1. Abelian varieties in char. p

<u>Notation</u> p prime, $q = p^r$

$k = \overline{\mathbb{F}_p} \supseteq \mathbb{F}_q \supseteq \mathbb{F}_p$,

K any of these

Def 1.13 An AV $X / \mathbb{F}_q$ has a Frobenius endomorphism π_X $\left(= F^n_{X/\mathbb{F}_q}\right)$

It's an $\mathbb{F}_q$-morphism, $f \mapsto f^q$ on regular functions.

So on projective points:

$$\pi_X : (x_0 : \dots : x_n) \mapsto (x_0^q : \dots : x_n^q)$$

Hence: $X(\mathbb{F}_q)$ is fixed by π_X,

$X(\mathbb{F}_{q^m})$ – " – —— π_X^m

Def 1.14 π_X has a characteristic polynomial

$h_{\pi_X}(x) \in \underset{!}{\mathbb{Z}}[x]$

Thm 1.15

- $\deg(h_{\pi_X}) = 2\cdot \dim(X)$
- All roots of h_{π_X} have abs. value $\sqrt{q}$
- α root $\Longleftrightarrow$ $\bar{\alpha} = \frac{q}{\alpha}$ root

Thm 1.17 If $h_{\pi_X}(x) = \prod_{i=1}^{2g}(x-\alpha_i)$ over $\bar{\mathbb{Q}}$,

then

$$|X(\mathbb{F}_{q^m})| = \prod_{i=1}^{2g}(1-\alpha_i^m)$$

$\forall m \geq 1$

Write $X \sim Y$ if X isogenous to Y,
i.e. $\exists\, \varphi : X \longrightarrow Y$ surjective + finite kernel

$\Rightarrow$ equivalence relation on AV's of dim g

Thm 1.10 (Tate) $X \underset{\mathbb{F}_q}{\sim} Y \Leftrightarrow h_{\pi_X} = h_{\pi_Y}$

Also, for "every" h_π,
$\exists$ AV $Z/\mathbb{F}_q$ s.t. $h_\pi = h_{\pi_Z}$.

§ p^n- torsion in char p

For E/K elliptic curve,

$$E[p](\bar{k}) \simeq \begin{cases} 0 & \underline{\text{supersingular}} \\ \mathbb{Z}/p\mathbb{Z} & \underline{\text{ordinary}} \end{cases}$$

For X/K AV of dim g,

Def 1.19 $|X[p](\bar{k})| = p^f$, $0 \leq f \leq g$.

$f(X) = f$ is the *p-rank* of X.

Def 1.20 $f(X) = g \iff X$ ordinary.

<u>**Def 1.22**</u> X/K is <u>supersingular</u> (ss)

if $X \sim_{\bar{k}} E^g$ E ss EC

~~supersingular~~

<u>superspecial</u>

if $X \simeq_{\bar{k}} E^g$, E ss EC

So X ss $\Rightarrow f(X) = 0$,

but converse need not hold if $g \geq 3$, as we'll see.

p-rank is an isogeny invariant.

Next: $p \longrightarrow p^n, p^\infty$

isogeny $\rightarrow$ isomorphism.

Def 1.25 The *p-divisible group* of X/K is $X[p^\infty] = \varinjlim X[p^n]$ w.r.t. natural inclusions $X[p^n] \hookrightarrow X[p^{n+1}]$

Thm 2.21 (Dieudonné-Manin)

$$X[p^\infty] \sim_{k} \sum_i \left(G_{m_i,n_i} \oplus G_{n_i,m_i} \right) \oplus \underbrace{G_{1,1}^{\oplus s}}_{ss} \oplus \underbrace{\left(G_{1,0} \oplus G_{0,1} \right)^{\oplus f}}_{\text{ordinary}}$$

for $(m_i,n_i)=1$, $0 \leq s,f$ s.t. $s+f \leq g$.

