Sep.17

We follow Demazure, Richard Pink, Lenstra [Len19] and Manin [Man63].

1. Overview

1.1. Our goal is to classifiy finite group scheme of p-power order by linear-algebraic data. We will define a contravariant functor M that sets up an anti-equivalence

$$M\colon \texttt{(order } p^n\texttt{) c.f.g.s} \to \texttt{(length-}n\texttt{) } E\texttt{-mods}$$

over a perfect field k. here E is the ring of non-commutative polynomials

$$W(k)\langle F, V\rangle/(Fa - \sigma(a)F, Va - \sigma^{-1}(a)V, FV - p, VF - p)$$

We will upgrade this to p-divisible groups and classify the linear algebraic data.

1.2. Recall that from last time, we know that over a perfect field, a finite group scheme splits into four parts $G_{rr} \times G_{rl} \times G_{lr} \times G_{ll}$. We will define the functor for each part. Using Cartier duality, it suffice to define M for G_{ll}, G_{rl}, the part on G_{lr} will be defined by $M(-^{\vee_{\texttt{Cariter}}})^{\vee_E}$.

1.3. Let us note that the previous decomposition only holds for finite commutative groups schemes over a perfect field. For example, Cartier duals are not defined for non-commutative affine group schemes. Splitness fails over non-perfect fields.

2. Frobenius-Verschiebung

Let us discuss Frobenius and Verschiebung in full generality. We work with any finite group scheme in a field k of positive characteristic p.

2.1. Note that the relative Frobenius morphism commutes with products, therefore $G^{(p)}$ is a group scheme if G is, and $F_G\colon G \to G^{(p)}$ is a homomorphism. Explicitly, let $\sigma\colon k \to k$ be the raise to p-power map, we have $A^{(p)} = A \otimes_{k,\sigma} k$, extension of scalars by f. Sometimes we will use the notion of scalar restriction $R_{[p]}$, where k acts by p-power. We have $G^{(p)}(R) = G(R_{[p]})$ by adjunction.

2.2. The Frobenius commutes with products, base extension, and functorial. Furthermore, it is compatible with Cartier duality $(G^\vee)^{(p)} \cong (G^{(p)})^\vee$. We check the equality on the functor of points:

$$\begin{aligned}
(G^\vee)^{(p)}(T) =& [G \times_S T_{[p]}, \mathbb{G}_m \times_S T_{[p]}]_{T_{[p]}} \\
=& [G \times_S T_{[p]}, (\mathbb{G}_m \times_S T)_{[p]}]_{T_{[p]}} \\
=& [(G \times_S T_{[p]})^{(p)}, \mathbb{G}_m \times_S T]_T \\
=& [G^{(p)} \times_S (T_{[p]})^{(p)}, \mathbb{G}_m \times_S T]_T \\
=& [G^{(p)} \times_S T, \mathbb{G}_m \times_S T]_T
\end{aligned}$$

By Cartier duality, $F_{G^\vee}\colon G^\vee \to (G^\vee)^{(p)} = (G^{(p)})^\vee$ induces a unique Verschiebung morphism $V_G\colon G^{(p)} \to G$ such that $(V_G)^\vee = F_{G^\vee}$

Theorem 1. *We have $F_G \circ V_G = p[1_{G^{(p)}}]$ and $V_G \circ F_G = p[1_G]$.*

Note that Frobenius and Verschiebung commutes with base change, therefore the base change of F_G along $V_{G^{(p)}}$ shows that shows that $F_G \circ V_G = V_{G^{(p)}} \circ F_{G^{(p)}}$, it suffices to show that $V_G \circ F_G = p[1_G]$, namely the following diagram commutes

$$\begin{tikzcd}
A \arrow[rr, "\Delta_p"] \arrow[dr, "\Delta_p"] \arrow[dd, "V"'] & & \bigotimes^p A \arrow[dd, "\bigotimes^p m"] \\
& \mathrm{TS}^p A \arrow[ur, hook] \arrow[dl, dotted, "\lambda_A"'] & \\
A^{(p)} \arrow[rr, "F_A"] & & A
\end{tikzcd}$$

