Лекция 13

То, что квадратичные формы над $\mathbb{Q}$ описываются простым образом, связано со следующим результатом.

Теорема 13.1 *Все элементы* $\mathrm{K}_n^M(\mathbb{Q})/2$ *для любого* n *являются чистыми символами.*

Доказательство: При $n \geq 3$ - доказывать нечего, так как единственный ненулевой элемент там - это чистый символ $\{-1, \dots, -1\}$. Так что остался только случай $n = 2$.

В доказательстве мы будем использовать следующий классический результат:

Теорема (Дирихле) *Пусть* $a, b \in \mathbb{N}$ *- взаимно простые числа. Тогда среди чисел вида* $a + bn$, $n \in \mathbb{N}$ *имеется бесконечно много простых.*

Мы знаем, что гомоморфизм $j \oplus (\oplus_{p-\text{неч.}} \partial_p/2)$ задаёт изоморфизм группы $\mathrm{K}_2^M(\mathbb{Q})/2$ с $\mathbb{Z}/2 \oplus (\oplus_{p-\text{неч.}} \mathbb{Z}/2)$. Условимся записывать элементы наших групп $\mathbb{Z}/2$ аддитивно. Пусть $u \in \mathrm{K}_2^M(\mathbb{Q})/2$ - произвольный элемент. Пусть $p_1, \dots, p_k$ - такое множество различных простых чисел, что $(\partial_l/2)(u) = 0$ при всех $l \neq p_i$.

Добавив к этому множеству одно простое вида $4n - 1$, если нужно, мы можем считать, что $(-1)^{j(u)} \cdot p_1 \cdot \ldots \cdot p_k \equiv -1 \,(\,mod\, 4)$. Для всех $1 \leq i \leq k$ обозначим через $a_{p_i} \in \mathbb{Z}/p_i$ некоторый (ненулевой) квадрат, если $(\partial_{p_i}/2)(u) = 0$, и некоторый неквадрат, если $(\partial_{p_i}/2)(u) \neq 0$. Положим также: $a_2 = (-1)^s \in \mathbb{Z}/4$, где s - это число ненулевых среди $j(u), (\partial_p/2)(u)$. По теореме Дирихле, имеется простое число q, такое, что $q\,(\,mod\, p_i) = (-1)^{j(u)} a_{p_i}$ и $q\,(\,mod\, 4) = (-1)^{j(u)} a_2$. Утверждается, что $\{(-1)^{j(u)} p_1 \cdot \ldots \cdot p_k, (-1)^{j(u)} q\} = u$.

Действительно, достаточно проверить, что значение j и $(\partial_l/2)$ на этих элементах совпадают. Ясно, что $(\partial_l/2)(\{(-1)^{j(u)} p_1 \cdot \ldots \cdot p_k, (-1)^{j(u)} q\}) = 0 = (\partial_l/2)(u)$ для любого простого l кроме p_i-ых и q. Также видно, что $j(\{(-1)^{j(u)} p_1 \cdot \ldots \cdot p_k, (-1)^{j(u)} q\}) = j(u)$. $\partial_{p_i}(\{(-1)^{j(u)} p_1 \cdot \ldots \cdot p_k, (-1)^{j(u)} q\}) \equiv a_{p_i}\,(\,mod\, p_i)$, и стало быть, $(\partial_{p_i}/2)(\{(-1)^{j(u)} p_1 \cdot \ldots \cdot p_k, (-1)^{j(u)} q\})$ будет нулевое если и только если a_{p_i} - квадрат, а последнее равносильно тому, что $(\partial_{p_i}/2)(u) = 0$. Значит, $(\partial_{p_i}/2)(\{(-1)^{j(u)} p_1 \cdot \ldots \cdot p_k, (-1)^{j(u)} q\}) = (\partial_{p_i}/2)(u)$. Осталось проверить случай $(\partial_q/2)$.

По квадратичному закону взаимности (в аддитивной форме), $\psi(v) = \sum_p (\partial_p/2)(v) + j(v)$. Отсюда видно, что достаточно показать, что

$\psi(\{(-1)^{j(u)}p_1\cdot\ldots\cdot p_k,(-1)^{j(u)}q\})=\psi(u)$. Но $\psi(\{(-1)^{j(u)}p_1\cdot\ldots\cdot p_k,(-1)^{j(u)}q\})=((-1)^{j(u)}p_1\cdot\ldots\cdot p_k-1)/2)\cdot((-1)^{j(u)}q-1)/2)$. Так как первый множитель ненулевой по условию, то $\psi(\{(-1)^{j(u)}p_1\cdot\ldots\cdot p_k,(-1)^{j(u)}q\})$ - нулевое тогда и только тогда, когда $(-1)^{j(u)}q\equiv 1\,(\,mod\,4)$, то есть, когда среди $j(u),(\partial_{p_i}/2)(u)$ чётное количество ненулевых. Но так как $\psi(u)=\sum_{p_i}(\partial_{p_i}/2)(u)+j(u)$, то последнее условие равносильно тому, что $\psi(u)=0$. Значит, $\psi(\{(-1)^{j(u)}p_1\cdot\ldots\cdot p_k,(-1)^{j(u)}q\})=\psi(u)$, $(\partial_q/2)(\{(-1)^{j(u)}p_1\cdot\ldots\cdot p_k,(-1)^{j(u)}q\})=(\partial_q/2)(u)$, и $u=\{(-1)^{j(u)}p_1\cdot\ldots\cdot p_k,(-1)^{j(u)}q\}$. □

Квадратичные формы над полями, $\mathrm{K}^M_*/2$ которых состоит из чистых символов

Пусть k - некоторое поле. Обозначим через Λ множество наборов вида $(\alpha_1,\ldots,\alpha_m)$, где $\alpha_i\in\mathrm{K}^M_{r_i}(k)/2$ - это чистый символ, и $0\le r_1<\ldots<r_m$. Мы имеем естественное отображение $f:\Lambda\to W(k)$ заданное формулой $f((\alpha_1,\ldots,\alpha_m))=\sum_i(-1)^{i-1}\langle\langle\alpha_i\rangle\rangle$, где $\langle\langle\alpha_i\rangle\rangle$ - это r_i-кратная пфистерова форма, отвечающая чистому символу α_i.

