

# Глава VIII

## Теория Галуа

### § 1. Расширения Галуа

Пусть  $K$  — поле и  $G$  — группа автоморфизмов поля  $K$ . Мы будем обозначать через  $K^G$  подмножество в  $K$ , состоящее из всех элементов  $x \in K$ , таких, что  $x^\sigma = x$  для всех  $\sigma \in G$ . Это подмножество называется *неподвижным полем* группы  $G$ <sup>1)</sup>. Это действительно поле, поскольку из  $x, y \in K^G$  следует

$$(x + y)^\sigma = x^\sigma + y^\sigma = x + y$$

для всех  $\sigma \in G$  и аналогичным образом проверяется, что  $K^G$  замкнуто относительно умножения, вычитания и деления. Кроме того,  $K^G$  содержит 0 и 1 и, следовательно, содержит простое поле.

Алгебраическое расширение  $K$  поля  $k$  называется *расширением Галуа*, если оно нормально и сепарабельно. Мы будем считать  $K$  вложенным в некоторое алгебраическое замыкание. Группа автоморфизмов поля  $K$  над  $k$  называется *группой Галуа* поля  $K$  над  $k$  и обозначается символом  $G(K/k)$  или просто  $G$ . Она совпадает с множеством вложений поля  $K$  в  $\bar{K}$  над  $k$ .

Для удобства читателя мы сформулируем теперь основной результат теории Галуа для конечных расширений Галуа.

Пусть  $K$  — конечное расширение Галуа поля  $k$  с группой Галуа  $G$ . Тогда между множеством подполей  $E$  в  $K$ , содержащих  $k$ , и множеством подгрупп  $H$  в  $G$  существует биективное соответствие, задаваемое формулой  $E = K^H$ . Поле  $E$  будет расширением Галуа над  $k$  тогда и только тогда, когда подгруппа  $H$  нормальна в  $G$ , и в этом случае отображение  $\sigma \mapsto \sigma|_E$  индуцирует изоморфизм факторгруппы  $G/H$  на группу Галуа поля  $E$  над  $k$ .

Мы дадим доказательства шаг за шагом, причем, насколько возможно, мы даем их для бесконечных расширений.

Теорема 1. Пусть  $K$  — расширение Галуа поля  $k$ ,  $G$  — его группа Галуа. Тогда  $k = K^G$ . Если  $F$  — промежуточное поле,

<sup>1)</sup> Или, по другой терминологии, полем инвариантов группы  $G$ . — Прим. ред.

$k \subset F \subset G$ , то  $K$  — расширение Галуа над  $F$ . Отображение

$$F \mapsto G(K/F)$$

множества промежуточных полей в множество подгрупп группы  $G$  инъективно.

Доказательство. Пусть  $a \in K^G$  и  $\sigma$  — произвольное вложение поля  $k(a)$  в  $\bar{K}$ , индуцирующее тождественное отображение на  $k$ . Продолжим  $\sigma$  до вложения  $K$  в  $\bar{K}$ ; мы будем обозначать это продолжение по-прежнему через  $\sigma$ . Тогда  $\sigma$  — автоморфизм поля  $K$  над  $k$ , следовательно, элемент группы  $G$ . По предположению  $\sigma$  оставляет  $a$  неподвижным. Поэтому

$$[k(a) : k]_s = 1.$$

Так как  $a$  сепарабелен над  $k$ , то имеем  $k(a) = k$  и  $a$  есть элемент  $k$ . Это доказывает наше первое утверждение.

Пусть  $F$  — промежуточное поле. Тогда  $K$  нормально над  $F$  в силу теоремы 5 и сепарабельно над  $F$  в силу теоремы 9 из гл. VII. Следовательно,  $K$  — расширение Галуа над  $F$ . Если  $H = G(K/F)$ , то в силу доказанного выше заключаем, что  $F = K^H$ . Если  $F, F'$  — промежуточные поля и  $H = G(K/F)$ ,  $H' = G(K/F')$ , то

$$F = K^H \quad \text{и} \quad F' = K^{H'}.$$

Если  $H = H'$ , то  $F = F'$ , откуда вытекает, что отображение

$$F \mapsto G(K/F)$$

инъективно, что и доказывает нашу теорему.

Мы будем иногда называть группу  $G(K/F)$  над промежуточным полем  $F$  группой, ассоциированной с  $F$ . Мы будем говорить также, что подгруппа  $H$  в  $G$  принадлежит промежуточному полю  $F$ , если  $H = G(K/F)$ .

