ГЛАВА

ТЕОРИЯ ГАЛУА И ТФКП

7. Уравнения Галуа

Пусть K — поле характеристики нуль. Рассмотрим кольцо $K[x_1,\dots,x_n]$ полиномов от переменных $x_1,\dots,x_n$ с коэффициентами из поля K. На этом кольце действует симметрическая группа $S(n)$ при помощи перестановок переменных $x_1,\dots,x_n$. Кольцо инвариантов $K_S[x_1,\dots,x_n]$ относительно этого действия состоит из симметричных многочленов. Пусть $\alpha(x_1,\dots,x_n)$ — полином от n переменных. Рассмотрим $n!$ полиномов, получающихся из полинома α действием группы $S(n)$ и обозначим через W_α определитель Вандермонда, составленный из полученных $n!$ полиномов. Определитель Вандермонда W_α является полиномом от $x_1,\dots,x_n$, который не обращается в тождественный нуль, если и только если все $n!$ полиномов, полученных перестановками с полиномами α, являются различными. Полином W_α^2 является симметричным полиномом от переменных $x_1,\dots,x_n$

Теорема. *Если $n!$ полиномов, полученных всевозможными перестановками переменных из полинома $\alpha(x_1,\dots,x_n)$ различаются между собой, то для всякого полинома $Q\in K[x_1,\dots,x_n]$ существует полином $a_0+a_1\alpha+\dots+a_k\alpha^k$ степени $k<n!$ от полинома α, коэффициенты a_i — симметричные полиномы от $x_1,\dots,x_n$ такой, что выполняется тождество*

$$QW_\alpha^2\equiv a_0+a_1\alpha+\dots+a_k\alpha^k.$$

Доказательство. Доказательство получается применением теоремы 2 из параграфа 2.2 к действию симметрической группы $S(n)$ на кольце многочленов $K[x_1,\dots,x_n]$ с кольцом инвариантов $K_S[x_1,\dots,x_n]$ и элементом $z=Q$ и $y=\alpha$.

Пусть теперь P — поле, полученное присоединением к полю K всех корней $x_1^0,\dots,x_n^0$ алгебраического уравнения $b_0+b_1x+\dots+b_nx^n=0$ с коэффициентами из поля K, $b_i\in K$. Рассмотрим отображение $\pi\colon K[x_1,\dots,x_n]\to P$, сопоставляющее каждому полиному его значение в точке $x_1^0,\dots,x_n^0$.

Следствие. Пусть $\alpha\in K[x_1,\dots,x_n]$ — такой полином, что все $n!$ полиномов, полученные из α всевозможными перестановками переменных, принимают различные значения в точке $x_1^0,\dots,x_n^0$. Тогда элемент $\alpha(x_1^0,\dots,x_n^0)$ порождает поле P над полем K.

Доказательство. Действительно, по условию корни $x_1^0,\dots,x_n^0$ порождают поле P над полем K, поэтому каждый элемент поля P является частным

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

значений двух полиномов из кольца $K[x_1,\dots,x_n]$ в точке $x_1^0,\dots,x_n^0$. Но согласно теореме каждый полином после умножения на W_α^2 представляется в виде полинома от α с симметричными коэффициентами. Подставим в соответствующее тождество точку $x_1^0,\dots,x_n^0$. По условию функция $W^2\alpha$ в этой точке отлична от нуля, а значение симметричных полиномов в этой точке принадлежат полю K (т.к. симметрические полиномы от корней уравнения выражаются через его коэффициенты).

Лемма. *Пусть $x_1^0,\dots,x_n^0$ — попарно различные элементы поля P характеристики нуль. Тогда существует линейный многочлен $\alpha=\lambda_1x_1+\dots+\lambda_nx_n$ с рациональными коэффициентами $\lambda_1,\dots,\lambda_n$ такой, что все $n!$ многочленов, полученных из многочлена α перестановками переменных, принимают различные значения в точке $x_1^0,\dots,x_n^0$.*

Доказательство. Пространство линейных полиномов с рациональными коэффициентами является n-мерным векторным пространством над полем рациональных чисел. Рассмотрим $n!$ точек, полученных из точки $x_1^0,\dots,x_n^0$ всевозможными перестановками координат. По условию все $n!$ точек различаются. Значение линейного полинома на фиксированной точке является линейным отображением пространства полиномов с рациональными коэффициентами в поле P. Для различных точек эти линейные отображения различаются. Для каждой пары точек рассморим собственное подпространство в пространстве линейных многочленов, на котором два линейных отображения, соответствующих этим точках, совпадают. Получаем конечное множество собственных подпространств. Согласно лемме 2 из пункта 4 объединение конечного множества подпространств не может совпадать со всем пространством. Любой линейный полином α, не лежащий в объединении описанных собственных подпространств, удовлетворяет условиям леммы.

