Дополнительные главы алгебры

В. А. Артамонов

Оглавление

Глава 1

Расширения полей и теория Галуа

1. Целые расширения колец

Все кольца будут предполагаться ассоциативными и содержащими единицу.

Пусть k — коммутативное кольцо. Многочлен $f \in k[T]$ называется *унитарным*, если его старший коэффициент обратим в k. Если R является k-алгеброй и $x \in R$, то $k[x] = \{\sum a_i x^i \mid a_i \in k\}$. Легко проверяется, что $k[x]$ является k-подалгеброй в R.

Теорема 1.1. *Пусть k — коммутативное кольцо с единицей, R — ассоциативная алгебра с единицей над k и $x \in R$. Следующие условия эквивалентны:*

i) *x является корнем унитарного многочлена из $k[T]$;*
ii) *$k[x]$ является конечно порожденным k-модулем;*
iii) *существует точный модуль над $k[x]$, который является конечно порожденным модулем над k.*

Доказательство. Покажем, что i) $\Rightarrow$ ii). Действитльно, если $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, где $a_i \in k$, то $k[x] = k1 + kx + \cdots + kx^{n-1}$.

ii) $\Rightarrow$ iii), так как в качестве модуля можно взять $k[x]$.

iii) $\Rightarrow$ i). Пусть $M = ke_1 + \cdots + ke_n$ — точный конечно порожденный $k[x]$-модуль. Тогда

$$x \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = A \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix},$$

где $A \in \mathrm{Mat}(n, k)$. Тогда $\det(A - xE)$ аннулирует каждый элемент e_i, и, следовательно, M. В силу точности M получаем $\det(A - xE) = 0$, что дает искомый унитарный многочлен, корнем которого является x. □

Определение 1.2. Элемент x из теоремы 1.1 называется *целым* над k. Расширение колец $R \supset k$ *целое*, если каждый элемент из R является целым над k.

Теорема 1.3. *Пусть R — коммутативная k-алгебра, порождаемая конечным числом целых элементов. Тогда R является конечно порожденным k-модулем.*

Доказательство. Пусть кольцо R порождается над k элементами $x_1, \ldots, x_n$, причем x_i является корнем унитарного многочлена степени n_i с коэффициентами из k. Тогда R как k-модуль порождается всеми одночленми от $x_1, \ldots, x_n$, причем по x_i меньше n_i. $\square$

Теорема 1.4. *Пусть k — нетерово кольцо и R — коммутативная k-алгебра. Тогда все целые над k элементы из R образуют подалгебру в R.*

Доказательство. Предположим, что элементы $a, b \in R$ целы над k. Тогда подалгебра в R, порожденная a, b будет конечно порожденным k-модулем по теореме 1.3. Но $ab, a+b$ лежат в этой подалгебре. В силу нетеровости k получаем, что $k[ab]$, $k[a+b]$ являются конечно порожденными k-модулями. $\square$

Определение 1.5. Коммутативная область k *целозамкнуто*, если каждый целый над k элемент поля частных лежит в k.

2. Аффинные алгебры

В этом разделе вы будем преполагать, что k — поле и R – коммутативная k-алгебра являющаяся областью. Элементы

$$u_1, \ldots, u_n \in R \tag{1}$$

составляют *базис трансцендентности* R над k, если

1) элементы (1) алгебраически независимы, т.е. если многочлен $f(t_1, \ldots, t_n)$ с коэффициентами из k ненулевой, то $f(u_1, \ldots, u_n) \neq 0$;
2) каждый элемент из R *алгебраичен* над $k[u_1, \ldots, u_n]$, т.е. является корнем нетривиального многочлена с коэффициентами из $k[u_1, \ldots, u_n]$.

Из определения вытекают следующие два утверждения

Предложение 1.6. *Пусть F – поле дробей области R. Тогда базис трансцендентности R над k является базисом трансцендентности F над k.*

Предложение 1.7. *Пусть $R = k[u_1, \ldots, u_n]$. Тогда всякая максимальная алгебраически независимая подсистема из* (1) *является базисом трансцендентности R над полем k.*

Предложение 1.8. *Пусть $u_1, \ldots, u_n$ — базис трансцендентности R над k, и $v \in R$ трансцендентен над $k[u_2, \ldots, u_n]$. Тогда $v, u_2, \ldots, v_n$ — базис трансцендентности R над k.*

Доказательство. Система $v, u_2, \ldots, u_n$ алгебраически независима, но система $v, u_1, \ldots, v_n$ зависима. Поэтому существует ненулевой многочлен от $n+1$ переменной такой, что $f(v, u_1, \ldots, u_n) = 0$. В этот многочлен обязан входить u_1, откуда u_1 является корнем

нетривиального многочлена над $k[v, u_2, \ldots, u_n]$. Другими словами, $v, u_2, \ldots, u_n$ — базис трансцендентности. □

Теорема 1.9. *Все базисы трансцендентности R над k содержать одинаковое число элементов.*

Доказательство. Пусть заданы два базиса (1) и $v_1, \ldots, v_m$. Если все элементы v_i алгебраичны над $k[u_2, \ldots, u_n]$, то $u_2, \ldots, u_n$ — базис трансцендентности, что неверно.

Пусть v_{i_1} транцендентен над $k[u_2, \ldots, u_n]$. По предложению 1.8 элементы $v_{i_1}, u_2, \ldots, u_n$ составляют базис. Продолжая этот процесс замены мы получим, что элементы $v_{i_1}, \ldots, v_{i_n}$ составляют базис. Отсюда $\{v_1, \ldots, v_m\} = \{v_{i_1}, \ldots, v_{i_n}\}$ и $m \leqslant n$. Аналогично $m \leqslant n$ и $n = m$. □

Число элементов в базисе трансцендентности R над полем k называется *степенью трансцендентности* $tr.degR$.

Теорема 1.10 (Лемма Нетер о нормализации)**.** *Пусть $R = k[u_1, \ldots, u_n]$ — аффинная область. Тогда в R существует такой базис трансцендентности $v_1, \ldots, v_d$, что R цело над $k[v_1, \ldots, v_d]$.*

Доказательство. Если элементы (1) алгебраически независимы, то утверждение верно.

Пусть они зависимы и $f(u_1, \ldots, u_n) = 0$, где f — ненулевой многочлен из $k[t_1, \ldots, t_n]$. Пусть p — простое число, большее суммы показателей в любом одночлене из f. Сделав замену переменных вида

$$u_i = \begin{cases} z_i + z_n^{p^i}, & i < n, \\ z_n, & i = n \end{cases}$$

мы получим, что в одночлене $x_1^{m_1} \cdots x_n^{m_n}$ старший член по z_n будет равен $z_n^{m_n + m_1 p + \cdots + m_{n-1} p^{n-1}}$. Эти показатели имеют разные p-адические разложения, и потому они не сокращаются. Следовательно,

$$f = z_n^M + \sum_{i=1}^{M-1} a_i(z_1, \ldots, z_{n-1}) z^i.$$

Но тогда z_n цело над $k[z_1, \ldots, z_{n-1}]$. Продолжая этот процесс завершаем доказательство. □

Теорема 1.11. *Пусть R — аффинная алгебра над полем k, являющаяся полем. Тогда* $\dim_k R < \infty$.

Доказательство. Пусть $v_1, \ldots, v_n$ — базис трансцендентности R над k из теоремы 1.10. Тогда R цело над $k[v_1, \ldots, v_n]$. Для любого ненулевого $z \in k[v_1, \ldots, v_n]$ элемент z^{-1} цел над $k[v_1, \ldots, v_n]$,

т.е. $z^{-m} + \sum_{i=0}^{m-1} a_i z^{-i} = 0, \quad a_i \in k[v_1, \ldots, v_n]$. Отсюда

$$z^{-1} = -\sum_{i=0}^{m-1} a_i z^{-i+m-1} \in k[v_1, \ldots, v_n].$$

Отсюда вытекает, что $k[v_1, \ldots, v_n]$ является полем. В силу алгебраической независимости $v_1, \ldots, v_n$ получаем, что $n{=}0$ и $k[v_1, \ldots, v_n] = k$. Отсюда R цело над k и нужно применить теоремы 1.3. □

Следствие 1.12. *Пусть R — область над полем k, порождаемая конечным числом целых элементов. Тогда R является полем конечной размерности над k. Если k алгебраически замкнуто, то $R = k$.*

Доказательство. По теоремам 1.3 и 1.11 каждый элемент из R является целым над k и R имеет конечную размерность над k. Пусть $a \in R \setminus 0$ и $a^d = \sum_{i=1}^{d-1} \alpha_i a^i, \quad \alpha_i \in k$. Если $\alpha_0 = \cdots = \alpha_i = 0,\ \alpha_{i+1} \neq 0$, то сокращая на $a^i \neq 0$, получаем аналогичное равенство с ненулевым свободным членом α_{i+1}. Пусть для простоты $\alpha_0 \neq 0$. Тогда

$$a^{-1} = -\frac{1}{\alpha_0}\left(a^{d-1} - \sum_{i=1}^{d-1} \alpha_i a^{i-1}\right).$$

Если k алгебраически замкнуто, то $k = R$ по лемме **??**. □

Теорема 1.13. *Пусть R — аффинная алгебра над алгебраически замкнутым полем k, и a — ненильпотентный элемент из R. Тогда существует такой гомоморфизм k-алгебр $\phi : R \to k$, что $\phi(a) \neq 0$.*

Доказательство. Рассмотрим локализованное кольцо R_a, состоящую из дробей $\frac{b}{a^m}$, где $b \in A$. При этом

$$\frac{b}{a^m} = \frac{d}{a^n} \iff a^r(a^n b - d a^m) = 0$$

для некоторого $r \geqslant 0$. Так как a не является нильпотентным элементом, то a не лежит в ядре гомоморфизма k-алгебр $x \to \frac{x}{1}$ из R в R_a. При этом алгебра R_a конечно порождена над k. Пусть I — максимальный идеал в R_a. Тогда R_a/I является полем, и аффинной алгеброй. По теореме 1.12 оно является конечно порожденным векторным пространством над алгебраически замкнутым полем k. Отсюда $R_a/I \simeq k$ и $a \notin I$. Это дает нужный гомоморфизм. $R \to R_a \to R_a/I \simeq k$. □

Теорема 1.14 (Теорема Гильберта о нулях)**.** *Пусть k — алгебраически замкнутое поле и M — множество решений совместной системы алгебраичеких уравнений*

$$f_i(t_1, \ldots, t_n) = 0, \quad i = 1, \ldots, m. \tag{2}$$

Предположим, что f — многочлен от $t_1, \ldots, t_n$ с коэффициентами из k, обращающийся в нуль во всех точках из M. Тогда f^d для некоторого d лежит в идеале I алгебры $k[t_1, \ldots, t_n]$, порождаемом $f_1, \ldots, f_m$.

