

# Group Schemes

**The Big Picture.** We now have two sources of Galois representations, elliptic curves and modular curves. In this chapter we describe Galois representations in terms of group schemes. This will be used to define the general class of *semistable* representations in the following chapter. Ultimately, we define finite, flat group schemes and show that they provide a quite general source of such Galois representations.

## 0.1 Affine Group Schemes

We saw in Chapter 4 that elliptic curves defined over  $\mathbb{Q}$  yield abelian groups, namely the group structure over its complex points. Now if  $E$  is an elliptic curve over  $\mathbb{Q}$  and  $A$  is a subfield of the complex numbers, not only is  $E(A)$  contained in  $E(\mathbb{C})$  but it is also a subgroup. This fact follows immediately since if two points are in  $A$  the line that passes through them has coefficients in  $A$ . Hence the third intercept of the line with the curve has coordinates in  $A$ .

*Example:* Let  $E : y^2 = x^3 - 1$  and  $P = (1, 0), Q = (0, i)$  be elements of  $E(\mathbb{Q}(i))$ . The line going through  $P$  and  $Q$  is given by  $l : y = -ix + i$ . Since the other intercept of  $l$  with  $E$  is  $R = (-2, 2i + i)$  we have that  $P + Q = -R = (-2, -2i - i) \in E(\mathbb{Q}(i))$ .

Note that the above procedure is not only valid for  $\mathbb{Q}$ -algebras  $A$  lying inside  $\mathbb{C}$  but for any  $\mathbb{Q}$ -algebra  $A$ . If we follow the recipe for addition of a complex elliptic curve, we can write formal identities for the addition of two points for any elliptic curve over  $\mathbb{Q}$ . These formulas are rational functions in the original coordinates. Therefore given an elliptic curve  $E$  over  $\mathbb{Q}$ , we obtain an abelian group  $E(A)$  for each  $\mathbb{Q}$ -algebra  $A$ . This construction of groups from  $\mathbb{Q}$ -algebras is generalized below. A good resource for this section is (Wat).

Throughout this chapter, all rings will be commutative with 1 and all maps be-

tween rings shall be required to send 1 to 1.

**Definition 0.1.** Let  $R$  be a ring. A functor  $F : R_{alg} \dashrightarrow \mathbf{Sets}$ , from the category of  $R$ -algebras to the category of sets, is *representable* if there is a unique  $R$ -algebra  $\mathfrak{R}$  such that  $F(-) = \text{Hom}_{R_{alg}}(\mathfrak{R}, -)$ . We say that  $F$  is represented by  $\mathfrak{R}$ .

A representable functor from the category of  $R$ -algebras to the category of sets defines an *affine scheme* over  $R$ . If the image of the representable functor is the category of groups, then the representing ring  $\mathfrak{R}$  inherits an extra structure. We call a ring with this additional structure a *Hopf algebra*. This structure is discussed more thoroughly at the end of this section.

**Definition 0.2.** An *affine group scheme* over  $R$  is a representable functor from the category of  $R$ -algebras to the category of groups.

*Examples:* Let  $R$  be a ring, and let  $A$  be an  $R$ -algebra.

1. The group functor  $e : R_{alg} \dashrightarrow \mathbf{Grp}$  defined by sending every  $R$ -algebra to the trivial group is represented by  $R$ .
2. The group functor  $\mathbf{G}_a : R_{alg} \dashrightarrow \mathbf{Grp}$  given by  $\mathbf{G}_a(A) = A^+$  (the additive group of  $A$ ) is an affine group scheme over  $R$ . Indeed, an  $R$ -algebra homomorphism from  $R[T]$  to  $A$  is determined by the image of  $T$ , and it can be sent to any element of  $A$ . Thus,  $\mathbf{G}_a$  is represented by  $R[T]$ ;  $\mathbf{G}_a(A) = \text{Hom}_{R_{alg}}(R[T], A)$ .
3. The group functor  $\mathbf{G}_m$  given by  $\mathbf{G}_m(A) = A^\times$  (the units of  $A$ ) is an affine group scheme over  $R$ . The representing ring is  $R[X, Y]/(XY - 1)$ . Indeed, we see that an  $R$ -algebra homomorphism can send  $X$  to any invertible element in  $A$ , and  $Y$  must then map to its inverse.
4. Similarly, the group functor  $GL_n$  is an affine group scheme over  $R$ . It is representable since

$$GL_n(A) = \text{Hom}_{R_{alg}}(R[T_{11}, T_{12}, \dots, T_{n(n-1)}, T_{nn}, Y]/(\det(T_{ij})Y - 1), A).$$

Note that  $GL_1 = \mathbf{G}_m$ .

5. The group functor  $\mu_n$  defined by  $\mu_n(A) := \{x \in A \mid x^n = 1\}$  is an affine group scheme represented by  $R[T]/(T^n - 1)$ .

**Definition 0.3.** Let  $G$  and  $H$  be affine group schemes over  $R$ . A *homomorphism of affine group schemes* over  $R$  from  $G$  to  $H$  associates to each  $R$ -algebra  $A$  a group homomorphism  $\mathcal{F}(A) : G(A) \rightarrow H(A)$ , such that whenever  $\phi : A \rightarrow B$  is a homomorphism of  $R$ -algebras, the following diagram commutes:

$$\begin{array}{ccc} G(A) & \xrightarrow{\mathcal{F}(A)} & H(A) \\ G(\phi) \downarrow & & \downarrow H(\phi) \\ G(B) & \xrightarrow{\mathcal{F}(B)} & H(B) \end{array}$$

*Remark.* In the language of categories, a homomorphism of affine group schemes is a natural map from  $G$  to  $H$ .

*Examples:*

1. The determinant map gives a homomorphism of affine groups schemes over  $R$  from  $GL_n$  to  $\mathbf{G}_m$ .
2. The natural map from  $\mathbf{G}_m$  to  $\mathbf{G}_m$  given by  $x \mapsto x^n$  is a homomorphism.

An affine group scheme homomorphism relates two representable functors. Given such a map, can we find any relation between the representing algebras? Conversely, given a relation between two  $R$ -algebras is there any connection between the functors that they represent? The next example partially answers the second question, at least in the case of the determinant map from  $GL_n$  to  $\mathbf{G}_m$ .

