ЗАДАЧИ ПО ТЕОРИИ ГАЛУА (05.02.2017)

(1) Докажите, что эндоморфизмы левого модуля образуют кольцо.

(2) Пусть A – ассоциативное кольцо, т.е. абелева группа с операцией умножения. Пусть A^{op} – та же самая абелева группа, но с операцией умножения $x\cdot^{\mathrm{op}}y := yx$. Докажите, что (а) A^{op} – ассоциативное кольцо, (б) любой левый A-модуль является правым A^{op}-модулем.

(3) Пусть A – ассоциативное кольцо. Докажите, что для левого A-модуля M следующие свойства эквивалентны: (i) M является суммой некоторого множества I простых подмодулей; (ii) M является прямой суммой простых модулей; (iii) любой подмодуль M выделяется прямым слагаемым.

(4) Какие из следующих модулей (полу)просты (и когда): модули над телом, $\mathbb{Z}$-модуль $\mathbb{Z}$, $\mathbb{Z}$-модуль $\mathbb{Q}$, $\mathbb{Z}$-модуль $\mathbb{Z}/n\mathbb{Z}$?

(5) Пусть k – поле и V – конечномерное (скажем, n-мерное) k-векторное пространство. Докажите, что (а) V – простой модуль над кольцом $\mathrm{End}_k(V)$ эндоморфизмов пространства V (т.е. над кольцом $n\times n$ матриц с коэффициентами в k), (б) любой модуль над кольцом $\mathrm{End}_k(V)$ полупрост, а точнее, изоморфен прямой сумме копий модуля V.

(6) Изоморфны ли поля расщепления каких-либо из следующих многочленов: x^2-2, x^2-3, x^4-10x^2+1, x^2+x+1, x^4+1 (а) над $\mathbb{Q}$; (б) над $\mathbb{Q}(\sqrt{-1})$; (в) над $\mathbb{Q}(\sqrt{2})$?

(7) Найдите все квадратичные подполя поля расщепления многочлена x^n-1 над $\mathbb{Q}$.

(8) Докажите, что (а) конечное расширение полей алгебраично, (б) расширение алгебраично тогда и только тогда, когда оно является объединением конечных подрасширений.

(9) Докажите, что поле расщепления многочлена является расширением Галуа тогда и только тогда, когда оно сепарабельно.

(10) Докажите, что следующие условия на расширение полей $K|k$ эквивалентны: (i) в $K\smallsetminus k$ нет элементов сепарабельных над k, (ii) для каждого $\alpha\in K$ найдётся такое целое $n\geqslant 0$, что $\alpha^{p^n}\in k$, (iii) минимальный многочлен любого элемента поля K над k имеет вид $X^{p^n}-a$ для некоторого целого $n\geqslant 0$ и некоторого $a\in k$. Если условия выполняются, то расширение $K|k$ называют *чисто несепарабельным*.

(11) Пусть $\mathcal{P}$ – некоторый набор многочленов над полем k. Докажите, что (а) набор $\mathcal{P}$ имеет поле расщепления; (б) все поля расщепления набора $\mathcal{P}$ изоморфны над k.

(12) Докажите, что поле расщепления множества всех многочленов над полем k алгебраически замкнуто, т.е. любой непостоянный многочлен над ним имеет корень.

(13) Докажите, что следующие условия на алгебраическое расширение полей $K|k$ эквивалентны: (i) K является полем расщепления некоторого набора многочленов над k; (ii) если неприводимый над k многочлен имеет корень в K, то он является произведением линейных множителей над K; (iii) любой неприводимый над k многочлен является произведением неприводимых многочленов над K равных степеней; (iv) для любого расширения поля k образ вложения в него над k поля K не зависит от вложения; (v) для некоторого алгебраически замкнутого расширения поля k образ вложения в него над k поля K не зависит от вложения. Такие расширения называются *нормальными*.

(14) Определите нормальность, группы автоморфизмов и подполя следующих расширений: $\mathbb{Q}(\sqrt{-2},\sqrt{2})|\mathbb{Q}$, $\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$, $\mathbb{Q}(\sqrt[n]{2}+\sqrt[n]{3}+\sqrt[n]{5})|\mathbb{Q}$ $(n=2,3)$, $\mathbb{F}_p(t,\alpha)|\mathbb{F}_p(t)$, $\alpha^{2p}-t\alpha^p+1=0$.[1]

(15) Класс расширений полей $\mathcal{C}$ называется *отмеченным*, если (i) для $k\subseteq K\subseteq F$ расширение $k\subseteq F$ принадлежит $\mathcal{C}$ тогда и только тогда, когда расширения $k\subseteq K$ и $K\subseteq F$ принадлежат $\mathcal{C}$; (ii) для любого расширения $k\subseteq K$ из $\mathcal{C}$ и любого расширения $k\subseteq F$

[1] Проверьте неприводимость $X^{2p}-tX^p+1$.

в общем поле Ω композит $F \subseteq KF$ принадлежит $\mathcal{C}$; (iii) для любой пары расширений $k \subseteq K$ и $k \subseteq F$ из $\mathcal{C}$ в общем поле Ω композит $k \subseteq KF$ также принадлежит $\mathcal{C}$.

