t_{i,r} - \delta_{i,r}) - d_{s,2}\delta_{j,2}t_{i,r} - d_{s,2}\delta_{r,2}t_{i,r}\delta_{s,j}.$$

Значит, матрица $F_{r,s}$ отличается от единичной только во втором и s-м столбцах.

Так как $n \geqslant 4$, то можно для любых данных r и i взять $s > 2$ такое, что $s \neq r$. Тогда при $j = 2$ элемент $(F_{r,s} - E)_{i,2} = d_{s,2}t_{i,r}$ содержится в идеале $J_2(\mathcal{H})$, а если мы выберем $s = j$, то получим $(F_{r,s} - E)_{i,j} = -(t_{i,r} - \delta_{i,r}) - d_{s,2}t_{i,r}\delta_{r,2} \in J_2(\mathcal{H})$, поэтому $t_{i,r} - \delta_{i,r} \in J_2(\mathcal{H})$ для любых i и r. Таким образом, $J(T) \subseteq J_2(\mathcal{H})$. Так как по лемме 3.1 $J(T) = J(D)$, то

$$a_{2,1} \in J'(D) \subseteq J(D) = J(T) \subseteq J_2(\mathcal{H}).$$

Ясно, что изначально вместо $a_{2,1}$ можно было выбрать любое $a_{i,j}$, $i \neq j$. Значит, $a_{i,j} \in J_2(\mathcal{H})$ для всех $i \neq j$.

Кроме того, из

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_{1,1} + a_{2,1} & a_{1,2} - a_{2,1} + a_{2,2} - a_{1,1} \\ a_{2,1} & a_{2,2} - a_{2,1} \end{pmatrix}$$

мы видим, что если $a_{i,j}, a_{j,i} \in J_2(\mathcal{H})$, то $a_{i,i} - a_{j,j} \in J_2(\mathcal{H})$.

Значит, $J(A) \subset J_2(\mathcal{H})$ для любой матрицы $A \in \mathcal{H}$. Следовательно, $J(\mathcal{H}) = J_2(\mathcal{H})$.

Лемма доказана. □

3.1.3 Доказательство теоремы.

Ясно, что для построенного нами идеала $I = J(\mathcal{H})$ выполняется включение $\mathcal{H} \subseteq Z_I$.

Нам остается доказать включение $E_I \subseteq \mathcal{H}$.

Обозначим через $J_1(\mathcal{H})$ сумму всех идеалов $J(A)$, где $A \in \mathcal{H}$ отличается от тождественной матрицы ровно в одной строке.

Предположим, что $B \in \mathcal{H}$ и $b_{i,j} = \delta_{i,j}$ для $j > 2$ (т. е. B — это матрица, у которой только два первых столбца отличны от единичной матрицы). Рассмотрим различные r и s такие, что $r > 2$. Рассмотрим элемент

$$D_{r,s} = [B, E + E_{r,s}] \in \mathcal{H}.$$

Тогда, как и выше,

$$D_{r,s} = E + E_{r,s} - B^{-1}E_{r,s}B(E + E_{r,s}).$$

Так как $(B^{-1})_{i,j} = b_{i,j} = \delta_{i,j}$ для $j > 2$ (у обратной матрицы тоже только два первых столбца отличны от столбцов единичной матрицы), то

$$(D_{r,s} - E)_{i,j} = -\delta_{i,r}(b_{s,j} - \delta_{s,j})$$

для всех i, j, поэтому у матрицы $D_{r,s}$ только первая строка отлична от строк единичной матрицы, откуда получим, что $(b_{s,j} - \delta_{s,j}) \in J_1(\mathcal{H})$ для каждого j. Так как $n \geqslant 4$, то для любых индексов j и s всегда можно выбрать $r \neq s$, $r > 2$, поэтому $J(B) \subseteq J_1(\mathcal{H})$.

Теперь понятно, что $J_2(\mathcal{H}) \subseteq J_1(\mathcal{H})$, откуда $I = J(\mathcal{H}) = J_2(\mathcal{H}) = J_1(\mathcal{H})$.

