Введение.

Традиционная теория Галуа для полей изучает симметрии полей, полученных добавлением корней алгебраического уравнения к полю, порожденному его коэффициентами. Отправной точкой дифференциальной теории Галуа являются дифференциальные уравнения вида $z^{(n)} + a_{n-1}z^{(n-1)} + \ldots a_0 z = 0$, где a_i — мероморфные функции в некоторой области. Такой выбор коэффициентов обусловлен, в частности, тем, что функции, мероморфные в данной области, (в отличие, например, он действительнозначных гладких функций на интервале) образуют поле. На этом поле помимо обычных алгебраических операций определена также операция дифференцирования. Поэтому центральным объектом в дифференциальной теории Галуа является расширение дифференциальных полей.

Лекция 1 Дифференциальные кольца и поля, добавление корня линейного дифференциального уравнения.

Определение 1.1. Коммутативное кольцо R называется *дифференциальным кольцом*, если задано отображение, называемое дифференцированием, $D\colon R \to R$ такое, что:

1. $D(a+b) = D(a) + D(b)$;
2. $D(ab) = D(a)b + aD(b)$.

Часто вместо $D(a)$ мы будем писать a', а вместо $D^n(a)$ — $a^{(n)}$.
Дифференциальное кольцо, являющееся полем, называется *дифференциальным полем.*

Заметим, что если дифференцирование задано на кольце R, то оно однозначно продолжается на его поле частных по стандартной формуле дифференцирования частного.

Все рассматриваемые ниже поля имеют нулевую характеристику. Более того, для любого дифференциального кольца R мы будем предполагать, что $\mathbb{Q} \subset R$ (иногда такие дифференциальные кольца называют *кольцами Ритта*).

Пример 1.1. Рассмотрим кольцо многочленов $\mathbb{C}[z]$, где дифференцирование — взятие производной. Вообще говоря, взятие производной — не единственный способ задать дифференцирование на $\mathbb{C}[z]$. Однако, так как $(a_n z^n + \ldots + a_0)' = na_n(z')z^{n-1} + \ldots + a_1(z')$, достаточно задать дифференцирование на элементе z —на все кольцо оно продолжится однозначно. Таким образом, любое дифференцирование алгебры $\mathbb{C}[z]$ имеет вид $p(z)\frac{\partial}{\partial z}$, где $p(z) \in \mathbb{C}[z]$.

Поле рациональных функций $\mathbb{C}(z)$ является дифференциальным полем.

Докажем несколько простых, но важных фактов о дифференциальных кольцах.

Определение 1.2. Элемент a дифференциального кольца называется *константой*, если $a' = 0$. Множество констант кольца R будем обозначать через $C(R)$.

Лемма 1.1. *В дифференциальном кольце константы образуют подкольцо, в поле — подполе.*

Лемма 1.2. *Пусть $ab = 0$ $(a, b \in R)$. Тогда $D^k(a)b^{k+1} = 0$.*

Доказательство. Докажем импликацию $D^k(a)b^{k+1} = 0 \Rightarrow D^{k+1}(a)b^{k+2} = 0$. Продифференцируем первое равенство:

$$D^{k+1}(a)b^{k+1} + (k+1)D^k(a)D(b)b^k = 0$$

Домножив на b, получим требуемое.

□

Следствие 1.1. *Если a нильпотент, то a' тоже нильпотент.*

Доказательство. Из $a^n = 0$ следует $a'a^{n-1} = 0$. Будем многократно применять лемму 1.2:

$$a^{n-1}a' = 0 \Rightarrow (a^{n-2}a')(a')^2 = 0 \Rightarrow \cdots \Rightarrow (a')^{2^n-1} = 0$$

□

Пример 1.2. Фиксируем поле k (возможно, дифференциальное). Тогда «универсальной» дифференциальной алгеброй над k будет алгебра многочленов от счетного набора переменных $z = z_0, \ldots, z_n, \ldots$ с дифференцированием определенным на образующих формулой $(z_i)' = z_{i+1}$. Обозначать такую алгебру будем через $k\{z\}$.

Пусть фиксировано дифференциальное поле F. Тогда для элементов $a_0, \ldots, a_n$ рассмотрим уравнение $a_0y^{(n)}+a_1y^{(n-1)}+\ldots+a_ny = 0$. Его можно переписать в виде $(a_0D^n+a_1D^{n-1}+\ldots+a_n)y = 0$, где выражение в скобках будем называть *дифференциальным оператором* (порядка n). Если $a_0 = 1$, то оператор называется *унитарным.*

Определение 1.3. Для данного дифференциального кольца R можно также определить *кольцо дифференциальных операторов* $R[\partial]$. Это кольцо порождено R и символом ∂ с соотношением $\partial a = a' + a\partial$ для $a \in R$.

В частности, в случае, когда R — дифференциальное поле, кольцо $R[\partial]$ является левым и правым евклидовым (см. ??).

Определение 1.4. Пусть дифференциальное поле E содержит F как подполе и ограничение дифференцирования на F отображает его в себя. Тогда поле E называется *дифференциальным расширением* поля F.

Лемма 1.3. *Пусть $K \supset L$ — алгебраическое расширение дифференциальных полей. Тогда расширение $C(K) \supset C(L)$ алгебраично.*

Доказательство. Пусть $c \in C_K$ и $c^n + a_{n-1}c^{n-1} + \ldots + a_0$ — его минимальный многочлен над L. Дифференцируя, получаем: $a'_{n-1}c^{n-1} + \ldots + a'_0$. В силу минимальности многочлена, $a'_{n-1} = a'_{n-2} = \ldots = a'_0 = 0$. Что и требовалось. □

Предложение 1.1. *Для любого дифференциального поля F и любого дифференциального оператора L с коэффициентами в F существует такое расширение E поля F, что соответствующее дифференциальное уравнение имеет решение в поле E.*

Доказательство. Рассмотрим алгебру $F[z_0, z_1, \ldots, z_{n-1}]$ с дифференцированием, определенным на образующих по формулам:

1. $(z_i)' = z_{i+1}$ при $i < n - 1$;
2. $(z_{n-1})' = -(a_1z_{n-1} + \ldots + a_nz_0)$.

Эта алгебра не имеет делителей нуля и можно рассмотреть её поле частных. Оно будет дифференциальным расширением F и дифференциальное уравнение, соответствующее оператору L, будет иметь решение — z_0. □

Это предложение дает нам аналог процедуры присоединения корня из стандартной теории полей. Однако, здесь есть различие — в дифференциальном случае эту процедуру можно повторить бесконечно много раз. В качестве иллюстрации рассмотрим:

Пример 1.3. Фиксируем поле $F = \mathbb{C}(e^t)$ с производной по t в качестве дифференцирования и рассмотрим оператор $L = D - 1$. Результатом описанной выше операции будет поле $\mathbb{C}(e^t, z)$, где $z' = z$. Легко убедиться, что $\frac{z}{e^t}$ является в этом поле константой. Таким образом, увеличение множества решений произошло просто благодаря увеличению поля констант.

Возникает разумная гипотеза, что «содержательное» добавление корня не должно увеличивать поле констант. В следующей лекции мы опишем процедуру построения таких расширений.

Задача 1.1. Опишите все возможные дифференцирования на алгебре $\mathbb{C}[[x, y]]$. (см. пример 1.1)

Задача 1.2. Докажите, что из нильпотентности a следует нильпотентность a'. (следствие 1.1)

Задача 1.3. Рассмотрим дифференциальное поле $\mathbb{C}(y_1, \ldots, y_n)$ с дифференцированием заданным формулой $(y_i)' = y_i$. Опишите его поле констант.

Задача 1.4. Пусть F дифференциальное поле. Рассмотрим поле E, полученное из него добавлением одной свободной дифференциальной переменной (поле частных кольца $F\{x\}$, см. пример 1.2). Докажите, что поле констант E совпадает с полем констант F.

Задача 1.5. Пусть F — дифференциальное поле, а $E \supset F$ — его алгебраическое расширение (но не дифференциальное). Докажите, что структура дифференциального поля на E однозначно определена.

Задача 1.6. Пусть $E \supset F$ — расширение дифференциальных полей. Пусть $a_1, \ldots, a_n \in E$ — константы, алгебраически зависимые над F. Тогда они алгебраически зависимы над полем констант F. (см. лемму 1.3)

Лекция 2 Расширения без новых констант, вронскиан.

Первой задачей, решаемой в данной лекции, будет доказательство аналога предложения 1.1 с дополнительным условием — чтобы поля констант у исходного поля и его расширения совпадали.

Начнем со стандартного факта из коммутативной алгебры.

Лемма 2.1. *Пусть A — конечнопорожденная целостная k-алгебра* ($\operatorname{char} k = 0$). *Для данного $x \in A$ рассмотрим множество значений x при гомоморфизмах A в $\bar{k}$. Тогда либо оно конечно и x алгебраичен над k, либо оно является дополнением к конечному.*

Доказательство. Если x алгебраичен над A, то это множество, очевидно, конечно.

В противном случае дополним x до базиса трансцендентности $x = x_1, \ldots, x_r$. Его, в свою очередь, дополним до системы порождающих $x_1, \ldots, x_m$. Расширение $k(x_1, \ldots, x_m) \supset k(x_1, \ldots, x_r)$ алгебраично и у него можно выбрать примитивный элемент, причем можно считать, что он является k-линейной комбинацией $x_{r+1}, \ldots, x_m$. Без ограничения общности, можно считать, что он равен x_{r+1}. Тогда $x_{r+2}, \ldots, x_m$ представляются в виде многочленов от x_{r+1} с коэффициентами в $k(x_1, \ldots, x_r)$.

Попробуем теперь задать гомоморфизм из A в $\bar{k}$. Есть всего конечное количество значений x_1, при которых обращаются в тождественный нуль знаменатели коэффициентов унитарного минимального многочлена для x_{r+1} над $k(x_1, \ldots, x_r)$ и знаменатели коэффициентов представлений для $x_{r+2}, \ldots, x_m$. Если же ни один из них в нуль не обратился, то можно задать $x_2, \ldots, x_r$, чтобы эти знаменатели снова не обращались в нуль. Теперь значение x_{r+1} можно задать любым из корней его минимального многочлена, а остальные $x_{r+2}, \ldots, x_m$ окажутся заданы автоматически.

□

Определение 2.1. Идеал I в дифференциальном кольце R называется *дифференциальным идеалом*, если $I' \subset I$.

Заметим, что коммутативное кольцо, не имеющее нетривиальных идеалов, является полем, а вот для дифференциальных колец это **неверно**. Примером может служить кольцо $\mathbb{C}[x]$ их примера 1.1.

Лемма 2.2. *Пусть целостное дифференциальное кольцо R конечнопорождено над своим дифференциальным подполем F и не содержит нетривиальных дифференциальных идеалов. Тогда все константы поля частных R лежат в R. Кроме того, $C(R)$ алгебраично над $C(F)$.*

Доказательство. Обозначим поле частных R через $Q(R)$. Пусть существует такое $c \in C(Q(R))$, что $c \notin R$. Тогда множество $I = \{x \in R | xc \in R\}$ является дифференциальным идеалом, причем $1 \notin I$. Противоречие. Отсюда следует первое утверждение леммы.

Значит, $C(Q(R)) = C(R)$. Рассмотрим $c \in C(R)$. Если оно не алгебраично над F, то, согласно лемме 2.1, для всех кроме конечного числа элементов $f \in F$ существует гомоморфизм $\varphi \colon R \in \bar{F}$ такой, что $\varphi(c) = f$. В частности, существует рациональное f с таким свойством, но это бы означало необратимость $c - f$ в R. Противоречие. Второе утверждение леммы теперь следует из 1.3.

□

На самом деле, требование целостности в условии леммы излишне:

Лемма 2.3. *Если в дифференциальном кольце R нет нетривиальных дифференциальных идеалов, то в нем нет делителей нуля.*

Доказательство. По следствию 1.1 из леммы 1.2, нильпотентные элементы дифференциального кольца образуют идеал. Стало быть, в кольце R нет нильпотентов.

Пусть существуют такие $a, b \in R$, что $ab = 0$. Рассмотрим идеал порожденный a. Любой элемент этого идеала имеет вид $c = \sum_{i=0}^{n} D^i(a)c_i$. Из леммы 1.2 следует, что $cb^{n+1} = 0$. Так как b не является нильпотентом, весь идеал порожденный a состоит из делителей нуля, а значит не содержит единицу. Построенный нетривиальный дифференциальный идеал приводит нас к противоречию. $\square$

Предложение 2.1. *Для любого дифференциального поля F с алгебраически замкнутым полем констант и любого дифференциального оператора L с коэффициентами в F существует такое расширение без новых констант E поля F, что соответствующее дифференциальное уравнение имеет решение в поле E.*

Доказательство. Процедура будет аналогична уже описанной. Рассмотрим такую же дифференциальную алгебру $F[z_0, z_1, \dots, z_{n-1}]$, как и в доказательстве предложения 1.1. Однако, так как мы планируем её факторизовать по максимальному идеалу, надо позаботиться, чтобы предполагаемое решение уравнения не обнулилось — то есть надо рассматривать алгебру $F[z_0, z_1, \dots, z_{n-1}]\left[\frac{1}{z_0}\right]$. Обозначим через S её фактор по максимальному дифференциальному идеалу, а через $\bar{z}_0$ — образ z_0 в этом факторе. В S нет нетривиальных дифференциальных идеалов, а значит S целостна по лемме 2.3, и её поле частных является расширением F без новых констант по лемме 2.2. Нетрудно видеть, что $\bar{z}_0$ является решением уравнения $Ly = 0$. $\square$

Заметим, что по сравнению с предложением 1.1 появилось новое условие: алгебраическая замкнутость поля констант. Это условие оказывается довольно естественным, в частности, в поле мероморфных в данной области функций поле констант совпадает с $\mathbb{C}$. **Более того, всюду в дальнейшем мы будем предполагать, что поле констант алгебраически замкнуто.**

Теперь хочется понять, сколько раз можно «добавить нетривиальное решение» для данного дифференциального уравнения. Ответить на вопрос о «количестве решений» нам поможет определитель Вронского.

Определение 2.2. Пусть $y_1, \dots, y_n$ — элементы дифференциального кольца. Тогда их *определителем Вронского (вронскианом)* называется определитель *матрицы Вронского*:

$$\begin{pmatrix} y_1 & y_2 & \dots & y_n \\ y_1' & y_2' & \dots & y_n' \\ \vdots & \vdots & \ddots & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \dots & y_n^{(n-1)} \end{pmatrix}$$

Обозначается он через $w(y_1, \dots, y_n)$.

