Algebraic Groups

A course by Jarod Alper and Julia Pevtsova
Notes by Nico Courts

Autumn 2019/ Winter and Spring 2020

Abstract

The topic of algebraic groups is a rich subject combining both group-theoretic and algebro-geometric-theoretic techniques. Examples include the general linear group GL_n, the special orthogonal group SO_n or the symplectic group Sp_n. Algebraic groups play an important role in algebraic geometry, representation theory and number theory.

In this course, we will take the functorial approach to the study of linear algebraic groups (more generally, affine group schemes) equivalent to the study of Hopf algebras. The classical view of an algebraic group as a variety will come up as a special case of a smooth algebraic group scheme. Our algebraic approach will be independent (even complementary) to the analytic approach taken in the course on Lie groups.

1 September 25, 2019

1.1 Group objects

Let $\mathscr{C}$ be a category with a final object and finite products.

1.1.1 Definition: A **group object** G **in** $\mathscr{C}$ is an object in $\mathscr{C}$ along with multiplication, identity, and inverse morphisms satisfying the usual axioms.

One thing is that we are using that there is a final object $*$ along with our identity morphism $e : * \to G$. Here Jarrod explictly used the fact that there is a unique map to $*$.

Example 1.1
If $\mathscr{C}$ is Set, then G is a group. If $\mathscr{C} = $ Top, then G is a topological group, smooth manifolds give Lie groups, and finally (interesting to us):

1.1.2 Definition: Let S be a scheme and let $\mathscr{C}$ be the category of schemes over S. Then a group object G in $\mathscr{C}$ is a **group scheme over** S.

WHen k is a field and $\mathscr{C}$ is schemes of finite type over k, we get a group scheme of finite type over k. There is not a great consensus on what makes an **algebraic group**, but this is what we will use.

When we instead restrict to *affine schemes* we get an affine groupe scheme of finite tipe over k, or a **linear algebraic group.**

1.2 Examples

$\mathbb{G}_m = \operatorname{Spec} k[t]_t$ is one.

If we consider the map $f : \mathbb{G}_m \to \mathbb{G}_m$ which on the level of elements sends $t \mapsto t^p$, the kernel is

$$\mu_p = \ker(f) = \operatorname{Spec} k[t]/(t^p - 1)$$

and that's great, but when $\operatorname{char} k = p$, this causes the group scheme to be **unreduced**. This is (apparently) a case when you need to use schemes.

1.3 The Functorial Approach

Let $\mathscr{C}$ be a category with object X. Define the functor $h_X : \mathscr{C}^{op} \to \mathbf{Set}$ where

$$h_X(Y) = \operatorname{Hom}_{\mathscr{C}}(Y, X).$$

Then we have

1.3.1 Lemma (Yoneda)
Let $G : \mathscr{C}^{op} \to \mathbf{Set}$ be a functor. There is a natural bijection

$$G(X) \simeq \operatorname{Nat}(h_X, G).$$

1.3.2 Proposition
A group object G in $\mathscr{C}$ is the same as an aobject $X \in \mathscr{C}$ together with a choice of factorization of $h_X : \mathscr{C} \to \mathbf{Set}$ through $\mathbf{Grp}$.

1.4 Exercises

(a) Spell out all the details of the proof of the above propositon.

(b) Given a group object G, define in two ways what it means for it to act on another object. (In coordinates and functorially).

1.5   Some Interesting Facts

If we had to write down five results that we'd like to get out of this class:

1.5.1 Proposition
Every affine group scheme of finite type over a field embeds into GL_n as a closed subgroup.

1.5.2 Theorem (Chevalley's Theorem)
Let G be a finite type group scheme over a field. Then it factors as

$$1 \to H \to G \to A \to 1$$

where A is abelian and H is affine (linear algebraic).

1.5.3 Proposition
If G is an affine group scheme of finite type over k, then we have af actorization

$$1 \to U \to G \to R \to 1$$

where U is unipotent and R is reductive.

1.5.4 Proposition
$H \subseteq G$ a subgroup scheme. Then G/H is a projective scheme.

Finally we want to talk about Tanakka duality and how the representations of G define G itself.

2   September 27th, 2019

Last time we defined a group scheme (a group object in the category of schemes over a base scheme). We also mentioned that You could define it as a map $h_G : \mathbf{Sch}/S \to \mathbf{Set}$ along with a factorization through **Grp**.

