Лекции об алгебраических числах

рочев и. п.

10 ноября 2026 г.

Оглавление

Оглавление i

Как бы предисловие 1

1 Конечные и алгебраические расширения полей 2

2 Теорема о примитивном элементе 7

3 Введение в теорию Галуа 9

4 Конечные поля 14

5 След и норма 16

6 Дискриминант 19

7 Модули и порядки 21

8 Целые алгебраические числа 24

9 Сведения из геометрии чисел 27

A Программа осеннего семестра 28

Список литературы 29

Как бы предисловие

Настоящий текст представляет собой слегка переработанный и дополненный конспект лекций Нестеренко Ю. В. по алгебраическим числам [1]. Доказательства по большей части отсутствуют.

Глава 1

Конечные и алгебраические расширения полей

Определение 1.1. Поле K называется *расширением* поля F, если $F \subseteq K$. Принято писать: расширение K/F (это *не* фактор). Если K — конечномерное векторное пространство над F, то расширение K/F называется *конечным*. Размерность $\dim_F K$ этого пространства называется *степенью* расширения и обозначается через $[K : F]$.

Пример 1.2. $\mathbb{C}$ — конечное расширение $\mathbb{R}$ степени $[\mathbb{C} : \mathbb{R}] = 2$.

Замечание 1.3. $[K : F] = 1 \iff K = F$.

Теорема 1.4. *Рассмотрим «башню расширений» $F \subseteq K \subseteq L$. Расширение L/F конечно тогда и только тогда, когда конечны оба расширения K/F и L/K, причём в этом случае выполнено $[L : F] = [K : F] \cdot [L : K]$. Более того, если $\omega_1, \dots, \omega_n$ — базис K над F, $\Omega_1, \dots, \Omega_m$ — базис L над K, то всевозможные попарные произведения $\omega_i \Omega_j$ образуют базис L над F.*

Доказательство. См. [1, лемма 2 и следствие 1]. □

Определение 1.5. Пусть K — расширение F. Элемент $\alpha \in K$ называется *алгебраическим над F*, если существует ненулевой многочлен $P(z) \in F[z]$, такой что $P(\alpha) = 0$. Унитарный такой многочлен наименьшей возможной степени называется *минимальным многочленом α над F*, а его степень — *степенью α над F*. Обозначения: $\mu_\alpha(z) = \mu_{\alpha,F}(z)$, $\deg \alpha = \deg_F \alpha$. В частности, *алгебраическое число* — это комплексное число, алгебраическое над $\mathbb{Q}$ (то есть $F = \mathbb{Q}$, $K = \mathbb{C}$; слова «над $\mathbb{Q}$» обычно опускают). Обозначение: $\mathbb{A}$ — множество всех алгебраических чисел.

Пример 1.6. Числа $\alpha = 0$ и $\beta = \mathrm{i}\sqrt{2}/3$ алгебраические степеней $\deg \alpha = 1$ и $\deg \beta = 2$ соответственно. Минимальные многочлены: $\mu_\alpha(z) = z$, $\mu_\beta(z) = z^2 + 2/9$.

Лемма 1.7. *Пусть α алгебраичен над F. Тогда его минимальный многочлен (над F) определён однозначно и неприводим (над F). Кроме того, для любого многочлена $P(z) \in F[z]$, такого что $P(\alpha) = 0$, выполнено $\mu_\alpha(z) \mid P(z)$.*

Следствие 1.8. *Пусть $P(z) \in F[z]$ — унитарный неприводимый (над F) многочлен, $P(\alpha) = 0$. Тогда $P(z) = \mu_\alpha(z)$.*

Следствие 1.9. *Пусть α алгебраичен над F. Тогда его минимальный многочлен является минимальным для всех своих корней.*

Лемма 1.10. *Пусть K — конечное расширение F, $\alpha \in K$. Тогда α алгебраичен над F, причём* $\deg \alpha \leqslant [K : F]$.

Доказательство. Если $[K : F] = n$, то $1, \alpha, \alpha^2, \dots, \alpha^n$ линейно зависимы над F. □

Определение 1.11. Пусть K — расширение F, $\alpha_1, \dots, \alpha_n \in K$. Через $F(\alpha_1, \dots, \alpha_n)$ обозначается наименьшее по включению подполе K, которое содержит F (как подполе) и все α_i. Если $K = F(\alpha_1, \dots, \alpha_n)$, то говорят, что поле K *порождено элементами* $\alpha_1, \dots, \alpha_n$ над полем F. Такие расширения называются *конечно порождёнными*. Расширение вида $F(\alpha)$ (то есть порождённое одним элементом) называется *простым*.

Очевидно, что

$$F(\alpha_1, \dots, \alpha_n) = \left\{ \frac{P(\alpha_1, \dots, \alpha_n)}{Q(\alpha_1, \dots, \alpha_n)} \,:\, P(\boldsymbol{z}), Q(\boldsymbol{z}) \in F[\boldsymbol{z}], Q(\boldsymbol{\alpha}) \neq 0 \right\}.$$

Кроме того, несложно видеть, что

$$F(\alpha_1, \dots, \alpha_n) = F(\alpha_1)(\alpha_2) \dots (\alpha_n),$$

поэтому для начала разберёмся с простыми расширениями.

Если α трансцендентен (то бишь не алгебраичен) над F, то $F(\alpha)$ изоморфно полю рациональных функций (от одного неизвестного) над F. Случай алгебраического α более интересен.

Теорема 1.12. *Пусть α алгебраичен над F, $\deg_F \alpha = n$. Тогда $F(\alpha)$ — конечное расширение F степени n, причём $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ — базис $F(\alpha)$ над F. Более того, $F(\alpha) \cong F[z]/\mu_\alpha(z)F[z]$ (с естественным изоморфизмом $P(\alpha) \leftrightarrow P(z) + \mu_\alpha(z)F[z]$).*

Доказательство. См. [1, лемма 1]. □

Следствие 1.13 (уточнение леммы 1.10)**.** *Если K — конечное расширение F, $\alpha \in K$, то* $\deg \alpha$ *делит* $[K : F]$.

Доказательство. Рассмотрим башню расширений $F \subseteq F(\alpha) \subseteq K$. □

Следствие 1.14. *Расширение K/F конечно тогда и только тогда, когда $K = F(\alpha_1, \dots, \alpha_n)$ для некоторых $\alpha_1, \dots, \alpha_n$, алгебраических над F.*

Доказательство. См. [1, теорема 1]. □

Следствие 1.15. *Пусть K — расширение F. Тогда множество всех элементов поля K, алгебраических над F, замкнуто относительно основных арифметических операций, то есть является полем.* (*Оно называется* алгебраическим замыканием поля F в поле K.)

Доказательство. Если $\alpha, \beta \in K$ алгебраичны над F, то $\alpha \pm \beta$, $\alpha\beta$ и α/β (при $\beta \neq 0$) лежат в конечном расширении $F(\alpha, \beta)$ поля F. □

Следствие 1.16. *Множество $\mathbb{A}$ всех алгебраических чисел является полем.*

Определение 1.17. Расширение K/F называется *алгебраическим*, если все элементы K являются алгебраическими над F.

Пример 1.18. Всякое конечное расширение K/F алгебраично.

Пример 1.19. Расширение $\mathbb{A}/\mathbb{Q}$ алгебраично, но не конечно, поскольку многочлен $z^n - 2$ неприводим над $\mathbb{Q}$ при любом $n \in \mathbb{N}$ (докажите!).

Лемма 1.20. *Если расширения K/F и L/K алгебраические, то расширение L/F также алгебраическое.*

Доказательство. См. [1, следствие 3]. □

Определение 1.21. Пусть K, L — подполя U. *Композитом* K и L называется наименьшее по включению подполе U, содержащее K и L. Обозначение: KL.

Если F — (произвольное) подполе $K \cap L$, то KL состоит из всевозможных элементов вида

$$\frac{P(\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l)}{Q(\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l)},$$

где $\alpha_1, \dots, \alpha_k \in K$, $\beta_1, \dots, \beta_l \in L$, $P(\boldsymbol{x}, \boldsymbol{y}), Q(\boldsymbol{x}, \boldsymbol{y}) \in F[\boldsymbol{x}, \boldsymbol{y}]$, причём $Q(\boldsymbol{\alpha}, \boldsymbol{\beta}) \neq 0$. Более того, если $K = F(\alpha_1, \dots, \alpha_k)$, $L = F(\beta_1, \dots, \beta_l)$, то $KL = F(\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l)$.

