Local and global fields, and local-global principles (LGP).

Esp. Hasse-Minkowski:

If q is a q.f. $/\mathbb{Q}$, then

q is isotropic $/\mathbb{Q}$ $\iff$ q isotropic $/\mathbb{R}$ and $/\mathbb{Q}_p$ for all p.

Global fields F:

① Finite extensions of $\mathbb{Q}$: # fields.

② Finite extensions of $\mathbb{F}_p(t)$: global function fields.

discrete valuation — (non-archi) absolute value — Dedekind domain

$v \longleftrightarrow |\cdot|_v$ on $F = \mathrm{frac}\, R$

Completion $F_v \supset \widehat{R}_m \supset R_{(m)} \supset R$ ← Ded. dom

F_v ($\supset F$): cdvf; $\widehat{R}_m$: cdvr; $R_{(m)}$: dvr

Ex. $\mathbb{Q}_p \supset \mathbb{Z}_p \supset \mathbb{Z}_{(p)} \supset \mathbb{Z}$

(also archimedean abs val; not discr. val.)

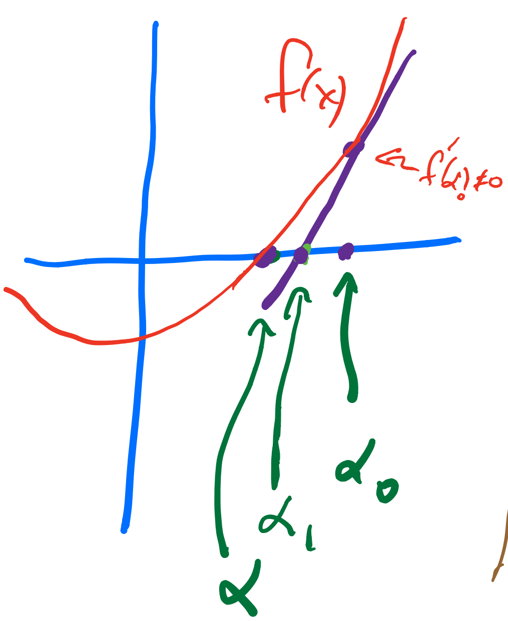
Ex. $\mathbb{R} \supset \mathbb{Q}$

A key result for cdvr's: (π) — uniformizer, $v(\pi)=1$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\;\;\shortparallel$

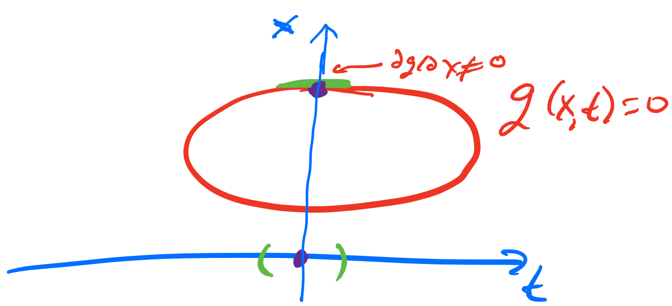
<u>Hensel's Lemma</u> R cdvr, $\mathfrak{m}$ = max'l ideal, $f(x) \in R[x]$, $\alpha_0 \in R$, $f(\alpha_0) \in \mathfrak{m}$, $f'(\alpha_0) \notin \mathfrak{m}$. Then $\exists\, \alpha \in R$ st $f(\alpha) = 0$ and $\alpha \equiv \alpha_0 \pmod{\mathfrak{m}}$.

Pf is essentially to use Newton's method (Newton-Raphson algorithm) together with completeness to get convergence to a solution.



Also parallel to Implicit Fn Thm

$\mathbb{R}[[t]] \longleftrightarrow \left\{\begin{array}{l}\text{functions on } t\text{-line} \\ \text{near } t=0\end{array}\right\}$



In Hensel's Lemma we have:

$v(f(\alpha_0)) > 0,\ v(f'(\alpha_0)) = 0 \Rightarrow \exists \alpha : f(\alpha) = 0,\ v(\alpha - \alpha_0) > 0.$

Strong form of Hensel's Lemma:

Say $\alpha_0 \in R$, $n \geq 0$, $r > 0$,

$v(f(\alpha_0)) \geq 2n + r$, $v(f'(\alpha_0)) = n$;

then $\exists \alpha \in R$ st

$f(\alpha) = 0$, $v(\alpha - \alpha_0) \geq n + r$.

(Usual form is the case $n = 0, r = 1$)

Ex. $R = \mathbb{Z}_p$
$m = (p)$
$k = \mathbb{F}_p$

Using the usual form, we get:

Prop R cdvr, max'l ideal m, residue fld $k = R/m$.

