Для зачета по каждому листку достаточно сдать все задачи со звездочками, либо все задачи без звездочек. Задачи с двумя звездочками можно не сдавать. Сдавшим k задач с двумя звездочками разрешается не сдавать $2k$ задач со звездочками из того же листочка. Задачи, обозначенные (!), следует сдавать всем.

Алгебра 11: Теория Галуа

Расширения Галуа

Задача 11.1 (!). Пусть задан полином $P(t) \in K[t]$ степени n с коэффициентами в поле K, у которого n попарно различных корней в K. Докажите, что кольцо $K[t]/P$ остатков по модулю P изоморфно прямой сумме n копий K.

Указание. Похожая задача была в листке 9.

Определение 11.1. Пусть K – алгебраическое расширение поля k (это часто обозначается как $[K : k]$). Говорят, что $[K : k]$ **расширение Галуа**, если $K \otimes_k K$ изоморфно (как алгебра) прямой сумме нескольких копий K.

Задача 11.2. Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней в $K = k[t]/P$. Докажите, что $[K : k]$ – расширение Галуа.

Задача 11.3. Докажите, что $[\mathbb{Q}[\sqrt{-1}\,] : \mathbb{Q}]$ – расширение Галуа.

Задача 11.4. Пусть $[k : \mathbb{Q}]$ – расширение степени 2 (т.е. K двумерно как векторное пространство над $\mathbb{Q}$). Докажите, что это расширение Галуа.

Задача 11.5 (!). Пусть p простое. Докажите, что для любого корня из единицы ζ степени p, $[\mathbb{Q}[\zeta] : \mathbb{Q}]$ – расширение Галуа.

Задача 11.6 (*). Будет ли $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$ расширением Галуа?

Задача 11.7 (*). Пусть F – поле характеристики p, а $k = F(z)$ – поле рациональных функций над F. Докажите, что полином $P(t) = t^p - z$ неприводим над k. Докажите, что $[k[t]/P : k]$ – не расширение Галуа.

Задача 11.8. Пусть $K_1 \supset K_2 \supset K_3$ – последовательность расширений полей. Докажите, что

$$K_2 \otimes_{K_3} K_1 \cong (K_2 \otimes_{K_3} K_2) \otimes_{K_2} K_1.$$

Задача 11.9. Пусть $K_1 \supset K_2 \supset K_3$ – последовательность расширений полей. Докажите, что

$$K_1 \otimes_{K_2} (K_2 \otimes_{K_2} \otimes_{K_3} K_2) \otimes_{K_2} K_1 \cong K_1 \otimes_{K_3} K_1.$$

Задача 11.10 (!). Пусть $K_1 \supset K_2 \supset K_3$ - последовательность расширений полей, причем $[K_1 : K_2]$ и $[K_2 : K_3]$ - расширения Галуа. Докажите, что $[K_1 : K_3]$ – расширение Галуа.

Задача 11.11. Докажите, что $\mathbb{Q}[\sqrt[3]{2}, \frac{\sqrt{-3}-1}{2}]$ – расширение Галуа.

Задача 11.12. Пусть $K_1 \supset K_2 \supset K_3$ – последовательность расширений полей. Докажите, что естественное отображение

$$K_1 \otimes_{K_3} K_1 \longrightarrow K_1 \otimes_{K_2} K_1$$

– сюрьективный гомоморфизм алгебр.

Задача 11.13 (!). Пусть $K_1 \supset K_2 \supset K_3$ – последовательность расширений полей, причем $[K_1 : K_3]$ – расширение Галуа. Докажите, что $[K_1 : K_2]$ – тоже расширение Галуа.

Указание. Воспользуйтесь задачей 9.28 листка Алгебра 9.

Задача 11.14. Пусть $P \in k[t]$ – полином степени n над полем k. Положим $K_1 = k$, и рассмотрим последовательность расширений, $K_l \supset K_{l-1} \supset \cdots \supset K_1$, полученных индуктивно следующим образом. Пусть K_j построено. Разложим P на неприводимые сомножители $P = \prod P_i$ в K_j. Если все P_i линейны, мы закончили. В противном случае, пусть P_0 – неприводимый сомножитель P степени > 1. Возьмем $K_{j+1} = K_j[t]/P_0$. Докажите, что этот процесс закончится через конечное число шагов и даст некоторое поле $K \supset k$.

Определение 11.2. Это поле называется **полем разложения** многочлена P.

Задача 11.15 (!). Пусть K – поле разложения для многочлена $P(t) \in k[t]$. Докажите, что K изоморфно подполю в алгебраическом замыкании $\overline{k}$, порожденному всеми корнями P.

