Нормирования, пополнения и глобальные поля

Задача 1° (поля функций на кривых). a) Опишите все нормирования на конечном расширении $K/\mathbb{F}_q(t)$.

b) Покажите, что всякое пополнение K изоморфно полю рядов Лорана $\mathbb{F}_{q^r}((s))$

c) Докажите, формулу произведения для K: $\prod\limits_v |x|_v = 1$, где произведение берётся по всем нормализованным нормированиям $|\ |_v$ поля K.

Задача 2°. Докажите, что поле K с неархимедовым нормированием локально компактно (т. е. существует компактная окрестность 0) тогда и только тогда, когда K — полно, нормирование дискретно, а поле вычетов $k = \mathcal{O}_K/\mathfrak{m}_K$ конечно.

Задача 3 (нормализованные нормирования и мера Хаара). a) Покажите, что на аддитивной группе K^+ локально компактного поля с неархимедовым нормированием, существует и единственна мера μ, инвариантная относительно сдвигов (т. е. $\mu(\alpha+U) = \mu(U)$ для любого $\alpha \in K$ и измеримого подмножества $U \subset K$), удовлетворяющая условию $\mu(\mathcal{O}_K) = 1$.

b) Покажите, что для меры μ из предыдущего пункта и нормализованного нормирования $\|\ \|$ на K выполнено $\mu(\alpha + \beta\mathcal{O}_K) = \|\beta\|$.

Подсказка: удобно решать одновременно оба пункта.

Задача 4 (ряды в $\mathbb{C}_p$). $a°$) Покажите, что степенной ряд $\sum\limits_{k=1}^{\infty} a_k x^k, a_k, x \in \mathbb{C}_p$ сходится при $|x|_p < r$ и расходится при $|x|_p > r$, где $\frac{1}{r} = \limsup |a_n|_p^{1/n}$. Что может происходить со сходимостью на границе $|x|_p = r$?

$b°$) Убедитесь, что ряд $\log(1 + x) = \sum\limits_{k=1}^{\infty} \frac{(-1)^{k+1}x^k}{k}$ сходится при $|x|_p < 1$ и расходится при $|x|_p \geq 1$.

$c°$) Покажите, что радиус сходимости ряда $\exp(x) = \sum\limits_{k=0}^{\infty} \frac{x^k}{k!}$ равен $p^{-1/(p-1)}$. Сходится ли этот ряд на границе круга сходимости?

$d°$) Проверьте, что в $\mathbb{C}_p$ имеют место равенства:

$$\log((1 + x)(1 + y)) = \log(1 + x) + \log(1 + y),\ \exp(x + y) = \exp(x)\exp(y),$$
$$\exp(\log(1 + x)) = 1 + x,\ \log(\exp(x)) = x.$$

Выведите отсюда, что exp и log — взаимно обратные изоморфизмы некоторой окрестности 0 в аддитивной группе $\mathbb{C}_p$ и некоторой окрестности 1 в мультипликативной группе $\mathbb{C}_p^\times$.

e) Исследуйте сходимость ряда $\sum\limits_{k=0}^{\infty} \frac{a(a-1)\ldots(a-k+1)}{k!} x^k$.

Задача 5 (насколько $\mathbb{C}_p$ больше $\bar{\mathbb{Q}}_p$). a) Приведите пример элемента из $\mathbb{C}_p$, не лежащего в $\bar{\mathbb{Q}}_p$.

Подсказка: используйте примитивные корни из единицы возрастающей степени.

b^*) Докажите, что $\mathbb{C}_p$ нельзя представить в виде алгебраического расширения поля, полученного присоединением счётного числа элементов поля $\mathbb{C}_p$ к $\bar{\mathbb{Q}}_p$ (т. е. $\mathbb{C}_p$ имеет несчётную степень трансцендентности над $\bar{\mathbb{Q}}_p$).

c^*) Будет ли счётной степень трансцендентности $\mathbb{C}_p$ над p-адическим пополнением максимального неразветвлённого расширения $\mathbb{Q}_p^{\mathrm{nr}}$?