We defined an **algebraic group** over k as a group scheme over $\operatorname{Spec} k$ of finite type and a **linear algebraic group** to be an *affine* group scheme over k of finite type.

2.1   Hopf Algebras

Let $G = \operatorname{Spec} A$ be a linear algebraic group over k. I have seen most of these before (see Waterhouse or my Hopf algebra notes)

2.1.1 REMARK: One think I haven't seen explicitly before: Notice that the augmentation ideal $\ker \varepsilon$, where ε is the counit, is the (maximal!) ideal corresponding in the algebro-geometric sense to the identity element in G.

2.1.2 Definition: A Hopf algebra is ...

2.1.3 Definition: Let G be an algebraic group over k. Then if h_G factors through **Ab**, G is called **commutative.**

2.2   Some Examples

2.2.1 REMARK: Note that to define a functor from schemes over k, is suffices to define it on affine schemes, thereby defining the (Zariski) local behavior of any such map. Thus we really only need to consider maps in $\mathbf{Alg}_k$.

- $\mathbb{G}_a$. Here we can define it as a functor that sends $S \mapsto \Gamma(S, \mathcal{O}_S)$. Geometrically, $\mathbb{G}_a = \mathbb{A}^1$ where the multiplication is addition, inverses send $x \mapsto -x$ and the unit is the zero map. The Hopf algebraic picture is the usual dual thing.

- $\mathbb{G}_m$ as a scheme isthe map $S \mapsto \Gamma(S, \mathcal{O}_S)^*$. In the geometric picture, $\mathbb{A}^1 \setminus \{0\}$ and the algebra structure comes from multiplciation. Hopf is pretty easy.

- GL_n is a scheme that sends

$$S \mapsto \left\{ A = (a_{ij}) : a_{ij} \in \Gamma(S, \mathcal{O}_S), \det(A) \in \Gamma(S, \mathcal{O}_S)^* \right\}$$

  the algebra is $\mathbb{A}^{n \times n} \setminus \{\det = 0\}$ with the usual multiplication. The coalgebra structure can be seen in the book.

This one requires some more explaination so I am setting it apart.

Example 2.1
Let V be a finite dimensionatl vector space over k. Then we can define the algebraic group V_a which sends
$$S \mapsto \Gamma(S, \mathcal{O}_S) \otimes_k V.$$
Geometrically we are looking at $\mathbb{A}(V) = \operatorname{Spec} \operatorname{Sym}^* V^\vee \simeq \operatorname{Spec} k[x_1, \ldots, x_n]$ where $n = \dim V$.

What about finite groups? As a scheme, we want $G = \sqcup_{g \in G} \operatorname{Spec} k$. The functor sends $S \mapsto \operatorname{Mor}_{\mathrm{Set}}(\pi_0(S), G)$, or maps from the connected components into G.

Example 2.2
Now consider the nth roots of unity: as a scheme, $\mu_n = \operatorname{Spec} k[t]/(t^n - 1) \subseteq \mathbb{G}_m$. If both $k = \bar{k}$ and $\operatorname{char} k \nmid n$, then $\mu_n \cong \mathbb{Z}/n\mathbb{Z}$.

But if (e.g.) $k = \mathbb{Q}$, then μ_3 is $\mathbb{Q}[t]/(t^3 - 1) = \operatorname{Spec} \mathbb{Q} \sqcup \operatorname{Spec} \mathbb{Q}(\xi)$ where ξ is a primitive third root of unity.

If, on the other hand, $k = \bar{\mathbb{F}}_3$ and consider μ_3, we get a single point with residye field $\bar{\mathbb{F}}_3$.

Example 2.3
If we are in the case of positive characteristic, then we get an algebraic group α_p. Here the scheme is $\operatorname{Spec} k[x]/x^p$ and functorially it is the map $S \mapsto \{F \in \Gamma(S, \mathcal{O}_S) | f^p = 0\}$.

2.3 Matrix Groups

We already defined GL_n, but we can also define

$$\operatorname{SL}_n : S \mapsto \{A = (a_{ij}) | \det A = 1\}$$

with scheme $\operatorname{Spec} k[x_{ij}]/(\det - 1)$.

We also have the (upper) triangular matrices T_n and unitary group U_n and diagonal group D_n

2.3.1 Definition: Let G be a linear algebraic group. Then

- G is a **vector group** if $G \cong V_a$ for some finite dimensional V.

