УДК 519.115.1

01.00.00 Физико-математические науки

ГЕНЕРИРУЮЩИЕ МНОГОЧЛЕНЫ

Сергеев Александр Эдуардович
к. ф.-м. н., доцент
Кубанский государственный аграрный Университет, Краснодар, Россия

Понятие генерирующего многочлена появилось в конце прошлого века в работах Сальтмана и связано с обратной задачей теории Галуа, которая ещё далека от своего полного решения. Пусть G – конечная группа и K – поле, многочлен $f(x,t_1, \dots , t_n)$ с коэффициентами из поля K является генерирующим для группы G, если группа Галуа этого многочлена над полем $K(t_1, \dots , t_n)$ изоморфна G и если для любого расширения Галуа L/K с группой Галуа изоморфной G, существуют такие значения параметров $t_i = a_i$, i = 1,2, … , n, что поле L – поле расщепления многочлена $f(x,a_1, \dots , a_n)$ над K. Генерирующие многочлены над данным полем K и данной конечной группы G не всегда существуют, а если существуют, то строить их не просто. Например, для циклической группы восьмого порядка C_8 над полем рациональных чисел Q не существует генерирующего многочлена, хотя найдены конкретные многочлены с рациональными коэффициентами, имеющие группу Галуа изоморфную С. Поэтому представляет интерес построение генерирующих многочленов для группы G в случае, если G – прямое произведение группы меньших порядков. В данной работе показывается как решать эту задачу в случае, когда G – прямое произведение определенных циклических групп, находится вид соответствующих генерирующих многочленов. Кроме того, приводятся конструкции и над полями характеристики 0 и над полями характеристики 2

Ключевые слова: ГЕНЕРИРУЮЩИЙ МНОГОЧЛЕН, ПРЯМОЕ ПРОИЗВЕДЕНИЕ ГРУПП, ХАРАКТЕРИСТИКА ПОЛЯ

UDC 519.115.1

Physical-Mathematical sciences

GENERIC POLYNOMIALS

Sergeev Alexandr Eduardovich
Cand. Phys.-Math. Sci., associate Professor
Kuban State Agrarian University, Krasnodar, Russia

The concept of generic polynomial appeared in Saltman's works at the end of the last century and it is connected with the inverse problem of Galois theory, which is still far from its complete solution. Let G be a finite group and K be a field, the polynomial $f(x,t_1, \dots , t_n)$ with coefficients from the field K is generic for the group G, if Galois group of this polynomial over the field $K(t_1, \dots , t_n)$ is isomorphic G and if for any Galois extension L/K with Galois group isomorphic G there are such values of parameters $t_i = a_i$, i = 1,2, … , n, that the field L is the splitting field of the polynomial $f(x,a_1, \dots , a_n)$ over K. Generic polynomials over a given field K and a given finite group G do not always exist, and if they exist then it's not easy to construct them. For example, for a cyclic group of the eight order C_8 there is no generic polynomial over the field of rational numbers Q, although there are found specific polynomials with rational coefficients having Galois group isomorphic C_8. Therefore, this is of interest to construct generic polynomials for the group G in cases when G is a direct product of groups of lower orders. In this study we show to solve this problem in case when G is a direct product of certain cyclic groups and there is a type of corresponding generic polynomials. Moreover, we give constructions over the fields of characteristic 0 and over the fields of characteristic 2

Keywords: GENERIC POLYNOMIALS, DIRECT PRODUCT OF GROUPS, PROPERTIES OF THE FIELD

Doi: 10.21515/1990-4665-131-044

Генерирующие многочлены

Существует немного методов нахождения генерирующих полиномов. Наиболее известный из них – метод Kemper'a [2], использующий теорию инвариантов и минимальный базис. Помимо этого метода существует также метод Rikuna (он применил метод Kemper'a к случаю ,когда основное поле содержит примитивный корень n-ой степени из единицы) [7,8,9], метод Lacacheux [3], использующий теорию эллиптических кривых, метод Ledet'a [4,5,6], использующий свойства G-расширений. Интересно,что в [7] Rikuna получил генерирующие полиномы четных степеней над полями,содержащими первообразные корни из единицы,а Smith в [11], использовав резольвенты Лагранжа,получил генерирующие полиномы нечетных степеней над полями,содержащими первообразные корни из единицы.