Let us check that the dotted arrow exists, the lower square and the left triangle commutes. The first two follows from the decomposition $\mathrm{TS}^p A \cong A^{(p)} \oplus s(V^{\otimes p})$, where s is the symmetrizer without denominators, which we can check on basis[1]. It remains to show the left triangle commutes. Note that λ_A is the unique homomorphism that sends $c(a \otimes a \cdots \otimes a)$ to $a \otimes c$, it suffices to show that $V(a) = \lambda \circ \Delta_p(a)$, or $\langle c \otimes 1, V(a) \rangle = \langle c \otimes 1, \lambda \circ \Delta_p(a) \rangle, c \in A^\vee$. Left hand side equals to $\langle c^p, a \rangle = \langle \bigotimes^p c, \Delta_P(a) \rangle = \langle \bigotimes^p c, \lambda \circ \Delta_P(a) + s(r) \rangle$, finally note that $\langle \bigotimes^p c, s(r) \rangle = \langle s(\bigotimes^p c), r \rangle = 0$. The middle step uses the Cartier duality of products.

2.3. Using this, one easily shows that $(F, V) = (0, 0)$ on α_p, $(0, 1)$ on μ_p and $(1, 0)$ on $\mathbb{Z}/p\mathbb{Z}$. More generality, the étaleness can be tested by whether F is an isomorphism. This is because G is etale iff tangent space is trivial, but F is zero on the tangent space, then note that F is a bijection on points. On the other hand, G is local iff F_G is nilpotent: a point $G(R)$ determines a homomorpshim $A \to R$, we want to see if $\mathfrak{m}_A$ maps to zero. This is clear as $\mathfrak{m}_A$ itself is nilpotent, killed by absolute frobenius, therefore it is killed by relative frobenius, as change of base fields if faithfully flat.

3. Naive local-local group schemes

3.1. We have determined the étale group schemes as π_1-groups. Therefore over a perfect field, it remains to understand finite group schemes of type G_{ll}. We show that they are made up of α_p.

Theorem 2. *Any finite group scheme with $F_G = 0, V_G = 0$ is isomorphic to a direct sum of α_p.*

3.2. A useful observation is that $\mathrm{End}(\alpha_{p,k}) = k$ over any field. Note that multiplication by k and action on tangent space gives isomorphism $k \to \mathrm{End}(\alpha_p) \to k$. We show the second map is injective. Given any ϕ with $\mathrm{d}\phi = 0$, then $\ker(\phi)$ has a nonzero tangent space, contradicting the simpleness of α_p.

[1]Group the basis according to the decomposition types of permutation in S_p, the only term with p coefficient has type $(1, \dots, 1)$. For example take $p = 3$, the symmetrizer of $a \otimes a \otimes b$ is $2(aab + aba + baa)$, here 2 is invertible in char 3

3.3. Let I be the kernel of $A \to k$. Since $F_G = 0$, we know I is p-power zero. By Nakayama, we can present A as a quotient of $k[X_1, \ldots, X_n]/(X_1^p, \ldots, X_n^p)$. Here $n = \dim T_{G,0}$. Let us recall a useful lemma:

Lemma 3. *There is an isomorphism of k-vector spaces $T_{G,0} \cong \mathrm{Hom}(G^\vee, \mathbb{G}_a)$.*

Note that the tangent space corresponds to maps $A \to k \oplus kt$ of form $\epsilon + \lambda t$ such that $\lambda(ab) = \lambda(a)\epsilon(b) + \epsilon(a)\lambda(b)$ and $\lambda(e(1)) = 0$. Note that $k[T] \to A^\vee$ consists of an element λ. The previous conditions sums up to $\mu^*(\lambda) = \lambda \otimes 1 + 1 \otimes \lambda$, $e^*(\lambda) = 0$.

3.4. Note that given $\phi\colon G^* \to \mathbb{A}^1$, by functoriality, $F_{\mathbb{A}^1} \circ \phi = \phi^{(p)} \circ F_{G^\vee} = \phi^*(p) \circ (V_G)^\vee = 0$. Therefore ϕ factors through α_p. We claim there exists an epimorphism $G^\vee \to \alpha_p^{\oplus n}$. Suppose an epimorphism $G^\vee \to \alpha_p^i$ is established, then $k^i \to \mathrm{Hom}(G^\vee, \alpha_p)$ is an embedding. Any homomorphism $\varphi^*\colon G^\vee \to \alpha_p$ not in the image has nontrivial restriction to ϕ. Since α_p is simple. The combined $G^\vee \to \alpha_p^i \oplus \alpha_p$ is an epimorphism. By Cartier duality we get $\alpha_p^{\oplus n} \to G$, then the order forces this an isomorphism.

