M. V. Bondarko, S. V. Vostokov, Decomposability of ideals as Galois modules in complete discrete valuation fields, *Algebra i Analiz*, 1999, Volume 11, Issue 2, 41–63

Алгебра и анализ
Том 11 (1999), вып. 2

# РАЗЛОЖИМОСТЬ ИДЕАЛОВ КАК МОДУЛЕЙ ГАЛУА В ПОЛНЫХ ДИСКРЕТНО-НОРМИРОВАННЫХ ПОЛЯХ

© М. В. Бондарко, С. В. Востоков

Находятся необходимые и достаточные условия разложимости идеалов как модулей Галуа в абелевых $p$-расширениях полных дискретно-нормированных полей.

## Введение

Исследование аддитивных модулей Галуа в локальных полях (конечных расширениях поля $\mathbb{Q}_p$) продолжается свыше шестидесяти лет, начавшись с работы [N]. Особенно активная деятельность происходила в 60-70-е годы, другой всплеск активности наблюдается в настоящее время. Основной объект изучения — кольцо целых элементов и его идеалы. Исследование происходит с разных точек зрения [E, EM, By, M4, Le, T].

Настоящая работа продолжает цикл работ [BV, V1, V2], а также работ [M1, M2, M3] и является непосредственным продолжением работы [BVZ], в которой найдены условия существования разложимых идеалов в абелевых $p$-расширениях полных дискретно-нормированных полей. Основной результат этой работы формулируется следующим образом.

**Теорема A.** *Пусть $K/k$ — абелево $p$-расширение полного дискретно-нормированного поля характеристики 0 с полем вычетов характеристики $p > 2$. Предположим, что соответствующее расширение полей вычетов сепарабельно. Пусть $G = \mathrm{Gal}(K/k)$ и $\mathfrak{o}$ — кольцо целых поля $k$. Тогда в поле $K$ существуют дробные идеалы, разложимые как $\mathfrak{o}[G]$-модули, в том и только в том случае, когда индекс ветвления $p^m$ расширения $K/k$ делит дифференту $\mathfrak{D}$ этого расширения.*

В настоящей работе мы усиливаем этот результат и находим условия разложимости данного идеала в абелевом $p$-расширении полного дискретно-нормированного поля. Мы докажем следующую теорему.

Работа поддержана РФФИ, грант N 97-01-0058a.

**Теорема B.** *Пусть мы находимся в условиях теоремы A и $\mathfrak{M}$ — максимальный идеал кольца целых поля $K$. Тогда идеал $I = \mathfrak{M}^{\varkappa}$ разложим как $\mathfrak{o}[G]$-модуль в том и только в том случае, если $p^m \mid \mathfrak{D}$ и выполнено одно из условий:*

a) $p \mid \varkappa$;

b) *в $p$-адическом разложении $\varkappa = \varkappa_0 + \varkappa_1 p + \ldots$, $0 \leqslant \varkappa_i \leqslant p-1$, найдется коэффициент $\varkappa_i$, $0 \leqslant i \leqslant m-1$, такой, что $\varkappa_i > \overline{h}$, где $\overline{h}$ — остаток при делении на $p$ максимального скачка ветвления $h$ расширения $K/k$.*

В §1 работы формулируются известные результаты, которые используются в дальнейшем, а также доказывается ряд вспомогательных утверждений. Следующий параграф посвящен случаю циклического расширения степени $p$, который является базой при индукционном рассуждении в общем доказательстве. Наконец, в последнем §3 доказывается основной результат работы — теорема B.

Часть исследований проводилась в Institut-Fourier UFR de Mathematiques города Гренобля, и авторы глубоко признательны профессору Жилларду и профессору Панчишкину за прекрасные условия для научной работы.

## Обозначения

Во всей статье будут приняты следующие обозначения:

$p$ — фиксированное простое число;

$\overline{a}$ — остаток целого числа $a$ при делении на $p$;

$\zeta_n$ — первообразный корень из 1-й степени $n$;

$v_F$ — нормирование на данном дискретно-нормированном поле $F$;

$\mathfrak{o}_F$ — кольцо целых поля $F$;

$\mathfrak{M}_F$ — максимальный идеал кольца $\mathfrak{o}_F$;

$e_F = v_F(p)$, предполагая $\operatorname{char} F = 0$ и $\operatorname{char} \overline{F} = p$;

$k$ — полное дискретно-нормированное поле характеристики 0 с произвольным полем вычетов характеристики $p$;

$\mathfrak{o}$ — кольцо целых поля $k$;

$e$ — абсолютный индекс ветвления поля $k$;

$v_0$ — нормирование на $k$;

$K/k$ — нормальное $p$-расширение с группой Галуа $G$;

$v$ — нормирование на $K$;

$\mathrm{tr} = \mathrm{tr}_{K/k}$;

$p^m$ — индекс ветвления расширения $K/k$;

$k' = k(\zeta_p)$, $K' = K(\zeta_p)$.

Будем называть отображение $P$ модуля $C$ на модуль $A$, $A \subset C$, проектором, если $P$ тождественно на $A$. Если $C$ равно $A \bigoplus B$, то можно взять $P$, являющееся канонической проекцией $A \bigoplus B$ на первое слагаемое. Очевидно, если ядро $P$ равно $B$, то $C = A \bigoplus B$. Тогда получаем, что проектор однозначно задается своим ядром и образом. Несложно доказать, что если $K/k$ абелево, $C$, $A$ —

$k[G]$-модули, $C \subset K$, то $P$ будет равно ограничению на $C$ некоторого идемпотента из $k[G]$. Если $kC = K$, то такой элемент $k[G]$, очевидно, определен однозначно.

## §1. Вспомогательные результаты

**1.1.** Группы ветвления $G_i$, $i \geqslant 1$ (см. [Se, Chapter IV] или [FV, Chapter II, §4]), расширения $K/k$ определяются следующим образом:

$$G_i = \{\sigma \in G \mid v_K(\pi^{\sigma-1} - 1) \geqslant i\},$$

где $\pi$ — произвольный простой элемент $K$. Целое положительное число $h$ называется скачком ветвления $K/k$, если $G_h \neq G_{h+1}$.

В предложении 1.5 работы [BVZ] был доказан следующий важный результат.

**Предложение 1.1.** *В случае $p = 2$ будем требовать, чтобы минимальный скачок ветвления расширения $K/k$ был больше 1. Тогда следующие условия эквивалентны:*

1) *индекс ветвления $p^m$ делит дифференту $\mathfrak{D} = \mathfrak{D}_{K/k}$;*

2) *расширение $K/k$ — циклическое со скачками ветвления $h_1 < \cdots < h_m$ такими, что*

$$h_j - \left[\frac{h_j}{p}\right] = p^{j-1}e, \quad j = 1, \ldots, m.$$

**1.2.** Следующий результат сводит рассмотрение вопроса о разложимости идеалов к вполне разветвленным расширениям. Пусть соответствующее $K/k$ расширение полей вычетов сепарабельно. Пусть $T$ — подполе инерции и $G_1 = \mathrm{Gal}(K/T)$.

**Предложение 1.2.** *Любое $\mathfrak{o}[G]$-разложение идеала в $K$ является также $\mathfrak{o}_T[G_1]$-разложением (см. предложения* 4.6.1 *и* 4.6.2 *работы* [BVZ]).

**1.3.** Пусть $K/k$ — вполне разветвленное циклическое $p$-расширение степени $p^m$ и $\zeta_{p^m} \in k$. Тогда $K = k(\theta)$, где $\theta^{p^m} \in k$.

**Лемма 1.3.1.** *Если скачки ветвления расширения $K/k$ взаимно-просты с $p$, то $v(\theta) \equiv 0 \mod p$.*

**Доказательство.** Если $(v(\theta), p) = 1$, то в качестве радикального элемента $\theta$ можно взять простой элемент поля $K$, а тогда скачки ветвления расширения $K/k$ будут делиться на $p$ (см. [Se, Ch IV, §2] или [FV, Ch. III]), что противоречит условию. •

Пусть, как и выше, расширение $K/k$ — вполне разветвленное циклическое расширение степени $p^m$, при этом $\zeta_p \notin k$, но $\zeta_{p^m} \in k' = k(\zeta_p)$. Тогда расширение $K'/k'$, где $K' = K(\zeta_p)$, будет куммеровским и, значит, $K' = k'(\theta)$, где $\theta^{p^m} \in k'$.

**Лемма 1.3.2.** $v'(\theta) \equiv 0 \mod p^m$, *где* $v'$ — *нормирование на* $K'$.

**Замечание 1.3.3.** В силу результата леммы, мы в дальнейшем в такой ситуации будем в качестве $\theta$ всегда брать единицу поля $K'$, т.е. требовать

$$v'(\theta) = 0.$$

**Доказательство леммы 1.3.2.** Пусть $\sigma$ — образующий элемент циклической группы $G = \mathrm{Gal}(K/k)$, а $g$ — образующий циклической группы $G' = \mathrm{Gal}(k'/k)$, $G' \subset (\mathbb{Z}/p\mathbb{Z})^*$.

