Subfile Example

Team Learn ShareLaTeX

9 Вопросы на 9

9.1 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 многолена 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 $\varphi K \to \overline{F}$, сохраняющий F переводит элементы K в сопряженные к ним над F.

Доказательство утверждения 1:

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

С другой стороны $0 = \varphi(m_{\alpha,F}(\alpha)) = \varphi(\sum\limits_{k=0}^{n} a_k \alpha^k) = \sum\limits_{k=0}^{n} a_k \varphi(\alpha)^k = m_{\alpha,F}(\varphi(\alpha))$, что и означает, что $\varphi(\alpha)$ сопряжен к α над F.

Утверждение 2. Пусть $\varphi : K \to \overline{F}$ — 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 $K = F(\alpha_1, \ldots, \alpha_n)$.

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 $\{\alpha_1, \ldots, \alpha_n\}$ 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 $\beta \in K, \beta = \sum\limits_{k=0}^{n} a_k\alpha_k, a_k \in F$. Тогда $\varphi(\beta) = \varphi(\sum\limits_{k=0}^{n} a_k\alpha_k) == \sum\limits_{k=0}^{n} a_k\alpha_{\sigma(k)} \in K$.

То есть $\varphi(K) \subset K$.

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

Итого, $\varphi : K \to K$ — 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 $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_m$ — корни $m_{\gamma,F}$.

Вспомним утверждение 6.13 (точнее, его доказательство).

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

$\varphi : K \to \overline{F}$ — гомоморфизм, сохраняющий F, следовательно, по утверждению 2 он является автоморфизмом K, сохраняющем F. То есть для любого i существует $\varphi \in Aut_F K : \varphi(\gamma_1) = \gamma_i \Rightarrow |Aut_F K| \geqslant m$.

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, $Aut_F K \leqslant m$. Значит, $Aut_F K = m = \deg m_{\gamma,F} = [K : F]$, что и требовалось доказать.

$3 \Rightarrow 4$

Пусть $K^{Aut_F K} = L.K \supset L \supset F$ (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 $|Aut_L K| \leqslant \deg m_{\gamma,L} = [K : L]$

Все автоморфизмы, сохраняющие F сохраняют и L (по определению L), значит, $|Aut_F K| \leqslant |Aut_L K| \leqslant [K : L] \leqslant [K : F]$.

Но $|Aut_F K| = [K : F] \Rightarrow [K : L] = [K : F] \Rightarrow L = F$.

$4 \Rightarrow 1$

Рассмотрим вспомогательное утверждение:

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

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

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 гомомофизм из H в группу биекций $K[x]$).

1) Инъективность:

Пусть $\alpha_h(g_1) = \alpha_h(g_2)$, тогда образы всех коэффициенто 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:

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

3) Гомоморфность:

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

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

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

Возьмем произвольный $g \in H$. Учитывая вышесказанное

$\alpha_g(f_\beta) = \prod\limits_{h \in H} \alpha_g(x - h(\beta)) = \prod\limits_{h \in H}(x - gh(\beta))$. Но умножение на элемент группы есть автоморфизм группы, то есть $gH = H$, то есть $\alpha_g(f_\beta) = f_\beta$. То есть все коэфиициенты 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, $\deg m_{\beta,f} \leqslant \deg f_\beta = |H|$ (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.

9.2 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 вложеных в $K[x]$ идеалов $I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I_n \subsetneq \ldots$

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

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

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

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

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

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

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

Рассмотрим $f = f_{N+1} - \sum\limits_{i=1}^{N} b_i \cdot f_i \cdot x^{\deg f_{N+1} - \deg f_i}$. (Все степени x-ов неотрицательны по замечанию выше). Степень f строго меньше степени f_{N+1}. С другой стороны, если $f \in (f_1, \ldots, f_N) \Rightarrow f_{N+1} \in (f_1, \ldots, f_N)$, 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.

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

Известное всем утверждение: если K — область целостности, то и $K[x]$ — область целостности, причем $\deg ab \geqslant \deg a, \deg b$. (Ссылка!!!)

Для начала покажем, что если p неразложим в K, то p неразложим в $K[x]$. Действительно, пусть $\deg p \leqslant 0, p = ab$. Тогда $\deg a, \deg b \leqslant 0$, то есть $a \in K, b \in K$. Но поскольку p неразложим в K, то $a \in K^* \vee b \in K^*$. А поскольку обратимые элементы K — это в точности обратимые элементы $K[x]$ (в силу того, что единица одна и та же и соображений степеней), получаем требуемое утверждение.

