A (linear) algebraic group is, roughly, a group of matrices (under matrix multiplication) that consists of all matrices whose entries obey some polynomial equations.

We'll work with matrices having entries in any field $K$.

**Def:** Let $M(n,K)$ be the vector space of $n \times n$ matrices with entries in $K$. We'll write $M(n)$ for short.

**Def:** Let the general linear group $GL(n,K)$ be the group of all invertible $n \times n$ matrices with entries in $K$:

$$GL(n,K) = \{ g \in M(n,K) : \det(g) \neq 0 \}$$

We'll write $GL(n)$ for short.

**Def:** A (linear) algebraic group is a subgroup of $GL(n,K)$ of this form:

$$G = \{ g \in GL(n,K) : P_1(g) = \cdots = P_n(g) = 0 \}$$

where $P_i : M(n,K) \rightarrow K$ are polynomials in the matrix entries.

(This is just a first version of the definition; see Springer for other equivalent definitions. Allowing infinitely many polynomial equations would not change anything, since polynomial rings are Noetherian).
Examples of algebraic groups:

1. $\text{GL}(n, k)$ is the king of all algebraic groups!

2. Let $\text{SL}(n, k)$ (or $\text{SL}(n)$) be the special linear group:

$$\text{SL}(n, k) = \{ g \in \text{GL}(n, k) : \det(g) = 1 \}$$

This is an algebraic group because $\det$ is a polynomial. This partially eliminates the center of $\text{GL}(n, k)$: the center of $\text{SL}(n, k)$ is just the matrices

$$
\begin{pmatrix}
\alpha & 0 & \cdots & 0 \\
0 & \alpha & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \alpha
\end{pmatrix}
$$

s.t. $\alpha^n = 1$.

so it's finite. We'll find out why we want to get rid of the center later.

3. Let $\text{O}(n, k)$ (or $\text{O}(n)$ for short) be the orthogonal group:

$$\text{O}(n, k) = \{ g \in \text{GL}(n, k) : g v \cdot g w = v \cdot w, \forall v, w \in k^n \}$$

where $v \cdot w = \sum_{i=1}^n v_i w_i$.

Note: We could also write $\text{O}(n, k) = \{ g \in \text{GL}(n, k) : g^T g = I \}$ where $g^T$ is the transpose of $g$. This makes it more clear that $\text{O}(n, k)$ is actually an algebraic group, since it's defined by $n^2$ quadratic equations.
\[(g v \cdot g w = v \cdot w \iff v \cdot g^T g w = v \cdot w \iff g^T g = 1)\]

Intuitively, \(O(n)\) consists of rotations, reflections, and products of those. A typical reflection is:

\[
\begin{pmatrix}
-1 & 0 \\
0 & 1
\end{pmatrix}
\]

4. If \(g \in O(n)\), \(\det(g^T g) = 1\), so \(\det(g) = \pm 1\). So there's an algebraic group called the **special orthogonal group**:

\[SO(n, K) := O(n, K) \cap SL(n, K)\]

\[= \{ g \in GL(n, K) : g^T g = 1 \text{ and } \det(g) = 1 \}.
\]

Note that in general, the intersection of linear algebraic groups in \(GL(n, K)\) is again algebraic, as seen here.

\(SO(n)\) consists only of rotations.

5. The **Euclidean group** \(E(n, K)\) (or \(E(n)\) for short) is the group of all maps \(f : K^n \to K^n\) of the form

\[f(x) = Rx + v\]

where \(R \in SO(n, K)\) is a rotation and \(v \in K^n\) gives a translation.
For \( n=2 \), \( K=\mathbb{R} \), this is the symmetry group of the Euclidean plane. It's a group because:

\[
R' (R'x + v') + v = (RR')x + (Rv' + v'); \quad R, R' \in SO(n), v, v' \in K^n.
\]

So as a set \( E(n) \cong SO(n) \times K^n \) is not isomorphic as groups though. Multiplication is instead given by

\[
(R, v)(R', v') = (RR', Rv' + v)
\]

It's not then a product of groups; instead it's a "semidirect product."