Пусть $d = [k' : k]$. Тогда имеем $\theta^\sigma = \zeta\theta$ при некотором первообразном корне $\zeta$ степени $p^m$ из 1, и при этом

$$\zeta^g = \zeta^r$$

при некотором первообразном корне $r$ степени $d$ из 1 по модулю $p^m$, т.е., в частности,

$$r - 1 \not\equiv 0 \mod p^m. \tag{1}$$

Возьмем элемент

$$\alpha = \theta^r/\theta^g$$

и проверим, что $\alpha \in k'$. Действительно,

$$\alpha^\sigma = (\theta^r)^\sigma/(\theta^g)^\sigma = \zeta^r\theta^g/\zeta^r\theta^g = \alpha a.$$

Поэтому $v'(\alpha) \equiv 0 \mod p^m$. Но

$$v'(\alpha) = rv'(\theta) - v'(\theta^g) = (r-1)v'(\theta).$$

Учитывая (1), получаем утверждение леммы. •

**1.4.** Пусть $K/k$ — циклическое вполне разветвленное расширение степени $p$ со скачком ветвления $h$ взаимно-простым с $p$. Пусть $\sigma$ — образующий автоморфизм группы Галуа $G = \mathrm{Gal}(K/k)$.

**Лемма 1.4.1.** *Если* $x \in K$ *и* $v(x) = \varkappa$, *то*

$$v\left(\frac{tr}{p}x\right) \geqslant \varkappa + (p-1)h - pe, \tag{2}$$

*при этом если* $\varkappa \equiv h \mod p$, *то*

$$v\left(\frac{tr}{p}x\right) = \varkappa + (p-1)h - pe. \tag{3}$$

**Доказательство.** Возьмем идеал $I = \mathfrak{M}^{\varkappa}$. Он имеет $\mathfrak{o}$-базис вида

$$I = \langle \xi, \lambda_1(\sigma-1)\xi, \ldots, \lambda_{p-1}(\sigma-1)^{p-1}\xi \rangle,$$

где $v(\xi) = \varkappa + \overline{h-\varkappa}$, $\lambda_i \in k$, $v_0(\lambda_i) = -\left[\frac{\overline{h-\varkappa}+ih}{p}\right]$.

Ясно, что

$$x = \alpha_0\xi + \cdots + \alpha_{p-1}\lambda_{p-1}(\sigma-1)^{p-1}\xi, \quad \alpha_i \in \mathfrak{o}. \tag{4}$$

Значит,

$$\frac{\mathrm{tr}}{p}(x) = \alpha_0 \frac{\mathrm{tr}}{p}(\xi).$$

Проверим, что

$$v\left(\frac{\mathrm{tr}}{p}(\xi)\right) = v\left(\frac{(\sigma-1)^{p-1}}{p}(\xi)\right) = v(\xi) + (p-1)h - pe. \tag{5}$$

Действительно, так как $(h,p) = 1$, то $(p-1)h < pe$ (см. [Se]). Поэтому

$$v(a_i(\sigma-1)^i\xi) \geqslant v(\xi) + ih > v\left(\frac{(\sigma-1)^{p-1}}{p}(\xi)\right) = v(\xi) + (p-1)h - pe.$$

Теперь из равенства

$$\frac{\mathrm{tr}}{p}(\xi) = \sum_{i=0}^{p-1} a_i(\sigma-1)^i\xi + \frac{(\sigma-1)^{p-1}}{p}(\xi), \quad a_i \in \mathbb{Z},$$

следует (5).

Равенство (5) дает нам неравенство (2) леммы.

Равенство (3) леммы вытекает из того, что когда $\varkappa \equiv h \mod p$, коэффициент $\alpha_0$ в разложении (4) должен быть единицей кольца $\mathfrak{o}$. Лемма доказана. •

Пусть $k' = k(\zeta_p)$, при этом $k$ и $k'$ могут совпадать.

Будем предполагать, что $k'/k$ вполне разветвлено, и пусть $d = [k' : k]$. Пусть $K' = K(\zeta_p)$, $h$ и $h'$ — скачки ветвления расширений $K/k$ и $K'/k'$ соответственно. Ясно, что в нашем случае $h' = dh$. Пусть $e'$ — абсолютный индекс ветвления поля $k'$.

Предположим, что в расширении $K/k$ $p$ делит дифференту этого расширения, что равносильно условию

$$h - \left[\frac{h}{p}\right] = e \tag{6}$$

(см. предложение 1.1).

**Лемма 1.4.2.** *Для любого элемента $x$ из поля $K'$, $v'(x) = \varkappa$ имеем*

$$v'\left(\frac{\mathrm{tr}}{p}x\right) \geqslant \varkappa - d\overline{h},$$

*где* $\mathrm{tr} = \mathrm{tr}_{K'/k'}$, *а* $v'$ — *нормирование на* $K'$.

*При этом если* $v'(x) = \varkappa \equiv d\overline{h} \equiv h' \mod p$, *то*

$$v'\left(\frac{\mathrm{tr}}{p}x\right) = \varkappa - d\overline{h}.$$

**Доказательство.** В нашем случае

$$(p-1)h' = pe' - d\overline{h},$$

так как $h' = dh$, $e' = de$, а из (6) следует, что $(p-1)h = pe - \overline{h}$. Для окончания доказательства применяем лемму 1.4.1. •

Пусть $e_i$ — одномерный идемпотент (т.е. проектор на одномерное пространство) вида

$$e_i = (1 + \sigma\zeta_p^i + \cdots + (\sigma\zeta_p^i)^{p-1})/p$$

и пусть $K' = k'(\theta)$. При этом $v'(\theta) = 0$ (см. замечание 1.3.3).

**Лемма 1.4.3.** *В условиях леммы* 1.4.2 *имеем*

$$v'(e_i(x)) \geqslant \varkappa - d\overline{h}.$$

*При этом если* $v'(x) = \varkappa \equiv d\overline{h} \equiv h' \mod p$, *то*

$$v'(e_i(x)) = \varkappa - d\overline{h}.$$

**Доказательство.** Мы имеем очевидное равенство $e_i(x) = \theta^{-i}\frac{\mathrm{tr}}{p}(x\theta^i)$, из которого следует, что

$$v'(e_i(x)) = v'\left(\frac{\mathrm{tr}}{p}(x\theta^i)\right),$$

так как $v'(\theta) = 0$. Осталось применить предыдущую лемму, так как $v'(x\theta^i) = v'(x) = \varkappa$. •

## §2. Расширение степени $p$

**2.1.** Пусть $K/k$ — вполне разветвленное циклическое расширение степени $p$ с группой Галуа $G = \langle\sigma\rangle$. Мы будем рассматривать $\mathfrak{N}$ — $\mathfrak{o}[G]$-подмодуль $K$, имеющий $\mathfrak{o}$-базис вида

$$\langle\xi, \lambda_1(\sigma-1)\xi, \ldots, \lambda_{p-1}(\sigma-1)^{p-1}\xi\rangle, \quad \text{где } v(\xi) \equiv h \mod p, \tag{7}$$

где $\xi \in K$, $\lambda_1, \ldots, \lambda_{p-1} \in k$, $-e \leqslant v_0(\lambda_{p-1}) \leqslant \cdots \leqslant v_0(\lambda_1) \leqslant 0$.

Так же, как в предложении 2.1 работы [BVZ], доказывается следующее утверждение.

**Лемма 2.1.1.**

1) *Модуль $\mathfrak{N}$ с $\mathfrak{o}$-базисом* (7) *— полный $\mathfrak{o}[G]$-модуль в $K$ (т.е. $k\mathfrak{N} = K$).*

2) *Любой идеал в $K$ имеет базис вида* (7).

**Предложение 2.1.2.** *Следующие условия равносильны:*

a) *$\mathfrak{N}$ с базисом* (7) *разложим как $\mathfrak{o}[G]$-модуль;*

b) $\mathrm{tr}/p$ *переводит $\mathfrak{N}$ в себя;*

c) $v_0(\lambda_{p-1}) + e = 0$.

