Записки научных
семинаров ПОМИ
Том 265, 1999 г.

А. В. Яковлев

ПОГРУЖЕНИЕ ЦИКЛИЧЕСКОГО РАСШИРЕНИЯ В ЦИКЛИЧЕСКОЕ

Пусть k – поле, K – его циклическое расширение Галуа порядка m, и пусть n – натуральное число, делящееся на m. Мы говорим, что расширение K/k n-погружаемо, если существует расширение Галуа L/k с циклической группой Галуа порядка n, такое что $K \subseteq L$.

В настоящей работе изучается вопрос об условиях 2^n-погружаемости квадратичного расширения $k(\sqrt{a})/k$. Этой проблемой звнимался, в частности, К. Йенсен, который заметил, среди прочего, что при малых значениях n для 2^n-погружаемости достаточно, чтобы элемент $a \in k$ был нормой некоторого элемента из соответствующего кругового расширения (устное сообщение). Рассматриваемая задача является частным случаем задачи об условиях разрешимости задачи погружения полей с циклическим ядром четного порядка, которая была полностью решена в [1]. Однако, из полученного в [1] условия не так легко вывести простые достаточные условия 2^n-погружаемости. Используя те же идеи, что в [1], мы находим здесь необходимое и достаточное условие 2^n-погружаемости квадратичного расширения; в качестве простого следствия получается, что условие Йенсена достаточно не только для малых n, а всегда.

Теорема. *Пусть k – поле, характеристика которого отлична от 2; пусть, далее, $a \in k \setminus k^2$ и $m = 2^n$, $n \geqslant 1$. Обозначим через k_1 поле, полученное присоединением к полю k первообразного корня ζ степени m из 1.*

(a) *Если $k_1 = k$, то расширение $k(\sqrt{a})/k$ m-погружаемо.*

(b) *Если $(k_1 : k) = 2$ и $\zeta^\tau = \zeta^{-1}$ для единственного неединичного элемента τ из группы Галуа F расширения k_1/k, то расширение $k(\sqrt{a})/k$ m-погружаемо тогда и только тогда, когда существует элемент $v \in k_1$ такой, что $a = \mathrm{Nm}_{k_1/k}\, v = v^{1+\tau}$.*

Работа выполнена при финансовой поддержке РФФИ, грант 98-01-00825.

(c) *Если группа Галуа F расширения k_1/k циклическая и содержит такой элемент ρ, что $\zeta^\rho \neq \zeta^{\pm 1}$, то расширение $k(\sqrt{a})/k$ m-погружаемо тогда и только тогда, когда существуют элементы $u \in k$, $v \in k_1$, такие что $a = u^2 \mathrm{Nm}_{k_1/k}\, v$.*

(d) *Если группа Галуа расширения k_1/k не циклическая, то выберем порождающие ее элементы σ, τ так, чтобы $\zeta^\tau = \zeta^{-1}$, $\zeta^\sigma = \zeta^s$ для $s \equiv 1 (\mathrm{mod}\, 4)$. Обозначим через k_2 поле $k(\sqrt{-1})$. Далее, пусть a – такой элемент из k, что расширение $k(\sqrt{a})/k$ 4-погружаемо и потому существует элемент $b \in k_2$ такой, что $a = b^{1+\tau}$ (см. утверждение* (b) *этой теоремы). Расширение $k(\sqrt{a})/k$ m-погружаемо тогда и только тогда, когда существуют элементы $u \in k_2$, $v \in k_1$, такие что $a/b^2 = (u^{1-\tau})^2 \mathrm{Nm}_{k_1/k_2}\, v$.*

Доказательство. Утверждение (a) тривиально.

Доказательство утверждения (b).