Следствие 1. Пусть  $K/k$  — расширение Галуа с группой  $G$ . Пусть  $F, F'$  — два промежуточных поля и  $H, H'$  — подгруппы в  $G$ , принадлежащие  $F, F'$  соответственно. Тогда  $H \cap H'$  принадлежит полю  $FF'$ .

Доказательство. Всякий элемент из  $H \cap H'$  оставляет  $FF'$  неподвижным, и всякий элемент из  $G$ , оставляющий  $FF'$  неподвижным, оставляет неподвижным также  $F$  и  $F'$  и, следовательно, лежит в  $H \cap H'$ . Это доказывает наше утверждение.

Следствие 2. (Обозначения те же, что и в следствии 1.) Неподвижное поле наименьшей подгруппы в  $G$ , содержащей  $H, H'$ , есть  $F \cap F'$ .

**Доказательство.** Очевидно.

**Следствие 3.** Пусть обозначения те же, что и в следствии 1. Тогда  $F \subset F'$  в том и только в том случае, если  $H' \subset H$ .

**Доказательство.** Если  $F \subset F'$  и  $\sigma \in H'$  оставляет  $F'$  неподвижным, то  $\sigma$  оставляет неподвижным и  $F$ , так что  $\sigma$  лежит в  $H$ . Обратно, если  $H' \subset H$ , то неподвижное поле группы  $H$  содержится в неподвижном поле группы  $H'$ , так что  $F \subset F'$ .

**Следствие 4.** Пусть  $E$  — конечное сепарабельное расширение поля  $k$  и  $K$  — наименьшее нормальное расширение поля  $k$ , содержащее  $E$ . Тогда  $K$  — конечное расширение Галуа над  $k$ . Существует лишь конечное число промежуточных полей  $F$ , таких, что  $k \subset F \subset E$ .

**Доказательство.** Мы знаем, что  $K$  нормально и сепарабельно. Далее,  $K$  конечно над  $k$ , поскольку это, как мы видели, конечный композит конечного числа сопряженных с  $E$  полей. Группа Галуа расширения  $K/k$  имеет лишь конечное число подгрупп. Следовательно, существует лишь конечное число подполей в  $K$ , содержащих  $k$ , и тем более лишь конечное число подполей в  $E$ , содержащих  $k$ .

Конечно, следствие 4 было уже доказано в предыдущей главе, но здесь мы получили другое доказательство с иной точки зрения.

**Лемма 1.** Пусть  $E$  — алгебраическое сепарабельное расширение поля  $k$ . Предположим, что существует целое число  $n \geq 1$ , такое, что всякий элемент  $a$  из  $E$  имеет степень  $\leq n$  над  $k$ . Тогда  $E$  конечно над  $k$  и  $[E : k] \leq n$ .

**Доказательство.** Пусть  $a$  — элемент из  $E$ , для которого степень  $[k(a) : k]$  максимальна, скажем равна  $m \leq n$ . Мы утверждаем, что  $k(a) = E$ . Если это не так, то существует элемент  $\beta \in E$ , такой, что  $\beta \notin k(a)$ , и в силу теоремы о примитивном элементе найдется элемент  $\gamma \in k(a, \beta)$ , для которого  $k(a, \beta) = k(\gamma)$ . Но из башни

$$k \subset k(a) \subset k(a, \beta)$$

мы видим, что  $[k(a, \beta) : k] > m$ , откуда вытекает, что  $\gamma$  имеет степень  $> m$  над  $k$ , — противоречие.

**Теорема 2** (Артин). Пусть  $K$  — поле и  $G$  — конечная группа автоморфизмов поля  $K$ , имеющая порядок  $n$ . Пусть  $k = K^G$  — соответствующее неподвижное поле. Тогда  $K$  — конечное расширение Галуа над  $k$  и его группа Галуа есть  $G$ . Кроме того,  $[K : k] = n$ .