Задача 11.16. Пусть $P(t)$ – многочлен степени n. Докажите, что степень его поля разложения не больше $n!$.

Задача 11.17. Пусть $P \in k[t]$ – многочлен степени n, имеющий n попарно различных корней в алгебраическом замыкании k, и пусть $[K : k]$ – его поле разложения, а $K_l \supset K_{l-1} \supset \cdots \supset K_1$ соответствующая цепочка расширений. Докажите, что $K \otimes_{K_{i-1}} K_i$ изоморфно прямой сумме нескольких копий K.

Указание. Это сразу следует из Задачи 11.1.

Задача 11.18 (!). Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней в алгебраическом замыкании k (такой полином называется **не имеющим кратных корней**), а K – его поле разложения. Докажите, что $[K : k]$ – расширение Галуа.

Указание. Воспользуйтесь предыдущей задачей.

Задача 11.19 (*). Пусть $P(t) \in k[t]$ – неприводимый многочлен над полем k характеристики 0. Докажите, что у P нет кратных корней.

Указание. Докажите, что у $P(t) = t^n + a_{n-1}t^{n-1} + \ldots$ нет кратных корней тогда и только тогда, когда P не имеет общих множителей с многочленом

$$P'(t) = nt^{n-1} + (n-1)a_{n-1}t^{n-2} + \cdots + 2a_2 t + a_1.$$

Для этого докажите, что $(PQ)' = PQ' + Q'P$, и вычислите $P'(t)$ для $P = (t - b_1) \ldots (t - b_n)$.

Замечание. Из предыдущей задачи следует, что над полем характеристики 0, поле разложения любого многочлена является расширением Галуа.

Задача 11.20 (*). Приведите пример поля k (ненулевой характеристики) и такого неприводимого многочлена $P \in k[t]$, что его поле разложения не является расширением Галуа.

Группа Галуа

Определение 11.3. Пусть $[K : k]$ – расширение Галуа. **Группой Галуа** $[K : k]$ называется группа k-линейных автоморфизмов поля K. Мы обозначаем группу Галуа через $\mathrm{Gal}([K : k])$ или через $\mathrm{Aut}_k(K)$.

В дальнейшем мы будем рассматривать $K \otimes_k K$ как K-алгебру, с действием K^*, заданным формулой $a(v_1 \otimes v_2) = av_1 \otimes v_2$. Такое действие K^* называется **левым**. Оно отличается от "правого действия", заданного формулой $a(v_1 \otimes v_2) = v_1 \otimes av_2$.

Задача 11.21. Пусть $[K : k]$ – расширение Галуа. Постройте биекцию между множеством K-линейных гомоморфизмов $K \otimes_k K \longrightarrow K$ и множеством неразложимых идемпотентов в $K \otimes_k K$.

Задача 11.22. Пусть $\mu : K \otimes_k K \longrightarrow K$ – ненулевой K-линейный гомоморфизм, а $k \otimes_k K \subset K \otimes_k K$ – k-подалгебра, естественно изоморфная K. Докажите, что $\mu \mid_{k \otimes_k K}$ задает k-линейный автоморфизм $K \longrightarrow K$.

Задача 11.23. Докажите, что всякий k-линейный автоморфизм K получается таким образом.

Указание. Пусть $\nu \in \mathrm{Gal}([K : k])$. Определим гомоморфизм $K \otimes_k K$ по формуле $v_1 \otimes v_2 \longrightarrow v_1\nu(v_2)$.

Задача 11.24 (!). Пусть $[K : k]$ – расширение Галуа. Постройте естественную биекцию между $\mathrm{Gal}([K : k])$ и множеством неразложимых идемпотентов в $K \otimes_k K$. Докажите, что порядок группы Галуа равен размерности K как векторного пространства над k.

Задача 11.25. Пусть $[K : k]$ – расширение Галуа, $\nu \in \mathrm{Gal}([K : k])$ – элемент группы Галуа, а e_ν – соответствующий идемпотент в $K \otimes_k K$. Обозначим через μ_l стандартное (левое) действие K^* на $K \otimes_k K$, а за μ_r правое действие. Докажите, что $\mu_l(a)e_\nu = \mu_r(\nu(a))e_\nu$.

Задача 11.26. Пусть $[K : k]$ – расширение Галуа, а $a \in K$ – элемент, инвариантный относительно $\mathrm{Gal}([K : k])$. Докажите, что $a \otimes 1 = 1 \otimes a$ в $K \otimes_k K$.

Указание. Воспользуйтесь задачей 11.25.