Заметим,что приведенные выше методы не работают в характеристике 2.

Мы же приведем свой метод нахождения генерирующих полиномов, который позволит строить генерирующие полиномы для целого класса групп над любым полем.

Дади м вначале определение генерирующего полинома,согласно Kemper [2]:

Определение 1.(G.Kemper) Пусть К – поле и G – конечная группа. Назовем нормированный сепарабельный полином $g(t_1, \dots, t_m, X) \in K(t_1, \dots, t_m)[X]$ *генерирующим для группы G над* K, *если выполняются следующие два свойства:*

(1) *Группа Галуа полинома* g (*как полинома от* X *над* K $(t_1, \dots, t_m)$) есть G.

(2) *Если* L – *бесконечное поле, содержащее* K *и* N/L – *расширение Галуа*

с группой G, тогда существуют такие $\lambda_1, \dots, \lambda_m \in L$, *что N является полем расщипления полинома* $g(\lambda_1, \dots, \lambda_m, X)$ *над L.*

Докажем далее следующую основную теорему,благодаря которой мы построим генерирующие полиномы с группой Галуа изоморфной V_4, C_6 и C_{12} над полями Q и $Z_2(t)$.

Теорема 1. Пусть над произвольным полем K существует G_1 - генерирующий полином $f_1(X, t_1, \dots, t_s) \in K[t_1, \dots, t_s][X]$ и G_2- генерирующий полином $f_2(X, u_1, \dots, u_r) \in K[u_1, \dots, u_r][X]$. Тогда над полем K существует и $G_1 \times G_2$- генерирующий полином.

Доказательство. Рассмотрим полином g $(X, t_1, \dots, t_s, u_1, \dots, u_r) = f_1 f_2$. Этот полином является $G_1 \times G_2$ генерирующим. Действительно,пусть E – поле для расщепления этого полинома над K $(X, t_1, \dots, t_s, u_1, \dots, u_r)$ = M, а E_1 и E_2 – поля расщеплений соответственно полиномов f_1 и f_2 над полем M. Так как $t_1, \dots, t_s, u_1, \dots, u_r$ – алгебраически независимы, то поля E_1 и E_2 – линейно разделены над M и поэтому E = $E_1 \vee E_2$, $E_1 \cap E_2$ = M, следовательно:

$$\mathrm{Gal}_m(g) = \mathrm{Gal}_m(f_1) \times \mathrm{Gal}_m(f_2) \cong \mathrm{Gal}_m(E_1) \times \mathrm{Gal}_m(E_2) \cong G_1 \times G_2.$$

Таким образом, 1 пункт определения генерирующего полинома выполняется (см определение 1,выше). Докажем,что и 2 пункт определения генерирующего полинома выполняется.

Пусть K $\subset$ L $\subset$ N – расширение полей, N/L – расширение Галуа с группой Галуа изоморфной $G_1 \times G_2$. Пусть далее N^{G_1}, N^{G_2} – соответствующие под поля неподвижных элементов для G_1 и G_2. Так как $G_1 \times G_2$ – прямое произведение, то тогда $N^{G_1} \cap N^{G_2}$ = L, причем Gal $(N^{G_1}/L) \cong G_2$ и Gal $(N^{G_1}/L) \cong G_1$.

Следовательно, существуют такие специализации $t_1^{(0)}, \dots, t_s^{(0)}, u_1^{(0)}, \dots, u_r^{(0)} \in$ L, что N^{G_1} – поле расщепление полинома $f_2(X, u_1^{(0)}, \dots, u_r^{(0)})$ над L, а поле N^{G_2}– поле расщепление над L полинома g при указанных специализациях.

Можно получить неприводимый генерирующий полином для группы $G_1 \times G_2$ над бесконечным полем K, исходя из G_1-генерирующего полинома f_1 и G_2- генерирующего полинома f_2 из теоремы 1.

