зательства условия (i), может быть выполнено лишь с применением более сложной техники, чем та, которой мы располагаем сейчас. См. главу о трансцендентных расширениях.

§ 2. *Алгебраическое замыкание*

В этом и в следующем параграфе мы будем иметь дело с вложениями одного поля в другое. В связи с этим введем соответствующую терминологию.

Пусть E — расширение поля F, и пусть

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

— вложение (т. е. инъективный гомоморфизм) F в L. Тогда σ индуцирует изоморфизм поля F с его образом σF, который мы иногда будем обозначать также через F^σ. Вложение τ поля E в L называется *вложением над* σ, если ограничение τ на F равно σ. Мы говорим также, что τ *продолжает* σ. Если σ — тождественное вложение, то мы говорим, что τ есть *вложение* поля E *над* F.

Эти определения можно было бы дать и в более общих категориях, поскольку все зависит лишь от того, имеют ли смысл диаграммы

$$\begin{tikzcd} E \arrow[r, "\tau"] & L \\ F \arrow[u, "\text{вкл.}"] \arrow[r, "\sigma"'] & L \arrow[u, "\mathrm{Id}"'] \end{tikzcd} \qquad \begin{tikzcd} E \arrow[rr, "\tau"] & & L \\ & F \arrow[ul, "\text{вкл.}"] \arrow[ur, "\text{вкл.}"'] & \end{tikzcd}$$

Замечание. Пусть $f(X) \in F(X)$ — многочлен, скажем $f(X) = a_0 + \ldots + a_n X^n$, и пусть α — корень f в E. Тогда

$$0 = f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n.$$

Если, как и выше, τ продолжает σ, то мы видим, что $\tau\alpha$ будет корнем многочлена f^σ, поскольку

$$0 = \tau(f(\alpha)) = a_0^\sigma + a_1^\sigma(\tau\alpha) + \ldots + a_n^\sigma(\tau\alpha)^n.$$

Здесь мы пишем a^σ вместо $\sigma(a)$. Это экспоненциальное обозначение часто бывает удобно и будет неоднократно использоваться в дальнейшем. Аналогично мы пишем F^σ вместо $\sigma(F)$ или σF.

При изучении вложений нам будет полезна одна лемма, относящаяся к вложениям алгебраических расширений в себя. Предварительно отметим, что если $\sigma\colon E \to L$ — вложение над k (т. е. индуцирующее тождественное отображение на k), то σ можно рассматривать как k-гомоморфизм векторных пространств, потому что и E, и L могут рассматриваться как векторные пространства над k.

Лемма 1. *Пусть E — алгебраическое расширение поля k, и пусть σ: $E \to E$ — вложение E в себя над k. Тогда σ — автоморфизм.*

Доказательство. Так как гомоморфизм σ инъективен, то достаточно доказать, что он сюръективен. Пусть α — произвольный элемент из E, $p(X)$ — его неприводимый многочлен над k и E' — подполе в E, порожденное всеми корнями многочлена $p(X)$, лежащими в E. Тогда E' — конечно порожденное и, следовательно, будет конечным расширением над k. Кроме того, σ должно переводить всякий корень многочлена $p(X)$ в корень того же самого многочлена и, следовательно, σ отображает E' в себя. Мы можем рассматривать σ как k-гомоморфизм векторных пространств, поскольку σ индуцирует тождественное отображение на k. Так как отображение σ инъективно, то образ $\sigma(E')$ есть подпространство в E', имеющее ту же размерность, что и $[E': k]$. Следовательно, $\sigma(E') = E'$. Так как $\alpha \in E'$, то отсюда вытекает, что α лежит в образе отображения σ, и наша лемма доказана.

Пусть E, F — расширения поля k, содержащиеся в некотором большем поле L. Мы можем образовать кольцо $E[F]$, порожденное элементами F над E. Тогда EF будет полем частных этого кольца, а также полем частных кольца $F[E]$. Ясно, что элементы из $E[F]$ могут быть записаны в виде

$$a_1b_1 + \ldots + a_nb_n,$$

где $a_i \in E$ и $b_i \in F$. Таким образом, EF есть поле отношений этих элементов.

