Теория Галуа.

Задача 1 (несепарабельные расширения). Пусть $\operatorname{char} k = p > 0$ Назовем расширение K/k чисто несепарабельным, если $[K : k]_s = 1$.

a) Покажите, что следующие условия на K/k эквивалентны:
— K/k чисто несепарабельно;
— Минимальный многочлен над k любого элемента из K имеет вид $x^{p^n} - a$;
— $K = k(\alpha_i)_{i\in I}$ и минимальный многочлен над k каждого α_i имеет вид $x^{p^{n_i}} - a_i$.

b) Докажите, что чисто несепарабельные расширения образуют отмеченный класс расширений.

c) Пусть K/k — алгебраическое, K_0 — композит подполей K, сепарабельных над k. Тогда K_0/k сепарабельно, а K/K_0 чисто несепарабельно.

d) В некоторых случаях башню из предыдущей задачи можно „обратить“. Пусть K — нормальное расширение поля k, $G = \operatorname{Aut}(K/k)$ и K^G — неподвижное поле группы G. Докажите, что K^G чисто несепарабельно над k, а K сепарабельно над K^G. Кроме того, если K_0 — максимальное сепарабельное подрасширение K, то $K = K^G K_0$ и $k = K_0 \cap K^G$.
Подсказка: используйте рассуждение как в теореме Артина.

Задача 2 (примитивный элемент). a) Пусть E — конечное расширение поля k. Покажите, что элемент α, для которого $E = k(\alpha)$ существует тогда и только тогда, когда имеется конечное число промежуточных полей $k \subset F \subset E$.
Подсказка: в одну сторону воспользоваться тем, что, если $\alpha, \beta \in k$, то найдутся c_1 и c_2 такие, что $k(\alpha + c_1\beta) = k(\alpha + c_2\beta)$. В другую сторону, посмотреть на инъективное отображение $F \mapsto g_{\alpha,F}(x)$, сопостовляющее промежуточному полю F минимальный многочлен α над ним.

b) Пусть k — поле характеристики p, и пусть t, u алгебраически независимы над k. Покажите, что $k(u^p, t^p)$ имеет степень p^2 над $k(t, u)$, и между $k(t, u)$ и $k(u^p, t^p)$ существует бесконечно много промежуточных расширений.

c^{**}) Докажите, что между $k(t, u)$ и $k(u^p, t^p)$ найдется поле, не изоморфное $k(t, u)$.

Задача 3. a) Пусть x трансцендентен над $\mathbb{C}$. Покажите, что $\operatorname{Gal}(\mathbb{C}(x)/\mathbb{C}) \cong \mathrm{PGL}_2(\mathbb{C})$, т. е. состоит из отображений вида $x \mapsto \frac{ax+b}{cx+d}, ad - bc \neq 0$.
Подсказка: посмотрите на степень элементов из $\operatorname{Gal}(\mathbb{C}(x)/\mathbb{C})$.

b) Пусть x_1, x_2 алгебраически независимые переменные над $\mathbb{C}$. Сюръективно ли отображение $\mathrm{PGL}_3(\mathbb{C}) \hookrightarrow \operatorname{Gal}(\mathbb{C}(x_1, x_2)/\mathbb{C})$? Группа $\operatorname{Gal}(\mathbb{C}(x_1, x_2)/\mathbb{C})$ отождествляется с группой бирациональных автоморфизмов $\mathbb{P}^2_{\mathbb{C}}$ и называется *группой Кремоны*. Для ее исследования используются методы из алгебраической геометрии.

Задача 4′. [1] a) Пусть $K_1/k, K_2/k$ — расширения Галуа, содержащиеся в некотором поле F, и $\operatorname{Gal}(K_i/k) = G_i$. Убедитесь, что K_1K_2/k — расширение Галуа и отображение $\alpha : G \to G_1 \times G_2, \sigma \overset{\alpha}{\mapsto} (\sigma|_{K_1}, \sigma|_{K_2})$ инъективно. При этом оно сюръективно, если $K_1 \cap K_2 = k$.

b) Вычислите группу Галуа поля разложения $(x^4 - 2)(x^3 - 5)$ над $\mathbb{Q}$.