To make \( E(n) \) into an algebraic group, we need to think of \((R, v)\) as a matrix:

\[
\phi: (R, v) \rightarrow \begin{pmatrix} R & v \\ 0 \cdots 0 & 1 \end{pmatrix}_{n+1}
\]

and check \( \phi ((R, v)(R', v')) = \phi (R, v) \cdot \phi (R', v') \). So now the group operation is matrix multiplication, and we get a subgroup of \( GL(n+1, K) \) that's isomorphic to \( E(n) \). So now we'll say

\[
E(n) = \left\{ g \in GL(n+1); g = \begin{pmatrix} R & v \\ 0 \cdots 0 & 1 \end{pmatrix}, R \in SO(n), v \in K^n \right\}
\]

and this is an algebraic group. Indeed, Euclidean geometry and its generalizations led to the modern theory of algebraic groups.
Euclidean geometry, with $E(2,1)$ as symmetries.

- Originally formulated as a bunch of axioms. One in particular caused trouble: the "parallel postulate", which says:

```
    l'    l
   /    /
  /      /
P       l
```

\[ \forall p \in P, \forall l \in L \left( p \parallel l \Rightarrow \forall p' \left( \neg p' \parallel l \Rightarrow \exists l' \in L \left( p' \parallel l' \land \neg \exists q \left( q \parallel l \land q \parallel l' \right) \right) \right) \right) \]

where \( I \subseteq P \times L \) is the relation called "incidence": \( p \parallel l \) means \( p \) lies on \( l \).

There are 2 kinds of geometry that obey all the axioms of Euclidean geometry except the parallel postulate:

1) elliptic geometry

\[ x^2 + y^2 + z^2 = 1 \]

\[ P = \mathbb{RP}^2 = \mathbb{S}^2 / \sim \]

\[ L = \{ \text{great circles} \} \]

Here there are no parallel lines: any two distinct lines intersect in a single point (after identifying antipodal points).
2) hyperbolic geometry

\[ x^2 + y^2 - z^2 = 1 \]

\[ P = \exists (x^2 + y^2 - z^2 = 1 \land \exists p \sim p') \]

\[ L = \exists \text{intersections of the hyperboloid with planes through origin} \]

Here we have too many parallel lines:

\[ \exists \text{many classes of } l' \]

\[ P \quad l \]
3 Geometries and Their Algebraic Groups

1) Elliptic Geometry

Take $K^3$ with the usual inner product:

$$v \cdot w = v_1w_1 + v_2w_2 + v_3w_3$$

Form the sphere:

$$X = \{ v \in K^3 : v \cdot v = 1 \}$$

and define a set $P$ of points and a set $L$ of lines as follows:
\[ P = \bigoplus 1d\text{-}subspaces\ of\ K^3 \]

\[ L = \bigoplus 2d\text{-}subspaces\ of\ K^3 \]

We define the incidence relation "a point \( p \) lies on a line \( l \)" by \( p \subseteq l \). We use the dot product to define distances and angles between points and lines, resp.

The group \( SO(3) \) acts on \( K^3 \) preserving the dot product, and thus it acts on \( P \) and \( L \) preserving distances and angles and also the incidence relation: \( \forall g \in SO(3), \)

\[ p \subseteq l \Rightarrow g p \subseteq g l \]

2) Hyperbolic geometry

Give \( K^3 \) the Lorentzian dot product:

\[ v \cdot w = -v_1 w_1 - v_2 w_2 + v_3 w_3 \]

so that

\[ X = \{ v \in K^3 : v \cdot v = 1 \} \] is a hyperboloid w/ two sheets.

Define sets of points and lines by
\[ P = \{ \text{2d-subspaces of } K^2 \text{ with non-empty intersection with } X^2 \} \]
\[ L = \{ \text{2d-subspaces of } K^2 \text{ with non-empty intersection with } X^2 \} \]

(Note the new clause compared with elliptic geometry - it's not really new, it was just "invisible" before)

Let

\[ O(1,2) = \{ g \in GL(3) : g v \cdot g w = v \cdot w, \forall v, w \in K^3 \} \] where \( \cdot \) is the Lorentzian dot product.

Einstein realized that space and time form \( \mathbb{R}^4 \) with \( O(1,2) \) acting as symmetries.