Теперь покажем, что если p неразложим в K, то p прост в $K[x]$.

Пусть $p|gh$. Посмотрим на g и h как на элементы $(K/(p))[x]$. (то есть рассмотрим коэффициенты по модулю p). (Обозначим их как $\overline{g}$ и $\overline{h}$ соответственно).

Поскольку p неприводим в K и K факториально, то p прост в K (7.3), а значит, $(K/(p))$ — область целостности (6.9), а значит $(K/(p))[x]$ — область целостности.

$p|gh \Rightarrow \overline{g}\overline{h} = 0 \Rightarrow \overline{g} = 0 \vee \overline{h} = 0 \Rightarrow p|g \vee p|h$.

(Тут неявно используется простое утверждение, что $K \ni p|g \Leftrightarrow$ все коэффициенты g делятся на p: просто вынести p за скобку или наоборот, внести).

Теперь пусть f примитивный элемент $K[x]$ (то есть НОД всех его коэффициентов равен единице). Пусть $f = g \cdot h$ в $\mathrm{Quot}(K)[x]$, причем $\deg g, \deg h \geqslant 1$. Тогда существуют такие $\hat{g}, \hat{h} \in K[x] : f = \hat{g} \cdot \hat{h}, \deg \hat{g}, \deg \hat{h} \geqslant 1$.

В дальнейших рассуждениях, когда я буду говорить “числитель” и “знаменатель”, я буду иметь в виду, что все дроби записаны в несократимом виде (то есть что числитель и знаменатель взаимно просты)

Действительно, пусть $c_g = \frac{\text{НОД всех числителей g}}{\text{НОК всех знаменателей g}}$.

Обозначим $\hat{g} = \frac{1}{c_g} g, \hat{h} = \frac{1}{c_h} h$.

Утверждение: $\hat{g}$ — примитивный многочлен из $K[x]$.

Доказательство утверждения: Пусть $a_n, \ldots, a_0$ — числители g, $b_n, \ldots, b_0$ — знаменатели. Обозначим за (a, b) НОД двух (или более) чисел, за $[a, b]$ — НОК.

Пусть $a_i = (a_0, \ldots, a_n) \cdot a_i', b_i' = [b_n, \ldots, b_0]/b_i$.

$a_0, \ldots, a_n$ делятся на $(a_0, \ldots, a_n) \cdot (a_0', \ldots, a_n') \Rightarrow (a_0, \ldots, a_n) \cdot (a_0', \ldots, a_n') | (a_0, \ldots, a_n)$ (поскольку $(a_0, \ldots, a_n)$ — НОД). Но это значит, что $(a_0', \ldots, a_n') = 1$ и значит a_i' взаимно просты.

b_i' тоже взаимно просты: $b_i | [b_0, \ldots, b_n]/b_i' \Rightarrow b_i | [b_0, \ldots, b_n]/(b_0', \ldots, b_n') \forall i \Rightarrow [b_0, \ldots, b_n] | [b_0, \ldots, b_n]/(b_0', \ldots, b_n')$ (в силу определения НОК).

Теперь покажем, что $a_i' \cdot b_i'$ взаимно просты. (Эти числа и будут коэффициентами $\hat{g}$). Пусть они все делятся на какое-то необратимое число p. В силу факториальности K p можно считать простым. Каждое число $a_i' \cdot [b_0, \ldots, b_n]/b_i$ делится на p, значит, в силу определения простоты, для любого i либо a_i делится на p, либо $[b_0, \ldots, b_n]/b_i$ делится на p.

Все a_i одновременно делится на p не могут. Пусть k такое, что b_k делится на максимальную степень p (среди b_i). Пусть $p^l | b_k; p^{l+1} \nmid b_k$. Заметим, что именно на такую степень делится $[b_0, \ldots, b_n]$ (меньше не может быть, ведь $b_k | [b_0, \ldots, b_n]$, Пусть $p^{l+1} | [b_0, \ldots, b_n] . \forall i [b_0, \ldots b_n] = b_i' \cdot b_i$. Поскольку в разложении на неразложимые в левой части p входит в хотя бы p^{l+1} степени, а $p^{l+1} \nmid b_i$, то все b_i' делятся на p, что невозможно в силу их взаимной простоты).

Рассмотрим $a_k' \cdot [b_0, \ldots, b_n]/b_k$. С одной стороны, a_k' взаимно просто с b_k (так как a_k взаимно просто с b_k, а $a_k' | a_k$, то есть $p \nmid a_k'$. С другой стороны, в разложение на неразложимые $[b_0, \ldots, b_n]$ и b_k p входит в одной и той же степени). Значит, $[b_0, \ldots, b_n]/b_k$ не делится на p. Противоречие.

