# ЗАДАЧИ ПО ТЕОРИИ (21.04.2017)

3.1. **Конечные расширения.**

(1) Пусть $\alpha, \beta$ – корни неприводимого многочлена $P(t) \in k[X]$ степени $n > 1$. Докажите, что $\deg(\alpha + \beta) \leqslant \frac{n(n-1)}{2}$.
(2) Пусть $\alpha, \beta$ – различные корни корни неприводимого многочлена $P(t) \in k[X]$ над полем $k$ характеристики 0. Докажите, что $\deg(\alpha - \beta) \geqslant 2$, или найдите контрпример.
(3) Пусть $\alpha, \beta$ – различные корни корни неприводимого многочлена $P(t) \in k[X]$ над полем $k$ характеристики 0 степени $> 2$. Докажите, что $\deg(\alpha + \beta) > 2$, или найдите контрпример.
(4) Пусть $\alpha, \beta$ – различные корни корни неприводимого многочлена $P(t) \in k[X]$ над полем $k$ характеристики 0. Докажите, что $\deg(\alpha\beta - 1) > 2$, или найдите контрпример.
(5) Пусть $\alpha, \beta$ – различные корни корни неприводимого многочлена $P(t) \in k[X]$ над полем $k$ характеристики 0 степени $> 2$. Докажите, что $\deg(\alpha\beta) > 2$, или найдите контрпример.
(6) Пусть $K$ – поле и $c \in K$. Покажите, что если целые числа $m, n \geqslant 1$ взаимно просты, то $X^{mn} - c$ неприводим тогда и только тогда, когда неприводимы оба $X^m - c$ и $X^n - c$.

3.2. **Конечномерные кольца.** Обозначения: $[a, b]$ – наименьшее общее кратное; $(a, b)$ – наибольший общий делитель чисел $a$ и $b$; $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ – функция Эйлера.

(1) Докажите, что $\mathbb{F}_{q^a} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^b} \cong \underbrace{\mathbb{F}_{q^{[a,b]}} \oplus \cdots \oplus \mathbb{F}_{q^{[a,b]}}}_{(a,b)\text{ слагаемых}}$.
(2) Докажите, что $\mathbb{Q}(\mu_a) \otimes_{\mathbb{Q}(\mu_d)} \mathbb{Q}(\mu_b) \cong \underbrace{\mathbb{Q}(\mu_{[a,b]}) \oplus \cdots \oplus \mathbb{Q}(\mu_{[a,b]})}_{\varphi((a,b))/\varphi(d)\text{ слагаемых}}$, где $d|(a, b)$.
(3) Докажите, что $\mathbb{Q}[\sqrt{2}] \otimes_{\mathbb{Q}} \mathbb{Q}[\sqrt{3}]$ – поле.
(4) Пусть $k$ – поле. Докажите, что $k[t] \otimes_{k[t^n]} k[t]$ содержит нильпотенты тогда и только тогда, когда характеристика поля $k$ делит $n$.
(5) Докажите, что форма следа $\mathrm{tr}(xy)$ расширения конечных полей $K|k$ невырождена.
(6) Найдите расширение $K|k$ степени 3, такое, что $K \otimes_k K$ есть прямая сумма двух полей.

3.3. **Расширения Галуа.**

(1) Для каких натуральных $n$ существует расширение Галуа степени $n$ поля $\mathbb{Q}$ в $\mathbb{R}$?
(2) Покажите, что все подрасширения (во всех смыслах) абелева расширения абелевы.
(3) Пусть $n > 1$, $K$ – поле, содержащее $n$ корней $n$-ой степени из единицы, $a, b \in K$. Допустим, что многочлены $X^n - a$ и $X^n - b$ неприводимы над $K$. Докажите, что их поля расщепления изоморфны тогда и только тогда, когда $b = c^n a^r$ для некоторого $c \in K$ и $r \in \mathbb{N}$ с $(r, n) = 1$.
(4) Пусть $k|\mathbb{Q}$ – квадратичное расширение. Докажите, что $k(\sqrt[11]{3})|k$ – не расширение Галуа.
(5) (Расширения периода 2) Пусть $K$ – поле характеристики $\neq 2$. Докажите, что любое расширение $F|K$ степени $2^n$ и с $\mathrm{Aut}(F|K) \cong (\mathbb{Z}/2\mathbb{Z})^n$ имеет вид $F = K(\sqrt{a_1}, \ldots, \sqrt{a_n})$.
(6) Пусть $p_1 < \cdots < p_n$ – простые числа, $F = \mathbb{Q}(\sqrt{p_1} + \cdots + \sqrt{p_n})$. Найдите $[F : \mathbb{Q}]$ и $\mathrm{Aut}(F|\mathbb{Q})$.
(7) Докажите, что $\mathbb{Q}(\sqrt[n]{5})|\mathbb{Q}$ – не расширение Галуа для любого $n \geqslant 3$.