4. Ring of Witt vectors, after Lenstra

Let us start our journey to Dieudonne modules. We will begin with the Witt stuff.

4.1. Let A be an arbitrary ring. We define $\Lambda(A) = 1 + TA[[T]]$. This is a torsion free abelian group with respect to multiplication.

Theorem 4. *There exists a unique distributive multiplication such that*[2]

$$(1 - aT)^{-1} * (1 - bT)^{-1} = (1 - abT)^{-1}.$$

4.2. Let us remark that given complex vector bundles E, E' on a space X, we may associated chern polynomials $c_{E'}(t), c_{E''}(t)$. Their sum and tensor satisfy $c_E(t) = c_{E'}(t) \cdot c_{E''}(t)$ and $c_{E' \otimes E''}(t) = c_{E'}(t) * c_{E''}(t)$, where $\prod(1 - \alpha_i t) * \prod(1 - \beta_j t) = \prod(1 - \alpha_i \beta_j t)$. Our law resembles this one but different.

4.3. The structure of ring of Witt vectors is transported from $\Lambda(A)$. We have commutative diagram

$$\begin{tikzcd} W(A) \arrow[r, "\varphi"] \arrow[rrr, bend left, dotted, "\texttt{ghost}"] & \Lambda(A) \arrow[r, "Tu'/u"] & TA[[T]] \arrow[r, "\texttt{Coef}"] & \prod_1^\infty A \end{tikzcd}$$

where φ is bijective map $\varphi\colon \prod_1^\infty A \to \Lambda(A)$ defined by $(a_m)_{m \geq 1} \mapsto \prod_{m \geq 1}(1 - a_m T^m)^{-1}$. Therefore φ already defines the ring structure on $W(A)$.

---

[2]Let $M_n(A) \subset \Lambda_n(A)$ be the subgroup generated by $\{1 - aT\}_{a \in A}$. We define the $*$ on $M_n(A)$, and extend to $\Lambda_n(A)$, take limit to $\Lambda(A)$. Consider the A-algebra endomorphism $\varphi_a\colon T \to aT \in \mathrm{End}(\Lambda_n(A))$, let $E \subset \mathrm{End}(\Lambda_n(A))$ be the additive subgroup generated by $\{\varphi_a\}_{a \in A}$, is it a subring as $\varphi_a \varphi_b = \varphi_{ab}$. The map $E \to \Lambda_n(A), e \mapsto e(1 - T)^{-1}$ is a surjection onto $M_n(E)$, one transport the multiplication on E to $M_n(A)$.

4.4. Can we understand φ better? We can extract x from $(1+x)$ by logarithmic derivative $u \mapsto Tu'/u$. The "extraction is faithful" only if p is invertible, let us call the composition the ghost map. Explicitly, it sends $(a_n)_1^\infty$ to $(a^{(n)})_1^\infty$, where $a^{(n)} = \sum da_d^{n/d}$

$$\begin{aligned} &T(\log \prod_{m\geq 1}(1-a_mT^m)^{-1})' \\ =&T(\sum_{m\geq 1} -\log(1-a_mT^m))' \\ =&\sum_{m\geq 1} ma_mT^m \sum_{k\geq 0}(a_mT^m)^k \\ =&\sum_{m\geq 1}\sum_{k\geq 1} ma_m^kT^{mk} \\ =&\sum_{n\geq 1}(\sum_{d|n} da_d^{n/d})T^n \end{aligned}$$

As u'/u sends multiplication to addition, the ghost map is a homomorphism, namely, there exists groups laws in $\mathbb{Z}$-coefficients. Note that the p-primary components of $\prod^{\mathbb{N}} A$ is a summand, it inherits the group structure. How to describe the laws?

