§ 9. Уравнение $X^n - a = 0$

Когда корни из единицы не содержатся в основном поле, уравнение $X^n - a = 0$ по-прежнему представляет интерес, но требует более деликатного обращения.

Теорема 16. *Пусть k — поле, n — целое число $\geqslant 2$ и $a \in k$, $a \neq 0$, причем $a \notin k^p$ для всех простых чисел p, делящих n, и $a \notin -4k^4$, если $4 \mid n$. Тогда многочлен $X^n - a$ неприводим в $k[X]$.*

Доказательство. Наше первое предположение означает, что a не является p-й степенью в k. По индукции мы сведем нашу теорему к случаю, когда n — степень простого числа.

Запишем $n = p^r m$, где p взаимно просто с m и нечетно. Пусть

$$X^m - a = \prod_{\nu=1}^{m} (X - \alpha_\nu)$$

— разложение $X^m - a$ на линейные множители и, скажем, $\alpha = \alpha_1$. Подставляя X^{p^r} вместо X, получаем

$$X^n - a = X^{p^r m} - a = \prod_{\nu=1}^{m} (X^{p^r} - \alpha_\nu).$$

По индукции можно считать, что $X^m - a$ неприводим в $k[X]$. Мы утверждаем, что α не является p-й степенью в $k(\alpha)$. Действительно, пусть $\alpha = \beta^p$, $\beta \in k(\alpha)$ и N — норма из $k(\alpha)$ в k. Тогда

$$-a = (-1)^m N(\alpha) = (-1)^m N(\beta^p) = (-1)^m N(\beta)^p.$$

Если m нечетно, то a будет p-й степенью, что невозможно. Аналогично, если m четно (а p нечетно), мы также получаем противоречие. Это доказывает наше утверждение, поскольку m взаимно просто с p. Считая теорему известной для степеней простых чисел, заключаем, что многочлен $X^{p^r} - \alpha$ неприводим над $k(\alpha)$. Если A — корень многочлена $X^{p^r} - \alpha$, то $k \subset k(\alpha) \subset k(A)$ — башня, нижний этаж которой имеет степень m, а верхний — степень p^r. Отсюда вытекает, что A имеет степень n над k и что, следовательно, многочлен $X^n - a$ неприводим.

Пусть теперь $n = p^r$ — степень простого числа.

Предположим, что p совпадает с характеристикой. Пусть α — корень p-й степени из a. Тогда $X^p - a = (X - \alpha)^p$ и, следовательно, $X^{p^r} - a = (X^{p^{r-1}} - \alpha)^p$ при $r \geqslant 2$. По соображениям, еще более тривиальным, чем вышеприведенные, мы видим, что α не является p-й степенью в $k(\alpha)$ и, значит, $X^{p^{r-1}} - \alpha$ неприводим над $k(\alpha)$. Следовательно, $X^{p^r} - a$ неприводим над k.

Предположим, что p не совпадает с характеристикой. Снова рассуждаем по индукции. Пусть α — некоторый корень многочлена $X^p - a$. Сначала рассмотрим случай $r = 1$. Пусть ζ — примитивный корень p-й степени из единицы. Многочлен $X^p - a$ над $k(\zeta)$ либо неприводим, либо разлагается на линейные множители. Во втором случае $k(\alpha) \subset k(\zeta)$. Поскольку $k(\zeta)/k$ абелево, то $k(\alpha)$ есть расширение Галуа над k. Так как всякий сопряженный с α элемент имеет вид $\zeta'\alpha$, где ζ' — некоторый примитивный корень p-й степени из единицы, то $k(\alpha) = k(\zeta)$. Следовательно, все корни $X^p - a$, не лежащие в k, имеют одинаковую степень над k, делящую $p - 1$. Но это невозможно и, следовательно, многочлен $X^p - a$ неприводим. Пусть теперь $r \geqslant 2$. Положим $\alpha = \alpha_1$. Имеем

$$X^p - a = \prod_{\nu=1}^{p} (X - \alpha_\nu),$$

$$X^{p^r} - a = \prod_{\nu=1}^{p} (X^{p^{r-1}} - \alpha_\nu).$$

Предположим, что α не является p-й степенью в $k(\alpha)$. Пусть A — корень $X^{p^{r-1}} - \alpha$. Если p нечетно, то по индукции A имеет степень p^{r-1} над $k(\alpha)$, следовательно, степень p^r над k, и все готово. Если же $p = 2$, то предположим, что $\alpha = -4\beta^4$, где $\beta \in k(\alpha)$. Пусть N — норма из $k(\alpha)$ в k. Тогда $-a = N(\alpha) = 16N(\beta)^4$, т. е. $-a = b^2$, где $b \in k$. Ниже будет показано, что в этом случае из наших предположений относительно a вытекает неприводимость многочлена $X^{2^r} - a = X^{2^r} + b^2$. Предположим, что $\alpha = \beta^p$ для некоторого $\beta \in k(\alpha)$, и выведем из этого следствия.