Лемма 2. *Пусть E_1, E_2 — расширения поля k, содержащиеся в некотором большем поле E, и пусть σ — вложение поля E в поле L. Тогда $\sigma(E_1E_2) = \sigma(E_1)\sigma(E_2)$.*

Доказательство. Применяя σ к отношению элементов указанного выше вида, скажем

$$\sigma\left(\frac{a_1b_1 + \ldots + a_nb_n}{a_1'b_1' + \ldots + a_m'b_m'}\right) = \frac{a_1^\sigma b_1^\sigma + \ldots + a_n^\sigma b_n^\sigma}{a_1'^\sigma b_1'^\sigma + \ldots + a_m'^\sigma b_m'^\sigma},$$

мы видим, что образом служит элемент из $\sigma(E_1)\sigma(E_2)$. Отсюда ясно, что образ $\sigma(E_1E_2)$ есть $\sigma(E_1)\sigma(E_2)$.

Пусть k — поле, $f(X)$ — многочлен степени $\geqslant 1$ из $k[X]$. Рассмотрим задачу отыскания такого расширения E поля k, в котором f имеет корень. Если $p(X)$ — неприводимый многочлен в $k[X]$, делящий $f(X)$, то любой корень $p(X)$ будет также корнем $f(X)$, так что мы можем ограничиться неприводимыми многочленами.

Пусть $p(X)$ — неприводимый многочлен. Канонический гомоморфизм

$$\sigma\colon\ k[X] \to k[X]/(p(X))$$

индуцирует на k гомоморфизм, ядром которого служит 0, поскольку всякий ненулевой элемент из k, будучи обратимым в k, порождает единичный идеал, а 1 не лежит в ядре. Пусть ξ — образ X при гомоморфизме σ, т. е. $\xi = \sigma(X)$ есть класс вычетов $X \bmod p(X)$. Тогда

$$p^{\sigma}(\xi) = p^{\sigma}(X^{\sigma}) = (p(X))^{\sigma} = 0.$$

Следовательно, элемент ξ есть корень многочлена p^{σ} и как таковой алгебраичен над σk. Таким образом, мы нашли расширение поля σk, а именно $\sigma k(\xi)$, в котором p^{σ} имеет корень.

С помощью несложного теоретико-множественного рассуждения мы сейчас докажем

Предложение 7. *Пусть k — поле и f — многочлен из $k[X]$ степени $\geqslant 1$. Существует расширение E поля k, в котором f имеет корень.*

Доказательство. Можно предполагать, что многочлен $f = p$ неприводим. Мы показали, что существуют поле F и вложение

$$\sigma\colon\ k \to F,$$

такие, что p^{σ} имеет корень ξ в F. Пусть S — множество той же мощности, что и $F - \sigma k$ (дополнение σk в F), и не пересекающееся с k. Положим $E = k \cup S$. Мы можем продолжить $\sigma\colon k \to F$ до биекции E на F. Определим теперь на E структуру поля. Если $x, y \in E$, то полагаем

$$xy = \sigma^{-1}(\sigma(x)\sigma(y)),$$

$$x + y = \sigma^{-1}(\sigma(x) + \sigma(y)).$$

При ограничении на k эти операции совпадают с заданными операциями сложения и умножения нашего исходного поля k и ясно, что k есть подполе в E. Положим $\alpha = \sigma^{-1}(\xi)$. Тогда ясно также, что $p(\alpha) = 0$, что и требовалось доказать.

Следствие. *Пусть k — поле и $f_1, \ldots, f_n$ — многочлены из $k[X]$ степеней $\geqslant 1$. Тогда существует расширение E поля k, в котором каждый f_i имеет корень, $i = 1, \ldots, n$.*

Доказательство. Пусть E_1 — расширение, в котором f_1 имеет корень. Мы можем рассматривать f_2 как многочлен над E_1. Пусть E_2 — расширение E_1, в котором f_2 имеет корень. Продолжая по индукции, немедленно получаем наше следствие.

Поле L называется *алгебраически замкнутым*, если всякий многочлен из $L[X]$ степени $\geqslant 1$ имеет в L корень.

Теорема 1. *Для всякого поля k существует алгебраически замкнутое поле L, содержащее k в качестве подполя.*

Доказательство. Сначала мы построим расширение E_1 поля k, в котором всякий многочлен из $k[X]$ степени $\geqslant 1$ имеет корень. Можно действовать следующим образом (Артин). Каждому многочлену f из $k[X]$ степени $\geqslant 1$ сопоставим символ X_f. Пусть S — множество всех таких символов X_f (так что S находится в биективном соответствии с множеством многочленов из $k[X]$ степени $\geqslant 1$). Образуем кольцо многочленов $k[S]$. Мы утверждаем, что идеал, порожденный всеми многочленами $f(X_f)$ в $k[S]$, не является единичным. Если бы это было не так, то существовала бы конечная комбинация элементов из нашего идеала, равная 1:

$$g_1 f_1(X_{f_1}) + \ldots + g_n f_n(X_{f_n}) = 1,$$

где $g_i \in k[S]$. Для простоты будем писать X_i вместо X_{f_i}. Многочлены g_i включают в действительности только конечное число переменных, скажем $X_1, \ldots, X_N$ (где $N \geqslant n$). Наше соотношение тогда гласит:

$$\sum_{i=1}^{n} g_i(X_1, \ldots, X_N) f_i(X_i) = 1.$$

Пусть F — конечное расширение, в котором каждый многочлен $f_1, \ldots, f_n$ имеет корень, скажем α_i есть корень f_i в F при $i = 1, \ldots, n$. Положим $\alpha_i = 0$ при $i > n$. Подставив α_i вместо X_i в наше соотношение, мы получим $0 = 1$ — противоречие.

Пусть $\mathfrak{m}$ — максимальный идеал, содержащий идеал, порожденный всеми многочленами $f(X_f)$ в $k[S]$. Тогда $k[S]/\mathfrak{m}$ — поле и мы имеем каноническое отображение

$$\sigma\colon\ k[S] \to k[S]/\mathfrak{m}.$$

Для всякого многочлена $f \in k[X]$ степени $\geqslant 1$ многочлен f^σ имеет корень в поле $k[S]/\mathfrak{m}$, которое является расширением поля σk. Используя теоретико-множественное рассуждение того же типа, что и в предложении 7, мы заключаем, что существует расширение E_1 поля k, в котором каждый многочлен $f \in k[X]$ степени $\geqslant 1$ имеет корень.

По индукции мы можем построить такую последовательность полей

$$E_1 \subset E_2 \subset E_3 \subset \ldots \subset E_n \subset \ldots,$$

что каждый многочлен из $E_n[X]$ степени $\geqslant 1$ имеет корень в E_{n+1}. Пусть E — объединение всех полей E_n, $n=1, 2, \ldots$. Тогда E, естественно, является полем, поскольку для любых $x, y \in E$ найдется номер n, такой, что $x, y \in E_n$, и мы можем взять произведение xy или сумму $x+y$ в E_n. Эти операции, очевидно, не зависят от выбора того n, для которого $x, y \in E_n$, и определяют структуру поля на E. Всякий многочлен из $E[X]$ имеет коэффициенты в некотором подполе E_n и, следовательно, обладает корнем в E_{n+1}, а тем самым и корнем в E, что и требовалось доказать.

Следствие. *Для всякого поля k существует расширение $\bar{k}$, алгебраическое над k и алгебраически замкнутое.*

Доказательство. Пусть E — алгебраически замкнутое расширение поля k, и пусть $\bar{k}$ — объединение всех подрасширений из E, алгебраических над k. Тогда $\bar{k}$ алгебраично над k. Пусть элемент $\alpha \in E$ алгебраичен над $\bar{k}$. Тогда α алгебраичен над k в силу предложения 6. Если f — многочлен степени $\geqslant 1$ из $\bar{k}[X]$, то f имеет корень α в E и алгебраичен над $\bar{k}$. Следовательно, α лежит в $\bar{k}$ и $\bar{k}$ алгебраически замкнуто.

Заметим, что если L — алгебраически замкнутое и $f \in L[X]$ имеет степень $\geqslant 1$, то существует $c \in L$ и $\alpha_1, \ldots, \alpha_n \in L$, такие, что

$$f(X) = c(X-\alpha_1) \ldots (X-\alpha_n).$$

Действительно, f имеет корень α_1 в L, так что $f(X) = (X-\alpha_1)g(X)$, где $g(X) \in L[X]$. Если $\deg g \geqslant 1$, то мы можем повторить это рассуждение и по индукции представить f в виде произведения членов $(X-\alpha_i)$ $(i=1, \ldots, n)$ и некоторого элемента $c \in L$. Отметим, что c совпадает со старшим коэффициентом многочлена f, т. е.

$$f(X) = cX^n + \text{члены меньшей степени}.$$

Следовательно, если коэффициенты f лежат в подполе k поля L, то $c \in k$.

Пусть k — поле и σ: $k \to L$ — вложение k в алгебраически замкнутое поле L. Мы хотим исследовать продолжения σ на алгебраические расширения E поля k. Начнем с рассмотрения частного случая, когда E порождено одним элементом.

