29 Квадратичные иррациональности. Множество Z[$\sqrt{m}$]: сопряжение, замкнутость сложения, умножения. Согласованность сопряжения и умножения. Норма и её свойства.

Опр Иррациональное число $\overline{\alpha}$ называется *квадратичной иррациональностью*, если α - корень квадратного уравнения с целыми коэффициентами.

Опр Пусть $\alpha = a + b\sqrt{m}$ — квадратичная иррациональность. Назовем число $\alpha = a - b\sqrt{m}$ сопряженным к α числом
Утверждение
Множество Z[$\sqrt{m}$] = {a + b$\sqrt{m}$| a, b $\in Z$ } $\subset$ R замкнуто относительно операций:

1 Сопряжения

2 Сложения

3 Умножения

▲

1 a - b$\sqrt{m}$ = a + (-b)$\sqrt{m}$; a, -b $\in Z \Longrightarrow$ a - b$\sqrt{m}$ $\in$Z[$\sqrt{m}$]

2 $a_1 + b_1\sqrt{m} + a_2 + b_2\sqrt{m} = (a_1 + a_2) + (b_1 + b_2)\sqrt{m}$; $(a_1 + a_2),\ (b_1 + b_2) \in Z \Longrightarrow a_1 + b_1\sqrt{m} + a_2 + b_2\sqrt{m}$ $\in$Z[$\sqrt{m}$]

3 $(a_1 + b_1\sqrt{m}) * (a_2 + b_2\sqrt{m}) = (a_1a_2 + b_1b_2m) + (a_1b_2 + a_2b_1)\sqrt{m}; (a_1a_2 + b_1b_2m), (a_1b_2 + a_2b_1) \in Z \Longrightarrow (a_1 + b_1\sqrt{m}) * (a_2 + b_2\sqrt{m}) \in Z[\sqrt{m}]$ ■

Сопряжённость для квадратичной иррациональности согласована с общим определением. В алгебре сопряженными к элементу α над полем F называются корни неприводимого многочлена f(x) $\in$ F[x], для которого f(α) = 0. Это согласовано с определением комплексного сопряжения. А именно, для комплексного числа z $\in$ C R его сопряжённое — это второй корень квадратного многочлена, у которого первый корень — это z.
Опр
Для $\alpha \in$ Z[$\sqrt{m}$] определим норму N(α) = $\alpha\overline{\alpha}$.
Свойства

1 $N(\alpha) \in Z$ ▲ $N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{m}) * (a - b\sqrt{m}) = a^2 - b^2m \in Z$ ■

2 $N(\alpha\beta) = N(\alpha) * N(\beta)$
▲ $\alpha = a_1 + b_1\sqrt{m},\ \beta = a_2 + b_1\sqrt{m}$.
$\alpha\beta = (a_1a_2 + b_1b_2m) + (a_1b_2 + a_2b_1)\sqrt{m}$
$\overline{\alpha\beta} = (a_1a_2 + b_1b_2m) - (a_1b_2 + a_2b_1)\sqrt{m}$
$N(\alpha\beta) = ((a_1a_2 + b_1b_2m) + (a_1b_2 + a_2b_1)\sqrt{m})((a_1a_2 + b_1b_2m) - (a_1b_2 + a_2b_1)\sqrt{m}) =$
$= (a_1 + b_1\sqrt{m})(a_2 + b_2\sqrt{m}) * (a_1 - b_1\sqrt{m})(a_2 - b_2\sqrt{m}) = (a_1 + b_1\sqrt{m})(a_1 - b_1\sqrt{m}) * (a_2 + b_2\sqrt{m})(a_2 - b_2\sqrt{m}) = N(\alpha)N(\beta)$ ■

30 Пара (a, b), где a + b$\sqrt{2}$ = $(1 + \sqrt{2})^n$ является решением уравнения Пелля $a^2 - 2b^2 = \pm 1$.

Опр Уравнение вида $x^2 - my^2 = 1$, где m — натуральное число, не являющееся точным квадратом, называется уравнением Пелля. Решение (1, 0) называется тривиальным. Решение (x, y) называется положительным, если x > 0 и y > 0.

Определим a_n и b_nпри помощи равенства $(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}$

1. $(1+\sqrt{2})^n = \sum_{k=0}^{n} C_n^k (\sqrt{2})^k$
   $(1-\sqrt{2})^n = \sum_{k=0}^{n} C_n^k (-\sqrt{2})^k$. При четных k $(-\sqrt{2})^k = (\sqrt{2})^k \in N \implies (-\sqrt{2})^k \in a_n$. При нечетных k $(-\sqrt{2})^k = -(\sqrt{2})^k \notin Z \implies (-\sqrt{2})^k \in -b_n$
   Таким образом, $(1-\sqrt{2})^n = a_n - b_n\sqrt{2}$

2. $a_n^2 - 2b_n^2 = (a_n - b_n\sqrt{2})(a_n + b_n\sqrt{2}) = (1+\sqrt{2})^n(1-\sqrt{2})^n = (-1)^n$

Отсюда заключаем, что такие a_n и b_n: $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$ являются решениями уравнения Пелля $a^2 - 2b^2 = \pm 1$.

31 Связь между решениями уравнения Пелля $a^2 - 2b^2 = \pm 1$ и элементами Z$[\sqrt{2}]$ нормой 1.