Задача 11.27 (!). Пусть $[K : k]$ – расширение Галуа, а $a \in K$ – элемент, инвариантный относительно $\mathrm{Gal}([K : k])$. Докажите, что $a \in k$.

Задача 11.28. Пусть $[K : k]$ – расширение Галуа, а K' – промежуточное поле, $K \supset K' \supset k$. Докажите, что $K' = K^{G'}$, где $G' \subset \mathrm{Gal}([K : k])$ – группа K'-линейных автоморфизмов K, а $K^{G'}$ обозначает множество G'-инвариантов.

Указание. Докажите, что $[K : K']$ – расширение Галуа, и воспользуйтесь предыдущей задачей.

Задача 11.29 (!). Докажите **основную теорему теории Галуа:** пусть $[K : k]$ – расширение Галуа. Тогда $G' \longrightarrow K^{G'}$ устанавливает биекцию между множеством подгрупп $G' \subset \mathrm{Gal}([K : k])$ и множеством промежуточных подполей $K \supset K' \supset k$.

Задача 11.30. Пусть $[K : k]$ – расширение Галуа, а K' – промежуточное поле, $K \supset K' \supset k$. Постройте естественное отождествление между множеством k-линейных гомоморфизмов $K' \to K$ и множеством $\mathrm{Gal}([K : k])/\mathrm{Gal}([K : K'])$ смежных классов группы Галуа $\mathrm{Gal}([K : k])$ по погруппе $\mathrm{Gal}([K : K']) \subset \mathrm{Gal}([K : k])$.

Задача 11.31. Найдите группу Галуа $[\mathbb{Q}[\sqrt{a}] : \mathbb{Q}]$.

Задача 11.32 (!). Пусть $[K : k]$ – расширение Галуа, а $a \in K$ – элемент, порождающий K над k (такой элемент называется **примитивным**). Докажите, что если $\nu_1, \nu_2, \dots, \nu_n$ – попарно различные элементы $\mathrm{Gal}([K : k])$, то $\nu_1(a), \nu_2(a), \dots \nu_n(a)$ линейно независимы над k.

Задача 11.33 (!). Пусть $[K : k]$ – расширение Галуа, а $V \subset K$ – объединение всех промежуточных полей $k \subset K' \subset K$, которые строго меньше k. Пусть K бесконечно. Докажите, что $V \neq K$.

Указание. V есть объединение конечного числа k-подпространств в K, которые имеют (над k) размерность меньше, чем размерность K как линейного пространства над k. Докажите, что в такой ситуации $V \neq K$.

Замечание. Из этого следует, что в любом расширении Галуа $[K : k]$ бесконечного поля k есть примитивный элемент.

Задача 11.34 (!). Пусть $[K : k]$ – расширение Галуа. Докажите, что для любого $a \in K$ произведение $P(t) = \prod_{\nu_i \in \mathrm{Gal}([K:k])} \in (t - \nu_i(a))$ – многочлен с коэффициентами в k.

Задача 11.35 (*). В условиях предыдущей задачи предположим, что a примитивный. Докажите, что $P(t)$ неприводим.

Задача 11.36 (!). Напомним, что корень n-й степени из единицы называется **примитивным**, если он порождает группу корней n-й степени из единицы. Пусть $\xi \in \mathbb{C}$ – примитивный корень степени n. Докажите, что группа $\mathrm{Gal}([\mathbb{Q}[\xi] : \mathbb{Q}])$ изоморфна группе $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ автоморфизмов группы $\mathbb{Z}/n\mathbb{Z}$. Найдите ее порядок.

Задача 11.37 (*). Зафиксируем целое число n. Пусть $P(t) = \prod(t - \xi_i)$, где ξ_i пробегает все примитивные корни степени n из единицы. Докажите, что $P(t)$ имеет рациональные коэффициенты и неприводим над $\mathbb{Q}$.

Замечание. Этот многочлен называется **круговым многочленом**.

Задача 11.38 (*). Разложите $x^n - 1$ на неприводимые множители над $\mathbb{Q}$.

Задача 11.39. Пусть $a_1, \dots, a_n \in \mathbb{Z}$ – взаимно простые числа, не являющиеся квадратами. Докажите, что $[\mathbb{Q}[\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}] : \mathbb{Q}]$ – расширение Галуа.

Задача 11.40. Найдите группу Галуа этого расширения.

Задача 11.41 (!). Докажите, что $\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n}$ линейно независимы над $\mathbb{Q}$.