Лемма 1.22. *Пусть K, L — подполя U, F — подполе $K \cap L$. Тогда:*

1) *если расширения K/F и L/F конечны, то расширение KL/F конечно;*

2) *если расширения K/F и L/F алгебраичны, то расширение KL/F алгебраично.*

Доказательство. См. [1, следствия 2 и 4]. □

Поговорим немного подробнее о корнях многочленов.

Лемма 1.23. *Для любого поля F и любого непостоянного многочлена $P(z) \in F[z]$ существует расширение $K \supseteq F$, над которым $P(z)$ раскладывается на линейные множители, то есть имеет вид*

$$P(z) = a(z - \alpha_1) \cdots (z - \alpha_n), \quad \alpha_i \in K.$$

Доказательство. См. [1, лемма 3 и следствие 5]. □

Определение 1.24. В условиях леммы 1.23 поле $F(\alpha_1, \dots, \alpha_n)$ называется *полем разложения* многочлена $P(z)$ *над* F. Эквивалентно: это *минимальное* по включению расширение поля F, над которым $P(z)$ раскладывается на линейные множители.

Замечание 1.25. Можно доказать, что поле разложения единственно с точностью до изоморфизма (переводящего элементы F в себя).

Пример 1.26. Полем разложения $P(z) = z^3 - 2$ над $\mathbb{Q}$ является $\mathbb{Q}\left(\sqrt[3]{2}, e^{2\pi i/3}\right)$.

Лемма 1.27 (без док-ва)**.** *Для любого поля F существует расширение K, над которым всякий непостоянный многочлен $P(z) \in F[z]$ раскладывается на линейные множители.*

Замечание 1.28. Если поле F не более чем счётно, то можно перенумеровать все многочлены $P_n(z)$ и рассмотреть последовательность расширений

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots,$$

где K_n — поле разложения $P_n(z)$ над K_{n-1}. Тогда сгодится $K = \bigcup_n K_n$. Это рассуждение можно обобщить на произвольное поле F, если воспользоваться трансфинитной индукцией (есть и другие доказательства).

Теорема 1.29. *В условиях леммы 1.27 пусть A — алгебраическое замыкание поля F в поле K (см. следствие 1.15). Тогда A алгебраически замкнуто.*

Доказательство. Рассмотрим непостоянный многочлен $P(z) \in A[z]$. Найдётся расширение поля K, в котором многочлен $P(z)$ имеет корень β. Имеем башню алгебраических расширений $F \subseteq A \subseteq A(\beta)$, откуда следует алгебраичность β над F. Рассмотрим его минимальный многочлен $\mu_\beta(z)$ над F. По условию теоремы, все его корни лежат в K, следовательно, $\beta \in K$, откуда $\beta \in A$. □

Следствие 1.30. *Поле $\mathbb{A}$ алгебраически замкнуто.*

Определение 1.31. В условиях теоремы 1.29 поле A называется *алгебраическим замыканием* поля F. Эквивалентно: это минимальное по включению алгебраически замкнутое расширение поля F (или максимальное алгебраическое расширение). Обозначения: $F^{\mathrm{alg}} = \overline{F}$.

Замечание 1.32. Можно доказать, что алгебраическое замыкание единственно с точностью до изоморфизма.

Далее будем считать, что фиксировано некоторое алгебраическое замыкание F^{alg}, и по умолчанию все поля, коэффициенты и корни многочленов будут лежать в этом поле.

Определение 1.33. Если α алгебраичен над F, то корни его минимального многочлена над F называются *сопряжёнными* к α над F.

Согласно следствию 1.9, все сопряжённые к α имеют один и тот же минимальный многочлен, поэтому сопряжённость является отношением эквивалентности.

Лемма 1.34. *Пусть* $\operatorname{char} F = 0$. *Тогда всякий неприводимый над F многочлен не имеет кратных корней.*

Доказательство. Если α — кратный корень неприводимого многочлена $P(z)$, то $P'(\alpha) = 0$, что противоречит минимальности многочлена $P(z)$. □

Пример 1.35. Пусть $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ — поле из p элементов, $F = \mathbb{F}_p(x)$ — поле рациональных функций. Многочлен $P(z) = z^p - x$ неприводим над F, однако $P(z) = (z - \alpha)^p$, где $\alpha = x^{1/p}$ — корень многочлена $P(z)$.

Определение 1.36. Поле F называется *совершенным*, если всякий неприводимый над F многочлен не имеет кратных корней.

Если поле F совершенно, то всякий $\alpha \in F^{\mathrm{alg}}$ имеет ровно $\deg_F \alpha$ сопряжённых над F.

Всякое поле характеристики 0 совершенно. Позже мы убедимся, что все конечные поля совершенны. В частности, любое простое поле (то есть $\mathbb{Q}$ или $\mathbb{F}_p$) совершенно.

Лемма 1.37. *Если поле F совершенно, то любое его алгебраическое расширение также совершенно.*

Доказательство. Пусть K — алгебраическое расширение F и многочлен $P(z) \in K[z]$ неприводим над K. Фиксируем какой-нибудь его корень α. Тогда α алгебраичен над F. Если $Q(z) = \mu_{\alpha,F}(z)$ — его минимальный многочлен над F, то $Q(z)$ не имеет кратных корней. Но $P(z) \mid Q(z)$, поскольку $P(z)$ — минимальный многочлен α над K (с точностью до постоянного множителя), поэтому и $P(z)$ не имеет кратных корней. □

Определение 1.38. Многочлен называется *сепарабельным*, если он не имеет кратных корней (то есть взаимно прост со своей производной).

Определение 1.39. Элемент $\alpha \in F^{\mathrm{alg}}$ называется *сепарабельным над F*, если его минимальный многочлен над F сепарабелен.

Определение 1.40. Алгебраическое расширение K/F называется *сепарабельным*, если всякий $\alpha \in K$ сепарабелен над F.

Таким образом, поле F совершенно тогда и только тогда, когда расширение F^{alg}/F сепарабельно.

Пример 1.41. Расширение $\mathbb{F}_p(x^{1/p})/\mathbb{F}_p(x)$ (или $\mathbb{F}_p(x)/\mathbb{F}_p(x^p)$) несепарабельно.

Из свойств минимального многочлена следует, что все корни любого сепарабельного многочлена $P(z) \in F[z]$ сепарабельны над F. Отсюда следует, что если α сепарабелен над F, то α сепарабелен над любым расширением поля F. Следовательно, если расширение K/F сепарабельно, то сепарабельно и любое расширение вида K'/F', где $F \subseteq F' \subseteq K' \subseteq K$.

Средствами главы 3 можно доказать, что конечное расширение $F(\alpha_1, \dots, \alpha_n)$ поля F сепарабельно тогда и только тогда, когда все порождающие α_i сепарабельны над F.

В дальнейшем нас будут в основном интересовать конечные расширения поля $\mathbb{Q}$. Всякое такое поле называют *полем алгебраических чисел* (или *алгебраическим числовым полем*, иногда даже просто *числовым полем*). (Таким образом, поле $\mathbb{A}$ не является полем алгебраических чисел.)

Глава 2

Теорема о примитивном элементе

Теорема 2.1. *Пусть* $\operatorname{char} F = 0$, K *— конечное расширение* F. *Тогда найдётся* $\theta \in K$, *такой что* $K = F(\theta)$.

Доказательство. См. [1, теорема 2] с очевидными изменениями. □

Пример 2.2. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$.

Определение 2.3. Если $K = F(\theta)$, то θ называется *примитивным элементом* расширения K/F.

Замечание 2.4. Если $K = F(\alpha_1, \dots, \alpha_n)$, то из доказательства видно, что найдётся примитивный элемент вида $\theta = c_1\alpha_1 + \dots + c_n\alpha_n$, $c_i \in F$. (Более общо, коэффициенты c_i можно выбрать из любого бесконечного подмножества F, причём один произвольный коэффициент можно положить равным произвольному элементу F^*.)

Пример 2.5. Расширение $\mathbb{F}_p(x^{1/p}, y^{1/p})/\mathbb{F}_p(x, y)$ конечно (степени p^2), однако не является простым, поскольку для любого

$$\theta = R(x^{1/p}, y^{1/p}) \in \mathbb{F}_p(x^{1/p}, y^{1/p})$$

выполнено

$$\theta^p = R(x, y) \in \mathbb{F}_p(x, y),$$

так что $\deg \theta \leqslant p$.

Условие $\operatorname{char} F = 0$ в доказательстве теоремы используется два раза.

Во-первых, чтобы обеспечить различность сопряжённых к β (где $K = F(\alpha, \beta)$). Для этого достаточно, чтобы расширение K/F было сепарабельно.

Во-вторых, из этого условия следует бесконечность поля F (что обеспечивает существование $c \in F$, где $\theta = \alpha + c\beta$). Однако, для конечного поля F теорему легко доказать другим способом.