Продолжим.

Тогда $g = c_g \hat{g}$, $h = c_h \hat{h}$, где $\hat{g}, \hat{h} \in K[x]$ — примитивные многочлены.

Пусть $c_g \cdot c_h = \frac{u \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}}{v \cdot q_1^{\beta_1} \cdot \ldots \cdot q_l^{\beta_l}}$. (Разложили числитель и знаменатель дроби на неразложимые и обратимые. Напомню, что мы считаем, что числитель и знаменатель взаимно просты).

Рассмотрим q_1. $q_1 \cdot v \cdot q_1^{\beta_1 - 1} \cdot \ldots \cdot q_l^{\beta_l} \cdot f = u \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \hat{g} \cdot \hat{h}$, то есть $u \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \hat{g} \cdot \hat{h}$ делится на q_1 в K. q_1 прост в K, значит он прост в $K[x]$. Тогда либо $u \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ делится на q_1 (что не так в силу взаимной простоты числителя и знаменателя), либо $\hat{g}$ делится на q_1 либо $\hat{h}$. Но это тоже не так в силу примитивности $\hat{g}, \hat{h}$. То есть на самом деле никакого знаменателя нет (можно считать, что нет даже “обратимой” его части (v) так как ее всегда можно засунуть в $\hat{g}$, например. Давайте также считать, что и $u = 1$).

Итак, $f = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \cdot \hat{g}\hat{h}$. В силу примитивности f все α_i равны нулю, так что $f = \hat{g} \cdot \hat{h}$. Поскольку $\deg \hat{g} = \deg g, \deg \hat{h} = \deg h$ заключаем требуемое.

То есть мы доказали, что если f — примитивный элемент $K[x]$, то он неразложим тогда и только тогда, когда f неразложим в $\mathrm{Quot}(K)[x]$.

Покажем, что если f неразложим в $K[x]$, то f прост в $K[x]$.

Если $\deg f \leqslant 0$ то мы это уже показывали. Если $\deg f > 0$ и f не примитивный, то он не неразложим (f делится на НОД своих коэффициентов). Иначе же f неразложим в $\mathrm{Quot}(K)[x]$, следовательно, прост в $\mathrm{Quot}(K)[x]$. (Так как многочлены над полем — евклидово кольцо).

Пусть $f | gg_1$ в $K[x]$. Тогда $f | gg_1$ в $\mathrm{Quot}(K)[x]$, и значит $f | g \vee f | g_1$. Пусть, без потери общности, $f | g \Rightarrow fh = g$ в $\mathrm{Quot}(K)$. Заметим, что $f, g \in K[x]$. Покажем, что $h \in K[x]$.

$h = c_h \cdot \hat{h}$, где $\hat{h}$ — примитивный. f тоже примитивный и, значит, у c_h нет знаменателя (рассуждение недавно проводилось выше — пусть есть, возьмем простой делитель $\ldots$), то есть $h \in K[x]$.

Таким образом мы показали, что любой неразложимый элемент $K[x]$ прост.

Покажем существование разложения индукцией по степени.

Если $\deg f \leqslant 0$ то разложение совпадает с разложением в K.

Пусть $\deg f \neq 0$. Тогда $f = c_f \cdot \hat{f}$, где $\hat{f}$ — примитивный. У c_f есть разложение. Пусть $\hat{f}$ разложим, тогда $\hat{f} = gh$, где $\deg g, \deg h < \deg \hat{f} = \deg f$ (в силу примитивности $\hat{f}$), и значит, у g, h существуют разложения по предположению индукции. Перемножая разложения c_f, g, h получим разложение f в неразложимые.

Остается воспользоваться утверждением 7.2 и требуемое доказано.

9.4 Основная теорема теории Галуа

Теорема. (Основная теорема теории Галуа) Пусть $K \supset F$ — расширение Галуа. Тогда:

1) Существует биективное соответствие между подполями $K \supset L \supset F$ и подгруппами $Aut_F K$, задаваемое отображениями:

$\varphi : L \mapsto Aut_L K$ и $\psi : H \mapsto K^H$

2) $L \supset F$ нормальное тогда и только тогда, когда $Aut_L K$ нормальна в $Aut_F K$.