**Доказательство.** b) $\Longleftrightarrow$ c): Достаточно выяснить, когда оператор $\mathrm{tr}/p$ переводит базис модуля $\mathfrak{N}$ в $\mathfrak{N}$. Все элементы базиса, кроме первого, след переводит в 0. Для первого элемента имеем

$$\begin{aligned}\frac{\mathrm{tr}}{p}(\xi) &= \frac{1+\sigma+\cdots+\sigma^{p-1}}{p}(\xi)\\ &= \xi + a_1\lambda_1(\sigma-1)\xi + \cdots + a_{p-2}\lambda_{p-2}(\sigma-1)^{p-2}\xi\\ &\quad + \frac{1}{p\lambda_{p-1}}\lambda_{p-1}(\sigma-1)^{p-1}\xi,\end{aligned} \tag{8}$$

где $a_i = C_p^{i+1}/\lambda_i p$. Все коэффициенты разложения, кроме, возможно, последнего, являются целыми, так как $\lambda_1^{-1}, \ldots, \lambda_{p-1}^{-1} \in \mathfrak{o}_k$ по условию. Поэтому условие $b$ равносильно $\frac{1}{p\lambda_{p-1}} \in \mathfrak{o}_k$, т.е. $v_0(\lambda_{p-1}) + e \leqslant 0$. В обратную сторону неравенство всегда есть по условию.

a) $\Longleftrightarrow$ c): Пусть сперва $\zeta_p \in k$. Тогда $K = k(\theta)$, $\theta^p \in k$. Поле $K$, рассматриваемое как $\mathfrak{o}[G]$-модуль, представляется в виде суммы

$$K = \bigoplus_{i=0}^{p-1} k\theta^{-i}. \tag{9}$$

Проектор $e_i$ на одномерное собственное подпространство $k\theta^{-i}$ имеет вид $e_i = (1 + \zeta_p^i\sigma + \cdots + (\zeta_p^i\sigma)^{p-1})/p$. Если $i = 0$, то $e_0 = \mathrm{tr}/p$, если же $1 \leqslant i \leqslant p-1$, то идемпотент $e_i$ можно записать следующим образом:

$$e_i = a_1(\sigma - 1) + \cdots + a_{p-2}(\sigma - 1)^{p-2} + \frac{\zeta_p^{-i}}{p}(\sigma - 1)^{p-1},$$

где $a_\alpha \in ((\zeta_p - 1)^{-\alpha})$, $((\zeta_p - 1)^{-\alpha})$ — дробный идеал поля $\mathbb{Q}_p(\zeta_p)$. Проектор $e_I$ на сумму нескольких одномерных слагаемых

$$k\theta^{-i_1} \oplus \cdots \oplus k\theta^{-i_r}$$

будет суммой ортогональных идемпотентов

$$e_I = e_{i_1} + \cdots + e_{i_r}, \quad 0 \leqslant i_1 < \cdots < i_r \leqslant p-1.$$

Поэтому

$$e_I = \begin{cases} \sum_{\alpha=1}^{p-2} b_\alpha(\sigma-1)^\alpha + \frac{b_{p-1}}{p}(\sigma-1)^{p-1}, & \text{если } i_1 \neq 0, \\ \frac{\mathrm{tr}}{p} + \sum_{\alpha=1}^{p-2} b_\alpha(\sigma-1)^\alpha + \frac{b_{p-1}}{p}(\sigma-1)^{p-1}, & \text{если } i_1 = 0, \end{cases} \tag{10}$$

где $b_\alpha \in ((\zeta_p - 1)^{-\alpha})$, $1 \leqslant \alpha \leqslant p-2$ и $b_{p-1} \in \mathbb{Z}_p[\zeta_p]^*$.

Если выполнено условие c), то, согласно (8), оператор $\mathrm{tr}/p$ является идемпотентом на модуле $\mathfrak{N}$ , и, значит, получаем $\mathfrak{o}[G]$-разложение

$$\mathfrak{N} = \frac{\mathrm{tr}}{p}(\mathfrak{N}) \bigoplus \mathrm{Ker}\,\mathrm{tr}(\mathfrak{N}). \tag{11}$$

Пусть теперь $\mathfrak{o}[G]$-модуль $\mathfrak{N}$ разложим и для определенности $\mathrm{tr}\,\mathfrak{A} = 0$. Пусть $\mathfrak{A}' = k\mathfrak{A} = \bigoplus_{\alpha=1}^{r} k\theta^{-i_\alpha}$. Тогда $0 \notin I = (i_1, \ldots, i_r)$, и оператор $e_I$ является идемпотентным оператором на модуле $\mathfrak{N}$. Значит,

$$e_I(\xi) \in \mathfrak{N}.$$

Из (10) получаем разложение $e_I(\xi)$ по $\mathfrak{o}$-базису модуля $\mathfrak{N}$:

$$e_I(\xi) = \sum_{\alpha=1}^{p-2} \frac{b_\alpha}{\lambda_\alpha}\lambda_\alpha(\sigma-1)^\alpha\xi + \frac{b_{p-1}}{p\lambda_{p-1}}\lambda_{p-1}(\sigma-1)^{p-1}\xi \in \mathfrak{N}.$$

Все коэффициенты этого разложения должны быть целыми, в частности

$$b_{p-1}/p\lambda_{p-1} \in \mathfrak{o}.$$

Но $b_{p-1} \in \mathfrak{o}^*$, а значит, $1/p\lambda_{p-1} \in \mathfrak{o}$, т.е. получаем условие c).

Если в поле $k$ нет нетривиальных $p$-х корней из 1, то все приведенные выше рассуждения также можно провести. Действительно, пространство $K' = k'\mathfrak{A} \bigoplus k'\mathfrak{B}$ можно так же, как в (9), разложить в сумму одномерных, а значит, можно рассмотреть проектор на одну из компонент разложения, равный в кольце $k'[G]$ сумме ортогональных идемпотентов, получаем разложение вида (10), причем так как $\mathfrak{A}, \mathfrak{B}$ определены над $k$, то $e_I \in k[G]$, а значит, все $b_i$ лежат в $\mathbb{Q}(\zeta_p) \cap k$, а $b_\alpha$, $1 \leqslant \alpha \leqslant p-2$ (и $a_\alpha$ из предшествующей формулы) имеют в $k$ нормирование, не меньшее $-e\alpha/(p-1)$, где $e$ — индекс ветвления поля $k$. Далее, также получаем

$$b_{p-1}/p\lambda_{p-1} \in \mathfrak{o},$$

что снова влечет $1/p\lambda_{p-1} \in \mathfrak{o}$. •

Из предложения 2.1.2, примененного к идеалам поля $K$, получаем следующий результат.

**Следствие 2.1.3.** *В поле $K$ существуют разложимые идеалы тогда и только тогда, когда дифферента $\mathfrak{D}$ расширения $K/k$ делится на $p$.*

**2.2.** В работе [BVZ] для случая полей, не содержащих нетривиальные $p$-е корни из 1, был определен более широкий, чем идеалы, класс модулей в $K'$, которые были названы композит-модулями. Напомним определение.

Пусть $k' = k(\zeta_p)$, $K' = K(\zeta_p)$, $\mathfrak{o}' = \mathfrak{o}_{k'}$ и $\mathfrak{O} = \mathfrak{o}_K$.

**Определение 2.2.1.** Композит-модулем $\mathfrak{N}$ в $K'$ будем называть полный $\mathfrak{O}$-подмодуль в $K'$, который также является $\mathbb{Z}_p[\zeta_p][G]$-модулем и не равен всему $K'$, т. е. нормирования элементов в нем ограничены снизу. Говорим, что композит-модуль $\mathfrak{N}$ разложим, если $\mathfrak{N} = \mathfrak{A} \bigoplus \mathfrak{B}$, где $\mathfrak{A}$ и $\mathfrak{B}$ — нетривиальные $\mathbb{Z}_p[\zeta_p]\mathfrak{o}[G]$-подмодули $\mathfrak{N}$.

**Замечание 2.2.2.** Если $k'/k$ не является вполне разветвленным, то каждому разложению композит-модуля в $K'$ относительно $k$ соответствует разложение композит-модуля в $K'$ относительно $k_1$, где $k_1$ — подполе инерции в $k'/k$. Действительно, если $P$ — проектор на одну из компонент разложения $\mathfrak{N}$, то он остается идемпотентом и на $\mathfrak{N}\mathfrak{o}_{k_1} \subset K'$, так как действие $G$ на $\mathfrak{o}_{k_1}$ тривиально.

**2.3.** Пусть $K/k$ — вполне разветвленное циклическое расширение степени $p$. Пусть $d = [k' : k]$. Ясно, что $d$ делит $p-1$ и $h' = dh$ – скачок ветвления группы Галуа $K'/k'$. Через $\mathfrak{D}$ и $\mathfrak{D}'$ обозначим дифференты расширений $K/k$ и $K'/k'$ соответственно. Будем считать, согласно замечанию, что расширение $k'/k$ вполне развётвлено. Пусть $v'$ — нормирование в поле $K'$, $e'$ — абсолютный индекс ветвления поля $k'$.

**Определение 2.3.1.** Если композит-модуль $\mathfrak{N}$ содержит элемент с нормированием $d\varkappa$ и не содержит элементов с нормированием меньшим или равным $d(\varkappa-1)$, то мы будем называть $\varkappa$ степенью композит-модуля $\mathfrak{N}$ и обозначать

$$\varkappa = \deg \mathfrak{N}.$$

**Замечание 2.3.2.** Не у всякого композит-модуля есть степень.

**Предложение 2.3.3.**

1) *Следующие условия равносильны:*

a) *в $K$ существуют разложимые идеалы;*

b) *в $K'$ существуют разложимые композит-модули;*

c) *$p$ делит $\mathfrak{D}$.*

2) *Пусть $p \mid \mathfrak{D}$, и $\mathfrak{N}$ — композит-модуль в $K'$ степени $\varkappa$. Если $0 < \overline{\varkappa} \leqslant \overline{h}$, то композит-модуль $\mathfrak{N}$ неразложим.*

**Доказательство.**

1. Равносильность a) и c) была доказана в следствии 2.1.3 предложения 2.1.2.

Докажем теперь равносильность a) и b).

