18.782 Introduction to Arithmetic Geometry **Fall 2013**
Lecture #9 **10/3/2013**

9.1 Quadratic forms

We assume throughout k is a field of characteristic different from 2.

Definition 9.1. The four equivalent definitions below all define a *quadratic form* on k.

1. A *homogeneous quadratic polynomial* $f \in k[x_1, \ldots, x_n]$.
2. Associated to f is a *symmetric matrix* $A \in k^{n \times n}$ whose entries (a_{ij}) correspond to the coefficients of $x_i x_j$ in f via $f(x_1, \ldots, x_n) = \sum_{i,j} a_{ij} x^i x^j$.[1] Conversely, every symmetric matrix defines a homogeneous quadratic polynomial.
3. Each symmetric matrix A defines a *symmetric bilinear form* $B\colon k^n \times k^n \to k$ via $B_f(x, y) = x^t A y$, where x and $y$denote column vectors. It is symmetric, since
$$B(x, y) = x^t A y = (x^t A y)^t = y^t A^t x = y^t A x = B(y, x),$$
and it is bilinear, since for any $a \in k$ and $x, y, z \in k^n$ we have
$$B(ax + y, z) = (ax + y)^t A z = (ax^t + y^t) A z = ax^t A z + y^t A z = aB_f(x, z) + B(y, z).$$
Conversely, if B is a symmetric bilinear form, and $e_1, \ldots, e_n$ are basis vectors, the matrix $A = (a_{ij})$ defined by $a_{ij} = B(e_i, e_j)$ is symmetric.
4. The function $f\colon k^n \to k$ obtained by evaluating a homogeneous quadratic polynomial is a *homogeneous quadratic function*. In terms of the corresponding bilinear form $B(x, y)$, we have $f(x) = B(x, x)$. Conversely, we can recover $B(x, y)$ from $f(x)$ via
$$B(x, y) = \frac{f(x + y) - f(x) - f(y)}{2}.$$

We thus have canonical isomorphisms between four sets of objects: homogeneous quadratic polynomials, symmetric matrices, symmetric bilinear forms, and homogeneous quadratic functions. We use the symbol f to refer to both a homogeneous quadratic polynomial and its evaluation function, and we use the symbols A and B to refer to the associated matrix and bilinear form.

The definition of a symmetric bilinear form $B\colon V \times V \to k$ makes sense over any finite dimensional k-vector space V, and we can define the corresponding homogeneous function $f\colon V \to k$ abstractly as $f(v) = B(v, v)$. If we then choose a basis for V we can compute the symmetric matrix A whose coefficients define a homogeneous quadratic polynomial.

Symmetric bilinear forms can be viewed as a generalization of inner products to arbitrary fields. Inner products are also required to satisfy $B(v, v) > 0$ for any nonzero vector v, but this only makes sense if k is an *ordered field*.[2] In general, symmetric bilinear forms are allowed to vanish on nonzero vectors (indeed, the zero map is a symmetric bilinear form).

[1] Note that for $i \neq j$ this means that if f_{ij} is the coefficient of $x_i x_j$ then $a_{ij} = a_{ji} = f_{ij}/2$, so that $f_{ij} x_i x_j = a_{ij} x_i x_j + a_{ji} x_j x_i$. This is slightly unpleasant but makes everything else work nicely.

[2] An ordered field is a field with a total ordering $\leq$ that satisfies $a \leq b \Rightarrow a{+}c \leq b{+}c$ and $a, b > 0 \Rightarrow ab > 0$. In such a field 0 cannot be written as a sum of nonzero squares. This is a severe restriction; it rules out all fields of positive characterstic, all p-adic fields, the complex numbers, and most number fields.

The group $\mathrm{GL}_n(k)$ of invertible $n \times n$ matrices over k acts on the space of quadratic forms as a linear change of variables. If T is any invertible linear transformation on V, and A is the matrix of a quadratic form f on V, then we have

$$f(Tv) = (Tv)^t A(Tv) = v^t(T^t AT)v$$

where $T^t AT$ is a symmetric matrix that defines another quadratic form.

Definition 9.2. Two quadratic forms f and g are *equivalent* if $g(v) = f(Tv)$ for some $T \in \mathrm{GL}_n(k)$. This defines an equivalence relation on the set of all quadratic forms of the same dimension over the field k.

Note that, in general, the matrices $T^t AT$ and $T^{-1}AT$ are not the same, this $\mathrm{GL}_n(k)$ action is not the same as its action by conjugation. In particular, equivalent symmetric matrices need not be similar, as can be seen by the fact that equivalent matrices may have different determinants:

$$\det(T^t AT) = \det(T^t)\det(A)\det(T) = \det(T)^2\det(A).$$

Definition 9.3. The *rank* of a quadratic form is the rank of its matrix; rank is clearly preserved under equivalence. A quadratic form is *non-degenerate* if it has full rank, equivalently, the determinant of its matrix is nonzero.

If B is the symmetric bilinear form associated to a non-degenerate quadratic form on V, then each nonzero $v \in V$ defines a nonzero linear map $w \to B(v, w)$ (otherwise the matrix of the form with respect to a basis including v would have a zero row).