*Example:* Consider the  $R$ -algebra homomorphism

$$\begin{aligned} \alpha : R[X, Y]/(XY - 1) &\rightarrow R[T_{11}, \dots, T_{nn}, Y]/(\det(T_{ij})Y - 1) \\ X &\mapsto \det(T_{ij}) \\ Y &\mapsto Y. \end{aligned}$$

Then the affine group scheme homomorphism  $\tilde{\alpha} : GL_n \rightarrow GL_1$

$$\begin{aligned} \tilde{\alpha}(A) : GL_n(A) &\rightarrow GL_1(A) \\ \beta &\mapsto \beta \circ \alpha \end{aligned}$$

is the determinant map.

The next result, known as Yoneda's lemma, will help us to study the natural maps between affine schemes. One a priori disadvantage of natural maps, is that we have to deal with a family of maps, one for each  $R$ -algebra. With Yoneda's lemma we avoid this by just focusing our attention on the representing algebras.

**Theorem 0.4.** *Let  $G : R_{alg} \dashrightarrow \text{Sets}$  and  $H : R_{alg} \dashrightarrow \text{Sets}$  be functors represented by the  $R$ -algebras  $\mathfrak{R}$  and  $\mathcal{S}$ , respectively. Then the natural maps  $G \rightarrow H$  correspond to  $R$ -algebra homomorphisms  $\mathcal{S} \rightarrow \mathfrak{R}$ .*

*Proof.* Let  $\alpha \in \text{Hom}_{R_{alg}}(\mathcal{S}, \mathfrak{R})$ . For any  $R$ -algebra  $A$ , composition with  $\alpha$  defines a map between  $\text{Hom}_{R_{alg}}(\mathfrak{R}, A)$  and  $\text{Hom}_{R_{alg}}(\mathcal{S}, A)$ .

$$\begin{aligned} \mathcal{F}_\alpha(A) : G(A) &\rightarrow H(A) \\ \beta &\mapsto \beta \circ \alpha \end{aligned}$$

If  $B$  is any other  $R$ -algebra and  $\phi \in \text{Hom}_{R_{alg}}(A, B)$  we have, by functoriality of  $G$  and  $H$ , maps  $G(\phi) : G(A) \rightarrow G(B)$  and  $H(\phi) : H(A) \rightarrow H(B)$ . Explicitly they are just left composition with  $\phi$ . Putting all this together we see that the following diagram commutes.

$$\begin{array}{ccc} G(A) & \xrightarrow{\mathcal{F}_\alpha(A)} & H(A) \\ G(\phi) \downarrow & & \downarrow H(\phi) \\ G(B) & \xrightarrow{\mathcal{F}_\alpha(B)} & H(B) \end{array}$$

Conversely, a natural map  $\mathcal{F}$  from  $G$  to  $H$  gives a map

$$\mathcal{F}(\mathfrak{R}) : \text{Hom}_{R_{alg}}(\mathfrak{R}, \mathfrak{R}) \rightarrow \text{Hom}_{R_{alg}}(\mathcal{S}, \mathfrak{R}).$$

Let  $\alpha := \mathcal{F}(\mathfrak{R})(1_{\mathfrak{R}})$ , and  $\phi \in \text{Hom}_{R_{alg}}(\mathfrak{R}, A)$ . By the definition of natural map,  $\phi \circ \mathcal{F}(\mathfrak{R})(\gamma) = \mathcal{F}(A)(\phi \circ \gamma)$  for all  $\gamma \in G(\mathfrak{R})$ . Taking  $\gamma = 1_{\mathfrak{R}}$ ,  $\phi \circ \alpha = \mathcal{F}(A)(\phi \circ (1_{\mathfrak{R}})) = \mathcal{F}(A)(\phi)$ . In other words  $\mathcal{F}(A) = \mathcal{F}_\alpha(A)$ , thus every natural map comes from a unique  $\alpha : \mathcal{S} \rightarrow \mathfrak{R}$ .  $\square$

*Remark.* Note that if  $G$  and  $H$  are affine group schemes represented by  $\mathfrak{R}$  and  $\mathcal{S}$  respectively, then the existence of a morphism between their corresponding algebras does not imply that there is a homomorphism of group schemes  $G \rightarrow H$ . (see Exercise 0.3 for an example.)

Given an affine group scheme  $G$  over a ring  $R$ , it is often desirable to consider  $G$  over a different ring. If there is a ring homomorphism  $\phi : R \rightarrow R'$ , then we can consider  $G$  as a functor  $G' : R'_{alg} \dashrightarrow Grp$ . Indeed, if  $A$  is an  $R'$ -algebra, then by composing with  $\phi$ ,  $A$  is an  $R$ -algebra. Also, it is clear that if  $\alpha \in \text{Hom}_{R'_{alg}}(A, B)$ , then  $\alpha \in \text{Hom}_{R_{alg}}(A, B)$ . In fact, this homomorphism makes  $G$  into an affine group scheme over  $R'$ , and there is an explicit description of its representing ring which we describe next.

Given a ring homomorphism  $R \rightarrow R'$  and an  $R$ -algebra  $A$ , consider the collection  $\mathfrak{T} = \{(B, \phi)\}$  of rings  $B$  and homomorphisms  $\phi : A \rightarrow B$  that make the following diagram commute:

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \uparrow & & \uparrow \\ R & \longrightarrow & R' \end{array} \quad (1)$$

A morphism between two objects  $(B_1, \phi_1)$  and  $(B, \phi)$  of  $\mathfrak{T}$  consists of a ring homomorphism  $\alpha : B_1 \rightarrow B$  such that the following diagram commutes

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \phi_1 \downarrow & \nearrow \alpha & \uparrow \\ B_1 & \longleftarrow & R' \end{array} \quad (2)$$

It can be shown that this collection forms the objects in a category of  $R'$ -algebras, with an initial object,  $A \otimes_R R'$ , called the *tensor product* of  $A$  and  $R'$  (see (Mat) and Exercise 0.2). By the definition of initial object, there is an isomorphism  $\text{Hom}_{R'_{alg}}(A, B) \cong \text{Hom}_{R'_{alg}}(A \otimes_R R', B)$ .