Утверждение
Любой элемент Z$[\sqrt{2}]$ нормы 1 является решением уравнения $a^2 - 2b^2 = 1$, любое решение уравнения $a^2 - 2b^2 = 1$ - элемент Z$[\sqrt{2}]$ нормы 1
■

- -> Пусть (a,b) - решение уравнения Пелля $a^2 - 2b^2 = 1$, тогда $(a+b\sqrt{2})(a-b\sqrt{2}) = 1 \implies N(a+b\sqrt{2}) = 1; a, b \in Z[\sqrt{2}]$
- <- Пусть a, b $\in Z[\sqrt{2}],\ N(a+b\sqrt{2}) = 1 \implies (a+b\sqrt{2})(a-\sqrt{2}) = 1 = a^2 - 2b^2 \implies (a,b)$ - решение уравнения Пелля ■

Аналогичное утверждение можно сформулировать для $a^2 - 2b^2 = -1$

32 Алгебраические и трансцендентные числа. Существование трансцендентных чисел (из соображения мощности). Степень алгебраического числа. Теорема Лиувилля (б/д).

Опр Число α - алгебраическое, если существует многочлен с целыми коэффициентами, корнем которого является α

Обозначим множество алгебраических чисел A. Это множество счетно (достаточно занумеровать все многочлены)
Опр $R \backslash A$ $(C\backslash A)$ имеет мощность континуум, все числа из этого множества - *трансцендентные числа*

Опр *Степень алгебраического числа* - это минимальная степень уравнения, корнем которого является это число

Теорема Лиувилля
Пусть α - алгебраическое число степени d, тогда $\exists c = c(\alpha)$: неравенство $|\alpha - \frac{p}{q}| \leq \frac{c}{q^d}$ не имеет решени в $\frac{p}{q}$

33 Определение решётки (эквивалентность двух определений) и дискретного подмножества. Определитель решётки. Независимость значения определителя от выбора базиса.

Опр Пусть $(e_1, ..., e_k)$ — набор линейно независимых векторов в R^n. Тогда дискретная абелева группа в R^n, порождённая $\{e_i\}$, называется решёткой, а набор $(e_1, ..., e_k)$ называется базисом решётки. Иными словами, решётка есть множество $\Lambda = \{a_1e_1 + ... + a_ke_k\}, a_i \in Z$

Опр Подмножество X пространства R^n называется дискретным, если для любой точки x $\in$ X существует окрестность этой точки, не содержащая других точек множества X.

Опр Определителем $det\Lambda$ решётки Λ называется определитель матрицы, составленной из координат её базисных векторов.(Он равен объёму фундаментального параллелепипеда, то есть параллелепипеда, составленного из базисных векторов.)

Утверждение
Определитель решетки не зависит от выбора базиса
▲ Пусть A, B - матрицы в разных базисах, S - матрица перехода от A к B. Тогда $B = A * S$. В силу того, что векторы нового безиса - это ЛК векторов старого базиса с какими-то целочисленными коэффициентами, матрица S целочисленная. По этим же соображениям, S^{-1} - целочисленная матрица. Тогда
$detB = detA\ detS, detA = detS^{-1}detB \Longrightarrow \frac{1}{detS} = detS^{-1} \Longrightarrow detS^{-1}detS = 1. \Longrightarrow detS = \pm 1 \Longrightarrow detA = detB$ ■

34 Определение решётки и его определителя. Решётка $\Lambda_{\overline{a}}$ и её определитель.

Опр Дано простое число p и зафиксирован вектор $\overline{a} = (\frac{a_1}{p}, ..., \frac{a_n}{p})$, где $a_i \in Z$. Определим множество $\Lambda_{\overline{a}} = \{l\overline{a} + \overline{b},\ l \in Z, \overline{b} \in Z^n\}$
Утверждение
$\Lambda_{\overline{a}}$ - решетка
▲ Заметим, что все это множество порождается векторами $(\overline{a}, \overline{e_1}, \overline{e_2}, ..., \overline{e_n})$. Покажем, что если убрать из этого набора векторов $\overline{e_1}$, они все равно будут порождать множество $\Lambda_{\overline{a}}$.

Заметим, что если все $a_i \vdots p$, то ничего нового мы не получим, т.е. $\overline{a}$ линейно выражается через $(\overline{e_1}, ...\overline{e_n})$, и мы нашли базис, порождащий это множество, тогда $\Lambda_{\overline{a}}$ - решетка.

Предположим, какой-то из $a_i \not\vdots p$; Пусть БОО это a_1. Научимся из вектора $\gamma = (\frac{1}{p}, ..., \frac{la_n}{p})$ получать вектор $\overline{a}$ и вектор $\overline{e_1}$.
Возьмем в качестве $\overline{b} = k\overline{e_1}$, тогда $l\overline{a} + \overline{b} = (\frac{la_1+kp}{p}, \frac{la_2}{p}, ..., \frac{la_n}{p})$
Заметим, что всегда можно выбрать l и k так, чтобы $la_1 + kp = 1$, т.к. $(a_1, p) = 1$
Покажем, что $(\gamma, e_2, ..., e_n)$ образуют базис. Для начала заметим, что $\overline{e_1} = p\gamma - la_2\overline{e_2} - la_3\overline{e_3} - ...la_n\overline{e_n}$. $l\overline{a} = \gamma - \overline{b}$. Мы умеем выражать все базисные векторы и $l\overline{a} \Longrightarrow$ умеем выражать $\overline{a} \Longrightarrow$ нашли базис■

Найдем $det\Lambda_{\overline{a}}$
Заметим, что матрица, составленная из базисных векторов $\Lambda_{\overline{a}}$ нижняя треугольная, diag$(\frac{1}{p}, 1, 1, ..., 1)$, исходя из того, какой базис мы нашли. Тогда $det\Lambda_{\overline{a}} = \frac{1}{p}$