Пусть $E = k(\alpha)$, где α алгебраичен над k,

$$p(X) = \operatorname{Irr}(\alpha, k, X).$$

Пусть β — корень многочлена p^σ в L. Всякий данный элемент из $k(\alpha) = k[\alpha]$ мы можем записать в виде $f(\alpha)$, где $f(X) \in k[X]$ — некоторый многочлен. Определим продолжение σ как отображение

$$f(\alpha) \mapsto f^\sigma(\beta).$$

Это отображение, на самом деле, правильно определено, т. е. не зависит от выбора многочлена $f(X)$, использованного для представления нашего элемента в $k[\alpha]$. Действительно, если многочлен $g(X)$ лежит в $k[X]$ и таков, что $g(\alpha)=f(\alpha)$, то $(g-f)(\alpha)=0$, а потому $p(X)$ делит $g(X)-f(X)$. Следовательно, $p^{\sigma}(X)$ делит $g^{\sigma}(X)-f^{\sigma}(X)$ и, таким образом, $g^{\sigma}(\beta)=f^{\sigma}(\beta)$. Далее, очевидно, что наше отображение есть гомоморфизм, индуцирующий σ на k, и что оно служит продолжением σ на $k(\alpha)$. Таким образом, получаем

Предложение 8. *Число возможных продолжений σ на $k(\alpha)$ не превосходит числа корней многочлена p, а именно равно числу различных корней p.*

Это важный факт, который мы позже проанализируем подробнее. А сейчас нас интересуют продолжения σ на произвольные алгебраические расширения k. Мы получим их, используя лемму Цорна.

Теорема 2. *Пусть k — поле, E — его алгебраическое расширение и σ: $k\to L$ — вложение k в алгебраически замкнутое поле L. Тогда существует продолжение σ до вложения E в L. Если E алгебраически замкнуто и L алгебраично над σk, то любое такое продолжение σ будет изоморфизмом поля E на L.*

Доказательство. Пусть S — множество всех пар (F, τ), где F — подполе в E, содержащее k, и τ — продолжение σ до вложения F в L. Мы пишем $(F, \tau)\leqslant(F', \tau')$ для таких пар (F, τ) и (F', τ'), если $F\subset F'$ и $\tau'|F=\tau$. Отметим, что множество S не пусто [оно содержит (k, σ)] и индуктивно упорядочено: если $\{(F_i, \tau_i)\}$ линейно упорядоченное подмножество, то положим $F=\bigcup F_i$ и определим τ на F, положив его равным τ_i на каждом F_i. Тогда (F, τ) служит верхней гранью для этого линейно упорядоченного подмножества. Применяя лемму Цорна, находим (K, λ)—максимальный элемент в S. Тогда λ есть продолжение σ, и мы утверждаем, что $K=E$. В противном случае существует $\alpha\in E$, $\alpha\notin K$; в силу предыдущего вложение λ имеет продолжение на $K(\alpha)$ вопреки максимальности (K, λ). Таким образом, существует продолжение σ на E. Мы обозначаем это продолжение снова через σ.

Если E алгебраически замкнуто и L алгебраично над σk, то σE алгебраически замкнуто и L алгебраично над $\sigma(E)$, следовательно, $L=\sigma E$.

В качестве следствия получаем некую теорему единственности для „алгебраического замыкания“ поля k.

Следствие. *Пусть k — поле и E, E' — алгебраические расширения над k. Предположим, что E, E' алгебраически замкнуты. Тогда существует изоморфизм*

$$\tau\colon E\longmapsto E'$$

поля E на E', индуцирующий тождественное отображение на k.

Доказательство. Продолжим тождественное отображение поля k до вложения E в E' и применим теорему.

Мы видим, что алгебраически замкнутое и алгебраическое расширение поля k определено однозначно с точностью до изоморфизма. Всякое такое расширение будет называться *алгебраическим замыканием* k и будет обозначаться через $\bar{k}$. Фактически, если не оговорено противное, символ $\bar{k}$ мы будем использовать только для обозначения алгебраического замыкания.

Теперь стоит рассмотреть общую ситуацию с изоморфизмами и автоморфизмами в общих категориях.