Действительно, пусть K — конечное расширение конечного поля F. Тогда $K \cong F^n$ (как векторные пространства), где $n = [K : F]$, поэтому $|K| = |F|^n$, так что поле K тоже конечно. Как учат в школе, всякая конечная подгруппа мультипликативной группы поля является циклической, то есть $K^* = \langle\theta\rangle$. Очевидно, что $K = F(\theta)$.

Таким образом, справедливо следующее обобщение теоремы 2.1.

Теорема 2.6. *Всякое сепарабельное конечное расширение является простым.*

Более того, различность сопряжённых к α в доказательстве на самом деле не используется, поэтому теорему можно обобщить и на некоторые несепарабельные расширения.

Упражнение 2.7. Пусть $K = F(\alpha_1, \dots, \alpha_n)$ — конечное расширение F, причём елементы $\alpha_2, \dots, \alpha_n$ сепарабельны над F. Докажите, что расширение K/F простое.

Глава 3

Введение в теорию Галуа

Правила игры: всюду в этой главе фиксировано некоторое алгебраически замкнутое поле A (можно считать, что $A = \mathbb{C}$). По умолчанию предполагается, что все рассматриваемые поля, коэффициенты и корни многочленов содержатся в A.

Напомним, что отображение $\sigma : K \to L$ (K, L — поля) называется *гомоморфизмом полей*, если выполнены свойства:

1) $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$ и $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$;

2) $\sigma(1) = 1$.

(Условие $\sigma(1) = 1$ является следствием $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$, если σ не тождественно нулевое.)

Любой гомоморфизм полей является *вложением*, то есть инъективен (имеет нулевое ядро). Действительно:

$$\alpha \neq 0 \implies \alpha\alpha^{-1} = 1 \implies \sigma(\alpha)\sigma(\alpha^{-1}) = 1 \implies \sigma(\alpha) \neq 0.$$

Вложения $K \to A$ далее будем называть просто вложениями поля K.

Определение 3.1. Пусть K, L — расширения F. Вложение $\sigma : K \to L$ называется вложением *над* F, если $\sigma(a) = a$ при всех $a \in F$.

Пример 3.2. Комплексное сопряжение $z \to \overline{z}$ является вложением $\mathbb{C} \to \mathbb{C}$ над $\mathbb{R}$.

Пример 3.3. Всякое вложение является вложением над F_0, где F_0 — простое подполе A (F_0 изоморфно $\mathbb{Q}$ или $\mathbb{F}_p$, если $\operatorname{char} A = 0$ или $\operatorname{char} A = p$ соответственно).

Лемма 3.4. *Пусть σ — вложение поля K над F, $\alpha \in K$, причём α алгебраичен над F. Тогда $\sigma(\alpha)$ является сопряжённым к α над F.*

Доказательство. Очевидно ([1, лемма 4]). □

Для простоты далее мы ограничимся только сепарабельными расширениями. Это позволит нам среди прочего использовать теорему о примитивном элементе.

Любой гомоморфизм полей $\sigma : K \to L$ естественным образом продолжается до гомоморфизма колец многочленов $K[z] \to L[z]$, а именно:

$$\sigma\Big(\sum \alpha_i z^i\Big) = \sum \sigma(\alpha_i) z^i$$

(для продолжения используют ту же букву σ). Далее это продолжение подразумевается.

Теорема 3.5. *Пусть K/F — сепарабельное конечное расширение, $[K : F] = n$. Тогда каждое вложение σ поля F имеет ровно n продолжений до вложения поля K. Если $K = F(\theta)$, $\mu_\theta(z)$ — минимальный многочлен θ над F, то для любого корня ω многочлена $\sigma(\mu_\theta)(z)$ существует единственное продолжение τ, такое что $\tau(\theta) = \omega$, а именно:*

$$\tau\left(\sum_{i=0}^{n-1} a_i\theta^i\right) = \sum_{i=0}^{n-1} \sigma(a_i)\omega^i, \quad a_i \in F.$$

Все продолжения получаются таким образом.

Доказательство. См. [1, лемма 5].

Нужно только проверить, что все корни многочлена $\sigma(\mu_\theta)(z)$ различны. Для этого достаточно применить σ к равенству

$$1 = \text{н.о.д.}\big(\mu_\theta(z), \mu'_\theta(z)\big) = \mu_\theta(z)P(z) + \mu'_\theta(z)Q(z). \qquad \square$$

Следствие 3.6. *Пусть K/F — сепарабельное конечное расширение. Тогда существует ровно $[K : F]$ вложений поля K над F. Более того, если $\alpha \in K$, α' — произвольное сопряжённое к α над F, то существует ровно $[K : F(\alpha)]$ вложений σ поля K над F, таких что $\sigma(\alpha) = \alpha'$.*

Доказательство. Рассмотрим башню расширений $F \subseteq F(\alpha) \subseteq K$ и два раза применим теорему. $\square$

Следствие 3.7. *Пусть K/F — сепарабельное конечное расширение, $\alpha \in K$. Если для всякого вложения σ поля K над F выполнено $\sigma(\alpha) = \alpha$, то $\alpha \in F$.*

Доказательство. Условие означает, что α имеет единственный сопряжённый над F. $\square$

Замечание 3.8. Если K/F — несепарабельное конечное расширение, то те же рассуждения показывают, что любое вложение поля F можно продолжить до вложения поля K, однако количество продолжений меньше чем $[K : F]$ (с помощью более тонких рассуждений можно показать, что ещё и делит $[K : F]$).

Упражнение 3.9. Докажите, что конечное расширение $F(\alpha_1, \dots, \alpha_n)$ поля F сепарабельно тогда и только тогда, когда все порождающие α_i сепарабельны над F.

В качестве бонуса докажем уточнение теоремы о примитивном элементе.

Теорема 3.10. *Пусть $K = F(\alpha_1, \dots, \alpha_n)$ — сепарабельное конечное расширение поля F. Далее, при $j = 1, \dots, n$ пусть $\alpha_j^{(1)} = \alpha_j, \alpha_j^{(2)}, \dots, \alpha_j^{(m_j)}$ — все сопряжённые к α_j над F (так что $m_j = \deg \alpha_j$). Предположим, что числа $c_j \in F$ таковы, что*

$$\theta = c_1\alpha_1 + \dots + c_n\alpha_n \neq c_1\alpha_1^{(i_1)} + \dots + c_n\alpha_n^{(i_n)}$$

при всех $(i_1, \dots, i_n) \neq (1, \dots, 1)$. Тогда $K = F(\theta)$.

Доказательство. Предположим противное. Тогда найдётся нетождественное вложение σ поля K над $F(\theta)$. Имеем

$$\theta = \sigma(\theta) = \sum_{j=1}^{n} c_j \sigma(\alpha_j) = \sum_{j=1}^{n} c_j \alpha_j^{(i_j)}$$

для некоторых i_j. Из условий теоремы следует, что все $i_j = 1$, то есть $\sigma(\alpha_j) = \alpha_j$. Но тогда σ тождественно на $F(\alpha_1, \dots, \alpha_n) = K$. Противоречие. □

Теорема 3.11. *Пусть K/F — алгебраическое расширение. Следующие условия эквивалентны:*

1) *Всякое вложение σ поля K над F является эндоморфизмом поля K, то есть $\sigma(K) \subseteq K$.*
2) *Всякое вложение σ поля K над F является автоморфизмом поля K, то есть $\sigma(K) = K$.*
3) *Для всякого $\alpha \in K$ все его сопряжённые над F также принадлежат K.*
4) *Всякий неприводимый над F многочлен $P(z) \in F[z]$, имеющий корень в K, раскладывается над K на линейные множители.*

Доказательство для сепарабельного конечного расширения. См. [1, теорема 3]. □

Определение 3.12. В условиях теоремы 3.11 расширение K/F называется *нормальным*. Также говорят, что поле K нормально над F. Сепарабельное нормальное расширение называется *расширением Галуа*.

Теорема 3.13. *Пусть K/F — конечное расширение. Следующие условия эквивалентны:*

1) *Расширение K/F нормально.*
2) *Если $K = F(\alpha_1, \dots, \alpha_n)$, то все сопряжённые над F к каждому α_i принадлежат K.*
3) *Поле K является полем разложения некоторого многочлена $P(z) \in F[z]$ над F.*

Доказательство. См. [1, теорема 3]. Эквивалентность 2 $\iff$ 3 очевидна. □

Следствие 3.14. *Для любого конечного расширения K/F найдётся нормальное конечное расширение L/F, такое что $K \subseteq L$. При этом если K/F сепарабельно, то можно найти L, такое что L/F сепарабельно (т. е. расширение Галуа).*

Доказательство. Если $K = F(\alpha_1, \dots, \alpha_n)$, то в качестве L можно взять расширение, порождённое всеми сопряжёнными к α_i. □

Пример 3.15. Если $[K : F] = 2$, то расширение K/F нормально.