Теперь предположим, что $A \in \mathcal{H}$, матрица A отличается от единичной только в r-ой строке. Пусть i, j и t — произвольные индексы, $i \neq j$. Выберем еще индекс s, не совпадающий с i, r, t. Тогда группа $\mathcal{H}$ содержит

$$[E + E_{t,s}, A^{-1}] = E + (a_{r,t} - \delta_{r,t})E_{r,s}.$$

Значит,

$$E_{J(A)} \subseteq \mathcal{H},$$

что нам и требовалось. □

3.1.4 Упражнения.

1. Приведите пример коммутативного кольца R и подгруппы $\mathcal{H}$ в $\mathrm{GL}_n(R)$, нормализуемой группой $E_n(R)$, но не нормальной в $\mathrm{GL}_n(R)$.

2. С помощью основной теоремы этой лекции опишите в точности все нормальные подгруппы группы $\mathrm{GL}_n(\mathbb{Z})$, $\mathrm{GL}_n(\mathbb{Z}[x])$.

3. Приведите пример кольца R, для которого теорема не будет верна при
а) $n = 2$;
б)* $n = 3$.

4. Докажите аналогичную теорему для произвольного тела $\mathbb{F}$.

Глава 4

Основная теорема.

4.1 Лекция 8.

4.1.1 Теоремы Нётер об изоморфизме.

Нам понадобятся две теоремы об изоморфизме (см. [9]), первая из которых является аналогом формулы $(A/K)/(B/K) = A/B$ для обычных числовых дробей, вторая — законом сокращения для групп

$$(AB/B) \cong (A \cap AB)/(A \cap B) = A/(A \cap B).$$

Предложение 4.1. (Теорема о соответствии). *Пусть $f : A \to A'$ — сюръективный гомоморфизм групп. Пусть B — подгруппа группы A, $B' = f(B)$. Тогда соответствие $\widetilde{f} : B \mapsto B'$ является биективным отображением между подгруппами группы A, содержащими ядро $\ker f$, и множеством подгрупп группы A.*

Пусть B и K — нормальные подгруппы группы A, $K \subseteq B$. Тогда отображение

$$\begin{cases} A/K \to A/B \\ aK \mapsto aB \end{cases}$$

является гомоморфизмом групп с ядром $\{aK \mid a \in B\}$, и следующая диаграмма с точными строками, где α — канонический гомоморфизм, коммутативна:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & A & \longrightarrow & A/B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B/K & \longrightarrow & A/K & \longrightarrow & A/B & \longrightarrow & 0 \end{array}$$

Доказательство. Пусть S — множество подгрупп группы A, содержащих $\ker f$, S' — множество подгрупп группы A'. Очевидно, что $\widetilde{f}$ — отображение из S в S'. Ясно, что $\widetilde{f}(f^{-1}(Y)) = Y$ для любой подгруппы $Y \subseteq A'$. Значит, отображение $\widetilde{f}$ сюръективно.

Если B_1, B_2 — подгруппы в A, содержащие $\ker f$, и такие, что $\widetilde{f}(B_1) = \widetilde{f}(B_2) = B' \subseteq A'$, то рассмотрим $b_1 \in B_1 \setminus B_2$, тогда $b = f(b_1) \in B'$, поэтому существует $b_2 \in B_2$ такое, что $f(b_2) = b$. Значит, $b_1 b_2^{-1} \in \ker f$. Так как $\ker f \subseteq B_2$, то $b_1 \in B_2$. Таким образом, отображение $\widetilde{f}$ инъективно, что и требовалось.

Остальные утверждения теоремы очевидны. □

Предложение 4.2. (Первая теорема Нётер об изоморфизме). *Если $f : A \to A'$ — сюръективный гомоморфизм групп, N — нормальная подгруппа группы A, содержащая $\ker f$, то существует единственный изоморфизм $f' : A/N \to A'/f(N)$, называемый изоморфизмом, индуцированным гомоморфизмом f, который замыкает диаграмму*

$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha'} \\ A/N & \xrightarrow[f']{} & A'/f(N) \end{array}$$

где α и α' — канонические гомоморфизмы. В частности, f индуцирует изоморфизм $A/\ker f \cong A'$.