Задача 6° (многоугольник Ньютона). Найдите многоугольник Ньютона следующих многочленов. Что можно сказать об их корнях?

a) $1 - X + pX^2$; b) $1 - X^3/p^2$; c) $1 + X^2 + pX^4 + p^3X^6$;
d) $\sum_{i=1}^{p} iX^{i-1}$; e) $(1-X)(1-pX)(1-p^3X)$; f) $\prod_{i=1}^{p^2}(1-iX)$.

g) Найдите два приведённых многочлена степени 3 в $\mathbb{Q}_5[X]$ с одинаковым многоугольником Ньютона, таких что один из них неприводим, а другой нет.

h) Найдите неприводимый приведённый многочлен в $\mathbb{Z}[X]$ степени 6, который разлагается в $\mathbb{Q}_5[X]$ в произведение трёх неприводимых многочленов степени 2.

i) Пусть $f(X) \in 1 + X\mathbb{Z}_p[X]$ — многочлен, многоугольник Ньютона которого состоит из одного отрезка, соединяющего точки $(0,0)$ и (n,m). Покажите, что $f(X)$ неприводим в $\mathbb{Z}_p$, если n и m взаимно просты. Выведите отсюда критерий неприводимости Эйзенштейна.

j) Всякий ли неприводимый многочлен $f(X) \in 1 + X\mathbb{Z}_p[X]$, имеет многоугольник Ньютона того же типа, что в предыдущем пункте?

Задача 7 (приложения леммы Краснера). a°) Пусть p — такое простое число, что -1 не имеет квадратного корня в $\mathbb{Q}_p$. Найдите ϵ, для которого $\mathbb{Q}_p(\sqrt{-a}) = \mathbb{Q}_p(\sqrt{-1})$ при любом a с $|a-1|_p < \epsilon$.

b°) Для какого ϵ из неравенства $|a-1|_p < \epsilon$ следует совпадение $\mathbb{Q}_p(\sqrt{a})$ с $\mathbb{Q}_p(\sqrt{p})$?
Подсказка: отдельно исследуйте случай $p = 2$.

c°) Определите все неизоморфные квадратичные расширения поля $\mathbb{Q}_p$.
Подсказка: в случае $p = 2$ их 7 штук.

d) Определите все различные кубические расширения поля $\mathbb{Q}_7$.

Задача 8. Убедитесь, что для локально компактного поля K и его расширения L имеет место равенство $\mathcal{O}_L = \mathcal{O}_K[a]$ для некоторого $a \in L$.
Подсказка: в качестве a можно взять $\Pi + b$, где Π — униформизующая L, $b \in \mathcal{O}_L$ — поднятие порождающего элемента $\bar{b}$ для поля вычетов $l = k[\bar{b}]$.

Задача 9 (слабо разветвлённые расширения). Пусть K — локально-компактное поле с неархимедовым нормированием, $k = \mathcal{O}_K/\mathfrak{m}_K$ — поле вычетов, $p = \operatorname{char} k$. Напомним, что конечное расширение L/K называется слабо разветвлённым, если $p \nmid e(L/K)$ (как обычно, $e(L/K)$ — индекс ветвления, $f(L/K) = [l:k]$ — степень расширения поля вычетов).

a) Пусть L/K — произвольное конечное сепарабельное расширение K. Покажите, что в L есть такое подполе L_1, что всякое слабо разветвлённое расширение $K'/K, K' \subset L$, является подполем L_1 и обратно. Убедитесь, что $[L:L_1]$ является степенью p.

b) Убедитесь, что L_1 есть неподвижное поле первой группы ветвления $G_1 = \{\sigma \in \operatorname{Gal}(L/K) \mid |\sigma(\Pi) - \Pi| < |\Pi|\}$.

c) Пусть L/K — нормальное вполне и слабо разветвлённое расширение степени e. Докажите, что K содержит первообразный корень степени e из единицы и существует элемент $c \in K^\times$, являющийся униформизующей для K, для которого $L = K(c^{1/e})$.
Подсказка: используйте лемму Гензеля, чтобы показать наличие корней из единицы, и теорию Куммера, для того, чтобы убедиться, что $L = K(c^{1/e})$.

d) Обратно, если $p \nmid e$ и K содержит первообразный корень степени e из единицы, и, если c — униформизующая K, то $L = K(c^{1/e})$ нормально, вполне и слабо разветвлено над K и имеет степень e.

e) Покажите, что группа Галуа максимального слабо разветвлённого расширения K над его максимальным неразветвлённым расширением $\operatorname{Gal}(K^{\mathrm{tr}}/K^{\mathrm{nr}}) \cong \prod_{l \neq p} \mathbb{Z}_l$.

f^*) В условиях предыдущего пункта изучите структуру $\operatorname{Gal}(K^{\mathrm{tr}}/K)$.