Алгебраическое уравнение $a_0+a_1x+\dots+a_nx^n=0$ над полем K называется уравнением Галуа, если любой корень этого уравнения выражается через любой другой корень этого уравнения при помощи арифметических операций и элементов поля K. Точнее.

Определение. Уравнение

$$(*)\qquad a_0+a_1x+\dots+a_nx^n=0$$

называется *уравнением Галуа*, если его корни $x_1^0,\dots,x_n^0$ обладают следующим свойством: для любой пары корней x_i^0,x_j^0 найдется многочлен $b_0+b_1x+\dots+b_{n-1}x^{n-1}$, коэффициенты b_i которого лежат в поле K, а его значение в точке x_i^0 равно x_j^0.

Теорема. *Пусть поле P получается из поля K при помощи присоединения всех корней полиномиального уравнения. Тогда то же самое поле P можно получить из поля K, присоединяя корень неприводимого уравнения Галуа.*

Доказательство. Прежде всего можно считать, что все корни исходного уравнения некратны. Действительно, если это не так, то исходное уравнение $Q=0$ можно заменить новым уравнением $L=0$, которое имеет те же корни, но с кратностью единица. Для этого нужно полином Q поделить на наибольший общий делитель полинома Q и его дискриминанта. Итак,

пусть все корни $x_1^0, \ldots, x_n^0$ различны. Рассмотрим линейную комбинатсию α этих корней такую, что все $n!$ линейных полиномов, полученных из полинома α перестановкой переменных, принимают в точке $x_1^0, \ldots, x_n^0$ различные значения. Рассмотрим теперь полином степени $n!$, корнями которого являются эти значения. Согласно доказанному выше следствию, полученное уравнение является уравнением Галуа, а его корни порождают поле P. Полученное уравнение Галуа могло оказаться приводимым. Приравнивая к нулю любой из неприводимых сомножителей, получим искомое неприводимое уравнение.

Перейдем теперь к группам Галуа — центральному объекту теории Галуа. Пусть поле P получается из поля K присоединением всех корней неприводимого уравнения

$$(**) \qquad a_0 + a_1 x + \cdots + a_n x^n = 0.$$

В этом случае можно определить группу Галуа поля P над полем K.

Определение. *Группой Галуа* поля P над полем K называется группа всех автоморфизмов поля K, сохраняющих на месте все элементы поля K.

Каждый элемент σ из группы Галуа поля P над полем K переставляет корни уравнения $**$. Действительно, применяя автоморфизм σ к равенству $**$, получаем

$$\sigma(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1\sigma(x) + \cdots + a_n(\sigma(x))^n = 0.$$

Таким образом, группа Галуа поля P над K имеет предствление в группе перестановок корней уравнения $**$. Эти представление точное. (Действительно, если автоморфизм оставляет неподвижными все корни уравнения $**$, то он сохраняет на месте все элементы поля P и является тривиальным.)

Соотношением, определенным над полем K, между корнями уравнения $**$ называется любой полином Q, принадлежащий кольцу $K[x_1, \ldots, x_n]$, который обращается в нуль в точке $x_1^0, \ldots, x_n^0$, где $x_1^0, \ldots, x_n^0$ — набор корней уравнения $**$..

