We follow [CS86] and various online resources, e.g. this, and this.

1. Lagrange's theorem

1.1. We will focus on finite flat group schemes over connected bases. Here is our goal:

Theorem 1 (Lagrange)**.** *Let S be a scheme, let G be a finite group scheme over S. Let N be a flat subgroup scheme of G. Then the quotient scheme G/N exists, it is flat and finite over S. We have $\#|G| = \#|N| \cdot \#|G/N|$.*

1.2. Let us clarify what the quotient means, it is taken in the category of fppf sheaves. Injectivity is clear. By the right half of the short exact sequence $N \to G \to Q \to 0$, we mean Q is coequalizer of the diagram $N \times G = R \to G \to Q$. The existence is promised by Grothendieck's theorem on quotient by flat projective equivalence relations.

Theorem 2 (Grothendieck)**.** *Let $X \to S$ be quasi-projective morphism of noetherian schemes, let $f\colon R \to X \times_S X$ be a schematic equivalence relation on X over S, such that the projections $R \to X$ are proper (thus projective) and flat, then an coequalizer exists, the induced morphism $X \to Q$ is faithfully flat and effective.*

1.3. By Grothendieck's theorem, we know the quotient exists, we need to check that the quotient $\mathcal{O}_{G/N}$ is flat over S, and that Lagrange's theorem holds. Since G is flat and $G \to Q$ is faithfully flat, we know Q is flat, by descent of flatness. Flatness allows us to count over base change $N \times_S G \cong G \times_Q G$, over which $ng = (g/q)^2 q$ (the flatness of $G \to Q$ allow us to write $\mathcal{O}_G$ as a locally free $\mathcal{O}_Q$-module).

2. Cartier Duality

2.1. Let G be a finite flat group scheme over R represented by A. The R-algebra A is a commutative Hopf algebra with multiplication μ, unit η, comultiplication Δ, counit ϵ, antipode S, $(A, \mu, \eta, \Delta, \epsilon, S)$. When G is commutative, taking dual we arrive at the Cartier dual of the group scheme D, represented by the Hopf algebra $A^\vee$.

2.2. Unwrapping the abstract definition, we can show

Theorem 3 (Cartier)**.** *The functor of points of the Cartier dual G^D is given by*

$$G^D(T) = \mathrm{Hom}(G \otimes_R T, \mathbb{G}_{m,T}).$$

Let us note that the dual Hopf algebra is given by $(A^\vee, \Delta^\vee, \epsilon^\vee, \mu^\vee, \eta^\vee, S^\vee)$, therefore an element $g \in G^D(T)$, or an R-algebra morphism $g\colon A^\vee \to T$ is an R-module homomorphism $g\colon A^\vee \to T$ such that the following diagrams commute

$$\begin{array}{ccc} A^\vee \otimes_R A^\vee & \xrightarrow{\Delta^\vee} & A^\vee \\ \downarrow{\scriptstyle g\otimes g} & & \downarrow{\scriptstyle g} \\ T \otimes_R T & \xrightarrow{\mu_T} & T \end{array} \qquad \begin{array}{ccc} & R & \\ {\scriptstyle \epsilon^\vee}\swarrow & & \searrow{\scriptstyle \eta_T = 1_T} \\ A^\vee & \xrightarrow{g} & T \end{array}$$

Therefore

$$\Delta(g) = g \otimes g, \quad \epsilon(g) = 1$$

Note that $g \in A^\vee \otimes T$ is a multiplicative unit (here $A^\vee \otimes T$ is the base change of A), because by the axioms of group schemes, we have

$$g \cdot S(g) = \mu \circ (1 \times S)(g \otimes g) = \mu \circ (1 \otimes S) \circ \Delta(g) = \eta \circ \epsilon(g) = 1$$

Therefore g can be identified as a T-map $T[X, X^{-1}] \to A \otimes_R T$ of algebras that sends $X \to g$. This is a morphism of Hopf algebras, where the left hand side is viewed as $\mathbb{G}_{m,T}$, as we checked that $\Delta(g) = g \otimes g$ and $\epsilon(g) = 1$.

2.3. Let us note that, viewing the pairing $G \times G^D \to \mathbb{G}_m$ as a morphism of group schemes, then X is sent to $\sum e \otimes e^D$ for any basis $\{e_i\}$ of $\mathcal{O}_G$ we pick. The reason is that the map $R[X, X^{-1}] \to A \otimes_R A^\vee$ sends X to the identity element.

2.4. The Cartier dual of the constant group scheme is $(\mathbb{Z}/n\mathbb{Z})_R$ is $\mu_{n,R}$, by the previous theorem we have $G^D = \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{G}_m)$, where 1 is mapped to an n-th root of unity. One can also check on the level of algebras, which is less explicit.

