# Commutative Finite Group Schemes

James Taylor

October 28, 2020

# Overview

## Basics and Examples

# Basics and Examples

All rings are commutative with unit.

$R$ is a ring and $k$ is a field.

$R$-algebra = commutative associative unital $R$-algebra.

# Basics and Examples

Last time we saw group objects in a category.

A group object $G$ is called *commutative* if the multiplication commutates with the twist map $\pi_2 \times \pi_1 : G \times G \to G \times G$.

Equivalently, if the group structure on each $\mathrm{Hom}(X, G)$ is commutative.

# Basics and Examples

A morphism of group objects $f : G \to H$ is a morphism in the category such that $m_H \circ (f \times f) = f \circ m_G$.

Equivalently, the induced map $\mathrm{Hom}(X, G) \to \mathrm{Hom}(X, H)$ is a homomorphism of groups for all objects $X$.

Group objects with such morphisms form a subcategory.

# Basics and Examples

## Definition

A morphism of schemes $f : X \to Y$ is *finite* if there is an open cover by affine schemes $V_i = \mathrm{Spec}(A_i)$ such that for all $i$, $f^{-1}(V_i) = \mathrm{Spec}(B_i)$ is affine, with $B_i$ a finitely generated $A_i$-module.

## Proposition

*$f : X \to Y$ is finite if and only if for any affine open $V = \mathrm{Spec}(A)$, then $f^{-1}(V) = \mathrm{Spec}(B)$ is affine open with $B$ is a finitely generated $A$-module.*

# Basics and Examples

If the base $Y = \text{Spec}(R)$ is affine, then $f : X \to \text{Spec}(R)$ is finite if and only if $X = \text{Spec}(A)$ and $A$ is a finite $R$-algebra.

Similarly, an *affine* scheme $X = \text{Spec}(A)$ over an affine base $\text{Spec}(R)$ is of finite-type if and only if $A$ a finitely-*generated* $R$-algebra.

We call group schemes over $R$ *algebraic* if they are of finite-type.

# Basics and Examples

Therefore, we can talk about commutative finite group schemes over $R$.

There are automatically affine.

They are the same as finite dimensional commutative cocommutative hopf algebras over $R$.

# Basics and Examples

Notation: $G = \text{Spec}(A)$ is a group scheme over $R$.

- $\triangle : A \to A \otimes A$ the comultiplication.
- $\epsilon : A \to R$ the counit.
- $S : A \to A$ the antipode.

# Basics and Examples

Group Object $G$ in $(\mathrm{Aff}/R)$ $\longleftrightarrow$ Functor $F : (\mathrm{Aff}/R)^{op} \to \underline{\mathrm{Grp}}$ s.t. $\mathrm{Forget} \circ F = \mathrm{Hom}(-, G)$

$\updownarrow$ $\qquad\qquad$ $\updownarrow$

Commutative, Cocommutative Hopf Algebra $A$ over $R$ $\longleftrightarrow$ Functor $F : (R\text{-}\mathrm{Alg}) \to \mathrm{Grp}$, $\mathrm{Forget} \circ F = \mathrm{Hom}(A, -)$

$\Delta = \iota_1 * \iota_2$ in $\mathrm{Hom}(A, A \otimes A)$

$\varepsilon =$ identity of $\mathrm{Hom}(A, R)$

$S =$ inverse of $id_A$ in $\mathrm{Hom}(A, A)$

- Mult: $A \xrightarrow{\Delta} A \otimes A \xrightarrow{f \otimes g} B$
- Identity: $A \xrightarrow{\varepsilon} R \longrightarrow B$
- Inverse: $A \xrightarrow{S} A \xrightarrow{f} B$

$f$ in $\mathrm{Hom}(A, B)$

# Basics and Examples

Hopf ideal of $A$: ideal $I$ of $A$ such that

- $\triangle(I) \subset A \otimes I + I \otimes A$.
- $S(I) \subset I$.
- $\epsilon(I) = 0$.

Example: the *augmentation ideal* $\ker(\epsilon) \subset A$.

Closed subschemes of $\mathrm{Spec}(A)$ correspond to ideals of $A$.

Hopf ideals correspond to closed sub-group schemes.

These conditions: there is an induced comultiplication, antipode and counit on the quotient $A/I$.

# Basics and Examples

From now we will work over the field $k$.

$G = \mathrm{Spec}(A)$ be a commutative finite group scheme.

$k$ is a field so this is automatically flat.

More generally: consider commutative finite flat group schemes over a noetherian ring.

Later we will discuss commutative finite flat group schemes over a noetherian hensellian local ring.

# Example: Idempotents in a Ring

The idempotent elements ($e = e^2$) of a ring $B$ form a group.

The multiplication is defined by

$$(y, z) \to y(1 - z) + z(1 - y),$$

with identity 0 and all elements self-inverse.

Note: $yz$, $y(1 - z)$, $z(1 - y)$ and $(1 - y)(1 - z)$ are pairwise orthogonal idempotents.

Transport group structure to turn $A := R[X]/(X^2 - X)$ into a finite commutative hopf algebra.

# Example: Idempotents in a Ring

Given a group structure on $\mathrm{Hom}(A, B)$ for all rings $B$ how do we recover the multiplication, counit and antipode?

Let $f, g : A \to B$.