Необходимость. Если $k(\sqrt{a})/k$ – 2^n-погружаемое расширение, то оно 4-погружаемо. Пусть $K_0 \supset k(\sqrt{a})$ – расширение Галуа поля k с циклической группой Галуа C порядка 4. Обозначим через K алгебру $K_0 \otimes_k k_1$; тогда K/k_1 циклическое расширение Галуа порядка 4 и, следовательно, $K = k_1(\beta)$ для некоторого элемента $\beta \in K$ такого, что $\beta^4 \in k_1$, $\beta^\xi = \beta i$, где ξ – какой-то порождающий элемент группы C, а $i = \sqrt{-1}$. Пусть $\alpha = \beta^{1-\tau}$; тогда $\alpha^{\xi - 1} = i^{1-\tau}$, и потому элемент $v = \alpha^{-1}\sqrt{a}$ ξ-инвариантен, т.е. $v \in k_1$. Таким образом,

$$a = (\sqrt{a})^{1+\tau} = (v\alpha)^{1+\tau} = v^{1+\tau}\beta^{(1-\tau)(1+\tau)} = v^{1+\tau} = \mathrm{Nm}_{k_1/k}\, v.$$

Достаточность. Пусть $a = \mathrm{Nm}_{k_1/k}\, v = v^{1+\tau}$, $v \in k_1$. Положим $K = k_1(\beta)$, где $\beta^m = v^{1-\tau}$. Определим действие операторов τ, $\xi \in F \times C$ на $K : \beta^\tau = \beta^{-1}$, $\beta^\xi = \beta\zeta$. Проверим, что определенные так операторы не нарушают равенство $\beta^m = v^{1-\tau}$ и удовлетворяют всем соотношениям между порождающими элементами τ, ξ группы $F \times C$:

$$(\beta^\tau)^m = (\beta^{-1})^m = (\beta^m)^{-1} = v^{\tau - 1} = (v^{1-\tau})^\tau;$$

$$(\beta^\xi)^m = (\beta\zeta)^m = \beta^m = (v^{1-\tau})^\xi;$$

$$\tau^2 = 1 : \beta^{\tau^2 - 1} = (\beta^{\tau+1})^{\tau-1} = (-1)^{\tau - 1} = 1;$$

$\xi^m = 1$ – очевидно;

$$\tau\xi = \xi\tau : \beta^{\tau\xi - \xi\tau} = (\beta^{-1})^\xi(\beta\zeta)^{-\tau} = (\beta^{-1}\zeta^{-1})(\beta^{-1}\zeta^{-1})^{-1} = 1.$$

Итак, мы доказали, что расширение $K = k_1(\beta)$ является расширением Галуа поля k с группой Галуа $G = F{\times}C$. Тогда подалгебра $K_0 = K^F$ всех F-инвариантных элементов алгебры K представляет собой циклическое расширение порядка $m = 2^n$ поля k. Пусть $\alpha = \beta^{m/2}\, v^\tau$; тогда

$$\alpha^{1-\tau} = (\beta^{m/2})^{1-\tau}\, v^{\tau-1} = \beta^m\, v^{\tau-1} = v^{1-\tau}\, v^{\tau-1} = 1,$$

$$\alpha^2 = \beta^m\, v^{2\tau} = (v^{1-\tau})v^{2\tau} = v^{1+\tau} = a.$$

Итак, $\alpha \in K_0$, и $\sqrt{a} = \pm\alpha \in K_0$.

Доказательство утверждения (d). Пусть l – порядок элемента σ группы Галуа F расширения k_1/k. Напомним, что $s \equiv 1 (\operatorname{mod} 4)$; поэтому $q = (1-s)/4$ – целое число, и легко убедиться, что $s^l \equiv 1(\operatorname{mod} 2^n)$, но $s^l \not\equiv 1(\operatorname{mod} 2^{n+1})$; следовательно, $x = (1-s^l)/2^n$ – нечетное целое число.

Определим элементы целочисленного группового кольца $\mathbb{Z}[F]$, которые будут играть важную роль в наших построениях:

$$N = 1 + \sigma + \sigma^2 + \cdots \sigma^{l-1},$$

$$\Delta = s^{l-1} + \sigma s^{l-2} + \sigma^2 s^{l-3} + \cdots + \sigma^{l-2} s + \sigma^{l-1}.$$

Лемма. $(\sigma - s)\Delta = 1 - s^l = mx$; $(\sigma - s)N = (1-s)N$; $\zeta^{2qN} = -1$.