Лемма 2.4. *Вронскиан элементов $y_1, \dots, y_n$ дифференциального поля равен нулю тогда и только тогда, когда $y_1, \dots, y_n$ линейно зависимы над полем констант.*

Доказательство. Если $c_1, \dots, c_n$ — константы, то из $\sum_{i=1}^{n} c_i y_i = 0$ следует $\sum_{i=1}^{n} c_i y_i^{(k)} = 0$. Это означает, что столбцы матрицы Вронского линейно зависимы, то есть вронскиан равен нулю.

Обратно, пусть $w(y_1, \dots, y_n) = 0$. Будем также считать, что этот набор минимален, то есть для любого меньшего подмножества $\{y_1, \dots, y_n\}$ вронскиан нулю не равен. Между столбцами матрицы Вронского есть линейная зависимость, причем единственная — иначе можно было бы исключить одну из переменных и получить линейную зависимость не на все столбцы, что противоречило бы минимальности.

Пусть $a_1, \ldots, a_n$ — коэффициенты этой линейной зависимости. Можно считать, что $a_1 = 1$. Из соотношений $\sum\limits_{i=1}^{n} a_i y_i^{(k+1)} = 0$ и $\sum\limits_{i=1}^{n} (a_i' y_i^{(k)} + a_i y_i^{(k+1)}) = 0$ следует, что $\sum\limits_{i=2}^{n} a_i' y_i^{(k)} = 0$ при k от нуля до $n-2$. Таким образом, $a_2', \ldots, a_n'$ — коэффициенты линейной зависимости для столбцов матрицы Вронского для $y_2, \ldots, y_n$. Так как они линейно независимы, все a_i — константы. Что и требовалось. □

Пусть теперь L - линейный дифференциальный оператор порядка n с коэффициентами в поле F. Легко видеть, что решения уравнения $Ly = 0$ образуют линейное пространство над $C(F)$. Более того:

Предложение 2.2. *Размерность пространства решений уравнения $Ly = 0$ над $C(F)$ не превосходит n.*

Доказательство. Пусть $y_1, \ldots, y_{n+1}$ — линейно независимые над $C(F)$ решения уравнения $Ly = 0$. Тогда по лемме 2.4 $w(y_1, \ldots, y_{n+1}) \neq 0$, но с другой стороны коэффициенты оператора L доставляют линейную зависимость для строк матрицы Вронского для $y_1, \ldots, y_{n+1}$. □

Теперь аналогично операции «добавление решения уравнения» приведем конструкцию «добавление всех решений уравнения».

Предложение 2.3. *Пусть F дифференциальное поле и L — унитарный линейный дифференциальный оператор над F. Тогда существует расширение $E \supset F$ без новых констант такое, что пространство решений $Ly = 0$ n-мерно над $C(F)$.*

Доказательство. Будем действовать по аналогии с предложением 2.1. Пусть $L = D^n + a_1 D^{n-1} + \ldots + a_n$. Рассмотрим дифференциальную алгебру $A = F[y_{i,j}, i = 1, \ldots, n, j = 0, \ldots, n-1]$ с дифференцированием:

1. $(y_{i,j})' = z_{i,j+1}$ при $j < n-1$;
2. $(y_{i,n-1})' = -(a_1 y_{i,n-1} + \ldots + a_n y_{i,0})$.

Теперь рассмотрим дифференциальную алгебру $S = A\left[\frac{1}{w(y_{1,0}, \ldots, y_{n,0})}\right]$. Кольцо частных её фактора по максимальному дифференциальному идеалу и будет искомым расширением. Действительно, по лемме 2.2, поле констант не расширится. Кроме того, образы $y_{i,0}$ будут решениями уравнения $Ly = 0$ с ненулевым вронскианом. Что и требовалось.

□

Определение 2.3. Алгебра S из доказательства называется *полной универсальной алгеброй решений* для оператора L.

Задача 2.1. Рассмотрим дифференциальное поле $\mathbb{C}(z)$ и оператор $D + z^2$. Примените к ним операцию добавления решения из предложения 2.1.

Решение. Предложение 2.1 предписывает нам рассмотреть алгебру $\mathbb{C}(z)\left[y, \frac{1}{y}\right]$ с дифференцированием $y' = -z^2 y$ и найти в ней максимальный дифференциальный идеал. Покажем, что такой идеал — нулевой. Пусть некоторый полином Лорана от y с коэффициентами в $\mathbb{C}(z)$ лежит в этом идеале. Среди всех таких полиномов, куда не входит $\frac{1}{y}$ рассмотрим полином наименьшей степени. Тогда он имеет вид $f = y^k + a_{k-1} y^{k-1} + \ldots + a_0$ $(a_i \in \mathbb{C}(z))$, причем в силу минимальности степени $a_0 \neq 0$. Рассмотрим $kz^2 f - f'$. Этот многочлен также лежит в идеале, но имеет степень строго меньше, а значит равен нулю. Но тогда получаем условие на свободный член $a_0' = kz^2 a_0$. Степень рациональной функции слева хотя бы на три меньше степени рациональной функции справа, а значит такое равенство невозможно.

Итогом будет поле частных алгебры $\mathbb{C}(z)\left[y, \frac{1}{y}\right]$, то есть поле $\mathbb{C}(z, y)$.

Задача 2.2. Приведите пример такого дифференциального поля F и оператора L, что при выборе разных максимальных идеалов конструкция из предложения 2.1 дает неизоморфные расширения.

Задача 2.3. Пусть элементы $y_1, \ldots, y_n$ поля F линейно независимы над полем констант и L_1, L_2 — дифференциальные операторы порядка не более n. Пусть $L_i y_j = 0$. Докажите, что L_1 и L_2 пропорциональны.

Решение. Если какой-то из операторов имеет порядок строго меньше n, то он не может иметь n-мерного пространства решений. Значит, оба оператора имеют порядок n, более того, поделив на старший коэффициент, можно считать, что D^n входит в них с коэффициентом единица. Тогда их разность имеет порядок строго меньше n, но размерность решений разности не меньше n. Стало быть, разность равна нулю, а сами операторы пропорциональны.

Задача 2.4. Приведите пример дифференциального поля с не алгебраически замкнутым полем констант, у которого процедура из предложения 2.1 все-таки увеличивает поле констант.

Задача 2.5. Пусть $E \supset F$ — расширение дифференциальных полей. Пусть также f и g являются решениями некоторых (возможно, разных) линейных дифференциальных уравнений с коэффициентами из F. Докажите, что $f + g$ и fg также являются корнями некоторых линейных дифференциальных уравнений с коэффициентами из F.

Решение. Заметим, что условие «быть решением линейного дифференциального уравнения с коэффициентами из F» равносильно условию «F-пространство, порожденное всеми производными, конечномерно». Будем обозначать F-пространство порожденное производными элемента a через $V(a)$. Тогда $V(f)$ и $V(g)$ конечномерны. Однако, $V(f+g) \subset V(f) + V(g)$ и $V(fg) \subset V(f)V(g)$, а значит пространства $V(f+g)$ и $V(fg)$ конечномерны. Что и требовалось.

Лекция 3 Свойства расширений Пикара-Вессио.

Нас далее будут интересовать расширения построенного типа. Дадим формальное определение.

Определение 3.1. Пусть F — дифференциальное поле, L — линейный дифференциальный оператор порядка n над F. *Расширением Пикара-Вессио* для L будем называть такое расширение полей $E \supset F$:

1. $C(E) = C(F)$;
2. пространство решений V уравнения $Ly = 0$ имеет размерность n над $C(F)$;
3. E порождается над F пространством V.

Предложение 3.1. *Пусть F — дифференциальное поле и L — линейный дифференциальный оператор над F. Пусть E_1 и E_2 — два различных расширения Пикара-Вессио для L. Тогда между ними существует изоморфизм тождественный на F.*

Заметим, что это свойство не выполнено для операции прибавления одного решения из предложения 2.1 (см. задачу 2.2).

Доказательство. Сначала установим наличие такого изоморфизма для случая, когда расширение $E_2 \supset F$ построено с помощью конструкции из предложения 2.3. Требуемое утверждение будет получаться композицией двух таких автоморфизмов.

Обозначим универсальную алгебру решений для E_2 через S и выберем в S максимальный дифференциальный идеал такой, что E_2 — поле частных S/P. Рассмотрим алгебру $E_1 \otimes_F (S/P)$ и выберем в ней максимальный дифференциальный идеал Q. Так как подалгебры $E_1 \otimes 1$ и $1 \otimes (S/P)$ дифференциально просты, при гомоморфизме факторизации по Q они изоморфно вложатся в $(E_1 \otimes (S/P))/Q$. Тогда E_1 и E_2 вкладываются в поле частных E этой алгебры, причем эти вложения будут изоморфизмами на F. Теперь достаточно показать, что их образы при этих вложениях совпадут — это и даст требуемый изоморфизм.

Пусть оператор L имеет порядок n. Образ E_i порождается в E пространством решений уравнения $Ly = 0$ размерности n над полем констант F. Так как алгебра $E_1 \otimes_F (S/P)$ конечнопорождена, $C(E) = C(F)$, а значит это пространство определено однозначно. Что и требовалось. $\square$

Следствие 3.1. *Любое расширение Пикара-Вессио получается с помощью конструкции из предложения 2.3.*

Из доказательства предложения 3.1 можно также извлечь следующее следствие:

Следствие 3.2. *Пусть $E \supset F$ — расширение Пикара-Вессио поля F, и $K \supset F$ — расширение без новых констант. И пусть σ_1 и σ_2 — два вложения E в K тождественные на F. Тогда $\sigma_1(E) = \sigma_2(E)$.*

Отметим, что свойство, о котором идет речь в этом следствии, аналогично понятию нормальности расширения из классической теории полей.

Разберем два основных примера простейших расширений Пикара-Вессио.

Пример 3.1. Рассмотрим оператор $L = D - a$, где $a \in F$. Полная система решений будет одномерна, универсальная алгебра решений — $F\left[z, \frac{1}{z}\right]$, где $z' = az$. Эта алгебра является кольцом главных идеалов, поэтому любой нетривиальный дифференциальный идеал порожден одним многочленом: $p = z^n + a_{n-1}z^{n-1} + \ldots + a_0$. Так как в кольце есть $\frac{1}{z}$, можно считать, что $a_0 \neq 0$. Кроме того, выберем n наименьшим возможным. p' также должен лежать в этом идеале, а значит p и

p' пропорциональны, откуда $a_0' = ana_0$. Отсюда следует, что z^n и a_0 пропорциональны над полем констант, значит в идеале лежит многочлен $q = z^n - ca_0$ (где c лежит в поле констант). В силу минимальности степени p, $p = q$.

Итак, имеется две возможности:

1. существуют такие n и a_0, что $a_0' = naa_0$. Тогда построенное расширение будет получаться присоединением корня n-ой степени из a_0. Например, такое расширение будет построено для оператора $D - \frac{1}{3}$ в поле $\mathbb{C}(e^t)$ — результат будет изоморфен $\mathbb{C}(e^{\frac{t}{3}})$;

2. такого элемента не существует. В таком случае алгебра $F\left[z, \frac{1}{z}\right]$ дифференциально проста — расширение Пикара-Вессио будет её полем частных. Например, такое расширение будет построено для оператора $D - 1$ в поле $\mathbb{C}$ — результат будет изоморфен $\mathbb{C}(e^t)$.

Расширение такого типа называется *присоединением экспоненты.*

Пример 3.2. Хотелось бы рассмотреть уравнение $z' = a$. Однако, соответствующий оператор, будучи линейным, не является однородным. Поэтому рассматривают оператор $D^2 - \frac{a'}{a}D$. В пространстве решений соответствующего уравнения лежат все константы. Поэтому можно считать, что универсальная алгебра решений имеет вид $F\left[z, z', \frac{1}{z'}\right]$. Так как $D(z' - a) = \frac{a'}{a}(z' - a)$, $z' - a$ порождает нетривиальный дифференциальный идеал. Профакторизовав по нему, получим алгебру $F[z]$ с $z' = a$. Если в этой алгебре есть нетривиальный дифференциальный идеал, то он главный. Пусть он порожден многочленом $p = z^n + a_{n-1}z^{n-1} + \ldots + a_0$. Как и в прошлом примере, p и p' должны быть пропорциональны, но степень p' строго меньше, а значит $p' = 0$. Тогда $a_{n-1}' + na = 0$. Это бы означало, что в поле F уже есть двумерное пространство решений нашего уравнения: $\langle 1, \frac{-a_{n-1}}{n} \rangle$.

Итак, имеется две возможности:

1. в поле F есть элемент z такой, что $z' = a$. Тогда расширение тривиально;

2. в поле F нет такого элемента. Тогда расширение изоморфно полю рациональных функций $F(z)$ с дифференцированием $z' = a$.

Расширение такого типа называется *взятием интеграла.*

В дальнейшем нам неоднократно понадобится следующий стандартный факт из коммутативной алгебры.

Лемма 3.1. *Пусть K и L — расширения поля k, причем $\operatorname{char} k = 0$. Тогда в кольце $K \otimes_k L$ нет нильпотентов.*

Заметим, что требование нулевой характеристики здесь существенно — в положительной характеристике это утверждение, вообще говоря, неверно.

Доказательство. Рассмотрим произвольный ненулевой элемент этого кольца $\sum k_i \otimes l_i$. Рассмотрим алгебру L_0 порожденную элементами l_i. Это конечнопорожденная целостная алгебра, выбрав в ней базис трансцендентности и примитивный элемент, порождающий алгебру над этим базисом (аналогично доказательству леммы 2.1), можно представить её в виде $L_0 = k[x_1, \ldots, x_n]/(P)$, где P — неприводимый многочлен от $x_1, \ldots, x_n$ ($x_1, \ldots, x_{n-1}$ составляют базис трансцендентности). Кроме того, P взаимно прост со своей частной производной по x_n. Кольцо $K \otimes_k L_0$ изоморфно $K[x_1, \ldots, x_n]/(P)$. Пусть там есть нильпотент n, его можно считать неприводимым над K. Он зависит от x_n, так как $x_1, \ldots, x_{n-1}$ по-прежнему алгебраически независимы. Но это означало бы, что $n^2 | P$. Этого не может быть, так как эти многочлены можно рассмотреть относительно x_n, а P все ещё взаимно прост со своей производной по x_n.

Значит, каждый элемент кольца $K \otimes_k L$ лежит в подкольце без нильпотентов. $\square$

Введем обозначения. Пусть группа G действует на множестве X. Через X^G будем обозначать множество неподвижных точек.

