Group Schemes

Affine and Projective

Leonardo Finzi

Contents

1 Group Schemes **1**
1.1 Some Group Theory 5
1.2 Automorphisms of Group Schemes 6
1.3 Algebraic Groups and Tangent Spaces 7

2 Hopf Algebras **9**
2.1 Categorical Remarks 10
2.2 Cartier Duality 13

3 Abelian k-Varieties **14**
3.1 An Extreme Theorem 16
3.2 Isogenies and a Decomposition Theorem 17

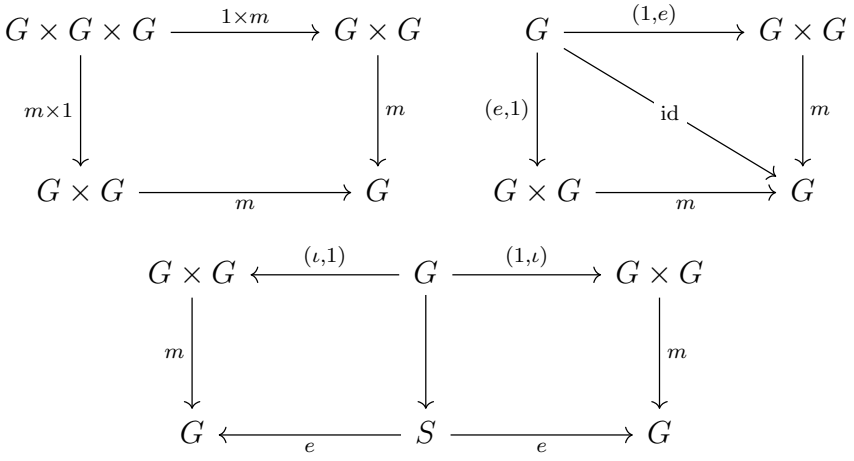
4 Acknowledgments **20**

1. Group Schemes

To begin, we will define group schemes in a few (equivalent) ways.

Definition 1.1. Let S be a scheme. A *group scheme* over S, or an *S-group*, is a tuple (G, m, e, ι), where G is an S-scheme, $m : G \times G \to G$ is a multiplication map, $\iota : G \to G$ is an inversion map, and $e : S \to G$ is a unit map such that the following

diagrams commute, where $G \to S$ is the associated S-scheme structure map for G:



Note that we can form the category $\mathtt{Gp}_S$ of S-groups whose morphisms are S-morphisms compatible with group laws:

$$\mathtt{Gp}_S(G, G') = \{f \in \mathtt{Sch}_S(G, G') \mid f \circ m_G = m_{G'} \circ (f \times f)\}$$

Hence, $\mathtt{Gp}_S$ is a subcategory of $\mathtt{Sch}_S$. Note further that the diagrams in Definition 1.1 correspond to the axioms of a group, namely, associativity, existence of an identity element, and the existence of inverses, respectively. Additionally, this definition of group schemes is not restricted to the category of S-schemes. These diagrams generally define a *group object* in a category with products. For example, the category of graphs admits group objects called *group graphs*.

Of course, this definition, although explicit, is generally not very useful to us algebraically. As group schemes are schemes, we can equivalently formulate them in terms of their sections.

Definition 1.2. Let G be an S-scheme. Then G is a *group scheme* if

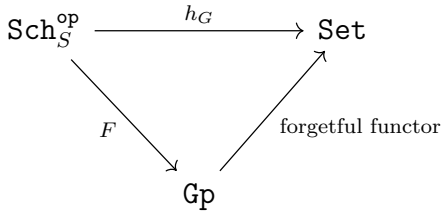
(i) for all S-schemes T, the sections $G(T) = \mathtt{Sch}_S(T, G)$ are a group; and

(ii) if $T \to T'$ is an S-morphism, then $G(T') \to G(T)$ is a group homomorphism.

If k is a field, to check that a k-scheme G is a group scheme over k, it suffices to consider only the R-valued points $G(R)$ whenever R is a k-algebra.

As a final equivalent formulation, just as we may view schemes as representable functors [MO15, 41], we can represent group schemes with a functor.

Definition 1.3. A *group scheme* over S is an S-scheme G and a functor $F : \mathtt{Sch}_S^{\mathtt{op}} \to \mathtt{Gp}$ such that the following diagram commutes:



Here, h_G denotes the Yoneda functor, which takes $X \mapsto \mathtt{Sch}_S^{\mathtt{op}}(X, G)$.

A functor $\mathtt{Sch}_S^{\mathtt{op}} \to \mathtt{Set}$ that factors through the forgetful functor $\mathtt{Gp} \to \mathtt{Set}$ is called a *group functor* (on S-schemes). Thus, we may view an S-group as a group functor representable by an S-scheme. For completeness, we note the following proposition:

Proposition 1.4. Definitions 1.1, 1.2, and 1.3 are equivalent.

In all three formulations of group schemes, it is clear that groups are central to their definition, as the name suggests. We will see in the following examples that these group schemes can correspond to very straight-forward groups. For example, for a scheme S, for $\mathbb{A}_S^n = \mathbb{A}_{\mathbb{Z}}^n \times_{\mathbb{Z}} S$, $\mathbb{A}_S^n$ is an S-group called the *additive group scheme over S of dimension n*. Recall that $\Gamma(-)$ denotes the global sections of S. Then we have that $\mathbb{A}_S^n$ is a group scheme. Indeed, since $\mathbb{A}_S^n = \operatorname{Spec}(\mathcal{O}_S[x_1, \ldots, x_n])$, for any S-scheme T with structure map $\pi : T \to S$,

$$\mathbb{A}_S^n(T) = \mathtt{Sch}_S(T, \mathbb{A}_S^n) = \operatorname{Hom}_{\mathcal{O}_S - \mathtt{alg}}(\mathcal{O}_S[x_1, \ldots, x_n], \pi_* \mathcal{O}_T) = \Gamma(T)^n,$$

which is an additive group under coordinate-wise addition. Since, for any S-morphism $T \to T'$, $\Gamma(T)^n \to \Gamma(T')^n$ is a group homomorphism, this gives the Definition 1.2 version of a group scheme. But we may also give the more explicit Definition 1.1 version as well. If $S = \operatorname{Spec} k$ for a field k, then $(\mathbb{A}_S^n, m, e, \iota)$ is a group scheme where, for any k-algebra R,

$$\begin{aligned} m : R^n \times R^n &\longrightarrow R^n \\ ((a_1, \ldots, a_n), (b_1, \ldots, b_n)) &\longmapsto (a_1 + b_1, \ldots, a_n + b_n) \end{aligned}$$

$$e = (0, \ldots, 0) \in R^n$$

$$\begin{aligned} \iota : R^n &\longrightarrow R^n \\ (a_1, \ldots, a_n) &\longmapsto (-a_1, \ldots, -a_n) \end{aligned}$$