Пусть $\mathcal{A}$ — категория и A, B — объекты в $\mathcal{A}$. Обозначим через $\mathrm{Iso}(A, B)$ множество изоморфизмов A на B. Предположим, что существует по крайней мере один такой изоморфизм σ: $A \to B$ с обратным σ^{-1}: $B \to A$. Если φ — автоморфизм объекта A, то $\sigma \circ \varphi$: $A \to B$ — снова изоморфизм. Аналогично, если ψ — автоморфизм B, то $\psi \circ \sigma$: $A \to B$ — снова изоморфизм. Кроме того, группы автоморфизмов $\mathrm{Aut}(A)$ и $\mathrm{Aut}(B)$ изоморфны относительно взаимно обратных отображений

$$\varphi \longmapsto \sigma \circ \varphi \circ \sigma^{-1},$$
$$\sigma^{-1} \circ \psi \circ \sigma \longleftarrow\!\shortmid \psi.$$

Автоморфизм $\sigma \circ \varphi \circ \sigma^{-1}$ определяется тем, что делает коммутативной следующую диаграмму:

$$\begin{tikzcd} A \arrow[r, "\sigma"] \arrow[d, "\varphi"'] & B \arrow[d, "\sigma \circ \varphi \circ \sigma^{-1}"] \\ A \arrow[r, "\sigma"'] & B \end{tikzcd}$$

Аналогичную диаграмму имеем и для $\sigma^{-1} \circ \psi \circ \sigma$.

Пусть τ: $A \to B$ — какой-нибудь другой изоморфизм. Тогда $\tau^{-1} \circ \sigma$ есть автоморфизм объекта A и $\tau \circ \sigma^{-1}$ — автоморфизм B. Таким образом, два изоморфизма отличаются на автоморфизм (объекта A или B). Мы видим, что группа $\mathrm{Aut}(B)$ действует на множестве $\mathrm{Iso}(A, B)$ слева, а $\mathrm{Aut}(A)$ — на множестве $\mathrm{Iso}(A, B)$ справа.

Мы видим также, что группа $\mathrm{Aut}(A)$ определена однозначно с точностью до отображения, аналогичного сопряжению Это совершенно не похоже на тот тип единственности, который свойствен универсальным объектам в категории. Такие объекты имеют лишь тождественный автоморфизм и, следовательно, определены с точностью до однозначно определенного изоморфизма.

Не так обстоит дело в случае алгебраического замыкания поля, которое обычно имеет большое количество автоморфизмов. Бо́льшая

часть этой главы и вся следующая глава посвящены изучению этих автоморфизмов.

Примеры. Позже в этой книге будет доказано, что поле комплексных чисел алгебраически замкнуто. Комплексное сопряжение является автоморфизмом поля $\mathbf{C}$. Имеется и еще много автоморфизмов, но уже не непрерывных. Мы рассмотрим другие возможные автоморфизмы в главе о трансцендентных расширениях. Подполе поля $\mathbf{C}$, состоящее из всех чисел, алгебраических над $\mathbf{Q}$, есть алгебраическое замыкание $\overline{\mathbf{Q}}$ поля $\mathbf{Q}$. Легко видеть, что $\overline{\mathbf{Q}}$ счетно. Действительно, докажите в качестве упражнения следующее утверждение.

Если k — поле, не являющееся конечным, то любое алгебраическое расширение над k имеет ту же мощность, что и k.

(Если k счетно, то можно сначала перенумеровать все многочлены над k, а затем перенумеровать все элементы произвольного алгебраического расширения.)

В частности, $\overline{\mathbf{Q}} \neq \mathbf{C}$. Для поля $\mathbf{R}$ вещественных чисел $\overline{\mathbf{R}} = \mathbf{C}$.

Если k — конечное поле, то алгебраическое замыкание $\bar{k}$ поля k счетно. Позднее в этой главе мы во всех подробностях опишем природу алгебраических расширений конечных полей.

Не все интересные поля являются подполями поля комплексных чисел. Например, представляет интерес исследовать алгебраические расширения поля $\mathbf{C}(X)$, где X — переменная над $\mathbf{C}$. Изучение этих расширений равносильно изучению разветвленных накрытий сферы (рассматриваемой как риманова поверхность), и фактически имеется точная информация о природе таких расширений, поскольку известна фундаментальная группа сферы, из которой выколото конечное число точек. Мы вернемся к этому примеру позднее, когда будем рассматривать группы Галуа.

§ 3. Поля разложения и нормальные расширения

Пусть k — поле, f — многочлен из $k[X]$ степени $\geqslant 1$. Под *полем разложения* K многочлена f мы будем понимать расширение K поля k, в котором f разлагается на линейные множители, т. е.

$$f(X) = c(X - \alpha_1) \ldots (X - \alpha_n),$$

где $\alpha_i \in K$, $i = 1, \ldots, n$, причем $K = k(\alpha_1, \ldots, \alpha_n)$ порождается всеми корнями f.

Теорема 3. *Пусть K — поле разложения многочлена $f(X) \in k[X]$. Если E — какое-нибудь другое поле разложения f, то существует изоморфизм $\sigma\colon E \to K$, индуцирующий тождествен-*