ВОПРОСЫ К ЗАЧЁТУ ПО КУРСУ «АЛГЕБРАИЧЕСКИЕ ЧИСЛА»

Е. А. Уланский, 2012 г.

1. Простые расширения. Степень расширения. Поведение степени в башнях расширений.

2. Теорема об эквивалентности конечности и конечной порожденности алгебраических расширений и ее следствия.

3. Алгебраическая замкнутость поля всех алгебраических чисел.

4. Теорема о примитивном элементе.

5. Доказательство теоремы о примитивном элементе в конечных полях. Структура конечных полей.

6. Лемма о продолжении вложений и ее следствия.

7. Нормальные расширения. Эквивалентность различных определений.

8. Характеристический многочлен числа, его связь с минимальным многочленом. Норма и след в алгебраических расширениях, их свойства.

9. Дискриминант совокупности чисел, его свойства. Взаимный базис.

10. Лемма о дискретных подгруппах в $\mathbb{R}^n$.

11. Теорема о том, что множество целых алгебраических чисел произвольного поля алгебраических чисел есть порядок.

12. Теоремы Блихфельда и Минковского.

13. Существование в полном модуле чисел с заданными ограничениями на величину их сопряженных.

14. Теорема Дирихле о единицах. Гомоморфизм группы единиц в $\mathbb{R}^{s+t}$. Структура образа и ядра этого отображения.

15. Конструкция $s + t - 1$ независимых единиц.

16. Максимальность простых идеалов. Свойство обрывания возрастающих цепочек идеалов.

17. Дробные идеалы. Доказательство равенства $M \cdot M^{-1} = \mathbb{Z}_K$.

18. Теорема о существовании и единственности разложения идеалов в произведение простых.

19. Показатели и их свойства.

20. Норма идеала. Мультипликативность нормы.

21. Норма главного идеала.

22. Конечность группы классов идеалов.

23. Разложение целых рациональных чисел в $\mathbb{Z}_K$. Теорема Куммера.

24. Конечность множества разветвленных простых чисел.

25. Теорема о делимости дискриминантов (условие Эйзенштейна).

Для получения зачёта необходимо правильно решить не менее четырёх из пяти предложенных задач и показать полное владение теоретическим материалом курса

ЗАДАЧИ К ЗАЧЁТУ ПО КУРСУ «АЛГЕБРАИЧЕСКИЕ ЧИСЛА»

Е. А. Уланский, 2012 г.

1. Вычислить $\Sigma = \sum_{k=0}^{6} \left(\frac{k}{7}\right) e^{\frac{2\pi i}{7}k}$, где $\left(\frac{k}{p}\right)$ – символ Лежандра.

РЕШЕНИЕ:

$$\Sigma^2 = \sum_{k=1}^{6} \left(\frac{k}{7}\right) e^{\frac{2\pi i}{7}k} \sum_{l=1}^{6} \left(\frac{l}{7}\right) e^{\frac{2\pi i}{7}l}.$$

Заменим во внутренней сумме l на lk. Это не изменит результата суммирования, так как lk вместе с l пробегает приведённую систему вычетов по модулю 7, а символ Лежандра и экспонента периодичны с периодом 7. Имеем

$$\Sigma^2 = \sum_{k=1}^{6} \left(\frac{k}{7}\right) e^{\frac{2\pi i}{7}k} \sum_{l=1}^{6} \left(\frac{lk}{7}\right) e^{\frac{2\pi i}{7}lk} = \sum_{l=1}^{6} \left(\frac{l}{7}\right) \sum_{k=1}^{6} e^{\frac{2\pi i(l+1)}{7}k} = 6\left(\frac{6}{7}\right) - \sum_{l=1}^{5} \left(\frac{l}{7}\right) = 7\left(\frac{6}{7}\right) = -7.$$

Здесь использовалось, что все степени от 1 до 6 числа $e^{\frac{2\pi i}{7}}$ есть корни многочлена $x^6 + \ldots + x + 1$. Значит, $\Sigma = \pm i\sqrt{7}$. Чтобы определиться со знаком, запишем явно

$$\Sigma = e^{\frac{2\pi i}{7}} + e^{\frac{2\pi i}{7}2} + e^{\frac{2\pi i}{7}4} - e^{\frac{2\pi i}{7}3} - e^{\frac{2\pi i}{7}5} - e^{\frac{2\pi i}{7}6} = 2i\left(\sin\left(\frac{2\pi}{7}\right) + \sin\left(\frac{4\pi}{7}\right) - \sin\left(\frac{6\pi}{7}\right)\right).$$

Выражение в скобках, очевидно, положительно.

ОТВЕТ: $\Sigma = i\sqrt{7}$.

2. Разложить на неприводимые над $\mathbb{Q}$ множители многочлен $x^{56} - 1$.