Задача 5′. Являются ли следующие расширения расширениями Галуа поля $\mathbb{Q}$? Если да, посчитайте их группу Галуа.

a) $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ b) $\mathbb{Q}(\sqrt{\sqrt{2} + \sqrt{-2}})$ c) $\mathbb{Q}(\sqrt[3]{2} + \sqrt{2})$ d) $\mathbb{Q}(\cos(\frac{\pi}{12}))$

Задача 6′. Покажите, что всякая конечная группа является группой Галуа некоторого расширения.
Подсказка: посмотрите сначала на S_n.

Задача 7′. Опишите все расширения Галуа поля $\mathbb{Q}$ с группами порядка $2, 3, 4$.

[1]Задачи со значком ′ очень рекомендуется научиться решать.

Задача 8 (посчитаем группы Галуа). Для многочлена $f(x) \in k[x]$ без кратных корней пусть G_f обозначает группу Галуа поля разложения k_f многочлена f. Предположим, что $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$ в k_f. Отождествим G_f с подгруппой в группе S_n перестановок корней $\alpha_1, \dots, \alpha_n$.

a') Определим дискриминант f как $\mathrm{Disc}(f) = \prod\limits_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$. Покажите, что $\mathrm{Disc}(f) \in k$.

b') Докажите, что G_f состоит из четных перестановок (т. е. $G_f \subset A_n$) $\Leftrightarrow$ $\mathrm{Disc}(f)$ — квадрат в k.

c') Покажите, что G_f действует на корнях f транзитивно тогда и только тогда, когда f неприводим.

d') Как считать группу Галуа произвольного многочлена степени 3? Чему равна $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$, если $f(x) = x^3 - 3x + 1$? А если $f(x) = x^3 + 3x + 1$?

e') Пусть $\deg f = 4$. Положим $\alpha = \alpha_1\alpha_2 + \alpha_3\alpha_4$, $\beta = \alpha_1\alpha_3 + \alpha_2\alpha_4$, $\gamma = \alpha_1\alpha_4 + \alpha_2\alpha_3$, и пусть $V = \{1, (12)(34), (13)(24), (14)(23)\} \subset S_4$ — подгруппа Клейна. Покажите, что неподвижное поле для $G_f \cap V$ совпадает с $k(\alpha, \beta, \gamma)$.

f') Выразите коэффициенты кубической резольвенты $g(x) = (x - \alpha)(x - \beta)(x - \gamma)$ для $f(x)$ через коэффициенты многочлена f. Как определить индекс $(G_f : G_f \cap V)$?

g') Вычислите группу Галуа поля разложения произвольного многочлена степени 4. Приведите примеры многочленов степени 4 со всеми возможными группами Галуа.

Подсказка: подгруппы S_4 — это S_4, A_4, D_4, V и $\mathbb{Z}/4\mathbb{Z}$.

h) Пусть $f(x) = x^5 + ax + b, a, b \in \mathbb{Q}$. Покажите, что $G_f \cong D_5$ (группа диэдра), тогда и только тогда, когда $f(x)$ неприводим над $\mathbb{Q}$, дискриминант $D_f = 4^4a^5 + 5^5b^4$ — квадрат в $\mathbb{Q}$ и уравнение $f(x) = 0$ разрешимо в радикалах.

i) Пусть $p \ge 5$ — простое, m — четное положительное число, $n_1 < n_2 < \dots < n_{p-1}$ — четные. Положим $g(x) = (x^2 + m)(x - n_1) \dots (x - n_{p-1})$. Выберем нечетное $n > 0$ так, что $\frac{2}{n} < \min_{g'(x)=0} |g(x)|$. Покажите, что, если $f(x) = g(x) - \frac{2}{n}$, то $G_f = S_p$.

Подсказка: воспользуйтесь тем, что у $f(x)$ ровно два невещественных корня, а группа S_p порождена транспозицией и p-циклом.

j^*) Покажите, что $G_f = \mathrm{PGL}_2(\mathbb{F}_5)$ для $f = x^6 + 2x^5 + 3x^4 + 4x^3 + 5x^2 + 6x + 7$.

