M. V. Bondarko, S. V. Vostokov, Additive Galois modules in Dedekind rings. Decomposability,
Algebra i Analiz, 1999, Volume 11, Issue 6, 103–121

Алгебра и анализ
Том 11 (1999), вып. 6

АДДИТИВНЫЕ МОДУЛИ ГАЛУА ДЕДЕКИНДОВЫХ КОЛЕЦ. РАЗЛОЖИМОСТЬ

© М. В. Бондарко, С. В. Востоков

Находятся необходимые и достаточные условия наличия разложимых как модулей Галуа идеалов в абелевых расширениях полей частных дедекиндовых колец нулевой характеристики.

Введение

Настоящая работа является продолжением работ [BVZ, BV1, BV2], в которых рассматривалась проблема разложимости идеалов в абелевых p-расширениях полного дискретно-нормированного поля нулевой характеристики (см. также [BV, V1, V2, M1, M2, M3] для обычного локального поля), и работы [BLV], в которой изучалась та же проблема в абелевых p-расширениях дедекиндовых колец. Мы рассматриваем теперь общий случай абелевых расширений.

Сформулируем сперва результат локальной ситуации, на который мы будем опираться. Пусть K/k — абелево p-расширение полного дискретно-нормированного поля характеристики 0 с полем вычетов характеристики $p > 2$ и группой Галуа G. Пусть T — подполе инерции в K/k. Мы предполагаем, что соответствующее расширение полей вычетов сепарабельно. Пусть $\mathfrak{o}$ и $\mathfrak{O}_K$ — кольца целых полей k и K соответственно и $\mathfrak{M}$ — максимальный идеал в кольце $\mathfrak{O}_K$. Пусть, наконец, p^m — индекс ветвления расширения K/k, а e — абсолютный индекс ветвления поля k.

Теорема A (слабая форма). *В поле K существуют дробные идеалы, разложимые как $\mathfrak{o}[G]$-модули, в том и только в том случае, когда p^m, $m > 1$, делит дифференту $\mathfrak{D}_{K/k}$ этого расширения* [BVZ, теорема 1].

Теорема A′ (сильная форма). *Идеал $\mathfrak{M}^{\varkappa}$ разложим как $\mathfrak{o}[G]$-модуль в том и только в том случае, если выполнены два условия*:

a) $p^m \mid \mathfrak{D}_{K/k}$;

b) *или $K = K_1(\sqrt[p]{\pi_{K_1}})$, где π_{K_1} — униформизующий элемент подрасширения K_1 в K/k такого, что $[K : K_1] = p$, или в p-адическом разложении $\varkappa = \varkappa_0 +$*

Работа поддержана РФФИ, грант № 97-01-00058-а.

$\varkappa_1 p + \ldots$, $0 \leqslant \varkappa_i \leqslant p-1$, *либо* $\varkappa_0 = 0$, *либо существует* $\varkappa_i$, $0 \leqslant i \leqslant m-1$, *такой, что* $\varkappa_i > \bar{e}$, *где* $\bar{e} \equiv e \mod (p-1)$, $1 \le \bar{e} \le p-1$ [BV1, теорема A].

Замечание. Условие $p^m \mid \mathfrak{D}_{K/k}$ равносильно тому, что расширение K/T является циклическим со скачками ветвления h_i, удовлетворяющими условию

$$h_i - \left[\frac{h_i}{p}\right] = p^{i-1} e$$

(см. [BVZ], предложение 1.5).

Основной результат этой работы формулируется следующим образом. Пусть $\mathfrak{o}$ — дедекиндово кольцо нулевой характеристики с полем отношений k. Пусть K/k — абелево расширение нечетной степени с группой Галуа G. Мы предполагаем, что расширения соответствующих полей вычетов сепарабельны. Пусть $\mathfrak{O}_K$ — целое замыкание кольца в K и $\mathfrak{D}_{K/k}$ — дифферента расширения K/k.

Теорема B. *В K/k существуют G-инвариантные идеалы, разложимые как $\mathfrak{o}[G]$-модули, тогда и только тогда, когда существует подрасширение F в K/k, $F \neq K$, такое, что степень $[K:F]$ делит дифференту $\mathfrak{D}_{K/F}$ этого подрасширения.*

В §1 работы даются основные определения, в частности композит-модулей, играющих важную роль в доказательстве теоремы B (см. п. 1.1), и доказываются некоторые вспомогательные результаты, связанные с разложениями композит-модулей. В следующем параграфе мы доказываем, что разложение любого композит-модуля должно происходить над кольцом целых подполя разложения простого идеала, делящего n. Наконец, в §3, дано доказательство основного результата.

§1. Вспомогательные результаты и определения

1.1. Пусть K/k — абелево расширение, $n = [K:k]$, $G = \mathrm{Gal}(K/k)$. Пусть, далее, S — порядок в некотором конечном расширении k, являющийся $\mathfrak{o}$-алгеброй. Рассмотрим тензорное произведение колец $K \otimes_\mathfrak{o} S$, на котором введена структура $S[G]$-модуля, полагая действие группы G на S тривиальным. Заметим, что $K \otimes_\mathfrak{o} S$ является kS свободным kS-модулем ранга n, а значит, не имеет kS-кручения и, кроме того,

$$K \otimes_\mathfrak{o} S \approx K \otimes_\mathfrak{o} kS.$$

Определение 1. Композит-модулем $\mathfrak{N}$ в $K \otimes_\mathfrak{o} S$ будем называть полный $\mathfrak{O}_K \otimes_\mathfrak{o} S[G]$-подмодуль $K \otimes_\mathfrak{o} S$, лежащий в $a\mathfrak{O}_K \otimes_\mathfrak{o} S$, где a — некоторый элемент k.

Замечание 1.1.1. Для наших дальнейших целей достаточно, чтобы $\mathfrak{N}$ лежал в локализации $\mathfrak{O}_K \otimes_\mathfrak{o} S$ по всем элементам, взаимно-простым с n, умноженной на степень n (отрицательную).

Определение 2. Говорим, что композит-модуль $\mathfrak{N}$ разложим, если $\mathfrak{N} = \mathfrak{A} \oplus \mathfrak{B}$, где $\mathfrak{A}$ и $\mathfrak{B}$ — нетривиальные $S[G]$-подмодули $\mathfrak{N}$.

Определение 3. Пусть C — модуль и A — его подмодуль. Отображение $P_A : C \to A$ назовем проектором, если сужение P_A на A является тождественным отображением.

Замечание 1.1.2. Если C равно $A \oplus B$, то можно взять в качестве P_A каноническую проекцию $A \oplus B$ на первое слагаемое. Очевидно, если $P_A : C \to A$ и $\operatorname{Ker} P_A(C) = B$, то $C = A \oplus B$. Поэтому проектор однозначно задается своим ядром и образом.

Лемма 1.1.3. *Пусть K/k — абелево расширение, $G = \operatorname{Gal}(K/k)$ и $\mathfrak{N}$ — композит-модуль над $\mathfrak{O}_K \otimes_o S$. Пусть $\mathfrak{N} = \mathfrak{A} \oplus \mathfrak{B}$ — $S[G]$-разложение и $P_\mathfrak{A}$ — проектор $\mathfrak{N}$ на $\mathfrak{A}$. Тогда $P_\mathfrak{A}$ равен ограничению на $\mathfrak{N}$ некоторого идемпотента из $kS[G]$.*

Доказательство. Вложим $P_\mathfrak{A}$ в $kS[G]$. Для этого возьмем элемент $x \in K \cap \mathfrak{N}$, образующий нормальный базис K/k. Тогда $x = y + z$, где $y \in \mathfrak{A}$, $z \in \mathfrak{B}$. Существует единственный элемент $P \in kS[G]$ такой, что $P(x) = y$. Действительно, $y = \sum a_\sigma \sigma(x)$, так как элементы $\sigma(x)$ образуют базис K/k. Тогда в качестве P берем $\sum a_\sigma \sigma$.

Докажем теперь, что $P = P_\mathfrak{A}$. Действительно, любой элемент $c \in \mathfrak{N}$ раскладывается $c = a + b$, $a \in \mathfrak{A}$, $b \in \mathfrak{B}$, при этом c представляется как $f(x)$, где $f \in kS[G]$, как и выше. Поэтому

$$c = f(x) = f(y + z) = f(y) + f(z).$$

Ясно, что $f(y) \in k\mathfrak{A}$, $f(z) \in k\mathfrak{B}$ и $c \in k\mathfrak{N}$. Из единственности разложения в $\mathfrak{N} = \mathfrak{A} \oplus \mathfrak{B}$ следует, что

$$a = f(y) = f(P(x)) = P(f(x)) = P(c)$$

(мы воспользовались тем, что G — абелева группа и, значит, $fP = Pf$). Таким образом, P — проектор $\mathfrak{N}$ на $\mathfrak{A}$, и поэтому $P = P_\mathfrak{A}$. •

1.2. Пусть F — промежуточное поле в расширении K/k и $\mathfrak{N}$ — композит-модуль в $K \otimes_o S$ над $\mathfrak{O}_K \otimes_o S$ (см. определение 1).

