З. И. Боревич, О мультипликативной группе циклических p-расширений локального поля, *Тр. МИАН СССР*, 1965, том 80, 16–29

З. И. БОРЕВИЧ

О МУЛЬТИПЛИКАТИВНОЙ ГРУППЕ ЦИКЛИЧЕСКИХ p-РАСШИРЕНИЙ ЛОКАЛЬНОГО ПОЛЯ

§ 1. Введение

Пусть k — локальное поле (конечное расширение поля p-адических чисел R_p) и K/k — нормальное расширение с группой Галуа G. Мультипликативную группу K^* поля K мы можем рассматривать как операторную группу с операторами из G. Определенный интерес представляет вопрос о строении этой G-операторной группы K^*. Однако к настоящему времени строение G-группы K^* изучено лишь в отдельных частных случаях.

Для группы K^* мы имеем разложение в прямое произведение трех групп

$$K^* = \{\Pi\} \times Q \times E,$$

где $\{\Pi\}$ — бесконечная циклическая группа, порожденная простым элементом Π поля K; Q — конечная циклическая группа, порядок которой взаимно прост с p; E — группа главных единиц поля K (сравнимых с 1 по модулю Π). Группы Q и E инвариантны относительно операторов из G. При исследовании группы K^* (с операторами из G) надо фактически изучить лишь строение группы главных единиц E (см. § 2).

Группа E естественным образом допускает операторы из кольца целых p-адических чисел O_p. Ее можно поэтому рассматривать как мультипликативно записанный O_p-модуль. Если поле K *регулярно*, т. е. не содержит первообразного корня p-й степени из 1, то E является свободным O_p-модулем, ранг которого равен степени $(K:R_p)$ поля K над R_p. В *иррегулярном* же случае группа E распадается в прямое произведение конечной циклической группы порядка p^s ($s \geqslant 1$) и свободного O_p-модуля ранга $(K:R_p)$. Натуральное число s мы будем называть *показателем иррегулярности* иррегулярного поля K.

Так как операторы из O_p перестановочны с автоморфизмами из G, то E является мультипликативно записанным модулем над групповым кольцом $O = O_p[G]$ группы G над O_p. Строение O-модуля E известно в следующих случаях.

В статье Ивасава [1] структура O-группы E изучена в предположениях: 1) поле K иррегулярно, 2) K/k — полупрямое расширение без высшего ветвления и 3) если s — показатель иррегулярности поля K и ζ — содержащийся в K первообразный корень степени p^s из 1, то степень $(K:k(\zeta))$ делится на p при $p>2$ и делится на 4 при $p=2$.

В работе Краснера [2] доказано, что если расширение K/k не имеет высшего ветвления и поле K регулярно, то E является свободным

O-модулем (ранга $(k:R_p)$). В случае регулярного K отсутствие высшего ветвления для K/k является также и необходимым условием для того, чтобы O-модуль E был свободным (см. [3]). В статье [2] установлено также, что если степень $(K:k)$ не делится на p, то E распадается в прямое произведение конечной группы (порядка p^s) и свободного O-модуля. В этом случае говорят, что для группы главных единиц поля K существует *нормальный базис* (относительно расширения K/k).

Для расширений K/k с высшим ветвлением строение O-модуля E известно лишь в следующих двух простейших случаях. В работе [4] Ивасава выяснил строение группы E при $k=R_p$ и $K=R_p(\zeta)$, где ζ — первообразный корень степени p^s из 1. В заметке [5] рассматриваемый вопрос решен для произвольного циклического расширения K/k с регулярным K.

К перечисленным работам примыкает также статья Д. К. Фаддеева [6], в которой изучено строение G-операторной группы K^*/K^{*p} для циклического p-расширения K/k иррегулярного поля k.

В настоящей работе, исходным пунктом которой является статья [6], выяснено строение G-группы K^* для ряда типов циклических p-расширений иррегулярного поля k (относительно циклических p-расширений регулярного k см. [5]). Разобранные нами случаи полностью охватывают все циклические расширения простой степени p. Вне рассмотрения остались не круговые расширения K/k, для которых либо степень инерции и индекс ветвления одновременно отличны от 1, либо показатели иррегулярности полей k и K различны. В случае $p=2$ в §§ 5 и 7 мы дополнительно предполагаем, что поле k содержит первообразный корень степени 4 из 1.

Заметим, что группа E для циклических расширений степени p с иррегулярным k рассматривалась в работе [7]. В этой работе для E была найдена система O-образующих, но строение O-модуля E осталось невыясненным, так как для найденных образующих не удалось найти определяющих соотношений.

Условимся в следующих обозначениях:

n — степень поля k над полем p-адических чисел R_p;

σ — образующий автоморфизм циклического p-расширения K/k;

$\zeta=\zeta_s$ — содержащийся в k первообразный корень степени p^s из 1, где $s\geqslant 1$ — показатель иррегулярности k; E_0 и E — группы главных единиц полей k и K соответственно;

$N=N_{K/k}$ — норма относительного расширения K/k; $\Gamma=N(E)$ — группа норм главных единиц поля K.

В случае иррегулярного k всякое циклическое расширение K/k простой степени p имеет вид $K=k\left(\sqrt[p]{\alpha}\right)$, $\alpha\in k^*$. Легко видеть, что в качестве α всегда можно выбрать либо некоторый простой элемент π поля k, либо некоторую главную единицу из E_0. Если во втором случае показатель иррегулярности поля K равен $s+1$, то можно взять $\alpha=\zeta$. Для наших целей следует различать три типа расширений $k\left(\sqrt[p]{\alpha}\right)/k$.

I. $\alpha=\pi$. Очевидно, что расширение $k\left(\sqrt[p]{\pi}\right)/k$ вполне разветвлено.

II. $\alpha=\zeta$.

III. $\alpha=\varepsilon\in E_0$ и показатели иррегулярности полей $k\left(\sqrt[p]{\varepsilon}\right)$ и k совпадают.

Строение O-модуля E (для расширений $k\left(\sqrt[p]{\alpha}\right)/k$) зависит еще от двух обстоятельств: 1) принадлежит ли корень ζ группе норм Γ или не принадлежит и 2) является ли расширение K/k неразветвленным

($e=1$) или вполне разветвленным ($e=p$). Для каждой из получающихся семи возможностей группа главных единиц E как O-модуль имеет строение, указанное в приведенной таблице (в случае кругового расширения, т. е. при $\alpha=\zeta$, под g понимается некоторое натуральное число, для которого $g\equiv 1 \pmod{p^s}$ и $g\not\equiv 1 \pmod{p^{s+1}}$).