**Доказательство.** Пусть  $a \in K$ , и пусть  $\sigma_1, \dots, \sigma_r$  — такое максимальное множество элементов из  $G$ , что  $\sigma_1 a, \dots, \sigma_r a$  различны. Для всякого  $\tau \in G$  наборы  $\{\tau\sigma_1 a, \dots, \tau\sigma_r a\}$  и  $\{\sigma_1 a, \dots, \sigma_r a\}$  отличаются лишь перестановкой, поскольку  $\tau$  инъективно и каждый элемент  $\tau\sigma_i a$  содержится в множестве  $\{\sigma_1 a, \dots, \sigma_r a\}$ , иначе это множество не было бы максимальным. Следовательно,  $a$  — корень многочлена

$$f(X) = \prod_{i=1}^r (X - \sigma_i a)$$

и для любого  $\tau \in G$  имеем  $f^\tau = f$ . Таким образом, коэффициенты многочлена  $f$  лежат в  $K^G = k$ . Кроме того,  $f$  сепарабелен. Следовательно, всякий элемент  $a$  из  $K$  есть корень сепарабельного многочлена степени  $\leq n$  с коэффициентами в  $k$ . Далее, этот многочлен разлагается на линейные множители в  $K$ . Таким образом,  $K$  сепарабельно над  $k$ , нормально над  $k$  и является поэтому расширением Галуа над  $k$ . В силу леммы 1 имеем  $[K : k] \leq n$ . Группа Галуа поля  $K$  над  $k$  имеет порядок  $\leq [K : k]$  (в силу теоремы 6 из гл. VII, § 4), и, следовательно, группа  $G$  должна быть полной группой Галуа. Этим доказаны все наши утверждения.

**Следствие.** Пусть  $K$  — конечное расширение Галуа поля  $k$  и  $G$  — его группа Галуа. Тогда всякая подгруппа в  $G$  принадлежит некоторому подполю  $F$ , такому, что  $k \subset F \subset K$ .

**Доказательство.** Пусть  $H$  — подгруппа в  $G$  и  $F = K^H$ . В силу теоремы Артина  $K$  — расширение Галуа над  $F$  с группой  $H$ .

**Замечание.** Для бесконечных расширений Галуа  $K$  поля  $k$  предыдущее следствие уже перестает быть справедливым. Это показывает, что использование того или иного вычислительного соображения действительно необходимо в доказательстве для конечного случая. В настоящем изложении использовано старомодное рассуждение. Читатель может посмотреть собственное доказательство Артина в его книге „Теория Галуа“. В бесконечном случае на группе Галуа  $G$  вводится топология Крулля (см. упражнения) и  $G$  превращается в компактную вполне несвязную группу. Подгруппы, принадлежащие промежуточным полям, — это *замкнутые* подгруппы. Если читатель желает полностью игнорировать бесконечный случай во всех наших рассмотрениях, он может это сделать без какого-либо ущерба для понимания. Доказательства для бесконечного случая обычно тождественны с доказательствами для конечного случая.

Понятия расширения Галуа и группы Галуа определяются чисто алгебраически. Следовательно, их формальное поведение при изоморфизмах точно такое же, какого можно ожидать от объектов в любой категории. Мы опишем это поведение для рассматриваемого случая в более ясном виде.

Пусть  $K$  — расширение Галуа поля  $k$  и

$$\lambda: K \rightarrow K^\lambda = \lambda K$$

— изоморфизм. Тогда  $K^\lambda$  — расширение Галуа поля  $k^\lambda$ ,

$$\begin{array}{ccc} K & \xrightarrow{\lambda} & K^\lambda \\ | & & | \\ k & \xrightarrow{\lambda} & k^\lambda \end{array}$$

Пусть  $G$  — группа Галуа поля  $K$  над  $k$ . Тогда отображение

$$\sigma \mapsto \lambda \circ \sigma \circ \lambda^{-1}$$

определяет гомоморфизм  $G$  в группу Галуа поля  $K^\lambda$  над  $k^\lambda$ , обратный к которому задается правилом

$$\lambda^{-1} \circ \tau \circ \lambda \leftarrow \tau.$$

Следовательно, группа  $G(K^\lambda/k^\lambda)$  изоморфна  $G(K/k)$  относительно предыдущего отображения. Мы можем записать это так:

$$G(\lambda K/\lambda k)^\lambda = G(K/k)$$

или

$$G(\lambda K/\lambda k) = \lambda G(K/k) \lambda^{-1},$$

где показатель  $\lambda$  означает „сопряжение“

$$\sigma^\lambda = \lambda^{-1} \circ \sigma \circ \lambda.$$

Контравариантности никак нельзя избежать, если мы хотим сохранить правило

$$(\sigma^\lambda)^\omega = \sigma^{\lambda\omega}$$

для композиции отображений  $\lambda$  и  $\omega$ .