Let \( SO(1,2) = O(1,2) \cap SL(3) \). Then \( SO(1,2) \) acts on \( K^2 \) preserving the Lorentzian dot product and thus it acts on \( X, P, \) and \( L \). You can define distances between points and angles between lines and \( SO(1,2) \) preserves these.

We say \( p \in P \) lies on a line \( l \in L \) if \( p \in l \), and then \( SO(1,2) \) preserves this incidence relation: \( \forall g \in SO(1,2), p \in l \Rightarrow gp \in g l. \)
3) Euclidean Geometry

Take $k^3$ with the degenerate dot product:

$$v \cdot w = v_3 w_3$$

Note (looking at the bilinear forms in the different geometries here):

- Elliptic: $+++$
  - $s = 1$
  - $s(x^2 + y^2) + z^2 = 1$

- Euclidean: $00+$
  - $s = \frac{1}{2}$
  - $s = 0$

- Hyperbolic: $-+-$
  - $s = \frac{1}{2}$
  - $s = -1$

As $s$ varies, get a different geometry.

Now $X = \{ v \in k^3 : v \cdot v = 1 \}$ is the set $\{ z^2 = 1 \} \subset \text{two parallel planes}$

So we let

$$P = \{ \text{4d-subspaces of } k^3 \text{ having nonempty intersection with } X \}$$

$$L = \{ \text{2d-subspaces of } k^3 \text{ having nonempty intersection with } X \}$$
The Euclidean group

\[ E(3) = \left\{ \left( \begin{array}{cc} R & \nu \\ 0 & 1 \end{array} \right) : R \in SO(2) \text{ and } \nu \in \mathbb{R} \right\} \]

acts on \( \mathbb{R}^3 \) preserving

\[ X = \left\{ (x, y, z) \in \mathbb{R}^3 : z = \pm 1 \right\} \]

\[
\left( \begin{array}{c} R \\ 0 \end{array} \right) \cdot \left( \begin{array}{c} x \\ y \\ z \end{array} \right) = \left( \begin{array}{c} R(x) + \nu \\ y \\ 1 \end{array} \right)
\]

So \( E(3) \) preserves the plane \( z = 1 \) and acts on it just as a Euclidean transformation should:

\[
\left( \begin{array}{c} x \\ y \end{array} \right) \mapsto R \left( \begin{array}{c} x \\ y \end{array} \right) + \nu
\]

\( E(3) \) also preserves the plane \( X = -1 \), hence \( X \). We can define distance b/w points and angles b/w lines, and \( E(3) \) preserves these; it also preserves the incidence relation \( p \subseteq \ell \). So the main weird thing about this case is that \( E(3) \) is not the group of all \( \text{det} = 1 \) transformations preserving the degenerate dot product. It's only the subgroup where \( R \in SO(2) \subseteq SL(2) \).

People looked at the 3 geometries and noticed they're all subsumed (as far as incidence relations go) in a single geometry: projective geometry.
4) Projective Geometry

Here we define points and lines in a simpler way:

\[ P = \mathop{\Xi} 1d\text{-subspaces of } K^3 \]

\[ L = \mathop{\Xi} 2d\text{-subspaces of } K^3 \]

We won't define distances b/w points and angles b/w lines; all we care about is the incidence geometry: we say \( p \in P \) is incident to \( l \in L \) (or \( p \) lies on \( l \)) if \( p \subseteq l \).

Now the symmetry group is all of \( GL(3) \): all invertible linear transfs. Since all of them act on \( P \) and \( L \) preserving the incidence relation:

\[ p \subseteq l \Rightarrow gp \subseteq gl \]

Actually, projective geometry goes back at least to the Renaissance painters, who developed perspective.

"Tin Can with Apple"
If we fix any plane $X \subseteq K^3$ not containing the origin, most (but not all) 1d-subspaces of $K^3$ will intersect $X$ in a single point (some won't intersect at all).

Thus most points $p \in P$ correspond to points of $X$. The remaining points of $P$ are called "points at infinity." Mathematically, we can do this trick in any dimension: start with $K^n$, and form a set of points called projective $(n-1)$-space:

$$KP^{n-1} = \{ 1d\text{-subspaces of } K^n \}$$

Most points in $KP^{n-1}$ will intersect the plane

$$X = \{ (x_1, \ldots, x_{n-1}, 1) : x_i \in K \} \text{ in a single point.}$$

So we get a 1-1 correspondence between $X$ and an "open dense" set in $KP^2$: only 1d-subspaces lying in xy-plane don't correspond to points of $X$. 