Finally, in the Definition 1.3 version of a group scheme, we have that $\mathbb{A}^n_S$ represents the group functor

$$\begin{aligned}\mathbb{G}^n_{a,S} : \mathtt{Sch}^{\mathtt{op}}_S &\to \mathtt{Set}\\ T &\mapsto \Gamma(T)^n\end{aligned}$$

which is also called the additive group scheme of dimension n over S. To avoid confusion, we refer to the group functor $\mathbb{G}^n_{a,S}$ as the additive group scheme instead of $\mathbb{A}^n_S$. If $S = \operatorname{Spec} R$ for a general ring R, we let $\mathbb{G}_{a,R} := \mathbb{G}_{a,S}$. This notation serves as a nice companion to the next example.

For a scheme S, we call $\mathbb{G}_{m,S}$ the *multiplicative group scheme over* S, where for any S-scheme T,

$$\mathbb{G}_{m,S}(T) = \Gamma(T)^* = \{g \in \Gamma(T) : g \text{ is a unit}\},$$

which is a multiplicative group. In the manner of Definition 1.2, if $S = \operatorname{Spec} k$ for some field k, then $(\mathbb{G}_{m,S}, m, e, \iota)$ is a group scheme where for any k-algebra R,

$$\begin{aligned}m : R^* \times R^* &\longrightarrow R^*\\ (a, b) &\longmapsto ab\end{aligned}$$

$$e = 1 \in R^*$$

$$\begin{aligned}\iota : R^* &\longrightarrow R^*\\ a &\longmapsto a^{-1}\end{aligned}$$

Finally, as in Definition 1.3, we have that $\mathbb{G}_{m,S}$ is represented by the S-scheme $\operatorname{Spec}(\mathcal{O}_S[x, x^{-1}])$. For higher dimensions, we define $\mathbb{G}^n_{m,S} = \mathbb{G}_m \times \cdots \times \mathbb{G}_m$, which is sometimes referred to as an n-torus, since the complex points of $\mathbb{G}^n_{m,\mathbb{C}}$ make up $(\mathbb{C}^*)^n$, which deformation retracts onto the topological n-torus $\mathbb{T}^n = (S^1)^{\times n}$.

Here we present more interesting examples of group schemes, following [MO15, 265]. For a fixed scheme S, the multiplicative group scheme of nth roots of unity $\mu_{n,S}$, where, for any S-scheme T,

$$\mu_{n,S}(T) = \{\zeta \in \Gamma(T, \mathcal{O}_T)^* : \zeta^n = 1\},$$

and if S has prime characteristic p, $\alpha_{p,S}$ is the p-characteristic group scheme, where, for any S-scheme T,

$$\alpha_{p,k}(T) = \{\xi \in \Gamma(T, \mathcal{O}_T) : \xi^p = 0\}.$$

In the style of Definition 1.3, we have that $\mu_{n,S}$ is represented by

$$\operatorname{Spec}\left(\frac{\mathcal{O}_S[x]}{(x^n-1)}\right)$$

and that $\alpha_{p,S}$ is represented by

$$\operatorname{Spec}\left(\frac{\mathcal{O}_S[x]}{(x^p)}\right).$$

1.1. **Some Group Theory**

Having gone over some examples of group schemes, we have seen that the group scheme theory has some overlap with group theory. For example, we discuss additive and multiplicative group schemes (as opposed to additive or multiplicative groups) and examples of group schemes are scheme-versions of groups we work with often (for a further example, see 1.2). In this section, we will briefly describe some of the group scheme terminology analogous to terminology we encounter in group theory.

Definition 1.5. Let G be an S-group. A *subgroup scheme* H of G is a locally closed subscheme of G such that for all S-schemes T, $H(T)$ is a subgroup of $G(T)$.

As a trivial example, the unit section e of a group scheme G, as in Definition 1.1, is a subgroup scheme of G. This is because $e : G \to S$ is an immersion, which are locally closed. Certainly G is also a subgroup scheme of G.

As in the usual group theory, we may define a normal subgroup scheme.

Definition 1.6. Let G be an S-group and H be a subgroup scheme of G. We say H is *normal* in G if for all S-schemes T, $H(T)$ is a normal subgroup of $G(T)$.

Notice that so far, both subgroup schemes and normal subgroup schemes are defined by their T-sections, which begs the question whether these subgroup schemes behave the same as their analogous subgroups. In particular, do the normal subgroup schemes behave like their normal subgroup counterparts? We give kernels as an example of where the theory differs.

Definition 1.7. Let $f : G \to H$ be a morphism of S-groups. The *kernel* of f is defined to be

$$\operatorname{Ker} f := f^{-1}(e_H).$$

At the very least, we see that this coincides with how we define kernels of group homomorphisms, since for any S-scheme T,

$$(\operatorname{Ker} f)(T) = \{x \in G(T) : f(T)(x) = e_H(T)\} = \ker f(T).$$

In particular, Ker f is a subgroup scheme of G. For a more geometric view, we also have that Ker $f \cong G \times_H S$.

As some explicit examples, we have that $\mu_{n,S}$ and $\alpha_{p,S}$ arise as kernels of a morphism of S-groups. For instance, $\mu_{n,S} = \text{Ker } \varphi$ where $\varphi : \mathbb{G}_{m,S} \to \mathbb{G}_{m,S}$ taking $x \mapsto x^n$. More number-theoretically, if char $S = p$, then $\alpha_{p,S} = \text{Ker}(\text{Frob})$, where $\text{Frob} : \mathbb{A}^1_S \to \mathbb{A}^1_S$ is the Frobenius map taking $\xi \mapsto \xi^p$.

Now, as in the usual group theory, if H is a subgroup scheme of G such that $H = \text{Ker } f$, for some morphism of S-groups $f : G \to G'$, then H is a normal subgroup scheme of G. Unfortunately, it is not the case that every normal subgroup scheme of G is of the form Ker f, for some morphism of S-groups $f : G \to G'$. Simply put, quotients do not behave in the same way as in usual group theory, since there is more structure we wish to keep track of. In particular, if we were to naively define G/H as

$$(G/H)(T) := G(T)/H(T)$$

for all S-schemes T, then we run into the problem that G/H may not be representable. The issue is usually resolved using the fppf topology, which we do not discuss further here (see [GW23, (27.6-27.9)]). In Section 3.2, we will discuss a situation in which every normal subgroup scheme is of the form Ker f, for an f of a certain form.

