# Group Schemes and Dieudonné Theory

Casimir Kothari
No Theory 5/1/24

## 1 Group Schemes

### 1.1 Motivation: $p$-torsion in characteristic $p$

Suppose that $E$ is an elliptic curve over $k = \overline{\mathbb{F}}_p$. Recall that for each prime $\ell$, multiplication by $\ell$ is a degree $\ell^2$ isogeny from $E$ to $E$. If $\ell \neq p$, the $\ell$-torsion points of $E$ over $k$ form a group of order $\ell^2$ isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. However, we know that for $\ell = p$, things are very different. We have that the $p$-torsion of $E$ over $k$ is either $\mathbb{Z}/p$ or 0, depending on if $E$ is ordinary or supersingular. Why doesn't this contradict the fact that the degree of $\times p$ is $p^2$?

The answer lies in the way that we define the kernel of the multiplication by $p$ map. When we allow ourselves to work with schemes instead of varieties, we find that there is extra nonreduced structure which explains this discrepancy. In other words, $E[p]$ considered as a group scheme is finite of order $p^2$, but its underlying reduced variety has only order 1 or $p$. So, group schemes provide the right conceptual framework to understand torsion phenomena in characteristic $p$ from a uniform/conceptual group-theoretic perspective. Even if one is only interested in characteristic 0, this still proves useful as one can try to understand things by reducing modulo $p$.

### 1.2 Definitions and First Properties

#### 1.2.1 Group Objects in a Category

Let $\mathcal{C}$ be a category admitting finite products, and let $S$ denote the final object of $\mathcal{C}$(e.g. $\mathcal{C}$ = the category of varieties or schemes over a field $k$, and $S = \operatorname{Spec} k$). A group object in $\mathcal{C}$ is an object $G \in \mathcal{C}$ together with a multiplication $m : G \times G \to G$, inverse $i : G \to G$, and identity $e : S \to G$ such that $G$ satisfies all of the formal axioms of a group. For instance, associativity of the group law means that the diagram

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times \mathrm{id}} & G \times G \\ \downarrow{\scriptstyle \mathrm{id} \times m} & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G \end{array}$$

commutes. i.e. $G$ is a "group" for which all group operations are actually morphisms in the category $\mathcal{C}$. Group objects in $\mathcal{C}$ themselves form a category, where the morphisms are "group homomorphisms": maps in $\mathcal{C}$ which respect the multiplication laws.

There is an alternate useful perspective on group objects via the Yoneda lemma. Recall that we have a fully faithful embedding $\mathcal{C} \to \mathrm{Fun}(\mathcal{C}^{\mathrm{op}}, \mathrm{Sets})$, by sending $X \in \mathcal{C}$ to the representable functor $Y \mapsto X(Y) := \mathrm{Hom}(Y, X)$. In this optic, a group object in $\mathcal{C}$ is equivalently an object $G \in \mathcal{C}$ together with a group structure on $G(T)$ for every $T \in \mathcal{C}$ such that the for each map $T' \to T$, the induced map $G(T) \to G(T')$ is a group homomorphism. Under this perspective, a group homomorphism $G \to G'$ is just a group homomorphism $G(T) \to G'(T)$ for every $T \in \mathcal{C}$ which is compatible with induced maps from $T' \to T$.

#### 1.2.2 Group schemes

We now specialize the above general discussion to the category $\mathrm{Sch}/k$ of schemes over a field $k$.

**Definition 1.1.** A group scheme over $k$ is a contravariant functor $G : (\mathrm{Sch}/k) \to Gp$ such that the underlying functor $\mathrm{Sch}/k \to \mathrm{Sets}$ is representable by a scheme.

Equivalently by what we have said, a group scheme $G/k$ consists of a $k$-scheme $G$ together with multiplication, inverse, and identity morphisms.

A group scheme $G/k$ is **commutative** if the corresponding functor factors through abelian groups, or equivalently if the multiplication $m : G \times G \to G$ be commutative. In this talk, we will only be considering commutative group schemes.

If $P$ is a property of schemes, we say that a group scheme has property $P$ if its underlying scheme does. So for instance we can speak of finite/affine/smooth/etc. group schemes over $k$. If $G$ is a finite group scheme over $k$, then $G = \operatorname{Spec} A$ for a finite $k$-algebra $A$, and we define the **order** $|G|$ of $G$ to be $\dim_k A$.

Before giving examples, we mention one more useful fact that lets us work with commutative group schemes in much the same way as we work with usual commutative groups.