Пусть $E \supset F$ — расширение дифференциальных полей. Через $G(E/F)$ будем обозначать группу дифференциальных автоморфизмов E тождественных на F.

При помощи конструкции из доказательства предложения 3.1 можно доказать также следующее ключевое свойство расширений Пикара-Вессио:

Предложение 3.2. *Пусть F — дифференциальное поле, и L — линейный дифференциальный оператор над F. Пусть также $E \supset F$ — расширение Пикара-Вессио для L над F. Тогда $E^{G(E/F)} = F$.*

Доказательство. Очевидно, что $E^{G(E/F)} \supset F$. Пусть $x \in E \backslash F$. Построим элемент $\sigma \in G(E/F)$ такой, что $\sigma(x) \neq x$.

Рассмотрим полную универсальную алгебру решений S и максимальный дифференциальный идеал P в ней. Пусть $x = \frac{a}{b}$, где $a, b \in S/P$. Тогда условие $x \in E \backslash F$ равносильно тому, что $c = a \otimes_F b - b \otimes_F a \neq 0$. Так как $(S/P) \otimes_F (S/P)$ вкладывается в $E \otimes_F E$, c не нильпотентен по лемме 3.1, что позволяет нам рассмотреть алгебру $(S/P) \otimes_F (S/P) \left[\frac{1}{c}\right]$. Аналогично доказательству предложения 3.1 выберем в этой алгебре максимальный дифференциальный идеал Q. E вкладывается в кольцо частных фактора по Q двумя способами: через $\sigma_1 \colon S/P \to S/P \otimes_F 1$ или через $\sigma_2 \colon S/P \to 1 \otimes_F S/P$. Пусть $\sigma_1^{-1}(\sigma_2(x)) = x$. Тогда $\sigma_1(x) = \sigma_2(x)$, то есть $\frac{a \otimes 1}{b \otimes 1} = \frac{1 \otimes a}{1 \otimes b} \pmod{Q}$. Отсюда следовало бы, что $c \in Q$. Противоречие. Значит $\sigma_1^{-1}\sigma_2$ — искомый автоморфизм.

□

Задача 3.1. Опишите расширения Пикара-Вессио:

1. для $L = (D - \alpha)(D - \beta)$ $(\alpha, \beta \in \mathbb{C})$ над $\mathbb{C}$;
2. для $L = (D - \alpha)^k$ $(\alpha \in \mathbb{C})$ над $\mathbb{C}(z)$;
3. для $L = (D - \alpha)^k$ $(\alpha \in \mathbb{C})$ над $\mathbb{C}$.

Задача 3.2. Приведите пример такого расширения дифференциальных полей $E \supset F$, чтобы оно являлось расширением Пикара-Вессио для двух разных (непропорциональных) линейных дифференциальных операторов.

Задача 3.3. Покажите, что расширение Пикара-Вессио для набора операторов единственно с точностью до изоморфизма над F.

Задача 3.4.
1. пусть $E \supset F$ — расширение Пикара-Вессио, и $E \supset K \supset F$ — промежуточное дифференциальное поле. Докажите, что $E \supset K$ — расширение Пикара-Вессио;
2. каждому промежуточному подполю можно сопоставить подгруппу $G(E/F)$, состоящую из тех элементов, которые оставляют это подполе неподвижным. Каждой подгруппе H можно сопоставить промежуточное подполе E^H. Покажите, что композиция этих двух отображений тождественна. (заметим, что это одна из частей соответствия Галуа)

Задача 3.5. Пусть F — поле частных свободной дифференциальной алгебры $\mathbb{C}\{a_0, \ldots, a_{n-1}\}$ от n переменных (см. пример 1.2). Опишите расширение Пикара-Вессио для оператора $D^n + a_{n-1}D^{n-1} + \ldots + a_0$.

Лекция 4 Расширения Пикара-Вессио для нескольких операторов. Алгебраичность группы автоморфизмов расширения Пикара-Вессио.

Теперь мы можем дать такое альтернативное определение расширения Пикара-Вессио, не содержащее дифференциального оператора в явном виде.

Предложение 4.1. *Пусть F — дифференциальное поле с алгебраически замкнутым полем констант C. Расширение $E \supset F$ является расширением Пикара-Вессио тогда и только тогда, когда:*

1. *$C(E) = C$;*
2. *существует конечномерное C-пространство V в E такое, что E порождается над F элементами V;*
3. *для некоторой группы G дифференциальных автоморфизмов E над F такой, что $G(V) \subset V$, выполнено $F = E^G$.*

Доказательство. Если $E \supset F$ — расширение Пикара-Вессио для оператора L, то достаточно положить V равным пространству решений уравнения $Ly = 0$.

Пусть теперь $E \supset F$ — расширение, удовлетворяющее всем трём условиям. Пусть $f_1, \ldots, f_n$ — C-базис пространства V. Рассмотрим дифференциальный оператор $L(y) = \frac{w(f_1,\ldots,f_n,y)}{w(f_1,\ldots,f_n)}$. Его пространство решений — в точности V. Теперь достаточно показать, что его коэффициенты лежат в F. Нетрудно убедиться, что они инвариантны относительно всех невырожденных C-линейных преобразований пространства V. Отсюда следует, что они G-инвариантны, а значит лежат в F. □

Теперь докажем утверждение, которое гарантировало бы нам существование «достаточно большого количества автоморфизмов» (чтобы удовлетворять условию 3 предложения 4.1).

Лемма 4.1. *Пусть $E \supset F$ — расширение Пикара-Вессио для дифференциального оператора L и σ — автоморфизм поля F, оставляющий неподвижными коэффициенты оператора L. Тогда существует автоморфизм $\bar{\sigma}$ поля E такой, что $\bar{\sigma}|_F = \sigma$. Более того, $\bar{\sigma}$ переводит пространство решений $Ly = 0$ в себя.*

Доказательство. Будем строить этот автоморфизм при помощи конструкции из предложения 2.3. Возьмем две копии полной универсальной алгебры решений для L над F (более подробно см. доказательство предложения 2.3): $S_1 = F\left[y_{i,j}, \frac{1}{\det(y_{i,j})}\right]$ и $S_2 = F\left[z_{i,j}, \frac{1}{\det(z_{i,j})}\right]$. Построим между этими алгебрами изоморфизм $\bar{\sigma}$ такой, что $\bar{\sigma}|_F = \sigma$ и $\bar{\sigma}(y_{i,j}) = z_{i,j}$. Так, как σ действует тождественно на коэффициенты оператора L (это нужно для проверки соотношения $\bar{\sigma}(y'_{i,n-1}) = z'_{i,n-1}$), этот изоморфизм будет изоморфизмом дифференциальных алгебр. Выберем в S_1 максимальный дифференциальный идеал P. $\bar{\sigma}(P)$ будет максимальным дифференциальным идеалом в S_2. Изоморфизм $\bar{\sigma}$ продолжается до изоморфизма факторов S_1/P и $S_2/\bar{\sigma}(P)$. Перейдя в этом изоморфизме к полю частных, получим требуемый автоморфизм поля E.

Второе утверждение леммы очевидно, так как $\bar{\sigma}$ оставляет неподвижными коэффициенты L. □

Предложение 4.2. *Пусть F — дифференциальное поле, и $L_1, \ldots, L_k$ — линейные дифференциальные операторы с коэффициентами из F. Тогда существует такое расширение Пикара-Вессио $E \supset F$, что для любого i найдется промежуточное поле $E \supset E_i \supset F$ такое, что $E_i \supset F$ — расширение Пикара-Вессио для оператора L_i.*

Доказательство. Определим цепочку расширений $K_0 \subset K_1 \subset \ldots \subset K_k$: $K_0 = F$ и K_i — расширение Пикара-Вессио для L_i над K_{i-1}.

Докажем индукцией по i, что $K_i \supset F$ — расширение Пикара-Вессио. Пусть $K_{i-1} \supset F$ — расширение Пикара-Вессио, причем соответствующие пространство и группу из предложения 4.1 обозначим через V и G. Пусть U — пространство решений уравнения $L_i y = 0$. Тогда положим $W = V + U$ и рассмотрим группу H, порожденную продолжениями всех элементов G на K_i (как в лемме 4.1) и группой автоморфизмов $G(K_i/K_{i-1})$. Легко видеть, что $H(W) \subset W$ и $K_i^H = F$. Стало быть, согласно предложению 4.1, $K_i \supset F$ является расширением Пикара-Вессио.

Положим теперь $E = K_k$. Так как каждый из операторов L_i имеет в E полное пространство решений, соответствующее расширение Пикара-Вессио $E_i \supset F$ вкладывается в E. $\square$

Определение 4.1. Пусть F — дифференциальное поле с алгебраически замкнутым полем констант, $L_1, \ldots, L_k$ — линейные дифференциальные операторы с коэффициентами из F, причем L_i имеет порядок n_i. Тогда расширение $E \supset F$ называется расширением Пикара-Вессио для набора операторов $L_1, \ldots, L_k$, если:

1. поля констант E и F совпадают;

2. пространство решений уравнения $L_i y = 0$ над полем констант V_i имеет размерность n_i;

3. E порождается над F пространством $V_1 + \ldots + V_k$.

Теперь перейдем к изучению группы автоморфизмов расширения Пикара-Вессио. Пусть $E \supset F$ — расширение Пикара-Вессио с полем констант C и пространством решений V. Тогда группа $G(E/F)$ вкладывается в группу $\mathrm{End}_C(V)$линейных преобразований пространства V. Более того:

Предложение 4.3. *Подгруппа $G(E/F) \subset \mathrm{End}_C(V)$ задается полиномиальными соотношениями на элементы матриц.*

Сначала докажем лемму.

Лемма 4.2. *Пусть $k[x_1, \ldots, x_n]$ — алгебра многочленов, а I — идеал в ней. Рассмотрим тогда всевозможные обратимые линейные преобразования пространства $\langle x_1, \ldots, x_n \rangle$ — они индуцируют автоморфизмы алгебры. Тогда условие $\varphi(I) \subset I$ записывается полиномиальными соотношениями на элементы матрицы исходного линейного преобразования.*

Доказательство. Рассмотрим базис Гребнера идеала I — $f_1, \ldots, f_k$. Достаточно выразить полиномиальными соотношениями условия $\varphi(f_i) \in I$. Так как автоморфизмы указанного типа не меняют степень, каждое такое соотношение записывается как принадлежность многочлена $\varphi(f_i)$ конечномерному подпространству многочленов вида $\sum h_j f_j$, где $\deg(h_j f_j) \leqslant \deg(f_i)$. Это условие, в свою очередь, записывается в виде полиномиальных соотношений. $\square$

Доказательство. Вновь воспользуемся конструкцией из предложения 2.3. Рассмотрим полную универсальную алгебру решений $S = F\left[y_{i,j}, \frac{1}{\det(y_{i,j})}\right]$, выберем в ней максимальный дифференциальный идеал P. При факторизации по нему $S \to S/P \to E$ пространство $T = \langle y_{1,0}, \ldots, y_{n,0} \rangle$ изоморфно отображается на V. Более того, любое обратимое C-линейное преобразование T продолжается до дифференциального автоморфизма алгебры S. Осталось понять, какие из этих автоморфизмов продолжаются на E. Пусть φ — автоморфизм такого типа. Легко видеть, что он продолжается до автоморфизма E тогда и только тогда, когда $\varphi(P) \subset P$.

Осталось показать, что включение $\varphi(P) \subset P$ может быть записано как соотношение на элементы матрицы преобразования пространства T. Так как на пространство $\langle y_{1,i}, \ldots, y_{n,i} \rangle$ автоморфизм действует такой же матрицей, что и на T, а на $\frac{1}{\det y_{i,j}}$ действует делением на определитель, это следует из леммы 4.2, примененной к алгебре $F[y_{i,j}, d]$ и идеалу $P|_{d=\frac{1}{\det(y_{i,j})}} \cup \{d \det(y_{i,j}) = 1\}$. $\square$

Задача 4.1. Задайте полиномиальными соотношениями следующие подгруппы в $GL(V)$:

1. подгруппу ортогональных преобразований;
2. подгруппу, состоящую из всех операторов, переводящим подпространство $W \subset V$ в себя;
3. подгруппу матриц диагональных в данном базисе.

Задача 4.2. Для расширений из задачи 3.1 найдите группы автоморфизмов и задайте их полиномиальными соотношениями в соответствующей линейной группе.

Задача 4.3. Рассмотрим два линейных оператора L_1, L_2 с коэффициентами из поля F. Пусть E_1 — расширение Пикара-Вессио для набора операторов $\{L_1, L_2\}$, а E_2 — расширение Пикара-Вессио для оператора L_1L_2. Докажите, что $E_1 \subset E_2$ и приведите пример, когда включение строгое.

Задача 4.4. Докажите аналог предложения 4.2 для бесконечного множества операторов. (указание: воспользуйтесь леммой Цорна)

Задача 4.5. Рассмотрим дифференциальное поле F. Для него определим поле $E(F) \supset F$ как расширение из задачи 4.4, где в качестве множества операторов взято множество всех возможных операторов с коэффициентами из F. Приведите пример такого F, что существует оператор с коэффициентами в $E(F)$, не обладающий в $E(F)$ полным пространством решений.

Задача 4.6. Докажите, что для любого дифференциального поля F существует расширение $E \supset F$ без новых констант такое, что любой дифференциальный оператор с коэффициентами из E имеет в E полную систему решений.

Лекция 5 Аффинные алгебраические множества.

Фиксируем алгебраически замкнутое поле k нулевой характеристики.

Определение 5.1. Подмножество X в k^n называется *аффинным алгебраическим множеством*, если X задано как множество нулей системы многочленов.

Если набор многочленов $\{f_\alpha\}$ задает множество X, любой многочлен из идеала порожденного f_α обращается в нуль на множестве X. Поэтому вместо набора уравнений обычно рассматривают идеал ими порожденный. Применяя к этому идеалу теорему Гильберта о базисе, получаем:

Лемма 5.1. *Любое аффинное алгебраическое множество может быть задано конечным количеством уравнений.*

Кроме того, стандартные теоретико-множественные операции могут быть выражены на языке этих идеалов:

Лемма 5.2. *Пусть множества X и Y в k^n заданы идеалами I и J соответственно. Тогда:*

1. *$X \cup Y$ можно задать идеалом IJ;*

2. *$X \cap Y$ можно задать идеалом $I + J$.*

Определение 5.2. Несложно проверить, что аффинные замкнутые множества удовлетворяют всем аксиомам замкнутых множеств. Таким образом, на пространстве k^n оказывается задана топология. Она называется *топологией Зарисского.* Так же называют топологию, которая индуцируется на аффинных подмножествах.