Лемма 1.2. *Пусть $\mathfrak{N} = \mathfrak{A} \oplus \mathfrak{B}$ — $S[G]$-разложение композит-модуля $\mathfrak{N}$. Если соответствующее разложение пространств $k\mathfrak{N} = k\mathfrak{A} \oplus k\mathfrak{B}$ будет $F \otimes_o S[G]$-разложением, то $\mathfrak{N} = \mathfrak{A} \oplus \mathfrak{B}$ будет разложением над $o_F \otimes_o S$.*

Доказательство. Пусть $c \in \mathfrak{N}$ и $c = a + b$, где $a \in \mathfrak{A}$, $b \in \mathfrak{B}$. Тогда для элемента $\alpha \in o_F \otimes_o S$ имеем $\alpha c = \alpha a + \alpha b$, где $\alpha a \in k\mathfrak{A}$, так как $\alpha \in o_F \otimes_o S$ и $k\mathfrak{N} = k\mathfrak{A} \oplus k\mathfrak{B}$ является $o_F \otimes_o S$-разложением.

С другой стороны, $a \in \mathfrak{A} \subset \mathfrak{N}$, $\alpha \in o_F \otimes_o S \subset \mathfrak{O}_K \otimes_o S$. Поэтому $\alpha a \in \mathfrak{N}$, так как $\mathfrak{N}$ является $\mathfrak{O}_K \otimes_o S$-модулем. Наконец, $\mathfrak{A} = \mathfrak{N} \cap k\mathfrak{A}$, $\mathfrak{B} = \mathfrak{N} \cap k\mathfrak{B}$, что завершает доказательство. •

1.3. Замена S на большую алгебру. Пусть S' — S-алгебра (с единицей), являющаяся порядком в некотором конечном расширении kS. Пусть $\mathfrak{N}$ — композит-модуль в $K\otimes_o S$. Тогда вложение $S\to S'$ дает нам возможность вложить $\mathfrak{N}$ в композит-модуль в $K\otimes_o S'$. Ясно, что $S[G]$-разложение $\mathfrak{N}=\mathfrak{A}\oplus\mathfrak{B}$ индуцирует $S'[G]$-разложение

$$\mathfrak{N}'=\mathfrak{A}'\oplus\mathfrak{B}', \tag{1}$$

где $\mathfrak{A}'=\mathfrak{A}S'$, $\mathfrak{B}'=\mathfrak{B}S'$.

Лемма 1.3. *Если разложение* (1) *тривиально, то и исходное разложение было тоже тривиальным.*

Доказательство очевидно.

1.4. Пусть мы находимся в условиях п. 1.1. Пусть $\widehat{G}(G)\subset S$, где $\widehat{G}$ — группа характеров G. Тогда произвольный элемент t из $K\otimes_o S$ можно записать в виде

$$t=\frac{1}{n}\sum_{\chi\in\widehat{G}}\Bigl(\sum_{\sigma\in G}\chi(\sigma)^{-1}\sigma(t)\Bigr). \tag{2}$$

Для доказательства достаточно подсчитать коэффициент a_σ при $\sigma(t)$ в двойной сумме:

$$a_\sigma=\sum_{\chi\in\widehat{G}}\chi(\sigma)^{-1}=\begin{cases}0, & \text{если } \sigma\neq 1,\\ n=\#G, & \text{если } \sigma=1.\end{cases}$$

Обозначим внутреннюю сумму через p_χ, т.е.

$$p_\chi=\sum_{\sigma\in G}\chi(\sigma)^{-1}\sigma.$$

Лемма 1.4.1. *Для любых $\chi\in\widehat{G}$, $\sigma\in G$ имеет место*

$$\sigma p_\chi(t)=\chi(\sigma)p_\chi(t)$$

(непосредственная проверка).

Лемма 1.4.2. *Пусть $f\in kS[G]$, $f=\sum a_\sigma\sigma$, $a_\sigma\in kS$. Тогда*

$$p_\chi(f)=p_\chi\sum a_\sigma\chi(\sigma).$$

Доказательство. Имеем

$$p_\chi(f)=p_\chi\Bigl(\sum a_\sigma\sigma\Bigr)=\sum a_\sigma\sigma p_\chi=p_\chi\sum a_\sigma\chi(\sigma).$$

Мы применили лемму 1.4.1 и абелевость группы G. •

Лемма 1.4.3. *Элемент p_χ/n, где $n = [K : k] = \#G$, является идемпотентом в $kS[G]$.*

Доказательство. В лемме 1.4.2 в качестве элемента f возьмем

$$p_\chi = \sum a_\sigma \sigma.$$

По определению p_χ имеем $p_\chi = \sum_{\sigma \in G} \chi(\sigma)^{-1}\sigma$, поэтому $a_\sigma = \chi(\sigma)^{-1}$. Отсюда и из леммы 1.4.2 получаем

$$p_\chi(p_\chi) = p_\chi \sum a_\sigma \chi(\sigma) = p_\chi \sum \chi(\sigma)^{-1}\chi(\sigma) = p_\chi \sum_\sigma 1 = np_\chi. \quad \bullet$$

1.5. Модуль R_χ. Определим kS-модуль R_χ как

$$R_\chi = \{a \in K \otimes_o S \mid \sigma(a) = \chi(\sigma)a, \sigma \in G\}.$$

R_χ действительно является kS-модулем, так как если $\lambda = \alpha\beta$, $\alpha \in k, \beta \in S$ и $a = \sum x_i \otimes y_i$, то $\alpha a = \sum \alpha x_i \otimes \beta y_i \in K \otimes_o S$, и при этом $\sigma(\lambda a) = \lambda\sigma(a) = \chi(\sigma)\lambda a$, так как на kS операторы из G действуют тривиально.

Лемма 1.5.1. $R_\chi = p_\chi(K \otimes_o S)$.

Доказательство. Проверим сперва, что $p_\chi(K \otimes_o S) \subset R_\chi$. Действительно, если $x \in p_\chi(K \otimes_o S)$, то $x = p_\chi(t)$, где $t \in K \otimes_o S$. Элемент x принадлежит $K \otimes_o S$, и при этом, согласно лемме 1.4.1,

$$\sigma p_\chi(t) = \chi(\sigma)p_\chi(t).$$

Значит, $x \in R_\chi$.

Обратно, пусть $a \in K \otimes_o S$ и $\sigma(a) = a\chi(\sigma)$. Применим p_χ к элементу a:

$$p_\chi(a) = \sum_{\sigma \in G} \chi(\sigma)^{-1} a\chi(\sigma) = \sum_{\sigma \in G} a = na.$$

Таким образом $na \in p_\chi(K \otimes_o S)$, а поэтому и $a \in p_\chi(K \otimes_o S)$, так как $a = p_\chi(\frac{a}{n})$. $\bullet$

Лемма 1.5.2. $R_{\chi_1} R_{\chi_2} \subset R_{\chi_1\chi_2}$.

Замечание 1.5.3. Позже (см. следствие 1.5.9) будет доказано, что на самом деле имеет место равенство.

Доказательство леммы. Пусть $a \in R_{\chi_1}$, $b \in R_{\chi_2}$, тогда $\sigma(a) = a\chi_1(\sigma)$ и $\sigma(b) = b\chi_2(\sigma)$. Поэтому

$$\sigma(ab) = \sigma(a)\sigma(b) = \chi_1(\sigma)\chi_2(\sigma)ab = (\chi_1\chi_2)(\sigma)ab.$$

Значит, $ab \in R_{\chi_1\chi_2}$. $\bullet$

Следствие 1.5.4. $R_{\chi^n} \subset R_1$ *(здесь* 1 *— единичный характер).*

Действительно, $R_{\chi^n} \subset R_{\chi^n} = R_1$.

Лемма 1.5.5. $R_1 = kS$.

Доказательство. По определению $R_1 = (K \otimes_o S)^G$. Далее, $K \otimes_o S$ является свободным K-модулем ранга $d = [kS : k]$, образующими которого являются образующие поля kS над k, т.е.

$$K \otimes_o S = \left\{ \sum_{i=1}^{d} a_i x_i,\ a_i \in K,\ x_i \text{ — образующие } kS \text{ над } k \right\}.$$

Таким образом, в этом разложении σ действует на $\sum_{i=1}^{d} a_i x_i$ покомпонентно, а значит,

$$R_1 = \left\{ \sum_{i=1}^{d} a_i x_i,\ a_i \in k \right\} = kS. \quad \bullet$$

Заметим, что kS, а значит, и R_1 — поле.

