Классификация билинейных форм

Пусть основное поле имеет характеристику, отличную от 2. Существование и единственность разложения Витта позволяет определить следующую операцию. Пусть $[V_1]$ и $[V_2]$ — классы конечномерных анизотропных пространств с точностью до изометрии. Определим $[V_1]+[V_2]$ как класс анизотропного подпространства в разложении Витта $V_1 \overset{\perp}{\bigoplus} V_2$.

Предложение 1 *Классы анизотропных пространств с такой операцией образуют коммутативную группу. Ноль соответствует нулевому пространству. Обратный элемент — обращению знака формы.*

Доказательство: Коммутативность следует из определения, докажем ассоциативность. В силу единственности разложения Витта и того, что ортогональная сумма гиперболических пространств является гиперболическим пространством, оба способа вычисления $[V_1]+[V_2]+[V_3]$ приведут к классу анизотропного подпространства в разложении Витта $V_1 \overset{\perp}{\bigoplus} V_2 \overset{\perp}{\bigoplus} V_3$.

С нулём всё ясно из определения, посмотрим на обратный элемент. Пусть V — пространство с формой, за V^- обозначим изоморфное V пространство с обращённым знаком формы. Для вектора $v \in V$ обозначим v^- его образ в V^-. Тогда заметим, что форма на ортогональной прямой сумме V и V^- невырождена, а векторы вида $v+v^-$ составят в этом пространстве изотропное подпространство половинной размерности. Значит, это пространство гиперболическое, и $[V]+[V^-]=0$.

Определение 1. Определённая выше группа называется *группой Витта* поля F и обозначается $W(F)$.

Следствие 1 *Всякая симметрическая билинейная форма на конечномерном векторном пространстве однозначно задаётся своим образом в группе Витта и двумя натуральными числами: размерностью ядра и размерностью максимального изотропного подпространства, не пересекающегося с ядром.*

Приведение матрицы к диагональному виду позволяет указать образующие этой группы.

Следствие 2 *Образующими группы Витта $W(F)$ можно выбрать классы $[x]$ одномерных подпространств с матрицей Грама (x), где $x \in F$, $x \neq 0$. При этом $[x_1]=[x_2]$ тогда и только тогда, когда x_1/x_2 — квадрат элемента F.*

Предложение 2 *Пусть F — алгебраически замкнутое поле. Тогда $W(F) \cong \mathbb{Z}/2\mathbb{Z}$.*

Доказательство: Так как все ненулевые элементы F являются квадратами, у $W(F)$ есть ровно одна образующая $[1]$, при этом $-[1]=[-1]=[1]$.

Предложение 3 *Имеем $W(\mathbb{R}) \cong \mathbb{Z}$.*

Доказательство: Группа $W(\mathbb{R})$ порождена $[1]$ и $[-1]$, при этом $[-1]=-[1]$. Значит, $W(\mathbb{R})$ является факторгруппой $\mathbb{Z}$. Кроме того, $[1]+\dots+[1] \neq 0$ так как соответствующее пространство анизотропно, откуда получаем требуемое утверждение.

Теорема 1 *Пусть p — простое. Тогда если p имеет вид $4k+1$, то $W(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, а если p имеет вид $4k+3$, то $W(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/4\mathbb{Z}$.*

Доказательство: Начнём с $p=4k+1$, где (-1) является квадратом по модулю p. Пусть $x \in \mathbb{Z}/p\mathbb{Z}$ — не квадрат по модулю p. Тогда всякий элемент $\mathbb{Z}/p\mathbb{Z}$ либо является квадратом, либо отличается от x умножением на квадрат. Значит, образующими будут $[1]$ и $[x]$.

При этом $2[1]=[1]+[1]$ соответствует форме с матрицей Грама $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ Но так как -1 является квадратом, уравнение a^2+b^2 имеет ненулевое решение в $\mathbb{Z}/p\mathbb{Z}$, что говорит о том, что имеется изотропный вектор. В силу невырожденности матрица Грама приводится к виду $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, а значит форма представляет ноль группы Витта, то есть $2[1]=0$. Аналогично, $2[x]$ соответствует форме с матрицей Грама $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$, у которой есть изотропный вектор (тот же самый), значит $2[x]=0$. Так как группа коммутативна, получаем, что она изоморфна $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Теперь пусть $p=4k+3$, тогда (-1) не является квадратом по модулю p. И для всякого $a \in \mathbb{Z}/p\mathbb{Z}$ либо a либо $-a$ является квадратом. Образующими здесь будут $[1]$ и $[-1]$. При этом форма (-1) получается обращением знака формы (1), поэтому $[-1]=-[1]$ и группа является циклической с образующей $[1]$. Осталось найти порядок этой группы.

Мы знаем, что $2[1]$ соответствует форме с матрицей Грама $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, которая будет анизотропной, так как нет ненулевых решений уравнения $a^2+b^2=0$ (иначе $(a/b)^2=-1$). Значит, порядок группы больше 2.