РЕШЕНИЕ:

Мы знаем, что $x^n - 1 = \prod_{d|n} \Phi_d(x)$, где $\Phi_d(x)$ – многочлен деления круга, как известно, неприводимый. Имеем $56 = 2^3 \cdot 7$.Воспользуемся свойствами многочленов деления круга:

$$\Phi_{2n}(x) = \Phi_n(-x) \text{ при } 2 \nmid n,\ n > 2, \quad \Phi_{p^{r+1}}(x) = \Phi_p(x^{p^r}), \quad \Phi_{p_1^{r_1+1} \cdots\, p_k^{r_k+1}}(x) = \Phi_{p_1 \cdots p_k}(x^{p_1^{r_1} \cdots\, p_k^{r_k}}).$$

Находим $\Phi_1(x) = x - 1$, $\Phi_2(x) = \dfrac{x^2 - 1}{\Phi_1(x)} = x + 1$, $\Phi_7(x) = \dfrac{x^7 - 1}{\Phi_1(x)} = x^6 + \ldots + x + 1$. Далее $\Phi_4(x) = \Phi_2(x^2) = x^2 + 1$, $\Phi_8(x) = \Phi_2(x^4) = x^4 + 1$, $\Phi_{14}(x) = \Phi_7(-x) = x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$. Теперь $\Phi_{28}(x) = \Phi_{14}(x^2) = x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$, $\Phi_{56}(x) = x^{24} - x^{20} + x^{16} - x^{12} + x^8 - x^4 + 1$.

ОТВЕТ: $x^{56} - 1 = \Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_7(x)\Phi_8(x)\Phi_{14}(x)\Phi_{28}(x)\Phi_{56}(x)$. Явные формулы см. выше.

3. Найти кольцо множителей и норму модуля $M = \{7, 3 + \sqrt{-5}\}$ в поле $K = \mathbb{Q}(\sqrt{-5})$. Подобен ли этот модуль $\mathbb{Z}_K$?

РЕШЕНИЕ:

$\mathbb{Z}_K = \{1, \sqrt{-5}\}$. Мы знаем, что $E_M = \{1, c\sqrt{-5}\}$ с некоторым $c \in \mathbb{N}$. Запишем

$$c\sqrt{-5} \cdot 7 = 7c \cdot (3 + \sqrt{-5}) - 3c \cdot 7 \in M, \quad c\sqrt{-5} \cdot (3 + \sqrt{-5}) = 3c\sqrt{-5} - 5c = 3c \cdot (3 + \sqrt{-5}) - 2c \cdot 7 \in M.$$

Значит, подходит уже $c = 1$, и $E_M = \mathbb{Z}_K$.

Норма модуля может быть найдена как абсолютная величина определителя матрицы перехода от базиса кольца множителей модуля к базису самого модуля. Имеем

$$N(M) = |\det \begin{pmatrix} \frac{1}{7} & 0 \\ -\frac{3}{7} & 1 \end{pmatrix}| = \frac{1}{7}.$$

Модули $\{1,\alpha\}$ и $\{1,\beta\}$ подобны тогда и только тогда, когда числа α и β эквивалентны. Приведённые же квадратичные иррациональности эквивалентны тогда и только тогда, когда они равны. Число $\sqrt{-5}$ уже является приведённым, то есть принадлежит фундаментальной области

$$H = \left\{\tau \in \mathbb{C} \;\middle|\; -\frac{1}{2} < \operatorname{Re}\tau < 0,\ \operatorname{Im}\tau > 0, |\tau| > 1\right\} \bigcup \left\{\tau \in \mathbb{C} \;\middle|\; 0 \leqslant \operatorname{Re}\tau \leqslant \frac{1}{2},\ \operatorname{Im}\tau > 0, |\tau| \geqslant 1\right\}.$$

А число $\dfrac{3+\sqrt{-5}}{7}$ эквивалентно приведённому числу $\dfrac{1+\sqrt{-5}}{2}$. Отсюда видно, что модуль M не подобен $\mathbb{Z}_K$.

ОТВЕТ: $\{1,\sqrt{-5}\}$, $\frac{1}{7}$, нет.

4. Найти группу единиц в кольце $\mathbb{Z}_K$ при $K = \mathbb{Q}(\sqrt{7})$.

РЕШЕНИЕ:

Из теории следует, что в действительном квадратичном поле алгебраических чисел есть одна фундаментальная единица. Она будет соответствовать минимальному решению уравнения Пелля $x^2 - 7y^2 = \pm 1$. Это решение, как известно, доставляется числителем и знаменателем 3-й подходящей дроби, получаемой при разложении в цепную дробь числа $\sqrt{7} = [2;\overline{1,1,1,4}]$. Находим $x = 8,\ y = 3$.

ОТВЕТ: $\{\pm\left(8+3\sqrt{7}\right)^n,\ n \in \mathbb{Z}\}$.

5. Разложить главный идеал (3) в произведение простых идеалов в поле $K = \mathbb{Q}(\sqrt{7})$.

РЕШЕНИЕ:

$\mathbb{Z}_K = \{1,\sqrt{7}\}$. Минимальный многочлен $x^2 - 7$ числа $\sqrt{7}$ имеет по модулю 3 корни 1 и -1. Согласно общей теории можно записать

ОТВЕТ: $(3) = (3,\sqrt{7}-1)\cdot(3,\sqrt{7}+1)$.

Для получения зачёта необходимо правильно решить не менее четырёх из пяти предложенных задач и показать полное владение теоретическим материалом курса