Кольца целых и разложение на простые множители.

Задача 1°. Найдите кольцо целых в расширении, полученном присоединением корня следующего многочлена. Какие дискриминанты имеют соответствующие поля?
a) x^3-2; b) x^3-10; c) $x^3-12x+2$; d) x^4+2x^2+3x+1; e) x^5-x-1.

Задача 2°. Как устроено разложение на простые идеалы простых элементов из $\mathbb{Z}$ для каждого из полей в задаче 1.

Задача 3. *a°*) Найдите базис кольца целых и дискриминант $\mathbb{Q}(i,\sqrt{5})$ над $\mathbb{Q}(i)$ и над $\mathbb{Q}$.
b°) Найдите $\mathbb{Z}[i]$-базис кольца целых и дискриминант над $\mathbb{Q}$ расширения $\mathbb{Q}(i,\sqrt{d})$ для целого $d\neq\pm1$, свободного от квадратов.
c) Покажите, что дискриминант расширения Галуа $\mathbb{Q}$ степени 4 с группой Галуа $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ является полным квадратом.
Подсказка: когда группа Галуа поля разложения многочлена вложена в A_n?

Задача 4. Пусть $K/\mathbb{Q}$ — конечное расширение. Определите кольцо целых расширения $K(\sqrt{\alpha})$, где $\alpha\in\mathcal{O}_K$ свободно от квадратов.

Задача 5. Опишите кольцо целых $\mathcal{O}_K$ поля разложения многочлена x^3-a при $a=2,\ 3,\ 5,\ 6$. Как разлагаются простые из $\mathbb{Z}$ в $\mathcal{O}_K$?

Задача 6. Пусть k — поле, $K=k(t)$ — поле рациональных функций от t, $L=K(\sqrt{f(t)})$, где $f(t)\in k[t]$ — приведенный неприводимый многочлен. Найдите целое замыкание $k[t]$ в L.

Задача 7. Пусть $K/\mathbb{Q}$ — конечное расширение, σ_i — его различные вложения в $\mathbb{C}$, $\alpha\in\mathcal{O}_K\setminus\{0\}$.
a) Покажите, что, если α не корень из единицы, то $|\sigma_i(\alpha)|>1$ для некоторого i.
b) Пусть $\alpha\in\mathbb{R}$. Покажите, что, если $\alpha\neq2\cos(r\pi)$, $r\in\mathbb{Q}$, то $|\sigma_i(\alpha)|>2$ для некоторого i.

Задача 8. Пусть $K/\mathbb{Q}$ — конечное расширение, $\sigma_1,\dots,\sigma_{r_1}$ — различные вещественные вложения K в $\mathbb{C}$, а $\sigma_{r_1+1},\bar\sigma_{r_1+1},\dots,\sigma_{r_1+r_2},\bar\sigma_{r_1+r_2}$ — различные пары комплексно сопряженных комплексных вложений K в $\mathbb{C}$. Определим отображение $\phi\colon K\to\mathbb{R}^n$ формулой:
$x\mapsto(\sigma_1(x),\dots,\sigma_{r_1}(x),\operatorname{Re}\sigma_{r_1+1}(x),\operatorname{Im}\sigma_{r_1+1}(x),\dots,\operatorname{Re}\sigma_{r_1+r_2}(x),\operatorname{Im}\sigma_{r_1+r_2}(x))$.
a°) Покажите, что для любого N найдется лишь конечное число таких элементов $\alpha\in\mathcal{O}_K$, что $|\sigma_i(\alpha)|\leq N$ для всех i.
b°) Убедитесь, что $\phi(\mathcal{O}_K)$ — решетка полного ранга в $\mathbb{R}^n$.
c) Докажите, что объем ее фундаментального параллелепипеда равен $2^{-r_2}\sqrt{|\mathrm{Disc}_{K/\mathbb{Q}}|}$.
d) Пусть $\mathfrak{a}\subset\mathcal{O}_K$ — идеал. Убедитесь, что $\phi(\mathfrak{a})$ — решетка и найдите объем ее фундаментального параллелепипеда.

Задача 9 (Теорема Брилля). Докажите, что для конечного расширения $K/\mathbb{Q}$ знак дискриминанта $\mathrm{Disc}_{K/\mathbb{Q}}$ равен числу пар комплексно сопряженных комплексных вложений K в $\mathbb{C}$ (т. е. таких, что их образ не лежит в $\mathbb{R}$).
Подсказка: если $\{\alpha_j\}_{j=1\dots n}$ — базис $K/\mathbb{Q}$, а $\{\sigma_i\}_{i=1\dots n}$ — различные вложения K в $\mathbb{C}$, то $\mathrm{Disc}(\alpha_1,\dots,\alpha_n)=\det(\sigma_i(\alpha_j))^2$.