Взяв норму из $k(\alpha)$ в k, находим

$$-a = (-1)^p N(\alpha) = (-1)^p N(\beta^p) = (-1)^p N(\beta)^p.$$

Если p нечетно, то a будет p-й степенью в k — противоречие. Следовательно, $p = 2$ и $-a = N(\beta)^2$ — квадрат в k. Запишем $-a = b^2$, где $b \in k$. Так как a не является квадратом в k, то заключаем, что и -1 не является квадратом в k. Пусть $i^2 = -1$. Над $k(i)$ справедливо разложение

$$X^{2^r} - a = X^{2^r} + b^2 = (X^{2^{r-1}} + ib)(X^{2^{r-1}} - ib).$$

Каждый множитель имеет степень 2^{r-1}, и мы рассуждаем по индукции. Если $X^{2^{r-1}} \pm ib$ приводим над $k(i)$, то $\pm ib$ либо есть квадрат в $k(i)$, либо лежит в $-4(k(i))^4$. В любом случае $\pm ib$ будет квадратом в $k(i)$, скажем

$$\pm ib = (c + di)^2 = c^2 + 2c\,di - d^2,$$

где c, $d \in k$. Отсюда получаем $c^2 = d^2$, т. е. $c = \pm d$, и $\pm ib = 2c\,di = \pm 2c^2 i$. Возведение в квадрат дает противоречие, а именно

$$a = -b^2 = -4c^4.$$

Из однозначности разложения на множители мы теперь заключаем, что $X^{2^r} + b^2$ не может разлагаться в $k[X]$ на множители, что и доказывает теорему.

Условия нашей теоремы необходимы, поскольку

$$X^4 + 4b^4 = (X^2 + 2bX + 2b^2)(X^2 - 2bX + 2b^2).$$

При $n = 4m$ и $a \in -4k^4$ многочлен $X^n - a$ приводим.

Следствие 1. *Пусть k — поле и для некоторого простого числа p элемент $a \in k$, $a \neq 0$, не является p-й степенью. Если p совпадает с характеристикой или же нечетно, то для всякого $r \geqslant 1$ многочлен $X^{p^r} - a$ неприводим.*

Доказательство. Это утверждение логически слабее, чем утверждение теоремы.

Следствие 2. *Пусть k — поле, причем алгебраическое замыкание $\bar{k}$ поля k имеет конечную степень > 1 над k. Тогда $\bar{k} = k(i)$, где $i^2 = -1$, и k имеет характеристику 0.*

Доказательство. Заметим, что $\bar{k}$ нормально над k. Если $\bar{k}$ несепарабельно над k, то $\bar{k}$ — чисто несепарабельно над некоторым подполем и имеет над ним степень > 1 (в силу гл. VII, § 7), следовательно, существуют подполе E, содержащее k, и элемент $a \in E$, такие, что $X^p - a$ неприводим над E. В силу следствия 1, $\bar{k}$ не может быть конечной степени над E. (Если читатель опустил § 7 гл. VII, то он может ограничиться рассмотрением случая характеристики 0.)

Итак, мы можем предполагать, что $\bar{k}$ является расширением Галуа над k. Пусть $k_1 = k(i)$. Тогда $\bar{k}$ будет расширением Галуа также и над k_1. Пусть G — группа Галуа $\bar{k}/k_1$. Предположим, что имеется простое число p, делящее порядок G. Пусть H — подгруппа порядка p и F — соответствующее неподвижное поле. Тогда $[\bar{k} : F] = p$. Если p равно характеристике, то упражнение 5 в конце главы дает противоречие. Поэтому мы можем предполагать, что p не равно характеристике. Тогда корни p-й степени из единицы, отличные от 1, являются корнями многочлена степени $\leqslant p - 1$ (а именно, $X^{p-1} + \ldots + 1$) и, следовательно, должны лежать в F. В силу теоремы 10 из § 6 отсюда вытекает, что $\bar{k}$ есть поле разложения некоторого многочлена $X^p - a$ с $a \in F$. Многочлен $X^{p^2} - a$ должен быть приводим. В силу

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 $G\to \mathrm{Aut}(A)$. 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.*