*Example:*  $\text{Hom}_{\mathbb{R}}(\mathbb{R}[x]/\langle x^2 - 1 \rangle, \mathbb{C}) \cong \text{Hom}_{\mathbb{C}}(\mathbb{C}[x]/\langle x^2 - 1 \rangle, \mathbb{C})$  can be deduced from  $\mathbb{C}[x]/\langle x^2 - 1 \rangle \cong \mathbb{R}[x]/\langle x^2 - 1 \rangle \otimes_{\mathbb{R}} \mathbb{C}$ . On the other hand any element in  $\text{Hom}_{\mathbb{R}}(\mathbb{R} \times \mathbb{R}, \mathbb{C})$ , or  $\text{Hom}_{\mathbb{C}}(\mathbb{C} \times \mathbb{C}, \mathbb{C})$  is totally determined by its value at  $(1, 0)$ , it is 0 or 1. This induces an isomorphism between them, thus

$$\text{Hom}_{\mathbb{R}}(\mathbb{R}[x]/\langle x^2 - 1 \rangle, \mathbb{C}) \cong \text{Hom}_{\mathbb{R}}(\mathbb{R} \times \mathbb{R}, \mathbb{C}) \cong \text{Hom}_{\mathbb{C}}(\mathbb{C} \times \mathbb{C}, \mathbb{C}) \cong \text{Hom}_{\mathbb{C}}(\mathbb{C}[x]/\langle x^2 - 1 \rangle, \mathbb{C})$$

If  $G$  is represented by the  $R$ -algebra  $\mathfrak{R}$ , then  $G'$  is represented by the  $R'$ -algebra  $\mathfrak{R} \otimes_R R'$ . This process is called *base change*. Often the maps  $R \rightarrow R'$  we are interested in will be when  $R'$  is a fraction field or residue field of  $R$ . For instance, we call the result of base change from  $\mathbb{Z}_p$  to  $\mathbb{Q}_p$  (respectively  $\mathbb{F}_p$ ) the *generic fiber*

(respectively the *closed fiber*).

*Example:* Let  $A = \mathbb{Z}_3[x, y]/\langle y^2 - (x^3 - 1) \rangle$ . Then  $A$  is  $\mathbb{Z}_3$ -algebra with generic fiber isomorphic to  $A_g = \mathbb{Q}_3[x, y]/\langle y^2 - (x^3 - 1) \rangle$  and closed fiber isomorphic to  $A_c = \mathbb{F}_3[x, y]/\langle y^2 - (x^3 - 1) \rangle \cong \mathbb{F}_3[x, y]/\langle y^2 - x^3 \rangle$ .

*Remark.* It can be proved that  $A_g$  is a Dedekind domain. On the other hand since  $y/x$  is an integral element not belonging to  $A_c$ , this last is not Dedekind. This algebraic fact has a geometric meaning:  $y^2 - (x^3 - 1)$  is an elliptic curve over  $\mathbb{Q}_3$  but not over  $\mathbb{F}_3$ .

**Lemma 0.5.** *Let  $G$  and  $H$  be affine group schemes represented by the  $R$ -algebras  $\mathfrak{R}$  and  $\mathcal{S}$  respectively. The functor  $F(-) := G(-) \times H(-)$  is an affine group scheme represented by the  $R$ -algebra  $\mathfrak{R} \otimes_R \mathcal{S}$ .*

*Proof.* Let  $A$  be a  $R$ -algebra. The result follows immediately from

$$\mathrm{Hom}_{R_{alg}}(\mathfrak{R}, A) \times \mathrm{Hom}_{R_{alg}}(\mathcal{S}, A) \cong \mathrm{Hom}_{R_{alg}}(\mathfrak{R} \otimes_R \mathcal{S}, A).$$

□

Let  $G$  be an affine group scheme over  $R$  represented by  $\mathfrak{R}$ . Suppose  $A \rightarrow B$  is a homomorphism of  $R$  algebras. Let  $inv(A)$  and  $inv(B)$  be the inverses operations on  $G(A)$  and  $G(B)$ . Since the induced map  $G(A) \rightarrow G(B)$  is a group homomorphism the following diagram is commutative.

$$\begin{array}{ccc} G(A) & \xrightarrow{inv(A)} & G(A) \\ \downarrow & & \downarrow \\ G(B) & \xrightarrow{inv(B)} & G(B) \end{array}$$

In other words the map between functors,  $inv : G \rightarrow G$ , given by  $inv(A) : G(A) \rightarrow G(A)$  is a natural map. Similarly, the maps  $m : G \times G \rightarrow G$ , given by multiplication, and  $unit : e \rightarrow G$  given by the identity are natural maps.

Let  $G$  be an affine group scheme over  $R$  represented by  $\mathfrak{R}$ . By Lemma 0.5,  $G \times G$  is represented by  $\mathfrak{R} \otimes_R \mathfrak{R}$ . Thus, by Yoneda's lemma, we know that the maps  $m$ ,  $unit$ , and  $inv$  correspond to  $R$ -algebra homomorphisms, as denoted below.

$$\Delta : \mathfrak{R} \rightarrow \mathfrak{R} \otimes_R \mathfrak{R}, \text{ comultiplication}$$

$\epsilon : \mathfrak{R} \rightarrow R$ , counit or augmentation

$S : \mathfrak{R} \rightarrow \mathfrak{R}$ , coinverse or antipode

Since the following diagrams are commutative,

$$\begin{array}{ccc}
 G \times G \times G & \xrightarrow{id \times m} & G \times G \\
 \downarrow m \times id & & \downarrow m \\
 G \times G & \xrightarrow{m} & G
 \end{array}
 \quad
 \begin{array}{ccc}
 G & \xrightarrow{(inv, id)} & G \times G \\
 \downarrow & & \downarrow m \\
 \{e\} & \xrightarrow{unit} & G
 \end{array}
 \quad
 \begin{array}{ccc}
 \{e\} \times G & \xrightarrow{unit \times id} & G \times G \\
 \downarrow id \times unit & & \downarrow m \\
 G \times G & \xrightarrow{m} & G
 \end{array}$$

we have that their counterparts satisfy the following commutative diagrams.

$$\begin{array}{ccc}
 \mathfrak{R} \otimes \mathfrak{R} \otimes \mathfrak{R} & \xleftarrow{id \otimes \Delta} & \mathfrak{R} \otimes \mathfrak{R} \\
 \Delta \otimes id \uparrow & & \uparrow \Delta \\
 \mathfrak{R} \otimes \mathfrak{R} & \xleftarrow{\Delta} & \mathfrak{R}
 \end{array}
 \quad
 \begin{array}{ccc}
 \mathfrak{R} & \xleftarrow{(S, id)} & \mathfrak{R} \otimes \mathfrak{R} \\
 \uparrow & & \uparrow \Delta \\
 R & \xleftarrow{\epsilon} & \mathfrak{R}
 \end{array}
 \quad
 \begin{array}{ccc}
 R \otimes \mathfrak{R} & \xleftarrow{\epsilon \otimes id} & \mathfrak{R} \otimes \mathfrak{R} \\
 id \otimes \epsilon \uparrow & & \uparrow \Delta \\
 \mathfrak{R} \otimes \mathfrak{R} & \xleftarrow{\Delta} & \mathfrak{R}
 \end{array}$$

**Definition 0.6.** An  $R$ -algebra,  $\mathfrak{R}$ , with morphisms  $\Delta$ ,  $\epsilon$ , and  $S$  satisfying such commutativity is called a *Hopf Algebra*.