Пусть K_1 = K($t_1, \dots, t_s$), $f_1 = f_1(X, t_1, \dots, t_s)$ – G_1- генерирующий полином над K степени n с корнями $\alpha_1, \dots, \alpha_n$) в его поле расщепления K_1. Пусть K_2 = K ($u_1, \dots, u_r$), $f_1 = f_2(X, u_1, \dots, u_r)$ – G_2-генерирующий полином над K степени m с корнями $\beta_1, \dots, \beta_n$ в его поле расщепления над K_2. Имеем:

$$\mathrm{Gal}(K_1(\alpha_1, \dots, \alpha_n)/ K_1) \cong G_1,\ \mathrm{Gal}(K_2(\beta_1, \dots, \beta_m)/ K_2) \cong G_2.$$

Пусть далее, $K_3 = K_1 \vee K_2$ = K($t_1, \dots, t_s, u_1, \dots, u_r$), тогда:

$$\mathrm{Gal}(K_3(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)/ K_3) \cong G_1 \times G_2.$$

Предположим,что $\theta_{ij} = \alpha_i + c\beta_j$,тогда можно выбрать c ϵ K так,чтобы все элементы θ_{ij} (i = 1,2, … , n; j = 1,2, … , m) были различными. Составим полином:

$$h = \prod_{i,j}(X - \theta_{ij})$$

Тогда степень degh = m·n и $K_3(\alpha_i, \beta_j)$ = K(θ_{ij}) [12].

Таким образом, поле E=$K_3(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m)$ = $K_3(\theta_{11}, \theta_{12}, \dots, \theta_{nm})$.

Коэффиценты полинома h выражаются рациональным образом через коэффициенты полиномов f_1 и f_2,следовательно, многочлен h ϵ K_3[X] = = K[$t_1, \dots, t_s, u_1, \dots, u_r$], degh = m·n, и так как выполняются следующие равенства:

$$[K_3(\alpha_1, \beta_j): K_3] = m \cdot n = [K_3(\theta_{ij}): K_3],$$

то, заключаем, что многочлен h является неприводимым над полем K_3.

Таким образом,доказана теорема:

Теорема 2. Пусть K – бесконечное поле и существует G_1 -

генерирующий полином $f_1(X, t_1, \dots, t_s)$ *над K степени m и* G_2 *- генерирующий полином* $f_2(X, u_1, \dots, u_r)$ *над K степени n. Тогда существует непроводимый над полем* K_3 = $K(t_1, \dots, t_s, u_1, \dots, u_r)$ $G_1 \times G_2$-генерирующий полином степени m·n.

Из этих двух теорем вытекает следствие:

Следствие 3. При выполнении условий теоремы 1,если порядки групп G_1 и G_2 *взаимно просты,то в качестве элемента* θ_{ij} *можновзять* $\theta_{ij} = \alpha_i + \beta_j$, *где (I = 1,2,… ,n; j=1,2,… ,m).*

Приведем новые примеры нахождения генерирующих полиномов над полями характеристики 0 и 2.

Пример 1. Если charK=2, то многочлены f(x,t) = $x^2 + tx + 1$ и g(x,u) = x^3+(u^2+u+1)x + u^2+ u +1 есть C_2 и C_3 генерирующие многочлены над полем K (см. [10]). Корнями первого полином является $\alpha_1 = \alpha$ и $\alpha_2 = \alpha + t$. Корнями второго полинома являются $\beta_1 = \beta$, $\beta_2 = \beta u + \beta^2$ и $\beta_3 = \beta(u+1) + \beta^2$.

Непосредственные вычисления дают полином:

$$h(t,u,X) = \prod_{\substack{1 \le i \le 2 \\ 1 \le j \le 3}} (X - (\alpha_i + \beta_j)) =$$

$$X^6 + tX^5 + (1+t^2)X^4 + t^3X^3 + (t^3u^3 + u^4 + tu + t^2u + tu^2 + t + u^2)X^2 + (tu^4 + t^3 + t^3u^2 + t^2 + u^2 + t^3u + tu^2 + t^2 + ut^2) + t^3u^2 + tu^4 + ut^3 + t^2u^2 + t^3 + t^2u + t^2 + tu + 1$$

По теореме этот полином является C_6 генерирующим полином над полем charK=2.

Пример 2. Если charK $\neq$ 2, то многочлены f(x,t) = $x^2 - t$ и g(x,u) = x^3 − ux^3 + (u−3)x +1 есть C_2 и C_3 генерирующие многочлены над полем K (см. [10]).

