Глава VII

Алгебраические расширения

§ 1. Конечные и алгебраические расширения

Пусть F — поле. Если F — подполе поля E, то мы говорим также, что E есть *расширение* поля F. Мы можем рассматривать E как векторное пространство над F, и мы говорим, что E — *конечное* или *бесконечное* расширение F, в зависимости от того, конечна или бесконечна размерность этого векторного пространства.

Пусть F — подполе поля E. Элемент α из E называется *алгебраическим* над F, если в F существуют элементы $a_0, \ldots, a_n$ $(n \geqslant 1)$, не все равные 0 и такие, что

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

Для алгебраического элемента $\alpha \neq 0$ мы всегда можем найти такие элементы a_i в предыдущем равенстве, что $a_0 \neq 0$ (сокращая на подходящую степень α).

Пусть X — переменная над F. Можно также сказать, что элемент α алгебраичен над F, если гомоморфизм

$$F[X] \to E,$$

тождественный на F и переводящий X в α, имеет ненулевое ядро. В таком случае это ядро будет главным идеалом, порожденным одним многочленом $p(X)$, относительно которого мы можем предполагать, что его старший коэффициент равен 1. Имеет место изоморфизм

$$F[X]/(p(X)) \approx F[\alpha],$$

и так как кольцо $F[\alpha]$ целостное, то $p(X)$ неприводим. Если $p(X)$ нормализован условием, что его старший коэффициент равен 1, то $p(X)$ однозначно определяется элементом α и будет называться неприводимым многочленом элемента α над F. Иногда мы будем обозначать его через $\operatorname{Irr}(\alpha, F, X)$.

Расширение E поля F называется *алгебраическим*, если всякий элемент из E алгебраичен над F.

Предложение 1. *Всякое конечное расширение E поля F алгебраично над F.*

Доказательство. Пусть $\alpha \in E$, $\alpha \neq 0$. Степени α

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

не могут быть линейно независимы над F для всех целых положительных n, иначе размерность E над F была бы бесконечна. Линейное соотношение между этими степенями показывает, что элемент α алгебраичен над F.

Заметим, что утверждение, обратное предложению 1, не верно: существуют бесконечные алгебраические расширения. Позднее мы увидим, что подполе поля комплексных чисел, состоящее из всех чисел, алгебраических над $\mathbf{Q}$, является бесконечным расширением $\mathbf{Q}$.

Если E — расширение поля F, то мы обозначаем символом

$$[E : F]$$

размерность E как векторного пространства над F. Будем называть $[E : F]$ *степенью* E над F. Она может быть бесконечной.

Предложение 2. *Пусть k — поле и $F \subset E$ — расширения k. Тогда*

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

Если $\{x_i\}_{i \in I}$ — базис поля F над k и $\{y_j\}_{j \in J}$ — базис поля E над F, то $\{x_i y_j\}_{(i,\, j) \in I \times J}$ будет базисом поля E над k.

Доказательство. Пусть $z \in E$. По предположению существуют элементы $\alpha_j \in F$, почти все равные нулю и такие, что

$$z = \sum_{j \in J} \alpha_j y_j.$$

Для каждого $j \in J$ существуют элементы $b_{ji} \in k$, из которых почти все равны 0, такие, что

$$\alpha_j = \sum_{i \in I} b_{ji} x_i,$$

и, следовательно,

$$z = \sum_j \sum_i b_{ji} x_i y_j.$$

Это означает, что $\{x_i y_j\}$ является семейством образующих для E над k. Мы должны показать, что оно линейно независимо. Пусть $\{c_{ij}\}$ — семейство элементов из k, почти все из которых равны 0, такое, что

$$\sum_j \sum_i c_{ij} x_i y_j = 0.$$

Тогда для каждого j

$$\sum_i c_{ij} x_i = 0,$$

поскольку элементы y_j линейно независимы над F. Наконец, $c_{ij}=0$ для всякого i, так как $\{x_i\}$ — базис поля F над k, что и доказывает наше предложение.

Следствие. *Расширение $E \supset F \supset k$ поля k конечно в том и только в том случае, если E конечно над F и F конечно над k.*

Как и в случае групп, мы называем *башней* полей последовательность расширений

$$F_1 \subset F_2 \subset \ldots \subset F_n.$$

Для *конечности башни* необходимо и достаточно, чтобы каждый ее этаж был конечен.

Пусть k — поле, E — его расширение и $a \in E$. Мы обозначаем через $k(\alpha)$ наименьшее подполе в E, содержащее k и α. Оно состоит из всех дробей $f(\alpha)/g(\alpha)$, где f, g — многочлены с коэффициентами в k и $g(\alpha) \neq 0$.

