Теория Галуа 6: Группы 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.

6.1. Основная теорема теории Галуа

Определение 6.1. 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 6.1 (!). 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 6.2. 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 6.3. Докажите, что всякий k-линейный автоморфизм K получается таким образом.

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

Задача 6.4 (!). 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 6.5. 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 6.6. 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 6.5.

Задача 6.7 (!). Пусть $[K : k]$ – расширение Галуа, а $a \in K$ – элемент, инвариантный относительно $\mathrm{Gal}([K : k])$. Докажите, что $a \in k$.

Задача 6.8. 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 6.9 (!). 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 6.10 (!). Пусть $[K : k]$ расширение степени n.

а. Докажите, что $\mathrm{Aut}_k K \leqslant n$.

б. Докажите, что K – расширение Галуа тогда и только тогда, когда $|\mathrm{Aut}_k K| = n$.

6.2. Группы Галуа и корни многочленов

Задача 6.11. Найдите группу Галуа $[\mathbb{Q}[\sqrt{a}] : \mathbb{Q}]$.

Задача 6.12. 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 6.1. Из этого следует, что в любом расширении Галуа $[K : k]$ бесконечного поля k есть примитивный элемент.

Задача 6.13. Пусть $[K : k]$ – расширение Галуа. Докажите, что для любого $a \in K$ произведение $P(t) = \prod_{\nu_i \in \mathrm{Gal}([K:k])}(t - \nu_i(a))$ – многочлен с коэффициентами в k.

Задача 6.14 (!). Пусть $[K : k]$ – расширение Галуа. Докажите, что для любого $a \in K$ существует многочлен $P(t) \in k[t]$, $P(a) = 0$, все корни которого лежат в K.

Указание. Воспользуйтесь предыдущей задачей.

Задача 6.15 (!). Пусть $[K : k]$ – конечное расширение, $\mathsf{char}\, k = 0$. Докажите, что это расширение Галуа тогда и только тогда, когда для любого $a \in K$ существует многочлен $P(t) \in k[t]$, $P(a) = 0$, все корни которого лежат в K.

Задача 6.16 (*). Докажите утверждение предыдущей задачи для любого сепарабельного расширения $[K : k]$ (без условия $\mathsf{char}\, k = 0$).

Задача 6.17. 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 6.18 (**). 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 6.2. Этот многочлен называется **круговым многочленом** (cyclotomic polynomial).

Задача 6.19. 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 6.20. Найдите группу Галуа этого расширения.

Задача 6.21 (!). В условиях предыдущей задачи, докажите, что $\sqrt{a_1}$, $\sqrt{a_2}$, $\dots$, $\sqrt{a_n}$ линейно независимы над $\mathbb{Q}$.

Задача 6.22. Докажите, что $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2}]) = \{1\}$.

Задача 6.23 (*). Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней в $K = k[t]/P$. Докажите, что его группа Галуа абелева, или найдите контрпример.

Задача 6.24. Пусть $P(t) = x^3 - 2$.

а. Докажите, что поле разложения P над $\mathbb{Q}$ имеет степень 6.

б. (!) Найдите его группу Галуа.

Задача 6.25 (**). Докажите, что $\mathbb{Q}[\sqrt[4]{2}, \sqrt{-1}]$ – расширение Галуа $\mathbb{Q}$, а его группа Галуа – диэдральная порядка 8.

Задача 6.26 (**). Найдите пример расширения $[K : k]$ степени 4 такого, что не существует промежуточных полей $K \supsetneq K' \supsetneq k$, или докажите, что такого не бывет.

Задача 6.27 (*). Пусть $P(t) \in \mathbb{Q}[t]$ – неприводимый полином, у которого есть вещественные и комплексные корни. Докажите, что группа Галуа поля разложения $P(t)$ неабелева.