№№ п. п.	$k(\sqrt[p]{\alpha})/k$	σ-образующие группы	Определяющие соотношения
1	$\alpha=\pi,\ \zeta\notin\Gamma$	$\theta_1, \ldots, \theta_n, \zeta$	$\zeta^{p^s}=1,\ \zeta^{\sigma-1}=1$
2	$\alpha=\pi,\ \zeta\in\Gamma$	$\theta_1, \ldots, \theta_{n-1}, \xi, \gamma$	$N(\xi^{p^s})=1,\ \gamma^{\sigma-1}=1$
3	$\alpha=\zeta,\ e=1$	$\theta_1, \ldots, \theta_n, \zeta'$	$\zeta'^{\sigma-g}=1$
4	$\alpha=\zeta,\ e=p$	$\theta_1, \ldots, \theta_{n-1}, \theta, \gamma, \zeta'$	$N(\theta)=1,\ \gamma^{\sigma-1}=1,\ \zeta'^{\sigma-g}=1$
5	$\alpha=\varepsilon,\ e=1$	$\theta_1, \ldots, \theta_{n-1}, \xi, \omega$	$\omega^{\sigma-1}=\xi^{p^s}$
6	$\alpha=\varepsilon,\ e=p,\ \zeta\notin\Gamma$	$\theta_1, \ldots, \theta_{n-1}, \theta, \omega, \zeta$	$\begin{cases} N(\theta)=1,\ \zeta^{p^s}=1 \\ \zeta^{\sigma-1}=1,\ \omega^{\sigma-1}=\zeta^{p^{s-1}} \end{cases}$
7	$\alpha=\varepsilon,\ e=p,\ \zeta\in\Gamma$	$\begin{cases} \theta_1, \ldots, \theta_{n-2} \\ \theta, \gamma, \xi, \omega \end{cases}$	$\begin{cases} N(\theta)=1,\ \gamma^{\sigma-1}=1 \\ \omega^{\sigma-1}=\xi^{p^s} \end{cases}$

В случаях 1 и 3 образующие $\theta_1, \ldots, \theta_n$ не связаны никакими соотношениями; это значит, что они образуют так называемый нормальный базис, т. е. что группа E распадается в прямое произведение конечной группы и свободного O-модуля ранга n (см. [3]). Особенно интересен в этом отношении случай 1, так как он указывает на возможность существования нормального базиса в E для расширений с высшим ветвлением. Заметим, что в случаях 2, 5 и 7 мы имеем $\zeta=N(\xi)$. Кроме того, для расширений 4, 6 и 7 в качестве образующей θ можно взять $\theta=\Pi^{\sigma-1}$, где Π — произвольный простой элемент поля K, для которого $\Pi^{\sigma-1}\in E$.

При $p=2$ в случаях 3, 4, 6 и 7 предполагается, что $s\geqslant 2$.

§ 2. Группы K^* и E

Пусть K/k — произвольное нормальное расширение локального поля k с группой Галуа G. Покажем, что группа K^* как абстрактная группа с операторами из G вполне определена G-операторной группой всех единиц U поля K.

Пусть Π — произвольный простой элемент поля K. Равенством

$$\Pi^{\sigma-1}=\varepsilon_\sigma \quad (\sigma\in G)$$

определен одномерный коцикл ε_σ группы G на U. Класс когомологий с представителем ε_σ является образующим элементом циклической группы $H^1(G, U)$, порядок которой равен индексу ветвления e расширения K/k. Выберем теперь произвольный 1-коцикл u_σ группы G на U, для которого соответствующий класс когомологий порождает $H^1(G, U)$. На прямом произведении $X=\{A\}\times U$ бесконечной циклической группы $\{A\}$ и группы U определим действие операторов $\sigma\in G$, полагая

$$A^{\sigma-1}=u_\sigma.$$

Мы утверждаем, что группы X и K^* операторно изоморфны. Для доказательства воспользуемся разложением $U = Q \times E$ и положим

$$\varepsilon_\sigma = \eta_\sigma \theta_\sigma \quad (\eta_\sigma \in Q,\ \theta_\sigma \in E),$$

$$u_\sigma = w_\sigma v_\sigma \quad (w_\sigma \in Q,\ v_\sigma \in E).$$

Если $e = e_0 p^m$, $(e_0, p) = 1$, то группы $H^1(G, Q)$ и $H^1(G, E)$ имеют соответственно порядки e_0 и p^m. Число e_0 является, как известно, делителем порядка группы Q. Так как классы когомологий с представителями η_σ и w_σ являются образующими группы $H^1(G, Q)$, то при некотором целом k, взаимно простом с порядком группы Q, имеем

$$w_\sigma = \eta_\sigma^k \eta^{1-\sigma} \quad (\eta \in Q).$$

Аналогично при некотором l, не делящемся на p, имеем

$$v_\sigma = \theta_\sigma^l \theta^{1-\sigma} \quad (\theta \in E).$$

Отображения $\beta \to \beta^k (\beta \in Q)$ и $\gamma \to \gamma^l (\gamma \in E)$ являются, очевидно, G-автоморфизмами групп Q и E соответственно. Легко теперь проверяется, что отображения

$$\Pi \to A\eta\theta,\ \beta \to \beta^k (\beta \in Q),\ \gamma \to \gamma^l (\gamma \in E)$$

индуцируют операторный изоморфизм группы K^* на группу X.

Действие операторов из G на группе Q известно. Именно, если автоморфизм $\sigma \in G$ на подполе инерции индуцирует автоморфизм Фробениуса, то $\beta^\sigma = \beta^q (\beta \in Q)$, где q — число элементов в поле вычетов поля k. Таким образом, строение G-операторной группы K^* целиком определяется строением группы главных единиц E.

§ 3. Вспомогательные леммы

Фактор-группа K^*/K^{*p} мультипликативной группы поля K по подгруппе p-ых степеней является элементарной абелевой p-группой. Ее можно рассматривать, следовательно, как линейное пространство над полем из p-элементов. Мы будем говорить, например, что элементы $\alpha_1, \ldots, \alpha_k$ из K^* являются образующими для K^*/K^{*p}, если соответствующие им классы смежности по подгруппе K^{*p} порождают линейное пространство K^*/K^{*p}. Точно так же на элементы из K^* переносится понятие базиса K^*/K^{*p}, понятие линейной зависимости и независимости в K^*/K^{*p}.

Аналогичным образом такие понятия, как система образующих, базис, линейная зависимость и линейная независимость, будут употребляться и по отношению к единицам из E относительно линейного пространства E/E^p.

Лемма 1. *Если единицы $\theta_1, \ldots, \theta_k$ являются образующими для E/E^p, то они являются образующими и для группы E* (которую мы рассматриваем как операторную группу над кольцом целых p-адических чисел O_p).

Доказательство очевидно.