2.5. The Cartier dual of α_p is α_p. This is a group scheme that represents p-nilpotent elements. In characteristic p, we have freshman's dream, making it a subscheme of $\mathbb{A}^1$.

- The group scheme α_p is represented by $R[X]/(X^p = 0)$ with
$$\Delta(X) = X \otimes 1 + 1 \otimes X, \quad \epsilon(X) = 0, \quad S(X) = -X$$
- The dual algebra has basis Y_i dual to X^i for $i \in [0, p-1]$, the multiplication is given by
$$Y_i \cdot Y_j = \sum_0^{p-1} \Delta^\vee(Y_i \otimes Y_j)(X^k)Y_k = \sum_0^{p-1} Y_i \otimes Y_j(\Delta(X^k))Y_k$$
Let us note that $\Delta(X^k) = \sum \binom{k}{a} X^a \otimes X^b$, the binomial coefficient vanishes for $i + j \geq p$, therefore $Y_i \cdot Y_j = \binom{i+j}{i} Y_{i+j}$ if $i + j < p$ and 0 otherwise.
- Therefore with $Y = Y_1$, we have $A^\vee = R[Y]/(Y^p = 0)$.
- Moreover, we have

$$\Delta(Y) = \sum_{a,b} \mu^\vee(Y)(X^a \otimes X^b)Y_a \otimes Y_b = \sum_{a,b} Y(X^{a+b})Y_a \otimes Y_b = Y \otimes 1 + 1 \otimes Y$$

$$\epsilon(Y) = \eta^\vee(Y) = Y(1) = 0, \quad \text{pairing as dual basis}$$

$$S(Y) = \sum_0^{p-1} S^\vee(Y)(X^i)Y_i = Y(S(X))Y = Y(-X)Y = -Y$$

- Finally, the dual to X^a is $Y_a = \frac{1}{a!}Y^a$, the pairing is given by truncated exponential $U \mapsto \sum_0^{p-1} \frac{1}{a!} X^a \otimes Y^a$.

3. Deligne's Order-kills-group

We will consider commutative group schemes over connected bases.

3.1. The goal of this section is Deligne's theorem

Theorem 4 (Deligne)**.** *Let G be a finite flat commutative group scheme of order n over a locally noetherian base S, then G is killed by its order $[n]\colon G \to G$.*

The analogue for G non-commutative is not known in general, we only know this is true when we are over a field, or the dual numbers.

3.2. The proof is inspired by the fact that

$$\prod_G g = \prod_{Gx}(gx) = \prod_G (gx) = (\prod_G g)x^{|G|}.$$

In order to apply the trick to group schemes, Deligne defines the following trace map.

- Let $G = \mathrm{Spec}(A)$ be a finite commutative group scheme over $S = \mathrm{Spec}(B)$, and $T = \mathrm{Spec}(C)$ a finite flat scheme (not necessarily group scheme) of order m over S with structure map $f\colon T \to S$. Then we define a trace map $G(T) \to G(S)$, it is defined in a way such that compatible with the norm $A^\vee \otimes C \to A^\vee \otimes B$, namely

$$\begin{array}{ccc} G(T) & \hookrightarrow & A^\vee \otimes_R C \\ \downarrow{\scriptstyle \mathrm{tr}_f} & & \downarrow{\scriptstyle N} \\ G(S) & \hookrightarrow & A^\vee \otimes_R B \end{array}$$

  We need to check that $\mu^\vee(N(g)) = N(g) \otimes N(g), \eta^\vee(N(g)) = 1$, follows from properties of determinant. Intuitively, when G is a finite group, $T \to S$ is a covering of sets, this recovers the product of elements.
- One check: $\mathrm{tr}_f\colon G(T) \to G(S)$ is a group homomorphism and $\mathrm{tr}_f(f^*u) = u^m$.
- Suppose $t\colon T \to T$ is an S-automorphism, then $\mathrm{tr}_f(\beta) = \mathrm{tr}_f(t\beta)$
- Let $u \in G(S)$, our goal is to show $u^m = 1$. Let us denote by $t_u\colon G \to G$ the translation on G by u. We consider the identity element $1_G \in G(G)$, the analogue of $\prod_G g$.
- Note that $\mathrm{tr}_f(1_G) = \mathrm{tr}_f(1_G \circ t_u)$. As $1_G \circ t_u = 1_G \times f^*u$, we know

$$\mathrm{tr}_f(1_G) = \mathrm{tr}_f(1_G \times f^*u) = \mathrm{tr}_f(1_G) \times \mathrm{tr}_f(f^*u) = \mathrm{tr}_f(1_G) \times u^m.$$

