

Subfile Example

Team Learn ShareLaTeX

1 Вопросы на 9

1.1 Эквивалентность определений нормального сепарабельного расширения (расширения Галуа)

Пусть $K \supset F$ — конечное сепарабельное расширение. Тогда следующие условия эквивалентны:

1. Для любого элемента $\alpha \in K$, любой сопряженный к α над F тоже лежит в K
2. K является полем разложения какого-либо многочлена над F
3. $|Aut_F K| = [K : F]$
4. $K^{Aut_F K} = F$

Такое расширение называется *нормальным* или *расширением Галуа*.

$1 \Rightarrow 2$

Так как расширение конечное, $K = F(\alpha_1, \dots, \alpha_n)$.

Положим $f := m_{\alpha_1, F} \cdot \dots \cdot m_{\alpha_n, F}$. Тогда, поскольку все сопряженные к $\alpha_1, \dots, \alpha_n$ лежат в K , K содержит все корни f . С другой стороны, если $K \supset L$ содержит все корни f , то $\alpha_1, \dots, \alpha_n \in L \Rightarrow F(\alpha_1, \dots, \alpha_n) \subset L \Rightarrow K \subset L \subset K \Rightarrow L = K$, то есть K — поле разложения f над F .

$2 \Rightarrow 3$

Утверждение 1. Любой гомоморфизм $\varphi: K \rightarrow \bar{F}$, сохраняющий F переводит элементы K в сопряженные к ним над F .

Доказательство утверждения 1:

Пусть $\alpha \in K$, $m_{\alpha, F} = \sum_{k=0}^n a_k x^k$. $m_{\alpha, F}(\alpha) = 0 \Rightarrow \varphi(m_{\alpha, F}(\alpha)) = \varphi(0) = 0$.

С другой стороны $0 = \varphi(m_{\alpha, F}(\alpha)) = \varphi(\sum_{k=0}^n a_k \alpha^k) = \sum_{k=0}^n a_k \varphi(\alpha)^k = m_{\alpha, F}(\varphi(\alpha))$,

что и означает, что $\varphi(\alpha)$ сопряжен к α над F .

Утверждение 2. Пусть $\varphi: K \rightarrow \bar{F}$ — гомоморфизм, сохраняющий F . Тогда φ является автоморфизмом K .

Действительно, пусть K — поле разложения f над F , и $\alpha_1, \dots, \alpha_n$ — корни f .

Тогда $K = F(\alpha_1, \dots, \alpha_n)$.

Поскольку для любого $i : m_{\alpha_i, F} | f \Rightarrow$ то все сопряженные к α_i над F находятся среди корней f .

По утверждению 1 множество $\{\alpha_1, \dots, \alpha_n\}$ переходит в свое подмножество, а учитывая, что любой нетривиальный гомоморфизм полей инъективен, то на самом деле оно переходит само в себя (в силу конечности). Тогда φ задает на множестве индексов корней f некую перестановку σ .

Пусть $\beta \in K, \beta = \sum_{k=0}^n a_k \alpha_k, a_k \in F$. Тогда $\varphi(\beta) = \varphi(\sum_{k=0}^n a_k \alpha_k) = \sum_{k=0}^n a_k \alpha_{\sigma(k)} \in K$.

То есть $\varphi(K) \subset K$.

С другой стороны $\varphi(\sum_{k=0}^n a_k \alpha_{\sigma^{-1}(k)}) = \sum_{k=0}^n a_k \alpha_k = \beta$. То есть $\varphi(K) = K$.

Итого, $\varphi : K \rightarrow K$ — сюръективный гомоморфизм полей, а значит — автоморфизм K .

Поскольку $K \supset F$ — конечное сепарабельное, то по теореме о примитивном элементе найдется такое γ , что $K = F(\gamma)$.

Пусть $\gamma = \gamma_1, \gamma_2, \dots, \gamma_m$ — корни $m_{\gamma, F}$.

Вспомним утверждение 6.13 (точнее, его доказательство).

$K = F(\gamma_1) \xrightarrow{\varphi} F(\gamma_i)$, причем φ сохраняет F и $\varphi(\gamma_1) = \gamma_2$.