Say char $k \nmid r$. Let $u \in U := R^\times$ with

image $\bar{u} \in k^\times$. Then,

$$u \in R^{\times r} \Leftrightarrow \bar{u} \in k^{\times r}.$$

Ex. $R = k[[t]]$
$m = (t)$
$U = \{$non-0 constant term$\}$ $= R - m$

Cor Here, if $u \in R$ and $u \equiv 1 \pmod{m}$ then

$u \in U$, $\bar{u} = 1 \in k^{\times r}$, and $u \in R^{\times r} \subset F^{\times r}$.

$F = \operatorname{frac} R$

uniformizer

More generally, every non-0 element $a \in F$

can be written as $a = u\pi^n$,

$v(u) = 0$

where $n = v(a)$, and u is a unit in R. Have:

$$a \in F^{\times r} \Leftrightarrow r \mid n \text{ and } \bar{u} \in k^{\times r}.$$

In particular, take $r=2$, and char $k \neq 2$.

$u \in U = R^\times$ is a square $\iff \bar{u} \in k^\times$ is a square.

$u\pi^n \in F^{\times 2} \iff \bar{u} \in k^{\times 2}$ and n is even.

This leads to a map

$$k^\times/k^{\times 2} \longrightarrow F^\times/F^{\times 2}$$

as follows:

Take a square class in $k^\times/k^{\times 2}$;

pick a representative $\bar{a} \in k^\times$.

Choose a lift:
$$\begin{array}{ccc} a \in R^\times = U \subset F^\times \\ \downarrow \quad \downarrow \\ \bar{a} \in k^\times \end{array}$$

Send the given square class in $k^\times/k^{\times 2}$

to the square class of a in $F^\times/F^{\times 2}$

Well defined: For a different lift a'

$a'/a \equiv 1 \pmod{\mathfrak{m}}$, so $a'/a \in F^{\times 2}$,

So get the same class.

Easy to check this is an injective hom,

and image $= \{$square classes of $u \mid v(u)=0\}$ i.e. unit

Get $1 \to k^\times/k^{\times 2} \xrightarrow[i]{} F^\times/F^{\times 2} \xrightarrow{v} \mathbb{Z}/2 \to 0$

$\exists$ section
$1 \leftarrow 0$
$\pi \leftarrow 1$

v is well def mod 2 on sq. classes

As a result we get a map

$$i : \hat{W}(k) \longrightarrow \hat{W}(F)$$
$$\langle a_1, \dots, a_n \rangle \longmapsto \langle i(a_1), \dots, i(a_n) \rangle$$

Also define

$$j : \hat{W}(k) \longrightarrow \hat{W}(F)$$
$$\langle a_1, \dots, a_n \rangle \longmapsto \langle i(a_1)\pi, \dots, i(a_n)\pi \rangle$$
$$= \langle \pi \rangle \, i(\langle a_1, \dots, a_n \rangle).$$

We will show: (i,j) induces a group iso $W(k) \oplus W(k) \xrightarrow{\sim} W(F)$.

(Theorem of Springer)

This follows from:

Claim $(i,j) : \hat{W}(k) \oplus \hat{W}(k) \longrightarrow \hat{W}(F)$
$$(\alpha, \beta) \longmapsto i(\alpha) + j(\beta)$$
is a surjective group hom with

$$\ker(i,j) = \mathbb{Z} \cdot (h, -h),$$

i.e. have a group iso

$$f = (i,j) : \big(\hat{W}(k) \oplus \hat{W}(k)\big) / \mathbb{Z}\cdot(h,-h) \xrightarrow{\sim} \hat{W}(F).$$

Viz: To get the thm from the claim: In the claim, on left mod out by $\mathbb{Z}h \oplus 0$ and on right " " " $\mathbb{Z}h$ ← image of $\mathbb{Z}h \oplus 0$

and get $W(k) \oplus W(k) \xrightarrow{\sim} W(F)$.

To prove the above claim re

$(i, j): \hat{W}(k) \oplus \hat{W}(k) \longrightarrow \hat{W}_0(F)$:

note $(h, -h) \xmapsto{(i,j)} \underset{\overset{\shortparallel}{h-h}}{0}$

$\overset{\shortparallel}{(\langle 1,-1\rangle, -\langle 1,-1\rangle)} \mapsto \langle 1,-1\rangle - \langle \pi, -\pi\rangle$

So $\mathbb{Z}\cdot(h,-h) \subset \ker(i,j)$; i.e. have

$$\left(\hat{W}(k) \oplus \hat{W}(k)\right) / \mathbb{Z}\cdot(h,-h) \to \hat{W}(F).$$

Want this is iso. STS $\exists$ inverse, g.