As we mentioned before, if  $G$  and  $H$  are affine group schemes represented by  $\mathfrak{R}$  and  $\mathfrak{S}$  respectively, then the existence of a morphism between their corresponding algebras does not imply that there is a homomorphism  $G \rightarrow H$ . However if the morphism  $\mathfrak{S} \rightarrow \mathfrak{R}$  is a *Hopf algebra homomorphism*, i.e. it preserves the Hopf algebra structures, it corresponds to a homomorphism  $G \rightarrow H$ .

## 0.2 Étale Group Schemes and Galois Representations

In this section we will show how certain affine group schemes give rise to Galois representations. A good first example is a generalization, to an arbitrary field, of the  $\ell$ -adic representation of  $G_{\mathbb{Q}}$  seen at the beginning of Chapter 4.

*Example:* Let  $K$  be a field, and let  $\ell$  be a prime  $\neq \text{char}K$ . Group schemes  $\mu_{\ell^n}$  over  $K$  produce representations as follows. Consider  $\overline{K}$  an algebraic closure of  $K$ . Since  $\ell \neq \text{char}K$ ,  $\mu_{\ell^n}(\overline{K}) \cong \mathbb{Z}/\ell^n\mathbb{Z}$ . The natural action of  $G_K$  over  $\mu_{\ell^n}(\overline{K})$  yields a

continuous homomorphism  $\chi_{\ell^n} : G_K \rightarrow \text{Aut}(\mu_{\ell^n}(\overline{K})) \cong \text{GL}_1(\mathbb{Z}/\ell^n\mathbb{Z})$ . Therefore by the universal property of inverse limits, we have a continuous representation  $\chi_{\ell^\infty} : G_K \rightarrow \text{GL}_1(\mathbb{Z}_\ell)$  called the  $\ell$ -adic cyclotomic character. As with elliptic curves, we can provide an alternative definition by doing the inverse limit before the Galois action; namely letting  $Ta_\ell(\mu) := \varprojlim \mu_{\ell^n}(\overline{K})$ . Then  $\chi_{\ell^\infty}$  gives the action of  $G_K$  on the Tate module  $Ta_\ell(\mu)$ .

We now define characteristics of group schemes that will be useful to us in later chapters.

**Definition 0.7.** An  $R$ -algebra  $A$  is called *finite* if it is finitely generated as an  $R$ -module. (Note that this is stronger than being finitely generated as an  $R$ -algebra - consider e.g.  $R[T]$ .) Let  $G$  be an affine group scheme over  $R$ . We call  $G$  a *finite group scheme* over  $R$  if its representing ring  $\mathfrak{R}$  is a finite  $R$ -algebra.

*Example:* The affine group scheme  $\mathbf{G}_m$  over  $\mathbb{Q}$  is not finite since  $\dim_{\mathbb{Q}}(\mathbb{Q}[x, x^{-1}])$  is infinite. On the other hand  $\mu_2$  over  $\mathbb{Q}$  is finite, since  $\dim_{\mathbb{Q}}(\mathbb{Q}[x]/\langle x^2 - 1 \rangle) = 2$ .

**Definition 0.8.** An  $R$ -algebra  $A$  is called *flat* if tensoring with  $A$  is an exact functor, i.e. if for any short exact sequence  $0 \rightarrow M \rightarrow N \rightarrow L \rightarrow 0$  of  $R$ -modules,  $0 \rightarrow M \otimes_R A \rightarrow N \otimes_R A \rightarrow L \otimes_R A \rightarrow 0$  is also exact. A finite group scheme over  $R$  is called *flat* if its representing ring  $A$  is a flat  $R$ -algebra.

*Example:* The group functor  $\mu_2$  over  $\mathbb{Q}$  is flat since  $\mathbb{Q}[x]/\langle x^2 - 1 \rangle \cong \mathbb{Q} \times \mathbb{Q}$  is a flat  $\mathbb{Q}$ -algebra.

Given  $R$  a domain it is easy to show that a flat  $R$ -algebra  $A$  is torsion free (see Exercise 0.6). If  $R$  is a P.I.D every finitely generated module is of the form  $R^n \oplus T$ , where  $T$  consists of torsion elements. Thus we have the following result:

**Lemma 0.9.** *Let  $R$  be a principal ideal domain and  $A$  an  $R$ -module. Then  $A$  is finite and flat over  $R$  if and only if  $A \cong R^n$ , for some non negative integer  $n$ .*

In particular any finite, flat group scheme over  $\mathbb{Z}_\ell$  is represented by a ring isomorphic, as a  $\mathbb{Z}_\ell$ -module, to  $\mathbb{Z}_\ell^n$ .

**Definition 0.10.** Let  $G$  be a finite, flat group scheme over  $\mathbb{Z}_\ell$ . The *Rank* of  $G$  is the rank of its representing ring as a  $\mathbb{Z}_\ell$ -module.

**Definition 0.11.** Let  $G$  be a finite group scheme over a field  $K$ , represented by  $\mathfrak{R}$ . We call  $G$  *étale* if  $\mathfrak{R}$  is an étale (or separable)  $K$ -algebra, i.e.  $\mathfrak{R} \otimes_K \overline{K} \cong \overline{K} \times \dots \times \overline{K}$ .

*Example:* Let  $G = \mu_\ell$ ,  $\ell$  prime. We saw that  $\mathfrak{R} = K[T]/(T^\ell - 1)$ . Then  $\mathfrak{R} \otimes_K \bar{K} = \bar{K}[T]/(T^\ell - 1)$ . If  $\text{char } K = \ell$ , then this is  $\bar{K}[T]/(T-1)^\ell$ , which contains nilpotents and so  $G$  is not étale (see exercises). If  $\text{char } K \neq \ell$ , there exists  $\zeta \in \bar{K}$  a primitive  $\ell^{\text{th}}$ -root of unity. Then by Chinese remainder theorem this is  $\prod_{i=0}^{\ell-1} \bar{K}[T]/(T-\zeta^i) \cong \bar{K} \times \dots \times \bar{K}$ , and so  $G$  is étale. Note that the  $\ell$ -adic cyclotomic character arises as an inverse limit of representations from étale group schemes.

