Лекция 3

Квадратичные формы над конечными полями

Как обычно, мы будем предполагать, что $char(k) \neq 2$.

Утверждение 3.1 *Пусть $\mathbb{F}_q$ - конечное поле из q элементов ($char(k) \neq 2$). Если $q = \langle a, b\rangle$ - невырожденная форма над $\mathbb{F}_q$, то любое $c \in \mathbb{F}_q^*$ является значением q. В частности, любая форма размерности ≥ 3 над $\mathbb{F}_q$ - изотропна.*

Доказательство: Так как значений вида ax^2, равно как и вида $c - by^2$, будет $(q+1)/2$ штук в $\mathbb{F}_q$, то уравнение $ax^2 + by^2 = c$ имеет решение в $\mathbb{F}_q$. □

Таким образом, анизотропные формы над $\mathbb{F}_q$ могут иметь размерность $0, 1$ и 2. Форм размерности 1 будет столько же, сколько элементов в группе $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$, то есть, две: $\langle 1\rangle$ и $\langle\varepsilon\rangle$, где ε - не квадрат.

Определение 3.2 *Пусть q - невырожденная квадратичная форма над полем k. Определим $\det_{\pm}(q) \in k^*/(k^*)^2$ как $(-1)^{[\dim(q)/2]} \cdot \det(B_q)$, где $\det(B_q)$ - определитель соответствующей билинейной формы. Если $q = \langle a_1, \dots, a_n\rangle$, то $\det_{\pm}(q) = (-1)^{[\dim(q)/2]} \prod_{i=1}^{n} a_i$. Заметим, что если p - чётномерная, то $\det_{\pm}(q \perp p) = \det_{\pm}(q) \cdot \det_{\pm}(p)$. А так как $\det_{\pm}(\mathbb{H}) = 1$, то $\det_{\pm}$ спускается до отображения $W(k) \to k^*/(k^*)^2$.*

Лемма 3.3 *Если q - двумерная форма над полем k, то $q \cong \mathbb{H} \Leftrightarrow \det_{\pm}(q) = 1$.*

Доказательство: Очевидно ввиду равенства $a \cdot \mathbb{H} \cong \mathbb{H}$. □

Если q - двумерная форма над $\mathbb{F}_q$, то $q = \lambda \cdot \langle 1, -\det_{\pm}(q)\rangle$. Но форма $\langle 1, -\det_{\pm}(q)\rangle$ принимает все ненулевые значения в $\mathbb{F}_q$, по утверждению 3.1. Значит, по упражнению 2.1(2), $\lambda \cdot \langle 1, -\det_{\pm}(q)\rangle \cong \langle 1, -\det_{\pm}(q)\rangle$. Значит, различных невырожденных 2-мерных форм над k будет столько же, сколько элементов в $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$, то есть две. При этом, одна из них, отвечающая 1, будет гиперболичной. Стало быть, единственной анизотропной 2-мерной формой над $\mathbb{F}_q$ будет форма $\langle 1, -\varepsilon\rangle$, где ε - не квадрат в $\mathbb{F}_q$. Мы установили, что $W(\mathbb{F}_q)$ содержит 4 элемента: 0, $\langle 1\rangle$, $\langle\varepsilon\rangle$, и $\langle 1, -\varepsilon\rangle$.

Имеются два случая: 1) -1 - квадрат в $\mathbb{F}_q$; 2) -1 - не квадрат.

1) Тогда форма $\langle 1, 1\rangle$ - гиперболична, и все элементы $W(\mathbb{F}_q)$ имеют порядок 2. Если обозначить $x := \langle 1, -\varepsilon\rangle$, то получаем сюрьекцию $\mathbb{Z}/2[x] \to$

$W(\mathbb{F}_q)$. А так как форма $\langle 1, -\varepsilon\rangle \cdot \langle 1, -\varepsilon\rangle$ - гиперболична, то $W(\mathbb{F}_q) \cong \mathbb{Z}/2[x]/(x^2)$.

2) В этом случае, форма $\langle 1, 1\rangle$ негиперболична, а значит, $\langle 1\rangle$ имеет порядок 4. Тогда $W(k) \cong \mathbb{Z}/4$.

Таким образом, мы получаем:

Теорема 3.4

(1) *Если* $q \equiv 1\,(\,mod\,4)$, *то* $W(\mathbb{F}_q) \cong \mathbb{Z}/2[x]/(x^2)$.

(2) *Если* $q \equiv 3\,(\,mod\,4)$, *то* $W(\mathbb{F}_q) \cong \mathbb{Z}/4$.