Пусть, в частности,  $F$  — промежуточное поле,  $k \subset F \subset K$  и  $\lambda: F \rightarrow \lambda F$  — вложение  $F$  в  $K$ , предполагаемое продолженным до автоморфизма поля  $K$ . Тогда  $\lambda K = K$ . Следовательно,

$$G(K/\lambda F)^\lambda = G(K/F)$$

и

$$G(K/\lambda F) = \lambda G(K/F) \lambda^{-1}.$$

**Теорема 3.** Пусть  $K$  — расширение Галуа поля  $k$  с группой  $G$ . Пусть  $F$  — подполе,  $k \subset F \subset K$  и  $H = G(K/F)$ . Тогда для нормальности  $F$  над  $k$  необходимо и достаточно, чтобы подгруппа  $H$  была нормальной в  $G$ . Если  $F$  нормально над  $k$ , то отображение  $\sigma \mapsto \sigma|_F$  будет гомоморфизмом  $G$  на

группу Галуа поля  $F$  над  $k$ , ядро которого есть  $H$ . Таким образом  $G(F/k) \approx G/H$ .

**Доказательство.** Пусть  $F$  нормально над  $k$  и  $G'$  — его группа Галуа. Отображение ограничения  $\sigma \mapsto \sigma|F$  переводит  $G$  в  $G'$ , и по определению его ядро есть  $H$ . Следовательно,  $H$  нормальна в  $G$ . Кроме того, любой элемент  $\tau \in G'$  продолжается до вложения  $K$  в  $\bar{K}$ , которое должно быть автоморфизмом поля  $K$ , так что отображение ограничения сюръективно. Это доказывает последнее утверждение. Наконец, предположим, что  $F$  не нормально над  $k$ . Тогда существует вложение  $\lambda$  поля  $F$  в  $K$  над  $k$ , которое не является автоморфизмом, т. е.  $\lambda F \neq F$ . Продолжим  $\lambda$  до автоморфизма поля  $K$  над  $k$ . Группы Галуа  $G(K/\lambda F)$  и  $G(K/F)$  сопряжены и, принадлежа разным подполям, не могут совпадать. Следовательно, подгруппа  $H$  не нормальна в  $G$ .

Расширение Галуа  $K/k$  называется *абелевым* (соответственно *циклическим*), если его группа Галуа  $G$  абелева (соответственно циклическая).

**Следствие.** Пусть  $K/k$  — абелево (соответственно циклическое) расширение. Если  $F$  — промежуточное поле,  $k \subset F \subset K$ , то  $F$  — расширение Галуа над  $k$  и притом абелево (соответственно циклическое).

**Доказательство.** Это вытекает немедленно из того факта, что всякая подгруппа абелевой группы нормальна и всякая факторгруппа абелевой (соответственно циклической) группы абелева (соответственно циклическая).

**Теорема 4.** Пусть  $K$  — расширение Галуа поля  $k$ , а  $F$  — произвольное расширение, причем  $K, F$  — подполя некоторого другого поля. Тогда  $KF$  является расширением Галуа над  $F$ , а  $K$  — расширением Галуа над  $K \cap F$ . Пусть  $H$  — группа Галуа поля  $KF$  над  $F$  и  $G$  — группа Галуа поля  $K$  над  $k$ . Если  $\sigma \in H$ , то ограничение  $\sigma$  на  $K$  лежит в  $G$  и отображение

$$\sigma \mapsto \sigma|K$$

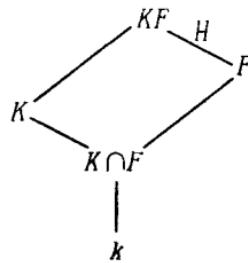
дает изоморфизм  $H$  на группу Галуа поля  $K$  над  $K \cap F$ .