Пусть корнями первого полинома являются α_1 и α_2, а корнями второго полинома являются $\beta_1, \beta_2, \beta_3$. Найдем полином h(t,u,x) без вычисления корневых полиномов, а именно: так как $\theta_{11} = \alpha_1 + \beta_1$, то тогда $\theta_{11} - \alpha_1 = \beta_1$ – корень полинома g(u,x), находим выражени для α_1:

$$\alpha_1 = \frac{\theta_{11}^3 + 3t\theta_{11} - u\theta_{11}^2 - tu + u\theta_{11} - 3\theta_{11} + 1}{3\theta_{11}^2 + t - 2\theta_{11}u + u - 3}$$

Далее ,подставив это выражение в f(x,t),мы легко получим полином шестой степени относительно θ_{11}. Заменяя θ_{11} на x,получим полином:

h(t,u,X) =

$$X^6 - 2uX^5 + (u^2 - 3t + 2u - 6)X^4 + (6u - 2u^2 + 4tu + 2)X^3 + (3t^2 - 8u + u^2 - 2tu^2 + 9)X^2 + (2u + 6t - 6 - 2t^2u - 6tu + 2tu^2)X - 9t + 6t^2 - t^3 - 2t^2u + 1 - tu^2 + t^2u^2 + 4tu.$$

По теореме этот полином является C_6 генерирующим полиномом над полем charK $\neq$ 2.

Заметим,что специализации u = 2, t = 0; u= 2, t=2; u=5, t= 3 этого полинома приводят соответственно к полиномам:

h(0,2,X) = $X^6 - 12X^4 + 2X^3 + 21X^2 + 6X - 1$,

h(2,2,X) = $X^6 - 4X^5 - 4X^4 + 22X^3 - 7X^2 - 14X + 7$,

h(3,5,X) = $X^6 - 10X^5 + 20X^4 + 42X^3 - 129X^2 - 8X$+121,

которые,ввиду своей неприводимости,имеют группу Галуа C_6. Это также легко проверить на Maple.

Можно также найти генерирующий полином для группы $C_2 \times C_2 \cong V_4$ над полем K характеристики равной два. Алгоритм построения следующий.

Пусть $f_1(X)$ = X^2+X + t_1 – генерирующий поленом для группы C_2 над полем K с charK = 2,а $f_2(X)$ = X^2+X + t_2 – другой генерирующий полином для группы C_2 над полем K, charK = 2,причем t_1 и t_2 – трансцендентные и алгебраически независимые над K элементы. Тогда понятно,что,α – корень полинома $f_1(X)$ в соответствуещем поле расщепления над K(t_1) (другой корень при этом – (α+1)), аналогично, если β– корень поленома $f_2(X)$ в соответствующем поле расщепления над K(t_2) (другой при этом–(β+1)), и если уравнение $b^2+b+t_2+t_1=0$ не имеет корня $b \in$ K, следовательно при этих условиях, K(α, β) – расширение с группой Галуа V_4.

Рассмотрим далее поле K(t_1,t_2) – алгебраическое замыкание поля K(t_1,t_2). Будем считать,что α,β ∈ K(t_1,t_2). Пусть M = K(t_1,t_2). Очевидно,что поля M(α) и M(β) линейно разделены над M.

Расширение M(α, β) является нормальным над M и M(α, β) = M(α)∨ M(β) (композит линейно - разделенных нормальных, сепарабельных расширений над M), поэтому Gal(M(α, β)/M) ≅ V_4 = {(1), (12)(34), (13)(24), (14)(23)}. Очевидно,что группа Галуа Gal(M(α, β)/M)={e,σ,τ,στ},где:

$$e(\alpha)=\alpha, \qquad e(\beta)=\beta,$$
$$\sigma(\alpha)=\alpha+1, \qquad \sigma(\beta)=\beta,$$
$$\tau(\alpha)=\alpha, \qquad \tau(\beta)=\beta+1,$$
$$\sigma\tau(\alpha)=\alpha+1, \qquad \sigma\tau(\beta)=\beta+1.$$

Пусть θ=αβ. Т.к. сопряженные с ним элементы σ(θ)=(α+1)β, t(θ)=(β+1)α, στ(θ)= (α+1)(β+1) являются различными над M элементами, то θ –корень непроводимого над M полинома четвертой степени, имеющего своими корнями θ, σ(θ), τ(θ), στ(θ). Найдем теперь вид этого полинома.