Задача 10 (Теорема Штикельбергера). Покажите, что дискриминат конечного расширения $K/\mathbb{Q}$ сравним с 1 или 0 по модулю 4.
Подсказка: разбейте $\det(\sigma_i(\alpha_j))$ *в сумму по четным и нечетным перестановками.*

Задача 11° (Теорема Дедекинда). Пусть $K/\mathbb{Q}$ — конечное расширение, $\alpha\in\mathcal{O}_K$, индекс $[\mathcal{O}_K:\mathbb{Z}[\alpha]]$ конечен и $p\nmid[\mathcal{O}_K:\mathbb{Z}[\alpha]]$. Пусть $f(x)$ — минимальный многочлен α.
a) Покажите, что $\mathcal{O}_K/p\mathcal{O}_K\cong\mathbb{F}_p[x]/(\bar f(x))$, где $\bar f(x)\in\mathbb{F}_p[x]$ — редукция $f(x)$ по модулю p.

b) Докажите следующее обобщение теоремы Куммера. Пусть $\bar{f}(x) = \prod_i \bar{f}_i(x)^{e_i}$ — разложение $\bar{f}(x)$ на неприводимые множители в $\mathbb{F}_p[x]$, и $f_i(x)$ — любое поднятие $\bar{f}_i(x)$ до многочлена из $\mathbb{Z}[x]$. Тогда $p\mathcal{O}_K = \prod_i \mathfrak{p}_i^{e_i}$, где $\mathfrak{p}_i = (p, f_i(\alpha))$ — простые идеалы.

Задача 12. Пусть $K = \mathbb{Q}(\gamma)$, где $\gamma^3 - \gamma^2 - 2\gamma - 8 = 0$.

a) Убедитесь, что $1, \gamma, \gamma' = \frac{1+\gamma^2}{2}$ образуют базис $\mathcal{O}_K$.

b) Покажите, что для любого $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$, $2 \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. В частности, $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ для любого $\alpha \in K$.

Подсказка: вычислите определитель матрицы перехода от $1, \alpha, \alpha^2$ *к* $1, \gamma, \gamma'$.

Задача 13. a) Пусть $K/\mathbb{Q}$ — конечное расширение и идеал (p) имеет больше p простых сомножителей с нормой p в разложении в произведение простых идеалов в $\mathcal{O}_K$. Покажите, что $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ для любого $\alpha \in K$.

b) Пусть $K = \mathbb{Q}(\gamma)$, $\gamma^3 - 2\gamma^2 - 9\gamma + 2 = 0$. Найдите базис $\mathcal{O}_K$ и вычислите Disc_K.

c) Покажите, что $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, где $\mathfrak{p}_i \subset \mathcal{O}_K$ — простые идеалы. Таким образом $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$ для любого $\alpha \in K$. Как устроено разложение остальных простых из $\mathbb{Z}$ в $\mathcal{O}_K$?

Задача 14*. Докажите, что для любого n найдется конечное расширение $\mathbb{Q}$, кольцо целых которого не порождается n элементами (как кольцо над $\mathbb{Z}$).

Задача 15. Докажите, что кубическое поле K (т. е. $[K : \mathbb{Q}] = 3$) является чисто кубическим (т. е. $K = \mathbb{Q}(\sqrt[3]{m})$ тогда и только тогда, когда $D_K = -3d^2$, $d \in \mathbb{N}$.

Задача 16°. Пусть $f_1(x) = x^3 - x^2 - 20x - 1$, $f_2(x) = x^3 - x^2 - 34x - 24$, $f_3(x) = x^3 - x^2 - 52x + 159$, $f_4(x) = x^3 - 41x - 95$ и пусть $K_i/\mathbb{Q}$ — соответствующие раширения.

a) Покажите, что $\mathrm{Disc}_{K_i} = 32009$ для любого i.

b) Убедитесь, что K_i попарно не изоморфны.

Подсказка: Посмотрите на разложение простых в $\mathcal{O}_{K_i}$.

Задача 17. Пусть a, b, c, d — свободные от квадратов взаимно простые натуральные числа, большие единицы, одно из которых делится на 3.

a) Покажите, что поля $\mathbb{Q}(\sqrt[3]{abc^2d^2})$ и $\mathbb{Q}(\sqrt[3]{acb^2d^2})$ различны, но имеют один и тот же дискриминант $-27a^2b^2c^2d^2$.

b) Докажите, что для любого натурального n можно построить n различных чисто кубических полей с одним и тем же дискриминантом.

Задача 18. Пусть A — дедекиндово кольцо.

a) Докажите, что, если в A конечное число простых идеалов, то A — кольцо главных идеалов.