Пусть теперь K/k — циклическое расширение иррегулярного поля k и σ — образующий автоморфизм его группы Галуа. Автоморфизм σ индуцирует на пространстве K^*/K^{*p} (размерности $np^m + 2$) линейный оператор, который мы будем обозначать той же буквой σ.

Лемма 2. *Если нормы $N_{K/k}(\alpha_j)$ элементов $\alpha_j (1 \leqslant j \leqslant k)$ из K^* линейно независимы в K^*/K^{*p}, то линейно независимыми в K^*/K^{*p} будут и элементы*

$$\alpha_j^{\sigma^i} (1 \leqslant j \leqslant k,\ 0 \leqslant i < p^m).$$

Доказательство. Рассмотрим в пространстве K^*/K^{*p} нульстепенный оператор $\sigma - 1$ (см. [6]). Его показатель нульстепенности равен p^m, так как

$$(\sigma - 1)^{p^m} \equiv 0 \pmod p,$$

$$(\sigma - 1)^{p^m - 1} \equiv 1 + \sigma + \ldots + \sigma^{p^m - 1} = N_{K/k} \pmod p.$$

Допустим, что имеет место зависимость

$$\prod_{i,j} \alpha_j^{a_{ij}(\sigma-1)^i} \equiv 1 \pmod{K^{*p}},$$

где не все целые рациональные a_{ij} делятся на p. Пусть i_0 есть наименьший из индексов i, для которого существует такое j, что $a_{i_0 j} \not\equiv 0 \pmod p$. Применив к нашему соотношению оператор $(\sigma - 1)^{p^m - i_0 - 1}$, мы получим

$$\prod_j (N(\alpha_j))^{a_{i_0 j}} \equiv 1 \pmod{K^{*p}},$$

а это противоречит независимости норм $N(\alpha_j)$. Таким образом, элементы $\alpha_j^{(\sigma-1)^i}$ независимы в K^*/K^{*p}, а так как они связаны с $\alpha_j^{\sigma^i}$ неособенным треугольным преобразованием, то и последние элементы линейно независимы в K^*/K^{*p}. Лемма 2 доказана.

Фактически то же самое доказательство дает нам также следующее утверждение.

Лемма 3. *Если для элементов $\gamma \in k^*$ и $\alpha_j \in K^*$ $(1 \leqslant j \leqslant k)$ система γ, $N(\alpha_1), \ldots, N(\alpha_k)$ линейно независима в K^*/K^{*p}, то система*

$$\gamma,\ \alpha_j^{\sigma^i} \quad (1 \leqslant j \leqslant k,\ 0 \leqslant i < p^m)$$

будет также линейно независимой в K^*/K^{*p}.

Вложение $k^* \to K^*$ естественным образом индуцирует гомоморфизм $k^*/k^{*p} \to K^*/K^{*p}$. Из теории куммеровых расширений очевидным образом вытекает

Лемма 4. *При иррегулярном k и циклическом p-расширении K/k ядром гомоморфизма $k^*/k^{*p} \to K^*/K^{*p}$ является подгруппа порядка p* (подпространство размерности 1).

Вложение $E \to K^*$ индуцирует мономорфизм $E/E^p \to K^*/K^{*p}$, поэтому E/E^p можно рассматривать как подпространство пространства K^*/K^{*p} (на единицу меньшей размерности). Ясно, что это подпространство инвариантно относительно оператора σ. Аналогичным образом фактор-группу E_0/E_0^p можно считать подпространством линейного пространства k^*/k^{*p}.

Лемма 5. *Естественный гомоморфизм $E_0/E_0^p \to E/E^p$ имеет нетривиальное ядро (т. е. не является мономорфизмом) тогда и только тогда, когда $\zeta_1 \in E^{\sigma-1}$* (здесь ζ_1 — первообразный корень степени p из 1).

Действительно, если единица ε из E_0 не принадлежит E_0^p, но $\varepsilon = \beta^p$, $\beta \in E$, то $\beta^{\sigma-1} \neq 1$ и $(\beta^{\sigma-1})^p = 1$. Обратно, если $\zeta_1 = \beta^{\sigma-1}$ $(\beta \in E)$, то β не принадлежит E_0, однако $\beta^p \in E_0$.

Для расширения K/k через t обозначим наибольшее целое число, для которого $\zeta_t \in E^{\sigma-1}$ (ζ_t — первообразный корень степени p^t из 1). Легко видеть, что $0 \leqslant t \leqslant \min(m, s)$. Согласно лемме 5, условие $t=0$ равносильно тому, что отображение $E_0/E_0^p \to E/E^p$ является мономорфизмом.

Лемма 6. *Пусть K/k — разветвленное (не обязательно вполне разветвленное) циклическое p-расширение, для которого $t>0$. Предположим, что ядро гомоморфизма $E_0/E_0^p \to E/E^p$ содержится в группе $\Gamma E_0^p/E_0^p$. Тогда, если нормы $N(\theta_j)$ $(1 \leqslant j \leqslant n-1)$ единиц $\theta_j \in E$ линейно независимы в E/E^p, то для любого простого элемента Π поля K система*

$$\theta_j^{\sigma^i},\ \Pi^{\sigma^i}\ (1 \leqslant j \leqslant n-1,\ 0 \leqslant i < p^m)$$

будет линейно независимой в K^*/K^{*p}.

Доказательство. Так как по условию $(E_0:\Gamma)>1$, то группа $\Gamma E_0^p/E_0^p$ является линейным пространством размерности n. Положим $N(\theta_j)=\varepsilon_j$ $(1 \leqslant j \leqslant n-1)$. Если единица ε из Γ является образующим элементом для ядра гомоморфизма $E_0/E_0^p \to E/E^p$, то система $\varepsilon, \varepsilon_1, \ldots$ $\ldots, \varepsilon_{n-1}$ будет базисом для $\Gamma E_0^p/E_0^p$. Следовательно, пространство $\Gamma E^p/E^p$ имеет размерность $n-1$ и, значит, при разложении пространства E/E^p в прямую «сумму» циклических подпространств относительно нульстепенного оператора $\sigma-1$ мы будем иметь ровно $n-1$ подпространств максимальной размерности p^m. В качестве этих подпространств можно взять подпространства, порожденные единицами $\theta_1, \ldots, \theta_{n-1}$. Далее, как показано в работе [6], в линейном пространстве K^*/K^{*p} имеется n прямых «слагаемых», являющихся циклическими подпространствами размерности p^m. В качестве σ-образующих для них можно, очевидно, взять систему $\theta_1, \ldots, \theta_{n-1}, A$, где $A \in K^*$. Образующая A не может быть единицей, поэтому $A=\Pi^k\mu$, где $k \not\equiv 0 \pmod p$ и μ — некоторая единица поля K. Но всякая главная единица поля K в пространстве E/E^p может быть выражена через $\theta_1, \ldots, \theta_{n-1}$ и через «корневые векторы» высоты $<p^m$. В силу этого единицу μ можно отбросить, т. е. можно взять $A=\Pi^k$. Далее, возведением в надлежащую степень и отбрасыванием p-й степени можно сделать k равным 1. Таким образом, при выполнении условий леммы всегда можно взять $A=\Pi$, а это и завершает ее доказательство.