Если $I$ — разложимый идеал в $K$, $I = \mathfrak{A} \bigoplus \mathfrak{B}$, то $\mathfrak{o}'I = \mathfrak{o}'\mathfrak{A} \bigoplus \mathfrak{o}'\mathfrak{B}$ — разложимый композит-модуль в $K'/k$.

Обратно, пусть все идеалы в $K$ неразложимы, но в $K'/k$ существует разложимый композит-модуль

$$\mathfrak{N} = \mathfrak{A} \bigoplus \mathfrak{B}. \tag{12}$$

Докажем, что в этом случае $p \mid \mathfrak{D}$, а значит, в $K$ есть разложимые идеалы. Пусть $K' = k'(\theta)$, где $\theta^p \in k'$.

Заметим, что существование разложимых идеалов в $K/k$ равносильно, согласно предложению 2.1.2, а также предложению 1.1 (или предложению 1.5 работы [BVZ]), следующему:

$$\begin{aligned} p \mid \mathfrak{D} &\iff h - \left[\frac{h}{p}\right] = e \\ &\iff (p-1)h + \overline{h} = pe \iff h \geqslant \frac{pe}{p-1} - 1 \\ &\iff h' \geqslant \frac{pe'}{p-1} - d, \text{ считая, что } (h,p) = 1. \end{aligned} \tag{13}$$

Рассмотрим прямое слагаемое $\mathfrak{A}$ из (12) и предположим для определенности, что $\operatorname{tr}\mathfrak{A} = 0$, тогда пространство $k'\mathfrak{A}$ натянуто на $\theta^{-i_1}, \ldots, \theta^{-i_r}$, где $0 < i_1 < \cdots <$

$i_r \leqslant p-1$, и проектор $e_I$, $I=(i_1,\dots,i_r)$, пространства $K'$ на $k'\mathfrak{A}$, который в силу разложения (12) будем проектором модуля $\mathfrak{N}$ на $\mathfrak{A}$, имеет вид

$$e_I = \sum_{\alpha=1}^{p-2} b_\alpha(\sigma-1)^\alpha + \frac{b_{p-1}}{p}(\sigma-1)^{p-1}, \tag{14}$$

где $b_\alpha \in (\zeta_p-1)^{-\alpha}\mathbb{Z}_p[\zeta_p]$, $1\leqslant\alpha\leqslant p-2$, $b_{p-1}\in\mathbb{Z}_p[\zeta_p]^*$ (см. (10)).

Пусть $x\in\mathfrak{N}$ — элемент с наименьшим возможным нормированием $v'(x)=\varkappa$. Тогда найдется элемент $y$ такой, что

$$\begin{aligned} &v'(y)\equiv h' \mod p,\\ &v'(y)\in\{\varkappa,\varkappa+d,\dots,\varkappa+(p-1)d\}. \end{aligned} \tag{15}$$

Действительно, будем домножать последовательно $x$ на степени простого элемента в $K$, и так как $d$ делит $p-1$, а расширение $K'/K$ вполне разветвлено по нашему соглашению, то мы легко находим элемент $y$, удовлетворяющий (15).

Поскольку $y\in\mathfrak{N}$ и $e_I$ — идемпотент на $\mathfrak{N}$, то $e_I(y)\in\mathfrak{N}$ и, значит, в частности, $v'(e_I(y))\geqslant\varkappa$. Вычислим это нормирование, используя (14). Из (15), а также из условия $v'(b_{p-1})=0$ (см. 14) следует

$$\begin{aligned} &v'(b_\alpha(\sigma-1)^\alpha y) = v'(b_\alpha)+\alpha h'+v'(y), \quad 1\leqslant\alpha\leqslant p-2;\\ &v'\left(b_{p-1}\frac{(\sigma-1)^{p-1}}{p}\right) = (p-1)h'-pe'+v'(y). \end{aligned}$$

Из нашего предположения о неразложимости в $K$ всех идеалов следует (см. (12)), что

$$h' < \frac{pe'}{p-1} - d, \tag{16}$$

и, значит, учитывая, что $b_\alpha\in(\zeta_p-1)^{-\alpha}\mathbb{Z}[\zeta_p]$, получаем

$$\begin{aligned} &v'(b_\alpha(\sigma-1)^\alpha y) - v'\left(\frac{b_{p-1}}{p}(\sigma-1)^{p-1}y\right)\\ &\quad\geqslant \left(-\frac{\alpha pe'}{p-1}+\alpha h'+v'(y)\right) - ((p-1)h'-pe'+v'(y))\\ &\quad= \left(\frac{pe'}{p-1}-h'\right)(p-1-\alpha) > 0, \end{aligned} \tag{17}$$

откуда следует, что,

$$\begin{aligned} \varkappa\leqslant v'(e_I(y)) &= v'\left(\frac{b_{p-1}}{p}(\sigma-1)^{p-1}y\right)\\ &= (p-1)h'-pe'+v'(y)\leqslant(p-1)h'-pe'+\varkappa+(p-1)d \end{aligned}$$

(в последнем неравенстве мы использовали (15)). Значит,

$$h' \geqslant \frac{pe'}{p-1} - d,$$

что противоречит (16). Таким образом, утверждение 1) нашего предложения доказано.

2. Докажем утверждение 2) нашего предложения. Пусть $\mathfrak{N} = \mathfrak{A} \bigoplus \mathfrak{B}$ и для определенности $\operatorname{tr} \mathfrak{A} = 0$. Тогда $k'\mathfrak{A} = \langle \theta^{-i_1}, \dots, \theta^{-i_r} \rangle$, где $0 < i_1 < \dots < i_r \leqslant p-1$. Как и в п. 1, $e_I$ — проектор $\mathfrak{N}$ на прямое слагаемое $\mathfrak{A}$, и он имеет вид (14).

Пусть $x \in \mathfrak{N}$ — элемент с нормированием $d\varkappa$ и $\pi$ — простой элемент кольца $\mathfrak{O} = \mathfrak{o}_K$. Считаем, что $K'/K$ вполне разветвлено (см. замечание 2.2.2 к определению 2.2.1). Тогда элемент $y = x\pi^{\overline{h}-\overline{\varkappa}}$ будет иметь нормирование

$$v'(y) = d(\varkappa + \overline{h} - \overline{\varkappa}) \geqslant d\varkappa = v'(x),$$

так как, по нашему условию, $\bar{\varkappa} \leqslant \overline{h}$. Кроме того,

$$v'(y) \equiv dh \equiv h' \mod p,$$

где $h'$ — скачок ветвления расширения $K'/k'$, равный $dh$.

Элемент $y \in \mathfrak{N}$, а $e_I$ — идемпотент на $\mathfrak{N}$, а значит, $e_I(y) \in \mathfrak{N}$, и поэтому $v'(e_I(y)) \geqslant d\varkappa$. Так же, как в п. 1, получаем

$$v'(b_\alpha(\sigma-1)^\alpha y) > v'\left(\frac{b_{p-1}}{p}(\sigma-1)^{p-1}y\right)$$

(см. (17)). Отсюда следует, что

$$\begin{aligned} v'(e_I(y)) &= v'\left(\frac{b_{p-1}}{p}(\sigma-1)^{p-1}y\right) \\ &= (p-1)h' - pe' + v'(y) = -d\overline{h} + d(\varkappa + \overline{h} - \overline{\varkappa}) = d(\varkappa - \overline{\varkappa}). \end{aligned}$$

Но $v'(e_I(y)) \geqslant d\varkappa$, значит, $d\overline{\varkappa} \leqslant 0$, т.е. $\overline{\varkappa} = 0$, что противоречит условию $0 < \overline{\varkappa} \leqslant \overline{h}$.

Утверждение 2 предложения доказано. •

**2.4.** Пусть $K/k$ — вполне разветвленное нормальное $p$-расширение, в котором индекс ветвления $p^m$ делит дифференту $\mathfrak{D}$. Тогда, согласно предложению 1.1, расширение $K/k$ циклическое.

Пусть

$K_i$ — подрасширение степени $p^i$ в $K/k$, $[K : K_i] = p^i$,

$\mathfrak{M}_i$ — максимальный идеал в кольце целых поля $K_i$,

$h$ — максимальный скачок ветвления группы Галуа $G$.

Рассмотрим идеал $I = \mathfrak{M}^\varkappa$ в поле $K$, и пусть

$$\varkappa = \varkappa_0 + \varkappa_1 p + \dots, 0 \leqslant \varkappa_i < p,$$

— $p$-адическое разложение.