Подсказка: используйте китайскую теорему об остатках.

b) Покажите, что, если $0 \neq \mathfrak{a} \subset \mathfrak{b} \subset A$ — два идеала, то существует такой $a \in A$, что $\mathfrak{b} = \mathfrak{a} + (a)$. Выведите отсюда, что в дедекиндовом кольце всякий идеал может быть порожден двумя элементами.

c) Докажите, что для любого ненулевого идеала $\mathfrak{a} \subset A$ найдется такой идеал $\mathfrak{a}' \subset A$, что $\mathfrak{a}\mathfrak{a}' = (a)$ — главный. При этом можно наложить на $\mathfrak{a}'$ или a любое из ограничений (но не оба): $\mathfrak{a}'$ взаимно прост с заданным идеалом $\mathfrak{b}$ или a — любой заданный элемент из $\mathfrak{a}$.

d) Покажите, что дедекиндова область с однозначным разложением на простые множители является кольцом главных идеалов.

Задача 19 (Евклидовы кольца). Кольцо $\mathcal{O}_K$ назвается евклидовым относительно функции $f : \mathcal{O}_K \to \mathbb{N}$, если $f(x) = 0$ тогда и только тогда, когда $x = 0$, и для всех $\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ существует такое $\gamma \in \mathcal{O}_K$, что $f(\alpha - \gamma\beta) < f(\beta)$.

a°) Покажите, что, если $\mathcal{O}_K$ — евклидово, то оно является кольцом главных идеалов.
На самом деле „почти известно“, что „почти“ верно обратное: в предположении обобщенной гипотезы Римана кольцо $\mathcal{O}_K$ для K, не являющегося мнимым квадратичным, евклидово тогда и только тогда, когда оно является кольцом главных идеалов.

b) Покажите, что для евклидова кольца функцию f можно выбрать удовлетворяющей неравенству $f(a) \leq f(ab)$ для всех ненулевых a и b.
Подсказка: замените произвольную функцию f на $g(x) = \min\limits_{a \in \mathcal{O}_K \setminus \{0\}} f(ax)$.

c) Назовем $\mathcal{O}_K$ почти евклидовым относительно функции $f : \mathcal{O}_K \to \mathbb{N}$, если $f(x) = 0$ тогда и только тогда, когда $x = 0$, и для всех $\alpha, \beta \in \mathcal{O}_K$, $\beta \nmid \alpha$ существуют такие $\gamma, \delta \in \mathcal{O}_K$, что $0 < f(\alpha\gamma - \beta\delta) < f(\beta)$. Докажите, что $\mathcal{O}_K$ почти евклидово тогда и только тогда, когда оно является кольцом главных идеалов.
Подсказка: в кольце главных идеалов качестве f можно взять $f(x) = 2^{n_1 + \dots + n_m}$, где $x = \epsilon p_1^{n_1} \dots p_m^{n_m}$ — разложение на простые, $\epsilon \in \mathcal{O}_K^\times$.

d) Пусть d — целое отрицательное число, свободное от квадратов, $K = \mathbb{Q}(\sqrt{d})$. Докажите, что кольцо $\mathcal{O}_K$ является евклидовым относительно $f(x) = \mathrm{N}_{K/\mathbb{Q}}(x) = x \cdot \bar{x}$ тогда и только тогда, когда сдвиги единичного круга на вектора решетки $\mathcal{O}_K$ покрывают все $\mathbb{C}$.

e) Убедитесь, что условие предыдущего пункта выполнено в том и только в том случае, когда $d \in \{-1, -2, -3, -7, -11\}$.

f^*) Покажите для значений d, не принадлежащих этому списку, $\mathcal{O}_K$ не является евклидовым ни для какой функции $f(x)$.

g) Является ли кольцо целых поля $\mathbb{Q}(\sqrt{2})$ евклидовым относительно $\mathrm{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(x)$?

h^*) Покажите, что кольцо целых поля $\mathbb{Q}(\sqrt{47})$ является кольцом главных идеалов, но не является евклидовым относительно $\mathrm{N}_{\mathbb{Q}(\sqrt{47})/\mathbb{Q}}(x)$.
Для квадратичных полей известен полный список колец $\mathcal{O}_K$, являющихся евклидовыми относительно нормы. В случае произвольных расширений $\mathbb{Q}$ такое описание неизвестно.

Задача 20°. Пусть ω — примитивный корень степени три из единицы.

a) Опишите разложение простых из $\mathbb{Z}$ в $\mathbb{Q}(\omega)$.

b) Покажите, что $\mathbb{Q}(\omega)$ является кольцом главных идеалов.

c) Докажите, что простое $p \in \mathbb{Z}$ имеет вид $p = x^2 + xy + y^2$, $x, y \in \mathbb{Z}$ тогда и только тогда, когда $p \equiv 1 \mod 3$.