Следствие 1.5.6. $R_{\chi^n} = kS$.

Действительно, согласно следствию 1.5.3 и лемме 1.5.4, имеем $R_{\chi^n} \subset R_1 = kS$. Но R_{χ^n} — ненулевой (так как в $K \otimes_o S$ нет нильпотентов) kS-модуль и kS — поле, значит, $R_{\chi^n} = kS$.

Лемма 1.5.7. R_χ *— одномерный* kS*-модуль для любого характера* χ *из* $\widehat{G}$.

Доказательство. Так как $R_{\chi^n} = kS$, то в R_χ есть обратимый элемент a. Легко видеть, что $a^{-1} \in R_{\chi^{-1}}$. Тогда из

$$R_\chi R_{\chi^{-1}} \subset R_1$$

следует, что $R_\chi \subset akS$, а так как R_χ — kS-модуль, то $R_\chi = akS$. $\bullet$

Следствие 1.5.8. *Все отличные от нуля элементы* R_χ *обратимы.*

Действительно, если $R_\chi = akS$, то каждый элемент $x \in R_\chi$ представляется в виде az, $z \in kS$, а тогда элемент $a^{-1}z^{-1}$ будет обратным к нему.

Следствие 1.5.9. $R_{\chi_1} R_{\chi_2} = R_{\chi_1\chi_2}$.

Действительно, согласно лемме 1.5.2, $R_{\chi_1} R_{\chi_2} \subset R_{\chi_1\chi_2}$, и при этом справа стоит одномерный kS-модуль.

Лемма 1.5.10. *Пусть $x \in R_\chi$, $\chi \in \widehat{G}$. Тогда для любого $\chi' \in \widehat{G}$ имеем $xR_{\chi'} = R_{\chi\chi'}$.*

Доказательство. Было доказано, что $R_{\chi'} = \langle a \rangle$ — одномерный kS-модуль. Поэтому

$$xR_{\chi'} = \langle xa \rangle.$$

По лемме 1.5.2 имеем $R_\chi R_{\chi'} \subset R_{\chi\chi'}$, откуда $xR_{\chi'} \subset R_{\chi\chi'}$. Тогда и из одномерности $xR_{\chi'} = R_{\chi\chi'}$. •

Лемма 1.5.11. $K \otimes_0 S = \bigoplus\limits_{\chi \in \widehat{G}} R_\chi$.

Доказательство. По определению все $R_\chi \subset K \otimes_0 S$; далее, для любого $t \in K \otimes_0 S$ имеем (см. (2)):

$$t = \frac{1}{n} \sum_{\chi \in \widehat{G}} p_\chi(t), \tag{3}$$

при этом, согласно лемме 1.5.1, $p_\chi(t)$ лежит в R_χ. Далее, мы знаем, что $K \otimes_0 S$ — n-мерный kS-модуль и из (3) следует, что R_χ порождают $K \otimes_0 S$ (как группу по сложению). Так как $\sum \dim R_\chi = \dim K \otimes_0 S$, то $K \otimes_0 S$ является прямой суммой R_χ. •

1.6. Разложение $K \otimes_0 S$ над подрасширениями. Пусть F — подрасширение в K/k такое, что $\mathrm{Gal}(K/F) = H$, $[F : k] = m$. Обозначим через j естественный эпиморфизм

$$j : \widehat{G} \to \widehat{H}$$

и определим для каждого $\psi \in \widehat{H}$ модуль Q_ψ следующим образом:

$$Q_\psi = \bigoplus_{j(\chi)=\psi} R_\chi. \tag{4}$$

Лемма 1.6.1. *Для любого элемента $y \in F$ и любого $\chi \in \widehat{G}$ такого, что $j(\chi) \neq 1$, имеет место равенство $p_\chi(y) = 0$.*

Доказательство. Пусть $\sigma_1, \dots, \sigma_m$ — представители классов смежности G/H. Тогда

$$\begin{aligned} p_\chi(y) &= \sum_{\sigma \in \widehat{G}} \chi(\sigma)^{-1}\sigma(y) = \sum_{i=1}^{m} \sum_{\tau \in H} \chi(\sigma_i\tau)^{-1}(\sigma_i\tau)(y) \\ &= \sum_{i=1}^{m} \sum_{\tau \in H} \chi(\sigma_i)^{-1}\chi_i(\tau)^{-1}\sigma_i(y) = \sum_{i=1}^{m} \chi(\sigma_i)^{-1}\sigma_i(y) \sum_{\tau \in H} \chi(\tau)^{-1} = 0, \end{aligned}$$

так как $\sum_{\tau \in H} \chi(\tau)^{-1} = 0$, если $j(\chi) \neq 1_H$. •

Следствие 1.6.2. $F \otimes_o S = Q_1$.

Доказательство. Действительно, так как $p_\chi(F \otimes_o S) = 0$, $j(\chi) \neq 1_H$, то из разложения (2) получаем, что $F \otimes_o S \subset Q_1$. Так как $F \otimes_o S$ и Q_1 являются kS-модулями размерности m, то $F \otimes_o S = Q_1$. •

Лемма 1.6.3. *Пусть* $x \in R_\chi$, *где* $\chi \in \widehat{G}$. *Тогда*

$$xQ_1 = Q_{j(\chi)}.$$

Доказательство. По определению Q_1 (см. (4)) имеем $Q_1 = \bigoplus_{j(\chi')=1} R_{\chi'}$. Значит,

$$xQ_1 = x\left(\bigoplus_{j(\chi')=1} R_{\chi'}\right) = \bigoplus_{j(\chi')=1} xR_{\chi'},$$

и по лемме 1.5.5 имеем, далее,

$$\bigoplus_{j(\chi')=1} xR_{\chi'} = \bigoplus_{j(\chi')=1} R_{\chi'\chi} = \bigoplus_{j(\chi')=j(\chi)} R_{\chi'} = Q_{j(x)}. \quad \bullet$$

Следствие 1.6.4. $Q_{j(\chi)} = x(F \otimes_o S)$ *для* $x \in R_\chi \setminus \{0\}$.

Доказательство получается соединением следствия 1.6.2 и леммы 1.6.3. •

Пусть ψ_i пробегают все характеры группы H. Возьмем по одному прообразу χ_i из $\widehat{G}$, таким образом, $j(\chi_i) = \psi_i$, и возьмем, далее, $x_i \in R_{\chi_i} \subset K \otimes_o S$.

Лемма 1.6.5.

$$K \otimes_o S = \bigoplus_i x_i(F \otimes_o S). \tag{5}$$

Доказательство. Согласно лемме 1.5.11, имеем

$$K \otimes_o S = \bigoplus_{\chi \in \widehat{G}} R_\chi.$$

Группируем R_χ, чтобы получить по определению Q_{ψ_i}:

$$Q_{\psi_i} = \bigoplus_{j(\chi)=\psi_i} R_\chi.$$

Тогда

$$K \otimes_o S = \bigoplus_{\psi_i \in \widehat{H}} \left(\bigoplus_{j(\chi)=\psi_i} R_\chi\right) = \sum_{\psi_i \in \widehat{H}} Q_{\psi_i}.$$

Для каждого ψ_i возьмем один прообраз χ_i, т.е. $j(\chi_i) = \psi_i$ и $x_i \in R_{\chi_i}$, тогда, согласно следствию 1.6.4,

$$Q_{\psi_i} = Q_{j(\chi_i)} = x_i(F \otimes_o S),$$

и мы приходим к равенству (5). •

1.7. Пусть K/k — абелево расширение степени $n = p^r m$, $(m,p) = 1$, с группой Галуа G, тогда $G = G_p G_m$, где G_p — максимальная p-подгруппа в G, а G_m — подгруппа порядка m. Определим поле $K_p = K^{G_m}$. Пусть S_n — целое замыкание кольца $\mathfrak{o}$ в поле $k(\zeta_n)$, где ζ_n — первообразный корень из 1 степени n.

Ясно, что

$$\widehat{G} \approx \widehat{G}_p \times \widehat{G}_m.$$

Возьмем характеры χ_i из $\widehat{G}$, которые тривиальны на G_p, т.е. $\chi_i(\tau) = 1$ для всех $\tau \in G_p$, $1 \le i \le m$. Выберем по одному элементу z_i из модуля R_{χ_i} (см. п. 1.5).