**Доказательство.** Пусть  $\sigma \in H$ . Ограничение  $\sigma$  на  $K$  есть вложение поля  $K$  над  $k$ , следовательно, элемент группы  $G$ , поскольку  $K$  нормально над  $k$ . Отображение  $\sigma \mapsto \sigma|K$ , очевидно, является гомоморфизмом. Если  $\sigma|K$  тождественно, то  $\sigma$  должно быть тождественно на  $KF$  (так как всякий элемент из  $KF$  может быть выражен как комбинация сумм, произведений и отношений элементов из  $K$  и  $F$ ). Следовательно, наш гомоморфизм  $\sigma \mapsto \sigma|K$  инъективен. Пусть  $H'$  —

его образ. Тогда  $H'$  оставляет  $K \cap F$  неподвижным, и, обратно, если элемент  $a \in K$  неподвижен относительно  $H'$ , то  $a$  неподвижен и относительно  $H$ , откуда  $a \in F$  и  $a \in K \cap F$ . Поэтому  $K \cap F$  — соответствующее неподвижное поле. Если  $K$  конечно над  $k$  или даже если  $KF$  конечно над  $F$ , то в силу теоремы 2  $H'$  есть группа Галуа поля  $K$  над  $K \cap F$ , и теорема в этом случае доказана.

(В бесконечном случае нужно еще добавить замечание, что наше отображение  $\sigma \mapsto \sigma|K$  непрерывно, откуда вытекает, что его образ замкнут, поскольку  $H$  компактна.)

Следующая диаграмма иллюстрирует теорему 4:



Полезно мыслить себе противоположные стороны параллелограмма равными.

**Следствие.** Пусть  $K$  — конечное расширение Галуа и  $F$  — произвольное расширение поля  $k$ . Тогда  $[KF : F]$  делит  $[K : k]$ .

**Доказательство.** Пусть обозначения те же, что и выше. Как мы знаем, порядок группы  $H$  делит порядок группы  $G$ , откуда и вытекает наше утверждение.

**Предостережение.** Утверждение следствия, как правило, неверно, если  $K$  не является расширением Галуа над  $k$ . Например, пусть  $a = \sqrt[3]{2}$  — вещественный кубический корень из 2,  $\zeta$  — кубический корень из 1, не равный 1, скажем

$$\zeta = \frac{-1 + \sqrt{-3}}{2},$$

и пусть  $\beta = \zeta a$ . Рассмотрим  $E = \mathbf{Q}(\beta)$ . Так как  $\beta$  — комплексная величина, а  $a$  — вещественная, то  $\mathbf{Q}(\beta) \neq \mathbf{Q}(a)$ . Положим  $F = \mathbf{Q}(a)$ . Тогда  $E \cap F$  будет подполем в  $E$ , степень которого над  $\mathbf{Q}$  делит число 3. Следовательно, эта степень есть 3 или 1 и, значит, должна быть равна 1, поскольку  $E \neq F$ . Но

$$EF = \mathbf{Q}(a, \beta) = \mathbf{Q}(a, \zeta) = \mathbf{Q}(a, \sqrt{-3})$$

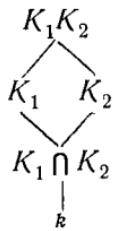
Следовательно,  $EF$  имеет степень 2 над  $F$ .

**Теорема 5.** Пусть  $K_1$  и  $K_2$  — расширения Галуа над полем  $k$  с группами Галуа  $G_1$  и  $G_2$  соответственно. Предположим, что  $K_1$ ,  $K_2$  — подполя некоторого поля. Тогда  $K_1K_2$  — расширение Галуа над  $k$ . Пусть  $G$  — его группа Галуа. Отобразим  $G \rightarrow G_1 \times G_2$  посредством ограничений, а именно

$$\sigma \mapsto (\sigma|K_1, \sigma|K_2).$$

Это отображение инъективно. Если  $K_1 \cap K_2 = k$ , то это отображение есть изоморфизм.

**Доказательство.** Нормальность и сепарабельность сохраняются при взятии композита двух полей, так что  $K_1K_2$  есть расширение Галуа над  $k$ . Наше отображение, очевидно, является гомоморфизмом  $G$  в  $G_1 \times G_2$ . Если элемент  $\sigma \in G$  индуцирует тождественные автоморфизмы на  $K_1$  и  $K_2$ , то он индуцирует тождественный автоморфизм и на их композите, так что наше отображение инъективно. Предположим, что  $K_1 \cap K_2 = k$ . Согласно теореме 4, для заданного элемента  $\sigma_1 \in G_1$  найдется элемент  $\sigma$  из группы Галуа поля  $K_1K_2$  над  $K_2$ , индуцирующий  $\sigma_1$  на  $K_1$ . Этот элемент  $\sigma$  наверняка лежит в  $G$  и индуцирует тождественное отображение на  $K_2$ . Следовательно,  $G_1 \times \{e_2\}$  содержится в образе нашего гомоморфизма (где  $e_2$  — единичный элемент группы  $G_2$ ). Аналогично  $\{e_1\} \times G_2$  содержится в этом образе. Следовательно, их произведение содержится в образе, а их произведение есть в точности  $G_1 \times G_2$ . Это доказывает теорему 5.