Заметим, что в случае $k = \mathbb{C}$ топология Зарисского не совпадает со стандартной топологией на $\mathbb{C}^n$. В частности, пространство с топологией Зарисского как правило не является хаусдорфовым. Другим важным свойством этого топологического пространства является следующая переформулировка теоремы Гильберта о базисе:

Лемма 5.3. *Любая убывающая цепочка замкнутых подмножеств стабилизируется.*

Определение 5.3. Функция на аффинном алгебраическом множестве X называется *регулярной*, если она является ограничением полиномиальной функции на всем k^n на X.

Регулярные функции образуют кольцо, которое обычно называется координатным кольцом (или просто кольцом регулярных функций) и обозначается через $k[X]$.

Обозначим через $I(X)$ идеал, состоящий из всех полиномиальных функций на k^n, обращающихся в нуль на X.

Лемма 5.4. *Обозначим k^n через V. Тогда $k[X] = k[V]/I(X)$.*

Пример 5.1. Рассмотрим параболу X в $\mathbb{C}^2$. Её можно задать, например, как множество нулей уравнения $y - x^2$. Пусть $f \in k[x, y]$ — многочлен из $I(X)$. Тогда как многочлен от y он должен делиться на $y - x^2$. Легко видеть, что отсюда следует, что он должен делиться на $y - x^2$ и в кольце $k[x, y]$. Таким образом, идеал $I(X)$ оказывается главным и порожден $y - x^2$. Тогда $k[X] = k[x, y]/(y - x^2) \cong k[x]$.

Отметим также, что ту же самую параболу можно было задать и соотношением $(y - x^2)^2$. Возникает, вопрос, насколько сильно могут отличаться идеал, порожденный определяющими соотношениями, и идеал $I(X)$? Теорема Гильберта о нулях говорит, что все различия будут такого же рода, что и уже указанное.

Теорема 5.1. *Пусть многочлен f обращается в нуль во всех общих нулях идеала I. Тогда некоторая степень f лежит в I.*

Обозначим множество общих нулей идеала I через $V(I)$. Радикалом идеала I будем называть идеал $\sqrt{I} = \{f | \exists k \colon f^k \in I\}$. Тогда теорему Гильберта о нулях можно переписать в виде $I(V(I)) = \sqrt{I}$.

Определение 5.4. Определим теперь морфизмы между аффинными замкнутыми множествами. Будем рассматривать те морфизмы между объемлющими пространствами k^n и k^m, которые задаются полиномиальными функциями, то есть координаты образа в k^m точки $x \in k^n$ являются многочленами от координат x. Заметим, что такие отображения непрерывны в топологии Зарисского. Морфизмом между аффинными алгебраическими множествами X и Y будем называть морфизм объемлющих пространств, переводящий X в подмножество Y.

Заметим также, что морфизм $\varphi \colon X \to Y$ задает гомоморфизм алгебр $\varphi^* \colon k[Y] \to k[X]$. Иными словами, сопоставление аффинному алгебраическому множеству его координатного кольца является контравариантым функтором из категории аффинных алгебраических множеств над k в категорию k-алгебр.

Пример 5.2. Пусть X — гипербола, заданная уравнением $xy = 1$. Отобразим содержащее её k^2 в k^1 по формуле $(a, b) \to a$. Тогда гипербола перейдет в подмножество прямой, заданное условием $x \neq 0$. Алгебра регулярных функций на гиперболе изоморфна алгебре многочленов Лорана $k\left[t, \frac{1}{t}\right]$, а алгебра регулярных функций на прямой — $k[t]$. Соответствующее отображение алгебр — как раз вложение $k[t]$ в $k\left[t, \frac{1}{t}\right]$.

Построенный функтор наводит на мысль заменить само множество X вложенное каким-то образом в пространство на его координатное кольцо. Оказывается, что по кольцу действительно можно восстановить множество точек X и топологию Зарисского на нем. Ключевым соображением в построении этого соответствия является то, что для данной точки $x \in X$ вычисление значений функций в этой точке задает гоморфизм $k[X]$ в основное поле k. Таким образом, каждой точке соответствует максимальный идеал. То, что это соответствие биективно, составляет смысл теоремы Гильберта о нулях в слабой форме.

Приведем конкретную (но не каноническую!) конструкцию построения вложения в объемлющее пространство по алгебре $k[X]$. Итак, пусть дана конечнопорожденная алгебра $k[X]$. В силу её конечнопорожденности существует сюръекция $k[x_1, \ldots, x_n] \to k[X]$ (здесь n равно числу порождающих). Обозначим ядро этого отображения через I. Легко видеть, что тогда множество X будет вложено в n-мерное аффинное пространство и будет задаваться в нем уравнениями из I.

Теперь, когда определены точки (то есть максимальные идеалы) и процедура вычисления значений функций в точках (взятие образа в факторе по этому идеалу), легко определить и топологию Зарисского — действительно, замкнутыми будут множества общих нулей идеалов кольца.

В координатном кольце «зашифрованы» основные свойства множества X. Основными интересующими нас будут связность и приводимость.

Лемма 5.5. *Топологическое пространство X связно, если и только если в кольце $k[X]$ нет нетривиальных идемпотентов. Кроме того, связные компоненты соответствуют минимальным идемпотентам.*

Доказательство. Пусть e — нетривиальный идемпотент. Тогда $1 - e$ будет идемпотентом оргональным ему. Более того, алгебра $k[X]$ распадается в прямую сумму идеалов $k[X] = k[X]e \oplus k[X](1 - e)$. Соответственно, X распадется в дизъюнктное объединение двух своих замкнутых подмножеств.

Наоборот, пусть $X = X_1 \sqcup X_2$, где X_1, X_2 — замкнутые множества. Очевидно, идеалы $I(X_1)$ и $I(X_2)$ пересекаются только по нулю. Пусть $I(X_1) + I(X_2)$ не совпадает с $k[X]$. Тогда идеал

$I(X_1) + I(X_2)$ лежит в некотором максимальном, но этот идеал должен соответствовать точке не из X_1 и не из X_2. Значит $k[X] = I(X_1) \oplus I(X_2)$. Тогда есть соответствующее разложение для единицы: $1 = e_1 + e_2$. Легко видеть, что e_1 и e_2 — ортогональные идемпотенты. Кроме того, $k[X] = k[X_1] \oplus k[X_2]$.

□

Более тонким свойством является неприводимость множества.

Определение 5.5. Топологическое пространство называется *неприводимым*, если его нельзя представить в виде объединения двух нетривиальных замкнутых подмножеств. *Приводимым* оно называется в противном случае.

Заметим, что в силу леммы 5.3 всегда есть разложение пространства в объединение конечного числа неприводимых подмножеств.

Лемма 5.6. *Неприводимость множества X равносильна отсутствию в $k[X]$ делителей нуля.*

Доказательство. Пусть существуют такие $f, g \in k[X]$, что $fg = 0$. Тогда $V(f)$ и $V(g)$ и являются искомыми множествами.

Пусть $X = X_1 \cup X_2$. Рассмотрим $f \in I(X_1)$ и $g \in I(X_2)$. Тогда $fg \in I(X_1) \cap I(X_2)$, то есть $fg = 0$. □

Возникает также естественный вопрос: а что «знает» о морфизме аффинных алгебраических множеств соответствующее отображение колец?

Лемма 5.7. *Пусть $\varphi\colon X \to Y$ — морфизм алгебраических множеств, а $\varphi^*\colon k[Y] \to k[X]$ — соответствующий гомоморфизм алгебр. Тогда замыкание (в топологии Зарисского) образа X совпадает с замкнутым подмножеством Y, заданным идеалом $\operatorname{Ker}\varphi^*$.*

Доказательство. На языке колец образом являются те гомоморфизмы $k[Y] \to k$, которые получаются из композиции некоторого гомоморфизма $k[X] \to k$ и φ^*. Очевидно, пересечение их ядер содержит $\operatorname{Ker}\varphi^*$. Если замыкание $\varphi(X)$ меньше, то пересечение ядер этих гомоморфизмов было бы больше. Иначе говоря, существовал бы $f \in k[Y]$ так, что $\varphi^*(f) \neq 0$, но значение $\varphi^*(f)$ во всех точках X было бы равно нулю. Такого быть не может. □

Определение 5.6. В случае, когда замыкание $\varphi(X)$ совпадает с Y (согласно доказанному, когда $\operatorname{Ker}\varphi^* = 0$), морфизм называется *доминантным.*

Задача 5.1. Каждое ли отображение непрерывное в топологии Зарисского является морфизмом аффинных алгебраических множеств?

Задача 5.2. Покажите, что аффинное алгебраическое множество компактно в топологии Зарисского.

Задача 5.3. Рассмотрим аффинное алгебраическое множество X в $\mathbb{C}^2$ заданное соотношением $x^3 = y^2$. Покажите, что морфизм $\mathbb{C} \to X$ заданное формулой $t \to (t^2, t^3)$ не является изоморфизмом аффинных алгебраических множеств.

Задача 5.4. Будем называть разложение множества X в объединение неприводимых минимальным, если из этого разложения нельзя выкинуть ни одного элемента. Докажите, что минимальное разложение единственно (как набор подмножеств).

Задача 5.5. Приведите пример морфизма аффинных алгебраических множеств такого, что его образ не является ни открытым, ни замкнутым множеством в топологии Зарисского.

Задача 5.6. Пусть $\varphi\colon X \to Y$ — морфизм неприводимых множеств. Пусть, кроме того, любой элемент $k[X]$ является корнем многочлена со старшим коэффициентом 1 с коэффициентами из $\varphi^*(k[Y])$. Докажите, что φ сюръективен.

Лекция 6 Аффинные алгебраические группы.

Начнем с того, что проинтерпретируем в геометрических терминах ещё одну важную алгебраическую конструкцию — тензорное произведение. На самом деле эта операция нам будет встречаться в двух контекстах — в прямом произведении аффинных множеств и в расширении поля скаляров.

Рассмотрим сначала прямое произведение. Пусть X и Y — аффинные алгебраические множества. Тогда можно рассмотреть алгебру $k[X] \otimes_k k[Y]$. Она, очевидно, конечнопорождена. Кроме того, по лемме 3.1, в этой алгебре нет нильпотентов, а значит она является алгеброй регулярных функций для некоторого аффинного алгебраического множества.

Определение 6.1. Аффинное алгебраическое множество, соответствующее алгебре $k[X] \otimes k[Y]$, будем называть *прямым произведением множеств X и Y* и обозначать через $X \times Y$.

Заметим, что имеются канонические отображения $X \times Y \to X$ и $X \times Y \to Y$ заданные вложениями алгебр $k[X] \to k[X] \otimes k[Y]$ (f переходит в $f \otimes 1$) и $k[Y] \to k[X] \otimes k[Y]$ (g переходит в $1 \otimes g$).

Сконструируем теперь это же множество более «конкретным» способом. Пусть X — подмножество в k^l, а Y — подмножество в k^s. Тогда для любой точки $(\alpha_1, \ldots, \alpha_l) \in k^l$ и любой точки $(\beta_1, \ldots, \beta_s) \in k^s$ сопоставим точку $(\alpha_1, \ldots, \alpha_l, \beta_1, \ldots, \beta_s) \in k^{l+s}$. Пусть множество X задавалось уравнениями $f_1, \ldots, f_r$, а множество Y — уравнениями $g_1, \ldots, g_d$. Тогда, очевидно, построенное множество задается системой $f_1, \ldots, f_r, g_1, \ldots, g_d$. Построенное множество обозначим через $X \times' Y$.

Лемма 6.1. *Множества $X \times Y$ и $X \times' Y$ изоморфны.*

Доказательство. Докажем, что изоморфны соответствующие алгебры. Любая точка из $X \times' Y$ является парой (x, y), где $x \in X$ и $y \in Y$. Более того, любая $F \in k[X \times' Y]$ имеет вид $F(x, y) = \sum p_i(x) q_i(y)$. Например, можно считать p_i и q_i образами соответствующих мономов из $k[k^l]$ и $k[k^s]$. Тогда определим гомоморфизм $\varphi \colon k[X] \otimes k[Y] \to k[X \times' Y]$:

$$\varphi\left(\sum p_i(x) \otimes q_i(y)\right) = \sum p_i(x) q_i(y)$$

Заметим, что φ — эпиморфизм, так как в его образе лежат $k[X]$ и $k[Y]$, порождающие $k[X \times' Y]$.

Покажем, что это отображение — мономорфизм. Пусть $\sum p_i \otimes q_i$ — элемент из ядра, причем p_i линейно независимы и q_i линейно независимы. Тогда из равенства $\sum p_i(x) q_i(y) = 0$, фиксируя y, получаем, что $q_i(y) = 0$ при любом y, то есть все q_i равны нулю. □

Таким образом, введенные нами $X \times Y$ и $X \times' Y$ изоморфны. Соответствующий объект будем далее обозначать через $X \times Y$.

Другой важной ситуацией, где возникает тензорное произведение, является *расширение скаляров.* Действительно, пусть у нас есть расширение $L \supset k$. Тогда систему уравнений с коэффициентами из k можно рассматривать не только на k^n, но и на L^n. Пусть множество X задавалось над k системой уравнений. Рассмотрим теперь множество X_L, задаваемое над L системой из тех же уравнений.

Лемма 6.2. *L-алгебра $L[X_L]$ изоморфна $L \otimes_k k[X]$.*

Доказательство. Пусть соответствующий идеал порождается многочленами $f_1, \ldots, f_m$ в $k[x_1, \ldots, x_n]$. Тогда:

$$L \otimes_k (k[x_1, \ldots, x_n]/(f_1, \ldots, f_m)) \cong L[x_1, \ldots, x_n]/(f_1, \ldots, f_m) \cong L[X_L]$$

. □

Далее вместо $L[X_L]$ будем писать просто $L[X]$.

Теперь мы готовы определить понятие аффинной алгебраической группы.

Определение 6.2. Пусть на множестве G заданы структура группы и структура аффинного алгебраического множества. Тогда оно называется *аффинной алгебраической группой* если отображения умножения $G \times G \to G$ и взятия обратного $G \to G$ являются морфизмами аффинных алгебраических множеств.

