

Другими словами, первая группа когомологий тривиальна в обоих случаях.

Доказательство. Пусть $\{a_\sigma\}_{\sigma \in G}$ — 1-коцикл группы G в K^* . Соотношение, которому должен удовлетворять коцикл, в мультипликативной записи выглядит так:

$$a_0 a_\tau^\sigma = a_{\sigma\tau}.$$

В силу линейной независимости характеров существует $\theta \in K$, для которого элемент

$$\beta = \sum_{\tau \in G} a_\tau \tau(\theta)$$

отличен от нуля. Тогда

$$\sigma\beta = \sum_{\tau \in G} a_\tau^\sigma \sigma\tau(\theta) = \sum_{\tau \in G} a_{\sigma\tau} a_\sigma^{-1} \sigma\tau(\theta) = a_\sigma^{-1} \sum_{\tau \in G} a_{\sigma\tau} \sigma\tau(\theta) = a_\sigma^{-1} \beta.$$

Мы получаем, что $a_\sigma = \beta/\sigma\beta$, и использование β^{-1} вместо β дает нам то, что нужно.

Что касается аддитивной части теоремы, то найдем элемент $\theta \in K$, для которого след $\text{Tr}(\theta)$ не равен 0. Для заданного 1-коцикла $\{a_\sigma\}$ в аддитивной группе поля K положим

$$\beta = \frac{1}{\text{Tr}(\theta)} \sum_{\tau \in G} a_\tau \tau(\theta).$$

Сразу же получаем $a_\sigma = \beta - \sigma\beta$, что и требовалось.

§ 11. Алгебраическая независимость гомоморфизмов

Пусть A — аддитивная группа, K — поле и $\lambda_1, \dots, \lambda_n: A \rightarrow K$ — аддитивные гомоморфизмы. Мы будем говорить, что $\lambda_1, \dots, \lambda_n$ алгебраически зависимы (над K), если существует многочлен $f(X_1, \dots, X_n)$ в $K[X_1, \dots, X_n]$, такой, что

$$f(\lambda_1(x), \dots, \lambda_n(x)) = 0$$

для всех $x \in A$, но при этом f не индуцирует нулевую функцию на $K^{(n)}$, т. е. на прямом произведении K с собой n раз. Мы знаем, что с каждым многочленом f можно сопоставить однозначно определенный редуцированный многочлен, дающий ту же самую функцию. Если K бесконечно, то редуцированный многочлен совпадает с f . В нашем определении зависимости мы могли бы предполагать f редуцированным.

Многочлен $f(X_1, \dots, X_n)$ будет называться *аддитивным*, если он индуцирует аддитивный гомоморфизм $K^{(n)}$ в K . Пусть $(Y) = (Y_1, \dots, Y_n)$ — переменные, независимые от (X) . Положим

$$g(X, Y) = f(X + Y) - f(X) - f(Y),$$

где $X + Y$ обозначает результат покомпонентного сложения векторов. Тогда полная степень g , рассматриваемого как многочлен от (X) с коэффициентами в $K[Y]$, строго меньше, чем полная степень f , и аналогично его степень по каждому X_i не больше, чем степень f по этому X_i . Это сразу видно из рассмотрения разности одночленов $M_{(v)}(X + Y) - M_{(v)}(X) - M_{(v)}(Y) =$

$$= (X_1 + Y_1)^{v_1} \dots (X_n + Y_n)^{v_n} - X_1^{v_1} \dots X_n^{v_n} - Y_1^{v_1} \dots Y_n^{v_n}.$$

Аналогичное утверждение справедливо и для g , рассматриваемого как многочлен от (Y) с коэффициентами в $K[X]$. Отсюда вытекает, что если f редуцированный, то g также редуцированный. Следовательно, если f аддитивный, то g — нулевой многочлен.

ПРИМЕР. Пусть K имеет характеристику p . Тогда в случае одной переменной отображение

$$\xi \mapsto a\xi^{p^m},$$

где $a \in K$ и $m \geq 1$, аддитивно и задается аддитивным многочленом aX^{p^m} . Ниже мы увидим, что это типичный пример.

Теорема 18 (Артин). Пусть $\lambda_1, \dots, \lambda_n: A \rightarrow K$ — аддитивные гомоморфизмы аддитивной группы в поле. Если эти гомоморфизмы алгебраически зависят над K , то в $K[X]$ имеется аддитивный многочлен $f(X_1, \dots, X_n) \neq 0$, такой, что

$$f(\lambda_1(x), \dots, \lambda_n(x)) = 0$$

для всех $x \in A$.

