Предположим, что $K \supset E \supset k$ и что K нормально над k. Пусть σ — некоторое вложение K над E. Тогда σ есть также вложение K над k, и наше утверждение справедливо по определению.

Наконец, если K_1, K_2 нормальны над k, то для любого вложения σ поля K_1K_2 над k имеем

$$\sigma(K_1K_2) = \sigma(K_1)\,\sigma(K_2),$$

и наше утверждение снова вытекает из сделанных предположений. Утверждение, касающееся пересечения, справедливо потому, что

$$\sigma(K_1 \cap K_2) = \sigma(K_1) \cap \sigma(K_2).$$

Заметим, что если K — конечно порожденное нормальное расширение над k, скажем $K = k(\alpha_1, \ldots, \alpha_n)$, и $p_1, \ldots, p_n$ — соответствующие неприводимые многочлены для $\alpha_1, \ldots, \alpha_n$ над k, то K есть уже поле разложения для конечного семейства $p_1, \ldots, p_n$. Позже мы исследуем, когда K будет полем разложения для одного неприводимого многочлена.

§ 4. *Сепарабельные расширения*

Пусть E — алгебраическое расширение поля F и

$$\sigma\colon F \to L$$

— вложение F в алгебраически замкнутое поле L. Исследуем более подробно продолжения σ на E. Любое такое продолжение σ отображает E на подполе в L, алгебраическое над σF. Таким образом, для наших целей мы можем предполагать, что L алгебраично над σF и, следовательно, совпадает с алгебраическим замыканием поля σF.

Обозначим через S_σ множество продолжений σ до вложения E в L.

Пусть L' — другое алгебраически замкнутое поле, и пусть $\tau\colon F \to L'$ — вложение. Мы предполагаем, как и выше, что L' есть алгебраическое замыкание поля τF. В силу теоремы 2 существует изоморфизм $\lambda\colon L \to L'$, продолжающий отображение $\tau \circ \sigma^{-1}$, определенное на σF. Это иллюстрируется следующей диаграммой:

$$\begin{tikzcd}
L' & & L \arrow[ll, "\lambda"'] \\
 & E \arrow[ul] \arrow[ur, "\sigma^*"] & \\
\tau F \arrow[uu] & F \arrow[l, "\tau"] \arrow[r, "\sigma"'] \arrow[u] & \sigma F \arrow[uu]
\end{tikzcd}$$

Обозначим через S_τ множество вложений E в L', продолжающих τ.

Если $\sigma^* \in S_\sigma$ — продолжение σ до вложения E в L, то $\lambda \circ \sigma^*$ будет продолжением τ до вложения E в L', поскольку при ограничении на F мы имеем

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

Таким образом, λ индуцирует отображение S_σ в S_τ. Ясно, что обратное отображение индуцируется изоморфизмом λ^{-1} и, следовательно, S_σ, S_τ приводятся во взаимно однозначное соответствие отображением

$$\sigma^* \to \lambda \circ \sigma^*.$$

В частности, мощность S_σ, S_τ одна и та же. Таким образом, эта мощность зависит только от расширения E/F; мы будем обозначать ее через

$$[E : F]_s$$

и называть *сепарабельной степенью* E над F. Она представляет интерес главным образом в том случае, когда E/F конечно.

Теорема 6. *Для всякой башни* $E \supset F \supset k$

$$[E : k]_s = [E : F]_s [F : k]_s.$$

Если, кроме того, E конечно над k, то $[E: k]_s$ конечна и

$$[E : k]_s \leqslant [E : k].$$

Таким образом, сепарабельная степень не превосходит степени.

Доказательство. Пусть σ: $k \to L$ — вложение поля k в алгебраически замкнутое поле L, $\{\sigma_i\}_{i \in I}$ — семейство различных продолжений σ на F, и для каждого i пусть $\{\tau_{ij}\}$ — семейство различных продолжений σ_i на E. В силу доказанного выше каждое σ_i имеет ровно $[E : F]_s$ продолжений до вложения E в L. Множество вложений $\{\tau_{ij}\}$ содержит ровно

$$[E : F]_s [F : k]_s$$

элементов. Всякое вложение E в L над σ должно быть одним из τ_{ij}, и, таким образом, мы видим, что первая формула выполняется, т. е. имеет место мультипликативность сепарабельных степеней в башнях.