$f$ corresponds to $f(X) \in B$, thus

$$(f * g)(X) = f(X)(1 - g(X)) + g(X)(1 - f(X)).$$

# Example: Idempotents in a Ring

- Comultiplication $\triangle$: the product of the inclusion maps $\iota_1, \iota_2 : A \to A \otimes A$ in $\mathrm{Hom}(A, A \otimes A)$.

$$
\begin{aligned}
\triangle(X) &= (\iota_1 * \iota_2)(X) \\
&= (X \otimes 1)(1 \otimes 1 - 1 \otimes X) + (1 \otimes X)(1 \otimes 1 - X \otimes 1) \\
&= (X \otimes 1)(1 \otimes (1 - X)) + (1 \otimes X)((1 - X) \otimes 1) \\
&= X \otimes (1 - X) + (1 - X) \otimes X \\
&= 1 \otimes X + X \otimes 1 - 2X \otimes X.
\end{aligned}
$$

- Counit $\epsilon$: the identity element of $\mathrm{Hom}(A, R)$: $\epsilon(X) = 0$.
- Antipode $S$: the inverse of $\mathrm{id}_A$ in $\mathrm{Hom}(A, A)$: $S(X) = X$.

# Basics and Examples

**Definition**

The rank/order of a finite group scheme $G = \operatorname{Spec}(A)$ over $k$ is $\dim_k A$.

More generally over a noetherian ring $R$: the order of $G$ is the locally constant function on $\operatorname{Spec}(A)$

$$P \mapsto \operatorname{rank}_{R_P} A_P$$

# Example: Constant Group Schemes

The constant group scheme of a finite group $H$ has order $|H|$.

$k$-algebra $k^H$: functions from $H \to k$, with

- $\triangle(f)(x, y) = f(xy)$,
- $S(f)(h) = f(h^{-1})$,
- $\epsilon(f)(h) = f(1)$.

Cocommutative if and only if $H$ is abelian.

# Example: Constant Group Schemes

The group algebra $kH$ has

- $\triangle(h) = h \otimes h$ (group-like),
- $S(h) = h^{-1}$,
- $\epsilon(h) = 1$,

for all $h \in H$.

# Basics and Examples

Cartier dual of $G$: group scheme defined by the dual hopf algebra.

We need both cocommutativity and finite dimension of $A$.

If $A$ was not cocommutative then $A^*$ would not be commutative so would not even correspond to a group scheme.

If $A$ not finite dimensional, then $A^*$ is not well defined ($A^* \otimes A^*$ is a proper subset of $(A \otimes A)^*$, so one might have $m_A^*(A) \not\subset A^* \otimes A^*$).

# Example: Duals

- Let $k$ has characteristic $p > 0$.

  $\alpha_p$ is the kernel of the power of $p$ map.

  Represented by $k[t]/(t^p)$.

  This is self dual.

  The isomorphism is given by: if $\{e_i^*\}_{0 \leq i < p}$ is the dual basis of $k[t]/(t^p)$ coming from the standard basis $\{1, T, T^2, ..., T^{p-1}\}$, then send

$$e_k^* \to T^k/k!.$$

# Example: Characteristic $p$

If $k$ has characteristic $p > 0$, then $\underline{\mathbb{Z}/p\mathbb{Z}}$, $\mu_p$ and $\alpha_p$ are pairwise non-isomorphic.

$\underline{\mathbb{Z}/p\mathbb{Z}}$ is reduced (because $k$ is).

Both others aren't: represented by $k[T]/(T^p - 1)$ and $k[X]/(X^p)$.

These last two have isomorphic algebras ($T \mapsto X + 1$).

But are *not* isomorphic as hopf algebras: the dual of the first is $\underline{\mathbb{Z}/p\mathbb{Z}}$ but the second is self dual.

# Basics and Examples

Here is an interesting theorem by Deligne.

**Theorem**

*Let $G$ be a finite flat commutative group scheme over $R$ of order $n$. Then $n$ kills $G$: the multiplication by $n$ map $n : G \to G$ is zero.*

This is also conjectured to hold for non-commutative finite flat groups.

# Group Schemes of Rank 2

Classify all finite group schemes free of rank 2 over $R$.

### Proposition

*Let $G = \mathrm{Spec}(A)$ be a finite group scheme over $R$ that is free of rank 2. Then $G$ is isomorphic to*

$$G_{a,b} = \mathrm{Spec}\,(B)\,,\; B = R[X]/(X^2 - aX)$$

*with group law $\triangle(X) = 1 \otimes X + X \otimes 1 - bX \otimes X$, and $a, b \in R$ with $ab = 2$.*

*Furthermore, $G_{a,b}$ as defined above is a group scheme and $G_{a,b} \cong G_{c,d}$ if and only if $(c,d) = (ua, u^{-1}b)$ for a unit $u \in R$.*

# Group Schemes of Rank 2

**Proof.**

The augmentation ideal gives a direct sum $A = R \oplus I$.

$I$ is actually free, $I = Rx$, so any element of $A$ is $r + sx$.

As $I$ is an ideal, then $x^2 = ax \in Rx$ for a unique $a \in R$.

Therefore, we can view $A = R[X]/(X^2 - aX)$.

Comultipliciation determined by $\triangle(x)$.

$R$-linear combination of $1 \otimes x$, $x \otimes 1$, $1 \otimes 1$, $x \otimes x$. □

# Group Schemes of Rank 2

**Proof.**

Use both $m \circ (\mathrm{id}_A \otimes \epsilon) \circ \triangle = \mathrm{id}_A = m \circ (\epsilon \otimes \mathrm{id}_A) \circ \triangle$.

