Часть 1. Продолжение гомоморфизмов

Пусть $\sigma : K \to L$ — гомоморфизм полей. Часто для обозначения действия гомоморфизма используют экспоненциальную запись: $a^\sigma := \sigma(a)$, где $a \in K$. В частности, если $f(x) = \sum a_k x^k$, то $f^\sigma(x) := \sum a_k^\sigma x^k$.

Пусть K'/K и L'/L — расширения полей, а $\sigma : K \to L$ и $\tau : K' \to L'$ — гомоморфизмы. Будем говорить, что τ **продолжает** σ, если $\tau\rceil_K = \sigma$.

Лемма 1.1. *Пусть $\sigma : K \to L$ — гомоморфизм полей, а K'/K и L'/L — расширения. Если $K' = K(\alpha)$, α — алгебраичен над K и $p(x) = \mathrm{Irr}_\alpha^K(x)$, то множество гомоморфизмов $\tau : K' \to L'$, продолжающих гомоморфизм σ, находится в биекции с множеством корней многочлена $p^\sigma(x)$ в поле L'.*

Доказательство: если τ — такой гомоморфизм, то $p^\sigma(\alpha^\tau) = p^\tau(\alpha^\tau) = (p(\alpha))^\tau = 0$, поэтому $\beta = \alpha^\tau \in L'$ — корень многочлена $p^\sigma(x) \in L[x]$. Обратно, предположим, что $\beta \in L'$ — корень $p^\sigma(x)$. Заметим, что всякий элемент в $K' = K(\alpha) = K[\alpha]$ представим в виде $f(\alpha)$, где $f(x) \in K[x]$. Положим $(f(\alpha))^\tau := f^\sigma(\beta)$. Тогда, во-первых, отображение τ определено корректно. Действительно, если $f(\alpha) = g(\alpha)$, то $(f-g)(\alpha) = 0$, следовательно $f(x) - g(x) = h(x)p(x)$, где $h(x) \in K[x]$, значит $f^\sigma(\beta) - g^\sigma(\beta) = h^\sigma(\beta)p^\sigma(\beta) = 0$. Во-вторых, легко видеть, что τ является гомоморфизмом полей. Наконец, ясно, что τ продолжает σ. $\square$

Следствие 1.2. *Число возможных продолжений гомоморфизма $\sigma : K \to L$ на поле $K' = K(\alpha)$ не превосходит $[K' : K] = \deg \mathrm{Irr}_\alpha^K(x)$.*

Пусть K'/K и K''/K — расширения. Будем говорить, что $\sigma : K' \to K''$ — **гомоморфизм полей над** K, если σ продолжает тождественный гомоморфизм $K \to K$.

Лемма 1.3. *Если L/K — алгебраично, а $\sigma : L \to L$ — гомоморфизм над K, то σ — автоморфизм.*

Доказательство: достаточно проверить, что σ сюрьективно. Пусть $\alpha \in L$ и $p(x) = \mathrm{Irr}_\alpha^K(x)$. Пусть $\{\alpha_1, \ldots, \alpha_m\}$ — все корни $p(x)$ в L (можно считать, что $\alpha_1 = \alpha$). Положим $L' = K(\alpha_1, \ldots, \alpha_m)$. Тогда, во-первых L' конечно порождено и алгебраично над K, следовательно $\dim_K L' = [L' : K] < \infty$. Во-вторых, ясно, что $\sigma(\alpha_i) = \alpha_j$, поэтому $\sigma(L') \subset L'$, то есть σ переводит L' в себя. Наконец, так как $\sigma : L' \to L'$ — инъективен и K-линеен, а $\dim_K L' < \infty$, то σ сюръективен на L', значит $\alpha \in \mathrm{Im}\,\sigma$. $\square$

Теорема 1.4. *Если K'/K — алгебраическое расширение, а $\sigma : K \to L$ — гомоморфизм в алгебраически замкнутое поле L, то существует гомоморфизм $\sigma' : K' \to L$, продолжающий σ.*

Доказательство: пусть $K'' \subset K'$ — максимальное подполе, содержащее K, на которое можно продолжить σ[1]. Предположим, что $K'' \neq K'$. Обозначим через σ'' продолжение σ на K'' и пусть $\alpha \in K' \setminus K''$. По лемме 1.1 гомоморфизм σ'' можно продолжить на поле $K''(\alpha) \subset K'$ (так как L — алгебраически замкнуто), что противоречит максимальности поля K''. Значит $K'' = K'$ и теорема доказана. $\square$

