INTRODUCTION TO FINITE GROUP SCHEMES

Contents

Date: October 19–December 7, 2000.

Notes by John Voight, `jvoight@math.berkeley.edu`, taken from a seminar taught by René Schoof.

The following are notes taken from a seminar taught by René Schoof at the University of California, Berkeley, in the Fall semester, 2000.

1. Tate's theorem

We begin with a motivating theorem for the course:

Theorem (Tate)**.** *There is no elliptic curve over $\mathbb{Q}$ with good reduction modulo every prime p.*

We will see later the generalization by Fontaine: there are no abelian varieties over $\mathbb{Q}$ with good reduction modulo every prime p. The problem is reduced to certain properties of the torsion points of abelian varieties, i.e. points of finite flat group schemes over $\mathbb{Z}$.

The proof is as follows (see [Tat2]):

Proof. An elliptic curve E defined over $\mathbb{Q}$ has a Weierstrass equation [Sil, Proposition III.3.1]

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

and after clearing denominators, we may assume $a_i \in \mathbb{Z}$. Compute the discriminant $\Delta_E = \Delta \neq 0$ (because E is nonsingular). To say that E has good reduction modulo p is to say there exists a change of coordinates [Sil, Proposition VII.1.3]

$$X' = p^2X + r, \quad Y' = p^3Y + sX + t$$

for $r, s, t \in \mathbb{Z}$ so that the resulting curve when reduced modulo p remains nonsingular. We find $\Delta' = \Delta/p^{12}$. Repeat this process for all primes dividing Δ until we are left with a unit (E will have bad reduction at any prime dividing the minimal discriminant, cf. [Sil, Proposition VII.5.1]) and $\Delta = \pm 1$. The fact that $\mathbb{Z}$ is a PID is important here, since it allows us to find a minimal global Weierstrass equation [Sil, Proposition VIII.8.2].

Let [Sil, §III.1]:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= a_1a_3 + 2a_4 \\
b_6 &= a_3^2 + 4a_6 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= \frac{c_4^3 - c_6^2}{1728}
\end{aligned}$$

These come about as follows: we complete the square by letting $X' = 4X$ and $Y' = 8Y + 4a_1X + 4a_3$, we obtain

$$\begin{aligned}
Y'^2 &= X'^3 + (a_1^2 + 4a_2)X'^2 + (8a_1a_3 + 16a_4)X' + (16a_3^2 + 64a_6) \\
&= X'^3 + b_2X'^2 + 8b_4X' + 16b_6 = f(X').
\end{aligned}$$

If we eliminate b_2 by $X'' = 9X' + 3b_2$, $Y'' = 27Y'$, we obtain

$$\begin{aligned} Y''^2 &= X''^3 - 27(b_2^2 - 24b_4)X'' + 54(b_2^3 - 36b_2b_4 + 216b_6) \\ &= X''^3 - 27c_4X'' - 54c_6. \end{aligned}$$

We will write

$$Y'^2 = f(X') = X'^3 + a_2'X'^2 + a_4'X' + a_6'.$$

The roots of f give the 2-torsion points (as $[2](x,y) = O$ iff $y = 0$), and $\Delta' = 2^{12}\Delta = \pm 2^{12}$; the discriminant of f is $2^6\Delta = \pm 2^6$ (each root is quartered).

Claim. E has a rational point of order 2.

Proof of claim. Adjoin all of the 2-torsion points $E[2]$ to $\mathbb{Q}$. The field L thus obtained is Galois (since σP is also a 2-torsion point for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, or because it is the splitting field of f), and

$$\mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow GL_2(\mathbb{F}_2) \simeq S_3,$$

and

$$\begin{array}{c} L \\ | \\ K = \mathbb{Q}(\sqrt{\Delta}) \\ | \\ \mathbb{Q} \end{array}$$

(L contains $\sqrt{\Delta}$ because the discriminant is the square of a matrix with elements of L), hence $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}$.

In order to show that at least one 2-torsion point is defined over $\mathbb{Q}$, we need to show that f is not irreducible, that is, that 3 does not divide the degree of the extension $[L : \mathbb{Q}]$, so that the image of the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is contained in a (cyclic) subgroup of order two.

Case 1 ($K = \mathbb{Q}$, or $\Delta = 1$). The extension L is now Galois over $\mathbb{Q}$ and hence cyclic of degree dividing 3. By class field theory (which over $\mathbb{Q}$ is just the Kronecker-Weber Theorem), any abelian extension of $\mathbb{Q}$ ramified outside m is contained $\mathbb{Q}(\zeta_m)$ [L, §X.3, Corollary 3]. L is only ramified only at 2 (the discriminant of the defining cubic is a power of 2, and $\Delta_L \mid \Delta$), so $\mathbb{Q} \subset L \subset \mathbb{Q}(\zeta_{2^n})$; but $[L : \mathbb{Q}] \mid [\mathbb{Q}(\zeta_{2^n}) : \mathbb{Q}]$ has 2-power order, a contradiction.

Alternatively, one can compute the discriminant of L: at unramified primes, the local discriminant of L is ± 1; at 2, we have $\mathbb{Q}_2 \subset L_2$. The minimal polynomial $g(\pi) = 0$ is Eisenstein (a prime degree Galois extension of local fields is either unramified or totally ramified, since $n = 3 = ef$). Therefore Δ_L is equal to the local discriminant [Ser, §III.4, Proposition 9], which we can take to be $N(g'(\pi))$ for a uniformizer π [Ser, §III.6, Proposition 12]. Since $g(T) \equiv T^3 \pmod 2$, we have $g'(\pi) \equiv 3\pi^2 \pmod 2$, hence $v_\pi(g'(\pi)) = v_\pi(\pi^2) = 2$, and $v_2(N(g'(\pi))) = v_2(N(\pi)^2) = 2$ again because g is Eisenstein. This implies that $|\Delta_L| \leq 2^2$.

We now use discriminant bounds: by the Minkowski bound [L, §V.4, Theorem 4], if $\mathfrak{a} \subset \mathfrak{O}_L$ is nonzero, then there is an $\alpha \in \mathfrak{a}$ such that

$$|N(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|\Delta_L|}N(\mathfrak{a})$$

where $n = [L : \mathbb{Q}] = 3$, r_2 the number of complex places of L, which in our case is 0 (if there were two complex roots, we would have the automorphism complex conjugation of order 2). Thus

$$|\Delta_L| \geq \left(\frac{n^n}{n!}\right)^2 = \left(\frac{27}{3!}\right)^2 \geq 21,$$

a contradiction.

Case 2 ($K = \mathbb{Q}(i)$, $\Delta = -1$). In this case, we have $K = \mathbb{Q}(i) \subset L$, with $L/\mathbb{Q}(i)$ cyclic of degree dividing 3, only ramified at $1+i$, the (ramified) prime over 2. One can now use class field theory to show that any ray class field of conductor a power of 2 has 2-power order, taking the cycle $\mathfrak{c} = (1+i)^e$ (since K is already totally imaginary) for e sufficiently large, we have by [L, §VI.1, Theorem 1] that the order of the ray class field modulo $\mathfrak{c}$ is

$$h_{\mathfrak{c}} = \frac{h_L \phi(\mathfrak{c})}{(U : U_{\mathfrak{c}})} = 2^{e-3}.$$

Or we can compute the discriminant of L using a relative discriminant formula: we have

$$\Delta_{L/\mathbb{Q}(i)} \mid \langle 1+i \rangle^2$$

as before by the Eisenstein condition, so [Ser, §III.4, Proposition 8]

$$\Delta_{L/\mathbb{Q}} = N(\Delta_{L/\mathbb{Q}(i)})\Delta^3_{\mathbb{Q}(i)} = 2^2 4^3 = 2^8 = 256.$$

Now the Minkowski bound gives with $n = 6$, $e_2 = 3$,

$$|\Delta_L| \geq \left(\frac{6^6}{6!}\left(\frac{\pi}{4}\right)^3\right)^2 > 985,$$

a contradiction. This concludes the proof of the claim. □

Now from the equation

$$Y'^2 = X'^3 + a'_2 X'^2 + a'_4 X' + a'_6,$$

since the cubic is monic, the 2-torsion point will necessarily have integral coordinates, so after translating we may assume that $a'_6 = 0$. This implies by our equations that $b'_2 = 4a'_2$, $b'_4 = 2a'_4$, and $b'_6 = 0$, and hence $c'_4 = b'^2_2 - 24b'_4 = 16(a'^2_2 - 3a'_4)$ and $c'_6 = 32(9a'_2 a'_4 - 2a'^3_2)$. Since $1728\Delta' = c'^3_4 - c'^2_6$, we have

$$1728(\pm 2^{12}) = 2^{12}(a'^2_2 - 3a'_4)^3 - 2^{10}(9a'_2 a'_4 - 2a'^3_2)^2$$

and simplifying this gives

$$\pm 2^8 = a'^2_4(a'^2_2 - 4a'_4).$$

This implies $a'_4 \mid 2^4$, and the only values of $a'_4 = \pm 2^k$ for which $\pm 2^{8-2k} + 2^{k+2}$ is a square are $(a'_2, a'_4) = (0, \pm 4), (\pm 6, 8)$. These correspond to the curves

$$Y'^2 = X'^3 \pm 4X'$$
$$Y'^2 = X'^3 \pm 6X'^2 + 8X'.$$

A direct calculation shows that each of these curves has j-invariant equal to 1728.

We will show that the second curve cannot occur; the proof of the first is the similar. If this curve had good reduction, we could use a transformations of the form $Y' = 8Y + sX + t$, $X' = 4X + r$, and we find

$$(8Y + sX + t)^2 = (4X + r)^3 + 6(4X + r)^2 + 8(4X + r)$$

which is

$$64Y^2 + 16sXY + 16tY = 64X^3 + (48r + 96 - s^2)X^2 + (12r^2 + 48r - 2st)X + (r^3 + 6r^2 - t^2 + 8).$$

Since this new equation is to have good reduction at 2 while keeping integral coordinates, we must be able to make the coefficient on Y^2 and X^3 a unit, so every coefficient must be divisible by 64. In particular, this implies that $4 \mid s$ (say $s = 4s'$) and $4 \mid t$ by the XY and Y coefficients, and $4 \mid (3r + 6 - s'^2)$ by the X^2 coefficient. Modulo 16 we obtain $0 \equiv 12r^2 \equiv 0 \pmod{16}$ in the X coordinate, so that $r = 2r'$, and $4 \mid (6r' + 6 - s'^2)$, so s' is even and r' is odd. Now, modulo 64, we obtain by the X coordinate that

$$0 \equiv 48 \pm 96 + 0 \equiv 48 \pmod{64},$$

and this is false. □

There is another proof of this theorem:

Second proof [O]. For a curve

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

in the most general form to have good reduction everywhere, we must have that the discriminant

$$\Delta = \pm 1 = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

is a unit, where $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$ and the other coefficients as above (see e.g. [Sil, §III.1]). If a_1 were even, we would have $b_2 = a_1^2 + 4a_2 \equiv 0 \pmod 4$ and that $b_4 = a_1a_3 + 2a_4 \equiv 0 \pmod 2$. This implies that

$$\pm 1 = \Delta \equiv -27b_6^2 \equiv 5b_6^2 \equiv 0, 4, 5 \pmod 8,$$

a contradiction. Therefore a_1 is odd, which implies that $b_2 \equiv 1 \pmod 4$ and $c_4 = b_2^2 - 24b_4 \equiv 1 \pmod 8$.

We have that $c_4^3 - c_6^2 = 1728\Delta = \pm 1728$, which implies that

$$(c_4 \mp 12)(c_4^2 \pm 12c_4 + 144) = c_6^2.$$

Since c_4 is odd, $\gcd(c_4 \mp 12, c_4^2 \pm 12c_4 + 144)$ is a power of 3. Since in addition $c_4^2 \pm 12c_4 + 144 > 0$, we have that $c_4 \mp 12 > 0$ and hence $c_4 \mp 12 = 3^em^2$ for some $e \geq 0$ and odd $m \in \mathbb{Z}$. This implies that

$$3^e \equiv 3^em^2 = c_4 \mp 12 \equiv 1 \mp 12 \equiv 5 \pmod 8,$$

a contradiction. □

Exercises. The following are exercises for §1.

Problem 1.1. Show that there are no elliptic curves over $\mathbb{Q}(i)$ with good reduction everywhere.

2. Introduction to group schemes

For more background information about group schemes, consult [Wat] for an introduction to affine group schemes, [Tat] for an emphasis on finite flat group schemes, and [Sha] and [TO] for other results of group schemes.

Definition (as a functor). Let R be a Noetherian base ring (we will usually take either the ring of integers of a number field, a p-adic ring i.e. a complete local Noetherian ring, or a perfect field). Let $\mathfrak{C}$ be the category of R-algebras, and $\mathfrak{C}^\vee$ the category of affine R-schemes, the dual category.

Let F be a covariant functor $\mathfrak{C} \to \mathbf{Grps}$ (the category of groups) and $F^\vee : \mathfrak{C}^\vee \to \mathbf{Grps}$ the corresponding contravariant functor.

Example. If S is an R-algebra, we can let $F(S) = S^\times$, for if we have a map $f : S \to T$, then we have an induced map $F(S) = S^\times \to T^\times = F(T)$ by f.

Example. We can also associate to every S a fixed finite group Γ, with the maps $\Gamma \to \Gamma$ just the identity.

Suppose that F is *representable* [Mac, §III.2], i.e. we have $G \in \mathfrak{C}^\vee$ so that $G = \mathrm{Spec}(A)$ with the property that $F(\mathrm{Spec}\, S) = \mathrm{Mor}_R(\mathrm{Spec}\, S, G)$. Dualizing, this is equivalent to $\mathrm{Mor}_R(\mathrm{Spec}\, S, G) \simeq \mathrm{Hom}_R(A, S)$. We let $G(S) = \mathrm{Mor}_R(\mathrm{Spec}\, S, G)$ be the set of *S-valued points of G*, and in this case, G is what is called a group scheme. (See [Tat, (1.6)].)

Definition. $G = \mathrm{Spec}\, A$ is a *group scheme* if there is a contravariant functor $F : \mathfrak{C} \to \mathbf{Grps}$ such that the underlying functor $F : \mathfrak{C} \to \mathbf{Sets}$ is representable, i.e. $G(S) = F(\mathrm{Spec}\, S) = \mathrm{Mor}_R(\mathrm{Spec}\, S, G) \simeq \mathrm{Hom}_R(A, S)$.

For a concrete explication of the functoriality of group schemes, see [Wat, §1.2].

Example. Let $G = \mathrm{Spec}\, A$, $A = R[T, 1/T]$. Then

$$F(S) = \mathrm{Hom}_R(R[T, 1/T], S) \simeq S^\times$$

(since such a map is determined by image of T, which must also be an invertible element of S).

Example. If S is an R-algebra, then if $G = \mathrm{Spec}\, A$ were to represent the constant functor to a group Γ in the second example above, then we would have

$$\Gamma \simeq \mathrm{Hom}_R(A, S \times S) = \mathrm{Hom}_R(A, S) \times \mathrm{Hom}_R(A, S) = \Gamma \times \Gamma,$$

so we must have $\#\Gamma = 1$. Therefore only a trivial group can be represented in this way.

Definition (as a group object). There is an alternative definition of group schemes using the Yoneda lemma [Mac, §III.2]:

Lemma (Yoneda lemma)**.** *If $\mathfrak{C}$ is a category, then the functor*

$$F : \mathfrak{C} \to \mathbf{Func}(\mathfrak{C}, \mathbf{Sets})$$
$$A \mapsto F_A$$

where $F_A(S) = \mathrm{Mor}_{\mathfrak{C}}(A, S)$ is fully faithful, so that

$$\mathrm{Mor}_{\mathfrak{C}}(A, B) \leftrightarrow \mathrm{Mor}_{\mathbf{Func}}(F_B, F_A).$$

This map is indeed a functor because if we have a map $\phi : A \to B$ then have induced map $\mathrm{Mor}_{\mathfrak{C}}(B, S) \to \mathrm{Mor}_{\mathfrak{C}}(A, S)$ by $f \mapsto f \circ \phi$.

The inverse of the functor is given on $f_S : \mathrm{Mor}_{\mathfrak{C}}(B, S) \to \mathrm{Mor}_{\mathfrak{C}}(A, S)$ by $(f_S)_S \mapsto f_B(\mathrm{id}_B)$.

In other words, if you "know the functor", then you "know the original object", and vice versa. (See [Sha, §2] for an explication of this concept of a group scheme as a family.) Hence the set of maps $F_A(S) \xleftarrow{f_S} F_B(S)$ corresponds to a map $A \to B$ (see the discussion in [Wat, §1.3]). In particular, if F is a group functor, then

$F(S)$ is a group, hence we have a group operation $F(S) \times F(S) \to F(S)$. If F is representable, $G(S) \times G(S) \to G(S)$, i.e.

$$\mathrm{Mor}_R(\operatorname{Spec} S, G) \times \mathrm{Mor}_R(\operatorname{Spec} S, G) \to \mathrm{Mor}_R(\operatorname{Spec} S, G),$$

which is to say we have a group operation

$$\mathrm{Hom}_R(A, S) \times \mathrm{Hom}_R(A, S) \to \mathrm{Hom}_R(A, S).$$

Therefore

$$\mathrm{Hom}_R(A \otimes A, S) = (G \times G)(S) \to \mathrm{Hom}_R(A, S) = G(S),$$

and all of these compatible group laws $F_A(S) \leftarrow F_{A\otimes A}(S)$ must come from a single morphism $A \to A \otimes A$, i.e. one from $G \leftarrow G \times G$.

Therefore we can also define a group scheme by the following ([Tat, (1.5)] or [Sha, §2]):

Definition. An *R-group scheme* G is a *group object* in the category $\mathfrak{C}$ of R-schemes, which is to say that G is an (affine) R-scheme together with a morphism $c : G \times G \to G$, called the *composition* law, a morphism $e : \operatorname{Spec} R \to G$ called the *unit* or *neutral* element, and an inverse map $i : G \to G$, which satisfy the group axioms.

This definition is a statement in the category $\mathfrak{C}^\vee$. Therefore if we have $G = \operatorname{Spec} A$, then for the R-algebra A with everything dualized, we have a maps $c : A \to A \otimes_R A$, $e : A \to R$, and $i : A \to A$ so that the dual diagrams commute. In this case, the group operations (maps) are called *comultiplication*, *counit*, and *coinverse*.

Example. In the case of $\mathbb{G}_m = \operatorname{Spec} R[T, 1/T] = \operatorname{Spec} A$, then $\mathbb{G}_m(S) = S^\times = \mathrm{Hom}_R(R[T, 1/T], S)$ by the association of ϕ with $\phi(T)$.

On the level of algebras, comultiplication is

$$\begin{aligned} R[T, 1/T] &\to R[U, 1/U] \otimes R[V, 1/V] = R[U, 1/U, V, 1/V] \\ T &\mapsto UV \end{aligned}$$

under usual multiplication. The neutral element $R[T, 1/T] \to R$ is $T \mapsto 1$, and the inverse map is $R[T, 1/T] \to R[T, 1/T]$ by $T \mapsto 1/T$.

The group axioms can be phrased in terms of the commutativity of certain diagrams (see [Wat, §1.4]). For example, associativity corresponds to the diagram

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

with the corresponding dual diagram:

$$\begin{array}{ccc} A \otimes A \otimes A & \xleftarrow{c \otimes \mathrm{id}_A} & A \otimes A \\ \uparrow{\scriptstyle \mathrm{id}_A \otimes c} & & \uparrow{\scriptstyle c} \\ A \otimes A & \xleftarrow{c} & A \end{array}$$

The neutral element satisfies

$$\begin{array}{ccc} G & \longrightarrow & G \times_R \operatorname{Spec} R \\ \| & & \downarrow{\scriptstyle \mathrm{id}_A \times e} \\ G & \xleftarrow[c]{} & G \times G \end{array}$$

where $G \to G \times_R \operatorname{Spec} R$ is the natural injection, and the inverse map has

$$\begin{array}{ccccc} G & \xrightarrow{\Delta} & G \times G & \xrightarrow{\mathrm{id}_G \times i} & G \times G \\ & & & & \downarrow{\scriptstyle c} \\ & & \operatorname{Spec} R & \xrightarrow{e} & G \end{array}$$

where Δ is the diagonal map, dual to:

$$\begin{array}{ccccc} A & \xleftarrow[m]{} & A \otimes A & \xleftarrow[\mathrm{id}_A \otimes i]{} & A \otimes A \\ & & & & \uparrow{\scriptstyle c} \\ & & R & \xleftarrow[e]{} & A \end{array}$$

A is a finitely generated R-algebra, and any such A equipped with morphisms c, i, e (called *comultiplication*, *counit*, and *coinverse*) making the above diagrams commute is called a commutative *Hopf algebra* [Tat, (2.2)]. Therefore by definition the category of Hopf algebras is equivalent to the category of affine group schemes with arrows reversed.

We have $A = R[X_1, \dots, X_n]/\langle f_i \rangle_i$ where f_i are a (finite, since R is assumed Noetherian) set of relations. The maps have a very simple description: the multiplication map is represented as

$$\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \begin{pmatrix} X_1' \\ \vdots \\ X_n' \end{pmatrix} = \begin{pmatrix} c_1(X_1, \dots, X_n, X_1', \dots, X_n') \\ \vdots \\ c_n(X_1, \dots, X_n, X_1', \dots, X_n') \end{pmatrix}$$

and hence the comultiplication map has

$$\begin{aligned} c : A \to A \otimes A &= R[X_1, \dots, X_n, X_1', \dots, X_n']/\langle f_i, f_i' \rangle_i \\ X_i &\mapsto c_i(X_1, \dots, X_n, X_1', \dots, X_n') \end{aligned}$$

for $1 \le i \le n$. Similarly, $e(X_i)$ gives the coordinates of the neutral element in A.

Examples of group schemes. Here are some examples of group schemes:

Example. The *multiplicative group* $\mathbb{G}_m$ is the affine scheme over R defined by the equation $XY = 1$ with group operation $(X, Y)(X', Y') = (XX', YY')$ [Tat, (2.4)]. The associated Hopf algebra

$$A = R[X, Y]/\langle XY - 1 \rangle \simeq R[X, 1/X],$$

has comultiplication $A \to A \otimes A$ by

$$\begin{aligned} R[X, Y]/\langle XY - 1 \rangle &\to R[U, V, U', V']/\langle UV - 1, U'V' - 1 \rangle \\ X, Y &\mapsto UU', VV' \end{aligned}$$

The identity map $A \to R$ is $X, Y \mapsto 1$ and the inverse map $A \to A$ is $X, Y \mapsto 1/X, 1/Y$.

Indeed, the association $\mathbb{G}_m(S) = S^\times$ is a functorial one. Since

$$\mathrm{Mor}_R(\operatorname{Spec} S, \mathbb{G}_m) = \mathrm{Hom}_R(R[T, 1/T], S) \simeq S^\times,$$

(any map is determined by the image of T, which must be invertible), we need only verify that the maps giving the group operations are correctly induced. We have comultiplication $S^\times \times S^\times \to S^\times$ which is dual to

$$\mathrm{Hom}_R(R[U, 1/U], S) \times \mathrm{Hom}_R(R[U', 1/U'], S) \leftarrow \mathrm{Hom}_R(R[T, 1/T], S).$$

We need to verify that $\phi \mapsto \phi \circ c$ arises from the group maps; this follows from

$$(\phi \circ c)(T) = \phi(UU') = \phi(U)\phi(U') = (\phi(U), \phi(U')).$$

Example. The *additive group* $\mathbb{G}_a = \operatorname{Spec} A$ where $A = R[X]$ under the group law of addition, neutral element 0 and inverse $X \mapsto -X$ is an affine group scheme [Tat, (2.4)]. The map $c : A = R[X] \to R[U, V] = A \otimes A$ is $X \mapsto U + V$, $e : R[X] \to R$ is $X \mapsto 0$, and inverse $i : R[X] \mapsto R[x]$ by $X \mapsto -X$. The functor it represents on R-algebras is the one that maps $S \mapsto S^+$, S treated as an additive group. One can verify functoriality as above.

Example. For *roots of unity* [Tat, (2.7)], we will represent the functor $S \mapsto \mu_n(S)$, the nth roots of unity in S under multiplication, by $\mu_n = \mathrm{Spec}(A)$, $A = R[T]/\langle T^n - 1\rangle$, so that $\mathrm{Hom}_R(A, S) \simeq \mu_n(S)$.

The group law is multiplication, so the Hopf algebra has composition $c : A \to A \otimes A$ taking $T \mapsto UV$, $e : A \to R$ taking $T \mapsto 1$, and $i : A \to A$ taking $T \mapsto T^{n-1} = T^{-1}$.

Example. If $\operatorname{char} R = p$, then $\alpha_p(S) = \{\alpha \in S : \alpha^p = 0\}$ is a group under addition, with $\alpha_p = \operatorname{Spec} A$, $A = R[T]/\langle T^p\rangle$ with the addition formulas as above.

Example. (See [Sha, §3, p.45].) The group of matrices $\begin{pmatrix} 1 & \alpha_p \\ 0 & \mu_p \end{pmatrix}$, i.e. matrices of the form

$$\left\{ \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} : x, y \in R,\ x^p = 0,\ y^p = 1 \right\}$$

is a group scheme when $\operatorname{char} R = p > 0$. We have

$$\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \begin{pmatrix} 1 & x' \\ 0 & y' \end{pmatrix} = \begin{pmatrix} 1 & x' + xy' \\ 0 & yy' \end{pmatrix}.$$

Since $(yy')^p = y^p y'^p = 1$ and $(x' + xy')^p = x'^p + x^p y'^p = 0$, this is a well-defined group operation. The corresponding algebra is $A = R[X, Y]/\langle X^p, Y^p - 1\rangle$, and the composition law is

$$\begin{aligned} A \to A \otimes A &= R[U, V, U', V']/\langle U^p, U'^p, V^p - 1, V'^p - 1\rangle \\ X, Y &\mapsto U' + UV', VV' \end{aligned}$$

This is an example of a *noncommutative* group ring (the formulas are not symmetric in U and V). The neutral map is $X, Y \mapsto 0, 1$ and the inverse map is $X, Y \mapsto -XY^{-1}, Y^{-1}$.

Rank and the augmentation ideal. We will be primarily interested with finite group schemes, for which we need the following definition.

Definition. G is called *finite of rank n (or order n)* if $G = \operatorname{Spec} A$ and A is a locally free R-algebra of rank n.

The ideal $I = \ker e$ is called the *augmentation ideal*.

(See [Tat, (2.3)] and [Wat, §2.1].)

Since we are assuming that R is locally noetherian, G is of finite order over $\operatorname{Spec} R$ iff it is finite and flat over $\operatorname{Spec} R$ [TO, §1].

Example. For example, μ_n has rank n, α_p has rank p, and the previous matrix algebra example has rank p^2.

Example. A finite (affine) group scheme of rank 1 has $G = \operatorname{Spec} A$, $R \to A \xrightarrow{e} R$ so $A \simeq R$, and $\operatorname{Hom}_R(A, S) = \operatorname{Hom}_R(R, S) = \{e\}$ so G is the *trivial group scheme.*

We will now determine finite group schemes of rank 2 (see [TO, p.1] and [Tat, (3.2)]). Let $G = \operatorname{Spec} A$, and suppose for simplicity that A is actually free of rank 2 over R. The splitting

$$R \to A \xrightarrow{e} R$$

gives $A \simeq I \times R$ as an R-module.

Exercise. *From the exact sequence*

$$0 \to I \to R \times R = A \xrightarrow{e} R \to 0,$$

show that the ideal I is generated by $e((1,0))(0,1) - e((0,1))(1,0)$ and that I is free of rank 1 over R.

Hence A must be $R[X]$ modulo a quadratic relation. Substituting $X - e(X)$ in for X, we may assume the quadratic polynomial vanishes at zero, and that $e(X) = 0$. We are left with

$$A \simeq R[X]/\langle X^2 + aX \rangle$$

for some $a \in R$. The group law is a morphism

$$R[T]/\langle T^2 + aT \rangle \to R[X, X']/\langle X^2 + aX, X'^2 + aX' \rangle$$

defined by $T \mapsto \alpha + \beta X + \gamma X' + \delta X X'$, say. The identity map $e : X, X' \mapsto 0$ tells us that $\alpha = 0$, $\beta = 1$ on $X' = 0$ and similarly $\gamma = 1$ for $X = 0$. Replace $b = \delta$, so that composition is $T \mapsto X + X' + bXX'$. But we must also have that

$$(X + X' + bXX')^2 + a(X + X' + bXX') = 0 \in A \otimes A.$$

Computing we find

$$-aX + 2XX' - aX' - 2abXX' - 2abXX' + a^2b^2XX' + aX + aX' + abXX' = 0$$

so that the coefficient of XX' must vanish:

$$2 - 3ab + a^2b^2 = (2 - ab)(1 - ab) = 0.$$

Associativity is always satisfied, so it gives no new information. However, if the inverse map $X \mapsto r + sX$ for some $r, s \in R$, then

$$X + (r + sX) + \delta X(r + sX) = 0 \in A;$$

thus the constant term $r = 0$ and thus the coefficient of X, $1 + s - abs = 0$, which implies $(1 - ab)s = -1$, a unit, so from the above we conclude $ab = 2$. Since $1 - ab = -1$, so $s = 1$, so $i(X) = X$. (Without the inverse map, we do not have a R-group scheme, but instead a monoid [Tat, (3.2)].)

Finally, one checks that these conditions are also sufficient.

Proposition. *The scheme $G_{a,b} = \operatorname{Spec} R[X]/\langle X^2 + aX \rangle$ with group law*

$$X \mapsto X + X' + bXX'$$

and $ab = 2$ is a group scheme.

One can show:

Exercise. *$G_{a,b} \simeq G_{a',b'}$ as group schemes iff $a = ua'$, $b = (1/u)b'$ for some $u \in R^\times$.*

Returning to the augmentation ideal, we prove [Tat, (2.3)]:

Lemma. *Let $G = \operatorname{Spec} A$ be a group scheme over R and $I = \ker e$ so that*

$$0 \to I \to A \xrightarrow{e} R \to 0$$

is exact. If $f \in I$ then we have

$$c(f) = 1 \otimes f + f \otimes 1 \pmod{I \otimes I}.$$

Proof. By the commutative diagram for e, $(e \otimes \mathrm{id}_A) \circ c = 1 \otimes \mathrm{id}_A$. Therefore if

$$c(f) = \alpha + \beta + \gamma + \delta \in A \otimes A$$

with $\alpha \in R \otimes R$, $\beta \in R \otimes I$, $\gamma \in I \otimes R$, and $\delta \in I \otimes I$, then

$$((e \otimes \mathrm{id}_A) \circ c)(f) = \alpha + \beta = (1 \otimes \mathrm{id})(f) \pmod{I \otimes I}$$

so that $\alpha = 0$, $\beta = 1 \otimes f$. Similarly, applying $\mathrm{id}_A \otimes e$ we find $\gamma = f \otimes 1$. □

This lemma says that if $A = R[X_1, \ldots, X_n]/\langle f_i \rangle_i$ with the generators chosen so that the neutral element is at the origin (and thus $X_i \in I$), then

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \begin{pmatrix} x_1' \\ \vdots \\ x_n' \end{pmatrix} \equiv \begin{pmatrix} x_1 + x_1' \\ \vdots \\ x_n + x_n' \end{pmatrix} \pmod{I \otimes I}.$$

Corollary. *$c(I) \subset I \otimes A + A \otimes I$.*

Subgroup schemes, morphisms and kernels. We define the following:

Definition. A *closed subgroup scheme* H is $H = \operatorname{Spec}(A/J) \hookrightarrow G = \operatorname{Spec} A$, where H is a group scheme with the multiplication and identity morphisms induced from that of G.