Доказательство. Все соотношения, кроме последнего, тривиальны. Докажем последнее соотношение:

$$\zeta^{N\cdot 2q} = \zeta^{(1+\sigma+\cdots+\sigma^{l-1})\cdot 2q} = \zeta^{(1+s+\cdots+s^{l-1})(1-s)/2} =$$

$$= \zeta^{(1-s^l)/2} = (\zeta^{m/2})^x = -1,$$

потому что $\zeta^{m/2} = -1$, а x нечетно.

Необходимость. Пусть $K_0 \supset k(\sqrt{a})$ – расширение Галуа поля k с циклической группой Галуа C порядка m. Обозначим через K алгебру $K_0 \otimes_k k_1$; тогда K/k – расширение Галуа с группой Галуа $G = F{\times}C$. Обозначим через ξ какой-то порождающий элемент группы C. Группа Галуа C расширения K/k_1 – циклическая группа C порядка m, а поле k_1 содержит первообразный корень ζ степени m из 1; поэтому $K = k_1(\beta)$, где $\beta^m \in k_1$, $\beta^\xi = \beta\zeta$. Очевидно, что элементы $d = \beta^{\tau+1}$, $c = \beta^{\sigma-s}$ принадлежат полю k_1 (поскольку они ξ-инвариантны). Обозначим через γ элемент $(\beta^2/d)^{Nq} \in K$ и через v элемент $c/d^{2q} \in k_1$. Пользуясь леммой, получаем:

$$\gamma^{\xi-1} = \beta^{2(\xi-1)Nq} = \zeta^{N\cdot 2q} = -1,$$

$$\gamma^{\sigma-1} = (\beta^2/d)^{qN(\sigma-1)} = 1,$$

$$\gamma^{\tau+1} = (\beta^2/d)^{(1+\tau)Nq} = \left(\beta^{2(1+\tau)}/d^{1+\tau}\right)^{Nq} = (d^2/d^2)^{Nq} = 1,$$

$$\gamma^2 = \beta^{(1-s)N}/d^{2qN} = \beta^{(\sigma-s)N}/d^{2qN} = \left(c/d^{2q}\right)^N = \mathrm{Nm}_{k_1/k_2}\, v.$$

Пусть $\alpha = \sqrt{a}/b$; этот элемент обладает следующими свойствами:

$$\alpha^{\xi-1} = -1, \quad \alpha^{1+\tau} = (\sqrt{a})^{1+\tau}/b^{1+\tau} = a/b^{1+\tau} = 1, \quad \alpha^{\sigma-1} = 1.$$

Поэтому элемент $w = \gamma^{-1}\alpha$ является ξ-инвариантным и σ-инвариантным, т.е. $w \in k_2$ и $w^{1+\tau} = 1$; следовательно, существует элемент $u \in k_2$ такой, что $u^{1-\tau} = w = \gamma^{-1}\,\alpha$. Итак,

$$a/b^2 = \alpha^2 = \left(u^{1-\tau}\right)^2\gamma^2 = \left(u^{1-\tau}\right)^2\mathrm{Nm}_{k_1/k_2}\, v.$$

Достаточность. Пусть $u \in k_2$, $v \in k_1$ – такие элементы, что

$$a/b^2 = b^{\tau-1} = \left(u^{1-\tau}\right)^2\mathrm{Nm}_{k_1/k_2}\, v = \left(u^{1-\tau}\right)^2 v^N.$$

Тогда $v^{(1+\tau)N} = 1$; поэтому существует элемент $d \in k_1$ такой, что $v^{1+\tau} = d^{\sigma-1}$, $d^\tau = d$. Пусть $c = vd^{(1-s)/2}$. Элементы c, d, очевидно, удовлетворяют соотношениям $c^{1+\tau} = d^{\sigma-s}$, $d^\tau = d$.