Доказательство. Пусть $f(X) = f(X_1, \dots, X_n) \in K[X]$ — редуцированный многочлен наименьшей возможной степени, такой, что $f \neq 0$, но $f(\Lambda(x)) = 0$ для всех $x \in A$, где $\Lambda(x)$ — вектор $(\lambda_1(x), \dots, \lambda_n(x))$. Докажем, что f аддитивен.

Пусть $g(X, Y) = f(X + Y) - f(X) - f(Y)$. Тогда

$$g(\Lambda(x), \Lambda(y)) = f(\Lambda(x + y)) - f(\Lambda(x)) - f(\Lambda(y)) = 0$$

для всех $x, y \in A$. Мы утверждаем, что g индуцирует нулевую функцию на $K^{(n)} \times K^{(n)}$. Предположим противное. Возможны два случая.

Случай 1. Имеем $g(\xi, \Lambda(y)) = 0$ для всех $\xi \in K^{(n)}$ и для всех $y \in A$. По предположению существует вектор $\xi' \in K^{(n)}$, для которого $g(\xi', Y)$ не равен тождественно 0. Положим $P(Y) = g(\xi', Y)$. Так

как степень g по (Y) строго меньше степени f , то получаем противоречие.

Случай 2. Существуют $\xi' \in K^{(n)}$ и $y' \in A$, такие, что $g(\xi', \Lambda(y')) \neq 0$. Положим $P(X) = g(X, \Lambda(y'))$. Тогда $P(X)$ — ненулевой многочлен, но $P(\Lambda(x)) = 0$ для всех $x \in A$ — снова противоречие.

Таким образом, g индуцирует нулевую функцию на $K^{(n)} \times K^{(n)}$, чем и доказано нужное нам утверждение, а именно, что f аддитивен.

Рассмотрим теперь аддитивные многочлены более подробно.

Пусть f — аддитивный многочлен от n переменных над K и при этом редуцированный. Положим

$$f_i(X_i) = f(0, \dots, X_i, \dots, 0),$$

где X_i стоит на i -м месте, а остальные компоненты равны 0. В силу аддитивности

$$f(X_1, \dots, X_n) = f_1(X_1) + \dots + f_n(X_n),$$

поскольку разность между правой и левой частями есть редуцированный многочлен, принимающий на $K^{(n)}$ значение 0. Кроме того, f_i для каждого i — аддитивный многочлен от одной переменной. Сейчас мы изучим такие многочлены.

Пусть $f(X)$ — редуцированный многочлен от одной переменной, индуцирующий линейное отображение K в себя. Предположим, что в f встречается одночлен $a_r X^r$ с коэффициентом $a_r \neq 0$. Тогда одночлены степени r в

$$g(X, Y) = f(X + Y) - f(X) - f(Y)$$

задаются выражениями

$$a_r (X + Y)^r - a_r X^r - a_r Y^r.$$

Но, как мы уже видели, g тождественно равен 0. Следовательно, предыдущее выражение есть тождественный 0, так что многочлен

$$(X + Y)^r - X^r - Y^r$$

является нулевым. Но он содержит член $r X^{r-1} Y$. Следовательно, при $r > 1$ наше поле должно иметь характеристику p , а r должно делиться на p . Запишем $r = p^m s$, где s взаимно просто с p . Тогда

$$0 = (X + Y)^r - X^r - Y^r = (X^{p^m} + Y^{p^m})^s - (X^{p^m})^s - (Y^{p^m})^s.$$

Рассуждая, как и выше, заключаем, что $s = 1$.

Итак, если f — аддитивный многочлен от одной переменной, то

$$f(X) = \sum_{v=0}^m a_v X^{p^v},$$

где $a_i \in K$. В случае характеристики 0 единственными аддитивными многочленами от одной переменной являются многочлены вида aX , где $a \in K$.

Как и следовало ожидать, мы называем $\lambda_1, \dots, \lambda_n$ алгебраически независимыми, если любой редуцированный многочлен f , такой, что $f(\Lambda(x)) = 0$ для всех $x \in A$, является нулевым многочленом.

Применим теорему 18 к тому случаю, когда $\lambda_1, \dots, \lambda_n$ — автоморфизмы поля, и скомбинируем ее с теоремой о линейной независимости характеров.