1.2. **Automorphisms of Group Schemes**

We will now briefly deal with a type of example that Definition 1.3 can be particularly useful for. That is, we will determine the structure of the group of automorphisms of certain group schemes. The key move that will be employed is to use the functorial representability of group schemes.

Consider $\mathbb{G}_{a,k}$, for k a field of characteristic zero. What is $\text{Aut}_k\ \mathbb{G}_{a,k}$? We know that $\mathbb{G}_{a,k}$ is represented by Spec $k[x]$, so it suffices to consider $\text{Aut}_k\ k[x]$. Let $f \in \text{Aut}_k\ k[x]$. Since f is determined uniquely by where it sends x, we will consider $f(x)$. Since f is additive, the formal derivative of $f(x)$ is constant. Such a polynomial over a field of characteristic zero is of the form $cx+d$ for some scalars $c, d \in k$. In particular, f is an automorphism, so

$$x = (f^{-1} \circ f)(x) = f^{-1}(cx + d) = cf^{-1}(x) + d,$$

which implies that $d = 0$. Hence, $f(x) = cx$ for some $c \in k$. Finally, since f^{-1} is also an automorphism, for some $c' \in k$,

$$x = (f^{-1} \circ f)(x) = f^{-1}(cx) = cf^{-1}(x) = cc'x,$$

so $c \in k^*$. Thus, $\text{Aut}_k\ \mathbb{G}_{a,k} \cong \text{Aut}_k\ k[x] \cong k^*$. In fact, Aut $\mathbb{G}_{a,k}$ is k-group scheme

isomorphic to $\mathbb{G}_{m,k}$.

Now, consider $\mathbb{G}_{m,k}$ where k is a field. We may ask again, what is $\mathrm{Aut}_k\ \mathbb{G}_{m,k}$? Since $\mathbb{G}_{m,k}$ is represented by Spec $k[x, x^{-1}]$, it suffices to consider $\mathrm{Aut}_k\ k[x, x^{-1}]$. Similarly as before, it follows that any $f \in \mathrm{Aut}_k\ k[x, x^{-1}]$ must take x to a unit, i.e., $f(x) = cx^m$ for some $c \in k^*$ and $m \in \mathbb{Z}$. Since f^{-1} is also an automorphism then for some $c' \in k^*$ and $m' \in \mathbb{Z}$,

$$x = (f^{-1} \circ f)(x) = f^{-1}(cx^m) = c(f^{-1}(x))^m = c(c'x^{m'})^m = cc'x^{m'm},$$

so $m = \pm 1$. Additionally, since $1 = f(1) = c \cdot 1$, then $c = 1$. Thus, $\mathrm{Aut}_k\ \mathbb{G}_{m,k} \cong \mathrm{Aut}_k\ k[x, x^{-1}] \cong \mathbb{Z}/2\mathbb{Z}$.

1.3. **Algebraic Groups and Tangent Spaces**

So far, all examples we have given of group schemes have fallen under the following umbrella:

Definition 1.8. Let $S = \mathrm{Spec}\ k$ for a field k. A group scheme G over k is an *(affine) algebraic group* if it is locally of finite type over k.

Taking $S = \mathrm{Spec}\ k$, we have that $\mathbb{G}_{a,S}, \mathbb{G}_{m,S}, \mu_{n,S}, \alpha_{p,S}$ are all algebraic groups since they are represented by Spec $k[-]$.

For another example of an algebraic group, consider the group scheme $\mathrm{GL}_{n,k}$ over a field k, where for all k-algebras R,

$$\mathrm{GL}_{n,k}(R) = \{A \in \mathcal{M}_n(R) : \det A \in R^*\}.$$

This is an algebraic group since it is represented by

$$\mathrm{Spec}\left(k[x_{ij}, \det(x_{ij})^{-1}]\right).$$

As in Definition 1.1, we may endow $\mathrm{GL}_{n,k}$ with maps $(\mathrm{GL}_{n,k}, m, e, \iota)$ where all maps are the usual respective matrices and matrix operations, i.e., matrix multiplication, identity matrix, and matrix inversion.

For a similar example of an algebraic group, consider the determinant map det : $\mathrm{GL}_{n,k} \to \mathbb{G}_{m,k}$. As in the usual linear algebra, we have that for all k-algebras R,

$$(\mathrm{Ker}\det)(R) = \{A \in \mathcal{M}_n(R) : \det A = 1\} = \mathrm{SL}_{n,k}(R).$$

Though, $\mathrm{SL}_{n,k}$, unlike a general kernel of a k-morphism, is a *closed* subgroup scheme of $\mathrm{GL}_{n,k}$, not just locally closed as Definition 1.5 requires. In fact, all affine algebraic groups are closed subgroups of $\mathrm{GL}_{n,k}$.

We will now explore the definition of $\mathrm{GL}_{n,k}$ as an example of how algebraic groups allow us to understand their associated tangent spaces. Recall the following definition

[GW20, 149]:

Definition 1.9. Let X be a scheme. Then for any $x \in X$, the *absolute tangent space at* x is the vector space

$$T_x X = (\mathfrak{m}_x/\mathfrak{m}_x^2)^*,$$

where $\mathfrak{m}_x$ denotes the maximal ideal of the local ring $\mathcal{O}_{X,x}$.

Of course, we can construct tangent spaces in a more functorial way. First, for a field k, denote $k[\varepsilon] := k[T]/(T^2)$, where $\varepsilon^2 = 0$, to be the ring of dual numbers over k. Then we have the following proposition:

Proposition 1.10. For a k-scheme X and a k-valued point x, the map

$$T_x X \to X(k[\varepsilon])_x$$

is a bijection which is functorial in (X, x).

Proof. A proof can be found in [GW20, 152]. □

This construction of a tangent space, although it is notationally heavy, is extremely clear when broken down. Note that because $\varepsilon^2 = 0$, then for any $n \in k[\varepsilon]$, $n = a + \varepsilon b$, for $a, b \in k$ [MO15, 267]. So, what we have done is found an algebraic way to describe tangent lines, which we have put in bijection with the $T_x X$. Hence, the natural map from $T_x X \to X(k[\varepsilon])_x$ takes a tangent vector $v \in T_x X$ to a tangent line $x + \varepsilon v$. We may thus interpret ε as an algebraic way to denote a very small change along v.