**Proposition 1.2** (Grothendieck)**.** The category of commutative group schemes over a field is abelian.

Thus we can take kernels and cokernels of morphisms of group schemes, take direct sums and quotients of group schemes, and consider Hom and Ext groups between group schemes. For instance, if $f : G \to G'$ is a morphism of commutative group schemes, we define $\ker(f)$ to be the group scheme whose $T$-valued points are $\ker(G(T) \to G'(T))$ for any $k$-scheme $T$. However the construction of cokernels is more subtle, and in particular $\operatorname{coker}(f)$ is not just constructed by $T \mapsto \operatorname{coker}(G(T) \to G'(T))$.

## 1.3 Examples

1. Perhaps the most basic group scheme is the additive group $\mathbb{G}_a$, which is defined by $\mathbb{G}_a(R) = R$, where we view the $k$-algebra $R$ as an additive group. The underlying scheme of $\mathbb{G}_a$ is just $\mathbb{A}^1 = \operatorname{Spec} k[t]$.

2. Another basic example is the multiplicative group $\mathbb{G}_m$, which is defined by $\mathbb{G}_m(R) = R^\times$ viewed as a multiplicative group. The underlying scheme of $\mathbb{G}_m$ is just $\mathbb{A}^1 - \{0\} = \operatorname{Spec} k[t, t^{-1}]$.

3. Any abelian variety $A/k$ is a group scheme. In fact, abelian varieties can be characterized as proper connected smooth group schemes over a field.

4. (Constant Group Schemes) Given any abstract group $G$, we can form a group scheme $\underline{G}/k$, defined as the constant sheaf $\mathrm{Sch}/k \to \mathrm{Gp}$ determined by $G$. We can see $\underline{G}$ as a scheme via $\underline{G} = \sqcup_{g \in G} \operatorname{Spec} k$ and with addition law determined by that of $G$. We will just denote such a group scheme by $G$. If $G$ is finite, we get a finite group scheme of order equal to the order of the abstract group $G$. Such constant group schemes are always smooth over $k$.

5. (Roots of Unity Group Schemes) For any positive integer $n$, we have the group scheme $\mu_n$ of $n$-th roots of unity, defined by $\mu_n(R) = \{r \in R : r^n = 1\}$. It is represented by the scheme Spec $\frac{k[x]}{(x^n-1)}$, and hence evidently a finite group scheme of order $n$. We have $\mu_n = \ker(\mathbb{G}_m \overset{x \mapsto x^n}{\to} \mathbb{G}_m)$.

   If $n$ is coprime to the characteristic of $k$, then $\mu_n$ is a smooth group scheme over $k$. However, note that if $k$ has characteristic $p$, then $\mu_p = \operatorname{Spec} \frac{k[x]}{(x-1)^p}$ is a non-reduced scheme with only one physical point. In particular, $\mu_p$ has order $p$ despite the fact that $\mu_p(k') = \{1\}$ for any field $k'/k$.

6. If $k$ has characteristic $p$, a curious group scheme is $\alpha_p$, defined by $\alpha_p(R) = \{r \in R : r^p = 0\}$. Note that this only forms a group because of the relation $(x+y)^p = x^p + y^p$ in characteristic $p$! It is represented by the scheme Spec $\frac{k[x]}{(x^p)}$. Hence $\alpha_p$ has order $p$ and is a nonreduced group scheme with only one physical point.

What does the general commutative group scheme look like? The following proposition tells us that in fact these examples are the atomic building blocks of any (finite type) commutative group scheme:

**Proposition 1.3** ([O], Lemma II.6.1)**.** Let $k$ be an algebraically closed field, and $G/k$ a commutative group scheme of finite type. Then there exists a chain of subgroup schemes

$$0 = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

such that the quotients $G_i/G_{i-1}$ are each isomorphic to one of the following groups:

1. $\mathbb{G}_a$;
2. $\mathbb{G}_m$;
3. An abelian variety;
4. The finite group schemes $\mathbb{Z}/\ell\mathbb{Z}$ for $\ell$ prime and (if $k$ has characteristic $p$) the group schemes $\mu_p, \alpha_p$.

Of course, this doesn't on its own give us a complete classification of commutative group schemes over an algebraically closed field; one also needs to understand extensions of such group schemes, which can get somewhat complicated.

**Example 1.4.** Let $E/\overline{\mathbb{F}}_p$ be an elliptic curve. Then $E[p] := \ker(E \stackrel{\times p}{\to} E)$ is a group scheme of order $p^2$. If $E$ is ordinary, we have

$$0 \subset \mathbb{Z}/p \subset E[p]$$

with $E[p]/(\mathbb{Z}/p) \cong \mu_p$, while if $E$ is supersingular we have

$$0 \subset \alpha_p \subset E[p]$$

with $E[p]/\alpha_p = \alpha_p$. Thus group schemes offer an approach to studying the difference between ordinarity and supersingularity in characteristic $p$.