Задача 10. Пусть K — конечное расширение $\mathbb{Q}_p$, m — натуральное число, а $(K^\times)^m$ множество m-х степеней элементов из $K^\times$.

a) Предположим, что $|m|_p = 1$ и K не содержит корней степени m из 1, отличных от 1. Докажите, что индекс мультипликативной подгруппы $(K^\times)^m$ в $K^\times$ равен m.

b) Опустим предположения предыдущего пункта. Докажите, что индекс $(K^\times : (K^\times)^m) = \frac{m\omega}{|m|_p}$, где ω — число корней из 1 степени m, содержащихся в K.

Задача 11*. Пусть L/K — конечное неразветвлённое расширение локально компактных полей.

a) Покажите, что отображение следа сюръективно переводит $\mathcal{O}_L$ в $\mathcal{O}_K$, а отображение нормы сюръективно переводит $\mathcal{O}_L^\times$ в $\mathcal{O}_K^\times$.

b) Покажите, что, если отображение нормы сюръективно переводит $\mathcal{O}_L^\times$ в $\mathcal{O}_K^\times$, то расширение неразветвлено.

Задача 12. a) Пусть K — глобальное поле, $\mathfrak{a}$ — собственный идеал в $\mathcal{O}_K$. Покажите, что естественное отображение $SL_n(\mathcal{O}_K) \longrightarrow SL_n(\mathcal{O}_K/\mathfrak{a})$ является сюръекцией.

Подсказка: теорема об аппроксимации Вам поможет.

b) Проделайте то же самое для группы GL_n.

Задача 13 (теорема Гельфанда—Торнхейма). a) Пусть F — нормированное поле, содержащее $\mathbb{C}$, при этом нормирование $|\ |$ на F продолжает обычное нормирование на $\mathbb{C}$. Пусть $x_0 \in F \setminus \mathbb{C}$. Положим $f(z) = (x_0 - z)^{-1} : \mathbb{C} \to F$. Убедитесь, что функция $z \mapsto |f(z)|$ непрерывна, ограничена и достигает наибольшего значения M на некотором замкнутом множестве $D \subset \mathbb{C}$.

b) В обозначениях предыдущего пункта предположим, что $0 \in D$. Пусть ω — примитивный корень степени n из $1, r \in \mathbb{R}, |r/x_0| < 1$. Положим $S(n) = \frac{1}{n}\sum\limits_{k=1}^{n} \frac{1}{x_0 - \omega^k r}$. Убедитесь, что $\lim\limits_{n\to\infty} |S(n)| = |1/x_0| = M$.

c) Докажите, что для любого комплексного числа λ такого, что $|\lambda| = 1$, имеет место $\left|\frac{1}{x_0 - \lambda r}\right| = M$. Выведите отсюда, что $F = \mathbb{C}$.

Подсказка: рассмотрите маленький интервал, содержащий λ, и корни из 1, лежащие в нём.

d) Покажите, что любое поле F с *архимедовым* нормированием изоморфно подполю $\mathbb{C}$ так, что при изоморфизме нормирование на F переходит в стандартное нормирование на $\mathbb{C}$.

Задача 14 (вычисление групп Галуа). Пусть K — числовое поле, $f(x) \in \mathcal{O}_K[x]$ — приведённый многочлен без кратных корней, $\deg f = n$, G — группа Галуа поля разложения $f(x)$.

a°) Предположим, что G имеет в точности s орбит как группа перестановок n-элементного множества корней $f(x)$, а порядки орбит равны $n_1, \dots, n_s$. Тогда имеется разложение $f(x) = f_1(x) \dots f_s(x)$, где $f_i(x) \in K[x]$ — неприводимые многочлены степени n_i.

b°) Пусть $\mathfrak{p}$ — простой идеал $\mathcal{O}_K$ и $f(x) \equiv f_1(x) \dots f_s(x) \mod \mathfrak{p}$, где $f_i(x)$ — различные неприводимые многочлены степени n_i с коэффициентами из $k = \mathcal{O}_K/\mathfrak{p}$. Тогда в G найдется перестановка σ, являющаяся произведением непересекающихся циклов длин n_i.

c°) Каков аналог утверждения предыдущего пункта для вещественных нормирований?

d°) Вычислите группу Галуа многочлена $x^5 - x - 1$.

e) Пусть H — подгруппа S_n, действующая транзитивно на множестве корней и содержащая $(n-1)$-цикл и транспозицию. Тогда $H = S_n$.

f) Используя предыдущую задачу, найдите для всех n многочлен степени n над $\mathbb{Q}$, имеющий группу Галуа S_n.