Now, we finish with the promised example involving GL_n, inspired by Exercise 6.4 in [GW20, 168]. We have that for $G = \mathrm{GL}_{n,k}$, (G, m, e, ι) is an algebraic group, where m is the usual matrix multiplication map, $e = I_n$, and ι is the usual invertible-matrix inversion map. Given that we can pass to tangent spaces, we can ask, what are dm_e and $d\iota_e$ on $T_e\mathrm{GL}_{n,k}$, where $d-$ denotes derivation? First, given $m : G \to G$, by Proposition 1.10, the diagram below commutes:

$$\begin{array}{ccc} T_eG \times T_eG & \xrightarrow{dm_e} & T_eG \\ \downarrow & & \downarrow \\ G(k[\varepsilon])_e \times G(k[\varepsilon])_e & \xrightarrow{m\circ -} & G(k[\varepsilon])_e \end{array}$$

In particular, let $(v, w) \in T_eG \times T_eG$. Under the first vertical map, $(v, w) \mapsto (e + \varepsilon v, e + \varepsilon w)$. Precomposing with m gives

$$m(e + \varepsilon v, e + \varepsilon w) = e^2 + \varepsilon(v + w) + \varepsilon^2 vw = e + \varepsilon(v + w),$$

which under the inverse of the final vertical isomorphism, maps to $v + w$. Since the diagram commutes, dm_e maps $(v, w) \mapsto v + w$. Second, given $\iota : G \to G$, by

Proposition 1.10, the diagram below commutes:

$$\begin{array}{ccc} T_eG & \xrightarrow{di_e} & T_eG \\ \downarrow & & \downarrow \\ G(k[\varepsilon])_e & \xrightarrow[i\circ -]{} & G(k[\varepsilon])_e \end{array}$$

Letting $v \in T_eG$, under the first isomorphism, $v \mapsto e + \varepsilon v$. Precomposing with i gives

$$i(e+\varepsilon v) = \frac{1}{e+\varepsilon v} = e - \varepsilon v + O(\varepsilon)^2 = e - \varepsilon v = e + \varepsilon(-v),$$

which under the last isomorphism maps to $-v$. Hence, di_e maps v to $-v$.

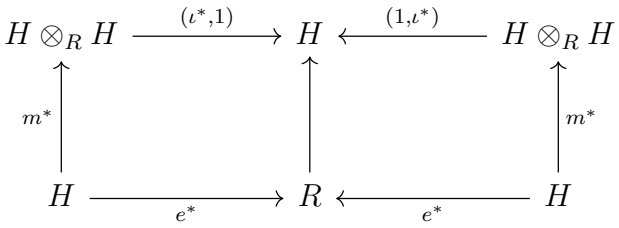
From scheme theory, we know that the two general types of schemes we care about are affine schemes and projective schemes. The remainder of this paper will deal with understanding how having the "group" condition affects the structures of affine and projective group schemes.

2. **Hopf Algebras**

So far, all examples we have encountered of group schemes have been affine. As in general scheme theory, we will define affine group schemes to be group schemes of the form Spec H, but it begs the question, since group schemes have the additional group structure on its sections, what analogous structure must H have?

Definition 2.1. Let R be a ring. A *commutative Hopf algebra over* R, or a Hopf R-algebra, is a tuple (H, m^*, e^*, ι^*) where H is an R-algebra, $m^* : H \to H \otimes_R H$ is a comultiplication map, $e^* : H \to R$ is a counit map, and $\iota^* : H \to H$ is an antipodal map such that the following diagrams commute, where $H \to R$ is the associated R-algebra structure map for H:

$$\begin{array}{ccc} H \otimes_R H \otimes_R H & \xleftarrow{1\otimes_R m^*} & H \otimes_R H \\ {\scriptstyle m^*\otimes_R 1}\uparrow & & \uparrow{\scriptstyle m^*} \\ H \otimes_R H & \xleftarrow[m^*]{} & H \end{array} \qquad \begin{array}{ccc} H = H \otimes_R R & \xleftarrow{m^*} & H \otimes_R H \\ {\scriptstyle e^*\otimes_R 1}\uparrow & \nwarrow^{\mathrm{id}} & \uparrow{\scriptstyle m^*} \\ H & \xleftarrow[e^*\otimes_R 1]{} & H \end{array}$$



For example, $(R[x]/(x^n-1), m^*, e^*, \iota^*)$ is a Hopf R-algebra where:

$$\begin{aligned} m^* : \frac{R[x]}{(x^n-1)} &\longrightarrow \frac{R[x]}{(x^n-1)} \otimes_R \frac{R[x]}{(x^n-1)} \\ x &\longmapsto x \otimes_R x \end{aligned}$$

$$\begin{aligned} e^* : \frac{R[x]}{(x^n-1)} &\longrightarrow R \\ x &\longmapsto 1 \end{aligned}$$

$$\begin{aligned} \iota^* : \frac{R[x]}{(x^n-1)} &\longrightarrow \frac{R[x]}{(x^n-1)} \\ x &\longmapsto x^{n-1} \end{aligned}$$

Note that the definition provided for a Hopf R-algebra is dual to the definition of a group scheme given in Definition 1.1. Indeed, this correspondence is not by accident, as we will see soon. At the very least, this dual structure allows us to make the suitable definition.

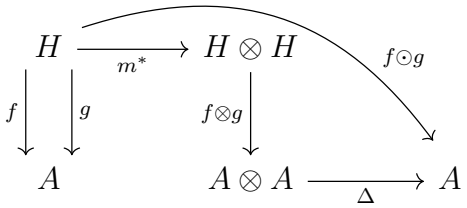
Definition 2.2. Let S be a scheme. An *affine S-group scheme* is an S-group schemes of the form Spec H where H is a commutative Hopf algebra.

