Соответствие Галуа.

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

A13◇1. Всегда ли в конечном расширении Галуа $\mathbb{F} \supset \Bbbk$ есть элемент, орбита которого под действием группы Галуа $\operatorname{Gal} \mathbb{F}/\Bbbk$ является базисом векторного пространства $\mathbb{F}$ над $\Bbbk$?

A13◇2. Пусть $f \in \Bbbk[x]$ неприводим, и $\operatorname{char} \Bbbk \neq 2$. Равносильно ли условие $D(f) \in \Bbbk^2$ тому, что группа $\operatorname{Gal} f/\Bbbk$ осуществляет лишь чётные перестановки корней f?

A13◇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 $\mathbb{Q}$.

A13◇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 $\mathbb{Q}$.

A13◇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.

A13◇6. Предъявите угол, который нельзя разбить на три равных угла циркулем и линейкой.

A13◇7. Найдите группу Галуа над $\mathbb{Q}$ многочлена $x^4 + 2x^2 + x + 3$.

A13◇8. Предъявите неприводимый $f \in \mathbb{Z}[x]$ степени 6 с $\operatorname{Gal} f/\mathbb{Q} \simeq S_6$.

A13◇9. Выразите **а)** $\sqrt[5]{1}$ **б)** $\sqrt[17]{1}$ через квадратные корни, а **в)** $\sqrt{13}$ через $\sqrt[13]{1}$

A13◇10. Для простого $p > 2$ и $\mathbb{F} = \mathbb{Q}[\sqrt[p]{1}]$ покажите, что $G = \operatorname{Gal} \mathbb{F}/\mathbb{Q}$ содержит единственную подгруппу индекса 2 и опишите отвечающее ей квадратичное расширение поля $\mathbb{Q}$.

A13◇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 $\mathbb{A}^1(\mathbb{F}_p)$.

A13◇12 (квадратичная взаимность). Для простых $p, q > 2$ положим $\mathbb{K} = \mathbb{Q}[x]/(x^2 - q^*)$, где $q^* \stackrel{\text{def}}{=} (-1)^{(q-1)/2} q$, обозначим через $\mathcal{O} \subset \mathbb{K}$ кольцо целых, а через $[z]_p$ — класс z в $\mathcal{O}/(p)$.

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) Опишите кольцо $\mathcal{O}/(p)$ и действие на нём F_p, когда $[q^*]_p \notin \mathbb{F}_p^2$.

в) Постройте такое вложение $\mathbb{Q}$-алгебры $\mathbb{K}$ в подполе $\mathbb{Q}[\sqrt[q]{1}] \subset \mathbb{C}$, чтобы эндоморфизм $z \mapsto z^p$ мультипликативной группы $\mathbb{C}^*$ корректно ограничивался на $\mathcal{O} \subset \mathbb{K} \subset \mathbb{Q}[\sqrt[q]{1}]$ и приводился по модулю (p) в эндоморфизм Фробениуса $F_p : \mathcal{O}/(p) \to \mathcal{O}/(p)$.

г) Получите явное выражение $\sqrt{q^*}$ через корни q-той степени из единицы и выясните, как действует на него F_p.

д) Докажите *квадратичный закон взаимности*[1]: $[p/q] \cdot [q/p] = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

A13◇13. Постройте циркулем и линейкой правильный 17-угольник.

A13◇14. Покажите, что **а)** $\mathbb{Q}[\sqrt{p}] \subset \mathbb{Q}[\sqrt[4p]{1}]$ при простом $p \equiv 3 \pmod 4$ **б)** любое квадратичное расширение поля $\mathbb{Q}$ содержится в некотором круговом поле $\mathbb{Q}[\sqrt[m]{1}] \subset \mathbb{C}$.

A13◇15. Верно ли, что $\operatorname{Aut}_{\Bbbk} \Bbbk(t) \simeq \mathrm{PGL}_2(\Bbbk)$?

---

[1] Напомню, что *символ Лежандра–Якоби* $[p/q] \stackrel{\text{def}}{=} \begin{cases} 0 & \text{если } [n]_p = 0 \text{ в } \mathbb{F}_p \\ 1 & \text{если } [n]_p \in \mathbb{F}_p^2 \smallsetminus 0 \\ -1 & \text{если } [n]_p \notin \mathbb{F}_p^2. \end{cases}$