Предложение 3. *Пусть элемент α алгебраичен над k. Тогда $k(\alpha)=k[\alpha]$ и поле $k(\alpha)$ конечно над k. Степень $[k(\alpha): k]$ равна степени многочлена* $\operatorname{Irr}(\alpha, k, X)$.

Доказательство. Пусть $p(X)=\operatorname{Irr}(\alpha, k, X)$. Пусть многочлен $f(X) \in k[X]$ таков, что $f(\alpha) \neq 0$. Тогда $f(X)$ не делится на $p(X)$ и, следовательно, существуют многочлены $g(X)$, $h(X) \in k[X]$, такие, что

$$g(X)\,p(X)+h(X)\,f(X)=1.$$

Отсюда мы получаем, что $h(\alpha)\,f(\alpha)=1$ и, значит, $f(\alpha)$ обратим в $k[\alpha]$. Следовательно, $k[\alpha]$ не только кольцо, но и поле, а потому должно быть равно $k(\alpha)$. Пусть $d=\deg p(X)$. Степени

$$1,\ \alpha,\ \ldots,\ \alpha^{d-1}$$

линейно независимы над k; действительно, предположим, что

$$a_0+a_1\alpha+\ \ldots\ +a_{d-1}\alpha^{d-1}=0,$$

где $a_i \in k$, причем не все $a_i=0$. Положим $g(X)=a_0+\ldots+a_{d-1}X^{d-1}$. Тогда $g \neq 0$ и $g(\alpha)=0$. Следовательно, $g(X)$ делится на $p(X)$ — противоречие. Наконец, пусть $f(\alpha) \in k[\alpha]$, где $f(X) \in k[X]$. Существуют многочлены $q(X)$, $r(X) \in k[X]$, такие, что $\deg r < d$ и

$$f(X)=q(X)\,p(X)+r(X).$$

Тогда $f(\alpha)=r(\alpha)$ и мы видим, что $1, \alpha, \ldots, \alpha^{d-1}$ порождают $k[\alpha]$ как векторное пространство над k. Это доказывает наше предложение.

Пусть E, F — расширения поля k. Если E и F содержатся в некотором поле L, то мы обозначаем через EF наименьшее подполе в L, содержащее и E, и F, и называем его *композитом* E и F в L.

Если не заданы вложения E, F в общее поле L, то мы не можем определить их композит.

Пусть k — подполе в E, $\alpha_1, \ldots, \alpha_n$ — элементы из E. Мы обозначаем через

$$k(\alpha_1, \ldots, \alpha_n)$$

наименьшее подполе в E, содержащее k и $\alpha_1, \ldots, \alpha_n$. Его элементы состоят из всех дробей

$$\frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)},$$

где f, g — многочлены от n переменных с коэффициентами в k и $g(\alpha_1, \ldots, \alpha_n) \neq 0$. Действительно, множество таких дробей образует поле, содержащее k и $\alpha_1, \ldots, \alpha_n$. Обратно, любое поле, содержащее k и

$$\alpha_1, \ldots, \alpha_n,$$

должно содержать эти дроби.

Заметим, что E является объединением всех своих подполей $k(\alpha_1, \ldots, \alpha_n)$, когда $(\alpha_1, \ldots, \alpha_n)$ пробегает все конечные подсемейства элементов из E. Можно было бы определить *композит произвольного подсемейства подполей поля* L как наименьшее подполе, содержащее все поля этого семейства. Мы говорим, что E *конечно порождено* над k, если существует конечное семейство элементов $\alpha_1, \ldots, \alpha_n$ из E, такое, что

$$E = k(\alpha_1, \ldots, \alpha_n).$$

Мы видим, что E есть композит всех своих конечно порожденных подполей над k.

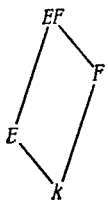
Предложение 4. *Всякое конечное расширение E поля k конечно порождено.*

Доказательство. Пусть $\{\alpha_1, \ldots, \alpha_n\}$ — базис поля E как векторного пространства над k. Тогда, очевидно, $E = k(\alpha_1, \ldots, \alpha_n)$.

Если $E = k(\alpha_1, \ldots, \alpha_n)$ — конечно порожденное поле и F — расширение поля k, причем как F, так и E содержатся в L, то

$$EF = F(\alpha_1, \ldots, \alpha_n)$$

и поле EF конечно порождено над F. Мы часто будем рисовать такую картинку:



Наклонные линии указывают на отношение включения между полями. Мы будем также называть расширение EF поля F *подъемом* E до F.

Пусть элемент α алгебраичен над полем k и F — расширение k. Предположим, что оба поля $k(\alpha)$, F содержатся в некотором поле L. Тогда α алгебраичен над F. Действительно, неприводимый многочлен для α над k a fortiori имеет коэффициенты в F и дает линейную зависимость между степенями α над F.