Следствие 1.5. *Если $\overline{K}'/K$ и $\overline{K}''/K$ — алгебраические замыкания, то $\overline{K}' \cong \overline{K}''$ (изоморфизм над K). Более того, всякий гомоморфизм $\overline{K}' \to \overline{K}''$ над K является изоморфизмом.*

Доказательство: пользуясь теоремой 1.4 строим гомоморфизмы $\sigma : \overline{K}' \to \overline{K}''$ и $\tau : \overline{K}'' \to \overline{K}'$ над K. Далее, по лемме 1.3 комопозиции $\tau\sigma$ и $\sigma\tau$ являются автоморфизмами, поэтому σ и τ — изоморфизмы. $\square$

[1] Чтобы убедиться в том, что такое K'' существует воспользуемся леммой Цорна. Нам надо проверить, что для любой башни $K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K'$ и любого набора гомоморфизмов $\sigma_i : K_i \to L$ $(\sigma_0 = \sigma)$, продолжающих друг друга, найдется поле $\widetilde{K} \subset K'$ и гомоморфизм $\tilde{\sigma} : \widetilde{K} \to L$, такие что $\forall i$ имеем $K_i \subset \widetilde{K}$ и $\tilde{\sigma}$ продолжает σ_i. Действительно, возьмем $\widetilde{K} = \bigcup_{i=1}^\infty K_i$ и положим $\tilde{\sigma}(x) = \sigma_i(x)$, если $x \in K_i$. Ясно, что $\tilde{\sigma}$ — корректо определен (так как σ_i продолжает σ_j при $i > j$) и является гомоморфизмом. Кроме того, очевидно, что $\tilde{\sigma}$ продолжает любой из σ_i.

Часть 2. Поле разложения

Пусть K — поле и $f(x) \in K[x]$ — произвольный многочлен.

Определение 2.1. Поле L называется полем разложения многочлена f, если, во-первых, $f(x)$ над полем L раскладывается на линейные множители $f(x) = c(x - \alpha_1)\dots(x - \alpha_n)$, и, во-вторых, $L = K(\alpha_1, \dots, \alpha_n)$.

Лемма 2.2. *Всякое алгебраическое замыкание $\overline{K}$ поля K содержит единственное подполе L, являющееся полем разложения многочлена $f(x)$. Всякое вложение $\sigma : L \to \overline{K}$ над K является автоморфизмом поля L. Любые два поля разложения многочлена $f(x)$ изоморфны.*

Доказательство: Рассмотрим алгебраическое замыкание $\overline{K}$ поля K. Тогда $f(x) = c(x-\alpha_1)\dots(x-\alpha_n)$ в $\overline{K}[x]$. Ясно, что c — старший коэффициент в $f(x)$, поэтому $c \in K$. Пусть $L = K(\alpha_1, \dots, \alpha_n) \subset \overline{K}$. Тогда L является полем разложения многочлена $f(x)$. Более того, ясно что никакое другое подполе в $\overline{K}$ не может быть полем разложения этого многочлена. Тем самым, первое утверждение доказано.

Докажем теперь второе утверждение. Пусть $\alpha_1, \dots, \alpha_n$ — корни многочлена $f(x)$ в поле $\overline{K}$. Тогда ясно, что $f^\sigma(x) = f(x)$, так как σ — вложение над K, а $f(x) \in K[x]$; значит $f(\alpha_i^\sigma) = f^\sigma(\alpha_i^\sigma) = (f(\alpha_i))^\sigma = 0$, поэтому σ переводит множество корней многочлена $f(x)$ в себя. Следовательно, σ индуцирует гомоморфизм $L \to L$, который является автоморфизмом, так как $L = K(\alpha_1, \dots, \alpha_n)$.

Пусть, наконец, L' — другое поле разложения многочлена $f(x)$. Ясно, что $L' \subset \overline{K}'$ для некоторого алгебраического замыкания поля K. Выберем изоморфизм $\sigma : \overline{K} \to \overline{K}'$ над K. Повторяя те же рассуждения, что и выше, легко показать, что σ задает изоморфизм $L \to L'$. $\square$

Аналогично определяется поле разложения произвольного семейства многочленов $\{\, f_i(x) \mid f_i(x) \in K[x] \,\}_{i \in I}$. Полем разложения семейства $\{\, f_i(x) \,\}$ называется поле L, такое что, во-первых, каждый из многочленов $f_i(x)$ раскладывается над полем L на линейные множители, и, во-вторых, поле L порождается корнями всех многочленов $f_i(x)$. Следующее утверждение доказывается аналогично лемме 2.2.