This definition implies that $c : A \to A \otimes A$ induces a well-defined comultiplication map

$$c : A/J \to A/J \otimes A/J = (A \otimes A)/(A \otimes J + J \otimes A),$$

i.e. $c(J) \subset J \otimes A + A \otimes J$. We insist that $J \subset I$ (to exclude for example the unit ideal), and we say J is a *Hopf ideal*. It follows that this holds for the inverse map as well.

Note I itself is a Hopf ideal corresponding to the trivial subgroup of G.

Example. μ_n is a closed subgroup scheme of $\mathbb{G}_m$. Since $\mathbb{G}_m = \operatorname{Spec} R[T, 1/T]$, $\mu_n = \operatorname{Spec} R[T]/\langle T^n - 1 \rangle$, we have for $J = \langle T^n - 1 \rangle$ that

$$c(T^n - 1) = (UV)^n - 1 = (U^n - 1)(V^n - 1) + (U^n - 1) + (V^n - 1) \subset J \otimes A + A \otimes J.$$

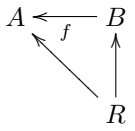
Example. α_p is a closed subgroup scheme of $\mathbb{G}_a$.

Definition. A map $f : G \to H$ is a *(homo)morphism of group schemes* if it is a morphism of schemes such that

$$\begin{array}{ccc} G \times G & \xrightarrow{c_G} & G \\ \downarrow{\scriptstyle f \times f} & & \downarrow{\scriptstyle f} \\ H \times H & \xrightarrow{c_H} & H \end{array}$$

commutes.

By functoriality, we have if $G = \operatorname{Spec} A$ and $H = \operatorname{Spec} B$ that

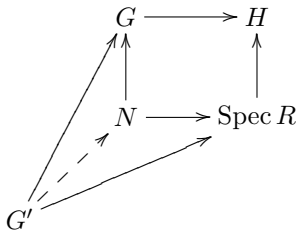


and therefore we find $(f \otimes f) \circ c_B = c_A \circ f$, $e_A \circ f = e_B$, and $i_A \circ f = f \circ i_B$ on the level of Hopf algebras. (See also [Wat, §2.1].)

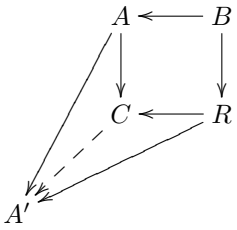
Definition. The *kernel* $\ker(G \xrightarrow{f} H) = N$ (as a functor) is

$$N(S) = \ker G(S) \xrightarrow{f_S} H(S).$$

This functor is representable [Tat, (1.7)], and it has the universal property described by the following diagram:



which by algebras shows us that if $N = \operatorname{Spec}(C)$ then we have the universal diagram:



This is the universal property of the tensor product, so

$$C = A \otimes_B R = A \otimes_B (B/I_B) = A/f(I_B)A,$$

and we conclude that $N = \operatorname{Spec} A/f(I_B)A$.

We now should verify that $f(I_B)A$ is a Hopf ideal, so that N is a closed subscheme: we have

$$\begin{aligned} c(f(I_B)A) = (f \otimes f)(c(I_B)A) &\subset (f \otimes f)\left((I_B \otimes B + B \otimes I_B)A\right) \\ &\subset f(I_B)A \otimes A + A \otimes f(I_B)A. \end{aligned}$$

Example. The map $\mathbb{G}_m \xrightarrow{n} \mathbb{G}_m$ by $x \mapsto x^n$ is a homomorphism. At the level of Hopf algebras, we have

$$\begin{array}{ccc} R[X, 1/X] & \xleftarrow[n]{} & R[X, 1/X] \\ \downarrow & & \downarrow \\ R[X]/\langle X^n - 1\rangle & \longleftarrow & R \end{array}$$

since $R[X]/\langle X^n - 1\rangle \simeq R[X, 1/X] \otimes_R R[X]/\langle X^n - 1\rangle$.

The definition of the cokernel is much harder, and we will take it up at another time.

Diagonalizable group schemes. (See also [Wat, §2.2].) If Γ is a finitely generated abelian group, we have a group ring

$$R[\Gamma] = \{\textstyle\sum_\gamma \alpha_\gamma \gamma : \alpha_\gamma \in R\}.$$

This is a Hopf algebra in a natural way [Tat, (2.6)], which is to say $\mathrm{Hom}_R(R[\Gamma], S)$ for $G = \mathrm{Spec}(R[\Gamma])$, obtained from $\mathrm{Mor}_R(\mathrm{Spec}\, S, G)$, is a group in a natural way: since

$$\mathrm{Hom}_R(R[\Gamma], S) \simeq \mathrm{Hom}(\Gamma, S^\times),$$

the group operation is $(fg)(\gamma) = f(\gamma)g(\gamma)$.

One can check that the group morphisms are given by

$$\begin{aligned} c : R[\Gamma] &\to R[\Gamma] \otimes R[\Gamma] \\ \gamma &\mapsto \gamma \otimes \gamma, \end{aligned}$$

$e : R[\Gamma] \to R$ by $\gamma \mapsto 1$, and $i : R[\Gamma] \to R[\Gamma]$ by $\gamma \mapsto \gamma^{-1}$. This verification is exactly as above for the functoriality of the multiplicative group scheme: to check that c induces the natural group law on $\mathrm{Hom}(\Gamma, S^\times)$, we write

$$\mathrm{Hom}_R(\Gamma, S^\times) \times \mathrm{Hom}_R(\Gamma, S^\times) \to \mathrm{Hom}_R(\Gamma, S^\times)$$

is

$$\mathrm{Hom}_R(R[\Gamma], S) \times \mathrm{Hom}_R(R[\Gamma], S) \simeq \mathrm{Hom}_R(R[\Gamma] \otimes R[\Gamma], S) \to \mathrm{Hom}_R(R[\Gamma], S)$$

so for a chosen γ, we compute that $\phi(\gamma) = (\phi \circ c)(\gamma \otimes \gamma) = \phi(\gamma)$.

Example. If $\Gamma = \mathbb{Z}$, $R[\Gamma] \simeq R[\mathbb{Z}] = R[T, 1/T]$ and we recover $\mathbb{G}_m$; if $\Gamma = \mathbb{Z}/n\mathbb{Z}$, $R[\Gamma] = R[T]/\langle T^n - 1\rangle$, and we recover μ_n.

Since $\Gamma \simeq \mathbb{Z}^r \times \prod_{i=1}^s \mathbb{Z}/m_i\mathbb{Z}$, we have

$$R[\Gamma] \simeq R[X_1, \ldots, X_r, Y_1, \ldots, Y_s, 1/X_1, \ldots, 1/X_r]/\langle Y_1^{m_1} - 1, \ldots, Y_s^{m_s} - 1\rangle,$$

and the coordinatized multiplication is just

$$\begin{pmatrix} X_1 \\ \vdots \\ X_r \\ Y_1 \\ \vdots \\ Y_s \end{pmatrix} \begin{pmatrix} X_1' \\ \vdots \\ X_r' \\ Y_1' \\ \vdots \\ Y_s' \end{pmatrix} = \begin{pmatrix} X_1X_1' \\ \vdots \\ X_rX_r' \\ Y_1Y_1' \\ \vdots \\ Y_sY_s' \end{pmatrix}$$

with neutral element

$$e = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

Constant group schemes. (See also [Wat, §2.3].) Let Γ be a finite group, and denote [Tat, (2.10)]

$$R^{(\Gamma)} = \underbrace{R \times \cdots \times R}_{\#\Gamma} = R[e_\gamma]_{\gamma\in\Gamma}.$$

The $e_\gamma = (0, \ldots, 1, \ldots, 0)$ (in the γ slot) form an orthogonal system of idempotents of $R^{(\Gamma)}$, since $e_\gamma^2 = e_\gamma$ and $e_\gamma e_{\gamma'} = 0$ if $\gamma \neq \gamma'$, and $\sum_\gamma e_\gamma = 1$.

We have for a decomposition of $S = \prod_i S_i$ into connected components (i.e. $\operatorname{Spec} S_i$ is connected, which is to say the only idempotents in S_i are 0 and 1),

$$\operatorname{Hom}_R(R^{(\Gamma)}, S) = \operatorname{Hom}_R(R^{(\Gamma)}, \textstyle\prod_i S_i) = \prod_i \operatorname{Hom}_R(R^{(\Gamma)}, S_i);$$

since e_γ must map to an idempotent element of S_i (hence 0 or 1) and must also satisfy the mutual orthogonality relation, we find that the position where $e_\gamma \mapsto 1$ uniquely determines the map, and thus

$$\operatorname{Hom}_R(R^{(\Gamma)}, S) \simeq \textstyle\prod_i \Gamma.$$

We define the map

$$\begin{aligned} c : R^{(\Gamma)} &\to R^{(\Gamma)} \otimes R^{(\Gamma)} \\ e_\gamma &\mapsto \sum_{\sigma\tau=\gamma} e_\sigma \otimes e_\tau \end{aligned}$$

and $e : R^{(\Gamma)} \to R$ by $e_1 \mapsto 1, e_\gamma \mapsto 0$ for $\gamma \neq 1$, and $i : R^{(\Gamma)} \to R^{(\Gamma)}$ by $e_\gamma \mapsto e_{\gamma^{-1}}$.

One can verify that these maps are compatible (functorial) as follows. If $\operatorname{Spec} S$ is connected, then $\operatorname{Hom}_R(R^{(\Gamma)}, S) \simeq \Gamma$, so the law $\Gamma \times \Gamma \to \Gamma$ is supposed to be induced by

$$\begin{aligned} \operatorname{Hom}_R(R^{(\Gamma)} \otimes R^{(\Gamma)}, S) &\to \operatorname{Hom}_R(R^{(\Gamma)}, S) \\ \phi &\mapsto \phi \circ c; \end{aligned}$$

We must match idempotents, hence any such morphism is of the form $f_\gamma : e_\gamma \mapsto 1$, $e_{\gamma'} \mapsto 0$ for $\gamma' \neq \gamma$. If we let $(f_\gamma, f_{\gamma'}) = (\phi, \phi')$ on coordinates, then

$$(\phi \circ c)(\gamma'') = \sum_{\sigma\tau=\gamma'} f_\gamma(e_\sigma) f_{\gamma'}(e_\tau) = \begin{cases} 1, & \gamma'' = \gamma\gamma'; \\ 0, & \text{else} \end{cases}$$

by mutual orthogonality, and hence $\phi \circ c = f_{\gamma''} = f_{\gamma\gamma'}$ as needed.

In terms of coordinates,

$$R^{(\Gamma)} = R[X_\gamma]_{\gamma\neq 1} / \langle X_\gamma^2 - X_\gamma, X_\gamma X_{\gamma'} \rangle_{\gamma\neq\gamma'\in\Gamma},$$

with $e = (1, 0, \ldots, 0)$.

Exercises. The following are exercises for §2.

Problem 2.1. The group functor $R \mapsto SL_2(R)$ on the category of commutative rings ($\mathbb{Z}$-algebras) is representable by a group scheme $G = \operatorname{Spec} A$. Describe the Hopf algebra A: give the ring structure and the comultiplication, coinverse, and counit morphisms.

Problem 2.2. Let $G = \operatorname{Spec} A$ be an R-group scheme with comultiplication morphism $c : A \to A \otimes A$, counit $e : A \to R$ and coinverse $i : A \to A$.

(a) Show that the diagonal morphism $G \to G \times G$ corresponds to the algebra multiplication map $m : A \otimes A \to A$.

(b) Show that $m \circ (i \otimes \mathrm{id}_A) \otimes c = e$.
(c) Show that if $m \circ c = e$, then G is commutative.

Problem 2.3. Let R be a ring.

(a) Show that there are no nontrivial homomorphisms from $\mathbb{G}_m$ to $\mathbb{G}_a$.
(b) If R is reduced, show that there are no nontrivial homomorphisms from $\mathbb{G}_a$ to $\mathbb{G}_m$.
(c) For each $\epsilon \in R$ with $\epsilon^2 = 0$, construct a nontrivial homomorphism from $\mathbb{G}_a$ to $\mathbb{G}_m$.

Problem 2.4. Let $A = \mathbb{Z}[X]/\langle X^2 - X\rangle$.

(a) Show that $G = \operatorname{Spec} A$, with multiplication law $X + X' - 2XX'$, neutral element given by $X = 0$, and inverse of X given by X, is a group scheme.
(b) Show that G is isomorphic to the constant group scheme $\mathbb{Z}/2\mathbb{Z}$.
(c) Show that the morphism $G \to \mu_2$ given by $X \mapsto 1-2X$ is a homomorphism of group schemes.
(d) Determine the kernel of the homomorphism of part (c).

Problem 2.5. Let k be a field of characteristic $p > 0$.

(a) Show that for every k-algebra S the map given by $x \mapsto 1 + x$ induces a bijection $\alpha_p(S) \to \mu_p(S)$.
(b) Show that the group schemes μ_p and α_p are not isomorphic over k.

Problem 2.6.

(a) Let k be a field of characteristic $p > 0$. Show that the k-algebra homomorphism $k[T] \to k[T]$ given by $T \mapsto T^p - T$ induces a morphism $g : \mathbb{G}_a \to \mathbb{G}_a$.
(b) Show that the kernel of g is isomorphic to the constant group scheme $\mathbb{Z}/p\mathbb{Z}$.

Problem 2.7. Let R be a ring whose only idempotents are 0 and 1. Let Γ be a finite commutative group and let $A = R^{(\Gamma)}$ denote the Hopf algebra of the corresponding constant group scheme. Determine the elements $a \in A^\times$ for which $c(a) = a \otimes a$. Here $c : A \to A \otimes A$ denotes the comultiplication map of A.

Problem 2.8. Let R be a ring and let F be the functor for which $F(S) = \{(x, y) \in S \times S : x^2 + y^2 = 1\}$ for an R-algebra S.

(a) Show that the functor F is represented by the R-algebra $R[X, Y]/\langle X^2 + Y^2 - 1\rangle$.
(b) Show that the composition rules $F(S) \times F(S) \to F(S)$ given by
$$(x, y) + (x', y') = (xx' - yy', xy' + yx')$$
induce natural group structures on the sets $F(S)$.
(c) Determine the group scheme structure of $G = \operatorname{Spec}(R[X, Y]/\langle X^2+Y^2-1\rangle)$ that induces the group laws of part (b).
(d) If there exists an element $i \in R$ for which $i^2 = -1$, then the maps $G(S) \to S^\times$ given by $(x, y) \mapsto x + iy$ are induced by a homomorphism of group schemes $j : G \to \mathbb{G}_m$. Prove this. Show that j is an isomorphism iff $2 \in R^\times$.

Problem 2.9. Let R be a ring and let F be the functor that associates to each R-algebra S the set of its idempotent elements.

(a) Show that the functor F is represented by the R-algebra $R[X]/\langle X^2 - X\rangle$.
(b) Show that the maps $F(S) \times F(S) \to F(S)$ given by $(e, e') \mapsto e + e' - 2ee'$ induce natural group structures on the sets $F(S)$.
(c) Show that $G = \operatorname{Spec} R[X]/\langle X^2 - X\rangle$ has a group scheme structure that induces the group laws of part (b).
(d) Prove that G is isomorphic to the constant group scheme $\mathbb{Z}/2\mathbb{Z}_R$.

3. Duality and Deligne's theorem

Cartier duality. Let $G = \operatorname{Spec} A$ be commutative (the formula for composition is symmetric). Assume that A is a finite flat algebra over R (e.g. $R^{(\Gamma)}$ and $R[\Gamma]$ when Γ is finite and commutative). Let $A^\vee = \operatorname{Hom}_R(A, R)$. This is an R-module by

$$(\lambda f)(a) = \lambda f(a) = f(\lambda a)$$

for $\lambda \in R$, $a \in A$.

If A is free,

$$\operatorname{Hom}_R(A \otimes A, R) \simeq \operatorname{Hom}_R(A, R) \times \operatorname{Hom}_R(A, R)$$

since A is flat and R is noetherian, so A is projective. Therefore $(A \otimes A)^\vee \simeq A^\vee \otimes A^\vee$.

If A is a Hopf algebra, we have the following R-algebra homomorphisms:

$$\begin{aligned} m &: A \otimes A \to A \\ c &: A \to A \otimes A \\ & R \to A \\ e &: A \to R \\ i &: A \to A \end{aligned}$$

where m is the algebra multiplication map, and $R \to A$ is the structure map. Notice the nice symmetry in this situation. Dualizing, we obtain maps

$$\begin{aligned} m^\vee &: A^\vee \to A^\vee \otimes A^\vee \\ c^\vee &: A^\vee \otimes A^\vee \to A^\vee \\ & A^\vee \to R \\ e^\vee &: R \to A^\vee \\ i^\vee &: A^\vee \to A^\vee \end{aligned}$$

Theorem (Cartier)**.** *With these homomorphisms, $A^\vee$ becomes an R-Hopf algebra with $A^\vee$ finite and flat over R. $G^\vee = \operatorname{Spec} A^\vee$ is called the* dual group scheme.

Moreover, for any R-algebra S,

$$G^\vee(S) = \operatorname{Hom}_S^{\mathbf{Sch}}(G/S, \mathbb{G}_m/S) = \operatorname{Hom}_S^{\mathbf{Hopf}}(S[T, 1/T], A \otimes S),$$

an equality of morphisms of group schemes and Hopf algebra homomorphisms.

Proof. (See also [Tat, (3.8)], [Wat, §2.4], [Sha, §4].) We need to reverse arrows in diagrams and check for compatibility. Almost all of these follow immediately; but to check that $i^\vee$ is an algebra homomorphism, we need the commutativity of the

diagram

$$\begin{array}{ccc} A^\vee \otimes A^\vee & \xrightarrow{c^\vee} & A^\vee \\ \downarrow{\scriptstyle i^\vee \otimes i^\vee} & & \downarrow{\scriptstyle i^\vee} \\ A^\vee \otimes A^\vee & \xrightarrow{c^\vee} & A^\vee \end{array}$$

so we dualize and obtain

$$\begin{array}{ccc} A \otimes A & \xleftarrow[c]{} & A \\ \uparrow{\scriptstyle i \otimes i} & & \uparrow{\scriptstyle i} \\ A \otimes A & \xleftarrow[c]{} & A \end{array}$$

and invoke the antiequivalence of categories

$$\begin{array}{ccc} G \times G & \xrightarrow{c} & G \\ \downarrow{\scriptstyle i \times i} & & \downarrow{\scriptstyle i} \\ G \times G & \xrightarrow{c} & G \end{array}$$

which is commutative iff $(gh)^{-1} = g^{-1}h^{-1}$, i.e. we need that the group scheme is commutative.

We also, for example, need to check that $c^\vee$ makes $A^\vee$ into a (commutative) R-algebra, which also needs underlying commutativity:

$$\begin{array}{ccc} A^\vee \otimes A^\vee & \xrightarrow{c^\vee} & A^\vee \\ \downarrow\uparrow & & \| \\ A^\vee \otimes A^\vee & \xrightarrow{c^\vee} & A^\vee \end{array}$$

gives rise to

$$\begin{array}{ccc} A \otimes A & \xleftarrow[c]{} & A \\ \uparrow\downarrow & & \| \\ A \otimes A & \xleftarrow[c]{} & A \end{array}$$

and finally

$$\begin{array}{ccc} G \times G & \xrightarrow{c} & G \\ \downarrow\uparrow & & \| \\ G \times G & \xrightarrow{c} & G \end{array}$$

where the map $\wr$ interchanges the two coordinates. This last diagram commutes iff $gh = hg$.

Now we must check the final statement regarding functoriality of the S-valued points, that $G^\vee(S) = \mathrm{Hom}_R(A^\vee, S)$. We need to check that

$$\mathrm{Hom}_R^{\mathbf{Alg}}(\mathrm{Hom}_R^{\mathbf{Mod}}(A, R), S) \simeq \mathrm{Hom}_S^{\mathbf{Hopf}}(S[T, 1/T], A \otimes S)$$

where this is interpreted as R-algebra homomorphisms of R-module homomorphisms isomorphic to Hopf algebra homomorphisms. By the universal property of the tensor product,

$$\mathrm{Hom}_S(\mathrm{Hom}_S(A \otimes S, S), S) \simeq \mathrm{Hom}_R(\mathrm{Hom}_R(A, R), S),$$

we may assume $R = S$.

We want to show that

$$\mathrm{Hom}_R(\mathrm{Hom}_R(A,R),R) \simeq \mathrm{Hom}_R(R[T,1/T],A) = \{a \in A^\times : c(a) = a \otimes a\} \subset A^\times,$$

where the equality on the left gives compatibility with the composition law. The left-hand side can be viewed as the set of elements $a \in A$ such that $\phi \mapsto \phi(a)$ is an R-algebra homomorphism (for a finite module, the dual of the dual is canonically isomorphic with the module itself). We want therefore that $(\phi\psi)(a) = \phi(a)\psi(a)$ for all $\phi, \psi \in A^\vee$; but

$$(\phi\psi)(a) = ((\phi \otimes \psi) \circ c)(a) = \phi(a)\psi(a) = (\phi \otimes \psi)(a \otimes a)$$

iff $c(a) = a \otimes a$.

The unit element of the R-algebra $\mathrm{Hom}(A,R)$ e (arising from the structure morphism) must map to the unit element of R, so $e \mapsto 1$, so $e(a) \mapsto 1$. The inverse axiom gives $m \circ (\mathrm{id}_A \otimes i) \circ c = e$ so we have $m(a \otimes i(a)) = ai(a) = 1$, so a is a unit, so actually $G^\vee(R) \subset A^\times$, which completes the proof. □

Here are some examples of duality:

Example. The dual of μ_n, if we write R for S, is given by

$$\mathrm{Hom}_R(\mu_n, \mathbb{G}_m) \simeq \mathrm{Hom}_R(R[T,1/T], R[X]/\langle X^n - 1\rangle)$$

by $T \mapsto p(X)$ with $p(U)p(V) = p(UV)$. If we let $p(X) = \sum_{i=0}^{n-1} a_i X^i$ for $a_i \in R$, this says that

$$\sum_{i=0}^{n-1} a_i (UV)^i = \left(\sum_{i=0}^{n-1} a_i U^i\right)\left(\sum_{i=0}^{n-1} a_i V^i\right)$$

in $R[U,V]/\langle U^n - 1, V^n - 1\rangle$. So looking at the coefficients of crossterms we find $a_i a_j = 0$ when $i \neq j$, and on diagonal terms we have $a_i = a_i^2$, and since $\phi(1) = \phi(1)\phi(1)$, we have $\phi(1) = 1$, and therefore $\sum_i a_i = 1$. Therefore the a_i are orthogonal idempotents.

Hence the a_i are a point in the constant scheme $(\mathbb{Z}/n\mathbb{Z})_R = \mathrm{Spec}\, R^{(\mathbb{Z}/n\mathbb{Z})}$, and therefore this scheme is dual to μ_n.

If $R = S$ is connected, then

$$\begin{aligned}\mathrm{Hom}_R(R[T,1/T], R[X]/\langle X^n - 1\rangle) &= \{\phi(X) : \phi(UV) = \phi(U)\phi(V)\} \\ &= \{\phi_i = X_i : 0 \le i \le n-1\},\end{aligned}$$

and indeed $\phi_i(X)\phi_j(X) = X^{i+j} = \phi_{i+j}(X)$ matches the group law.

Example. We have $(G_1 \times G_2)^\vee \simeq G_1^\vee \times G_2^\vee$. So the diagonalizable group scheme $\mathrm{Spec}(R[\Gamma])$ for Γ finite and commutative is dual to the constant scheme $\Gamma = \mathrm{Spec}(R^{(\Gamma)})$.

Example. For α_p, $\mathrm{char}\, R = p$, where $\alpha_p(S) = \{s \in S : s^p = 0\}$ under addition, the dual is

$$\begin{aligned}\mathrm{Hom}_R(\alpha_p, \mathbb{G}_m) &= \mathrm{Hom}_R(R[T,1/T], R[X]/\langle X^p\rangle) \\ &= \{\phi(X) \in R[X]/\langle X^p\rangle : \phi(U+V) = \phi(U)\phi(V)\}.\end{aligned}$$

This implies that if $\phi(X) = \sum_{i=0}^{p-1} a_i X^i$ then

$$\sum_{i=0}^{p-1} a_i (U+V)^i = \left(\sum_{i=0}^{p-1} a_i U^i\right)\left(\sum_{i=0}^{p-1} a_i V^i\right)$$

so $a_0 = 1$, a_1 is a free parameter, and if the the characteristic p is sufficiently large, we have by the UV term that $2a_2 = a_1^2$, so $a_2 = a_1^2/2!$, and by the U^2V term that $3a_3 = a_1a_2$ so $a_3 = a_1^3/3!$, and continuing in this way $a_k = a_1^k/k!$ for $k \leq p-1$. By the coefficient $U^{p-1}V$ we find $a_1^p = 0$, so $\phi(U) = \exp(aU)$ with $a^p = 0$, which corresponds to a point in $\alpha_p(R)$. Hence

$$\exp(aU)\exp(a'U) = \exp((a+a')U)$$

and α_p is self-dual.

Example. For the (free) group schemes of order 2, namely

$$G_{a,b} = \operatorname{Spec} R[X]/\langle X^2 + aX\rangle$$

under $X \mapsto X + X' + bXX'$, $ab = 2$, the dual is

$$\begin{aligned}&\operatorname{Hom}_R(R[T,1/T], R[X]/\langle X^2+aX\rangle)\\ &\quad = \{\phi(X) \in R[X]/\langle X^2+aX\rangle : \phi(X+X'+bXX') = \phi(X)\phi(X')\}.\end{aligned}$$

since $\phi(0) = 1$, $\phi = 1 - \epsilon X$ for some $\epsilon \in R$, and

$$1 - \epsilon(X + X' + bXX') = (1-\epsilon X)(1-\epsilon X')$$

hence $-\epsilon b = \epsilon^2$, and $\epsilon^2 + \epsilon b = 0$. In other words, $\epsilon \in R[X]/\langle X^2 + bX\rangle$, and then

$$(1-\epsilon X)(1-\epsilon' X) = 1 - \epsilon X - \epsilon' X + \epsilon\epsilon'(-aX) = 1 - (\epsilon + \epsilon' + a\epsilon\epsilon')X,$$

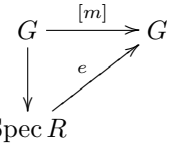
so that $G_{a,b}^\vee \simeq G_{b,a}$.

Deligne's theorem. The goal of the following sections is to prove (see [TO, §1]):

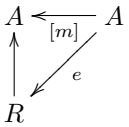
Theorem (Deligne)**.** *If G is a finite flat commutative group scheme over R, so that $G = \operatorname{Spec} A$, A flat of finite rank m, then $[m]$ annihilates G, that is, repeating the group law m times gives a form vanishing identically on the scheme (the neutral element).*

Example. For $G = \mu_n$, a point in $\mu_n = \operatorname{Spec} R[X]/\langle X^n - 1\rangle$ has $X \xrightarrow{n} X^n = 1$, the neutral element.

$[m] : G \to G$ is the repetition of the group law on an element m times, and is dual to $[m] : A \leftarrow A$. To say that it kills G is to say it factors



or



but in this case $I = \ker e \subset \ker[m]$, so it is enough to show $[m](I) = 0$.

We may assume that R is local (because of the flatness condition, if it is zero locally, it is zero globally), so that A is free over R. Recall that

$$G(R) \subset A^\vee, \quad G(S) \subset A^\vee \otimes S \simeq (A \otimes S)^\vee,$$

so by dualizing, we have $G^\vee(R) \subset A$, where

$$G^\vee(R) = \mathrm{Hom}_R^{\mathbf{Alg}}(\mathrm{Hom}_R^{\mathbf{Mod}}(A, R), R) = \{a \in A : c(a) = a \otimes a\}$$

Since we may assume S is finite and free over R, we have:

Lemma. *We have a map*

$$G(R) \longrightarrow G(S) \xrightarrow{N} G(R)$$

Proof. We must construct this latter map. Define $N : S \to R$ as follows: for any $s \in S$, $N(s)$ is the determinant of the multiplication by s map $S \to S$, an element of R. By the properties of determinant, $N(ss') = N(s)N(s')$. For any R-algebra we have a norm

$$S \otimes A \xrightarrow{N} R \otimes A$$

viewing $S \otimes A$ as a free $R \otimes A$-algebra.

We have

$$\begin{array}{ccc} G(S) & \longrightarrow & A^\vee \otimes S \\ \vdots & & \downarrow N \\ G(R) & \longrightarrow & A^\vee \end{array}$$

where the claim is that the norm N maps $G(S)$ to $G(R)$.

Claim. If $f : B \to C$ is a homomorphism of R-algebras, then

$$\begin{array}{ccc} B \otimes S & \xrightarrow{f \otimes \mathrm{id}_S} & C \otimes S \\ \downarrow N & & \downarrow N \\ B & \xrightarrow{f} & C \end{array}$$

is commutative.

Proof of claim. Let e_i be a basis for S over R, so that $1 \otimes e_i$ are a B-basis for $B \otimes S$ and a C-basis for $C \otimes S$. If $\alpha \in B \otimes S$,

$$\alpha(1 \otimes e_i) = \textstyle\sum_j \mu_{ij}(1 \otimes e_j)$$

for $\mu_{ij} \in B$ so $N(\alpha) = \det(\mu_{ij})$.

Hence

$$f(\alpha)(1 \otimes e_i) = \textstyle\sum_j f(\mu_{ij})(1 \otimes e_j)$$

and $N(f(\alpha)) = \det(f\mu_{ij}) = f(N(\alpha))$. □

We apply this to $A^\vee \xrightarrow{\mathrm{id}_A \otimes 1} A^\vee \otimes A^\vee$ by substitution into the first coordinate, then $N(f \otimes 1) = N(f) \otimes 1$. If we apply this to $A^\vee \xrightarrow{c^\vee} A^\vee \otimes A^\vee$, we find $N(c^\vee f) = c^\vee(N(f))$.

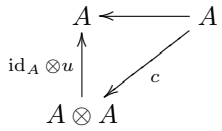
If $f \in G(S)$, then f is a unit and $c^\vee(f) = f \otimes f$. Hence $N(f)$ is also a unit, and we verify

$$\begin{aligned} c^\vee(N(f)) = N(c^\vee(f)) = N(f \otimes f) &= N(1 \otimes f)N(f \otimes 1) \\ &= (N(f) \otimes 1)(1 \otimes N(f)) = N(f) \otimes N(f). \end{aligned}$$

This proves the lemma. □

Proof of theorem. It is enough to show that $G(R)$ is killed by $[m]$. Let $u \in G(R) \subset A^\vee$ be a section. We have $c(u) = u \otimes u$, so $[m]u = u^m$, and we want to show that $u^m = 1$.