2.1. **Categorical Remarks**

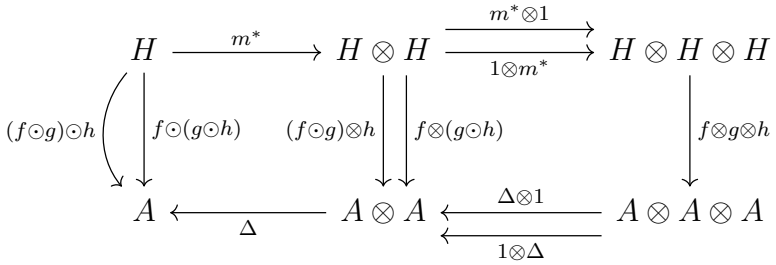
Out of the many reasons why schemes are advantageous to use, one of the crowning reasons is that there is an anti-equivalence between the category of affine schemes and the category of commutative rings [MO15, 16]. This allows us to turn questions about schemes, which are generally hard to answer, into questions about commutative rings, which we know much about. As it turns out, affine S-groups can be nicely characterized as well.

Theorem 2.3. There is a categorical anti-equivalence between the category of affine S-groups and the category of commutative quasi-coherent Hopf $\mathcal{O}_S$-algebras.

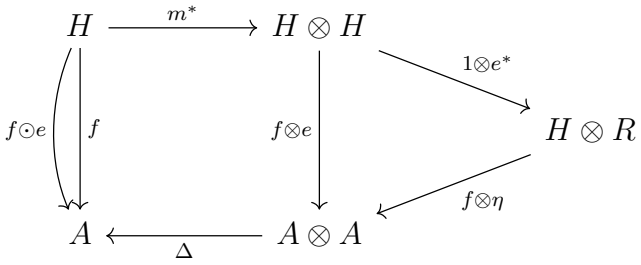
Proof. We will only show how to construct an affine S-group from a Hopf algebra in the case where $S = \operatorname{Spec} R$. Let (H, m^*, e^*, ι^*) be a Hopf algebra. Define $G = \operatorname{Spec} H$ and let A be an R-algebra. We will now check that $G(A)$ is a group, which would satisfy the definition of a group scheme from Definition 1.2. For $f, g \in G(A) = \mathtt{Sch}_R(\operatorname{Spec} A, G) = R\text{-}\mathtt{alg}(H, A)$, define $f \odot g$ as



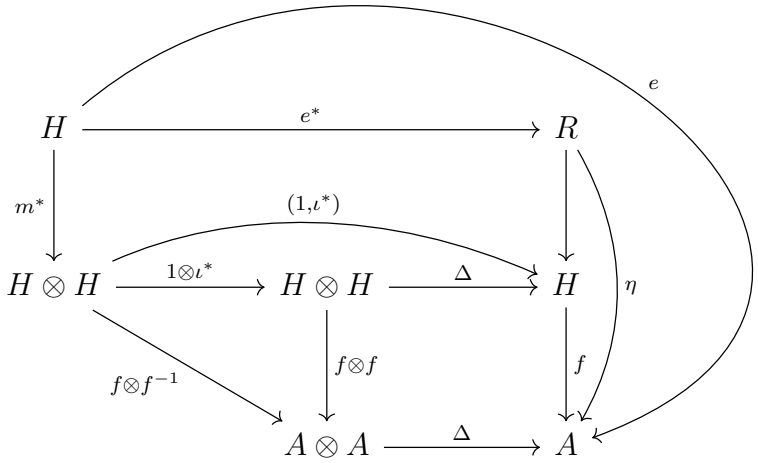
where $\Delta : a_1 \otimes_R a_2 \mapsto a_1 a_2$. That is, $f \odot g = \Delta \circ (f \otimes g) \circ m^*$. From this definition, we get associativity:



Let $e = \eta \circ e^*$ where $\eta : R \to A$ is the associated R-algebra structure map. Then we get that e is the identity on $G(A)$:



Finally, setting $f^{-1} = f \circ \iota^*$, we get that f^{-1} is the inverse of f:



Thus, $G(A)$ is a group. □

Perhaps the earlier example of noting that $R[x]/(x^n - 1)$ was a Hopf algebra looked familiar. We have already encountered its corresponding group scheme $\mu_{m,R}$, the group scheme of nth roots of unity over Spec R. For an arbitrary scheme S, the group functor $\mu_{m,S} : T \mapsto \{a \in \mathcal{O}_T(T) : a^n = 1\}$ is an affine group scheme corresponding to the Hopf $\mathcal{O}_S$-algebra $\mathcal{O}_S[x]/(x^n - 1)$.

We briefly introduce an attribute of Hopf algebras that will lead us into an important type of Hopf algebras.

Definition 2.4. A Hopf R-algebra (H, m^*, e^*, ι^*) is called *cocommutative* if there exists a map $s : H \otimes_R H \to H \otimes_R H$ such that $m^* = s \circ m^*$. Such s is called a *twist map*.

As an example, consider the Hopf R-algebra $(R[x], m^*, e^*, \iota^*)$, where in particular $m^* : R[x] \to R[y] \otimes R[z] \cong R[y, z]$ sends $x \mapsto y + z$. Letting $s : R[y, z] \to R[y, z]$ take $y \mapsto z$ and $z \mapsto y$, we see that

$$(s \circ m^*)(x) = s(y + z) = z + y = y + z = m^*(x),$$

so s is a twist map. Hence, $R[x]$ is a cocommutative Hopf algebra.

Similarly, focusing specifically on cocommuatitive Hopf algebras, we get another categorical antiequivalence as in Theorem 2.3.

Theorem 2.5. For a fixed scheme S, there is a categorical anti-equivalence between the category of commutative affine S-group schemes and commutative cocommutative quasi-coherent Hopf $\mathcal{O}_S$-algebras.

Perhaps unsurprisingly, according to Theorem 2.5, $R[x]$ corresponds to $\mathbb{G}_{a,R}$. As another example, $\mu_{m,S}$ is indeed a commutative affine group scheme, and the corresponding Hopf $\mathcal{O}_S$-algebra $\mathcal{O}_S[x](x^n - 1)$ is cocommutative.

2.2. **Cartier Duality**

As a final note on affine group schemes, we will briefly discuss a natural duality that arises in the study of group schemes.

Consider $G = \operatorname{Spec} A$, a commutative finite locally-free group scheme over a commutative ring k with unity. For $G_R := G \times_{\operatorname{Spec} k} \operatorname{Spec} R$, define the following group functor:

$$\begin{aligned} \hat{G} : k\texttt{-alg} &\longrightarrow \texttt{Gp} \\ R &\longmapsto \operatorname{Hom}_{R-\texttt{Gp}}(G_R, \mathbb{G}_{m,R}) \\ (R_1 \to R_2) &\longmapsto (\hat{G}(R_1) \to \hat{G}(R_2)) \end{aligned}$$

Theorem 2.6 (Cartier Duality)**.** Let G and G_R be as above.