# 2 Dieudonné Theory

Suppose now that $G/k$ is a finite commutative group scheme over a field $k$. It turns out that

1. If $|G|$ is coprime to the characteristic of $k$, then $G$ is an étale (i.e. smooth) group scheme over $k$.
2. The association $G \mapsto G(\overline{k})$ defines an equivalence of categories between the categories of finite étale group schemes over $k$ and finite $\mathrm{Gal}(\overline{k}/k)$-modules.

In other words: étale group schemes are the same as finite Galois representations, and $char(k) \nmid |G|$ implies étale!

However, as the examples of $\alpha_p$ and $\mu_p$ show, taking $\overline{k}$-points cannot be the whole story for finite group schemes of $p$-power order in characteristic $p$. So we might wonder if there is some linear data, analogous to Galois representations in the $p \nmid |G|$ case, which can be used to fully understand finite group schemes of $p$-power order. This is what Dieudonné theory does.

Let $k$ be a perfect field of characteristic $p$. Let $W = W(k)$ be the ring of Witt vectors of $k$. It is a complete discrete valuation ring with maximal ideal $(p)$ and residue field $k$; for example $W(\mathbb{F}_p) = \mathbb{Z}_p$, and when $k = \mathbb{F}_{p^n}$, then $W(k) = \mathbb{Z}_p[\zeta_{p^n-1}]$, the ring of integers in the unramified degree $n$ extension of $\mathbb{Q}_p$.

The ring $W$ has a Frobenius map $\sigma : W \to W$, reducing to the Frobenius on $k = W/p$, which is an isomorphism since $k$ is perfect.

**Definition 2.1.** A Dieudonné module over $k$ is a $W$-module $D$ together with additive morphisms $F, V : D \to D$ such that $F(ad) = \sigma(a)F(d), V(ad) = \sigma^{-1}(a)V(d)$, and $FV = VF = p$.

We say $F$ is $\sigma$-linear and $V$ is $\sigma^{-1}$-linear. Note that a Dieudonné module can also be understood as a module over a certain noncommutative ring $W\{F, V\}/(FV = VF = p, Fa = \sigma(a)F, Va = \sigma^{-1}(a)V)$.

The main theorem of Dieudonné theory tells us that we can understand commutative $p$-power order group schemes in terms of Dieudonné modules:

**Theorem 2.2.** There is an contravariant equivalence of categories $M$ : finite commutative group schemes of $p$-power order over $k \to$ Dieudonné modules of finite length over $W$. Moreover this equivalence satisfies the following properties:

1. $M$ is an exact functor (this is true of any equivalence between abelian categories).
2. $|G| = p^{length_W(M(G))}$.
3. $G$ is connected if and only if $F$ is nilpotent on $M(G)$.
4. $G$ is étale (i.e. smooth) if and only if $F$ is an isomorphism on $M(G)$

Dieudonné theory should be thought of as saying that finite commutative $p$-power order group schemes in characteristic $p$ are essentially linear-algebraic in nature: they behave just like modules over some ring.

## 2.1 Example: Group schemes of order $p$

Let's use the Dieudonné equivalence to classify all group schemes of order $p$ over an arbitrary perfect field $k$ of characteristic $p$.

Let $G/k$ be a group scheme of order $p$. Then $M(G)$ is a Dieudonné module of length 1 over $W(k)$, and hence $M(G) \cong k$ as a $W(k)$-module. Write $M(G) = k\langle e \rangle$. The semilinear operators $F$ and $V$ are determined by $a, b \in k$ such that $F(e) = ae, V(e) = be$. By the relation $FV = VF = 0$, we conclude that either $a = 0$ or $b = 0$. Letting $M_{a,b}$ be the associated Dieudonné module, we are reduced to classifying the $M_{a,b}$ up to isomorphism. There are three cases:

1. $a = b = 0$: In this case, we get the unique Dieudonné module $M(G) = k$ with $F = V = 0$.
2. $a \neq 0, b = 0$: We need to determine when $M_{a,0} \cong M_{a',0}$. Suppose that $\phi : M_{a,0} \to M_{a',0}$ is an isomorphism, so that $\phi(e) = ce$ for some $c \in k^\times$. The condition that $\phi$ be compatible with $F$ means that $\phi(ae) = F(ce)$. Expanding, this gives $ace = c^p a' e$, or in other words $a = c^{p-1}a'$. Consequently we conclude that the isomorphism classes in this case are in bijection with the set $k^\times/(k^\times)^{p-1}$.
3. $a = 0, b \neq 0$: By a completely analogous procedure, we find that $M_{0,b} \cong M_{0,b'}$ if there is $c \in k^\times$ with $b = c^{1-p}b'$, and thus we get isomorphism classes in this case in bijection with $k^\times/(k^\times)^{p-1}$.