4. Naive extensions

4.1. Let S be a regular scheme of dimension one. We show that:

Theorem 5. *Let G be a finite group scheme over S, then*

- *Each subgroup scheme of the generic fiber $H_\eta \subset G_\eta$ extends uniquely to a flat subgroup scheme of $H \subset G$.*
- *The subgroup schemes H_η is conjugate to H'_η if and only if H is conjugate to H' in G. Also $H_\eta \subset G_\eta$ is normal iff $H \subset G$ is normal.*

4.2. Let us consider the Hilbert scheme $\mathrm{Hilb}^r_{G/S}(T)$ of length r finite subschemes of G, valuative criteria gives us a flat extension. We need to show that there is a structure of subgroup scheme. The structure of group scheme is given by diagram of products. The Hilbert scheme construction also extends products of the subscheme. Flatness show that the fibers product-limit equals to the product of fiber-limit, as they have the same length.

4.3. The aforementioned theorem allows us to prove sylow theorem, by reducing to generic fiber.

5. Connected-étale sequence

5.1. Here is the goal of this section

Theorem 6. *Let R be a henselian local ring and let G by an affine group scheme, flat and finite type over R. Then there is an exact sequence*

$$0 \to G^0 \to G \to G^{et} \to 0$$

5.2. The Henselian condition show that idempotents on the special fiber lifts to idempotents over R. But idempotents are determined by local ring of maximal ideals, in our case maximal ideals are concentrated in the special fiber, therefore idempotents of the generic fiber uniquely lifts.

5.3. Let $e_0, \dots e_n$ be the idempotent generators of A^{et}. Then $A = \oplus e_i A$. The section ϵ^* vanishes on all but one component, say $\epsilon^*(e_0) = 1$. Let us set $G^0 = \mathrm{Spec}(e_0 A)$, we see it is flat over R. We have the sequence

$$0 \to \mathrm{Spec}(e_0 A) \to \mathrm{Spec}(A) \to \mathrm{Spec}(\bigoplus e_i R_i) \to 0$$

This is exact by counting the rank and apply Lagrange's theorem.

5.4. The decomposition satisfies universal properties: any connected group scheme to G factors through G^0, any morphism to a étale group scheme factors through G^{et}.

Theorem 7. *In case G is a finite group scheme over a perfect field, the sequence splits.*

For perfect field, taking reduce subscheme commutes with base change. Therefore we have $(G^{\mathrm{red}})_{\overline{k}} = (G_{\overline{k}})^{red} = (G^{et})_{\overline{k}}$, then apply Galois descent.

5.5. Galois correspondence. Let S be a scheme, let $\overline{s} \in S$ be a geometric point. We have the fiber functor

$$F_{\overline{s}} \colon \mathtt{Fet}_{/S} \to \mathtt{Sets}, \quad Y \mapsto Y_{\overline{s}}$$

We define the fundamental group $\pi_1(X, \overline{s})$ to be the automorphism group of $F_{\overline{s}}$. It is a profinite group, where the topology is induced from

$$\pi_1(X, \overline{s}) = \mathrm{Aut}(F_{\overline{s}}) \hookrightarrow \prod_{Y \in \mathtt{Fet}_{/S}} \mathrm{Aut}_X(Y)$$

Theorem 8 (Grothendieck)**.** *The functor*

$$F_{\overline{s}} \to \pi_1(X, \overline{s})\text{-}\mathtt{Sets}$$

is an equivalence of categories.

The reverse morphism is given by taking coproduct of the factors and quotient out the automorphism. The equivalence admits various decorations. For example, to the subcategory of group objects, we know the category of étale group schemes is equivalent to the category of π_1-groups.

5.6. Let us show that

Theorem 9. *The functor $G \to G^{et}$ and $G \to G^0$ are exact.*

It suffices to show that the first one is exact. Right exactness is clear. Left exactness follows from fact that kernel commutes with taking reduced geometric fiber (Fubini for limits) and that reduced geometric fiber determine the étale group scheme.