- G is a **split torus** if $G \cong \mathbb{G}_m^n$.

- G is a **torus** if there is a field extention $k \to k'$ such that

$$G \times_{\operatorname{Spec} k} \operatorname{Spec} k' \cong \mathbb{G}_{m,k'}^n$$

3 September 30th, 2019

Another example to consider:

Example 3.1
Let $G = \mathrm{PGL}_n$, the projective linear group. Recall we want to define this as GL_n / k^* (from group theory). To do this for algebraic groups, we define

$$\mathrm{PGL}_n = \mathrm{Proj}\, k[x_{ij}]_{det} := \mathrm{Spec}(k[x_{ij}]_{det})_0$$

The geometric picture is difficult since we haven't yet defined quotients, but as a functor we say PGL_n is $\mathrm{Aut}(\mathbb{P}^n)$, the functor that sends $S \mapsto \mathrm{Aut}(\mathbb{P}^n_S)$ where $\mathbb{P}^n_S = \mathbb{P}^n_k \times_{\mathrm{Spec}\, k} S$.

3.1 Non-affine group schemes

Example 3.2
Let $\lambda \neq 0, 1$ be an element in k. Then we can define the elliptic curve

$$E_\lambda = V(y^2 z - x(x-z)(x-\lambda z)) \subset \mathbb{P}^2$$

Which gives us a double cover over $(0, 1)$ and (λ, ∞) with singleton fiber (ramified) over $0, 1$, and λ.
   Then for any $\lambda \neq 0, 1$, E_λ is a **projective** group scheme.

3.1.1 REMARK: If you look at the $\mathbb{C}$-points, you get $E_\lambda(\mathbb{C}) = \Lambda_\lambda$, giving you a torus. Recall (from e.g. complex analysis) that the moduli here is $\mathrm{SL}_2(\mathbb{Z})$ of all elliptic curves.

3.2 Abelian Varieties

3.2.1 Definition: An **abelian variety over** k is asmooth, geometrically connected ($A \times_{\mathrm{Spec}\, k} \mathrm{Spec}\, \bar{k}$ is connected), proper group scheme A over k.

Example 3.3
Over $\mathbb{C}$, $\mathbb{C}^g / \Lambda$ where $\Lambda \cong \mathbb{Z}^{2g} \subseteq \mathbb{C}^g$ gives us a genus g example.

3.2.2 Theorem
Any abelian variety over k is commutative and projective.

3.2.3 Theorem (Chevalley)

If G is any group scheme, then the sequence

$$1 \to H \to G \to A \to 1$$

is exact, where H is a linear algebraic group (affine!) and A is an abelian variety.

Example 3.4

Let $X \to \operatorname{Spec} k$ be a geometrically integral projective scheme (proper may suffice). The idea here is that over $\mathbb{C}$ the rings over every open set are integral domains.

Now consider the **Picard functor** $\operatorname{Pic}_X : \operatorname{Pic} : \mathbf{Sch}/\mathbf{k} \to \mathbf{Grp}$ sending

$$S \mapsto \operatorname{Pic}(X_S = X \times_k S)/p^k \operatorname{Pic}(S)$$

3.2.4 Theorem

Pic_X is represented by a scheme locally of finite type, thus Pic_X^0, the connected component of the identity in $[\mathcal{O}_X] \in \operatorname{Pic}_X$ is an abelian variety.

3.3   Relative Group Schemes

Example 3.5

Consider $\mathbb{G}_{m,\mathbb{Z}} = \operatorname{Spec} \mathbb{Z}[t]_t$. Then $G_{m,S} = \mathbb{G}_{m,\mathbb{Z}} \times_{\operatorname{Spec} \mathbb{Z}} S$. In the case that $S = \operatorname{Spec} R$, $\mathbb{G}_{m,S} = \operatorname{Spec} R[t]_t$.

Example 3.6

Let $\mathbb{A}^1 = \operatorname{Spec} k[x]$ and define $G = \operatorname{Spec} k[x,y]_{xy+1} \subseteq \mathbb{A}^2$. Notice this is the plane minus a hyperbola.

Define $\cdot : G \times_{\mathbb{A}^1} G \to G$ to be given by

$$(x,y) \cdot (x,y') = (x, xyy' + y + y')$$

Then the thing here is the fiber (think vertical line in the plane!) over 0 is $\mathbb{G}_a$ and is isomorphic to $\mathbb{G}_m$ otherwise.