Заметим, что эти два морфизма индуцируют гомоморфизмы алгебр: $\Delta\colon k[G] \to k[G] \otimes k[G]$ и $S\colon k[G] \to k[G]$. На самом деле структура группы неявно предполагает наличие ещё одного морфизма — отображающего точку в единицу группы. Ему соответствует гомоморфизм $\varepsilon\colon k[G] \to k$. Разумеется, аксиомы группы некоторым образом транслируются в условия на эти гомоморфизмы. Соответствующая алгебраическая структура на $k[G]$ называется (коммутативной) алгеброй Хопфа.

Определение 6.3. Коммутативная k-алгебра A называется *коммутативной алгеброй Хопфа*, если заданы гомоморфизмы $\Delta\colon A \to A \otimes A$ (коумножение), $S\colon A \to A$ (антипод) и $\varepsilon\colon A \to k$ (коединица), удовлетворяющие следующим соотношениям (через m обозначим гомоморфизм $A \otimes A \to A$ заданный $m(a \otimes b) = ab$, а через $\nu\colon k \to A$ гомоморфизм заданный $\nu(\alpha) = \alpha \cdot 1$):

1. $(1 \otimes \Delta)\Delta = (\Delta \otimes 1)\Delta$ (коассоциативность);

2. $m(1 \otimes S)\Delta = m(S \otimes 1)\Delta = \nu\varepsilon$ (взятие обратного);

Прежде чем доказывать, что кольцо регулярных функций аффинной алгебраической группы имеет структуру алгебры Хопфа, разберем два базовых примера.

Пример 6.1. Рассмотрим поле $\mathbb{C}$ как группу по сложению. Тогда гомоморфизм $+\colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ задает гомоморфизм $\Delta\colon k[t] \to k[t] \otimes k[t]$. Несложно увидеть, что он задается формулой $\Delta(t) = t \otimes 1 + 1 \otimes t$. Антипод же задается формулой $S(t) = -t$.

Пример 6.2. Рассмотрим группу $\mathbb{C}^*$. Этому аффинному алгебраическому множеству соответствует алгебра $k\left[t, \frac{1}{t}\right]$. Непосредственная проверка показывает, что коумножение и антипод задаются формулами $\Delta(t) = t \otimes t, \Delta\left(\frac{1}{t}\right) = \frac{1}{t} \otimes \frac{1}{t}$ и $S(t) = \frac{1}{t}$.

Предложение 6.1. *Алгебра регулярных функций наделена структурой алгебры Хопфа.*

Доказательство. Нужно просто заметить, что первая и вторая аксиомы алгебр Хопфа соответствуют ассоциативности умножения и определению обратного элемента. □

Пусть теперь нам дана структура коммутативной алгебры Хопфа на $k[X]$. Приведем конструкцию восстановления умножения на X. Пусть есть две точки из X, то есть два гомоморфизма $\varphi_1, \varphi_2\colon k[X] \to k$. Тогда их произведение записывается в виде $m(\varphi_1 \otimes \varphi_2)\Delta$.

Задача 6.1. Докажите, что прямое произведение неприводимых аффинных алгебраических множеств неприводимо.

Задача 6.2. На данной конечной группе G введите структуру алгебраической группы, опишите соотвествующую алгебру Хопфа.

Задача 6.3. Опишите коумножение и антипод, соответствующие алгебраической группе GL_2.

Задача 6.4. Рассмотрим замкнутое подмножество в G. Найдите необходимое и достаточное условие на соответствующий идеал, чтобы это подмножество было ещё и подгруппой.

Задача 6.5. Определите прямое произведение аффинных алгебраических множеств как стандартную категорную конструкцию в категории аффинных алгебраических множеств над k.

Лекция 7 Действия аффинных алгебраических групп.

Определение 7.1. Пусть G — аффинная алгебраическая группа. Аффинное алгебраическое множество X называется G-*множеством*, если задано действие G на X, причем отображение $G \times X \to X$ — морфизм аффинных алгебраических множеств.

Совершенно аналогичным образом, алгебраическое G-действие задает гомоморфизм $\Delta \colon k[X] \to k[G] \otimes k[X]$ с условием $(1 \otimes \Delta)\Delta = (\Delta \otimes 1)\Delta$. Кроме того, G-действие на X индуцирует действие G на $k[X]$, в котором элемент $g \in G \colon k[G] \to k$ действует по формуле $(g \otimes 1)\Delta$.

Лемма 7.1. *Линейная оболочка орбиты любого элемента $f \in k[X]$ конечномерна, причем G действует на этом пространстве алгебраически.*

Доказательство. Пусть $\Delta(f) = \sum \varphi_i \otimes f_i$, где $\varphi_i \in k[G]$ и $f_i \in k[X]$. Таким образом, вся орбита f лежит в конечномерном пространстве натянутом на f_i. Это доказывает первую часть утверждения. Вторая следует из того, что φ_i — регулярные функции на $k[G]$, то есть задаются полиномами. □

Заметим, что всякая группа G является G-множеством, причем это действие транзитивно. Это соображение имеет ряд геометрических последствий.

Лемма 7.2. *Связные компоненты группы G неприводимы.*

Доказательство. Рассмотрим разложение группы G в минимальное объединение неприводимых множеств $G = G_1 \cup \ldots \cup G_n$. Если эти множества не пересекаются, то они будут связными компонентами. Если они пересекаются, то, в силу минимальности этого разложения, есть собственное непустое подмножество X тех точек, которые входят хотя бы в две из G_i. В силу задачи 5.4 данное разложение единственно, а значит множество X инвариантно относительно действия G, что противоречит транзитивности. □

Следствие 7.1. *Связная компонента единицы, обозначаемая через G_0, является нормальной подгруппой конечного индекса.*

Доказательство. Фиксируем $h \in G_i$ и рассмотрим отображение $G_0 \to G$, заданное $g \to hg$. Так как G_0 неприводимо, её замыкание неприводимо, а значит лежит целиком в G_i. Так как это отображение, как и обратное (умножение на h^{-1}), инъективны, получаем, что умножение на h задает изоморфизм G_0 с G_i. Отсюда следует как то, что G_0 — подгруппа, так и то, что остальные компоненты связности — её смежные классы.

Нормальность вытекает из того, что образ G_0 под действием морфизма $g \to hgh^{-1}$ неприводим и содержит единицу, а значит лежит в G_0. □

С любым действием группы естественно связаны два понятия: орбиты и стабилизатора. Они также оказываются наделены геометрическими свойствами. Сначала докажем лемму, которая будет одним из базовых инструментов. Напомним, что доминантным называется морфизм, чей образ плотен. На языке гомоморфизмов алгебр это означает отсутствие ядра.

Лемма 7.3. *В образе доминантного морфизма в неприводимое множество содержится открытое множество.*

Доказательство. Доказательство, по существу, повторяет доказательство леммы 2.1.

В случае доминантного морфизма $X \to Y$ имеет место вложение алгебр $k[Y] \subset k[X]$. Хочется доказать, что те гомоморфизмы $k[Y] \to k$, которые поднимаются до гомоморфизмов $k[X] \to k$, содержат открытое подмножество. Дополним систему порождающих $y_1, \ldots, y_r$ алгебры $k[Y]$ до системы порождающих в $k[X]$, добавив элементы $x_1, \ldots, x_s, x_{s+1}, \ldots, x_m$. Причем будем считать, что $x_1, \dots, x_s$ — базис трансцендентности $k[X]$ над $k[Y]$. Расширение $k(X) \supset k(Y)(x_1, \dots, x_s)$ алгебраично и можно считать x_{s+1} его примитивным элементом. Через $c_{s+1} \in k[Y][x_1, \dots, x_s]$ обозначим старший коэффициент в алгебраической зависимости для x_{s+1} над $k[Y][x_1, \dots, x_s]$, а через $c_{s+2}, \dots, c_m$ — наименьшие общие кратные знаменателей в выражении для $x_{s+2}, \dots, x_m$ через степени x_{s+1}. Тогда, аналогично доказательству леммы 2.1, неравенство тождественному нулю $c_{s+1}, \dots, c_m$ после применения гомоморфизма $k[Y] \to k$ является достаточным условием для поднятия этого гомоморфизма до $k[X] \to k$, откуда и следует утверждение леммы.

□

Лемма 7.4. *1. Стабилизатор любой точки является алгебраической подгруппой;*

2. Орбита любого элемента открыта и плотна в своем замыкании;

3. Существует замкнутая орбита.

Доказательство. Фиксируем G-множество X.

1. Фиксируем точку $x_0 \in X$. Рассмотрим морфизм $G \to X \times X$, заданный формулой $g \to (x_0, gx_0)$. Стабилизатор будет прообразом точки (x_0, x_0), а значит замкнутым множеством.

2. Рассмотрим точку x_0 и замыкание её орбиты под действием G_0 обозначим через Y. Множество Y неприводимо (см. доказательство леммы 7.2), а значит образ доминантного морфизма $G_0 \to Y$, заданного $g \to gx_0$, содержит открытое подмножество. В силу транзитивности действия G_0 на своей орбите, каждая точка орбиты содержится в открытом множестве, а значит орбита открыта в Y. Утверждение для G получается объединением соответствующих множеств для классов смежности по G_0.

3. Введем на замыканиях орбит отношение частичного порядка по включению. Если орбита точки x не замкнута, то в её замыкании дополнение до орбиты является замкнутым G-множеством, а значит содержит замыкание другой орбиты. Таким образом, замкнутые орбиты соответствуют минимальным относительно этого порядка элементам. Так как все убывающие цепочки замкнутых множеств стабилизируются, такой минимальный элемент существует.

□

Следствие 7.2. *Замыкание орбиты действия связной группы связно.*

Доказательство. Замыкание орбиты точки x есть замыкание образа отображения $\varphi\colon G \to X$, заданного формулой $g \to gx$. Его алгебра функций есть фактор $k[X]$ по ядру φ^* — эта алгебра оказывается вложенной в $k[G]$ посредством φ^*. Так как G связна, в ней нет нетривиальных идемпотентов, а значит их нет и в любой подалгебре. □

Следующая фундаментальная теорема объясняет, почему аффинные алгебраические группы иногда называют «линейными алгебраическими группами».

Теорема 7.1. *Любая аффинная алгебраическая группа изоморфна некоторой алгебраической подгруппе группы невырожденных операторов.*

Доказательство. Начнем со следующей леммы.

Лемма 7.5. *У любой аффинное алгебраической группы есть точное алгебраическое действие на конечномерном пространстве.*

Доказательство. Действие G на $k[G]$ точно, а значит оно точно и на линейной оболочке орбит порождающих алгебры $k[G]$. Каждая из этих орбит конечномерна, всего их конечное количество. Значит, есть конечномерное пространство, где G действует точно и алгебраично. $\square$

Таким образом, мы получили инъективный морфизм алгебраических групп $G \to \mathrm{GL}(V)$. Осталось показать, что образ этого отображения замкнут. Заметим, что G действует на $\mathrm{GL}(V)$ и образ построенного морфизма — одна из орбит этого действия. Кроме того, все орбиты изоморфны. Действительно, орбиты матриц A и B получаются друг из друга правым умножением на $A^{-1}B$ и $B^{-1}A$. Так как среди орбит есть замкнутая, они все замкнуты. Что и требовалось.

$\square$

Задача 7.1. Алгебраическая группа G действует транзитивно на множестве X. Докажите, что количество компонент связности X не превосходит количества компонент связности в G.

Задача 7.2. Докажите, что центр алгебраической группы является её алгебраической подгруппой.

Задача 7.3. Приведите пример доминантного морфизма в неприводимое множество, образ которого не является открытым.

Задача 7.4. Опишите орбиты и их замыкания для действия $\mathrm{GL}_2(\mathbb{C})$ на себе сопряжением.

Задача 7.5. Рассмотрим d-мерный тор $(\mathbb{C}^*)^d$ как аффинную алгебраическую группу. Докажите, что элементы конечного порядка задают в ней всюду плотное множество в топологии Зарисского.

Задача 7.6. Докажите, что коммутант алгебраической группы является её алгебраической подгруппой. (лемма 8.2)

Лекция 8 Разрешимые алгебраические группы.

Определение 8.1. Алгебраическая группа G называется *разрешимой*, если она разрешима как абстрактная группа.

Определение 8.2. Морфизм алгебраических групп $G \to k^*$ называется *характером*. Характеры можно поточечно умножать и они образуют *группу характеров*, $\mathrm{Hom}(G, k^*)$.

Рассмотрим линейное представление алгебраической группы G в пространстве V. Вектор $v \in V$ такой, что подпространство $\langle v \rangle$ является G-инвариантным, называется *полуинвариантом*. По полуинварианту v можно определить характер χ так, чтобы $gv = \chi(g)v$. Этот характер называется *весом* полуинварианта v.

Фундаментальным фактом о характерах групп (не только алгебраических) является *лемма Артина*:

Лемма 8.1. *Различные характеры группы G линейно независимы над k.*

Лемма 8.2. *Коммутант связной группы G — её связная алгебраическая подгруппа.*

Доказательство. Рассмотрим отображения $\varphi_n \colon G^{2n} \to G$, заданные формулой $(x_1, y_1, x_2, y_2, \ldots, x_n, y_n) \to x_1 y_1 x_1^{-1} y_1^{-1} \cdot \ldots \cdot x_n y_n x_n^{-1} y_n^{-1}$. Очевидно, что $\mathrm{Im}\, \varphi_n \subset \mathrm{Im}\, \varphi_{n+1}$. Тогда замыкания $\overline{\mathrm{Im}\, \varphi_n}$ образую неубывающую цепочку замкнутых множеств, которая стабилизируется. Пусть она стабилизируется на N-ом шаге, обозначим это замкнутое множество через X. Заметим, что X связно, так как является образом неприводимого множества. Осталось показать, что $X = [G, G]$.

Обозначим $Y = \mathrm{Im}\, \varphi_N$. Достаточно показать, что $YY^{-1} = X$, так как $YY^{-1} \subset [G, G]$. Y является образом доминантного морфизма в X, а значит содержит Y' открытое в X. Рассмотрим любой элемент $x \in X$. Тогда $Y'x$ также открыто в X и в силу связности X пересекается с Y'. Значит $y_1 x = y_2$, то есть $x = y_1^{-1} y_2$ для некоторых $y_1, y_2 \in Y'$. Что и требовалось. □

Теорема 8.1. *(теорема Ли-Колчина) Пусть G — связная разрешимая подгруппа в GL_n. Тогда в некотором базисе все элементы подгруппы G являются верхнетреугольными матрицами.*

Доказательство. Доказательство теоремы разбивается на два шага:

1. Доказать, что в любом линейном представлении группы G есть общий собственный вектор;

2. Индуктивно построить искомый базис, выбирая собственный вектор и переходя к фактор-представлению.