3) $[L : F] = [Aut_F K : Aut_L K]$

Докажем ее:

1) Заметим, что если $K \supset L \supset F$, то $K \supset L$ — расширение Галуа, поскольку K является полем разложения некоторого многочлена f над F (в силу нормальности $K \supset F$), а значит, K является полем разложения f над L (f раскладывается к K на линейные множители, а если есть какое-то промежуточное поле $K \supset K' \supset L$, что в K' f раскладывается на линейные множители, то существует $K \supset K' \supset F$ с нужными свойствами, что противоречит тому, что K — поле разложения f над F)

Итак, $\psi(\varphi(L)) = \psi(Aut_L K) = K^{Aut_L K} = L$ в силу 3-го определения расширения Галуа.

Пусть $\psi(H) = K^H =: L$, тогда пусть $\varphi(\psi(H)) = Aut_L K =: H'$. Заметим, что из определения L $H \subset H'$. Поскольку $K \supset L$ — расширение Галуа, а значит конечное и сепарабельное, можно применить теорему о примитивном элементе (или ее конечный аналог — теорему о цикличности мультипликативной группы поля), то есть $K = L(\gamma)$.

С другой стороны, по утверждению из доказательства 9.1, примененного к расширению $K \supset L$ и $H : |H| \geqslant \deg m_{\gamma,L} = [K : L] = |H'|$. То есть на самом деле $H' = H$.

Таким образом, φ и ψ — взаимно обратные преобразования, а значит биекции.

2) Возьмем $g \in Aut_F K$. $K^{gHg^{-1}} = \{x \in K \mid \forall h \in H ghg^{-1}(x) = x\} = \{x \in K \mid \forall h \in H hg^{-1}(x) = g^{-1}(x) = \{x \in gK \mid \forall h \in H h(x) = x\} = gK^H$

То есть $H \triangleleft Aut_F K \Leftrightarrow \forall g \in Aut_F K\ gHg^{-1} = H \overset{\varphi\text{ — биекция}}{\Leftrightarrow} \forall g \in Aut_F K K^H = K^{gHg^{-1}} = gK^H$

Покажем, что $\forall g \in Aut_F K K^H = gK^H \Leftrightarrow K \supset K^H$ — нормальное.

$\Rightarrow$

Пусть $\forall g \in Aut_F K\ K^H = gK^H$. Пусть $\alpha \in K^H$. Поскольку группа Галуа $Aut_F K$ действует транзитивно на корнях $m_{\alpha,F}$, для любого β сопряженного с α над F существует $g \in Aut_F K : g(\alpha) = \beta$. Но $\alpha \in K^H \Rightarrow \beta \in g(K^H) = K^H$, то есть все сопряженные к любому элементу K^H лежат в K^H, то есть $K^H \supset F$ — нормальное.

$\Leftarrow$

Поскольку $\forall \alpha \in K^H, \forall g \in Aut_F K : g(\alpha)$ сопряжен к α, а все сопряженные к α элементы лежат в K^H поскольку $K^H \supset F$ — нормальное, то $g(K^H) \subset K^H \forall g \in Aut_F K$.

Но тогда $g^{-1}(K^H) \subset K^H \Rightarrow g(K^H) = K^H$.

Что и требовалось доказать.

3) $[L : F] = [K : F]/[K : L] = |Aut_F K|/|Aut_L K| = [Aut_F K : Aut_L K]$. Второе равенство выполнено, так как $K \supset L$ и $K \supset F$ — расширения Галуа.

4) (Бонус) Если $K \supset L \supset F$, и $K \supset F$, $L \supset F$ нормальные, то $Aut_F L \cong {Aut_F K}/{Aut_L K}$.

Доказательство: Построим гомоморфизм $\varphi : Aut_F K \to Aut_F L$ следующим образом: $\varphi(g) = g|_L$. Это определение корректно, так как $g|_L$ — гомоморфизм из L в $\overline{F}$, а значит, по утверждению из доказательства 9.1, $g|_L$ — автоморфизм L. Ядро же этого гомоморфизма, очевидно $Aut_L K$.

Применим основную теорему о гомоморфизмах: $Aut_F L \gtrsim {Aut_F K}/{Aut_L K}$. Но по пункту 3 порядки этих групп равны, то есть $Aut_F L \cong {Aut_F K}/{Aut_L K}$, что и требовалось.

9.5 Основная теорема алгебры

Теорема. $\mathbb{C}$ — алгебраически замкнутое поле.

Нам понадобятся два следующих утверждения:

1) Над $\mathbb{R}$ не бывает нетривиальных конечных расширений нечетной степени.