4.5. Let us view $(a_m) \mapsto \prod(1-a_mT^m)^{-1}$ as

$$\phi\colon (a_m) \mapsto \prod_{m>0} \exp(\sum_{k\geq 0}(a_mT^m/m)^k),$$

where the later is $\prod \exp(-\log(1-a_mT^m))$, the natural analogue is

$$E:(a_{p^m}) \mapsto \prod_{m>1} \exp(\sum_{k\geq 0}(a_{p^m}T^{p^m}/p^m)^k)$$

We call this map the Artin-Hasse exponential, it actually works. The key of this notion is, when p is not invertible, we cannot operate in the Witt ring via ghost components, we determine the operations[3] via Artin-Hasse exponentials in $\Lambda(A)$.

5. Basic operations on Witt vectors

5.1. Let $T\colon W \to W$ be the monomorphism defined by $(a_0, a_1, \cdots) \mapsto (0, a_0, \cdots)$. Let us note that $\Phi_0(Tw) = 0, \Phi_n(Tw) = p\Phi_{n-1}(w)$, therefore T is a group homomorphism, called translation. We define W_n the group of Witt vector so length n by $\mathrm{Coker}(T^n)$

$$0 \longrightarrow W \xrightarrow{T^n} W \xrightarrow{R_n} W_n \longrightarrow 0\ .$$

5.2. Let $\tau\colon \mathbb{G}_a \to W$ be the morphism $a \mapsto (a, 0, \dots)$, then $\Phi_n(\tau(a)) = a^{p^n}$, and the Artin-Hasse exponential $E(\tau(a), t) = F(at)$, this is the Teichmuller lift.

5.3. We are interested in finite groups scheme in positive characteristic, rather than lifting. When k is a field in positive characteristic, the ghost components are $(a_n) \mapsto a_0^{p^n}$. We define $W_k = W_{\mathbb{F}_p} \otimes_{\mathbb{F}_p} k$, $W_{n,k}$, we study its Frobenius and Verschiebung.

[3] In particular, Frobenius and Verschiebung

5.4. As we are over a finite field, we may identify W_k with $W_k^{(p)}$, the Frobenius F on W is given by $F((a_i)) \mapsto (a_i^p)$, on Λ is given by raising coefficients to p-power. The Verschiebung on Λ_k is $\phi(t) \mapsto \phi(t^p)$. The Verschiebung on W is T.

Theorem 5. *We have $V(Fx \cdot y) = x \cdot Vy$, as a corollary, $E(x \cdot Vy, t) = E(Fx \cdot y, t^p)$*

Note that F is an epimorphism, we can write $y = Fz$, then $V(Fx \cdot y) = V(Fx \cdot Fz) = VF(x \cdot z) = p(x \cdot z) = x \cdot pz = x \cdot VFz = x \cdot Vy$.

6. Finite Witt schemes: structure and duality

6.1. Let $W_n^m = \mathrm{Ker}(F^m \colon W_n \to W_n)$. We think of it as the universal group scheme such that F^m, V^n vanishes.

Theorem 6. *Every $G \in$ `c.g.f.s` such that $F_G^m = 0, V_G^n = 0$ can be written as*

$$0 \longrightarrow G \longrightarrow (W_n^m)^{\oplus r} \longrightarrow (W_n^m)^{\oplus s}$$

The embedding part is essential. It follows from the key lemma that the following sequence always splits ($n = 1, m = 1$), and standard homological algebra.

$$\begin{tikzcd} 0 \arrow[r] & W_n^m \arrow[r] \arrow[d] & G \arrow[r] \arrow[dl, dotted, "\varphi"'] & \alpha_p \arrow[r] & 0 \\ & W_{n+1}^{m+1} & & & \end{tikzcd}$$