Compatibility of multiplication and comultiplication, and $a\triangle(x) = \triangle(x^2)$:

$$(ab-1)(ab-2)=0.$$

$\epsilon \circ S = \epsilon$ implies $S(I) = I$.

Hence for a unique $c \in R$, $S(x) = cx$.

Cocommutatively of $S$ means that $S^2 = \mathrm{id}_A$, thus $c^2 = 1$. □

# Group Schemes of Rank 2

**Proof.**

Axiom for antipode: $m \circ (\mathrm{id}_A \otimes S) \circ \triangle$ is the zero map.

Hence $c + 1 = abc$. Therefore,

$$0 = c^2 - 1 = (c-1)(c+1) = abc^2 - abc = ab - abc,$$

hence $c + 1 = ab$ and $ab - 1 = c$ is a unit, thus $ab = 2$.

Conversely, this defines a cocommutative hopf algebra.

The isomorphism type claim follows from direct computation. □

**Corollary**

*All finite group schemes over $R$ of rank 2 are commutative.*

# Group Schemes of Rank 2

## Example

$R = k$ is a field, characteristic two: exactly 3. We have actually seen all three already!

1. $\mu_2$ is represented by $k[t]/(t^2 - 1)$, with $m(t) = t \otimes t$.

   $$k[t]/(t^2 - 1) \to k[x]/(x^2), \;\; t \mapsto x + 1$$

   New multiplication is then

   $$\begin{aligned} \triangle'(x) &= \triangle(t-1) = \triangle(t) - \triangle(1) \\ &= t \otimes t - 1 \otimes 1 \\ &= (x+1) \otimes (x+1) - 1 \otimes 1 \\ &= 1 \otimes x + x \otimes 1 + x \otimes x, \end{aligned}$$

   thus $b = -1 = 1$ and $\mu_2 \cong G_{0,1}$ .

# Group Schemes of Rank 2

### Example

2. $\alpha_2$ is already of the above form, $G_{0,0}$.
3. Idempotent hopf algebra: $k[x]/(x^2 - x)$. Thus $a = 1$, and multiplication has $x$ primitive, hence $b = 0$, and this is $G_{1,0}$.

### Example

$R = k$ is a field, characteristic $\neq$ two: one finite group scheme over $k$.

### Example

If $R$ is not a field, then there can be more. Let $R = \mathbb{Z}_2[\sqrt[79]{2}]$. Then there are 80, corresponding to the factorisations of $2 = (\sqrt[79]{2})^i(\sqrt[79]{2})^{79-i}$ for $0 \leq i \leq 79$.

# Group Schemes of Rank 2

Oort and Tate in [1] classify finite group schemes of order $p$ over a complete noetherian local ring of residue characteristic $p$: for such $R$: isomorphism classes of finite flat group schemes over $R$ of order $p$ are classified by factorisations of $p = ac$ in $R$, with $ac = a'c'$ equivalent if there is some unit $u$ with $a = u^{p-1}a'$, $c = u^{1-p}c'$.

[1] Tate, John, and Frans Oort. "Group schemes of prime order." Annales scientifiques de l'École Normale Supérieure. Vol. 3. No. 1. 1970.

## The Category of Finite Commutative Group Schemes

# The Category

Commutative finite group schemes form an abelian category.

$G = \mathrm{Spec}(A)$ and $H = \mathrm{Spec}(B)$ be commutative finite group schemes.

$f, g : G \to H$ are elements of $\mathrm{Hom}(G, H)$.

Abelian group structure: $f + g$ is the morphism

$$G \xrightarrow{\text{diag}} G \times G \xrightarrow{f \times g} H \times H \xrightarrow{m_H} H.$$

# The Category

Corresponds to the convolution product on maps between hopf algebras:

$$A \leftarrow A \otimes A \xleftarrow{f' \otimes g'} B \otimes B \xleftarrow{\triangle} B.$$

Furthermore, the $f - g$ in $\mathrm{Hom}(B, A)$ is

$$A \leftarrow A \otimes A \xleftarrow{f' \otimes g'} B \otimes B \xleftarrow{\mathrm{id} \otimes S} B \otimes B \xleftarrow{\triangle} B.$$

# The Category

The zero morphism $G \to H$ is the composition of the morphism to and then from the zero object $\mathrm{Spec}(k)$.

The kernel of $f$ is $G \times_H \mathrm{Spec}(k)$, which corresponds to the cokernel $A \otimes_B k$.

The cokernel is exists in this category but is harder to describe - see last week.

# The Category

We can give exact sequences a more down to earth description:

**Proposition**

*Let* $K = \mathrm{Spec}(A)$, $G = \mathrm{Spec}(B)$, $H = \mathrm{Spec}(C)$ *and*

$$1 \to K \xrightarrow{g} G \xrightarrow{f} H \to 1$$

*be morphisms of commutative finite group schemes over* $k$*.*

*Then this sequence is exact if and only if*

- $(K, g)$ *is the kernel of* $f$*.*
- $f' : C \to B$ *is faithfully flat.*

# The Category

Fortunately, this becomes even easier.

**Theorem**

*Let $A \subset B$ be hopf algebras over a field. Then $B$ is faithfully flat over $A$.*

**Proof.**

Waterhouse Chapter 14. □

# The Category

The theorem above can actually be used for the following.