Пример 3.16. Расширения $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ и $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)$ нормальны, однако расширение $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$ не нормально.

Упражнение 3.17. Докажите, что $\mathbb{Q}(\cos(2\pi/7))$ — нормальное расширение $\mathbb{Q}$ степени 3.

Определение 3.18. Если K/F — расширение Галуа, то группа автоморфизмов K над F (относительно композиции) называется *группой Галуа* расширения. Обозначение: $\mathrm{Gal}(K/F)$.

Лемма 3.19. *Если K/F — конечное расширение Галуа, то* $|\mathrm{Gal}(K/F)| = [K : F]$.

Пример 3.20. Пусть $P(z) = (z - \alpha_1) \cdots (z - \alpha_n) \in F[z]$ — сепарабельный многочлен, $K = F(\alpha_1, \dots, \alpha_n)$ — его поле разложения над F (тогда K/F — расширение Галуа). Каждый автоморфизм $\sigma \in \mathrm{Gal}(K/F)$ индуцирует перестановку корней $\alpha_1, \dots, \alpha_n$ многочлена $P(z)$, причём разным автоморфизмам соответствуют разные перестановки. Таким образом, группа Галуа $\mathrm{Gal}(K/F)$ вкладывается в группу подстановок множества $\{\alpha_1, \dots, \alpha_n\}$. В частности, $[K : F] \mid n!$.

Упражнение 3.21. Пусть K — поле разложения многочлена $P(z) \in F[z]$ над F, $\deg P = n$. Докажите, что $[K : F] \mid n!$ (даже если расширение K/F несепарабельно).

Пример 3.22. Пусть многочлен $P(z) = (z - \alpha_1)(z - \alpha_2)(z - \alpha_3) \in F[z]$ неприводим над F и сепарабелен (если $\mathrm{char}\, F \neq 3$, то сепарабельность следует из неприводимости), $\mathrm{char}\, F \neq 2$, $K = F(\alpha_1, \alpha_2, \alpha_3)$, $G = \mathrm{Gal}(K/F)$. Будем отождествлять G с соответствующей подгруппой S_3. Поскольку $|G| = [K : F]$ делится на 3, то $G = A_3$ или $G = S_3$. Как понять?

Положим $\delta = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)$, $\Delta = \delta^2 = -P'(\alpha_1)P'(\alpha_2)P'(\alpha_3)$ (дискриминант многочлена $P(z)$). Для любого $\sigma \in G$ имеем

$$\sigma(\delta) = \mathrm{sgn}(\sigma)\delta \implies \sigma(\Delta) = \Delta,$$

так что $\Delta \in F$. В частности, если $P(z) = z^3 + az + b$, то $\Delta = -4a^3 - 27b^2$.

Если $G = A_3$, то аналогично получаем $\delta \in F$, так что $\Delta = \delta^2 \in (F^*)^2 = \{a^2 : a \in F^*\}$.

Если же $G = S_3$, то найдётся нечётная подстановка $\sigma \in G$. Тогда $\sigma(\delta) = -\delta \neq \delta$, поэтому $\delta \notin F$, так что $\Delta \notin (F^*)^2$.

Таким образом, $G = A_3$ или S_3 (в частности, $[K : F] = 3$ или 6) в зависимости от того, является ли дискриминант Δ многочлена $P(z)$ квадратом в F или нет соответственно.

Определение 3.23. Если K/F — алгебраическое расширение, то поля вида $\sigma K := \sigma(K)$, где σ — вложение K над F, называют *сопряжёнными* с K *над* F.

В частности, расширение K/F нормально тогда и только тогда, когда все поля, сопряжённые с K над F, совпадают с K.

Лемма 3.24. *Пусть $F \subseteq K \subseteq L$ — башня конечных расширений, причём расширение L/F нормально. Тогда расширение L/K также нормально, причём если L/F — сепарабельно, то* $\mathrm{Gal}(L/K) \subseteq \mathrm{Gal}(L/F)$. *Более того, все поля, сопряжённые с K над F, содержатся в L.*

Доказательство. Очевидно ([1, следствие 9]). □

Теорема 3.25. *Пусть L/F — конечное расширение Галуа. Тогда отображения*

$$K \mapsto \mathrm{Gal}(L/K),$$
$$H \mapsto L^H := \{\alpha \in L : \sigma(\alpha) = \alpha \text{ при всех } \sigma \in H\}$$

задают взаимно обратные биекции между промежуточными полями K и подгруппами H группы Галуа $\mathrm{Gal}(L/F)$.

Доказательство. См. [1, теорема 4]. □

Следствие 3.26. *В условиях теоремы 3.25 имеем* $[L : L^H] = |H|$, $[L^H : F] = [\mathrm{Gal}(L/F) : H]$.

Следствие 3.27. *Пусть K/F — сепарабельное конечное расширение. Тогда существует лишь конечное число промежуточных полей.*

Доказательство. См. [1, следствие 10]. □

Замечание 3.28. Если K/F — произвольное конечное расширение, то оно является простым (то есть существует примитивный элемент) тогда и только тогда, когда существует лишь конечное число промежуточных полей (теорема Штайница [Steinitz]).

Лемма 3.29. *В условиях теоремы 3.25 пусть $F \subseteq K \subseteq L$. Тогда*:

1) *для всякого $\sigma \in \mathrm{Gal}(L/F)$ выполнено*

$$\mathrm{Gal}(L/\sigma K) = \sigma \,\mathrm{Gal}(L/K)\sigma^{-1}$$

(*так что сопряжённым полям соответствуют сопряжённые подгруппы*);

2) *расширение K/F нормально тогда и только тогда, когда $\mathrm{Gal}(L/K)$ — нормальная подгруппа $\mathrm{Gal}(L/F)$, причём в этом случае*

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(L/F) \,\big/\, \mathrm{Gal}(L/K).$$

Доказательство.

1) Имеем

$$\begin{aligned}\mathrm{Gal}(L/\sigma K) &= \{\tau \in \mathrm{Gal}(L/F) \,:\, \forall \alpha \in \sigma K \quad \tau(\alpha) = \alpha\} \\ &= \{\tau \,:\, \forall \beta \in K \quad \tau\sigma(\beta) = \sigma(\beta)\} \\ &= \{\tau \,:\, \forall \beta \in K \quad \sigma^{-1}\tau\sigma(\beta) = \beta\} \\ &= \{\tau \,:\, \sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/K)\} \\ &= \sigma \,\mathrm{Gal}(L/K)\sigma^{-1}.\end{aligned}$$

2) Поскольку любое вложение K над F можно продолжить до $\sigma \in \mathrm{Gal}(L/K)$, то расширение K/F нормально тогда и только тогда, когда для всякого $\sigma \in \mathrm{Gal}(L/F)$ верно $\sigma K = K$. Имеем

$$\sigma K = K \iff \mathrm{Gal}(L/\sigma K) = \mathrm{Gal}(L/K) \iff \sigma \,\mathrm{Gal}(L/K)\sigma^{-1} = \mathrm{Gal}(L/K),$$

поэтому нормальность расширения K/F равносильна нормальности соответствующей подгруппы.

Пусть расширение K/F нормально (и следовательно, является расширением Галуа). Рассмотрим гомоморфизм групп

$$\varphi : \ \mathrm{Gal}(L/F) \ni \sigma \mapsto \sigma\big|_K \in \mathrm{Gal}(K/F).$$

Очевидно, что $\ker\varphi = \mathrm{Gal}(L/K)$. Кроме того, из теоремы о продолжении вложений следует, что σ сюръективен. Из теоремы о гомоморфизме следует требуемое. □

Глава 4

Конечные поля

Лемма 4.1. *Пусть F — конечное поле, $\operatorname{char} F = p$, $\mathbb{F}_p$ — его простое подполе. Тогда F является конечным расширением $\mathbb{F}_p$, причём $|F| = p^n$, где $n = [F : \mathbb{F}_p]$.*

Лемма 4.2. *Если F — произвольное поле характеристики p, то отображение $\varphi(x) = x^p$ является эндоморфизмом F (вложением F в себя). В частности, если F конечно, то φ является автоморфизмом F.*

Определение 4.3. В условиях леммы 4.2 отображение φ называется *эндоморфизмом Фробениуса* (автоморфизмом, если φ сюръективно).