Этому паттерну следуют доказательства ещё нескольких теорем того же типа: теорем Ли и Энгеля для алгебр Ли и теоремы Ли для групп Ли.

Докажем сначала, что в любом представлении связной разрешимой группы есть общий собственный вектор (иначе говоря, инвариантное одномерное подпространство). Доказывать это будем индукцией по длине ряда коммутантов.

Перейдя к минимальному инвариантному подпространству, можно считать, что группа G действует на пространстве V неприводимо. По предположению индукции, у группы $[G, G]$ есть в V собственный вектор v, соответствующий характеру χ. Пусть $g \in G$, $c \in [G, G]$: $c(gv) = g(g^{-1}cg)v = \chi(g^{-1}cg)gv$. Таким образом, gv также является $[G, G]$-полуинвариантом, но, возможно, с другим весом. Полуинварианты разных весов линейно независимы по лемме Артина, а значит подпространств $[G, G]$-полуинвариантов в V конечное количество. Подгруппа G_χ, переводящая инварианты веса χ в инварианты веса χ замкнута и имеет конечный индекс. В связной группе такого быть не может (так как такая группа была бы приводима), а значит все веса полуинвариантов одинаковы.

Получается, что вся G-орбита v состоит из полуинвариантов веса χ, то есть таково все пространство V в силу неприводимости. Значит, $[G,G]$ действует на V умножениями на скаляр. Кроме того, $[G,G] \subset \mathrm{SL}_n$, то есть соответствующий скаляр должен быть равен корню из единицы степени $\dim V$. Из связности $[G,G]$ следует, что $[G,G]$ действует на V тривиально.

Так как коммутант действует тривиально, получаем семейство коммутирующих операторов на пространстве V. У них, как известно, есть общий собственный вектор.

Теперь из существования собственного вектора выведем утверждение теоремы. Докажем его индукцией по размерности пространства. Выделим общий собственный вектор v. Он будет первым базисным вектором. Осталось выбрать подходящий базис в факторпредставлении $V/\langle v\rangle$. В нем действует группа G' (она является образом G под действием гомоморфизма ограничения). Будучи фактором связной разрешимой группы, она связна и разрешима. Переход индукции доказывает теорему. □

Эта теорема дает мощный инструмент для исследования факторов в композиционном ряду. Через U_n будем обозначать подгруппу верхнетреугольных матриц в GL_n. Рассмотрим в ней также подгруппы $U_{n,k}$, где на диагонали стоят единицы, а на последующих k диагоналях нули. Тогда образуется цепочка групп $U_n \supset U_{n,0} \supset \ldots \supset U_{n,n-1} = \{e\}$. Все эти группы нормальны в U_n. Кроме того, $U_n/U_{n,0} = (k^*)^n$ и $U_{n,k}/U_{n,k+1} = k^{n-1-k}$.

Рассмотрим разрешимую связную подгруппу $G \subset \mathrm{GL}_n$. Пусть уже выбран базис, в котором она верхнетреугольна. Тогда получаем цепочку нормальных подгрупп $G \supset G \cap U_{n,0} \supset \ldots \supset G \cap U_{n,n-1} = \{e\}$. Факторы соседних подгрупп в этом ряду являются либо подгруппой n-мерного тора в случае $G/\left(G \cap U_{n,0}\right)$, либо подгруппой векторного пространства по сложению в остальных случаях. Поэтому задача выяснения вида факторов в построенном композиционном ряду сводится к задаче изучения алгебраических подгрупп тора и векторного пространства.

Лемма 8.3. *Замкнутая подгруппа группы k^n имеет вид k^m и является подпространством.*

Доказательство. Обозначим эту подгруппу через H. Достаточно доказать, что для любого ненулевого $v \in H$ вся прямая kv тоже лежит в H. Рассмотрим пересечение этой прямой и H. Они заведомо пересекаются по точкам $\mathbb{Z}v$, но их пересечение должно быть замкнутым подмножеством прямой. Так как единственным бесконечным замкнутым подмножеством прямой является сама прямая, $kv \subset H$. Что и требовалось. □

Теорема 8.2. *Замкнутая подгруппа тора $(k^*)^n$ изоморфна прямому произведению $(k^*)^m \times H$ тора на конечную группу H.*

Доказательство. Основная идея доказательства в том, что подгруппа тора однозначно задается характерами, которые на ней тождественно равны единице. В этом смысле торы и аффинные пространства представляют собой две крайности — у тора «много» характеров, а у аффинного пространства нет нетривиальных характеров (задача 8.4).

Лемма 8.4. *Характеры тора $T = (k^*)^n$ образуют базис $k[T]$ как векторного пространства.*

Доказательство. Алгебра $k[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$ имеет базис из элементов $x_1^{m_1} \cdot \ldots \cdot x_n^{m_n}$, где $m_i \in \mathbb{Z}$. Все эти функции являются характерами. Более того, они являются *различными* характерами, а значит ни одна их линейная комбинация характером не является. □

Для замкнутой подгруппы $T' \subset T$ через $A(T')$ обозначим множество всех характеров, которые тождественно равны единице на T'.

Лемма 8.5. *Пусть $T' \subset T$ — замкнутая подгруппа, а I — соответствующий ей идеал (то есть ядро $k[T] \to k[T']$). Тогда идеал порожден множеством $\{\chi - 1 | \chi \in A(T')\}$.*

Доказательство. Рассмотрим произвольный элемент $f \in I$. f суть есть линейная комбинация мономов, то есть линейная зависимость на характеры в T'. По лемме Артина, среди них найдутся равные, пусть χ_1 и χ_2. Тогда $\chi_1^{-1}\chi_2 \in A(T')$. Вычитая $c(\chi_1 - \chi_2) = c\chi_1(\chi_1^{-1}\chi_2 - 1)$ из f, мы уменьшаем количество мономов в f. Таким образом, f, а значит и весь I лежит в идеале порожденном $\{\chi - 1 | \chi \in A(T')\}$. □

Следствие 8.1. *Из равенства $A(T_1) = A(T_2)$ следует $T_1 = T_2$.*

Возникает разумный вопрос: как может выглядеть множество $A(T')$? Как мы уже видели, характеры тора T образуют решетку $\mathbb{Z}^n$. В этой решетке любое множество $A(T')$ является подрешеткой. Известно, что для любой подрешетки можно выбрать такой базис $e_1, \ldots, e_n$ в большой решетке, что базис подрешетки будет иметь вид $a_1 e_1, \ldots, a_k e_k$. Как мы знаем из доказательства леммы 8.5 идеал соответствующей подгруппы будет порожден многочленами $x_i^{a_i} - 1$. Отсюда утверждение теоремы очевидно — последние $n-k$ координат дадут тор, а первые k — конечную коммутативную группу.

□

Результатом всей этой нашей деятельности является следующая теорема:

Теорема 8.3. *Пусть группа G — связная разрешимая алгебраическая группа. Тогда в ней найдется такой ряд подгрупп $G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$, где G_i нормальна в G_{i-1}, причем фактор G_0/G_1 — конечная коммутативная группа, следующие несколько факторов изоморфны k^*, а остальные изоморфны k.*

Задача 8.1. Докажите, что элементы конечного порядка в торе $(k^*)^n$ всюду плотны в топологии Зарисского.

Задача 8.2. Приведите пример несвязной разрешимой группы, для которой теорема Ли-Колчина неверна.

Задача 8.3. Докажите, что любая подрешетка в группе характеров тора соответствует некоторой замкнутой подгруппе.

Задача 8.4.

1. Докажите, что у группы k^n нет нетривиальных характеров (указание: какому элементу в алгебре регулярных функций соответствует характер?);
2. Пусть в связной группе G для любого элемента $g \neq e$ существует характер χ такой, что $\chi(g) \neq 1$. Докажите, что G — тор.

Задача 8.5. Докажите, что любое линейное представление тора диагонализуемо.

Лекция 9 Структура расширений Пикара-Вессио.

Одним из основных шагов на пути к дифференциальному соответствию Галуа будет «выделение» из расширения Пикара-Вессио $E \supset F$ такой F-подалгебры, которую можно было бы интерпретировать как алгебру $F[G(E/F)]$. Определим эту алгебру.

Определение 9.1. Фиксируем расширение Пикара-Вессио дифференциальных полей $E \supset F$ с полем констант C. Через $T(E/F)$ (иногда просто через T) будем обозначать множество таких $f \in E$, что C-линейная оболочка орбиты f под действием $G(E/F)$ конечномерна.

Лемма 9.1. *В условиях определения 9.1:*

1. *$T(E/F)$ совпадает со множеством таких $f \in E$, что f является решением уравнения $Lf = 0$ для некоторого линейного дифференциального оператора с коэффициентами из F;*
2. *$T(E/F)$ является F-подалгеброй в E.*

Доказательство. 1. Докажем, что $T(E/F)$ лежит в описанном множестве. Фиксируем $f \in T(E/F)$. Обозначим C-линейную оболочку орбиты f через V. Рассмотрим подполе $E_1 \supset F$ порожденное над F в E пространством V. Оно удовлетворяет условиям предложения 4.1, а значит является расширением Пикара-Вессио. Значит, существует оператор L с коэффициентами из F такой, что $Lf = 0$.

   Проверим обратное включение. Пусть $f \in E$ таков, что $Lf = 0$. Тогда $G(E/F)$ переводит f только в другие решения этого уравнения. Значит C-линейная оболочка орбиты f лежит в пространстве решений этого уравнения, а значит конечномерна.

2. Так как $(D - \frac{a'}{a})a = 0$, $F \subset T(E/F)$. Для $f \in T(E/F)$ через $V(f)$ обозначим C-линейную оболочку орбиты f. Тогда тот факт, что $T(E/F)$ — алгебра, непосредственно следует из соотношений $V(f+g) \subset V(f) + V(g)$ и $V(fg) \subset V(f)V(g)$ (см. задачу 2.5).

□

Нашей основной целью в этой лекции будет доказательство того, что $T(E/F)$ конечнопорождена как F-алгебра. Тогда её можно будет рассматривать как алгебру функций на некотором алгебраическом многообразии.

Определение 9.2. Пусть G — алгебраическая группа над алгебраически замкнутым полем C. Обозначим $X(G) = \mathrm{Hom}(G, C^*)$ — *группу характеров* группы G.

Заметим, что G-полуинварианты в E образуют группу по умножению, а отношение двух полуинвариантов одного веса является инвариантом.

Кроме того, так как все элементы орбиты полуинварианта пропорциональны, все полуинварианты действия $G(E/F)$ на E лежат в $T(E/F)$.

Лемма 9.2. *Пусть $f \in T(E/F)$ и $f_1, \dots, f_n$ — C-базис линейной оболочки $G(E/F)$-орбиты элемента f. Тогда $w(f_1, \dots, f_n)$ является полуинвариантом.*

Доказательство. Каждому элементу $g \in G(E/F)$ соответствует C-линейный оператор $\bar{g}$ на пространстве порожденном $f_1, \dots, f_n$. Утверждение леммы следует из соотношения: $g \cdot w(f_1, \dots, f_n) = \det(\bar{g}) w(f_1, \dots, f_n)$. □

Лемма 9.3. *Пусть S — $G(E/F)$-инвариантная F-подалгебра в $T(E/F)$, и I — $G(E/F)$-инвариантный идеал в ней. Тогда в I лежит полуинвариант.*

Доказательство. Пусть f — некоторый элемент I. Тогда линейная оболочка его орбиты лежит в I, а значит там же будет лежать и полуинвариант построенный в лемме 9.2. $\square$

Рассмотрим группу весов полуинвариантов $G(E/F)$-действия на T. Так как это подгруппа конечнопорожденной абелевой группы $X\left(G(E/F)\right)$ (задача 9.2), она конечнопорождена. Рассмотрим конечное множество Ξ, куда будет входить по одному полуинварианту на каждую из порождающих характеров этой группы и по одному на каждый характер, обратный к порождающей. Иначе говоря, множество Ξ таково, что я могу получить полуинвариант любого веса, взяв произведение нескольких (не обязательно различных) элементов Ξ.

Лемма 9.4. *Для любой $G(E/F)$-инвариантной F-подалгебры $S \subset T(E/F)$ алгебра $S[\Xi^{-1}]$ не содержит нетривиальных $G(E/F)$-инвариантных идеалов.*

Доказательство. Пусть такой идеал имеется. Тогда в нем лежит полуинвариант s веса χ. Рассмотрим полуинвариант t, являющийся произведением элементов Ξ, веса χ. Тогда st^{-1} — инвариант, а значит по предложения 3.2 лежит в F, что противоречит нетривиальности идеала. $\square$

Нам хотелось бы теперь говорить о построенных F-алгебрах на геометрическом языке. Для этого необходимо перейти к алгебраически замыканию F. Поэтому вместо E будем рассматривать $\overline{F} \otimes_F E$, вместо T — $\overline{F} \otimes_F T$. Самый нетривиальный шаг — расширение поля скаляров у группы $G(E/F)$. Получится группа $\overline{G}$, алгебра функций на которой будет $\overline{F} \otimes_C C\left[G(E/F)\right]$, где все отображения алгебры Хопфа действуют на первый сомножитель тривиально. Покажем, что доказанные свойства сохранятся и после замыкания основного поля.

Лемма 9.5. *Пусть S — целостная алгебра над полем k $(\operatorname{char} k = 0)$. На ней действует алгебраическая группа G, причем S не содержит нетривиальных G-инвариантных идеалов. Обозначим $\bar{S} = S \otimes_k \bar{k}$.*

1. *$\bar{S}$ не содержит нильпотентов;*

2. *в $\bar{S}$ нет нетривиальных G-инвариантных идеалов;*

Доказательство.

1. Алгебра $\bar{S}$ вкладывается в тензорное произведение двух полей характеристики 0, а значит не содержит нильпотентов по лемме 3.1.

2. Пусть в $\bar{S}$ есть нетривиальный G-инвариантный идеал I. Рассмотрим элемент $\sum\limits_{i=1}^{n} a_i \otimes b_i \in I$ с наименьшим n. Рассмотрим также идеал $J = \{c_1 | \exists c_2, \ldots, c_n \sum c_i \otimes_k b_i \in I\}$. J является G-инвариантным идеалом, а значит содержит единицу. Тогда для некоторых $c_2, \ldots, c_n$ $x = 1 \otimes b_1 + c_2 \otimes b_2 + \ldots + c_n \otimes b_n \in I$. Для каждого $g \in G$ выражение $g(x) - x$ содержит меньше n слагаемых, а значит равно нулю. Значит, x инвариантен, откуда следует что $x \in \bar{k}$.

