Методы алгебраической геометрии в защите информации

А. Э. Маевский

1 Элементы теории Галуа

Определение 1. Алгебраическое расширение L/K называется *нормальным*, если каждый неприводимый над K многочлен, имеющий в L корень, разлагается над L на линейные множители.

Определение 2. *Группой автоморфизмов поля* K называется множество

$$\mathrm{Aut}(K) \stackrel{\text{def}}{=} \{\varphi\colon K \to K\}$$

с операцией композиции.

Упражнение 1. Доказать, что $\mathrm{Aut}(K)$ группа.

Упражнение 2. Пусть G — подгруппа в $\mathrm{Aut}(K)$. Доказать, что

$$K^G \stackrel{\text{def}}{=} \{x \in K \mid \forall g \in G\colon g(x) = x\}$$

подполе в K.

Определение 3. Группа автоморфизмов L над K определяется так:

$$\mathrm{Aut}(L/K) = \mathrm{Aut}_K(L) = \{\varphi \in \mathrm{Aut}(L) \mid \varphi|_K = \mathrm{id}_K\}.$$

Теорема 1. *Пусть L/K — нормальное алгебраическое. Тогда*

$$\forall g \in \mathrm{Aut}(\overline{L}/K)\colon\ g|_L \in \mathrm{Aut}(L/K).$$

Доказательство. Т.к. L — алгебраическое, то

$$\forall \alpha \in L\ \exists m_\alpha(x) \in K[x] \text{ — минимальный многочлен для } \alpha.$$

Пусть $\alpha \in L$. Все корни $m_\alpha(x)$ принадлежат $\overline{L}$ и, более того, L (нормальность).

Пусть $g \in \mathrm{Aut}(\overline{L}/K)$.

$$0 = g(\alpha) = g(m_\alpha(\alpha)) = \ldots = m_\alpha(g(\alpha)).$$

Следовательно, $g(\alpha)$ — корень $m_\alpha(x)$, а значит, принадлежит $\overline{L}$ и L. ■

Теорема 2. *Пусть L/K — произвольное алгебраическое расширение. Тогда*

$$\forall g \in \mathrm{Aut}(L/K)\colon\ \exists \tilde{g} \in \mathrm{Aut}(\overline{L}/K)\colon \tilde{g}|_L = g.$$

Доказательство. По Т. о вложении алг. расширений $g \in \mathrm{Aut}(L/K)$ рассмотрим как вложение $g\colon L \hookrightarrow \overline{L}$, причём $g|_K = \sigma\colon K \hookrightarrow \overline{L}$. Разным g соответствуют различные вложения. ■

Теорема 3 (о мощности $\mathrm{Aut}(L/K)$)**.** *Пусть L/K — конечное алгебраическое расширение, тогда*

$$|\mathrm{Aut}(L/K)| \leqslant [L : K].$$

Доказательство. Пусть $\alpha \in \overline{K}$, существует минимальный над K многочлен α.

$$K(\alpha) \cong K[x]/(m_\alpha(x)).$$

Пусть $d = \deg m_\alpha(x)$. Пусть $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_s$ — различные корни $m_\alpha(x)$ в $\overline{K}$ (sd). Для каждого $i \in [1, s]_{\mathbb{N}}$ существует единственный $\sigma_i\colon K(\alpha) \hookrightarrow \overline{K}$ и других вложений $\hat{\sigma}\colon K(\alpha) \hookrightarrow \overline{K}$, $\hat{\sigma}|_K = \sigma$ нет.

Это рассуждение продолжается по индукции для любого конечного алгебраического расширения (которое, как известно, можно рассматривать как последовательность простых расширений). ■

Определение 4. Число s различных вложений $K(\alpha)$ в $\overline{K}$ называется *степенью сепарабельности* α. Обозначение: $\deg_s(K(\alpha)/K) = [K(\alpha) : K]_s$

Замечание. Степень сепарабельности $\alpha \in K$ совпадает с количеством корней минимального многочлена α в $\overline{K}$.