Этот метод вычисления групп Галуа применим к произвольным многочленам и является самым эффективным на практике. Дополнительными ингредиентами, которые обеспечивают работу метода, являются теорема плотности Чеботарёва, гарантирующая существование простого, элемент Фробениуса которого имеет любой заданный циклический тип из G, а также характеризацию подгрупп S_n (при небольших n) в терминах классов сопряжённости.

Задача 15 (разложение многочленов на множители).

a) Пусть K — поле дискретного нормирования, $f(x), g(x), h(x) \in \mathcal{O}_K[x]$ — приведённые многочлены. Предположим, что $\delta = |f(x) - g(x)h(x)| < |\mathrm{Res}(g,h)|^2 = r^2$ (норма многочлена — максимум модулей его коэффициентов, Res — результант двух многочленов). Докажите, что найдутся такие $G(x), H(x) \in \mathcal{O}_K[x]$, что $|G(x) - g(x)| < r$, $|H(x) - h(x)| < r$ и $f(x) = G(x)H(x)$.

Подсказка: последовательно строим всё лучшие приближения к $f(x)$, записывая $g(x) = g^*(x) + \gamma(x)$, $h(x) = h^*(x) + \chi(x)$, где $\deg(\gamma) = \deg g - 1$, $\deg(\chi) = \deg h - 1$. Определитель матрицы левой части уравнения $g\chi + h\gamma = f - gh$ на коэффициенты $\gamma(x)$ и $\chi(x)$ совпадает с результантом $\mathrm{Res}(g,h)$. Отсюда находим γ и χ, при этом $|\chi(x)|, |\gamma(x)| \leq \frac{\delta}{r}$. Теперь $|f(x) - g^*(x)h^*(x)| < \delta$ и $|\mathrm{Res}(g^*, h^*)| = |\mathrm{Res}(g,h)|$.

b) Проверьте, что утверждение предыдущего упражнения верно, если заменить условие $\delta < r^2$ на $\delta < \mathrm{Disc}(f)$.

Подсказка: $\mathrm{Disc}(gh) = \mathrm{Disc}(g)\mathrm{Disc}(h)\mathrm{Res}(g,h)^2$

Задача 16 (вычисление колец целых).

a) Пусть $K = \mathbb{Q}(\alpha)$ — конечное расширение, $\alpha \in \mathcal{O}_K$. Покажите, что, если минимальный многочлен α является многочленом Эйзенштейна (как многочлен над $\mathbb{Q}_p$, в частности, он неприводим над $\mathbb{Q}_p$), то $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

b) Найдите кольца целых расширений $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt[5]{2})$.

c) Покажите, что расширение $\mathbb{Q}(\zeta_{p^k})$, полученное присоединением примитивного корня степени p^k из единицы, неразветвлено вне p.

Подсказка: посмотрите на производную $x^{p^k} - 1 \mod p$.

d) Убедитесь, что расширение $\mathbb{Q}(\zeta_{p^k})$ вполне разветвлено в p. Используя это, покажите, что $\mathcal{O}_{\mathbb{Q}(\zeta_{p^k})} = \mathbb{Z}[\zeta_{p^k}]$.

Подсказка: элементы $\frac{\zeta^i - 1}{\zeta^j - 1}$ обратимы в $\mathcal{O}_K$ (здесь $\zeta = \zeta_{p^k}$).

e) Найдите кольцо целых циклотомического (т.е. кругового) поля $\mathbb{Q}(\zeta_m)$ для произвольного m.

f) Посчитайте дискриминант кругового поля.

g) Как устроено разложение на простые в $\mathbb{Q}(\zeta_m)$?

Циклотомическое расширение $\mathbb{Q}(\zeta_m)$ является важнейшим примером в алгебраической теории чисел, многие общие результаты (теорема Дирихле о единицах, разложение на простые, теория полей классов) доказывались для случая этого поля, а затем переносились (если получалось) на более сложные поля. С теоремы Кронекера–Вебера о том, что всякое абелево расширение $\mathbb{Q}$ вкладывается в $\mathbb{Q}(\zeta_m)$ начинается теория полей классов.