Лемма 1.7. $K \otimes_{\mathfrak{o}} S_n = \bigoplus\limits_i z_i(K_p \otimes_{\mathfrak{o}} S_n)$.

Доказательство. Является частным случаем леммы 1.6.5, если положить F равным K_p. •

1.8. Полное дискретно-нормированное поле характеристики 0 с полем вычетов характеристики p является частным случаем дедекиндовой области характеристики 0, поэтому все определения и результаты п. 1.1–1.7 относятся и к этому случаю.

1.9.

Лемма 1.9.1. *Пусть K/k — нормальное расширение степени n. Следующие условия эквивалентны:*

a) $n = [K:k]$ *делит дифференту* $\mathfrak{D}_{K/k}$;

b) $\mathrm{tr}_{K/k}/n$ — *идемпотент на кольце* $\mathfrak{O}_K$;

c) n *делит* $\mathfrak{d}_{K/k} = \mathrm{tr}_{K/k}\,\mathfrak{O}_K$.

Доказательство.

a) $\Longleftrightarrow$ b). Пусть n делит $\mathfrak{D}_{K/k}$, тогда $\frac{1}{n}\mathrm{tr}_{K/k}\mathfrak{O}_K \subset \mathfrak{o}$, значит, $\mathrm{tr}_{K/k}/n$ — идемпотент на $\mathfrak{O}_K$.

Обратно, если $\mathrm{tr}_{K/k}/n$ — идемпотент на $\mathfrak{O}_K$, то идеал $\frac{1}{n}\mathfrak{O}_K$ удовлетворяет соотношению

$$\mathrm{tr}_{K/k}(\mathfrak{O}_K/n) \subset \mathfrak{o}.$$

Поэтому $\frac{1}{n}\mathfrak{O}_K \subset \mathfrak{D}^{-1}_{K/k}$, значит, $n \mid \mathfrak{D}_{K/k}$.

b) $\Longleftrightarrow$ c). Если $\mathrm{tr}_{K/k}/n$ — идемпотент на $\mathfrak{O}_K$, то получаем, что $\frac{\mathrm{tr}_{K/k}}{n}(\mathfrak{O}_K) \subset \mathfrak{o}$, т.е. $\frac{1}{n}\mathfrak{d}_{K/k} \subset \mathfrak{o}$, значит, n делит $\mathfrak{d}_{K/k}$.

Обратное очевидно. •

Лемма 1.9.2. *Следующие условия эквивалентны:*

a) $n = [K:k]$ *не делит дифференту* $\mathfrak{D}_{K/k}$;

b) *существует простое число* $p \mid n$ *и простой идеал* $\wp \mid (p)$ *в кольце* $\mathfrak{o}$, *который входит в* $\mathfrak{d}_{K/k} = tr_{K/k}\mathfrak{O}_K$ *в степени меньшей, чем в идеал* (n).

Доказательство. Условие a), согласно лемме 1.9.1, равносильно тому, что идеал (n) не делит $\mathfrak{d}_{K/k}$.

Пусть

$$\mathfrak{d}_{K/k} = \prod_{\wp} \wp^{a_\wp}, \quad (n) = \prod_{\wp} \wp^{b_\wp},$$

тогда $n \nmid \mathfrak{d}_{K/k} \iff$ существует $\wp$, для которого $a_\wp < b_\wp$. •

Пусть $\wp$ — простой идеал из п. b) леммы 1.9.2. Предположим, что $\wp$ не раскладывается в расширении K/k и вполне разветвлен в p-расширении K_p/k, где K_p — максимальное p-подрасширение в K/k. Тогда над $\wp$ есть только один простой идеал $\mathcal{P}$ в K. Обозначим через $\widetilde{k}$ и $\widetilde{K}$ соответствующие пополнения. Ясно, что при наших условиях $[K : k] = [\widetilde{K} : \widetilde{k}]$. Пусть $\widetilde{\mathfrak{o}}$ и $\widetilde{\mathfrak{O}}_{\widetilde{K}}$ — кольца целых в $\widetilde{k}$ и $\widetilde{K}$ соответственно и пусть $\widetilde{\wp}$ — максимальный идеал в кольце $\widetilde{\mathfrak{o}}$. Обозначим через $\mathfrak{D}_{\widetilde{K}/\widetilde{k}}$ дифференту расширения $\widetilde{K}/\widetilde{k}$, и пусть $\mathfrak{d}_{\widetilde{K}/\widetilde{k}} = \mathrm{tr}_{\widetilde{K}/\widetilde{k}} \widetilde{\mathfrak{O}}_{\widetilde{K}}$. Пусть, наконец, F — максимальное p-подрасширение в $\widetilde{K}/\widetilde{k}$, таким образом, $[F : \widetilde{k}] = p^r$.

Лемма 1.9.3. *Пусть $\widetilde{K}/\widetilde{k}$ — расширение степени n и $F/\widetilde{k}$ — максимальное p-подрасширение в нем степени p^r. Если выполнены условия леммы* 1.9.2, *то степень p^r не делит дифференту $\mathfrak{D}_{F/\widetilde{k}}$ расширения $F/\widetilde{k}$.*

Доказательство. Из условия b) следствия 1.9.2 получаем, что если $\mathfrak{d}_{\widetilde{K}/\widetilde{k}} = \wp^a$, $(n) = \wp^b$, то $a < b$. Ясно, что в локальной ситуации $(n) = (p^r)$, значит, $(p^r) = \wp^b$. С другой стороны, расширение $\widetilde{K}/F$ не имеет высшего ветвления, поэтому $\mathrm{tr}_{\widetilde{K}/F} \widetilde{\mathfrak{O}}_{\widetilde{K}} = \widetilde{\mathfrak{o}}_F$ и, значит,

$$\mathfrak{d}_{F/\widetilde{k}} = \mathfrak{d}_{\widetilde{K}/\widetilde{k}} = \wp^a.$$

Поскольку $a < b$, то p^r не делит $\mathfrak{d}_{F/\widetilde{k}}$. Отсюда, проводя такие же рассуждения, что и в лемме 1.9.1, получаем, что в расширении $F/\widetilde{k}$ степень не делит дифференту. Лемма доказана. •

§2. Поле разложения

2.1. Чтобы перейти к локальной ситуации, мы должны избавиться от поля разложения. Рассмотрим сперва случай циклического расширения степени p.

Лемма 2.1. *Пусть K/k — циклическое расширение степени p и простой идеал $\wp$ из k разлагается в K. Тогда для произвольного S любое $S[G]$-разложение композит-модуля $\mathfrak{N}$ в $K \otimes_{\mathfrak{o}} S$ тривиально.*

Доказательство. Пусть σ — образующий элемент группы Галуа $G = \mathrm{Gal}(K/k)$. Мы можем считать, что S содержит ζ_p, согласно лемме 1.4. Действительно, мы можем заменить алгебру S на $S[\zeta_p]$.

Пусть имеется $S[G]$-разложение $\mathfrak{N} = \mathfrak{A} \oplus \mathfrak{B}$ и P— соответствующий проектор $: \mathfrak{N} \to \mathfrak{A}$, который, согласно лемме 1.1.3, является идемпотентом на $\mathfrak{A}$ и лежит в $kS[G]$. Тогда P можно представить в виде суммы одномерных идемпотентов (т.е. проекторов на одномерные kS-пространства):

$$P = \bigoplus_{i \in I} e_i, \tag{6}$$

где $e_i = (1+\zeta_p^i\sigma+\dots+(\zeta_p^i\sigma)^{p-1})/p$, I — подмножество $[0,1,\dots,p-1]$. При этом если разложение $\mathfrak{N} = \mathfrak{A} + \mathfrak{B}$ нетривиально, то

$$r = \#I \not\equiv 0 \mod p. \tag{7}$$

Из (6) следует, что P лежит в $k'[G]$, где $k' = k(\zeta_p)$. Поэтому P является идемпотентом на композит-модуле

$$\mathfrak{N}' = \mathfrak{o}_{k'}\mathfrak{N} \cap (K \otimes_{\mathfrak{o}} k');$$

из нетривиального разложения $\mathfrak{N} = \mathfrak{A} \oplus \mathfrak{B}$ мы получаем нетривиальное $\mathfrak{o}_{k'}[G]$-разложение $\mathfrak{N}' = \mathfrak{A}' + \mathfrak{B}'$, где $\mathfrak{A}' = \mathfrak{o}_{k'}\mathfrak{A} \cap (K \otimes_{\mathfrak{o}} k')$, $\mathfrak{B}' = \mathfrak{o}_{k'}\mathfrak{B} \cap (K \otimes_{\mathfrak{o}} k')$. Можем считать с этого места, что $S = \mathfrak{o}_{k'}$. Вложим $\mathfrak{N}' \subset K \otimes_{\mathfrak{o}} k'$ в поле $K' = K(\zeta_p)$ (мы можем это сделать потому, что $[k' : k] \mid p-1$, а значит, $([k' : k], [K : k]) = 1$). Тогда получим нетривиальное $\mathfrak{O}_K[\zeta_p][G]$-разложение $\mathfrak{O}_K[\zeta_p][G]$-подмодуля N' в K' над $\mathfrak{o}_{k'}[G]$.