Обозначим через G прямое произведение группы F и циклической группы C порядка m; пусть ξ – порождающий элемент группы C. Мы построим теперь явно расширение K/k_1, которое является расширением Галуа поля k с группой Галуа G. Именно, положим $K = k_1(\beta)$, где $\beta^m = c^\Delta$ и порождающие элементы σ, τ, ξ группы G действуют на β по следующим формулам:

$$\beta^\xi = \beta\zeta, \quad \beta^\sigma = \beta^s\, c^x, \quad \beta^\tau = \beta^{-1}\, d^x$$

(ξ действует на k_1 тривиально). Заметим, что K – не обязательно поле, а только алгебра. Проверим, что так определенные операторы на K не нарушают равенство $\beta^m = c^\Delta$ и что они удовлетворяют всем соотношениям между элементами σ, τ, ξ группы G.

$$(\beta^\tau)^m = \beta^{-m} d^{xm} = c^{-\Delta} d^{(\sigma-s)\Delta} = c^{-\Delta} c^{(\tau+1)\Delta} = \left(c^\Delta\right)^\tau.$$

$$(\beta^\sigma)^m = (\beta^s c^x)^m = (\beta^m)^s c^{xm} = c^{\Delta s} c^{(\sigma-s)\Delta} = c^{\Delta\sigma}.$$

$(\beta^\xi)^m = (\beta\zeta)^m = \beta^m = c^\Delta = \left(c^\Delta\right)^\xi.$

$\tau^2 = 1 : \beta^{\tau^2-1} = \left(\beta^{\tau+1}\right)^{\tau-1} = (d^x)^{\tau-1} = 1.$

$\sigma^l = 1 : \beta^{\sigma^l-1} = \beta^{\sigma^l-s^l}\,\beta^{s^l-1} = \beta^{(\sigma-s)\Delta}\beta^{-mx} = c^{x\Delta}c^{-\Delta x} = 1.$

$\xi^m = 1$ – очевидно.

$\tau\sigma = \sigma\tau : \beta^{\sigma\tau-\tau\sigma} = (\beta^s c^x)^\tau(\beta^{-1}d^x)^{-\sigma} = \left(\beta^{-s}d^{sx}c^{x\tau}\right)\left(\beta^s c^x d^{-\sigma x}\right) =$
$\left(c^{1+\tau}/d^{\sigma-s}\right)^x = 1.$

$\tau\xi = \xi\tau : \beta^{\tau\xi-\xi\tau} = (\beta^{-1}d^x)^\xi(\beta\zeta)^{-\tau} = (\beta^{-1}d^x\zeta^{-1})(\beta^{-1}d^x\zeta^{-1})^{-1} = 1.$

$\sigma\xi = \xi\sigma : \beta^{\sigma\xi-\xi\sigma} = (\beta^s c^x)^\xi(\beta\zeta)^{-\sigma} = (\beta^s c^x\zeta^s)(\beta^s c^x\zeta^s)^{-1} = 1.$

Итак, мы показали, что $K = k_1(\beta)$ – расширение Галуа поля k с группой Галуа $G = F\times C$. Но тогда подалгебра $K_0 = K^F$ всех F-инвариантных элементов алгебры K является циклическим расширением степени $m = 2^n$ поля k.

Пусть $\gamma = \beta^2/d^x \in K$, $w = u^{1-\tau}b \in k_2$ (напомним, что оба элемента u, b принадлежат k_2). Элементы γ, w удовлеворяют следующим соотношениям:

$$\begin{aligned}
&\gamma^{1-\tau} = \gamma/\gamma^\tau = (\beta^2 d^{-x})/(\beta^{-2}d^{2x})d^{-x} = \beta^4/d^{2x} = \gamma^2;\\
&\gamma^{2qN} = \beta^{(1-s)N}/d^{2xqN} = \beta^{(\sigma-s)N}/d^{2xqN} = (c/d^{2q})^{Nx} = v^{Nx};\\
&w^2 = (u^{1-\tau}b)^2 = u^{2(1-\tau)}b^2 = a/v^N;\\
&w^{1-\tau} = u^{2(1-\tau)}b^{1-\tau} = v^{-N}
\end{aligned}$$