Задача 21. Сколько решений в зависимости от n имеют уравнения $x^2 - dy^2 = n$ для каждого из $d \in \{-1, -2, -3, -7, -11\}$.

Задача 22. Покажите, что уравнение $x^4 + 2y^4 = 17z^4$ имеет только тривиальное решение в $\mathbb{Q}$.
Подсказка: используйте однозначность разложения на простые в $\mathbb{Z}[\sqrt{-2}]$.

Задача 23. Пусть $K/\mathbb{Q}$ — конечное расширение и число классов идеалов $\mathcal{O}_K$ равно 2.

a) Предположим, что элемент p неразложим в $\mathcal{O}_K$ и идеал (p) не является простым. Покажите, что $(p) = \mathfrak{p}\mathfrak{p}'$, где $\mathfrak{p}$, $\mathfrak{p}'$ — простые идеалы в $\mathcal{O}_K$ (не обязательно различные).

b) Пусть $a = p_1 \dots p_m = q_1 \dots q_n$ два разложения $a \in \mathcal{O}_K$ в произведение неразложимых элементов. Покажите, что $m = n$.

Задача 24. Для идеал $\mathfrak{a} \subset \mathcal{O}_K$ обозначим через $\varphi(\mathfrak{a})$ число классов вычетов $\bar{\alpha} \in \mathcal{O}_K/\mathfrak{a}$, взаимно простых с $\mathfrak{a}$ (т. е. $\mathfrak{a} + (\alpha) = \mathcal{O}_K$). Покажите, что

a) если $\mathfrak{a}$ и $\mathfrak{b}$ взаимно просты, то $\varphi(\mathfrak{a}\mathfrak{b}) = \varphi(\mathfrak{a})\varphi(\mathfrak{b})$;

b) $\varphi(\mathfrak{a}) = \mathrm{N}(\mathfrak{a}) \prod\limits_{\mathfrak{p}} \left(1 - \frac{1}{\mathrm{N}\mathfrak{p}}\right)$, где $\mathfrak{p}$ пробегает простые идеалы, делящие $\mathfrak{a}$;

c) (обобщение малой теоремы Ферма) если $\mathfrak{p}$ — простой идеал, $\alpha \in \mathcal{O}_K$, то $\alpha^{\mathrm{N}\mathfrak{p}} - \alpha \in \mathfrak{p}$;

d) (обобщение теоремы Эйлера) если $\alpha \in \mathcal{O}_K$ взаимно просто с $\mathfrak{a}$, то $\alpha^{\varphi(\mathfrak{a})} - 1 \in \mathfrak{a}$;

e) (обобщение теоремы Вильсона) если $\mathfrak{p}$ — простой идеал, а $\alpha_1, \ldots, \alpha_s \in \mathcal{O}_K$ — полная система представителей $(\mathcal{O}_K/\mathfrak{p}) \setminus \{0\}$, то $\alpha_1 \ldots \alpha_s + 1 \in \mathfrak{p}$.

Задача 25. Пусть $K/\mathbb{Q}$ — расширение Галуа, в котором простой идеал $(p) \subset \mathbb{Z}$ остается простым. Покажите, что группа $\mathrm{Gal}(K/\mathbb{Q})$ является циклической.

Задача 26*. Пусть $K/\mathbb{Q}$ — конечное расширение, содержащее примитивный корень степени n из единицы, $E = K(\sqrt[n]{a})$, где $a \neq b^m$, $b \in K$ для $m \mid n$.

a) Покажите, что дискриминант $D_{E/K} \mid n^n a^{n-1}$.

b) Предположим, что простой идеал $\mathfrak{p} \subset O_K$ неразветвлен в $\mathcal{O}_E$ (т. е. $\mathfrak{p} \nmid na$). Покажите, что степень поля классов вычетов $\mathfrak{p}$ равна f, где f — такое наименьшее натуральное число, что сравнение $x^n \equiv a^f \mod \mathfrak{p}$ разрешимо.

c) Покажите, что, если $\mathfrak{p}^r \mid a$, $\mathfrak{p}^{r+1} \nmid a$, $\mathfrak{p} \nmid n$, где $2 \leq r \leq n-1$, то индекс ветвления идеала $\mathfrak{p}$ равен $n/(r,n)$.

Задача 27*. Покажите, что следующие условия на целостное кольцо A эквивалентны:

a) A — дедекиндово;

b) дробные идеалы в A обратимы;

c) A — нётерово и для всякого ненулевого простого идеала $\mathfrak{p} \subset A$ кольцо $A_{\mathfrak{p}}$ является кольцом дискретного нормирования.