Пусть $\wp$ представим в K в виде

$$\wp = \wp_o\wp_1 \dots \wp_{p-1},$$

где $\wp_i$ — простые идеалы в K, и пусть каждый $\wp_i$ представим в виде

$$\wp_i = \prod \wp_{ij}, \quad j \geq 0,$$

где $\wp_{ij}$ — простые идеалы в K'. Из того, что идеал (p) равен $(\zeta_p - 1)^{p-1}$, следует, что показатели $\zeta_p - 1$ по всем идеалам $\wp_{ij}$ положительны.

Пусть $\varkappa = \min\limits_{z \in \mathfrak{N}} v_{ij}(z)$, где v_{ij} — нормирование, соответствующее идеалу $\wp_{ij}$. Перенумерацией $\wp_{ij}$ можно добиться того, чтобы этот минимум достигался бы на $i = j = 0$ и при этом

$$\sigma^i(\wp_0) = \wp_i, \qquad \sigma^i(\wp_{0j}) = \wp_{ij}. \tag{8}$$

Обозначим z, при котором достигается минимум, через x. Согласно аппроксимационной теореме, найдется элемент $w \in \mathfrak{O}$, для которого $v_0(w) = 0$ и $v_i(w) > 0$ при $i \geq 1$. Тогда элемент $y = wx$, с одной стороны, лежит в $\mathfrak{N}'$, так как $\mathfrak{N}'$ является $\mathfrak{O}_K$-модулем, а с другой стороны, удовлетворяет условию: $v_{00}(y) = \varkappa$, $v_{i0}(y) > \varkappa$ для $i \geq 1$. Поэтому $v_{00}(\sigma^i(y)) > \varkappa$ при $i \geq 1$, так как $v_{00}(\sigma^i(y)) = v_{p-i\ 0}(y) > \varkappa$, согласно (8). Отсюда следует, что

$$v_{00}(\mathrm{tr}_{K/k}(y)) = v_{00}(y + \sigma(y) + \dots + \sigma^{p-1}(y)) = v_{00}(y) = \varkappa. \tag{9}$$

Кроме того, из определения идемпотента e_i получаем

$$e_i(y) = \frac{\mathrm{tr}}{p}(y) + \frac{\zeta_p - 1}{p}\Big(\sum a_i g^i(y)\Big),$$

где $a_i = (\zeta_p^i - 1)/(\zeta_p - 1) \in S = \mathfrak{o}_{k'}$. Отсюда следует, что

$$P(y) = \frac{r}{p}\,\mathrm{tr}_{K/k}(y) + \sum_{j=1}^{p-1} b_i\sigma^i(y),$$

где $b_i \in \frac{(\zeta_p-1)}{p}\mathfrak{o}_{k'}$. Заметим, далее, что $y \in \mathfrak{N}'$ и P — идемпотент на $\mathfrak{N}'$, значит,

$$P(y) \in \mathfrak{N}'. \tag{10}$$

По доказанному (см. (9)):

$$v_{00}\Big(\frac{r}{p}\operatorname{tr}_{K/k}(y)\Big) = \varkappa - v_{00}(p),$$

так как $(r,p) = 1$ (см. (7)). Кроме того,

$$\begin{aligned} v_{00}(b_i\sigma^i(y)) &\geq v_{00}(\zeta_p - 1) - v_{00}(p) + v_{00}(\sigma^i(y)) \\ &> \varkappa - v_{00}(p) + v(\zeta_p - 1) > \varkappa - v_{00}(p) = v_{00}\Big(\frac{r}{p}\operatorname{tr}_{K/k}(y)\Big). \end{aligned}$$

Значит,

$$v_{00}(P(y)) = v_{00}\Big(\frac{r}{p}\operatorname{tr}_{K/k}(y)\Big) = \varkappa - v_{00}(p) < \varkappa.$$

Поэтому $P(y) \notin \mathfrak{N}'$, что противоречит (10). Лемма доказана. •

2.2. Пусть K/k — произвольное p-расширение и F — промежуточное подполе, $[F : k] = p$; пусть $H = \operatorname{Gal}(K/F)$ и $\widehat{H} = \{\psi_i\}$. Как и в лемме 1.6.5, выберем по одному представителю из группы характеров $\widehat{G}$ так, что

$$j(\chi_i) = \psi_i$$

при эпиморфизме $j : \widehat{G} \to \widehat{H}$. Возьмем, далее, $x_i \in R_{\chi_i}$ (см. п. 1.5). Тогда, согласно лемме 1.6.5, имеем

$$K \otimes_{\mathfrak{o}} S = \bigoplus_i x_i(F \otimes_{\mathfrak{o}} S).$$

Рассмотрим для $S[G]$-разложения композит-модуля следующие модули:

$$\begin{aligned} \mathfrak{N}_i &= x_i^{-1}\mathfrak{N} \cap (F \otimes_{\mathfrak{o}} S), \\ \mathfrak{A}_i &= x_i^{-1}\mathfrak{A} \cap (F \otimes_{\mathfrak{o}} S), \\ \mathfrak{B}_i &= x_i^{-1}\mathfrak{B} \cap (F \otimes_{\mathfrak{o}} S). \end{aligned}$$

Лемма 2.2.1. *Модуль $\mathfrak{N}_i$ является композит-модулем над $\mathfrak{o}_F \otimes_{\mathfrak{o}} S$ в $F \otimes_{\mathfrak{o}} S$, и при этом $\mathfrak{N}_i = \mathfrak{A}_i \oplus \mathfrak{B}_i$ является его $S[G]$-разложением.*

Доказательство. Ясно, что $x_i^{-1}\mathfrak{N}$ и $F \otimes_{\mathfrak{o}} S$ являются $\mathfrak{o}_F \otimes_{\mathfrak{o}} S$-модулями, поэтому и $\mathfrak{N}_i$ — $\mathfrak{o}_F \otimes_{\mathfrak{o}} S$-модуль. Далее, $\sigma(x_i^{-1}) \in x_i^{-1}S$, так как $\sigma(x_i^{-1}) = \chi_i^{-1}(\sigma)x_i^{-1}$ (см. определение R_χ в п. 1.5). Значит, $\sigma(x_i^{-1}\mathfrak{N}) \subset x_i\mathfrak{N}$, так как $\chi_i^{-1}(\sigma) \in S$ и $\mathfrak{N}$ — S-модуль. Таким образом, мы проверили, что $\mathfrak{N}_i$ является G-модулем.

Теперь проверим, что $\mathfrak{N}_i$ — подмодуль в $b\mathfrak{O}_K \otimes_{\mathfrak{o}} S$ при некотором $b \in k$.

Из определения композит-модуля существует такое $a \in k$, что $\mathfrak{N} \subset a\mathfrak{O}_K \otimes_{\mathfrak{o}} S$. Мы можем делить a на элементы $\mathfrak{o}$, поэтому будем считать, что $a^{-1} \in \mathfrak{o}$. Мы знаем, что $x_i\mathfrak{N}_i$ лежит в $a\mathfrak{O}_K \otimes_o S$, а значит, $\mathfrak{N}_i$ лежит в $x_i^{-1}a\mathfrak{O}_K \otimes_o S$. Поделив x_i^{-1} на некоторый элемент из $\mathfrak{o}$, мы получим, что $\mathfrak{N}_i$ лежит в $y^{-1}\mathfrak{O}_K \otimes_o S$, где $y \in \mathfrak{O}_K \otimes_o S$. Рассмотрим естественное отображение нормы N из $K \otimes_o S$, рассматриваемой, как k-алгебра, в k. Так как $y \in \mathfrak{O}_K \otimes_o S$, то характеристический многочлен y в $K \otimes_o S$, как в k-алгебре, имеет целые коэффициенты, а тогда существует такой многочлен $f \in \mathfrak{o}[x]$, что $N(y) = yf(y)$. Тогда получаем, что $N(y)$ делит y в $\mathfrak{O}_K \otimes_o S$, а значит, $\mathfrak{N}_i$ лежит в $N(y)^{-1}\mathfrak{O}_K \otimes_o S$. Так как $\mathfrak{N}_i \in F \otimes_o S$, то $\mathfrak{N}_i \subset N(y)^{-1}\mathfrak{o}_F \otimes_o S$.