(i) Then $\hat{G}$ is represented by a commutative finite locally-free k-group scheme $\operatorname{Spec} A'$, with
$$A' := \operatorname{Hom}_{k\texttt{-mod}}(A, k)$$
endowed with a commutative co-commutative Hopf algebra structure over k.

(ii) There is a canonical isomorphism between G and $\hat{\hat{G}}$.

Proof. A proof can be found in [MO15, 271]. □

We call $\hat{G}$ the *Cartier dual* of G. This duality result is quite interesting, particularly because of how straightforward the duality is. In the most basic duality theory, we have that the dual vector space consists of morphisms from a vector space to the field the vector space is defined over. In the case of the Cartier dual where k is a field, we have that it consists of applying the Spec functor to a dual vector space. So, the theory of Cartier duals is only slightly more complicated than the theory of duality from linear algebra.

3. Abelian k-Varieties

Finally, having dealt with affine group schemes, we conclude with a discussion on projective group schemes, which are often of importance in research in modern algebraic geometry. In particular, we will discuss abelian k-varieties. We provide a definition below.

Definition 3.1. An *abelian variety over a field* k, or *abelian* k*-variety*, is a connected, proper, smooth group scheme over k.

As an example, elliptic curves, or smooth curves of degree 3 in $\mathbb{P}^2_{\mathbb{C}}$, are abelian k-varieties for $k = \mathbb{C}$.

Proposition 3.2. Every abelian k-variety is projective.

Proof. A proof for this proposition can be found in [VDGM, 25]. The idea for the proof is that given an abelian k-variety, one can construct a very ample divisor giving a closed embedding into projective space. □

Additionally, we may form the category of abelian k-varieties, whose morphisms consist of morphisms of k-groups. In particular, the category of abelian k-varieties is a full subcategory of the category of k-groups.

We can understand further what abelian k-varieties are by connecting them directly to a particular scheme, whose definition is given below [MO15, 277].

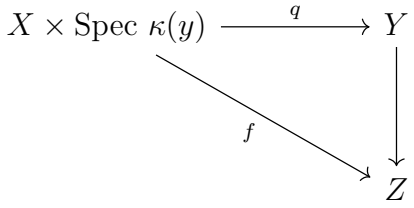
Definition 3.3. Let S be a scheme. An *abelian* S*-scheme* is an S-group that is smooth and proper with connected geometric fibers.

Alternatively, an abelian k-variety is an abelian S-scheme such that $S = \operatorname{Spec} k$ for a field k [MO15, 277]. These abelian S-schemes have a special relationship to abelian k-varieties. That is, abelian S-schemes parametrize abelian k-varieties in the following way: Let $\pi : X \to S$ be an abelian S-scheme. Then, for any $s \in S$, the fiber $\pi^{-1}(s) \cong X \times_S \operatorname{Spec} \kappa(s)$, where $\kappa(s)$ denotes the residue field of s. So, $\pi^{-1}(s)$ is an abelian $\kappa(s)$-variety.

So far, we have described abelian k-varieties as *abelian*, which is strange given that projective schemes do not have to be "abelian" in any sense. We will show that abelian k-varieties are indeed commutative. To prove it, we use a technical lemma that is often useful when working with abelian k-varieties.

Lemma 3.4 (Rigidity Lemma)**.** For a field k, let X be a geometrically reduced and geometrically connected proper k-scheme, let Y be an integral k-scheme, and let Z be a separated k-scheme. Let $f : X \times Y \to Z$ be a morphism with the property that

for some $y \in Y(k)$, $f|_{X \times \text{Spec } \kappa(y)}$ factors through a k-valued point $z \in Z(k)$. Then the following diagram commutes, where $q : X \times Y \to Y$ is the projection morphism:



Proof. A proof can be found in [GW20, 539]. □

Theorem 3.5. Let A and B be abelian k-varieties, with unit sections e_A and e_B respectively.

(a) Let $f : (A, e_A) \to (B, e_B)$ be a pointed k-morphism. Then f is a morphism of k-groups.

(b) A is a commutative k-group scheme.

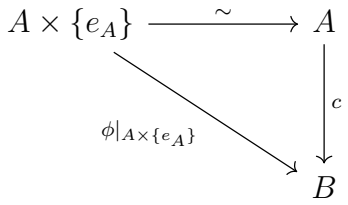
Proof. (a) Let f be as above. Let $\phi : A \times A \to B$ be defined taking

$$\phi(a_1, a_2) = f(a_1)f(a_2)f(a_1a_2)^{-1}.$$

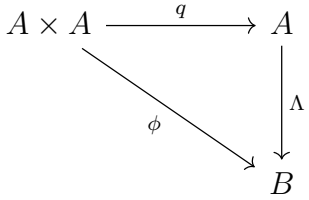
Since f is a pointed k-morphism, then $f(e_A) = e_B$, so

$$\phi(e_A, a) = f(a)f(a)^{-1} = e_B.$$

Thus, $\phi(A \times \{e_A\}) = \{e_B\}$, meaning that the following diagram commutes, for $c : A \to B$ being the constant map taking $a \mapsto e_B$:



Let $q : A \times A \to A$ be the projection $(a_1, a_2) \mapsto a_2$. By Lemma 3.4, we have that there is a map $\Lambda : A \to B$ such that the following diagram commutes:



In particular, $\Lambda(a_2) = (\Lambda \circ q)(e_A, a_2) = \phi(e_A, a_2) = e_B$. In fact, $\phi(a_1, a_2) = \Lambda(a_2) = e_B$, so for all $(a_1, a_2) \in A \times A$,

$$f(a_1)f(a_2) = f(a_1a_2),$$

and thus f is a homomorphism of k-groups.

(b) Since multiplication $m : (A \times A, e_A \times e_A) \to (A, e_A)$ is a pointed k-morphism, then by (a) it is a morphism of k-groups. Thus,

$$m(a_1, a_2) = m((e_A, a_2), (a_1, e_A)) = m(e_A, a_2)\ m(a_1, e_A),$$

and so A is commutative. □

3.1. **An Extreme Theorem**

We have seen in Section 2 that for the most part, affine group schemes behave as we would expect. Interestingly, abelian k-varieties act very differently. In this section, we give a proof for a rather extreme theorem. First, we give a crucial definition.