Доказательство. Пусть $R = k[t_1, \ldots, t_n]/I$. Если образ f в R не нильпотентен, то существует гомоморфизм $\phi : R \to k$, при котором $\phi(I) = 0$, но $\phi(f) \neq 0$. Тогда $(\phi(t_1), \ldots, \phi(t_n)) \in M \subset k^n$, но в этом точке f не обращается в нуль, что неверно. □

Следствие 1.15. *Система алгебраических уравнений* (2) *над произвольным полем k несовместна тогда и только тогда, когда существуют такие многочлены $g_1, \ldots, g_n$, что $1 = f_1 g_1 + \cdots + f_n g_n$.*

Доказательство. Пусть система (2) несовместна. Тогда система

$$t_0 f_i(t_1, \ldots, t_n) = 0, \quad i = 1, \ldots, m. \tag{3}$$

совместна и имеет решения, при которых $t_0 = 0$. Следовательно, $t_0 = 0$ является следствием (3). По теореме 1.14 существует такое число $d \geqslant 1$, что

$$t_0^d = \sum_{i=1}^{m} t_0 f_i g_i(t_0, \ldots, t_n), \quad g_i(t_0, \ldots, t_n) \in k[t_0, \ldots, t_n].$$

Полагая $t_0 = 1$ и $g_i = g_i(1, t_1, \ldots, t_n) \in k[t_1, \ldots, t_n]$ завершаем доказательство. □

3. Алгебраические расширения полей

Определение 1.16. Пусть A – ассоциативная k-алгебра с 1. Элемент $z \in A$ называется *алгебраическим* или *целым* над k, если существует такой ненулевой многочлен $f \in k[X]$, $\deg f \geqslant 1$, что $f(z) = 0$. *Минимальным* многочленом алгебраического элемента z над k называется такой многочлен $f(X) \in k[X]$ минимальной степени со старшим коэффициентом 1, что $f(z) = 0$.

Упражнение 1.17. Пусть A – конечномерная ассоциативная алгебра над полем k с единицей. Доказать, что каждый элемент из A алгебраичен над k.

Упражнение 1.18. Пусть $z \in A$ — алгебраический элемент и I — множество всех таких многочленов $g \in k[X]$, что $g(z) = 0$. Доказать, что I является идеалом в $k[X]$ и $I = (f)$, где f — минимальный многочлен элемента z.

Предложение 1.19. *Пусть A – область над полем k, и $z \in A$ – алгебраический элемент с минимальным многочленом $f(X)$. Тогда f неприводим. Положим*

$$k[z] = \{a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \mid a_i \in k, n = \deg f\}.$$

Тогда $k[z]$ является подполем в A, содержащим k и z, причем

$$k[z] \simeq k[X]/(f). \tag{4}$$

Предложение 1.20. *Пусть $f \in k[X]$ имеет степень n. Тогда* $\dim_k (k[X]/(f)) = n$.

Доказательство. Убедимся, что элементы

$$1 + (f), X + (f), \ldots, X^{n-1} + (f) \tag{5}$$

составляют базис $k[X]/(f)$. □

Теорема 1.21. *Если k – поле, то $k[X]/(f)$ является полем тогда и только тогда, когда многочлен $f \in k[X]$ неприводим.*

Доказательство. Пусть $f = uv$, где $0 < \deg u, \deg v < n = \deg f$. По предложению 1.20 элементы $u+(f), v+(f) \neq 0$ в $k[X]/(f)$, но $(u + (f))(v + (f)) = 0$ в $k[X]/(f)$. Тогда в $k[X]/(f)$ имеются делители нуля, что невозможно.

Обратно, если f – неприводим и $u \in k[X] \setminus (f)$, то $(u, p) = 1$. Следовательно, найдутся такие элементы $r, s \in k[X]$, что $1 = su + rf$. Тогда $(u + (f))^{-1} = s + (f)$. □

Предложение 1.22. *Элемент $X+(f) \in k[X]$ является корнем f в поле $k[X]/(f)$. Минимальный элемент для z равен f.*

Определение 1.23. Пусть $f \in k[X]$, $\deg f \geqslant 1$. *Поле разложения f* – это такое расширение полей F/k, что

1) в F многочлен f разлагается на линейные множители;
2) в F нет меньшего подполя, содержащего k, в котором многочлен f разлагался на линейные множители.

Второе условие означает, что если $a_1, \ldots, a_n$ — корни f в алгебраическом замыкании k, то $F = k[a_1, \ldots, a_n]$.

Предложение 1.24. *Если F/k – поле разложения многочлена $f \in k[t]$, то F/k конечно.*

Доказательство. Пусть $a_, \ldots, a_m$ – все корни f в F. Рассмотрим подалгебру $A = k[a_1, \ldots, a_m]$ в F. По следствию 1.12 A имеет конечную размерность и является подполем. В силу условия 2) получаем, что $F = A$. □

Теорема 1.25. *Поле разложения F/k для заданного многочлена $f \in k[X]$, $\deg f \geqslant 1$ существует.*

Доказательство. Индукция по степени $\deg f$. Разложим f в произведение неприводимых многочленов, и пусть p – неприводимый множитель f. Тогда в поле $K = k[X]/(p)$ многочлен p имеет корень $z = X + (p)$. Следовательно, в кольце $K[X]$ многочлен f представим в виде $f = g(X - z)$, где $g \in K[X]$ имеет степень $\deg f - 1$. По индукции для g существует поле разложения F/K. Остается заметить, что F/k – поле разложения для f. □

Теорема 1.26. *Пусть $\xi : k_1 \to k_2$ – изоморфизм полей, $f \in k_1[X]$, $\deg f \geqslant 1$, и $f^\xi \in k_2[X]$ – образ f при изоморфизме ξ. Пусть F_1/k_1 и F_2/k_2 – два поля разложения для многочлена $f \in k_1[X]$ и $f^\xi \in k_2[X]$, соответственно. Тогда существует изоморфизм полей $\phi : F_1 \to F_2$, продолжающий ξ.*

Доказательство. Индукция по степени $\deg f$. Случай $\deg f = 1$ очевиден. Разложим f в произведение неприводимых многочленов, и пусть p – неприводимый множитель f. Пусть $z_1 \in F_1$ – корень p и $z_2 \in F_2$ – корень p^ξ. По предложениям 1.22, 1.19 существует изоморфизм полей $\psi : k_1[z_1] \to k_2[z_2]$, продолжающий ξ. Нетрудно видеть, что F_1 является полем разложения для $\frac{f}{X-z_1}$ – многочлена с коэффициентами из $k_1[z_1]$, а F_2 – полем разложения для $\frac{f^\xi}{X-z_2} \in k_2[z_2][X]$. По индукции существует изоморфизм $F_1 \to F_2$, продолжающий ψ. □

Поле k *алгебраически замкнуто*, если каждый многочлен с коэффициентами из k степени не ниже 1 имеет в k корень. Поле $\overline{k}$ является *алгебраическим замыканием* поля k, если $\overline{k}$ алгебраически замкнуто, $\overline{k} \supset k$, и каждый элемент из $\overline{k}$ алгебраичен над k.

Следствие 1.27. *Алгебраическое замыкание $\overline{k}$ поля k существует и единственно с точностью до изоморфизма.*

Предложение 1.28. *Если характеристика* $\operatorname{char} k$ *поля k равна $p > 0$, то k содержит поле вычетов $\mathbb{Z}/p\mathbb{Z}$. Если* $\operatorname{char} k = 0$, *то k содержит поле рациональных чисел $\mathbb{Q}$.*

Предложение 1.29. *Пусть K/k – конечное расширение полей. Тогда любое вложение $\sigma : k \to \overline{k}$ продолжается до вложения $K \to \overline{k}$. Число различных продолжений не превосходит* $\dim_k K$.

Доказательство. Достаточно рассмотреть случай $K = k[a]$. Если $f = a_0 + a_1 T + \cdots + a_{n-1}T^{n-1} + T^n \in k[T]$ – минимальный многочлен для $a \in K$, то $K \simeq k[T]/(f)$, и

$$\sigma\left(f(T)\right) = \sigma(a_0) + \sigma(a_1)T + \cdots + \sigma(a_{n-1})T^{n-1} + T^n \in \sigma(k)[T].$$

Существует корень $b \in \overline{k}$ многочлена $\sigma(f)$. Заметим, что многочлен $\sigma(f)$ неприводим над $\sigma(k)$. Поэтому

$$\sigma(k)[b] \simeq \sigma(k)[T]/\left(\sigma(f)\right) \simeq k[T]/(f) \simeq k[a].$$

Поэтому существует продолжение σ до изоморфизма $\sigma : k[a] \to \sigma(k)[b]$, при котором $\sigma(a) = b$.

Нетрудно видеть, что $\sigma\left(\sum_i \alpha_i a^i\right) = \sum_i \sigma(\alpha_i) b^i$, где $\alpha_i \in k$.

Число различных продолжений на $k[a]$ не больше числа корней $\sigma(f)$ в $\overline{k}$, т.е. не больше степени f. □

Следствие 1.30. *Пусть $K \supset k$ - конечное расширение полей, $x \in K$ и $f \in k[t]$ — минимальный многочлен для x. Если $\sigma : K \to \overline{k}$*

— гомоморфизм k-алгебр, то $\sigma(x)$ — корень многочлена f. Обратно, если $c \in K$ — корень многочлена f, то существует такой гомоморфизм k-алгебр $\sigma : K \to \overline{k}$, что $\sigma(x) = c$.

4. Конечные поля

Предложение 1.31. *Пусть K – конечное поле, содержащее подполе k. Тогда $|K| = |k|^n$, где $n = \dim_k K$. В частности, если F – конечное поле и $\operatorname{char} F = p > 0$, то $|F| = p^n$.*

Предложение 1.32. *Пусть k – поле и $|k| = q$. Тогда $x^q = x$ для всех $x \in k$.*

Предложение 1.33. *Пусть k – поле характеристики $p > 0$. Если $x, y \in k$, то $(x + y)^p = x^p + y^p$.*

Предложение 1.34. *Пусть F – поле характеристики $p > 0$, в котором многочлен $f = X^q - X$ разлагается на линейные множители, где q – степень p. Тогда множество всех корней многочлена f является подполем в F, содержащим $\mathbb{Z}_p$. В частности, если F – поле разложения $f \in \mathbb{Z}_p[T]$, то F совпадает с множеством всех корней f.*

Доказательство. Пусть x, y – корни f, и $q = p^n$, то по предложению 1.33 $(x + y)^q = x^q + y^q = x + y$, т. е. $x + y$ является корнем f. Аналогично, $xy, x^{-1}, -x$ являются корнями f. Кроме того, по предложению 1.32 элементы из $\mathbb{Z}_p$ являются корнями f. □

Теорема 1.35. *Пусть q – степень простого числа p. Тогда существует и единственное поле порядка q. Оно обозначается $\mathbb{F}_q$. В частности, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.*

Доказательство. Пусть $k = \mathbb{Z}/pZ$ – поле вычетов характеристики p, и $f = T^q - T \in k[T]$. Пусть F – поле разложения f. По предложению 1.34 $F/\mathbb{Z}_p$ состоит из всех корней многочлена f. Остается показать, что у f нет кратных корней.