Следствие 4.4. *Если F — конечное поле, $\operatorname{char} F = p$, то для любого $n \in \mathbb{N}_0$ отображение $\varphi^n(x) = x^{p^n}$ является автоморфизмом F.*

Фиксируем некоторое поле $\mathbb{F}_p$ из p элементов (например, $\mathbb{Z}/p\mathbb{Z}$) и его алгебраическое замыкание $\mathbb{F}_p^{\text{alg}}$.

Лемма 4.5. *Для любого $q = p^n$ ($n \in \mathbb{N}$) существует единственное подполе $\mathbb{F}_p^{\text{alg}}$ из q элементов, а именно:*

$$\mathbb{F}_q = \{\alpha \in \mathbb{F}_p^{\text{alg}} : \alpha^q = \alpha\}.$$

Лемма 4.6. *$\mathbb{F}_{q_1} \subseteq \mathbb{F}_{q_2}$ тогда и только тогда, когда $q_2 = q_1^n$, $n \in \mathbb{N}$. При этом $[\mathbb{F}_{q_2} : \mathbb{F}_{q_1}] = n$.*

Лемма 4.7. *Любое конечное поле совершенно.*

Доказательство. По лемме 1.37, достаточно доказать, что $\mathbb{F}_p$ совершенно.

Предположим противное. Пусть $P(z) \in \mathbb{F}_p[z]$ неприводим над $\mathbb{F}_p$, но имеет кратный корень. Тогда $P'(z) = 0$, поэтому $P(z) = Q(z^p)$ для некоторого $Q(z) \in \mathbb{F}_p[z]$. Но тогда $P(z) = (Q(z))^p$. Противоречие. □

Упражнение 4.8. Пусть F — произвольное поле характеристики p. Докажите, что F совершенно тогда и только тогда, когда эндоморфизм Фробениуса сюръективен.

Лемма 4.9. *Пусть G — конечная подгруппа мультипликативной группы некоторого поля. Тогда G является циклической.*

Следствие 4.10. *Группа $\mathbb{F}_q^*$ циклическая.*

Теорема 4.11. *Расширение $\mathbb{F}_{q^n}/\mathbb{F}_q$ является расширением Галуа, причём его группа Галуа циклическая и порождена автоморфизмом $\sigma(x) = x^q$.*

Доказательство. Отображения σ^i, $i = 0, 1, \dots, n-1$, являются автоморфизмами $\mathbb{F}_{q^n}$ над $\mathbb{F}_q$, причём различными, поскольку

$$\sigma^i(\alpha) = \sigma^j(\alpha) \iff \sigma^{i-j}(\alpha) = \alpha \iff \alpha \in \mathbb{F}_{q^{i-j}} \quad (i > j).$$

Поскольку $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, то других вложений $\mathbb{F}_{q^n}$ над $\mathbb{F}_q$ нет. □

Следствие 4.12. *Допустим, что многочлен $P(z) \in \mathbb{F}_q[z]$ унитарный и неприводимый над $\mathbb{F}_q$, $\deg P = n$, $P(\alpha) = 0$. Тогда*

$$P(z) = \prod_{i=0}^{n-1} \left(z - \alpha^{q^i}\right).$$

Упражнение 4.13. Пусть $\alpha \in \mathbb{F}_p^{\mathrm{alg}}$. Докажите, что

$$\deg_{\mathbb{F}_q} \alpha = \min\left\{n \in \mathbb{N} : \alpha^{q^n} = \alpha\right\}.$$

Упражнение 4.14. Докажите, что для любого $n \in \mathbb{N}$ справедливо разложение

$$z^{q^n} - z = \prod P(z),$$

где произведение берётся по всем унитарным неприводимым (над $\mathbb{F}_q$) многочленам $P(z) \in \mathbb{F}_q[z]$ с условием $\deg P(z) \mid n$, и выведите отсюда, что количество унитарных неприводимых многочленов степени n равно $\frac{1}{n}\sum_{d|n} \mu(d) q^{n/d}$, где μ — функция Мёбиуса.

Глава 5

След и норма

Пусть K — конечное расширение F. Будем рассматривать K как (конечномерную) алгебру над F.

Каждому $\alpha \in K$ сопоставим линейный оператор $\mathcal{L}_\alpha : x \mapsto \alpha x$. Легко видеть, что получается вложение K (как алгебры) в алгебру линейных операторов (известное как *регулярное представление* K).

Определение 5.1. Характеристический многочлен (унитарный), след и определитель оператора $\mathcal{L}_\alpha$ называются соответственно *характеристическим многочленом, следом* и *нормой* α *относительно расширения* K/F. Обозначения: $\chi_\alpha(z) = \chi_{\alpha,K/F}(z)$ (характеристический многочлен), $\operatorname{Tr}(\alpha) = \operatorname{Tr}_F^K(\alpha) = \operatorname{Tr}_{K/F}(\alpha)$ (след), $\mathrm{N}(\alpha) = \mathrm{N}_F^K(\alpha) = \mathrm{N}_{K/F}(\alpha)$ (норма).

(Если α — алгебраическое число, то $\operatorname{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha)$ и $\mathrm{N}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}(\alpha)$ называются просто следом и нормой числа α.)

Пусть $\omega_1, \dots, \omega_n$ — базис K над F, $A = (a_{i,j}) \in F^{n\times n}$ — матрица оператора $\mathcal{L}_\alpha$ в этом базисе, то есть

$$\alpha\omega_j = \sum_{i=1}^{n} a_{i,j}\omega_i. \tag{5.1}$$

Тогда $\chi_\alpha(z) = \det(zI - A)$, $\operatorname{Tr}(\alpha) = \operatorname{Tr}(A)$, $\mathrm{N}(\alpha) = \det(A)$. При этом

$$\chi_\alpha(z) = z^n - \operatorname{Tr}(\alpha)z^{n-1} + \dots + (-1)^n \mathrm{N}(\alpha).$$

Лемма 5.2 (простейшие свойства)**.** *Пусть* $\alpha, \beta \in K$, $a, b \in F$. *Тогда:*

1) $\chi_\alpha(z) \in F[z]$; *в частности,* $\operatorname{Tr}(\alpha), \mathrm{N}(\alpha) \in F$.

2) $\operatorname{Tr}(a\alpha + b\beta) = a\operatorname{Tr}(\alpha) + b\operatorname{Tr}(\beta)$.

3) $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$.

4) $\mathrm{N}(\alpha) = 0 \iff \alpha = 0$.

Доказательство. Последнее свойство следует из того, что при $\alpha \neq 0$ оператор $\mathcal{L}_\alpha$ обратим. Остальные свойства очевидны. □

Если $\alpha \in F$, то $\chi_\alpha(z) = (z-\alpha)^n$, $\mathrm{Tr}(\alpha) = n\alpha$, $\mathrm{N}(\alpha) = \alpha^n$, где $n = [K : F]$. Эти равенства — частный случай следующего утверждения.

Лемма 5.3. *Пусть $F \subseteq K \subseteq L$ — башня конечных расширений, $\alpha \in K$. Тогда справедливы равенства:*

$$\begin{aligned} \chi_{\alpha,L/F}(z) &= \big(\chi_{\alpha,K/F}(z)\big)^m, \\ \mathrm{Tr}_F^L(\alpha) &= m\,\mathrm{Tr}_F^K(\alpha), \\ \mathrm{N}_F^L(\alpha) &= \big(\mathrm{N}_F^K(\alpha)\big)^m, \end{aligned}$$

где $m = [L : K]$.

Доказательство. Пусть $\omega_1, \dots, \omega_n$ — базис K над F, $\Omega_1, \dots, \Omega_m$ — базис L над K. В качестве базиса L над F возьмём

$$\omega_1\Omega_1, \dots, \omega_n\Omega_1, \omega_1\Omega_2, \dots, \omega_n\Omega_2, \dots, \omega_1\Omega_m, \dots, \omega_n\Omega_m.$$

Легко видеть, что матрица оператора $\mathcal{L}_\alpha$ в этом базисе имеет блочно-диагональный вид

$$\begin{pmatrix} A & O & \cdots & O \\ O & A & \cdots & O \\ \vdots & \vdots & \ddots & \vdots \\ O & O & \cdots & A \end{pmatrix},$$

где A — матрица оператора $\mathcal{L}_\alpha\big|_K$ в базисе $\omega_1, \dots, \omega_n$, откуда следует требуемое. □

Лемма 5.4. *Если K/F — конечное расширение, $\alpha \in K$, то справедливо равенство*

$$\chi_\alpha(z) = \big(\mu_\alpha(z)\big)^m,$$

где $\mu_\alpha(z)$ — минимальный многочлен α над F, $m = [K : F(\alpha)]$.