For $u \in G(R) = \mathrm{Hom}_R(A, R)$, we have the composition map $G(R) \to G(A) \xrightarrow{N} G(R)$. From the map $G(R) \to G(S)$, we may lift u, and we obtain a map $G(S) \to G(S)$ for every S, which is translation by u in the group. By the Yoneda lemma, these come from a map on the corresponding algebras, namely



because it is obtained from

$$\begin{array}{ccc} G(A) = \mathrm{Hom}_R(A, A) & \twoheadrightarrow & A^\vee \otimes A \\ \downarrow N & & \downarrow N \\ G(R) = \mathrm{Hom}_R(A, R) & \longrightarrow & A^\vee \end{array}$$

where the top map is the isomorphism $f \otimes a \mapsto (b \mapsto af(b))$. Therefore this translation $\tau : A \to A$ is the composition $a \mapsto ((\mathrm{id}_A \otimes u) \circ c)(a)$.

Now if we extend $A^\vee$ linearly to $A^\vee \otimes A$, we have

$$\tau(f \otimes \beta) = f \otimes \tau(\beta)$$

and for $a = \sum_i r_i \otimes e_i$ for e_i an R-basis for A, we have

$$\tau(a) = \textstyle\sum_i r_i \otimes \tau(e_i)$$

which implies $N(a) = N(\tau(a))$ and hence $N(\mathrm{id}_A) = N(\tau(\mathrm{id}_A))$.

For $\mathrm{id}_A \in G(A)$, we have

$$\tau(\mathrm{id}_A) = u\,\mathrm{id}_A \in G(A),$$

since $((\mathrm{id}_A \otimes u) \circ c)(a) = \tau(\mathrm{id}_A)(a)$.

Finally, since $N(u) = u^m$, we have

$$N(\mathrm{id}_A) = N(u\,\mathrm{id}_A) = N(u)N(\mathrm{id}_A) = u^m N(\mathrm{id}_A)$$

so since $N(\mathrm{id}_A)$ is invertible, u is killed by m. □

This theorem is still unknown in full generality when G is not commutative, but we can check it in certain cases:

Example. For G the set of matrices $\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix}$ with $x^p = 0$, $y^p = 1$, we have

$$A = R[X, Y]/\langle X^p, Y^p - 1\rangle$$

of rank p^2. We indeed find

$$\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix}^{p^2} = \begin{pmatrix} 1 & x(1 + y + \cdots + y^{p^2-1}) \\ 0 & y^{p^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

since $y^p = 1$ and R has characteristic p.

Exercises. The following are exercises for §3.

Problem 3.1. Let k be a field of characteristic $p > 0$ and let $W(X, Y)$ denote the polynomial $((X + Y)^p - X^p - Y^p)/p \in \mathbb{Z}[X, Y]$.

(a) Show that the k-scheme $\mathrm{Spec}(k[X, Y]/\langle X^p, Y^p\rangle)$ with group law given by $(x, y) + (x', y') = (x + x', y + y' - W(x, x'))$ is a group scheme.
(b) Compute the Cartier dual of α_{p^2}; show it is isomorphic to the group scheme of part (a). Here α_{p^2} denotes the closed subgroup scheme of $\mathbb{G}_a$ given by $\alpha_{p^2}(R) = \{x \in R : x^{p^2} = 0\}$ for any k-algebra R.

4. Étale schemes

Differentials. For background on differentials, consult [Wat, §11.1], [Mat, §26], or [Tat, (2.11)].

If R is our base ring, A an R-algebra, and M an A-module, then

$$\mathrm{Der}_R(A, M) = \{D : A \to M : R\text{-linear}, D(ab) = aD(b) + bD(a)\}.$$

As a consequence, $D(r) = 0$ for all $r \in R$. We have

$$\mathrm{Der}_R(A, M) \simeq \mathrm{Hom}_A(\Omega^1_{A/R}, M)$$

for a universal object $\Omega^1_{A/R}$, called the *Kähler differentials* [Mat, §26, Proposition, p.182], given by

$$\Omega^1_{A/R} = \textstyle\bigoplus_{a\in A} A\, da/\langle d(a + b) - da - db,\ d(ab) - a\, db - b\, da,\ dr\rangle.$$

In the case that $A = R[X_1, \ldots, X_n]/\langle f_i\rangle_i$ is a finitely generated R-algebra, then

$$\Omega^1_{A/R} = \textstyle\bigoplus_{i=1}^n A\, dX_i/\langle \sum_{j=1}^n (\partial f_i/\partial X_j)\, dX_j\rangle.$$

We find [Wat, §11.2]

$$\Omega^1_{(A\otimes S)/S} \simeq \Omega^1_{A/R} \otimes S,$$

and that

$$\Omega^1_{(A\times B)/S} \simeq \Omega^1_{A/S} \times \Omega^1_{B/S}.$$

Example. If we let $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/\langle X^2 + 1\rangle$, we have

$$\Omega^1_{\mathbb{Z}[i]/\mathbb{Z}} = \mathbb{Z}[i]\, dX/\langle 2X\, dX\rangle \simeq \mathbb{Z}[i]/\langle 2i\rangle.$$

From the map $A \to \Omega^1_{A/R}$ by $a \mapsto da$, we have

$$\begin{array}{ccc} A & \xrightarrow{\delta} & M \\ \downarrow{\scriptstyle d} & \nearrow & \\ \Omega^1_{A/R} & & \end{array}$$

So that $\mathrm{Hom}_A(\Omega^1_{A/R}, M) \simeq \mathrm{Der}_R(A, M)$ by the universal property of $\Omega^1_{A/R}$.

Étale group schemes (over a field). We will construct a larger set of group schemes containing the constant group schemes. We first suppose R is a field k.

Definition. A finite k-algebra A is *étale* if A is a finite product $A = \prod_i k_i$ for $k \subset k_i$ a finite separable field extension.

Proposition. *If A is any finite k-algebra (so that it is an Artin k-algebra), then $A \simeq \prod_i A_i$, where each A_i is a local k-algebra with maximal ideal $\mathfrak{m}_i$ nilpotent.*

For the proof, see [AM, Theorem 8.7] or [Wat, §6.2]. For the commutative algebra behind separable extensions, see [Mat, §27].

Proposition. *If k is a field, A a finite k-algebra, then the following are equivalent:*

(i) *A is étale;*
(ii) *$A \otimes k^{\mathrm{sep}} \simeq k^{\mathrm{sep}} \times \cdots \times k^{\mathrm{sep}}$;*
(iii) *$A \otimes \overline{k} \simeq \overline{k} \times \cdots \times \overline{k}$;*
(iv) *$A \otimes \overline{k}$ is reduced (i.e. has no nilpotents);*
(v) *$\Omega^1_{A/k} = 0$;*
(vi) *$\Omega^1_{(A\otimes\overline{k})/k} = 0$.*

This implies that a subalgebra of an étale algebra is étale by (iv), and by (ii) we find that a tensor product of étale algebras and a quotient algebra of an étale algebra are étale.

Proof. (See [Wat, §6.2] or [Mil, Proposition I.3.1].)

(i) ⇒ (ii) is clear by tensoring the relation. (ii) ⇒ (iii) directly. (iii) ⇒ (iv) because $k \times \cdots \times k$ has no nilpotents. (iv) ⇒ (iii) because it is a product of local algebras and hence we must have all $\mathfrak{m}_i = 0$.

(iii) ⇒ (i): If $A \otimes \overline{k} \simeq \overline{k} \times \cdots \times \overline{k}$, then A has no nilpotents, so by the proposition above, $A = \prod_i A_i$ and each A_i is a field. Thus

$$\mathrm{Hom}_k(A, \overline{k}) = \bigcup_i \mathrm{Hom}_k(A_i, \overline{k})$$

By Galois theory, the order of the right-hand side is $\leq$ the sum of the degrees of A_i, which by the left-hand side is $\leq \mathrm{rk}(A)$, with equality iff all A_i are separable. But

$$\mathrm{Hom}_k(A, \overline{k}) = \mathrm{Hom}_{\overline{k}}(A \otimes \overline{k}, \overline{k})$$

has rank equal to that of A since $A \otimes \overline{k}$ is a product of $\overline{k}$, we conclude that the A_i are separable and thus A is étale.

(iii) ⇒ (vi) because the differentials of a product is the product of the differentials, which then is trivial, and clearly (v) ⇔ (vi).

(vi) ⇒ (iii): We may assume $k = \overline{k}$ is algebraically closed. We have $\Omega^1_{A/k} = 0$ so $\Omega^1_{A_i/k} = 0$, where $A = \prod_i A_i$, each A_i a local k-algebra. For $\mathfrak{m}_i$ the maximal ideal of A_i, then for $A_i = k[x_1, \ldots, x_n]/\langle f_i \rangle_i$,

$$\Omega^1_{A_i/k} = \bigoplus_i A\, dx_i / \langle \textstyle\sum_{j=1}^n (\partial f_i/\partial x_j) dx_j \rangle$$

and reducing modulo $\mathfrak{m}_i$ (by tensoring with the residue field), we obtain

$$0 = \bigoplus_i k\, dx_i / \langle \textstyle\sum_{j=1}^n (\partial f_i/\partial x_j)(0)\, dx_j \rangle \simeq \mathfrak{m}_i/\mathfrak{m}_i^2.$$

Therefore we find $\mathfrak{m}_i/\mathfrak{m}_i^2 = 0$, so $\mathfrak{m}_i = 0$ by Nakayama's lemma, and A_i is a field and hence $\overline{k}$. □

Let $\pi = \mathrm{Gal}(k^{\mathrm{sep}}/k)$. We have a functor

$$\{\text{Finite étale algebras}\} \to \{\text{Finite } \pi\text{-sets}\}$$

(i.e. those with a continuous π-action) defined the dual

$$\{\text{Finite affine étale } k\text{-schemes}\} \to \{\text{Finite } \pi\text{-sets}\}$$
$$X = \operatorname{Spec} A \mapsto X(k^{\mathrm{sep}}) = \mathrm{Mor}_k(\operatorname{Spec} k^{\mathrm{sep}}, X) = \mathrm{Hom}_k(A, k^{\mathrm{sep}})$$

with $\sigma \in \pi$ acting on $f : A \to k^{\mathrm{sep}}$ by

$$(\sigma f)(a) = \sigma(f(a)).$$

We also have an inverse functor $Y \mapsto \mathrm{Map}_\pi(Y, k^{\mathrm{sep}})$, and if we tensor with k^{sep} we obtain étale algebras over k. These functors induce equivalences of categories [Wat, §§6.3–6.4], [Sha, §3]. (For more information about Galois coverings of fields and the fundamental group, see [Mil, §5] or [Tat, (3.6)] and for proofs, see [Mur, Chapter IV].)

The same functors induce an equivalence of categories [Wat, §6.4]

$$\{\text{Finite étale affine commutative } k\text{-group schemes}\} \leftrightarrow \{\text{Finite } \pi\text{-modules}\}$$
$$G \mapsto G(k^{\mathrm{sep}}) = G(\overline{k})$$

The π-module structure commutes with the group structure, since this is in fact a functor, and so the product is an element of the left-hand side.

Example. In this equivalence, we have constant group schemes correspond to exactly those with trivial π-action. $\Gamma(\overline{k}) = \mathrm{Hom}(k^{(\Gamma)}, \overline{k})$ by $f_\gamma : e_\gamma \mapsto 1$, $e_{\gamma'} \mapsto 0$ for $\gamma' \neq \gamma$. Explicitly, we see

$$(\sigma f_\gamma)(e_{\gamma'}) = \sigma(f_\gamma(e_{\gamma'})) = f_\gamma(e_{\gamma'})$$

since this is $0, 1 \in k$ and so is fixed by the Galois action.

Example. Let $k = \mathbb{R}$ and take $\mu_3(S) = \{s \in S : s^3 = 1\}$, where

$$\mu_3 = \operatorname{Spec} A, \quad A = \mathbb{R}[X]/\langle X^3 - 1\rangle \simeq \mathbb{R} \times \mathbb{C}.$$

We have

$$\mu_3(\mathbb{C}) = \mathrm{Hom}_{\mathbb{R}}(A, \mathbb{C}) = \mathrm{Hom}_{\mathbb{R}}(\mathbb{R} \times \mathbb{C}, \mathbb{C}) = \{f_1, f_2, f_3\}$$

where $f_1 : \mathbb{R} \to \mathbb{C}, \mathbb{C} \to 0$, $f_2 : \mathbb{R} \to 0, \mathbb{C} \to \mathbb{C}$, $f_3 : \mathbb{R} \to 0, \mathbb{C} \to \overline{\mathbb{C}}$. Check that $\sigma f_1 = f_1$, $\sigma f_2 = f_3$, $\sigma f_3 = f_2$, where $\sigma(z) = \overline{z}$ is complex conjugation generating the Galois group.

Characteristic zero. We will now prove:

Theorem (Cartier)**.** *If k is a field of characteristic 0, then every finite group scheme is étale.*

We will need the following result:

Proposition. *If R is a noetherian ring, A an Hopf algebra over R, and $G = \operatorname{Spec} A$, then*

$$\Omega^1_{A/R} \simeq A \otimes_R (I/I^2)$$

where $I = \ker(A \xrightarrow{e} R)$.

Corollary. *If $R = k$ is a field, then I/I^2 is free, so the differentials are free over A.*

Proof. (See also [Wat, §11.3, Theorem].) We have the following commutative diagrams:

$$\begin{array}{ccc} G \times G & \longrightarrow & G \times G \\ {\scriptstyle \mathrm{id}_G \times e}\uparrow & & \uparrow{\scriptstyle \Delta} \\ G & = & G \end{array}$$

where the top map is $(g, h) \mapsto (g, gh)$. This is dual to

$$\begin{array}{ccc} A \otimes A & \longleftarrow & A \otimes A \\ \downarrow{\scriptstyle \mathrm{id}_A \otimes e} & & \downarrow{\scriptstyle m} \\ A & = & A \end{array}$$

where the top map is $a \otimes b \mapsto c(b)(a \otimes 1)$.

Therefore we have an isomorphism of groups $\ker m \simeq \ker(\mathrm{id}_A \otimes e)$. Since $a \otimes 1 \mapsto a \otimes 1$ on the top map, the A-module structure is preserved, acting on the first coordinate.

But $\ker(\mathrm{id}_A \otimes e) = A \otimes I$, and letting $\ker m = J$, we have

$$(A \otimes I)/(A \otimes I)^2 = A \otimes I/I^2 \simeq J/J^2 \simeq \Omega^1_{A/R}$$

as A-modules. To see this last map, we note that in the case that $A = R[X_1, \ldots, X_n]$, we have the map $A \otimes A \xrightarrow{m} A$ which is

$$\begin{aligned} R[X_1, \ldots, X_n, Y_1, \ldots, Y_n]/\langle f_i(X), f_i(Y)\rangle &\xrightarrow{m} R[T_1, \ldots, T_n]/\langle f_i(T)\rangle \\ X_i, Y_i &\mapsto T_i \end{aligned}$$

It is clear that $Y_i - X_i$ are elements of the kernel, but we can always convert an element in the kernel to a polynomial in X_i so actually $\ker m = J = \langle Y_i - X_i\rangle_i$. Let $\epsilon_i = Y_i - X_i$. Then

$$A \otimes A = k[X_1, \ldots, X_n, \epsilon_1, \ldots, \epsilon_n]/\langle f_i(X), f_i(X_i + \epsilon_i)\rangle_i$$

so that

$$J/J^2 = \langle \epsilon_1, \ldots, \epsilon_n\rangle/\langle \epsilon_i\epsilon_j, \sum_j (\partial f_i/\partial X_j)\epsilon_j\rangle \simeq \Omega^1_{A/R}.$$

(This also works even when A is not finitely generated.)

Therefore $A \otimes_R I/I^2 \simeq \Omega^1_{A/R}$. □

Corollary. *If $m \in \mathbb{Z}$ kills G, then it also kills $\Omega^1_{A/R}$.*

Proof. If $m \in \mathbb{Z}$ kills G then the multiplication map $[m]$ factors through $\operatorname{Spec} R$; by duality, it suffices to show that it factors through $\Omega^1_{R/R} = 0$, for then it would also kill $\Omega^1_{A/R}$. But we showed that if $a \in I \subset A$, then $c(a) = 1 \otimes a + a \otimes 1 \pmod{I \otimes I}$, so $[n](a) = na \pmod{I^2}$, and therefore if n kills G then $[n](a) = 0$. □

We are now able to prove the result of this section:

Theorem (Cartier)**.** *If G is a finite (flat) group scheme over a field k of characteristic 0, then G is étale, which is to say that if $G = \operatorname{Spec} A$, then $A \otimes_k \overline{k} \simeq \overline{k} \times \cdots \times \overline{k}$.*

Proof. (See [Wat, §11.4, Theorem], [Tat, Lemma 3.7.1], [Sha, §3, Theorem].) Let I be the augmentation ideal of A and $x_1, \dots, x_n$ a basis for I/I^2. Then

$$\varprojlim A/I^n = A/\textstyle\bigcap_n I^n = A/J;$$

since $A = \prod_i A_i$ with A_i local and $\mathfrak{m}_i$ nilpotent, taking large powers each component will either vanish or remain the unit ideal, so J is a direct factor of A as an R-algebra. Thus

$$A/J \simeq k[x_1, \dots, x_n]/\langle f_i \rangle_i$$

and $A \simeq A/J \times A/J'$ since it is a direct factor for some J'. Since

$$\Omega^1_{A/k} \simeq A \otimes_k I/I^2$$

is a free A-module, we have it as $\bigoplus_{i=1}^n A\,dx_i$ as an A-module, and

$$\Omega^1_{A/k} \simeq \Omega^1_{(A/J)/k} \times \Omega^1_{(A/J')/k}$$

so that $\Omega^1_{(A/J)/k} \simeq \bigoplus_{i=1}^n A/J\,dx_i$ is free over A/J, since the ideals are coprime. But this is also isomorphic to

$$\textstyle\bigoplus_{i=1}^n (A/J)\,dx_i/\langle \sum_j (\partial f_i/\partial x_j)\,dx_j \rangle_i$$

so if $f \in J$ then $\partial f/\partial x_i \in J$ for all i. But up to certain factorials, every coefficient is already in J (by taking a high partial derivatives), so since the characteristic of k is 0, we already have every coefficient in J and thus all coefficients are 0. Thus $A/J \simeq k[x_1, \dots, x_n]$, but this is a finite-dimensional algebra, so $n = 0$, so $I/I^2 = 0$, so $\Omega^1_{A/k} = 0$, and so A is étale. □

This immediately implies Lagrange's theorem, since an étale group scheme is also just a module which is a group, so it follows from the classical Lagrange's theorem.

Étale group schemes (over a ring). We now extend the results of the previous section from fields to more general rings.

Definition. If R is a connected (noetherian) base ring, and G a finite R-group scheme, then $G = \operatorname{Spec} A$ is *étale* if it is flat (locally free) and $A \otimes k$ is étale for any residue field $R \to k \to 0$.

A over R is étale iff $\Omega^1_{A/R} = 0$ and A is flat.

Remark. If $K \subset L$ is a finite extension of a number fields, then $\mathfrak{O}_L$ is an étale $\mathfrak{O}_K$-algebra iff L/K is unramified.

Pick a geometric point of $\operatorname{Spec} R$, $\operatorname{Spec}(k^{\text{sep}}) \to \operatorname{Spec} R$ from $R \to k \hookrightarrow k^{\text{sep}}$ (the first map surjective). We have seen that there exists a functor F from the category of finite étale affine R-schemes to sets, which for $X = \operatorname{Spec} A$ takes

$$X \mapsto X(k^{\text{sep}}) = \operatorname{Mor}_R(\operatorname{Spec} k^{\text{sep}}, X) = \operatorname{Hom}_R(A, k^{\text{sep}}).$$

We have $\pi = \operatorname{Aut}(F)$, i.e. π consists of automorphisms of functors $\pi_S : F(S) \to F(S)$ for any R-algebra S. π is a profinite group; think of it as the absolute Galois group of k if $R = k$ is a field (see especially [Mil, Examples 5.2]).

If we restrict the functor to finite sets, then it factors through finite π-sets, and it is a theorem is that this functor (from finite étale affine R-schemes to finite π-sets) becomes an equivalence of categories [Mil, Theorem 5.3]. This immediately implies by functoriality that there is an equivalence of categories F from finite étale commutative affine R-schemes to finite π-modules (we just equip each with a group structure).

Example. If $R = k$ is a field, then $\pi = \mathrm{Gal}(k^{\mathrm{sep}}/k)$.

If R is a complete local Noetherian ring, we can look at algebras over the residue field $k = R/\mathfrak{m}$ by Hensel's lemma, hence $\pi = \mathrm{Gal}(k^{\mathrm{sep}}/k)$.

Example. Let $R = \mathfrak{O}_S$ be the ring of S-integers of a number field F, where S is a finite set of primes of $\mathfrak{O}_S$, i.e. elements which are integral at every prime $\mathfrak{p} \notin S$). Then $\pi = \mathrm{Gal}(L/F)$ where L is the maximal algebraic extension of F unramified at the primes outside S.

For example, if we take $S = \emptyset$, $\pi(\mathbb{Z}) = 1$ by Minkowski (there are no unramified extensions of $\mathbb{Q}$). Also, $\pi(\mathbb{Z}[\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z}$, where the unramified extension is $\mathbb{Z}[\sqrt{-5}] \subset \mathbb{Z}[i, (\sqrt{-5}+i)/2]$. Finally, $\pi(\mathbb{Z}[(1+\sqrt{-283})/2]) \simeq A_4$.

There are no known examples of π if S is not the empty set. If $S = \emptyset$, then $\pi/[\pi,\pi]$ is finite (it is the ideal class group), but π need not be finite (a problem related to infinite class field towers).

Example. Take $\mathfrak{O} = \mathbb{Z}[\sqrt{-5}]$, so that π is order 2. There should be an étale group scheme over $\mathfrak{O}$ of order 3 with nontrivial action by π. We hope that $G = \operatorname{Spec} A$, $A = \mathfrak{O}[X]/\langle f(X)\rangle$, which may not be the case in general, but here we are lucky. By translation to get the origin at zero, we guess that $A = \mathfrak{O}[X]/\langle X^3 + aX^2 + cX\rangle$. Since A is étale, c is a unit (either computing the differentials or because the determinant must be invertible, as it must be unramified). Writing down quadratics with discriminant -1, we find $a = \sqrt{-5}$, $c = -1$. (As an $\mathfrak{O}$-algebra, since there is only one unramified extension of $\mathfrak{O}$, we must have A isomorphic to $\mathfrak{O}[(i+\sqrt{-5})/2]$.)

Thus

$$A = \mathfrak{O}[X]/\langle X^3 + \sqrt{-5}X^2 - X\rangle,$$

with the three points (tensoring with the quotient field) $0, (-\sqrt{-5} \pm i)/2$. The multiplication law is

$$X \mapsto X + X' + aXX' + b(X^2X' + XX'^2) + c(X^2X'^2)$$

for certain (different) $a, b, c \in \mathfrak{O}$. Since we can compute directly by adding the points together in the cyclic group, we have to solve a linear system. It turns out to have solutions in $\mathfrak{O}$, and in fact

$$X \mapsto X + X' + 3\sqrt{-5}XX' + 6(XX'^2 + X'^2X) - 2\sqrt{-5}X^2X'^2.$$

Characteristic p. What can be salvaged from the previous proof when $\operatorname{char} k \neq 0$? We go to the other extreme, and look at the following objects:

Definition. A *local group scheme* $G = \operatorname{Spec} A$ is a group scheme for which the base ring R is a local ring, A is a local algebra over R (i.e. the map $R \to A$ is a local homomorphism).

We will restrict to the case where $R = k$ is a field with $\operatorname{char} k = p > 0$ (and later, using Hensel's lemma, we will get information about complete local rings).

Proposition. *Let $G = \operatorname{Spec} A$ be a finite local group scheme of height 1 (if $A = k[X_1, \ldots, X_n]/J$ then $J \supset \langle X_1^p, \ldots, X_n^p\rangle$). Then*

$$A \simeq k[X_1, \ldots, X_n]/\langle X_1^p, \ldots, X_n^p\rangle.$$

Proof. (See [Tat, Lemma 3.7.3].) Let $I \subset A$ be the augmentation ideal. I must be the maximal ideal of A and therefore is nilpotent. If $x_1, \ldots, x_n$ is a k-basis of I/I^2 then by Nakayama, $A \simeq k[x_1, \ldots, x_n]/J$. Hence

$$A \otimes_k I/I^2 \simeq \Omega^1_{A/k} \simeq \textstyle\bigoplus_{i=1}^n A\, dx_i$$

is free over A of rank n, which is just

$$\bigoplus_{i=1}^n A\,dx_i/\langle\textstyle\sum_j(\partial f_i/\partial x_j)x_j\rangle$$

so this ideal of partials must be equal to zero; if $f \in J$ then $\partial f/\partial x_j \in J$, so again we have a factorial multiplied by each coefficient must vanish. In particular, every coefficient of a monomial $f = x_1^{i_1}\dots x_n^{i_n} \in J$ with all $i_k < p$ must vanish, so $J \subset \langle x_1^p, \dots, x_n^p\rangle$. Since we have assumed containment in the other direction, equality must hold. □

Our goal now is to prove:

Theorem. *If k is a perfect field of characteristic $p > 0$, $G = \operatorname{Spec} A$ a finite local group scheme, then*

$$A \simeq k[X_1, \dots, X_n]/\langle X_1^{p^{e_1}}, \dots, X_n^{p^{e_n}}\rangle.$$

Since $\dim_k A = p^{e_1+\dots+e_n}$, we have:

Corollary. *If G is a local finite group scheme over k, then $\#G$ is a power of p.*

Corollary. *If G is a finite local flat group scheme over R which is a complete local Noetherian ring with perfect residue field, then (after lifting variables by Hensel's lemma) $G = \operatorname{Spec} A$, and A is a complete intersection algebra.*

Corollary. *If R is a complete local noetherian ring, $G = \operatorname{Spec} A$ a finite flat local group scheme over R, with $R/\mathfrak{m}$ perfect of characteristic p, then*

$$A \simeq R[[X_1, \dots, X_n]]/\langle f_1, \dots, f_n\rangle$$

where $f_i \in X_i^{p^{e_i}} + \mathfrak{m}R[X_1, \dots, X_n]$ where the polynomial in the maximal ideal is degree $< p^{e_i}$.

Proof. If $G = \operatorname{Spec} A$ for A a finite flat R-algebra, then by the theorem, $G_k = \operatorname{Spec}(A \otimes_R k) \simeq k[X_1, \dots, X_n]/\langle X_1^{p^{e_1}}, \dots, X_n^{p^{e_n}}\rangle$. Lift X_i to A and again call them X_i; by Nakayama, the same X_i will generate A as an R-algebra. Thus

$$A \simeq R[[X_1, \dots, X_n]]/J$$

so that

$$0 \to J \to R[[X_1, \dots, X_n]] \to A \to 0$$

(as R-modules) is R-split because A is flat and therefore free, and

$$0 \to J \otimes_R k \to R[[X_1, \dots, X_n]] \to A \otimes_R k \to 0$$

is also k-split, and $J \otimes k = \langle X_1^{p^{e_1}}, \dots, X_n^{p^{e_n}}\rangle$, so we lift $X_i^{p^{e_i}}$ to J and call them f_i, such that $f_i \in X_i^{p^{e_i}} + \mathfrak{m}R[X_1, \dots, X_n]$; we can do this because the monomials $X_1^{a_1}\dots X_n^{a_n}$ $(0 \le a_i \le p^{e_i} - 1)$ are an R-basis for the free R-module A, so the f_i generate J. □

To prove the theorem, we will use induction with respect to the dimension of A over k. First:

Lemma. *If $B \subset A$ are finite k-Hopf algebras, with B local, then A is free over B.*

Proof. Letting $G = \operatorname{Spec} A$, $H = \operatorname{Spec} B$, we have

$$\begin{array}{ccc} A & \longleftarrow & B \\ \downarrow & & \downarrow e \\ A \otimes_B R & \longleftarrow & R \end{array}$$

so that $N = \ker(G \to H) = \operatorname{Spec}(A \otimes_B R) = \operatorname{Spec}(A/I_B A)$ where I_B is nilpotent.

The functor which sends a k-algebra $S \mapsto G(S) \times N(S)$ is represented by the algebra $A \otimes_k A/I_B A$. The functor which sends

$$S \mapsto G(S) \times_{H(S)} G(S) = \{(g,h) \in G(S) \times G(S) : \operatorname{img}(g) = \operatorname{img}(h) \in H(S)\}$$

is represented by $A \otimes_B A$. These functors are isomorphic by mapping $(g,n) \mapsto (g, gn)$, which are isomorphisms of algebras and as A-modules where A acts on the first coordinate. Therefore $A \otimes_k A/I_B A \simeq A \otimes_B A$ as k-algebras and as A-modules.

We know that $A/I_B A$ is free over A and $A \otimes_B A$ is also free over A. Let $C = A \otimes_B R = A/I_B A$. Take e_i a k-basis for C, and lift it to A and call it e_i again.

Claim. $g : \sum_i Be_i \subset A$ is in fact an isomorphism of B-algebras.

Proof. Since $B/I_B = k$, we know $\sum_i ke_i \simeq C$ is an isomorphism, so g is surjective as I_B is nilpotent (B is local).

We have the diagram

$$\begin{array}{ccccccccc} & & & & \bigoplus_i Be_i & \longrightarrow & A & \longrightarrow & 0 \\ & & & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K & \longrightarrow & \bigoplus_i Ae_i & \longrightarrow & A \otimes_B A & \longrightarrow & 0 \end{array}$$

where K is the kernel. But the bottom exact sequence splits as $A \otimes_B A$ is free over A. Since $A \otimes_B A$ is free of rank n, and the same is true of $\bigoplus_i Ae_i$, the kernel itself is zero. Since $\bigoplus_i Be_i \hookrightarrow \bigoplus_i Ae_i$ is an injection and $\bigoplus_i Ae_i \hookrightarrow A \otimes_B A$, the map is an isomorphism. □

This concludes the proof of the lemma. □

Proof of theorem. (See [Wat, §14.4, Theorem].) We have $G = \operatorname{Spec} A$ where A is a finite local k-Hopf algebra, $\operatorname{char} k = p$. We know $A \simeq k[T_1, \dots, T_r]/\langle f_i \rangle_i$. Look at A^p, the subalgebra generated by $T_1^p, \dots, T_r^p$; this is in fact a sub-Hopf algebra.

By induction, $A^p \simeq k[X_1, \dots, X_n]/\langle X_1^{p^{e_1}}, \dots, X_n^{p^{e_n}} \rangle$, for $X_i \in A^p$. Choose $y_i^p = X_i$ for $i = 1, \dots, n$. Pick

$$\{a \in A : a^p = 0\}/I^2 \cap \{a \in A : a^p = 0\} \hookrightarrow I_A/I_A^2$$

and a k-basis $z_1, \dots, z_m$ for the quotient from $\{a \in A : a^p = 0\}$. Then

$$C = k[Y_1, \dots, Y_n, Z_1, \dots, Z_m]/\langle Y_1^{p^{e_1+1}}, \dots, Y_n^{p^{e_n+1}}, Z_1^p, \dots, Z_m^p \rangle$$

has an inclusion $A^p \hookrightarrow C$ by $X_i \mapsto Y_i^p$. C is actually free over A^p, but $A^p \hookrightarrow A$, with A free over A_p, and the map $Y_i \mapsto y_i$, $Z_i \mapsto z_i$ gives a map $g : C \to A \to 0$. We will show that g is an isomorphism modulo I_{A^p}, which is also its maximal ideal. Since g is a surjection, and they have the same rank over A, g itself will be an isomorphism.