$\varphi : K \rightarrow \overline{F}$ — гомоморфизм, сохраняющий F , следовательно, по утверждению 2 он является автоморфизмом K , сохраняющим F . То есть для любого i существует $\varphi \in \text{Aut}_F K : \varphi(\gamma_1) = \gamma_i \Rightarrow |\text{Aut}_F K| \geq m$.

С другой стороны, тем, куда переходит $\gamma = \gamma_1$ автоморфизм, сохраняющий F полностью определяется (поскольку любой элемент K разлагается по степеням γ с коэффициентами из F). Значит, $|\text{Aut}_F K| \leq m$. Значит, $|\text{Aut}_F K| = m = \deg m_{\gamma, F} = [K : F]$, что и требовалось доказать.

$3 \Rightarrow 4$

Пусть $K^{\text{Aut}_F K} = L. K \supset L \supset F$ (5.31)

Пусть, по-прежнему, $K = F(\gamma)$. Мы уже выяснили, что при автоморфизме K , сохраняющем F γ переходит в корень $m_{\gamma, F}$, причем тем, куда переходит γ полностью определяется автоморфизм.

Заметим, что $K = L(\gamma)$, и что все вышесказанное справедливо и для расширения $K \supset L$, то есть $|\text{Aut}_L K| \leq \deg m_{\gamma, L} = [K : L]$

Все автоморфизмы, сохраняющие F сохраняют и L (по определению L), значит, $|\text{Aut}_F K| \leq |\text{Aut}_L K| \leq [K : L] \leq [K : F]$.

Но $|\text{Aut}_F K| = [K : F] \Rightarrow [K : L] = [K : F] \Rightarrow L = F$.

$4 \Rightarrow 1$

Рассмотрим вспомогательное утверждение:

Пусть $K^H = F$. Тогда для любого $\beta \in K : |H| \geq m_{\alpha, F}$ (это нам конкретно сейчас не понадобится) и любой сопряженный к β над F лежит в K (а вот это будем использовать).

Докажем его. Рассмотрим $f_\beta = \prod_{h \in H} (x - h(\beta))$.

Рассмотрим действие элементами H на элементах $K[x]$:

$$H \ni h \mapsto \alpha_h(\sum a_k x^k) = \sum h(a_k) x^k.$$

Проверим, что это действие (напомню: действие, это гомоморфизм из H в группу биекций $K[x]$).

1) Инъективность:

Пусть $\alpha_h(g_1) = \alpha_h(g_2)$, тогда образы всех коэффициентов g_1 совпадают с образами всех коэффициентов g_2 . Но h — автоморфизм, так что все *коэффициенты* g_1 совпадают с коэффициентами g_2

2) Сюръективность:

$$\alpha_h(\sum h^{-1}(a_k) x^k) = \sum a_k x^k$$

3) Гомоморфность:

$$\alpha_{h_1} \circ \alpha_{h_2}(\sum a_k x^k) = \alpha_{h_1}(\sum h_2(a_k) x^k) = \sum h_1 h_2(a_k) x^k = \alpha_{h_1 h_2}$$

$$\text{Заметим также, что } \alpha_h((\sum a_k x^k)(\sum b_k x^k)) = \alpha_h(\sum (\sum_{i+j=k} a_i b_j) x^k) = \sum h(\sum_{i+j=k} a_i b_j) x^k =$$

$$\sum (\sum_{i+j=k} h(a_i) h(b_j)) x^k = (\sum h(a_k) x^k)(\sum h(b_k) x^k) = \alpha_h(\sum a_k x^k) \alpha_h(\sum b_k x^k).$$

Иными словами, $\alpha_h(fg) = \alpha_h(f) \alpha_h(g)$.

Возьмем произвольный $g \in H$. Учитывая вышесказанное

$$\alpha_g(f_\beta) = \prod_{h \in H} \alpha_g(x - h(\beta)) = \prod_{h \in H} (x - gh(\beta)). \text{ Но умножение на элемент}$$

группы есть автоморфизм группы, то есть $gH = H$, то есть $\alpha_g(f_\beta) = f_\beta$. То есть все коэффициенты f_β сохраняются под действием любого элемента H .

Поскольку $K^H = F$, все коэффициенты f_β лежат в F , то есть $f_\beta \in F[x]$.