Definition 3.6. Let A be an abelian k-variety. Let $m : A \times A \to A$ be the group law and $p_1, p_2 : A \times A \to A$ be the projections onto the first and second factors, respectively. The *dual abelian k-variety* is

$$A^t := \mathrm{Pic}^0 A,$$

where $\mathrm{Pic}^0 A = \{\mathcal{L} \in \mathrm{Pic}\ A : m^*\mathcal{L} \cong p_1^*\mathcal{L} \otimes p_2^*\mathcal{L}\}$.

We can now prove the extreme theorem. Note that the extremeness comes from the fact that the statement is true for *all* $i \geq 0$.

Theorem 3.7. Let A be an abelian k-variety. Let $\mathcal{L} \in A^t$. If $\mathcal{L}$ is non-trivial, i.e., $\mathcal{L} \ncong \mathcal{O}$, then

$$H^i(A, \mathcal{L}) = 0$$

for all $i \geq 0$, where $H^i(A, \mathcal{L})$ denotes the ith cohomology group of $\mathcal{L}$ over A.

To make the proof easier, we will first prove the following lemma.

Lemma 3.8. Let $\mathcal{L}$ be a line bundle on a proper integral k-scheme X. Then $\mathcal{L}$ is trivial if and only if $H^0(X, \mathcal{L}) \neq 0$ and $H^0(X, \mathcal{L}^{-1}) \neq 0$.

Proof. Since X is proper and integral, $H^0(X, \mathcal{O})$ is a finite field extension of k; in particular, $H^0(X, \mathcal{O}) \neq 0$. If $\mathcal{L}$ is trivial, then

$$H^0(X, \mathcal{L}) \cong H^0(X, \mathcal{L}^{-1}) \cong H^0(X, \mathcal{O}) \neq 0$$

Conversely, suppose there are nonzero sections $s \in \Gamma(X, \mathcal{L})$ and $t \in \Gamma(X, \mathcal{L}^{-1})$. We may view s and t as nonzero maps of $\mathcal{O}$-modules $s : \mathcal{O} \to \mathcal{L}$ and $t : \mathcal{L} \to \mathcal{O}$. As X is integral, s and t are injective, so the composition

$$\mathcal{O} \xrightarrow{\ s\ } \mathcal{L} \xrightarrow{\ t\ } \mathcal{O}, \qquad t \circ s : \mathcal{O} \to \mathcal{O}$$

is injective. Now $t \circ s$ is uniquely determined by a global section $u \in H^0(X, \mathcal{O})$ such that the k-linear operator $H^0(X, \mathcal{O}) \xrightarrow{u} H^0(X, \mathcal{O})$ is injective. Injective linear operators on finite dimensional vector spaces are surjective, so u is a unit of $H^0(X, \mathcal{O})$. Hence, $t \circ s$ is an isomorphism. This implies that t is surjective. We already determined that t is injective, so t is an isomorphism. □

We now proceed with the proof of Theorem 3.7.

Proof of Theorem 3.7. Let A be an abelian k-variety. Suppose $\mathcal{L}$ is a non-trivial line bundle on A. Since an abelian k-variety is a proper integral k-scheme, then by Lemma 3.8, it follows that $H^0(A, \mathcal{L}) = 0$. Suppose there is a smallest n such that $H^n(A, \mathcal{L}) \neq 0$. Since A is a group scheme, consider the associated multiplication map $m : A \times A \to A$ and let $\mathcal{L} \boxtimes \mathcal{L} := p_1^*\mathcal{L} \otimes p_2^*\mathcal{L}$. Then $m^*\mathcal{L} = \mathcal{L} \boxtimes \mathcal{L}$. In particular, $m^* : H^n(A, \mathcal{L}) \to H^n(A \times A, \mathcal{L} \boxtimes \mathcal{L})$, which is injective because $m \circ (\mathrm{id}, e) = \mathrm{id}$ implies that $(\mathrm{id}, e)^* \circ m^* = \mathrm{id}$. But by the Künneth isomorphism,

$$H^n(A \times A, \mathcal{L} \boxtimes \mathcal{L}) \cong \bigoplus_{i+j=n} (H^i(A, \mathcal{L}) \otimes H^j(A, \mathcal{L})) = 0$$

since, by assumption, $H^0(A, \mathcal{L}), \ldots, H^{n-1}(A, \mathcal{L}) = 0$. So, $\ker m^* = H^n(A \times A, \mathcal{L} \boxtimes \mathcal{L}) \neq 0$, contradicting that m^* is injective. Thus, $H^i(A, \mathcal{L}) = 0$ for all $i \geq 0$. □

3.2. **Isogenies and a Decomposition Theorem**

To finish this section on projective group schemes, we will discuss isogenies of abelian k-varieties, which form an equivalence relation on abelian k-varieties [VDGM, 75], and, as an application, an important decomposition theorem. We give the definition of an isogeny below.

Definition 3.9. Let X, Y be abelian k-varieties and let $f : X \to Y$ be a morphism of k-groups. We say f is an *isogeny* if f is finite flat and surjective. We say X and Y are *isogeneous* if such f exists.

This definition, although quite algebraic, sheds little insight into what an isogeny is. We will see that isogenies are directly tied to kernels of k-morphisms, which we discussed briefly in Section 1.1.

Proposition 3.10. Let X, Y be abelian k-varieties and let $f : X \to Y$ be a morphism of k-groups. Then the following are equivalent:

(a) f is surjective and $\dim X = \dim Y$.

(b) $\operatorname{Ker} f$ is a finite group scheme and $\dim X = \dim Y$.

(c) f is an isogeny.

Proof. A proof can be found in [VDGM, 72]. □

In fact, Proposition 3.10 gives us an analogous first isomorphism theorem as in group theory, i.e.,

$$\frac{X}{\operatorname{Ker} f} \cong Y$$

for $f : X \to Y$ an isogeny. Additionally, by Proposition 3.10, we have that every finite subgroup scheme is of the form $\operatorname{Ker} f$ for an isogeny f. In particular, since by Theorem 3.5 every abelian k-variety is commutative, then every subgroup scheme is normal, and every finite normal subgroup scheme is of the form $\operatorname{Ker} f$ for an isogeny f.

Definition 3.11. Let $f : X \to Y$ be an isogeny for X, Y abelian k-varieties. The *degree* of the isogeny f is $\deg(f^* : k(Y) \hookrightarrow k(X))$, where $k(X)$ and $k(Y)$ denote field extensions of k.

Indeed, such definition is well-defined because f^* is a finite extension. In fact, for an isogeny f, $\deg f$ is equal to the order of $\operatorname{Ker} f$.