**Предложение 2.4.1.** *Если для идеала* $I = \mathfrak{M}^{\varkappa}$ *имеем*

a) $p \mid \varkappa$

*или*

b) $0 < \varkappa_0 \leqslant \overline{h}$, $0 \leqslant \varkappa_1 \leqslant \overline{h}, \ldots, 0 \leqslant \varkappa_{r-2} \leqslant \overline{h}$, $\varkappa_{r-1} > \overline{h}$, *где* $1 \leqslant r \leqslant m$,

*то имеет место* $\mathfrak{o}[G]$*-разложение*

$$I = \frac{\mathrm{tr}_{K/K_r}}{p^r}(I) \bigoplus (\mathrm{Ker}\,\mathrm{tr}_{K/K_r} \cap I).$$

**Доказательство.** Подсчитаем степени идеалов

$$\mathfrak{M}_i{}^{c_i} = \frac{\mathrm{tr}_{K/K_i}}{p^i}(\mathfrak{M}^{\varkappa}).$$

Имеем

$$c_1 = \frac{\varkappa + \overline{h - \varkappa} + (p-1)h}{p} - p^{m-1}e = \left[\frac{\varkappa}{p}\right] \tag{18}$$

(см. [Se, Ch. 4, §3]), так как $\overline{h - \varkappa} = \overline{h} - \overline{\varkappa}$ и $\overline{h} + (p-1)h = p^{m-1}e$. Аналогично

$$c_2 = \left[\frac{c_1}{p}\right] = \left[\frac{\varkappa}{p^2}\right], \ldots, \quad c_{r-1} = \left[\frac{\varkappa}{p^{r-1}}\right].$$

Но так как $\varkappa_{r-1} > \overline{h}$, то

$$c_r = \left[\frac{\varkappa}{p^r}\right] + 1.$$

Отсюда следует, что $p^r c_r \geqslant \varkappa$. Значит, $\frac{\mathrm{tr}_{K/K_r}}{p^r}$ — идемпотентный оператор на идеале $I = \mathfrak{M}^{\varkappa}$. Это дает нам утверждение предложения. •

**Следствие 2.4.2.** *Если* $h$ *делится на* $p$*, то любой идеал поля* $K$ *является разложимым* $\mathfrak{o}[G]$*-модулем.*

**Доказательство.** Доказательство очевидно, так как в этом случае $h = \frac{p^m e}{p-1}$ и $\overline{h} = 0$. •

**2.5.** Пусть, как и в п. 2.3, $K/k$ — циклическое вполне разветвленное расширение степени $p$, $G = \mathrm{Gal}(K/k)$, $h$ — скачок ветвления группы Галуа $G$.

**Предложение 2.5.** *Идеал $I = \mathfrak{M}^{\varkappa}$ поля $K$ разложим как $o[G]$-модуль тогда и только тогда, когда $p$ делит дифференту $\mathfrak{D}$ расширения $K/k$, и при этом*

$$p \mid \varkappa \quad \text{или} \quad \overline{\varkappa} > \overline{h}. \tag{19}$$

**Доказательство.** Согласно следствию 2.1.3 из предложения 2.1.2, можно считать, что $p \mid \mathfrak{D}$.

Если при этом для идеала $I = \mathfrak{M}^{\varkappa}$ выполнено одно из условий (19), то он разложим, согласно предложению 2.4.1.

Пусть $I = \mathfrak{M}^{\varkappa}$ — идеал в $K$, для которого $0 < \overline{\varkappa} < \overline{h}$. Перейдем к композит-модулю $\mathfrak{N} = \mathbb{Z}_p[\zeta_p]I$, степень которого будет $\varkappa$ в духе определения 2.3.1 (в случае $\zeta_p \in K$ $\mathfrak{N}$ равен $I$ и естественно имеет ту же степень). Этот композит-модуль будет неразложим из п. 2 предложения 2.3.3, а значит, и идеал неразложим. Предложение доказано. •

**Лемма 2.6.** *Пусть $K/k$ — конечное расширение и $F$ — промежуточное поле в нем. Пусть для идеала $I$ поля $K$ имеет место $o[G]$-разложение*

$$I = \mathfrak{A} \bigoplus \mathfrak{B}. \tag{20}$$

*Если $k\mathfrak{A}$, $k\mathfrak{B}$ являются $F$-модулями, то $\mathfrak{A}$, $\mathfrak{B}$ являются модулями над кольцом целых $o_F$ поля $F$.*

**Доказательство.** Пусть $x = a + b \in I$, $a \in \mathfrak{A}$, $b \in \mathfrak{B}$ и $\alpha \in o_F$. Тогда $\alpha x = \alpha a + \alpha b$ и при этом $\alpha a \in k\mathfrak{A}$, $\alpha b \in k\mathfrak{B}$. С другой стороны, $\alpha x \in I$, а значит, $\alpha x = a' + b'$, $a' \in \mathfrak{A} \subset k\mathfrak{A}$, $b' \in \mathfrak{B} \subset k\mathfrak{B}$, откуда $\alpha a = a' \in \mathfrak{A}$, $\alpha b = b' \in \mathfrak{B}$. Лемма доказана. •

## §3. Доказательство основной теоремы

**3.1.** Целью этого параграфа будет доказательство теоремы B Введения. При этом мы можем считать, что расширение $K/k$ вполне разветвлено (см. предложение 1.2) и, кроме того, в нем индекс ветвления $p^m$ делит дифференту $\mathfrak{D}$ (см. теорему A Введения). Поскольку при выполнении условий a) или b) теоремы B для данного идеала $I$ его разложимость была доказана в предложении 2.4.1, то остаток этого параграфа будет посвящен доказательству неразложимости идеала $I = \mathfrak{M}^{\varkappa}$ в оставшихся случаях. Итак, пусть $\varkappa = \varkappa_0 + \varkappa_1 p + \ldots$, $0 \leqslant \varkappa_i \leqslant p-1$, удовлетворяет условию

$$\begin{cases} 0 < \varkappa_0 \leqslant \overline{h}, \\ 0 \leqslant \varkappa_i \leqslant \overline{h}, \quad 1 \leqslant i \leqslant m-1. \end{cases} \tag{21}$$

Докажем индукцией по $m$, что идеал $I$ неразложим.

База индукции была доказана в предложении 2.5.1.

**3.2.** Пусть идеал $I$ в расширении $K/k$ разложим и выполнено индукционное предположение для расширений меньшей степени. Обозначим через $F$ подрасширение в $K/k$ такое, что $[K : F] = p$ (напомним, что наше расширение $K/k$ — циклическое, так как $p^m \mid \mathfrak{D}$).

**Лемма 3.2.1.** *Если для расширения $F/k$ теорема* B *выполнена, то поле $F$ лежит или в $k\mathfrak{A}$, или в $k\mathfrak{B}$.*

**Доказательство.** Из разложения $I = \mathfrak{A} \bigoplus \mathfrak{B}$ вытекают следующие два разложения:

$$I_1 = \mathfrak{A}_1 \bigoplus \mathfrak{B}_1,$$
$$I_2 = \mathfrak{A}_2 \bigoplus \mathfrak{B}_2,$$

где $I_1 = I \cap F$, $\mathfrak{A}_1 = \mathfrak{A} \cap F$, $\mathfrak{B}_1 = \mathfrak{B} \cap F$, $I_2 = \frac{\mathrm{tr}}{p} I$, $\mathfrak{A}_2 = \frac{\mathrm{tr}}{p}\mathfrak{A}$, $\mathfrak{B}_2 = \frac{\mathrm{tr}}{p}\mathfrak{B}$ (здесь $\mathrm{tr} = \mathrm{tr}_{K/F}$). Если степень идеала $I$ равна $\varkappa$, то степень идеала $I_1$ поле $F$ равна $[\frac{\varkappa}{p}] + 1$, а степень идеала $I_2$ равна $[\frac{\varkappa}{p}]$, так как $0 < \overline{\varkappa} \leqslant \overline{h}$ по условию (см. (18)).

Легко видеть, что одна из степеней обязательно удовлетворяет условию (21), и, значит, соответствующий идеал в расширении $F/k$ неразложим по индукционному предположению. Пусть для определенности это будет идеал $I_1$ и, например, $\mathfrak{B}_1 = \{0\}$, тогда $\mathfrak{A}_1 = I_1$ и, значит, $k\mathfrak{A}_1 = F$.

Ясно, что $k\mathfrak{A}_1 \subset k\mathfrak{A}$, и тем самым лемма доказана. •

**3.3.** Пусть $G = \mathrm{Gal}(K/k) = \langle\sigma\rangle$ — группа Галуа расширения $K/k$ с образующим автоморфизмом $\sigma$. Обозначим через $\tau$ степень $\sigma^{p^{m-1}}$. С расширением $K/k$ связываем расширение $K'/k'$, где $K' = K(\zeta_p)$, $k' = k(\zeta_p)$ (вообще говоря, штрихованные поля могут совпадать с нештрихованными). Через $v$ и $v'$ обозначим показатели в полях $K$ и $K'$ соответственно. Пусть $h$ — максимальный скачок ветвления группы $G$, который мы будем считать взаимно-простым с $p$ (если $p \mid h$, то см. следствие 2.4.2). Далее будем рассматривать следующие три случая:

I) $\zeta_{p^m} \in k$, и, таким образом, $K = k(\theta)$, где $\theta^{p^m} \in k$;

II) порядок $p$-кручения в мультипликативной группе поля $k'$ меньше $p^m$, т.е. $\zeta_{p^s} \in k'$, $\zeta_{p^{s+1}} \notin k'$ и $s < m$;

III) $\zeta_p \notin k$, но $\zeta_{p^m} \in k'$, и значит, $K' = k'(\theta)$, $\theta^{p^m} \in k'$.

**Замечание.** В случае I имеем $v(\theta) \equiv 0 \mod p$, а в случае III $v'(\theta) \equiv 0 \mod p^m$ (см. леммы 1.3.1, 1.3.2).