Example 3.7
Let $\mathcal{E}_\lambda = V(y^2 z - x(x-z)(x-\lambda z))$ over $\operatorname{Spec} k[\lambda]$. Then when $\lambda = 0$, we get the nodal cubic given by $y^2 z - x^2(x-z)$ (node at the origin).

Now if you look at the connected component around 0 of $\operatorname{Aut}(\mathcal{E}_\lambda)/\mathbb{A}_\lambda$, you actually find (when $\lambda = 0$) that $\mathbb{G}_m \cong \operatorname{Aut}(\mathcal{E}_0)^0$.

3.4 Some definitions

3.4.1 Definition: A **homomorphism** $\phi : G \to G$ of group schemes over S is a map $\phi : H \to G$ of schemes such that

$$\begin{array}{ccc} H \times_S H & \xrightarrow{m_H} & H \\ \downarrow{\phi \times \phi} & & \downarrow{\phi} \\ G \times_S G & \xrightarrow{m_G} & G \end{array}$$

Problem 3.1
Show that this automoatically imples that the identity and inversion maps are respected as well (automatically).

3.4.2 Definition: A **subgroup of** $G \to S$ is a subscheme $H \subseteq G$ such that $H(T) \leq G(T)$ for all T over S.

Problem 3.2
Show that $\ker(\phi) \subseteq H$ *is a subgroup.*

3.4.3 REMARK: This gives you a nice way to construct new group schemes. For example, the following are exact:

$$1 \to \operatorname{SL}_n \to GL_n \xrightarrow{\det} \mathbb{G}_m \to 1$$

and

$$1 \to \mathbb{G}_m \to \operatorname{GL}_n \to \operatorname{PGL}_n \to 1$$

3.4.4 Proposition

Let $G \to S$ be a group scheme. Then $G \to S$ is separated if andy only if $e : S \to G$ is a closed immersion.

Proof
The idea here is that $S \to G$ is a closed immersion. Then we consider the map $m \circ (\mathrm{id}, S) :$ $G \times_S G \to G$ and consider this along with the diagonal map $\Delta : G \to G \times_S G$ and this is a pullback square!   ♠

3.4.5 Corollary

Any group scheme over k is separated.

The idea is going to be that if X is any scheme over k, then any point $X \in X(k)$ is closed.

4   October 2, 2019

Notice that a **relative group scheme** (referred to in last lecture) refers to a groups scheme over an arbitrary base scheme S.

4.1   Properties of schemes

Today we are going to be talking about reducedness, connectedness, irreduciblility, regularity, and smoothness.

Recall that a scheme X is **reduced** if and only if $\forall x \in X$, $\mathcal{O}_{X,x}$ is reduced. An example of a non-reduced scheme is $\operatorname{Spec} k[x]/(x^2)$.

4.1.1 Definition: We say a scheme X over k is **geometrically reduced** if for all field extensions k'/k,

$$X_{k'} = X \times_{\operatorname{Spec} k} \operatorname{Spec} k'$$

is reduced.

4.1.2 Remark: It is equivalent that $X_{\bar{k}}$ is reduced if and only if every k'/k is purely inseperable (I think).

4.1.3 Remark: If k is perfect, then X is reduced if and only if X is geometrically reduced.

4.1.4 Definition: A local ring $(A, \mathfrak{m})$ is **regular** if $\dim_{\mathrm{Krull}} A = \dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$

4.1.5 Definition: A scheme X is regular if for all $x \in X$, $\mathscr{O}_{X,x}$ is regular.

4.1.6 REMARK: If $X \to \operatorname{Spec} k$ and $x \in X(k)$, the tangent space at x is

$$T_{X,x} = (\mathfrak{m}/\mathfrak{m}^2)^\vee = \{f : \operatorname{Spec} k[\varepsilon]/\varepsilon^2 \to X \mid 0 \mapsto x\}$$

4.1.7 REMARK: Notice that if $X \to \operatorname{Spec} k$ is regular and k'/k is a field extension, then $X_{k'}$ is not necessarily regular.

4.1.8 Definition: A Scheme $X \to \operatorname{Spec} k$ of finite type is **smooth** if $X_{\bar{k}}$ is regular.

4.2 Facts about algebraic groups

Then we can return to the proposition we want to prove:

4.2.1 Proposition
Let $G \to \operatorname{Spec} k$ be an algebraic group. Then G is geometrically reduced if and only if G is smooth over $\operatorname{Spec} k$.