The following theorem gives us an example of an isogeny and its degree.

Theorem 3.12. Let $n \in \mathbb{Z}$ be non-zero and let A be an abelian k-variety. Then the morphism $[n]_A : A \to A$ taking $a \mapsto na$ is an isogeny. In particular, if $g = \dim A$, then $\deg [n]_A = n^{2g}$.

Proof. A proof for this theorem can be found in [VDGM, 74], which makes use of divisor theory. □

Isogenies, besides giving an equivalence relation on abelian k-varieties, are important because they allows us to decompose abelian k-varieties. As a final application of isogenies, we will prove such a decomposition theorem, which will follow from the following fundamental theorem. Note that given an abelian k-variety A, an *abelian k-subvariety* of A is a subgroup scheme of A that is also an abelian k-variety.

Theorem 3.13 (Poincaré Splitting Theorem)**.** Let A be an abelian k-variety and let B be an abelian k-subvariety of A. Then there exists an abelian k-subvariety C of A such that the homomorphism $f : B \times C \to A$ defined by $f(b, c) = b + c$ is an isogeny.

Proof. A proof for this theorem is given in [VDGM, 180]. □

Before stating the decomposition theorem, we need to give some definitions [VDGM, 181].

Definition 3.14. Let A be a non-zero abelian k-variety.

(a) A is *simple* if A has no non-trivial abelian k-subvarieties, i.e., all abelian k-subvarieties are 0 and A.

(b) A is *elementary* if there exists a simple abelian k-variety B, $m \geq 1$, and an isogeny $f : A \to B^m$.

Theorem 3.15 (Decomposition Theorem)**.** Let A be a non-zero abelian k-variety. Then there exist simple non-isogeneous abelian k-varieties $B_1, \ldots, B_n$ and positive integers $m_1, \ldots, m_n$ such that A is isogeneous to $B_1^{m_1} \times \cdots \times B_n^{m_n}$. Additionally, such B_i are unique up to permutation and such m_i are unique.

Proof. We show the existence part of the result by induction on the dimension of A. If $\dim A = 1$ then A is simple and we are done. Suppose for all abelian k-varieties with dimension less than A that the result holds. If A is elementary then we are done. If instead A is not simple (and hence not elementary), then by Theorem 3.13, for a non-trivial abelian k-subvariety C_1 of A, there exists an abelian k-subvariety C_2 of A such that $C_1 \times C_2$ is isogeneous to A. Since C_1 is non-trivial, then $\dim C_1 < \dim A$ and so $\dim C_2 < \dim A$. By the inductive hypothesis, C_1 and C_2 are isogeneous to decompositions $D_1^{d_1} \times \cdots \times D_\ell^{d_\ell}$ and $E_1^{e_1} \times \cdots \times E_q^{e_q}$ where each D_i and each E_i are simple abelian k-varieties and non-isogeneous. Since A is isogeneous to $C_1 \times C_2$, then by isogeneity being an equivalence relation, A is isogeneous to

$$D_1^{d_1} \times \cdots \times D_\ell^{d_\ell} \times E_1^{e_1} \times \cdots \times E_q^{e_q}.$$

After combining isogeneous simple factors and relabeling, we have that A is isogeneous to

$$B_1^{m_1} \times \cdots \times B_n^{m_n}$$

for non-isogeneous simple abelian k-varieties B_i and positive integers m_i.

To see uniqueness, suppose A is isogeneous to both $B_1^{m_1} \times \cdots \times B_n^{m_n}$ and $\tilde{B}_1^{\tilde{m}_1} \times \cdots \times \tilde{B}_r^{\tilde{m}_r}$. Then there exists an isogeny

$$f : B_1^{m_1} \times \cdots \times B_n^{m_n} \to \tilde{B}_1^{\tilde{m}_1} \times \cdots \times \tilde{B}_r^{\tilde{m}_r}.$$

Each B_i embeds as a subvariety of $B_1^{m_1} \times \cdots \times B_n^{m_n}$, whose image in $\tilde{B}_1^{\tilde{m}_1} \times \cdots \times \tilde{B}_r^{\tilde{m}_r}$ is nonzero. Indeed, $\ker f$ is zero dimensional and B_i is positive dimensional, so B_i is not contained in kernel of f. Hence, there exists a $j \in \{1, \ldots, r\}$ such that the map $B_i \to \tilde{B}_j$ induced by f (followed by a projection onto a coordinate factor of $\tilde{B}_j^{\tilde{m}_j}$) is nonzero. Therefore, B_i is isogeneous to $\tilde{B}_j$. Note that B_i is not isogenous to no other $\tilde{B}_\ell$. Furthermore, $n = r$.

Without loss of generality, we assume B_i is isogeneous to $\tilde{B}_i$. Then Φ is represented by a block diagonal matrix of members of $\mathrm{Hom}(B_i^{m_i}, B_i^{\tilde{m}_i})$; since f is an isogeny, so is each diagonal. Therefore, $B_i^{m_i}$ is isogeneous to $B_i^{\tilde{m}_i}$ for every i. By Proposition 3.10, $\dim B_i^{m_i} = \dim B_i^{\tilde{m}_i}$, so $m_i = \tilde{m}_i$ since $\dim B_i \neq 0$. □

4. **Acknowledgments**

I would like to thank the Joint CMU-Pitt Directed Reading Program for accepting me for Spring 2026 and allowing me to learn about group schemes. In particular, I would like to thank my mentor and friend Eugene Eyeson for his assistance in co-organizing the DRP and for his unwavering support throughout this directed reading in carefully planning weekly lectures and exercises, and in carefully discussing and reviewing my final presentation and paper.

References

[GW20] Ulrich Görtz and Torsten Wedhorn. *Algebraic Geometry I: Schemes. With Examples and Exercises.* Springer Stud. Math. – Master. Wiesbaden: Springer Spektrum, 2nd edition edition, 2020.

[GW23] Ulrich Görtz and Torsten Wedhorn. *Algebraic Geometry II: Cohomology of Schemes. With Examples and Exercises.* Springer Stud. Math. – Master. Wiesbaden: Springer Spektrum, 2023.

[MO15] David Mumford and Tadao Oda. *Algebraic Geometry II*, volume 73 of *Texts Read. Math.* New Delhi: Hindustan Book Agency, 2015.

[VDGM] Gerard Van Der Geer and Ben Moonen. *ABELIAN VARIETIES (PRELIMINARY VERSION OF THE FIRST CHAPTERS).*