

Math 493 Lecture 20

Thomas Cohn

11/13/19

Recall from last time: We have F , a field not of characteristic 2, V , a finite dimensional F -vector space, and $\langle \cdot, \cdot \rangle$, a symmetric bilinear form on V ($\langle \cdot, \cdot \rangle : V \times V \rightarrow F$).

Prop: (From last time) there is an orthogonal basis for V , i.e., a basis (e_1, \dots, e_n) s.t. $\langle e_i, e_j \rangle = 0$ for $i \neq j$, if and only if $V \cong [a_1, \dots, a_n]$ for some choice of $a_1, \dots, a_n \in F$, for which $a_i = \langle e_i, e_i \rangle$.

Notation: given $a_1, \dots, a_n \in F$, $[a_1, \dots, a_n]$ is the quadratic space with vector space F^n and the form is

$$\langle e_i, e_j \rangle = \begin{cases} 0 & i \neq j \\ a_i & i = j \end{cases}$$

For $[a_1, \dots, a_n]$ in the standard basis, the matrix of the form is the diagonal matrix

$$\begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix}$$

Recall: The kernel of a quadratic space V is $\{v \in V \mid \langle v, w \rangle = 0, \forall w \in V\}$.

Defn: We say V is **non-degenerate** if $\ker V = \{0\}$.

Prop: Say $V = [a_1, \dots, a_n]$. The following are equivalent:

- (1) V is non-degenerate
- (2) $a_i \neq 0, \forall i$
- (3) The discriminant is nonzero

Proof: (2) \Leftrightarrow (3) is clear because the discriminant is $a_1 \cdots a_n$.

If some $a_i = 0$, then $\langle e_i, e_j \rangle = 0, \forall j$. So $e_i \in \ker V$, as $\langle e_i, \sum_{j=1}^n \alpha_j e_j \rangle = \sum_{j=1}^n \alpha_j \langle e_i, e_j \rangle = 0$. So V is degenerate.

Say all a_i are nonzero. Then let $v = \alpha_1 e_1 + \cdots + \alpha_n e_n$ be a nonzero element of V . So $\exists \alpha_i \neq 0$. So $\langle v, e_i \rangle = \alpha_i \langle e_i, e_i \rangle = \alpha_i a_i \neq 0$. So $v \notin \ker V$, so $\ker V = \{0\}$. \square

Cor: Every V is isomorphic to $U \perp W$, where the form is identically 0 on U and W is non-degenerate.

Proof: Write $V = [a_1, \dots, a_n]$. Say $a_1, \dots, a_m = 0, a_{m+1}, \dots, a_n \neq 0$. Then let $U = [a_1, \dots, a_m]$ and $W = [a_{m+1}, \dots, a_n]$. \square

This is great! It allows us to basically always work with non-degenerate forms.

Observe that for any field F , we have $[a] \cong [ab^2]$, for any $b \in F^\times$.

Proof: Let $V = [a]$ for basis e with $\langle e, e \rangle = a$. Let $W = [ab^2]$ for basis f with $\langle f, f \rangle = ab^2$. Then define a linear map $T : V \rightarrow W$ where $e \mapsto \frac{1}{b}f$. We have

$$\langle T(e), T(e) \rangle = \left\langle \frac{1}{b}f, \frac{1}{b}f \right\rangle = \left(\frac{1}{b}\right)^2 \langle f, f \rangle = \left(\frac{1}{b}\right)^2 ab^2 = a = \langle e, e \rangle$$

so T is an isometry. Thus, $V \cong W$. In fact, we have $[a_1, \dots, a_n] \cong [a_1 b_1^2, \dots, a_n b_n^2]$ for any $b_1, \dots, b_n \in F^\times$. \square

Prop: Two non-degenerate quadratic spaces over \mathbb{C} are isometric iff they have the same dimension.

Proof: The same dimension requirement is obviously necessary.

By our previous observation, $[a_1, \dots, a_n] \cong [1, \dots, 1]$ if a_1, \dots, a_n are all nonzero (we can select $b_i = \frac{1}{\sqrt{a_i}}$). In particular, $[a_1, \dots, a_n] \cong [a'_1, \dots, a'_n]$ if both are non-degenerate. \square

Over \mathbb{R} , if $a > 0$, then $[a] \cong [1]$, and if $a < 0$, then $[a] \cong [-1]$. (In both cases, take $b = 1/\sqrt{|a|}$). In general,

$$[a_1, \dots, a_n] \cong [\underbrace{1, \dots, 1}_r, \underbrace{-1, \dots, -1}_{n-r}]$$