Что касается второго утверждения, то предположим, что E/k конечно. Тогда мы можем получить E как башню расширений, каждый этаж которой порождается одним элементом

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \ldots \subset k(\alpha_1, \ldots, \alpha_r) = E.$$

Если мы определим индуктивно $F_{\nu+1} = F_\nu(\alpha_{\nu+1})$, то в силу предложения 8 из § 2 будем иметь

$$[F_\nu(\alpha_{\nu+1}) : F_\nu]_s \leqslant [F_\nu(\alpha_{\nu+1}) : F_\nu].$$

Таким образом, наше неравенство выполняется для каждого этажа башни. В силу мультипликативности отсюда вытекает, что неравенство справедливо для расширения E/k, что и требовалось показать.

Следствие. *Пусть E конечно над k и $E \supset F \supset k$. Равенство $[E : k]_s = [E : k]$ выполняется тогда и только тогда, когда соот-*

ветствующее равенство выполняется для каждого этажа башни, т. е. для E/F и F/k.

Доказательство. Очевидно.

Позднее будет показано (это нетрудно показать), что $[E:k]_s$ делит степень $[E:k]$, когда E конечно над k. Определим $[E:k]_i$ как частное, так что

$$[E:k]_s\,[E:k]_i = [E:k].$$

Из мультипликативности в башнях степени и сепарабельной степени вытекает, что символ $[E:k]_i$ также мультипликативен в башнях. Мы будем иметь с ним дело в § 7.

Пусть E — конечное расширение поля k. Мы будем говорить, что E *сепарабельно* над k, если $[E:k]_s = [E:k]$. Алгебраический над k элемент α называется *сепарабельным* над k, если $k(\alpha)$ сепарабельно над k. Мы видим, что это условие эквивалентно тому, что неприводимый многочлен $\operatorname{Irr}(\alpha, k, X)$ не имеет кратных корней.

Многочлен $f(X) \in k[X]$ называется *сепарабельным*, если у него нет кратных корней. Если α — корень сепарабельного многочлена $g(X) \in k[X]$, то неприводимый многочлен элемента α над k делит g и, следовательно, α сепарабелен над k.

Сейчас мы сделаем несколько дополнительных замечаний к предложению 8. Читатель может опустить эти замечания, если он интересуется только полями характеристики 0 или сепарабельными расширениями.

Пусть $f(X) = (X-\alpha)^m g(X)$ — многочлен из $k[X]$, причем $g(X)$ не делится на $X-\alpha$. Напомним, что m называется кратностью α в f. Мы говорим, что α — *кратный* корень f, если $m > 1$. В противном случае мы говорим, что α — *простой* корень.

Предложение 9. *Пусть α — алгебраический элемент над k, $\alpha \in \bar{k}$, и пусть $f(X) = \operatorname{Irr}(\alpha, k, X)$. Если $\operatorname{char} k = 0$, то все корни многочлена f имеют кратность 1 (f сепарабелен). Если $\operatorname{char} k = p > 0$, то существует целое число $\mu \geqslant 0$, такое, что всякий корень f имеет кратность p^μ. Далее,*

$$[k(\alpha):k] = p^\mu\,[k(\alpha):k]_s$$

и элемент α^{p^μ} сепарабелен над k.

Доказательство. Пусть $\alpha_1, \ldots, \alpha_r$ — различные корни многочлена f в $\bar{k}$ и m — кратность корня $\alpha = \alpha_1$ в f. Для всякого $1 \leqslant i \leqslant r$ существует изоморфизм

$$\sigma\colon\ k(\alpha) \to k(\alpha_i)$$

над k, для которого $\sigma\alpha = \alpha_i$. Продолжим σ до автоморфизма поля $\bar{k}$; будем обозначать это продолжение по-прежнему через σ. Так как

коэффициенты f лежат в k, то $f^{\sigma} = f$. Заметим, что

$$f(X) = \prod_{i=1}^{r} (X - \sigma\alpha_i)^{m_i},$$

где m_i — кратность α_i в f. В силу однозначности разложения на множители заключаем, что $m_i = m_1$ и, следовательно, все m_i равны одному и тому же целому числу m.

