Комплексные пространства 7: теория Галуа (2)

Правила: Зачеты по листкам бывают двух типов: когда сданы все (или или 2/3) задачи со звездочками, либо все (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 или факториалом из того же листочка. Задачи, обозначенные (!), следует сдавать и тем и другим.

Если сданы 2/3 задач со звездочками и (!), студент получает $6t$ баллов, если все, кроме (максимум) одной – $10t$ баллов.

Если сданы 2/3 задач без звездочки и с (!), студент получает $6t$ баллов, если все, кроме (максимум) двух – $10t$ 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 31 день после выдачи, 1, если между 31 и 50 днями, и 0.7, если позже.

Результаты сдачи записываются на листке ведомости, которая выдается студенту; просьба не терять ее, больше нигде результаты храниться не будут.

7.1. Расширения Галуа

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

Задача 7.1. 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 7.1. 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 7.2. Пусть $[K : \mathbb{Q}]$ – расширение степени 2 (т.е. K двумерно как векторное пространство над $\mathbb{Q}$). Докажите, что это расширение Галуа.

Задача 7.3 (*). Пусть p простое. Докажите, что для любого корня из единицы ζ степени p, $[\mathbb{Q}[\zeta] : \mathbb{Q}]$ – расширение Галуа.

Задача 7.4. 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 7.2. Это поле называется **полем разложения** (splitting field) многочлена P.

Задача 7.5. 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 7.6 (!). Пусть все корни $P(t)$ разные. Докажите, что поле разложения $P(t)$ есть минимальное расширение Галуа, содержащее $k[t]/(P)$.

Задача 7.7. Пусть $P(t)$ – многочлен степени n. Докажите, что степень его поля разложения не больше $n!$

Задача 7.8. 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 7.1.

Задача 7.9. 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 7.10 (!). Пусть $a_1, ..., a_n$ – целые числа. Докажите, что $\mathbb{Q}[\sqrt{a_1}, ..., \sqrt{a_n}]$ – расширение Галуа (или прямая сумма расширений Галуа).

7.2. Группы Галуа

Определение 7.3. 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" $\mu_r : K^* \times K \otimes_k K \longrightarrow K \otimes_k K$, заданного формулой $a(v_1 \otimes v_2) = v_1 \otimes av_2$.

Задача 7.11 (!). Пусть $[K : k]$ – расширение Галуа. Постройте биекцию между множеством K-линейных гомоморфизмов $K \otimes_k K \longrightarrow K$ и множеством неразложимых идемпотентов в $K \otimes_k K$.

Указание. Докажите, что каждый такой гомоморфизм переводит все неразложимые идемотенты, кроме одного, в нуль.

Задача 7.12. 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 7.13. Докажите, что всякий k-линейный автоморфизм $\nu\in \operatorname{Aut}_k(K)$ получается таким образом.

Указание. Домножьте на себя, и убедитесь, что ν продолжается до K-линейного автоморфизма $K\otimes_k K$, заданного формулой $v_1\otimes v_2\longrightarrow v_1\nu(v_2)$.

Задача 7.14 (!). Пусть $[K:k]$ – расширение Галуа. Постройте естественную биекцию между $\operatorname{Gal}([K:k])$ и множеством неразложимых идемпотентов в $K\otimes_k K$. Докажите, что порядок группы Галуа равен размерности K как векторного пространства над k.

Указание. Разложите $K\otimes_k K$ в прямую сумму полей, изоморфных K, и воспользуйтесь задачей 7.11.

Задача 7.15. Пусть $[K:k]$ – расширение Галуа, $\nu\in\operatorname{Gal}([K:k])$ – 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 7.16. Пусть $[K:k]$ – расширение Галуа, а $a\in K$ – элемент, инвариантный относительно $\operatorname{Gal}([K:k])$. Докажите, что $a\otimes 1=1\otimes a$ в $K\otimes_k K$.

Указание. Воспользуйтесь задачей 7.15.

Задача 7.17 (!). Пусть $[K:k]$ – расширение Галуа, а $a\in K$ – элемент, инвариантный относительно $\operatorname{Gal}([K:k])$. Докажите, что $a\in k$.

Указание. Воспользуйтесь предыдущей задачей.

Задача 7.18. Пусть $[K:k]$ – расширение Галуа, а K' – промежуточное поле, $K\supset K'\supset k$. Докажите, что $K'=K^{G'}$, где $G'\subset\operatorname{Gal}([K:k])$ – группа K'-линейных автоморфизмов K, а $K^{G'}$ обозначает множество G'-инвариантов.

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

Задача 7.19 (!). Докажите **основную теорему теории Галуа:** пусть $[K : k]$ – расширение Галуа. Тогда $G' \longrightarrow K^{G'}$ устанавливает биекцию между множеством подгрупп $G' \subset \operatorname{Gal}([K : k])$ и множеством промежуточных подполей $K \supset K' \supset k$.

Задача 7.20 (!). Пусть $[K : k]$ – расширение степени n.

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

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

Указание. Разложите $K \otimes_k K$ в прямую сумму полей, и воспользуйтесь $\operatorname{Aut}_k K = \operatorname{Aut}_k(K \otimes_k K)$.

Определение 7.4. Пусть $[K : k]$ – расширение полей. Элемент $\alpha \in K$ называется **примитивным**, если он порождает K.

Задача 7.21 (!). (теорема Артина о примитивном элементе)
Докажите, что каждое конечное расширение $[K : k]$ в характеристике 0 порождено примитивным элементом.

Указание. Воспользуйтесь основной теоремой теории Галуа.

Задача 7.22 (*). Найдите конечное расширение в характеристике p, которое не может быть порождено примитивным элементом.

Задача 7.23. 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 7.24. Найдите группу Галуа этого расширения.

Задача 7.25 (!). В условиях предыдущей задачи, докажите, что $\sqrt{a_1}$, $\sqrt{a_2}$, $\dots$, $\sqrt{a_n}$ линейно независимы над $\mathbb{Q}$.

Задача 7.26. Докажите, что $\operatorname{Aut}_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2}]) = \{1\}$.

Задача 7.27. Пусть $P(t) = x^3 - 2$.

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

б. (!) Найдите его группу Галуа.

Задача 7.28 (*). 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.