In Chapter 4 we looked at representations  $G_{\mathbb{Q}} \rightarrow \text{Aut}(T_{a_\ell}(E))$  where  $\text{Aut}(T_{a_\ell}(E)) \cong \text{GL}_2(R)$ , and  $R$  is a local ring with finite residue field  $F$ . Taking residue classes we have a continuous action of the absolute Galois group  $G_{\mathbb{Q}}$  on a finite group, namely  $\text{GL}_2(F)$ . Therefore we are interested in actions of  $G_{\mathbb{Q}}$  on finite groups. The following theorem shows that any such representations can be realized from étale group schemes (more details can be found in (Wat)).

**Theorem 0.12.** *Let  $K$  be a field. The category of étale group schemes over  $K$  is equivalent to the category of finite groups with continuous  $G_K$ -action.*

*Proof.* Given an étale group scheme  $G$  represented by the étale  $K$ -algebra  $\mathfrak{R}$ , consider the group  $G(\bar{K}) = \text{Hom}_{K\text{-alg}}(\mathfrak{R}, \bar{K}) \cong \text{Hom}_{\bar{K}\text{-alg}}(\mathfrak{R} \otimes_K \bar{K}, \bar{K})$ . Since  $\mathfrak{R}$  is étale,  $|\text{Hom}_{K\text{-alg}}(\mathfrak{R}, \bar{K})| = |\text{Hom}_{\bar{K}\text{-alg}}(\bar{K} \times \dots \times \bar{K}, \bar{K})|$  which, by Exercise 0.10, is equal to  $\dim_{\bar{K}}(\bar{K} \times \dots \times \bar{K})$ . Thus  $G(\bar{K})$  is a finite group. Given a  $K$ -algebra homomorphism  $\mathfrak{R} \rightarrow \bar{K}$  and  $\sigma \in G_K$ , the action is given by composing to get  $\mathfrak{R} \rightarrow \bar{K} \xrightarrow{\sigma} \bar{K}$ . The images of  $\mathfrak{R}$  all lie in some finite Galois extension of  $K$  and so the action is continuous.

Conversely, given a finite group  $H$  with continuous  $G_K$ -action, consider first the case of transitive action, say  $H = G_K h$ . By continuity, there exists a finite Galois extension  $L$  of  $K$  such that the action of  $G_K$  factors through  $\text{Gal}(L/K)$ . Let  $S \subseteq \text{Gal}(L/K)$  be the stabilizer of  $h$  under  $\text{Gal}(L/K)$ , and  $\mathfrak{R} \subseteq L$  its fixed field. Since the extension  $L/K$  is Galois, all  $K$ -algebra homomorphisms  $\mathfrak{R} \rightarrow \bar{K}$  map to  $L$  and are conjugate. This yields a  $G_K$ -isomorphism  $H \rightarrow \text{Hom}_{K\text{-alg}}(\mathfrak{R}, \bar{K})$  by sending  $h$  to one of them. The desired group scheme is that with representing ring  $\mathfrak{R}$ . If the action is intransitive, we obtain for each orbit a ring  $\mathfrak{R}_i$  and then  $\prod \mathfrak{R}_i$  works.

□

### 0.3 General schemes and Elliptic curves

We now have the objects and morphisms of the category of affine group schemes over a fixed ring  $R$ . An elliptic curve  $E : y^2 = f(x)$  over  $\mathbb{Q}$  gives for each  $\mathbb{Q}$ -algebra  $A$ , a group  $E(A)$  and for each  $\mathbb{Q}$ -algebra map  $A \rightarrow B$  a group homomorphism

$E(A) \rightarrow E(B)$ . Is it an affine group scheme? Actually no. A natural guess is  $\mathfrak{R} = \mathbb{Q}[x, y]/(y^2 - f(x))$ , in which case  $\text{Hom}_{\mathbb{Q}\text{-alg}}(\mathfrak{R}, A)$  yields the points  $(x, y)$  with coordinates in  $A$  satisfying  $y^2 = f(x)$ . This, however, misses the point at  $\infty$ . In other words, it shows that  $E(-) \setminus \{\infty\}$  defines an affine scheme. A suitable way to remedy this problem is to define group schemes, or more generally schemes, as algebraic analogues of Riemann surfaces. This is done by patching together affine schemes called *charts*. For instance,  $E(A) \setminus \{\infty\}$  provides such a chart. We say more about non-affine group schemes later.

### 0.3.1 A brief introduction to Sheaves and Schemes

We next reconcile the definition of affine schemes given in 0.2 with the usual one. These small sections are not intended as a learning material in theory of schemes. Our purpose is to present the basic scheme theoretic language, with the only aim to define group schemes in this setting. We strongly recommend to the interested reader in this beautiful topic to consult (Ha).

Let  $R$  be a commutative ring with 1, and let  $\text{Spec } R$  denote the set of prime ideals of  $R$ . For example,  $\text{Spec } \mathbb{Z}_p = \{(0), p\mathbb{Z}_p\}$ . Then  $\text{Spec } R$  comes with a topology (see Exercise 0.7), the *Zariski topology*, defined by having the closed sets be the sets  $V(I)$  as  $I$  runs through all ideals of  $R$ , where

$$V(I) := \{\mathfrak{p} \in \text{Spec } R \mid I \subseteq \mathfrak{p}\}. \quad (3)$$

*Example:* The Zariski topology for  $\text{Spec}(\mathbb{Z})$  is the same as the cofinite topology. Open sets are the ones with finite complement plus the empty set.

If  $f : R \rightarrow S$  is a ring homomorphism and  $\mathfrak{p}$  is a prime ideal of  $S$ , then  $R/f^{-1}(\mathfrak{p}) \rightarrow S/\mathfrak{p}$  is an injective homomorphism into an integral domain, and so  $f^{-1}(\mathfrak{p})$  is a prime ideal of  $R$ . Thus  $f$  induces a map  $\text{Spec } S \rightarrow \text{Spec } R$  which can be checked to be continuous with respect to the Zariski topologies. For example if  $I$  is an ideal then, since the prime ideals of  $R$  containing  $I$  are in bijection with those of  $R/I$ ,  $\text{Spec } (R/I) \rightarrow \text{Spec } R$  is an injection with image  $V(I)$ . If  $x \in R$ , then likewise  $\text{Spec } R_x \rightarrow \text{Spec } R$  (from localization) is a continuous injection with image  $\text{Spec } R \setminus V((x))$ . Note that if  $x$  varies over  $R$  the open sets  $\text{Spec } R_x$  form a cover of  $\text{Spec } R$ . Each of these sets has attached a ring, namely  $R_x$ . This construction which is similar to that of manifolds and its rings of continuous, differential or holomorphic maps, can be in fact seen as a particular case of a more general notion called *sheaf*.