Т.к. θ= αβ,то α= $\frac{\theta}{\beta}$, т.е. $\frac{\theta}{\beta}$ – корень полинома $f_1(X)$. Таким образом, подставив это выражение в $f_1(X)$, мы найдем, что $\beta = \frac{\theta^2+t_1 t_2}{\theta+t_1}$. Подставив это выражение для β в $f_2(X)$ (β —корень этого поленома),мы получим уравнение четвертой степени,которому удовлетворяет элемент θ. Заменяя теперь θ на X, мы получим полином:

$$f(X)= X^4 + X^3 + X^2(t_1 + t_2) + Xt_1t_2 + t_1^2t_2^2.$$

Предложение 4. Полином f(X) является генерирующим полиномом над бесконечным полем K характеристики 2 для группы Галуа V_4.

Доказательство. Пусть L —расширение поля K, N/L – некоторое V_4 - расширение Галуа. Пусть N_1/L и N_2/L — какие-либо его различные квадратичные подполя. Тогда N_1/L — поле расщепления над L полинома $f_1(X) = X^2$+X+t_1 при некоторой специализации $t_1 = t_1^{'} \epsilon$ L и пусть $\beta^{'}$ – один из корней полинома, полученного в результате специализации из f_1: $\overline{f_1} = X^2$+X + $t_1^{'} \epsilon$ L [x]. Аналогично N_2/L — после расщепления над L полинома f_2(X)= X^2+X +t_2 при некоторой специализации $t_2 = t_2^{'} \epsilon$ L и пусть $\beta^{'}$ – один из корней полинома, полученного в результате специализации из f_2: $\overline{f_2} = X^2$+X + $t_2^{'} \epsilon$ L [x]. Тогда N=L($\alpha^{'}, \beta^{'}$) и ясно,что при указанных специализациях $t_1 = t_1^{'} \epsilon$ L и $t_2 = t_2^{'} \epsilon$ L имеем $\theta^{'}$=$\alpha^{'} \beta$ – один из корней полинома f(X) и K($\theta^{'}$) = K($\alpha^{'}, \beta^{'}$)=N.

Заметим,что полином f(X) является непроводимым.

Аналогичным образом можно построить генерирующий полином над полем K характеристики 2 для группы $C_2 \times C_2 \times C_2$(для этого достаточно,чтобы уравнения вида b^2+b+$t_2 + t_1$=0, c^2+c+$t_2 + t_3$=0 и c^2+c+$t_1 + t_3$=0 не имели бы корней b, c, d ϵ K, а в качестве элемента θ надо взять элемент θ =αβγ и проделать далее те же самые рассуждения,что и в предложении 6). Имеем:

$$f(X)=X^8+X^7+X^6+(t_1+t_2+t_3)+X^5(t_2t_3+t_1t_2t_3)+$$
$$+X^4(t_1^2t_2+t_2^2t_1+t_1^2t_3+t_2^2t_3^2)+X^3(t_1^2t_2^2t_3^2+t_1^2t_2^2t_3+t_1^2t_2^2+t_1^2t_2t_3+t_1t_2^2t_3^2)+$$
$$+X^2(t_1^3t_2^2t_3+t_1^3t_2^2t_3^2+t_1^2t_2^3t_3^2+t_1^3t_2^3)+X(t_1^2t_2^2t_3+t_1^3t_2^3t_3^3+t_1^2t_2^2t_3^3)+$$
$$t_1^4t_2^4t_3^4.$$

*Предложение 5. Полином f(X) (*определенный выше) *является генерирующим полиномом над бесконечным полем K характеристика 2 для группы Галуа* $C_2\times C_2\times C_2$.

После этого ясно,что таким же способом можно находить генерирующий поленом над полем характеристики 2 и для группы $\underbrace{C_2\times C_2\times\ldots\times C_2}_{n}$.

Блягодаря теореме 1 автору удалось получить генерирующий полином для циклической группы 12 порядка C_{12}, однако ввиду громоздкости этого полинома мы его не проводим в этой работе.

