С. О. Горчинский. Теории Галуа: классическая и дифференциальная

Листок 1. Расширения полей

Упражнение 1.1. Конечные поля

(i) Пусть A — конечное кольцо, не имеющее делителей нуля. Докажите, что A поле. (Указание: приведите рассуждение, похожее на доказательство леммы 1 из лекции 1.)

(ii) Докажите, что любое конечное поле $\mathbb{F}$ имеет p^r элементов, где $p = \mathrm{char}(\mathbb{F})$, $r \geqslant 1$. (Указание: рассмотрите степень $[\mathbb{F} : \mathbb{F}_p]$.)

Упражнение 1.2. Степень композиции расширений полей

Пусть задана композиция расширений полей $K \subset E \subset L$, и пусть $X \subset L$ — базис в L над E, $Y \subset E$ — базис в E над K. Докажите, что тогда подмножество $X \cdot Y = \{xy \mid (x, y) \in X \times Y\} \subset L$ является базисом в L над K (и, в частности, $xy \neq x'y'$ для различных пар $(x, y), (x', y') \in X \times Y$.)

Упражнение 1.3. Кольцо многочленов над полем

Пусть K — поле, $K[T]$ — кольцо многочленов над K.

(i) Докажите, что любой идеал $I \subset K[T]$ главный, т.е. имеет вид

$$I = (P) = \{P \cdot Q \mid Q \in K[T]\}$$

для некоторого многочлена $P \in K[T]$. (Указание: воспользуйтесь алгоритмом Евклида для многочленов.) Покажите, что два многочлена $P_1, P_2 \in K[T]$ взаимно просты тогда и только тогда, когда существуют многочлены $Q_1, Q_2 \in K[T]$, для которых $P_1Q_1 + P_2Q_2 = 1$.

(ii) Покажите, если многочлен P неприводим и P делит QR, то P делит Q или R. Другими словами, простые идеалы в $K[T]$ — это идеалы, порожденные неприводимыми многочленами.

(iii) Докажите, что любой многочлен однозначно с точностью до умножения на ненулевые элементы из K раскладывается в произведение неприводимых многочленов. Другими словами, кольцо $K[T]$ факториально. (Указание: проведите аналогичное рассуждение, как для целых чисел.)

Упражнение 1.4. Норма Галуа

Пусть $P \in \mathbb{Q}[T]$ — неприводимый многочлен степени n над $\mathbb{Q}$, $P = \prod_{i=1}^{n}(T - \alpha_i)$ — его разложение над $\mathbb{C}$, $\alpha = \alpha_1 \in \mathbb{C}$ — один из его корней.

(i) Выразим произвольный элемент $\beta \in \mathbb{Q}(\alpha) \subset \mathbb{C}$ как $\beta = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$, где $a_0, \ldots, a_{n-1} \in \mathbb{Q}$. Определим *норму Галуа* элемента β по формуле:

$$\mathrm{Nm}(\beta) = \prod_{i=1}^{n}(a_0 + a_1\alpha_i + \ldots + a_{n-1}\alpha_i^{n-1})\,.$$

Докажите, что $\mathrm{Nm}(\beta) \in \mathbb{Q}$. (Указание: проверьте, что норма задается симметрическим многочленом от $\alpha_1, \ldots, \alpha_n$, а затем воспользуйтесь теоремой о симметрических многочленах.) Например, $\mathrm{Nm}(\alpha) = (-1)^n a_0$.

(ii) Покажите, что отображение $\mathrm{Nm}\colon \mathbb{Q}(\alpha) \to \mathbb{Q}$ является мультипликативным гомоморфизмом, т.е. что для любых $\beta, \beta' \in \mathbb{Q}(\alpha)$ выполняется равенство $\mathrm{Nm}(\beta\beta') = \mathrm{Nm}(\beta)\mathrm{Nm}(\beta')$. (Указание: воспользуйтесь тем, что вложения полей $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$, заданные условиями $\alpha \mapsto \alpha_i$, являются, в частности, мультипликативными гомоморфизмами и переводят элемент β как выше в $a_0 + a_1\alpha_i + \ldots + a_{n-1}\alpha_i^{n-1}$.)

(iii) Норма Галуа позволяет выразить в явном виде обратный элемент к β, обобщая формулу для обратного комплексного числа. Докажите, что число $\gamma = \prod_{i=2}^{n}(a_0 + a_1\alpha_i + \ldots + a_{n-1}\alpha_i^{n-1}) \in \mathbb{C}$ принадлежит полю $\mathbb{Q}(\alpha)$, и что $\alpha^{-1} = \gamma/\mathrm{Nm}(\alpha)$. (Указание: действуйте подобно решению пункта (i), пользуясь тем, что многочлен $P/(T-\alpha)$ имеет коэффициенты в поле $\mathbb{Q}(\alpha)$.)