Let  $S$  be a topological space and  $\mathcal{C}$  be a category. Usually  $\mathcal{C}$  is the category of sets, the category of groups, the category of abelian groups, or the category of commutative

rings. Let  $\text{Top}_S$  the category which objects are open sets of  $S$ , and morphism between objects are given by inclusions.

**Definition 0.13.** A  $\mathcal{C}$ -valued *presheaf* is contravariant functor  $\mathfrak{F} : \text{Top}_S \rightarrow \mathcal{C}$ .

Let  $U \subseteq V$  be open subsets of  $S$ . Suppose  $S$  has a presheaf  $\mathfrak{F}$  defined over a category  $\mathcal{C}$ . By definition there is a morphism  $\text{res}_{V,U} : \mathfrak{F}(V) \rightarrow \mathfrak{F}(U)$  called *restriction map*.

*Example:* Let  $S = \text{Spec}(\mathbb{Z})$  and let  $U = \text{Spec}(\mathbb{Z}) \setminus \{p_1, \dots, p_n\}$  an open set. Let  $\mathfrak{F}(U)$  be the set of rational numbers, written in reduced form, such that the denominator has no prime factors outside of  $\{p_1, \dots, p_n\}$ . Letting  $\mathfrak{F}(\emptyset) = \mathbb{Q}$  we see that  $\mathfrak{F}$  is a presheaf of commutative rings, where  $\text{res}_{V,U}$  is the inclusion from  $\mathfrak{F}(V)$  to  $\mathfrak{F}(U)$  whenever  $U \subseteq V$ .

We can think a presheaf on  $S$  as a tool to study local properties of  $S$ . Usually this is done via continuous functions on open sets of  $S$ . Since we want some sort of algebraic structure we require these continuous functions to have image not only in a topological object but also an algebraic one as rings, groups or modules. Let  $X, Y$  be a topological spaces. The set of continuous functions from  $X$  to  $Y$  is denoted by  $C(X, Y)$ .

*Example:* Let  $S = \mathbb{R}$  the real numbers with the usual topology. We can define the presheaf of real valued continuous functions. For  $\emptyset \neq U \subseteq \mathbb{R}$  an open set, let  $\mathfrak{F}(U) = C(U, \mathbb{R})$  and  $\mathfrak{F}(\emptyset) = 0$ . If  $U \subseteq V$  the restriction of a continuous function on  $V$  to  $U$  defines  $\text{res}_{V,U}$ .

It is not a difficult exercise to show that the presheaf of the previous example satisfies the following properties. Let  $U \subseteq S$  be an open set.

- **Identity axiom.** If  $(U_i)_{i \in I}$  is an open cover of  $U$ . Suppose that there are  $f, g \in \mathfrak{F}(U)$  such that  $\text{res}_{U,U_i}(f) = \text{res}_{U,U_i}(g)$  for all  $i$ . Then  $f = g$ .
- **Gluing axiom.** If  $(U_i)_{i \in I}$  is an open cover of  $U$ . Suppose that there is  $f_i \in \mathfrak{F}(U_i)$  for all  $i$ , such that  $\text{res}_{U_i, U_i \cap U_j}(f_i) = \text{res}_{U_j, U_i \cap U_j}(f_j)$  for all  $i, j$ . Then there is  $f \in \mathfrak{F}(U)$  such that  $\text{res}_{U,U_i}(f) = f_i$  for all  $i$ .

**Definition 0.14.** A presheaf is called a *sheaf* if it satisfies the identity and gluing axioms.

*Example:* Let  $S$  be a Riemann surface. The set of analytic functions  $O(U) := \{f : U \rightarrow \mathbb{C}\}$  for each  $U$  open in  $X$  defines a sheaf of rings.

The previous example is a particular case of an important notion to us.

**Definition 0.15.** A *ringed space* is a topological space  $S$  with a sheaf of commutative rings.

*Example:* We can think of  $\text{Spec } R$  as a ringed space (see (Ha)) by having  $R_x$  be the ring of functions on the basic open set  $\text{Spec } R_x$ .

## Group Schemes from Schemes

Now we briefly describe the notion of morphism between ringed spaces of the form  $\text{Spec } R$ . With this in hand we finally define what is a scheme and group scheme over it. We again recommend the reader to consult (Ha) as a source for this section.

Note that if  $A$  is an  $R$ -algebra, then the map  $R \rightarrow A$  induces a map  $\text{Spec } A \rightarrow \text{Spec } R$ , and  $\text{Spec } A$  will be called an affine scheme over  $\text{Spec } R$  via this map. Base change to  $\text{Spec } \mathfrak{K}$  replaces  $\text{Spec } A$  by  $\text{Spec } (A \otimes_R \mathfrak{K})$ . Let  $B$  be an  $R$ -algebra. An  $R$ -algebra homomorphism  $A \rightarrow B$  yields a commutative diagram:

$$\begin{array}{ccc} \text{Spec } B & \xrightarrow{\phi} & \text{Spec } A \\ & \searrow \phi_i & \swarrow \pi_i \\ & \text{Spec } R & \end{array}$$

The above plus the local morphisms  $A_{\phi^{-1}(P)} \rightarrow B_P$ , for  $P \in \text{Spec } B$ , give a morphism of affine schemes over  $\text{Spec } R$ . Moreover, any such morphism of affine schemes is induced by some  $\phi : A \rightarrow B$ . In fact it can be shown that

$$\text{Hom}_{\text{Spec } R}(\text{Spec } B, \text{Spec } A) \cong \text{Hom}_{R_{\text{alg}}}(A, B) \quad (4)$$

In other words, the category of affine schemes over  $\text{Spec } R$  is dually-equivalent to the category of  $R$ -algebras.

We identify  $\text{Spec } \mathfrak{K}$  with the affine scheme represented by  $\mathfrak{K}$ . This is fair since  $\text{Hom}_{\text{Spec } R}(-, \text{Spec } \mathfrak{K}) \cong \text{Hom}_{R_{\text{alg}}}(\mathfrak{K}, -)$ .

**Definition 0.16.** A ringed space admitting a covering by open sets that are affine schemes is called a *scheme*.

Morphisms of schemes are defined locally. In other words  $f : S' \rightarrow S$  is a morphism if there is an open affine cover,  $\text{Spec } R_i$  of  $S$ , such that  $f^{-1}(\text{Spec } R_i)$  is an affine scheme  $\text{Spec } R'_i$ , and the restriction map  $\text{Spec } R'_i \rightarrow \text{Spec } R_i$  is a morphism of affine schemes.