We have that $I_{A^p} = \langle T_1^p, \dots, T_r^p \rangle = \langle X_1, \dots, X_n \rangle$, and modulo I_{A^p}, g becomes

$$k[y_1, \dots, y_n, z_1, \dots, z_m]/\langle y_1, \dots, y_n^p, z_1^p, \dots, z_m^p \rangle \simeq k[T_1, \dots, T_r]/\langle T_1^p, \dots, T_r^p \rangle.$$

It suffices to show that these two algebras have the same number of variables (since this determines the isomorphism class), g induces an isomorphism $\mathfrak{m}_C/\mathfrak{m}_C^2 \to \mathfrak{m}_A/\mathfrak{m}_A^2$ on the tangent spaces, since the dimension of these spaces gives the number of variables. This is equivalent to showing that y_i, z_j form a k-basis for

$I_A/I_A^2 = \mathfrak{m}_A/\mathfrak{m}_A^2$ (it is surjective by the above, so it suffices to show they are independent).

First we prove that they generate the ideal. If $x \in I$, then $x^p \in I_{A^p} = \langle X_1, \dots, X_n \rangle$, where the X_i are actually a basis for the ideal modulo squares. Thus $x^p = \phi(X_1, \dots, X_n) \in k[X_1, \dots, X_n]$, but $x^p = \phi(y_1^p, \dots, y_n^p)$ so that $\widetilde{\phi}$ is taken modulo I_A^2 so it is linear. Therefore $\left(x - \widetilde{\phi}(y_1, \dots, y_n)\right)^p = 0$ for k perfect must be in $\{a \in A : a^p = 0\} \cap I_A$, so $x - \widetilde{\phi}(y_1, \dots, y_n) = \sum_i \lambda_i z_i \pmod{I_A^2}$.

Now we must show that the y_i, z_j are independent. Suppose $\sum_i \alpha_i y_i + \sum_j \beta_j z_j = 0 \in I_A/I_A^2$ for $\alpha_i, \beta_j \in k$. Then $\alpha_i^p y_i^p = 0$ in $I_{A^p}/I_{A^p}^2$, where the x_i are a basis, so $\alpha_i^p = 0$, so the $\alpha_i = 0$, and therefore $\sum_j \beta_j z_j = 0$ so since the z_j are a basis $b_j = 0$.

The reason it is enough to show that $C/\mathfrak{m}_{A^p} \simeq A/\mathfrak{m}_{A^p}$ is as follows: Letting $C/\mathfrak{m}_{A^p} = k[Y_1, \dots, Y_n, Z_1, \dots, Z_m]/\langle Y_1^p, \dots, Y_n^p, Z_1^p, \dots, Z_m^p \rangle$ and $A/\mathfrak{m}_{A^p} = k[T_1, \dots, T_r]/\langle T_1^p, \dots, T_r^p \rangle$ even though $A = k[T_1, \dots, T_r]/\langle f_i \rangle_i$, since the Hopf algebra structure is the kernel of $\ker(\operatorname{Spec} A \to \operatorname{Spec} A^p)$, which has height 1 and is killed by Frobenius and therefore the result follows by induction. □

Example. If k is not perfect, this is false: choose $a \in k \setminus k^p$, and for a k-algebra S we take $G(S) = \{(x, y) : x^{p^2} = 0,\ x^p = ay^p\}$ is rank p^3, a closed subscheme of $\mathbb{G}_a \times \mathbb{G}_a$, but is not represented in the form given by the theorem.

Connected and étale components. For the details of this section, see [Wat, §6.4–6.7] or [Tat, (3.7)]. Let $G = \operatorname{Spec} A$ be a (possibly noncommutative) group scheme, A finite flat over k. Then $A \simeq \prod_i A_i$ where the A_i are local k-algebras, so $G = \operatorname{Spec} A = \bigsqcup_i \operatorname{Spec} A_i$. The unit section $e : A = \prod_i A_i \to k$ has all but one $e_i \mapsto 0 \in k$, so it factors $e : A \to A_0 \to k$.

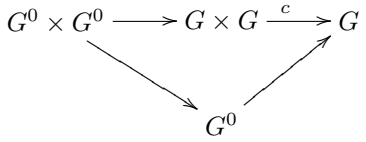
Definition. For $e : A \to A_0 \to k$, $G_0 = \operatorname{Spec} A_0$ is the *connected component of the identity.*

Similarly, let $A_{\text{ét}}$ be the maximal separable (equivalently étale) subalgebra of A. This makes sense because if $B, B' \subset A$ are étale subalgebra, so is $B \otimes_k B'$ as well as the compositum BB' [Wat, §6.5].

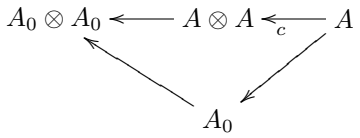
Theorem. *With the above,*

(a) *G_0 is a closed subgroup scheme of G.*
(b) *$A_{\text{ét}}$ is a sub-Hopf algebra, and hence $G^{\text{ét}} = \operatorname{Spec} A_{\text{ét}}$ is a group scheme.*
(c) *The sequence*
$$0 \to G^0 \to G \to G^{\text{ét}}$$
is exact, which is to say G^0 is the kernel of the map on algebras induced by the inclusion.
(d) *Any map $H \to G$ with H a connected group scheme factors through G_0; any map $G \to H$ with H an étale group scheme factors through $G^{\text{ét}}$.*
(e) *If k is perfect, then $A \simeq A_0 \otimes_k A_{\text{ét}}$ as k-algebras.*

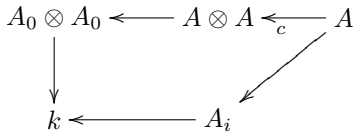
Proof of (a). (See [Wat, §6.6].) We need to show that the composition map factors:



On algebras, then, we want:



A_0 is a local ring with residue field k, because there is a section $e : A \to k$; the tensor product is also local because it has residue field $k \otimes_k k = k$, so this factors:



The composition $A \to k$ must be the unit section and hence factors through A_0 by definition; hence $i = 0$ as desired. (One can also in this way also show that the inverse map takes $G^0 \to G^0$.) □

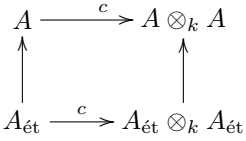
Proof of (b). We first need:

Claim. Let $A = \prod_i A_i$, with A_i local with residue field k_i, $k \subset {k_i}^{\text{sep}} \subset k_i$ finite (${k_i}^{\text{sep}}$ denotes the separable closure of k in k_i). Then the product $\prod_i {k_i}^{\text{sep}}$ is a k-subalgebra of A and $A_{\text{ét}} = \prod_i {k_i}^{\text{sep}}$.

Proof. Such a k-algebra is certainly étale. Conversely, if $x \in A_{\text{ét}}$ and $k \notin \prod_i {k_i}^{\text{sep}}$, then there exists an x_i (multiplying by idempotents), a component of x, for which $x_i \in A_i$ is étale, but $x_i \notin {k_i}^{\text{sep}}$. There is a power of p such that $x_i^{p^a} \in {k_i}^{\text{sep}}$. If we look at the reduction map $x_i \in A_i \to A_i/\mathfrak{m}_i = k_i$, $x_i^{p^a} \mapsto t \in {k_i}^{\text{sep}} \in A_i$, so $x_i^{p^a} - t \in \mathfrak{m}_i$ so $(x_i^{p^a} - t)^{p^b} = 0$ and therefore $x_i^{p^{a+b}} \in {k_i}^{\text{sep}}$ since the maximal ideal is nilpotent, a contradiction.

(The same is not true for an inseparable extension (we may not be able to lift k to A): if A is a local k-algebra, k not perfect, then if $a \in k \backslash k^p$, and $A = k[X]/\langle X^p - a\rangle$, we find that $A/\mathfrak{m} \simeq k[X]/\langle X^p - a\rangle$ has no section to k.) □

We want to show $A_{\text{ét}}$ is a sub-Hopf algebra, i.e. we need to show the commutativity of:



First we show $A_{\text{ét}} \otimes_k \overline{k} = (A \otimes_k \overline{k})_{\text{ét}}$ [Wat, §6.5, Theorem]. The inclusion $\subset$ is clear, since $A_{\text{ét}} \otimes_k \overline{k}$ is étale. For the converse, we count points over $\overline{k}$: if we let $A = \prod_i A_i$, A_i local, then

$$\begin{aligned}\#\operatorname{Spec}(A^{\text{ét}} \otimes_k \overline{k}) &= \#\operatorname{Hom}_{\overline{k}}(A_{\text{ét}} \otimes_k \overline{k}, \overline{k}) = \#\operatorname{Hom}_k(A_{\text{ét}}, \overline{k}) \\ &= \#\operatorname{Hom}_k(\textstyle\prod_i {k_i}^{\text{sep}}, \overline{k}) = \sum_i [{k_i}^{\text{sep}} : k] = \sum_i [k_i : k]^{\text{sep}}.\end{aligned}$$

The number of points on the right-hand side is

$$\begin{aligned}\#\operatorname{Spec}(A \otimes_k \overline{k})_{\text{ét}} &= \#\operatorname{Hom}_{\overline{k}}((A \otimes_k \overline{k})_{\text{ét}}, \overline{k}) \\ &= \#\operatorname{Hom}_{\overline{k}}(A \otimes_k \overline{k}, \overline{k}) = \textstyle\sum_i \#\operatorname{Hom}_k(k_i, \overline{k}) = \sum_i [k_i : k]^{\text{sep}}.\end{aligned}$$

So equality holds.

Next, $(A \otimes_k B)_{\text{ét}} = A_{\text{ét}} \otimes_k B_{\text{ét}}$; the inclusion $\supset$ is clear, and to prove the inclusion $\subset$, tensor with $\overline{k}$, and use the previous formula to conclude they have the same rank.

Now we have maps

$$\begin{array}{ccc} A & \xrightarrow{c} & A \otimes_k A \\ \uparrow & & \uparrow \\ A_{\text{ét}} & \xrightarrow{c} & (A \otimes_k A)_{\text{ét}} \end{array}$$

so the map factors as desired. □

Proof of (c). (See [Wat, §6.7], [Sha, §3, Proposition].) If k is perfect, then we want to show $G^0 \simeq \ker(G \to G^{\text{ét}})$. The map $G \to G^{\text{ét}}$ is given by the inclusion $A_{\text{ét}} = \prod_i {k_i}^{\text{sep}} \hookrightarrow A$; the kernel is represented by $A/(\prod_{i \neq 0} {k_i}^{\text{sep}})A$ since this arises from the unit section:

$$\begin{array}{ccc} A_{\text{ét}} = \prod_i {k_i}^{\text{sep}} & \xrightarrow{e} & k \\ \downarrow & \nearrow & \\ k_0 & & \end{array}$$

But this is

$$A/(\textstyle\prod_{i \neq 0} {k_i}^{\text{sep}})A = (\prod_i A_i)/(\prod_{i \neq 0} {k_i}^{\text{sep}} A_i) = \prod_i A_i / \prod_{i \neq 0} A_i \simeq A_0.$$

Therefore $G^0 = \ker(G \to G^{\text{ét}})$. □

Proof of (d). (See [Wat, §6.7].) We want to show the following: If G and H are finite k-group schemes, with $G = \operatorname{Spec} A$ connected, A local, $H = \operatorname{Spec} B$, B étale, then any $f : G \to H$ factors through $G^{\text{ét}}$; this is because the induced map of the separable algebra B to A has image in $A_{\text{ét}}$, so the map on schemes factors through $G^{\text{ét}}$. Conversely, if we have a map $f : H \to G$ with H connected, then the structure map $H \to \operatorname{Spec} k$ lifts via $e : \operatorname{Spec} k \to G^0$, and since H is connected its image is also connected, hence contained in the connected scheme G^0, hence the map factors $H \to G^0$. □

Proof of (e). (See [Wat, §6.8].) We want to show $A \simeq A_0 \otimes_k A_{\text{ét}}$ as k-algebras.

From (c) we know $G^0 \times G \simeq G \times_{G^{\text{ét}}} G$ by $(h, g) \to (g, gh)$; on algebras, this is a map $A \otimes_k A^0 \leftarrow A \otimes_{A^{\text{ét}}} A$ by $a \otimes b \mapsto c(b)a$.

If $A = \prod_i A_i$, A_i local with maximal ideal $\mathfrak{m}_i$, the nilradical of A is $\prod_i \mathfrak{m}_i$. If k is perfect, $A/\prod_i \mathfrak{m}_i \simeq \prod_i k_i = \prod_i {k_i}^{\text{sep}} = A_{\text{ét}}$, so A modulo the nilradical has a natural Hopf algebra structure. So if we take our original map $A \otimes_k A^0 \leftarrow A \otimes_{A_{\text{ét}}} A$ modulo the nilradical, we obtain an isomorphism $A_{\text{ét}} \otimes_k A_0 \simeq A/\prod_i \mathfrak{m}_i \otimes_k A_0 \simeq A/\prod_i \mathfrak{m}_i \otimes_{A_{\text{ét}}} A \simeq A$ which is $a \mapsto 1 \otimes a \mapsto c(a)$ and is indeed an isomorphism. □

Exercises. The following are exercises for §4.

Problem 4.1. Let k be a field.

(a) For any finite-dimensional k-vector space M, determine the group scheme that represents the functor that maps a k-algebra S to the additive group $\operatorname{End}_S(M \otimes S)$.

(b) Answer the same question for the functor that maps a k-algebra S to the multiplicative group $\operatorname{Aut}_{S/k}(M \otimes S)$.

(c) Assume now that R is a finite k-algebra (resp. Hopf algebra). Show that the functor that maps a k-algebra S to the multiplicative group of algebra (resp. Hopf algebra) automorphisms $\mathrm{Aut}_{S/R}(R \otimes S)$ is represented by a closed subgroup scheme of the group scheme of part (b).
(d) Let R be a separable k-algebra. Show that $\mathrm{Aut}_{S/R}(R)$ is étale.

Problem 4.2. Compute the Kähler differentials $\Omega^1_{A/R}$ for the following rings R and R-algebras A:

(a) $R = \mathbb{Z}$ and $A = \mathbb{Z}[\sqrt{2}]$.
(b) $R = \mathbb{Z}$ and $A = (\mathbb{Z}/6\mathbb{Z})[X]/\langle X^2 + X + 1\rangle$.
(c) $R = \mathbb{Q}[T]$ and $A = \mathbb{Q}[X, Y]/\langle X^2 + Y^2 - XY + X, Y^4 - X^3Y + X^2Y\rangle$ where A is an R-algebra via $T \cdot f(X, Y) = Xf(X, Y)$ for $f(X, Y) \in A$.

Problem 4.3. Let k be a non-perfect field and let $a \in ksetminusk^p$. Let G be the closed subgroup scheme of $\mathbb{G}_a \times \mathbb{G}_a$ defined by $G(S) = \{(x, y) \in S \times S : x^{p^2} = 0,\ x^p = ay^p\}$ for a k-algebra S. Show that the Hopf algebra of G is not isomorphic to a k-algebra of the form $k[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}}\rangle$.

Problem 4.4. Let $\zeta = (1 + \sqrt{-3})/2$ denote a cube root of unity.

(a) Show that the fundamental group $\pi_1(\mathbb{Z}[\zeta])$ is trivial. [Hint: Use Minkowski's theorem.]
(b) Show that $\pi_1(\mathbb{Z}[\sqrt{6}])$ has order 2. Show that the ring $\mathbb{Z}[\sqrt{-2}, \zeta]$ is a quadratic unramified extension of $\mathbb{Z}[\sqrt{6}]$.
(c) Show that the étale $\mathbb{Z}[\sqrt{6}]$-algebra $\mathbb{Z}[\sqrt{6}] \times \mathbb{Z}[\sqrt{-2}, \zeta]$ has the structure of a Hopf-algebra.

Problem 4.5. Let $G = \mathrm{Spec}\, A$ be an R-group scheme. Suppose that n annihilates the group scheme G. In other words, the morphism $[n] : A \to A$ factors through the counit morphism $e : A \to R$.

(a) Prove that n kills the group I/I^2.
(b) Suppose that $R = k$ is a field of characteristic p and assume that G is commutative. Show that G is étale whenever n is coprime to p. (This is also true when G is not commutative.)

Problem 4.6. Let $\alpha = (3 + \sqrt{-23})/2$ and let R denote the ring $\mathbb{Z}[\alpha]$. By $\overline{\alpha}$ we denote the conjugate $(3 - \sqrt{-23})/2$.

(a) Show that the polynomial $f(X) = X^3 - \alpha X^2 - \overline{\alpha}X + 1 \in R[X]$ is irreducible and has discriminant 1.
(b) Let β denote a zero of $f(X)$. Show that $\mathbb{Q}(\sqrt{-23}) \subset \mathbb{Q}(\sqrt{-23}, \beta)$ is Galois of degree 3.
(c) The R-algebra $R \times R[\beta] \simeq R[X]/\langle Xf(X)\rangle$ can be given the structure of a Hopf algebra of an étale group scheme of order 4 and exponent 2. Determine the group law explicitly in terms of the coordinate X. [Hint: Work over $\mathbb{Q}(\sqrt{-23})$ and solve a linear system in six unknowns.]

5. Fontaine's theorem

The goal of the final section of these notes is to establishing the following theorem: If G is a finite flat group scheme over the ring of integers of a number field $\mathfrak{O}_K$, then adjoining the points of G to K, we obtain an extension with very little

ramification. It will imply that there are no abelian varieties over $\mathbb{Z}$ and other small number fields.

Ramification theory. For more information, consult [Ser, Chapter IV].

Consider a finite extension $\mathbb{Q}_p \subset K \subset L$ where $G = \mathrm{Gal}(L/K)$, $\pi \in \mathfrak{O}_K$ a uniformizer, with valuation $v(\pi) = 1$. The ring of integers is $\mathfrak{O}_L = \mathfrak{O}_K[\alpha]$: take α to be a uniformizer in L, and add ζ, a lift of a generator of the multiplicative group of the residue field $(\mathfrak{O}_L/\pi_L)^\times$ [Ser, III, §6, Proposition 12].

Extend the valuation v to L in a unique way, with $v(\pi_L) = 1/e_{L/K}$, where $e_{L/K}$ is the ramification index. The inertia group

$$I = \{\sigma \in G : \sigma(x) \equiv x \text{ (`mod } \pi_L) \text{ for all } x \in \mathfrak{O}_L\} \subset G$$

is a normal subgroup, and $\#I = e_{L/K}$ [Ser, IV, §1, Proposition 1]. We also have $I = \{\sigma \in G : v(\sigma(\alpha) - \alpha) > 0\}$.

This numbering matches that given in the article by Fontaine [F], and is off by 1 from the one used by Serre [Ser].

Definition. We define the *higher ramification groups (with lower numbering)* as follows: for $i \in \mathbb{R}$,

$$\begin{aligned} G_{(i)} &= \{\sigma \in G : v(\sigma(x) - x) \geq i \text{ for all } x \in \mathfrak{O}_L\} \\ &= \{\sigma \in G : v(\sigma(\alpha) - \alpha) \geq i\}. \end{aligned}$$

Definition. We let $i(\sigma) = v(\sigma(\alpha) - \alpha) = \min_{x \in \mathfrak{O}_L} v(\sigma(x) - x)$ (if $\sigma = \mathrm{id}_L$, then $i(\sigma) = +\infty$), and $i_{L/K} = \max_{\sigma \neq \mathrm{id}_L} i(\sigma)$.

We know $i_{L/K}, i(\sigma) \in (1/e_{L/K})\mathbb{Z}$.

Example. If $i \leq 0$, then $G_{(i)} = G$. If $i > 0$, then $G_{(i)} \subset I$. $G_{(i)} = I$ iff $0 < i \leq 1/e_{L/K}$.

Definition. We define the function

$$\phi_{L/K}(i) = \textstyle\sum_{\sigma \in G} \min(i, i(\sigma)) : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}.$$

$\phi_{L/K}$ is piecewise linear, monotone increasing, and continuous [Ser, IV, §3, Proposition 12]. If $i \gg 0$, then $G_{(i)} = \{1\}$.

Definition. We define the *higher ramification groups (with upper numbering)* as follows: Let $G^{(\phi_{L/K}(i))} = G_{(i)}$, so $G^{(u)} = G_{(\phi^{-1}_{L/K}(u))}$ for $u \geq 0$.

For the lower numbering, we have $G_{(i)} \subset G_{(i')}$ if $i \geq i'$, $G_{(i)} = \{1\}$ if $i \gg 0$, and $G_{(0)} = G$.

Definition. Let $u_{L/K} = \phi_{L/K}(i_{L/K})$.

$u_{L/K}$ is the largest u for which $G^{(u)} \neq \{1\}$, since $i_{L/K}$ is the largest i for which $G_{(i)} \neq \{1\}$ [Ser, IV, §1, Proposition 3]. We have

$$\begin{aligned} u_{L/K} = \phi_{L/K}(i_{L/K}) &= \sum_{\sigma \in G} \min(i_{L/K}, i(\sigma)) \\ &= i_{L/K} + \sum_{\sigma \neq 1 \in G} i(\sigma) = i_{L/K} + \sum_{\sigma \neq 1 \in G} v(\sigma\alpha - \alpha) + i_{L/K} \\ &= i_{L/K} + v\left(\textstyle\prod_{\sigma \neq 1 \in G}(\sigma\alpha - \alpha)\right). \end{aligned}$$

Let $f(T) \in \mathfrak{O}_K[T]$ be the minimal polynomial of α, so that $f(T) = \prod_{\sigma\in G}(T - \sigma\alpha)$. Then

$$f'(\alpha) = v\left(\prod_{\sigma\neq 1\in G}(\sigma\alpha - \alpha)\right) + i_{L/K} = v(\mathscr{D}_{L/K}) + i_{L/K},$$

where $\mathscr{D}_{L/K}$ is the different, and $N_{L/K}(\mathscr{D}_{L/K}) = \Delta_{L/K}$ is the discriminant of L/K.

We conclude that $v(\mathscr{D}_{L/K}) = u_{L/K} - i_{L/K}$ and $v(\Delta_{L/K}) = [L:K](u_{L/K} - i_{L/K})$ [F, Proposition 1.3] (see also [Ser, IV, §1, Proposition 4]). This implies that if the higher ramification groups $G^{(u)} = \{1\}$ for $u > u_0$, then $v(\Delta_{L/K}) < [L:K]u_0$. Therefore $K \subset L$ is unramified iff $u_{L/K} = 0$, and in this case $\phi_{L/K}(i) = i$. $K \subset L$ is tamely ramified ($p \nmid e_{L/K}$) iff $u_{L/K} = 1$, and $K \subset L$ is wildly ramified iff $u_{L/K} > 1$.

Example. (See [Ser, IV, §4].) Let $K = \mathbb{Q}_p$ and $L = \mathbb{Q}_p(\zeta_{p^n})$, $p^n > 2$. Then $G = \mathrm{Gal}(L/K) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$, and $\alpha = \zeta_{p^n}$ so that $\mathfrak{O}_L = \mathbb{Z}_p[\zeta_{p^n}]$ lies over $\mathfrak{O}_K = \mathbb{Z}_p$. If we normalize $v(p) = 1$, then for $\sigma \in G$ we have $i(\sigma) = v(\sigma\zeta_{p^n} - \zeta_{p^n}) = v((\sigma\zeta_{p^n})/\zeta_{p^n} - 1)$.

We compute $i(\sigma) = p^j/(p-1)p^{n-1}$ for all $\sigma \neq 1$ such that $\sigma \equiv 1 \pmod{p^j}$ but $\sigma \not\equiv 1 \pmod{p^{j+1}}$ for each $0 \leq j \leq n-1$. Hence $i_{L/K} = 1/(p-1)$.

We find that

$$G_{(i)} = G = \{\sigma \in G : \sigma \equiv 1 \pmod{p}\}, \text{ for } 0 < i \leq \frac{1}{e} = \frac{1}{(p-1)p^{n-1}} = \frac{1}{\#G}.$$

If i is such that $1/(p-1)p^{n-1} < i \leq p/(p-1)p^{n-1}$ then

$$G_{(i)} = \{\sigma \in G : \sigma \equiv 1 \pmod{p^2}\}.$$

Continuing, we find

$$G_{(i)} = \{\sigma \in G : \sigma \equiv 1 \pmod{p^{n-1}}\}$$

for $p^{n-2}/\#G < i \leq p^{n-1}/\#G$, and $G_{(i)} = 1$ for $i > p^{n-1}/\#G = 1/(p-1)$.

We can also compute $\phi(i)$: for $0 < i \leq 1/\#G$, $\phi(i) = i/\#G$. For $1/\#G < i \leq p/\#G$,

$$\begin{aligned}\phi(i) &= \sum_{\sigma\in G} \min(i(\sigma), i) \\ &= \sum_{\sigma\neq 1 \ (p)} i(\sigma) + \sum_{\sigma\equiv 1 \ (p)} i \\ &= (\#G - \#G_1)\frac{1}{\#G} + \#G_1 i = 1 - \frac{1}{p-1} + \frac{\#G}{p} i\end{aligned}$$

where $G_1 = \{\sigma \in G : \sigma \equiv 1 \pmod{p}\}$. Continuing, we find for $p^{n-2}/\#G < i \leq p^{n-1}/\#G$,

$$\phi(i) = n - 1 - \frac{1}{p-1} + \frac{\#G}{p^{n-2}(p-1)} i$$

and the largest $\phi(i_{L/K}) = \phi(1/(p-1)) = n - 1 - 1/(p-1) + p/(p-1) = n$.

So in this case $u_{L/K} = n$, and

$$v(\mathscr{D}_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p}) = u_{L/K} - i_{L/K} = n - 1/(p-1),$$

and therefore $\Delta_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p} = p^{(n-1/(p-1))\phi(p^n)}$.

Fontaine's theorem: Statement and examples. We are now ready to state [F, Théroème A]:

Theorem (Fontaine)**.** *Suppose that a finite flat group scheme Γ over $\mathfrak{O}_K \supset \mathbb{Z}_p$ is killed by p^n. Let the absolute ramification index of $\mathfrak{O}_K$ be e_K (i.e. $v(p) = e_K$), and let L be the field obtained by adjoining the points of Γ to K, a finite Galois extension of K, with $G = \mathrm{Gal}(L/K)$.*

Then $G^{(u)} = \{1\}$ for $u > e_K(n + 1/(p-1))$.

The *points of* Γ are obtained as follows: if $\Gamma = \operatorname{Spec} A$, for A a finite flat $\mathfrak{O}_K$ algebra, then $A \otimes_{\mathfrak{O}_K} K$ is a finite dimensional étale algebra and therefore can be written in the form $\prod_i L_i$ for $L_i \supset K$, with $L_i \hookrightarrow \overline{K}$. Take L to be the compositum of the $L_i \subset \overline{K}$.

Corollary. $u_{L/K} \leq e_K(n + 1/(p-1))$ *(by definition of $u_{L/K}$).*

Corollary. $v(\mathscr{D}_{L/K}) = u_{L/K} - i_{L/K} < e_K(n + 1/(p-1)$.

Example. Let $K = \mathbb{Q}_p$ and $\Gamma = \mu_{p^n} = \operatorname{Spec} \mathbb{Z}_p[X]/\langle X^{p^n} - 1\rangle = \operatorname{Spec} A$, $A \otimes K \simeq \prod_{i=0}^{n} \mathbb{Q}_p(\zeta_{p^i})$ so that $L = \mathbb{Q}_p(\zeta_{p^n})$. Then $u_{L/K} = n$ and $i_{L/K} = 1/(p-1)$. The Fontaine bound is $u_{L/K} \leq n + 1/(p-1)$, which is quite good for p large.

Example (Katz-Mazur). Let R be a ring (e.g. $\mathbb{Z}_p$) and $\epsilon \in R^\times$. Let S be an R-algebra, $n \geq 1$, and define $G_\epsilon(S) = \{(x, i) : x \in S^\times : x^n = \epsilon^i,\ 0 \leq i < n\}$. The composition

$$(x,i)(y,i) = \begin{cases} (xy, i+j), & i+j < n \\ (xy/\epsilon, i+j-n), & i+j \geq n \end{cases}$$

has neutral element $(1, 0)$ and inverse $(\epsilon x^{-1}, n-i)$ if $i \neq 0$ and $(x^{-1}, 0)$ if $i = 0$. This is associative, and is functorial, and therefore G_ϵ is a group functor, represented by a group scheme $G_\epsilon = \operatorname{Spec} \prod_{i=0}^{n-1} R[X]/\langle X^n - \epsilon^i\rangle$.

We have a map

$$\prod_{i=0}^{n-1} R[X]/\langle X^n - \epsilon^i\rangle \to R[X]/\langle X^n - 1\rangle,$$

which gives a map of group schemes $\mu_n \to G_\epsilon$. We also have an injection $\prod_{i=0}^{n-1} R \hookrightarrow \prod_{i=0}^{n-1} R[X]/\langle X^n - \epsilon^i\rangle$, which induces a map $G_\epsilon \to \mathbb{Z}/n\mathbb{Z}$. In a suitable category (which will be explained later), the sequence

$$0 \to \mu_n \to G_\epsilon \to \mathbb{Z}/n\mathbb{Z} \to 0$$

is exact, and therefore $G_\epsilon^0 = \mu_n$ is the connected component and ${G_\epsilon}^{\text{ét}} = \mathbb{Z}/n\mathbb{Z}$ is the étale component.

n kills G_ϵ because $(x, i) \cdots (x, i) = (1, 0)$. If we take $R = \mathbb{Z}_p$, $K = \mathbb{Q}_p$, $n = p$, then $L = \mathbb{Q}_p(\zeta_p, \sqrt[p]{\epsilon})$. The extension L/K is abelian with $H \simeq \mathbb{Z}/p\mathbb{Z}$, but $G = \mathrm{Gal}(L/\mathbb{Q}_p)$ is no longer Galois. It is not necessary but we take $\epsilon \equiv 1 \pmod p$, $\epsilon \not\equiv 1 \pmod{p^2}$.

One computes that $u_{L/K} = 1 + 1/(p-1)$. Fontaine predicts that $u_{L/K} \leq 1(1 + 1/(p-1))$, which is then sharp.

A converse to Krasner's lemma. We now proceed with the proof. We will show first that there is a sort of converse to Hensel's lemma.

Let $\mathbb{Q}_p \subset K \subset L$, with $G = \mathrm{Gal}(L/K)$, $X = \operatorname{Spec} \mathfrak{O}_L$, $v(\pi_K) = 1$. For any finite extension $K \subset E \subset \overline{K}$ and any $t \in \mathbb{R}_{\geq 0}$, let $\mathfrak{m}_E^t = \{x \in \mathfrak{O}_E : v(x) \geq t\}$ [F, §1].

Proposition. *Let $0 < t < 1$. Then $K \subset L$ is unramified iff for all E that*

$$X(\mathfrak{O}_E) = \mathrm{Mor}_{\mathfrak{O}_K}(\operatorname{Spec}\mathfrak{O}_E, X) = \mathrm{Hom}_{\mathfrak{O}_K}(\mathfrak{O}_L, \mathfrak{O}_E) \to X(\mathfrak{O}_E/\mathfrak{m}^t)$$

is surjective.