Каноническая фильтрация на $W(k)$

Обозначим через I идеал чётномерных форм в $W(k)$. Заметим, что $I = \mathrm{Ker}(\dim/2)$, где $\dim/2 : W(k) \to \mathbb{Z}/2$ отображение размерности $(\,mod\,2)$. I порождает мультипликативную фильтрацию $W(k) \supset I \supset I^2 \supset \ldots \supset I^n \supset \ldots$ на $W(k)$. Присоединённое градуированное кольцо мы будем обозначать $\mathrm{gr}^*_{I^{\cdot}}(W(k))$.

Упражнение 3.1 *Показать, что* I *- это единственный простой идеал в* $W(k)$, *поле вычетов которого имеет характеристику* 2. *(Использовать гиперболичность формы* $\langle 1, -a\rangle \cdot \langle 1, a\rangle$.*)*

Заметим, что если поле k не является формально вещественным (то есть, для некоторого n, форма $\perp_{i=1}^{n} \langle 1\rangle$ - изотропна), то I - это единственный простой идеал в $W(k)$.

Очевидно, что $\mathrm{gr}^0_{I^{\cdot}}(W(k)) \cong \mathbb{Z}/2$. Заметим, что $\det_{\pm}$ задаёт гомоморфизм групп $\mathrm{gr}^1_{I^{\cdot}}(W(k)) \to k^*/(k^*)^2$.

Теорема 3.5 *Отображение* $\det_{\pm} : \mathrm{gr}^1_{I^{\cdot}}(W(k)) \to k^*/(k^*)^2$ *является изоморфизмом.*

Доказательство: Определим обратное отображение ρ формулой $a \mapsto \langle 1, -a\rangle\,(\,mod\,I^2)$. Покажем, что ρ - гомоморфизм групп. Действительно, $\rho(a) + \rho(b) - \rho(ab) = \langle 1, -a\rangle + \langle 1, -b\rangle - \langle 1, -ab\rangle = \langle 1, -a, -b, ab\rangle$. Но так как $\langle 1, -a, -b, ab\rangle = \langle 1, -a\rangle \cdot \langle 1, -b\rangle \in I^2$, то $\rho(a) + \rho(b) = \rho(ab)$.

Ясно, что $\det_{\pm} \circ \rho = id_{k^*/2}$. С другой стороны, I аддитивно порожден формами вида $\langle 1, -a\rangle$, и ρ - сюрьективно. Значит, $\det_{\pm}$ и ρ - взаимнообратные изоморфизмы. □

Попробуем описать $\mathrm{gr}^n_{I^{\cdot}}(W(k))$ при $n \geq 2$. Ясно, что $\mathrm{gr}^*_{I^{\cdot}}(W(k))$ порождено как алгебра над $\mathbb{Z}/2$ своей компонентой степени 1. Иначе говоря, мы имеем сюрьективный гомоморфизм алгебр $\mathrm{T}^*_{\mathbb{Z}/2}(k^*/(k^*)^2) \to$

$\mathrm{gr}^*_{I^\cdot}(W(k))$. При этом, образом элемента $a_1 \otimes \ldots \otimes a_n$ будет класс формы $\langle 1, -a_1\rangle \cdot \ldots \cdot \langle 1, -a_n\rangle$ в I^n/I^{n+1}.

Определение 3.6 *Форма вида $\langle 1, -a_1\rangle \cdot \ldots \cdot \langle 1, -a_n\rangle$ называется n-кратной пфистеровой, и обозначается $\langle\langle a_1, \ldots, a_n\rangle\rangle$.*

Заметим, что некоторые 2-кратные пфистеровы формы будут заведомо гиперболичны.

Утверждение 3.7 *Пусть $a \in k\backslash 0, 1$. Квадратичная форма $\langle\langle a, 1-a\rangle\rangle := \langle 1, -a\rangle \cdot \langle 1, -(1-a)\rangle$ является гиперболической.*

Доказательство: Так как $\dim(\langle\langle a, 1-a\rangle\rangle) = 4$, то достаточно указать 2-мерное изотропное подпространство в подлежащем векторном пространстве. Легко видеть, что линейная оболочка векторов $(1,1,1,0)$ и $(a,1,0,1)$ будет изотропной для нашей формы $\langle 1, -a, a-1, a-a^2\rangle$. $\square$

Это показывает, что имеется сюрьективный гомоморфизм

$$\varphi : \mathrm{T}^*_{\mathbb{Z}/2}(k^*/(k^*)^2)/(a \otimes (1-a)) \to \mathrm{gr}^*_{I^\cdot}(W(k)).$$

Кольцо $\mathrm{T}^*_{\mathbb{Z}/2}(k^*/(k^*)^2)/(a \otimes (1-a))$ - это $\mathrm{K}^M_*(k)/2$ - Милноровская K-теория поля k, профакторизованная по 2.

(2-я) Гипотеза Милнора *φ является изоморфизмом.*