**Theorem**

*Let $A$ represent a finite connected group scheme over a perfect field $k$ of characteristic $p$. Then*

$$A \cong k[X_1, ..., X_n]/(X_1^{e_1} \cdots X_n^{e_n})$$

*for some $e_1, ..., e_n \in \mathbb{N}$.*

In particular the order is a power of $p$.

# Étale Group Schemes and Separable Algebras

## Étale Group Schemes and Separable Algebras

**Theorem**

*Let $B$ be any ring. Then idempotents of $B$ are in one-to-one correspondence with clopen sets of* $\operatorname{Spec}(B)$.

The open set of $\operatorname{Spec}(B)$ corresponding to an idempotent $e \in B$ is $Z(e) = \{P \in \operatorname{Spec}(B) \mid e \in P\}$, with complement $Z(1-e)$.

$\operatorname{Spec}(A)$ is connected if and only if $A$ has no non-trivial idempotents.

# Étale Group Schemes and Separable Algebras

Now consider the finite group scheme $\mu_3$ over a field $k$, represented by $A = k[X]/(x^3 - 1)$.

Over $\mathbb{R}$, the has two connected components corresponding to the factorisation $X^3 - 1 = (X - 1)(X^2 + X + 1)$.

However, the base extension to $\mathbb{C}$ has 3 connected components as this splits into linear polynomials.

# Étale Group Schemes and Separable Algebras

Therefore, we see that base extension can create additional idempotents.

Want a nicer theory of connected components which detects potential idempotents that appear after base extension.

To do this we use separable algebras.

**Lemma**

*Let $A$ be a finite dimensional $k$-algebra.*

*Then (as a $k$-algebra) $A$ is isomorphic to a finite product $A_i$ of $k$-algebras each with a unique prime/maximal ideal consisting of nilpotent elements.*

# Étale Group Schemes and Separable Algebras

### Example

- $\mathbb{Q}[X]/(X^2)$ is of this form already with unique maximal ideal generated by $X$.
- $\mathbb{Q}[X,Y]/(X^2,XY,Y^2) \cong \mathbb{Q}[X]/(X^2) \times \mathbb{Q}[Y]/(Y^2)$.

### Corollary

*A finite dimensional k-algebra $A$ is connected ($\mathrm{Spec}(A)$ is connected) if and only if $A$ is local.*

# Étale Group Schemes and Separable Algebras

**Proposition**

*Let $A$ be a finite dimensional $k$-algebra. The following are equivalent.*

1. $A \otimes k^a$ *is reduced.*
2. $A \otimes k^a \cong k^a \times \cdots \times k^a$ *as a* $k^a$*-algebra.*
3. $\dim(A)$ *is equal to the number of* $k$*-algebra homomorphisms* $A \to k^a$.
4. $A$ *is a product of separable field extensions.*
5. $A \otimes k^s \cong k^s \times \cdots \times k^s$ *as a* $k^s$*-algebra.*

*If* $k$ *is perfect this is further equivalent to* $A$ *being reduced.*

# Étale Group Schemes and Separable Algebras

**Definition**

We call a finite dimensional $k$-algebra $A$ *separable* if $A$ satisfies the above properties.

**Example**

- Separable field extensions are separable.
- $\mathbb{Q}[X]/(X^2)$ is a finite dimensional $\mathbb{Q}$-algebra that is not separable.

# Étale Group Schemes and Separable Algebras

From the proposition one can see that products, tensor products, subalgebras and quotients of separable algebras are separable.

Separability is invariant under base change:

**Proposition**

*Let $A$ be a finite dimensional $k$-algebra, and $L$ be any field extension of $k$. Then $A$ is separable over $k$ if and only if $A \otimes_k L$ is separable over $L$.*

# Kähler Differentials

For any $R$-algebra $A$, an $R$-derivation of $A$ with values in an $A$-module $M$, is an $R$-linear map $\delta : A \to M$ such that

$$\delta(xy) = x\delta(y) + \delta(x)y.$$

Universal derivation $d : A \to \Omega^1_{A/R}$.

Constructed as the quotient of the free $A$-module on symbols $da$ for all $a \in A$, by the obvious relations

- $d(a - b) - da - db$,
- $r(da) - d(ra)$,
- $d(ab) - adb - bda$.

# Kähler Differentials

Under base change: $R \to R'$, the universal property implies that

$$\Omega^1_{A/R} \otimes_R R' \cong \Omega^1_{(A \otimes_R R')/R'}.$$

This has lots of nice properties which we won't be concerned with.

This construction does allow us to generalise the separable algebras to bases other than fields.

# Étale Group Schemes and Separable Algebras

**Definition**

An *étale* map is a ring homomorphism $A \to B$ which is flat, finitely presented and $\Omega_{B/A} = 0$.

The condition on the morphism $A \to B$ that $\Omega_{B/A} = 0$ is sometimes called being unramified.

# Étale Group Schemes and Separable Algebras

The following proposition shows how that this coincides with the notion of an étale morphism of schemes.

**Proposition**

*If $h : A \to B$ is flat of finite presentation, then $h$ is étale if and only if for each $P \in \mathrm{Spec}(A)$, $B \otimes_A (A/P)$ is an étale $A/P$-algebra.*

# Étale Group Schemes and Separable Algebras

Over a field this becomes simpler and more tangible:

**Proposition**

*Thus over a field, a finitely generated algebra is étale if and only if $\Omega_{B/A} = 0$, if and only if $A$ is separable.*

# Classification of Separable Algebras

Now we would like to classify separable algebras.

Idea: separable algebras over $k$ look essentially the same over $k^s$.