In this situation we say that  $S'$  is a *scheme over*  $S$ . In Grothendieck's approach, this relative notion is important rather than absolute questions about a scheme. Questions about  $f$  turn into questions about the ring maps  $f_i : R_i \rightarrow R'_i$ . In particular, we say that  $f$  has property  $(*)$  (for example, is finite or flat), if there is a covering of  $S$  such that each of the ring maps  $f_i$  has this property.

If  $S$  is a scheme, then a *group scheme over*  $S$  is a representable functor  $F$  from the category of schemes over  $S$  to the category of groups, i.e. there exists some scheme  $\mathcal{S}$  over  $S$  such that  $F(-) = \text{Hom}_{S_{\text{schemes}}}(-, \mathcal{S})$ . Note that in the case  $S = \text{Spec } R$  and  $\mathcal{S} = \mathfrak{R}$  a  $R$ -algebra, (4) tells us that  $F$  is equivalent to the affine group scheme over  $R$ , represented by  $\mathfrak{R}$ .

### 0.3.2 The group scheme $E[n]$

An elliptic curve  $E$  over  $\mathbb{Q}$  induces a group functor from the category of  $\mathbb{Q}$ -algebras. As we mentioned before this does not define an affine group scheme. It turns out that under certain conditions the group functor  $E[n]$  is an affine group scheme. In the next chapter this fact will be a key ingredient in proving the link between the notions of semistability for an elliptic curve, and semistability of the Galois representation associated to it. These concepts will be fully described in the next chapter.

**Proposition 0.17.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  and  $p$  a prime of good reduction. Then the  $\mathbb{Q}_p$ -group scheme  $E[n]$  is the generic fiber of a finite flat group scheme over  $\text{Spec } \mathbb{Z}_p$  of rank  $n^2$ .*

We have not developed enough tools from algebraic geometry to give a proof of this proposition. However for the more experimented reader in this area we have tried to describe, in a very informal way, how a proof of this proposition should read. For some of the geometric terminology used next we refer the reader to (Ha).

*Sketch of proof.* i) First write the equations of  $E/\mathbb{Q}_p$  in such way that you can think of it as a closed subscheme  $\mathcal{E}$  of  $\mathbb{P}_{\mathbb{Z}_p}^2$ , which is a good model of  $E/\mathbb{Q}_p$ . In other words homogenize the equations, so that your polynomial is over  $\mathbb{Z}_p$  in Weierstrass form and has good reduction at  $p$ .

ii) Show that  $\mathcal{E}$  has the structure of a group scheme over  $\mathbb{Z}_p$  which extends to the one on  $E/\mathbb{Q}_p$  via the fiber product. The first part means that addition operation can be defined over  $\mathbb{Z}_p$ . For the second part we need ((Si), remark IV.5.4.1).

At this point, it is enough to prove that  $\mathcal{E}[n]$  is finite and flat over  $\mathbb{Z}_p$ . This is divided into steps.

- iii) First we assume that  $\mathcal{E}[n]$  is an affine scheme, say over  $\text{Spec}(R)$ , and we deduced that it is finite and flat. Since  $\mathcal{E}[n]$  is a closed subscheme of  $\mathbb{P}_{\mathbb{Z}_p}^2$  and  $\mathbb{P}_{\mathbb{Z}_p}^2 \rightarrow \text{Spec } \mathbb{Z}_p$  is proper, the map  $\text{Spec } R \rightarrow \text{Spec } \mathbb{Z}_p$  is universally closed. Therefore Proposition 0.18 below implies that  $R$  is integral over  $\mathbb{Z}_p$ . From here is easy to prove that it is finite of dimension  $n^2$ . Since it has to be finitely generated as a  $\mathbb{Z}_p$ -algebra, being integral implies that is a finite over  $\mathbb{Z}_p$ . Note that in the case that  $p$  and  $n$  are relatively prime, the generic and closed fiber have the same number of geometric points, namely  $n^2$ . On the other hand this number is the dimension of the generic and closed fiber, therefore after taking the tensor product of  $R$  with  $\mathbb{Q}_p$  and  $\mathbb{F}_p$  we get the same number of copies. This implies, as we will see below, that  $R$  is a free  $\mathbb{Z}_p$ -module of rank  $n^2$ . We should mention that the general case reduces to show that the rank of the generic and closed fibers are equal to the degree of the map  $[n]$ . This degree is  $n^2$  regardless of whether  $p$  and  $n$  are coprime, and this gives the desired result. Note that in the case  $p$  and  $n$  are relatively prime this degree is the number of geometric points.
- iv) Finally we must show that  $\mathcal{E}[n]$  is affine. Since  $\mathcal{E}[n]$  is a closed subscheme of  $\mathbb{P}_{\mathbb{Z}_p}^2$ , It suffices to find an open affine set containing it. The idea here is to find an homogeneous polynomial  $f \in \mathbb{Z}_p[X, Y, Z]$  whose zero set on  $\mathbb{P}_{\mathbb{Z}_p}^2$  does not intersects  $\mathcal{E}[n]$ . This polynomial is going to be a lifting of one  $\tilde{f} \in \mathbb{F}_p[X, Y, Z]$  such that its zero set does not intersects  $\mathcal{E}[n] \times_{\text{Spec}(\mathbb{Z}_p)} \text{Spec}(\mathbb{F}_p)$  in  $\mathbb{P}_{\mathbb{F}_p}^2$ .

□

*Example:* Consider the elliptic curve  $E : x^3 + y^3 = z^3$  over  $\mathbb{Q}$ . Over  $\mathbb{F}_5$ , this equation also defines an elliptic curve, thus 5 is a prime of good reduction. It can be shown that  $-[x : y : z] = [y : x : z]$  is the inverse for the group operation on  $E$ . In particular  $E[2](\mathbb{Q}_5) = \{[1 : -1 : 0], [1 : 1 : a], [1 : 1 : b], [1 : 1 : c]\}$  where  $a, b, c$  are the solutions of  $z^3 = 2$ . Note that all the 2-torsion belongs to an affine chart, namely  $x = 1$ . If  $\mathfrak{R} = \mathbb{Q}_5[y, z]/\langle(2 - z^3, y - 1)(z, y + 1)\rangle$ , then  $E[2](A) = \text{Hom}_{\mathbb{Q}_5}(\mathfrak{R}, A)$  for any  $\mathbb{Q}_5$ -algebra  $A$ . Furthermore, this affine group scheme over  $\mathbb{Q}_5$  is the generic fiber of the affine group scheme over  $\mathbb{Z}_5$  represented by  $R = \mathbb{Z}_5[y, z]/\langle(2 - z^3, y - 1)(z, y + 1)\rangle \cong \mathbb{Z}_5[y, z]/\langle(2 - z^3, y - 1) \times \mathbb{Z}_5[y, z]/(z, y + 1) \cong \mathbb{Z}_5[z]/(z^3 - 2) \times \mathbb{Z}_5$ . Therefore as  $\mathbb{Z}_5$ -modules  $R \cong \mathbb{Z}_5^4$ , and  $E[2]$  is indeed the generic fiber of a finite, flat group scheme of rank 4 over  $\mathbb{Z}_5$ .

