Расширения полей

A$7\frac{1}{2}$◇1° (поле разложения). Пусть k — поле и $f \in k[x]$. Поле $K_f \supset k$ называется *полем разложения* многочлена f, если f полностью раскладывается в $K_f[x]$ на линейные множители, и для любого расширения $K \supset k$, над которым f полностью раскладывается на линейные множители, существует вложение $K_f \hookrightarrow K$, тождественное на k. Покажите, что у любого неприводимого многочлена имеется единственное с точностью до тождественного на k изоморфизма поле разложения.

Терминология. Расширение полей $K \supset k$ называется *конечным*, если $\dim_k K < \infty$, и *алгебраическим*, если каждый элемент K является корнем какого-нибудь многочлена из $k[x]$. Расширение вида $K = k[x]/(f)$ называется *примитивным*, и класс $\vartheta = x \pmod{f} \in K$ называется *примитивным элементом* поля K над k. Расширение $K \supset k$ называется *нормальным*, если всякий многочлен из $k[x]$, имеющий корень в K, полностью разлагается в $K[x]$ на линейные множители. Алгебраический над k элемент называется *сепарабельным*, если его минимальный многочлен не имеет кратных корней ни в каком расширении поля k. Алгебраическое расширение, в котором все элементы сепарабельны, называется сепарабельным. Конечные нормальные сепарабельные расширения называются *расширениями Галуа*.

A$7\frac{1}{2}$◇2°. Докажите, что всякая конечная мультипликативная подгруппа любого поля является циклической, и найдите степень минимального многочлена для образующей полной мультипликативной группы поля $\mathbb{F}_{p^n}$.

A$7\frac{1}{2}$◇3. Всякое ли конечное поле является **а)** примитивным **б)** нормальным расширением своего простого подполя?

A$7\frac{1}{2}$◇4. Каков порядок группы автоморфизмов конечного поля $\mathbb{F}_{p^n}$? Порождается ли она автоморфизмом Фробениуса?

A$7\frac{1}{2}$◇5. Приведите пример несепарабельного расширения полей. Бывают ли несепарабельные алгебраические расширения у поля характеристики нуль?

A$7\frac{1}{2}$◇6. Укажите какие-нибудь примитивные над $\mathbb{Q}$ элементы для полей $\mathbb{Q}(\sqrt{2},\sqrt{3})$ и $\mathbb{Q}(\sqrt{2},\sqrt[3]{2})$.

A$7\frac{1}{2}$◇7 (лемма о примитивном элементе). Пусть поле k бесконечно, а поле K порождается над k двумя алгебраическими элементами α, β, причём α сепарабелен. Докажите, что $\alpha + t\beta$ является при подходящем $t \in k$ примитивным элементом поля K над k.

A$7\frac{1}{2}$◇8. Нормальны ли над $\mathbb{Q}$ поля **а)** $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ **б)** $\mathbb{Q}(\sqrt[3]{2})$.

A$7\frac{1}{2}$◇9. Нормально ли над k поле разложения неприводимого многочлена из $k[x]$?

A$7\frac{1}{2}$◇10. В расширении полей $K \supset F \supset k$ поле K нормально над k. Нормально ли K над F?

A$7\frac{1}{2}$◇11. Пусть G – конечная группа автоморфизмов поля K. Проверьте, что её неподвижные точки $K^G \stackrel{\text{def}}{=} \{\vartheta \in K \mid g\vartheta = \vartheta \ \forall g \in G\}$ образуют поле. Нормально ли K над K^G?

A$7\frac{1}{2}$◇12 (расширения Галуа). Пусть $K \supset k$ — конечное сепарабельное расширение полей, и G — группа автоморфизмов поля K, тождественных на k. Может ли $|G|$ превышать $\dim_k K$? Как связаны между собою условия: **а)** $k = K^G$ **б)** $|G| = \dim_k K$ **в)** K нормально над k?

A$7\frac{1}{2}$◇13 (целые алгебраические числа). Элементы конечного расширения $K \supset \mathbb{Q}$, целые над $\mathbb{Z}$, называются *целыми алгебраическими числами*. Покажите, что:

а) целые алгебраические числа образуют кольцо, являющееся одновременно свободным $\mathbb{Z}$-модулем конечного ранга;

б) некоторое целочисленное кратное любого $a \in K$ является целым алгебраическим числом;

в) существует базис K над $\mathbb{Q}$, состоящий из целых алгебраических чисел.

A$7\frac{1}{2}$◇14. Опишите кольца всех целых алгебраически чисел в полях:

а) $\mathbb{Q}[\sqrt{2}]$ **б)** $\mathbb{Q}[\sqrt{3}]$ **в)** $\mathbb{Q}[\sqrt{5}]$ **г)** $\mathbb{Q}[\sqrt{-1}]$ **д)** $\mathbb{Q}[\sqrt{-3}]$ **е)** $\mathbb{Q}[\sqrt{-5}]$