(iv) Проверьте равенство $\mathrm{Nm}(\beta) = \det(M_\beta)$, где $M_\beta\colon \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ — $\mathbb{Q}$-линейный оператор умножения на β, т.е. $M_\beta(x) = \beta x$. Таким образом, норма Галуа корректно определена для любого кольца A конечной размерности над содержащимся в нем поле K, являясь мультипликативным гомоморфизмом $\mathrm{Nm}\colon A \to K$. (Указание: надо показать, что существует комплексная линейная замена переменных, после которой все операторы вида M_β становятся диагональными с собственными значениями $a_0 + a_1\alpha_i + \ldots + a_{n-1}\alpha_i^{n-1}$, где $1 \leqslant i \leqslant n$. Для этого заметьте, что после замены рациональных чисел на комплексные кольцо $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[T]/(P)$ становится $\mathbb{C}[T]/(P)$, а по китайской теореме об остатках для многочленов последнее изоморфно $\mathbb{C} \times \ldots \times \mathbb{C}$ с покомпонентным умножением. При этом соответствующее отображение $\mathbb{Q}(\alpha) \to \mathbb{C} \times \ldots \times \mathbb{C}$ задается указанными выше вложениями $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$, $\alpha \mapsto \alpha_i$, где $1 \leqslant i \leqslant n$.)

Упражнение 1.5. Алгебраические элементы

Покажем явным образом, что алгебраические элементы образуют поле. Пусть $\alpha, \beta \in \mathbb{C}$ являются корнями многочленов $P, Q \in \mathbb{Q}[T]$, соответственно. Пусть $P = \prod_{i=1}^{m}(T-\alpha_i)$, $Q = \prod_{j=1}^{n}(T-\beta_j)$ — разложения данных многочленов над $\mathbb{C}$.

(i) Проверьте, что многочлены

$$\prod_{i=1}^{m}\prod_{j=1}^{n}(T-\alpha_i-\beta_j), \quad \prod_{i=1}^{m}\prod_{j=1}^{n}(T-\alpha_i\cdot\beta_j) \in \mathbb{C}[T]$$

имеют коэффициенты из $\mathbb{Q}$. (Указание: коэффициенты данных многочленов являются многочленами с целыми коэффициентами от $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots \beta_n$, причем они инвариантны относительно перестановок множества $\alpha_1, \ldots, \alpha_m$ и перестановок множества $\beta_1, \ldots, \beta_n$. Далее воспользуйтесь теоремой о симметрических многочленах.)

(ii) Найдите явно многочлены над $\mathbb{Q}$, корнями которых являются $-\alpha$ и α^{-1}, соответственно.

Упражнение 1.6. Сепарабельные многочлены

Многочлен $P = a_nT^n + \ldots + a_1T + a_0$ из $K[T]$ называется *сепарабельным*, если P и его формальная производная $P' = na_nT^{n-1} + \ldots + a_1 \in K[T]$ взаимно просты.

(i) Проверьте, что корень многочлена кратный тогда и только тогда, когда он является одновременно корнем данного многочлена и его производной. (Указание: воспользуйтесь равенствами $R = (T-\alpha)S$, $R' = S + (T-\alpha)S'$.)

(ii) Докажите, что многочлен $P \in K[T]$ сепарабельный тогда и только тогда, когда для любого расширения полей $K \subset L$ многочлен P не имеет кратных корней в L. (Указание: импликация в одну сторону доказана в лекции 1. Для импликации в другую сторону рассмотрите непостоянный общий множитель Q у P и P', возьмите примитивное расширение $K \subset K_Q$, содержащее корень многочлена Q, и воспользуйтесь пунктом (i).)

(iii) Покажите, что если $\mathrm{char}(K) = 0$, то любой неприводимый многочлен сепарабелен.

(iv) Докажите, что если $\mathrm{char}(K) = p > 0$, то неприводимый многочлен $P \in K[T]$ несепарабельный тогда и только тогда, когда P можно представить в виде $Q(T^{p^r})$, где $Q \in K[T]$ — неприводимый сепарабельный многочлен, $r \geqslant 1$. (Указание: воспользуйтесь определением сепарабельного многочлена через взаимную простоту с производной.)

Листок 2. Расширения Галуа

Упражнение 2.1. Степень поля разложения

Покажите, что для произвольного многочлена $P \in K[T]$ над полем $K \subset \mathbb{C}$ выполняется неравенство $[L : K] \leqslant n!$ для его поля разложения L. (Указание: представьте $K \subset L$ как композицию примитивных расширений.)

Упражнение 2.2. Кубические расширения

Пусть $P \in K[T]$ — неприводимый многочлен степени 3 со старшим коэффициентом 1 над полем $K \subset \mathbb{C}$. Пусть $K \subset L$ — поле разложения многочлена P. В частности, $P = (T - \alpha_1)(T - \alpha_2)(T - \alpha_3)$, где $\alpha_1, \alpha_2, \alpha_3 \in L$.