- Let us assume this is true, we induct on order of $|G|$, given $0 \to G' \to G \to \alpha_p \to 0$, assume there exists $G' \to (W_n^m)^{\oplus r}$, take push-out we get $0 \to W_n^m \to G_i \to \alpha_p \to 0$. By the property we get $G_i \to W_{n+1}^{m+1}$. Then take direct sum with $G \to \alpha_p$.
- Let us deduce the key lemma by induction. The first step being $W_{1,1}$. Suppose G is an extension of α_p by α_p. Let U be the kernel of $rf = fr \colon W_2^2 \to \alpha_p$. It surjects onto $\ker(f), \ker(r)$. We have $0 \to \alpha_p \to U \to \alpha_p \oplus \alpha_p \overset{(r',f')}{\to} 0$. Since F_U, V_U acts as zero on α_p, the F_U, V_U induces from $k^{\oplus 2} \to \mathrm{Hom}(\alpha_p^{\oplus 2}, \alpha_p) \to \mathrm{Hom}(U, U))$. One finds that F_U, V_U corresponds to $(0,1)$ and $(1,0)$. For any

short exact sequence $0 \to \alpha_p \to U \to \alpha_p \to 0$, we have push-forward

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & \alpha_p \arrow[r] \arrow[d] & G \arrow[r] \arrow[d] & \alpha_p \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & U \arrow[r] \arrow[d] & G' \arrow[r] \arrow[d] & \alpha_p \arrow[r] & 0 \\
 & \alpha_p^{\oplus 2} \arrow[r, equal] \arrow[d] & \alpha_P^{\oplus 2} \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

There is an induced short exact sequence $0 \to \alpha_p \to G' \to \alpha_p^{\oplus 3} \to 0$. One shows that $F_{G'}, V_{G'}$ induces $k^{\oplus 3} \to \mathrm{Hom}(\alpha_p^{\oplus 3}, \alpha_p) \to \mathrm{Hom}(G', G')$ We consider the pullback of G' induced from $\alpha_p \to \alpha_p^{\oplus 3}$, given by $(1, -y, -x)$. One finds $F_{G''}, V_{G''}$ are zero, therefore G'' splits. This yields the splitting of $G' = U \oplus \alpha_p$. Then $G \to G' \to U \to W_2^2$ yields required embedding.

- Finally we show the $W_n^m \to W_{n+1}^{m+1}$ via induction. We take the push-out $0 \to W_n^{m+1} \to G' \to \alpha_p \to 0$. Consider $F\colon W_n^{m+1} \to W_n^m \to W_n^{m+1}$, we have $G' \to W_n^m$. However the map is F, we need to divide out frobenius by f. Let G'' be the kernel of $G' \to W_n^m$. We have diagram $W_n^1 \to G''$ and $W_n^{m+1} \to G'$, we check this is a push-out. We get the induced map $G' \to W_{n+1}^{m+1}$ by universal property of push-out.

6.2. Let $\sigma_n\colon W_n \to W$ be the section to $R_n\colon W \to W_n$ defined by $\sigma_n(a_0, \dots, a_{n-1}) = (a_0, \dots, a_{n-1}, 0, \dots)$. Clearly σ_n sends W_n^m to W'. The image consists of elements which almost all zero and nilpotent. It is easy to check that $W'(R)$ is an ideal and $E(w, t)$ is a polynomial for $w \in W'(R)$. In particular, $E(w, 1)$ is defined for any $w \in W'(R)$.

Theorem 7. *For $x \in W_n^m(R), y \in W_m^n(R)$, define $\langle x, y\rangle = E(\sigma_n(x)\sigma_m(y), 1)$, this is bilinear and gives an isomorphism $W_n^m \cong W_m^{n,\vee}$*

The key is to check the map is bilinear and non-degenerate.

6.3. Let us remark without proof that $M(G^\vee) = M(G)^\vee$, the dual of modules is given by $W(k)[1/p]/W(k)$.

7. The Dieudonné functor

7.1. When G is local-local, we defined $M(G) = \mathrm{colim}(G, W_n^m) = \mathrm{colim}(G, W_n)$. When G is étale, we define $M(G) = \mathrm{colim}(G, W_n)$. This is an anti-equivalence of categories, mainly following from Pontraygin duality, Dieudonne lemma (Lang's theorem).

Theorem 8 (Lang)**.** *Let k be an algebraically closed field of positive char. Let G be a connected algebraic group of finite type. Let $F\colon G \to G$ be a homomorphism that $dF = 0$, Then $G(k) \to G(k), g \mapsto g^{-1} \cdot F(g)$ is surjective.*

Note that $h \mapsto h^{-1}gF(h)$ has derivative -1, therefore surjective. As G is connected, the image is an open dense U_g. Note that $U_1 \cap U_g \neq \emptyset$, we have $h_1^{-1}gF(h_1) = h_2^{-1}F(h_2)$, therefore $g = (h_2h_1^{-1})F(h_2h_1^{-1})$.