Модули $\mathfrak{A}$ и $\mathfrak{B}$ являются $S[G]$-модулями, кроме того, $\sigma(x_i^{-1}) = \chi_i(\sigma)^{-1}x_i^{-1}$ для любого $\sigma \in G$. Осталось заметить, что $\chi_i(\sigma)^{-1} \in S$, откуда получаем, что $\mathfrak{A}_i$ и $\mathfrak{B}_i$ — $S[G]$-модули, и, значит, разложение $\mathfrak{N}_i = \mathfrak{A}_i \oplus \mathfrak{B}_i$ является $S[G]$-разложением композит-модуля $\mathfrak{N}_i$. •

Предложение 2.2.2. *Пусть K/k — p-расширение. Пусть для простого дивизора $\wp$ из k существует подрасширение F в K/k, $[F : k] = p$, в котором $\wp$ полностью разложим. Тогда любое $S[G]$-разложение композит-модуля $\mathfrak{N}$ из $K \otimes_o S$ является разложением над $\mathfrak{o}_F$, где $\mathfrak{o}_F$ — целое замыкание кольца $\mathfrak{o}$ в F.*

Доказательство. Рассмотрим композит-модули $\mathfrak{N}_i$ из леммы 2.2.1 и соответствующие им $S[G]$-разложения $\mathfrak{N}_i = \mathfrak{A}_i \oplus \mathfrak{B}_i$.

Согласно лемме 2.1, все эти разложения тривиальны, поэтому $k\mathfrak{A} = \bigoplus k\mathfrak{A}_i$ и $k\mathfrak{B} = \bigoplus k\mathfrak{B}_i$ являются F-модулями и, значит, согласно лемме 1.3, $\mathfrak{A}$ и $\mathfrak{B}$ являются $\mathfrak{o}_F$-модулями. Предложение доказано. •

Замечание 2.2.3. Таким образом, мы можем считать с этого момента, что в максимальном p-подрасширении K/k любой простой делитель $\wp$ числа p не имеет нетривиального разложения на простые сомножители.

2.3. Проверим теперь утверждение для локальной ситуации, сходное с предложением 2.2.2.

Пусть K/k — абелево p-расширение с группой Галуа G полного дискретно-нормированного поля характеристики 0. Мы предполагаем, что соответствующее расширение полей вычетов характеристики p является сепарабельным. Пусть $k_m = k(\zeta_m)$, $(m,p) = 1$ и $\mathfrak{o}_m$ — кольцо целых поля k_m.

Рассмотрим композит-модуль $\mathfrak{N}$ из $F \otimes_o \mathfrak{o}_m$ над $\mathfrak{o}_F \otimes_o \mathfrak{o}_m$ (напомним, что по определению композит-модуля группа G действует тривиально на $\mathfrak{o}_m$). Пусть T — подполе инерции в расширении K/k.

Предложение 2.3. *Любое $\mathfrak{o}_m[G]$-разложение $\mathfrak{N} = \mathfrak{A} \oplus \mathfrak{B}$ композит-модуля $\mathfrak{N}$ является разложением над $\mathfrak{o}_T$.*

Доказательство.

1. Пусть $[K : k] = p$ и $T = K$. В этом случае снова, как в п. 2.1, можно сделать $S = \mathfrak{o}_{k'}$, и тогда $(p, [kS : k]) = 1$. Мы имеем $\mathfrak{O}_T \otimes_o S = \mathfrak{o}_{k'}\mathfrak{O}_T = \mathfrak{o}_{Tk'}$, так как расширение T/k неразветвлено. Значит, $\mathfrak{N}$ — идеал в композите полей $k'K = Tk'$. Тем самым получили разложение над $\mathfrak{o}_{k'}[G]$ идеала в неразветвленном расширении Kk'/k' степени p. Это расширение сепарабельно по условию, и,

значит, любой идеал в K изоморфен неразложимому групповому кольцу $\mathfrak{o}_{k'}[G]$, т.е. разложение $\mathfrak{N} = \mathfrak{A} \oplus \mathfrak{B}$ тривиально и предложение в этом случае доказано.

2. Пусть теперь K/k — произвольное абелево p-расширение. Действуем далее точно так же, как и в доказательстве предложения 2.2.2, взяв в качестве базы индукции вместо леммы 2.1 результат доказанного п. 1 и используя, согласно замечанию 1.8, все необходимые результаты из п. 1.1–1.7. Предложение доказано. •

§3. Доказательство теоремы

3.1. Пусть K/k — абелево расширение нечетной степени n, для которого не выполнено условие теоремы B, т.е. не существует промежуточного подрасширения K/F, $K \neq F$ такого, что $[K : F]$ делит дифференту $\mathfrak{D}_{K/F}$. Пусть тем не менее нашелся G-инвариантный идеал в K, для которого имеет место нетривиальное $\mathfrak{o}[G]$-разложение

$$I = \mathfrak{A} \oplus \mathfrak{B}. \tag{11}$$

Мы считаем при этом, что выполнено следующее условие.

$$\left.\begin{array}{l}\text{Если } E \text{ — промежуточное поле в } K/k \text{ такое, что разложение}\\ \mathfrak{N} = \mathfrak{A} \oplus \mathfrak{B} \text{ будет } \mathfrak{o}_E(\mathrm{Gal}(K/E))\text{-разложением, то } E = k.\end{array}\right\} \quad (*)$$

Мы можем так считать, так как если $(*)$ не выполнено и найдется промежуточное поле $E \neq k$ такое, что $I = \mathfrak{A} \oplus \mathfrak{B}$ — $\mathfrak{o}_E[\mathrm{Gal}(K/E)]$-разложение, то расширение K/k можно заменить на K/E. Действительно, в этом случае достаточно доказывать утверждение для него.

3.2. Поскольку при нашем условии степень n не делит дифференту $\mathfrak{D}_{K/k}$, то, согласно лемме 1.9.2, найдется простой делитель p числа n и простой идеал $\wp$ в кольце $\mathfrak{o}$, делящий p, который входит в $\mathfrak{d}_{K/k} = \mathrm{tr}_{K/k}\, \mathfrak{D}_K$ в степени меньшей, чем в идеал (n).

С этого момента мы фиксируем число p и простой идеал $\wp$. Пусть при этом $n = p^r m$, $(m, p) = 1$.

3.3. Пусть G_p — максимальная p-подгруппа в G, тогда $G = G_p \times G_m$, где G_m — подгруппа порядка m. Пусть $K_p = K^{G_m}$ — поле неподвижных относительно группы G_m элементов K, тогда $G_p \approx \mathrm{Gal}(K_p/k)$. Возьмем S_n равным целому замыканию кольца $\mathfrak{o}$ в поле $k(\zeta_n)$.

Ясно, что группа характеров $\widehat{G}$ изоморфна $\widehat{G}_p \times \widehat{G}_m$. Возьмем те характеры χ_i, $t \leqslant i \leqslant m$ из $\widehat{G}$, которые тривиальны на G_p, т.е. $\chi_i \in \widehat{G}$, $\chi_i(\tau) = 1$ для любого $\tau \in G_p$. Выберем по одному элементу z_i из R_{χ_i} (см. п. 1.5), тогда

$$z_i \in K \otimes_{\mathfrak{o}} S_n, \quad \sigma(z_i) = \chi(\sigma) z_i. \tag{12}$$

Мы имеем разложение

$$K \otimes_{\mathfrak{o}} S_n = \bigoplus_{i=1}^{m} z_i (K_p \otimes_{\mathfrak{o}} S_n)$$

(см. лемму 1.7).

Для композит-модуля $\mathfrak{N} = I \otimes_{\mathfrak{o}} S_n$ в $K \otimes_{\mathfrak{o}} S_n$ из $\mathfrak{o}[G]$-разложения (11) получаем $S_n[G]$-разложение

$$\mathfrak{N} = \mathfrak{A}' \oplus \mathfrak{B}', \tag{13}$$

где $\mathfrak{A}' = \mathfrak{A} \otimes_{\mathfrak{o}} S_n$, $\mathfrak{B}' = \mathfrak{B} \otimes_{\mathfrak{o}} S_n$. Заметим при этом, что если разложение (11) было нетривиальным, то и разложение (13) будет тоже нетривиальным, и наоборот. Тогда для модулей

$$\begin{aligned} \mathfrak{N}_i &= x_i^{-1}\mathfrak{N} \cap (K_p \otimes_{\mathfrak{o}} S_n), \\ \mathfrak{A}_i &= x_i^{-1}\mathfrak{A} \cap (K_p \otimes_{\mathfrak{o}} S_n), \\ \mathfrak{B}_i &= x_i^{-1}\mathfrak{B} \cap (K_p \otimes_{\mathfrak{o}} S_n) \end{aligned}$$

имеем равенства

$$\mathfrak{N}_i = \mathfrak{A}_i \oplus \mathfrak{B}_i, \quad 1 \le i \le m. \tag{14}$$

Доказательство точно такое, что и в лемме 2.2.1.