Доказательство. Рассмотрим $g = \alpha' f : A \to A'/f(N)$, где α' — канонический гомоморфизм. Благодаря теореме о соответствии следующие утверждения эквивалентны: (1) $a \in \ker g$; (2) $f(a) \in f(N)$; (3) $a \in N$. Значит, $\ker g = N$. В силу теоремы о соответствии существует $f' : A/N \to A'/f(N)$ такое, что $f'\alpha = g$. В сумме мы получаем нужную коммутативную диаграмму. □

Следствие 4.1. *Пусть $A \supseteq B \supseteq N$ — группы, а B и N — нормальные подгруппы в A. Тогда существует изоморфизм $A/B \to (A/N)/(B/N)$, дополняющий диаграмму*

$$\begin{array}{ccccc} 0 & & 0 & & \\ \downarrow & & \downarrow & & \\ B & \xrightarrow{\alpha} & B/N & \longrightarrow & 0 \\ {\scriptstyle i}\downarrow & & \downarrow & & \\ A & \xrightarrow{\beta} & A/N & \longrightarrow & 0 \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\delta} & & \\ A/B & \longrightarrow & (A/N)/(B/N) & \longrightarrow & 0 \end{array}$$

где i — вложение, а $\alpha, \beta, \gamma, \delta$ — канонические гомоморфизмы.

Предложение 4.3. (Вторая теорема Нётер об изоморфизме). *Если A и B — подгруппы группы G, причем B нормальна, то $AB = \{ab \mid a \in A, b \in B\}$ — подгруппа группы G и $A \cap B$ — нормальная подгруппа в A. Отображение $A \to AB/B$, индуцированное каноническим*

отображением $G \to G/B$, называется каноническим, а его ядро равно $A \cap B$. Таким образом,

$$\gamma : \begin{cases} A/(A \cap B) \to AB/B \\ a(A \cap B) \mapsto ab \end{cases}$$

является изоморфизмом, и существует коммутативная диаграмма с точными строками и столбцами

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A \cap B & \xrightarrow{i} & A & \xrightarrow{\alpha} & A/(A \cap B) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle l} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & B & \xrightarrow[k]{} & AB & \xrightarrow[\beta]{} & AB/B & \longrightarrow & 0 \\ & & & & & & \downarrow & & \\ & & & & & & 0 & & \end{array}$$

где i, j, l, k — гомоморфные вложения, а α и β — канонические гомоморфизмы.

Доказательство. Каждый элемент в AB/B имеет вид aB для некоторого $a \in A$. Поэтому отображение $A \to AB/B$, состоящее в переходе к смежному классу, является гомоморфным наложением, а его ядро совпадает с $A \cap B$. Тогда аналогично определяемое отображение $A/(A \cap B) \to AB/B$ дополняет диаграмму. □

4.1.2 Формулировка основных шагов доказательства.

Если R — кольцо, I — его идеал, то через $\lambda_I : \mathrm{GL}_n(R) \to \mathrm{GL}_n(R/I)$ будем обозначать гомоморфизм, получающийся при сопоставлении каждому элементу матрицы $A \in \mathrm{GL}_n(R)$ ее образа при естественном гомоморфизме $R \to R/I$.

Напомним, что через Z_I мы обозначаем прообраз центра группы $\mathrm{GL}_n(R/I)$ при гомоморфизме λ_I.

Определение 4.1. Пусть C_I обозначает группу $Z_I \cap E_n(R)$, $N_I = \ker \lambda_I \cap E_n(R)$.

Предложение 4.4. *Пусть Φ — произвольный автоморфизм группы $E_n(R)$, I — максимальный идеал кольца R. Тогда существует максимальный идеал J кольца R такой, что $\Phi(N_I) = N_J$.*

Доказательство. Очевидно, что группа C_I нормальна в группе $E_n(R)$. В прошлой главе мы показали, что для такой подгруппы G в $\mathrm{GL}_n(R)$ которая нормализуется группой $E_n(R)$ выполняется включение

$$E_I \subseteq G \subseteq Z_I,$$

откуда следует, что подгруппы вида C_I, и только они, являются максимальными нормальными подгруппами группы $E_n(R)$. Таким образом, для максимального идеала I кольца R существует максимальный идеал J кольца R такой, что $\Phi(C_I) = C_J$. Покажем, что $\Phi(N_I) = N_J$.

Рассмотрим группу $G = E_n(R)/C_I = E_n(R)/(Z_I \cap E_n(R))$. По второй теореме об изоморфизме эта группа естественно изоморфна группе $E_n(R) \cdot Z_I/Z_I$. Теперь воспользуемся первой теоремой об изоморфизме (точнее, следствием из нее), для чего профакторизуем обе части по C_I.