Пусть $c \in F$ – корень кратности $s > 1$ многочлена f. Тогда $f = T^q - T = (T - c)^s g(T)$, откуда

$$f' = qT^{q-1} - 1 = -1 =$$
$$s(T - c)^{s-1} g(T) + (T - c)^s g(T)' = (T - c)^{s-1} h(T), \quad h(T) \in F[T],$$

что невозможно. Следовательно, $|F| = q$.

Итак, поле F разложения f – искомое. Его единственность вытекает из теоремы 1.26. □

Теорема 1.36. *Пусть k – поле и G – конечная подгруппа в k^*. Тогда группа G циклична.*

Доказательство. Группа G является прямым произведением своих силовских подгрупп. Поэтому в G существует элемент x наибольшего порядка d, причем порядок любого элемента в G делит d. Следовательно, каждый элемент из G является корнем уравнения $t^d - 1 = 0$. Но все степени x, а их d штук, являются корнями этого многочлена. Поэтому каждый элемент из G является степенью x. □

Следствие 1.37. *Мультипликативная группа $\mathbb{F}_q^*$ поля $\mathbb{F}_q$ циклична.*

Теорема 1.38. *Пусть p – простое число, и q — степень p. Для любого натурального числа d существует такой неприводимый многочлен $f \in \mathbb{F}_q[X]$ степени d, что $\mathbb{F}_{q^d} \simeq \mathbb{F}_q[X]/(f)$.*

Доказательство. По теореме 1.36 группа $\mathbb{F}_{q^d}$ циклична с порождающим элементом a. В частности, $\mathbb{F}_q[a] = \mathbb{F}_{q^d}$. По предложению 1.19 получаем, что $\mathbb{F}_{q^d} = \mathbb{F}_q[a] \simeq \mathbb{F}_q[X]/(f)$, где f – неприводимый многочлен из $\mathbb{F}_q[X]$. По предложению 1.20 степень f равна d. □

Теорема 1.39. *Пусть q является степенью простого числа p, и m, n — натуральные числа. Поле $\mathbb{F}_{q^m}$ является подполем $\mathbb{F}_{q^n}$ тогда и только тогда, когда $m \mid n$. При этом группа автоморфизмов $\mathbb{F}_{q^n}$, тождественных на $\mathbb{F}_{q^m}$ является циклической группой, порожденной автоморфизмом $\psi(x) = x^{q^m}$. В частности, группа автоморфизмов $\mathbb{F}_{q^n}$ является циклической группой порядка n, порождаемой автоморфизмом $\phi(x) = x^p$*

Доказательство. Заметим, что если $n = dm$, то каждый элемент $x \in \mathbb{F}_{q^m}$, отличный от нуля, удовлетворяет условию

$$x^{q^n-1} = x^{q^{dm}-1} = \left(x^{q^m-1}\right)^{1+q^m+\cdots+q^{m(d-1)}} = 1.$$

Поэтому $x \in \mathbb{F}_{q^n}$.

Обратное утверждение вытекает из предложения 1.31.

Пусть $\alpha \in \operatorname{Aut} \mathbb{F}_{q^n}$, причем α тождественно на $\mathbb{F}_{q^m}$. По теореме 1.38 получаем $\mathbb{F}_{q^n} = \mathbb{F}_{q^m}[X]/(g)$, где $g \in \mathbb{F}_{q^m}[X]$ – неприводимый многочлен степени $d = nm^{-1}$, корнем которого является элемент $a \in \mathbb{F}_{q^n}^*$, порождающий мультипликативную группу $\mathbb{F}_{q^n}^*$. Тогда g – минимальный многочлен для a. Следовательно, $0 = \alpha(g(a)) = g(\alpha(a))$, откуда $\alpha(a)$ – снова корень g. Но число корней g в $\mathbb{F}_{q^n}$ не выше степени g, т. е. не больше d. Но α однозначно определяется своим значением на a. Следовательно, порядок $\operatorname{Aut} \mathbb{F}_{q^n}$ не больше d. Для доказательства теоремы достаточно проверить, что порядок ϕ равен d, поскольку в этом случае группа автоморфизмов $\mathbb{F}_{q^n}$, тождественных на $\mathbb{F}_{q^m}$, будет состоять из степеней ϕ.

Пусть $\phi^r = 1$, т, е. $x^{q^{mr}} = x$ для всех $x \in \mathbb{F}_{q^n}$. Тогда каждый элемент $\mathbb{F}_{q^n}$ является корнем многочлена $T^{q^{mr}} - T$, откуда $r \geqslant n$. □

5. Теорема о примитивном элементе

Многочлен $f \in k[T]$ *сепарабельный*, у него нет кратных корней в $\bar{k}$.

Предложение 1.40. *Пусть многочлен $f \in k[T]$ имеет положительную степень. Производная $f' = 0$ тогда и только тогда, когда $\operatorname{char} k = p > 0$ и $f(T) = g(T^p)$ для некоторого многочлена $g(T) \in k[T]$.*

Предложение 1.41. *Неприводимый многочлен $f \in k[T]$ степени не меньше 1 сепарабелен тогда и только тогда, когда $f' \neq 0$.*

Доказательство. Действительно, пусть $f' = 0$ и $f = g(T^p)$. Предположим, что c — корень g. Тогда $f = (T^p - c)h(T^p) = (T - \sqrt[p]{c})^p h(T^p)$ и $\sqrt[p]{c}$ — кратный корень f. □

Следствие 1.42. *Если $\operatorname{char} k = 0$, то любой неприводимый многочлен сепарабелен.*

Элемент конечного расширения полей K/k *сепарабелен*, если его минимальный многочлен из $k[T]$ сеперабелен. Расширение полей K/k *сепарабельно*, если каждый элемент из K сепарабелен.

Теорема 1.43. *Пусть f – неприводимый сепарабельный многочлен. Тогда $k[T]/(f)$ – сепарабельное расширение поля k.*

Доказательство. Можно считать, что $p = \operatorname{char} k > 1$. Пусть

$$x = h(T) + (f) \in K = k[T]/(f), \quad \deg h < \deg f.$$

Если $g(T^p)$ – минимальный многочлен элемента x, то $g\left(h(T)^p\right) = u(T)f(T)^m$ для некоторого многочлена $u(T) \in k[T]$ и некоторого натурального числа m, причем u, f взаимно просты. Беря производную, получаем $0 = u'f^m + muf'f^{m-1}$, откуда

$$u'f = -muf'. \tag{6}$$

При этом $f' \neq 0$ в силу сепарабельности f. Таким образом $(f, f') = (u, f) = 1$ в силу неприводимости f. Следовательно, (6) влечет $f|m$, т.е. $p|m$ и $u' = 0$. Но тогда $u = v(T^p)$ для некоторого $v \in k[T]$. Итак,

$$g\left(h(T)^p\right) = v(T^p)f(T)^{pd}. \tag{7}$$

Обозначим через k^p все элементы вида z^p, где $z \in k$. Легко видеть, что k^p является подполем в k и $h(T)^p$, $f(T)^{pd} \in k^p[T^p]$. Пусть e_i, $i \in I$ – базис k над k^p. Тогда

$$g(T) = e_1 g_1(T) + \cdots + e_n g_n(T), \quad \deg g_i(T) \leqslant \deg g(T),$$
$$v(T) = e_1 v_1(T) + \cdots + e_n v_n(T),$$

где $g_i(T), v_i(T) \in k^p[T]$. Поэтому в (7) имеем $\sum_{i=1}^n e_i g_i\left(h(T)^p\right) = \sum_{i=0}^n e_i v_i(T^p) f(T)^{pd}$, откуда $g_i\left(h(T)^p\right) = v_i(T^p)f(T)^{pd}$ для любого i

Пусть $v_i \neq 0$. Тогда и $g_i \neq 0$. В силу определения k^p найдутся такие многочлены $t_i(T), w_i(T) \in k[T]$, что $t_i(T)^p = g_i(T^p),\ w_i(T)^p = v_i(T^p)$. Но тогда $t_i\left(h(T)\right) = w_i(T)f(T)^d$ и $t_i(x) = 0$ в K, что противоречит минимальности многочлена $g(T^p)$. □

Упражнение 1.44. Пусть задано конечное расширение полей $k \subset F \subset K$. Если K/k – сепарабельное расширение, то F/k, K/F – сепарабельные расширения. Обратно, если F/k, K/F – сепарабельные расширения, то из расширение K/k сепарабельно.

Теорема 1.45. *Пусть K/k – конечное сепарабельное расширение полей. Тогда $\dim_k K$ равно числу различных вложений K в $\overline{k}$.*

Доказательство. Можно считать, что $K = k[x]$. Тогда минимальный многочлен $f(T)$ для x не имеет кратных корней. При вложении $\sigma : K \to \overline{k}$ получаем, что $\sigma(x)$ – любой корень $f(T)$. Остается учесть, что у $f(T)$ нет кратных корней. □

Теорема 1.46 (Теорема о примитивном элементе)**.** *Пусть задано конечное сепарабельное расширение полей K/k. Тогда существует* примитивный элемент $z \in K$ *т.е. $K = k[z]$.*

Доказательство. Можно считать, что $K = k[x, y]$, где x, y сепарабельны над k. Предположим, что $\sigma_1, \ldots, \sigma_n$ – различные гомоморфизмы k-алгебр $K \to \overline{k}$. По теореме 1.45 $\dim_k K = n$. Предполагая, что k бесконечно, рассмотрим ненулевой многочлен

$$P(t) = \prod_{i \neq j} \left(\sigma_i(x) + t\sigma_i(y) - \sigma_j(x) - t\sigma_j(y)\right) \in \overline{k}[t].$$

В силу бесконечности k найдется такой элемент $c \in k$, что $P(c) \neq 0$. В этом случае все элементы $\sigma_i(x+cy)$ различны. Отсюда минимальный многочлен элемента $x+cy$ делится на $\prod_i \left(T - \sigma_i(x + cy)\right)$, и его степень $\geqslant n = \dim_k K$. Поэтому степень минимального многочлена для $x + yc$ равна n, т. е. $k[x, y] = k[x + cy]$.

Случай конечного поля рассмотрен в §4. □

Расширение полей K/k называется *нормальным*, если каждый неприводимый многочлен из $k[T]$, имеющий в K корень, разлагается в $K[T]$ на линейные множители.

