§ 5. Норма и след

Пусть E — конечное расширение поля k, $[E:k]_s = r$. Положим также

$$p^\mu = [E:k]_i,$$

если характеристика равна $p > 0$, и 1 — в противном случае. Пусть $\sigma_1, \ldots, \sigma_r$ — различные вложения E в алгебраическое замыкание $\bar{k}$ поля k. Для всякого элемента α из E определим его *норму* из E в k формулой

$$N_k^E(\alpha) = \prod_{\nu=1}^{r} \sigma_\nu \alpha^{p^\mu} = \left(\prod_{\nu=1}^{r} \sigma_\nu \alpha\right)^{[E\ k]_i}.$$

Аналогично определяем *след*

$$\mathrm{Tr}_k^E(\alpha) = [E:k]_i \sum_{\nu=1}^{r} \sigma_\nu \alpha.$$

След равен 0, если $[E:k]_i > 1$, другими словами, если E/k не сепарабельно. Таким образом, если E сепарабельно над k, то

$$N_k^E(\alpha) = \prod_{\sigma} \sigma\alpha,$$

где произведение берется по всем различным вложениям E в $\bar{k}$ над k.

Аналогично, если E/k сепарабельно, то

$$\mathrm{Tr}_k^E(\alpha) = \sum_{\sigma} \sigma\alpha.$$

Теорема 8. *Пусть E/k — конечное расширение. Тогда норма N_k^E является мультипликативным гомоморфизмом E^* в k^*, а след — аддитивным гомоморфизмом E в k. Если $E \supset F \supset k$ — башня полей, то оба эти отображения транзитивны, или, что равносильно,*

$$N_k^E = N_k^F \circ N_F^E \quad \text{и} \quad \mathrm{Tr}_k^E = \mathrm{Tr}_k^F \circ \mathrm{Tr}_F^E.$$

Если $E = k(\alpha)$ и $f(X) = \mathrm{Irr}(\alpha, k, X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, то

$$N_k^{k(\alpha)}(\alpha) = (-1)^n a_0 \quad \text{и} \quad \mathrm{Tr}_k^{k(\alpha)}(\alpha) = -a_{n-1}.$$

Доказательство. Для доказательства первого утверждения заметим, что элемент α^{p^μ} сепарабелен над k, если $p^\mu = [E:k]_i$. С другой стороны, произведение

$$\prod_{\nu=1}^{r} \sigma_\nu \alpha^{p^\mu}$$

остается неподвижным при любом изоморфизме в $\bar{k}$, поскольку применение такого изоморфизма просто переставляет множители. Следовательно, это произведение должно лежать в k, так как α^{p^μ} сепарабелен над k. Аналогичное рассуждение применимо и к следу.

Что касается второго утверждения, то пусть $\{\tau_j\}$ — семейство различных вложений F в $\bar{k}$ над k. Продолжим каждое τ_j до изоморфизма $\bar{k}$ на $\bar{k}$ и обозначим это продолжение по-прежнему через τ_j. (Не теряя общности, мы можем предполагать, что $F \subset \bar{k}$.) Пусть $\{\sigma_i\}$ — семейство вложений E в $\bar{k}$ над F. Если σ — некоторое вложение E над k в $\bar{k}$, то $\tau_j^{-1}\sigma$ при каком-то j оставляет F неподвижным и, таким образом, $\tau_j^{-1}\sigma = \sigma_i$ для некоторого i. Следовательно, $\sigma = \tau_j\sigma_i$ и, значит, семейство $\{\tau_j\sigma_i\}$ дает все различные вложения E в $\bar{k}$ над k. В башнях степень несепарабельности мультипликативна, так что наше утверждение о транзитивности нормы и следа очевидно, поскольку, как мы уже показали, N_F^E отображает E в F, и аналогично для следа.

Предположим теперь, что $E = k(\alpha)$. Имеем

$$f(X) = ((X - \alpha_1) \dots (X - \alpha_r))^{[E:k]_i},$$

где $\alpha_1, \dots, \alpha_r$ — различные корни f. Рассмотрение постоянного члена f дает нам выражение для нормы, а рассмотрение второго члена — выражение для следа.

Заметим, что след является k-линейным отображением поля E в k, а именно

$$\mathrm{Tr}_k^E(c\alpha) = c\,\mathrm{Tr}_k^E(\alpha)$$

для всех $\alpha \in E$ и $c \in k$. Это очевидно, поскольку c остается неподвижным при всяком вложении E над k. Таким образом, след есть k-линейный функционал из E в k. Для простоты мы будем писать Tr вместо Tr_k^E.

Теорема 9. *Пусть E — конечное сепарабельное расширение поля k. Тогда функционал* $\mathrm{Tr}\colon E \to k$ *ненулевой. Отображение* $E \times E \to k$, *определяемое правилом*

$$(x, y) \longmapsto \mathrm{Tr}(xy),$$

билинейно и отождествляет E с дуальным ему пространством.