Proof. For the implication ($\Rightarrow$), take any E. A point of $X(\mathfrak{O}_E/\mathfrak{m}^t)$ is an algebra homomorphism $f : \mathfrak{O}_L \to \mathfrak{O}_E/\mathfrak{m}^t$. Since $\mathfrak{O}_L = \mathfrak{O}_K[\alpha] = \mathfrak{O}_K[X]/\langle f(X)\rangle$, there exists $\beta \in \mathfrak{O}_E$ such that $f(\beta) \equiv 0 \pmod{\mathfrak{m}^t}$. Since $t > 0$, the polynomial has no double roots and thus by Hensel's lemma, there exists a $\widetilde{\beta} \in \mathfrak{O}_E$ such that $f(\widetilde{\beta}) = 0$, so we have a map $\mathfrak{O}_L \to \mathfrak{O}_E$ by $\alpha \mapsto \widetilde{\beta}$, with $\widetilde{\beta} \equiv \beta \pmod{\mathfrak{m}}$, so the map is surjective.

For the implication ($\Leftarrow$), take $E = K'$ to be the unramified extension of K that has residue field k_L, so $K \to K' = L^I \to L$. We have a surjection $\mathfrak{O}_L \to k_L \simeq k_E = \mathfrak{O}_E/\mathfrak{m}_E^t = \mathfrak{O}_E/\mathfrak{m}_E = \mathfrak{O}_E/\pi_K\mathfrak{O}_E$. So by assumption, this lifts $\mathfrak{O}_L \to \mathfrak{O}_E$, so we have an inclusion $L \subset E$, but E is unramified, so $L = E$ is unramified. □

Lemma. *Let $\mathfrak{O}_L = \mathfrak{O}_K[\alpha]$, $K \subset L$ with $G = \mathrm{Gal}(L/K)$. Suppose $\beta \in \overline{K}$, and let $u = v\prod_{\sigma\in G}(\sigma\alpha - \beta)$, $i = \sup_{\sigma\in G} v(\sigma\alpha - \beta)$. Then $u = \phi_{L/K}(i)$.*

Note that u and i depend only on β up to conjugacy (because of the unicity of the extension of v).

Proof. (See [F, Proposition 1.4].) i is the largest of $v(\sigma\alpha - \beta)$. Without loss of generality, we may assume that $v(\alpha - \beta)$ is the largest by considering conjugates. Then

$$v(\beta - \sigma\alpha) \geq \min(v(\beta - \alpha), v(\alpha - \sigma\alpha)),$$

and if the inequality is strict then they have equal valuation, so this is $v(\beta - \alpha) \leq v(\beta - \sigma\alpha)$, so we have equality.

We have

$$\phi_{L/K}(i) = \sum_{\sigma\in G} \min(i(\sigma), i) = \sum_{\sigma\in G} \min(v(\sigma\alpha - \alpha), v(\alpha - \beta)) = \sum_{\sigma\in G} v(\beta - \sigma\alpha) = u.$$

□

We will also need:

Lemma (Krasner's lemma)**.** *If $\alpha, \beta \in \overline{K}$, and $v(\beta - \alpha) > v(\sigma\alpha - \alpha)$ for all $\sigma \in \mathrm{Aut}(\overline{K})$, $\sigma\alpha \neq \alpha$, then $K(\alpha) \subset K(\beta)$.*

Proof. ([L, II, §2, Proposition 3].) Take $\tau \in \mathrm{Aut}(\overline{K})$ fixing β. Then $v(\tau\beta - \tau\alpha) = v(\beta - \alpha) > v(\sigma\alpha - \alpha)$ for all $\sigma \in \mathrm{Aut}(\overline{K})$ such that $\sigma\alpha \neq \alpha$. Then

$$v(\tau\alpha - \alpha) \geq \min(v(\tau\alpha - \beta), v(\alpha - \beta)) > v(\sigma\alpha - \alpha)$$

so τ fixes α. □

Proposition (Fontaine)**.** *If $K \subset L$, $\mathfrak{O}_L = \mathfrak{O}_K[\alpha]$, $v(\pi_K) = 1$, and $\mathfrak{m}_E^t = \{x \in \mathfrak{O}_E : v(x) \geq t\}$, $\mathfrak{O}_E \subset E \subset \overline{K}$. Let $X = \operatorname{Spec}\mathfrak{O}_L$, and $t > 0$.*

If $t > u_{L/K}$, then for all finite extensions $K \subset E$ such that $X(\mathfrak{O}_E/\mathfrak{m}^t) \neq \emptyset$ we have $X(\mathfrak{O}_E) \neq \emptyset$. If this latter condition holds, then $t > u_{L/K} - 1/e_{L/K}$.

Proof of first implication. (See [F, Proposition 1.5].) For the first implication, we have $t > u_{L/K}$. A point is an $\mathfrak{O}_K$-algebra homomorphism $\mathfrak{O}_L = \mathfrak{O}_K[X]/\langle f(X)\rangle \to \mathfrak{O}_E/\mathfrak{m}_E^t$, with $\alpha \mapsto \beta$ with $f(\beta) \equiv 0 \pmod{\mathfrak{m}_E^t}$, i.e. $v(f(\beta)) \geq t > u_{L/K}$. But this is

$$v\left(\prod_{\sigma\in G}(\beta - \sigma\alpha)\right) > u_{L/K} = \sup_{\sigma\in G} v(\beta - \sigma(\alpha)) > i_{L/K} = \sup_{\sigma\neq 1\in G}(\sigma(\alpha) - \alpha).$$

Therefore there is $\tau \in G$ such that $v(\beta - \tau\alpha) > \sup_{\sigma\in G}(\sigma\alpha - \alpha) = \sup_\sigma(\sigma\tau\alpha - \tau\alpha)$. So by Kranser's lemma, $K(\tau\alpha) = L \subset K(\beta) \subset E$, so we have an inclusion $\mathfrak{O}_L \to \mathfrak{O}_E$, so $X(\mathfrak{O}_E) \neq \emptyset$.

For the second implication, first if $K \subset L$ is unramified, $u_{L/K} = 0$, so the theorem is true. If it is ramified, we want to show that if $t \leq u_{L/K} - 1/e_{L/K}$, then there exists an $\mathfrak{O}_E$ for which $X(\mathfrak{O}_E/\pi_K^t\mathfrak{O}_E) \neq \emptyset$, but $X(\mathfrak{O}_E) = \emptyset$. Without loss of generality, we may assume $t = u_{L/K} - 1/e_{L/K}$.

If $K \subset L$ is tamely ramified, then $u_{L/K} = 1$: To be tame is to say that $v(\sigma(\alpha) - \alpha) > 1/e_{L/K}$ implies $\sigma = \mathrm{id}$, which implies that $i(\sigma) = 1/e_{L/K}$ for all $\sigma \neq \mathrm{id}$, which implies that $i_{L/K} = 1/e_{L/K}$, hence

$$u_{L/K} = \phi(i_{L/K}) = \sum_\sigma \min(i_{L/K}, i(\sigma)) = e_{L/K}(1/e_{L/K}) = 1.$$

In this case, $t = 1 - 1/e_{L/K} > 0$. Suppose we have $K \subset K' \subset L$ where the inertia group $I = \mathrm{Gal}(L/K')$. Let E be the totally ramified extension of degree $d < e$ over K'. Then $X(\mathfrak{O}_E) = \{\phi : \mathfrak{O}_L \to \mathfrak{O}_E\} = \emptyset$ since they have different ramification indices. There does exist, however, $f : \mathfrak{O}_L \to \mathfrak{O}_E/\langle\pi_K^t\mathfrak{O}_E\rangle$ where

$$\phi_K^t = \phi_K - 1/e_{L/K} \in \{x \in \mathfrak{O}_E : v(x) \geq 1 - 1/e_{L/K}\} = \langle\pi_K\rangle$$

(as $1 - 1/d < 1 - 1/e_{L/K}$.) We have $f : \mathfrak{O}_L = \mathfrak{O}_K[\alpha] \to \mathfrak{O}_E/\pi_K$ where α is a uniformizer, where we may α to a uniformizer $\beta \in \mathfrak{O}_E$. Then the minimal polynomial of α evaluated at β has $v(\prod_\sigma(\sigma(\alpha) - \beta)) = e_{L/K}(1/e_{L/K}) = 1$.

If $K \subset L$ is wild, then $p \mid e_{L/K}$. Although $t = u_{L/K} - 1/e_{L/K}$, we claim that $t > 1$. As proof, $u_{L/K} \geq 1 + p/e_{L/K}$ so $t \geq 1 + (p-1)/e_{L/K}$, as this is the slope and the function is increasing. Since $t \in (1/e_{L/K})\mathbb{Z}$, $e_{L/K}t \in \mathbb{Z}$, so write $e_{L/K}t = re_{L/K} + s$ where $0 \leq s < e_{L/K}$; then if $K \subset K' \subset L = K'(\alpha)$ where again $K \subset K'$ is unramified, let $f \in \mathfrak{O}_{K'}[X]$ be the minimal polynomial of α. Take $F = K'(\beta)$, where β is a zero of $f(X) - \pi_K^r\alpha^s$.

The claim is that this polynomial is Eisenstein: it has degree $e_{L/K} > s$ so it is still monic, $r \geq 1$ so π_K still divides all other coefficients, and if $s = 0$, $r \geq 2$ so $\pi_K^2 \nmid f_0$ still. So $v(\beta) = 1/e_{L/K}$, and there exists $\mathfrak{O}_L \to \mathfrak{O}_E/\pi_K^t\mathfrak{O}_E$ by $\alpha \mapsto \beta$. Check: $f(\beta) = \pi_K^r\beta^s$, $v(f(\beta)) = v(\pi_K^r\beta^s) = r + s/e_{L/K} = t$, so it is well-defined. If $X(\mathfrak{O}_E) \neq \emptyset$, then $\mathfrak{O}_L \to \mathfrak{O}_E$ implies $L \subset E$ so $L = E$, which implies α, β are both in $E = L$, and therefore $v(\sigma\alpha - \beta) \in (1/e_{L/K})\mathbb{Z}$ for all r, but on the other hand,

$$\prod_\sigma(\sigma(\alpha) - \beta) = f(\beta) = \pi_K^r\beta^s = \pi_E^{er+s}\epsilon$$

so $v(\pi\sigma(\alpha) - \beta) = r + s/e_{L/K} = t = u_{L/K} - 1/e_{L/K}$.

By the lemma, $\sup(v(\sigma\alpha - \beta)) = \phi^{-1}(u_{L/K} - 1/e_{L/K})$, and we know $\phi(i_{L/K}) = u_{L/K}$, so by slopes $\phi(i_{L/K} - 1/de_{L/K}) = u_{L/K} - 1/e_{L/K}$, therefore $\sup(v(\sigma(\alpha) - \beta)) = i_{L/K} - 1/de_{L/K}$, but $1/de_{L/K} \in (1/e_{L/K})\mathbb{Z}$ implies $d = 1$, a contradiction. Therefore $X(\mathfrak{O}_E) = \emptyset$. □

Definition. A *divided power ideal* $I \subset R$ a $\mathbb{Z}_p$-algebra if $x \in I$ implies $x^n/n! \in I$ for all $n \geq 1$.

Then $I^{[n]} = \langle x_1^{a_1} \dots x_t^{a_t}/(a_1! \dots a_t!) : a_1 + \dots + a_t \geq n \rangle$ is also divided power, and $I = I^{[1]} \supset I^{[2]} \supset \dots$. If $\bigcap_n I^{[n]} = 0$, then I is *topologically nilpotent.*

Example. If $\mathfrak{O}_E$ is a ring of p-adic integers, then $\{\alpha : v(\alpha) \geq t\}$ is divided power iff $t \geq e_K/(p-1)$, and topologically nilpotent iff $t > e_K/(p-1)$.

$\langle p \rangle \subset \mathbb{Z}_p$ is a divided power ideal since $p \mid x$ implies $p \mid x^n/n!$. For $p > 2$ it is topologically nilpotent, but for $p = 2$ it is not: $v(2^{2^k}/2^k!) = 2^k - (2^{k-1} + \dots + 1) = 1$.

We have [F, Proposition 1.7]:

Proposition. *Let A be a finite flat $\mathfrak{O} = \mathfrak{O}_K$-algebra, $Y = \operatorname{Spec} A$. Assume that $A \simeq \mathfrak{O}_K[[x_1, \dots, x_m]]/\langle f_1, \dots, f_m \rangle$ and $\Omega^1_{A/\mathfrak{O}_K}$ is a free A/aA-module for some $0 \neq a \in \mathfrak{O}_K$. Then:*

(a) *For every finite flat $\mathfrak{O}_K$-algebra S and for all $I \subset S$ topologically nilpotent divided power ideal, then*

$$Y(S) \simeq \operatorname{img}(Y(S/aI) \to Y(S/I)).$$

(b) *$L = K(Y(\overline{K}))$, then $u_{L/K} \leq v(a) + e_K/(p-1)$.*

This implies [F, Corollary 1.8]:

Corollary. *If $\Gamma = \operatorname{Spec} A$ is a finite flat commutative group scheme over $\mathfrak{O}_K$ killed by $[p^n]$, and $G = \operatorname{Gal}(L/K)$, $L = K(\Gamma(\overline{K}))$, then $G^{(u)}$ is trivial for $u > e_{K/\mathbb{Q}_p}(n + 1/(p-1))$.*

Proof. $\Omega^1_{A/\mathfrak{O}_K} \simeq A \otimes_{\mathfrak{O}} I/I^2$ as A-modules (from our theory of group schemes). If $[p^n]$ kills Γ, then p^n kills I/I^2 (it acts linearly on the tangent space). Therefore $\Omega^1_{A/\mathfrak{O}_K}$ is an A/p^nA-module.

If $n = 1$, i.e. $[p]$ kills Γ, and $e_{K/\mathbb{Q}_p} = 1$, K unramified over $\mathbb{Q}_p$, then $\mathfrak{O}/p\mathfrak{O}$ is a finite field, so I/I^2 is free over $\mathfrak{O}/p\mathfrak{O}$, so $\Omega^1_{A/\mathfrak{O}_K}$ is free over A/pA.

Therefore we may assume that $\Omega^1_{A/\mathfrak{O}_K}$ is free over some A/aA (for the more general result, see [BM]). Write $A = \prod_i A_i$, A_i local. Then

$$A = \prod_i \mathfrak{O}_i[[X_1, \dots, X_m]]/\langle f_1^{(i)}, \dots, f_m^{(i)} \rangle,$$

where the $\mathfrak{O}_i$ are unramified DVR extensions of $\mathfrak{O}_K$. We may replace $\mathfrak{O}$ by $\mathfrak{O}_i$ (the upper numbering stays the same). From (b), we know that $u_{L_i/K} \leq v(a) + e_K/(p-1) \leq nv(p) + e_K/(p-1) = e_K(n + 1/(p-1))$, where L_i adjoins the points of $\operatorname{Spec} A_i$ to K, and L is the compositum. Then $u_{L/K} \leq e_K(n + 1/(p-1))$, and $G(L/K)^{(u)}/H_i \simeq (G(L/K)/H_i))^{(u)}$ (we need to show that the numbering behaves well with respect to quotients). □

Proof of (a) $\Rightarrow$ (b). We will show that for any $t > v(a) + e_K/(p-1)$, we have the property in the the converse to Krasner's lemma (for every $K \subset E \subset \overline{K}$ finite, if $X(\mathfrak{O}_E/\pi_K^t\mathfrak{O}_E) \neq \emptyset$ then $X(\mathfrak{O}_E) \neq \emptyset$). Then $t > u_{L/K} - 1/e_{L/K}$, which implies that $u_{L/K} \leq v(a) + e_K/(p-1) + 1/e_{L/K}$.

To show that $t > v(a) + e_K/(p-1)$, we let $K \subset E \subset \overline{K}$ be finite. Suppose we have a point modulo π_K^t: $\mathfrak{O}_L \to \mathfrak{O}_E/\pi_k^t\mathfrak{O}_E$. We want to show that there exists $\mathfrak{O}_L \to \mathfrak{O}_E$. Let L be the field generated by the points of Y. Then $Y(\mathfrak{O}_L)$ has all points, so for every E, $\#Y(\mathfrak{O}_E) \leq \#Y(\mathfrak{O}_L)$, with equality iff $L \subset E$ iff we have a map $\mathfrak{O}_L \to \mathfrak{O}_E$.

Now $\pi_K^t \mathfrak{O}_E = aI$, $I = \{A \in \mathfrak{O}_E : v(\alpha) \geq t - v(a) > e_K/(p-1)\}$. I is a topologically nilpotent divided power ideal. The kernel

$$I' = \ker(\mathfrak{O}_L \to \mathfrak{O}_E/\pi_K^t \mathfrak{O}_E \to I\mathfrak{O}_E)$$

is also a topologically nilpotent divided power ideal. So now take $S = \mathfrak{O}_E$, $I = I$ and $S = \mathfrak{O}_L$, $I = I'$. Then by (a),

$$Y(\mathfrak{O}_E) \simeq \operatorname{img}\left(Y(\mathfrak{O}_E/aI) \to Y(\mathfrak{O}_E/I)\right)$$

and

$$Y(\mathfrak{O}_L) \simeq \operatorname{img}\left(Y(\mathfrak{O}_L/aI') \to Y(\mathfrak{O}_L/I')\right).$$

we have a diagonal map and therefore we have an injection on the right, and hence all are isomorphic. Hence $\#Y(\mathfrak{O}_L) \leq \#Y(\mathfrak{O}_E)$. □

Remark. It would be enough to prove that if $A \simeq \mathfrak{O}[[X_1, \ldots, X_m]]/\langle f_1, \ldots, f_m\rangle$ finite flat, and suppose $0 \neq a \in \mathfrak{O}$ kills $\Omega^1_{A/\mathfrak{O}}$, then if there exists $B \to A \to 0$, with B also complete intersection finite flat, then $\Omega^1_{B/\mathfrak{O}}$ is free over B/aB. (This would be a significant shortcut, but it is not yet known.)

Proof of (a). Write $J = \langle f_1, \ldots, f_m\rangle \subset \mathfrak{O}[[x_1, \ldots, x_m]]$, x_i a basis of $\mathfrak{m}/(\mathfrak{m}^2 + \pi_K\mathfrak{m})$, and $\Omega^1_{A/\mathfrak{O}}$ free over A/aA, $0 \neq a \in \mathfrak{O}$. This means $\partial f_i/\partial x_j = ap_{ij}$ with $p_{ij} \in A$. The matrix (p_{ij}) is invertible, because it has inverse obtained from $a\,dx_i = \sum_j q_{ij}\,df_j$.

Suppose we start with a point of Y modulo aI, and we must lift it uniquely modulo I. Consider $I^{[n]}$; we have $\bigcap_n I^{[n]} = 0$. We will lift in steps. Assume we have a point modulo $aI^{[n]}$. We will now lift the image modulo $I^{[n]}$ to a point modulo $aI^{[n+1]}$. Lift to $u_1, \ldots, u_m \in S$ such that $f_i(u_1, \ldots, u_m) \in aI^{[n]}$. We want to find $\epsilon_i \in I^{[n]}$, unique modulo $I^{[n+1]}$ such that $f(u_1 + \epsilon_1, \ldots, u_m + \epsilon_m) \in aI^{[n+1]}$.

Write a Taylor expansion: for $f_i \in J$,

$$f_i(u_1 + \epsilon_1, \ldots, u_m + \epsilon_m) = f_i(u_1, \ldots, u_m) + \sum_{j=1}^{m} \frac{\partial f_i}{\partial x_j}(u_1, \ldots, u_m)\epsilon_j + \sum_{|r|\geq 2} \frac{\partial^r f_i}{\partial x_r}(u_1, \ldots, u_m)\frac{\epsilon^r}{r!}$$

which converges because the ideal is a topologically nilpotent divided power ideal.

Let $a\lambda_i = f_i(u_1, \ldots, u_m)$ for some $\lambda_i \in I^{[n]}$. We have $\partial f_i/\partial x_j = ap_{ij} + \phi$ where $p_{ij} \in \mathfrak{O}[[x_1, \ldots, x_m]]$, $\phi \in J$. Then $(\partial f_i/\partial x_j)(u_1, \ldots, u_m)\epsilon_j = (ap_{ij}(u_1, \ldots, u_m) + \phi(u_1, \ldots, u_m))\epsilon_j$, and since the $\phi(u_1, \ldots, u_m) \in aI^{[n]}I^{[n]} \subset aI^{[n+1]}$, we have

$$\phi \in ap_{ij}(u_1, \ldots, u_m) \text{ modulo } aI^{[n+1]}.$$

For the last piece, for $f \in J$, then $\partial f/\partial x_i \in a\mathfrak{O}[[x_1, \ldots, x_m]] + J$ and the same is true of all higher derivatives. Substituting u, $(\partial^r f/\partial x_r)(u_1, \ldots, u_m) \in aS + aI^{[n]} \subset aS$. The monomials are in $(I^{[n]})^{[2]} \subset I^{[n+1]}$ (see the lemma following), so the whole thing is in $aI^{[n+1]}$.

We are left to solve

$$0 = a\lambda_i + \textstyle\sum_j ap_{ij}(u_1, \ldots, u_m)\epsilon_j \pmod{aI^{[n+1]}},$$

which is the same as

$$0 = \lambda_i + \textstyle\sum_j p_{ij}(u_1, \ldots, u_m)\epsilon_j \pmod{I^{[n+1]}},$$

which has a unique solution (modulo $I^{[n+1]}$) because the matrix defining the p_{ij} is invertible (due to the freeness of the Kahler differentials), and is in $I^{[n]}$ since $\lambda_i \in I^{[n]}$. □

Lemma. $(I^{[n]})^{[2]} \subset I^{[n+1]}$.

Proof. Let xy be such that $x, y \in I^{[n]}$, $x^2/2$ has $x \in I^{[n]}$; we want to show that $x \in I^{[n]}$ implies $x^2/2 \in I^{[n+1]}$. We may assume that $p = 2$, and that

$$x = \frac{x_1^{a_1} \dots x_t^{a_t}}{a_1! \dots a_t!} \text{ implies } \frac{x^2}{2} \in I^{[n+1]}.$$

We may replace x_i by the one with the smallest valuation. $x = \alpha^{a_1+\dots+a_t}/a_1! \dots a_t!$; the hardest case is $x = \alpha^n/n! \in I^{[n]}$ implies $(1/2)(\alpha^n/n!)^2 \in I^{[n+1]}$, but this is $\alpha^{2n}(2n)!(1/2)\binom{2n}{n} \in I^{[2n]} \subset I^{[n+1]}$. □

Fontaine's theorem: An overview.

Theorem (Fontaine)**.** *There exists no abelian variety over $\mathbb{Q}$ having good reduction at all primes; equivalently, there are no abelian varieties over $\mathbb{Z}$.*

The method of proof will also give the result for "small" fields K, e.g. $\mathbb{Q}(\zeta_n)$ for $n \leq 7$. We will examine the torsion $A[p]$ and show it cannot exist for certain primes, say, $p = 2$; the p-torsion is a finite flat group scheme of rank p^{2g}, hence affine and can be investigated by the methods we have learned so far.

Here is an outline of the proof: Let G be any finite flat group scheme over $\mathfrak{O}_K$ annihilated by p. Let $K \subset L = K(G(\overline{K}))$. We will show the following:

(1) L/K is unramified outside p.
(2) L/K is "moderately" ramified over p (Fontaine).
(3) $\delta_L = |\Delta_{L/\mathbb{Q}}|^{1/[L:\mathbb{Q}]} < \delta_K p^{1+1/(p-1)}$.
(4) By the Odlyzko discriminant bounds, $[L : \mathbb{Q}]$ is bounded.
(5) By class field theory, $\mathrm{Gal}(L/K)$ is a p-group.
(6) Any finite, flat, commutative, *simple* (having no closed subgroup scheme) group scheme over $\mathfrak{O}_K$ of p-power order has order p.
(7) Filter $A[p]$ such that all quotients are simple. (We can get away even though we have not defined quotients because they correspond to Galois modules.) Suppose we know these quotients for p and $\mathfrak{O}_K$.
(8) Conclude that $A[p]$ or $A^\vee[p]$ has "too many points" when reduced modulo a prime of $\mathfrak{O}_K$ (by the Weil bounds.)

Proof of (6). Let G be a p-power order and simple. $G[p] \hookrightarrow G$, so this must be an isomorphism, and therefore G is annihilated by P. So if we can prove that $\mathrm{Gal}(L/K)$ is a p-group (assuming (5)), then $G/K = G \times_{\mathrm{Spec}\,\mathfrak{O}_K} \mathrm{Spec}\,K$ corresponds to a finite group of order $\#G$ together with an action of $\mathrm{Gal}(\overline{K}/K)$ by automorphisms. This action factors via $\mathrm{Gal}(L/K)$, which is a p-group. Since the number of fixed points is congruent to 0 modulo p, there exists a nontrivial subgroup of order p fixed by $\mathrm{Gal}(\overline{K}/K)$, hence a subgroup scheme $G_p \hookrightarrow G/K$; from the exercises, this corresponds to a subgroup over $\mathscr{O}_K$ which by simplicity implies $G_p = G$ and thus G has order p. □

Example. If $p = 2$, $K = \mathbb{Q}$, we know that any $G/\mathbb{Z}$ of order 2 is either μ_2 or $\mathbb{Z}/2\mathbb{Z}$; and if $K = \mathbb{Q}(\zeta_7)$, $G/\mathbb{Z}[\zeta_7]$ of order 2 must either be μ_2, $\mathbb{Z}/2\mathbb{Z}$, G_π, $G_{\overline{\pi}}$ where $\pi\overline{\pi} = 2$ (see the exercises); these are just $G_{a,b}$ for factorizations $ab = 2$.

Let $G = \operatorname{Spec} A$ be a finite flat commutative group scheme over $\mathfrak{O}_K$ annihilated by p, and let $L = K(G(\overline{\mathbb{Q}}))$.

Proposition (1)**.** *$K \subset L$ is unramified outside p.*

Proof. Let $A \supset I$ be the augmentation ideal. We know that $[p](I) = 0$. Looking at the comultiplication map modulo I^2, $[p]I = pI \pmod{I^2}$; therefore p annihilates I/I^2, so it annihilates $\Omega_{A/\mathfrak{O}_K} = A \otimes_{\mathfrak{O}_K} I/I^2$. Let $\mathfrak{q}$ be a prime of $\mathfrak{O}_K$ *not* lying over p. Then for $k(\mathfrak{q}) = \mathfrak{O}_K/\mathfrak{q}\mathfrak{O}_K$, $A \otimes_{\mathfrak{O}_K} k(\mathfrak{q})$ is étale over $k(\mathfrak{q})$ (since the differentials are killed by p, a unit in the field, and therefore vanish). $A \otimes_{\mathfrak{O}_K} \mathfrak{O}_\mathfrak{q}$ is finite and étale as well over $\mathfrak{O}_\mathfrak{q}$ (the differentials again vanish). The two categories of finite étale algebras over $k(\mathfrak{q})$ and $\mathfrak{O}_\mathfrak{q}$ are the same (we reduce or lift via Hensel), so $A \otimes_{\mathfrak{O}_K} \mathfrak{O}_\mathfrak{q}$ is the product of extension rings $\mathfrak{O}_{\mathfrak{q}'} \supset \mathfrak{O}_\mathfrak{q}$, so local extension is unramified at $\mathfrak{q}$ as claimed. □

The statement of (2) follows from Fontaine's result: For $L_\mathfrak{q}/K_\mathfrak{p}$, we have

$$v(\mathscr{D}(L_\mathfrak{q}/K_\mathfrak{p})) < e_{K_\mathfrak{p}}(1 + 1/(p-1)),$$

where $e_{K_\mathfrak{p}}$ is the absolute ramification index of $\mathfrak{p}$, and $v(\pi_\mathfrak{p}) = 1$ for $\pi_\mathfrak{p}$ a uniformiser.

Proposition (3)**.** *$\delta_L < \delta_K p^{1+1/(p-1)}$.*

Proof. $\Delta_{L/\mathbb{Q}} = (N_{K/\mathbb{Q}}\Delta_{L/K})\Delta_{K/\mathbb{Q}}^{[L:K]}$ by familiar formulae, so

$$\delta_L = \delta_K (N_{K/\mathbb{Q}}\Delta_{L/K})^{1/[L:\mathbb{Q}]}.$$

We know that L is unramified outside p so this norm is only divisible by primes lying over p.

For any prime $\mathfrak{p}$ of K lying over p, since L/K is Galois it factors $\mathfrak{p}\mathfrak{O}_L = (\mathfrak{q}_1 \dots \mathfrak{q}_r)^e$ where we let $f = f(\mathfrak{q}_i/\mathfrak{p})$ so that $n = ref$. Then $\mathscr{D}_{L_{\mathfrak{q}_i}/K_\mathfrak{p}} = \mathfrak{q}_i^m$, and therefore $m < e(e_{K_\mathfrak{p}})(1 + 1/(p-1))$. We conclude that

$$(\mathscr{D}_{L/K})_\mathfrak{p} = (\mathfrak{q}_1 \dots \mathfrak{q}_r)^m = (\mathfrak{p}\mathfrak{O}_L)^{m/e}$$

where $m/e < e_{K_\mathfrak{p}}(1 + 1/(p-1))$. Taking the norm from L/K we obtain

$$(\Delta_{L/K})_\mathfrak{p} = \mathfrak{p}^{frm} = \mathfrak{p}^{[L:K]m/e} = s_\mathfrak{p}$$

so $\operatorname{ord}_\mathfrak{p}(\Delta_{L/K}) < [L:K]e_{K_\mathfrak{p}}(1 + 1/(p-1))$.

Now let $p\mathfrak{O}_K = \prod_i \mathfrak{p}_i^{e_i}$, with $f_i = f(\mathfrak{p}_i/p)$ and $s_\mathfrak{p} = s_i$. Then

$$\begin{aligned}\operatorname{ord}_p(N_{K/\mathbb{Q}}(\Delta_{L/K})) = \sum_i s_i f_i &< \sum_i [L:K]e_i(1 + 1/(p-1))f_i \\ &= [L:K](1 + 1/(p-1)) \sum_i e_i f_i = [L:\mathbb{Q}](1 + 1/(p-1))\end{aligned}$$

as claimed. □

For (4), we use lower bounds on discriminants for totally imaginary fields (see the table below) [Mar, Table IV]. If $[L:\mathbb{Q}] = n = r_1 + 2r_2$, then there exist constants $a_1, a_2 \in \mathbb{R}_{>0}$ depending only on (r_1, r_2) such that

$$\Delta_L = |\Delta_{L/\mathbb{Q}}|^{1/n} \geq a_1^{r_1/n} a_2^{2r_2/n}.$$

N	Lower bound	N	Lower bound	N	Lower bound
2	1.7221	72	15.3591	360	19.5903
4	3.2545	76	15.5549	380	19.6813
6	4.5570	80	15.7371	400	19.7652
8	5.6593	84	15.9071	480	20.0443
10	6.6003	88	16.0663	500	20.1029
12	7.4128	92	16.2158	600	20.3483
14	8.1224	96	16.3563	700	20.5363
16	8.7484	100	16.4889	720	20.5688
18	9.3056	110	16.7898	800	20.6858
⋮	⋮	⋮	⋮	⋮	⋮
64	14.9193	320	19.3823	3000	21.6585
68	15.1479	340	19.4911	4000	21.7825

If δ_L is reasonably small, we obtain an upper bound for $[L:\mathbb{Q}]$.