В результате получим $E_n(R/I) \cdot Z(\mathrm{GL}_n(R/I))/Z(\mathrm{GL}_n(R/I))$. Заметим, что так как элементарные матрицы над полем порождают всю группу SL, то $E_n(R/I) \cong \mathrm{SL}_n(R/I)$. Кроме того, снова воспользуемся второй теоремой об изоморфизме, получим, что $G \cong \mathrm{SL}_n(R/I)/(\mathrm{SL}_n(R/I) \cap Z(\mathrm{GL}_n(R/I)) \cong \mathrm{PSL}_n(R/I)$. Таким образом, $E_n(R)/C_I \cong \mathrm{PSL}_n(R/I)$.

Так как $\Phi(C_I) = C_J$, то автоморфизм Φ индуцирует изоморфизм $\overline{\Phi}$ групп $E_n(R)/C_I \cong \mathrm{PSL}_n(R/I)$ и $E_n(R)/C_J \cong \mathrm{PSL}_n(R/J)$ такой, что диаграмма

$$\begin{array}{ccc} E_n(R) & \xrightarrow{\Phi} & E_n(R) \\ \downarrow & & \downarrow \\ \mathrm{PSL}_n(R/I) & \xrightarrow{\overline{\Phi}} & \mathrm{PSL}_n(R/J) \end{array}$$

коммутативна. Изоморфизмы групп PSL_n, $n \geqslant 4$, над полями мы описали в главе 2. Получается, что поля R/I и R/J изоморфны (обозначим соответствующий изоморфизм через δ), и возможны два случая: $\overline{\Phi}(A) = i_{\overline{g}}\overline{\delta}(A)$, либо $\overline{\Phi}(A) = i_{\overline{g}}\overline{\Lambda}(\overline{\delta}(A))$ для любого представителя $A \in \mathrm{PSL}_n(R/I)$, $g \in \mathrm{GL}_n(R/J)$, $\overline{g}$ — представитель элемента g в группе $\mathrm{PGL}_n(R/J)$, Λ — контрградиентный автоморфизм группы $\mathrm{GL}_n(R/J)$.

Так как контрградиентный автоморфизм группы $\mathrm{PSL}_n(R/J)$ поднимается до контрградиентного автоморфизма группы $E_n(R)$, а последний группу N_J переводит в себя, то достаточно рассмотреть первый случай.

Получается, что в группе $E_n(R)$ выполняется равенство

$$\lambda_J\Phi(E + \lambda E_{i,j}) = g(E + \delta(x + I)E_{i,j})g^{-1}c, \quad c \in Z(E_n(R/J)).$$

Так как $E + xE_{i,j} = [E + xE_{i,k}, E + E_{k,j}]$, то центральный элемент c исчезает из образа. Таким образом, получается, что

$$\lambda_J\Phi(E + \lambda E_{i,j}) = g(E + \delta(x + I)E_{i,j})g^{-1}.$$

Пусть теперь $M = (E + x_1E_{i_1,j_1}) \dots (E + x_kE_{i_k,j_k})$ — произвольный элемент из группы N_I. Тогда

$$\lambda_J\Phi(M) = g(E + \delta(x_1 + I)E_{i_1,j_1}) \dots (E + \delta(x_k + I)E_{i_k,j_k})g^{-1} = g(\overline{\delta}\lambda_I(m))g^{-1} = E.$$

Таким образом, $\Phi(N_I) \subseteq N_J$. Ясно, что включение $\Phi^{-1}(N_J) \subseteq N_I$ доказывается аналогично. Значит, $\Phi(N_I) = N_J$. $\square$

Рассмотрим кольцо R и его максимальный идеал I. Как обычно, кольцо, полученное локализацией R по I, обозначим через R_I, его радикал (он же наибольший идеал) — через $\operatorname{Rad} R_I$. Заметим, что имеется два поля — R/I и $R_I/\operatorname{Rad} R_I$. Кроме того, рассмотрим произвольный $r \in R$. Образ этого элемента в поле R/I — это класс $r + I$. Образ его в локальном кольце R_I — это дробь $r/1$, которая отображается в поле $R_I/\operatorname{Rad} R_I$ как $r/1 + I = (r + I)/1$. Ясно, что существует гомоморфизм $\mu_I : R/I \to R_I/\operatorname{Rad} R_I$, который замыкает соответствующую диаграмму до коммутативной, он отображает каждое $r + I$ в $(r + I)/1$.