(i) Докажите, что *дискриминант* $D = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_1 - \alpha_3)^2$, являющийся по определению элементом из L, на самом деле принадлежит подполю $K \subset L$. (Указание: дискриминант является симметрическим многочленом от $\alpha_1, \alpha_2, \alpha_3$.)

(ii) Заметьте, что $\sqrt{D} \in L$ и проверьте, что $L = K(\alpha_1, \sqrt{D})$. (Указание: выразите α_2, α_3 как многочлены от α_1 и $\sqrt{D}$ с коэффициентами в K, пользуясь тем, что $\alpha_1 + \alpha_2 + \alpha_3 \in K$, $\alpha_1\alpha_2\alpha_3 \in K$ и $(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) \in K(\alpha_1)$.)

(iii) Докажите, что если дискриминант D не является квадратом в поле K, то $[L : K] = 6$, а если D является квадратом в K, то $[L : K] = 3$, причем в этом случае $L = K(\alpha_1)$.

Упражнение 2.3. Транзитивность группы Галуа

Покажите, что для любого неприводимого многочлена $P \in K[T]$ над полем $K \subset \mathbb{C}$ группа Галуа его поля разложения действует тринзитивно на множестве корней многочлена P. (Указание: в противном случае найдите разложение многочлена P в произведение многочленов, группируя корни по орбитам относительно действия группы Галуа.)

Упражнение 2.4. Галуа замыкание произвольного конечного расширения

Покажите, что для любого расширения полей $K \subset E \subset \mathbb{C}$, $[E : K] < \infty$, существует расширение Галуа $K \subset L$, для которого $E \subset L$. (Указание: воспользуйтесь тем, что $K \subset E$ примитивно.)

Упражнение 2.5. Циклотомические расширения поля $\mathbb{Q}$

(i) Пусть p — простое число, $F \in \mathbb{Z}[T]$ — многочлен со старшим коэффициентом 1, такой что многочлен $F \pmod p \in \mathbb{F}_p[T]$ сепарабельный. Покажите, что многочлен F сепарабельный над $\mathbb{Q}$. (Указание: по лемме Гаусса любой делитель со старшим коэффициентом 1 многочлена F имеет целые коэффициенты.)

(ii) Пусть $\mathbb{Q} \subset L$ — поле разложения многочлена F из пункта (i), $\alpha \in L$ — некоторый корень многочлена F, и пусть P — минимальный многочлен элемента α над $\mathbb{Q}$. Предположим, что $F(\alpha^p) = 0$. Докажите, что тогда $P(\alpha^p) = 0$. (Указание: по лемме Гаусса P и минимальный многочлен Q элемента α^p над $\mathbb{Q}$ имеют целые коэффициенты. Рассмотрите многочлены $P \pmod p$ и $Q^p \equiv Q(T^p) \pmod p$ в $\mathbb{F}_p[T]$ и воспользуйтесь сепарабельностью многочлена $F \pmod p$.)

(iii) Пусть $\zeta \in \mathbb{C}$ — примитивный корень степени n из 1, т.е. порождающий элемент группы μ_n. Покажите, что минимальный многочлен R элемента ζ над $\mathbb{Q}$ обращается в нуль в ζ^p для любого p, взаимно простого с n. (Указание: воспользуйтесь пунктом (ii).)

(iv) Покажите, что $R(T) = \prod_{i \in (\mathbb{Z}/n\mathbb{Z})^*} (T - \zeta^i)$. (Указание: воспользуйтесь пунктом (iii) и основной теоремой арифметики.)

(v) Докажите, что $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.

Упражнение 2.6. Диэдральная группа Галуа

Пусть $a \in \mathbb{Q}$, $a > 0$, не является квадратом. Докажите, что тогда поле разложения L многочлена $T^4 - a \in \mathbb{Q}[T]$ является $\mathbb{Q}(\sqrt[4]{a}, i)$ и имеет группу Галуа D_4. Опишите все подполя в L, используя соответствие Галуа и описание всех подгрупп в D_4.

Упражнение 2.7. Галуа замыкание произвольного конечного расширения

Покажите, что для любого расширения полей $K \subset E \subset \mathbb{C}$, $[E : K] < \infty$, существует расширение Галуа $K \subset L$, для которого $E \subset L$. (Указание: воспользуйтесь тем, что $K \subset E$ примитивно.)

Упражнение 2.8. Полная группа Галуа

(i) Предположим, что транзитивная подгруппа $G \subset S_5$ содержит транспозицию. Докажите, что тогда $G = S_5$. (Указание: введем на множестве $\{1, \ldots, 5\}$ отношение эквивалентности: $i \sim j$ тогда и только тогда, когда G содержит транспозицию (ij). Данное отношение эквивалентности инвариантно относительно действия группы G, причем G действует транзитивно на множестве классов эквивалентности. Из этого следует, что все классы эквивалентности имеют одинаковое число элементов. Поскольку G содержит транспозицию, то это число больше 1.)