Лемма 7. *Если расширение K/k вполне разветвлено и $s \geqslant 2$ при $p=2$, то ядро гомоморфизма $E_0/E_0^p \to E/E^p$ содержится в группе $\Gamma E_0^p/E_0^p$.*

Доказательство. Пусть $t>0$ и пусть единица $\varepsilon \in E_0$ порождает ядро гомоморфизма $E_0/E_0^p \to E/E^p$. Положим $\varepsilon=\omega^p$, где $\omega \in E$. Так как расширение $k(\omega)/k$ вполне разветвлено и имеет степень p, то группа норм (в поле k) группы главных единиц поля $k(\omega)$ совпадает с ΓE_0^p. С другой стороны, норма $N_{k(\omega)/k}(\omega)$ равна ε при $p>2$ и равна $-\varepsilon$ при $p=2$. Но при $p=2$ по условию $-1 \in E_0^2$, поэтому во всех случаях $\varepsilon \in \Gamma E_0^p$, что и требовалось доказать.

Лемма 8. *Если $\alpha^{\sigma-1}=\lambda$, $\alpha \in K^*$, то*

$$N(\alpha)=\alpha^{p^m}\lambda^{-\varphi},$$

где

$$\varphi=1+2\sigma+3\sigma^2+\ldots+p^m\sigma^{p^m-1}.$$

Для доказательства следует заметить, что

$$(\sigma-1)\varphi=p^m-(1+\sigma+\sigma^2+\ldots+\sigma^{p^m-1}).$$

§ 4. Случай $t=0$

Условие $t=0$ равносильно, как мы видели, тому, что отображение $E_0/E_0^p \to E/E^p$ является мономорфизмом. Таким образом, при $t=0$ всякая система единиц из E_0, линейно независимая в E_0/E_0^p, остается линейно независимой и в E/E^p. В частности, показатели иррегулярности полей k и K совпадают. Ясно также, что при $t=0$ расширение K/k вполне разветвлено, а значит для группы норм $\Gamma = N_{K/k}(E)$ фактор-группа E_0/Γ есть циклическая группа порядка p^m.

Мы предположим сначала, что корень $\zeta = \zeta_s (s \geqslant 1)$ является образующим элементом для E_0/Γ, т. е. что $E_0 = \{\zeta, \Gamma\}$. Очевидно, что последнее может иметь место только при $m \leqslant s$.

Теорема 1. *Если отображение $E_0/E_0^p \to E/E^p$ является мономорфизмом и если $E_0 = \{\zeta, \Gamma\}$, то для главных единиц поля K существует нормальный базис над k, т. е. O-модуль E распадается в прямое произведение конечной группы $\{\zeta\}$ и свободного O-модуля (ранга n).*

Доказательство. В группе норм Γ выберем единицы $\varepsilon_1, \ldots, \varepsilon_n$ так, чтобы $E_0 = \{\zeta, \varepsilon_1, \ldots, \varepsilon_n\}$. Пусть $\varepsilon_j = N(\theta_j)$, $1 \leqslant j \leqslant n$. Так как единицы $\zeta, \varepsilon_1, \ldots, \varepsilon_n$ линейно независимы в E_0/E_0^p, то они линейно независимы и в E/E^p. По лемме 3 система $\zeta, \theta_j^{\sigma^i}$ $(1 \leqslant j \leqslant n,\ 0 \leqslant i < p^m)$ будет линейно независимой в K^*/K^{*p}, а значит она будет образовывать базис пространства E/E^p. Применив теперь лемму 1, мы и получаем утверждение теоремы.

Теорема 2. *Если отображение $E_0/E_0^p \to E/E^p$ является мономорфизмом и $\zeta \in \Gamma$, то O-модуль E допускает систему образующих $\theta_1, \ldots, \theta_{n-1}, \xi, \gamma$ с определяющими соотношениями:*

$$N(\xi^{p^s}) = 1, \quad \gamma^{\sigma-1} = 1.$$

Доказательство. Пусть единица $\gamma \in E_0$ такова, что $E_0 = \{\gamma, \Gamma\}$. Так как γ не является p-й степенью в E_0, то в Γ можно, помимо ζ, выбрать такие единицы $\varepsilon_1, \ldots, \varepsilon_{n-1}$, что система $\gamma, \zeta, \varepsilon_1, \ldots, \varepsilon_{n-1}$ будет базисом для E_0/E_0^p. Пусть

$$N(\xi) = \zeta, \quad N(\theta_j) = \varepsilon_j \quad (1 \leqslant j \leqslant n-1).$$

По лемме 3 система $\gamma, \xi^{\sigma^i}, \theta_j^{\sigma^i}$ будет базисом для E/E^p, а значит, по лемме 1, — системой O_p-образующих для E. Соотношение $N(\xi)^{p^s} = 1$ для этих образующих над O_p будет единственным. Теорема 2 доказана.

Обозначим через r наибольшее целое число, для которого ζ_r (первообразный корень степени p^r из 1) принадлежит группе норм Γ, и через p^h — индекс подгруппы $\{\zeta, \Gamma\}$ в группе E_0. Ясно, что $h+s = m+r$. В теоремах 1 и 2 число h принимает крайние возможные значения $h=0$ и $h=m$.

Теорема 2*. *Если $t=0$ и $0 < h < m$, то в O-модуле E имеется система образующих $\theta_1, \ldots, \theta_{n-1}, \xi, \gamma$ с определяющими соотношениями:*

$$(\gamma^{p^h} N(\xi))^{p^s} = 1, \quad \gamma^{\sigma-1} = 1.$$

Доказательство. Пусть $E_0 = \{\gamma, \Gamma\}$ и пусть единицы $\varepsilon_j \in \Gamma$ $(1 \leqslant j \leqslant n)$ таковы, что система $\gamma, \varepsilon_1, \ldots, \varepsilon_n$ является базисом для E_0/E_0^p. По лемме 1 эти единицы порождают E_0, поэтому при некоторых целых p-адических показателях будем иметь

$$\zeta = \gamma^{x_0} \varepsilon_1^{x_1} \ldots \varepsilon_n^{x_n}.$$

Согласно условию, x_0 делится на p^h и не делится на более высокую степень p. Изменив, быть может, единицу γ, мы можем добиться того, чтобы $x_0 = p^h$. Все остальные показатели x_j не могут делиться на p одновременно, так как в противном случае корень ζ был бы p-й степенью в E_0, что не так. Пусть, например, x_n не делится на p. Положив

$$\bar{\varepsilon} = \varepsilon_1^{x_1} \ldots \varepsilon_n^{x_n} \in \Gamma,$$

мы получаем для E_0 новую систему образующих γ, $\bar{\varepsilon}$, $\varepsilon_1, \ldots, \varepsilon_{n-1}$. Если теперь $\bar{\varepsilon} = N(\xi)$, $\varepsilon_j = N(\theta_j)$ $(1 \leqslant j \leqslant n-1)$, то единицы γ, ξ^{σ^i}, $\theta_j^{\sigma^i}$ будут образующими для E (над O_p), а так как $\zeta = \gamma^{p^h} N(\xi)$, то образующие γ, ξ, θ_j (над O) удовлетворяют требованиям теоремы 2*.