Конечные поля

Из предыдущих листков нам известны следующие вещи про конечные поля. Порядок конечного поля равен p^n, где p – его характеристика. На любом поле k характеристики p задан **гомоморфизм Фробениуса**, $Fr : k \longrightarrow k$, $x \longrightarrow x^p$. В любое поле характеристики p естественно вложено конечное поле $\mathbb{F}_p$ из p элементов.

Мы обозначаем поле порядка p^n через $\mathbb{F}_{p^n}$.

Задача 11.42. Пусть $x \in \mathbb{F}_{p^n}$, $x \neq 0$. Докажите, что $x^{p^n-1} = 1$.

Указание. Воспользуйтесь теоремой Лагранжа (порядок элемента делит число элементов в группе).

Замечание. Из этого следует, что многочлен $P(t) = t^{p^n-1} - 1$ имеет ровно $p^n - 1$ корней в $\mathbb{F}_{p^n}$.

Задача 11.43 (!). Докажите, что $\prod_{\xi \in \mathbb{F}_{p^n} \setminus 0} = t^{p^n-1} - 1$.

Задача 11.44 (!). Докажите, что $[\mathbb{F}_{p^n} : \mathbb{F}_p]$ – расширение Галуа.

Задача 11.45 (!). Докажите, что $Fr, Fr^2, \ldots, Fr^{n-1}$ – попарно различные автоморфизмы $\mathbb{F}_{p^n}$.

Задача 11.46 (!). Докажите, что $\mathrm{Gal}([\mathbb{F}_{p^n} : \mathbb{F}_p])$ – циклическая группа порядка n.

Задача 11.47 (*). Докажите, что поле разложения многочлена $t^{p^n-1}-1$ над $\mathbb{F}_p$ имеет порядок p^n.

Задача 11.48 (*). Докажите, что поле порядка p^n единственно с точностью до изоморфизма.

Задача 11.49 (!). Перечислите все подполя в $\mathbb{F}_{p^n}$.

Задача 11.50 (!). Пусть $[K : k]$ – расширение Галуа. Докажите, что в K есть примитивный элемент.

Замечание. Для бесконечных полей мы это уже доказали, см. замечание к задаче 11.33.

Теорема Абеля

Теорема Абеля утверждает, что общий многочлен пятой степени неразрешим в радикалах; иначе говоря, что решение общего уравнения пятой степени нельзя выразить через посредство алгебраических операций (умножения, сложения, деления) и операции извлечения корня n-й степени. В этом разделе мы приведем пример уравнения, неразрешимого в радикалах.

Задача 11.51. Пусть $[K : k]$ – расширение Галуа. Докажите, что подгруппа $G' \subset \mathrm{Gal}([K : k])$ нормальна тогда и только тогда, когда $[K^{G'} : k]$ – расширение Галуа.

Задача 11.52 (!). Пусть $G' \subset \mathrm{Gal}([K : k])$ – нормальная подгруппа. Докажите, что группа $\mathrm{Gal}([K^{G'} : k])$ изоморфна фактору $\mathrm{Gal}([K : k])/G'$.

Определение 11.4. Расширение Галуа $[K : k]$ называется **циклическим**, если его группа Галуа циклическая.

Задача 11.53 (!). Пусть группа Галуа $[K : k]$ разрешима. Докажите, что $[K : k]$ можно представить в виде последовательности расширений Галуа $k = K_0 \subset K_1 \subset ... \subset K_n = K$, таким образом, что для каждого i, $\mathrm{Gal}([K_i : K_{i-1}])$ - циклическая группа.

Задача 11.54 (*). Пусть поле k содержит все корни из единицы порядка n, а $[K : k]$ – поле разложения многочлена $t^n - a$, не имеющего корней над k. Докажите, что это расширение циклическое.

Указание. Пусть α – какой-то корень многочлена $t^n - a$. Тогда все корни $t^n - a$ имеют вид $\alpha, \alpha\xi, \alpha\xi^2, \dots, \alpha\xi^{p-1}$, где ξ – корень из единицы. Докажите, что автоморфизм, переводящий α в $\alpha\xi^i$, переводит $\alpha\xi^q$ в $\alpha\xi^{q+i}$.

Задача 11.55 (*). Зафиксируем $n \in \mathbb{N}$ и $n \in \mathbb{Q}$. Пусть для любого $k > 1$, делящего n, $a \in \mathbb{Q}$ не равен k-й степени никакого рационального числа, а $[K : \mathbb{Q}]$ – поле разложения многочлена $t^n - a$. Докажите, что K содержит все корни n-й степени из единицы, а $\mathrm{Gal}([K : \mathbb{Q}])$ изоморфно скрученному произведению $\mathbb{Z}/n\mathbb{Z} \rtimes \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.