Доказательство. Тот факт, что Tr отличен от нуля, следует из теоремы о линейной независимости характеров. Для всякого $x \in E$ отображение

$$\mathrm{Tr}_x\colon E \to k,$$

для которого $\mathrm{Tr}_x(y) = \mathrm{Tr}(xy)$, будет, очевидно, k-линейным, и отображение

$$x \longmapsto \mathrm{Tr}_x$$

будет k-гомоморфизмом E в дуальное ему пространство $\hat{E}$. (Мы не обозначаем сейчас дуальное пространство через E^*, используя звездочку для обозначения мультипликативной группы поля E.) Если Tr_x — нулевое отображение, то $\mathrm{Tr}(xE) = 0$. Но $xE = E$ при $x \neq 0$. Следовательно, ядро отображения $x \longmapsto \mathrm{Tr}_x$ равно 0 и мы получаем инъективный гомоморфизм E в дуальное пространство $\hat{E}$. Так как эти пространства имеют одинаковую размерность, то, значит, мы получаем изоморфизм. Это доказывает нашу теорему.

Следствие 1. *Пусть* $\omega_1, \ldots, \omega_n$ *— базис* E *над* k. *Тогда существует базис* $\omega_1', \ldots, \omega_n'$ *пространства* E *над* k, *для которого* $\mathrm{Tr}(\omega_i \omega_j') = \delta_{ij}$.

Доказательство. Базис $\omega_1', \ldots, \omega_n'$ есть не что иное, как дуальный базис, который мы определили, когда рассматривали дуальное пространство для произвольного векторного пространства.

Следствие 2. *Пусть* E *— конечное сепарабельное расширение поля* k *и* $\sigma_1, \ldots, \sigma_n$ *— множество различных вложений* E *в* $\bar{k}$ *над* k. *Пусть* $w_1, \ldots, w_n$ *— некоторые элементы из* E. *Тогда векторы*

$$\xi_1 = (\sigma_1 w_1, \ldots, \sigma_1 w_n),$$
$$\ldots\ldots\ldots\ldots$$
$$\xi_n = (\sigma_n w_1, \ldots, \sigma_n w_n)$$

линейно независимы над $\bar{k}$ *в том и только в том случае, если* $w_1, \ldots, w_n$ *образуют базис* E *над* k.

Доказательство. Предположим, что $w_1, \ldots, w_n$ образуют базис расширения E/k. Пусть $\alpha_1, \ldots, \alpha_n$ — элементы из $\bar{k}$, для которых

$$\alpha_1 \xi_1 + \ldots + \alpha_n \xi_n = 0.$$

Тогда отображение

$$\alpha_1 \sigma_1 + \ldots + \alpha_n \sigma_n,$$

примененное к каждому из элементов $w_1, \ldots, w_n$, дает 0. Но $\sigma_1, \ldots, \sigma_n$ линейно независимы как характеры мультипликативной группы E^* в $\bar{k}^*$. Отсюда вытекает, что $\alpha_i = 0$ для $i = 1, \ldots, n$ и наши векторы линейно независимы.

Обратно, предположим, что $w_1, \ldots, w_n$ линейно зависимы над k. Тогда в E найдется элемент $\alpha \neq 0$, для которого $\mathrm{Tr}\,\alpha\omega_i = 0$

при всех i, откуда $\sum_{j=1}^{n} \sigma_j(\alpha)\,\xi_j = 0$. А это и означает, что векторы ξ_j линейно зависимы.

Замечание. В случае характеристики 0 тот факт, что след не равен тождественно 0, совсем тривиален. Действительно, если $c \in k$ и $c \neq 0$, то $\mathrm{Tr}(c) = nc$, где $n = [E : k]$ и $nc \neq 0$. Это соображение сохраняет силу также и в случае характеристики p, взаимно простой с n.

Предложение 1. *Пусть $E = k(\alpha)$—сепарабельное расширение, $f(X) = \mathrm{Irr}(\alpha, k, X)$ и $f'(X)$—производная многочлена $f(X)$. Пусть*

$$\frac{f(X)}{(X-\alpha)} = \beta_0 + \beta_1 X + \ldots + \beta_{n-1} X^{n-1},$$

где $\beta_i \in E$. Тогда дуальным базисом для $1, \alpha, \ldots, \alpha^{n-1}$ будет

$$\frac{\beta_0}{f'(\alpha)}, \ \ldots, \ \frac{\beta_{n-1}}{f'(\alpha)}.$$

Доказательство. Пусть $\alpha_1, \ldots, \alpha_n$ — различные корни f. Тогда

$$\sum_{i=1}^{n} \frac{f(X)}{(X-\alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)} = X^r \quad \text{для} \quad 0 \leqslant r \leqslant n-1.$$

Чтобы усмотреть это, обозначим через $g(X)$ разность левой и правой частей этого равенства. Тогда g — многочлен степени не более $n-1$, имеющий n корней $\alpha_1, \ldots, \alpha_n$. Следовательно, g тождественно равен нулю.

Многочлены

$$\frac{f(X)}{(X-\alpha_i)} \frac{\alpha_i^r}{f'(\alpha_i)}$$

все сопряжены между собой. Если мы назовем следом многочлена с коэффициентами в E многочлен, полученный применением следа к коэффициентам, то

$$\mathrm{Tr}\left[\frac{f(X)}{(X-\alpha)} \frac{\alpha^r}{f'(\alpha)}\right] = X^r.$$

Рассмотрев коэффициенты при каждой степени X в этом равенстве, мы найдем, что

$$\mathrm{Tr}\left(\alpha^i \frac{\beta_j}{f'(\alpha)}\right) = \delta_{ij},$$

что и доказывает наше предложение.