(ii) Пусть $P \in \mathbb{Z}[T]$ — многочлен степени 5 со старшим коэффициентом 1. Предположим, что P неприводим, и что P имеет ровно два невещественных комплексных корня. Покажите, что тогда группа Галуа поля разложения многочлена P равна S_5. (Указание: из неприводимости P следует транзитивность группы Галуа. Из наличия двух комплексных корней у P следует наличие транспозиции в группе Галуа.)

(iii) Проверьте, что группа Галуа поля разложения многочлена $P = T^5 - 4T + 2$ равна S_5. (Указание: опишите все вещественные корни P, рассмотрев нули производной P' и воспользовавшись теоремой Ролля. Также проверьте, что P неприводим, воспользовавшись критерием Эйзенштейна.)

Упражнение 2.9. Построения циркулем и линейкой

(i) Покажите, что любое комплексное число, построенное при помощи циркуля и линейки начиная с конечного множества отмеченных чисел на комплексной плоскости, лежит в башне квадратичных расширений поля, порожденного исходными отмеченными точками. (Указание: интерпретируйте построение точек циркулем и линейкой как процесс пересечения окружностей и прямых, проходящих через уже полученные точки.)

(ii) Покажите, как при помощи циркуля и линейки построить комплексные числа $z_1 z_2$ и z_1/z_2, имея отмеченными на плоскости комплексные числа z_1 и $z_2 \neq 0$. (Указание: воспользуйтесь теоремой Фалеса.) Покажите, как при помощи циркуля и линейки построить число $\sqrt{z}$, имея отмеченным число z. (Указание: вспомните, как делить угол пополам, а также вспомните, чему равен квадрат высоты, опущенной на гипотенузу в прямоугольном треугольнике.)

(iii) Покажите, что циркулем и линейкой невозможно построить квадрат, имеющий ту же площадь, что и нарисованный круг (квадратура круга). (Указание: воспользуйтесь трансцендентностью числа π.)

(iv) Докажите, что деление при помощи циркуля и линейки заданного угла на три равные части (трисекция угла) возможно тогда и только тогда, когда число $\xi = \cos(\varphi) + i\sin(\varphi)$ является кубом в поле $\mathbb{Q}(\xi)$, где φ — величина исходного угла. Покажите, что для угла вида $2\pi/n$, где $n \in \mathbb{N}$, его трисекция возможна тогда и только тогда, когда n не делится на 3. (Указание: воспользуйтесь критерием обратимости остатка 3 по модулю n.)

(v) Опишите способ построения циркулем и линейкой правильного 5-угольника. (Указание: примените соответствие Галуа к подгруппе $\mathbb{Z}/2\mathbb{Z} \subset \mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$, порожденной комплексным сопряжением, и выразите таким образом примитивный корень степени 5 из 1 через квадратные корни. Далее воспользуйтесь пунктом (ii).)

Листок 3. Дифференциальные кольца и модули

Упражнение 3.1. Дифференцирование дробей
Пусть (R, ∂) — дифференциальное кольцо, $a, b \in R$, причем b обратим. Покажите, что тогда $\partial(\frac{a}{b}) = \frac{\partial(a)b - a\partial(b)}{b^2}$.

Упражнение 3.2. Дифференциальность ниль-радикала
Пусть (R, ∂) — дифференциальное кольцо. Предположим, что R не имеет нетривиального $\mathbb{Z}$-кручения. Докажите, что тогда ниль-радикал $\mathrm{Nil}(R) = \{a \in R \mid a^n = 0, n \in \mathbb{N}\}$ является дифференциальным идеалом. (Указание: предполагая, что $a^n = 0$, покажите индукцией по r, $0 \leqslant r \leqslant n$, что $a^{n-r}\partial(a)^{2r-1} = 0$. Затем рассмотрите случай $r = n$.)

Далее (K, ∂) обозначает дифференциальное поле, а $k = K^\partial$ обозначает подполе констант.

Упражнение 3.3. Продолжение дифференцирований
Пусть $\mathrm{char}(K) = 0$, $K \subset L$ — расширение полей конечной степени. Докажите, что существует единственное дифференцирование $\tilde{\partial}$ поля L, для которого $\tilde{\partial}|_K = \partial$. (Указание: произвольный элемент $a \in L$ является корнем его минимального многочлена $P \in K[T]$. Проверьте тождество $0 = \tilde{\partial}\big(P(a)\big) = P'(a)\tilde{\partial}(a) + (\partial P)(a)$, где ∂P обозначает результат применения ∂ к коэффициентам многочлена P. Затем воспользуйтесь тем, что $P'(a) \neq 0$.) Для случая произвольной характеристики надо дополнительно требовать, чтобы расширение $K \subset L$ было сепарабельным, т.е. чтобы минимальные многочлены всех элементов из L были сепарабельными.