Рассмотрим производную $f'(X)$. Если f и f' имеют общий корень, то α будет корнем многочлена меньшей степени, чем $\deg f$. Это невозможно, за исключением случая, когда $\deg f' = -\infty$, другими словами, когда производная f' тождественно равна 0. Если характеристика равна 0, этого не может произойти. Следовательно, если f имеет кратные корни, то мы имеем случай характеристики p и $f(X) = g(X^p)$ для некоторого многочлена $g(X) \in k[X]$. Поэтому α^p — корень многочлена g, степень которого $< \deg f$. Продолжая по индукции, мы получим наименьшее целое число $\mu \geqslant 0$, такое, что α^{p^μ} является корнем сепарабельного многочлена из $k[X]$, а именно такого многочлена h, для которого

$$f(X) = h(X^{p^\mu}).$$

Сравнивая степени f и g, заключаем, что

$$[k(\alpha) : k(\alpha^p)] = p.$$

По индукции находим

$$[k(\alpha) : k(\alpha^{p^\mu})] = p^\mu.$$

Так как h имеет корни кратности 1, то

$$[k(\alpha^{p^\mu}) : k]_s = [k(\alpha^{p^\mu}) : k]$$

и, сравнивая степени многочленов f и h, мы видим, что число различных корней у f равно числу различных корней у h. Следовательно,

$$[k(\alpha) : k]_s = [k(\alpha^{p^\mu}) : k]_s.$$

Отсюда наша формула для степеней вытекает в силу мультипликативности, так что утверждение доказано. Отметим, что корнями многочлена h являются

$$\alpha_1^{p^\mu}, \ldots, \alpha_r^{p^\mu}.$$

Следствие 1. *Для любого конечного расширения E поля k сепарабельная степень $[E : k]_s$ делит степень $[E : k]$. Частное равно 1 в случае поля характеристики 0 и равно некоторой степени p в случае поля характеристики $p > 0$.*

Доказательство. Разложим E/k в башню, каждый этаж которой порождается одним элементом, и применим предложение 9 с учетом мультипликативности наших индексов в башнях.

Если E/k конечно, то мы называем

$$\frac{[E:k]}{[E:k]_s}$$

несепарабельной степенью (или *степенью несепарабельности*) и обозначаем ее через $[E:k]_i$. Таким образом,

$$[E:k]_s\,[E:k]_i = [E:k].$$

Следствие 2. *Конечное расширение сепарабельно тогда и только тогда, когда* $[E:k]_i = 1$.

Доказательство. По определению.

Следствие 3. *Если* $E \supset F \supset k$ — *два конечных расширения, то*

$$[E:k]_i = [E:F]_i\,[F:k]_i.$$

Доказательство. Очевидно.

Отметим, что если элемент α сепарабелен над k и F — произвольное расширение поля k, то α сепарабелен над F. Действительно, если f — сепарабельный многочлен из $k[X]$, для которого $f(\alpha) = 0$, то, поскольку коэффициенты f лежат также и в F, α сепарабелен и над F. (Можно сказать, что сепарабельный элемент остается сепарабельным при подъеме.)

Теорема 7. *Пусть E — конечное расширение поля k. Тогда для сепарабельности E над k необходимо и достаточно, чтобы каждый элемент из E был сепарабельным над k.*

Доказательство. Пусть E сепарабельно над k и $\alpha \in E$. Рассмотрим башню

$$k \subset k(\alpha) \subset E.$$

В силу теоремы 6 мы должны иметь равенство $[k(\alpha):k] = [k(\alpha):k]_s$, означающее, что α сепарабелен над k. Обратно, предположим, что каждый элемент из E сепарабелен над k. Мы можем записать $E = k(\alpha_1, \ldots, \alpha_n)$, где каждый α_i сепарабелен над k. Рассмотрим башню

$$k \subset k(\alpha_1) \subset k(\alpha_1, \alpha_2) \subset \ldots \subset k(\alpha_1, \ldots, \alpha_n).$$

Будучи сепарабельным над k, каждый элемент α_i сепарабелен над $k(\alpha_1, \ldots, \alpha_{i-1})$ при $i \geqslant 2$. Следовательно, по теореме о башне E сепарабельно над k.

Заметим, что наше последнее рассуждение показывает, что если E порождается конечным числом элементов, каждый из которых сепарабелен над k, то E сепарабельно над k.

Пусть E — произвольное алгебраическое расширение поля k. Будем говорить, что E *сепарабельно* над k, если всякое его конечно

порожденное подрасширение сепарабельно над k, т. е. если всякое расширение $k(\alpha_1, \ldots, \alpha_n)$, где $\alpha_1, \ldots, \alpha_n \in E$, сепарабельно над k.

Теорема 8. *Пусть E — алгебраическое расширение поля k, порожденное семейством $\{\alpha_i\}_{i \in I}$. Если каждый элемент α_i сепарабелен над k, то E сепарабельно над k.*

Доказательство. Всякий элемент из E лежит в некотором конечно порожденном подполе $k(\alpha_{i_1}, \ldots, \alpha_{i_n})$; как мы отметили выше, каждое такое подполе сепарабельно над k. Следовательно, в силу теоремы 7, всякий элемент из E сепарабелен над k, что и завершает доказательство.