Theorem. *If G is a finite, flat, simple, commutative group scheme of 2-power order over $\mathbb{Z}$, then $G \simeq \mathbb{Z}/2\mathbb{Z}$ or $G \simeq \mu_2$.*

Proof. G is killed by 2 by the above arguments. Replace G by $\widetilde{G} = G \times G_{-1}$, where G_ϵ is the Katz-Mazur group scheme annihilated by $n = 2$, $\epsilon \in R^\times$; recall $G_\epsilon(S) = \{(x,i) : x \in S, 0 \le i < n-1,\ x^n = \epsilon^i\}$, with

$$1 \to \mu_n \to G_\epsilon \to \mathbb{Z}/n\mathbb{Z} \to 1.$$

Let $L = \mathbb{Q}(\widetilde{G}(\overline{\mathbb{Q}}) \supset \mathbb{Q}(i) \supset \mathbb{Q}$. L is unramified outside 2 and $\delta_L < \delta_Q 2^{1+1/(2-1)} = 4$ which implies that $[L:\mathbb{Q}] \le 4$ by the Odlyzko bound. Hence $L = \mathbb{Q}(i)$ or L is a quadratic extension of $\mathbb{Q}(i)$. So $\mathrm{Gal}(L/\mathbb{Q})$ is a 2-group, and by our standard arguments, $L \supset \mathbb{Q}(G(\overline{Q}) = L' \supset \mathbb{Q}$, and the order of G is 2. So over $\mathbb{Q}$, it must be $G_{a,b}$ which over $\mathbb{Z}$ gives us the two above. □

Example: $\mathbb{Z}[\zeta_7]$. We now give an example outside of $\mathbb{Z}$.

Theorem. *The only simple 2-power order group schemes over $R = \mathbb{Z}[\zeta_7]$ are μ_2, $\mathbb{Z}/2\mathbb{Z}$, G_π, $G_{\overline{\pi}}$, where $G_\pi = \operatorname{Spec} R[X]/\langle X^2 + \pi X\rangle$ with group law $X \mapsto X + X' + \overline{\pi}XX'$, and $\pi = (1+\sqrt{-7})/2$.*

To do this, we prove:

Theorem. *If G is a finite, flat commutative group scheme over $\mathbb{Z}[\zeta_7]$, then G has order 2.*

Proof. Take $\widetilde{G}$ to be the product of G with all of the Galois conjugates of G over $\mathbb{Q}$ together with all G_ϵ for $n = 2$, $\epsilon \in \mathbb{Z}[\zeta_7]^\times/\mathbb{Z}[\zeta_7]^{\times 2}$. Let $L = K(\widetilde{G}(\overline{\mathbb{Q}}))$ containing $K = \mathbb{Q}(\zeta_7) \subset \mathbb{Q}(\zeta_7, i, \sqrt{\epsilon_1}, \sqrt{\epsilon_2})$ (of degree 48) if we let $\mathbb{Z}[\zeta_7]^\times = \langle -\zeta_7\rangle \times \langle \epsilon_1\rangle \times \langle \epsilon\rangle$. Then $\delta_L < \delta_K(2^{1+1/(2-1)}) = 7^{5/6} \cdot 4 \approx 20.245$, so from the table, $[L:\mathbb{Q}] \le 600$, so

$$\deg L/\mathbb{Q}(\zeta_7, i, \sqrt{\epsilon_1}, \sqrt{\epsilon_2}) \le \lfloor 600/48 \rfloor = 12.$$

$\mathbb{Q}(\zeta_7) = K \subset L$ is unramified outside 2. We want to show that $\mathrm{Gal}(L/K)$ is a 2-group. We have

$$\mathbb{Q} \subset_6 \mathbb{Q}(\zeta_7) \subset \mathbb{Q}(\zeta_{28}) \subset_4 \mathbb{Q}(\zeta_{28}, \sqrt{\epsilon_1}, \sqrt{\epsilon_2}) \subset_{\le 12} L$$

The extension $\mathbb{Q}(\zeta_{28})$ is the maximal abelian subextension, since if $F \subset L$ is such, then $\mathbb{Q}(\zeta_{28}) \subset F \subset \mathbb{Q}(\zeta_{56})$, which has $\delta = 4 \cdot 7^{5/6}$, a contradiction (the inequality is strict). So $E = \mathbb{Q}(\zeta_{28}) \subset L$ gives the commutator subgroup π'.

We will show: π' is a 2-group. $\#\pi' \leq 48$ is solvable, so we have $\pi' \supset \pi'' \supset \cdots \supset \{1\}$.

Step 1. π'/π'' is a 2-group. If not, there exists $E = \mathbb{Q}(\zeta_{28}) \subset F \subset L$ where F is abelian of odd degree unramified outside 2. Let $\widetilde{F} \supset E$ be the maximal abelian unramified outside primes $\mathfrak{p}_1, \mathfrak{p}_2$ lying over 2 and at most tamely ramified at $\mathfrak{p}$. By class field theory, $\mathrm{Gal}(\widetilde{F}/E)$ is the ray class group $\mathrm{Cl}_{\mathfrak{p}}$ modulo $\mathfrak{p}$, and we have an exact sequence

$$1 \to (\mathfrak{O}/\mathfrak{p}_1\mathfrak{p}_2)^\times / \operatorname{img} \mathfrak{O}^\times \to \mathrm{Cl}_{\mathfrak{p}} \to \mathrm{Cl} \to 0.$$

But $\mathbb{Q}(\zeta_{28})$ has $\mathrm{Cl}(\mathbb{Z}[\zeta_{28}]) = 1$ (one shows it has a trivial Hilbert class field via the Odlyzko bounds, since the two have the same Hilbert class field and the degree is bounded). So we obtain

$$(\mathfrak{O}/\mathfrak{p}_1\mathfrak{p}_2)^\times / \operatorname{img} \mathfrak{O}^\times \simeq \mathbb{F}_8^\times \times \mathbb{F}_8^\times / \operatorname{img} \mathbb{Z}[\zeta^{28}]^\times = 1.$$

It suffices to show that all simple group schemes have order 2.

Claim. If every extension L of $\mathbb{Q}(\zeta_7)$ such that we get L by adjoining the points of a group scheme killed by 2 to $\mathbb{Q}(\zeta_7)$ has: $\delta_L < \delta_{Q(\zeta_7)} 2^{1+1/(2-1)} = 4 \cdot 7^{5/6}$, $\mathbb{Q}(\zeta_7) \subset L$ is unramified outside 2, $\mathbb{Q} \subset L$ is Galois, $\sqrt{\epsilon} \in L$ for all $\epsilon \in \mathbb{Z}[\zeta_7]^\times$, and $[L : \mathbb{Q}(\zeta_7)]$ is a power of 2, then all simple 2-group schemes have order 2.

To verify the conditions of the claim, we have

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_7) \subset \mathbb{Q}(\zeta_7, i, \sqrt{\epsilon_1}, \sqrt{\epsilon_2}) \subset L$$

where $\mathbb{Z}[\zeta_7]^\times = \langle \pm\zeta_7 \rangle \times \epsilon_1^{\mathbb{Z}} \times \epsilon_2^{\mathbb{Z}}$. The Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is solvable, since $L/\mathbb{Q}(\zeta_7, i, \sqrt{\epsilon_1}, \sqrt{\epsilon_2})$ has degree ≤ 12. We have π/π' covering the Galois group $\mathbb{Q} \subset \mathbb{Q}(\zeta_7, i)$.

The claim is that π' is a 2-group. We will show that π'/π'' is a 2-group, etc. Class field theory tells us there is a maximal abelian unramified extension H of a number field F with $\mathrm{Gal}(H/F) \simeq \mathrm{Cl}(\mathfrak{O}_F)$, and one F_S that is unramified outside a finite set S of places, and

$$0 \to (\prod_{\mathfrak{p} \in S} (\mathfrak{O}_{\mathfrak{p}}^\times)/(\operatorname{img} \mathfrak{O}_F^\times) \to \mathrm{Gal}(F_S/F) \to \mathrm{Gal}(F_\emptyset/F) = \mathrm{Cl}(\mathfrak{O}_F) \to 0.$$

In our situation, we take S to be the primes dividing 2, including ∞. If we reduce

$$0 \to \textstyle\prod_{1\ (\mathfrak{p})}/(\operatorname{img} \mathfrak{O}_F^\times) \to \prod_{\mathfrak{p} \in S} \mathfrak{O}_{\mathfrak{p}}^\times/(\operatorname{img} \mathfrak{O}_F^\times) \to \prod_{\mathfrak{p} \in S} k_{\mathfrak{p}}^\times/(\operatorname{img} \mathfrak{O}_F^\times) \to 0.$$

The first is a pro p-group, and the latter has order prime to p isomorphic to the Galois group of the maximal extension uramified outside S which is tamely ramified at $\mathfrak{p} \in S$.

Every abelian extension of F unramified outside p is a p-group iff $h_F = \#\,\mathrm{Cl}(F)$ is a power of p and $\mathfrak{O}_F^\times \to \prod_{\mathfrak{p}} k_{\mathfrak{p}}^\times \to 0$. For $F = \mathbb{Q}(\zeta_{28})$, $\#\,\mathrm{Cl}(\mathfrak{O}_F) = 1$, and the Galois group $\mathbb{F}_8^\times \times \mathbb{F}_8^\times$ generated by $\langle \zeta_{28}, 1 - \zeta_{28} \rangle$, and thus π'/π'' is a 2-group.

Claim. If π is a finite group, π'/π'' is a 2-group, and $\#\pi'' < 9$. Then π' is a 2-group.

Proof of claim. π' is solvable, so it suffices to show that π''/π''' is a 2-group (and then repeat). Let $\pi''' \subset H \subset \pi''$ where $\pi''' \subset H$ is the 2-part, and $H \subset \pi''$ is odd. We have

$$1 \to \pi''/H \to \pi'/H \to \pi'/\pi'' \to 1.$$

The group π''/H is odd order, and π/π'' is 2-power, so the groups have relatively prime orders, so the sequence is split (it is a semi-direct product).

π'/π'' acts trivially on π''/H because $\pi \to \mathrm{Aut}(\pi''/H)$, where π''/H is odd < 9 and hence cyclic and thus abelian, so π' is contained in the kernel. Therefore π/H is a direct product, and thus abelian, but π'/π'' is maximal abelian, so $\pi'' = H$, and π''/π''' is indeed a 2-group. □

The lemma is sharp: take the semi-direct product of $(\mathbb{F}_3 \times \mathbb{F}_3)$ with $SL_2(\mathbb{F}_3)$.

So $\#\pi'/\pi'' \geq 4$. If ≥ 8, $\#\pi'' \leq 6$, we are done by the lemma. If $= 4$, show (by Odlyzko) that $\mathrm{Cl}(\mathbb{Q}(\zeta_{28}, \sqrt{\epsilon_1}, \sqrt{\epsilon_2}) = 1$ by the Odlyzko bounds, so there is no tame extension and π''/π''' is a 2-group. If $= 1$, we are done by solvability, and $\# \geq 2$, $\#\pi''' \leq 6$, so we apply the lemma to π'.

So to finish, we know $\#\pi'/\pi'' \geq 4$. Therefore if $\#\pi'/\pi'' = 8$ and $\#\pi'' \leq 6$, and the lemma applies. If $\#\pi/\pi' = 4$, then work to show that $h_{\mathbb{Q}(\zeta_{28}, \sqrt{\epsilon_1}, \sqrt{\epsilon_2})} \leq 2$ by the Odlyzko bounds, so there does not exist a tame extension unramified outside 2, hence π''/π''' is a 2-group. □

Reduction to the étale case.

Lemma. *If R is a Dedekind domain, and G is a finite flat group scheme over R, then we can consider G over the quotient field K. The goal is to show that there is a one-to-one correspondence between closed flat subgroup scheme between G over R and G over K.*

Proof. If R is a Dedekind domain, A is a flat R-module iff torsion-free. Always have flat implies torsion-free over a domain, because if $0 \neq \lambda \in R$, $R \xrightarrow{\lambda} R$ is injective, so tensoring with A we have $A \xrightarrow{\lambda} A$ injective. Conversely, it suffices to show that $(I \subset R) \otimes A$ is still injective. If we localize, $R_{\mathfrak{p}}$ is a PID, so $I \subset R_{\mathfrak{p}}$ is principal, $I = \langle a \rangle \simeq R$, and thus $R \xrightarrow{a} R$, tensoring over R with A we have $A \xrightarrow{a} A$ is injective since it is torsion-free, and thus $A_{\mathfrak{p}}$ is flat for all $\mathfrak{p}$, and thus A is flat.

If $G = \mathrm{Spec}\, A$, where A is a finite flat R-algebra, a closed flat subgroup scheme H of G is $\mathrm{Spec}\, A/J$ where J is an ideal that is a Hopf ideal ($c(J) \subset A \otimes J + J \otimes A$) and A/J is flat. Now $G/K = \mathrm{Spec}(A \otimes K)$; we have a map of ideals in A to ideals in $A \otimes K$ by $J \mapsto J \otimes K$. If $J \subset A \otimes K$ is an ideal, then if we tensor the injection $R \hookrightarrow K) \otimes_R A$ we have an inclusion $A \hookrightarrow A \otimes_R K$, so we can take $J \cap A$, which is an ideal of A. Indeed, $A/(J \cap A)$ is flat, because we have

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A \cap J & \longrightarrow & A & \longrightarrow & A/(A \cap J) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & J & \longrightarrow & A \otimes K & \longrightarrow & (A \otimes K)/J & \longrightarrow & 0
\end{array}$$

is Cartesian, so by a well-known diagram chase, $A/(A \cap J)$ is torsion free, hence flat.

Therefore we claim that we have a one-to-one correspondence between Hopf ideals $J \subset A$ such that A/J is flat, and Hopf ideals of $A \otimes K$ by $J \mapsto J \otimes K$ and $J' \mapsto J' \cap A$. If $J \subset A$, then $(J \otimes K) \cap A = J$; clearly we have $\supset$, and if $x \in A$, there exists a $\lambda \in R$ such that $\lambda x = 0$, and looking at $x \in A/J$ which

is flat, and hence torsion free, we find $x \in J$. Similarly, $(J' \cap A) \otimes K = J'$. Finally, we need to check that Hopf ideals correspond to Hopf ideals. If we have $c(J) \subset A \otimes J + J \otimes A$, this remains true after tensoring with K. Conversely, if we have $J' \subset A \otimes K$ a Hopf ideal, and $c(J') \subset (A \otimes_R K) \otimes_K J' + J' \otimes_K (A \otimes_R K)$, and we want to show for $J = J' \cap A$, that $c(J) \subset A \otimes J + J \otimes A$. We know that $c(J) \subset ((A \otimes J + J \otimes A) \otimes K) \cap (A \otimes A) \subset A \otimes J + J \otimes A$, since if we do the same thing as above, since $A \otimes A/(A \otimes J + J \otimes A) \simeq A/J \otimes A/J$ is flat. □

We can apply this as in the following example:

Example. Let $R = \mathbb{Z}[(1+\sqrt{-7})/2] = \mathbb{Z}[\pi]$. We have the 2-group schemes $\mathbb{Z}/2\mathbb{Z}$, μ_2, and G_π and $G_{\overline{\pi}}$, since $2 = \pi\overline{\pi}$, where $G_\pi = \operatorname{Spec} R[X]/\langle X^2 - \pi X\rangle$, with group law $X \mapsto X + X' - \overline{\pi} X X'$.

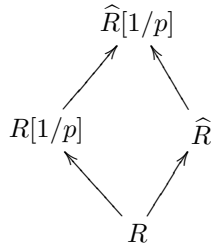
Consider $G_\pi \times G_{\overline{\pi}}$, of order 4, given by $A = R[X,Y]/\langle X^2 - \pi X, Y^2 - \overline{\pi} Y$. What are the closed flat subgroup schemes of order 2? If we tensor with $K = \mathbb{Q}(\sqrt{-7})$, it has the 4 points $\{(0,0),(\pi,0),(0,\pi),(\pi,\overline{\pi})\}$. The action of Galois $\operatorname{Gal}(\overline{K}/K)$ is trivial, and thus there are three subgroup schemes generated by each of the three nontrivial points (it is a group of type 2-2).

For example, $J \subset A \otimes K$ for $\langle(\pi,0)\rangle$ is $J = \langle Y\rangle$ since $y = 0$ on $(0,0)$ and $(\pi,0)$. So we have $H = \operatorname{Spec}(A/\langle Y\rangle) \simeq \operatorname{Spec} R[X]/\langle X^2 - \pi X\rangle \simeq G_\pi$. Similarly, $\langle(0,\overline{\pi})$ gives $\operatorname{Spec}(A/\langle X\rangle) \simeq G_{\overline{\pi}}$. Finally, for $\langle(\pi,\overline{\pi})\rangle$, we take $J \subset A \otimes K$ is $\langle Y - (\overline{\pi}/\pi)X$. So

$$\begin{aligned} J \cap A &= \{f(X) = bX + cY + dXY \in A : f(\pi,\overline{\pi}) = 0\} \\ &= \{bX + cY + dXY : \pi b + \overline{\pi} c + 2d = 0\} \\ &= \langle \overline{\pi} X - XY, \pi Y - XY\rangle. \end{aligned}$$

This may not at first appear to be flat, but the map $A = R[X,Y]/\langle X^2 - \pi X, Y^2 - \overline{\pi} Y\rangle \to R[T]/\langle T^2 - T\rangle$ by $X \mapsto \pi T$, $Y \mapsto \overline{Y} T$, since $(\pi T)^2 = \pi^2 T = \pi(\pi T)$. It is surjective because $\gcd(\pi,\overline{\pi}) = 1$, and the kernel consists of polynomials $a + bX + cY + dXY$ for which $a + b\pi T + c\overline{\pi} T + d\pi\overline{\pi} T^2 = 0$, which requires $a = 0$ and $b\pi + c\overline{\pi} + 2d = 0$, which is exactly I. Hence the third group scheme is $\mathbb{Z}/2\mathbb{Z}$.

An equivalence of categories. For the material in this section, see [J, Lemma 2.4.4, Remark 2.4.10] or [A, Theorem 2.6]. Let R be noetherian, $p \in R$, and $\widehat{R} = \varinjlim_n R/\langle p^n\rangle$, with maps



Let $\mathfrak{C}$ be the category of triples (M_1, M_2, ϕ) where M_1 is a finitely generated $\widehat{R}$-module, M_2 is a finitely generated $R[1/p]$-module, and

$$\phi : M_1 \otimes_{\widehat{R}} \widehat{R}[1/p] \simeq M_2 \otimes_{R[1/p]} \widehat{R}[1/p].$$

Theorem. *The functor*

$$M \mapsto (M \otimes_R \widehat{R}, M \otimes_R R[1/p], \mathrm{id} \otimes \widehat{R}[1/p])$$

induces an equivalence of categories between the category of finitely generated R-modules and $\mathfrak{C}$.

Corollary. *The functor*

$$G \mapsto (G \times_{\operatorname{Spec} R} \operatorname{Spec} \widehat{R}, G \times_{\operatorname{Spec} R} R[1/p], \mathrm{id})$$

is an equivalence of categories between the category of finite flat group schemes over R and triples (G_1, G_2, ϕ) where G_1, G_2 are finite flat group schemes over $\widehat{R}$ and $R[1/p]$, respectively.

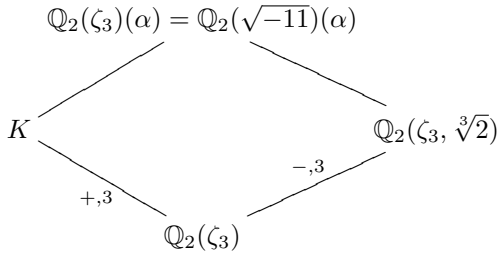
Proof. We need only to check that if $G \times_{\operatorname{Spec} R} \operatorname{Spec} \widehat{R}$ and $G \times_{\operatorname{Spec} R} R[1/p]$ are flat that G is flat. The reason is that $R \mapsto R[1/p] \times \widehat{R}$ is faithfully flat. It is flat because completion and localization are flat, and faithful because $\operatorname{Spec}(R[1/p]) \cup \operatorname{Spec} \widehat{R} \to \operatorname{Spec} R$, since if $p \notin \mathfrak{p}$ then $\mathfrak{p}$ is a prime of $\operatorname{Spec} R[1/p]$, and if $p \in \mathfrak{p}$ then we have a map $\widehat{R} \to R/\mathfrak{p}$ and the kernel gives a prime of $\widehat{R}$. So if $G = \operatorname{Spec} A$ where A is an R-algebra, where $R \otimes_R \widehat{R}$, $A \otimes_R R[1/p]$ are flat, then $A \otimes_R (\widehat{R} \times R[1/p])$ is flat and $\widehat{R} \times R[1/p]$ is faithful, so A is flat. □

Main application: If $R = \mathfrak{O}_K$ is a ring of integers, $p \in \mathbb{Z}$ a prime number, then if $G/\mathfrak{O}_K$ is a p-power order group scheme, then by the theorem, we may look at $(G \times \operatorname{Spec} \widehat{R}, G \times \operatorname{Spec} R[1/p], \mathrm{id})$, where $\widehat{R} = \prod_{\mathfrak{p}|p} \mathfrak{O}_\mathfrak{p}$ where the $\mathfrak{O}_\mathfrak{p}$ are finite extensions of the p-adics, and G is étale outside p and therefore localizing at p we know that $G \times R[1/p]$ is étale, and hence a π-module, where π is the fundamental group, namely $\operatorname{Gal}(\widetilde{K}/K)$, where $\widetilde{K}$ is the maximal extension of K inside some $\overline{K}$ which is unramified outside p.

Example. Here is an example of an "exotic" group scheme over $\mathbb{Z}[(1+\sqrt{-11})/2]$. It will be described by $G \leftrightarrow (G_1/\widehat{R}, G_2/R[1/p], \phi)$. G is of order 4, $p = 2$, $\widehat{R} = \mathbb{Z}_2[(1+\sqrt{-11})/2] \simeq \mathbb{Z}[\zeta_3]$. For G_2, we take $\mathbb{Q}(\sqrt{-11})$ which allows a cyclic cubic extension F which is only ramified at 2, the ray class field of conductor 2 with Galois group $\mathbb{F}_4^\times$, where $F = \mathbb{Q}(\sqrt{-11}, \alpha)$ where $\alpha^3 + \alpha^2 - \alpha + 1 = 0$; we let G_2 be $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with nontrivial action by $\pi = (1+\sqrt{-11})/2$, namely by matrices $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. For G_1, take the elliptic curve $Y^2 + Y = X^3$ over $\mathbb{Z}_2[\zeta_3] = \widehat{R}$, which only has bad reduction over 3. $E[2]$ is finite and flat of order 4; we need to show there is an isomorphism $\operatorname{Spec} \widehat{R}[1/p] \times G_1 \to G_2 \times \operatorname{Spec} \widehat{R}[1/p]$. But $\widehat{R}[1/p] = \mathbb{Q}_2(\zeta_3)$ is a local field, so we need only check that the Galois action of the local Galois group of points of G_1 and G_2 coincide.

The 2-torsion points of E are given by the roots of $X^3 + 1/4$, i.e. $X = \zeta_3(\sqrt[3]{2}/2)$. We have to show that $\mathbb{Q}_2(\zeta_3)(\alpha) = \mathbb{Q}_2(\sqrt{-11})(\alpha) = \mathbb{Q}_2(\zeta_3, \sqrt[3]{2})$; from local class

field theory, we have



But the extensions correspond to these eigenspaces, so we indeed have equality. In terms of equations, $G = \operatorname{Spec} R[X]/\langle X^4 + (1+\sqrt{-11})X^3 + (-3+\sqrt{-11})X^2 - 2X\rangle$.

This group scheme also actually comes from the 2-torsion points on a Neron model of an elliptic curve of conductor 121 with CM by -11 over $\mathbb{Z}[(1+\sqrt{-11})/2]$. (It is also an example of Raynaud.)

Now we begin with the proof of the equivalence of categories.

Lemma. *If M is a finitely generated R-module, the square*

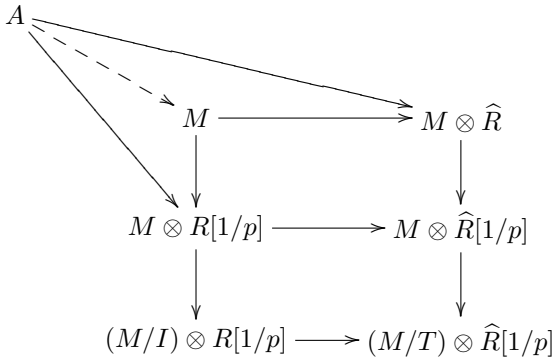
$$\begin{array}{ccc} M & \longrightarrow & M \otimes_R \widehat{R} \\ \downarrow & & \downarrow \\ M \otimes_R R[1/p] & \longrightarrow & M \otimes \widehat{R}[1/p] \end{array}$$

is Cartesian*, i.e. it is a fibre product in the category of modules.*

Proof. It suffices to show this for p-torsion free M: Let $T = \{m \in M : p^i m = 0 \text{ for some } i \geq 0\}$. Let $T \otimes_R \widehat{R} = \varinjlim T/p^i T \simeq T$ by the notherian hypothesis. We have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T & \longrightarrow & M & \longrightarrow & M/T & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & T \otimes \widehat{R} & \longrightarrow & M \otimes \widehat{R} & \longrightarrow & (M/T) \otimes \widehat{R} & \longrightarrow & 0 \end{array}$$

From the commutative cube obtained by the faces of these cartesian squares, we obtain



since if we tensor $0 \to T \to M \to M/T \to 0$ with $R[1/p]$ we have an injection $M \otimes R[1/p] \hookrightarrow (M/T) \otimes R[1/p]$.

So let M be p-torsion free. Then $M \otimes_R \widehat{R}$ is $p\widehat{R}$-torsion free, since $M \xrightarrow{p} M \otimes \widehat{R}$ is injective. Since M is p-torsion free, $M \subset M \otimes R[1/p]$ by $m \mapsto m \otimes 1$. We want to show

$$\begin{array}{ccc} M & \longrightarrow & M \otimes_R [1/p] \\ \downarrow & & \downarrow \\ M \otimes \widehat{R} & \longrightarrow & M \otimes \widehat{R}[1/p] \end{array}$$

If $y \in M \otimes \widehat{R}$ and $x \mapsto y$ for $x \in M \otimes R[1/p]$, we want $x \in M$. Consider inside $M \otimes R[1/p]$, $M \subset \langle M, x\rangle$. Then $\langle M, x\rangle \otimes \widehat{R} = M \otimes \widehat{R}$ and $\langle M, x\rangle \otimes R[1/p] = M \otimes R[1/p]$, so $\langle M, x\rangle \otimes (\widehat{R} \times R[1/p]) = M \otimes (\widehat{R} \times R[1/p])$, where the latter is faithfully flat, so $M = \langle M, x\rangle$ (by the cokernel property of faithful flatness), and thus $x \in M$. □

Theorem. *If R is a noetherian ring, $p \in R$, the functor*

$$F : M \mapsto (M \otimes_R \widehat{R}, M \otimes_R R[1/p], \mathrm{id} \otimes \widehat{R}[1/p])$$

from the category $\mathfrak{C}$ of finitely generated R-modules to triples of modules finitely generated over $\widehat{R}$ and $R[1/p]$ with an isomorphism ϕ, is an equivalence of categories.

Lemma. *If M is a finitely generated R-module then the square*

$$\begin{array}{ccc} M & \longrightarrow & M \otimes R[1/p] \\ \downarrow & & \downarrow \\ M \otimes \widehat{R} & \longrightarrow & M \otimes \widehat{R}[1/p] \end{array}$$

is cartesian.

Corollary. *F is fully faithful, i.e.*

$$\mathrm{Hom}_R(M, N) \simeq \mathrm{Hom}_{\mathfrak{C}}(F(M), F(N)).$$

Proof. If $f : M \to N$ becomes 0 then

$$f \otimes (\widehat{R} \times R[1/p]) = 0$$

since the product is faithfully flat implies $f = 0$. This shows injectivity; for surjectivity, if we have

$$(M \otimes \widehat{R}, M \otimes R[1/p], \mathrm{id}) \to (N \otimes \widehat{R}, N \otimes R[1/p], \mathrm{id})$$

then we have maps

$$M \to M \otimes \widehat{R} \to N \otimes \widehat{R}$$

and

$$M \to M \otimes R[1/p] \to N \otimes \widehat{R}[1/p]$$

so by the cartesian property, we have a unique map $M \to N$. □

Proposition. *F is essentially surjective.*

Proof. For (M_1, M_2, ϕ), we want to construct M. We have

$$\phi : M_1 \otimes_{\widehat{R}} \widehat{R}[1/p] \to M_2 \otimes_{R[1/p]} \widehat{R}[1/p]$$

Choose m_i to generate M_1 such that the image generates M_2. Then we have

$$\begin{array}{ccccccccc}
 & & \bigoplus_j Rf_j & = & \bigoplus Rf_j & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \to & (N_1, N_2, \phi) & \to & (\bigoplus_i \widehat{R}e_i, \bigoplus_i R[1/p]e_i, \mathrm{id}) & \to & (M_1, M_2, \phi) & \to & (T,0,0) \to 0 \\
 & & \downarrow & & \downarrow & & & & \\
0 & \to & (S,0,0) & \to & M = (M, M, \mathrm{id}) & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

where T is p-torsion. Therefore we have

$$0 \to M/S = M' \to (M_1, M_2, \phi) \to (T, 0, 0) \to 0$$

and in the first coordinate

$$0 \to M' \otimes \widehat{R} \to M_1 \to T \to 0$$

which gives

$$\mathrm{Ext}^1_R(T, M') \simeq \mathrm{Ext}^1_{\widehat{R}}(T, M' \otimes \widehat{R}).$$

□

Cokernels and sheaves. For the material in this section, see [A2], [Mil], or [R].

If $f : G \to H$ is a morphism of group schemes over R, $(\ker f)(S) = \ker(G(S) \to H(S))$, so that if $G = \operatorname{Spec} A$, $H = \operatorname{Spec} B$, then $\ker f = \operatorname{Spec}(A \otimes_B R) = \operatorname{Spec}(A/I_B A)$.

What is the cokernel? We would like that $\mu_d \to \mu_n \to \mu_{n/d}$ from

$$R[X]/\langle X^d - 1\rangle \leftarrow R[X]/\langle X^n - 1\rangle \leftarrow R[X]/\langle X^{n/d} - 1\rangle$$

where the right-hand map is $X \mapsto X^d$, and we would like $\mu_n(S) \to \mu_{n/d}(S)$ by $z \mapsto z^d$ surjective, but this is not always so. Therefore we cannot take $(\operatorname{coker} f)(S) = \operatorname{coker}(G(S) \to H(S))$. We would, however, have surjectivity if we viewed the map over the algebraic closure (a faithfully flat extension).

Let F be a functor from R-algebras to a category $\mathfrak{A}$.

Definition. F is a *sheaf* if for all objects S and faithfully flat extensions $S \to T$, the sequence

$$0 \to F(S) \to F(T) \overrightarrow{\to} F(T \otimes_S T)$$

is exact.

Example. If $T = \prod_i S[1/f_i]$, such that $\langle f_i \rangle_i = S$, then T is a faithfully flat ring extension. $\operatorname{Spec} S \leftarrow \bigsqcup_i U_i$ where $U_i = \operatorname{Spec} S[1/f_i]$. (It may be alright to take an infinite index set, but we will restrict to the finite case.) Then the exactness of the sequence corresponds to equality on the intersections $U_i \cap U_j$, which is exactly the usual sheaf condition.

Theorem. *Representable functors F from R-algebras to $\mathfrak{A}$ are sheaves.*

If $\mathfrak{A}$ is an abelian category, then the category of sheaves from R-algebras to $\mathfrak{A}$ form an abelian category as well, which allows us to construct cokernels.