Упражнение 3.4. Алгебраическая замкнутость констант

(i) Докажите, что если $\mathrm{char}(K) = 0$, то k алгебраически замкнуто в K, т.е. если элемент $a \in K$ алгебраический над k, то $a \in k$. (Указание: для минимального многочлена $P \in k[T]$ элемента a проверьте тождество $0 = \partial\big(P(a)\big) = P'(a)\partial(a)$, пользуясь тем, что коэффициенты P константы. Затем воспользуйтесь тем, что $P'(a) \neq 0$.) Для случая произвольной характеристики надо дополнительно требовать, чтобы минимальный многочлен элемента a был сепарабельным.

(ii) Пусть $\mathrm{char}(K) = 0$, $K \subset L$ — расширение полей конечной степени и продолжим однозначно ∂ на L по упражнению 3.3. Докажите, что все элементы из L^∂ алгебраические над k. (Указание: для $a \in L^\partial$ рассмотрите его минимальный многочлен $P \in K[T]$ со старшим коэффициентом 1 и воспользуйтесь тождеством $0 = \partial(P(a)) = (\partial P)(a)$.)

Упражнение 3.5. Дифференциальные модули ранга один
Пусть (M, ∂_M) — дифференциальный модуль ранга один над (K, ∂).

(i) Выберем ненулевой базисный элемент $e \in M$ и пусть $\partial_M(e) = -a \cdot e$, где $a \in K$. Покажите, что тогда для любого $y \in K$ выполняется равенство $\partial(y \cdot e) = \big(\partial(y) - ay\big) \cdot e$.

(ii) Пусть $e' = g \cdot e$, где $g \in K$, $g \neq 0$. Покажите, что тогда $\partial_M(e') = -a' \cdot e'$, где $a' = a - \partial\log(a)$, где $\partial\log(a) = \frac{\partial(a)}{a}$.

(iii) Проверьте, что существует изоморфизм $(M, \partial_M) \simeq (K, \partial)$ тогда и только тогда, когда существует $e' \in M$, $e' \neq 0$, для которого $\partial_M(e') = 0$, и тогда и только тогда, когда существует $y \in K$, для которого $\partial(y) = ay$, т.е. $y = \exp(\int a)$. Например, для $K = \mathbb{C}(x)$, $\partial = \partial_x$ дифференциальный модуль ранга один, заданный $\partial_M(e) = -e$ нетривиален.

(iv) Проверьте, что отображение $\partial\log\colon K^* \to K$ является гомоморфизмом групп и докажите, что класс изоморфизма (M, ∂_M) однозначно определяется классом a в фактор-группе $K/\partial\log(K^*)$. При этом сложение элементов в этой фактор-группе соответствует тензорному произведению дифференциальных модулей ранга один.

(v) Покажите, что для $K = \mathbb{C}(x)$, $\partial = \partial_x$ подгруппа $\partial\log(K^*) \subset K$ состоит из рациональных функций вида $\sum_{i=1}^n \frac{n_i}{x-c_i}$, где $n_i \in \mathbb{Z}$, $c_i \in \mathbb{C}$. (Указание: любую рациональную функцию из $\mathbb{C}(x)^*$ можно представить в виде $\lambda\prod_{i=1}^n (x-c_i)^{n_i}$, где $\lambda \in \mathbb{C}^*$.)

(vi) Для $K = \mathbb{C}(x)$, $\partial = \frac{\partial}{\partial x}$ проверьте изоморфизм

$$K/\partial\log(K^*) \simeq \mathbb{C}[x] \oplus \bigoplus_{c,n\geqslant 2} \mathbb{C}\tfrac{1}{(x-c)^n} \oplus \bigoplus_c \mathbb{C}^*\tfrac{1}{x-c},$$

где $c \in \mathbb{C}$. (Указание: воспользуйтесь изоморфизмом $\mathbb{C}/\mathbb{Z} \simeq \mathbb{C}^*$.)

Упражнение 3.6. Матрица связности

Пусть M — дифференциальный модуль ранга n над (K, ∂). Пусть $A \in \mathrm{Mat}_n(K)$ — матрица связности относительно базиса $e = (e_1, \ldots, e_n)$ в M над K, т.е. $\partial(e) = -eA$.

(i) Пусть другой базис $e' = (e'_1, \ldots, e'_n)$ удовлетворяет $e' = eG$ для $G \in \mathrm{GL}_n(K)$. Покажите, что тогда для матрицы связности A' в базисе e' выполняется равенство $A' = G^{-1}AG - G^{-1}\partial G$.

(ii) Пусть $M^\vee$ — двойственный дифференциальный модуль, $e^\vee$ — двойственный базис в $M^\vee$ над K. Покажите, что соответствующая матрица связности для $M^\vee$ равна $-A^\top$.

(iii) Пусть $\det(M) = \wedge_R^n M$, $e_1 \wedge \ldots \wedge e_n$ — порождающий модуля $\det(M)$ над R. Покажите, что соответствующая матрица связности для $\det(M)$ равна $\mathrm{Tr}(A)$.