Лемма 2.3. *Всякое алгебраическое замыкание $\overline{K}$ поля K содержит единственное подполе L, являющееся полем разложения семейства многочленов $\{\, f_i(x) \,\}_{i \in I}$. Всякое вложение $\sigma : L \to \overline{K}$ над K является автоморфизмом поля L. Любые два поля разложения семейства многочленов $\{\, f_i(x) \,\}_{i \in I}$ изоморфны.*

Часть 3. Нормальные расширения

Определение 3.1. Пусть L/K — алгебраическое расширение, $L \subset \overline{K}$. Расширение L/K называется нормальным, если любой гомоморфизм $\sigma : L \to \overline{K}$ над K является автоморфизмом поля L.

Лемма 3.2. *Расширение L/K нормально $\iff$ любой неприводимый многчлен $f(x) \in K[x]$, имеющий корень в L, раскладывается в L на линейные множители.*

Доказательство: $\Longleftarrow$) Пусть $\sigma : L \to \overline{K}$ — гомоморфизм над K. Выберем произвольный элемент $\alpha \in L$ и пусть $p(x) = \mathrm{Irr}_\alpha^K(x)$. Ясно, что α^σ является корнем многочлена $p(x)$. С другой стороны, $p(x)$ раскладывается в L на линейные множители, следовательно L содержит все корни $p(x)$ в $\overline{K}$. Значит $\alpha^\sigma \in L$. Отсюда следует, что $\sigma(L) \subset L$, значит по лемме 1.3 гомоморфизм σ является автоморфизмом поля L.

$\Longrightarrow$) Пусть $f(x) \in K[x]$ — неприводим и $\alpha \in L$ — его корень. Пусть β — другой корень $p(x)$ в $\overline{K}$. Тогда по лемме 1.1 существует гомоморфизм $\sigma : L \to \overline{K}$, такой что $\alpha^\sigma = \beta$. Из нормальности поля L тут же следует, что $\beta \in L$. Значит все корни многочлена $p(x)$ содержатся в L, следовательно $p(x)$ раскладывается в L на линейные множители. $\square$

Лемма 3.3. *Расширение L/K нормально $\iff$ L является полем разложения некоторого семейства многочленов $\{\, f_i(x) \mid f_i(x) \in K[x] \,\}_{i \in I}$.*

Доказательство: если L/K — нормально, то L является полем разложения для семейства многочленов $\{\, \mathrm{Irr}_\alpha^K(x) \,\}_\alpha$, где α пробегает произвольную систему образующих поля L над K, так как по лемме 3.2 каждый из многочленов $\mathrm{Irr}_\alpha^K(x)$ раскладывается в L на линейные множители. Это доказывает импликацию $\Longrightarrow$. В свою очередь импликация $\Longleftarrow$ следует из леммы 2.3. $\square$

Часть 4. Конечные поля

Пусть p — простое число и K — поле характеристики p.

Лемма 4.1. *Отображение $\Phi : K \to K$, $x \mapsto x^p$ является гомоморфизмом поля K в себя над $\mathbb{F}_p$.*

Доказательство: очевидная проверка показывает, что $\Phi(xy) = \Phi(x)\Phi(y)$, $\Phi(x^{-1}) = \Phi(x)^{-1}$ и $\Phi(1) = 1$. Далее, заметим, что $(-1)^p = -1$ (если p — нечетно, то это очевидно, а если $p = 2$, то $(-1)^p = 1 = -1$). Значит $\Phi(-x) = (-x)^p = (-1)^p x^p = -x^p = -\Phi(x)$. Кроме того, ясно что $\Phi(0) = 0$. Остается проверить, что $\Phi(x+y) = \Phi(x) + \Phi(y)$. Действительно, $\Phi(x+y) = (x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{p-1}xy^{p-1} + y^p$. Заметим, что при $1 \leqslant k \leqslant p-1$ число $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ делится на p, следовательно равно нулю в любом поле характеристики p. Значит $\Phi(x+y) = x^p + y^p = \Phi(x) + \Phi(y)$. $\square$