Define $g(\langle a \rangle) = \begin{cases} (\langle \bar{u}\rangle, 0), & n \text{ even} \\ (0, \langle \bar{u}\rangle), & n \text{ odd} \end{cases}$ where $a = u\pi^n$

And extend to $\langle a_1, \dots, a_n\rangle$.

Using chain equivalence, can check this is well defined, and is a 2-sided inverse to f. So ✓.

So we get the claim, + get

$(i, j): W(k) \oplus W(k) \xrightarrow{\sim} W(F)$.

We can also describe the inverse map.

First: Each square class has a representative of the form $u \in U$ or πu, for $u \in U$.
So a reg. q.f. q over F can be put in the form $q = q_1 \perp \langle \pi \rangle q_2$ where

$q_1 = \langle u_1, \ldots, u_r \rangle$, $q_2 = \langle u_{r+1}, \ldots, u_n \rangle$.
for some units $u_i \in U = R^\times \subset F^\times$.

Get q.f.'s over k:
$\bar{q}_1 = \langle \bar{u}_1, \ldots, \bar{u}_r \rangle$, $\bar{q}_2 = \langle \bar{u}_{r+1}, \ldots, \bar{u}_n \rangle$.
Now define $\partial_1 : W(F) \to W(k)$ by $q \longmapsto \bar{q}_1$.
and similarly define ∂_2 using $\bar{q}_2$.
("1st & 2nd residue maps")

The inverse of $(i, j) : W(k) \oplus W(k) \to W(F)$
is $(\partial_1, \partial_2) : W(F) \longrightarrow W(k) \oplus W(k)$

We can also use this to write
$$W(F) \cong W(k)[C_2]$$ (group ring)

where $W(k)$ is identified with its image in $W(F)$ under i.

Under above hypotheses (incl. char $k \neq 2$):

Prop Say $q = \langle u_1, \dots, u_r \rangle$ with $u_i \in U = R^\times$.
Then: q is isotropic over F
$\iff$ $\bar{q} = \langle \bar{u}_1, \dots, \bar{u}_r \rangle$ is isotropic over k.

Proof ($\Rightarrow$) $q(v) = 0$ for some $v = (c_1, \dots, c_r) \neq 0$,
$c_i \in F$, not all 0.
After multiplying v by some π^m,
WMA each $c_i \in R$ and some $c_i \in U$.
So $\bar{q}(\bar{v}) = 0 \in k$ and $\bar{v} \neq 0 \in k$.
So $\bar{q}$ is isotropic over k.
($\Leftarrow$) Since $\bar{q}$ is regular + isotropic,
$\bar{q} = h \perp \bar{q}'$ ← $\dim r-2$, can lift to a q' over F with entries in U.
↑ hyperbolic plane/k
So q and $h \perp q'$ have same image in $W(k) \oplus W(k)$ under (∂_1, ∂_2),
hyp.pl./F
viz. $(h \perp \bar{q}', 0)$. So
$q \cong h \perp q'$, isotropic. ✓

As a consequence, in this situation:

Theorem (Springer)

Let $q = q_1 \perp \langle \pi \rangle q_2$ over F, with reg. q.f. /F

q_1, q_2 diagonal and each entry a unit.

Then q is anisotropic $/F$

$\Longleftrightarrow$ $\bar{q}_1, \bar{q}_2$ are anisotropic $/k$.

$$\begin{array}{cc} \bar{q}_1, & \bar{q}_2 \\ \shortparallel & \shortparallel \\ \partial_1 q & \partial_2 q \end{array}$$

Here: $q = \langle u_1, \dots, u_r, \pi u_{r+1}, \dots, \pi u_s \rangle$ u_i: units in R

$\bar{q}_1 = \langle \bar{u}_1, \dots, \bar{u}_r \rangle$, $\bar{q}_2 = \langle \bar{u}_{r+1}, \dots, \bar{u}_s \rangle$.

This reduces anisotropy $/F$ to

" $/k$.

Ex. If $F = \mathbb{Q}_p$, then we're reduced to checking anisotropy $/\mathbb{F}_p$.

Equivalent version of thm:

q isotropic $\Longleftrightarrow$ $\bar{q}_1$ or $\bar{q}_2$ is isotropic.

Will prove in this form.

Pf of thm:

i) Say $\bar{q}_i$ isotropic ($i=1$ or $i=2$).