Definition 9.4. The *discriminant* of a nondegenerate quadratic form with matrix A is the image of $\det A$ in $k^\times/k^{\times 2}$; it is clearly preserved by equivalence.

Inequivalent forms may have the same discriminant; over $\mathbb{C}$ for example, every nondegenerate form has the same discriminant (in fact all nondegenerate forms of the same dimension are equivalent). However, quadratic forms with different discriminants cannot be equivalent; this implies that over $\mathbb{Q}$, for example, there are infinitely many distinct equivalence classes of quadratic forms in every dimension $n > 0$.

A quadratic form is said to be *diagonal* if its matrix is diagonal.

Theorem 9.5. *Every quadratic form is equivalent to a diagonal quadratic form.*

Proof. We proceed by induction on the dimension n. The base cases $n \leq 1$ are trivial. Let f be a quadratic form on a vector space V, and let B be the corresponding symmetric bilinear form. If f is the zero function then its matrix is zero, hence diagonal, so assume otherwise and pick $v \in k^n$ so that $f(v) \neq 0$. The map $x \to B(x, v)$ is a nonzero linear map from k^n to k, hence surjective, so its kernel $v^\perp = \{x \in V : B(x, v) = 0\}$ has dimension $n - 1$. We know that $v \notin v^\perp$, since $B(v, v) = f(v) \neq 0$, so $V \simeq \langle v\rangle \oplus v^\perp$. Thus any $y \in V$ can be written as $y = y_1 + y_2$ with $y_1 \in \langle v\rangle$ and $y_2 \in v^\perp$. We then have

$$f(y_1 + y_2) = B(y_1 + y_2, y_1 + y_2) = B(y_1, y_1) + B(y_2, y_2) + 2B(y_1, y_2) = f(y_1) + f(y_2),$$

since $B(y_1, y_2) = 0$ for any $y_1 \in \langle v\rangle$ and $y_2 \in v^\perp$. By the inductive hypothesis, the restriction $f|_{v^\perp}$ of f to $v^\perp$ can be diagonalized (that is, there is a diagonal quadratic form on $v^\perp$ that is equivalent to $f|_{v^\perp}$), and the same is certainly true for the restriction of f to the 1-dimensional subspace $\langle v\rangle$, thus f can be diagonalized. $\square$

So to understand equivalence classes of quadratic forms we can restrict our attention to diagonal quadratic forms.

Example 9.6. The quadratic form $x^2 + y^2$ is equivalent to $2x^2 + 2y^2$, since

$$(x+y)^2 + (x-y)^2 = 2x^2 + 2y^2,$$

but it is not equivalent to $3x^2 + 3y^2$. Indeed, for $x^2 + y^2$ to be equivalent to $\alpha x^2 + \beta y^2$ we must have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+c^2 & ab+cd \\ ab+cd & b^2+d^2 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix},$$

and in particular, α and β must both be sums of squares, which 3 is not.

Thus equivalence of quadratic forms depends on arithmetic properties of the field k.

Definition 9.7. A quadratic form f on V *represents* $a \in k$ if a lies in the image of $f\colon V \to k$. Equivalent forms necessarily represent the same elements (but the converse need not hold).

Example 9.8. The form $x^2 - 2y^2$ represents -7 but not 0.

The constraint that $x \neq 0$ is critical, otherwise every quadratic form would represent 0; the quadratic forms that represent 0 are of particular interest to us.

Theorem 9.9. *If a nondegenerate quadratic form f represents* 0 *then it represents every element of k.*

Proof. Assume $f(v) = 0$ for some $v \in V$. Since f is nondegenerate, there exists $w \in V$ with $B(v,w) \neq 0$, and v and w must be independent, since $B(v,v) = f(v) = 0$ and therefore $B(v,xv) = cB(v,v) = 0$ for any $c \in k$. For any $x \in k$ we have

$$f(xv+w) = B(xv+w, xv+w) = B(v,v)x^2 + 2B(v,w)x + B(w,w) = ax + b,$$

with $a = 2B(v,w) \neq 0$ and $b = f(w)$. For any $c \in k$ we can solve $ax + b = c$ for x, proving that f represents $c = f(xv+w)$. □

Our main goal is to prove the following theorem of Minkowski, which was generalized to number fields by Hasse.

Theorem 9.10 (Hasse-Minkowski)**.** *A quadratic form over $\mathbb{Q}$ represents* 0 *if and only if it represents* 0 *over every completion of $\mathbb{Q}$, that is, over $\mathbb{Q}_p$ for all primes $p \leq \infty$.*

This is an example of a *local-global* principle. We have an object f (in this case a quadratic form) defined over a "global" field (in this case $\mathbb{Q}$) and a certain property of interest (in this case representing 0). Since f is defined over the global field, we can also consider f as an object over any of the "local fields" associated to the global field (in this case the completions of $\mathbb{Q}$). If f satisfies the property of interest over the global field then it typically must satisfy this property over every local field (this is certainly true in our case), but the question is whether the converse holds. In the case of quadratic forms representing 0, the answer is "yes", but in many other cases we will see later in this the answer is "no," and it is a major point of interest in arithmetic geometry to understand exactly when and how various local-global principles can fail.

18.782 Introduction to Arithmetic Geometry
Fall 2013