$\square$

Покажем теперь, что если эти алгебры «достаточно большие», то соответствующее действие имеет ещё и тривиальные стабилизаторы.

Пусть S — универсальная алгебра решений расширения $E \supset F$, P — выбранный в ней максимальный идеал. Тогда через $\tilde{S}$ обозначим образ S/P в E. На алгебре $\tilde{S}$ действует группа $G(E/F)$. Рассмотрим теперь алгебру $\overline{F} \otimes_F S$, в ней есть дифференциальный идеал $\overline{F} \otimes_F P$, фактор по этому идеалу изоморфен $\overline{F} \otimes_F \tilde{S}$. Действие C-группы $G(E/F)$ на $\tilde{S}$ продолжается до действия этой же группы над $\overline{F}$ на $\overline{F} \otimes_F \tilde{S}$. Оказывается, полученное действие имеет тривиальный стабилизатор.

Лемма 9.6. *Пусть $\varphi\colon \overline{F} \otimes_F \tilde{S} \to \overline{F}$ и $\sigma \in \bar{G}$ таковы, что $\sigma(\varphi) = \varphi$. Тогда $\sigma = e$.*

Доказательство. Поднимемся в $\overline{F} \otimes_F S$. Рассмотрим матрицу из присоединяемых элементов $Y = (y_{i,j})$ (см. обозначения из доказательства предложения 2.3). Элемент σ представляется некоторой $\overline{F}$-матрицей T так, что выполнено матричное равенство: $\sigma(Y) = TY$. Применив к обеим частям равенства φ, получим $\tilde{Y} = T\tilde{Y}$. Однако, определитель $\tilde{Y}$ равен образу вронскиана переменных $y_{1,0}, \ldots, y_{n,0}$ при отображении φ, то есть не равен нулю. Таким образом, это матричное уравнение имеет единственное решение $T = E$. Что и требовалось. □

Теперь мы готовы доказать основной результат лекции:

Теорема 9.1. *Пусть F — дифференциальное поле с алгебраически замкнутым полем констант, и $E \supset F$ — расширение Пикара-Вессио. Тогда алгебра $T(E/F)$ конечнопорождена над F.*

Доказательство. Рассмотрим в E образ универсальной алгебры решений $\tilde{S}$. Это конечнопорожденная $G(E/F)$-инвариантная алгебра, лежащая в $T(E/F)$, поле частных которой равно E. Добавив к ней Ξ^{-1} как в лемме 9.4, можем считать, что в ней нет нетривиальный $G(E/F)$-инвариантных идеалов.

Обозначим полученную алгебру через A и пусть $\overline{A} = \overline{F} \otimes_F A$. $\overline{A}$ можно считать алгеброй функций на множестве X, снабженном действием $\bar{G}$. Любой максимальный идеал в $\overline{A}$ задает максимальный идеал в $\overline{F} \otimes \tilde{S}$. Таким образом, стабилизатор действия $\bar{G}$ на X имеет тривиальный стабилизатор в каждой точке.

Пусть $\overline{A} \neq \overline{F} \otimes T(E/F)$. Значит существует промежуточная конечнопорожденная $\bar{G}$-инвариантная алгебра $B = \overline{F}[Y]$ без нетривиальных $\bar{G}$-идеалов. Вложение $\overline{A} \to B$ задает доминантный морфизм $Y \to X$, перестановочный с $\bar{G}$-действием. Его образ открыт, а дополнение замкнуто и $\bar{G}$-инвариантно. То есть, морфизм сюръективен. Пусть он не инъективен. Тогда у точки $x \in X$ есть два разных прообраза $y_1, y_2 \in Y$. Так как действие $\bar{G}$ на Y транзитивно, существует $g \in \bar{G}$, что $g(y_1) = y_2$, то есть $g(x) = x$, что противоречит тривиальности стабилизатора x.

А значит, $\overline{A} = \overline{F} \otimes T(E/F)$, откуда следует конечнопорожденность последней из алгебр. Из неё же, согласно 10.3, следует конечнопорожденность $T(E/F)$.

□

Задача 9.1. Группа G действует на множестве X без замкнутых G-инвариантных подмножеств. Докажите, что это действие транзитивно.

Задача 9.2. Докажите, что группа характеров алгебраической группы G конечнопорождена.

Задача 9.3. Для расширений из задачи 3.1 найдите алгебру $T(E/F)$.

Задача 9.4. Приведите пример, когда частное двух элементов $T(E/F)$ не лежит в $T(E/F)$.

Лекция 10 Основная теорема дифференциальной теории Галуа.

Теорема 10.1. *Пусть F — дифференциальное поле с алгебраически замкнутым полем констант C. Пусть $E \supset F$ — расширение Пикара-Вессио. Тогда имеет место изоморфизм:*

$$\bar{T} = \bar{F} \otimes_F T(E/F) \to \bar{F} \otimes_C C[G(E/F)]$$

Доказательство. Действие $G(E/F)$ на $T(E/F)$ продолжается до действия $\bar{G}$ на $\bar{T}(E/F)$. По лемме 9.5, в $\bar{T}$ нет нетривиальных $\bar{G}$-инвариантных идеалов.

Фиксируем точку $x \in X$, иначе говоря гомоморфизм $f_x \colon \bar{T} \to \bar{F}$. Тогда композиция $(f_x \otimes 1)\Delta$, где $\Delta \colon \bar{T} \to \bar{T} \otimes \bar{F}[\bar{G}]$, задает отображение $\bar{T} \to \bar{F}[\bar{G}]$. Геометрически оно соответствует отображению $\bar{G} \to X$ заданному формулой $g \to g(x)$. Ядро его является $\bar{G}$-инвариантным идеалом, то есть равно нулю. Так как этот морфизм является доминантным морфизмом в неприводимое многообразие, его образ содержит открытое множество (лемма 7.3). Так как на образе $\bar{G}$ действует транзитивно, образ является открытым множеством. Дополнение к нему является инвариантным замкнутым множеством, а значит пусто. Таким образом, построенное отображение сюръективно.

Докажем его инъективность. Пусть отображение не инъективно, тогда у точки x есть нетривиальный стабилизатор в $\bar{G}$. Это противоречит лемме 9.6. □

Теперь мы можем перейти к доказательству основной теоремы теории Галуа в дифференциальном случае.

У нас есть два отображения:

1. сопоставляющее промежуточному подполю K ($E \supset K \supset F$) подгруппу $G(E/K) \subset G(E/F)$; (алгебраичность этой подгруппы утверждается задачей 10.4)
2. сопоставляющее подгруппе $H \subset G(E/F)$ подполе E^H;

Для начала нужно проверить, что их композиция в прямом и обратном порядке даёт тождественное отображение. Первая часть почти очевидна — это задача 3.4. Вторая теперь легко выводится из теоремы 10.1:

Лемма 10.1. *Рассмотрим алгебраическую подгруппу $H \subset G(E/F)$. Тогда она изоморфна $G(E/E^H)$.*

Доказательство. Прежде всего, заметим, что в доказательстве теоремы 10.1 от группы $G(E/F)$ требовалось только, чтобы $E^{G(E/F)} = F$. Иначе говоря, утверждение теоремы 10.1 верно для любой подгруппы в $G(E/F)$ с таким свойством.

Для расширения Пикара-Вессио $E \supset E^H$ обе группы H и $G\left(E/E^H\right)$ обладают требуемым свойством. Обозначим через $\overline{T}$ алгебру $\overline{E^H} \otimes_{E^H} T\left(E/E^H\right)$, а через X — соответствующее алгебраическое множество. Выбрав в теореме 10.1 одну и ту же точку для построение измоморфизма, мы получим изоморфизмы между $\overline{E^H}[X]$ и $\overline{E^H}[H]$ и между $\overline{E^H}[X]$ и $\overline{E^H}\left[G(E/E^H)\right]$ согласованные с вложением H в $G(E/E^H)$. Таким образом, эти группы совпадают. □

Отдельную ценность и трудность представляет собой соответствие Галуа в случае нормальных подгрупп. Одна из половин соответствия тривиальна:

Лемма 10.2. *Пусть $E \supset F$ — расширение Пикара-Вессио, и K — промежуточное подполе такое, что $K \supset F$ также является расширением Пикара-Вессио. Тогда подгруппа $G(E/K)$ в $G(E/F)$ нормальна.*

Доказательство. Это прямое следствие «нормальности» расширений Пикара-Вессио — следствия 3.2. Это следствие утверждает, что все вложения расширения Пикара-Вессио в большее расширение имеют один и тот же образ. Отсюда следует, что все автоморфизмы $G(E/F)$ переводят K обратно в K, что, очевидно, влечет нормальность $G(E/K)$ в $G(E/F)$. □

В обратную сторону утверждение ощутимо содержательнее:

Теорема 10.2. *Пусть H — нормальная подгруппа в $G(E/F)$. Тогда $E^H \supset F$ — расширение Пикара-Вессио, и гомоморфизм ограничения $G(E/F)$ в $G(E^H/F)$ — сюрьективный морфизм алгебраических групп.*

Доказательство. Рассмотрим подалгебру $T = T(E/F)$. Утверждение о том, что $E^H \supset F$ — расширение Пикара-Вессио теперь следует из двух фактов:

1. T^H конечнопорождена;

2. E^H является полем частных алгебры T^H.

Действительно, достаточно теперь взять в T^H конечномерное H-инвариантное C-подпространство, содержащее все порождающие T^H. Тогда $E^H \supset F$ будет расширением с группой $G(E/F)/H$ по лемме 4.1. Осталось эти факты доказать:

1. Воспользуемся теоремой 10.1: $\overline{F} \otimes T^H = \left(\overline{F} \otimes T\right)^H = \overline{F} \otimes C[G]^H = \overline{F} \otimes C[G/H]$ (последнее равенство следует из задачи 10.5). Последняя алгебра конечнопорождена, откуда следует конечнопорожденность T^H (см. задачу 10.3).

2. Рассмотрим некоторый элемент $f \in E^H$. С ним связан H-инвариантный идеал знаменателей $I = \{x \in T | xf \in T\}$. Аналогично лемме 9.2, рассмотрев вронскиан, получаем, что в этом идеале лежит полуинвариант t веса χ. Тогда tf также полуинвариант веса χ. Если бы в T нашелся полуинвариант u веса χ^{-1}, мы получили бы представление $f = \frac{u(tf)}{ut}$, где и числитель, и знаменатель лежат в T^H.

   Докажем просто, что для любого характера χ группы H в алгебре $C[G(E/F)]$ найдется полуинвариант веса χ. Обозначим для краткости $G(E/F)$ через G. Тогда из теоремы 10.1 будет следовать существование такого полуинварианта в T. Рассмотрим в H подгруппу H_0 — пересечение ядер всех характеров. Из обычных теоретико-групповых соображений следует, что H_0 нормальна не только в H, но и в G, что задает инъекцию $H/H_0 \to G/H_0$, которая двойственна сюръекции $C[G/H_0] \to C[H/H_0]$. В алгебре $C[H/H_0]$ есть полуинварианты всех весов, а алгебра $C[G/H_0]$ вкладывается в $C[G]$ в силу нормальности H_0 (это вложение двойственно канонической сюръекции на фактор). Значит, надо доказать, что в прообразе любого полуинварианта $C[H/H_0]$ в $C[G/H_0]$ есть полуинвариант.

   Для этого забудем о том, что у нас есть структура алгебры и просто посмотрим на отображение $C[G/H_0] \to C[H/H_0]$ как на отображение линейных представлений группы H/H_0. Тогда, выбрав справа полуинвариант, а слева конечномерное подпредставление в его прообразе, получим отображение H/H_0-представлений $V \to W$, где W одномерно. Осталось доказать, что ядро этого отображения выделяется прямым слагаемым.

   Согласно задаче 8.4, группа H/H_0 является подгруппой тора, откуда, согласно 8.5, её представление в пространстве V диагонализуемо. Что и требовалось.

□

Задача 10.1. Докажите, что если F алгебраически замкнуто, что группа $G(E/F)$ связна.

Задача 10.2. Над полем $F = \mathbb{C}(z)$ рассмотрим дифференциальный оператор $L = y^{(2)} + 2zy^{(1)}$. Пусть базис его пространства решений в соответствующем расширении Пикара-Вессио состоит из 1 и f. Докажите, что:

1. $f' \notin F$;
2. $f \notin F(f)$.

Задача 10.3. Пусть есть расширение полей $K \supset k$ и k-алгебра A. Докажите, что из конечнопорожденности K-алгебры $K \otimes_k A$ следует конечнопорожденность алгебры A.

Задача 10.4. Пусть $E \supset F$ — расширение Пикара-Вессио и K — промежуточное подполе. Докажите, что $G(E/K)$ — замкнутая подгруппа в $G(E/F)$.

Задача 10.5. Пусть H— нормальная замкнутая продгруппа в G. Докажите, что алгебра инвариантов $k[G]^H$ изоморфна $k[G/H]$.

Лекция 11 Виртуально разрешимые группы и расширения Лиувилля; интегрируемость в элементарных функциях.

Определение 11.1. Группа алгебраическая группа G называется *виртуально разрешимой*, если разрешима группа G_0.

Из теоремы 8.3 следует, что у виртуально разрешимой группы есть композиционный ряд, где первый фактор конечен, несколько последующих изоморфны k^*, а остальные изоморфны k.

Таким образом, для того, чтобы понять, как устроено расширение Пикара-Вессио с разрешимой группой Галуа, нужно понять, что из себя представляют расширения с конечной группой Галуа, k^* и k.