Thm: (Sylvester's Law of Inertia) The number r is well-defined, i.e.,

$$[\underbrace{1, \dots, 1}_p, -1, \dots, -1] \cong [\underbrace{1, \dots, 1}_q, -1, \dots, -1] \Rightarrow p = q$$

Proof: Let V be a non-degenerate quadratic space. Say e_1, \dots, e_n and f_1, \dots, f_n are orthogonal bases s.t.

$$\langle e_i, e_i \rangle = \begin{cases} 1 & 1 \leq i \leq p \\ -1 & p < i \leq n \end{cases} \quad \text{and} \quad \langle f_i, f_i \rangle = \begin{cases} 1 & 1 \leq i \leq q \\ -1 & q < i \leq n \end{cases}$$

Let $U = \text{span}(e_1, \dots, e_p)$ and $W = \text{span}(f_{q+1}, \dots, f_n)$. We claim $U \cap W = \{0\}$.

Let $v \in U \cap W$. Then

$$\begin{aligned} v \in V &\Rightarrow v = \alpha_1 e_1 + \dots + \alpha_p e_p, \alpha_i \in \mathbb{R} &\Rightarrow \langle v, v \rangle = \sum_{i=1}^p \alpha_i^2 \geq 0 \\ v \in W &\Rightarrow v = \beta_{q+1} f_1 + \dots + \beta_n f_n, \beta_i \in \mathbb{R} &\Rightarrow \langle v, v \rangle = \sum_{i=q+1}^n \beta_i^2 \leq 0 \end{aligned}$$

So $\langle v, v \rangle = 0$, so $v = 0$.

Thus, we have $U \cap W = \{0\}$, so $\dim U + \dim W \leq \dim V$. Thus, $p + (n - q) \leq n$, so $p \leq q$. We can now repeat our argument in the opposite direction, to obtain $q \leq p$, so we have $q = p$. \square

In summary, if V is a non-degenerate quadratic space over \mathbb{R} of dimension n , $\exists! r, s$ s.t. $r + s = n$ and $V \cong [\underbrace{1, \dots, 1}_r, \underbrace{-1, \dots, -1}_s]$.

Defn: (r, s) is the **signature** of V .

Let $F = \mathbb{F}_p$ (p odd, i.e., $p \neq 2$).

Prop: $F^\times / (F^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$.

Proof: \mathbb{F}^\times is cyclic of even order. \square

Proof 2: Let $f : F^\times \rightarrow F^\times$ take $x \mapsto x^2$.

This is a group homomorphism - $f(xy) = (xy)^2 = x^2 y^2 = f(x)f(y)$.

$\text{im}(f) = (F^\times)^2$. $\text{ker}(f) = \{x \in F^\times \mid x^2 = 1\}$. Well,

$$\begin{aligned} x^2 = 1 &\Leftrightarrow x^2 - 1 = 0 \\ &\Leftrightarrow (x+1)(x-1) = 0 \\ &\Leftrightarrow x+1 = 0 \text{ or } x-1 = 0 \\ &\Leftrightarrow x = -1 \text{ or } x = 1 \end{aligned}$$

So by the First Isomorphism Theorem, $\#(F^\times)^2 = \#\text{im}(f) = \frac{\#F^\times}{\#\ker(f)} = \frac{\#F^\times}{2}$.
Thus, $\#F^\times/(F^\times)^2 = 2$. \square

In summary, $\exists a \in F^\times$ s.t. every element of F^\times has the form b^2 or ab^2 , for some $b \in F^\times$. This a is a non-square, and is not unique. Sometimes, we can have $a = -1$; other times, we cannot. In fact, -1 is a square iff $p \equiv 1 \pmod{4}$.

Ex: Let $p = 43$. Then $p \equiv 3 \pmod{4}$, so -1 is not a square, so $a = -1$ is allowed. So every element of \mathbb{F}_{43}^\times has the form $\pm b^2$ for some $b \in \mathbb{F}_{43}^\times$.

Ex: Let $p = 41$. Then $p \equiv 1 \pmod{4}$, so -1 is a square, so we can't use $a = -1$. 2 is also bad, as $2 = 17^2 \pmod{41}$.

Exer: Find some value for a for $p = 41$.

Fix $\varepsilon \in F^\times$ not a square. Just as in the real case, for any $a_1, \dots, a_n \in F^\times$, we have an isomorphism $[a_1, \dots, a_n] \cong \underbrace{[1, \dots, 1]}_r, \underbrace{[\varepsilon, \dots, \varepsilon]}_{n-r}$. But r is **not** well-defined – only $r \pmod{2}$ is, because $[\varepsilon, \varepsilon] \cong [1, 1]$.

The key point of all of this is every element of F is a sum of 2 squares.