3. Теория Галуа и теория чисел

3.1. Найти факторкольцо $\mathbb{R}[x]/(x^2+ax+b)$ в зависимости от $a, b \in \mathbb{R}$.

3.2. Выполнить действия в кольце $\mathbb{Q}[x]/(f(x))$:

а) $(\xi^2+\xi+1)^3$, $f(x)=x^3-1$.

б) $\frac{1}{(1+\xi)^m}$, $f(x)=x^n$.

(Здесь $\xi = x + (f(x))$.)

3.3. Найти степени расширений и их группы автоморфизмов над $\mathbb{Q}$: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, $\mathbb{Q}(\sqrt{2}+\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(\sqrt{\sqrt{2}+\sqrt{-2}})$, $\mathbb{Q}(\sqrt{6+3\sqrt{3}})$. Какие из них являются расширениями Галуа?

3.4. Доказать, что $\cos(\pi/11)$ — алгебраическое число. Будет ли нормальным расширение $\mathbb{Q}(\cos(\pi/11))/\mathbb{Q}$? Найти его степень и группу автоморфизмов.

3.5. Найти степени расширений $\mathbb{F}_p(\sqrt{2})$, $\mathbb{F}_p(\sqrt{3})$.

3.6. Найти степени расширений $\mathbb{F}_p(\zeta_m)$, где ζ_m — примитивный корень из единицы степени m.

3.7. Найти степени и группы автоморфизмов расширений

$$\mathbb{C}(\sqrt{1-\sqrt{z}})/\mathbb{C}(z), \qquad \mathbb{C}(\sqrt{z+\sqrt{z}})/\mathbb{C}(z).$$

Являются ли они расширениями Галуа?

3.8. Найти $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$.

3.9. Доказать, что число $\cos 15^\circ$ является целым алгебраическим. Указать 10 неизоморфных конечных полей, содержащих это число.

3.10. Существуют ли конечные расширения полей $\mathbb{F}_p$, $\mathbb{Q}$, не содержащие никаких собственных подполей, кроме простых?

3.11. Найти группы Галуа следующих многочленов над $\mathbb{Q}$:

а) x^2-2, б) x^4+2, в) $(x^2-2)(x^2-3)(x^2-5)$,

г) x^3-2, д) x^3+px+q в зависимости от p и q.

3.12. Используя ряд коммутантов групп S_3 и S_4, доказать, что уравнения степеней 3 и 4 разрешимы в радикалах.

3.13. Доказать, что правильный n-угольник строится циркулем и линейкой тогда и только тогда, когда $n = 2^m p_1 \dots p_s$, где p_i — различные простые числа вида $2^{2^k}+1$.

3.14. Описать все расширения Галуа поля $\mathbb{Q}$ с группами Галуа Z_2, $Z_2 \oplus Z_2$.

3.15. Построить расширения Галуа поля $\mathbb{Q}$ с каждой из групп порядка 8 (Z_8, $Z_4 \oplus Z_2$, $Z_2 \oplus Z_2 \oplus Z_2$, D_4, Q_8).

3.16. Описать кольцо целых поля $\mathbb{Q}(\sqrt{3}+\sqrt{7})$.

3.17. Элемент p целостного кольца A называется *простым*, если из $d \mid p$ следует, что либо d есть обратимый элемент кольца A, либо d ассоциирован с p. Доказать, что в евклидовом кольце элемент p прост тогда и только тогда, когда прост порожденный им идеал (p).

3.18. Однозначно ли разложение на простые множители в кольцах $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[\sqrt{7}]$? Какие из них являются евклидовыми?

3.19. Описать $\operatorname{Spec}\mathbb{Z}$, $\operatorname{Spec}\mathbb{Z}[i]$, $\operatorname{Spec}\mathbb{Z}[\sqrt{-5}]$, $\operatorname{Spec}\mathbb{Z}[x]$.

3.20. (Гауссовы целые числа.) Пусть $\Gamma = \mathbb{Z}[\sqrt{-1}]$.

а) Показать, что Γ — евклидово кольцо.

б) Описать все простые элементы Γ.