Лемма 4.1. *Гомоморфизм $\mu_I : R/I \to R_I/\operatorname{Rad} R_I$, который каждому классу $r+I$, $r \in R$, ставит в соответствие класс $r/1 + \operatorname{Rad} R_I$, является изоморфизмом.*

Доказательство. Покажем, что гомоморфизм μ_I инъективен.

Действительно, если $(r+I)/1 = 0/1$ в кольце $R_I/\operatorname{Rad} R_I$, то $r/1 \in \operatorname{Rad} R_I$ в кольце R_I, т. е. $r \in I$. Но тогда $r + I = 0$ в поле R/I. Значит, гомоморфизм μ_I инъективен.

Теперь докажем сюръективность гомоморфизма μ_I.

Ясно, что для этого нужно показать, что для любого элемента r/s, $r \in R$, $s \in R \setminus I$, существуют элемент $m/t \in \operatorname{Rad} R_I$ (т. е. $m \in I$, $t \in R \setminus I$) и элемент $r' \in R$, что $r/s + m/t = r'/1$ в кольце R_I. Это означает, что $rt + ms = r'ts$. Будем искать необходимые m, t, r' так, чтобы $t = s$. Тогда достаточно будет найти m и r', для которых бы выполнялось равенство $r + m = r's$. Заметим, что пересечение множеств $r + I$ и Rs непусто, так как иначе идеал $I + Rs$ не содержал бы элемента r, поэтому являлся бы собственным идеалом кольца R, содержащим максимальный идеал I, что невозможно. Значит, существуют элементы $m \in I$ и $r' \in R$ такие, что $r + m = r's$, что и требовалось. □

Таким образом, можно обернуть стрелку μ_I в диаграмме

$$\begin{array}{ccc} R & \longrightarrow & R_I \\ {\scriptstyle \lambda_I}\downarrow & & \downarrow{\scriptstyle \lambda_{\operatorname{Rad} R_I}} \\ R/I & \xrightarrow{\mu_I} & R_I/\operatorname{Rad} R_I \end{array}$$

Теперь пусть Φ — произвольный автоморфизм группы $E_n(R)$. Предложение 4.4 дает возможность рассмотреть коммутативную диаграмму

$$\begin{array}{ccc} E_n(R) & \xrightarrow{\Phi} & E_n(R) \\ {\scriptstyle r_I}\downarrow & & \downarrow{\scriptstyle r_J} \\ E_n(R_I) & & E_n(R_J) \\ {\scriptstyle \lambda_{\operatorname{Rad} R_I}}\downarrow & & \downarrow{\scriptstyle \lambda_{\operatorname{Rad} R_J}} \\ E_n(R_I/\operatorname{Rad} R_I) & & E_n(R_J/\operatorname{Rad} R_J) \\ {\scriptstyle s_I}\downarrow & & \downarrow{\scriptstyle s_J} \\ E_n(R/I) & \xrightarrow{\overline{\Phi}} & E_n(R/J) \end{array} \tag{4.1}$$

Группы $E_n(R/I)$ и $E_n(R/J)$ — это просто группы $\mathrm{SL}_n(R/I)$ и $\mathrm{SL}_n(R/J)$ над полями, изоморфизмы над которыми уже описаны на самом деле в главе 2. (Почему описание изоморфизмов между группами $\mathrm{PSL}_n(K)$ и $\mathrm{PSL}_n(L)$, полученное в главе 2, легко переносится на описание изоморфизмов между группами $\mathrm{SL}_n(K)$ и $\mathrm{SL}_n(L)$? См. упражнение 1.)

Оказывается, что поля R/I и R/J изоморфны (как и прежде, обозначим соответствующий изоморфизм через δ), при этом

$$\overline{\Phi}(A) = i_g \circ \Lambda^\varepsilon \delta(A)\ \forall A \in E_n(R/I), \quad \varepsilon = 0, 1,\ g \in \mathrm{GL}_n(R/J).$$

Описание автоморфизмов группы $E_n(R)$ происходит по такой схеме. Кольцо R вкладывается в кольцо $S = \prod R_I$ — декартово произведение всех локальных колец R_I, полученных локализацией кольца R по различным максимальным идеалам I. Обозначим через R_0 кольцо $\prod R_I$, где максимальные идеалы берутся такие, что соответствующее $\varepsilon = 0$, R_1 — такое $\prod R_J$, что идеалы J таковы, что $\varepsilon = 1$. Ясно, что тогда $S = R_0 \oplus R_1$. Пусть в кольце S $a = (1, 0)$, $b = (0, 1)$.

