

ЗАДАЧИ ПО ТЕОРИИ ГАЛУА (19.01.2017)

Пусть P – непостоянный многочлен от одной переменной над полем k .

- (1) Пусть $\varphi : A \rightarrow B$ – инъективный гомоморфизм коммутативных колец (например, A – поле), $Q(x) = \sum_{i=0}^n a_i x^i \in A[x]$ и $\sum_{i=0}^n \varphi(a_i) x^i \in B[x]$ неприводим над B . Тогда $Q(x)$ неприводим над A .
- (2) Докажите, что многочлен P имеет корень в некотором расширении поля k .
- (3) Предположим, что многочлен P неприводим. Докажите, что а) среди расширений L , в которых есть корни многочлена P , есть минимальные (относительно включения); б) все такие минимальные расширения L изоморфны над k .
- (4) Докажите, что над некоторым расширением поля k многочлен P разлагается на линейные множители.
- (5) Докажите, что существует минимальное расширение поля k , в котором многочлен P имеет разложение на линейные множители, и все такие минимальные расширения изоморфны над k . Такие поля называются *полями расщепления многочлена P* .
- (6) Докажите, что (а) порядок конечного поля является степенью его характеристики, (б) для любой степени q любого простого числа существует конечное поле порядка q , (в) любые два поля, состоящие из одинакового конечного числа элементов, изоморфны.
- (7) Расширение полей $K|k$ конечно, если K конечномерно как k -векторное пространство. Размерность K как k -векторного пространства называется степенью расширения и обозначается $[K : k]$.

Композитом набора подполей называется минимальное их содержащее подполе, или эквивалентно, пересечение всех их содержащих подполей.

Докажите, что а) композит конечных подрасширений $K_1|k, K_2|k, \dots, K_{n-1}|k, K_n|k$ любого расширения полей $L|k$ конечен, б) $[K_n : K_1] = [K_n : K_{n-1}] \cdots [K_2 : K_1]$, если $K_n \supseteq K_{n-1} \supseteq \cdots \supseteq K_2 \supseteq K_1$ – башня полей.

- (8) Расширение полей $K|k$ алгебраично, если любой элемент поля K является корнем некоторого ненулевого многочлена над k . Докажите, что (а) расширение полей является алгебраическим тогда и только тогда, когда оно является объединением конечных подрасширений, (б) если расширение полей $K|k$ алгебраично, то любой эндоморфизм поля K тождественный на k обратим, т.е. является автоморфизмом, (в) если расширение полей $K|k$ конечно, то автоморфизмы из пункта (б) образуют конечную группу.
- (9) Пусть K – поле расщепления многочлена P и S – множество корней многочлена P в поле K .

(а) Проверьте, что поле K порождено над k множеством S , т.е. минимальное подполе в K , содержащее k и S , совпадает с K .

Назовём группой Галуа многочлена P (и обозначим через $G_{P/k}$) множество таких перестановок множества S , которые сохраняют полиномиальные соотношения над k между элементами S .

(б) Объясните, что $G_{P/k}$ совпадает с множеством эндоморфизмов поля K тождественных на подполе k .

(в) Докажите, что $G_{P/k}$ – группа автоморфизмов поля расщепления многочлена P тождественных на k .

- (г) Проверьте, что $G_{P/k}$ транзитивно действует на S , если P неприводим.
- (10) Найдите группу Галуа произвольного квадратичного многочлена ax^2+bx+c , возможно приводимого.
- (11) (а) Какой может быть группа Галуа кубического многочлена, возможно приводимого?
 (б) Проверьте, что $\sqrt[3]{a+\sqrt{b}}+\sqrt[3]{a-\sqrt{b}}$ – решение уравнения $X^3=(3\sqrt[3]{a^2-b})X+2a$. Сведите произвольное кубическое уравнение к «приведённому» виду $x^3+px+q=0$. Пусть x_1, x_2, x_3 – корни приведённого уравнения. Положим $\delta=-4p^3-27q^2$, $\zeta=-\frac{1}{2}-\frac{1}{2}\sqrt{-3}$, $y_1=x_1+\zeta^2x_2+\zeta x_3$, $y_2=x_1+\zeta x_2+\zeta^2x_3$. Тогда (формулы Кардано) $y_1=\sqrt[3]{-\frac{27}{2}q+\frac{3}{2}\sqrt{-3\delta}}$, $y_2=\sqrt[3]{-\frac{27}{2}q-\frac{3}{2}\sqrt{-3\delta}}$ для подходящих кубических корней из единицы. Поскольку уравнение приведено, $x_1+x_2+x_3=0$. Поэтому вычисление его корней x_i сводится к решению системы трёх линейных уравнений $x_1+x_2+x_3=0$, $x_1+\zeta^2x_2+\zeta x_3=y_1$, $x_1+\zeta x_2+\zeta^2x_3=y_2$.
- (12) Пусть k – поле. Докажите, что группа Галуа многочлена $x^n-s_1x^{n-1}+s_2x^{n-2}-\dots+(-1)^{n-1}s_{n-1}x+(-1)^ns_n$ над полем рациональных функций $k(s_1,\dots,s_n)$ изоморфна группе перестановок n элементов. (Указание: элементы $s_1,\dots,s_n$ можно считать элементарными симметрическими многочленами от корней.)
- (13) Опишите и «классифицируйте» все расширения поля степени 2. (Обратите внимание на случай характеристики 2.)
- (14) Пусть P – многочлен над полем k степени n с корнями $\alpha_1,\dots,\alpha_n$ в некотором поле расщепления, т.е. $P(x)=c\prod_{i=1}^n(x-\alpha_i)$. Положим $\Delta=\prod_{i<j}(\alpha_i-\alpha_j)$ и определим дискриминант $D(P)=\Delta^2=\prod_{i<j}(\alpha_i-\alpha_j)^2$.
 Вычислите дискриминанты многочленов x^n-a , $(x-a)Q(x)$, x^3+px+q , $x^n+\dots+x+1$. Докажите, что (а) $D(P)$ лежит в k ,
 (б) автоморфизм $\sigma\in G_{P/k}$ является чётной перестановкой корней тогда и только тогда, когда $\sigma(\Delta)=\Delta$ (и σ нечётна тогда и только тогда, когда $\sigma(\Delta)=-\Delta$),
 (в) если характеристика поля k отлична от 2, то $G_{P/k}$ состоит только из чётных перестановок тогда и только тогда, когда $D(P)$ является квадратом элемента поля k .
- (15) Если многочлен P над $\mathbb{Q}$ простой степени p неприводим и имеет ровно 2 мнимых комплексных корня, то его группа Галуа – полная симметрическая группа $\mathfrak{S}_p$ перестановок множества из p элементов. (Указание. Докажите, что
 (а) степень неприводимого многочлена делит порядок его группы Галуа,
 (б) группа Галуа неприводимого многочлена содержит элементы, порядки которых являются простыми (и даже примарными) делителями его степени,
 (в) группа всех перестановок конечного множества простого порядка порождена двумя перестановками: любой циклической перестановкой всех элементов и транспозицией любой пары элементов.
- (16) Найдите группы Галуа многочленов x^n-2 , x^n-1 , x^3-3x+1 , x^5-10x^4+2 , x^3+3x^2-2x+1 над $\mathbb{Q}$, над произвольным полем характеристики 0.
- (17) Выясните, какой может быть группа Галуа многочлена x^n-a над некоторым полем. В частности, в каких случаях эта группа Галуа является циклической.
- (18) Докажите, что если корень неприводимого многочлена над некоторым полем выражается в радикалах, то группа Галуа многочлена разрешима. Верно ли обратное?