It makes sense that this can be done with galois theory, which classifies separable extensions.

# Étale Group Schemes and Separable Algebras

Recall:

Let $L/k$ be a finite Galois extension of $k$.

Then any automorphism of $k^s/k$ maps $L$ to $L$.

On the other hand, any automorphism of $L/k$ can be uniquely extended to one of $k^s/k$.

Give $\mathrm{Gal}(k^s/k)$ the standard profinite topology.

Basis of open subgroups at the identity is $\mathrm{Gal}(k^s/L)$, where $L$ is a finite extension of $k$.

# Classification of Separable Algebras

If $X$ is a set with an action of a topological group $G$, then this action is called *continuous* if for all $x \in X$, $\mathrm{Stab}_G(x)$ is open in $G$.

Equivalently, regarding $X$ as having the discrete topology, $G \times X \to X$ is continuous.

Therefore, an action of $\Gamma$ on a set $X$ is continuous if and only for every point there is some finite extension $L$ of $k$ with $\mathrm{Gal}(k^s/L)$ acting trivially.

# Classification of Separable Algebras

**Theorem**

*Separable $k$-algebras are anti-equivalent to finite sets with a continuous action of $\Gamma = \mathrm{Gal}(k^s/k)$.*

Idea: Any finite separable field extension $L$ of $k$ has $[L : k]$ embeddings into $k^a$, and so into $k^s$.

Now $\Gamma$ has a natural action by left multiplication on the finite set of left cosets of $\mathrm{Gal}(k^s/L)$, with stabiliser $\mathrm{Stab}_\Gamma(x\,\mathrm{Gal}(k^s/L)) = x\,\mathrm{Gal}(k^s/L)x^{-1}$, an open subgroup.

# Classification of Separable Algebras

In order to phrase this action for more general algebras, we can identity the coset space of $\mathrm{Gal}(k^s/L)$ canonically with $\mathrm{Hom}_k(L, k^s)$ (any $k$-linear field morphism $L \to k^s$ can be extended to one $k^s \to k^s$).

This is unique exactly up precomposition with an element of $\mathrm{Gal}(k^s/L)$.

# Classification of Separable Algebras

For a separable $k$-algebra $A$: $X_A = \mathrm{Hom}_k(A, k^s)$ be the finite set of $k$-algebra homomorphisms, with natural action $\psi(f)(a) = \psi(f(a))$ from the action of $\psi \in \Gamma$ on $k^s$.

This action of $\Gamma$ is continuous: the image of each $f : A \to k^s$ lies in some finite extension of $k$.

Any algebra map $A \to B$ induces a map $G$-sets $X_B \to X_A$.

# Classification of Separable Algebras

Given a finite set with continuous action of Γ, define

$$A_X = \mathrm{Map}_\Gamma(X, k^s) = \{f : X \to k^a \mid f(x)^\gamma = f(x^\gamma) \text{ for all } \gamma \in \Gamma\},$$

This is a ring using pointwise operations in $k^s$, and a $k$-algebra via the embedding sending each $r \in k$ to the constant function on $X$ with value $r$.

# Classification of Separable Algebras

Want to show that $A_X$ is a finite-dimensional separable $k$-algebra.

Enough to show this for $X_1 \subset X$ a transitive $\Gamma$-set.

If this is separable, then

$$A_X = A_{X_1 \sqcup \cdots \sqcup X_r} = A_{X_1} \times \cdots \times A_{X_r}$$

is separable too.

# Classification of Separable Algebras

As $X_1$ has continuous action of $\Gamma$ and is finite, for any $x_1 \in X_1$, there is some galois $L/k$ with $H = \mathrm{Stab}_\Gamma(x_1) \supset \mathrm{Gal}(k^s/L)$ acting trivially on $x_1$ and hence $X_1$.

Thus for all $f \in A_{X_1}$, $x \in X_1$, $\gamma(f(x)) = f(x)$ so we have $f(x) \in L$ (if not then some $\gamma \in \Gamma$ has $\gamma(f(x)) \neq f(x)$).

Claim: $L^H \cong A_{X_1}$, so $A_{X_1}$ is a separable field extension of $k$.

$f \in A_{X_1}$ is determined by its value on $x_1$: $y \mapsto f_y(x_1) = y$ and $f \to f(x_1) \in L^H$.

# Classification of Separable Algebras

Note that this correspondence matches the size of $X$ with the dimension of $A$.

$[L^H : k] = [\Gamma : H] = |\Gamma/H|$, which is equal to $|X|$ by the orbit stabiliser theorem as the action is transitive.

Additionally, writing $A$ the product of separable field extensions, the orbits of $X$ match up to each factor.

# Classification of Separable Algebras

**Example**

The $\mathbb{Q}$-algebra $\mathbb{Q}(\sqrt{2})$ corresponds to a set with two elements, with action of $C_2 = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{2}))$ swapping the elements.

**Definition**

A finite group scheme $\mathrm{Spec}(A)$ over $k$ is called etale if $A$ is separable.

# Classification of Separable Algebras

Then in light of the last theorem:

**Theorem**

*Finite étale group schemes over $k$ are anti-equivalent to finite groups with a continuous action of $\Gamma = \mathrm{Gal}(k^s/k)$ by group automorphisms.*

# Classification of Separable Algebras

**Proof.**

The above equivalence specialises to one here.

A finite étale group scheme $\mathrm{Spec}(A)$ induces a group structure naturally on $\mathrm{Hom}_k(A, k^s)$ that is compatible with the group action.