Which group schemes do these Dieudonné modules correspond to? Using the properties of the Dieudonné equivalence, we can figure it out:

1. The module $M_{0,0}$ is the Dieudonné module of $\alpha_p$.
2. This is the étale case. The module $M_{1,0}$ is the Dieudonné module of $\mathbb{Z}/p$, and $M_{a,0}$ is the Dieudonné module of a *twisted form* of $\mathbb{Z}/p$, i.e. a group scheme $G/k$ such that $G \times_k \overline{k}$ is isomorphic to $\mathbb{Z}/p$ over $k$.
3. The module $M_{0,1}$ corresponds to $\mu_p$, and $M_{0,a}$ corresponds to a twisted form of $\mu_p$.

**Corollary 2.3.** Over $\mathbb{F}_q$, there are $2p - 1$ isomorphism classes of group schemes of order $p$. Over $k = \overline{\mathbb{F}}_p$, there are three group schemes of order $p$: $\mathbb{Z}/p, \mu_p$, and $\alpha_p$.

We also ended up proving the following fun corollary in the process:

**Corollary 2.4.** Representations $\mathrm{Gal}(\overline{k}/k) \to \mathbb{F}_p^\times$ are in bijection with $k^\times/(k^\times)^{p-1}$.

*Proof.* Such representations are in bijection with finite étale order $p$ group schemes over $k$, which are in bijection with the modules $M_{a,0}$ with $a \neq 0$, which we have shown to be $k^\times/(k^\times)^{p-1}$. □

An alternate proof of this fact can be given with Kummer theory.

## 2.2 Beyond perfect fields

Let $S = \operatorname{Spec} R$ be an arbitrary affine scheme. We can make sense of the notion of a group scheme over $S$ in the same way as before: a group object in the category of $\mathrm{Sch}/S$. However, in order to study the properties of such group schemes, we want to enforce some uniformity that says that a group scheme $G/S$ is a nicely varying family of group schemes parametrized by $S$. To do this, we define a finite locally free group scheme over $S$ to be a group scheme $G/S$, such that $G = \operatorname{Spec} A$ with $A$ a finitely generated projective $R$-module. In this case, the order of $G$ is defined to be $|G| = \mathrm{rk}_R(A)$.

Looking at our previous computations, we saw that to give an order $p$ group scheme over a perfect field $k$ is the same as giving $(a, b) \in k \times k$ with $ab = 0$, up to the equivalence relation $(a, b) \sim (\lambda^{p-1}a, \lambda^{1-p}b)$ for $\lambda \in k^\times$. A natural question to ask is if we can say anything similar for group schemes of order $p$ over an arbitrary base $S$. In 1970, Oort and Tate answered this question in the affirmative:

**Theorem 2.5** ([OT])**.** Let $R$ be any local ring of characteristic $p$. Then there is a bijection between the set of isomorphism classes of order $p$ group schemes over $R$ and the set up tuples $(a, b) \in R^2$ with $ab = 0$ up to the equivalence relation $(a, b) \sim (\lambda^{p-1}a, \lambda^{1-p}b)$ for $\lambda \in R^\times$.

In fact, Oort and Tate classify order $p$ group schemes over an arbitrary ring $R$ of characteristic $p$; in this case one needs to allow $a$ and $b$ to be sections of line bundles over $R$ instead of $R$ itself. In more geometric terms, the result is that the moduli stack of group schemes of order $p$ in characteristic $p$ is isomorphic to the stack

$$\left[\frac{\mathbb{F}_p[x, y]}{(xy)}/\mathbb{G}_m\right], \quad \lambda \cdot x = \lambda^{p-1}x, \lambda \cdot y = \lambda^{1-p}y,$$

where here $x$ is like the $F$ and $y$ is like the $V$ on a Dieudonné module.

# References


[O] Frans Oort. *Commutative Group Schemes.* Springer-Verlag, 1966.

[OT] Oort, Tate. Group Schemes of Prime Order, 1970.

[S] Andrew Snowden. Online Course on Mazur's Theorem. https://websites.umich.edu/ asnowden/teaching/2013/679/.

[T] Tate. Finite Flat Group Schemes. In Cornell-Silverman-Stevens, Modular Forms and Fermat's Last Theorem, 1997.