Теорема 1.47. *Для конечного расширения K/k следующие условия эквивалентны:*

1) *K/k нормально;*
2) *K является полем разложения некоторого многочлена из $k[T]$;*
3) *любое вложение $K \to \overline{k}$, тождественное на k является автоморфизмом K.*

Доказательство. Пусть выполнено условие 1) и $\sigma : K \to \overline{k}$ – вложение полей. Пусть $x \in K$ и $f(T) \in k[T]$ – его минимальный многочлен. Тогда $\sigma(x)$ снова корень неприводимого многочлена $f(T)$ по следствию 1.30. По условию $\sigma(x) \in K$, т. е. выполнено 3).

Предположим, что выполнено условие 3) и $K = k[x_1, \ldots, x_n]$. Пусть $f_i(T) \in k[T]$ – минимальный многочлен для x_i. Положим $f = f_1 \cdots f_n$. Из условия 3) следует, что все корни f лежат в K и поэтому K – поле разложения f т. е. выполнено условие 2).

Пусть, наконец выполнено условие 2). Тогда, ясно, выполнено условие 3), а из условия 3) вытекает условие 1). □

6. Теория Галуа

Конечное нормальное сепарабельное расширение K/k называется *расширением Галуа*. *Группой Галуа* $\mathrm{Gal}(K/k)$ называется группа автоморфизмов $\mathrm{Aut}_k K$ для K как k-алгебры.

Упражнение 1.48. Пусть $k \subset F \subset K$, причем K/k – расширение Галуа. Тогда K/F также расширение Галуа.

Теорема 1.49. *Пусть задано расширение Галуа K/k и $G = \mathrm{Gal}(K/k)$. Тогда $k = K^G$. Отображение $F \mapsto \mathrm{Gal}(K/F)$ промежуточных полей $k \subset F \subset K$ в подгруппы в $\mathrm{Gal}(K/k)$ инъективно.*

Доказательство. Предположим, что $x \in K^G$ и $\sigma : k[x] \to \overline{k}$ – произвольное вложение. Оно продолжается до вложения $\sigma : K \to \overline{k}$. По теореме 1.47 σ является автоморфизмом из $\mathrm{Gal}(K/k)$. Следовательно, $\sigma(x) = x$. Но $\sigma(x)$ может быть любым корнем своего минимального многочлена. Следовательно, у этого многочлена один корень x, откуда $x \in k$.

Пусть F, F' – два подполя в K, содержащие k. Если

$$H = \mathrm{Gal}(K/F) = \mathrm{Gal}(K/F') \subseteq \mathrm{Gal}(K/k),$$

то $F = K^H = F'$. □

Теорема 1.50 (Артин)**.** *Пусть K – поле и G – конечная группа его автоморфизмов порядка n. Положим $k = K^G$. Тогда K/k – расширение Галуа степени n, причем $\mathrm{Gal}(K/k) = G$.*

Доказательство. Возьмем элемент $x \in K$ и предположим, что $\{\sigma_1 x, \ldots, \sigma_r x\}$ – орбита действия G на x. Рассмотрим многочлен $f(T) = \prod_{j=1}^{r} (T - \sigma_j(x))$. Тогда $\tau(f) = f$ для всех $\tau \in G$, т. е. $f \in k[T]$. По построению этот многочлен сепарабелен, неприводим и разложим в K на линейные множители. Поэтому K/k сепарабельно. Кроме того, каждое конечное расширение F/k, где $F \subseteq K$, примитивно, и потому имеет степень $r \leqslant n$. Отсюда следует, что расширение K/k конечно и имеет степень не выше n.

Более того, расширение K/k нормально по теореме 1.45, и теореме 1.47 условие **3**, и, следовательно, K/k является расширением Галуа.

Как отмечалось расширение K/k примитивно по теореме 1.46. Для соответствующего минимального многочлена f как и выше имеем $r = \deg f = \dim_k K$. Но тогда $n = |G| = r$. С другой стороны, $|\operatorname{Gal}(K/k)| = r$. Так как $G \subseteq \operatorname{Gal}(K/k)$ имеет тот же порядок, то $G = \operatorname{Gal}(K/k)$. □

Теорема 1.51 (Основная теорема теории Галуа)**.** *Пусть задано расширение Галуа K/k и $G = \operatorname{Gal}(K/k)$. Имеется взаимно однозначное соответствие $H \mapsto K^H$ между подгруппами H в G и подполями в K, содержащими k. Подполе $F = K^H$ в K будет расширением Галуа F/k тогда и только тогда, когда $H \lhd G$. При этом $\operatorname{Gal}(F/k) = G/H$.*

Доказательство. Наличие взаимно однозначного соответствия вытекает из теорем 1.49 и 1.50.

Пусть H – подгруппа в G и $F = K^H$. Для любого вложения $\tau \in G$ имеем $\tau(F) = K^{\tau H \tau^{-1}}$. Следовательно, $\tau(F) = F \iff \tau H \tau^{-1} = H$. Но $\tau(F) = F$ для любого $\tau \in G$ в том и только в том случае, если F/k нормально.

В силу нормальности K/F и теоремы 1.47 каждый автоморфизм K переводит F в себя. Поэтому имеется гомоморфизм ограничения

$$\operatorname{Gal}(K/k) \longrightarrow \operatorname{Gal}(F/k), \tag{8}$$

с ядром $\operatorname{Gal}(K/F)$.

Если $\sigma \in \operatorname{Gal}(F/k)$, то по предложению 1.29 и теореме 1.47 σ поднимается до некоторого элемента из $\operatorname{Gal}(K/k)$. Таким образом, гомоморфизм групп (8) сюръективен. Поэтому точна последоваиательность

$$1 \longrightarrow \operatorname{Gal}(K/F) \longrightarrow \operatorname{Gal}(K/k) \longrightarrow \operatorname{Gal}(F/k) \longrightarrow 1.$$

□

Группой Галуа многочлена $f(t) \in K[T]$ называется группа Галуа K/k, где K поле разложения многочлена f. Рассмотрим примеры расширений Галуа.

Теорема 1.52. *Пусть k – поле, и m – натуральное число, взаимно простое с характеристикой поля. Если ζ – примитивный корень степени m из 1 и $K = k[\zeta]$, то расширение K/k является расширением Галуа с группой Галуа, изоморфной подгруппе группы $(\mathbb{Z}/m)^*$ обратимых элементов кольца вычетов по модулю m.*

Доказательство. Минимальный многочлен ζ над k является делителем сепарабельного многочлена $X^m - 1$. Поэтому расширение K/k сепарабельно. В силу примитивности ζ расширение K/k нормально и потому является расширением Галуа.

Каждый элемент $g \in \mathrm{Gal}(K/k)$ переводит ζ в другой примитивный корень $g(\zeta)$ степени m из 1. Поэтому $\mathrm{Gal}(K/k)$ является подгруппой абелевой группы обратимых элементов $(\mathbb{Z}/m)^*$. $\square$

7. Разрешимые расширения полей

Пусть задана группа G и поле k. *Характером* G в k называется гомоморфизм группы G в мультипликативную группу k^* поля k.

Теорема 1.53 (Артин)**.** *Различные характеры G в k линейно независимы.*

Доказательство. Будем вести доказательство по числу характеров. Пусть $\chi_1, \ldots, \chi_n : G \to k^*$ – различные характеры, причем существуют такие элементы $\alpha_, \ldots, \alpha_n \in k$, что $\alpha_1\chi_1 + \cdots + \alpha_n\chi_n = 0$.

Будем вести доказательство индукцией по n. Случай $n = 1$ очевиден. Пусть для $n-1$ утверждение верно. Тогда для любых $h, g \in G$ выполнено равенство

$$\begin{aligned} 0 &= [\alpha_1\chi_1(hg) + \cdots + \alpha_n\chi_n(hg)] - \chi_1(h)\,[\alpha_1\chi_1(g) + \cdots + \alpha_n\chi_n(g)] \\ &= \alpha_2\,[\chi_2(h) - \chi_1(h)]\,\chi_2(g) + \cdots + \alpha_n\,[\chi_n(h) - \chi_1(h)]\,\chi_n(g). \end{aligned}$$

По индукции $\alpha_i\,[\chi_i(h) - \chi_1(h)] = 0$ для всех $i = 2, \ldots, n$. Так как при разных i характеры различны, то $\alpha_i = 0$ при $i = 2, \ldots, n$. Подставляя в исходное равенство, получаем, что и $\alpha_1 = 0$. $\square$

Пусть K/k – расширение Галуа и $G = \mathrm{Gal}(K/k)$. Если $x \in K$, то *нормой* элемента x называется $N(x) = \prod_{\sigma\in G}\sigma(x)$. Несложно видеть, что $\sigma\,(N(x)) = N(x)$ для всех $\sigma \in G$. Поэтому в силу теоремы 1.49 получаем, что $N(x) \in k$.

Упражнение 1.54. Если $x, y \in K$, то $N(xy) = N(x)N(y)$. Кроме того, $N(\sigma(x)) = N(x)$ для всех x. Если $x \in k$, то $N(x) = x^{|G|}$.

Теорема 1.55 (Гильберт)**.** *Пусть K/k – расширение Галуа степени n с циклической группой Галуа $\langle\sigma\rangle$. Для элемента $x \in K$ следующие условия эквивалентны:*

(1) *$x = y\sigma\,(y^{-1})$ для некоторого $y \in K^*$;*
(2) *$N(x) = 1$.*

Доказательство. Если выполнено условие **(1)**, то $N(x) = N\,(y\sigma\,(y^{-1})) = N(y)N\,(\sigma\,(y))^{-1} = N(y)N(y)^{-1} = 1$, по упражнению 1.54, т.е. выполнено условие **(2)**.

Обратно, пусть выполнено условие **(2)**. Применяя теорему 1.53 для случая $G = K^*$, $k = K$, получаем, что отображение

$$z \mapsto z + x\sigma(z) + x\,\sigma(x)\sigma^2(z) + \cdots + x\sigma(x)\cdots\sigma^{n-2}(x)\sigma^{n-1}(z),$$

является ненулевым. Поэтому найдется такой элемент $z \in K^*$, что

$$z + x\sigma(z) + x\,\sigma(x)\sigma^2(z) + \cdots + x\sigma(x)\cdots\sigma^{n-2}(x)\sigma^{n-1}(z) = y \neq 0.$$

Из условия **(2)** вытекает, что

$$\begin{aligned} x\sigma(y) &= x\sigma(z) + x\,\sigma(x)\sigma^2(z) + \cdots + x\sigma(x)\cdots\sigma^{n-2}(x)\sigma^{n-1}(z) \\ &+ x\sigma(x)\cdots\sigma^{n-1}(x)\sigma^n(z) \\ &= x\sigma(z) + x\,\sigma(x)\sigma^2(z) + x\sigma(x)\cdots\sigma^{n-2}(x)\sigma^{n-1}(z) + N(x)\sigma^n(z) \\ &= x\sigma(z) + x\,\sigma(x)\sigma^2(z) + \cdots + x\sigma(x)\cdots\sigma^{n-2}(x)\sigma^{n-1}(z) + z = y. \end{aligned}$$

откуда $x = y\sigma\,(y^{-1})$. □

Теорема 1.56. *Пусть k – поле и n – натуральное число, взаимно простое с характеристикой поля, причем в k содержатся все корни степени n из 1.*

Если K/k – циклическое расширение Галуа степени n, то существует то существует такой элемент $\alpha \in K$, что $K = k[\alpha]$ и $\alpha^n \in k$.