**Proposition 0.18.** *Let  $R$  be a ring and  $S$  a Noetherian  $R$ -algebra. If for all  $R$ -algebra  $T$ , the induced map  $\text{Spec}(S \otimes_R T) \rightarrow \text{Spec}(T)$  is closed, then  $R \rightarrow S$  Is an*

*integral extension.*

For a proof of this proposition see (Mat) or (Bo).

**Lemma 0.19.** *Let  $A$  be a finite  $\mathbb{Z}_p$ -algebra. Then  $A$  is free if and only if  $\dim_{\mathbb{F}_p}(A \otimes_{\mathbb{Z}_p} \mathbb{F}_p) = \dim_{\mathbb{Q}_p}(A \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$ .*

*Proof.* Since  $A$  is finitely generated as  $\mathbb{Z}_p$ -module,  $A \cong \mathbb{Z}_p^n \oplus T$  where  $T$  is a finite  $\mathbb{Z}_p$ -module. If  $T \neq 0$ , then  $\dim_{\mathbb{F}_p}(T \otimes_{\mathbb{Z}_p} \mathbb{F}_p) \geq 1$  and  $\dim_{\mathbb{F}_p}(A \otimes_{\mathbb{Z}_p} \mathbb{F}_p) \geq n + 1$ . On the other hand  $\dim_{\mathbb{Q}_p}(A \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = n$  hence  $T = 0$  and  $A$  is free.  $\square$

## Exercises

- 0.1. Let  $G$  and  $H$  be as in (0.3). For each  $R$ -algebra  $A$ , define  $F(A) = \ker(G(A) \rightarrow H(A))$ . Show that  $F$  is a group scheme over  $R$ .
- 0.2. Given ring homomorphism  $R \rightarrow S$  and  $R$ -algebra  $A$ , consider the collection of rings  $B$  and homomorphisms that satisfy (1). Show that these form the objects in a category of  $S$ -algebras, with an initial object. This initial object is the *tensor product*  $A \otimes_R S$ . In particular,  $R[T_1, \dots, T_n] \otimes_R S = S[T_1, \dots, T_n]$ .
- 0.3. Find two  $R$ -algebra morphisms from  $R[x] \rightarrow R[x, x^{-1}]$ . In contrast show that there is only one homomorphism  $\mathbf{G}_m \rightarrow \mathbf{G}_a$ .
- 0.4. Consider the maps  $\Delta : \mathbb{Z}[x] \rightarrow \mathbb{Z}[x_1, x_2] \cong \mathbb{Z}[x_1] \otimes_{\mathbb{Z}} \mathbb{Z}[x_2]$  given by  $x \mapsto x_1 + x_2$ ,  $\epsilon : \mathbb{Z}[x] \rightarrow \mathbb{Z}$  induced by  $x \mapsto 0$  and  $S : \mathbb{Z}[x] \rightarrow \mathbb{Z}[x]$  such that  $x \mapsto -x$ . Show that these  $\mathbb{Z}$ -algebra morphisms give  $\mathbb{Z}[x]$  a Hopf Algebra structure. (Hint: Consider  $\mathbf{G}_a$  as a group scheme over  $\text{Spec } \mathbb{Z}$ ).
- 0.5. Let  $K$  be a field and let  $\mathfrak{R}$  be a finite  $K$ -algebra. Show that  $\mathfrak{R}$  is étale if and only if  $\mathfrak{R}$  is *reduced*, i.e 0 is the only nilpotent element.
- 0.6. Let  $A$  be a flat  $R$ -algebra, where  $R$  is a domain. Show that as a  $R$ -module,  $A$  is torsion free.
- 0.7. Show that (3) does indeed define a topology on  $\text{Spec } R$ , i.e. that  $\emptyset, R$  are closed sets and that arbitrary intersections and finite unions of closed sets are closed. Show that  $\text{Spec } \mathbb{Z}_p$  is not Hausdorff. Show that  $\text{Spec } R$  is always compact.
- 0.8. Let  $\wp \in \text{Spec } R$  and let  $\kappa(\wp) = \text{Frac}(R/\wp)$ . Show that  $\kappa(\wp)$  is an  $R$ -algebra, so that  $\text{Spec } \kappa(\wp)$  embeds in  $\text{Spec } R$ . Let  $A$  be an  $R$ -algebra, so that  $\text{Spec } A$  maps to  $\text{Spec } R$ . Show that its fiber over  $\wp$  is homeomorphic to  $\text{Spec } (A \otimes_R \kappa(\wp))$ .
- 0.9. Calculate the rank of  $\mu_n$  as a group scheme over  $\text{Spec } \mathbb{Q}$ .
- 0.10. Let  $R_1, \dots, R_n$  be a set of commutative rings with 1. Show that any ideal of  $R_1 \times \dots \times R_n$  is of the form  $I_1 \times \dots \times I_n$  for some ideals  $I_i$  of  $R_i$  for all  $i$ . In particular if  $K$  is a field the  $K$ -algebra  $K \times \dots \times K$  has exactly  $n$  maximal ideals, where  $n$  is the number of copies of  $K$ . Deduce that  $|\text{Hom}_{K\text{-alg}}(K \times \dots \times K, K)| = \dim_K(K \times \dots \times K)$

## References

- [Bo] Bourbaki, N, *Commutative algebra. Chapters 1–7*, Springer-Verlag, Berlin, 1998.
- [Ha] Hartshorne, Robin, *Algebraic Geometry*, Springer-Verlag, New York Inc., 1979, Graduate Texts in Mathematics 52.
- [Mat] Matsumura, Hideyuki, *Commutative algebra*, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1990, Mathematics Lecture Note Series 56, second edition.
- [Si] Silverman, J.H, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1999, Graduate Texts in Mathematics 151.
- [Wat] Waterhouse, W, *Introduction to affine group schemes*, Springer-Verlag, New York, 1979, Graduate Texts in Mathematics 66.