1.

We will explain how algebraic geometry over finite fields gives rise to interesting finite groups. In order, we will borrow from:

- Milne, *Algebraic Groups* (2017)
- Geck, *An Introduction to Algebraic Geometry and Algebraic Groups* (2003)
- Carter, "On the Representation Theory of the Finite Groups of Lie Type in Characteristic 0", in *Algebra IX* (1996)

I have also drawn ideas from Brion's 2019 SCGP lectures.

1.1.

Start with algebraic varieties over an arbitrary algebraically closed field k. In practice, they don't form a nice category, so instead, we implicitly work in Sch_k, the category of all schemes of finite type over k.

An *algebraic group* over k ought to be a group object in Sch_k: This entails maps $m : G \times G \to G$ and $e : \operatorname{Spec} k \to G$ and $i : G \to G$ satisfying certain axioms. Some authors add more adjectives, especially smoothness. Examples of affine algebraic groups:

$$\mathbf{G}_a, \quad \mathbf{G}_m, \quad \mu_n, \quad \mathrm{GL}_n, \quad \mathrm{Sp}_{2n}, \quad \mathrm{Aff}_n = \mathrm{GL}_n \ltimes \mathbf{G}_a^n.$$

Examples of non-affine algebraic groups: Abelian varieties, like elliptic curves. They are precisely the connected, smooth, proper algebraic groups. Barsotti–Chevalley says that if k is *perfect*, then any connected, smooth algebraic group over k is an extension of an abelian variety by an affine algebraic group, in the sense that we will define below.

Remark 1.1. By Milne Prop. 1.28 and Prop. 1.37, the following conditions on an algebraic group G over k are equivalent:

(1) G is smooth.
(2) G is reduced.
(3) Its k-dimension equals that of its tangent space at the identity, *i.e.*, its Lie algebra.

For example: If $k = \bar{\mathbf{F}}_p$ for some prime p, then $\mu_n = \operatorname{Spec} k[t]/(t^n - 1)$, the algebraic group of nth roots of unity, is smooth if and only if $p \nmid n$. When is it connected?

1.2.

An affine algebraic group G is controlled by its coordinate ring $k[G]$. The multiplication on G corresponds to a coproduct $\Delta : k[G] \to k[G] \otimes k[G]$ satisfying certain axioms. Similarly, if V is a vector space over k, then a

representation of G on V given by action morphism $G \times V \to V$ in Sch_k corresponds to a *coaction* morphism $k[V] \to k[G] \otimes k[V]$ satisfying certain axioms. The linearity of the G-action on V corresponds to the coaction restricting to a morphism $V^\vee \to k[G] \otimes V^\vee$. In this case, $V^\vee$ is an example of what we call a *$k[G]$-comodule*.

One can check that any $k[G]$-comodule M is a filtered union of its finite-dimensional sub-comodules. The key idea is that the coaction map must send any vector to a finite sum of tensors. In particular, taking $M = k[G]$, we can find a finite-dimensional sub-comodule $M' \subseteq M$ that contains a generating set for $k[G]$ as a k-algebra. If we now write $M' = V^\vee$, then V turns out to be a finite-dimensional representation of G such that the induced map $k[\mathrm{GL}(V)] \to k[G]$ is surjective. See Milne Chapter 4 for the details of the proof. Altogether:

Theorem 1.2. *Any affine algebraic group is* linear*: a closed subgroup of* $\mathrm{GL}(V)$ *for some* V.

Example 1.3. In the coordinates

$$\mathrm{GL}_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \det \neq 0 \right\},$$

we have $k[\mathrm{GL}_2] = k[a, b, c, d][\det^{-1}]$. The formulas that describe the coaction of $k[\mathrm{GL}_2]$ on itself, *i.e.*, the comultiplication Δ, correspond to the formulas that describe matrix multiplication: *e.g.*, $a \mapsto a \otimes a + b \otimes c$.

Let V be the vector space of all 2×2 matrices. Then $V^\vee = k\langle a, b, c, d \rangle$ is a sub-comodule of $k[\mathrm{GL}_2]$ viewed as a comodule over itself. The fact that it contains a generating set for $k[\mathrm{GL}_2]$ as an algebra reflects the fact that the representation of GL_2 on V by multiplication is faithful.