Замечание 1. Легко показать, что в условиях теорем 1, 2 и 2* при надлежащем выборе простого элемента Π и при надлежащих образующих в E будут справедливы равенства:

$$1)\ \Pi^{\sigma-1} = \zeta_m,$$
$$2)\ \Pi^{\sigma-1} = \xi^{p^s},$$
$$2^*)\ \Pi^{\sigma-1} = \gamma^{p^r} \xi^{p^s}.$$

Замечание 2. Утверждение теоремы 2* справедливо также при $h = 0$ и $h = m$: простая замена образующих приводит нас к соотношениям теорем 1 и 2.

§ 5. Круговые расширения

В этом параграфе мы будем предполагать, что $s \geqslant 2$, если только $p = 2$ (и $s \geqslant 1$ при $p \neq 2$).

Рассмотрим поле $K = k(\zeta')$, где $\zeta' = \zeta_{s+m}$ — первообразный корень степени p^{s+m} из 1. Расширение K/k, называемое *круговым*, циклично и имеет степень p^m.

Теорема 3. *Если круговое расширение K/k неразветвлено, то для главных единиц поля K существует нормальный базис.*

Доказательство. Пусть система единиц ζ, $\varepsilon_1, \ldots, \varepsilon_n$ из E_0 является базисом для E_0/E_0^p и пусть $\varepsilon_j = N(\theta_j)$, $1 \leqslant j \leqslant n$. По лемме 4 единицы $\varepsilon_1, \ldots, \varepsilon_n$ линейно независимы в E/E^p, поэтому (лемма 2) линейно независимыми в E/E^p будут и единицы $\theta_j^{\sigma^i}$ $(1 \leqslant j \leqslant n,\ 0 \leqslant i < p^m)$. Нам достаточно теперь показать, что единицы ζ', $\theta_j^{\sigma^i}$ порождают $\overline{E}$. Допуская, что эти единицы линейно зависимы в E/E^p, мы смогли бы корень ζ' с точностью до p-й степени выразить через $\theta_j^{\sigma^i}$. Но тогда, перейдя в таком выражении к нормам, мы получили бы выражение корня ζ, равного $N(\zeta')$ при $p \neq 2$ и $-N(\zeta')$ при $p = 2$, через ε_j (с точностью до p-й степени в E_0), а это невозможно. Полученное противоречие и завершает доказательство теоремы 3.

Для полного описания действия оператора σ на группе E к теореме 3 следует добавить, что $\zeta'^{\sigma} = \zeta'^{g}$, где число g удовлетворяет условиям $g \equiv 1 \pmod{p^s}$, $g \not\equiv 1 \pmod{p^{s+1}}$.

Теорема 4. *Если круговое расширение K/k вполне разветвлено, то для группы главных единиц E поля K существует система образующих $\theta_1, \ldots, \theta_{n-1}$, θ, γ, ζ' (над O) с определяющими соотношениями*

$$N(\theta) = 1,\ \gamma^{\sigma-1} = 1,\ \zeta'^{\sigma-g} = 1.$$

Доказательство. Пусть $E_0 = \{\gamma, \Gamma\}$. Так как $\pm\zeta \in \Gamma$ (минус берется при $p = 2$), то при некоторых $\varepsilon_1, \ldots, \varepsilon_{n-1}$ из Γ система $\varepsilon_1, \ldots, \varepsilon_{n-1}$, γ, ζ будет базисом для E_0/E_0^p. Пусть $\varepsilon_j = N(\theta_j)$ $(1 \leqslant j \leqslant n-1)$

и пусть $\pi = N(\Pi)$, где Π — простой элемент поля K, выбранный так, что $\Pi^{\sigma-1} = \theta \in E$. Ясно, что элементы $\varepsilon_1, \ldots, \varepsilon_{n-1}, \pi, \gamma, \zeta$ линейно независимы в k^*/k^{*p}, а значит, ввиду леммы 4 элементы $\varepsilon_1, \ldots, \varepsilon_{n-1}, \pi, \gamma$ линейно независимы в K^*/K^{*p}. По лемме 3 система $\theta_j^{\sigma^i}, \Pi^{\sigma^i}, \gamma$ также линейно независима в K^*/K^{*p}. Покажем, что к ней можно присоединить ζ', не нарушая линейной независимости в K^*/K^{*p}. В самом деле, если бы расширенная система оказалась зависимой, то, как и при доказательстве теоремы 3, мы получили бы выражение для ζ (с точностью до p-й степени) через $\varepsilon_j, \pi, \gamma$, что невозможно. Таким образом, система $\theta_j^{\sigma^i}, \Pi^{\sigma^i}, \gamma, \zeta'$ является базисом для K^*/K^{*p}. В этом базисе элементы Π^{σ^i} можно заменить на Π и θ^{σ^i}, где i пробегает все значения $0, 1, \ldots$ $\ldots, p^m - 1$, кроме одного. Убрав Π, мы получим базис для E/E^p. Заметив теперь, что единицы θ^{σ^i} $(0 \leqslant i < p^m)$ связаны соотношением $N(\theta) = 1$, и применив лемму 1, мы и получаем утверждение теоремы 4.

Теорема 4*. *Пусть для кругового расширения K/k степень инерции $f = p^v$ и индекс ветвления $e = p^u$ одновременно больше* 1. *Тогда для E существуют О-образующие $\theta_1, \ldots, \theta_{n-1}, \theta, \gamma, \zeta'$ с определяющими соотношениями*

$$N(\theta) = 1, \quad \gamma^{\sigma-1} = \theta^e, \quad \zeta'^{\sigma} = \zeta'^{g}.$$

Доказательство. Так как $\zeta \in \Gamma E_0^p$, то для расширения K/k выполнены условия леммы 6. Выберем единицы $\varepsilon_j = N(\theta_j)$ $(1 \leqslant j \leqslant n-1)$ так, чтобы система $\zeta, \varepsilon_1, \ldots, \varepsilon_{n-1}$ являлась базисом подпространства $\Gamma E_0^p/E_0^p$. Если Π — простой элемент поля K, то по лемме 6 система $\theta_j^{\sigma^i}, \Pi^{\sigma^i}$ линейно независима в K^*/K^{*p}. Мы будем считать Π выбранным так, что $\Pi^{\sigma-1} = \theta$ является главной единицей.