Ясно, что группа $E_n(R)$ вкладывается в группу

$$\mathrm{GL}_n(S) = \mathrm{GL}_n(\prod R_I) = \mathrm{GL}_n(R_0 \oplus R_1) = \mathrm{GL}_n(R_0) \times \mathrm{GL}_n(R_1).$$

Первый шаг. Доказывается, что для каждого максимального идеала J выполняется равенство

$$r_J \Phi(E + E_{i,j}) = i_{g_J} \Lambda^\varepsilon r_J(E + E_{i,j}),$$

где $g_J \in \mathrm{GL}_n(R_J)$, $\varepsilon = 0$, если R_J принадлежит R_0, иначе $\varepsilon = 1$.

Второй шаг.

Показывается, что на самом деле идемпотенты a и b содержатся в кольце R, а внутренний автоморфизм группы $\mathrm{GL}_n(S)$, порожденный матрицей $g = \prod g_J$, индуцирует автоморфизм группы $\mathrm{GL}_n(R)$.

4.1.3 Проективные модули над локальными кольцами.

Чтобы доказать результат, нам понадобится лемма Накаямы.

Лемма Накаямы — важная техническая лемма в коммутативной алгебре и алгебраической геометрии, следствие правила Крамера. Она имеет множество эквивалентных формулировок. Вот одна из них:

Лемма 4.2. *Пусть R — коммутативное локальное кольцо с единицей 1, $J = \mathrm{Rad}\, R$, а M — конечно порожденный модуль над кольцом R. Если $JM = M$, то $M = 0$.*

Доказательство. Пусть $m_1, m_2, \ldots, m_n$ — образующие модуля M. Так как $M = JM$, каждый из них представим в виде $m_i = a_{i,1}m_1 + \cdots + a_{i,n}m_n$, где $a_{i,j}$ — элементы идеала J. То есть $\sum\limits_j (\delta_{i,j} - a_{i,j})m_j = 0$. Из формулы Крамера для этой системы следует, что при всяком j

$$\det(\delta_{i,j} - a_{i,j}) \cdot m_j = 0.$$

Так как $\det(\delta_{i,j} - a_{i,j})$ представим в виде $1 - a$, $a \in J$, то данный определитель обратим, поэтому все m_j равны нулю. Таким образом, модуль M — нулевой. Лемма доказана. $\square$

Пусть при предыдущих условиях $\varphi : M \to M/JM$ — гомоморфизм факторизации. Лемма Накаямы дает удобное средство для перехода от модуля M над локальным кольцом R к фактормодулю M/JM, которое есть конечномерное векторное пространство над полем $k = R/J$. Следующее утверждение также считается одной из форм леммы Накаямы, применительно к этому случаю:

Элементы $m_1, m_2, \ldots, m_n \in M$ порождают модуль M тогда и только тогда, когда их образы $\varphi(m_1), \ldots, \varphi(m_n)$ порождают фактормодуль M/JM.

Доказательство. Пусть S — подмодуль в M, порожденный элементами $m_1, m_2, \ldots, m_n$, $Q = M/S$ — фактормодуль и $\pi : M \to Q$ — гомоморфизм факторизации. Так как $\varphi(m_1), \ldots, \varphi(m_n)$ порождают фактормодуль M/JM, это означает, что для всякого $m \in M$ существует $s \in S$, такой что $m - s \in JM$. Тогда $\pi(m) = \pi(m - s) \in JQ$. Поскольку π сюръективно, это означает, что $Q = JQ$. По лемме Накаямы $Q = 0$, то есть $S = M$. □

На основе этой формы леммы Накаямы выводится следующая важная теорема:

Теорема 4.1. *Конечно порожденный проективный модуль над локальным кольцом свободен.*