Lemma 9 (Dieudonne)**.** *Let k be an algebraically closed field of positive char. Let N be a $W(k)$-module with σ-linear automorphism $F\colon N \to N$. THen $W(k) \otimes_{\mathbb{Z}_p} N^F \to N$ is an isomorphism. In particular* $\mathrm{length}_{W(k)}(N) = \log_p |N|$.

Take an example, say $N^F = W_n(k^F) = W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$, for $N = W_n(k)$ with $F = \sigma$. We begin with an isomorphism of $W(k)$-modules $\phi\colon \oplus W_{n_i}(k) \to N$. The endomorphism ring of N is affine, therefore the automorphisms $G = \mathrm{Aut}(N)$ is an open subscheme, connected algebraic group over k. The given F then can be written as $\phi g \sigma(\phi^{-1})$ for some $g \in G(k)$. Lang's theorem allows us to write $g = h^{-1}\sigma(h)$. Then $F = (\phi h^{-1})\sigma(\phi h^{-1})^{-1}$. Therefore ϕh^{-1} is the desired F-equivariant isomorphism.

7.2. To sum up, we have an equivalence of categories from finite commutative group schemes of p-power order to the category of left E-modules of finite length where E is an isomorphism, over an arbitrary perfect field (Galois descent). Passing to limits we have

Theorem 10. *The functor $G \to M(G)$ is an equivalence between the category of p-torsion formal groups and the category of triples (M, F_M, V_M) where M is a finitely generated $W(k)$-module and the obvious relations. In this correspondence, G is finite iff M is, G is p-divisible iff M is torsion-less, the height of G equals to the rank of M. The dimension of G equals to length of M/FM.*

8. Classification of p-divisible groups

8.1. Let k be a perfect field. We say an F-lattice a free $W(k)$-module together with an injective σ-linear endomorphism. Since k is perfect, this is also a F-crystal over k. Given a p-divisible group, we have the corresponding F-crystal $M(G)$. And the M-isocrystal (F-space) $E(G)$. One sees that

- $E(G)$ and $E(H)$ are isomorphic iff there is an isogeny $G \to H$, as there exists m such that $\phi(M(H)) \subset p^{-m}M(G)$.
- An F-space is called effective if it contains an lattice that is stable by F. Is comes from a p-divisible group if it has a lattice stable under F, pF^{-1} (a Dieudonne module).

Let $\mathfrak{o}(1)$ be the F-isocrystal $B(k) = W(k)[1/p]$, where F-action is given by $x \mapsto p^{-n}x^{(p)}$. We use notation $E(n) := E \otimes \mathfrak{o}(n)$, etc.

8.2. The building blocks of F-isocrystals are $M^\lambda = \mathbb{Z}_p[T]/(T^r - p^s)$, where $\lambda = s/r$ coprime and F action is multiplication by T. When $0 \leq s \leq r$, we can consider $\overline{M}^\lambda = \mathbb{Z}_p[F,V]/(FV - p, F^{r-s} - V^s)$, assigning $F = T$ and $V = p/T = p^{ar+bs}/T = p^{ar}T^{rb-1}$.

This is a lattice in E^λ. We may consider the kernel G of $W(p)$, the p-divisible group of $W_{\mathbb{F}_p}$ via $F^{r-s}-V^s$, one see that $M(G^\lambda)=\overline{M}^\lambda$. G has height r dimension s, $G_\lambda^\vee=G_{1-\lambda}$. We can also write M_k^λ as $W(k)[p^{1/r}]$, where the action is trivial and the Frobenius is given by $F_s\colon w_ip^{i/r}\mapsto w_i^{(p)}p^{i+s/r}$. Let us take $ar+bs=1$, consider the $B(\mathbb{F}_{p^r})$-algebra K^λ generated by ξ such that $\xi^r=p, \xi\alpha=\alpha^{p^b}\xi$. It is a left vector space over $B(\mathbb{F}_{p^r})$ with basis $1,\cdots,\xi^{r-1}$ hence of degree r^2 over $\mathbb{Q}_p$. It is central division algebra. Central follows from definition of $\mathbb{F}_{p^r}$. Division follows from right multiplication by $\sum a_i\xi_i$, the matrix has norm not zero (upper triangular modulo p, the diagonal give the norm). One checks that sending $\xi^i\to p^{i/r}$ yields an isomorphism $B(k)\otimes_{B(\mathbb{F}_{p^r})}K_\lambda=E_k^\lambda$. The endomorphism ring is right multiplication by K^λ:

Lemma 11. $\mathrm{Hom}(E^\lambda,H)$ *consists of all* $x\in H$ *such that* $F^rx=p^sx$.

Note that $x=\sum\alpha_i\xi^i$, $F^rx=\sum p^s\alpha_i^{p^r}\otimes\xi^i$, $F^rx=p^sx$ implies that $\alpha_i^{p^r}=\alpha_r$. Therefore $x=1\otimes\sum\alpha_i\xi^i\in 1\otimes K^\lambda$.

8.3. We show that

- for $\lambda\neq\lambda'$, we have $\mathrm{Hom}(E^\lambda,E^{\lambda'})=0$. By the lemma, we are looking for $x\in E_k^{\lambda'}$ such that $F^rx=p^sx$. Let s write $x=b_jf_j$, then $F^{r'}x=\sum b_j^{p^{r'}}p^{s'}f_j$ hence $F^{rr'}=\sum b_j^{p^{rr'}}p^{s'r}f_j$. When $F^r=p^s$, this equals $(p^s)^{r'}x=\sum b_jp^{sr'}f_j$. We compare the valuation, the two are different as $sr'\neq s'r$.
- $E_k^\lambda\otimes E_k^{\lambda'}\cong(E_k^{\lambda+\lambda'})^{\mathtt{gcd}(r,r')}$, $e_{i+k}\otimes e_{j+k}$ for g running through $rr'/(r,r')$ form a space with slope $\lambda+\lambda'$. We have $K^\lambda\otimes_{\mathbb{Q}_p}K^{\lambda'}\cong M_{\mathtt{gcd}(r,r')}(K^{\lambda+\lambda'})$. One sees that $M_k^\lambda(-n)\cong M_k^{\lambda+n}$. Let us remark that $\mathbb{Q}/\mathbb{Z}\to\mathrm{Br}(\mathbb{Q}_p),\lambda\mapsto K^\lambda$ is an isomorphism.

8.4. We classify F-spaces over an algebraically closed field. Every F-space splits into a direct sum of E^λs. The key points (both need algebraic closedness) are

- Any extension $0\to E_k^\lambda\to E\to E_k^{\lambda'}\to 0$ splits.
- Let $P=F^n+a_1F^{n-1}+\cdots+a_n\in W(k)[F]$, then there exists $b_0\cdots b_{n-1}$ such that $P=(b_0F^{n-1}+\cdots+b_{n-1})(F-p^{s/r})u$ with $b_i,u\in W(k)[p^{1/r}]$.
- Every nonzero F-space admits a nonzero morphism $E\to E_k^\lambda$ for some λ.

8.5. For the first key point, we easily reduce to show that F^r-p^s on E_k^λ is surjective. We use the previous lemma, need to find some x such that $(F^r-p^s)(x)=0$. Surjectivity follows from surjectivity of $F^{rr'}-p^{sr'}$. It acts on $\sum a_ie_i'$ by as $\sum(p^{rs'}a_i^{(p^{rr'})}-p^{sr'}a_i)e_i'$. It suffice to show $x\mapsto p^bx^{p^a}-x$ is surjective for $a,b\in\mathbb{Z}$. It follows from iteration by contraction $x\mapsto px-c$, except in the case $b=0$, we use algebraic closedness of the residue field and successive approximation: for $b\in W(k)$ consider $x^{(p)}-x-b=p^mw$. We want to find $x_1=x+p^my$ such that $x_1^{(p)}-x_1-b=p^{m+1}t$ expanding we reduce to solving $p^m(y^{(p)}-y+(x^{(p)}-x-b)/p^m)=0$, we solve it modulo p.