Обратно, пусть $a \in k$ и $\alpha \in K$ – корень уравнения $X^n - a = 0$. Тогда расширение $k[\alpha]/k$ – циклическое.

Доказательство. Пусть K/k – расширение Галуа с циклической группой Галуа $\mathrm{Gal}(k/k) = \langle\sigma\rangle$. Пусть $\zeta \in k$ – примитивный корень степени n из 1. Тогда $N(\zeta^{-1}) = (\zeta^{-1})^n = 1$, так как в k элементы из $\mathrm{Gal}(K/k)$ действует тождественно. По теореме 1.55 найдется такой элемент $\alpha \in K^*$, что $\sigma(\alpha) = \zeta\alpha$. При этом $\sigma^j(\alpha) = \zeta^j\alpha$ для всех j. Поэтому все элементы $\sigma^j(\alpha)$ различны при $j = 0, \ldots, n-1$. В силу теоремы 1.51 гомоморфизм ограничения $\mathrm{Gal}(K/k) \to \mathrm{Gal}(k[\alpha]/k)$ инъективен, т.е. является изоморфизмом. Отсюда по той же теореме $K = k[a]$. Заметим, что $\sigma(\alpha^n) = \zeta^n\alpha^n = \alpha^n$, т.е. $\alpha^n \in k$, и первое утверждение доказано.

Обратно, пусть α – корень многочлена $X^n - a \in k[X]$. Тогда $\zeta^j\alpha$ также корень этого многочлена и, следовательно, $k[\alpha]/k$ – нормальное расширение. Все эти корни различны, и поэтому это расширение сепарабельно, т.е. оно является расширением Галуа.

Пусть $G = \mathrm{Gal}(k[\alpha]/k)$ и $\sigma \in G$. Тогда $\sigma(\alpha) = \xi_\sigma\alpha$, где ξ_σ – корень степени n из 1. Отображение $\sigma \mapsto \xi_\sigma$ задает вложение G в циклическую группу корней степени n из 1. Следовательно, группа G циклическая как подгруппа циклической группы. □

Определение. Конечное расширение полей E/k *разрешимо*, если для существует такое расширение Галуа K/k, что $E \subseteq K$ и группа Галуа $\mathrm{Gal}(K/k)$ разрешима. Конечное расширение полей

E/k нулевой характеристики *разрешимо в радикалах*, если существует такое конечное расширение Галуа K/k, что $E \subseteq K$ и последовательность расширений полей $K = K_0 \supset K_1 \supset \cdots \supset K_m = k$, где каждое расширение K_i/K_{i+1} получается присоединением корня из многочлена $X^{n_i} - a_i$, где $a_i \in K_{i+1}$.

Теорема 1.57. *Пусть E/k – расширение полей нулевой характеристики. Оно разрешимо в том и только в том случае, если оно разрешимо в радикалах.*

Доказательство. Пусть E/k разрешимо и K/k – конечное разрешимое расширение Галуа поля k, содержащее E. Обозначим через m произведение всех простых делителей степени $[K : k]$. Рассмотрим поле $F = k[\zeta]$, где ζ – примитивный корень степени m из 1. По теореме 1.52 расширение F/k абелево. Нетрудно видеть, что $K[\zeta]$ разрешимо над $F = k[\zeta]$, поскольку имеется последовательность расширений Галуа $k \subset K \subset K[\zeta]$. При этом степень расширения $K[\zeta]/k[\zeta]$ имеет те же простые делители, что и m.

По теореме **??** в $G = \mathrm{Gal}\,(K[\zeta]/k[\zeta])$ имеется ряд подгрупп (**??**) в котором $G_{i+1} \lhd G_i$ и каждая факторгруппа G_i/G_{i+1} для любого i является циклической группой простого порядка. По теореме 1.51 в $K[\zeta]$ имеется ряд подполей $K[\zeta] = K_0 \supset K_1 \supset \cdots \supset K_n \supset K_{n+1} = k[\zeta] \supset k$, что K_i/K_{i+1} – расширение Галуа простой степени, делящей m. По теореме 1.56 $K[\zeta]$ над $k[\zeta]$ разрешимо в радикалах. Отсюда следует, что $K[\zeta]/k$ разрешимо в радикалах, т.е. E/k разрешимо в радикалах.

Обратно, пусть E/k разрешимо в радикалах и K из условия разрешимости. Для любого вложения $\sigma : K \to \overline{k}$ над k расширение $\sigma(K)/k$ также разрешимо в радикалах. Пусть подполе F в $\overline{k}$ порождается всеми $\sigma(K)$. Число вложений $\sigma : K \to \overline{k}$ не превосходит не превосходит $\dim_k K$. Таким образом, если $K = k[a_1, \ldots, a_m]$ и $\sigma_1, \ldots, \sigma_r$ — все такие вложения, то $F = k[\sigma_i(a_j)]$, где $1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant r$, т.е. расширение F/k конечно. Кроме того, оно нормально по теореме 1.47, условие 3. Поскольку характеристика нулевая, то расширение F/k сепарабельно и потому является расширением Галуа.

Пусть ζ – примитивный корень из 1 степени m, равной произведению всех простых делителей степени $[F : k]$. Как и выше можно считать, что $\zeta \in k$.

Пусть K_i — подполе из условия разрешимости в радикалах. Получаем цепь подполей

$$k \subseteq \sigma_1(K_n) \subseteq \cdots \subseteq \sigma_1(K_0) \subseteq \sigma_2(K_n)\sigma_1(K_0) \subseteq \cdots \\ \cdots \subseteq \sigma_2(K_0)\sigma_1(K_0) \subseteq \cdots \sigma_r(K_0) \cdots \sigma_1(K_0) = F,$$

в котором все факторы получаются присоединением корня двучлена. Остается применить теоремы 1.56, **??**.

□

Глава 2

Алгебры Ли

1. Алгебры Ли и их примеры

Определение 2.1. *Алгеброй Ли* L называется неассоциативная алгебра с умножением $[x, y]$, удовлетворяющая тождествам

$$[x, x] = [[x, y], z] + [[y, z], x] + [[z, x], y] = 0.$$

Пример 2.2. Алгебра $A^{(-)}$, алгебра $\mathbb{R}^3, [x, y] = x \times y$.

Упражнение 2.3. В алгебре Ли выполнено тождество антикоммутативности $[x, y] = -[y, x]$.

Определение 2.4. Пусть A – произвольная алгебра. Линейное оператор D на A называется *дифференцированием*, если

$$D(xy) = D(x)y + xD(y).$$

Через $\mathrm{Der}(A)$ обозначается множество всех дифференцирований алгебры A.

Предложение 2.5. $\mathrm{Der}(A)$ *является подалгеброй Ли в алгебре Ли всех линейных операторов* $\mathcal{L}(A)^{(-)}$ *на* A.

Если x – элемент алгебры Ли L, то линейный оператора $\mathrm{ad}\, x$ в L, задаваемый по правилу $(\mathrm{ad}\, x)(y) = [x, y]$, называется *внутренним дифференцированием* в L.

Предложение 2.6. *Внутреннее дифференцирование является дифференцированием. Кроме того, отображение* $x \to \mathrm{ad}\, x$ *является гомоморфизмом алгебр Ли* $\mathrm{ad} : L \to \mathcal{L}(L)^{(-)}$.

Доказательство. Из тождества Якоби вытекает, что

$$(\mathrm{ad}\, x)[y, z] = [(adx)y, z] + [x, (\mathrm{ad}\, x)z].$$

Из этого же тождества следует, что

$$\mathrm{ad}[x, y] = (\mathrm{ad}\, x)(\mathrm{ad}\, y) - (\mathrm{ad}\, y)(\mathrm{ad}\, x).$$

□

Упражнение 2.7. Пусть f – билинейная симметричная форма на n-мерном пространстве k^n, где k – поле. Через $\mathfrak{o}(n, f)$ – обозначается множество всех кососимметричных относительно f линейных операторов в k^n. т. е. множество всех таких линейных операторов $\mathcal{C}$ в k^n, что $f(\mathcal{C}x, y) = -f(x, \mathcal{C}y)$. Доказать, что $\mathfrak{o}(n, f)$ – подалгебра Ли в $\mathrm{Mat}(n, k)^{(-)}$.

Упражнение 2.8. Пусть задана полуторалинейная эрмитова функция f в n-мерном комплексном пространстве $\mathbb{C}^n$. Обозначим через $\mathfrak{su}(n, f)$ обозначим множество всех кососимметричных относительно f линейных операторов в $\mathbb{C}^n$, т. е. множество всех таких линейных операторов $\mathcal{A}$ в $\mathbb{C}^n$, что $f(\mathcal{A}x, y) = -f(x, \mathcal{A}y)$. Доказать, что $\mathfrak{su}(n, f)$ – подалгебра Ли в $\mathrm{Mat}(2n, \mathbb{R})^{(-)}$.

Обозначение 2.9. Через $\mathfrak{sl}(n, k)$ обозначается множество всех матриц из $\mathrm{Mat}(n, k)$ со следом 0.

Упражнение 2.10. $\mathfrak{sl}(n, k)$ является подалгеброй Ли в алгебре $\mathrm{Mat}(n, k)^{(-)}$.

2. Простые алгебры Ли

Подпространство I в алгебре Ли L называется *идеалом*, если $[x, y] \in I$ для любого $x \in I$, $y \in L$. Если $I \lhd L$, то факторпространство L/I является алгеброй Ли относительно умножения $[a + I, b + I] = [a, b] + I$. Для алгебр Ли также справедливы теоремы о гомоморфизмах и изоморфизмах.

Алгебра Ли L называется *простой*, если в ней только два идеала 0, L.

Теорема 2.11. *Алгебра $\mathfrak{sl}(n, k)$ проста, если $\operatorname{char} k$ не делит $2n$.*

Доказательство. Нам предварительно потребуется несколько утверждений. Через E_{ij} будем обозначать матричную единицу. Из правила $E_{ij}E_{rs} = \delta_{jr}E_{is}$ умножения матричных единиц имеем

$$[E_{ij},\ E_{rs}] = \delta_{jr}E_{is} - \delta_{is}E_{rj}. \tag{9}$$

Матричная единичка E_{rs} лежит в $\mathfrak{sl}(n, k)$ при $r \neq s$.