Лемма 4.2. *Если L — поле из q элементов, то $\forall \alpha \in L$ имеем $\alpha^q - \alpha = 0$.*

Доказательство: мультипликативаня группа поля L имеет порядок $q-1$, поэтому $\forall \alpha \in L^*$ имеем $\alpha^{q-1} = 1$, следовательно $\alpha^q - \alpha = 0$. Остается заметить лишь, что $0^q - 0 = 0$. $\square$

Следствие 4.3. *Если L — поле из q элементов, то L — поле разложения многочлена $f(x) = x^q - x$.*

Пусть теперь $q = p^n$ и пусть L — поле разложения многочлена $x^q - x$ над $\mathbb{F}_p$.

Лемма 4.4. *Поле L совпадает с множеством корней многочлена $f(x) = x^q - x$ и состоит из q элементов.*

Доказательство: заметим, что $x^q = x^{p^n} = \Phi^n(x)$, поэтому по лемме 4.1 множество $L_0 = \{\, \alpha \in L \mid f(\alpha) = 0 \,\}$ замкнуто относительно сложения, умножения и т.д. Иначе говоря, L_0 является подполем в L. Далее, ясно что L_0 содержит $\mathbb{F}_p$ и порождается над ним всеми корнями многочлена $f(x)$, следовательно L_0 является полем разложения $f(x)$ над $\mathbb{F}_p$, то есть $L_0 = L$. Остается проверить, что L_0 состоит из q элементов. Действительно, заметим, что $f'(x) = qx^{q-1} - 1 = -1$, поэтому НОД$(f(x), f'(x)) = 1$, и значит $f(x)$ не имеет кратных корней в силу следующей леммы. $\square$

Лемма 4.5. *Многочлен $f(x) \in K[x]$ имеет кратный корень в $\overline{K} \iff$ НОД$(f(x), f'(x)) \neq 1$.*

Доказательство: если $f(x) = (x-\alpha)g(x)$, то $f'(x) = g(x) + (x-\alpha)g'(x)$, поэтому $(x-\alpha)|f'(x) \iff (x-\alpha)|g(x) \iff (x-\alpha)^2|f(x)$. $\square$

Следствие 4.6. *Для всякого $q = p^n$ существует единственное с точностью до изоморфизма поле $\mathbb{F}_q$ из q элементов, а именно поле разложения многочлена $x^q - x$ над $\mathbb{F}_p$.*

Займемся теперь изучением эндоморфизмов конечных полей.

Лемма 4.7. *Всякий эндоморфизм поля $\mathbb{F}_q$ является автоморфизмом.*

Доказательство: как мы знаем, всякий эндоморфизм поля является вложением, но инъективное отображение конечного множества в себя сюръективно. $\square$

Следствие 4.8. *Гомоморфизм $\Phi : \mathbb{F}_q \to \mathbb{F}_q$ является автоморфизмом.*

Автоморфизм Φ называется автоморфизмом Фробениуса.

Теорема 4.9. *Если $q = p^n$, то группа $\mathrm{Aut}(\mathbb{F}_q)$ является циклической группой порядка n, порожденной автоморфизмом Фробениуса.*

Доказательство: покажем вначале, что Φ имеет порядок n в группе $\mathrm{Aut}(\mathbb{F}_q)$. Действительно, по лемме 4.2 $\Phi^n(\alpha) = \alpha^q = \alpha$ для любого $\alpha \in \mathbb{F}_q$, поэтому $\Phi^n = \mathrm{Id}$. С другой стороны, если $\Phi^k = \mathrm{Id}$, то $\forall \alpha \in \mathbb{F}_q$ имеем $\alpha^{p^k} = \alpha$, следовательно $\alpha \in \mathbb{F}_{p^k}$, значит $k \geqslant n$. Остается проверить, что всякий автоморфизм поля $\mathbb{F}_q$ имеет вид Φ^k. Действительно, пусть α — образующая мультипликативной группы $\mathbb{F}_q^*$. Ясно, что $\mathbb{F}_p(\alpha) = \mathbb{F}_q$, поэтому $\deg \mathrm{Irr}_\alpha^{\mathbb{F}_p}(x) = n$. Применяя следствие 1.2, получаем, что $|\mathrm{Aut}(\mathbb{F}_q)| \leqslant n$. $\square$