Пусть

$$P_i : \mathfrak{N}_i \to \mathfrak{A}_i, \quad P_i \in kS_n[G],$$

— соответствующие проекторы.

Лемма 3.3.1. *$P_i \in kS_m[G]$, где S_m — целое замыкание кольца $\mathfrak{o}$ в поле $k(\zeta_m)$.*

Доказательство. Проектор P, соответствующий разложению идеала $I = \mathfrak{A} \oplus \mathfrak{B}$, принадлежит кольцу $k[G]$, так как является идемпотентом этого кольца (см. лемму 1.1.3). Пусть

$$P = \sum_{\sigma \in G} a_\sigma \sigma, \quad a_\sigma \in k. \tag{15}$$

Рассмотрим

$$P_i = \sum_{\tau \in G_p} \left(\sum_{\sigma \in G,\ \sigma = \tau \mod G_m} \chi_i(\sigma) a_\sigma \right) \tau$$

и докажем, что $P_i : \mathfrak{N}_i \to \mathfrak{A}_i$ — проектор.

По определению z_i (см. (12)) имеем $\sigma(z_i)^{-1} = \chi_i^{-1}(\sigma) z_i^{-1}$, и при этом $\chi_i^{-1}(\sigma) \in S_n$. Таким образом, из разложения (13) мы получаем $S_n[G]$-разложение

$$z_i^{-1}\mathfrak{N} = z_i^{-1}\mathfrak{A}' \oplus z_i^{-1}\mathfrak{B}',$$

причем если разложение (13) нетривиально, то и полученное разложение нетривиально.

Ясно, что

$$P_i' = \sum_{\sigma \in G} a_\sigma \chi_i(\sigma) \sigma. \tag{16}$$

Действительно, из (15) и определения z_i (см (12)) следует, что для $x \in \mathfrak{N}$ выполнено

$$\begin{aligned} P_i'(z_i^{-1}x) &= \sum_\sigma a_\sigma \chi_i(\sigma)\sigma(z_i^{-1}x) = \sum_\sigma a_\sigma \chi_i(\sigma)\sigma(z_i^{-1})\sigma(x) \\ &= \sum_\sigma a_\sigma \chi_i(\sigma)\chi_i^{-1}(\sigma) z_i^{-1}\sigma(x) = z_i^{-1}\sum_\sigma a_\sigma\sigma(x) = z_i^{-1}P(x) \\ &= z_i^{-1}a, \end{aligned}$$

где $a \in \mathfrak{A}$.

Проверим теперь, что

$$P_i = P_i'|_{K_p \otimes_o S_n}. \tag{17}$$

Пусть $z \in K_p \otimes_o S_n$, тогда из (16) получаем

$$\begin{aligned} P_i'(z) &= \sum_{\sigma\in G} a_\sigma \chi_i(\sigma)\sigma(z) = \sum_{\tau\in G_p}\Bigl(\sum_{\sigma\equiv\tau \mod G_m} a_\sigma\chi_i(\sigma)\sigma(z)\Bigr) \\ &= \sum_{\tau\in G_p}\Bigl(\sum_{\sigma\equiv\tau \mod G_m} a_\sigma\chi_i(\sigma)\Bigr)\tau(z) = P_i(z). \end{aligned} \tag{18}$$

Отсюда следует (17). Кроме того, так как в последнем равенстве $\sigma \equiv \tau \mod G_m$ и $\chi_i(\tau) = 1$ для всех $\tau \in G_p$, то $\chi_i(\sigma) \in k(\zeta_m)$, т.е. $\chi_i(\sigma) \in k(\zeta_m)$ для всех $\sigma \in G$. Таким образом, равенство (17) доказывает нашу лемму.

Следствие 3.3.2. *Оператор P_i переводит $K_p \otimes_o S_m$ в себя (непосредственно выводится из леммы* 3.3.1).

Пересечем модули $\mathfrak{N}_i, \mathfrak{A}_i$ и $\mathfrak{B}_i$ с $K_p \otimes_o S_m$:

$$\begin{aligned} \mathfrak{N}_i^{(m)} &= \mathfrak{N}_i \cap (K_p \otimes_o S_m), \\ \mathfrak{A}_i^{(m)} &= \mathfrak{A}_i \cap (K_p \otimes_o S_m), \\ \mathfrak{B}_i^{(m)} &= \mathfrak{B}_i \cap (K_p \otimes_o S_m). \end{aligned}$$

Лемма 3.3.3. *$\mathfrak{N}^{(m)}$ — композит-модуль в $K_p \otimes_o S_m$ и $\mathfrak{N}_i^{(m)} = \mathfrak{A}_i^{(m)} \oplus \mathfrak{B}_i^{(m)}$ — его $S_m[G]$-разложение.*

Доказательство проходит так же, как в лемме 2.2.1.

Замечание 3.3.4. Проектор $P_i \in kS_m[G_p]$ будет проектором $\mathfrak{N}_i^{(m)} \to \mathfrak{A}_i^{(m)}$.

3.4. Переходим теперь к пополнению полей k и K_p. Отметим, что, согласно замечанию 2.2.3, мы можем считать, что любой простой идеал $\wp$, делящий p, имеет единственный лежащий над ним простой идеал $\mathcal{P}$ в K_p. Пусть $\widetilde{k}$ и $\widetilde{K}_p$— пополнения полей k и K_p по $\wp$ и $\mathcal{P}$ соответственно. Пусть $k_m = \widetilde{k}(\zeta_m)$ и $\mathfrak{o}_m$ — кольцо целых в k_m. Так как $(m,p) = 1$, то K_m/k — неразветвленное расширение, и поэтому, если $\mathfrak{o}_{\mathcal{P}}$ — кольцо целых в $\widetilde{K}_p$, то композит колец $\mathfrak{o}_m\mathfrak{o}_{\mathcal{P}}$ совпадает с кольцом целых композита полей $k_m\widetilde{K}_p$. Рассмотрим естественные отображения модулей $f : K_p \otimes_{\mathfrak{o}} S_m \to \widetilde{K}_p \otimes_{\mathfrak{o}} \mathfrak{o}_m$ и $g : \widetilde{K}_p \otimes_{\mathfrak{o}} \mathfrak{o}_m \to \widetilde{K}_p \otimes_{\widetilde{\mathfrak{o}}} \mathfrak{o}_m$ и рассмотрим $gf(\mathfrak{N}_i^{(m)})$. Возьмем теперь модуль $\mathfrak{N}_i' = \widetilde{\mathfrak{o}}gf(\mathfrak{N}_i^{(m)})$, являющийся пополнением $gf(\mathfrak{N}_i^{(m)})$ в $\widetilde{K}_p \otimes_{\widetilde{\mathfrak{o}}} \mathfrak{o}_m$, рассмотрим его как композит-модуль над $\mathfrak{o}_{\mathcal{P}} \otimes_{\widetilde{\mathfrak{o}}} \mathfrak{o}_m[G_p]$ (здесь $\widetilde{\mathfrak{o}}$ — кольцо целых поля $\widetilde{k}$).

Так как отображения f, g являются G-модульными, то проектор P_i из $kS_m[G_p]$, рассматриваемый как элемент групповой алгебры, является идемпотентом на $gf(\mathfrak{N}_i^{(m)})$. Ясно, что P_i действует на $\widetilde{K}_p \otimes_{\widetilde{\mathfrak{o}}} \mathfrak{o}_m$ непрерывно, и поэтому его действие на $gf(\mathfrak{N}_i^{(m)})$ продолжается до действия на $\mathfrak{N}_i'$ и P_i будет на $\mathfrak{N}_i'$ идемпотентом. Кроме того, если $P \neq 0, \mathrm{id}$ на $\mathfrak{N}_i^{(m)}$, то P_i, $1 - P_i$ будут нетождественными проекторами и на $\mathfrak{N}_i'$.