Обозначим через Θ подгруппу группы главных единиц E, состоящую из единиц с нормой 1. Фактор-группа $\Theta/E^{\sigma-1} = H^1(G, E)$ является циклической группой порядка $e = p^u$, и единица θ является ее образующим элементом. Следовательно, существует такая единица $\gamma \in E$, что

$$\gamma^{\sigma-1} = \theta^e.$$

Покажем, что в пространстве E/E^p единица γ не является линейной комбинацией единиц $\theta_j^{\sigma^i}, \theta^{\sigma^i}$, т. е. что она не принадлежит подпространству $E'E^p/E^p$, где $E' = \{\theta_j^{\sigma^i}, \theta^{\sigma^i}\}$.

По лемме 8 $N(\Pi) = \Pi^{p^m}\theta^{-\varphi}$. Отсюда следует, что все собственные векторы в инвариантном относительно σ подпространстве $E'E^p/E^p$ порождаются единицами $\varepsilon_1, \ldots, \varepsilon_{n-1}, \theta^{\varphi}$. Допустим, что $\gamma \in E'E^p$. Так как γ — собственный вектор оператора σ в E/E^p, то

$$\gamma = \varepsilon_1^{x_1} \ldots \varepsilon_{n-1}^{x_{n-1}} \theta^{\varphi x} \beta^p, \quad \beta \in E$$

с целыми рациональными $x_1, \ldots, x_{n-1}, x$. Применим к этому равенству оператор $\sigma - 1$. Мы получим

$$\theta^{p^u} = \theta^{p^m x} (\beta^{\sigma-1})^p,$$

откуда

$$\theta^{p^{u-1}} = \theta^{p^{m-1}x} \beta^{\sigma-1} \zeta_1^k.$$

Так как $m-1 \geqslant u$, то $\theta^{p^{m-1}} \in E^{\sigma-1}$. По лемме 5 корень ζ_1 также принадлежит $E^{\sigma-1}$. Следовательно,

$$\theta^{p^{u-1}} \in E^{\sigma-1},$$

и мы получили противоречие, так как θ является образующим элементом для циклической группы $\Theta/E^{\sigma-1}$ порядка p^u. Доказано, таким образом, что γ не принадлежит группе $E'E^p$.

Рассмотрим норму $N(\gamma)$. По лемме 8 мы имеем

$$N(\gamma)=\gamma^{f e}\theta^{-e\varphi}=\bar{\varepsilon}^{e},$$

где $\bar{\varepsilon}=\gamma^{f}\theta^{-\varphi}$. Но $\bar{\varepsilon}^{\sigma-1}=\theta^{ef}\theta^{-p^m}=1$, поэтому $\bar{\varepsilon} \in E_0$, а значит $N(\gamma)$ есть p-я степень в E_0.

Покажем теперь, что корень ζ' не является линейной комбинацией (в E/E^p) единиц $\theta_j^{\sigma^i}$, θ^{σ^i}, γ. Так как $\zeta'^{\sigma-1}=\zeta'^{g-1} \in E^p$, то ζ' — также собственный вектор в E/E^p. Поэтому, допуская противное, мы имели бы:

$$\zeta'=\varepsilon_1^{x_1}\ldots\varepsilon_{n-1}^{x_{n-1}}\theta^{\varphi x}\gamma^{y}\beta^{p}, \quad \beta \in E.$$

Но такое равенство невозможно: после перехода к нормам оно дает нам, что $\zeta \in E_0^p$, а это не так.

Нами показано, что единицы $\theta_j^{\sigma^i}$, θ^{σ^i}, γ, ζ', между которыми имеется только одно соотношение $N(\theta)=1$, порождают пространство E/E^p, а значит, по лемме 1, порождают и группу E (над кольцом O_p). Теорема 4* доказана.

Замечание. Утверждение теоремы 4* справедливо и в условиях теорем 3 и 4.

§ 6. Неразветвленные расширения

Нижеследующая теорема 5 является частным случаем более общего результата Ивасава (см. [1]). Мы приводим ее здесь с целью охватить все случаи расширений простой степени p. Кроме того, наше доказательство основывается на существенно другом подходе, что представляет известный интерес.

Теорема 5. *Если расширение K/k неразветвлено, а поля K и k имеют один и тот же показатель иррегулярности, то для O-модуля E существует система образующих $\theta_1, \ldots, \theta_{n-1}$, ξ, ω с единственным определяющим соотношением*

$$\omega^{\sigma-1}=\xi^{p^s}.$$

Доказательство. Так как ζ не является p-й степенью в E, то в E_0 можно выбрать такие единицы $\varepsilon_1, \ldots, \varepsilon_{n-1}$, что система $\zeta, \varepsilon_1, \ldots, \varepsilon_{n-1}$ линейно независима в E/E^p. Пусть $\zeta=N(\xi)$, $\varepsilon_j=N(\theta_j)$ $(1 \leqslant j \leqslant n-1)$. По лемме 2 система

$$\theta_j^{\sigma^i},\ \xi^{\sigma^i}\ (1 \leqslant j \leqslant n-1,\ 0 \leqslant i < p^m)$$

также линейно независима в E/E^p. Далее, так как $N(\xi^{p^s})=1$, а группа $H^1(G, E)$ для неразветвленного расширения тривиальна, то существует единица $\omega \in E$ такая, что $\omega^{\sigma-1}=\xi^{p^s}$. Покажем, что единица ω в пространстве E/E^p не является линейной комбинацией единиц $\theta_j^{\sigma^i}$, ξ^{σ^i}. Допуская противное и учитывая, что ω — собственный вектор в E/E^p, мы нашли бы для ω представление в виде

$$\omega = \varepsilon_1^{x_1} \dots \varepsilon_{n-1}^{x_{n-1}} \zeta^x \beta^p, \quad \beta \in E,$$

с целыми рациональными $x_1, \dots, x_{n-1}, x$. Применим к этому равенству оператор $\sigma - 1$. Мы получим

$$\xi^{p^s} = (\beta^{\sigma-1})^p,$$

откуда

$$\xi^{p^{s-1}} = \beta^{\sigma-1} \zeta_1^k,$$

что после взятия нормы дает нам противоречивое равенство $\zeta^{p^{s-1}} = 1$. Этим доказано, что единицы $\theta_j^{\sigma^i}$, ξ^{σ^i}, ω порождают группу E (над O_p). Так как $N(\xi) = \zeta$, то единственным соотношением между этими единицами (над O_p) будет соотношение $N(\xi)^{p^s} = 1$. Теорема 5 доказана.

