Соответствие Галуа.

Терминология и обозначения. Нормальные сепарабельные расширения называются *расширениями Галуа*. Для конечного расширения $\Bbbk \subset \mathbb{F}$ это равносильно равенству $[\mathbb{F} : \Bbbk] = |\mathrm{Aut}_{\Bbbk}\,\mathbb{F}|$, и в таком случае группа $\mathrm{Aut}_{\Bbbk}\,\mathbb{F}$ называется *группой Галуа* $\mathbb{F}$ над $\Bbbk$ и обозначается $\mathrm{Gal}\,\mathbb{F}/\Bbbk$. Группа Галуа $\mathrm{Gal}\,\mathbb{L}_f/\Bbbk$ поля разложения $\mathbb{L}_f$ сепарабельного многочлена $f \in \Bbbk[x]$ называется *группой Галуа многочлена f над* $\Bbbk$ и обозначается $\mathrm{Gal}\,f/\Bbbk$. Мы полагаем $\sqrt[n]{1} \overset{\text{def}}{=} e^{\frac{2\pi i}{n}} \in \mathbb{C}$.

А13◇1. Всегда ли в конечном расширении Галуа $\mathbb{F} \supset \Bbbk$ есть элемент, $\mathrm{Gal}\,\mathbb{F}/\Bbbk$-орбита которого является базисом векторного пространства $\mathbb{F}$ над $\Bbbk$?

А13◇2. Пусть $f \in \Bbbk[x]$ неприводим, и $\mathrm{char}\,\Bbbk \neq 2$. Равносильно ли условие $D(f) \in \Bbbk^2$ тому, что группа $\mathrm{Gal}\,f/\Bbbk$ осуществляет лишь чётные перестановки корней f?

А13◇3. Является ли расширением Галуа поля $\mathbb{Q}$ **а)** поле $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ **б)** поле $\mathbb{Q}(\sqrt[3]{1}+\sqrt[3]{2})$ **в)** поле разложения многочлена x^7-5 и если да, то найдите его группу Галуа над $\mathbb{Q}$.

А13◇4. Опишите все подполя каждого из трёх полей предыдущей задачи и вычислите группы Галуа над $\mathbb{Q}$ всех тех подполей, что являются расширениями Галуа поля $\mathbb{Q}$.

А13◇5. Найдите группу Галуа над $\mathbb{Q}$ у многочленов **а)** x^3-3x+1 **б)** x^3+2x+1 **в)** x^4-5x^2+6 **г)** x^4+x^2+1 **д)** x^4+1 и выразите их корни через квадратные и кубические радикалы.

А13◇6. Предъявите угол, который нельзя разбить на три равных угла циркулем и линейкой.

А13◇7. Найдите группу Галуа над $\mathbb{Q}$ многочлена x^4+2x^2+x+3.

А13◇8. Предъявите неприводимый $f \in \mathbb{Z}[x]$ степени 6 с $\mathrm{Gal}\,f/\mathbb{Q} \simeq S_6$.

А13◇9. Выразите **а)** $\sqrt[5]{1}$ **б)** $\sqrt[17]{1}$ через квадратные корни, а **в)** $\sqrt{13}$ через $\sqrt[13]{1}$

А13◇10. Для простого $p > 2$ и $\mathbb{F} = \mathbb{Q}[\sqrt[p]{1}]$ покажите, что $G = \mathrm{Gal}\,\mathbb{F}/\mathbb{Q}$ содержит единственную подгруппу индекса 2 и опишите отвечающее ей квадратичное расширение поля $\mathbb{Q}$.

А13◇11. Для простого $p \in \mathbb{N}$ и любого $a \in \mathbb{Q}$, не являющегося p-той степенью, покажите, что группа Галуа многочлена $x^p - a$ над $\mathbb{Q}$ изоморфна группе аффинных автоморфизмов прямой $\mathbb{A}^1(\mathbb{F}_p)$.

А13◇12 (квадратичная взаимность). Для простых $p, q > 2$ положим $q^* = (-1)^{\frac{q-1}{2}}q$, $\mathbb{K} = \frac{\mathbb{Q}[x]}{(x^2-q^*)}$, через $\mathcal{O} \subset \mathbb{K}$ обозначим целое замыкание $\mathbb{Z}$ в $\mathbb{Q}$-алгебре $\mathbb{K}$, через $[z]_p$ — класс $z \bmod (p)$.

- **а)** Покажите, что $[q^*]_p \in \mathbb{F}_p^2 \iff \mathcal{O}/(p) = \mathbb{F}_p \oplus \mathbb{F}_p \iff$ автоморфизм Фробениуса $F_p : \vartheta \mapsto \vartheta^p$ тождественно действует на $\mathcal{O}/(p)$.
- **б)** Каковы позитивные альтернативы 2-му и 3-му из предыдущих свойств кольца[1] $\mathcal{O}/(p)$?
- **в)** Постройте такое вложение $\mathbb{Q}$-алгебр $\mathbb{K} \hookrightarrow \mathbb{Q}[\sqrt[q]{1}] \subset \mathbb{C}$, что приведение по модулю (p) ограничения на $\mathcal{O} \subset \mathbb{K}$ эндоморфизма $z \mapsto z^p$ мультипликативной группы $\mathbb{C}^*$ совпадает с F_p.
- **г)** Получите явное выражение $\sqrt{q^*}$ через корни q-той степени из единицы и выясните, как действует на него эндоморфизм из предыдущего пункта.
- **д)** Докажите *квадратичный закон взаимности*[2]: $\left[\dfrac{p}{q}\right] \cdot \left[\dfrac{q}{p}\right] = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

А13◇13. Постройте циркулем и линейкой правильный 17-угольник.

А13◇14. Покажите, что **а)** $\mathbb{Q}[\sqrt{p}] \subset \mathbb{Q}[\sqrt[4p]{1}]$ при простом $p \equiv 3 \bmod (4)$ **б)** любое квадратичное расширение поля $\mathbb{Q}$ содержится в некотором круговом поле $\mathbb{Q}[\sqrt[m]{1}] \subset \mathbb{C}$.

А13◇15. Верно ли, что $\mathrm{Aut}_{\Bbbk}\,\Bbbk(t) \simeq \mathrm{PGL}_2(\Bbbk)$?

---

[1] т. е. чему оно изоморфно, если не $\mathbb{F}_p \oplus \mathbb{F}_p$, и как действует на нём F_p, если не тождественно?

[2] напомню, что *символ Лежандра – Якоби* $\left[\dfrac{n}{p}\right] \overset{\text{def}}{=} \begin{cases} 0 & \text{если } [n]_p = 0 \text{ в } \mathbb{F}_p \\ 1 & \text{если } [n]_p \in \mathbb{F}_p^2 \smallsetminus 0 \\ -1 & \text{если } [n]_p \notin \mathbb{F}_p^2 \end{cases}$

Персональный табель ______________________________.
(напишите свои имя, отчество и фамилию)

Листок № 13 (14 апреля 2015)

№	дата сдачи	имя и фамилия принявшего	подпись принявшего
1			
2			
3а			
б			
в			
4			
5а			
б			
в			
г			
д			
6			
7			
8			
9а			
б			
в			
10			
11			
12а			
б			
в			
г			
д			
13			
14а			
б			
15			