Задача 9 (круговые поля). Определим по индукции круговой многочлен $f_n(x)$ следующим образом:

$$f_n(x) = \frac{x^n - 1}{\prod\limits_{d|n, d<n} f_d(x)}, \ f_1(x) = x - 1.$$

a') Покажите, что $f_n(x)$ имеет целочисленные коэффициенты, а корни $f_n(x)$ — в точности примитивные корни степени n из 1.

b') Докажите, что $f_n(x)$ неприводим над $\mathbb{Q}$.

c) Убедитесь в том, что выполнены равенства:

$$f_p(x) = x^{p-1} + \dots + 1, \ p \text{ — простое};$$

$$f_n(x) = f_{p_1 \dots p_s}(x^{p_1^{r_1-1}} \dots x^{p_s^{r_s-1}}), \ n = p_1^{r_1} \dots p_s^{r_s} \text{— разложение на простые};$$

$$f_{pn}(x) = \frac{f_n(x^p)}{f_n(x)}, \text{где } p \text{ — простое число, } p \nmid n;$$

$$f_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}, \text{ где } \mu(d) \text{ — функция Мёбиуса.}$$

d) Пусть ζ — примитивный корень степени p из 1. Положим, $S = \sum\limits_{k=1}^{p-1} \left(\frac{k}{p}\right)\zeta^k$, где $\left(\frac{k}{p}\right)$ — символ Лежандра. Покажите, что $S^2 = \left(\frac{-1}{p}\right)p$.

e) Покажите, что любое квадратичное расширение поля $\mathbb{Q}$ содержится в поле, полученном присоединением к $\mathbb{Q}$ корня некоторой степени из 1. (Этот факт верен и для произвольных абелевых расширений $\mathbb{Q}$ — весьма трудная теорема Кронекера–Вебера.)

f) Чему равна степень расширения $\mathbb{Q}(\cos(\frac{2\pi}{n}))/\mathbb{Q}$? При каких n правильный n-угольник можно построить с помощью циркуля и линейки?

Задача 10$'$ (расширения Артина–Шрайера). a) Пусть k — поле, K/k — расширение степени n с циклической группой Галуа G (т. е. расширение K/k — циклическое). Пусть σ — образующая G и $\beta \in K$. Докажите, что след $\mathrm{Tr}_{K/k}(\beta) = 0$ в том и только том случае, когда существует $\alpha \in K$, такой, что $\beta = \alpha - \sigma\alpha$.

b) Пусть k — поле характеристики p. Если K/k — циклическое степени p, то существует $\alpha \in K$, такой, что $K = k(\alpha)$, причем α удовлетворяет уравнению $x^p - x - a = 0$ для некоторого $a \in k$.

c) Обратно, для $a \in k$ многочлен $x^p - x - a$ либо имеет корень в k и тогда все его корни лежат в k, либо неприводим. В последнем случае, если α — некоторый его корень, то $k(\alpha)/k$ — циклическое расширение степени p.

Задача 11*. a) Пусть k — поле, $n \geq 2$, $a \in k^*$, причем $a \notin k^p$ для всех простых p, делящих n и $a \notin -4k^4$, если $4 \mid n$. Докажите, что многочлен $x^n - a$ неприводим над $k[x]$.

Подсказка: сведите все к случаю, когда n — степень простого.

b) Пусть k — поле и алгебраическое замыкание $\bar{k}$ имеет конечную степень над k. Покажите, что в таком случае $\bar{k} = k(i)$, где $i^2 = -1$ и $\mathrm{char}\, k = 0$.

Подсказка: рассмотрите подгруппу порядка p группы $\mathrm{Gal}(\bar{k}/k)$ и воспользуйтесь свойствами расширений Куммера и Артина–Шрайера, а также предыдущим пунктом задачи.