**Следствие 1.** Пусть  $K_1, \dots, K_n$  — расширения Галуа поля  $k$  с группами Галуа  $G_1, \dots, G_n$ . Предположим, что  $K_{i+1} \cap (K_1 \dots K_i) = k$  для каждого  $i = 1, \dots, n-1$ . Тогда группа Галуа композита  $K_1 \dots K_n$  естественным образом изоморфна произведению  $G_1 \times \dots \times G_n$ .

**Доказательство.** Индукция.

**Следствие 2.** Пусть  $K$  — конечное расширение Галуа поля  $k$  с группой  $G$ , причем  $G$  может быть представлена в виде прямого произведения  $G = G_1 \times \dots \times G_n$ . Пусть  $K_i$  — неподвижное поле группы

$$G_1 \times \dots \times \{1\} \times \dots \times G_n,$$

где группа из одного элемента стоит на  $i$ -м месте. Тогда  $K_i$  — расширение Галуа над  $k$  и  $K_{i+1} \cap (K_1 \dots K_i) = k$ . Кроме того,  $K = K_1 \dots K_n$ .

**Доказательство.** В силу следствия 1 теоремы 1 композит всех  $K_i$  принадлежит пересечению соответствующих групп, состоящему, очевидно, из единицы. Следовательно, композит равен  $K$ . Каждый прямой множитель группы  $G$  нормален в  $G$ , так что  $K_i$  — расширение Галуа над  $k$ . В силу следствия 2 теоремы 1 пересечение нормальных расширений принадлежит произведению соответствующих им групп, откуда ясно, что  $K_{i+1} \cap (K_1 \dots K_i) = k$ .

## § 2. Примеры и приложения

Пусть  $k$  — поле,  $f(X)$  — многочлен степени  $\geq 1$  из  $k[X]$  и

$$f(X) = (X - a_1) \dots (X - a_n)$$

— его разложение на множители в поле разложения  $K$  над  $k$ . Пусть  $G$  — группа Галуа поля  $K$  над  $k$ . Мы называем  $G$  группой Галуа многочлена  $f(X)$  над  $k$ . Элементы из  $G$  переставляют корни многочлена  $f$ . Таким образом, мы имеем инъективный гомоморфизм группы  $G$  в симметрическую группу  $S_n$  на  $n$  элементах. Не всякая перестановка обязательно задается некоторым элементом из  $G$ . Ниже мы рассмотрим примеры.

**ПРИМЕР 1.** Пусть  $k$  — поле и  $a \in k$ . Если  $a$  не является квадратом в  $k$ , то многочлен  $X^2 - a$  не имеет корня в  $k$  и потому неприводим. Предположим, что  $\text{char} \neq 2$ . Тогда многочлен сепарабелен (поскольку  $a \neq 0$ ), и если  $a$  — некоторый его корень, то  $k(a)$  — поле разложения, являющееся расширением Галуа. Его группа Галуа — циклическая порядка 2. Выделение полного квадрата показывает, что так описывается всякое квадратичное расширение (для  $\text{char} \neq 2$ ).

**ПРИМЕР 2.** Пусть  $k$  — поле характеристики  $\neq 2$  или 3,  $f(X) = X^3 + bX + c$  — многочлен над  $k$ . (Любой многочлен степени 3 может быть приведен к такому виду посредством выделения полного куба.) Если  $f$  не имеет корней в  $k$ , то  $f$  неприводим (любое разложение на множители должно содержать множитель степени 1). Если  $a$  — корень многочлена  $f(X)$ , то  $[k(a) : k] = 3$ . Пусть  $K$  — поле разложения и  $G$  — его группа Галуа. Тогда  $G$  имеет порядок 3 или 6, поскольку  $G$  есть подгруппа симметрической группы  $S_3$ . Во втором случае  $k(a)$  не будет нормальным над  $k$ .

Имеется простой способ проверить, является ли группа Галуа полной симметрической группой. Рассмотрим дискриминант. Положим

$$\delta = (a_1 - a_2)(a_2 - a_3)(a_1 - a_3) \text{ и } \Delta = \delta^2,$$