Упражнение 3. L/K — алгебраическое расширение. $\varphi\colon L \to L$ — гомоморфизм полей над K. Тогда φ — изоморфизм.

Решение. Гомоморфизм φ переводит каждый элемент $\alpha \in L$ в сопряжённый с ним. Так как сопряжённых — конечное число, получается инъективный гомоморфизм *конечномерного* векторного пространства $K(\alpha)$, который (факт лин. алгебры) является изоморфизмом.

Замечание. В случае трансцендентных расширений предыдущее утверждение, вообще говоря, не верно.

Распространим понятие сепарабельности на произвольные алгебраические расширения.

Определение 5. L/K — конечное алг. расширение, $\sigma\colon K \to \overline{K}$. *Степень сепарабельности* L *над* K это количество различных вложений $\hat{\sigma}\colon L \to \overline{K}$, таких что $\hat{\sigma}|_K = \sigma$. Расширение L/K называется сепарабельным, если $[L : K]_s = [L : K]$.

Утверждение 1.

$$|\operatorname{Aut}(L/K)| \leqslant [L : K]_s \leqslant [L : K]. \tag{1}$$

Первое неравенство: два различных вложения $L \to \overline{K}$ могут не давать два различных автоморфизма L, если образы вложений не совпадают.

В двойном неравенстве (1) равенство слева — признак нормальности расширения, справа — сепарабельности.

Теорема 4.

$$[M : K]_s = [M : L]_s \cdot [L : K]_s$$

Доказательство. $\sigma\colon K \hookrightarrow \overline{K}$. $\sigma_i\colon L \hookrightarrow \overline{K}$, $\sigma_i|_K = \sigma$. $m = [L : K]_s$, $n = [M : K]_s$, $t = [M : L]_s$. $\tau_{ij}\colon M \hookrightarrow \overline{K}$, $\tau_{ij}|_L = \sigma_i$ (Здесь мы используем $\overline{L} = \overline{K}$, иначе, в соответствии с опр. сепарабельности, следовало бы писать $\tau_{ij}\colon M \hookrightarrow \overline{L}$.)

Надо показать, что

$$\tau_{ij} \neq \tau_{lk} \quad \text{при } i \neq l, j \neq k.$$

Если $\tau_{ij} = \tau_{lk}$, то $\sigma_i = \tau_{ij}|_L = \tau_{lk}|_L = \sigma_l$, а значит, $i = l$. Но тогда $j = k$.

Имеем $[M : K]_s \geqslant t \cdot m$. Осталось показать обратное нестрогое неравенство. Пусть $\rho\colon M \hookrightarrow \overline{K}$, $\rho|_K = \sigma$. Но $\rho|_L = \sigma_i$ для некоторого $i \in [1, m]_{\mathbb{N}}$. Следовательно $\rho = \tau_{ij}$ для некоторого j. ■

Определение 6. Многочлен $f(x) \in K[x]$ называется *сепарабельным*, если все его корни в $\overline{K}$ различны.

Лемма 1. *Любой неприводимый многочлен над полем характеристики* 0 *сепарабелен.*

Доказательство. Производная имеет конечную степень (не равна 0) и потому взаимно проста с неприводимым многочленом. ■

Лемма 2. *Пусть $f(x) \in K[x]$ неприводимый. $f(x) \in K[x]$ не сепарабелен тогда и только тогда, когда* $\operatorname{char} K = p > 0$, *$f(x) = g(x^{p^n})$ и $g(x)$ неприводим и сепарабелен над K.*

Утверждение 2. Несепарабельные неприводимые многочлены могут существовать только в полях K, таких что $\operatorname{char} K = p > 0$ и $K^p \neq K$ ($K^p \stackrel{\text{def}}{=} \{a^p \mid a \in K\}$).

Доказательство. Несепарабельный неприводимый многочлен $f(x) \in K[x]$ имеет вид $f(x) = g(x^{p^n})$, но в поле K, таком что $K^p = K$, можно извлекать корни p-ой степени, а значит $f(x) = (h(x))^{p^n}$ что противоречит неприводимости. ■

Пример 1. Пусть $K = \mathbb{F}_p(t)$, $f(x) = x^p + t$ — неприводимый несепарабельный многочлен.