Доказательство. Пусть R — локальное кольцо с радикалом J и полем вычетов $k = R/J$, пусть P — конечно порожденный проективный R-модуль, и пусть $r = \dim_k(P/JP)$. Тогда мы можем построить отображение $f : R^r \to P$, такое, что $\overline{f} : k^r \to P/JP$ есть изоморфизм. Благодаря второй формулировке леммы Накаямы $f(R^r) = P$. Мы получаем короткую точную последовательность

$$0 \to \ker f \to R^r \to P \to 0,$$

которая расщепляется, поскольку модуль P проективен. Следовательно, можно определить эпиморфизм $g : R^r \to K = \ker f$, для которого $\ker g = P' \cong P$. При этом $\overline{g} = 0$, значит, $K = g(R^r) \subseteq JR^r$, поэтому $JK = K \cap JR^r = K$ и K — конечно порожденный модуль; это позволяет еще раз применить лемму Накаямы, которая показывает, что $\ker f = 0$. Таким образом, f есть изоморфизм. □

4.1.4 Упражнения.

1. Опишите изоморфизмы между группами $\mathrm{SL}_n(K)$ и $\mathrm{SL}_m(L)$, где $n, m \geqslant 3$, K, L — поля, опираясь на описание изоморфизмов между группами $\mathrm{PSL}_n(K)$ и $\mathrm{PSL}_m(L)$.

2. Приведите пример модуля над локальным кольцом, который не является свободным.

3. Докажите теоремы 4.1 для проективных модулей, которые не являются конечно порожденными.

4. Приведите пример, когда автоморфизм группы $E_n(R)$ (или $\mathrm{GL}_n(R)$) не продолжается до автоморфизма некоторой его локализации $E_n(R_I)$ или $\mathrm{GL}_n(R_I)$. Может ли автоморфизм группы $E_n(R)$ не продолжаться до автоморфизма группы $E_n(S)$, где $S = \prod_I R_I$ (I — все максимальные идеалы кольца R)?

Литература

[1] Атья М., Макдональд И. Введение в коммутативную алгебру. Изд-во "Факториал Пресс", 2003.

[2] Голубчик И.З., Михалев А.В. Изоморфизмы общей линейной группы над ассоциативным кольцом. Вестник МГУ, серия математика, 1983, 3, 61–72.

[3] И.З. Голубчик. Линейные группы над ассоциативными кольцами. Диссертация на соискание степени доктора физико-математических наук. Уфа, 1997.

[4] Дьедонне Ж. Геометрия классических групп. Мир, М., 1974.

[5] Зельманов Е.И. Изоморфизмы полных линейных групп над ассоциативными кольцами. Сибирский математический журнал, 1985, 26(4), 49–67.

[6] Петечук В.М. Автоморфизмы матричных групп над коммутативными кольцами. Математический сборник, 1982, 117(4), 534–547.

[7] Петечук В.М. Автоморфизмы групп SL_n, GL_n над некоторыми локальными кольцами. Математические заметки, 28(2), 1980, 187–206.

[8] Петечук В.М. Автоморфизмы групп $\mathrm{SL}_3(K)$, $\mathrm{GL}_3(K)$. Математические заметки, 31(5), 1982, 657–668.

[9] К. Фейс. Алгебра: кольца, модули и категории, том 1. М., Мир, 1977.

[10] Dieudonne J. On the automorphisms of the classical groups. Mem. Amer. Math. Soc., 1951, 2, 1–95.

[11] Golubchik I.Z. Isomorphisms of the linear general group $\mathrm{GL}_n(R)$, $n \geq 4$, over an associative ring. Contemp. Math., 1992, 131(1), 123–136.

[12] Hua L.K., Reiner I., Automorphisms of unimodular groups, Trans. Amer. Math. Soc., 71, 1951, 331–348.

[13] O'Meara O.T., The automorphisms of linear groups over any integral domain, J. reine angew. Math., 223, 1966, 56–100.

[14] Rickart C.E. Isomorphic group of linear transformations. Amer. J. Math, 1950, 72, 451–464.

[15] Schreier O., van der Varden B.L. Die Automorphismen der projektiven Gruppen. Abh. Math. Sem. Univ. Hamburg, 1928, 6, 303–322.

[16] Wilson J.S. The normal and subnormal structure of general linear groups. Proceedings of the Cambridge Philosophical Society, 1972, 71, 163–177.