§ 7. Вполне разветвленные расширения при $t > 0$

В этом параграфе мы рассмотрим вполне разветвленные расширения K/k, для которых гомоморфизм $E_0/E_0^p \to E/E^p$ имеет нетривиальное ядро ($t > 0$) и для которых *поля K и k имеют один и тот же показатель иррегулярности $s \geqslant 1$*. В теоремах 6, 7 и 7* эти условия будут предполагаться выполненными без дополнительных оговорок. Кроме того, в случае $p = 2$ предполагаем, что $s \geqslant 2$.

Через Π мы обозначим простой элемент поля K, для которого $\Pi^{\sigma-1} = \theta$ принадлежит группе главных единиц E, и через ε — единицу из E_0, порождающую ядро гомоморфизма $E_0/E_0^p \to E/E^p$. Согласно лемме 7, можно считать, что $\varepsilon \in \Gamma$. Числа r и h будут иметь то же значение, что и в § 4.

Теорема 6. *Если $E_0 = \{\zeta, \Gamma\}$, то для E существуют O-образующие $\theta_1, \dots, \theta_{n-1}, \theta, \omega, \zeta$ с определяющими соотношениями*

$$N(\theta) = 1, \quad \zeta^{p^s} = 1, \quad \zeta^{\sigma-1} = 1,$$

$$\omega^{\sigma-1} = \begin{cases} \zeta^{p^r} & \text{при } t = m, \\ \zeta^{p^r} \theta^{p^t} & \text{при } t < m. \end{cases}$$

Доказательство. Пусть единицы $\zeta, \varepsilon, \varepsilon_1, \dots, \varepsilon_{n-1}$ образуют базис для E_0/E_0^p, причем $\varepsilon_j = N(\theta_j)$, $1 \leqslant j \leqslant n-1$. Положим $\pi = N(\Pi)$. Так как элементы $\zeta, \varepsilon_1, \dots, \varepsilon_{n-1}, \pi$ линейно независимы в K^*/K^{*p}, то по лемме 3 система ζ, $\theta_j^{\sigma^i}$, Π^{σ^i} будет также линейно независимой в K^*/K^{*p}. Из условия $h = 0$ следует, что $m \leqslant s$, а значит $\zeta_m \in E$. Но $N(\zeta_m) = 1$, поэтому по теореме Гильберта существует такое $\alpha \in K^*$, что $\alpha^{\sigma-1} = \zeta_m$. Легко видеть, что $N(\alpha) = \pm \alpha^{p^m}$; следовательно, при надлежащем выборе единицы ε будем иметь $N(\alpha) \equiv \varepsilon \pmod{k^{*p}}$. Если бы элемент α был линейной комбинацией системы ζ, $\theta_j^{\sigma^i}$, Π^{σ^i} (в пространстве K^*/K^{*p}), то, переходя к нормам, мы получили бы, что ε является линейной комбинацией элементов $\varepsilon_1, \dots, \varepsilon_{n-1}, \pi$ (в пространстве k/k^{*p}), а это невозможно. Таким образом, элементы $\theta_j^{\sigma^i}$, Π^{σ^i}, ζ, α образуют базис для K^*/K^{*p}.

Если теперь $t = m$, то в качестве α можно взять единицу $\omega \in E$ и для этой единицы $\omega^{\sigma-1} = \zeta_m = \zeta^{p^r}$.

Если же $1 \leqslant t < m$, то α единицей быть не может. В то же время α не может быть простым элементом поля K. Следовательно, α можно выбрать в виде $\alpha = \omega \Pi^{-p^x}$, где $\omega \in E$ и $1 \leqslant x < m$. Для E мы получаем, таким образом, систему образующих $\theta_j^{\sigma^i}$, θ^{σ^i}, ω, ζ, при этом $\omega^{\sigma-1} = \zeta_m \theta^{p^x}$, и нам остается только показать, что $x = t$.

Мы имеем (см. лемму 8)

$$(\omega^{p^{m-x}} \theta^{-\varphi})^{\sigma-1} = (\zeta_m \theta^{p^x})^{p^{m-x}} \theta^{-p^m} = \zeta_x,$$

значит $\zeta_x \in E^{\sigma-1}$. Далее,

$$(\alpha^{p^{m-x-1}})^{\sigma-1} = \zeta_{x+1};$$

если бы существовала единица $\mu \in E$, для которой $\mu^{\sigma-1} = \zeta_{x+1}$, то мы получили бы, что $\Pi^{p^{m-1}} \in Ek^*$, а этого не может быть. Следовательно, $x = t$, и доказательство теоремы 6 окончено.

Теорема 7. *Если $\zeta \in \Gamma$, то в группе E существуют образующие $\theta_1, \ldots, \theta_{n-2}, \theta, \gamma, \xi, \omega$ (над O) с определяющими соотношениями*

$$N(\theta) = 1, \ \gamma^{\sigma-1} = 1, \ \omega^{\sigma-1} = \begin{cases} \xi^{p^s} & \text{при } t = \min(s, m), \\ \xi^{p^s} \theta^{p^t} & \text{при } t < \min(s, m). \end{cases}$$

Доказательство. Пусть $E_0 = \{\gamma, \Gamma\}$ и пусть $E_0 = \{\gamma, \varepsilon, \zeta, \varepsilon_1, \ldots \ldots, \varepsilon_{n-2}\}$, где $\varepsilon_j = N(\theta_j)$, $1 \leqslant j \leqslant n-2$. Если $\zeta = N(\xi)$, то по леммам 6 и 3 система

$$\theta_j^{\sigma^i}, \ \xi^{\sigma^i}, \ \Pi^{\sigma^i}, \ \gamma$$

линейно независима в K^*/K^{*p}. Но $N(\xi^{p^s}) = 1$, поэтому по теореме Гильберта $\alpha^{\sigma-1} = \xi^{p^s}$ при некотором $\alpha \in K^*$. По лемме 8 мы имеем

$$N(\alpha) = \alpha^{p^m} \xi^{-\varphi p^s},$$

а значит $N(\alpha) \in K^{*p}$. В то же время

$$(\alpha^{p^{m-1}} \xi^{-\varphi p^{s-1}})^{\sigma-1} = \xi^{p^{m+s-1}} \xi^{-p^{m+s-1}} N(\xi)^{p^{s-1}} = \zeta_1,$$

поэтому можно считать, что $N(\alpha) \equiv \varepsilon (\mathrm{mod}\, k^{*p})$. Так же, как и при доказательстве теоремы 6, теперь легко устанавливается, что система

$$\theta_j^{\sigma^i}, \ \xi^{\sigma^i}, \ \Pi^{\sigma^i}, \ \gamma, \ \alpha$$

образует базис в K^*/K^{*p}.