Доказательство. По лемме 5.3 можно считать, что $K = F(\alpha)$. Из равенств (5.1) следует, что α — собственное значение матрицы A^T, поэтому $\chi_\alpha(\alpha) = 0$ (фактически теорема Гамильтона–Кэли). Поскольку $\deg\chi_\alpha = \deg\alpha$, имеем $\chi_\alpha = \mu_\alpha$. □

Следствие 5.5. *Пусть K/F — сепарабельное конечное расширение. Тогда для любого $\alpha \in K$ справедливы формулы*

$$\begin{aligned} \chi_\alpha(z) &= \prod_\sigma (z - \sigma(\alpha)), \\ \mathrm{Tr}(\alpha) &= \sum_\sigma \sigma(\alpha), \\ \mathrm{N}(\alpha) &= \prod_\sigma \sigma(\alpha), \end{aligned}$$

где σ пробегает все вложения поля K над F.

Доказательство. См. [1, следствие 11]. □

Следствие 5.6. *Пусть $F \subseteq K \subseteq L$ — башня конечных расширений, причём расширение L/F сепарабельно. Тогда для любого $\alpha \in L$ верно*

$$\mathrm{Tr}_F^L(\alpha) = \mathrm{Tr}_F^K\big(\mathrm{Tr}_K^L(\alpha)\big),$$
$$\mathrm{N}_F^L(\alpha) = \mathrm{N}_F^K\big(\mathrm{N}_K^L(\alpha)\big).$$

Доказательство. Фиксируем конечное расширение Галуа L'/F, такое что $L \subseteq L'$.

Пусть $\sigma_1, \dots, \sigma_n$ — все вложения K над F. Продолжим их произвольным образом на L'.

Далее, пусть $\tau_1, \dots, \tau_m$ — все вложения L над K. Тогда для любого $i = 1, \dots, n$ вложения $\sigma_i\tau_1, \dots, \sigma_i\tau_m$ — это все продолжения σ_i на L.

Следовательно,

$$\mathrm{Tr}_F^L(\alpha) = \sum_{i,j} \sigma_i\tau_j(\alpha) = \sum_i \sigma_i\big(\mathrm{Tr}_K^L(\alpha)\big) = \mathrm{Tr}_F^K\big(\mathrm{Tr}_K^L(\alpha)\big).$$

Для нормы аналогично. □

Замечание 5.7. Следствие 5.6 справедливо и для несепарабельных расширений.

Упражнение 5.8. Пусть K/F — конечное расширение, z — переменная. Докажите, что $K(z)/F(z)$ — конечное расширение той же степени (и более того, любой базис K над F является базисом $K(z)$ над $F(z)$), причём для любого $\alpha \in K$ верно

$$\chi_\alpha(z) = \mathrm{N}_{F(z)}^{K(z)}(z - \alpha).$$

Упражнение 5.9. Пусть K/F — несепарабельное конечное расширение. Докажите, что для любого $\alpha \in K$ верно $\mathrm{Tr}(\alpha) = 0$.

Глава 6

Дискриминант

Фиксируем *сепарабельное* конечное расширение K/F, $[K : F] = n$. Пусть $\mathrm{Tr} = \mathrm{Tr}_F^K$ — функция следа.

Определение 6.1. *Дискриминантом* набора $\alpha_1, \dots, \alpha_n \in K$ называется определитель

$$\Delta(\alpha_1, \dots, \alpha_n) = \Delta_{K/F}(\alpha_1, \dots, \alpha_n) \coloneqq \det \|\mathrm{Tr}(\alpha_i \alpha_j)\|_{i,j=1}^n.$$

(Вместо Δ также используются обозначения D, $\mathcal{D}$, disc, Disc.)

Лемма 6.2. *Пусть $\sigma_1, \dots, \sigma_n$ — все вложения K над F. Тогда верно равенство*

$$\Delta(\alpha_1, \dots, \alpha_n) = \left(\det \|\sigma_i(\alpha_j)\|\right)^2.$$

Доказательство. $\|\mathrm{Tr}(\alpha_i \alpha_j)\| = \|\sigma_i(\alpha_j)\|^{\mathsf{T}} \cdot \|\sigma_i(\alpha_j)\|$. □

Следствие 6.3. *Дискриминант не зависит от порядка элементов $\alpha_1, \dots, \alpha_n$.*

Следствие 6.4. *Пусть наборы $\alpha_1, \dots, \alpha_n$ и $\omega_1, \dots, \omega_n$ связаны линейными соотношениями*

$$\alpha_j = \sum_{i=1}^n c_{i,j} \omega_i, \quad c_{i,j} \in F,\ 1 \leqslant i, j \leqslant n.$$

Тогда

$$\Delta(\alpha_1, \dots, \alpha_n) = \Delta(\omega_1, \dots, \omega_n) \cdot |C|^2,$$

где $C = \|c_{i,j}\|_{i,j=1}^n$.

Доказательство. $\|\sigma_i(\alpha_j)\| = \|\sigma_i(\omega_j)\| \cdot C$. □

Теорема 6.5. *Элементы $\alpha_1, \dots, \alpha_n \in K$ образуют базис K над F тогда и только тогда, когда $\Delta(\alpha_1, \dots, \alpha_n) \neq 0$.*

Доказательство. Пусть $K = F(\theta)$. Обозначим через $\theta_1, \dots, \theta_n$ все сопряжённые к θ над F. Тогда дискриминант степенного базиса $1, \theta, \dots, \theta^{n-1}$ равен

$$\prod_{1 \leqslant i < j \leqslant n} (\theta_j - \theta_i)^2 \neq 0.$$

Применяя следствие 6.4, получаем требуемое. □

Альтернативное доказательство для характеристики 0. См. [1, теорема 5]. □

Замечание 6.6. Теорема 6.5 фактически означает, что (симметричная) билинейная форма $\mathcal{B}(x, y) = \operatorname{Tr}(xy)$ является невырожденной.

Следствие 6.7. *Пусть $\omega_1, \dots, \omega_n$ — базис K над F. Тогда для любых $a_1, \dots, a_n \in F$ найдётся единственный $\alpha \in K$, такой что $\operatorname{Tr}(\alpha\omega_i) = a_i$ $(1 \leqslant i \leqslant n)$.*

Доказательство. См. [1, следствие 13]. □

Следствие 6.8. *Пусть $\omega_1, \dots, \omega_n$ — базис K над F. Тогда найдётся базис $\omega'_1, \dots, \omega'_n$, такой что*

$$\operatorname{Tr}(\omega_i\omega'_j) = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

Доказательство. См. [1, следствие 14]. □

Определение 6.9. В условиях следствия 6.8 базис $\omega'_1, \dots, \omega'_n$ называется *взаимным* (*двойственным*, *дуальным*) для $\omega_1, \dots, \omega_n$.

Важность взаимного базиса заключается в том, что он даёт явное выражение для коэффициентов разложения любого елемента $\alpha \in K$ по базису $\omega_1, \dots, \omega_n$:

$$\alpha = \sum_{i=1}^{n} a_i\omega_i,\ a_i \in F,\ \Longrightarrow\ a_i = \operatorname{Tr}(\alpha\omega'_i).$$

Глава 7

Модули и порядки

Начиная с этой главы, мы ограничимся конечными расширениями $\mathbb{Q}$ (напомним, что они называются полями алгебраических чисел, или алгебраическими числовыми полями). (Существенную роль в дальнейшем играет тот факт, что кольцо $\mathbb{Z}$ является кольцом главных идеалов, а поле $\mathbb{Q}$ является его полем частных.)

Нам понадобятся сведения из алгебры про конечно порождённые абелевы группы (которые мы будем записывать аддитивно, тем самым наделяя их структурой $\mathbb{Z}$-модуля). Для простоты ограничимся группами без кручения (то есть не имеющими ненулевых элементов конечного порядка).

Теорема 7.1 (без доказательства)**.** *Всякая конечно порождённая абелева группа G без кручения является свободной, то есть изоморфна $\mathbb{Z}^n$ для некоторого $n \in \mathbb{N}_0$; при этом число n (называемое* рангом *группы G) определено однозначно. Любая подгруппа группы G также конечно порождена, причём ранг подгруппы не превосходит ранга группы.*

Таким образом, если G — конечно порождённая абелева группа без кручения, то найдутся линейно независимые над $\mathbb{Z}$ элементы $\omega_1, \dots, \omega_n \in G$, такие что

$$G = \mathbb{Z}\omega_1 + \dots + \mathbb{Z}\omega_n.$$

Всякий такой (упорядоченный) набор $\omega_1, \dots, \omega_n$ называется *базисом* группы G. (Для нулевой группы $n = 0$, то есть базисом является пустой набор.)