1.3.

The preceding discussion suggests that we should study specific algebraic groups that embed into GL_n. To this end, we transfer various definitions from group theory to the world of algebraic groups.

A *homomorphism* of algebraic groups $\varphi : H \to G$ is a morphism in Sch_k that takes the multiplication on H to that on G. The *kernel* of φ is its fiber over the identity of G. When the kernel is trivial, we say that H is an *algebraic subgroup* of G. In this case, we claim that φ is a closed embedding. Indeed, one can check that the Zariski closure of $H(k)$ in $G(k)$ is a group inside which $H(k)$ has finite index, which forces $H(k)$ to coincide with the closure.

We say that an algebraic subgroup $N \subseteq G$ is *normal* if and only if it is the kernel of some homomorphism. In this case, the fppf sheaf quotient G/N is represented by an algebraic group, called the *quotient* of G by N. The map

$G \to G/N$ is faithfully flat, or more simply, flat and surjective. Note that if G/N is smooth, then flatness follows from the generic flatness theorem via a homogeneity argument.

Having defined subgroups and quotients, we can now make sense of *extensions* of algebraic groups, *semidirect products*, *etc.*, and analogues of the isomorphism theorems from group theory. See Milne Chapter 5 for details.

1.4.

In the first lecture, we mentioned the algebraic subgroup of upper-triangular matrices $B \subseteq \mathrm{GL}_n$. Note that the derived subgroup of $B(k)$ is precisely $U(k)$, where $U \subseteq B$ is the algebraic subgroup of *unipotent* upper-triangular matrices. Moreover, $B(k) \simeq T(k) \ltimes U(k)$, where $T \subseteq B$ is the algebraic subgroup of diagonal matrices.

In any algebraic group H, we define the *derived subgroup* $[H, H] \subseteq H$ to be the intersection of all normal subgroups of H with abelian quotient. We can check that $U = [B, B]$, and that $B \simeq T \ltimes U$. With more work, we can check that B is *solvable* in the sense that its derived series has finite length.

A *torus* is an algebraic group isomorphic to a power of $\mathbf{G}_m$. A *Borel subgroup* of an algebraic group is a maximal connected, smooth, solvable algebraic subgroup. In our running example, T is a maximal torus, and B a Borel subgroup, of GL_n. Note that T is not the only maximal torus inside B!

Theorem 1.4 (Cartan–Lie–Kolchin)**.** *In any* connected *algebraic group G, any maximal torus T is contained in some Borel subgroup B, and all such pairs $T \subseteq B$ are conjugate under $G(k)$.*

By this theorem, an affine algebraic group is solvable, *resp.* unipotent, if and only if it has a faithful representation whose image is contained in the algebraic subgroup of upper-triangular, *resp.* unipotent upper-triangular, matrices. Thus unipotent implies solvable.

In any affine algebraic group G, the maximal connected, smooth normal subgroup that is solvable, *resp.* unipotent, is called the *radical*, *resp. unipotent radical* of G. We say that G is *semisimple*, *resp. reductive*, if and only if it has trivial radical, *resp.* unipotent radical. Thus semisimple implies reductive. The groups SL_n are semisimple; the groups GL_n are reductive but not semisimple.

Remark 1.5. The definition of a semisimple algebraic group matches up in a precise sense with that of a semisimple Lie algebra.[1] Recall that *complex* semisimple Lie algebras are classified by Dynkin diagrams.

However, the definition of a reductive algebraic group does not match up in this manner with that of a reductive Lie algebra. A better viewpoint is: The

[1] See https://math.stackexchange.com/q/1982569.

reductive algebraic groups over $\mathbf{C}$ are precisely the complexifications of the compact real Lie groups.[2] By work of Chevalley, the classification of reductive algebraic groups is the same over any (algebraically closed) field.

1.5.

Now we focus on affine algebraic groups over the algebraic closure of a finite field: say, G over $k = \bar{\mathbf{F}}_q$. We want to construct finite groups that look like $\mathrm{GL}_n(\mathbf{F}_q)$, but starting from geometry over k rather than $\mathbf{F}_q$ itself, because to the eye of an algebraic geometer, k is the simpler field.