Conversely, if $X$ is in fact as group with a continuous group action of $\Gamma$, then $A_X$ has hopf algebra structure:

- Comultiplication: $\triangle_X(f)(x, y) = f(xy)$, viewing $A_X \otimes A_X$ as the space of functions $X \times X \to k^s$.
- Counit: $\epsilon_X(f)(x) = f(1)$.
- Antipode: $S_X(f)(x) = f(x^{-1})$. □

# Classification of Separable Algebras

**Example**

A finite group $X$ with trivial action on $\Gamma$ corresponds to the constant group scheme associated to $X$.

Thus if $k$ is algebraically closed, then the finite étale group schemes over $k$ are exactly the constant group schemes of finite groups.

Finite group schemes which become constant group schemes after a finite extension are dubbed "twisted" constant group scheme.

# Classification of Separable Algebras

## Example

Let $k = \mathbb{R}$ so $k^s = \mathbb{C}$. Then to which finite group and action of $C_2 = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ does $\mu_3$ (represented by $\mathbb{R}[X]/(X^3 - 1)$) correspond?
Write $\omega$ for a non-trival third root of unity in $\mathbb{C}$.

Then $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}(\omega), \mathbb{C})$ has three elements so is $C_3$. One can see immediately that this is not the constant group scheme $C_3$, as $\mu_3$ has only one real point.

The action of $C_2$ by swapping the generators.

# Classification of Separable Algebras

**Example**

Alternatively, if $k = \mathbb{C}$, the $\Gamma = 1$ is trivial, and $\mathrm{Hom}_{\mathbb{C}}(\mathbb{C}[X]/(X^3 - 1), \mathbb{C}) \cong C_3$ (this is the same as asking how many one-dimensional representations are there of the group ring $\mathbb{C}[C_3]$) with trivial action.

So $\mu_3$ over $\mathbb{R}$ is an example of a twisted constant group scheme.

# Classification of Separable Algebras

## Example

Over $\mathbb{Q}$ there are infinitely many twisted forms of the constant group scheme $\mathbb{Z}/3\mathbb{Z}$.

Each distinct quadratic extension $L$ of $\mathbb{Q}$ gives a distinct continuous action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathrm{Aut}(C_3) = C_2$.

Each corresponds to the 3-dimensional algebra $\mathbb{Q} \times L$, which after changing base to $L$ becomes the constant group scheme.

# Classification of Separable Algebras

## Example

The $\mathbb{Q}$-algebra $\mathbb{Q}(\sqrt{2})$ example above shows that this admits no hopf algebra structure.

If so then we could put a group structure on $X = \{1, 2\}$ such that the non-trivial action by $C_2$ is a group action.

But the automorphism group of a group with two elements is trivial.

# Classification of Separable Algebras

In particular, commutative finite group schemes over $k$:

**Theorem**

*The above equivalence restricts to an equivalence between finite étale commutative group schemes over $k$ and finite continuous $\mathbb{Z}[\Gamma]$-modules.*

# Classification of Separable Algebras

**Proof.**

If Spec($A$) is commutative, then $X_A = \mathrm{Hom}_k(A, k^s)$ is then a $\mathbb{Z}$-module.

Further a $\mathbb{Z}[\Gamma]$-module, as the product $(f * g) = (f \otimes g) \circ \triangle$ is compatible with the action: for $f, g \in X_A$, $\gamma \in \Gamma$, $\gamma(f * g) = (\gamma f) * (\gamma g)$.

If $X$ is abelian, then $\triangle_X(f)(x, y) = f(xy) = f(yx)$ is cocommutative. □

# Connected-Étale Decomposition

# Connected Étale Decomposition

**Definition**

Let $A$ be a finitely-*generated* $k$-algebra.

$\pi_0(A)$ is the maximal separable $k$-subalgebra of $A$.

Is this well defined?

Let $B$ be a separable subalgebra.

$B \otimes_k k^a$ is a separable $k^a$-subalgebra of $A \otimes_k k^a$.

# Connected-Étale Decomposition

$B \otimes_k k^a$ is spanned by idempotents, hence

$$\dim_k(B) = \dim_{k^a}(B \otimes_k k^a)$$

is bounded by the number of connected components of $\mathrm{Spec}(A \otimes k^a)$, which is finite.

Let $B_1, B_2$ be separable subalgebras.

$B_1 B_2$ is a quotient of $B_1 \otimes_k B_2$, hence separable.

Then there exists a unique maximal subalgebra $\pi_0(A)$, as the dimension cannot keep increasing.

# Connected-Étale Decomposition

**Proposition**

*If $A, A'$ are finitely generated $k$-algebras, then*

$$\pi_0(A \times A') = \pi_0(A) \times \pi_0(A').$$

# Connected-Étale Decomposition

We can think of $\pi_0(G) = \mathrm{Spec}(\pi_0(A))$ as describing the connected components of $G = \mathrm{Spec}(A)$.

Clopen subsets of $\mathrm{Spec}(A)$ are in one to one correspondence with idempotents.

$\pi_0(A)$ contains all idempotents because $k[e]$ is separable.

