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)

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* ought to be a group object in Sch_k. Some authors add more adjectives. One quickly realizes that the affine algebraic groups behave differently from, say, the projective ones. Examples of affine algebraic groups:

$$\mathbf{G}_a, \mathbf{G}_m, \mathrm{GL}_n, \mathrm{SL}_n, \mathrm{Sp}_{2n}, \mathrm{Aff}_n, \mathrm{Heis}.$$

Examples of non-affine algebraic groups: Abelian varieties, which are projective, and group extensions of these. 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.

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

Example 1.2. 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 over k. 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.

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 group called $\mathrm{U}_n(\mathbf{F}_q)$, different in general.

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 that is convenient.

Remark 1.3. Many 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 1.4. 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 $F^*(t) = t^q$. It corresponds to the *split* $\mathbf{F}_q$-form of $\mathbf{G}_m$ 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 we do have an isomorphism $A_1 \otimes k \simeq k[t^{\pm 1}]$ given by

$$a = \tfrac{1}{2}(t + t^{-1}), \quad b = \tfrac{1}{2i}(t - t^{-1}).$$

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 $\operatorname{Spec} A_1$. The resulting $\mathbf{F}_q$-form of $\mathbf{G}_m$ may be viewed as 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).

1.4.

Suppose that $F : G \to G$ is a Frobenius map corresponding to an $\mathbf{F}_q$-form G_1. In Deligne–Lusztig theory, people like to write G^F in place of $G_1(\mathbf{F}_q)$. The latter is a finite set; the former can be viewed as either a set or a scheme.

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. Here is a rough statement of the classification of finite simple groups:

Theorem 1.5. *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,[1] 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:

(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 is meant to indicate that the associated pairs (G, F) are very special: The algebraic groups G all arise from irreducible Dynkin diagrams via a standard construction, and the maps F all arise from automorphisms of these Dynkin diagrams. In particular, *Dynkin diagrams classify algebraic groups G that satisfy some property closely related to the simplicity of the finite groups G^F.*

1.5.

Those of you with background in Lie theory know where this is going.

First, an algebraic group G (over an arbitrary algebraically closed field) is *solvable*, *resp.* *unipotent*, if and only if there exist an integer n and a faithful

[1] See `https://mathoverflow.net/q/136880`.

representation $G \to \mathrm{GL}_n$ whose image is contained in the closed subgroup of upper-triangular, *resp.* unipotent upper-triangular, $n \times n$ matrices. Thus unipotent implies solvable. The maximal connected, smooth normal subgroup of G 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. By work of Killing, É. Cartan, and Chevalley, to which we return later, semisimple algebraic groups can be classified using Dynkin diagrams. It turns out that any reductive algebraic group is a central extension of a semisimple one. The groups SL_n are semisimple; the groups GL_n are reductive but not semisimple.

We say that G is *almost-simple* if and only if it is semisimple, noncommutative, and has no connected, smooth normal subgroups other than itself and the identity subgroup. Almost-simplicity of G ensures that G^F is fairly close to being a finite simple group.

Remark 1.6. 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.

Remark 1.7. The definition of a semisimple algebraic group does match up in a precise sense with that of a semisimple Lie algebra. The details are somewhat involved.[2] 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 reductive algebraic groups over $\mathbf{C}$ are precisely the complexifications of the compact real Lie groups.[3] By work of Chevalley, the classification of reductive algebraic groups is the same over any (algebraically closed) field.

[2]See `https://math.stackexchange.com/q/1982569`.
[3]See `https://mathoverflow.net/q/299143`.