Лемма 7.2. *Если $\omega_1, \dots, \omega_n$ — базис группы G, то элементы $\eta_1, \dots, \eta_n \in G$ образуют базис G тогда и только тогда, когда*

$$\eta_j = \sum_{i=1}^{n} c_{i,j}\omega_i,$$

где $C = \|c_{i,j}\| \in \mathrm{GL}_n(\mathbb{Z})$ ($\iff \det C = \pm 1$).

Лемма 7.3. *Если H — подгруппа G, то найдутся базисы $\omega_1, \dots, \omega_n$ и $\eta_1, \dots, \eta_m$ групп G и H соответственно, такие что $\eta_i = c_i\omega_i$ при $1 \leqslant i \leqslant m$, где $c_i \in \mathbb{N}$, причём $c_i \mid c_{i+1}$ при $1 \leqslant i < m$.*

Замечание 7.4. В условиях леммы 7.3 числа c_i определены однозначно.

Следствие 7.5. *Пусть $\omega_1, \dots, \omega_n$ — базис группы G, H — подгруппа полного ранга с базисом $\eta_1, \dots, \eta_n$, причём*

$$\eta_j = \sum_{i=1}^{n} c_{i,j}\omega_i, \quad c_{i,j} \in \mathbb{Z}.$$

Тогда $[G : H] = |\det C|$ (в частности, факторгруппа G/H конечна).

Доказательство. Из леммы 7.2 следует, что $|\det C|$ не зависит от выбора базисов. Возьмём базисы, как в лемме 7.3. Тогда

$$G/H \cong \mathbb{Z}/c_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/c_n\mathbb{Z},$$

откуда

$$[G : H] = |G/H| = c_1 \cdots c_n = |\det C|. \qquad \square$$

Фиксируем некоторое поле алгебраических чисел K.

Определение 7.6. *Модулем* в поле K будем называть произвольную конечно порождённую подгруппу аддитивной группы поля K. (То есть фактически под «модулем» мы понимаем «конечно порождённый $\mathbb{Z}$-модуль».) При этом под рангом/базисом модуля понимается его ранг/базис как абелевой группы.

Таким образом, модуль (в K) — это множество вида

$$M = \mathbb{Z}\eta_1 + \dots + \mathbb{Z}\eta_m,$$

где $\eta_i \in K$. Числа η_i называются *образующими* модуля M. Если при этом образующие линейно независимы над $\mathbb{Z}$ (или, эквивалентно, над $\mathbb{Q}$), то такая система образующих является базисом модуля M (а количество образующих — рангом модуля M).

Лемма 7.7. *Любой модуль имеет базис из не более чем $[K : \mathbb{Q}]$ элементов. Всякая аддитивная подгруппа модуля также является модулем.*

Определение 7.8. Модуль называется *полным*, если его ранг равен $[K : \mathbb{Q}]$ (то есть базис модуля является базисом K над $\mathbb{Q}$).

Замечание 7.9. Полный модуль также называют *$\mathbb{Q}$-решёткой*, *$\mathbb{Z}$-решёткой* или просто *решёткой*.

Определение 7.10. *Дискриминантом* полного модуля M называют дискриминант его (произвольного) базиса. Обозначения: $D_M = D(M)$.

Замечание 7.11. Корректность определения, то есть независимость от выбора базиса, следует из леммы 7.2.

Лемма 7.12. *Если $M_1 \subseteq M_2$ — полные модули, то индекс $[M_2 : M_1]$ конечен, причём верно равенство $D_{M_1} = D_{M_2} \cdot [M_2 : M_1]^2$. В частности, если $M_1 \subseteq M_2$ и $D_{M_1} = D_{M_2}$, то $M_1 = M_2$.*

Доказательство. Следствия 6.4 и 7.5. $\square$

Определение 7.13. Если M — модуль, то множество

$$\mathcal{O}_M = \{\alpha \in K : \alpha M \subseteq M\}$$

называется *кольцом множителей* модуля M (очевидно, что $\mathcal{O}_M$ является кольцом с 1).

Лемма 7.14. *Кольцо множителей полного модуля является полным модулем.*

Доказательство. См. [1, лемма 12]. □

Упражнение 7.15. Пусть $M \neq \{0\}$ — модуль. Докажите, что $\mathcal{O}_M$ — тоже модуль, причём ранг $\mathcal{O}_M$ не превосходит ранга M.

Упражнение 7.16. Найдите кольцо множителей модуля $\mathbb{Z} + \mathbb{Z}\sqrt[3]{2}$.

Определение 7.17. *Порядком* в поле K называется подкольцо K с 1, являющееся полным модулем.

Лемма 7.18. *Множество $\mathcal{O} \subseteq K$ является порядком тогда и только тогда, когда $\mathcal{O} = \mathcal{O}_M$ для некоторого полного модуля M. Более того, если $\mathcal{O}$ — порядок, то $\mathcal{O} = \mathcal{O}_{\mathcal{O}}$.*

Глава 8

Целые алгебраические числа

Определение 8.1. Число $\alpha \in \mathbb{C}$ называется *целым алгебраическим* (или целым над кольцом $\mathbb{Z}$), если найдётся унитарный многочлен $P(z) \in \mathbb{Z}[z]$, такой что $P(\alpha) = 0$. Обозначение: $\mathbb{Z}_{\mathbb{A}}$ — множество всех целых алгебраических чисел.

Утверждение 8.2. *Если $\alpha \in \mathbb{Z}_{\mathbb{A}}$, то все сопряжённые к α также являются целыми алгебраическими.*

Утверждение 8.3. *Для любого $\alpha \in \mathbb{A}$ найдётся $a \in \mathbb{N}$, такое что $a\alpha \in \mathbb{Z}_{\mathbb{A}}$.*

Доказательство. Если $P(\alpha) = 0$, где $P(z) = a_n z^n + \cdots + a_0 \in \mathbb{Z}[z]$, то $a_n\alpha \in \mathbb{Z}_{\mathbb{A}}$. □

Утверждение 8.4. *Число $\alpha \in \mathbb{C}$ является целым алгебраическим тогда и только тогда, когда найдётся ненулевой конечно порождённый $\mathbb{Z}$-модуль $M \subseteq \mathbb{C}$, такой что $\alpha M \subseteq M$.*

Доказательство. Если $\alpha \in \mathbb{Z}_{\mathbb{A}}$, то годится $M = \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}$, где n — степень унитарного целого многочлена, корнем которого является α.

Пусть $\alpha M \subseteq M$, где $M = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$ (причём линейная независимость ω_i не предполагается). Тогда

$$\alpha\omega_i = \sum_{j=1}^{n} a_{i,j}\omega_j, \quad a_{i,j} \in \mathbb{Z},\ 1 \leqslant i, j \leqslant n,$$

откуда $\det(\alpha I - A) = 0$. □

Следствие 8.5. *$\mathbb{Z}_{\mathbb{A}}$ — кольцо.*

Доказательство. Если $\alpha, \beta \in \mathbb{Z}_{\mathbb{A}}$, то $\mathbb{Z}$-модуль $M = \mathbb{Z}[\alpha, \beta] = \mathbb{Z}[\alpha][\beta]$ конечно порождён (в качестве образующих годятся $\alpha^i\beta^j$ при $0 \leqslant i \leqslant n-1$, $0 \leqslant j \leqslant m-1$, где n и m — степени многочленов для α и β соответственно). При этом $(\alpha \pm \beta)M \subseteq M$ и $\alpha\beta M \subseteq M$. □

Следствие 8.6 (целозамкнутость кольца $\mathbb{Z}_{\mathbb{A}}$)**.** *Если $\alpha \in \mathbb{A}$ является корнем унитарного многочлена $P(z) \in \mathbb{Z}_{\mathbb{A}}[z]$, то $\alpha \in \mathbb{Z}_{\mathbb{A}}$.*

Доказательство. Если $P(z) = z^n + \alpha_{n-1}z^{n-1} + \cdots + \alpha_0$, то $\mathbb{Z}$-модуль $M_1 = \mathbb{Z}[\alpha_0, \ldots, \alpha_{n-1}]$ конечно порождён. Тогда конечно порождён и $\mathbb{Z}$-модуль

$$M = \mathbb{Z}[\alpha_0, \ldots, \alpha_{n-1}, \alpha] = M_1 + M_1\alpha + \cdots + M_1\alpha^{n-1}.$$

При этом $\alpha M \subseteq M$. □

До сих пор специфика кольца $\mathbb{Z}$ фактически не использовалась.

Определение 8.7. Многочлен $P(z) \in \mathbb{Z}[z]$ называется *примитивным*, если его коэффициенты взаимно просты в совокупности.