в) Пусть $\Pi = \operatorname{Spec}\Gamma - \{0\}$. Выразить ζ-функцию кольца Γ:

$$\zeta_\Gamma(s) = \prod_{\mathfrak{p}\in\Pi}\Big(1 - \frac{1}{N(\mathfrak{p})^s}\Big)^{-1}$$

через *ζ-функцию Римана*

$$\zeta_Z(s) = \prod_{p \text{ простое}}\left(1 - \frac{1}{p^s}\right)^{-1}$$

и *L-ряд*

$$L(s,\chi) = \prod_{p \text{ простое}}\left(1 - \frac{\chi(p)}{p^s}\right)^{-1},$$

где $\chi\colon Z \to \mathbb{C}^\times$ — *характер Дирихле* по модулю 4, т.е.

$$\chi(m) = \begin{cases} 0 & \text{при } m \equiv 0 \pmod 4, \\ 1 & \text{при } m \equiv 1 \pmod 4, \\ -1 & \text{при } m \equiv 3 \pmod 4. \end{cases}$$

Норма идеала $N(\mathfrak{p})$ — это количество элементов факторкольца $\Gamma/\mathfrak{p}$. Предварительно показать, что $N(\mathfrak{p}\mathfrak{q}) = N(\mathfrak{p})N(\mathfrak{q})$.

г) Показать, что в ряде Дирихле

$$\zeta_\Gamma(s) = \sum_{n\geqslant 1}\frac{a_n}{n^s}$$

число a_n есть количество представлений числа n в виде суммы двух квадратов, т.е. пар (x,y) целых неотрицательных чисел с $x^2+y^2=n$.

д) Сравнив результаты в) и г), получить, что

$$a_n = \begin{pmatrix}\text{количество делителей } n \\ \text{вида } 4k+1\end{pmatrix} - \begin{pmatrix}\text{количество делителей } n \\ \text{вида } 4k+3\end{pmatrix}.$$

3.21. а) Доказать, что имеют место включения

$$\left\{\begin{matrix}\text{евклидовы}\\ \text{кольца}\end{matrix}\right\} \subset \left\{\begin{matrix}\text{кольца}\\ \text{главных}\\ \text{идеалов}\end{matrix}\right\} \subset \left\{\begin{matrix}\text{факториальные}\\ \text{кольца}\end{matrix}\right\}.$$

б) Привести примеры, показывающие, что эти включения строгие.

3.22. а) Пусть $K = k(\alpha_1, \ldots, \alpha_n)$ — алгебраическое расширение поля k характеристики 0. Показать, что существует элемент $\theta \in K$, для которого $K = k(\theta)$ (теорема о примитивном элементе).

б) Верно ли аналогичное утверждение для кольца $A = \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$, порожденного целыми алгебраическими числами $\alpha_1, \ldots, \alpha_n$?

3.23. Доказать, что группа Галуа многочлена $x^5 - 4x + 2$ изоморфна S_5.

3.24. (Круговые поля.) Пусть $\zeta_m = e^{2\pi i/m}$ и $K_m = \mathbb{Q}(\zeta_m)$.

а) Доказать неприводимость многочлена $x^{p-1} + x^{p-2} + \cdots + 1$ для простого p.

б) Пусть

$$\Phi_m(x) = \prod_{\zeta}(x - \zeta),$$

где произведение берется по всем примитивным корням из 1 степени m. Доказать, что $\Phi_m(x) \in \mathbb{Z}[x]$.

в) Доказать, что многочлен $\Phi_m(x)$ неприводим при любом m. Найти степень расширения $K_m/\mathbb{Q}$.

г) Найти $\mathrm{Gal}(K_m/\mathbb{Q})$.

3.25. Доказать, что всякая конечная абелева группа может быть реализована как группа Галуа некоторого расширения поля $\mathbb{Q}$, содержащегося в K_m.

3.26. (Квадратичный закон взаимности.)

а) В круговом поле K_p с нечетным простым p существует единственное подполе степени 2 над $\mathbb{Q}$.

б) Из соотношения

$$p = \prod_{i=1}^{p-1}(1 - \zeta_p^i)$$

вывести, что $(-1)^{\frac{p-1}{2}} = g^2$ для некоторого $g \in K_p$.

в) Используя лемму Гаусса о том, что $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$, получить закон взаимности

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

для нечетных различных простых p и q.

г) Доказать, что

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

для нечетного простого p.

3.27. (Суммы Гаусса и снова квадратичный закон взаимности.) Пусть $g_a = \sum\limits_{x \in Z_p^\times} \left(\frac{x}{p}\right) \zeta_p^{ax}, \; a \in Z_p^\times$.

а) Доказать, что $g_a = \left(\frac{a}{p}\right) g_1$.

б) Вычислив двумя способами сумму $S = \sum_a g_a g_{-a}$, установить, что

$$p(p-1) = S = \left(\frac{-1}{p}\right)(p-1) g_1^2.$$

в) Из п. б) и леммы Гаусса получить квадратичный закон взаимности.

3.28. Найти количество решений сравнения $x^2 + y^2 \equiv z^2 \pmod{p}$.

3.29. Плотно ли в $\mathbb{C}$ множество всех целых алгебраических чисел?