**3.4.** Рассмотрим сперва случай I. В этом случае $h = \frac{p^m e}{p-1} - 1$ и, значит, $\overline{h} = p - 1$. Тем самым в этом случае нам надо доказать следующее утверждение.

**Предложение 3.4.** *Идеал $I = \mathfrak{M}^{\varkappa}$ в поле $K$ разложим тогда и только тогда, когда $p \mid \varkappa$.*

**Доказательство.** Если $p \mid \varkappa$, то разложимость доказана в предложении 2.4.1.

Пусть теперь $p \nmid \varkappa$, но $I = \mathfrak{A} \bigoplus \mathfrak{B}$. Проводим индукцию по степени расширения $K/k$.

База индукции — предложение 2.5.1.

Индукционный переход. Пусть $K = k(\theta)$, $\theta^{p^m} \in k$. Тогда $v(\theta) \equiv 0 \mod p$.

Если идеал $I$ разложим и $p \nmid \varkappa$, то разложимыми будут также идеалы $I_i = I\theta^{-i} = \mathfrak{A}\theta^{-i} \bigoplus \mathfrak{B}\theta^{-i}$. При этом идеал $I_i$ имеет степень, меньшую степени идеала $I$ на число, кратное $p$, а значит, не кратную $p$.

Поэтому, согласно лемме 3.2.1, поле $F$ входит или в $k\mathfrak{A}\theta^{-i}$, или в $k\mathfrak{B}\theta^{-i}$ для каждого $i$. А это значит, что $F\theta^i$ входит либо в $k\mathfrak{A}$, либо в $k\mathfrak{B}$. Рассмотрев разложение $K$ в сумму $F\theta^i$, как в (9), мы получим, что $k\mathfrak{A}$, $k\mathfrak{B}$ — $F$-пространства, а значит, разложение $I = \mathfrak{A} \bigoplus \mathfrak{B}$ является разложением над кольцом $\mathfrak{o}_F$ (см. лемму 2.6.1), и мы приходим к базе индукции. Предложение доказано. •

**3.5.** Рассмотрим теперь случай II, когда порядок мультипликативного $p$-кручения в $k'$ меньше, чем $p^m$. Пусть $I = \mathfrak{A} \bigoplus \mathfrak{B}$ и для определенности поле $F$ входит в $k\mathfrak{A}$ (см. лемму 3.2.1).

В этом случае в разложении кругового многочлена

$$x^{p^m} - 1 = (x^{p^{m-1}} - 1)(1 + x^{p^{m-1}} + \cdots + x^{(p-1)p^{m-1}})$$

над полем $k$ на неприводимые множители все неприводимые делители $(1 + x^{p^{m-1}} + \cdots + x^{(p-1)p^{m-1}})$ будут многочленами от $x^p$. Таким образом, $k\mathfrak{B} = \operatorname{Ker} f(\sigma)$, где многочлен $f(x)$ — делитель $(1 + x^{p^{m-1}} + \cdots + x^{(p-1)p^{m-1}})$. Так как $f(x)$ — многочлен от $x^p$, то $k\mathfrak{B}$, а значит, и $k\mathfrak{A}$ являются $E[G]$-модулями, где $E/k$ — подрасширение, а $K/k$ такое, что $[E : k] = p$. Значит, разложение $I = \mathfrak{A} \bigoplus \mathfrak{B}$ будет разложением над $\mathfrak{o}_E$ (см. лемму 2.6.1), и мы можем применить индукционное предположение к расширению $K/E$.

**3.6.** Осталось рассмотреть последний случай

$$\zeta_p \notin k, \quad \zeta_{p^m} \in k' = k(\zeta_p).$$

Пусть $K' = k'(\theta)$, $\theta^{p^m} \in k'$, тогда будем считать $v'(\theta) = 0$ (см. лемму 1.3.2). Пусть $G = \operatorname{Gal}(K/k)$ с образующим автоморфизмом $\sigma$. Согласно предложению 1.2, можем считать, что расширения $K/k$ и $K'/k'$ вполне разветвлены. Возьмем промежуточное поле $F$ в расширении $K/k$ такое, что $[F : k] = p$, и пусть при этом $F' = F(\zeta_p)$. Обозначим через $h$ и $h'$ скачки ветвления расширений $F/k$ и $F'/k'$ соответственно, а через $e$, $e'$ — абсолютные индексы ветвления полей $k$ и $k'$. Наконец, пусть $d = [k' : k]$.

Докажем следующее утверждение.

**Предложение 3.6.** *Пусть $I$ — идеал в поле $K$ степени $\varkappa = \varkappa_0 + \varkappa_1 p + \cdots + \varkappa_{m-1}p^{m-1}$, $0 \leqslant \varkappa_i \leqslant p-1$. Если $0 \leqslant \varkappa_{m-1} \leqslant \overline{h}$, то любое $\mathfrak{o}[G]$-разложение идеала $I$ является разложением над кольцом целых $\mathfrak{o}_F$ поля $F$.*

**Доказательство.** Рассмотрим два случая.

1) $0 \leqslant \varkappa_{m-1} < \overline{h}$;

2) $0 < \varkappa_{m-1} \leqslant \overline{h}$.

Разберем сперва случай 1. Заметим, что расширение $k'/k$ и соответственно $K'/K$ мы можем считать вполне разветвленными. Действительно, если $k_1$ — подполе инерции в $k'/k$ с кольцом целых $\mathfrak{o}_1$, то если $I$ — идеал $K$, то $I\mathfrak{o}_1$ — идеал $K_1 = k_1 K$ той же степени, и достаточно доказать утверждение для него.

Итак, в дальнейшем будем считать, что

$$k'/k \text{ и } K'/K \text{ вполне разветвлены.} \tag{22}$$

Пусть у нас есть $\mathfrak{o}[G]$-разложение

$$I = \mathfrak{A} \bigoplus \mathfrak{B}. \tag{23}$$

Тогда мы получаем следующее разложение поля $K'$:

$$K' = k'I = k'\mathfrak{A} \bigoplus k'\mathfrak{B}. \tag{24}$$

Обозначим через $e_{\mathfrak{A}}$ проектор $K'$ на модуль $k'\mathfrak{A}$, который будет одновременно проектором идеала $I$ на слагаемое $\mathfrak{A}$ в силу разложения (23), при этом $e_{\mathfrak{A}} \in k[G]$.

Рассмотрим систему ортогональных идемпотентов в $k'[G]$:

$$e_i = (1 + \sigma^p \zeta^{pi} + \cdots + (\sigma^p \zeta^{pi})^{p^{m-1}-1})/p^{m-1}, \quad 0 \leqslant i < p^{m-1} - 1,$$

где $\zeta = \zeta_{p^m}$ — первообразный корень из 1 степени $p^m$. Нетрудно видеть, что

$$\operatorname{Im} e_i = \operatorname{Ker}(\zeta^p - \zeta^{-pi}) = F'\theta^{-i},$$

и поле $K'$ представляется в виде суммы

$$K' = \bigoplus_{i=0}^{p^{m-1}-1} \operatorname{Im} e_i = \bigoplus_{i=0}^{p^{m-1}-1} F'\theta^{-i}.$$

Если каждый $\operatorname{Im} e_i$ входит или в $k'\mathfrak{A}$, или в $k'\mathfrak{B}$, то разложение (24) происходит над полем $F'$, а значит, разложение (23) является $\mathfrak{o}_F$-модульным (см. лемму 2.6.1), и тем самым все доказано. •

Пусть для какого-то $i$ модуль $\operatorname{Im} e_i$ нетривиально раскладывается в пространствах $k'\mathfrak{A}$ и $k'\mathfrak{B}$. Фиксируем это $i$. Проектор $e_i$ раскладывается далее в сумму одномерных проекторов:

$$e_{ij} = (1 + \sigma\zeta^{i+p^{m-1}j} + \cdots + (\sigma\zeta^{i+p^{m-1}j})^{p^m-1})/p^m, \quad 0 \leqslant j \leqslant p-1.$$

Тогда часть их входит в $e_{\mathfrak{A}}$ в качестве слагаемых (так как $e_{\mathfrak{A}}$ — идемпотент, то его можно разложить в сумму неразложимых идемпотентов). Пусть это будут $e_{ij_1}, \ldots, e_{ij_r}$, и для определенности считаем, что $1 \leqslant j_1 < \cdots < j_r \leqslant p-1$ (иначе перейдем к проектору на второе слагаемое). Обозначим

$$e_{i\gamma} = \bigoplus_{\alpha=1}^{r} e_{ij_\alpha}, \quad \gamma = \{j_1, \ldots, j_r\}.$$