Лемма 2.12. *Пусть u – матрица, причем $[u, E_{r,s}] = 0$ для всех $r \neq s$. Тогда $u = 0$.*

Доказательство. По условию матрица u перестановочна со всеми матрицами $E_{rs,}$, где $r \neq s$. Заметим, что $E_{ss} = E_{rs}E_{sr}$. Поэтому матрица u перестановочна со всеми матричными единицами и потому матрица $u = \lambda E$ для некоторого скаляра $\lambda \in k$. Но тогда $0 = \operatorname{tr} u = n\lambda$, откуда $\lambda = 0$, поскольку $\operatorname{char} k \nmid n$. Итак, $u = \lambda E = 0$. □

Лемма 2.13. *Если идеал I в $\mathfrak{sl}(n, k)$ содержит матрицу E_{rs} при некоторых $r \neq s$, то $I = \mathfrak{sl}(n, k)$.*

Доказательство. По (9) в I лежит матрица $[E_{ir}, E_{rs}] = E_{is}$ при $i \neq s$. Аналогично, $[E_{is}, E_{sj}] = E_{ij} \in I$ при любых $j \neq i$. Кроме того, в I лежит матрица $[E_{ij}, E_{ji}] = E_{ii} - E_{jj}$, откуда следует утверждение леммы. □

Пусть $0 \neq I \lhd \mathfrak{sl}(n,k)$ и $u \in I \setminus 0$. Без ограничения общности, по лемме 2.12 от u перейти к $v = [u, E_{rs}] \in I$ для некоторой пары индексов $r \neq s$. При этом в силу (9) можно считать, что все ненулевые элементы матрицы v лежат либо в r-ой строке, либо в s-ом столбце, т. е.

$$v = \sum_j a_{rj}E_{rj} + \sum_i b_{is}E_{is}, \quad a_{rj}, b_{is} \in k.$$

При этом $\operatorname{tr} v = a_{rr} + b_{ss} = 0$.

Предположим, что некоторый коэффициент $b_{ts} \neq 0$, где $s \neq t \neq r$. Тогда в идеале I лежит ненулевой элемент

$$\begin{aligned} w = [v, E_{rt}] &= \sum_j a_{rj}[E_{rj}, E_{rt}] + \sum_i b_{is}[E_{is}, E_{rt}] \\ &= \sum_j a_{rj}\left(\delta_{jr}E_{rt} - \delta_{rt}E_{rj}\right) + \sum_i b_{is}\left(\delta_{sr}E_{it} - \delta_{it}E_{rs}\right) \\ &= a_{rr}E_{rt} - b_{ts}E_{rs}. \end{aligned}$$

Следовательно, без ограничения общности можно считать, что $w = \alpha E_{rt} - E_{rs}$, где индексы t, r, s различны. Тогда в I лежит

$$-[w, E_{st}] = -\alpha[E_{rt}, E_{st}] + [E_{rs}, E_{st}] = E_{rt},$$

где $r \neq t$. Отсюда по лемме 2.13 вытекает утверждение теоремы.

Итак, можно считать, что $b_{ts} = 0$ при $t \neq r, s$, и, аналогично, $a_{rj} = 0$ при $j \neq r, s$. В этом случае

$$v = a_{rr}E_{rr} + a_{rs}E_{rs} + b_{ss}E_{ss},$$

причем $a_{rr} + b_{ss} = 0$. Тогда в I лежит элемент

$$\begin{aligned} [v, E_{rs}] &= a_{rr}[E_{rr}, E_{rs}] + a_{rs}[E_{rs}, E_{rs}] + b_{ss}[E_{ss}, E_{rs}] \\ &= a_{rr}E_{rs} - b_{ss}E_{rs} = (a_{rr} - b_{ss})E_{rs}. \end{aligned}$$

Таким образом, если $a_{rr} - b_{ss} \neq 0$, то можно применить лемму 2.13.

Пусть $a_{rs} = b_{ss}$. Так как $\operatorname{char} k \neq 2$, то $a_{rr} = b_{ss} = 0$ и $u = a_{rs}E_{rs}$. Остается применить лемму 2.13. □

Теорема 2.14. *Алгебра Ли* $(\mathbb{R}^3, \times)$ *проста.*

Доказательство. Убедимся сначала, что $(\mathbb{R}^3, \times)$ – алгебра Ли. Пусть e_1, e_2, e_3 – ортонормированный базис в $\mathbb{R}^3$. Тогда можно считать, что $[e_1, e_2] = e_3$, $[e_2, e_3] = e_1$, $[e_3, e_1] = e_2$. Непосредственная проверка показывает, что

$$[x, x] = J(e_1, e_2, e_3) = [[e_1, e_2], e_3] + [[e_2, e_3], e_1] + [[e_3, e_1], e_2] = 0.$$

Кроме того, якобиан $J(x, y, z)$ кососимметричен. Отсюда выводится $(\mathbb{R}^3, \times)$ – алгебра Ли.

Пусть I – ненулевой идеал в $(\mathbb{R}^3, \times)$. Можно считать, что $e_1 \in I$. Тогда I содержит $e_3 = [e_1, e_2], e_2 = [e_3, e_1] \in I$. Следовательно, $I = (\mathbb{R}^3, \times)$. □

3. Разрешимые алгебры Ли

Алгебра Ли $\mathfrak{g}$ *абелева*, если $[x, y] = 0$ для всех $x, y \in \mathfrak{g}$.

Упражнение. Пусть A – ассоциативная алгебра. Доказать, что алгебра Ли $A^{(-)}$ абелева в том и только в том случае, если A – коммутативная алгебра.

Пусть A, B – два идеала в алгебре Ли L. *Взаимным коммутантом* $[A, B]$ называется линейная оболочка всех коммутаторов $[a, b]$, где $a \in A,\ b \in B$.

Предложение 2.15. $[A, B] \lhd L$.

Доказательство. Если $a \in A,\ b \in B,\ x \in L$, то в силу тождества Якоби $[[a, b], x] = [[a, x], b] + [a, [b, x]] \in [A, B]$. □

Определим в алгебре Ли $\mathfrak{g}$ *производный ряд*

$$\mathfrak{g} = \mathfrak{g}^{(0)} \supset g^{(1)} \supset \cdots \supset \mathfrak{g}^{(t+1)} \supset \cdots$$

по правилу $\mathfrak{g}^{(t+1)} = [\mathfrak{g}^{(t)}, g^{(t)}]$. По предложению 2.15 каждое $\mathfrak{g}^{(t)} \lhd \mathfrak{g}$.

Алгебра Ли $\mathfrak{g}$ *разрешима ступени не выше* m, если в ней имеется ряд подалгебр

$$\mathfrak{g} = \mathfrak{g}_0 \rhd \mathfrak{g}_1 \rhd \cdots \rhd \mathfrak{g}_m \rhd \mathfrak{g}_{m+1} = 0, \tag{10}$$

в котором $g_{i+1} \lhd \mathfrak{g}_i$ и факторалгебра $\mathfrak{g}_i/\mathfrak{g}_{i+1}$ абелевы для всех i.

Теорема 2.16. *Для алгебры Ли* $\mathfrak{g}$ *следующие условия эквивалентны:*

1) *алгебра* $\mathfrak{g}$ *разрешима ступени не выше* m*;*
2) $\mathfrak{g}^{(m+1)} = 0$.

Доказательство. 1)⇒2). Действительно, из абелевости факторов ряда (10) индукцией по t проверяется, что $\mathfrak{g}^{(t)} \supseteq \mathfrak{g}_{(t)}$.

Обратно, если выполнено 2), то конечность производного ряда доказывает условие 1). □

Примером разрешимой алгебры Ли является алгебра $\mathrm{T}(n, k)^{(-)}$ всех верхнетреугольных матриц размера n с коэффициентами в поле k.

Упражнение. Доказать, что

- класс разрешимых алгебр Ли ступени не выше m замкнут относительно подалгебр, факторалгебр и прямых произведений;
- если $\mathfrak{h} \lhd \mathfrak{g}$, и $\mathfrak{h}$ разрешимо класса не выше m, а $\mathfrak{g}/\mathfrak{h}$ разрешимо класса не выше t, то $\mathfrak{g}$ разрешимо класса не выше $m + t + 1$.

Представлением ρ алгебры Ли $\mathfrak{g}$ в пространстве V называется гомоморфизм алгебр Ли $\rho : \mathfrak{g} \to L(V)^{(-)}$, где $L(V)$ – алгебра линейных операторов в V. Это означает, что каждому элементу $x \in \mathfrak{g}$ сопоставлен линейный оператор $\rho(x)$ на V, причем

$$\rho(\alpha x + \beta y) = \alpha\rho(x) + \beta\rho(y), \quad \rho([x, y]) = \rho(x)\rho(y) - \rho(y)\rho(x),$$

для всех $x, y \in \mathfrak{g}$ и любых скаляров α, β.

Если фиксировано представление ρ алгебра Ли $\mathfrak{g}$ в пространстве V, то мы будем писать $\rho(x)v = xv$ для всех $x \in \mathfrak{g}$, $v \in V$.

Предложение 2.17. *Пусть задано представление алгебры Ли $\mathfrak{g}$ в конечномерном пространстве V над полем нулевой характеристики. Пусть задан идеал $\mathfrak{h} \lhd \mathfrak{g}$ и такой вектор $v \in V \setminus 0$, что $hv = \chi(h)v$ для всех $h \in \mathfrak{h}$, где $\chi : \mathfrak{h} \to k$ – линейный функционал. Если $x \in \mathfrak{g}$, то $\chi([x, h]) = 0$ для всех $h \in \mathfrak{h}$.*

Доказательство. Зафиксируем $x \in \mathfrak{g}$ и рассмотрим линейную оболочку V_i векторов v, xv, $\ldots$, $x^{i-1}v$. Найдется такое наименьшее натуральное число n, что $V_{n-1} < V_n = V_{n+1}$. Тогда $V_n = V_{n+t}$ для всех $t \geqslant 0$ и векторы

$$v,\ xv,\ \ldots,\ x^{n-1}v \tag{11}$$

составляют базис V_n.

Покажем, что

$$hx^iv \equiv \chi(h)x^iv \mod V_i \tag{12}$$

для всех i. При $i = 0$ это следует из условия. Пусть для i утверждение верно. Тогда по индукции для некоторых $v', v'' \in V_i$ получаем

$$\begin{aligned} hx^{i+1}v &= hx \cdot x^iv = xhx^iv - [x, h]x^iv \\ &= x\left(\chi(h)x^iv + v'\right) - \chi([x, h])x^iv + v'' \\ &\equiv \chi(h)x^{i+1}v \mod V_{i+1} \end{aligned}$$

поскольку $[x, h] \in \mathfrak{h}$ и $xv' \in V_{i+1}$. Итак, (12) доказано.