Proof. We will show that if $S \to T$ is faithfully flat, then in fact

$$0 \longrightarrow S \longrightarrow T \rightrightarrows T \otimes_S T$$

is exact, where the second map is $t \mapsto t \otimes 1, 1 \otimes t$. It suffices to show exactness after tensoring with T (since T is faithfully flat). We obtain

$$0 \longrightarrow T \longrightarrow T \otimes_S T \rightrightarrows T \otimes_S T \otimes_S T$$

$t \mapsto 1 \otimes t$ and $a \otimes b \mapsto a \otimes 1 \otimes b, 1 \otimes a \otimes b$, and now we have a reverse map h (not quite a section) by $x \otimes y \otimes z \mapsto x \otimes yz$. If $\sum_i a_i \otimes b_i$ has the same image, then $\sum_i a_i \otimes 1 \otimes b_i = \sum_i 1 \otimes a_i \otimes b_i$, and applying the map h we find $\sum_i a_i \otimes b_i = \sum_i 1 \otimes a_i b_i \in \operatorname{img}(T \to T \otimes_S T)$.

If F is represented by A, then apply $\operatorname{Hom}_R(A, -)$, and it is still exact. □

Therefore group schemes can be considered representable sheaves from R-algebras to group schemes.

Definition. In the category of sheaves, if $f : G \to H$ is a morphism of sheaves, let P be the functor $P(S) = H(S)/f(G(S))$, which is only a *presheaf*. There is a construction "sheafify" which transforms a presheaf into a sheaf, by first taking

$$P^+(S) = \varinjlim_{S \to T} \ker(P(T) \rightrightarrows P(T \otimes_S T))$$

where $S \to T$ runs over all faithfully flat extensions, and then taking $P^{++} = aP$ is a sheaf.

Then $\operatorname{coker} f = aP$.

It has the universal property in the category of sheaves. If $f : G \to H$ is surjective, which is to say that if S is an R-algebra, and $x \in H(S)$, then there is a T such that there exists a $y \in G(T)$ which maps to $x \in H(T)$.

Example. The map $\mathbb{G}_m \xrightarrow{n} \mathbb{G}_m$ for $n \geq 1$ which raises each unit to its nth power, then for any $\epsilon \in S$, we take $T = S[X]/\langle X^n - \epsilon \rangle$ which is free and therefore faithfully flat, and then $X \mapsto \epsilon$ for trivial reasons, so the cokernel is trivial.

For the same reason, $\mu_n \to \mu_{n/d}$ is also surjective.

Theorem (Grothendieck)**.** *If $N \to G$ is a morphism of group schemes, $G = \operatorname{Spec} A$, and $N = \operatorname{Spec} A/J$ is a closed, commutative finite flat subgroup scheme in G, then the quotient sheaf $G/N = \operatorname{Spec} B$ is representable where*

$$B = \{a \in A : c(a) \equiv 1 \otimes a \pmod{J \otimes A}\}.$$

Moreover, A is faithfully flat over B (and thus if A itself is flat, B is also flat).

(See [R].)

If $A = R[X_1, \ldots, X_m]/\langle f_1, \ldots, f_r \rangle$, then

$$B = \{\phi(X_1, \ldots, X_m) \in A : \phi \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix} \begin{pmatrix} Y_1 \\ \vdots \\ Y_m \end{pmatrix} = \phi \begin{pmatrix} X_1 \\ \vdots \\ X_m \end{pmatrix}\}$$

for all Y_i for which $g(Y_i) = 0$ for all $g \in J$.

Example. The map $\mu_{n/d} \to \mu_n$ arises from $R[X]/\langle X^{n/d} - 1 \rangle \leftarrow R[X]/\langle X^n - 1 \rangle = A$ by raising to the dth power, the cokernel is

$$\{\phi \in R[X]/\langle X^n - 1 \rangle : \phi(X) = \phi(XY) \in R[X, Y]/\langle X^n - 1, Y^{n/d} - 1 \rangle\}$$

which implies ϕ is a polynomial in $X^{n/d}$, so the cokernel is $R[X^{n/d}] \subset A$, isomorphic to $R[T]/\langle T^d - 1\rangle$, and therefore we have an exact sequence

$$0 \to \mu_{n/d} \to \mu_n \to \mu_d \to 0$$

Example. If $R = \mathbb{Z}[(1+\sqrt{-7})/2] = \mathbb{Z}[\pi]$, $2 = \pi\overline{\pi}$. There are four group schemes over order 2, $\mathbb{Z}/2\mathbb{Z}$, $G_\pi = \operatorname{Spec} R[X]/\langle X^2 - \pi X\rangle$, $G_{\overline{\pi}}$, and μ_2. We have

$$0 \to \mathbb{Z}/2\mathbb{Z} \to G_\pi \times G_{\overline{\pi}}$$

induced from $R[T]/\langle T^2 - T\rangle \leftarrow R[X,Y]/\langle X^2 - \pi X, Y^2 - \overline{\pi}Y\rangle$ by $X, Y \mapsto \pi T, \overline{\pi}T$. (It is the map $1 \mapsto (\pi, \overline{\pi})$.)

The cokernel consists of polynomials $\{\phi(X,Y) : \phi((X,Y) + (\pi,\overline{\pi})) = \phi(X,Y)\}$, where the group law now gives

$$\phi(X + \pi - \overline{\pi}X\pi, Y + \overline{\pi} - \pi Y\overline{\pi}) = \phi(X,Y)$$

and therefore $\phi = -\overline{\pi}X - \pi Y + 2XY$. We check that $\phi^2 = -2\phi$ and therefore $B \simeq R[T]/\langle T^2 - 2T\rangle$, $c(\phi) = \phi \otimes 1 + 1 \otimes \phi - \phi \otimes \phi$.

The exact sequence

$$0 \to \mathbb{Z}/2\mathbb{Z} \to G_\pi \times G_{\overline{\pi}} \to \mu_2 \to 0$$

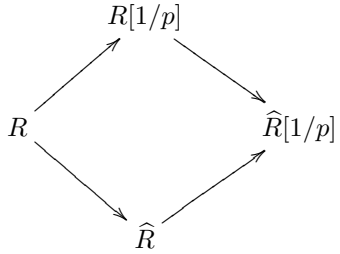
is not split (look at étale and connected parts), even though everywhere the Galois action is trivial.

If we have $0 \to N \to G \to G/N \to 0$, arising from $B \hookrightarrow A \to A/J$, then

$$A \otimes_B A \simeq A \otimes_R A/J.$$

If we localize and compute ranks, $((\operatorname{rk} G)/(\operatorname{rk} G/N))(\operatorname{rk} G)/(\operatorname{rk} G/N))\operatorname{rk} G/N = (\operatorname{rk} G)(\operatorname{rk} N)$ and therefore $\operatorname{rk} G = (\operatorname{rk} N)(\operatorname{rk} G/N)$, i.e. $\#N \cdot \#G/N = \#G$.

We also have a Mayer-Vielois exact sequence. If R is noetherian, $p \in R$, and G, H finite flat commutative group schemes over R; we are interested in $\operatorname{Ext}^1_R(G,H) = \{0 \to H \to A \to G \to 0\}/\sim$ in the category of sheaves, but one can show that any such A is representable if H and G are. We have



We know G and H are p-power order.

Theorem. *There exists an exact sequence*

$$0 \to \operatorname{Hom}_R(G,H) \to \operatorname{Hom}_R(G,H) \times \operatorname{Hom}_{R[1/p]}(G,H) \to \operatorname{Hom}_{\widehat{R}[1/p]}(G,H)$$
$$\xrightarrow{\delta} \operatorname{Ext}^1_R(G,H) \to \operatorname{Ext}^1_{\widehat{R}}(G,H) \times \operatorname{Ext}^1_{R[1/p]}(G,H) \to \operatorname{Ext}^1_{\widehat{R}[1/p]}(G,H)$$

where δ is defined by $\alpha \in \operatorname{Hom}_{\widehat{R}[1/p]}(G,H)$ is

$$\delta\alpha = ((G \times H)_{\widehat{R}}, (G \times H)_{R[1/p]}, \operatorname{id}_H \operatorname{id}_G + \alpha).$$

The exactness follows from the equivalence of categories above.

Remark. This was constructed by hand; a good question would be to understand what the Ext^2 groups are.

If we work over a field, and G is finite and flat, then we have an exact sequence

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0.$$

Moreover, we have exact functors $G \mapsto G^0$, $G \to G^{\text{ét}}$.

If G_i are commutative, and $0 \to G_1 \to G_2 \to G_3 \to 0$, then we also have an exact sequence

$$0 \leftarrow G_1^\vee \leftarrow G_2^\vee \leftarrow G_3^\vee \leftarrow 0.$$

Nonexistence of abelian varieties. To prove that there are no abelian varieties over $\mathbb{Q}$ with good reduction everywhere, we will use:

Theorem. *Every finite flat 2-power order commutative group scheme G over $\mathbb{Z}$ sits in an exact sequence*

$$0 \to M \to G \to C \to 0$$

where C is a constant group scheme, and hence $C \simeq \bigoplus \mathbb{Z}/2^k\mathbb{Z}$, and M is diagonalizable and hence its Cartier dual is constant, so $M \simeq \bigoplus \mu_{2^k}$.

Proof that the theorem implies Fontaine's theorem. If A is an abelian variety of good reduction, then $A[2^n]$ is a finite flat group scheme over $\mathbb{Z}$ of order 2^{2ng} where $g = \dim A$. Then we have an exact sequence

$$0 \to M \to A[2^n] \to C \to 0$$

by the theorem. Consider $C \hookrightarrow A/M$, and reduce modulo a prime q. Since C is étale, it remains étale and constant under the reduction map, and therefore $C(\mathbb{F}_q) \subset A/M(\mathbb{F}_q)$. By the Riemann hypothesis,

$$\#C(\mathbb{F}_q) \leq (\sqrt{q}+1)^{2g}.$$

So as $n \to \infty$, C is bounded. If we dualize, we obtain

$$0 \to C^\vee \to A[2^n]^\vee \to M^\vee \to 0;$$

there is a natural identification of $A[2^n]^\vee \simeq A^\vee[2^n]$, where now $C^\vee$ is diagonalizable and $M^\vee$ is constant. The same argument implies that $\#M^\vee = \#M \leq (\sqrt{q}+1)^{2g})$. This is a contradiction, since then $\#A[2^n]$ is bounded, hence $g = 0$. □

The first theorem will follow from the following concerning extensions of $\mathbb{Z}/2\mathbb{Z}$, μ_2.

Theorem.

(a) *Any extension of a group scheme composed of $\mathbb{Z}/2\mathbb{Z}$ is constant*
(b) *Any extension of a group scheme composed of μ_2 is diagonalizable.*
(c) *The sequence $0 \to \mathbb{Z}/2\mathbb{Z} \to G \to \mu_2 \to 0$ splits.*

Proof. If G is an extension of $\mathbb{Z}/2\mathbb{Z}$, G is étale, since

$$0 \to (\mathbb{Z}/2\mathbb{Z})^0 = 0 \to G^0 \to (\mathbb{Z}/2\mathbb{Z})^0 = 0 \to 0.$$

Since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acting on G is unramified at all p, and $h(\mathbb{Z}) = 1$, the action is trivial. This proves (a), and (b) follows by taking Cartier duals.

For (c), we use the Mayer-Vietais sequence. Let $R = \mathbb{Z}$, $p = 2$, $\widehat{R} = \mathbb{Z}_2$, $R[1/p] = \mathbb{Z}[1/2]$, and $\widehat{R}[1/p] = \mathbb{Q}_2$. Then we have

$$\begin{aligned} 0 \to \mathrm{Hom}_{\mathbb{Z}}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}_2}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \times \mathrm{Hom}_{\mathbb{Z}[1/2]}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \\ \to \mathrm{Hom}_{\mathbb{Q}_2}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \\ \to \mathrm{Ext}^1_{\mathbb{Z}_2}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \times \mathrm{Ext}^1_{\mathbb{Z}[1/2]}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Q}_2}(\mu_2, \mathbb{Z}/2\mathbb{Z}). \end{aligned}$$

Since $0 \to \mathbb{Z}/2\mathbb{Z} \to G \to \mu_2 \to 0$ is split over $\mathbb{Z}_2$, taking connected components we have

$$0 \to (\mathbb{Z}/2\mathbb{Z})^0 = 0 \to G^0 \to \mu_2^0 = \mu_2 \to 0$$

and therefore we get a section. Since it is split over $\mathbb{Z}_2$, it is killed by 2 and by flatness, it is also killed by 2 over $\mathbb{Z}$. As a Galois representation, it looks like $\begin{pmatrix} 1 & \chi \\ 0 & 1 \end{pmatrix}$ where χ is unramified outside 2. But since the sequence splits, it is also unramified at 2, but since $h(\mathbb{Z}) = 1$, the character must be trivial, so the Galois module is trivial. Therefore

$$\mathrm{Ext}^1_{\mathbb{Z}_2}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \times \mathrm{Ext}^1_{\mathbb{Z}[1/2]} = 0.$$

Now $\mathrm{Hom}_{\mathbb{Z}_2}(\mu_2, \mathbb{Z}/2\mathbb{Z}) = 0$ since any morphism must factor through the unit section (as one group is étale, one is connected), and the same argument shows $\mathrm{Hom}_{\mathbb{Z}}(\mu_2, \mathbb{Z}/2\mathbb{Z}) = 0$. Therefore $\mathrm{Hom}_{\mathbb{Q}_2}(\mu_2, \mathbb{Z}/2\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}[1/2]}(\mu_2, \mathbb{Z}/2\mathbb{Z}) = 2$, and we obtain

$$0 \to 0 \to 0 \times 2 \to 2 \to \mathrm{Ext}^1_{\mathbb{Z}}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \to 0$$

so this extension group is trivial. □

Proof that it implies the above. If G is 2-power order over $G(\overline{\mathbb{Q}})$; we have seen that a simple 2-group scheme of 2-power order is either $\mathbb{Z}/2\mathbb{Z}$ or μ_2. We can therefore filter G with quotients isomorphic to one of these two simple groups. Using the splitting, we can modify the filtration so we can switch if $\mathbb{Z}/2\mathbb{Z}$ is on the left of a μ_2. Pushing all of the quotients $\mathbb{Z}/2\mathbb{Z}$ to the right, we obtain a filtration composed first of μ_2 and then of $\mathbb{Z}/2\mathbb{Z}$, for which the first by (b) is diagonalizable and the second by (a) is constant. □

If we now look at cyclotomic fields, $\mathbb{Q}(\zeta_f)$, f the conductor, $f \not\equiv 2 \pmod 4$. It is known that $\mathrm{Jac}(X_1(f))/\mathrm{Jac}(X_0(f))$ acquires good reduction over $\mathbb{Q}(\zeta_f)$. This construction gives nonzero abelian varieties with good reduction everywhere when the genus of $X_1(f) \neq 0$, i.e. $f \notin \{1, 3, 4, 5, 7, 8, 9, 12\}$, and such that the genus of $X_1(f)$ is not the genus of $X_0(f)$, i.e. $f \notin \{11, 15\}$.

Theorem. *For all f in this list, except possibly $11, 15$, there do not exist abelian varieties with good reduction everywhere over $\mathbb{Q}(\zeta_f)$. Under the GRH, the same is true for $f = 11, 15$.*

We treat the case $f = 7$. Look at finite flat group schemes over $R = \mathbb{Z}[\zeta_7]$. Choose $p = 2$. The only such simple group schemes of 2-power order over R are $\mathbb{Z}/2\mathbb{Z}$, μ_2, G_π, and $G_{\overline{\pi}}$, where $G_\pi = \mathrm{Spec}\, R[X]/\langle X^2 - \pi X\rangle$, where $\pi = (1+\sqrt{-7})/2$ with group law $X \mapsto X + X' - \overline{\pi} X X'$.

Theorem. *For all finite flat group schemes G over $\mathbb{Z}[\zeta_7]$ over 2-power order, there exists a filtration*

$$0 \subset G_1 \subset G_2 \subset G$$

such that G_1 is diagonalizable, G/G_2 is constant, and G_2/G_1 is a direct product of factors from G_π and $G_{\overline{\pi}}$.

If we apply this to $G = A[2^n]$, where A is an abelian variety with good reduction everywhere, then $\#G_1 \leq (\sqrt{q}+1)^{2g}$ as above, and $\#G/G_2 \leq (\sqrt{q}+1)^{2g}$. Since $A[2^n] \simeq (\mathbb{Z}/2^n\mathbb{Z})^{2g}$, and G_2/G_1 is of exponent 2, $\#G_2/G_1 \leq 2^{2g}$, we again have that $\#A[2^n]$ is bounded, a contradiction.

Theorem. *If G is a finite flat group scheme over $\mathbb{Z}[\zeta_7]$.*

(a) *Any extension of a group scheme composed of $\mathbb{Z}/2\mathbb{Z}$ is constant.*
(b) *Any extension of a group scheme composed of μ_2 is diagonalizable.*
(c) $\mathrm{Ext}^1(\mu_2, \mathbb{Z}/2\mathbb{Z})$ *has order 2, generated by*

$$0 \to \mathbb{Z}/2\mathbb{Z} \to G_\pi \times G_{\overline{\pi}} \to \mu_2 \to 0.$$

(d) $\mathrm{Ext}^1(G_\pi, \mathbb{Z}/2\mathbb{Z}) = \mathrm{Ext}^1(G_{\overline{\pi}}, \mathbb{Z}/2\mathbb{Z}) = 0$. *By Cartier duality, we have* $\mathrm{Ext}^1(\mu_2, G_\pi) = \mathrm{Ext}^1(\mu_2, G_{\overline{\pi}}) = 0$.
(e) $\mathrm{Ext}^1(G_\pi, G_{\overline{\pi}}) = \mathrm{Ext}^1(G_\pi, G_\pi) = 0$.

This implies the filtration theorem, because we can filter with simple quotients as above, switching the order except when $\mathbb{Z}/2\mathbb{Z}$ is next to μ_2, for which we replace it with $G_\pi \times G_{\overline{\pi}}$.

Proof. If G is an extension of $\mathbb{Z}/2\mathbb{Z}$, then G is étale, so the Galois action is unramified, but $h(\mathbb{Q}(\zeta_7)) = 1$ (the group is a pro-2-group), so the action is trivial, so G is constant. This gives (a), and (b) implies (a) by duality.

For (c), we have now $R = \mathbb{Z}[\zeta_7]$, $p = 2$, $\widehat{R} = \mathfrak{O} \times \mathfrak{O}$, where $\mathfrak{O}$ is an unramified extension of $\mathbb{Z}_2$ is of degree 3, $\widehat{R}[1/2] = K \times K$, and $R[1/2] = \mathbb{Z}[\zeta_7, 1/2]$. Then

$$\begin{aligned} 0 \to \mathrm{Hom}_R(\mu_2, \mathbb{Z}/2\mathbb{Z}) &\to \mathrm{Hom}_{\widehat{R}}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \times \mathrm{Hom}_{R[1/2]}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \\ &\to \mathrm{Hom}_{\widehat{R}[1/2]}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{Ext}^1_R(\mu_2, \mathbb{Z}/2\mathbb{Z}) \\ &\to \mathrm{Ext}^1_{\widehat{R}}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \times \mathrm{Ext}^1_{R[1/2]}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \to \mathrm{Ext}^1_{\widehat{R}[1/2]}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \end{aligned}$$

If we have

$$0 \to \mathbb{Z}/2\mathbb{Z} \to G \to \mu_2 \to 0$$

again by looking at Galois representations, we have the product extension group trivial. As before, we obtain

$$0 \to 0 \to 0 \times 2 \to 2 \times 2 \to G \to 0$$

and therefore $\mathrm{Ext}^1_R(\mu_2, \mathbb{Z}/2\mathbb{Z})$ has order 2.

For (d), we look at extensions

$$0 \to \mathbb{Z}/2\mathbb{Z} \to G \to G_\pi \to 0.$$

Locally, $G_\pi \simeq \mu_2$ at π and $G_\pi \simeq \mathbb{Z}/2\mathbb{Z}$ at $\overline{\pi}$. At π (i.e. over $\mathfrak{O}_\pi$), we have

$$0 \to \mathbb{Z}/2\mathbb{Z} \to G \to \mu_2 \to 0$$

which is split, and at $\overline{\pi}$ we have

$$0 \to \mathbb{Z}/2\mathbb{Z} \to G \to \mathbb{Z}/2\mathbb{Z} \to 0$$

so G is étale at π. So it is killed by 2 over R, we again have a Galois representation with a character which is unramified everywhere, so χ is trivial. So it is locally

trivial, and therefore because it is étale at $\overline{\pi}$ and determined by this Galois action, it is also split at $\overline{\pi}$. This time,

$$\operatorname{Hom}_{\widehat{R}}(G_\pi, \mathbb{Z}/2\mathbb{Z}) = \operatorname{Hom}_{R_\pi}(\mu_2, \mathbb{Z}/2\mathbb{Z}) \times \operatorname{Hom}_{R_{\widetilde{\pi}}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = 0 \times 2$$

so we have

$$0 \to 0 \to (0 \times 2) \times 2 \to 2 \times 2 \to \#\operatorname{Ext}^1_R(\mu_2, \mathbb{Z}/2\mathbb{Z}) \to 0 \times 0$$

and thus this group is trivial.

The latter follow from the claim:

Claim. If R is a PID, $\operatorname{char} R \neq 2$, $R^\times/R^{\times 2}$ finite, R has quotient field K, and $0 \to \mu_2 \to G \to \mathbb{Z}/2\mathbb{Z} \to 0$, then the points of G are defined over $K(\sqrt{\epsilon})$ for some $\epsilon \in R^\times$, and G is determined by its Galois module.

Proof of claim. We know (for instance) the Katz-Mazur group schemes

$$0 \to \mu_2 \to G_\epsilon \to \mathbb{Z}/2\mathbb{Z} \to 0$$

killed by 2, where now χ corresponds to $\sqrt{\epsilon}$, $\epsilon \in R^\times/R^{\times 2}$. We also have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_2 & \longrightarrow & \mathbb{G}_m & \xrightarrow{2} & \mathbb{G}_m & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \mu_2 & \longrightarrow & G & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \end{array}$$

On the level of Hopf algebras, they arise from

$$\begin{array}{ccccc} & & R[T,1/T] & \longleftarrow & R[T^2,1/T^2] \\ & & \downarrow & & \downarrow \\ R[T]/\langle T^2-1\rangle & \longleftarrow & R[X,T]/\langle X^2-X, T^2-1+2X\rangle & \longleftarrow & R[X]/\langle X^2-1\rangle \end{array}$$

where the vertical map is $T^2 \mapsto 1-2X$. The group law in the pullback is obtained from

$$(x,t)(x',t') = (x+x'-2xx', tt').$$

Over a field, the points are the zero element $(0,1)$, and

$$(1,i)(1,i) = (0,-1), \quad (0,-1),(0,-1) = (0,1).$$

Therefore $\#\operatorname{Ext}^1(\mathbb{Z}/2\mathbb{Z}, \mu_2) \geq 2\#R^\times/R^{\times 2}$, and each of these are distinguished by their Galois modules, and if we show equality then we are done.

From $0 \to \mu_2 \to \mathbb{G}_m \to \mathbb{G}_m \to 0$, the functor $\operatorname{Hom}_R(\mathbb{Z}, -)$ gives

$$R^\times \to R^\times \to \operatorname{Ext}^1_R(\mathbb{Z}, \mu_2) \simeq \mathbb{R}^\times/\mathbb{R}^{\times 2} \to \operatorname{Ext}^1_R(\mathbb{Z}, \mathbb{G}_m) = H^1(\operatorname{Spec} R, \mathbb{G}_m) = 0$$

where the latter vanishes because it is the Picard group and R is a PID. Doing the same to

$$0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

we obtain

$$0 \to \mu_2(R) \to \operatorname{Ext}^1_R(\mathbb{Z}/2\mathbb{Z}, \mu_2) \to \mathbb{R}^\times/\mathbb{R}^{\times 2} \to 0$$

which gives the correct rank. □

To prove (e), then, we want to show that any sequence

$$0 \to G_\pi \to G \to G_{\overline{\pi}} \to 0$$

over $R = \mathbb{Z}[\zeta_7]$ splits. Locally at π, this looks like

$$0 \to \mu_2 \to G \to \mathbb{Z}/2\mathbb{Z} \to 0$$

and at $\overline{\pi}$ it is

$$0 \to \mathbb{Z}/2\mathbb{Z} \to G \to \mu_2 \to 0$$

which splits, and therefore G is killed by 2 over $\mathfrak{O}_\pi$, and by flatness G is killed by 2 over R. The Galois representation $\begin{pmatrix} 1 & \chi \\ 0 & 1 \end{pmatrix}$ has χ unramified at $\mathfrak{p} \not| 2$, and spli at $\overline{\pi}$, and at π it arises from cutting out $\sqrt{\epsilon}$, so the conductor of χ divides π^2.

But the ray class field of $\mathbb{Q}(\zeta_7)$ of conductor π^2 is trivial, as $\mathfrak{O}_\pi$ is unramified of degree 3 over $\mathbb{Z}_2$, so

$$\{x \equiv 1 \pmod{\pi}\}/\{x \equiv 1 \pmod{\pi^2}\} \simeq \mathbb{F}_8$$

where we map in the global units $\mathbb{Z}[\zeta_7]$, and we want to show that it is surjective. We have $-1 \equiv 1 \pmod{\overline{\pi}}$ but $-1 \not\equiv 1 \pmod{\pi^2}$ and cyclotomic units $(\zeta^a - 1)/(\zeta - 1)$ where $a \in (\mathbb{Z}/7\mathbb{Z})^\times$ which give us $1, \zeta/(1-\zeta), \zeta^2/(1-\zeta^2)$ which are a basis over $\mathbb{F}_2$, so the map is surjective, and χ is trivial. Therefore the global Galois acts trivial, so the local Galois acts trivial, so by the claim it is determined by this action, and locally at π it is also split. The rest follows from the long exact sequence. □

Exercises. The following are exercises for §5.

Problem 5.1. Let p be a prime, let $\epsilon \in \mathbb{Z}_p^\times$ be $\epsilon \equiv 1 \pmod{p}$ but $\epsilon \not\equiv 1 \pmod{p^2}$. Let $F = \mathbb{Q}_p(\zeta_p, \sqrt[p]{\epsilon})$. We have $G = \mathrm{Gal}(F/\mathbb{Q}_p)$ and its subgroup $H = \mathrm{Gal}(F/\mathbb{Q}_p(\zeta_p))$. Let v denote the p-adic valuation on F normalized by $v(p) = 1$.

(a) Show that $\mathfrak{O}_F = \mathbb{Z}_p[\zeta_p, \sqrt[p]{\epsilon}]$ iff $p = 2$.
(b) Show that $\alpha = (\zeta_p - 1)/(\sqrt[p]{\epsilon} - 1)$ is a uniformizer for $\mathfrak{O}_F$; show that $\mathfrak{O}_F = \mathbb{Z}_p[\alpha]$.
(c) Show that $i(\sigma) = 1/p(p-1)$ when $\sigma \notin H$ while $i(\sigma) = 2/p(p-1)$ when $\sigma \in H \setminus \{1\}$.
(d) Determine the lowering numbering of the higher ramification groups: show that $G_{(i)} = G$ when $i \leq 1/p(p-1)$, that $G_{(i)} = H$ when $1/p(p-1) < i \leq 2/p(p-1)$ and that $G_{(i)} = \{1\}$ when $i > 2/p(p-1)$.
(e) Determine the upper numbering of the higher ramification groups. Show that $G^{(u)} = G$ for $0 \leq u \leq 1$, that $G^{(u)} = H$ for $1 < u \leq 1 + 1/(p-1)$ and that $G^{(u)} = \{1\}$ when $u > 1 + 1/(p-1)$.
(f) Determine $i_{F/\mathbb{Q}_p}$ and $u_{F/\mathbb{Q}_p}$. Compute $v(\mathscr{D}_{F/\mathbb{Q}_p})$.

Problem 5.2. Let $R = \mathbb{Z}[(1 + \sqrt{-7})/2]$.

(a) Show that R has class number 1.
(b) Show that, up to isomorphism, there are precisely four finite flat group schemes of order 2 over R, viz. $\mathbb{Z}/2\mathbb{Z}$, μ_2, and two others G_1 and G_2, say.

Problem 5.3. Let $R = \mathbb{Z}_2[i]$ and let $\pi \in R$ denote the uniformizing element $i - 1$. Let G denote the R-group scheme with Hopf algebra $R[T]/\langle T^2 + \pi T \rangle$ and group

law $T \mapsto T + T' + i\pi TT'$. Let A denote the Hopf algebra of the group scheme $G \times \mu_2$.

(a) Determine the Kähler differentials $\Omega^1_{A/R}$.
(b) Show that there is no element $a \in A$ for which $\Omega^1_{A/R}$ is free over A/aA.

Problem 5.4. Let G be a finite flat commutative group scheme of 2-power order over $\mathbb{Z}[\zeta_3]$.

(a) If G has exponent 2, show that the extension generated by its points has degree at most 5 over $\mathbb{Q}(\zeta_3)$.
(b) If G is simple, show that it has order 2.
(c) If G is simple, show it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or to μ_2.

Problem 5.5. Show that the only simple finite flat commutative group schemes over $\mathbb{Z}[\zeta_5]$ of 2-power order are $\mathbb{Z}/2\mathbb{Z}$ and μ_2.

Problem 5.6. Show that all simple finite flat commutative group schemes over $\mathbb{Z}$ of 3-power order have order 3. [Hint: If G is simple, consider the extension L of $\mathbb{Q}$ generated by the points of $G \times \mu_3$ and show that $[L : \mathbb{Q}(\zeta_3)] \mid 3$.]

6. Comments on the Exercises

Problem 1.1. We are still in characteristic 0, so we look at $Y'^2 = X'^3 + a'_2X'^2 + a'_4X' + a'_6 = f(X')$ with $\Delta' = 2^6\Delta$, $\Delta = 1, -1, i, -i$, and $a'_i \in \mathbb{Z}[i]$ (we still have a global minimal model because $\mathbb{Q}(i)$ has trivial class group).

To show that there exist 2-torsion defined over $\mathbb{Z}[i]$, we first treat $\Delta = \pm 1$ so $\sqrt{\Delta} \in \mathbb{Q}(i)$, and thus the field L obtained by adjoining the 2-torsion is a cubic cyclic extension of $K = \mathbb{Q}(i)$ ramified only at $1 + i$, so it is contained in a ray class field of conductor $\mathfrak{c} = \langle 1 + i\rangle^e$ for some e; but for e sufficiently large,

$$h_{\mathfrak{c}} = \frac{h_K\phi(\mathfrak{c})}{(U : U_{\mathfrak{c}})} = 2^{e-3}$$

hence $[L : K]$ is a power of 2, a contradiction. Second, if $\Delta = \pm i$, then $K = \mathbb{Q}(\sqrt{i}) = \mathbb{Q}(\zeta_8)$. Here $\langle 2\rangle = \langle 1 - \zeta_8\rangle^4$, and again L/K is cyclic of order 3 unramified outside $1 - \zeta_8$. $\mathbb{Q}(\zeta_8)$ has class number 1 ($\Delta_{L/\mathbb{Q}} = \pm 2^8$ and $4!/4^4(4/\pi)^2\sqrt{2^8} < 3$ but 2 is already principal). The same argument (without computing the unit group) shows that $[L : K]$ has order dividing 2, a contradiction.