Поскольку $id \in H \Rightarrow f_\beta(\beta) = 0 \Rightarrow m_{\beta, F} | f_\beta$. То есть, во первых, $\deg m_{\beta, F} \leq \deg f_\beta = |H|$ (последнее равенство — из определения f_β).

Во-вторых, все корни $m_{\beta, F}$ являются корнями f_β , то есть образами β при каком-то автоморфизме K , то есть лежат в K .

Значит, все сопряженные к β лежат в K .

По условию $K^{Aut_F K} = F$, значит, по утверждению, любой сопряженный к любому элементу K лежит в K . Что и требовалось доказать.

1.2 Теорема Гильберта о базисе

Нужно доказать, что если K — нетерово, то и $K[x]$ тоже нетерово (это и есть теорема Гильберта о базисе).

Пусть есть цепочка строго вложенных в $K[x]$ идеалов $I_1 \subsetneq I_2 \subsetneq \dots \subsetneq I_n \subsetneq \dots$

Положим $I = \cup I_i$. Как неоднократно обсуждалось (5.6, 8.2) I — идеал.

Будем итеративно строить последовательность $f_1, \dots, f_n, \dots \in K[x]$

На i -м шаге будем выбирать $f_i \in I \setminus (f_1, f_2, \dots, f_{i-1}) : \deg f_i \rightarrow \min$.

(На первом шаге просто выберем $f_i \in I : \deg f_1 \rightarrow \min$. Под (f_1, \dots, f_{i-1}) подразумевается идеал, порожденный соответствующими многочленами).

Корректность выбора (т.е. что такое f_i существует) следует из того, что $f_1, \dots, f_{i-1} \in I_{i-1} \Rightarrow (f_1, \dots, f_{i-1}) \subset I_{i-1} \subsetneq I_i \subset I$.

Рассмотрим теперь старшие коэффициенты этих многочленов $a_1, a_2, \dots, a_n, \dots$. Сразу заметим, что при $i < j : I \setminus (f_1, \dots, f_i) \supset I \setminus (f_1, \dots, f_j) \Rightarrow \deg f_i \leq \deg f_j$.

Рассмотрим цепочку идеалов $(a_1) \subset (a_1, a_2) \subset \dots \subset (a_1, \dots, a_n) \subset \dots$. Это последовательность вложенных идеалов из K . Поскольку K — нетерово, она стабилизируется, то есть существует такое N , что $a_{N+1} \in (a_1, \dots, a_N) \Rightarrow \exists b_1, b_2, \dots, b_N : a_{N+1} = \sum_{i=1}^N b_i a_i$.

Рассмотрим $f = f_{N+1} - \sum_{i=1}^N b_i \cdot f_i \cdot x^{\deg f_{N+1} - \deg f_i}$. (Все степени x -ов неотрицательны по замечанию выше). Степень f строго меньше степени f_{N+1} . С другой стороны, если $f \in (f_1, \dots, f_N) \Rightarrow f_{N+1} \in (f_1, \dots, f_N)$, что не так. Получили противоречие с минимальностью степени f_{N+1} .

То есть в $K[x]$ не существует последовательности строго вложенных идеалов.

Пусть в $K[x]$ есть последовательность вложенных идеалов, которая не стабилизируется. Тогда из нее можно выделить подпоследовательность строго вложенных идеалов. (Не стабилизируется равносильно тому, что $\forall N \exists n > N : I_N \subsetneq I_n$).

Получили, что $K[x]$ нетерово, что и требовалось.

1.3 Если кольцо K факториально, то $K[x]$ тоже факториально

1.4 Основная теорема теории Галуа

1.5 Основная теорема алгебры

1.6 Теорема Ферма при $n = 3$ с использованием чисел Эйзенштейна

1.7 Сведение разрешимости уравнения в радикалах к разрешимости соответствующей группы Галуа

(Теоремой Куммера можно пользоваться без доказательства)

1.8 Пример уравнения, неразрешимого в радикалах

(Теоремой о разрешимости группы Галуа можно пользоваться без доказательства).

1.9 Неприводимость многочлена деления круга $\Psi(x)$ над \mathbb{Q}

1.10 Теорема Островского