Замечание 1. Известна теорема существования генерирующего полинома для полупрямого произведения группы $G_1\times G_2$ над бесконечным полем K, если существуют генерирующие полиномы для групп $G_1 u\, G_2$ над этим же полем K [1]. Однако доказательство этой теоремы не является конструктивной и требует дополнительной информации.

Литература

1. Jensen,C., Ledet,A., Yui, N. Generic polynomials, constructive aspects of the inverse Galois problem, Mathematical Science Research Institute Publications, Cambridge,to appear. Генерирующие полиномы,конструктивные аспекты обратной задачи Галуа,Публикации Института Научно-Математического исследования, Кэмбридж.
2. Kemper,G., Mattig, E. (2000), Generic polynomials with few parameters, Генерирующие полиномы с несколькими параметрами. J. Symb. Comp., 30, 843-857.
3. Lecacheux, O. (1998), Constructions de polynomes generique a groupe de Galois resoluble, Общие конструкции групп многочленнов Галуа. Acta Arithmetica, 86, 207-216.

4. Ledet,A. (2001) , Generic polynomials for Q_8 QC, QQ-extensions, J Algebra, 237,1-13.

5. Ledet,A. (1999), Generic polynomials for quasi-dihedral, dihedral and modular extensions of order 16, Proc.Amer.Math.Soc.,128,2213-2222.

6. Ledet,A. (2001) , Generic extensions and generic polynomials J. Symb. Comp., 30, 867-872.

7. Rikuna, Y. Explicit constructions of generic polynomials for some elementary groups, Определенные конструкции генерирующих полиномов для некоторых элементарных групп,to appear.

8. Rikuna, Y., Hashimoto, K. (2002), On generic families of cyclic polynomials with even degree, Manuscripta math., 107,no. 3, 283-288.

9. Rikuna, Y.(2002), On generic polynomials for the modular 2-groups, Proc Japan. Acad. Ser. A. Math. Sci., 78, no3, 33-35.

10. Serre, J.-P. (1992), Topics in Galois theory, Jones and Barthelett Pub., Boston.

11. Smith, G.W. Generic Cyclic Polynomials of Odd Degree, J.Comp. in Algebra,19, no 12, 3367- 3391.

12. Ван дер Варден Б.Л. (1976), Алгебра, М., Наука.

Literatura

1. Jensen,C., Ledet,A., Yui, N. Generic polynomials, constructive aspects of the inverse Galois problem, Mathematical Science Research Institute Publications, Cambridge,to appear. Generirujushhie polinomy,konstruktivnye aspekty obratnoj zadachi Galua,Publikacii Instituta Nauchno-Matematicheskogo issledovanija, Kjembridzh.

2. Kemper,G., Mattig, E. (2000), Generic polynomials with few parameters, Generirujushhie polinomy s neskol'kimi parametrami. J. Symb. Comp., 30, 843-857.

3. Lecacheux, O. (1998), Constructions de polynomes generique a groupe de Galois resoluble, Obshhie konstrukcii grupp mnogochlennov Galua. Acta Arithmetica, 86, 207-216.

4. Ledet,A. (2001) , Generic polynomials for Q_8 QC, QQ-extensions, J Algebra, 237,1-13.

5. Ledet,A. (1999), Generic polynomials for quasi-dihedral, dihedral and modular extensions of order 16, Proc.Amer.Math.Soc.,128,2213-2222.

6. Ledet,A. (2001) , Generic extensions and generic polynomials J. Symb. Comp., 30, 867-872.

7. Rikuna, Y. Explicit constructions of generic polynomials for some elementary groups, Opredelennye konstrukcii generirujushhih polinomov dlja nekotoryh jelementarnyh grupp,to appear.

8. Rikuna, Y., Hashimoto, K. (2002), On generic families of cyclic polynomials with even degree, Manuscripta math., 107,no. 3, 283-288.

9. Rikuna, Y.(2002), On generic polynomials for the modular 2-groups, Proc Japan. Acad. Ser. A. Math. Sci., 78, no3, 33-35.

10. Serre, J.-P. (1992), Topics in Galois theory, Jones and Barthelett Pub., Boston.

11. Smith, G.W. Generic Cyclic Polynomials of Odd Degree, J.Comp. in Algebra,19, no 12, 3367- 3391.

12. Van der Varden B.L. (1976), Algebra, M., Nauka.