Points and lines in either elliptic, hyperbolic or Euclidean geometry give points and lines in projective geometry, and their symmetry groups are all subgroups of its symmetry group $GL(3)$. 
Proyective Geometry

Recall that for any field $k$,

$$K^{n+1} = \prod_{i=1}^{n+1} k$$

Thm: As sets, $K^n \cong K^+ + K^{n-1} + K^{n-2} + \cdots + K^0$.

Here, $\cong$ means there's a bijection and $+$ means disjoint union. These pieces $K^n, K^{n-1}, \ldots, K^0$ are called Schubert cells. This is called a Schubert decomposition.

Pf: Any 1d-subspace of $K^{n+1}$ has the form $\langle (x_1, \ldots, x_{n+1}) \rangle$ with $(x_1, \ldots, x_{n+1}) \neq 0$ - where $\langle \rangle$ means the span - all linear combinations.

If $x_{n+1} \neq 0$, $p = \langle (x_1, x_2, \ldots, x_n, 1) \rangle = \langle (y_1, \ldots, y_n, 1) \rangle$ and this description is unique:

$$\langle (y_1, \ldots, y_n, 1) \rangle = \langle (y'_1, \ldots, y'_n, 1) \rangle$$

$$\Rightarrow y_1 = y'_1, \ldots, y_n = y'_n$$

So we get a bijection b/w $K^n$ and the set of 1d subspaces of $K^{n+1}$ of the form $\langle (x_1, \ldots, x_{n+1}) \rangle$ with $x_{n+1} \neq 0$. If $x_{n+1} = 0$, then $p$ is really a 1d subspace of $K^n$, where

$$K^n \cong \prod_{i=1}^{n} \{ (x_1, \ldots, x_n, 0) : x_i \in k \}$$
So we get a bijection

\[ KP^n \cong K^n + KP^{n-1} \]

By induction, we have

\[ KP^n \cong K^n + K^{n-1} + \ldots + K^0. \]

Examples:

1) The projective line \( KP' \) is in 1-1 correspondence with the affine line \( A_k' \) disjoint union \( K^0 \) (here \( A_k' = k' \))

The non-vertical lines have slopes determined by elements of \( K \). So \( KP' \) is \( k \) together with the "point at infinity" \( \infty \) corresponding to the vertical line. So

\[ KP' = k + \mathcal{Z} \mathcal{O} \]
2) $\mathbb{R}P^1$ as a set is $\mathbb{R} \cup \mathbb{C} \cup \mathbb{I}$. But as a topological space, it is $S^1$, the one-point compactification of $\mathbb{R}$:

![Diagram of $S^1$](image)

3) $\mathbb{C}P^1$, the complex projective line, is $\mathbb{C} \cup \mathbb{C} \cup \mathbb{I}$. As a space this is $S^2$, or as a complex variety, the Riemann sphere:

![Diagram of $S^2$](image)

4) $\mathbb{R}P^2$, the real projective plane, is homeomorphic to $S^2/\mathbb{I}v \sim -v^2$

![Diagram of $S^2$ with antipodal points identified](image)

or just the northern hemisphere, a disc $D^2$:

![Diagram of $D^2$](image)

with $v \sim -v$ for points on the boundary.
This is in bijection with:

This open interval is homeomorphic to \( IR^1 \)

This point is homeomorphic to \( IR^0 \).

This interior is homeomorphic to \( IR^2 \)

\[
\mathbb{RP}^1 \cong IR^2 + IR + \frac{1}{2} \mathbb{RP}^1
\]

"the line at infinity" "the point at infinity"

\[
\mathbb{RP}^2 \cong \mathbb{RP}^1 + \mathbb{RP}^1 + \frac{1}{2} \mathbb{RP}^2
\]

5) Any finite field \( K \) has \( q \) elements, where \( q \) is a prime power

\[
q = p^n
\]

where \( p \) is a prime number and \( n = 1, 2, \ldots \)

Moreover, all fields with \( q \) elements are isomorphic, so we write \( \mathbb{F}_q \) for "the" field with \( q \) elements are isomorphic.