Утверждение 8.8 (лемма Гаусса)**.** *Произведение примитивных многочленов — примитивный многочлен.*

Доказательство. См. [1, лемма 13]. □

Следствие 8.9. *Пусть многочлены $P(z), Q(z) \in \mathbb{Q}[z]$ унитарны, причём $P(z)Q(z) \in \mathbb{Z}[z]$. Тогда $P(z), Q(z) \in \mathbb{Z}[z]$.*

Доказательство. См. [1, доказательство леммы 14]. □

Следствие 8.10. *Число $\alpha \in \mathbb{A}$ является целым алгебраическим тогда и только тогда, когда $\mu_\alpha(z) \in \mathbb{Z}[z]$.*

Следствие 8.11 (целозамкнутость кольца $\mathbb{Z}$)**.** $\mathbb{Q} \cap \mathbb{Z}_\mathbb{A} = \mathbb{Z}$. (*Поэтому числа из $\mathbb{Z}$ также называют* целыми рациональными.)

Фиксируем некоторое алгебраическое числовое поле K.

Определение 8.12. Множество $\mathbb{Z}_K := K \cap \mathbb{Z}_\mathbb{A}$ называется *кольцом целых* (чисел или элементов) поля K.

Утверждение 8.13. *Если $\alpha \in \mathbb{Z}_K$, то $\chi_\alpha(z) \in \mathbb{Z}[z]$. В частности,* $\mathrm{Tr}(\alpha), \mathrm{N}(\alpha) \in \mathbb{Z}$.

Утверждение 8.14. *$\alpha \in \mathbb{Z}_K \iff \alpha \in \mathcal{O}_M$ для некоторого ненулевого модуля M в K.*

Следствие 8.15. *Если $\mathcal{O}$ — порядок в K, то $\mathcal{O} \subseteq \mathbb{Z}_K$.*

Утверждение 8.16. *Если $\mathcal{O}$ — порядок в K, $\alpha \in \mathcal{O}$, то $\mathrm{N}(\alpha) = \alpha\beta$, где $\beta \in \mathcal{O}$ (то есть $\alpha \mid \mathrm{N}(\alpha)$ в кольце $\mathcal{O}$).*

Доказательство. Если $\chi_\alpha(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0$, то

$$(-1)^n \mathrm{N}(\alpha) = a_0 = -(\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha).$$ □

Теорема 8.17. *$\mathbb{Z}_K$ — порядок в K.*

Доказательство. По утверждению 8.3 найдётся базис $\omega_1, \dots, \omega_n$ поля K, такой что $\omega_i \in \mathbb{Z}_K$. Пусть $\omega'_1, \dots, \omega'_n$ — взаимный базис.

Если $\alpha \in \mathbb{Z}_K$, то $\alpha = a_1\omega'_1 + \dots + a_n\omega'_n$, где $a_i = \mathrm{Tr}(\alpha\omega_i) \in \mathbb{Z}$ (см. следствие 8.13), то есть $\mathbb{Z}_K \subseteq \mathbb{Z}\omega'_1 + \dots + \mathbb{Z}\omega'_n$. Следовательно, $\mathbb{Z}_K$ — модуль. Очевидно, что полный. □

Следствие 8.18. *$\mathbb{Z}_K$ — наибольший по включению порядок в K.* (*Поэтому $\mathbb{Z}_K$ также называют* максимальным порядком *поля K и обозначают через $\mathcal{O}_K$.*)

Определение 8.19. Всякий базис $\mathbb{Z}_K$ (как модуля) называют *целым* (или *фундаментальным*) базисом поля K.

Определение 8.20. Дискриминант $\mathbb{Z}_K$ (как полного модуля) называют *дискриминантом* поля K (или *абсолютным дискриминантом*, если хотят подчеркнуть, что K рассматривается как расширение $\mathbb{Q}$). Обозначения: $D_K = D(K)$.

Утверждение 8.21. *$D_K \in \mathbb{Z}$. Более того, для любого полного модуля $M \subseteq \mathbb{Z}_K$ выполнено $D_M \in \mathbb{Z}$, причём справедливо равенство $D_M = D_K \cdot [\mathbb{Z}_K : M]^2$.*

Следствие 8.22. *Если $M \subseteq \mathbb{Z}_K$ — полный модуль и $D_M = D_K$, то $M = \mathbb{Z}_K$.*

Следствие 8.23. *Если $M \subseteq \mathbb{Z}_K$ — полный модуль, p — простое число, причём $p^2 \nmid D_M$, то $p \nmid [\mathbb{Z}_K : M]$ и $\nu_p(D_K) = \nu_p(D_M)$. В частности, если D_M бесквадратно, то $D_K = D_M$.*

Пример 8.24. Рассмотрим поле $K = \mathbb{Q}(\theta)$, где $\theta^3 - \theta - 1 = 0$. Легко проверить, что $[K : \mathbb{Q}] = 3$. Очевидно, $\theta \in \mathbb{Z}_K$, так что

$$M := \mathbb{Z}[\theta] = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 \subseteq \mathbb{Z}_K.$$

Имеем (см. формулу из примера 3.22):

$$D_M = \Delta(1, \theta, \theta^2) = 4 - 27 = -23.$$

Поскольку -23 бесквадратно, то $\mathbb{Z}_K = \mathbb{Z}[\theta]$ и $D_K = -23$.

Пример 8.25. Рассмотрим поле $K = \mathbb{Q}\left(\sqrt[3]{3}\right)$ и модуль $M = \mathbb{Z}\left[\sqrt[3]{3}\right] = \mathbb{Z} + \mathbb{Z}\sqrt[3]{3} + \mathbb{Z}\sqrt[3]{9}$ в нём. Имеем (по определению дискриминанта)

$$D_M = \Delta\left(1, \sqrt[3]{3}, \sqrt[3]{9}\right) = \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 9 \\ 0 & 9 & 0 \end{vmatrix} = -3^5.$$

Положим $d = [\mathbb{Z}_K : M]$. Тогда $d \mid 9$. Если $d > 1$, то в группе $\mathbb{Z}_K/M$ найдётся элемент порядка 3, то есть найдётся $\alpha \in \mathbb{Z}_K \setminus M$, такое что

$$3\alpha = a + b\sqrt[3]{3} + c\sqrt[3]{9}, \quad a, b, c \in \mathbb{Z}. \tag{8.1}$$

Отсюда следует, что $\sqrt[3]{3} \mid a$ в кольце $\mathbb{Z}_K$, то есть $a = \sqrt[3]{3}\beta$ для некоторого $\beta \in \mathbb{Z}_K$. Берём норму:

$$a^3 = \mathrm{N}(a) = 3\,\mathrm{N}(\beta) \in 3\mathbb{Z} \implies a \in 3\mathbb{Z}.$$

Но тогда из (8.1) аналогично получаем:

$$\sqrt[3]{3} \mid b \implies 3 \mid b \implies \sqrt[3]{3} \mid c \implies 3 \mid c.$$

Следовательно,

$$\alpha = \frac{a + b\sqrt[3]{3} + c\sqrt[3]{9}}{3} \in \mathbb{Z} + \mathbb{Z}\sqrt[3]{3} + \mathbb{Z}\sqrt[3]{9},$$

что противоречит выбору α. Значит, $d = 1$, $\mathbb{Z}_K = \mathbb{Z}\left[\sqrt[3]{3}\right]$ и $D_K = -243$.

Упражнение 8.26. Докажите, что для поля $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$ верно $\mathbb{Z}_K = \mathbb{Z}\left[\sqrt[3]{2}\right]$. (*Подсказка.* Если $\theta = \sqrt[3]{2} + 1$, то $\theta^3 \mid 3 = \mathrm{N}(\theta)$.)

Глава 9

Сведения из геометрии чисел

Приложение А

Программа осеннего семестра

1) Конечные и алгебраические расширения полей: степень расширения, теорема о башне расширений, структура простого расширения, связь между конечными и алгебраическими расширениями.
2) Алгебраическая замкнутость поля всех алгебраических чисел.
3) Теорема о примитивном элементе.
4) Вложения полей, продолжение вложений.
5) Нормальные расширения. Группа Галуа.
6) Основная теорема теории Галуа (взаимно однозначное соответствие между промежуточными полями конечного расширения Галуа и подгруппами группы Галуа). Нормальность промежуточного расширения.
7) Конечные поля.
8) Характеристический многочлен, его связь с минимальным многочленом. След и норма.
9) Дискриминант. Взаимный базис.
10) Модули и порядки.
11) Целые алгебраические числа. Кольцо целых, целый базис и дискриминант поля алгебраических чисел.

Список литературы

[1] Ю. В. Нестеренко. *Лекции об алгебраических числах.*