Элемент α не может быть простым в K (так как α и α^σ линейно зависимы в K^*/K^{*p}, лемма 6).

Легко видеть, что пара элементов $\alpha' \in K^*$ и $\xi' \in E$ также удовлетворяет условиям $N(\xi') = \zeta$, $\alpha'^{\sigma-1} = \xi'^{p^s}$ тогда и только тогда, когда $\xi' = \xi \beta^{\sigma-1}$, $\alpha' = \alpha \beta^{p^s} c$, где $\beta \in K^*$ и $c \in k^*$. Следовательно, при надлежащем выборе ζ и ξ в качестве α можно взять либо некоторую единицу $\omega \in E$, либо элемент вида $\omega \Pi^{-p^x}$, где $\omega \in E$ и $1 \leqslant x < \min(s, m)$. Во втором случае $\omega^{\sigma-1}=\xi^{p^s}\theta^{p^x}$. Для группы E мы получаем, таким образом, систему образующих (над O_p)

$$\theta_j^{\sigma^i},\ \xi^{\sigma^i},\ \theta^{\sigma^i},\ \gamma,\ \omega,$$

и для завершения доказательства теоремы 7 остается лишь проверить, что первый случай ($\alpha=\omega$) имеет место тогда и только тогда, когда $t=\min(s, m)$, а также что во втором случае $t=x$.

Пусть $\alpha=\omega$. Если $s\leqslant m$, то

$$\zeta_s=(\omega^{p^{m-s}}\xi^{-\varphi})^{\sigma-1};$$

если же $m\leqslant s$, то

$$\zeta_m=(\omega\xi^{-\varphi p^{s-m}})^{\sigma-1}.$$

Таким образом, при $\alpha=\omega$ мы имеем $t=\min(m, s)$.

Пусть теперь $\alpha=\omega\Pi^{-p^x}$, $1\leqslant x<\min(m, s)$. Корень ζ_s содержится в подгруппе, порожденной O-образующими ω, ξ, θ, и эта подгруппа выделяется в E прямым O-сомножителем. Следовательно, $\zeta_u\in E^{\sigma-1}$ тогда и только тогда, когда ζ_u выражается через $\omega^{\sigma-1}$, $\xi^{\sigma-1}$ и $\theta^{\sigma-1}$ (над O), т. е. когда

$$\zeta_u=N(\xi)^{p^{s-u}}=(\xi^{p^s}\theta^{p^x})^a\,\xi^{\mu(\sigma-1)}\theta^{\nu(\sigma-1)},$$

где $a\in O_p$, $\mu\in O$, $\nu\in O$. Для существования такого представления необходимо и достаточно, чтобы

$$ap^x\equiv 0\ (\mathrm{mod}\ p^m),\quad ap^s\equiv p^{m+s-u}\ (\mathrm{mod}\ p^{m+s})$$

при некотором $a\in O_p$, а для этого в свою очередь необходимо и достаточно выполнение неравенства $u\leqslant x$. Таким образом, наибольшее возможное значение для u равно x, т. е. $t=x$. Теорема 7 доказана полностью.

Теорема 7*. *Если* $(E_0:\{\zeta,\ \Gamma\})=p^h$, $0<h<m$, *то в E существуют O-образующие* $\theta_1, \ldots, \theta_{n-2}$, θ, γ, ξ, ω *с определяющими соотношениями*

$$N(\theta)=1,\quad \gamma^{\sigma-1}=1,\quad \omega^{\sigma-1}=\begin{cases}\gamma^{p^r}\xi^{p^s} & \textit{при}\ t=\min(s, m),\\ \gamma^{p^r}\xi^{p^s}\theta^{p^t} & \textit{при}\ t<\min(s, m).\end{cases}$$

Доказательство. Пусть $E_0=\{\gamma,\ \Gamma\}$ и пусть $E_0=\{\gamma, \varepsilon, \varepsilon_1, \ldots, \varepsilon_{n-1}\}$, причем $\varepsilon_j=N(\theta_j)$, $1\leqslant j\leqslant n-1$. Положим

$$\zeta=\gamma^{x_0}\varepsilon^{x}\varepsilon_1^{x_1}\ldots\varepsilon_{n-1}^{x_{n-1}}$$

(показатели здесь — целые p-адические числа). При надлежащем γ можно взять $x_0=p^h$. Так как ζ не является p-й степенью в E, то не все показатели $x_1, \ldots, x_{n-1}$ делятся на p. Положим

$$\bar\varepsilon=\varepsilon^{x}\varepsilon_1^{x_1}\ldots\varepsilon_{n-1}^{x_{n-1}}\in\Gamma,$$

$$\bar\varepsilon=N(\bar\xi).$$

Если $x_{n-1}\not\equiv 0\ (\mathrm{mod}\ p)$, то мы можем единицу ε_{n-1} заменить на $\bar\varepsilon$.

Так как $\zeta=\gamma^{p^h}N(\xi)$, то $N(\gamma^{p^r}\xi^{p^s})=1$, а значит при некотором $\alpha\in K^*$ будем иметь

$$\alpha^{\sigma-1}=\gamma^{p^r}\xi^{p^s}.$$

Далее доказательство проводится в том же плане, что и доказательство теоремы 7. При $p=2$ следует учесть, что в рассматриваемом случае $m\geqslant 2$.

Литература

1. K. Iwasawa. On Galois groups of local fields. Trans. Amer. Math. Soc., 1955, **80**, № 2, 448—469.
2. M. Krasner. Sur la représentation exponentielle dans les corps relativement galoisiens de nombres $\mathfrak{p}$-adiques. Acta arithm., 1939, **3**, 133—173.
3. D. Gilbarg. The structure of the group of $\mathfrak{p}$-adic 1-units. Duke Math. J., 1942, **9**, № 2, 262—271.
4. K. Iwasawa. On local cyclotomic fields. J. Math. Soc. Japan, 1960, **12**, № 1, 16—21.
5. З. И. Боревич. Мультипликативная группа регулярного локального поля с циклической группой операторов. Изв. АН СССР. сер, матем., 1964, **28**, № 3, 707—712.
6. Д. К. Фаддеев. К строению приведенной мультипликативной группы циклического расширения локального поля. Изв. АН СССР, сер. матем., 1960, **24**, № 2, 145—152.
7. G. E. Wahlin. The multiplicative representation of the principal units of a relative cyclic field. J. reine und angew. Math.,1932, **167**, 122—128.