Not canonically isomorphic

When \( p \) is prime, \( \mathbb{F}_p \) is just \( \mathbb{Z}/p\mathbb{Z} \) with the usual \( +, \cdot \).

To get \( \mathbb{F}_{p^n} \) with \( n > 1 \), take \( \mathbb{F}_p \) and throw in all the \( n \) roots of some degree \( n \) polynomial that has no roots in \( \mathbb{F}_p \).
What's the cardinality of \( \mathbb{F}_q P^n \)?

\[
| \mathbb{F}_q P^n | = | \mathbb{F}_q^n + \mathbb{F}_q^{n-1} + \ldots + \mathbb{F}_q^0 | \\
= \sum_{i=0}^{n} | \mathbb{F}_q^i | = q^n + q^{n-1} + \ldots + 1 = \frac{q^{n+1} - 1}{q-1}
\]

is called the q\text{-}integer \( \left[ \frac{n+1}{q} \right] \) (since it approaches \( n+1 \) as \( q \to 0 \)).

6) \( \mathbb{F}_2 P^2 \) is called the \underline{Fano plane} - the smallest projective plane. 
\( | \mathbb{F}_2 P^2 | = 2^2 + 2 + 1 = 7 \), so it has 7 points.
The Fano plane:

\[ \langle e_1, e_2, e_3 \rangle \]

\[ \langle e_1 + e_2 \rangle \]

\[ \langle e_1 + e_3 \rangle \]

\[ \langle e_2 + e_3 \rangle \]

\[ \langle e_1 + e_2 + e_3 \rangle \]

\[ \langle e_1 \rangle \]

\[ \langle e_2 \rangle \]

\[ \langle e_3 \rangle \]

e.g., \( \langle e_1, e_2, e_3 \rangle \) all lie on a line since they're in a 2d space \( \langle e_1, e_2 \rangle \).

So \( \mathbb{F}_2 P^2 \) has 7 points and 7 lines.

Thm: In any projective plane \( kP^2 \):

1) For any 2 distinct points \( p, p' \), \( \exists! \) line \( l \) with \( p, p' \subseteq l \).
2) For any 2 distinct lines \( l, l' \), \( \exists! \) point \( p \) with \( p \subseteq l, l' \).

Proof: 1) Given 2 distinct 1d-subspaces of \( K^3 \), \( p \) and \( p' \), the subspace sum \( p + p' = \{ \mathbf{v} + \mathbf{v}' : \mathbf{v} \in p, \mathbf{v}' \in p' \} \) is 2-dim \( l \), so it's a line \( l \) with \( p, p' \subseteq l \) and it's the unique one.

2) Given 2 distinct 2d-subspaces of \( K^3 \), \( l \) and \( l' \), we claim \( l \cap l' \) will be a 1d-subspace \( p = l \cap l' \). This follows from

\[ 3 = \dim(l + l') = \dim(l) + \dim(l') - \dim(l \cap l') \]

\[ = 2 + 2 - \dim(l \cap l'). \]
Thus \( \dim(l \cup l') = 1 \), so \( p = l \cap l' \) is a point on both lines, and we can show it's unique.

\[ \square \]

Axiomatic Projective Geometry

Def: An abstract projective plane consists of a set \( P \) of points, a set \( L \) of lines, and an incidence relation \( I \subseteq P \times L \). If \( (p, l) \in I \), we say \( p \in l \) or \( p \) lies on \( l \). We demand:

1) For any distinct \( p, p' \in P \), \( \exists! \; l \in L \) with \( p \in l \), \( p' \in l \)

2) For any distinct \( l, l' \in L \), \( \exists! \; p \in P \) with \( p \in l \), \( p \in l' \).

3) Nondegeneracy axiom:

\( \exists \) exist 4 points, no 3 of which lie on the same line.

This is equivalent to the following statement:

3'): \( \exists \) exist 4 lines, no 3 of which contain the same point.

The nondegeneracy eliminates these:

1) \( P = L = \emptyset \)

3) 

2) \( P = \emptyset \), \( L = \emptyset \) or \( P = \emptyset \), \( L = 1 \)

4) 