Задача 12 (теория Галуа для бесконечных расширений). Пусть Ω/F — бесконечное алгебраическое расширение Галуа. Определим *топологию Крулля* на группе $G = \mathrm{Gal}(\Omega/F) = \mathrm{Aut}(\Omega/F)$, взяв в качестве базы открытых окрестностей единицы всевозможные нормальные подгруппы $G(S) = \{\sigma \in G \mid \sigma(s) = s, \text{ для всех } s \in S\}$, где S — конечное подмножество Ω (иными словами, $G(S)$ оставляет неподвижным конечное расширение $F(S)/F$).

a) Убедитесь, что $G(S)$ действительно задают на G структуру топологической группы.

b) (для знакомых с проективными пределами) Убедитесь, что $G = \varprojlim\limits_{E/F-\text{конечно}} \mathrm{Gal}(E/F)$.

c) Для каждого конечного промежуточного расширения $\Omega \supset E \supset F$ имеется непрерывная сюрьекция $\sigma \mapsto \sigma\,|_E$: $\mathrm{Gal}(\Omega/F) \to \mathrm{Gal}(E/F)$ в дискретной топологии на $\mathrm{Gal}(E/F)$.

d) Покажите, что G в топологии Крулля Хаусдорфова (у любых 2-х элементов есть непересекающиеся открытые окрестности), вполне несвязана (связные компоненты — одноточечные множества) и компактна.

Подсказка: для компактности воспользуйтесь теоремой Тихонова о том, что произведение (бесконечное) компактов — компакт.

e) Покажите, что для любого промежуточного поля $\Omega \supset E \supset F$ группа Галуа $\mathrm{Gal}(\Omega/E)$ — замкнутая подгруппа в G и $\Omega^{\mathrm{Gal}(\Omega/E)} = E$.

f) Обратно, для любой погруппы H в G группа $\mathrm{Gal}(\Omega/\Omega^H)$ совпадает с замыканием H в G.

g) Докажите аналог основной теоремы теории Галуа для бесконечных расширений о соответствии между *замкнутыми* подгруппами G и промежуточными расширениями в $\Omega \supset F$.

h) Верно ли утверждение задачи 4 a) для бесконечных расширений Галуа?

i) Постройте изоморфизм $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) \cong \prod_{p-\text{простое}} \mathbb{Z}_p$, где $\mathbb{Z}_p$ — кольцо целых p-адических чисел.

Задача 13 (линейная независимость корней). В этой задаче цель — доказать, что дробные степени различных чисел линейно независимы, если нет „очевидных“ линейных зависимостей.

a) Пусть n, d — взаимно простые целые числа, $\phi, i : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ задаются формулами $i(x) = -x, \phi(x) = 1 + dx$. Тогда итерацией ϕ и i можно получить из нуля любой элемент $\mathbb{Z}/n\mathbb{Z}$.

b) Пусть ζ — примитивный корень степени n из 1. Покажите, что модуль определителя $n \times n$ матрицы V с элементами $v_{ij} = \zeta^{i(j-1)}, i, j = 1 \ldots n$ равен $n^{n/2}$.

c) Пусть $K \subset L \subset \mathbb{R}$ — расширение полей, $A \subset L, |A| \geq 2$. Пусть для любого $a \in A$ найдется n_a (которое мы предполагаем минимальным), такое, что $a^{n_a} \in K$, и пусть, кроме того, элементы A попарно линейно независимы над K. Покажите, что в этом случае элементы A линейно независимы над K.

Подсказка: пусть $B = \{b_i \mid i \in I\}$ — минимальное линейно зависимое подмножество, $\sum_{i \in I} k_i b_i = 0$, $n =$НОК$(\{n_{b_i} \mid i \in I\})$. Пусть M — поле разложения многочлена $(x^n - 1) \prod_{i \in I}(x^{n_{b_i}} - b_i^{n_{b_i}})$, $G = \mathrm{Gal}(M/K)$, $\zeta \in M$ — примитивный корень степени n из 1. Пусть $f \in G$, положим $B_{t,f} = \{i \in I \mid f(b_i) = b_i\zeta^t\}$ и $C_{t,f} = \sum_{i \in B_{t,f}} k_i b_i$. Действуя f и комплексным сопряжением на уравнение линейной зависимости и пользуясь пунктами a) и b), получите, что $C_{t,f} = 0$ для любого t, а значит $I = B_{t,f}$ для некоторого t. Выведите отсюда утверждение задачи.

d) Чему равна степень $[\mathbb{Q}(p_1^{1/n_1}, \ldots, p_k^{1/n_k}) : \mathbb{Q}]$, если $n_i \geq 2$ — натуральные, а p_i — различные простые?

e^*) Обобщите утверждение пункта c) на случай, когда $L \not\subseteq \mathbb{R}$.

Подсказка: последите за корнями из 1 в L.