By prev prop, q_i is isotropic: $q_i(v)=0$, $v \neq 0$

(Here $q_1 = \langle u_1, \ldots, u_r \rangle$, $q_2 = \langle u_{r+1}, \ldots, u_s \rangle$)

So q is isotropic (using $(v,0)$ or $(0,v)$ resp.) ✓

ii) Say q is isotropic. Also q regular,

so $q \cong h \perp q'$. $\dim q' = \dim q - 2$.

So q, q' represent the same elt of $W(F)$.

Have $q = q_1 \perp \langle \pi \rangle q_2$. Write $q' = q_1' \perp \langle \pi \rangle q_2'$.

In $W(k) \oplus W(k)$, $(\partial_1, \partial_2)(q) = (\partial_1, \partial_2)(q')$

$$(\partial_1,\partial_2)(q) = (\bar{q}_1, \bar{q}_2), \qquad (\partial_1,\partial_2)(q') = (\bar{q}_1', \bar{q}_2')$$

So $\bar{q}_i$, $\bar{q}_i'$ represent the same elt of $W(k)$

But $\dim q' < \dim q$

$$\dim q' = \dim \bar{q}_1' + \dim \bar{q}_2', \qquad \dim q = \dim \bar{q}_1 + \dim \bar{q}_2$$

So $\dim \bar{q}_i' < \dim \bar{q}_i$ for $i = 1$ or 2.

But $\bar{q}_i$, $\bar{q}_i'$ give same class in $W(k)$, so differ by copies of h. So $\bar{q}_i$ contains h, & is isotropic.

Cor If char $k \neq 2$, $u(F) = 2u(k)$.

Proof Let $n = u(k)$.

So $\exists$ anisotropic q.f. $\bar{q}$ /k of dim n, (1)

but every q.f. /k of dim $> n$ is isotropic. (2)

WTS same for F, with $2n$.

WMA $\bar{q}$ diagonal. Lift to a diagonal q.f. q / F with entries in U.

(anisotropic)

Then $q \perp \langle \pi \rangle q$ has dim $2n$ /F, + is anisotropic by the above thm. (1) ✓ /F

For (2) /F take a q.f. q' /F of dim $> 2n$.

WTS q' isotropic. We have

$2n < \dim q' = \dim \partial_1(q') + \dim \partial_2(q')$

so $\dim \partial_i(q') > n$ for $i = 1$ or 2.

So this $\partial_i(q')$ is isotropic /k.

By above thm, q' is isotropic /F. ✓

Cor If F is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ and $p \neq 2$ then $u(F) = 4$.

In Cor, F is an arbitrary non-archimedean local field (i.e. $\neq \mathbb{R}, \mathbb{C}$) of res char $\neq 2$.

In fact: Cor also holds if char $k = 2$ — a more involved proof due to Springer.

As another application of $u(F) = 2u(k)$:

$u(\mathbb{Q}_p((t))) = 8$:

Take $R = \mathbb{Q}_p[[t]]$, $F = \mathbb{Q}_p((t))$, $k = \mathbb{Q}_p$

$u = 4$ by above

$\therefore u = 8$

Similarly,

$u(\mathbb{F}_p((t))((s))) = 8$:

$R = \mathbb{F}_p((t))[[s]]$, $F = \mathbb{F}_p((t))((s))$, $k = \mathbb{F}_p((t))$

Let F be a local field of res. char $= p \neq 2$;

so a finite extension of $\mathbb{F}_p((t))$ or of $\mathbb{Q}_p$

so iso to $\mathbb{F}_q((s))$, $q = p^{\nu}$ (eg if take an extn of $\mathbb{F}_p$, + $s^r = t$)

Let π be a uniformizer; so $v(\pi) = 1$.

($\pi = t$ for $\mathbb{F}_q((t))$; $\pi = p$ for $\mathbb{Q}_p$)

We saw

$$1 \to k^\times/k^{\times 2} \to F^\times/F^{\times 2} \to \mathbb{Z}/2 \to 0$$

$\cong$ $\mathbb{Z}/2$ since char $k \neq 2$, + k finite.

One sq class: $[1]$
one non-sq. class: $[\bar{u}]$

$\therefore |F^\times/F^{\times 2}| = 4$

lifting $\bar{u} \in k^\times$

Four classes, rep by $1, u, \pi, u\pi$ (no two in same class)

Key example:

$\bar{u} \notin k^{\times 2} \Rightarrow \bar{u} \notin D(\langle 1 \rangle)$ over k

$\Rightarrow \langle 1, -\bar{u} \rangle$ anisotropic $/k$

$\Rightarrow \langle -1, \bar{u} \rangle$ " "

$\Rightarrow q := \langle 1, -u, -\pi, u\pi \rangle$ anisotropic $/F$

by Springer's thm,

since $\partial_1(q) = \langle 1, -\bar{u} \rangle$, $\partial_2(q) = \langle -1, \bar{u} \rangle$.