Лемма 3. *$K \subset L \subset M$ — произвольные алгебраические расширения. Если M/K сепарабельно, то M/L и L/K сепарабельны.*

Доказательство. $[M : L]_s[L : K]_s = [M : K]_s = [M : K] = [M : L][L : K]$, но $[\cdot]_s \leqslant [\cdot]$, следовательно, степени и степени сепарабельности промежуточных расширений равны. ■

Рассмотрим подробнее несепрабельные элементы (алгебраические элементы, минимальные многочлены которых несепарабельны).

Теорема 5. *Пусть α — алгебраический и несепарабельный элемент над полем K характеристики p, $m_\alpha(x) = g(x^{p^\mu})$. Тогда α^{p^μ} сепарабельный и*

$$[K(\alpha) : K]_s = \deg g(x), \quad [K(\alpha) : K] = p^\mu [K(\alpha) : K]_s.$$

Доказательство. ...

$$f(x) = g(x^{p^\mu}) = \prod_{i=1}^{m} (x^{p^\mu} - \alpha^{p^\mu}) = \prod_{i=1}^{m} (x - \alpha)^{p^\mu}.$$

■

Определение 7. L/K — конечное алгебраическое расширение. *Индекс несепарабельности*:

$$[L : K]_i = \frac{[L : K]}{[L : K]_s}.$$

Если $[L : K]_i$ максимально, то расширение называется *чисто несепарабельным*. Если $[K(\alpha) : K]_i$ максимально, то α называется *чисто несепарабельным*.

Определение 8. Элемент $\alpha \in L$ называется *чисто несепарабельным*, если

Лемма 4. *Элемент $\alpha \in L$ чисто несепарабелен тогда и только тогда, когда*

$$m_\alpha(x) = x^{p^\mu} - a, \quad a \in K.$$

Определение 9. Пусть L/K — произвольное (необязательно конечное) алгебраическое расширение. Оно называется *чисто несепарабельным*, если для любого $\alpha \in L$:

$$m_\alpha(x) = x^{p^\mu} - a_\alpha \in K[x].$$

Упражнение 4. Пусть $K \subset L \subset M$ — башня алгебраических расширений. Показать, что M/K чисто несепарабельно тогда и только тогда, когда чисто несепарабельны M/L и L/K.

Утверждение 3. Пусть L/K — алгебраическое расширение. Обозначим L^s — множество всех сепарабельных элементов L. Тогда L^s — поле.

Утверждение 4. L^s/K — сепарабельно, а L/L^s — чисто несепарабельно.

Доказательство. Пусть $\alpha \in L$ — несепарабельный. $m_\alpha(x) = g(x^{p^\mu})$, $g(x) \in K[x]$ — неприводимый и сепарабельный. $\alpha^{p^\mu} \in L^s$. $x^{p^\mu} - \alpha^{p^\mu} \in L^s[x]$. По лемме (4) α — чисто несепарабельным. ■

Определение 10. Алгебраическое расширение L/K называется *расширением Галуа*, если оно нормально и сепарабельно. *Группой Галуа* $\mathrm{Gal}(L/K)$ расширения Галуа L/K называется его группа автоморфизмов.

Теорема 6. *Пусть L/K — конечное расширение Галуа. Существует взаимно однозначное соответствие между подгруппами* $\mathrm{Gal}(L/K)$ *и подполями между L и K:*

$$H \leftrightarrow L^H (= \{x \in L \mid Hx = x\}),$$

при этом нормальным подгруппам соответствуют нормальные расширения K.

Определение 11. Поле K называется совершенным, если любое его алгебраическое расширение сепарабельно.

Определение 12. Абсолютной группой Галуа поля K называется группа $\mathrm{Aut}\left((\overline{K})^s/K\right)$.

Упражнение 5. $(\overline{K})^s/K$ — нормально.