Задача 11.56 (*). Пусть k – поле характеристики 0, а $[K : k]$ – поле разложения многочлена $t^n - a$. Докажите, что группа Галуа $\mathrm{Gal}([K : k])$ разрешима.

Указание. Если k содержит корни n-й степени из 1, мы все доказали. Если нет, докажите, что K их содержит. Рассмотрите промежуточное расширение K', полученное добавлением этих корней к k, и докажите, что $[K : K']$ и $[K' : k]$ – расширения Галуа с абелевыми группами Галуа.

Задача 11.57. Пусть $[K : k]$ – циклическое расширение порядка n, ν – образующий группы $\mathrm{Gal}[K : k]$, $\xi \in k$ – примитивный корень из единицы степени n, а $\alpha \in K$ – примитивный элемент. Напишем **резольвенту Лагранжа**

$$L = a + \xi^{-1}\nu(a) + \xi^{-2}\nu^2(a) + \dots + \xi^{-n+1}\nu^{n-1}(a)$$

Докажите, что $\nu(L) = \xi L$. Докажите, что $L \neq 0$.

Задача 11.58 (*). Докажите, что $\prod_{i=0}^{n-1}(t - \nu^i(L)) = t^n - L^n$. Докажите, что L порождает K над k, и что $L^n \in k$.

Указание. Чтобы убедиться в том, что L порождает K над k, воспользуйтесь тем, что $\mathrm{Gal}[k[\sqrt[n]{L^n}], k] = \mathbb{Z}/n\mathbb{Z}$, а следовательно, размерность $k[L]$ над k такая же, как размерность K над k.

Задача 11.59 (*). Пусть $[K : k]$ – расширение Галуа порядка n, причем k содержит все корни n-й степени из единицы. Докажите, что $[K : k]$ циклическое тогда и только тогда, когда его можно получить добавлением корня n-й степени из $a \in k$.

Задача 11.60 (*). (теорема Галуа) Выведите из этого такую теорему. Расширение Галуа $[K : k]$ порождается последовательным добавлением решений уравнения $t^n - a$ тогда и только тогда, когда группа $\mathrm{Gal}[K : k]$ разрешима.

Замечание. Пусть $P(t) \in k[t]$ – многочлен. **Группой Галуа** P называется группа Галуа его поле разложения. Теорема Галуа утверждает, что уравнение $P(t) = 0$ разрешимо в радикалах тогда и только тогда, когда группа Галуа $P(t)$ разрешима.

Определение 11.5. Пусть группа G действует на множестве Σ. Действие называется **транзитивным**, если любой $x \in \Sigma$ можно перевести в любой $y \in \Sigma$ применением подходящего $g \in G$.

Задача 11.61. Пусть $G \subset S_n$ – подгруппа, содержащая транспозицию и действующая транзитивно на $\{1, 2, 3, \dots, n\}$. Докажите, что $G = S_n$.

Задача 11.62. Пусть $P \in k[t]$ – неприводимый многочлен, $\xi_1, \dots, \xi_n$ – его корни, и пусть все эти корни различны. Докажите, что группа Галуа P действует на $\{\xi_1, \dots, \xi_n\}$ транзитивно.

Указание. Разобьем $\{\xi_1, \dots, \xi_n\}$ на смежные классы по действию $\mathrm{Gal}(P)$. Пусть S такой класс. Докажите, что полином $\prod_{\xi_i \in S}(t - \xi_i)$ имеет коэффициенты в k, и делит P.

Задача 11.63 (!). Пусть $P \in \mathbb{Q}[t]$ – неприводимый многочлен степени n, у которого ровно $n - 2$ вещественных корня. Докажите, что его группа Галуа равна S_n.

Указание. Докажите, что $\mathrm{Gal}(P)$ транзитивно действует на корнях P, а комплексное сопряжение сохраняет поле разложения P и действует на множестве корней как транспозиция.

Задача 11.64 (!). (теорема Эйзенштейна) Пусть $Q = t^n + t^{n-1}a_{n-1} + t^{n-2}a_{n-2} + \dots + a_0$ – такой многочлен с целыми коэффициентами, что все a_i делят заданное простое число p, а $a_0 \not\vdots p^2$. Докажите, что Q неприводим над $\mathbb{Q}$.

Задача 11.65 (*). Докажите, что $Q(t) = x^5 - 10x + 5$ – неприводимый (над $\mathbb{Q}$) многочлен, у которого ровно 3 вещественных корня. Выведите из этого, что его группа Галуа это S_5.

Задача 11.66 (*). Докажите, что уравнение $x^5 - 10x + 5 = 0$ неразрешимо в радикалах.