Ясно, что идемпотент $e_{i\gamma}$ ортогонален всем идемпотентам $e_{i'}$, $i' \neq i$. Отсюда следует, что если элемент $z \in \operatorname{Im} e_i = F'\theta^{-i}$, то

$$e_{\mathfrak{A}}(z) = e_{i\gamma}(z). \tag{25}$$

Пусть $x$ — элемент поля $F$ с нормированием $\overline{h}$. Докажем, что для элемента $y = x\theta^{-i}$ имеет место

$$v'(e_{i\gamma}(x\theta^{-i})) = 0. \tag{26}$$

Будем считать $\zeta_p = \zeta^{p^{m-1}}$, а $\tau = \sigma \mod \sigma^p$ — образующий группы Галуа $F/k$. Нетрудно видеть, что для $i \in \{0, 1, \ldots, p-1\}$ имеем

$$e_{ij}(x\theta^{-i}) = f_j(x)\theta^{-i},$$

где $f_j = (1 + \tau\zeta_p{}^j + \cdots + (\tau\zeta_p{}^j)^{p-1})/p$ — идемпотент в $k'[G/\langle\sigma^p\rangle]$. Тогда

$$e_{i\gamma}(x\theta^{-i}) = f_\gamma(x)\theta^{-i}, \tag{27}$$

где $f_\gamma = \sum_{\alpha=1}^{r} f_{j_\alpha}$. Разложим $f_\gamma$ по степеням $\tau - 1$ так же, как и в доказательстве предложения 2.1.2. Тогда мы получим, что

$$f_\gamma = \sum_{\alpha=1}^{p-2} b_\alpha(\tau-1)^\alpha + \frac{b_{p-1}}{p}(\tau-1)^{p-1},$$

где $b_\alpha \in (\zeta_p - 1)^{-\alpha}\mathbb{Z}_p$, $1 \leqslant \alpha \leqslant p-2$, $b_{p-1} \in \mathbb{Z}[\zeta_p]^*$ (см. (10)). Так же, как и в доказательстве предложения 2.3.3, получаем, что

$$v_0'(f_\gamma(x)) = v_0'\left(\frac{b_{p-1}}{p}(\tau-1)^{p-1}(x)\right)$$

(см. (17)), где $v'_0$ — нормирование в поле $F'$. Напомним, что по нашему выбору

$$v'_0(x) = d\overline{h},$$

где $d = [k' : k]$.

Значит,

$$v'_0(f_\gamma(x)) = v'_0(x) + (p-1)dh - pde = d((p-1)h + \overline{h} - pe). \tag{28}$$

По условию в нашем расширении $K/k$ индекс ветвления делит дифференту, а значит, по предложению 1.1

$$h - \left[\frac{h}{p}\right] = e,$$

т.е. $(p-1)h + \overline{h} = pe$. Отсюда и из (28) немедленно следует, что

$$v'_0(f_\gamma(x)) = 0,$$

а значит, учитывая (27), получаем (26).

Рассмотрим теперь элемент

$$y = \mathrm{tr}_{K'/K}(x\theta^{-i}).$$

Заметим, что $x \in K$, а расширение $K'/K$, по нашему предположению (см. (22)), вполне разветвлено и не имеет высшего ветвления, поэтому, $\mathrm{tr}_{K'/K}\theta^{-i}$ будет единицей в поле $K$, а значит,

$$v(y) = p^{m-1}v_0(x) = p^{m-1}\overline{h}$$

(здесь $v_0$ — показатель в поле $F$). Пусть $g$ — образующий группы Галуа $K'/K$ степени $d$. Тогда имеем

$$e_{\mathfrak{A}}(y) = e_{\mathfrak{A}}\left(\sum_{\alpha=0}^{d-1} g^\alpha(x\theta^{-i})\right) = \sum_{\alpha=0}^{d-1}(e_{\mathfrak{A}}(g^\alpha(x\theta^{-i}))$$
$$= \sum_{\alpha=0}^{d-1} g^\alpha(e_{\mathfrak{A}}(x\theta^{-i})) = \mathrm{tr}_{K'/K}(e_{\mathfrak{A}}(x\theta^{-i}))$$

(мы воспользовались тем, что $\sigma$ коммутирует с $g$). Элемент $x\theta^{-i}$ принадлежит $F'\theta^{-i}$, а значит, $e_{\mathfrak{A}}(x\theta^{-i}) = e_{i\gamma}(x\theta^{-i})$ (см. (25)), и поэтому из (26) получаем, что $e_{\mathfrak{A}}(x\theta^{-i})$ — единица поля $K'$. Учитывая опять, что расширение $K'/K$ вполне разветвлено и не имеет высшего ветвления, получаем, что элемент $e_{\mathfrak{A}}(y)$ — единица в поле $K$.

Итак, мы нашли элемент $y$ с нормированием $p^{m-1}\overline{h}$ в поле $K$ такой, что $e_{\mathfrak{A}}(y)$ является единицей поля $K$. По условию в степени $\varkappa$ идеала $I$ коэффициент $\varkappa_{m-1}$ строго меньше, чем $\overline{h}$, а значит, $\varkappa < p^{m-1}\overline{h} = v(y)$, т.е. $y \in I$.

Но из разложения (23) следует, что для любого $z \in I$ должно быть выполнено $e_{\mathfrak{A}}(z) \in I$, что в нашем случае противоречит $v(e_{\mathfrak{A}}(y)) = 0$. Случай 1 предложения 3.6.1 полностью доказан. •

**3.7.** Докажем теперь случай 2 предложения 3.6.1. Для этого рассмотрим композит-модуль $\mathfrak{N}$ в поле $K'$ и пусть $\mathfrak{N} = \mathfrak{A} \bigoplus \mathfrak{B}$ — его разложение. Пусть $e_{\mathfrak{A}}$ — проектор $\mathfrak{N}$ на $\mathfrak{A}$ и

$$e_i = (1 + \tau\zeta^i + \cdots + (\tau\zeta^i)^{p-1})/p$$

— одномерный идемпотент (здесь $\tau = \sigma^{p^{m-1}}$, $\zeta = \zeta_p$).

**Лемма 3.7.1.** *Если есть разложение $\mathfrak{N} = \mathfrak{A} \bigoplus \mathfrak{B}$, т.е. разложение*

$$e_i(\mathfrak{N}) = e_i(\mathfrak{A}) \bigoplus e_i(\mathfrak{B}). \tag{29}$$

**Доказательство.** Идемпотенты $e_i$ и $e_{\mathfrak{A}}$ коммутируют, поэтому

$$e_{\mathfrak{A}}(e_i(\mathfrak{N})) = e_i(e_{\mathfrak{A}}(\mathfrak{N})) = e_i(\mathfrak{N}).$$

Таким образом, $e_{\mathfrak{A}}$ — проектор $e_i(\mathfrak{N})$ на $e_i(\mathfrak{A})$, откуда следует утверждение леммы. •

Ясно, что $e_i(\mathfrak{N}) \subset \mathrm{Ker}(\tau - \zeta^{-i}) = F\theta^{-i}$. Поэтому можно записать

$$e_i(\mathfrak{A}) = \mathfrak{N}_i\theta^{-i}, \quad e_i(\mathfrak{A}) = \mathfrak{A}_i\theta^{-i}, \quad e_i(\mathfrak{B}) = \mathfrak{B}_i\theta^{-i},$$

где $\mathfrak{N}_i, \mathfrak{A}_i, \mathfrak{B}_i \subset F'$. Из разложения (29), таким образом, получаем разложение

$$\mathfrak{N}_i = \mathfrak{A}_i \bigoplus \mathfrak{B}_i. \tag{30}$$

**Лемма 3.7.2.** *$\mathfrak{N}_i$ — композит-модуль, и* (30) *— его разложение как композит-модуля.*

**Доказательство.** Ясно, что $\mathfrak{N}_i$ — $G$-модуль. Далее, для любого элемента $\alpha \in F$ и $x \in K'$ имеем $e_i(\alpha x) = \alpha e_i(x)$. Отсюда получаем, что $\mathfrak{N}$ — $\mathfrak{o}_F\mathbb{Z}_p[\zeta_p]$-модуль, а значит, композит-модуль.

Если теперь $a\theta^{-i} \in e_i(\mathfrak{A})$, то $a\theta^{-i} = e_i(a')$ при некотором $a' \in \mathfrak{N}$, значит, $\alpha a\theta^{-i} = \alpha e_i(a') = e_i(\alpha a')$ для $\alpha \in \mathbb{Z}_p[\zeta_p]$, при этом $\alpha a' \in \mathfrak{N}$, так как $\mathfrak{N}$ — $\mathbb{Z}_p[\zeta_p]$-модуль. Таким образом, $\alpha a\theta^{-i}$ — образ элемента из $\mathfrak{N}$, т.е. $\alpha a\theta^{-i} \in \mathfrak{A}_i\theta^{-i}$, а тогда $\alpha a \in \mathfrak{A}_i$. Лемма доказана. •

Без ограничения общности последующего утверждения будем считать, что степень композит-модуля $\mathfrak{N}$ существует (так как нам нужен $\mathfrak{N}$, получившийся из идеала) и имеет вид

$$\varkappa = \varkappa_0 + \varkappa_1 + \cdots + \varkappa_{m-1}p^{m-1}, \quad 0 \leqslant \varkappa_i \leqslant p-1.$$

**Лемма 3.7.3.** *Пусть $\mathfrak{N}$ — композит-модуль степени $\varkappa = \varkappa_0 + \varkappa_1 + \cdots + \varkappa_{m-1}p^{m-1}$. Если $0 < \varkappa_{m-1} \leqslant \overline{h}$, то разложение* (30) *является разложением над $\mathfrak{o}_F\mathbb{Z}_p[\zeta_p]$.*

**Доказательство.** Индукция по $m$.

База — предложение 2.3.3.