Упражнение 3.7. Кольцо дифференциальных операторов

(i) Положим $F_i = \{P \in K\{\partial\} \mid \deg(P) \leqslant i\} \subset K\{\partial\}$, где $i \geqslant 0$. Проверьте, что $F_i \cdot F_j \subset F_{i+j}$, $[F_i, F_j] \subset F_{i+j-1}$ и что прямая сумма $\bigoplus_{i\geqslant 0} F_i/F_{i-1}$ с индуцированной структурой кольца изоморфна коммутативному кольцу многочленов $K[p]$ от формальной переменной p.

(ii) Покажите, что для любого элемента $a \in K$ и $i \geqslant 1$ выполняется равенство $[\partial^i, a] = i\partial(a)\partial^{i-1} + Q$, где $\deg(Q) \leqslant i-1$. Другими словами, имеются вложения $[F_i, a] \subset F_{i-1}$, $i \geqslant 1$, а возникающие отображения $[-, a]$ из $F_i/F_{i-1} \simeq Kp^i$ в $F_{i-1}/F_{i-2} \simeq Kp^{i-1}$ совпадают с дифференцированием $\partial(a)\frac{\partial}{\partial p}$. (Указание: воспользуйтесь индукцией по i.)

(iii) Далее будем предполагать, что $\mathrm{char}(K) = 0$ и $\partial \neq 0$. Покажите, что если $P \in K\{\partial\}$ коммутирует со всеми элементами в K, то $P \in K$, т.е. что централизатор подкольца K в $K\{\partial\}$ совпадает с K. (Указание: воспользуйтесь пунктом (ii).)

(iv) Покажите, что если $P \in K\{\partial\}$ коммутирует со всеми элементами в $K\{\partial\}$, то $P \in k = K^\partial$, т.е. что центр кольца $K\{\partial\}$ равен k. (Указание: воспользуйтесь пунктом (iii), а также тем, что для любого $a \in K$ выполняется равенство $[\partial, a] = \partial(a)$ в $K\{\partial\}$.)

(iv) Докажите, что в кольце $K\{\partial\}$ нет нетривиальных двусторонних идеалов, т.е. что $K\{\partial\}$ простое кольцо. (Указание: для двустороннего идеала $I \subset K\{\partial\}$ сопоставьте каждому его элементу $P \in I$, $P = b_n\partial^n + \ldots + b_0$, $b_n \neq 0$, элемент $b_n p^n \in K[p]$ (*главный символ* дифференциального оператора). При помощи пункта (ii) покажите, что так получится дифференциальный идеал в $K[p]$ относительно $\frac{\partial}{\partial p}$.)

Упражнение 3.8. Дифференциальные операторы и дифференциальные модули

(i) Проверьте, что для ненулевого элемента $P \in K\{\partial\}$ степени n матрица связности дифференциального модуля $\big(K\{\partial\}/K\{\partial\}P\big)^\vee$ в базисе, двойственном к $\bar{1}, \bar{\partial}, \ldots, \bar{\partial}^{n-1}$ имеет вид

$$\begin{pmatrix} 0 & 1 & \ldots & 0 \\ & \ldots & \ldots & \\ 0 & 0 & \ldots & 1 \\ -a_0 & -a_1 & \ldots & -a_n \end{pmatrix}.$$

(ii) Докажите, что для любых ненулевых $P, P' \in K\{\partial\}$ имеется канонический изоморфизм между $\mathrm{Hom}_\partial(M_{P'}, M_P)$ и k-векторным пространством, состоящим из всех $Q \in K\{\partial\}$, для которых выполняется неравенство $\deg(Q) < \deg(P')$ и существует $Q' \in K\{\partial\}$ такой, что $PQ = Q'P'$. (Указание: рассмотрите, в какой элемент из $K\{\partial\}/K\{\partial\}P'$ переходит $\bar{1} \in K\{\partial\}/K\{\partial\}P$ при двойственном отображении.)

(iii) Покажите, что для любых ненулевых $P, P' \in K\{\partial\}$ имеется изоморфизм дифференциальных модулей $M_P \simeq M_{P'}$ тогда и только тогда, когда $\deg(P) = \deg(P')$ и существуют $Q, Q' \in K\{\partial\}$, для которых $\deg(Q) < \deg(P')$, $PQ = Q'P'$ и $K\{\partial\}Q + K\{\partial\}P' = K\{\partial\}$, или, что равносильно, не существует $R \in K\{\partial\}$, $R \notin K$, делящего справа Q и P'. Если данные условия выполняются, то говорят, что P и P' *одного типа*. (Указание: воспользуйтесь пунктом (ii), а также выразите условие сюръективности морфизма из M_P в $M_{P'}$, заданного Q.)

