1. Поле расщепления многочлена и вычисление групп Галуа

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

(1) Докажите, что многочлен P имеет корень в некотором расширении поля k.

(2) Предположим, что многочлен P неприводим. Докажите, что а) среди расширений L, в которых есть корни многочлена P, есть минимальные;[1] б) все такие минимальные расширения L изоморфны над k.

(3) Докажите, что над некоторым расширением поля k многочлен P разлагается на линейные множители.

(4) 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.

(5) Пусть K – поле расщепления многочлена P и S – множество корней многочлена P в поле 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.

Проверьте, что (а) поле K порождено над k множеством S, (б) $G_{P/k} = G_{K|k}$. В частности, $G_{P/k}$ – группа.

(6) Постройте естественное взаимно однозначное соответствие между орбитами группы $G_{P/k}$ на множестве S и неприводимыми над k множителями многочлена P. В частности, (а) $G_{P/k} \subseteq \mathfrak{S}_S$, где $\mathfrak{S}_S$ обозначает симметрическую группу, (б) $G_{P/k}$ транзитивно действует на S, если P неприводим.

(7) Пусть A – коммутативное кольцо. Многочлен Шёнеманна–Эйзенштейна над A – это многочлен со старшим коэффициентом 1 и всеми остальными коэффициентами в некотором простом идеале $\wp \subset A$, свободный член которого не лежит в $\wp^2$. Докажите неприводимость многочленов Шёнеманна–Эйзенштейна.

(8) Пусть A – коммутативная область целостности, $P(x) \in A[x]$ неприводим над A. Тогда $P(x)$ неприводим над полем частных кольца A.

(9) Пусть $\varphi : A \to B$ – гомоморфизм коммутативных колец, $P(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$ и $\sum_{i=0}^{n} \varphi(a_i) x^i \in B[x]$ неприводим над B. Тогда $P(x)$ неприводим над A.

(10) Выясните, в каких случаях поле расщепления многочлена $x^n - a$ над $\mathbb{Q}$ является циклическим.

(11) Если многочлен P над $\mathbb{Q}$ простой степени p неприводим и имеет ровно 2 мнимых комплексных корня, то его группа Галуа – полная симметрическая группа $\mathfrak{S}_p$. (Указание. Докажите, что (а) степень неприводимого сепарабельного многочлена делит порядок его группы Галуа, (б) группа Галуа неприводимого сепарабельного многочлена содержит элементы, порядки которых являются простыми (и даже примарными) делителями его степени, (в) группа всех перестановок конечного множества порождена двумя перестановками: любой циклической перестановкой всех элементов и инверсией любой пары элементов.)

(12) Какой может быть группа Галуа кубического многочлена, возможно приводимого?

(13) Найдите группы Галуа полей расщепления 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.

(14) Пусть P – многочлен над полем k степени n с корнями $\alpha_1, \ldots, \alpha_n$ в некотором поле расщепления, т.е. $P(x) = \prod_{i=1}^{n}(x - \alpha_i)$. 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 $x^n - a$, $(x-a)Q(x)$ и $x^n + \cdots + x + 1$. (Ответы: $-(-1)^{(n+1)n/2} n^n a^{n-1}$, $D(P) = Q(a)^2 D(Q)$, ...)

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

[1] т.е. такие расширения $K|k$, что многочлен P не имеет корней ни над одним из расширений поля k в K, отличном от K.

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) Докажите, что корень неприводимого многочлена над полем достаточно большой ($>$ степени многочлена) или нулевой характеристики выразим в радикалах тогда и только тогда, когда группа Галуа многочлена разрешима.

(16) Пусть k – поле. Докажите, что группа Галуа многочлена $x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^{n-1} s_{n-1} x + (-1)^n s_n$ над полем рациональных функций $k(s_1, \ldots, s_n)$ изоморфна группе перестановок n элементов. (Указание: элементы $s_1, \ldots, s_n$ можно считать элементарными симметрическими многочленами от корней.)

(17) Докажите, что (а) любая группа точно действует на некотором поле, (б) любая конечная группа является группой Галуа некоторого расширения Галуа.

(18) Докажите, что группа Галуа неприводимого многочлена является группой Галуа его поля расщепления.