(8) Пусть $k := \mathbb{F}_q(t)$ – поле рациональных функций над конечным полем $\mathbb{F}_q$. Постройте конечное расширение поля $k$, которое не является расширением Галуа.

(9) Пусть $G$ – конечная группа автоморфизмов поля $K$. Докажите, что расширение $K|K^G$ (i) конечно, (ii) нормально, (iii) сепарабельно.

3.4. **Обратная задача Галуа.**

(1) Постройте циклическое расширение Галуа поля $\mathbb{Q}$ степени $n$.

(2) Постройте расширение Галуа поля $\mathbb{Q}$ с группой Галуа $(\mathbb{Z}/3\mathbb{Z})^2$.

(3) Постройте произвольное абелево конечное расширение Галуа поля $\mathbb{Q}$.

(4) Пусть $k = \mathbb{R}(t)$ поле рациональных функций над $\mathbb{R}$, а $K|k$ – абелево расширение с группой Галуа $G$. Предположим, что порядок $G$ нечётный. Докажите, что $G$ циклическая, или найдите контрпример.

(5) Докажите, что (а) любая группа точно действует на некотором поле, (б) для любой конечной группы $G$ и любого поля $k$ найдутся расширение полей $K|k$ и конечное расширение Галуа $F|K$ с группой Галуа изоморфной $G$, (в) любая конечная абелева группа является группой Галуа над произвольным числовым полем.

3.5. **Вычисление группы Галуа.**

(1) Докажите, что многочлен $X^p + a\ell X + b\ell$ неприводим над $\mathbb{Q}$, где $p, \ell$ – простые, $a, b \in \mathbb{Z}$, $a \geqslant 0$, $\ell \not| b$. Найдите его группу Галуа.

(2) (i) Докажите, что многочлен $X^n - 2$ неприводим над $\mathbb{Q}$. (ii) Выясните, что происходит с неприводимостью многочлена $X^n - 2$ при присоединении к полю $\mathbb{Q}$ различных корней из единицы. (iii) Найдите группу Галуа многочлена $X^n - 2$ над $\mathbb{Q}$.

(3) Пусть $P(X)$ – неприводимый многочлен степени $n$ над конечным полем $k$. Докажите, что его группа Галуа – циклическая порядка $n$, или найдите контрпример.

(4) Пусть $K$ – поле, полученное добавлением к $\mathbb{Q}$ конечного числа корней из 1. Докажите, что все подполя поля $K$ являются расширениями Галуа поля $\mathbb{Q}$.

(5) Пусть $k$ – поле и $K = k(t)$ – поле рациональных функций над $k$ от одной переменной. Докажите, что многочлен $X^n - t$ неприводим для любого натурального $n$. Найдите порядок его группы Галуа, если $k$ конечно порядка 13 и $n = 5$.

(6)
  (a) Пусть $p$ – простое число и $a \in \mathbb{Z}$ не делится на $p$. Докажите, что многочлен $X^p - X + a$ неприводим над $\mathbb{Q}$.
  (b) (i) Докажите, что дискриминант $D$ многочлена $X^n - X - a$ равен $(-1)^{n(n+1)/2}((1-n)^{n-1} - a^{n-1}n^n)$, и что $|D| > 1$ для любого $n > 1$. (ii) Найдите кратные корни редукций многочлена $X^n - X - a$ по модулю простых делителей дискриминанта и их кратности.
  (c) В предположении, что многочлен $X^n - X - a$ неприводим над $\mathbb{Q}$ вычислите группу инерции его поля расщепления в каждом простом делителе числа его дискриминанта $D$.
  (d) Вычислите группу Галуа многочлена $X^n - X - 1$ над $\mathbb{Q}$ в предположении, что он неприводим.
  (e) Докажите, что многочлен $X^n - X - 1$ неприводим над $\mathbb{Q}$.

(7) Пусть $p, s+2$ – простые числа, $m \geqslant 1$, $n_1 < n_2 < \cdots < n_s$ – целые числа. Положим $g(X) = (X^2 + pm)(X - pn_1)\cdots(X - pn_s)$. Выберем целое $n > 0$, не делящееся на $p$, так, что $\frac{p}{n} < \min_{g'(x)=0} |g(x)|$. Покажите, что группа Галуа многочлена $g(X) = (X^2 + pm)(X - pn_1)\cdots(X - pn_s) - \frac{p}{n}$ изоморфна симметрической группе $s+2$ элементов.