PROOF
Smoothness over k implies reducedness. Now since we are only interested in the algebraic closure of k, we can say $k = \bar{k}$. Because G is reduced, there exists a nonempty open $U \subseteq G$ that is smooth. Then since $G(k) \subseteq |G|$ is dense in G (as a topological space) and Then $G = \cup_{g \in G(k)} m_g(U)$ for our smooth U, and this gives us a smooth cover of G.   ♠

We will see next itme that all linear algebraic groups over k where $\operatorname{char} k = 0$ are all geometrically reduced (and thus smooth).

4.3 Connectedness

Let G be an algebraic group over k. Then we have our maps $e : \operatorname{Spec} k \to G$, so consider it as $e \in G(k)$. Let $G^0 \subseteq G$ be the connected component of e. It is both open and closed.

4.3.1 REMARK: If $X \to \operatorname{Spec} k$ is of finite type and $x \in X(k)$, then X being connected implies that X is geometrically connected.

This establishes that G^0 is actually geometrically connected! We actually will see

4.3.2 Proposition
$G^0 \subseteq G$ is an (open and closed) algebraic subgroup.

The idea here is that $G^0 \times G^0$ is connected, so the image of the multipication map on this set lands in a connected component (since it is connected). Since $e \in G^0$, and $m(e, e) = e \in G^0$, this shows that the multiplication map restricts to a well-defined map $G^0 \times G^0 \to G^0$. A similar argument goes through for the inverset map, etc.

The upshot here is that if G is an algebraic group, then there exists a factorization

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

where $\pi_0(G)$ is given the structure of a discrete group.

4.3.3 REMARK: Now we also have that $(G^0)_{k'} = (G_{k'})^0$ for all k'/k. The idea is to get a map of of one into the other and then use clopenness and connectedness to show they are equal.

4.3.4 Proposition
A connected algebraic group over k is irreducible.

PROOF
We can assume $k = \bar{k}$. Suppose $G = X \cup Y$, where both are closed, X is irreducible, and $X \cap Y \neq \varnothing$. Thus there exists an element $g \in X \setminus Y$. That is, g lies in a single irreducible component.

But then using the multiplication by h map on G, we get to every other point in G, so every point is in a single irreducible component. But the intersection was nontrivial! Or something.   ♠

4.3.5 Proposition
If G_{red} is geometrically connected, then $G_{\mathrm{red}} \subseteq G$ is a subgroup. In particular, if k is perfect, then G_{red} is a subgroup of G.

4.3.6 REMARK: X is geometrically reduced implies that $X \times X$ is geometrically reduced.

5   October 4, 2019

Some review. Let G be an algebraic group and denote $e : \operatorname{Spec} k \to G$ be the identity. We saw a lot of propositions last time.

Now let k be a nonperfect field and take $t \in k \setminus k^p$. Then define

$$G \overset{\mathrm{def}}{=} V(x^{p^2} - t x^p) \subseteq \mathbb{G}_a$$

which Milne claims is not reduced. We can see why it's not geometrically reduced, but we're missing the details here.

5.1   Another special case

5.1.1 Theorem
When $k = \bar{k}$, G is smooth if and only if

$$\dim T_e G_{\mathrm{red.}} = \dim T_e G.$$

5.1.2 REMARK: When G is smooth, it is reduced, so the equality is clear. For the other direction, we get that k is pefect, so $G_{\text{red.}}$ which is geoemetrically reduced if and only if G is smooth. But
$$\dim G \leq \dim T_e G = \dim T_e G_{\text{red.}} = \dim G_{\text{red.}} = \dim G$$

5.1.3 Theorem
If G is a linear algebraic group over k and char $k = 0$, G is smooth,

PROOF
We can assume $k = \bar{k}$. Then set $G = \operatorname{Spec} A$ where A is a Hopf algebra. THen we get Hopf algebra maps m^* and e^*. Notice that the augmentation ideal $\mathfrak{m} = \ker(e^*)$ is a maximal ideal.
   Then we want to prove

  (a) $A \cong \mathfrak{m} \oplus k$ as a k-vector space (obvious).

  (b) $\forall a \in \mathfrak{m}$, $m^*(a) - a \otimes 1 - 1 \otimes a \in \mathfrak{m} \otimes \mathfrak{m}$.