Упражнение 3.9. Определитель Вронского

Докажите, что элементы $a_1, \ldots, a_n \in K$ линейно независимы над k тогда и только тогда, когда *определитель Вронского*

$$\det \begin{pmatrix} a_1 & \ldots & a_n \\ \partial(a_1) & \ldots & \partial(a_n) \\ & \ldots & \\ \partial^{n-1}(a_1) & \ldots & \partial^{n-1}(a_n) \end{pmatrix} \in K$$

не равен нулю. (Указание: индукцией по n постройте дифференциальный оператор $P \in K\{\partial\}$ степени n, для которого $P(a_1) = \ldots = P(a_n) = 0$. Для базы индукции рассмотрите $\partial - \partial(a_1)$, а для перехода индукции рассмотрите дифференциальный опреатор

$$P_n = \partial P_{n-1} - \frac{\partial\big(P_{n-1}(a_n)\big)}{P_{n-1}(a_n)} P_{n-1}\,.$$

Далее воспользуйтесь леммой о линейной независимости горизонтальных векторов применительно к дифференциальному модулю $\big(K\{\partial\}/K\{\partial\}P_n\big)^\vee$.)

Упражнение 3.10. Разложение дифференциальных операторов на множители

(i) Докажите, что любой идеал в $K\{\partial\}$ имеет вид $K\{\partial\}P$. (Указание: воспользуйтесь аналогом алгоритма Евклида для дифференциальных операторов.)

(ii) Покажите, что для любого ненулевого элемента $P \in K\{\partial\}$ имеется биекция между разложениями P в произведение дифференциальных операторов с точностью до умножения на элемент из K^* и подмодулями дифференциального модуля M_P, при которой разложению $P = Q'Q$ соответствует подмодуль $M_Q \subset M_P$, двойственный к естественной сюръекции дифференцильных модулей $K\{\partial\}/K\{\partial\}P \twoheadrightarrow K\{\partial\}/K\{\partial\}Q$. Покажите, что при этом $M_P/M_Q \simeq M_{Q'}$. (Указание: опишите левые идеалы в $K\{\partial\}$, содержащие $K\{\partial\}P$, пользуясь пунктом (i).)

(iii) Докажите, что любой ненулевой морфизм между неприводимыми (т.е. не содержащими нетривиальных дифференциальных подмодулей) дифференциальными модулями является изоморфизмом. Выведите из этого теорему Жордана–Гельдера в категории дифференциальных модулей конечного ранга: для любого такого M существует фильтрация дифференциальными подмодулями $0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$, для которой M_i/M_{i-1} неприводимы при всех i, $1 \leqslant i \leqslant n$, и при этом неупорядоченный набор классов изоморфизма неприводимых дифференциальных модулей M_i/M_{i-1}, $1 \leqslant i \leqslant n$, не зависит от выбора фильтрации.

(iv) Докажите, что в $K\{\partial\}$ определено разложение на неразложимые множители, однозначное с точностью до операторов одного типа. (Указание: воспользуйтесь алгоритмом Евклида для доказательства существования разложения. Далее примените теорему Жордана–Гельдера из пункта (iii) и воспользуйтесь пунктом (ii) и упражнением 3.8(iii).)

Листок 4. Теория Пикара–Вессио

Ниже (K, ∂) обозначает дифференциальное поле нулевой характеристики, а $k = K^\partial$ обозначает подполе констант.

Упражнение 4.1. Константы дифференциально простых колец
Пусть R — дифференциальное кольцо, являющееся областью целостности. Предположим, что в R нет нетривиальных дифференциальных идеалов, т.е. R *дифференциально просто*. Докажите, что тогда $R^\partial = F^\partial$, где $F = \mathrm{Frac}(R)$ —поле частных кольца R. (Указание: для $a \in F^\partial$ рассмотрите дифференциальный идеал $\{b \in R \mid ab \in R\}$ в R.)

Упражнение 4.2. Дифференциальная группа Галуа $\mathbb{G}_m$
Пусть M — дифференциальный модуль ранга один над (K, ∂), соответствующий дифференциальному уравнению $\partial y = ay$. Пусть $[a] \in K/\partial\log(K^*)$ — класс a в данной фактор-группе.

(i) Пусть $[a]$ имеет бесконечный порядок в $K/\partial\log(K)$. Рассмотрим расширение дифференциальных полей $K \subset L = K(y)$, где y — формальная переменная, $\partial(y) = ay$. Докажите, что $K \subset L$ является расширением Пикара–Вессио для M, и что дифференциальная группа Галуа изоморфна $\mathbb{G}_m = \mathrm{GL}_1$. (Указание: рассмотрите дифференциальное кольцо $R = K[y, y^{-1}]$ с $\partial(y) = ay$. Докажите, что R дифференциально просто, пользуясь тем, что любой нетривиальный идеал в R порожден многочленом вида $T^m + b_{m-1}T^{m-1} + \ldots + b_0 \in K[T]$, где $m > 0$, $b_0 \neq 0$. При этом такой идеал является дифференциальным тогда и только тогда, когда $\partial(b_i) = a(m-i)b_i$ для всех i, $0 \leqslant i \leqslant m-1$. Далее проверьте равенство $k = R^\partial$ и воспользуйтесь упражнением 4.1. Для вычисления дифференциальной группы Галуа G воспользуйтесь вложением $G \subset \mathrm{GL}_1$, заданным по формуле $g \mapsto g(y)/y$, и проверьте, что для любого $\lambda \in k^*$ корректно определен дифференциальный автоморфизм $y \mapsto \lambda y$ поля L над K.)

