Last time:

Classified quadratic forms over $\mathbb{F}_q$:

Prop Any n-dim quadratic form over $\mathbb{F}_q$ is $\simeq$

$$\langle 1, 1, \dots, 1, d \rangle, \text{ some } d \in \mathbb{F}_q^\times.$$

There are two iso classes of n-dim quadratic forms over $\mathbb{F}_q$, based on $d \in \mathbb{F}_q^\times / \mathbb{F}_q^{\times 2} \simeq \mathbb{Z}/2$

d is the called the determinant of the quadratic form

(b/c any 2-d quadratic form represents 1, i.e. has a vector v w/ $v \cdot v = 1$).

Rmk: Works over any field of u-inv ≤ 2, e.g. $\mathbb{C}(t)$

& $d \in F^\times / F^{\times 2}$.

Today: study isomorphisms classes & invariants of quadratic forms.

$a \in F^\times$
$u \in F^\times$

Ex) $\langle a \rangle \cong \langle au^2 \rangle$

$\langle a_1, a_2 \rangle \cong \langle a_2, a_1 \rangle$

$\langle a_1, a_2 \rangle \cong \langle a_1 + a_2, \frac{a_1 a_2}{a_1 + a_2} \rangle$

<u>Theorem</u> (Witt's chain equivalence theorem)

Suppose $\langle a_1, \dots, a_n \rangle \cong \langle b_1, \dots, b_n \rangle$.
Then we can get from the tuple $(a_1, \dots, a_n)$ to $(b_1, \dots, b_n)$ in a sequence of steps where at each stage only two entries are

changed via the moves of the above example.

Very useful to define iso invariants.

Pf: ~~Let's~~ say that $(a_1, \ldots, a_n)$ & $(a_1', \ldots, a_n')$ are chain equivalent if can get from first to second by above moves.

Show that $(a_1, \ldots, a_n)$ is chain equivalent to $(b_1, b_2', \ldots, b_n')$.

$\Rightarrow$ this means $\langle b_2', \ldots, b_n' \rangle \cong \langle b_2, \ldots, b_n \rangle$ by induction can make that into a chain equivalence, & then compose.

We know that if $(a_1, \ldots, a_n)$ is chain equivalent to some triple

$(a_1', \ldots, a_n')$, then

then $\langle a_1', \ldots, a_n' \rangle \cong \langle b_1, \ldots, b_n \rangle$

can solve $(*)$

$$b_1 = \sum a_i' x_i^2,$$

Find the chain equivalent triple $(a_1', \ldots, a_n')$

s.t. the number of nonzero terms in $(*)$ is minimized.

Claim: this solves the problem.

Suppose $b_1 = \sum_{i=1}^{r} a_i' x_i^2$ w/ r minimal.

By rescaling, $x_i = 1$

so $b_1 = \sum_{i=1}^{r} a_i'$.

Claim: $r = 1$ so $b_1 = a_1'$.

Why? $b_1 = a_1' + a_2' + \cdots + a_r'$.

& if $r > 1$, (by minimality $a_1' + a_2' \neq 0$.)

$(a_1', a_2', \ldots, a_n')$

$\updownarrow$

$\left(a_1' + a_2', \frac{a_1' a_2'}{a_1' + a_2'}, a_3', \ldots, a_n'\right)$

but then

$b_1 = (a_1' + a_2') + a_3' + \cdots + a_r'$

and this is a smaller expression ($r-1$ nonzero terms), a contradiction

(i.e., look at all chain equivalent tuples $(a_1', \ldots, a_n')$ that minimize the "b_1-length" $\rightsquigarrow$ must contain a b_1.)

Then continue by induction on dimension.

Def (Grothendieck-Witt ring)

The abelian gp $GW(F)$

$$= \left\{ \begin{array}{c} \text{all formal differences of} \\ \text{isomorphism classes of} \\ \text{quadratic forms over } F \end{array} \right\}.$$

= all expressions
$(V, q) - (W, q')$.

analogous to defn of integers as formal differences of natural numbers.

Ex) $(V_1, q_1) - (W_1, q_1') = (V_2, q_2) - (W_2, q_2')$

if $V_1 \oplus W_2 \cong V_2 \oplus W_1$.

This is actually a commutative ring, via the tensor product of quadratic (or symmetric bilinear forms).
(b/c can tensor symmetric bilinear forms).

Ex) $F = \mathbb{C}$,
then $GW(F) = \mathbb{Z}$

Two quadratic forms are isomorphic iff they yield <u>equal</u> elements of $GW(F)$.

Presentation of
$GW(F)$ as abelian gp:

Generators: $\langle a \rangle$ $\quad a \in F^\times$.

Relations: $\langle au^2 \rangle = \langle a \rangle \quad u \in F^\times$

$$\langle a_1 \rangle + \langle a_2 \rangle = \langle a_1 + a_2 \rangle + \left\langle \frac{a_1 a_2}{a_1 + a_2} \right\rangle.$$

Multiplication $\langle a \rangle \langle b \rangle = \langle ab \rangle$.

Observe: in the ring $GW(F)$ there is an ideal generated by $\langle 1 \rangle + \langle -1 \rangle$ (hyperbolic plane).

This ideal is $\mathbb{Z}$.
(b/c a hyperbolic form $\otimes$ any form is hyperbolic).
e.g. $\langle 1,-1\rangle \simeq \langle a,-a\rangle$.

So have an ideal
$$\mathbb{Z}\langle 1,-1\rangle \subseteq GW(F).$$

<u>Def</u> The Witt ring $W(F)$ is the quotient $GW(F)/\mathbb{Z}\langle 1,-1\rangle$.

In Witt ring, any class is represented by a <u>unique</u> anisotropic form (V,q).

For example the

additive inverse in $W(F)$
of (V, q) is $(V, -q)$.

(b/c $(V,q) \oplus (V, -q)$ is hyperbolic plane).

To add elts in Witt ring, add anisotropic forms, then remove hyperbolic part.

In the Witt ring, have relations in GW but also $\langle a \rangle = -\langle -a \rangle$.

A central question: what does the Witt ring of a given field look like?

Ex) $W(\mathbb{C}) \xrightarrow[\text{dim mod } 2]{=} \mathbb{Z}/2$

In general, any field F, have a dimension map

$$GW(F) \to \mathbb{Z}$$

$$W(F) \to \mathbb{Z}/2.$$

Ex) $W(\mathbb{R}) \xrightarrow[\text{signature}]{\sim} \mathbb{Z}$

In general, if F is a field which has an ordering (notion of positive & negative elements), then can define a generalized signature

$$W(F) \longrightarrow \mathbb{Z}$$

Pfister: any elt in kernel of all these is torsion

Can classify prime ideals of $W(F)$ in terms of orderings of F