To see the second, notice that $m^*(a) - a \otimes 1 - 1 \otimes a$ is in the kernel of
$$e^* \otimes \operatorname{id} : A \otimes A \to k \otimes A.$$

This is clear from the commutative diagram

$$
\begin{array}{ccc}
k \otimes A & \xleftarrow{\;\;e^* \otimes \operatorname{id}\;\;} & A \otimes A \\
 & \nwarrow{\scriptstyle \sim} & \uparrow{\scriptstyle m^*} \\
 & & A
\end{array}
$$

Then we conclude $f \in \ker(e^* \otimes \operatorname{id}) \cap \ker(\operatorname{id} \otimes e^*) = A \otimes \mathfrak{m} \cap \mathfrak{m} \otimes A$ by a symmetric argument. Finally we notice that $A \otimes \mathfrak{m} \cap \mathfrak{m} \otimes A = \mathfrak{m} \otimes \mathfrak{m}$, and so f lies in this ideal.
   Now we want to show that $\dim T_e G = \dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim_k \mathfrak{m}/(\sqrt{0} + \mathfrak{m}^2) = \dim T_e G_{\text{red.}}$. It suffices to show that for all $a \in \sqrt{0}$, $a \in \mathfrak{m}^2$. Suppose the opposite–so let $a \in \sqrt{0} \setminus \mathfrak{m}^2$. Consider the diagram

$$
\begin{array}{ccc}
A & \longrightarrow & A_{\mathfrak{m}} \\
\downarrow & & \downarrow \\
A/\mathfrak{m}^2 & \xrightarrow{\;\sim\;} & A_{\mathfrak{m}}/(\mathfrak{m} A_{\mathfrak{m}})^2
\end{array}
$$

Now the image of a in $A_{\mathfrak{m}}$ is nonzero, so there exists $n > 0$ such that $a^n \in A_{\mathfrak{m}}$ but $a^{n-1} \neq 0$ in $A_{\mathfrak{m}}$. Thus there exists $f \notin \mathfrak{m}$ such that $a^n f = 0 \in A$. Subsititute af for a, and thus there is an $a \in \sqrt{0}$ such that $a^n = 0$ in A but $a^{n-1} \neq 0$ in $A_{\mathfrak{m}}$.
   Then by fact 2,
$$m^*(a) = 1 \otimes a + a \otimes 1 + r, \quad r \in \mathfrak{m} \otimes \mathfrak{m}$$

and since m^* is a ring homomorphism,

$$0 = m^*(a^n) = (m^*(a))^n = (a \otimes 1 + (1 \otimes a + r))^n = a^n \otimes 1 + n(a^{n-1} \otimes a + (a^{n-1} \otimes 1)r) + X$$

where $X \in A \otimes \mathfrak{m}^2$. But since $a^n = 0$, we get

$$n(a^{n-1} \otimes a + (a^{n-1} \otimes 1)r) \in A \otimes \mathfrak{m}^2$$

Now since $(a^{n-1} \otimes 1)r \in (a^{n-1})\mathfrak{m} \otimes A$, so

$$n(a^{n-1} \otimes a) \in (a^{n-1})\mathfrak{m} \otimes A + A \otimes \mathfrak{m}^2$$

and since $\operatorname{char} k = 0$, we get that n is a unit, so

$$a^{n-1} \otimes a \in (a^{n-1})\mathfrak{m} \otimes A + A \otimes \mathfrak{m}^2$$

Now since this lives in $A \otimes A$, consider the image of the quotient map $A \otimes A \to A \otimes A/\mathfrak{m}^2$. Then

$$a^{n-1} \otimes \bar{a} \in (a^{n-1})\mathfrak{m} \otimes A/\mathfrak{m}^2 \subseteq A \otimes A/\mathfrak{m}^2$$

And note that $a^{n-1} \notin a^{n-1}\mathfrak{m}$ because otherwise $a^{n-1} = a^{n-1}q$ for $q \in \mathfrak{m}$. Then $a^{n-1}(1-q) = 0 \in A_\mathfrak{m}$, which implies that $a^{n-1} = 0 \in A_\mathfrak{m}$ (since $1-q$ is a unit here).

Then somehow we get that $\bar{a} = 0 \in A/\mathfrak{m}^2$, so $a \in \mathfrak{m}^2$. ♠