Лемма 3.4.1. *Модуль $\mathfrak{N}_i'$ является локальным композит-модулем над $\mathfrak{o}_{\mathcal{P}} \otimes_{\widetilde{\mathfrak{o}}} \mathfrak{o}_m[G_p]$, и при этом если $P_i \neq 0, \mathrm{id}$, то разложение*

$$\mathfrak{N}_i' = \mathfrak{A}_i' \oplus \mathfrak{B}_i', \tag{19}$$

где $\mathfrak{A}_i' = P_i(\mathfrak{N}_i')$, $\mathfrak{B}_i'$— дополнение, будет нетривиальным $\mathfrak{o}_m[G_p]$-разложением.

Доказательство. Как и в лемме 2.2.1, проверяем, что $\mathfrak{N}'$ — композит-модуль в $\widetilde{K}_p \otimes_{\widetilde{\mathfrak{o}}} \mathfrak{o}_m$ и разложение (19) будет $\widetilde{\mathfrak{o}}[G_p]$-разложением. Проверим, что это разложение будет над $\mathfrak{o}_m$. Действительно, если $\alpha \in \mathfrak{o}_m$, $x \in \mathfrak{N}_i^{(m)}$ и

$$\alpha P_i(x) = \sum_\sigma \alpha a_\sigma \sigma(x) = \sum_\sigma a_\sigma \sigma(\alpha x) = P_i(\alpha x),$$

так как $\sigma(\alpha) = \alpha$ (G_p действует на k_m тривиально). При этом если $P, 1 - P$ были нетождественными проекторами на $\mathfrak{N}_i^{(m)}$, то это же выполнено и для действия на $\mathfrak{N}_i'$.

Лемма доказана. •

Замечание 3.4.2. В лемме 3.4.1 если $\mathfrak{N}_i^{(m)} \subset a\mathfrak{O}_{K_p} \otimes_{\mathfrak{o}} S_m$, то $\mathfrak{N}_i' \subset a\mathfrak{o}_{\mathcal{P}} \otimes_{\widetilde{\mathfrak{o}}} \mathfrak{o}_m$. Таким образом, мы получаем, что локальный композит-модуль не равен всему $\widetilde{K}_p \otimes_{\widetilde{\mathfrak{o}}} \mathfrak{o}_m$ (это существенно использовалось в п. 2.3).

3.5. Доказательство теоремы В Введения. Пусть мы находимся в условиях п. 3.1 и из нетривиального $\mathfrak{o}[G]$-разложения идеала $I = \mathfrak{A} \oplus \mathfrak{B}$ в K/k получили нетривиальное разложение композит-модуля $\mathfrak{N}$ из $K \otimes_{\mathfrak{o}} S_n$ над $S_n[G]$:

$$\mathfrak{N} = \mathfrak{A}' \oplus \mathfrak{B}' \tag{20}$$

(см. (13)). Пусть K_p — максимальное p-подрасширение в K/k, в котором из разложения (20) получаем разложения композит-модулей

$$\mathfrak{N}_i = \mathfrak{A}_i \oplus \mathfrak{B}_i, \quad 1 \leq i \leq m, \tag{21}$$

над $S_n[G_p]$ (см. (14)) и из них — разложения композит-модулей

$$\mathfrak{N}_i^{(m)} = \mathfrak{A}_i^{(m)} \oplus \mathfrak{B}_i^{(m)}, \quad 1 \leq i \leq m, \tag{22}$$

в $K_p \otimes_{\mathfrak{o}} S_m$ над $S_m[G_p]$, где S_m — целое замыкание кольца $\mathfrak{o}$ в поле $k(\zeta_m)$ (см. лемму 3.3.3).

Согласно замечанию 2.2.3, расширение K_p/k не имеет нетривиального поля разложения для любого простого идеала $\wp$ в k, делящего (p). Поэтому мы из $S_m[G_p]$-разложения (22) получаем $\mathfrak{o}_m[G_p]$-разложения локальных композит-модулей:

$$\mathfrak{N}_i' = \mathfrak{A}_i' \oplus \mathfrak{B}_i', \tag{23}$$

где $\mathfrak{o}_m$ — кольцо целых поля $\widetilde{k}(\zeta_m)$ (см. лемму 3.4.1).

1. Пусть в расширении $\widetilde{K}_p/\widetilde{k}$ нет нетривиального поля инерции. Тогда так как $k_m/\widetilde{k}$ неразветвлено, то

$$\mathfrak{o}_{\mathcal{P}} \otimes_{\widetilde{\mathfrak{o}}} \mathfrak{o}_m = \mathfrak{o}_m \mathfrak{o}_{\mathcal{P}} = \mathfrak{O}_{k_m \widetilde{K}_p}$$

— кольцо целых композита полей k_m и $\widetilde{K}_p$. Кроме того, $\widetilde{K}_p$, k_m не пересекаются, и поэтому мы имеем $\mathfrak{o}_m[G]$-изоморфизм $\widetilde{K}_p \otimes_{\widetilde{\mathfrak{o}}} \mathfrak{o}_m \approx \mathfrak{o}_L$, где $L = \widetilde{K}_p k_m$. Поэтому композит-модуль $\mathfrak{N}_i'$, определенный над $\mathfrak{o}_{\mathcal{P}} \otimes_{\widetilde{\mathfrak{o}}} \mathfrak{o}_m$, будет идеалом в L и этот идеал имеет $\mathfrak{o}_m[G_p]$-разложение в p-расширении L/k_m, где $G_p \approx \mathrm{Gal}(L/k_m)$. Из того, что расширение k_m/k неразветвлено, следует, что $\mathfrak{D}_{L/k_m} = \mathfrak{o}_m \mathfrak{D}_{\widetilde{K}_p/\widetilde{k}}$. По условию п. 3.2 идеал $\wp$ входит в $\mathfrak{d}_{K/k}$ в степени меньшей, чем в идеал (n). Поэтому, согласно лемме 1.9.3, степень p^r расширения $\widetilde{K}_p/\widetilde{k}$ не делит дифференту этого расширения. Это значит, что в $\widetilde{K}_p/\widetilde{k}$ нет разложимых идеалов (см. [BVZ]), и поэтому все разложения (23) и вместе с ними разложения (22) и (21) тривиальны. Отсюда следует, что разложение (20), а вместе с ним и разложение исходного идеала $I = \mathfrak{A} \oplus \mathfrak{B}$ происходит над кольцом $\mathfrak{o}_{K_p}$ (см. лемму 1.2), и тем самым мы от расширения K/k переходим к расширению K/K_p меньшей степени, что противоречит условию $(*)$ п. 3.1.

2. Пусть в расширении K_p/k есть нетривиальное поле инерции T и $\widetilde{T}$ — его пополнение. Тогда, согласно предложению 2.3.1, все разложения (23) происходят над кольцом целых поля $\widetilde{T}$. Поэтому для каждого i, $1 \le i \le m$, проектор

$$P_i : \mathfrak{N}_i' \to \mathfrak{A}_i'$$

принадлежит $kS_m[G_p] \cap \widetilde{k}\mathfrak{o}_m[\mathrm{Gal}(\widetilde{K}_p/\widetilde{T})] = kS_m[\mathrm{Gal}(K_p/\widetilde{T})]$. Заметим, что в нашем случае $\mathrm{Gal}(\widetilde{K}_p/T) \approx \mathrm{Gal}(K/T)$. Значит, разложения (21) композит-модулей $\mathfrak{N}_i$, $1 \le i \le m$, происходят над $\mathfrak{O}_T$, где $\mathfrak{O}_T$ — целое замыкание кольца $\mathfrak{o}$ в T.

Применяя опять лемму 1.2, получаем, что разложение (20) композит-модуля $\mathfrak{N}$, а вместе с ним и разложение идеала $I = \mathfrak{A} \oplus \mathfrak{B}$ было над $\mathfrak{O}_T$, и мы опять переходим от расширения K/k к расширению меньшей степени K/T, что противоречит условию $(*)$ п. 3.1.

Теорема B полностью доказана. •

Список литературы

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

[BLV] Bondarko M. V., Lai K. F., Vostokov S. V., *Galois structure of Dedekind domain in abelian p-extension*, J. Reine Angew. Math., 1999.

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

[BV1] Бондарко М. В., Востоков С. В., *Разложимость идеалов как модулей Галуа в полных дискретно-нормированных полях*, Алгебра и анализ **11** (1999), № 2, 41–63.

[BV2] Бондарко М. В., Востоков С. В., *Разложение идеалов в абелевых p-расширениях полных дискретно нормированных полей*, Зап. науч. семин. ПОМИ **236** (1997), 23–33.

[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.

[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 structure 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 $\mathfrak{p}$-adic number field*, Nagoya Math. J. **77** (1980), 13–23.

[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.

С.-Петербургский
государственный университет
математико-механический факультет
198904, Санкт-Петербург
Петродворец, Библиотечная пл., 2

Поступило 15 октября 1998 г.