Доклады Академии Наук СССР
1949. Том LXIV, № 1

*МАТЕМАТИКА*

И. Р. ШАФАРЕВИЧ

# ОБЩИЙ ЗАКОН ВЗАИМНОСТИ

*(Представлено академиком И. М. Виноградовым 13 XI 1948)*

В 1796 г. Гаусс доказал первый частный случай закона взаимности — квадратичный закон взаимности. В работах Гаусса, Якоби, Эйзенштейна, Куммера, Гильберта, Такаги, Артина, Хассе и других математиков закон взаимности был выведен в некоторых других частных случаях. Гильберт (²) поставил задачу о нахождении закона взаимности в наиболее общем случае. В настоящей заметке излагается решение этой задачи.

Относительно всех необходимых в дальнейшем определений и результатов читатель отсылается к обзору (¹).

Задача заключается в нахождении явной формулы для выражения:

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1}, \tag{1}$$

где $\left(\frac{\alpha}{\beta}\right)$ — символ степенного вычета $n$-й степени, а $\alpha$ и $\beta$ — два любых отличных от нуля числа произвольного поля алгебраических чисел $k$, содержащего корень степени $n$ из единицы.

Как показано в работе (¹), задача о нахождении в явном виде выражения (1) сводится к нахождению явной формы для символа норменного вычета $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$, а эта задача легко сводится к случаю, когда $n$ есть степень простого числа $n = p^m$. В этой же работе показано, что задача решается тривиально, если $(p, \mathfrak{p}) = 1$. Достаточно, следовательно, вывести явную формулу для $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$ при $n = p^m$, $p \equiv 0 \pmod{\mathfrak{p}}$.

При этом выводе мы будем основываться на давно замеченной аналогии между символом $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$ в теории алгебраических чисел и вычетом в точке $\mathfrak{p}$ $\operatorname{Res}_{\mathfrak{p}} \alpha\, d\beta$ абелева дифференциала $\alpha\, d\beta$ в теории алгебраических функций. Мы попытаемся вывести для символа $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$ формулу, аналогичную той, при помощи которой определяется вычет абелева дифференциала.

Для вычисления вычета дифференциала $\alpha\, d\beta$ в точке $\mathfrak{p}$ функции $\alpha$ и $\beta$ раскладываются в ряды Лорана по степеням локальной униформизирующей в этой точке. Но, как известно, в аналогии между алгебраическими функциями и алгебраическими числами аддитивным

формулам в теории алгебраических функций соответствуют мультипликативные формулы в теории алгебраических чисел. Поэтому естественно для определения $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$ представить $\alpha$ и $\beta$ в виде некоторых произведений. Для этого мы используем функцию $E(\alpha, x)$, введенную в работе (3).

Пусть $\alpha$ — число из неразветвленного $p$-адического расширения и

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots$$

его запись с коэффициентами $\alpha_i$, принадлежащими мультипликативной системе представителей, т. е. системе представителей состоящей из корней степени $p^f - 1$ из единицы, где $f$ — порядок $p$ в этом поле. Под $\alpha \to \alpha^P$ мы будем понимать автоморфизм неразветвленного поля, индуцирующий автоморфизм $\alpha \to \alpha^p$ в поле классов вычетов.

Рассмотрим формальный степенной ряд:

$$L(\alpha, x) = \sum_{n=0}^{\infty} p^{-n} \alpha^{P^n} x^{p^n}.$$

В работе (3) доказывается, что формально рассмотренный степенной ряд

$$E(\alpha, x) = e^{L(\alpha, x)}$$

будет иметь целые $p$-адические коэффициенты. Следовательно, он сходится для всех $x$, делящихся на простой делитель $p$.

Кроме того, функция $E(\alpha, x)$ удовлетворяет функциональному уравнению

$$E(\alpha + \beta, x) = E(\alpha, x) E(\beta, x).$$

Пусть $\bar{k}$ — $p$-адическое замыкание поля $k$. Так как $\bar{k}$ содержит корень степени $n$ из единицы, то показатель ветвления $e$ поля $\bar{k}$ делится на $p - 1$:

$$e = (p-1) e_1.$$

Можно доказать, что если $\varepsilon \equiv 1 \ (\mathfrak{p})$ в поле $\bar{k}$, то $\varepsilon$ может быть представлено в виде

$$\varepsilon = \prod E(\alpha_i, \pi^i) \cdot \zeta^{p^m A}, \tag{2}$$

где $\pi$ — любое простое число в $\bar{k}$, $\zeta$ — корень степени $p^m$ из единицы, а $\zeta^{p^m A}$ — $p^m$-примарное число из $\bar{k}$, записанное в форме, выведенной в работе (4). Значок $i$ в произведении пробегает все целые значения $0 < i < e + e_1$, взаимно простые с $p$. В дальнейшем во всех произведениях будет предполагаться, что индексы $i$, $j$ и $k$ пробегают эту систему значений.

Не исследуя более подробно единственность записи (2), заметим только, что в ней $\alpha_i$ определены однозначно $(\mathrm{mod}\, p^m)$, а $\zeta^{p^m A}$ — с точностью до множителя, равного $p^m$-й степени единицы поля $\bar{k}$.

Ясно, что любое число из $\bar{k}$ может быть представлено в виде

$$\alpha = \pi^a w \prod E(\alpha_i, \pi^i) \zeta^{p^m A}, \tag{3}$$

где $a$ — целое число, $w$ — корень степени $p^f - 1$ из единицы, а $\alpha_i$ и $\zeta^{p^m A}$ имеют объясненное выше значение.

