Теория Галуа 5: Расширения Галуа

Правила: Зачеты по листкам бывают двух типов: когда сданы все (или 1/3, или 2/3) задачи со звездочками, либо все (или 1/3, или 2/3) 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.

Если сдана 1/3 задач с (*) и (!), студент получает $2t$ баллов, если 2/3 задач, $6t$ баллов, если все, кроме (максимум) двух – $10t$ баллов.

Если сдана 1/3 задач без звездочек и с (!), студент получает $2t$ баллов, если 2/3 задач, студент получает $6t$ баллов, если все, кроме (максимум) трех – $10t$ баллов.

Эти виды оценок не складываются, то есть больше $10t$ за листочек получить нельзя.

Коэффициент t равен 1.5, если задачи сданы не позже, чем через 20 дней после выдачи, 1, если между 20 и 35 днями, и 0.7, если позже.

Результаты сдачи записываются на листке ведомости, которая выдается студенту, и ее надо хранить до получения окончательных оценок по курсу.

5.1. Расширения Галуа

При сдаче задач (кроме тех, где это специально оговорено или подразумевается), можно предполагать, что $\operatorname{char} k = 0$.

Задача 5.1. 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.

Определение 5.1. Пусть $[K : k]$ – алгебраическое расширение поля k. Говорят, что $[K : k]$ **расширение Галуа**, если $K \otimes_k K$ изоморфно (как кольцо) прямой сумме нескольких копий K.

Задача 5.2. 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.

Определение 5.2. Напомню, что конечное расширение $[K : k]$ **несепарабельно**, если форма следа $\operatorname{Tr}_k : K \longrightarrow k$ равна нулю.

Задача 5.3 (!). Пусть $[K : k]$ – конечное расширение полей. Докажите, что $[K : k]$ несепарабельно тогда и только тогда, когда $K \otimes_k K$ содержит нильпотенты.

Задача 5.4. Докажите, что $[\mathbb{Q}[\sqrt{-1}] : \mathbb{Q}]$ – расширение Галуа.

Задача 5.5. Пусть $[K : \mathbb{Q}]$ – расширение степени 2 (т.е. K двумерно как векторное пространство над $\mathbb{Q}$). Докажите, что это расширение Галуа.

Задача 5.6 (!). Пусть p простое. Докажите, что для любого корня из единицы ζ степени p, $[\mathbb{Q}[\zeta] : \mathbb{Q}]$ – расширение Галуа.

Задача 5.7 (*). Будет ли $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$ расширением Галуа?

Задача 5.8 (**). Пусть $[K : \mathbb{Q}[\sqrt{-1}]]$ – расширение Галуа. Докажите, что $[K : \mathbb{Q}]$ – расширение Галуа, или найдите контрпример.

Задача 5.9 (*). 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 5.10. 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 5.11. Рассмотрим расширение $[\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}]$. Докажите, что это не расширение Галуа.

Задача 5.12 (*). 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, или найдите контрпример.

Указание. Воспользуйтесь предыдущей задачей.

Задача 5.13. Докажите, что $\mathbb{Q}[\sqrt[3]{2}, \frac{\sqrt{-3}-1}{2}]$ – расширение Галуа.

Задача 5.14. 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 5.15 (!). 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.

5.2. Поля разложения

Задача 5.16. 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 5.3. Это поле называется **полем разложения** (splitting field) многочлена P.

Задача 5.17. Пусть K – поле разложения для многочлена $P(t) \in k[t]$. Докажите, что K изоморфно подполю в алгебраическом замыкании $\bar{k}$, порожденному всеми корнями P.

Задача 5.18 (!). Пусть все корни $P(t)$ разные. Докажите, что поле разложения $P(t)$ есть минимальное расширение Галуа, содержащее $k[t]/(P)$.

Задача 5.19. Докажите, что поле разложения любого полинома единственно, с точностью до изоморфизма.

Указание. Воспользуйтесь предыдущей задачей.

Задача 5.20. Пусть $P(t)$ – многочлен степени n. Докажите, что степень его поля разложения не больше $n!$

Задача 5.21. 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 5.1.

Задача 5.22. 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 5.23. Пусть $P(t) \in k[t]$ – неприводимый многочлен над полем k характеристики 0. Докажите, что у P нет кратных корней.

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

$$P'(t) = nt^{n-1} + (n-1)a_{n-1}t^{n-2} + \dots + 2a_2t + a_1.$$

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

Замечание 5.1. Из предыдущей задачи следует, что над полем характеристики 0, поле разложения любого многочлена является расширением Галуа.

Задача 5.24. Пусть $a_1, ..., a_n$ – целые числа. Докажите, что $\mathbb{Q}[\sqrt{a_1}, ..., \sqrt{a_n}]$ – расширение Галуа (или прямая сумма расширений Галуа).

Задача 5.25 (**). Пусть $\operatorname{char} k = p$, а $f(x) = x^p - x + c$ – неприводимый многочлен над k. Докажите, что $k[t]/(f)$ есть расширение Галуа.

Задача 5.26 (*). Пусть $[K : \mathbb{Q}]$ – поле разложения многочлена $x^3 - 2$. Рассмотрим K как подполе в $\mathbb{C}$. Найдите комплексное число, которое порождает K над $\mathbb{Q}$.

Задача 5.27 (*). Пусть p простое, а $[K : \mathbb{Q}]$ – поле разложения многочлена $x^p - 2$. Докажите, что степень $[K : \mathbb{Q}]$ (то есть размерность K как $\mathbb{Q}$-линейного пространства) равна $p(p-1)$.