6. p-divisible groups

6.1. A p-divisible group of height h over a scheme S is an inductive system of group schemes (G_v, i_v) such that

- G_v is locally free of order p^{hv}
- We have short exact sequence $0 \to G_v \xrightarrow{i_v} G_{v+1} \xrightarrow{p^v} G_{v+1}$

6.2. The second condition factors into G_v, and is isomorphism by Lagrange's theorem. We denote such map by j_v or $j_{1,v}$. Let us denote the composition

$$i_{v+m-1} \circ \cdots \circ i_{v+1} \circ i_v$$

by $i_{v,m}$, here the first subscript v remembers the source. Similarly, let us denote the composition

$$j_v \circ j_{v+1} \circ \cdots \circ j_{v+m-1}$$

by $i_{m,v}$, here the second subscript v remembers the target. In general the map $G_{m+v} \xrightarrow{p^m} G_{m+v}$ factors into $i_{m,v} \circ j_{m,v}$

Theorem 10. *The second datum of a p-divisible group can be equivalently defined as compatible morphism $i_{v,m} \colon G_v \to G_{v+m}, j_{v,m} \colon G_{v+m} \to G_m$ such that*

$$i_{mv} \circ j_{m,v} = p^m, \quad j_{m,v} \circ i_{m,v} \quad \textit{exact}$$

6.3. There are some typical examples: $(\mathbb{Q}_p/\mathbb{Z}_p)^h$, $\mathbb{G}_m(p)$, $A(p)$. What is the height of $A(p)$? First of all, by miracle flatness, we know $A[n]$ is flat, then we lift to characteristic zero. Or we use theorem of cube, which implies that $[d]^*L = L^{d(d+1)/2} \otimes ([-1]^*L)^{\otimes d(d-1)/2}$. Let L be a symmetric line bundle, we see $[d]^*L = L^{d^2}$. Then apply $\deg_{f^*L}(Y) = \deg(f)\deg_L(X)$.

Non-example $\{\alpha_{p^r}\}$, as the kernel of addition p-times is the whole thing. Or we will later see that $n + n' = h = 1$ is not possible.

6.4. We apply the previous discussion to p-divisible groups.

Theorem 11. *The fiber functor yields a equivalence of categories*

$$\texttt{p-div}_{/S} \to \texttt{Free-}\pi_1(S,\overline{s})\texttt{-mods}$$

When R is henselian, we have $\pi_1(S,\overline{s}) = \pi_1(k(s))$, the p-divisible group over henselian dvr is uniquely determined by the special fiber.

6.5. For the connected-etale sequence, we have

Theorem 12. *Let G be a p-divisible group over a field k. Let R be any henselian local ring. Then G also has an connected-etale sequence. When k is perfect, the connected-etale sequence splits.*

6.6. The formation of Cartier dual also carries out to p-divisible groups, but j and i are switches. Given

$$0 \longrightarrow G_1 \xrightarrow{i_{1,v}} G_{v+1} \xrightarrow{j_{1,v}} G_v \longrightarrow 0$$

taking dual we have

$$0 \longrightarrow G_v^\vee \xrightarrow{j_{1,v}^\vee} G_{v+1}^\vee \xrightarrow{i_{1,v}^\vee} G_1^\vee \longrightarrow 0$$

Let us note that $i_{1,v} \circ j_{v,1} = [p^v]$, therefore $j_{v,1}^\vee \circ i_{1,v}^\vee = [p^v]$. Composing the later short exact sequence with $j_{v,1}^\vee$, we arrive at the definition of p-divisible groups. Note that taking dual preserves order, therefore $G^\vee = (G_v^\vee, j_{1,v}^\vee)$ is a p-divisible group of height h.

7. Serre-Tate Equivalence

Let R be a complete noetherian local ring with residue characteristic $p > 0$. Let $A = R[[X_1, \cdots, X_n]]$. An n-dimensional formal lie group Γ over R consists of a pair of maps

$$m\colon A \to A\widehat{\otimes}_R A, \quad e\colon A \to R$$

Let us describe f by the image $f_i(Y,Z) = m(X_i)$ in $R[[Y_i, Z_i]]$ satisfying the group axioms.

7.1. We say Γ is divisible if $[p]^*\colon A \to A$ is free. Let $A_v = A/[p^v]^* I$, where $I = (\underline{X})$, we will show this is a connected p-divisible group and

Theorem 13 (Serre-Tate)**.** *The functor $\Gamma \to \Gamma(p)$ is an equivalence of categories from the category of divisible commutative formal Lie groups to the category of connected p-divisible groups. We call the Krull dimension of A the dimension of the p-divisible group.*

8. Formal groups

8.1. Let G be an algebraic group over a field k. Let us consider the local artinian point of G concentrated at identity. This defines a functor $\widehat{G}\colon \mathtt{Art}_{/k} \to \mathtt{Sets}$ it is pro-represented by $\mathrm{Spf}(\widehat{O}_{G,e})$. When G is smooth, $\widehat{G}$ is a formal group.

Lemma 14. *Let $I = (X_1, \cdots, X_n)$ and $A_v = A/([p]^* I)$, this is a finite flat R-module.*

9. Serre-Tate: The proof

References

[CS86] Gary Cornell and Joseph H. Silverman, editors. *Arithmetic geometry*. Springer-Verlag, New York, 1986. Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984.