Теорема 19. Пусть K — бесконечное поле и $\sigma_1, \dots, \sigma_n$ — различные элементы конечной группы автоморфизмов K . Тогда $\sigma_1, \dots, \sigma_n$ алгебраически независимы над K .

Доказательство (Артин). В случае характеристики 0 теорема 18 и линейная независимость характеров показывают, что наше утверждение верно. Пусть характеристика $p > 0$, и пусть $\sigma_1, \dots, \sigma_n$ алгебраически зависимы.

Существует аддитивный многочлен $f(X_1, \dots, X_n)$ в $K[X_1, \dots, X_n]$, такой, что $f \neq 0$, но

$$f(\sigma_1(x), \dots, \sigma_n(x)) = 0$$

для всех $x \in K$. В силу предыдущего мы можем записать это соотношение в виде

$$\sum_{i=1}^n \sum_{r=1}^m a_{ir} \sigma_i(x)^{p^r} = 0$$

для всех $x \in K$, причем не все коэффициенты a_{ir} равны 0. Поэтому в силу теоремы о линейной независимости характеров эндоморфизмы

$$\{x \mapsto \sigma_i(x)^{p^r}\} \quad \text{для } i = 1, \dots, n \text{ и } r = 1, \dots, m$$

не могут быть все различны. Следовательно, для всех $x \in K$ мы имеем

$$\sigma_i(x)^{pr} = \sigma_j(x)^{ps},$$

где либо $i \neq j$, либо $r \neq s$. Пусть, скажем, $r \leqslant s$. Извлечение корня p -й степени в характеристике p однозначно. Значит,

$$\sigma_i(x) = \sigma_j(x)^{ps-r} = \sigma_j(x^{ps-r})$$

для всех $x \in K$. Положим $\sigma = \sigma_j^{-1} \sigma_i$. Тогда

$$\sigma(x) = x^{ps-r}$$

для всех $x \in K$. Если $\sigma^n = \text{id}$, то

$$x = x^{pn(s-r)}$$

для всех $x \in K$. Поскольку K бесконечно, это возможно только при $s = r$. Но тогда $\sigma_i = \sigma_j$, вопреки тому факту, что мы начинали с различных автоморфизмов.

§ 12. Теорема о нормальном базисе

Теорема 20. Пусть K/k — конечное расширение Галуа степени n и $\sigma_1, \dots, \sigma_n$ — элементы его группы Галуа G . Тогда существует элемент $w \in K$, такой, что $\sigma_1 w, \dots, \sigma_n w$ образуют базис K над k .

Доказательство. Здесь мы докажем это только для случая, когда k бесконечно. В случае конечного поля k доказательство можно будет провести позднее методами линейной алгебры как упражнение.

Для всякого $\sigma \in G$ пусть X_σ — переменная и $t_{\sigma, \tau} = X_{\sigma^{-1}\tau}$. Положим $X_i = X_{\sigma_i}$. Пусть

$$f(X_1, \dots, X_n) = \det(t_{\sigma_i, \sigma_j}).$$

Тогда f не является тождественным нулем, что видно, если подставить 1 вместо X_{id} и 0 вместо X_σ для $\sigma \neq \text{id}$. Так как k бесконечно, то по теореме 19 определитель не может быть равным нулю при всех $x \in K$, если мы в f подставим $\sigma_i(x)$ вместо X_i . Следовательно, существует элемент $w \in K$, для которого

$$\det(\sigma_i^{-1}\sigma_j(w)) \neq 0.$$

Предположим, что элементы $a_1, \dots, a_n \in k$ таковы, что

$$a_1\sigma_1(w) + \dots + a_n\sigma_n(w) = 0.$$

Применим σ_i^{-1} к этому соотношению для каждого $i = 1, \dots, n$. Поскольку $a_j \in k$, мы получим систему линейных уравнений относительно неизвестных a_j . Так как определитель из коэффициентов $\neq 0$, то

$$a_j = 0 \quad \text{для } j = 1, \dots, n$$

и, следовательно, w будет искомым элементом.

УПРАЖНЕНИЯ

1. Пусть k — поле, X — переменная над k и

$$\varphi(X) = \frac{f(X)}{g(X)}$$

— рациональная функция из $k(X)$, представленная в виде отношения двух взаимно простых многочленов f, g . Определим степень φ как $\max(\deg f, \deg g)$.