Теорема 9. *Сепарабельные расширения образуют отмеченный класс расширений.*

Доказательство. Пусть E сепарабельно над k и $E \supset F \supset k$. Всякий элемент из E сепарабелен над F, и всякий элемент из F, будучи элементом из E, сепарабелен над k. Следовательно, каждый этаж в башне сепарабелен. Обратно, предположим, что $E \supset F \supset k$ — некоторое расширение, для которого E/F сепарабельно и F/k сепарабельно. Если E конечно над k, то мы можем применить теорему 6. А именно мы имеем равенство сепарабельной степени и степени в каждом этаже башни, откуда в силу мультипликативности вытекает равенство степеней для E над k.

Пусть теперь E бесконечно и $\alpha \in E$. Тогда α будет корнем сепарабельного многочлена $f(X)$ с коэффициентами из F. Пусть этими коэффициентами будут $a_n, \ldots, a_0$. Положим $F_0 = k(a_n, \ldots, a_0)$. Тогда F_0 сепарабельно над k и α сепарабелен над F_0. Теперь из рассмотрения конечной башни

$$k \subset F_0 \subset F_0(\alpha)$$

заключаем, что $F_0(\alpha)$ сепарабельно над k и что, следовательно, α сепарабелен над k. Это доказывает условие (i) в определении „отмеченности“.

Пусть E сепарабельно над k и F — произвольное расширение поля k, причем оба расширения E, F являются подполями некоторого поля. Всякий элемент из E сепарабелен над k, а потому сепарабелен над F. Так как EF порождается над F всеми элементами из E, то EF сепарабельно над F в силу теоремы 8. Это доказывает условие (ii) в определении „отмеченности“ и завершает доказательство нашей теоремы.

Пусть E — конечное расширение над k. Пересечение всех нормальных расширений K поля k (в алгебраическом замыкании $\bar{E}$), содержащих E, есть нормальное расширение над k, которое содержит E и, очевидно, является наименьшим нормальным расширением поля k,

содержащим E. Если $\sigma_1, \ldots, \sigma_n$ — все различные вложения E в $\overline{E}$, то расширение

$$K = (\sigma_1 E)(\sigma_2 E) \ldots (\sigma_n E),$$

композит всех этих вложений, является нормальным расширением k. Действительно, любое его вложение, скажем τ, мы можем применить к каждому расширению $\sigma_i E$; тогда $(\tau\sigma_1, \ldots, \tau\sigma_n)$ будет перестановкой совокупности $(\sigma_1, \ldots, \sigma_n)$ и, следовательно, τ отображает K в себя. Всякое нормальное расширение поля k, содержащее E, должно содержать $\sigma_i E$ для каждого i, и, таким образом, *наименьшее нормальное расширение поля k, содержащее E, в точности равно композиту*

$$(\sigma_1 E) \ldots (\sigma_n E).$$

Если E сепарабельно над k, то из теоремы 9 с помощью индукции заключаем, что наименьшее нормальное расширение поля k, содержащее E, также сепарабельно над k.

Аналогичные результаты будут справедливы и для бесконечного алгебраического расширения E поля k, если взять бесконечный композит. Что касается терминологии, то если E — алгебраическое расширение поля k и σ — произвольное вложение E в $\overline{k}$ над k, то мы называем поле σE сопряженным с E в $\overline{k}$. Мы можем сказать, что *наименьшее нормальное расширение поля k, содержащее E, есть композит всех сопряженных с E подполей в $\overline{E}$.*

Пусть α — алгебраический элемент над k. Если $\sigma_1, \ldots, \sigma_n$ — различные вложения поля $k(\alpha)$ в $\overline{k}$ над k, то мы называем элементы $\sigma_1\alpha, \ldots, \sigma_r\alpha$ *сопряженными* с α в $\overline{k}$. Этими элементами являются попросту различные корни неприводимого многочлена над k, соответствующего элементу α. Наименьшее нормальное расширение поля k, содержащее один из этих сопряженных элементов, совпадает с $k(\sigma_1\alpha, \ldots, \sigma_r\alpha)$.

§ 5. Конечные поля

Мы получили достаточно общих теорем для того, чтобы описать строение конечных полей. Это интересно само по себе, а также дает примеры к общей теории.

Пусть F — конечное поле из q элементов. Как мы уже отмечали раньше, имеется гомоморфизм

$$\mathbf{Z} \to F,$$

переводящий 1 в 1, ядро которого не может быть 0, и, следовательно, является главным идеалом, порожденным простым числом p, по-