We again are reduced to the situation $\pm 2^8 = a'^2_4(a'^2_2 - 4a'_4)$. $\mathbb{Z}[i]$ is a UFD, so $a'_4 \mid 2^4$, so we check $a'_4 = u2^k$ for $0 \le k \le 4$, $u = \pm 1, \pm i$. Testing each one for when $\pm 2^{8-2k} + 4u2^k$ is a square (using the fact that only 2 ramifies) gives only the possibilities $(a'_2, a'_4) = (0, \pm 4), (\pm 6, 8)$ as before and now also $(a'_2, a'_4) = (\pm 6i, -8)$. Since this last case only differs by a unit, the same arguments as before show that these cannot occur.

Problem 2.1. We find that $\mathrm{Hom}_R(R[X, Y, Z, W]/\langle XW - YZ - 1\rangle, S) = SL_2(S)$ so $A = R[X, Y, Z, W]/\langle XW - YZ - 1\rangle$. Since

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} x' & y' \\ z' & w' \end{pmatrix} = \begin{pmatrix} xx' + yz' & xy' + yw' \\ x'z + wz' & y'z + ww' \end{pmatrix}$$

we have the comultiplication $c : A \to A \otimes A$ by $X \mapsto XX' + YZ', \ldots, W \mapsto Y'Z + WW'$. The identity matrix gives $e : A \to R$ by $X, Y, Z, W \mapsto 1, 0, 0, 1$, and the inverse $i : A \to A$ is $X, Y, Z, W \mapsto W, -Y, -Z, X$.

Problem 2.2(a). We have

$$\begin{array}{ccc} \mathrm{Hom}_R(A\otimes A, A) & \longleftarrow & \mathrm{Hom}_R(A,R)\times \mathrm{Hom}_R(A,R) = G\times G \\ \uparrow & \nearrow_{\Delta} & \\ \mathrm{Hom}_R(A,A) = G & & \end{array}$$

The diagonal map Δ maps $\phi \mapsto (\phi,\phi)$; the top map takes $(\phi,\psi)\mapsto \phi\otimes\psi$ which maps $(\phi\otimes\psi)(a\otimes b) = \phi(a)\psi(b)$, so the map m is the map on the left which takes $\phi \mapsto \phi\circ m = \phi\otimes\phi$, which since $(\phi\otimes\phi)(a\otimes b) = \phi(a)\phi(b) = \phi(ab)$, $m : A\otimes A \to A$ is $a\otimes b \mapsto ab$.

Problem 2.2(b). This is the dual statement to the property of the inverse morphism, which says $c\circ(i\times \mathrm{id}_G)\circ\Delta = e$.

Problem 2.2(c). In terms of groups, this says that $c\circ\Delta = e$, so on groups this means $g^2 = e$ for all g, which implies G is commutative $gh(hg)^2 = \cdots = hg$.

Problem 2.3(a). Such a map $\phi : \mathbb{G}_m = \operatorname{Spec} R[X,1/X] \to \mathbb{G}_a = \operatorname{Spec} R[X]$ would arise from a map $\phi^\sharp : R[X]\to R[X,1/X]$, determined by $X\mapsto f(X)\in R[X,1/X]$. If ϕ is a group morphism then it preserves the group law, so

$$\begin{array}{ccc} \mathbb{G}_m\times\mathbb{G}_m & \xrightarrow{\phi\times\phi} & \mathbb{G}_a\times\mathbb{G}_a \\ \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle c} \\ \mathbb{G}_m & \xrightarrow{\phi} & \mathbb{G}_a \end{array}$$

which is dual to

$$\begin{array}{ccc} R[X,1/X,X',1/X'] & \xleftarrow[(\phi,\phi)]{} & R[X,X'] \\ \uparrow{\scriptstyle c} & & \uparrow{\scriptstyle c} \\ R[X,1/X] & \xleftarrow[\phi]{} & R[X] \end{array}$$

In one direction $X\mapsto X+X'\mapsto f(X)+f(X')$ and in the other $X\mapsto f(X)\mapsto f(XX')$. If $f(X) = c_nX^n+\cdots+c_{-m}1/X^m$ and $n\ge 1$ one finds the coefficient $c_nX^nX'^n = 0$ so $c_i = 0$ for all $i\neq 0$. Looking at the map on the unit morphism shows that $f(1) = 0$ so $\phi^\sharp$ by $X\mapsto 0$ is trivial.

Problem 2.3(b). Such a morphism ϕ is induced by $\phi^\sharp : R[X,1/X]\to R[X]$, determined by the image $X\mapsto f(X)$, where f is a unit, which implies that $f(X) = c_nX^n+\cdots+c_0$ where $c_0\in R$ is a unit and c_i are nilpotent. Since R is reduced, $c_i = 0$, so the map is constant. By looking at the unit morphism we find $f(0) = 1$ so $f(X) = 1$ is trivial.

Problem 2.3(c). We map $R[X,1/X]\to R[X]$ by $X\mapsto 1+\epsilon X$. Then $(1+\epsilon X)(1+\epsilon X') = 1+\epsilon(X+X')$ preserves the group law and induces a morphism of group schemes. (Note $(1+\epsilon X)(1-\epsilon X) = 1$, for instance.)

Problem 2.4(a). We must check the commutativity of the three diagrams defining the group axioms. Associativity follows from the calculation

$$\begin{aligned} X &\mapsto X+X'-2XX' \mapsto (X+X''-2XX'')+X'-2X'(X+X''-2XX'') \\ &= X+(X'+X''-2X'X'')-2X(X'+X''-2X'X''). \end{aligned}$$

The unit map has $X\mapsto X+X'-2XX'\mapsto X'\mapsto X$, and the inverse has

$$X\mapsto X+X'-2XX'\mapsto X+X'-2XX'\mapsto 2X-2X^2 = 0.$$

Problem 2.4(b). By definition, $\mathbb{Z}/2\mathbb{Z}_R$ is defined by the algebra $B = R \times R$ on generators 1 and e with e idempotent, i.e. $B = R \times R \simeq R[X]/\langle X^2 - X\rangle$.
Problem 2.4(c). We have $G \to \mu_2$ given by $R[X]/\langle X^2 - 1\rangle \to R[X]/\langle X^2 - X$. We indeed have $(1-2X)^2 - 1 = -4X + 4X^2 = 0$, so this gives a morphism of schemes, and it is a map of group schemes because the composition laws give

$$X \mapsto XX' \mapsto (1-2X)(1-2X') = 1 - 2(X + X' - 2XX').$$

Problem 2.4(d). If $f : \mathbb{Z}[X]/\langle X^2 - 1\rangle = B \to \mathbb{Z}[X]/\langle X^2 - X\rangle = A$ is our map, then $K = \operatorname{Spec} A/f(I_B)A$ where $I_B = \ker e = \ker(\mathbb{Z}[X]/\langle X^2 - 1\rangle \to R) = \langle X - 1\rangle$, so $K = \operatorname{Spec}(\mathbb{Z}[X]/\langle X^2 - X\rangle)/\langle 2X\rangle = \operatorname{Spec}\mathbb{Z}[X]/\langle X^2 - X, 2X\rangle$.
Problem 2.5(a). We have $\alpha_p(S) = \{x \in S : x^p = 0\}$ and $\mu_p(S) = \{x \in S : x^p = 1\}$, we have for $x \in \alpha_p(S)$ that $(1+x)^p = 1 + x^p = 1$, and conversely if $x \in \mu_p(S)$ then $(x-1)^p = x^p - 1 = 0$.
Problem 2.5(b). This would imply that there is a ring isomorphism $k[X]/\langle X^p - 1\rangle = k[X]/\langle X - 1\rangle^p \to k[X]/\langle X^p$, which can only be $X \mapsto X + 1$. But this is not a morphism of groups, because it would have to preserve the group law, which it does not as

$$X \mapsto X + X' \mapsto (X+1) + (X'+1) \neq (X+1)(X'+1) = XX' + X + X' + 1.$$

Problem 2.6(a). The map preserves the group law because $T \mapsto T + T' \mapsto (T^p - T) + (T'^p - T') = (T + T')^p - (T + T')$.
Problem 2.6(b). We have $g(I_{R[T]}) = \langle T^p - T\rangle$ so $K = \operatorname{Spec} k[T]/\langle T^p - T\rangle = \operatorname{Spec} k[T]/\langle T(T-1)\dots(T-(p-1))\rangle$ when $\operatorname{char} k = p$, which splits and gives the same relations as the constant group scheme.
Problem 2.7. We have under c that

$$\textstyle\sum_{\gamma\in\Gamma} r_\gamma e_\gamma \mapsto \sum_\gamma \sum_\sigma r_\gamma (e_\sigma \otimes e_{\sigma^{-1}\gamma} = \sum_{\sigma,\tau} r_{\sigma\tau}(e_\sigma \otimes e_\tau).$$

We want this equal to

$$\textstyle\left(\sum_\gamma r_\gamma e_\gamma\right) \otimes \left(\sum_\gamma r_\gamma e_\gamma\right) = \sum_{\sigma,\tau} r_\sigma r_\tau (e_\sigma \otimes e_\tau).$$

This implies $r_1^2 = r_1$, so r_1 is an idempotent which since a is a unit must be $r_1 = 1$, and in general, these elements are represented by a group homomorphism $\Gamma \to R^\times$, which is to say a character.
Problem 2.8(a). This is the statement $\operatorname{Hom}_R(R[X,Y]/\langle X^2 + Y^2 - 1\rangle, S) = F(S)$.
Problem 2.8(b). Check $(xx' - yy')^2 + (xy' + yx')^2 = (x^2 + y^2)(x'^2 + y'^2) = 1$. It is natural because if $f : S \to T$, the diagram

$$\begin{array}{ccc} F(S) \times F(S) & \xrightarrow{f\times f} & F(T) \times F(T) \\ \downarrow & & \downarrow \\ F(S) & \xrightarrow{\quad f \quad} & F(T) \end{array}$$

commutes, as the group law is defined by polynomial equations.
Problem 2.8(c). The comultiplication is $c : A \to A \otimes A$ is $X, Y \mapsto XX' - YY', XY' + YX'$, the counit $e : A \to R$ is $X, Y \mapsto 1, 0$, and the coinverse $i : A \to A$ is $X, Y \mapsto X, -Y$.

Problem 2.8(d). The map $R[X,1/X] \to R[X,Y]/\langle X^2+Y^2-1\rangle$ by $X \mapsto X+iY$ induces the map j on schemes, since $1/X \mapsto 1/(X+iY) = X-iY$. It is also a group homomorphism because the comultiplication maps $X \mapsto XX' \mapsto (X+iY)(X'+iY)$ and in the other direction $X \mapsto X+iY \mapsto (XX'-YY')+i(X'Y+XY')$, and these expressions are equal. If $2 \in R^\times$, then the map is injective because the images of X and $1/X$ have $X - iY \neq X + iY$, and is surjective because $(X+1/X)/2 \mapsto X$ and $(X-1/X)/2i \mapsto Y$ by trigonometry.
Problem 2.9(a). This is the statement $\mathrm{Hom}_R(R[X]/\langle X^2-X\rangle, S) = \{s : s^2 = s\}$ since the map is determined by the image of X.
Problem 2.9(b). Check $(e+e'-2ee')^2 = e^2+ee'-2e^2e'+\cdots+4e^2e'^2 = 0 = e+ee'-2ee'+\cdots+4ee' = 0$. The unit element is 0 and the inverse element is $(e,e) \mapsto e+e-2e^2 = 0$. It is natural again because the group law is a polynomial expression.
Problem 2.9(c). Comultiplication is $c : X \mapsto X+X'+2XX'$, unit is $e : X \to 0$, and inverse is $i : X \mapsto X$.
Problem 2.9(d). This is (Ex. 2.4(b)).
Problem 3.1(a). Check $(x+x')^p = 0$ and $(y+y'-W(x,x'))^p = W(x^p,x'^p) = 0$. We have the unit $(0,0)$ and inverse $(-x,y)$ since $W(x,-x) = 0$.
Problem 3.1(b). α_{p^2} is a closed subgroup scheme because it is represented by $k[X]/\langle X^{p^2}\rangle$ which defines a closed subscheme of $\operatorname{Spec} k[X]$. We know that $\alpha_{p^2}^\vee(R)$ is represented by $\mathrm{Hom}_R(\alpha_{p^2}/R, \mathbb{G}_m/R) = \mathrm{Hom}(R[T,1/T], R[X]/\langle X^{p^2}\rangle)$, which are exactly elements $T \mapsto p(X) = \sum_{i=0}^{p^2-1} a_iX^i$ where $a_0 \neq 0$, subject to the group law condition

$$\textstyle\sum_{i=0}^{p^2-1} a_i(X+X')^i = \left(\sum_{i=0}^{p^2-1} a_iX^i\right)\left(\sum_{i=0}^{p^2-1} a_iX'^i\right)$$

which says

$$\sum_{i=0}^{p^2-1} a_i \sum_{j=0}^{i} \binom{i}{j} X^jX'^{i-j} = \sum_{i,j=0}^{p^2-1} a_ia_jX^iX'^j.$$

We find $a_0^2 = a_0$ and $a_1 = a_1a_0$ so $a_0 = 1$, and similarly $ia_i = a_{i-1}a_1$ for $1 \le i < p$, so $a_i = a_1^i/i!$. At p we have $pa_p = 0 = a_{p-1}a_1 = a_1^p/(p-1)!$ so $a_1^p = 0$. Continuing, we find $(p+i)a_{p+i} = a_{p+(i-1)}a_1 = a_pa_1^i/i!$ again for $1 \le i < p$, and then since $\binom{2p}{p} = (2p)(2p-1)\dots(p+1)/p! \equiv 2 \pmod p$ we have $a_{2p}\binom{2p}{p} = 2a_{2p} = a_p^2$, and in general $a_{ip} = a_p^i/i!$, and therefore from the above $a_{jp+i} = a_1^ia_p^j/i!j!$. Finally, $p^2a_p = 0 = a_p^p/(p-1)! = 0$ so $a_p^p = 0$, and we find $T \mapsto E(a_1X)E(a_pX^p)$, where

$$E(X) = 1 + X + \frac{X^2}{2!} + \cdots + \frac{X^{p-1}}{(p-1)!}.$$

Note that $E(a_1X) = \exp(a_1X)$ since a_1 is nilpotent, so since $\exp(a(X+X')) = \exp(aX)\exp(aX')$ as power series, they indeed give homomorphisms and $\alpha_{p^2}^\vee(R) = \{(x,y) : x^p = y^p = 0\}$.

To determine the group law, we note that in the homomorphism group it is induced by multiplication (coming from the multiplication law on the tensor product), so we look at

$$E(a_1X)E(a_pX^p)E(a_1'X)E(a_p'X) = E(b_1X)E(b_pX^p)$$

so that the group law is $(a_1, a_p)(a_1', a_p') = (b_1, b_p)$. Multiplying this out, we have

$$E(a_1X)E(a_1'X) = 1 + (a_1 + a_1')X + \cdots + \frac{(a_1 + a_1')^p}{p!}X^p$$

where the latter term is $W(a_1, a_1')/(p-1)! = -W(a_1, a_1')$ since $a_1^p = a_1'^p = 0$. Since $X^{p^2} = 0$ in our ring, the additivity of the X^p part is immediate, so the group law is indeed as above.

Problem 4.1(a). If we choose a basis $M = \bigoplus_i ke_i$, then $\mathrm{End}_k(M) = \mathrm{Hom}_k(M, M) = \prod_i \mathrm{Hom}_k(k, M) = \prod_i M$, so this is determined by the matrix Hopf algebra $k[X_{ij}]_{i,j}$, with the group law $X_{ij} \mapsto \sum_r X_{ir}X'_{rj}$.

Problem 4.1(b). We now require that the determinant $\det X_{ij}$ be invertible, so we have the Hopf algebra $k[X_{ij}, 1/\det X_{ij}]$.

Problem 4.1(c). The additional requirements can be rephrased in terms of certain equations defined over R.

Problem 4.2(a). Letting $A = \mathbb{Z}[X]/\langle X^2 - 2\rangle$, we have $\Omega^1_{A/\mathbb{Z}} = A\,dX/\langle 2X\,dX\rangle \simeq \mathbb{Z}[\sqrt{2}]/\langle 2\sqrt{2}\rangle$.

Problem 4.2(b). Letting $A = \mathbb{Z}[X]/\langle 6, X^2+X+1\rangle$, we have $\Omega_{A/\mathbb{Z}} = A\,dX/\langle 0, (2X+1)\,dX\rangle \simeq (\mathbb{Z}/6\mathbb{Z})[X]/\langle X^2 + X + 1, 2X + 1\rangle$.

Problem 4.2(c). Identifying $\mathbb{Q}[T]$ with its image $\mathbb{Q}[X]$ in A, we obtain

$$\begin{aligned}\Omega^1_{A/R} =&(A\,dX \oplus A\,dY)/\langle (2X - Y + 1)\,dX + (2Y - X)\,dY,\\ &(-3X^2Y + 2XY)\,dX + (4Y^3 - X^3 + X^2)\,dY\rangle.\end{aligned}$$

Problem 4.3. G is represented by $A = k[X, Y]/\langle X^{p^2}, X^p - aY^p\rangle$, which has rank p^3 (its dimension as a k-vector space). We then have only three possibilities. It cannot be $k[T]/\langle T^{p^3}\rangle$ because A has no element whose minimal nilpotence degree is p^3. It cannot be $k[T, U]/\langle T^{p^2}, U^p\rangle$ since then $X, Y \mapsto \phi(U, V), \psi(U, V)$, and then $\phi^p - a\psi^p = 0$; since p kills any monomial containing U, we are left with an equality of two pth powers of polynomials, which is impossible as a is not a pth power. It cannot be $k[T, U, V]/\langle T^p, U^p, V^p\rangle$ since it has no element whose minimal nilpotence degree is p^2.

Problem 4.4(a). $\pi_1(\mathbb{Z}[\zeta]) = \mathrm{Gal}(\mathbb{Q}(\zeta)^{\mathrm{unr}}/\mathbb{Q}(\zeta))$. So suppose $[K : \mathbb{Q}(\zeta)] = n$ is unramified; then $d_{K/\mathbb{Q}} = |N(\Delta_{K/\mathbb{Q}(\zeta)})|d^n_{\mathbb{Q}(\zeta)} = 3^n$. But then $[K : \mathbb{Q}] = 2n$, and then by Minkowski's theorem (since $\mathbb{Q}(\zeta)$ is totally imaginary),

$$3^n \geq \left(\frac{(2n)^{2n}}{(2n)!}\right)^2 \left(\frac{4}{\pi}\right)^{2n}.$$

If we substitute $n = 1$, we obtain $3 \geq 4(4/\pi)^2$, a contradiction, and since the function on the right grows faster than 3^n, as the quotient of two successive terms is

$$\frac{(2n+2)}{(2n+1)}\left(\frac{2n+2}{2n}\right)^{2n}\left(\frac{4}{\pi}\right)^2 \geq \left(1 + \frac{1}{n}\right)^{2n} \geq 2^2),$$

we obtain a contradiction.

Problem 4.4(b). The ring $R = \mathbb{Z}[\sqrt{-2}, \zeta]$ is unramified because the discriminant of a biquadratic extension is the product of its three quadratic subfields, hence this ring has discriminant $(-8)(-3)(24) = 676 = 24^2$ where $24 = \Delta_{\mathbb{Q}(\sqrt{6})}$.

The same argument as in (a) now shows that (since $\mathbb{Q}(\sqrt{-2},\zeta)$ is totally imaginary)

$$24^n \geq \left(\frac{(2n)^{2n}}{(2n)!}\right)^2 \left(\frac{4}{\pi}\right)^{2n},$$

which for $n \geq 5$ gives a contradiction. Therefore at most $\mathbb{Z}[\sqrt{6}]$ has at most a degree 4 unramified extension arising as a quadratic extension of R, and hence it can also be a quadratic unramified extension of $\mathbb{Z}[\sqrt{6}]$. Therefore it must arise from adjoining $\sqrt{m}$ with $m \mid 6$ since otherwise we would have other primes ramifying; the only choice is adjoining i. But $\mathbb{Z}[\sqrt{6},i]$ has discriminant $(24)(4)(-24) \neq 24^2$, so this is not unramified, and we conclude that we are limited to just R, so that π_1 has order 2.

Problem 4.4(c). It is étale because it is unramified, and therefore by the equivalence of categories (with obvious action of the Galois group π) it corresponds to the Hopf algebra of a (commutative) group scheme.

Problem 4.5(a). $[n] : A \to A$ factors through $e : A \to R$ iff $I = \ker e \subset \ker[n]$ iff $[n]I = 0$; but $[n]I \equiv nI \mod I^2$, so $[n]I = 0$ iff n kills I/I^2.

Problem 4.5(b). In $\operatorname{char} k = p$, n is a unit, hence n kills I/I^2 iff $I/I^2 = 0$, hence $\Omega^1_{A/R} = A \otimes_R I/I^2 = 0$, and G is étale.

Problem 4.6(a). The only factorizations could occur from roots which must be units of $\mathbb{Z}[\alpha]$ by Gauss' lemma. The unit group here is trivial, and one checks that $f(1), f(-1) \neq 0$, so the polynomial is irreducible.

A change of variables $X \mapsto X + \alpha/3$ puts the equation in the form $X^3 - (1/3)X - (1/27)\sqrt{-23}$, and then we have $-4(1/3)^3 - 27((1/27)\sqrt{-23})^2 = 1$.

Problem 4.6(b). A cubic extension is Galois iff the Galois group of the polynomial is cyclic of order 3 iff it is contained in the alternating group iff the square root of its discriminant is already in the field, which in this case is true.

If we let θ be a root of f, the Galois action is $\theta \mapsto -\theta^2 + (\alpha - 1)\theta + 2$.

Problem 4.6(c). If we compute with points, we find the four points 0, θ, $\theta_2 = -\theta^2 + (1-\alpha)\theta + 2$, and $\theta_3 = \theta^2 - \alpha\theta + (\alpha - 2)$, where 0 is the identity element. If this is to be a group of order 4 of exponent 2, then $[2]\theta = [2]\theta_2 = [2]\theta_3 = 0$ and adding any two nonzero points gives the third. The group law is

$$\begin{aligned} X \mapsto X + X' + aXX' + b(X^2X' + XX'^2) + c(X^3X' + XX'^3) \\ + d(X^2X'^2) + e(X^3X'^2 + X^2X'^3) + f(X^3X'^3) \end{aligned}$$

and substituting these we obtain linear equations, e.g. simplifying

$$0 = 2\theta + a\theta^2 + 2b\theta^3 + 2c\theta^4 + d\theta^4 + 2e\theta^5 + f\theta^6$$

we obtain for the constant coefficient

$$-2b - 2\alpha c - \alpha d + (10 - 4\alpha)e + (9 - \alpha)f = 0.$$

Solving this system we obtain

$$(a,b,c,d,e,f) = (2\alpha + 2, 4\alpha - 16, -3\alpha + 4, -10\alpha + 2, \alpha + 12, 2\alpha - 8).$$

Problem 5.1(a). If $p \neq 2$, then $\alpha = (\zeta_p - 1)/(\sqrt[p]{\epsilon} - 1)$ is integral: since

$$(\sqrt[p]{\epsilon} - 1)^p \equiv \epsilon - 1 \equiv 0 \pmod{p}$$

but not modulo p^2, $v_p(\sqrt[p]{\epsilon} - 1) = 1/p$, and it is a standard fact (here we use $p \neq 2$) that $v(\zeta_p - 1) = 1/(p-1)$. Hence $v(\alpha) = 1/(p-1) - 1/p = 1/p(p-1) > 0$, so α

is integral. If $p = 2$, then $\zeta_2 = -1$, so we have $\mathbb{Z}[\sqrt{\epsilon}]$; the discriminant is 4ϵ, and $\epsilon \equiv 1 \pmod 2$, and since the extension is Eisenstein, $2 \nmid (\mathscr{O} : \mathbb{Z}_2[\sqrt{\epsilon}])$, so it is the full ring of integers.

Problem 5.1(b). The extension is totally ramified and $v(\alpha) = 1/p(p-1) = [F : \mathbb{Q}_p]$, and α is integral, so it is a uniformizer.

Problem 5.1(c). $i(\sigma) = v(\sigma\alpha - \alpha)$. If $\sigma \in H \setminus \{1\}$, say $\sigma(\zeta_p) = \zeta_p$ and $\sigma(\sqrt[p]{\epsilon}) = \zeta_p^i \sqrt[p]{\epsilon}$, then

$$\begin{aligned} i(\sigma) &= v\left(\frac{\zeta_p - 1}{\zeta_p^i \sqrt[p]{\epsilon} - 1} - \frac{\zeta_p - 1}{\sqrt[p]{\epsilon} - 1}\right) \\ &= v(\zeta_p - 1) + v(\zeta_p^i - 1) - v(\zeta_p^i \sqrt[p]{\epsilon} - 1) - v(\sqrt[p]{\epsilon} - 1) \\ &= 2/(p-1) - 2/p = 2/p(p-1). \end{aligned}$$

If $\sigma \notin H$, then since $(\zeta_p^i - 1)/(\zeta_p - 1) = \omega$ is a unit such that $\omega - 1 = \zeta_p + \cdots + \zeta_p^{i-1} = \zeta_p(\zeta_p^{i-1} - 1)/(\zeta_p - 1)$ is also a unit, we have

$$\begin{aligned} i(\sigma) &= v\left(\frac{\zeta_p^i - 1}{\zeta_p^j \sqrt[p]{\epsilon} - 1} - \frac{\zeta_p - 1}{\sqrt[p]{\epsilon} - 1}\right) \\ &= v(\zeta_p - 1) + v(\omega - 1) - v(\sqrt[p]{\epsilon} - 1) = 1/p - 1/(p-1) = 1/p(p-1). \end{aligned}$$

Problem 5.1(d). This is just the statement of (*c*).

Problem 5.1(e). $G^{(u)} = G_{(\phi_{L/K}^{-1}(u))}$. We find

$$\phi(i) = \begin{cases} p(p-1)i, & 0 \le i \le 1/p(p-1); \\ 1 - 1/(p-1) + pi, & 1/p(p-1) < i \le 2/p(p-1); \\ 1 + 1/(p-1), & i > 2/(p-1). \end{cases}$$

Hence

$$\phi^{-1}(u) = \begin{cases} u/p(p-1), & 0 \le u \le 1; \\ (u-1)/p + 1/p(p-1), & 1 < u \le 1 + 1/(p-1); \\ 1 + 1/(p-1), & u > 1 + 1/(p-1) \end{cases}$$

which implies the result.

Problem 5.1(f). $i_{F/\mathbb{Q}_p} = 2/p(p-1)$ as this is the maximum value. Therefore

$$u_{F/\mathbb{Q}_p} = \phi(i_{F/\mathbb{Q}_p}) = 1 - 1/(p-1) + p(2/p(p-1)) = 1 + 1/(p-1)$$

and

$$v(\mathscr{D}_{F/\mathbb{Q}_p}) = u_{F/\mathbb{Q}_p} - i_{F/\mathbb{Q}_p} = 1 + 1/(p-1) - 2/p(p-1) = 1 + (p-2)/p(p-1).$$

Problem 5.2(a). For a quadratic imaginary extension, the class group is in one-to-one correspondence with reduced quadratic binary forms, $[a, b, c]$ such that $d = b^2 - 4ac = -7$, and reduced implies $-|a| < b \le |a| < |c|$ or $0 \le b \le |a| = |c|$. We need only check $0 < a \le \sqrt{-d/3}$, i.e. $a \le 1$; we find only $a = b = 1$, $c = 2$, so the class group is trivial.

Problem 5.2(b). The group schemes of order 2 are in one-to-one correspondence with factorizations of 2, for which we have the trivial factorization and $2 = \pi\overline{\pi}$, giving us 2 others.

Problem 5.3(a). We have $A = R[T,X]/\langle T^2 + \pi T, X^2 - 1\rangle$, so

$$\Omega^1_{A/R} = (A\,dT \oplus A\,dX)/\langle (2T+\pi)\,dT, 2X\,dX\rangle \simeq A/\langle 2T+\pi\rangle \oplus A/\langle 2X\rangle.$$

References

[AM] M.F. Atiyah and I.G. MacDonald, *Introduction to commutative algebra*, Reading, Mass.: Perseus, 1969.

[A] M. Artin, *Algebraization of formal moduli. II. Existence of modifications.*, Ann. of Math. (2) **91**, 1970, 88–135.

[A2] M. Artin, *The implicit function theorem in algebraic geometry*, 1969 Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), London: Oxford Univ. Press, 13–34.

[BM] Pierre Berthelot, Lawrence Breen, and William Messing, *Thorie de Dieudonn cristalline. II*, Lecture notes in mathematics, vol. 930, Berlin-New York: Springer-Verlag, 1982.

[F] Jean-Marc Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbb{Z}$, Invent. math. **81** (1985), 515–538.

[J] A. J. de Jong, *Crystalline Dieudonné module theory via formal and rigid geometry*, Inst. Hautes tudes Sci. Publ. Math., **82** (1995), 5–96.

[L] Serge Lang, *Algebraic number theory*, 2nd ed., Graduate texts in mathematics, 110, New York: Springer-Verlag, 1994.

[Mac] Saunders Mac Lane, *Categories for the working mathematician*, 2nd ed., Graduate texts in mathematics, vol. 5, New York: Springer-Verlag, 1998.

[Mar] Jacques Martinet, *Petits discriminants des corps de nombres*, Number theory days, (Exeter, 1980), London Math. Soc. lecture note series, vol. 56, Cambridge-New YorK: Cambridge Univ. Press, 1982, 151–193.

[Mat] Hideyuki Matsumura, *Commutative algebra*, New York: W.A. Benjamin, 1970.

[Mil] J.S. Milne, *Étale cohomology*, Princeton mathematical series, vol. 33, Princeton, New Jersey: Princeton University Press, 1980.

[Mur] J.P. Murre, *Lectures on an introduction to Grothendieck's theory of the fundamental group*, Tata Institute of Fundamental Research lectures on mathematics, No. 40, Bombay: Tata Institute of Fundamental Research, 1967.

[O] A. Ogg, *Abelian curves of* 2*-power conductor*, Proc. Cambr. Phil. Soc. **62** (1966), 143–148.

[R] M. Raynaud, *Passage au quotient par une relation d'quivalence plate*, Proc. Conf. Local Fields (Driebergen, 1966), Berlin: Springer, 78–85.

[Ser] Jean-Pierre Serre, *Local fields*, Graduate texts in mathematics, vol. 67, New York: Springer-Verlag, 1979.

[Sha] S.S. Shatz, Group schemes, formal groups, and p-divisible groups, in *Arithmetic geometry* (University of Connecticut, Storrs, Conn., 1984), eds. G. Cornell and J.H. Silverman, New York: Springer-Verlay, 1984, 29–78.

[Sil] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate texts in mathematics, vol. 106, Berlin: Springer, 1994.

[Tat] John Tate, Finite flat group schemes, in *Modular forms and Fermat's last theorem*, eds. Gary Cornell, Joseph H. Silverman, and Glenn Stevens, New York: Springer-Verlag, 1997, 121–154.

[Tat2] John T. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

[TO] John Tate and Frans Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3**, 1–21.

[Was] Lawrence C. Washington, *Introduction to cyclotomic fields*, Graduate texts in mathematics, vol. 83, New York: Springer-Verlag, 1982.

[Wat] William C. Waterhouse, *Introduction to affine group schemes*, Graduate texts in mathematics, vol. 66, New York-Berlin: Springer-Verlag, 1979.