Recall: up to isometry, the only anisotropic binary q.f. $/k$ is $\langle 1, -\bar{u}\rangle = x^2 - \bar{u}y^2$

So $q = \langle 1, -u, -\pi, u\pi\rangle$ is the only anisotropic qf $/F$ of dim 4 up to isometry. (by Springer & $u(k)=2$)

Here q = norm form of $\left(\frac{u,\pi}{F}\right)$.

Recall: quaternion alg's are classified by their norm forms; and a quat. alg. is a div algebra $\iff$ the norm form is anisotropic.

Conclusion:

$\left(\frac{u,\pi}{F}\right)$ is the unique quaternion division algebra over F.

The only other quat. alg. $/F$ is $M_2(F)$.

Also recall:

Quaternion algebras generate the 2-torsion in the Brauer group.

So: $Br(F)[2] \cong \mathbb{Z}/2 \cong \{\pm 1\}$.

split class $\longleftrightarrow 1$

non-split class $\longleftrightarrow -1$

Write $(a,b)_F = \pm 1$ if $\left(\frac{a,b}{F}\right) \longleftrightarrow \pm 1$ resp.

"Hilbert symbol";

"quadratic norm residue symbol"

(mentioned earlier re Bloch-Kato Conj.)

In particular, $(u,\pi)_F = -1$

From criteria for $\left(\frac{a,b}{F}\right)$ to be split, we have

Hilbert's criterion

$(a,b)_F = 1 \Leftrightarrow \langle a, b\rangle$ represents 1

$\Longleftrightarrow a \in F$ is the norm of an elt of $F(\sqrt{b})$

In # thy if consider $(a,b)_F$ for $F = \mathbb{Q}_p$

write $(a,b)_p$. (Local class field thy)

Various p

Re quadratic extensions in # thy:

Legendre symbol $\left(\frac{a}{p}\right) = \pm 1 \longleftrightarrow a$ is/is not a square mod p

odd prime

If $a = p^\alpha x$, $b = p^\beta y$, $x, y \in U = \mathbb{Z}_p^\times$,

then $(a,b)_p = (-1)^{\alpha \cdot \beta \cdot \frac{p-1}{2}} \left(\frac{x}{p}\right)^\beta \left(\frac{y}{p}\right)^\alpha$ (Lam, Chap VI, Exercise 10)

We can also use the above to find $W(F)$:

Recall: For k a finite field $\mathbb{F}_q$ (odd order),

$$W(k) = \begin{cases} \mathbb{Z}/2[C_2] \cong (\mathbb{Z}/2)^2 \text{ as gp} & \text{if } q \equiv 1 \pmod 4 \\ \mathbb{Z}/4 \text{ (as a gp or ring)} & \text{if } q \equiv 3 \pmod 4 \end{cases}$$

as ring

Also recall $W(F) \cong W(k)[C_2]$.

So get:

$$W(F) \cong \begin{cases} \mathbb{Z}/2[C_2^2] \cong (\mathbb{Z}/2)^4 \text{ as gp} & \text{if } q \equiv 1 \pmod 4 \\ \mathbb{Z}/4[C_2] \cong (\mathbb{Z}/4)^2 \text{ as gp} & \text{if } q \equiv 3 \pmod 4 \end{cases}$$

as ring

In each case: $|W(F)| = 16$

Can also analyze $\hat{W}(F)$ and get a description:

$\mathbb{Z} \oplus (\mathbb{Z}/2)^3$, $\mathbb{Z} \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/2$, resp.

(See Lam, Ch VI, Th 2.2 (5,6).)

Since $|W(F)| = 16$, and since

$W(F) \xleftrightarrow{\text{bij}}$ (isometry classes of) anisotropic q.f. /F :

$\exists$ exactly 16 anisotropic q.f. /F, including the 0 form (up to isometry)

Prop. If $a, b \in U$, $\left(\frac{a,b}{F}\right)$ splits.

$R^\times$

Pf. If $u_1, u_2, u_3 \in U$,

$u(k) = 2$

then $\langle \bar{u}_1, \bar{u}_2, \bar{u}_3 \rangle$ is isotropic /k,

So $\langle u_1, u_2, u_3 \rangle$ - - - - - - /F.

In particular $\langle a, b, -1 \rangle$ is isotropic /F,

so $1 \in D(\langle a, b \rangle)$, so $\left(\frac{a,b}{F}\right)$ splits. ■