# Connected-Étale Decomposition

**Theorem**

*Let $A$ be a finitely generated $k$-algebra, and $k \subset L$ a field extension. Then*

$$\pi_0(A) \otimes_k L = \pi_0(A \otimes_k L).$$

# Connected-Étale Decomposition

**Theorem**

*For an algebraic affine group scheme $G = \mathrm{Spec}(A)$ over $k$, the following are equivalent.*

1. *$\pi_0(G)$ is trivial (one dimensional).*
2. *$G$ is connected.*
3. *$G$ is irreducible.*
4. *$A/N(R)$ is an integral domain.*

# Connected-Étale Decomposition

**Corollary**

*Let $L$ be a field extension of $k$. Then an algebraic affine group scheme $G$ over $k$ is connected if and only if $G_L$ is connected.*

**Proof.**

$\pi_0(G)$ is invariant under base change. □

# Connected-Étale Decomposition

**Theorem**

*If $A$ and $B$ are finitely generated $k$-algebras, then*

$$\pi_0(A \otimes B) = \pi_0(A) \otimes \pi_0(B).$$

# Connected-Étale Decomposition

**Proposition**

*If $A$ is a finite dimensional hopf algebra, then $\pi_0(A)$ is a hopf subalgebra of $A$.*

**Proof.**

The comultiplication is an algebra homomorphism, hence

$$\triangle(\pi_0(A)) \subset \pi_0(A \otimes A) = \pi_0(A) \otimes \pi_0(A).$$

Similarly $S(\pi_0(A)) \subset \pi_0(A)$. $\square$

# Connected-Étale Decomposition

**Theorem**

*Let $G = \mathrm{Spec}(A)$ be an algebraic affine group over $k$.*

*Then $\pi_0(G) := \mathrm{Spec}(\pi_0(A))$ is étale, and all morphisms from $G$ to étale group schemes factor through $\pi_0(G)$ via the canonical map $G \to \pi_0(G)$.*

*The kernel of this map is the connected component of the identity. In particular we have the exact sequence*

$$1 \to G^0 \to G \to \pi_0(G) \to 1.$$

# Connected-Étale Decomposition

**Proof.**

We saw before that $\pi_0(A)$ is a hopf subalgebra of $A$.

Given any morphism $G$ to an étale group scheme $H = \mathrm{Spec}(B)$, this corresponds to a morphism of hopf algebras $H \to A$.

The image of $H$ is a separable algebra, hence maps to $\pi_0(A)$, so the morphism factors through the inclusion map. $\square$

# Connected-Étale Decomposition

**Proof.**

Let $G^0$ be the kernel of this map, represented by the algebra $A \otimes_{\pi_0(A)} k$.

Write $\pi_0(A) = k_1 \times \cdots \times k_r$ as a product of fields, corresponding to idempotents $f_1, ..., f_r \in A$, so $A = \bigoplus_{i=1}^r f_i A$.

Then the morphism $\pi_0(A) \to k$ is zero on all but one component, say $k_1$, and an isomorphism on $k_1$.

Therefore, $A \otimes_{\pi_0(A)} k \cong f_1 A$, which is local as $\pi_0(A)$ contains all idempotents of $A$, thus $G^0 = \mathrm{Spec}(f_1 A)$ is connected. $\square$

# Manin's Decomposition

# Manin's Decomposition

Now let $k$ be a perfect field.

Note: a finite dimensional $k$-algebra is separable if and only if $A$ is reduced.

An algebraic affine group scheme connected if and only if $G = G^0$.

This is equivalent to $A$ being local when $A$ is finite dimensional over $k$.

# Manin's Decomposition

**Lemma**

*If $A$ is a finitely generated $k$-algebra, then $\pi_0(A) \cong \pi_0(A/I)$ (via the canonical map) for any ideal $I$ of $A$ consisting of only nilpotent elements.*

# Manin's Decomposition

**Corollary**

*Let $A$ be a finite dimensional $k$-algebra. Let $N = N(A)$.*

*If $A/N$ is separable, then $\pi_0(A) = A/N$ (via the canonical map).*

# Manin's Decomposition

**Definition**

An affine algebraic group scheme over $k$ is a semidirect product of algebraic subgroups $N$, $Q$ ($G = N \rtimes Q$) if

- $N$ is normal in $G$,
- $(n, q) \to nq$ from $N(B) \times Q(B) \to G(B)$ is a bijection for all $B$.

# Manin's Decomposition

**Lemma**

*$G = N \rtimes Q$ if and only if there is a homomorphism $G \to Q'$ which is*

- *An isomorphism when restricted to $Q$,*
- *Has kernel $N$.*

# Manin's Decomposition

**Theorem**

*Let $G$ be a finite group scheme over the perfect field $k$.*

*Then $G$ is the semi-direct product of $G^0$ and $\pi_0(G)$.*

# Manin's Decomposition

**Proof.**

As $k$ is perfect then $A/N$ is separable (being reduced), and again because $k$ is perfect, $A/N \otimes A/N$ is reduced. Therefore,

$$A \to A \otimes A \to A/N \otimes A/N$$

factors through $A/N$, thus $A/N$ defines a closed subgroup scheme of $G$. By the previous corollary, the map $\mathrm{Spec}(A/N) \to G \to \pi_0(G)$ is an isomorphism, then use the proposition. □

# Manin's Decomposition

Over commutative finite group schemes, this is direct.

**Example**

If $k$ is not perfect, then this need not be true.

Let $k$ have characteristic 2 and imperfect, with $b \in k$ non-square.

Let $G = \mathrm{Spec}(A)$, for $A = k[X]/(X^4 - bX^2)$.

View $\mathrm{Hom}(A, B)$ as $\{x \in B \mid x^4 = bx^2\}$, a group under addition.