Докажите, что следующие классы расширений являются отмеченными: (а) алгебраические, (б) конечные, (в) сепарабельные, (г) чисто несепарабельные. (д) Верно ли, что нормальное расширение нормального расширения нормально?

(16) Пусть $K|k$ – алгебраическое расширение полей. Докажите, что (а) K чисто несепарабельно над максимальным сепарабельным подрасширением k_s поля k, (б) имеется ровно $[k_s : k]$ вложений поля K над k в алгебраически замкнутое расширение поля k.

(17) Постройте несепарабельное расширение поля $k = \mathbb{F}_p(x, y)$ без чисто несепарабельного подрасширения.

(18) Пусть $k \subseteq K \subseteq L$ – тройка вложенных полей. Докажите, что алгебра $K \otimes_k L$ изоморфна прямой сумме полей тогда и только тогда, когда расширение $K|k$ конечно и сепарабельно. Что это за поля, если $K|k$ – расширение Галуа?

(19) *Дифференцированием* коммутативного кольца A со значениями в A-модуле M называется аддитивный гомоморфизм $D : A \to M$, удовлетворяющий правилу Лейбница: $D(fg) = gD(f) + fD(g)$ для любых $f, g \in A$.

(а) Докажите, что для произвольного гомоморфизма коммутативных колец $B \longrightarrow A$ существует единственная с точностью до изоморфизма пара, состоящая из A-модуля $\Omega_{A|B}$ и дифференцирования $d : A \to \Omega_{A|B}$, такая, что любое дифференцирование кольца A, нулевое на образе B, является композицией d и морфизма A-модулей из $\Omega_{A|B}$.

Модуль $\Omega_{A|B}$ называется *модулем кэлеровых дифференциалов* и описывается явно как множество конечных формальных сумм $\sum_j f_j dg_j$, где d – формальный символ и $f_j, g_j \in A$, с соотношениями билинейности: $(f+g)dh = fdh+gdh$ и $hd(f+g) = hdf+hdg$, правилом Лейбница: $hd(fg) = hfdg + hgdf$, и $dc = 0$, если c лежит в образе B.

(б) Постройте канонический изоморфизм $\mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\sim} \Omega_{A|B}$, где $\mathfrak{m}$ – ядро гомоморфизма умножения $A \otimes_B A \xrightarrow{\times} A$. (в) Докажите, что умножения на A через $A \otimes 1$ и через $1 \otimes A$ на $A \otimes_B A$ индуцируют одну и ту же структуру A-модуля на $\Omega_{A|B}$.

(20) Вычислите группы $\Omega_{\mathbb{Z}[\sqrt{5}]|\mathbb{Z}}$, $\Omega_{K|\mathbb{Z}}$, где K – какое-нибудь поле алгебраических чисел (конечной или бесконечной степени над $\mathbb{Q}$), $\Omega_{k[[t]]|k[[t^2]]}$, где k –произвольное поле.

(21) Докажите, что элемент x некоторого расширения поля k сепарабелен (и, в частности, алгебраичен) над k тогда и только тогда, когда $\Omega_{k(x)|k} = 0$.

(22) Верно ли, что если $\Omega_{K|k} = 0$, то расширение $K|k$ сепарабельно? Верно ли, что если $K|k$ – алгебраическое расширение и $\Omega_{K|k} = 0$, то расширение $K|k$ сепарабельно?

(23) Докажите, что следующие условия на расширение $K|k$ эквивалентны:
  (a) расширение $K|k$ сепарабельно;
  (b) для любого подполя $k' \subset k$ естественный морфизм $\Omega_{k|k'} \otimes_k K \to \Omega_{K|k'}$ инъективен;
  (c) стандартное отображение $\Omega_k \otimes_k K \to \Omega_K$ инъективно;
  (d) любое дифференцирование поля k со значениями в любом K-модуле M продолжается до дифференцирования поля K со значениями в M.

(24) Пусть $K|L$ – расширение полей. Тогда $\Omega_{K|L}$ – K-векторное пространство. Докажите, что а) $\dim_K \Omega_{K|L}$ совпадает со степенью трансцендентности расширения $K|L$ в случае нулевой характеристики; б) если характеристика p поля K положительна, то имеется равенство $\Omega_{K|L} = \Omega_{K|K^pL}$; кроме того, $K = K^p$ тогда и только тогда, когда $\Omega_{K|\mathbb{Z}} = 0$.

(25) Докажите, что множество дифференцирований $\mathrm{Der}(A|B) \subseteq \mathrm{End}_B(A)$ коммутативного кольца A над некоторым подкольцом $B \subset A$ образует B-алгебру Ли относительно операции коммутирования: если $\xi_1, \xi_2 \in \mathrm{Der}(A|B)$, то и $[\xi_1, \xi_2] := \xi_1\xi_2 - \xi_2\xi_1 \in \mathrm{Der}(A|B)$.

(26) Пусть A – коммутативная $\mathbb{F}_p$-алгебра и ξ – дифференцирование кольца A над некоторым подкольцом $B \subset A$. Докажите, что а) $\Omega_{A|B} = \Omega_{A|A^pB}$; б) ξ^p также является дифференцированием кольца A над B.