8.6. For the second key point, we take $\lambda_i=\inf(v(a_i)/i)$ and put $a_i=p^{i\lambda}\alpha_i$, then α_i is a unit for some i. We look for b_i of the form $p^{r\lambda}\beta_i$. We compare the coefficients and solve by successive approximation.

8.7. For the third key point, we may assume E is simple $B(k)[F]$-module. It is a non-commutative Euclidean ring, every simple module can be written as $B(k)[F]/P$ for a monic polynomial P. Replacing E by $E(-m)$, we may assume coefficients are integral. Therefore E is determined by the F-lattice $W(k)[F]/P$. We write $P = Q(F - p^{s/r})u$. Then $x \mapsto xu^{-1}$ induces an epimorphism $W(k)[p^{1/r}] \otimes M \to W(k)[p^{1/r}][F]/(F - p^{s/r}) = M_k^\lambda$. We win by precompose with M.

8.8. The classification up to isogeny can be refined.

Theorem 12. *If G is isogenous to $G^{1/r}$ or $G^{r-1/r}$, then G is isomorphic to it.*

Equivalently, we want to show that any F-lattice in E_k^λ is isomorphic to M_k^λ. Let us pick a basis of E_k^λ such that $Fe_1 = e_2$,..., $Fe_{r-1} = e_r, Fe_r = pe_1$. Let $m_i = \inf\{m | p^m e_i \in M\}$, then $m_1 \geq m_2 \geq \cdots \geq m_n \geq m_1 - 1$. Replacing the basis[4] by $F^\alpha p^\beta e_i$, we may suppose $m_i = 0$ for all i. Namely $e_i \in M$ but $p^{-1}e_i \notin M$. Therefore $M \supset M_k^\lambda$ we write $m = \sum a_i e_i$. There exists α such that $F^{\alpha+1} \in M_k$ but $F^\alpha \notin M_k^\lambda$. Replacing m by $F^\alpha m$, we can suppose $m \notin M_k^\lambda$, $Fm \in M_k^\lambda$. But $Fm = pa_n e_1 + a_1 e_2 + \cdots + a_{n-1}e_n$ hence $a_1, \cdots, a_{n-1} \in W(k)$, $a_n \notin W(k)$, $pa_n \in W(k)$, this implies that $a_n e_n = m - a_1 e_1 - \cdots - a_{n-1}e_{n-1} \in M$, contradiction.

8.9. We call a formal group equidimensional if the kernel of multiplication by p is Artinian, or M/pM has finite length. We say an equidimensional module is special if it is isomorphic to a sum of homogeneous special modules $E/E(F^m - V^n)$. Among all special submodules, there exists a unique maximal one $M_0 \subset M$. Given a special module M_0, we say a module M belongs to M_0 if the maximal special submodule is isomorphic to M_0. There exists h, g such that $M_0 \subset M \subset p^{-h}M_0$ or $F^{-g}M_0$, call them the P-height and F-height. The h, g stabilizes.

Theorem 13. *There exist a bijection between the set of E-modules belonging to a fixed special module M_0 with $M_0 \subset M \subset p^{-h}M_0$, and the points of a certain algebraic variety over k.*

We first parameterize all W-modules satisfying the sandwich condition. Then select those E-modules. Any such modules is determined by its image in $p^{-h}M_0/M_0$, which is isomorphic to $\oplus W_h(k)/(p^{e_i})$. We can identify the automorphism group with $GL(N, W_h(k))$. The stabilizer is closed, and the p-divisible groups $A(M_0, h)$ are parameterized by G/G_0. There is a finite group $\Gamma(M_0, h)$ of automorphisms such that two poins correspond to isomorphic E-mnodules if and only if they belong to the same orbit $\Gamma(M_0, h)$. Let Γ be the group of automorphisms of M_0, it is infinite but acts very ineffectively on $A(M_0, h)$. We call an element special if $F^m x = V^n x$, one can show that every special element belongs to a finite number of cosets.

References

[Len19] Hendrik W. Lenstra. Construction of the ring of Witt vectors. *Eur. J. Math.*, 5(4):1234–1241, 2019.

[Man63] Ju. I. Manin. Theory of commutative formal groups over fields of finite characteristic. *Uspehi Mat. Nauk*, 18(6 (114)):3–90, 1963.

[4] rotate the beads