Индукционный переход.

Рассмотрим идемпотент $e_i$ и его образ $e_i\mathfrak{N} = \mathfrak{N}_i\theta^{-i}$. Мы уже проверили, что $\mathfrak{N}_i$ — композит-модуль в поле $F$ (лемма 3.7.2). Проверим, что его степень равна

$$\deg \mathfrak{N}_i = d\frac{t-\overline{h}}{p} = d\left[\frac{\varkappa}{p}\right], \tag{31}$$

где $t = \varkappa + \overline{h - \varkappa}$.

Действительно, пусть $x$ с $\mathfrak{N}$ нормированием $d\varkappa$, тогда, умножив его на $\pi^{\overline{h-x}}$, где $\pi$ — простой элемент кольца $\mathfrak{o}_K$, получим элемент $y \in \mathfrak{N}$ с нормированием

$$v'(y) = dt.$$

Поэтому $v'(y) \equiv h' \mod p$ и, согласно лемме 1.4.3,

$$v'(e_i(y)) = v'(y) - d\overline{h} = d(t - \overline{h}).$$

Поскольку элемент $y' = y\theta^i$ принадлежит $\mathfrak{N}_i$ и $v'(\theta) = 0$, то мы нашли в композит-модуле $\mathfrak{N}_i$ элемент с нормированием $d\frac{t-\overline{h}}{p}$.

Осталось проверить, что в композит-модуле $\mathfrak{N}_i$ нет элементов с нормированием, меньшим или равным $d(\frac{t-\overline{h}}{p} - 1)$.

Для этого возьмем произвольный элемент $z \in \mathfrak{N}$. По условию

$$v'(z) > d(\varkappa - 1).$$

Применяя лемму 1.4.3, получим

$$\begin{aligned} v'(e_i(z)) &\geqslant v'(z) - d\overline{h} > d(\varkappa - 1 - \overline{h}) \\ &= d(t - \overline{h} - (\overline{h - \varkappa} + 1)) \geqslant d(t - \overline{h} - p). \end{aligned}$$

Это означает, что элемент $z' = z\theta^i$ из $\mathfrak{N}_i$ имеет нормирование большее, чем $d(\frac{t-\overline{h}}{p} - 1)$. Итак, мы доказали (31).

Поэтому композит-модуль $\mathfrak{N}_i$ удовлетворяет условию предложения, а значит, по предположению индукции его разложение (30) является разложением над кольцом $\mathfrak{o}_F\mathbb{Z}_p[\zeta_p]$.

Ясно, что $k\mathfrak{A}_i\theta^{-i} \subset k\mathfrak{A}$, $k\mathfrak{B}_i\theta^{-i} \subset k\mathfrak{B}$, и при этом по выше сказанному они являются $F$-пространствами, значит, пространства $k\mathfrak{A}, k\mathfrak{B}$ также являются векторными пространствами над $F$. Применяя лемму 2.6.1, получаем, что разложение (30) определено над $\mathfrak{o}_F\mathbb{Z}_p[\zeta_p]$. Лемма доказана. •

**3.8.** Доказательство случая 2 предложения 3.6.1. Итак, пусть $I$ — идеал в поле $K$ степени $\varkappa = \varkappa_0 + \varkappa_1 p + \cdots + \varkappa_{m-1}p^{m-1}$, и при этом $0 < \varkappa_{m-1} \leqslant \overline{h}$. Перейдем из идеала $I$ к композит-модулю $\mathfrak{N} = \mathbb{Z}_p[\zeta_p]I$. Ясно, что $\deg \mathfrak{N} = \varkappa$, и при этом $\mathfrak{N}$ удовлетворяет условию леммы 3.7.3, согласно которой его разложение $\mathfrak{N} = \mathbb{Z}_p[\zeta_p]\mathfrak{A} \bigoplus \mathbb{Z}_p[\zeta_p]\mathfrak{B}$, где $I = \mathfrak{A} \bigoplus \mathfrak{B}$, является разложением над кольцом $o_F\mathbb{Z}_p[\zeta_p]$. Предложение 3.6.1 полностью доказано.

**3.9.** Доказательство неразложимости идеалов в теореме B Введения для случая $\zeta_p \notin k$, $\zeta_{p^m} \in k' = k(\zeta_p)$, где $p^m = [K : k]$.

Итак, пусть $I$ — идеал в поле $K$, степень которого $\varkappa = \varkappa_0 + \varkappa_1 p + \cdots + \varkappa_{m-1}p^{m-1}$ удовлетворяет условию $0 < \varkappa_o \leqslant \overline{h}$, $0 \leqslant \varkappa_i \leqslant \overline{h}$ для $1 \leqslant i \leqslant m-1$, и пусть

$$I = \mathfrak{A} \bigoplus \mathfrak{B} \tag{32}$$

— его $o[G]$-разложение.

Доказательство проводим индукцией по $m$. Для $m = 1$ см. предложение 2.5.1. Если $m > 1$, то разложение (32), согласно предложению 2.6.1, является также разложением для расширения $K/F$ степени $p^{m-1}$, где $[F : k] = p$. К последнему расширению применяем индукционное предположение и получаем, что разложение (32) тривиально.

Теорема B Введения полностью доказана.

## Список литературы


[BVZ] Бондарко М. В., Востоков С. В., Жуков И. Б., *Аддитивные модули Галуа в полных дискретно нормированных полях*, Алгебра и анализ **9** (1997), № 4, 28–46.

[BF] Боревич З. И., Фаддеев Д. К., *Теория гомологий в группах*. II. *О проективных резольвентах конечных групп*, Вестн. Ленингр. ун-та. Сер. мат. мех. астроном. **1959**, вып. 2, 72–87.

[BV] Боревич З. И., Востоков С. В., *Кольцо целых элементов расширения простой степени локального поля как модуль Галуа*, Зап. науч. семин. ЛОМИ **31** (1973), 24–37.

[By] Byott N., *On Galois isomorphisms between ideals in extensions of local fields*, Manuscripta Math. **73** (1991), 289–311.

[E] Elder G. G., *Galois module structure of ideals in wildly ramified cyclic extensions of degree $p^2$*, Ann. Inst. Fourier (Grenoble) **45** (1995), no. 3, 625–647.

[EM] Elder G. G., Madan M. L., *Galois module structure of the integers in weakly ramified extensions*, Arch. Math. (Basel) **64** (1995), 117–120.

[FV] Fesenko I., Vostokov S., *Local fields and their extensions: A constructive approach*, Transl. Math. Monogr., vol. 121, Amer. Math. Soc., Providence, RI, 1993.

[L] Leopoldt H.-W., *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. **201** (1959), 119–149.

[Le] Lettl G., *Note on the Galois module structure of quadratic extensions*, Colloq. Math. **67** (1994), no. 1, 15–19.

[M1] Miyata Y., *On the module structure of the ring of all integers of a $\mathfrak{p}$-adic number field*, Nagoya Math. J. **54** (1974), 53–59.

[M2] Miyata Y., *On the module in a cyclic extension over a* $\mathfrak{p}$*-adic number field*, Nagoya Math. J. **73** (1979), 61–68.

[M3] Miyata Y., *On the module structure of a* $p$*-extension over a* $\mathfrak{p}$*-adic number field*, Nagoya Math. J. **77** (1980), 13–23.

[M4] Miyata Y., *Vertices of ideals of a* $\mathfrak{p}$*-adic number field*, Illinois J. Math. **31** (1987), no. 2, 185–199.

[M5] Miyata Y., *On the Galois module structure of ideals and rings of all integers of* $\mathfrak{p}$*-adic number fields*, J. Algebra **177** (1995), 627–646.

[N] Noether E., *Normalbasis bei Körpern ohne höhere Verzweigung*, J. Reine Angew. Math. **167** (1932), 147–152.

[Se] Serre J.-P., *Local fields*, Grad. Texts in Math., vol. 67, Springer-Verlag, New York–Heidelberg, 1979.

[T] Taylor M. J., *Formal groups and the Galois module structure of local rings of integers*, J. Reine Angew. Math. **358** (1985), 97–103.

[U] Ullom S., *Integral normal bases in Galois extensions of local fields*, Nagoya Math. J. **39** (1970), 141–148.

[V1] Востоков С. В., *Идеалы абелева* $p$*-расширения иррегулярного локального поля как модули Галуа*, Зап. науч. семин. ЛОМИ **46** (1974), 14–35.

[V2] Востоков С. В., *Идеалы абелева* $p$*-расширения локального поля как модули Галуа*, Зап. науч. семин. ЛОМИ **57** (1976), 64–84.

[V3] Востоков С. В., *Кольцо целых элементов поля алгебраических чисел как модуль Галуа*, Зап. науч. семин. ЛОМИ **71** (1977), 80–84.

[V4] Востоков С. В., *Нормальный базис идеала локального поля*, Зап. науч. семин. ЛОМИ **64** (1976), 64–68.

Поступило 26 января 1998 г.