3.30. Пусть $\bar{\mathbb{Q}}$ — алгебраическое замыкание поля $\mathbb{Q}$ и k — максимальное по включению подполе $\bar{\mathbb{Q}}$, не содержащее $\sqrt{5}$. Доказать, что группа Галуа $\mathrm{Gal}(K/k)$ циклическая для любого конечного расширения K поля k.

3.31. Пусть $\bar{k}$ — алгебраическое замыкание поля k характеристики 0, σ — автоморфизм поля $\bar{k}$ и $L = \{ x \in \bar{k} \mid \sigma x = x \}$. Доказать, что если $k \subset L$, то группа $\mathrm{Gal}(P/L)$ циклическая для любого конечного расширения P поля L.

3.32. Доказать, что конечное расширение конечного поля всегда сепарабельно. То же верно и для конечного расширения поля характеристики 0.

3.33. Пусть K — поле характеристики p, L/K — конечное нормальное расширение, $G = \mathrm{Gal}(L/K)$, $L_0 = L^G$ — подполе G-инвариантных элементов. Докажите, что L/L_0 есть расширение Галуа, а L_0/K — чисто несепарабельное расширение (т. е. для любого $\alpha \in L_0$ найдется такое m, что $\alpha^{p^m} \in K$).

3.34. Доказать, что всякое конечное поле совершенно.

3.35. Пусть $F = K(\alpha)$ и $\mu(x)$ — минимальный многочлен α над K. Доказать, что $L \otimes_K F \cong L[x]/(\mu(x))$.

3.36. Пусть $K/\mathbb{Q}$ — конечное расширение, причем его кольцо целых $\mathcal{O}_K$ имеет вид $\mathbb{Z}[\theta]$, и $\mu(x)$ — минимальный многочлен θ. Доказать, что простые идеалы $P_1, \ldots, P_k$ в $\mathcal{O}_K$, участвующие в разложении $(p) = P_1 \ldots P_k$ для простого числа $p \in \mathbb{Z}$, имеют вид $P_i = (p, \mu_i(\theta))$, где

$\mu(x) \equiv \mu_1(x) \dots \mu_k(x) \pmod p$ — разложение на неприводимые множители по модулю p.

3.37. Найти число классов полей $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-5})$.

3.38. Пусть $x \in \mathbb{Z}_p^\times$. Доказать, что ряд

$$x + (x^p - x) + (x^{p^2} - x^p) + \cdots$$

сходится, и что его сумма есть $\bar{x} = \lim\limits_{n\to\infty} x^{p^n}$. Вывести отсюда, что уравнение $x^{p-1} - 1$ имеет $p-1$ корень в $\mathbb{Z}_p$.

3.39. Вычислить группу непрерывных автоморфизмов поля p-адических чисел $\mathbb{Q}_p$.

3.40. Доказать, что p-адическая запись числа $a^{p^{k-1}(p-1)}$ начинается k нулями для любого $a \in \mathbb{Z}_p$.

3.41. Какие из чисел 5, -7, $3 \cdot 11^{-2} + 6 \cdot 11^{-1} + 3 + 7 \cdot 11^2$ имеют квадратные корни в $\mathbb{Q}_{11}$? Вычислить эти корни с точностью до 11^{-3}.

3.42. Доказать, что p-адическое разложение рационального числа периодично. Верно ли обратное?

3.43. Доказать, что

$$|a|_\infty \prod_p |a|_p = 1$$

для всех $a \in \mathbb{Q}^\times$. (Здесь $|a|_\infty = |a|$ и $|a|_p = p^{-v_p(a)}$.)

3.44. Доказать, что

$$v_p(n!) = \left[\frac{n - \sigma_p(n)}{p-1}\right],$$

где $\sigma_p(n)$ есть сумма коэффициентов в p-адическом разложении числа n.

3.45. Доказать, что $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \oplus \mathbb{Z}_b$, если $(a,b) = 1$.

3.46. Найти степени расширений $\mathbb{Q}_p(\sqrt{-1})/\mathbb{Q}_p$, $\mathbb{Q}_p(\sqrt{3})/\mathbb{Q}_p$.

3.47. Найти степени расширений $\mathbb{Q}_p(\zeta_m)$, где ζ_m — примитивный корень из единицы степени m.

3.48. Найти радиус сходимости ряда $\exp(x)$ в $\mathbb{Q}_p$.

3.49. Вычислить с точностью до 10^{-3} корни уравнения $x^2 - 2x + 2 = 0$ в $\mathbb{Z}_5$.

3.50. Докажите, что нормы $|\cdot|_p$ и $|\cdot|_q$ при разных p и q задают неэквивалентные топологии на $\mathbb{Q}$. Ни одна норма $|\cdot|_p$ не задает на $\mathbb{Q}$ топологии, эквивалентной обычной топологии, задаваемой абсолютной величиной.