Из (12) вытекает, что в базисе (11) подпространства V_n каждый элемент из $\mathfrak{h}$ представляется верхнетреугольной матрицей. В частности, в V_n след $\mathrm{tr}_{V_n} h = n\chi(h)$ для всех $h \in \mathfrak{h}$. Из условия $V_n = V_{n+1}$ вытекает, что V_n инвариантно относительно оператора x. Отсюда при $x \in \mathfrak{g}$, $h \in \mathfrak{h}$ получаем $n\chi([x, h]) = \mathrm{tr}_{V_n}[x, h] = 0$, и поэтому $\chi([x, h]) = 0$. □

Предложение 2.18. *Пусть V, $\mathfrak{h}$, $\mathfrak{g}$, $\chi : \mathfrak{h} \to k$ из предложения 2.17 и W – множество всех таких $w \in V$, что $hw = \chi(h)w$ для всех $h \in \mathfrak{h}$. Тогда W инвариантно относительно $\mathfrak{g}$.*

Доказательство. Для любого $h \in \mathfrak{h}$ по предложению 2.17 имеем

$$hxw = xhw - [x, h]w = \chi(h)xw - \chi([x, h])w = \chi(h)xw.$$

□

Теорема 2.19 (Ли)**.** *Пусть $\mathfrak{g}$ – разрешимая конечномерная алгебра Ли над алгебраически замкнутым полем k нулевой характеристики. Предположим, что задано представление ρ алгебры $\mathfrak{g}$ в конечномерном пространстве V. Тогда в V существует базис, в котором матрицы всех операторов $\rho(x)$ верхнетреугольны.*

Доказательство. Нам потребуется

Лемма 2.20. *Существует ненулевой вектор $v \in V$, собственный для всех операторов $\rho(x)$, $x \in \mathfrak{g}$.*

Доказательство. Если $\dim \mathfrak{g} = 1$, то утверждение очевидно. Пусть для $\dim \mathfrak{g} \leqslant d$ лемма доказана и $\dim \mathfrak{g} = d + 1$. Тогда $\dim \mathfrak{g}' < \dim \mathfrak{g}$ в силу разрешимости. Пусть $\mathfrak{h}$ – подпространство коразмерности 1 в $\mathfrak{g}$, содержащее $\mathfrak{g}'$.

Упражнение. Доказать, что $\mathfrak{h} \lhd \mathfrak{g}$.

По индукции существует такой вектор $v \in V \setminus 0$, что $hv = \chi(h)v$ для всех $h \in \mathfrak{h}$, где $\chi : \mathfrak{h} \to k$ – линейный функционал. Обозначим через W множество всех таких векторов $w \in V$, что $hw = \chi(h)w$ для всех $h \in \mathfrak{h}$. По предложению 2.18 подпространство W инвариантно и ненулевое. Выберем элемент $x \in \mathfrak{g} \setminus \mathfrak{h}$. Для оператора $\rho(x)$ в W существует собственный вектор, который будет автоматически собственным и для $\mathfrak{h}$. Этот вектор и является искомым. □

Завершим доказательство теоремы. Пусть $v \in V \setminus 0$ – вектор из леммы 2.20. Тогда ρ задает представление на факторпространстве V/kv. Поэтому доказательство завершается индукцией по $\dim V$. □

По индукции положим $\mathfrak{g}_{(1)} = \mathfrak{g}'$ и $\mathfrak{g}_{(t+1)} = [\mathfrak{g}_t, \mathfrak{g}]$.

Упражнение 2.21. Доказать, что

1) если $\mathfrak{h}$ подалгебра в алгебре Ли $\mathfrak{g}$, то $h_{(t)} \subseteq \mathfrak{h} \cap \mathfrak{g}_{(t)}$;
2) если $f : \mathfrak{g} \to \mathfrak{h}$ – гомоморфизм алгебр Ли, то $f(\mathfrak{g}_{(t)}) \subseteq \mathfrak{h}_{(t)}$;
3) $\mathfrak{g}_{t+1}$ является линейной оболочкой элементов $(\operatorname{ad} x_1) \cdots (\operatorname{ad} x_t)y$ для всех $x_1, \ldots, x_n, y \in \mathfrak{g}$.

Алгебра Ли $\mathfrak{g}$ называется *нильпотентной*, если $\mathfrak{g}_{(t)} = 0$ для некоторого t. Примером нильпотентной алгебры Ли является алгебра Ли верхнетреугольных матриц, у которых на главной диагонали стоят нули.

Теорема 2.22. *Если поле k имеет нулевую характеристику и $\mathfrak{g}$ – разрешимая конечномерная алгебра Ли, то $\mathfrak{g}'$ – нильпотентная алгебра Ли.*

Доказательство. Пусть $\overline{k}$ – алгебраическое замыкание k. Переходя к $\overline{k}\otimes_k\mathfrak{g}$ можно считать, что $k=\overline{k}$ – алгебраически замкнуто. По теореме 2.19 в $\mathfrak{g}$ существует базис, в котором матрица каждого оператора $\operatorname{ad}x$, $x\in\mathfrak{g}$ записывается верхнетреугольной матрицей. Отсюда в каждой матрице $\operatorname{ad}[x,y]=[\operatorname{ad}x,\operatorname{ad}y]$ на главной диагонали стоят нули. Поэтому если $n=\dim\mathfrak{g}'$, то

$$(\operatorname{ad}[x_1,y_1])\cdots(\operatorname{ad}[x_n,y_n])[x,y]=0$$

для всех $x_1,\ldots,x_n,y_1,\ldots,y_n,x,y\in\mathfrak{g}$. Но это означает, что в силу упражнения 2.21, случай 3), что алгебра Ли $\mathfrak{g}'$ нильпотентна. □

Теорема 2.23 (Энгель)**.** *Пусть $\mathfrak{g}$ – конечномерная алгебра Ли, ρ – ее представление в конечномерном пространстве V, причем для любого $x\in\mathfrak{g}$ найдется такое натуральное число $m=m(x)$, что $\rho(x)^m=0$. Тогда в V существует базис, в котором все матрицы $\rho(x)$ записываются верхнетреугольными матрицами с нулевыми диагональными элементами. В частности, $\rho(\mathfrak{g})$ – нильпотентная алгебра Ли операторов на V.*

Доказательство. Как и в доказательстве теоремы 2.19 достаточно показать существование такого ненулевого элемента $v\in V$, что $\rho(x)v=0$ для всех $x\in\mathfrak{g}$.

Можно предполагать, что $\mathfrak{g}$ является подалгеброй Ли в алгебре линейных операторов в V. Пусть $x,y\in\mathfrak{g}$. Тогда $\operatorname{ad}(x)y=L_xy-R_xy$, где $L_xy=xy$, $R_xy=yx$. Заметим, что $L_xR_x=R_xL_x$. По условию существует такое натуральное число m, что $L_x^m=R_x^m=0$, откуда

$$\operatorname{ad}^{2m}(x)y=(L_x-R_x)^{2m}y=\sum_{i=0}^{2m}\binom{2m}{i}(-1)^iL_x^{2m-i}R_x^iy=0.$$

Таким образом, можно считать, что $\mathfrak{g}$ – подалгебра Ли в алгебре Ли линейных операторов на V, причем каждый оператор $\operatorname{ad}x$ нильпотентен на $\mathfrak{g}$.

Покажем теперь индукцией по $\dim\mathfrak{g}$ существование вектора v с условием $xv=0$ для всех $x\in L$. Если $\dim\mathfrak{g}=1$, то $\mathfrak{g}=kx$, и в V имеется собственный вектор v для x. Тогда $xv=\lambda v$, причем $0=x^mv=\lambda^mv$, откуда $\lambda=0$.

Пусть $\dim\mathfrak{g}=d$ и для алгебр меньшей размерности искомый вектор v существует. Предположим, что $\mathfrak{h}$ подалгебра меньшей размерности в $\mathfrak{g}$. Если $x\in\mathfrak{h}$, то $\operatorname{ad}x$ индуцирует нильпотентный эндоморфизм в факторпространстве $\mathfrak{g}/\mathfrak{h}$. Так как $\dim\mathfrak{h}<d$, то по индукции существует такой вектор $v\in\mathfrak{g}\setminus\mathfrak{h}$, что $(\operatorname{ad}x)v\in\mathfrak{h}$ для всех $x\in\mathfrak{h}$. Но тогда $\mathfrak{h}\lhd\mathfrak{h}+kv$, причем $\dim(\mathfrak{h}+kv)=d+1$. Продолжая эти рассуждения получаем в $\mathfrak{g}$ последовательность подалгебр

$$\mathfrak{g}=\mathfrak{g}_0\supset\mathfrak{g}_1\supset\cdots\supset\mathfrak{g}_n\supset\mathfrak{g}_{n+1}=0,$$

в которой $\mathfrak{g}_{m+1}\lhd\mathfrak{g}_m$ и каждый фактор $\mathfrak{g}_m/\mathfrak{g}_{m+1}$ – абелева алгебра Ли размерности 1. В частности, $\mathfrak{g}=kx+\mathfrak{g}_1$. Для $\mathfrak{g}_1$ существует

такой ненулевой вектор v, что $hv = 0$ для всех $h \in \mathfrak{g}_1$. Пусть W – множество всех таких векторов $w \in V$, что $hw = 0$ для всех $h \in \mathfrak{g}_1$. По предложению 2.18 W инвариантно относительно x. Тогда в W имеется ненулевой собственный вектор v с нулевым собственным значением для x. Он и является искомым. □

Следствие 2.24. *Конечномерная алгебра Ли* $\mathfrak{g}$ *нильпотентна в том и только в том случае, если каждый оператор* $\operatorname{ad} x$, $x \in \mathfrak{g}$, *нильпотентен на* $\mathfrak{g}$.

Доказательство. В силу упражнения 2.21, 3) из нильпотентности $\mathfrak{g}$ следует нильпотентность оператора $\operatorname{ad} x$ для любого $x \in \mathfrak{g}$.

Обратно, если каждый оператор $\operatorname{ad} x$ нильпотентен, то по теореме 2.23 для представлениея ad в L существует бакзис, в котором все операторы ad имеют верхнетреугольный вид с нулями по главной диагонали. Если размерности L равна n, то $(\operatorname{ad} x_1) \cdots (\operatorname{ad} x_n) = 0$ и поэтому L ниплпотентна. □

Упражнение. Пусть $\mathfrak{g}$ – конечномерная алгебра Ли и $\mathfrak{h} \lhd \mathfrak{g}$. предположим, что $\mathfrak{g}/\mathfrak{h}$ – нильпотентная алгебра Ли и для любого $x \in \mathfrak{g}$ ограничение $\operatorname{ad} x$ на $\mathfrak{h}$ нильпотентно в $\mathfrak{h}$. Доказать, что $\mathfrak{g}$ – нильпотентная алгебра Ли.