# Manin's Decomposition

**Example**

Now $G(k) = \{x \in k \mid x^2(x^2 - b) = 0\} = \{0\}$ has one element.

However $\pi_0(A) = k[y]$ for $y = X^2$, so $\pi_0(A) \cong k[Y]/(Y(Y - b))$.

Hence $\pi_0(G)(k) = \{0, b\}$ has two elements.

$G \ncong \pi_0(G) \times G^0$.

# Manin's Decomposition

**Corollary**

*Let $G$ be a finite commutative group scheme over the perfect field $k$. Then $G$ is a product of four factor of types:*

- *(EE) Étale with Étale dual.*
- *(EC) Étale with Connected dual.*
- *(CE) Connected with Étale dual.*
- *(CC) Connected with Connected dual.*

*Furthermore, between two finite commutative group schemes over $k$ of distinct types, there are no non-trivial homomorphisms.*

Therefore, the category of finite commutative group schemes is the product of these four subcategories.

# Manin's Decomposition

**Proof.**

$$G \cong (G^D)^D \cong ((G^D)^0 \times \pi_0(G^D))^D$$
$$\cong ((G^D)^0)^D \times \pi_0(G^D)^D.$$

Now $((G^D)^0)^D$ has a decomposition into a connected and an étale part $E \times C$.

$E^D \times C^D \cong (((G^D)^0)^D)^D \cong (G^D)^0$ so both have connected dual.

Similarly, $\pi_0(G^D)^D$ decomposes into a connected and étale part both with étale dual, lying in $\pi_0(G^D)$. □

# Manin's Decomposition

**Proof.**

Any morphism from a connected to an étale factors through $G \to \pi_0(G) = 0$, hence the only morphism is trivial.

Any morphism from an étale to connected corresponds to a morphism local to reduced.

This factors through $k$, thus is trivial.

Therefore, using duality, there are no morphisms between any of these four factors. □

# Manin's Decomposition

## Example

We have seen examples of all of these. Let $k$ have characteristic $p$, and let $q \in \mathbb{Z}$ be coprime to $p$.

- $\underline{\mathbb{Z}/q\mathbb{Z}}$ is étale, with étale dual $\mu_q$.
- $\underline{\mathbb{Z}/p\mathbb{Z}}$ is étale with connected dual $\mu_p$.
- $\mu_p$ is connected with with étale dual $\underline{\mathbb{Z}/p\mathbb{Z}}$.
- $\alpha_p$ is connected with connected dual.

# Manin's Decomposition

Note that the above examples are in finite characteristic.
This is necessary to provide an example of each.

**Theorem (Cartier's Theorem)**

*All finite group schemes over a field of characteristic* $0$ *are étale.*

This is proven using Kähler differentials.

# Manin's Decomposition

**Proposition**

*Let $k$ have characteristic $p$.*

*Let $G = \mathrm{Spec}(A)$ be a commutative finite group scheme.*

*Then $G$ is of type (EE) if and only if $G$ has order prime to $p$.*

*$G$ has order a power of $p$ otherwise.*

# Manin's Decomposition

The galois theory described before describes the first three types.

The forth requires the introduction of Dieudonné modules.

One can introduce maps $V_G$ and $F_G$.

The four possibilities correspond exactly to the four options for these being nilpotent / isomorphisms.

## Connected-Étale Decomposition Revisited

# Connected-Étale Decomposition Revisited

Now we briefly describe the connected-étale decomposition over more general rings then just fields, which requires more work.

First, let $R$ be a commutative ring. We want to consider finite flat commutative group schemes over $R$.

Because $R$ is noetherian and our algebra $A$ is finitely generated, the flatness condition here is equivalent to $A$ being locally free, which is also equivalent to $A$ begin projective.

If $R$ also local, then these are equivalent to $A$ being free.

# Connected-Étale Decomposition Revisited

First we recall some definitions.

**Definition**

A local ring $R$ is called hensellian if it satisfies any of the following equivalent conditions.

# Connected-Étale Decomposition Revisited

**Proposition**

*For a local ring $R$ with maximal ideal $m$, the following are equivalent.*

1. *For any monic polynomial $p \in R[x]$, any factorisation of $\overline{p}$ in $(R/m)[x]$ into a product of coprime monic polynomials can be lifted to a factorisation in $R[x]$.*
2. *For all $p \in R[x]$ monic, if $\overline{p}(a_0) = 0$ and $\overline{p}'(a_0) \neq 0$ for some $a \in R/m$, then there is some $a \in R$ with $p(a) = 0$ and $a = a_0$ in $R/m$.*
3. *Any finite $R$-algebra is isomorphic to a finite product of local $R$-algebras, each finite over $R$.*

# Connected-Étale Decomposition Revisited

**Proposition**

*Complete local rings are hensellian.*

**Example**

Fields and complete discrete valuation rings are hensellian.

# Connected-Étale Decomposition Revisited

**Theorem (Connected-Etale Decomposition)**

*Let $R$ be a noetherian hensellian local ring. Let $G$ be a finite flat commutative group scheme over $R$. Then there is a unique exact sequence*

$$1 \to G^0 \to G \to G^{et} \to 1$$

*where $G^0$ is connected and $G^{et}$ is etale.*

**Proof.**

See Stix Notes - Prop. 37. □

# References


- Waterhouse - Affine Group Schemes.
- Stix - Online Notes.
- Buzzard - Online Notes.
- Tate - Finite Group Schemes. $p$-Divisible Groups.

Thanks for listening.
Any questions?