Предложение 11.1. *Пусть $E \supset F$ — расширение Пикара-Вессио с конечной группой $G(E/F)$. Тогда $E = F(a)$, где a алгебраичен над F.*

Доказательство. Рассмотрим соответсвующий оператор L и пространство его решений V. Если мы докажем, что все элементы V алгебраичны над F, то E будет порождаться над F конечным числом алгебраичных элементов, то есть, по теореме о примитивном элементе, будет порождаться и одним. Возьмем любой элемент $f \in V$. Пусть $f_1, \ldots, f_k$ — его образы под действием $G(E/F)$. Рассмотрим многочлен $\prod(x - f_i)$. Его коэффициенты $G(E/F)$-инвариантны, а значит лежат в F. Кроме того, f его корень. Что и требовалось. $\square$

Предложение 11.2. *Пусть $E \supset F$ — расширение Пикара-Вессио, и $G(E/F) \cong {}^*$ ($C = C(E) = C(F)$). Тогда $E = F(a)$, где a трансцендентен над F и $\frac{a'}{a} \in F$.*

Доказательство. Рассмотрим соответствующий оператор L и пространство его решений V. V инвариантно относительно действия $G(E/F)$, кроме того, в силу задачи 8.5 это представление диагонализуемо. Все характеры одномерного тора имеют вид $\chi(x) = x^k$ для некоторого $k \in \mathbb{Z}$. Пусть $\chi_1, \ldots, \chi_m$ — характеры, которыми действует $G(E/F)$ на V. Если соответсвующие степени k имеют общий делитель d, то корни d-ой степени из единицы действуют тривиально на V, а значит и на $G(E/F)$, чего не может быть. Значит, соответствующие степени взаимно просты и среди характеров $\chi_1^{l_1} \ldots \chi_m^{l_m}$ ($l_i \in \mathbb{Z}$) есть характер $\chi(x) = x$. Взяв решения L в соответствующих степенях, получим полуинвариант такого веса. Итак, мы построили $a \in E$, на которое элемент $x \in C^*$ действует умножением на себя.

Заметим, что a трансцендентен над F. Так как минимальный многочлен p для a должен зануляться и во всех xa, где $x \in C^*$, что невозможно.

Рассмотрим теперь элемент $\frac{a'}{a}$. Заметим, что он $G(E/F)$-инвариантен, то есть $\frac{a'}{a} = \alpha \in F$. Так как $C(E) = C(F)$, $\alpha \neq 0$. Значит $E_1 = F(a)$, $G(E/F)$-инвариантное дифференциальное поле, порожденное $G(E/F)$-инвариантным пространством Ca, причем $E_1^{G(E/F)} = F$. Таким образом, $E \supset F$ и $E_1 \supset F$ являются расширениями Пикара-Вессио с одной и той же группой Галуа, причем $E_1 \subset E$. Значит, $E = F(a)$, что и требовалось.

$\square$

Предложение 11.3. *Пусть $E \supset F$ — расширение Пикара-Вессио, и $G(E/F) \cong C$. Тогда $E = F(a)$, где a трансцендентен над F и $a' \in F$.*

Доказательство. Пусть L — соответствующий оператор и V — его пространство решений. Рассмотрим такой базис $e_1, \ldots, e_m$ в V, в котором действие $G(E/F)$ будет верхнетреугольно. Так как у $G(E/F)$ нет нетривиальных характеров (см. задачу 8.4), e_1 является $G(E/F)$-инвариатным, то есть $e_1 \in F$. Рассмотрим минимальное k такое, что $e_k \notin F$. Тогда элемент x будет переводить его в $e_k + xf$, где $f \in F$. Рассмотрим $a = \frac{e_k}{f}$. $a \notin F$ и x переводит a в $a + x$, а a' в себя. Значит, $a' \in F$. Рассуждая аналогично предложению 11.2, доказываем, что a трансцендентен над F и $E = F(a)$. $\square$

Теперь мы готовы охарактеризовать расширения Пикара-Вессио с виртуально разрешимой группой автоморфизмов.

Теорема 11.1. *Пусть $E \supset F$ — расширение Пикара-Вессио с виртуально разрешимой группой автоморфизмов G. Тогда для G есть композиционный ряд $G = G_0 \supset G_1 \supset \ldots \supset G_n = \{e\}$, где G_0/G_1 конечна, $G_k/G_{k+1} \cong C^*$ при $1 \leqslant k \leqslant m$, $G_k/G_{k+1} \cong C$ при $m < k < n$. Кроме того, существует цепочка подполей $E = F_n \supset \ldots \supset F_0 = F$, что $F_k \supset F_{k-1}$ — расширение Пикара-Вессио и:*

1. *$F_1 = F_0(a_1)$, причем a_1 алгебраичен над F_0;*
2. *при $1 < k \leqslant m+1$: $F_k = F_{k-1}(a_k)$, причем a_k трансцендентен над F_k и $\frac{a_k'}{a_k} \in F_{k-1}$;*
3. *при $m+1 < k \leqslant n$: $F_k = F_{k-1}(a_k)$, причем a_k трансцендентен над F_k и $a_k' \in F_{k-1}$.*

Доказательство. Утверждение получается тривиальной композицией утверждений теорем 8.3 и 10.2 и предложений 11.3, 11.2 и 11.1. □

На самом деле, теорема 11.1 — не совсем то, что нам нужно. Действительно, мы показали, что расширения с виртуально разрешимой группой автоморфизмов получается путем добавлений решений уравнений, экспонент и интегралов. Однако, вообще говоря, итерация нескольких расширений Пикара-Вессио не является расширением Пикара-Вессио (см. задачу 11.2).

Реально хочется показать, что все уравнения, которые могут быть полностью решены при помощи трех элементарных операций имеют виртуально разрешимую группу автоморфизмов. Об этом нам говорит следующая теорема:

Теорема 11.2. *Пусть $K \supset F$ — расширение без новых констант, причем имеется башня подполей: $K = F_n \supset \ldots \supset F_0 = F$ такая, что для всякого k выполнено $F_k = F_{k-1}(a_k)$, причем:*

1. *либо a_k алгебраичен над F_{k-1};*
2. *либо $\frac{a_k'}{a_k} \in F_{k-1}$;*
3. *либо $a_k' \in F_{k-1}$.*

Пусть также поле E таково, что $K \supset E \supset F$ и $E \supset F$ — расширение Пикара-Вессио. Тогда группа $G(E/F)$ виртуально разрешима.

Лемма 11.1. *Пусть $K \supset F$ — расширение без новых констант, $K \supset E \supset F$ и $E \supset F$ — расширение Пикара-Вессио. Пусть также $K \supset M \supset F$. Тогда:*

1. *$EM \supset M$ — расширение Пикара-Вессио[1];*
2. *гомоморфизм $G(EM/M) \to G(E/F)$ инъективен и замыкание его образа есть $G(E/E \cap M)$.*

Доказательство. Пусть L — оператор для $E \supset F$, а V — его пространство решений. Так как $E = F\langle V\rangle$, $EM = M\langle V\rangle$. Кроме того, расширение $EK \supset K$ не имеет новых констант. Значит, $EM \supset M$ — расширение Пикара-Вессио.

В силу нормальности расширений Пикара-Вессио, любое преобразование из $G(EM/M)$ переводит E в себя, что и задает гомоморфизм $G(EM/M) \to G(E/F)$. Так как любое преобразование из $G(EM/M)$ задается своими значениями на E, этот гомоморфизм инъективен. Обозначим через H замыкание его образа. Тогда $E^H \subset (EM)^H = M$ и $E \cap M \subset E^H$, то есть $E^H = E \cap M$. В силу леммы 10.1 (то есть, в силу соответствия Галуа) $H = G(E/E \cap M)$. Что и требовалось. □

[1]как и в стандартной теории полей, через EM обозначается минимальное подполе в K содержащее E и M

Доказательство. Будем доказывать это утверждение индукцией по n. Случай $n = 1$ очевиден.

Согласно лемме 11.1, $EF_1 \supset F_1$ является расширением Пикара-Вессио, то есть, по предположению индукции, $G(EF_1/F_1)$ виртуально разрешима. Значит, такова и $G(E/E \cap F_1)$. Рассмотрим теперь тройку $F_1 \supset F_1 \cap E \supset F$. Расширение $F_1 \supset F$ является расширением Пикара-Вессио. Пусть его группа автоморфизмов конечна. Тогда $F_1 \cap E \supset F$ является конечномерным алгебраическим расширением, то есть $G(E/E \cap F_1)$ является подгруппой конечного индекса в $G(E/F)$, откуда следует виртуальная разрешимость последней. Если же $G(F_1/F)$ изоморфна C или C^*, то все её подгруппы абелевы и нормальны, а значит $E \cap F_1 \supset F$ — расширение Пикара-Вессио с абелевой группой автоморфизмов. Тогда $G(E/E \cap F_1)$ нормальна в $G(E/F)$ и фактор абелев. Значит, $G(E/F)$ также виртуально разрешима. Что и требовалось. $\square$

Определение 11.2. Расширения такого типа, как $K \supset F$ из теоремы выше, называются *расширениями Лиувилля.*

Пример 11.1. Над полем $\mathbb{C}(x)$ рассмотрим дифференциальное *уравнение Айри* $y'' - xy = 0$. Его группа Галуа изоморфна $\mathrm{SL}_2(\mathbb{C})$, то есть это уравнение неразрешимо в квадратурах. Однако, доказательство этого факта весьма утомительно, поэтому мы его опустим. Интересующихся отсылаем к примеру 4.29 книги [2].

Заметим, что функцию $\int e^{-x^2}\,\mathrm{dx}$ можно добавить к полю $\mathbb{C}(x)$ при помощи описанных элементарных операций. Однако, известно, что этот интеграл в элементарных функциях не берется. Оказывается, это утверждение тоже под силу дифференциальной теории Галуа.

Определение 11.3. Фиксируем алгебраически замкнутое поле C, на котором дифференцирование действует тривиально. Положим $F = C(x)$, где $x' = 1$. Тогда расширение $F(a_1, \ldots, a_k, b_1, \ldots, b_m) \supset F$ называется полем элементарных функций, если

1. $a_i' \in F$;
2. для всех $1 \leqslant j \leqslant m$ элемент b_j либо алгебраичен над $F(b_1, \ldots, b_{j-1})$, либо $\frac{b_j'}{b_j} \in F(b_1, \ldots, b_{j-1})$.

Лемма 11.2. *Пусть $M \supset E_1, E_2 \supset F$, и $E_i \supset F$ — расширение Пикара-Вессио. Тогда $E_1E_2 \supset F$ также является расширением Пикара-Вессио.*

Доказательство. Пусть L_1 и L_2 — соответствующие дифференциальные операторы, а V_1 и V_2 — их пространства решений. Тогда $E_1E_2 = F\langle V_1\rangle F\langle V_2\rangle = F\langle V_1 + V_2\rangle$. Однако, расширение Пикара-Вессио для пары операторов L_1 и L_2 (здесь существенно, что у обоих операторов коэффициенты в F) в смысле предложения 4.2 также порождается над F пространствами V_1 и V_2. Значит, эти расширения совпадают, то есть оба являются расширениями Пикара-Вессио в силу предложения 4.2. $\square$

Теорема 11.3. *Пусть $E \supset F$ — расширение Пикара-Вессио и $F(a_1, \ldots, a_k, b_1, \ldots, b_m) \supset E$. Тогда связная компонента единицы группы $G(E/F)$ абелева.*

Доказательство. Согласно задаче 11.1, $F(a_1, \ldots, a_k) \supset F$ — расширение Пикара-Вессио. По лемме 11.2, расширение $E \cdot F(a_1, \ldots, a_k) \supset F$ также является расширением Пикара-Вессио. Можем заменить теперь E на $EF(a_1, \ldots, a_k)$, так как $G(E/F)$ является факторгруппой $G\left(EF(a_1, \ldots, a_k)/F\right)$ — из абелевости связной компоненты единицы последней следует то же и для первой.

Рассмотрим цепочку расширений $F(a_1, \ldots, a_k, b_1, \ldots, b_m) \supset E \supset F(a_1, \ldots, a_k)$. К ней применима теорема 11.2, а точнее задача 11.3. Получаем таким образом, что связная компонента $G\left(E/F(a_1, \ldots, a_k)\right)$ — тор. Рассмотрим цепочку расширений Пикара-Вессио $E \supset F(a_1, \ldots, a_k) \supset F$. Согласно задаче 11.1, группа $G_1 = G(F(a_1, \ldots, a_k)/F)$ изоморфна группе векторов. Кроме того, связная компонента единицы группы $G_2 = G(E/F(a_1, \ldots, a_k))$ изоморфна тору. Наконец, интересующая нас группа $G_3 = G(E/F)$ характеризуется тем, что G_2 в ней нормальна, и фактор G_3/G_2 изоморфен G_1. Покажем, что в этом случае связная компонента единицы в G_3 абелева.

Так как G_1 связна, можно рассматривать связные компоненты единицы у G_2 и G_3. Так как G_1 абелева, $[G_3, G_3] \subset G_2$, то есть G_3 — подгруппа тора. Однако, коммутант связной разрешимой группы не может содержать тора и связен, то есть может быть только тривиальной подгруппой тора. Значит, коммутант G_3 тривиален, что и требовалось доказать. $\square$

Пример 11.2. Покажем теперь, что интеграл $\int e^{-x^2}\,\mathrm{dx}$ не записывается в элементарных функциях. Заметим, что он является решением дифференциального уравнения $y'' + 2xy' = 0$, вторым линейной независимым решением которого является единица. Таким образом, найти этот интеграл — то же, что и найти все решения этого уравнения, а значит достаточно показать, что связная компонента единицы в группе Галуа этого уравнения неабелева.

Найдем эту группу. Обозначим $F(x) = \int e^{-x^2}\,\mathrm{dx}$. Тогда группа автоморфизмов должна действовать линейным оператором на пространстве $\langle 1, F(x)\rangle$. На первый вектор автоморфизм действует тождественно, а второй может переводить в $aF(x) + b$, где $a \in \mathbb{C}^*$ и $b \in \mathbb{C}$. На интуитивном уровне это соответствует константе при взятии экспоненты и константе при взятии интеграла, однако, формально говоря, тот факт, что все такие преобразования являются автоморфизмами требует доказательства обоих пунктов задачи 10.2.

Таким образом, группа автоморфизмов получается изоморфна группе аффинных преобразований прямой, которая связна, разрешима, но неабелева. Что и требовалось.

Задача 11.1. Пусть расширение полей без новых констант $F(a_1, \ldots, a_k) \supset F$ таково, что $a_i' \in F$. Докажите, что это расширение является расширением Пикара-Вессио и группа его автоморфизмов изоморфна C^m.

Задача 11.2. Приведите пример расширений Пикара-Вессио $E \supset F$ и $K \supset E$ таких, что $K \supset F$ не является расширением Пикара-Вессио. (указание: в каком случае конечномерное расширение является расширением Пикара-Вессио?)

Задача 11.3. Докажите, что если в теореме 11.2 оставить расширения только первых двух типов, то связная компонента единицы у $G(E/F)$ будет тором.

Задача 11.4. Опишите в общем виде расширение Пикара-Вессио с группой C^2 и все его промежуточные подполя.

Задача 11.5. Докажите, что интеграл $\int \frac{\sin x}{x}\,\mathrm{dx}$ не берется в элементарных функциях.

Список литературы

[1] Атья-Макдональд.

[2] Andy R. Magid, Lectures on differential Galois theory.