(ii) Пусть $[a]$ имеет порядок $n \geqslant 1$ в $K/\partial\log(K)$ и пусть $\mu_n \subset K$. Рассмотрим расширение полей конечной степени $K \subset L = K(\sqrt[n]{b})$, где $b \in K$ такой, что $na = \partial\log(b)$ и однозначно продолжим ∂ на L по упражнению 3.3. Докажите, что $K \subset L$ является расширением Пикара–Вессио для M, и что дифференциальная группа Галуа изоморфна $\mu_m \subset \mathrm{GL}_1$. (Указание: проверьте, что $\partial(\sqrt[n]{b}) = a\sqrt[n]{b}$. Для вычисления дифференциальной группы Галуа воспользуйтесь описанием группы Галуа расширений Куммера, а также упражнениями 3.3 и 3.4(i).)

Упражнение 4.3. Дифференциальная группа Галуа $\mathbb{G}_a$
Пусть M — дифференциальный модуль ранга два над (K, ∂), соответствующий матрице связности $\left(\begin{smallmatrix} 0 & a \\ 0 & 0 \end{smallmatrix}\right)$, где $a \in K$, $b \notin \partial(K)$. Рассмотрим расширение дифференциальных полей $K \subset L = K(y)$, где y — формальная переменная, $\partial(y) = a$. Докажите, что $K \subset L$ является расширением Пикара–Вессио для M, и что дифференциальная группа Галуа изоморфна $\mathbb{G}_a = \mathrm{U}_2 = \{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\} \subset \mathrm{GL}_2$. (Указание: рассмотрите дифференциальное кольцо $R = K[y]$ с $\partial(y) = a$. Докажите, что R дифференциально просто, пользуясь тем, что любой нетривиальный идеал в R порожден многочленом вида $T^m + b_{m-1}T^{m-1} + \ldots + b_0 \in K[T]$, где $m > 0$. При этом такой идеал является дифференциальным тогда и только тогда, когда $\partial(b_i) + a(i+1)b_{i+1} = 0$ для всех i, $0 \leqslant i \leqslant m-1$. Далее проверьте равенство $k = R^\partial$ и воспользуйтесь упражнением 4.1. Для вычисления дифференциальной группы Галуа G воспользуйтесь вложением $G \subset \mathrm{GL}_2$, заданным по формуле $g \mapsto g(y) - y$, и проверьте, что для любого $\lambda \in k$ корректно определен дифференциальный автоморфизм $y \mapsto \lambda + y$ поля L над K.)

Упражнение 4.4. Конечная дифференциальная группа Галуа

Пусть $K \subset L$ — расширение Галуа с конечной группой Галуа G. Однозначно продолжим ∂ на L по упражнению 3.3. Предположим, что $k = L^{\partial}$ (например, по упражнению 3.4(ii) это выполняется, когда k алгебраически замкнуто). Докажите, что тогда $K \subset L$ является расширением Пикара–Вессио для L, рассматриваемого как дифференциальный модуль над K ранга $[L : K]$, и что дифференциальная группа Галуа изоморфна G. (Указание: из упражнения 3.3 следует, что действие G на L коммутирует с ∂, т.е. что G совпадает со всеми дифференциальными автоморфизмами L над K. Имеется изоморфизм L-векторных пространств

$$L \otimes_K L \xrightarrow{\sim} \prod_{g \in G} L\,, \qquad a \otimes b \longmapsto \big(g(a) \otimes b\big)_{g \in G}\,.$$

Это можно вывести, например, представив L как K_P для некоторого неприводимого многочлена $P \in K[T]$, расщепимого над L. Проверьте, что данный изоморфизм коммутирует с дифференцированием, заданным по правилу Лейбница на левой стороне и покомпонентно на правой стороне. Таким образом, L как дифференциальный модуль над K становится тривиальным после расширения скаляров на L, т.е. после применения $- \otimes_K L$.))

Упражнение 4.5. Дифференциальная группа Галуа SO_2

Пусть $k = \mathbb{R}$, $K = k(x)$, $\partial = \frac{\partial}{\partial x}$, $P = \partial^2 + 1$. Покажите, что тогда дифференциальное расширение полей $K \subset L = K\big(\sin(x), \cos(x)\big)$ является расширением Пикара–Вессио для дифференциального модуля M_P, и что дифференциальная группа Галуа изоморфна $\mathrm{SO}_2 \subset \mathrm{GL}_2(\mathbb{R})$ над $\mathbb{R}$ (окружность).