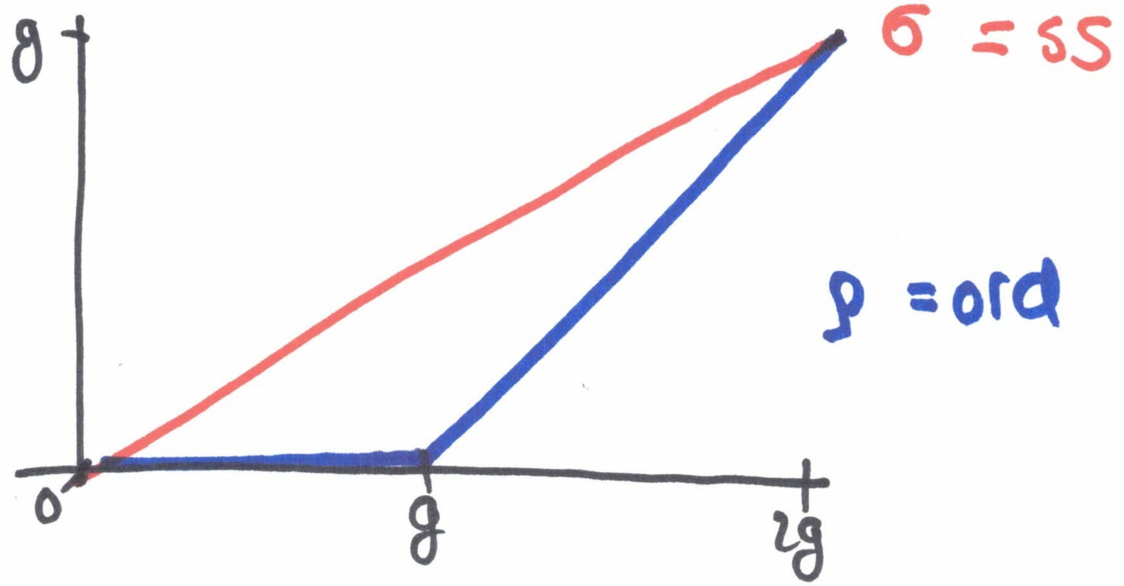
All $G_{m,n}$ are simple, dim m, height $m+n$. dual $G_{n,m}$ has dim n

$G_{m,n} \mapsto$ slope $\lambda = \frac{m}{m+n}$,
multiplicity $m+n$.

Def 2.23 The Newton polygon $\mathcal{N}(X)$ of X (of $X[p^\infty]$) is formed out of the slopes λ of $X[p^\infty]$ in non-decreasing order.

Note p-rank is number of zero slopes.

Ex 2.25



We say $\sigma \prec \rho$

Any other NP ξ satisfies $\sigma \prec \xi \prec \rho$

Example (g=3)

$$NP = \left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{2}{3}, \frac{2}{3}\right)$$

has p-rank 0 but it is not ss.

Thm (Honda-Serre)

Every symmetric NP occurs for some abelian variety.

There are three non-isomorphic group schemes $/\Bbbk$ of rank p:

$$\begin{tikzcd} \mu_p, \arrow[r, leftrightarrow, bend right, "\text{Cartier dual}"'] & \mathbb{Z}/p\mathbb{Z} & , \alpha_p = \operatorname{Spec}(\Bbbk[x]/x^p) \arrow[loop below, "\text{self-dual}"] \end{tikzcd}$$

<u>Def 1.31</u> The <u>a-number</u> of X/K is

$$a(X) := \dim_K \operatorname{Hom}(\alpha_p, X).$$

$$0 \leqslant a(X) + f(X) \leqslant g$$

So X ordinary $\Rightarrow a(X) = 0$.

Non-ord X generically has $a(X) = 1$.

[Oor] X superspecial $\Leftrightarrow a(X) = g = \dim(X)$.

$$\begin{tikzcd} X \arrow[d, phantom, "\cong_{\Bbbk}" sloped] \\ E^g \end{tikzcd}$$

Def 2.38 On $X[p]$ (group scheme) we have

$$0 = [p] = \underset{\text{Frobenius}}{F} \circ \underset{\text{Verschiebung}}{V} = V \circ F$$