Теорема 13.2 *Пусть k - такое поле, что $\mathrm{K}^M_n(k)/2$ состоит из чистых символов для любого n. Тогда отображение f является биекцией. Иными словами, каждая квадратичная форма q над k с точностью до гиперболической формы однозначно представляется в виде $\sum_{i=1}^m(-1)^{i-1}\langle\langle\alpha_i\rangle\rangle$, где α_i - ненулевой чистый символ степени r_i, и $0\le r_1<\ldots<r_m$.*

Доказательство: Сперва докажем сюрьективность f. Пусть $q=\langle a_1,\ldots,a_n\rangle$ - некоторая квадратичная форма. Тогда в $W(k)$,
$q=\langle a_1\rangle+\ldots+\langle a_n\rangle=\sum_{j=1}^n(-1)^{j-1}(1-\langle 1,(-1)^ja_j\rangle)=(1+(-1)^n)/2\cdot\langle 1\rangle-\sum_{j=0}^n(-1)^{j-1}(\langle\langle(-1)^ja_j\rangle\rangle)$.

Докажем индукцией по t, что если $\beta_1,\ldots,\beta_t\in\mathrm{K}^M_s(k)/2$, то $\sum_{l=1}^t(-1)^{l-1}\langle\langle\beta_l\rangle\rangle=\sum_{u=1}^{t'}(-1)^{u-1}\langle\langle\gamma_u\rangle\rangle$, где $\gamma_u\in\mathrm{K}^M_{s_u}(k)/2$ - это чистый символ, и $s\le s_1<\ldots<s_{t'}$. При $t=1$ доказывать нечего, а индуктивный переход доказывается с помощью следующего соображения.

Если $\xi_1,\xi_2\in\mathrm{K}^M_{s'}(k)/2$ - чистые символы, то $\xi_1+\xi_2$ - также чистый символ (по условию). Имеется два случая: $\xi_1+\xi_2$ - нулевой, или ненулевой. В первом случае, $\langle\langle\xi_1\rangle\rangle-\langle\langle\xi_2\rangle\rangle=0$. Во втором (используя соображения аналогичные доказательству теоремы 9.5), мы получаем, что ξ_1,ξ_2 имеют общий чистый делитель χ степени $s'-1$. Тогда $\langle\langle\xi_1\rangle\rangle-\langle\langle\xi_2\rangle\rangle=\langle\langle\chi\rangle\rangle(\langle\langle b_1\rangle\rangle-\langle\langle b_2\rangle\rangle)=\langle\langle\chi\rangle\rangle(\langle\langle -b_1b_2\rangle\rangle-\langle\langle b_1,-b_2\rangle\rangle)=\langle\langle\chi\cdot\{-b_1b_2\}\rangle\rangle-\langle\langle\chi\cdot\{b_1,-b_2\}\rangle\rangle$.

Поэтому, $\sum_{l=1}^t(-1)^{l-1}\langle\langle\beta_l\rangle\rangle=$ либо $\langle\langle\beta'\rangle\rangle-\sum_{j=1}^{t-1}\langle\langle w_j\rangle\rangle$, либо $\sum_{j=1}^{t-1}\langle\langle w_j\rangle\rangle$, где $w_j \in \mathrm{K}^M_{s+1}(k)/2$ - чистые символы, и $\beta' \in \mathrm{K}^M_s(k)/2$ - ненулевой чистый. Таким образом, индуктивный переход сделан, и сюрьективность f доказана.

Докажем инъективность f. Пусть $\sum_{i=1}^m (-1)^{i-1} \langle\langle \alpha_i \rangle\rangle = \sum_{j=1}^n (-1)^{j-1} \langle\langle \beta_j \rangle\rangle$ в $W(k)$. Пусть $\alpha_1 \in \mathrm{K}^M_{r_1}(k)/2$ и $\beta_1 \in \mathrm{K}^M_{s_1}(k)/2$. Если $r_1 > s_1$, то $\sum_{i=1}^m (-1)^{i-1} \langle\langle \alpha_i \rangle\rangle \in I^{r_1}$, в то время, как $\sum_{j=1}^n (-1)^{j-1} \langle\langle \beta_j \rangle\rangle \notin I^{s_1+1} \supset I^n$. Применяя аналогичные соображения к случаю $s_1 > r_1$, мы получаем $s_1 = r_1$. Кроме того, $\langle\langle \alpha_1 \rangle\rangle \equiv \langle\langle \beta_1 \rangle\rangle \ (\mathit{mod}\, I^{s_1+1})$. А это означает, что $\alpha_1 = \beta_1$. Сокращая первые слагаемые, мы получаем $\alpha_2 = \beta_2$, и т.д. ... . $\square$