Пользуясь представлением (3), мы введем символ $(\alpha, \beta)$, определенный для всех не равных нулю $\alpha$ и $\beta$ из $\bar{k}$, аналогичный вычету в теории алгебраических функций. Значением этого символа будет некоторое $p^m$-примарное число из $\bar{k}$, определенное с точностью до множителя, являющегося $p^m$-й степенью. В связи с этим все дальнейшие равенства надо понимать как равенства с точностью до множителя, являющегося $p^m$-й степенью.

Сначала при помощи формулы:

$$\left(\pi^a w \prod E(\alpha_i, \pi^i)\,\zeta^{p^m A},\ \ \pi^b w_1 \prod E(\beta_j, \pi^j)\,\zeta^{p^m B}\right) = \\ = (\pi, \pi)^{ab} \prod_{i,j} \left(E(\alpha_i, \pi^i),\ E(\beta_j, \pi^j)\right) \zeta^{p^m (aB - bA)} \tag{4}$$

мы сведем определение символа $(\alpha, \beta)$ для произвольной пары чисел к определению символов

$$(\pi, \pi) \quad \text{и} \quad (E(\alpha_i, \pi^i),\ E(\beta_j, \pi^j)).$$

Дальнейшая конструкция зависит от того, с каким случаем мы имеем дело: $p \neq 2$ или $p = 2$.

Сначала разберем случай $p \neq 2$. Здесь

$$(\pi, \pi) = 1. \tag{5}$$

Для определения символа

$$(E(\alpha, \pi^i),\ \ E(\beta, \pi^j))$$

представим число $E(j\alpha\beta, \pi^{i+j})$ в виде (2):

$$E(j\alpha\beta, \pi^{i+j}) = \prod_k E(\gamma_k, \pi^k)\,\zeta^{p^m C}.$$

Тогда, по определению:

$$(E(\alpha, \pi^i),\ E(\beta, \pi^j)) = \zeta^{p^m C}. \tag{6}$$

В случае $p = 2$ нужно несколько модифицировать эти определения. Для вычисления $(\pi, \pi)$ представим число $-1$ в виде (2)

$$-1 = \prod E(\delta_i, \pi^i)\,\zeta^{2^m D}.$$

Тогда:

$$(\pi, \pi) = \zeta^{2^m D}. \tag{7}$$

Для вычисления $(E(\alpha, \pi^i),\ E(\beta, \pi^j))$ представим в виде (2) число:

$$E(j\alpha\beta, \pi^{i+j}) \prod_{a,b}^{\infty} E\left((2^{a-1}i + 2^{b-1}j)\,\alpha^{2^a}\beta^{2^b},\ \pi^{2^a i + 2^b j}\right) = \prod E(\gamma_k, \pi^k)\,\zeta^{2^m C}.$$

Тогда, по определению:

$$(E(\alpha, \pi^i),\ \ E(\beta, \pi^j)) = \zeta^{2^m C}. \tag{8}$$

Формулы (4) — (8) определяют символ $(\alpha, \beta)$ для всех $\alpha$ и $\beta$ из $\bar{k}$. Следующие свойства этого символа легко следуют из определения:

1) билинейность, т. е.

$$(\alpha_1\alpha_2, \beta) = (\alpha_1, \beta)(\alpha_2, \beta)$$

и

$$(\alpha, \beta_1\beta_2) = (\alpha, \beta_1)(\alpha, \beta_2);$$

2) кососимметричность, т. е.

$$(\beta, \alpha) = (\alpha, \beta)^{-1}.$$

Как это имеет место и для вычета абелева дифференциала, наиболее глубоким свойством символа $(\alpha, \beta)$ является его инвариантность. Она устанавливается следующей теоремой.

Теорема 1. *Символ* $(\alpha, \beta)$ *зависит только от чисел* $\alpha$ *и* $\beta$ *и не зависит от выбора простого числа* $\pi$, *которое фигурирует в разложении* (2) *и в формулах* (4) — (8).

Символ норменного вычета связан очень просто с символом $(\alpha, \beta)$. Как показано в работе ([4]), число $A$ удовлетворяет уравнению

$$A^p - A = a,$$

где $a$ — целое число из поля инерции $\bar{k}$. Если под $S(a)$ подразумевать след в поле инерции $\bar{k}$ по отношению к полю рациональных $p$-адических чисел, то связь между символом норменного вычета и символом $(\alpha, \beta)$ может быть выражена следующим образом.

Теорема 2. *Если* $(\alpha, \beta) = \varepsilon^{p^m A}$, *то* $\left(\frac{\alpha, \beta}{p}\right) = \varepsilon^{S(a)}$.

Теорема 2 является простым следствием теоремы 1.

Все приведенные здесь результаты верны для чисел $\alpha$ и $\beta$ из произвольного дискретно нормированного поля характеристики нуль с совершенным полем классов вычетов. Это дает ответ на вопрос, поставленный в работе ([5]).

Поступило
13 XI 1948

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II, Leipzig, 1930. [2] D. Hilbert, Ges. Abh., 3, S. 310. [3] E. Artin u. H. Hasse, Abh. Math. Sem. Hamburg, 6 (1927). [4] H. Hasse, J. reine u. angew. Math., 176, 174 (1936). [5] E. Witt, ibid., 176, 153 (1936).