Доказательство: Пусть $K \supset \mathbb{R}$ — конечное расширение.

По теореме о примитивном элементе $K = \mathbb{R}(\gamma)$. $\deg m_{\gamma,\mathbb{R}} = [K : \mathbb{R}]$. Если $[K : \mathbb{R}]$ нечетно, то по известному факту из анализа, $m_{\gamma,\mathbb{R}}$ имеет корень. Но тогда, в силу неприводимости, его степень равна единице, то есть расширение — тривиально.

2) Над $\mathbb{C}$ не существует расширений второй степени.

Пусть $K \supset \mathbb{C}$ — расширение второй степени, то есть

$K = \mathbb{C}(\gamma)$, где $\deg m_{\gamma,\mathbb{C}} = 2$. Но над $\mathbb{C}$ не бывает неприводимых многочленов второй степени (поскольку можно найти корни через формулу с дискриминантом и разложить по теореме Виетта на два линейных сомножителя).

Теперь, пусть над $\mathbb{C}$ есть нетривиальное алгебраическое расширение K_1. Выберем $\gamma \in K_1 \backslash \mathbb{C}$. $\mathbb{C}(\gamma) \supset \mathbb{C} \supset \mathbb{R}$ — башня конечных алгебраических расширеший. Рассмотрим поле разложения $m_{\gamma,\mathbb{R}}$ над $\mathbb{C}$.

Лемма. Пусть $K \supset L \supset F$ и $L \supset F$ — нормальное, а K является полем разложения $f \in F[x]$ над L. (Соответственно, $K \supset L$ нормально). Тогда $K \supset F$ — нормально.

Пусть $\alpha_1, \ldots, \alpha_n$ — корни f, тогда $K = L(\alpha_1, \ldots, \alpha_n)$. Пусть L является полем разложения g над F, и корнями g являются $\beta_1, \ldots, \beta_m$. Тогда $L = F(\beta_1, \ldots, \beta_m)$. Тогда $K = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$, и, значит, K является полем разложения fg над F. То есть $K \supset F$ — нормальное.

Продолжим.

Итак, $\mathbb{C} \supset \mathbb{R}$ нормально (как поле разложения $x^2 + 1$), и K является полем разложения многочлена с коэффициентами из $\mathbb{R}$ над $\mathbb{C}$. (Многочлен — $m_{\gamma,\mathbb{R}}$).

То есть K нормально над $\mathbb{R}$. Пусть $[K : \mathbb{C}] = t$, и $t = 2^{n-1} \cdot m$, где $(m, 2) = 1$.

Пусть также $G = Aut_{\mathbb{R}} K$. Так как расширение нормально, $|G| = [K : \mathbb{R}] = 2^n \cdot m$. По теореме Силова в $|G|$ есть подгруппа порядка 2^n. Ей соответствует некоторое подполе $L : K \supset L \supset \mathbb{R}$, причем $[L : \mathbb{R}] = m$ (по основной теореме теории Галуа). Но так как m нечетно, то по первому утверждению $m = 1$.

То есть $[K : C] = 2^{n-1}$. Это расширение также нормально, пусть H — его группа Галуа. Тогда в ней есть подгруппа порядка 2^{n-2} (если $n \geqslant 2$) [Это факт из ТГ, например, следует из доказательства теоремы Силова, приведенного в Кострикине]. Тогда есть соответствующее ей подполе $L : K \supset L \supset \mathbb{C}$, причем $[L : \mathbb{C}] = 2$, чего не бывает. То есть $n = 1$ и $K = \mathbb{C}$, то есть над $\mathbb{C}$ нет нетривиальных алгебраических расширений. Что и требовалось доказать.

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

Нам нужно доказать, что $x^3 + y^3 = z^3$ неразрешимо в $\mathbb{Z}$. (нетривиальным образом).

Пусть разрешимо, тогда можно поделить на (x, y, z) (НОД) и получить взаимно простые в совокупности x, y, z. Заметим, что если простое $p|x, p|y$ $\Rightarrow p|x^3+y^3 = z^3 \Rightarrow p|z^3$, То есть $p|(x, y, z)$. То есть $(x, y) = (y, z) = (x, z) = 1$.

По задаче 6.8 $\lambda|xyz$ в $\mathbb{Z}[\omega]$.

9.7 Сведение разрешимости уравнения в радикалах к разрешимости соответствующей группы Галуа

(Теоремой Куммера можно пользоваться без доказательства)

9.8 Пример уравнения, неразрешимого в радикалах

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

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

9.10 Теорема Островского