А форма, соответствующая $3[1]$ уже не будет анизотропной. Действительно, если уравнение $a^2+b^2+c^2=0$ не имеет ненулевых решений, это означает, что сумма любых двух квадратов a^2+b^2 всегда является квадратом (а не минус квадратом), а значит, все элементы были бы квадратами. Тогда матрица Грама этой формы приводится к виду $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & c \end{pmatrix}$, где $c=\pm 1$. Но $c=1$ противоречит единственности разложения Витта, значит, $c=-1$ и $3[1]=[-1]$, то есть $4[1]=0$.

Симплектические формы

Интерес представляют не только симметрические формы. Распространены в приложениях и их противоположности — симплектические формы.

Определение 2. Билинейная форма называется *симплектической (symplectic)*, если $(v,v)=0$ для всех v.

Предложение 4 *Для симплектической формы выполнено $(u,v)=-(v,u)$. Если характеристика поля отлична от 2, то это свойство равносильно $(v,v)=0$.*

Доказательство: Первое утверждение следует из $(u,v)+(v,u)=(u+v,u+v)-(u,u)-(v,v)$. Кроме того, если $(v,v)=-(v,v)$, то в поле характеристики отличной от 2 имеем $(v,v)=0$.

Для таких форм аналогично определено ядро, невырожденность, ортогональное дополнение.

Теорема 2 *В пространстве с симплектической формой найдётся базис $f_1,\ldots,f_m$, $e_1,\ldots,e_n$, $e^1,\ldots,e^n$, такой что $(e_i,e^j)=\delta_{i,j}$, а значение формы на других парах векторов равно нулю. Другими словами, матрица Грама в этом базисе примет вид* $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & E \\ 0 & -E & 0 \end{pmatrix}$.

Доказательство: Индукция по размерности. В размерности 0 и 1 форма заведомо нулевая. Если $(u,v)=0$ для всех u и v, то форма нулевая, иначе, пусть $(u,v)\neq 0$. Тогда, возьмём пару неколлинеарных векторов $e=u/(u,v)$ и $e'=v$, значение формы на которых равно 1. Форма на подпространстве, порождённом e и e' невырождена и, аналогично симметрическому случаю, рассмотрим ортогональное дополнение к этому подпространству. По предположению индукции, в нём найдётся требуемый базис. Дополняя его до базиса во всём пространстве векторами $e_{n+1}=e$ и $e^{n+1}=e'$, получим требуемый базис.

Упражнение 1 *Докажите, что для симплектической формы на свободном модуле над евклидовым кольцом существует базис $f_1,\ldots,f_m$, $e_1,\ldots,e_n$, $e^1,\ldots,e^n$, такой что $(e_i,e^j)=\delta_{i,j}\lambda_i$, а значение формы на других парах векторов равно нулю.*

Для решения этого упражнения в качестве пары базисных элементов удобно выбрать такие e и e', что норма (e,e') — минимальная ненулевая.

Эрмитовы формы

Возможно и другое обобщение билинейных форм. В приложениях часто бывает важна положительная определённость, когда $(v,v)>0$ для всех $v\neq 0$, например, когда требуется убедиться в невырожденности суммы различных форм. Этого легко добиться над полем вещественных чисел, но невозможно в исходном определении для комплексных чисел.

Определение 3. Пусть V — векторное пространство над $\mathbb{C}$. Отображение $V\times V\to\mathbb{C}$ называется *Эрмитовой формой (Hermitian form)*, если
1) $(\lambda_1 u_1+\lambda_2 u_2, v)=\lambda_1(u_1,v)+\lambda_2(u_2,v)$
2) $(u,v)=\overline{(v,u)}$.

Такая форма уже не является билинейной — для неё $(u,v_1+v_2)=(u,v_1)+(u,v_2)$, но $(u,\lambda v)=\overline{\lambda}(u,v)$. При этом у Эрмитовой формы аналогично определены матрица Грама, ядро, невырожденность, ортогональное дополнение. Точно также определена квадратичная форма (v,v), причём так как $(v,v)=\overline{(v,v)}$, она принимает вещественные значения.

Предложение 5 *Эрмитова форма определяется своей квадратичной формой.*

Доказательство: Заметим, что $\Re e(u,v)=\frac{(u,v)+(v,u)}{2}=\frac{(u+v,u+v)-(u,u)-(v,v)}{2}$ однозначно определяется квадратичной формой. А $\Im m(u,v)=-\Re e(iu,v)$.

Теорема 3 *В пространстве с эрмитовой формой существует базис $e_1,\dots,e_n$, такой что $(e_i,e_j)=0$ при $i\neq j$, а (e_i,e_i) равно нулю или ±1. При этом количество нулей, единиц и минус единиц определено однозначно.*

Доказательство: Аналогично случаю вещественного поля для симметрических форм. Проведём индукцию по размерности. Если форма не нулевая, найдётся вектор v, такой что $(v,v)\neq 0$, умножая его на скаляр, получим $(v,v)=\pm1$. Применим предположение индукции к ортогональному дополнению, и добавим v к этому базису.

Для доказательства единственности заметим, что количество нулей на диагонали соответствует размерности ядра, количество единиц — максимальному подпространству, для которого $(v,v)>0$ при $v\neq 0$, минус единиц — максимальному подпространству, для которого $(v,v)<0$ при $v\neq 0$.