(в доказательстве второго соотношения мы воспользовались равенством $(1-s)N = (\sigma-s)N$ из леммы). Пусть, далее, $\alpha = \gamma^{Nq}w^x$. Пользуясь приведенными выше соотношениями и леммой, находим:

$$\alpha^{1-\tau} = \left(\gamma^{1-\tau}\right)^{Nq}w^{(1-\tau)x} = \gamma^{2Nq}w^{(1-\tau)x} = v^{Nx}(v^{-N})^x = 1;$$

$$\alpha^{\sigma-1} = (\gamma^q)^{N(\sigma-1)}w^{(\sigma-1)x} = 1 \quad \text{(напомним, что } \ w \in k_2);$$

$$\alpha^{\xi-1} = (\beta^2)^{(\xi-1)Nq} = \zeta^{2Nq} = -1;$$

$$\alpha^2 = \gamma^{2Nq}w^{2x} = v^{Nx}(av^{-N})^x = a^x.$$

Следовательно, $a \in K_0$ и $\sqrt{a} = \pm\alpha a^{(1-x)/2} \in K_0$. Итак, расширение $k(\sqrt{a})/k$ погружено в расширение Галуа K_0/k с циклической группой Галуа порядка $m = 2^n$.

Доказательство утверждения (с). Доказательство аналогично доказательству утверждения (d), но намного проще. Пусть l – порядок группы Галуа F расширения k_1/k. Обозначим через σ порождающий элемент циклической группы F; пусть s – такое целое число, что $\zeta^\sigma = \zeta^s$. Легко видеть, что $s^l \equiv 1(\operatorname{mod} 2^n)$, но $s^l \equiv 1(\operatorname{mod} 2^{n+1})$; следовательно, $x = (1 - s^l)/2^n$ – нечетное целое число. Мы снова будем использовать элементы N, Δ, введенные в доказательстве утверждения (d). Как и выше, эти элементы обладают следующими свойствами:

$$(\sigma - s)\Delta = 1 - s^l = mx, \quad (\sigma - s)N = (1 - s)N, \quad \zeta^{N(1-s)/2} = -1.$$

Необходимость Пусть $K_0 \supset k(\sqrt{a})$ – расширение Галуа поля k с циклической группой Галуа C порядка m. Обозначим через K алгебру $K_0 \otimes_k k_1$; тогда K/k – расширение Галуа с группой Галуа $G = F \times C$. Обозначим через ξ порождающий элемент группы C. Группа Галуа расширения K/k_1 – циклическая группа C порядка m, а поле k_1 содержит первообразный корень ζ степени m из 1; следовательно, $K = k_1(\beta)$, где $\beta^m \in k_1$, $\beta^\xi = \beta\zeta$. Очевидно, что элемент $c = \beta^{\sigma - s}$ принадлежит полю k_1 (поскольку он ξ-инвариантен). Обозначим через γ элемент $\beta^{N(1-s)/2} \in K$. Имеем:

$$\begin{aligned} \gamma^{\xi-1} &= \beta^{(\xi-1)N(1-s)/2} = \zeta^{N(1-s)/2} = -1, \\ \gamma^{\sigma-1} &= \beta^{(1-s)N(\sigma-1)} = 1, \\ \gamma^2 &= \beta^{(1-s)N} = \beta^{(\sigma-s)N} = \operatorname{Nm}_{k_1/k} c. \end{aligned}$$

Пусть $\alpha = \sqrt{a}$; этот элемент имеет следующие свойства:

$$\alpha^{\xi-1} = -1, \quad \alpha^{\sigma-1} = 1.$$

Поэтому элемент $w = \gamma^{-1}\alpha$ является ξ-инвариантным и σ-инвариантным, т.е. $w \in k$; следовательно, существует элемент $u \in k$ такой, что $\alpha = \gamma u$. Итак, $a = \alpha^2 = u^2\gamma^2 = u^2 \operatorname{Nm}_{k_1/k} c$.

