нашей теоремы имеем $p=2$ и $a=-4b^4$, где $b\in F$, откуда

$$\bar{k}=F\left(a^{1/2}\right)=F(i).$$

Но мы предполагали, что $i\in k_1$ — противоречие.

Остается доказать, что k имеет характеристику 0. Предположим, что k имеет характеристику >0 (но никакой буквы для обозначения характеристики мы не используем, поскольку p уже занято). Поле, получаемое присоединением примитивного корня из единицы ζ_{2^r} к простому полю $\mathbf{F}$, является циклическим над этим простым полем. В силу теоремы 4 из § 1 группа Галуа поля $\bar{k}$ над k, являющаяся циклической порядка 2 и порождаемая, скажем, элементом σ, соответствует некоторой подгруппе группы Галуа расширения $\mathbf{F}\left(\zeta_{2^r}\right)$ над $\mathbf{F}$. Однако расширение $\mathbf{F}\left(\zeta_{2^r}\right)$, будучи циклическим над $\mathbf{F}$, обладает только одним подполем степени 2 над $\mathbf{F}$, и это подполе должно содержать i, поскольку i имеет степень 1 или 2 над $\mathbf{F}$. Так как $\sigma i\neq i$, то неподвижное подполе в $\mathbf{F}\left(\zeta_{2^r}\right)$ относительно σ должно совпадать с $\mathbf{F}$. Это означает, что $\mathbf{F}\left(\zeta_{2^r}\right)$ имеет степень 2 над $\mathbf{F}$, что дает противоречие, если взять r достаточно большим.

Следствие 2 принадлежит Артину.

§ 10. Когомологии Галуа

Пусть G — группа и A — абелева группа, которую мы в наших общих замечаниях, предшествующих теореме, будем записывать аддитивно. Предположим, что G действует на A посредством гомоморфизма $G\to\operatorname{Aut}(A)$. Под *1-коциклом* группы G в A понимают семейство элементов $\{\alpha_\sigma\}_{\sigma\in G}$, где $\alpha_\sigma\in A$, удовлетворяющее соотношениям

$$\alpha_\sigma+\sigma\alpha_\tau=\alpha_{\sigma\tau}$$

для всех σ, $\tau\in G$. Если $\{\alpha_\sigma\}_{\sigma\in G}$ и $\{\beta_\sigma\}_{\sigma\in G}$ — 1-коциклы, то мы можем сложить их и получить 1-коцикл $\{\alpha_\sigma+\beta_\sigma\}_{\sigma\in G}$. Ясно, что 1-коциклы образуют группу; ее обозначают символом $Z^1(G, A)$. Семейство элементов $\{\alpha_\sigma\}_{\sigma\in G}$ называется *1-кограницей* группы G в A, если существует элемент $\beta\in A$, для которого $\alpha_\sigma=\sigma\beta-\beta$ при всех $\sigma\in G$. Ясно, что всякая 1-кограница является 1-коциклом и что 1-кограницы образуют группу, обозначаемую $B^1(G, A)$. Факторгруппа $Z^1(G, A)/B^1(G, A)$ называется первой группой когомологий группы G в A и обозначается символом $H^1(G, A)$.

Теорема 17. *Пусть K/k — конечное расширение Галуа с группой Галуа G. Тогда $H^1(G, K^*)=1$ для действия G на K^* и $H^1(G, K)=0$ для действия G на аддитивной группе поля K.*

Другими словами, первая группа когомологий тривиальна в обоих случаях.

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

$$\alpha_\sigma\alpha_\tau^\sigma=\alpha_{\sigma\tau}.$$

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

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

отличен от нуля. Тогда

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

Мы получаем, что $\alpha_\sigma=\beta/\sigma\beta$, 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 $\mathrm{Tr}(\theta)$ не равен 0. Для заданного 1-коцикла $\{\alpha_\sigma\}$ в аддитивной группе поля K положим

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

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

§ 11. Алгебраическая независимость гомоморфизмов

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

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

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.