Note that a scheme over k cannot have nontrivial $\mathbf{F}_q$-points. What we are actually doing is first choosing a scheme G_1 over $\mathbf{F}_q$ such that $G_1 \otimes k = \mathrm{GL}_n$, then taking the set of $\mathbf{F}_q$-points of G_1. One choice gives $\mathrm{GL}_n(\mathbf{F}_q)$. As it turns out, another choice gives a different group called $\mathrm{U}_n(\mathbf{F}_q)$.

If X, *resp.* X_1, is a scheme over k, *resp.* $\mathbf{F}_q$, and α is an isomorphism $X \xrightarrow{\sim} X_1 \otimes k$, then we say that (X_1, α) is a *descent of X to $\mathbf{F}_q$*, or an *$\mathbf{F}_q$-rational structure* on X. If X is an algebraic group and its multiplication, identity, and inversion maps descend to X_1 along α, then we say that (X_1, α) is an *$\mathbf{F}_q$-form* of X. Abusing notation, we will omit mention of α where convenient.

Remark 1.6. Most texts define algebraic groups in the setting of arbitrary fields. For clarity, I will try to speak only of algebraic groups over fields that are algebraically closed, and of forms of these groups over subfields.

Let $\sigma_X : X \to X$ and $\sigma_{X_1} : X_1 \to X_1$ be the morphisms that fix the underlying topological spaces and are given by $f \mapsto f^q$ on sections of the structure sheaves. By Fermat's Little Theorem, these are morphisms over $\mathbf{F}_q$. Let $F : X \to X$ be the morphism over k given by the transport of $\sigma_{X_1} \otimes \mathrm{id}_k$ along α. We refer to F as the *(relative) Frobenius map* on X induced by (X_1, α). By construction,

$$\sigma_X = (\mathrm{id}_{X_1} \otimes \sigma_{\operatorname{Spec} k}) \circ F = F \circ (\mathrm{id}_{X_1} \otimes \sigma_{\operatorname{Spec} k}).$$

We claim that we can recover X_1 up to isomorphism from X and F. Indeed, if $X = \operatorname{Spec} A$, then we can take $X_1 = \operatorname{Spec} A_1$, where $A_1 = \{f \in A \mid F^*(f) = f^q\}$; the general case follows from the affine one by gluing. Ultimately, $\mathbf{F}_q$-rational structures on X are classified by their Frobenius maps.

For an approach that starts from an abstract definition of relative Frobenius maps, then recovers $\mathbf{F}_q$-rational structures, see Section 4.1 of Geck's book.

Example 1.7. Write $\mathbf{G}_m = \operatorname{Spec} k[t^{\pm 1}]$. There is a Frobenius map $F : \mathbf{G}_m \to \mathbf{G}_m$ given by $F^*(t) = t^q$, corresponding to the $\mathbf{F}_q$-form arising from $\mathbf{F}_q[t^{\pm 1}]$.

Now suppose that $\mathbf{F}_q$ does not contain $i := \sqrt{-1}$. In particular, $2 \nmid q$. Here the algebra $A_1 = \mathbf{F}_q[a, b]/(a^2 + b^2 - 1)$ is not isomorphic to $\mathbf{F}_q[t^{\pm 1}]$, yet

[2] See https://mathoverflow.net/q/299143.

we do have an isomorphism $A_1 \otimes k \simeq k[t^{\pm 1}]$ given by $a = \frac{1}{2}(t + t^{-1})$ and $b = \frac{1}{2i}(t - t^{-1})$. What is the Frobenius map on $\mathbf{G}_m$ that corresponds to A_1? We claim that it is F defined by $F^*(t) = t^{-q}$. Indeed, $F^*(a) = a^q$, and since $i^q = -i$ by hypothesis, $F^*(b) = b^q$.

In fact, the group structure on $\mathbf{G}_m$ descends to Spec A_1. The resulting $\mathbf{F}_q$-form of $\mathbf{G}_m$ is the *circle group*

$$\mathrm{U}(1) := \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| \, a^2 + b^2 = 1 \right\}.$$

It generalizes to an $\mathbf{F}_q$-form of GL_n called the *$n \times n$ unitary group* and denoted $\mathrm{U}(n)$. Compare to Geck, §1.5.12 and §4.1.10(c).