Достаточность Пусть $u \in k_2$, $v \in k_1$ – такие элементы, что $a = u^2 \operatorname{Nm}_{k_1/k_2} v = u^2 v^N$. Обозначим через G прямое произведение группы F и циклической группы C порядка m; пусть ξ – какой-то порождающий элемент группы C. Мы явно построим расширение K/k_1, которое является расширением Галуа поля k

с группой Галуа G. Именно, $K = k_1(\beta)$, где $\beta^m = v^\Delta$ и порождающие элементы σ, ξ группы G действуют на β по следующим формулам:

$$\beta^\xi = \beta\zeta, \quad \beta^\sigma = \beta^s\, v^x$$

(ξ действует на k_1 тривиально). Заметим, что K – не обязательно поле, но лишь алгебра. Проверим, что так определенные операторы на K не нарушают равенство $\beta^m = v^\Delta$ и что они удовлетворяют всем соотношениям между элементами σ, ξ группы G.

$$(\beta^\sigma)^m = (\beta^s v^x)^m = (\beta^m)^s\, v^{xm} = v^{\Delta s}\, v^{(\sigma-s)\Delta} = v^{\Delta\sigma}.$$
$$(\beta^\xi)^m = (\beta\zeta)^m = \beta^m = v^\Delta = (v^\Delta)^\xi.$$
$$\sigma^l = 1 : \beta^{\sigma^l - 1} = \beta^{\sigma^l - s^l}\beta^{s^l - 1} = \beta^{(\sigma-s)\Delta}\beta^{-mx} = v^{x\Delta}v^{-\Delta x} = 1.$$
$\xi^m = 1$ – очевидно.
$$\sigma\xi = \xi\sigma : \beta^{\sigma\xi - \xi\sigma} = (\beta^s v^x)^\xi(\beta\zeta)^{-\sigma} = (\beta^s v^x\zeta^s)(\beta^s v^x \zeta^s)^{-1} = 1.$$

Итак, мы доказали, что расширение $K = k_1(\beta)$ – расширение Галуа поля k с группой Галуа $G = F \times C$. Тогда подалгебра $K_0 = K^F$ всех F-инвариантных элементов алгебры K является циклическим расширением Галуа степени $m = 2^n$ поля k.

Пусть $\alpha = \beta^{N(1-s)/2}$. Имеем

$$\alpha^{\sigma-1} = \left(\beta^{(1-s)/2}\right)^{N(\sigma-1)} = 1;$$
$$\alpha^{\xi-1} = \beta^{(\xi-1)N(1-s)/2} = \zeta^{N(1-s)/2} = -1;$$
$$\alpha^2 = \beta^{(1-s)N} = \beta^{(\sigma-s)N} = v^{xN} = (a/u^2)^x.$$

Следовательно, $\alpha \in K_0$ и $\sqrt{a} = \pm\alpha u^x/a^{(x-1)/2} \in K_0$. Итак, расширение $k(\sqrt{a})/k$ погружено в расширение Галуа K_0/k с циклической группой Галуа порядка $m = 2^n$.

Замечание. Хотя во всех случаях алгебра Галуа K – не обязательно поле, циклическое 2^n-расширение K_0 поля k, содержащее квадратичное *поле* $k(\sqrt{a})$, автоматически является полем.

Следствие. *Если $a \in k\backslash k^2$ – норма элемента из поля $k_1 = k(\sqrt[2^n]{1})$, то расширение $k(\sqrt{a})/k$ 2^n-погружаемо.*

Доказательство. Действительно, этот факт немедленно следует из теоремы в случаях (a), (b), (c). Если расширение k_1/k не циклическое, и если $a = \mathrm{Nm}_{k_1/k}\, v = v^{(1+\tau)N}$, то элемент $b = v^N$ содержится в k_2 и $b^{1+\tau} = a$. Имеем:

$$a/b^2 = v^{(\tau-1)N} = (1^{1-\tau})^2 \mathrm{Nm}_{k_1/k_2}(v^{\tau-1}).$$

По утверждению (d) теоремы, расширение $k(\sqrt{a})/k$ 2^n-погружаемо.

Литература

1. Р. А. Шмидт, А. В. Яковлев, *Условие погружаемости в случае циклического нормального делителя порядка* 2^n. Вестник Ленингр. ун-та, вып. 13 (1963).

Yakovlev A. V. The embedding of a cyclic Galois estension into a cyclic extension.

A necessary and sufficient condition of the existence of a cyclic Galois extension of degree 2^n containing a given quadratic extension is found.

С.-Петербургский
государственный университет

Поступило 20 декабря 1999 г.