ГЛАВА

ТЕОРИЯ ГАЛУА И ТФКП

5. Понижение степени уравнения

Можно ли выразить корни данного алгебраического уравнения степени n через его коэффициенты, используя арифметические операции, присоединения радикалов и присоединения решений алгебраических уравнений степени меньше чем n?

В этом параграфе мы приведем достаточное условие для положительного ответа на этот вопрос.

Определение. Скажем, что *нормальный делитель H* в группе G *имеет глубину, не превосходящую k*, если в группе G существует подгруппа G_0 индекса не превосходящего k такая, что нормальный делитель H является пересечением всех подгрупп, сопряженных с подгруппой G_0. Будем говорить, что *группа G имеет глубину, не превосходящую k*, если единичный элемент этой группы является ее нормальным делителем глубины, не превосходящей k.

Утверждение. *Пусть на поле P характеристики нуль действует конечная группа автоморфизмов G с полем инвариантов P_0. Пусть глубина группы G не превосходит k. Тогда поле P можно получить из поля P_0 присоединением всех корней некоторого алгебраического уравнения степени не превосходящей k с коэффициентами из поля P_0.*

Доказательство. Пусть G_0 — подгруппа группы G индекса m, не превосходящего k такая, что пересечение всех подгрупп, сопряженных с G_0 содержит лишь единичный элемент группы G. Согласно утверждению 3 пункта ???(0 деиствии группы) в поле P существует элемент x, обладающий следующим свойством: $g(x) = x$, если и только если $g \in G_0$. Орбиты элемента x относительно действия группы G содержат ровно m точек, поскольку индекс стационарной подгруппы элемента x равен m. Обозначим через $x_1, \dots, x_m$ точки орбиты элемента x. Основные симметрические функции от этих точек

$$\begin{aligned} \sigma_1 &= x_1 + \cdots + x_m, \\ &\vdots \\ \sigma_m &= x_1 \dots x_m \end{aligned}$$

остаются неподвижными при действии группы G и, следовательно принадлежат полю инвариантов. Точки орбиты удовлетворяют алгебраич-

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

ескому уравнению степени m

$$x^m - \sigma_1 x^{m-1} + \cdots + (-1)^m \sigma_m = 0$$

с коэффициентами из поля инвариантов P_0. Линейное пространство L над полем рациональных чисел, натянутое на точки орбиты, инвариантно при действии группы G, причем неединичный элемент группы G задает отлочное от тождественного линейное преобразование пространства L (потому что пересечение подгрупп, сопряженных с группой G_0, совпадает с единичным элементом группы G). Согласно утверждению 1 из пункта ?? в пространстве L существует элемент y, стационарная подгруппа которого тривиальна. Согласно утверждения ?? элемент y порождает поле P над полем P_0.

Теорема. *Пусть на поле P характеристики нуль действует конечная группа автоморфизмов G. Пусть группа G обладает цепочкой подгрупп*

$$G = H_0 \supset H_1 \supset \cdots \supset H_n = e$$

такой, что

1) *для каждого i, $0 < i \leq n$, подгруппа H_i является нормальным делителем подгруппы H_{i-1};*
2) *для каждого i, $0 < i \leq n$, либо глубина нормального делителы H_i в группе H_{i-1} не превосходит k, либо факторгруппа H_{i-1}/H_i коммутативна;*
3) *подгруппа H_0 совпадает с группой G, а подгруппа H_n совпадает с единичным элементом e группы G.*

Тогда поле P получается из поля P_0 при помощи присоединений радикалов и корней уравнений степени не выше k.

Доказательство. Индукция по длине n цепочки подгрупп в группе G. Группа G имеет нормальный делитель H_1, а группа H_1 обладает тем же свойством, что и группа G, но с цепочкой подгрупп

$$H_1 = H_1 \supset H_2 \supset \cdots \supset H_n = e$$

длины $n-1$. Обозначим через P_1 поле инвариантов группы H_1. Согласно индукционному предположению поле P получается из поля P_1 при помощи присоединений радикалов и корней уравнений степени не выше k. Факторгруппа G/H_1 действует на поле P_1 с полем инвариантов P_0. Если факторгруппа G/H_1 коммутативна, то поле P_1 получается из поля P_0 при помощи присоединеня радикалов (см. утверждение ?). Если факторгруппа G/H_1 имеет глубину, не превосходящую k, то поле P_1 получается из поля P присоедимемием всех корней алгебраического уравнения степени не выше k (см. утверждение выше).