Пусть нам дана башня полей

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

причем каждое поле порождено над предыдущим одним элементом. Предположим, что каждый элемент α_i алгебраичен над k, $i = 1, \ldots, n$. В качестве частного случая нашего предыдущего замечания получаем, что α_{i+1} алгебраичен над $k(\alpha_1, \ldots, \alpha_i)$. Следовательно, каждый этаж башни — алгебраический.

Предложение 5. *Пусть $E = k(\alpha_1, \ldots, \alpha_n)$ — конечно порожденное расширение поля k, причем α_i алгебраичен над k для каждого $i = 1, \ldots, n$. Тогда E — конечное алгебраическое расширение поля k.*

Доказательство. В силу предыдущих замечаний E можно считать вершиной башни, каждый из этажей которой порождается одним алгебраическим элементом и потому является конечным по предложению 3. Ввиду следствия предложения 2 мы заключаем, что E конечно над k и что оно алгебраично — в силу предложения 1.

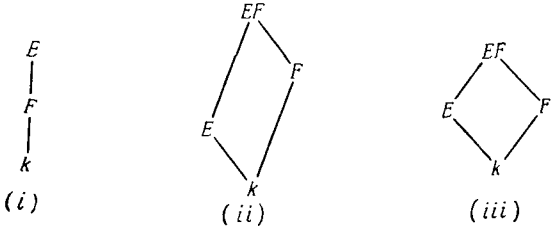
Пусть $\mathscr{C}$ — некоторый класс расширений $F \subset E$. Мы будем называть класс $\mathscr{C}$ *отмеченным*, если он удовлетворяет следующим условиям:

(i) Пусть $k \subset F \subset E$ — башня полей. Расширение $k \subset E$ принадлежит $\mathscr{C}$ тогда и только тогда, когда $k \subset F$ и $F \subset E$ принадлежат $\mathscr{C}$.

(ii) Если $k \subset E$ принадлежит $\mathscr{C}$, а F — любое расширение поля k и если E, F оба содержатся в некотором поле, то $F \subset EF$ принадлежит $\mathscr{C}$.

(iii) Если $k \subset F$ и $k \subset E$ принадлежат $\mathscr{C}$, причем F, E — подполя некоторого общего поля, то $k \subset EF$ принадлежит $\mathscr{C}$.

Указанные свойства иллюстрируются следующими диаграммами:



Эти структурные диаграммы чрезвычайно полезны при обращении с расширениями.

Заметим, что (iii) формально следует из первых двух условий. Действительно, можно рассматривать EF над k как башню с этажами $k \subset F \subset EF$.

Что касается обозначений, то иногда удобнее писать E/F вместо $F \subset E$. Это не может привести к смешению с факторгруппами, так как мы никогда не будем использовать записи E/F для обозначения соответствующей факторгруппы в тех случаях, когда E — расширение поля F.

Предложение 6. *Класс алгебраических расширений является отмеченным, и то же самое относится к классу конечных расширений.*

Доказательство. Рассмотрим сначала класс конечных расширений. Мы уже доказали условие (i). Что касается (ii), то предположим, что E/k конечно, а F — любое расширение поля k. В силу предложения 4 существуют элементы $\alpha_1, \ldots, \alpha_n \in E$, такие, что $E = k(\alpha_1, \ldots, \alpha_n)$. Тогда $EF = F(\alpha_1, \ldots, \alpha_n)$ и, следовательно, EF/F конечно порождено алгебраическими элементами. Используя предложение 5, заключаем, что EF/F конечно.

Рассмотрим теперь класс алгебраических расширений. Пусть

$$k \subset F \subset E$$

— башня. Предположим, что E алгебраично над k. Тогда a fortiori F алгебраично над k и E алгебраично над F. Обратно, предположим, что каждый этаж в башне алгебраический. Пусть $\alpha \in E$. Тогда α удовлетворяет уравнению

$$a_n\alpha^n + \ldots + a_0 = 0,$$

где $a_i \in F$, причем не все $a_i = 0$. Пусть $F_0 = k(a_n, \ldots, a_0)$. Тогда F_0 конечно над k в силу предложения 5 и α алгебраичен над F_0. Из наличия башни

$$k \subset F_0 = k(a_n, \ldots, a_0) \subset F_0(\alpha)$$

и из того факта, что каждый этаж в этой башне конечен, заключаем, что $F_0(\alpha)$ конечно над k, следовательно, α алгебраичен над k. Это доказывает, что E алгебраично над k и что, таким образом, условие (i) выполняется для алгебраических расширений. Выполнение условия (ii) уже отмечалось раньше: при подъеме алгебраический элемент остается алгебраическим и, следовательно, алгебраическое расширение при подъеме также остается алгебраическим.

Замечание. Верно, что конечно порожденные расширения также образуют отмеченный класс, но рассуждение, необходимое для дока-

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.