Утверждение. *Всякий автоморфизм из группы Галуа сохраняет все соотношения над полем K между корнями уравнения $**$. Обратно, всякая перестановка корней, сохраняющая все соотношения между корнями, определенные над полем K, продолжаются до автоморфизма из группы Галуа. Таким образом, группу Галуа поля P над полем K можно отождествить с группой всех перестановок корней уравнения $**$, сохранясющих все соотношения между корнями, определенные над полем K.*

Доказательство. Действительно, если перестановка $\sigma \in S(n)$ соответствует элементу группы Галуа, то полином σQ, полученный из соотношения Q перестановкой σ переменных $x_1, \ldots, x_n$, тоже обращается в нуль в точке $x_1^0, \ldots, x_n^0$. Обратно, пусть перестановка σ сохраняет все соотношения между корнями, определенные над полем K. Продолжим перестановку σ до автоморфизма поля P над полем K. Всякий элемент поля P является значением некоторого полинома Q_1, принадлежащего кольцу $K[x_1, \ldots, x_n]$

в точке $x_1^0, \ldots, x_n^0$. Значение автоморфизма σ на этом элементе естественно определить как значение полинома σQ_1, полученного из полинома Q перестановкой переменных σ, в точке $x_1^0, \ldots, x_n^0$. Нужно проверить, что это определение корректно. Пусть Q_2 — другой полином из кольца $K[x_1, \ldots, x_n]$, значение которого в точке $x_1^0, \ldots, x_n^0$ совпадает со значением в этой точке полинома Q_1. Но тогда полином $Q_1 - Q_2$ является соотношением над полем K между корнями. Поэтому полином $\sigma Q_1 - \sigma Q_2$ тоже должен обратиться в нуль в точке $x_1^0, \ldots, x_n^0$, но это и означает, что автоморфизм σ определен корректно.

Нашей ближайшей целью сейчас является доказательство следующего факта. Если элемент поля P остается неподвижным при всех автоморфизмах группы Галуа поля P над полем K, то он лежит в поле K. Для доказатаьства этого факта кроме приведенной выше теоремы об уравнениях Галуа нам понадобится несложная конструкция из теории полей, к которой мы и переходим.

Пусть $Q = b_0 + b_1 x + \cdots + b_n$ — неприводимый многочлен над полем K. Тогда все поля, порожденные над полем K одним корнем уравнения Q, изоморфны между собой и допускают следующее абстрактное описание: каждое такое поле изоморфно фактору кольца $K[x]$ по простому идеалу I_Q, порожденному неприводимым многочленом Q. Обозначим это поле через $K[x]/I_Q$. Пусть теперь M — расширение поля K, содерщее все n корней $x_1^0, \ldots, x_n^0$ уравнения $Q(x) = 0$. С каждым корнем x_i^0 свяжем поле K_i, являющееся расширением поля K при помощи корня x_i^0. Все поля K_i, $i = 1 \ldots, n$, изоморфны между собой и изоморфны полю $K[x]/I_Q$. Обозначим через σ_i изоморфное отображение поля $K[x]/I_Q$ в поле K_i, оставляющее на месте элементы поля коэффициентов K и переводящее многочлен x в элемент x_i^0.

Лемма. *Образы $\sigma_i(a)$ элемента a поля $K[x]/I_Q$ в поле M при всех изоморфизмах σ_i, $i = 1, \ldots, n$, совпадают между собой, если и только если элемент a лежит в поле коэффициентов K.*

Доказательство. Действительно, если $b = \sigma_1(a) = \cdots = \sigma_n(a)$, то $b = (\sigma_1(a) + \cdots + \sigma_n(a))/n$. Поэтому элемент b является значением симметрического многочлена от корней $x_1^0, \ldots, x_n^0$ уравнения $Q(x) = 0$, т.е. элемент b принадлежит полю коэффициентов K.

Теперь все готово для доказательства теоремы.

Теорема. *Пусть поле P получено из поля K присоединением всех корней алгебраического уравнения. Тогда элемент поля P неподвижен при всех автоморфизмах группы Галуа поля P над полем K, если и только если элемент содержится в поле K.*

Доказательство. Согласно доказанной выше теореме, можно считать, что поле P получено из поля K присоединением всех корней (или, что то же самое, одного корня) неприводимого уравнения Галуа. По ределению уравнения Галуа, все поля K_i, о которых идет речь в доказанной выше лемме, совпадают между собой и совпадают с полм P. В этом случае изоморфизм $\sigma_j \sigma_i^{-1}$ поля K_i в поле K_j является автоморфизмом поля P над

полем K. Согласно лемме элемент b поля P неподвижен при всех таких автоморфизмах, если и только если он лежит в K.