Глава 3

Решетки

1. Решетки

Частично упорядоченное множество L называется *решеткой*, если в L для любых двух элементов существует *точная верхняя грань* $x \vee y \in L$ и *точная нижняя грань* $x \wedge y \in L$. Легко проверяется, что справедливо

Предложение 3.1. *В любой решетке L операции $x \vee y$, $x \wedge y$ коммутативны, ассоциативны и идемпотентны, т. е. $x \vee x = x \wedge x = x$ и выполнены тождества*

$$x \vee (x \wedge y) = x, \quad x \wedge (x \vee y) = x. \tag{13}$$

Более того, справедлива

Теорема 3.2. *Пусть задана алгебра с двумя коммуттивными, ассоциотивными и идемпотнтными операциями $x \vee y$, $x \wedge y$, выпорлнены тождества* (13)*. Тогда L является решеткой, в которой $x \vee y$ — точная верхняя грань, а $x \wedge y$ — точная нижняя грань.*

Доказательство. Положим $x \leqslant y \iff x \wedge y = x$. Из ассоциативности, коммутативности и идемпотентности $x \wedge y$ следует, что это отношение является порядком, причем $x \wedge y$ – точная нижняя грань.

Покажем, что $x \leqslant y \iff x \vee y = y$. Действительно, если $x \wedge y = x$, то $x \vee y = (x \wedge y) \vee y = y$ по (13). Аналогично доказывается обратное утверждение. Из этого утверждения как и выше вытекает, что $x \vee y$ является точной верхней гранью. □

1.1. Дистрбутивные решетки и теорема Стоуна. Решетка L *дистрибутивна*, если в ней выполнено тождество

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

Предложение 3.3. *Решетка дистрибутивна тогда и только тогда, когда в ней выполнено* двойственное *тождество*

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

Доказательство. Имеем

$$x \vee (y \wedge z) = [x \vee (x \wedge z)] \vee (y \wedge z) =$$

$$x \vee [(x \wedge z) \vee (y \wedge z)] = x \vee [z \wedge (x \vee y)] =$$
$$[(x \vee y) \wedge x] \vee [(x \vee y) \wedge z] = (x \vee y) \wedge (x \vee z).$$

□

Теорема 3.4. *Подпрямо неразложимая дистриубтивная решетка двуэлемента.*

Доказательство. Пусть a – элемент дистриубтивной решетки L. Рассмотрим в L отображение $\psi : L \to L$, заданное по правилу $\psi(x) = a \wedge x$. Из дистриубивности следует, что ψ является эндоморфизмом. Аналогично, отображение $\zeta(x) = a \vee x$ является эндоморфизмом.

Лемма 3.5. $\ker\psi \cap \ker\zeta$ *является тривиальной конгруэнцией в* L.

Доказательство. Пусть $(x, y) \in \ker\psi \cap \ker\zeta$. Тогда

$$x \vee a = y \vee a, \quad x \wedge a = y \wedge a.$$

Отсюда

$$x = x \vee (x \wedge a) = (x \vee y) \wedge (x \vee a) =$$
$$(x \vee y) \wedge (y \vee a) = y \vee (x \wedge a) = y \vee (y \wedge a) = y.$$

□

Предположим теперь, что решетка L подпрямо неразложима. По лемме 3.5 одна из конгруэнций $\ker\psi$, $\ker\zeta$ является тривиальной. Если $\ker\psi$ одноэлемента. Заметим, что для любого $b \in L$ имеем $\psi(b \vee a) = a \wedge (b \vee a) = a$. Поэтому $b \vee a = a$, откуда $b \leqslant a$ для любого $b \in L$. Следовательно, a – наибольший элемент из L. Аналогично, если $\ker\zeta$ тривиально, то a – наименьший элемент из L. Следовательно, если решетка L подпрямо неразложима, то каждый ее элемент a является либо наибольшим, либо наименьшим. Поэтому $|L| = 2$. □

Теорема 3.6. *Пусть* L *— конечная дистрибутивная решетка, и* $a \neq b \in L$. *Тогда существует такой гомоморфизм решеток* $\alpha : L \to \begin{pmatrix}1\\0\end{pmatrix}$, *что* $\alpha(a) \neq \alpha(b)$.

Доказательство. Нам потребуется

Лемма 3.7. *Пусть* $a \in L$. *Отображения* $\beta(x) = x \vee a$, $\gamma(x) = x \wedge a$ *являются эндоморфизмами* L.

Доказательство. Имеем

$$\alpha(x \vee y) = (x \vee y) \vee a = (x \vee a) \vee (y \vee a) = \alpha(x) \vee \alpha(y).$$

Кроме того,

$$\alpha(x \wedge y) = (x \wedge y) \vee a = (x \vee a) \wedge (y \vee a) = \alpha(x) \wedge \alpha(y).$$

Аналогично проверяется свойство для β. □

Завершим доказательство теоремы. Заменяя a, b на $a \vee b$, $a \wedge b$ можно считать, что $a > b$. Веберем максимальный элемент $d < a$ и рассмотрим эндоморфизм (см. лемму) $\alpha(x) = (x \vee d) \wedge a$. Образ α состоит из двух элементов $d < a$. При этом $\alpha(b) = (b \vee d) \wedge a = d \wedge a = d$, и $\alpha(a) = a$. □

Теорема 3.8 (Стоун)**.** *Каждая дистрибутивная решетка вложима в решетку подмножеств некоторого множества.*

Доказательство. По теоремам **??** и 3.4 каждая дистрибутивная решетка L вложима в декартову степень $\mathbf{2}^I$, где $\mathbf{2}$ – двуэлемента решетка $\{0 < 1\}$. Можно считать, что $L \subseteq \mathbf{2}^I$. Таким образом каждой элемент $x \in L$ является отображением $x : I \to \{0 < 1\}$. Сопоставим x подмножество $\{i \in I \mid x(i) = 1\}$. Таким образом, x является характеристической функцией своего подмножества. □

Наибольший элемент решетки называется *единицей*, а наименьший — *нулем*. Решетка с нулем и единицей называется *ограниченной* Элемент a' дистрибутивной ограниченной решетки L называется *дополнением* к элементу $a \in L$, если

$$a \vee a' = 1, \quad a \wedge a' = 0.$$

Из леммы 3.5 следует, что дополнение определено однозначно.

Теорема 3.9 (Стоун)**.** *Каждая конечная дистрибутивная решетка вложима в решетку подмножеств некоторого множества.*

Доказательство. Пусть X — множество всех гомоморфизмов $L \to \binom{1}{0}$. Если $a \in L$, то сопоставим a множество всех таких $\alpha \in X$, что $\alpha(x) = 1$. Легко видеть, что это сопоставление является гомоморфизмом решеток.

По теореме 3.6 это сопоставление является вложением. □

1.2. Булевы алгебры. *Булевой алгеброй* называется ограниченная дистрибутивная решетка, в которой каждый элемент обладает дополнением. Основным примером булевой алгебры является булеан $\mathfrak{B}(X)$ всех подмножеств некоторого множества X.

Теорема 3.10 (Стоун)**.** *Каждая булева алгебра вложима в некоторый булеан $\mathfrak{B}(I)$. Конечная булева алгебра изоморфна булеву некоторого конечного множества.*

Доказательство. По теореме 3.8 булева алгебра L как дистрибутивная решетка вложима в булеан $\mathfrak{B}(I)$. При этом дополнению x' соответствует дополнение в I. □

Булевым кольцом называется ассоциативное кольцо с тождеством $x^2 = x$.

Предложение 3.11. *Каждое булево кольцо коммутативно м является алгеброй над полем из двух элементов.*

Доказательство. Имеем

$$0 = (x + y)^2 - (x + y) = xy + yx.$$

В частности, $2x^2 = 2x = 0$ и $xy = yx$. □

Предложение 3.12. *Каждая булева алгебра является булевым кольцом с единицей относительно операций*

$$x + y = (x \wedge y') \vee (x' \wedge y), \quad xy = x \wedge y.$$

Обратно, каждое булево кольцо с единицей является булевой алгеброй относительно операций $x \vee y = x+y+xy, \quad x \wedge y = xy, \quad x' = 1 + x$.

Теорема 3.13 (Стоун)**.** *Конечная булева алгебра изоморфна булеву некоторого конечного множества.*

Доказательство. Достаточно показать, что каждое конечное булево кольцо A является декартовой степенью поля $\mathbb{F}_2$. Из тождества $x^2 = x$ следует, что в A нет нильпотентов. Поэтому A полупросто и A коммутативная алгебра над полем $\mathbb{F}_2$ из двух элементов, т. е. $A \simeq \oplus F_i$, где F_i – конечные поля характеристики 2. При этом $x^2 = x$ в F_i, откуда $F_i = \mathbb{F}_2$. □

Дадим непосредственное доказательство теоремы 3.13 Назовем *атомом* в булевом алгебре L наименьший ненулевой элемент.

Предложение 3.14. *В конечной булевой алгебре каждый ненулевой элемент a является объединением всех атомов, меньших a.*

Доказательство. Пусть X — множество всех атомов, меньших a. Положим $b = \vee_{x \in X} x$. Тогда $b \leqslant a$. Пусть $b \neq a$. Тогда

$$a = a \wedge 1 = a \wedge (b \vee b') = (a \wedge b) \vee (a \wedge b') = b \vee (a \wedge b').$$

Из условия $b < a$ следует, что $a \wedge b' \neq 0$. Поэтому найдется атом $x_0 \leqslant a \wedge b' \leqslant a$. Тогда $x_0 \in X$ и поэтому $x_0 \leqslant b$, что неверно. Итак, $b = a$. □

Пусть A — множество всех атомов в L. Рассмотрим $B(A)$ — булеву алгебру всех подмножеств в A и отображение $\Phi : L \to B(A)$, сопоставляющее элементу $a \in L$ множество $\Phi(a)$ всех атомов, меньших a.

Предложение 3.15. Φ *является изоморфизмом булевых алгебр.*

Доказательство. Проверим, что

$$\Phi(a \vee b) = \Phi(a) \vee \Phi(b), \quad \Phi(a \wedge b) = \Phi(a) \wedge \Phi(b)$$

для всех $a, b \in L$. Действительно, пусть x — атом и $x \leqslant a \vee b$. Если $x \not\leqslant a$, то $x \wedge a = 0$, откуда

$$x = x \wedge (a \vee b) = (x \wedge a) \vee (x \wedge b) = 0 \vee (x \wedge b) = x \wedge b,$$

т.е. $x \leqslant b$. Поэтому $\Phi(a \vee b) \subseteq \Phi(a) \vee \Phi(b)$.

Обратно, если $x \leqslant a$, то $x \leqslant a \vee b$ и $\Phi(a) \vee \Phi(b) \subseteq \Phi(a \vee b)$. Итак, $\Phi(a \vee b) = \Phi(a) \vee \Phi(b)$.

Аналогично, $\Phi(a \wedge b) = \Phi(a) \wedge \Phi(b)$.

Остается показать, что Φ биективно. Пусть $\Phi(a) = \Phi(b)$. Тогда $a = b$ по предложению 3.14. Кроме того, по тому же утверждению Φ инъективно.