Теория Галуа 7: Конечные поля и абелевы расширения

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.

7.1. Конечные поля

Из курса алгебры 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 7.1. 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 7.1. Из этого следует, что многочлен $P(t) = t^{p^n-1} - 1$ имеет ровно $p^n - 1$ корней в $\mathbb{F}_{p^n}$.

Задача 7.2 (!). Пусть $\mathbb{F}^*_{p^n}$ – мультипликативная группа ненулевых элементов конечного поля. Докажите, что она циклическая.

Указание. Воспользуйтесь теоремой Безу (число корней многочлена степени n над полем не больше n), чтобы найти элемент порядка $p^n - 1$ в $\mathbb{F}^*_{p^n}$.

Задача 7.3. Докажите, что $\prod_{\xi \in \mathbb{F}^*_{p^n}} (t - \xi) = t^{p^n-1} - 1$.

Задача 7.4 (!). Докажите, что $[\mathbb{F}_{p^n} : \mathbb{F}_p]$ – расширение Галуа.

Задача 7.5. Докажите, что $Fr, Fr^2, \dots, Fr^{n-1}$ – попарно различные автоморфизмы $\mathbb{F}_{p^n}$.

Указание. Воспользуйтесь теоремой Безу.

Задача 7.6 (!). Докажите, что $\mathrm{Gal}([\mathbb{F}_{p^n} : \mathbb{F}_p])$ – циклическая группа порядка n.

Задача 7.7 (!). Докажите, что поле разложения многочлена $t^{p^n-1} - 1$ над $\mathbb{F}_p$ имеет порядок p^n.

Задача 7.8 (!). Докажите, что поле порядка p^n единственно с точностью до изоморфизма.

Задача 7.9. Перечислите все подполя в $\mathbb{F}_{p^n}$.

Задача 7.10 (!). Пусть $[K : k]$ – расширение Галуа. Докажите, что в K есть примитивный элемент.

Указание. Отдельно разберите случай конечных и бесконечных полей.

Задача 7.11 (!). Докажите, что каждое конечное расширение $[K : k]$ в характеристике 0 порождено примитивным элементом.

Указание. Воспользуйтесь основной теоремой теории Галуа.

Задача 7.12 (*). Докажите то же самое для любого сепарабельного расширения. «Сепарабельное расширение» есть расширение $[K : k]$, для которого функция следа $\mathsf{Tr}_k K$ не равна нулю.

Задача 7.13 (*). Найдите конечное (несепарабельное) расширение, которое не может быть порождено примитивным элементом.

Задача 7.14 (**). Пусть $P(t) \in \mathbb{F}_p[t]$ – неприводимый многочлен степени n. Докажите, что его поле разложения изоморфно $\mathbb{F}_{p^n}$.

Задача 7.15. Разложите $x^8 - x$ в произведение неприводимых полиномов над $\mathbb{F}_2$.

Задача 7.16. Докажите, что каждый элемент конечного поля представляется в виде суммы квадратов.

7.2. Циклические расширения

Определение 7.1. Расширение Галуа $[K : k]$ называется **циклическим**, если его группа Галуа циклическая.

Задача 7.17. 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 7.18. Зафиксируем $n \in \mathbb{N}$ и $a \in \mathbb{Q}$. Пусть для любого $k > 1$, $|a|$ не равен k-й степени никакого рационального числа, а $[K : \mathbb{Q}]$ – поле разложения многочлена $t^n - a$.

а. Докажите, что K содержит все корни n-й степени из единицы.

б. (*) Постройте вложение из $\mathrm{Gal}([K : \mathbb{Q}])$ в полупрямое произведение $\mathbb{Z}/n\mathbb{Z} \rtimes \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.

в. (**) Найдите пример n и a, для которого это не изоморфизм.

Задача 7.19. Пусть $[K : k]$ – циклическое расширение порядка n, ν – образующая группы $\mathrm{Gal}[K : k]$, $\xi \in k$ – примитивный корень из единицы степени n, а $a \in K$ – 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 $L \neq 0$, для какого-то примитивного a, если поле k бесконечно.

Задача 7.20. В условиях предыдущей задачи, 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 7.21 (!). 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 7.22 (*). Пусть p – простое число вида $2^{2^n} + 1$ (простое число Ферма, Fermat's prime), а $P(t) := \sum_{i=0}^{p-1} t^i$. Докажите, что $P(t)$ неприводимо, а поле K_0 разложения $P(t)$ имеет вид $[K_0 : K_1 : K_2 : ...K_n = k]$, где все расширения $[K_i : K_{i+1}]$ квадратичны, то есть степени 2.

Задача 7.23 (**). Пусть p – простое число вида $2^k + 1$. Докажите, что k есть степень 2.

Задача 7.24 (*). Докажите, что группа Галуа поля разложения $P(t) = t^5 - 2$ имеет порядок 20.

Определение 7.2. Циклотомическое расширение $[K : \mathbb{Q}]$ есть поле разложения для одного из неприводимых сомножителей многочлена $P(t) := \sum_{i=0}^{n-1} t^i$.

Задача 7.25 (**). Докажите, что каждое число вида $\sqrt{d}$, $d \in \mathbb{N}$, лежит в каком-то циклотомическом расширении.