Write $G = X[p]$. consider filtration

$$\begin{tikzcd}
G \arrow[r, phantom, "\supseteq"] & V(G) \arrow[rr, phantom, "\supseteq"] \arrow[dd, phantom, sloped, "\subseteq"] & & V^2(G) \arrow[rr, phantom, "\supseteq"] \arrow[dd, phantom, sloped, "\subseteq"] & & V^3(G) \arrow[r, phantom, "\supseteq"] \arrow[dd, phantom, sloped, "\subseteq"] & \cdots \\
& & VF^{-1}V(G) \arrow[ur, dash, dotted] & & VF^{-1}V^2(G) \arrow[ur, dash, dotted] & & \\
& F^{-1}V(G) \arrow[ur, phantom, sloped, "\supseteq"] \arrow[d, phantom, sloped, "\subseteq"] & & F^{-1}V^2(G) \arrow[ur, phantom, sloped, "\supseteq"] \arrow[d, phantom, sloped, "\subseteq"] & & F^{-1}V^3(G) \arrow[d, phantom, sloped, "\subseteq"] \arrow[uur, dash, dotted] & \\
& F^{-2}V(G) \arrow[urr, dash, dotted] & & \vdots \arrow[urr, dash, dotted] & & \vdots & \\
& \vdots & & & & &
\end{tikzcd}$$

Rank G is finite (p^r) $\Rightarrow$
stabilises after $< \infty$ many $(\leq 2(r-1))$ steps.

Def 2.39 Canonical filtration of $X[p] = G$

$$0 = G_0 \subseteq \dots\dots \subseteq G_s = V(G) \subseteq \dots\dots \subseteq G_t = G$$

Def 2.41 Encoded in canonical type

$$\tau = (\underset{V(G_i) = G_{v(i)}}{v}, \underset{F^{-1}(G_i) = G_{f(i)}}{f}, \rho) \longleftarrow \operatorname{rank}(G_i) = p^{\rho(i)}$$

Thm 2.43 Canonical type determines $X[p]$ up to k-isomorphism.

Note: For us: $s = g$, $t = 2g$.

Ex 2.40/2.42 $(g=3)$

Canonical filtration

$$\begin{array}{ccccccccccccc} G_0 & \subseteq & G_1 & \subseteq & G_2 & \subseteq & G_3 & \subseteq & G_4 & \subseteq & G_5 & \subseteq & G_6 \\ \| & & \| & & \| & & \| & & \| & & \| & & \| \\ 0 & \subseteq & V^2(G) & \subseteq & VF^{-1}V(G) & \subseteq & V(G) & \subseteq & F^{-1}V^2(G) & \subseteq & F^{-1}V(G) & \subseteq & G \end{array}$$

$v: V(G_i) = G_{v(i)}$ so

$v(0) = v(1) = v(2) = 0,\ v(3) = v(4) = 1,\ v(5) = 2,\ v(6) = 3$

$f: F^{-1}(G_i) = G_{f(i)}$ so

$f(0) = 3,\ f(1) = 4,\ f(2) = f(3) = 5,\ f(4) = f(5) = f(6) = 6.$

$\rho: \text{rank}(G_i) = p^{\rho(i)}$ so $\rho(i) = i \quad \forall i$

Next, canonical type $\Rightarrow$
elementary sequence $(\varphi(0)=0, \varphi(1), \ldots, \varphi(g))$

From $(\varphi(0), \ldots, \varphi(\rho(i)))$ with $\rho(i) < \rho(i+1)$
get $(\varphi(0), \ldots, \varphi(\rho(i+1)))$ via

$$\begin{cases} \varphi(\rho(i+1)) = \ldots \varphi(\rho(i)+1) = \varphi(\rho(i)) \\ \varphi(\rho(i+1)) \underset{1}{>} \ldots \underset{1}{>} \varphi(\rho(i)+1) \underset{1}{>} \varphi(\rho(i)) \end{cases}$$

if $v(i)=v(i$

if $v(i)<v(i+1$

Ex ctd $\varphi = (\cancel{0}, 0, 0, 1)$

Also call φ the **Ekedahl-Oort (EO) type**.

We can read off the a-number from φ

as $a(X) = g - \varphi(g)$

We can read off the p-rank from φ

as $f(X) = \max\{ i : \varphi(i) = i \}$.

But it's not as easy to see what the Newton polygon is.

Ex (ctd) $\varphi = (0,0,1)$, $g=3$

$a(X) = 3 - 1 = 2$

$f(X) = 0$

But supersingular .... ?

$\updownarrow$

$NP = (\frac{1}{2}, \ldots \frac{1}{2})$

Example other φ for $g=3$

- with a-number 2, p-rank 0:

  $(\cancel{0},0,1,1)$

- with a-number 2, p-rank 1:

  $(1,1,1)$

- with a-number 1 p-rank 0:

  $(0,1,2)$