1.6.

Suppose that $F : G \to G$ is a Frobenius map corresponding to an $\mathbf{F}_q$-form G_1. It acts on $\bar{\mathbf{F}}_q[G]$, hence on $\bar{\mathbf{F}}_q$-points of G viewed as $\bar{\mathbf{F}}_q$-algebra morphisms $\bar{\mathbf{F}}_q[G] \to \bar{\mathbf{F}}_q$. We have bijections of finite sets

$$G^F(\bar{\mathbf{F}}_q) \simeq G(\bar{\mathbf{F}}_q)^F \simeq G_1(\mathbf{F}_q).$$

In Deligne–Lusztig theory, people write G^F to denote $G^F(\bar{\mathbf{F}}_q)$ as well as the scheme. Similar notation applies to any scheme X with a Frobenius map $F : X \to X$ and G-action that are compatible, meaning $F(g \cdot x) = F(g) \cdot F(x)$.

By running over all possible choices of q, G, and F, we get a large supply of finite groups G^F. Which ones are the most interesting, or rather, the most fundamental? In "pure" group theory, the most fundamental finite groups are the *simple* ones: those that have no nontrivial proper normal subgroup. Remarkably, many of the finite simple groups are closely related to groups of the form G^F, though not necessarily of that form themselves.

Theorem 1.8 (Classification)**.** *Every finite simple group is one (or more) of the following:*

(1) A cyclic group of prime order.
(2) An alternating group A_n with $n \geq 5$.
(3) A finite simple "group of Lie type".
(4) One of 26 (or 27) sporadic groups.

What is a finite group of Lie type? Unfortunately, there is no widely accepted definition,[3] but morally, these are the groups that are most closely related to the groups G^F. Class (1) could have been folded into class (3), but wasn't (for good reason), and the controversy over the number of sporadic groups is a similar issue. The finite simple groups of Lie type themselves fall into subclasses:

[3] See https://mathoverflow.net/q/136880.

(1) Chevalley groups

$$A_n(q), B_n(q) \text{ for } n \geq 2, \quad C_n(q) \text{ for } n \geq 3, \quad D_n(q) \text{ for } n \geq 4,$$
$$E_n(q) \text{ for } n = 6, 7, 8, \quad F_4(q), \quad G_2(q).$$

(2) Steinberg groups

$${}^2A_n(q^2) \text{ for } n \geq 2, \quad {}^2D_n(q^2) \text{ for } n \geq 4, \quad {}^2E_6(q^2), \quad {}^3D_4(q^3).$$

(3) Suzuki groups ${}^2B_2(2^{2m+1})$ and Ree groups ${}^2G_2(3^{2m+1})$.
(4) The Tits group ${}^2F_4(2^{2m+1})$, sometimes counted as a sporadic group.

Above:

The Chevalley and Steinberg groups are all central quotients either of certain groups G^F or kernels of such groups along determinant or spinor norm maps. The Chevalley groups come from split $\mathbf{F}_q$-forms, while the Steinberg groups come from nonsplit forms—terms we will define later.

The Suzuki and Ree groups all take the form G^F, where F is a Frobenius map in a more general sense than we introduced earlier: Again, see Geck Chapter 4. They can also be constructed as fixed-point subgroups of groups G^F under exotic automorphisms, where F is a Frobenius map in our earlier sense, arising from some q and some $\mathbf{F}_q$-form of G. The Tits group also fits into this latter construction.

The notation for the finite simple groups of Lie type hints that the associated pairs (G, F) are very special. The group G is always *almost-simple*: This means G is semisimple, noncommutative, and has no connected, smooth normal subgroups other than itself and $\{1\}$. In particular, via the classification of semisimple Lie algebras, it comes from a connected Dynkin diagram. The map F then comes from an automorphism of this Dynkin diagram.

Remark 1.9. Some authors refer to *almost-simple* algebraic groups as *simple* algebraic groups. However, this notion is not quite analogous to that of a simple (abstract) group.