table of contents

1

Section 1
algebraic geometry

1.1 affine varieties

Review: Zariski topology, Hilbert's *Nullstellensatz*, irreducibility, noetherian, reducibility (of algebras), maximal ideal spectrum.

DEF 1.1 *F*-structures

If F is a subfield of k, say F is a **field of definition** for a closed subset $X \subseteq \mathbb{A}^n$, if $I(X)$ can be generated in $k[\mathbb{A}^n]$ by polynomials in F coefficients. (That is, X can be "*defined over* F".) A closed subset Y of X is called F-**closed** if $I_X(Y)$ is defined over F. The F-rational points are F-homomorphisms $F[X] \to F$, or equivalently, F-morphisms $\mathbb{A}^0 \to X$.

Kv

Equivalently, an F-structure on $k[X]$ is an F-algebra $F[X]$ such that $F[X] \otimes_F k \cong k[x]$ as k-algebras.

The same closed subset may admit two different F-structures. For example, $\mathbb{C}[x,y] / (x^2+y^2+1)$ admit two different $\mathbb{R}$-structures (with different $\mathbb{R}$-rational points): $\mathbb{R}[x,y] / (x^2+y^2-1)$ and $\mathbb{R}[x,y] / (x^2+y^2+1)$.

Review: regular functions, sheaves, stalks, affine varieties and morphisms, prevarieties.

Affine F-varieties are affine varieties defined over F. The category of affine varieties is anti-equivalent to the category of affine algebras (finitely generated reduced k-algebras).

1.2 products and varieties

DEF 1.2 product

We can form the product of two affine varieties $X \times Y$, by taking the maximal ideal spectrum of $k[X] \otimes k[Y]$. This topology is finer than the usual product, which is the maximal ideal spectrum of $k[X] \times k[Y]$; intuitively, we need to allow mixed polynomial of x and y, for example $x \cdot y$, which is inexpressible in $k[X] \times k[Y]$.

This product construction is the product in the categorical sense, and $k[X] \otimes k[Y]$ is the coproduct in the category of affine algebras. Products of prevarieties also exists in the categorical sense, defined chart by chart.

If X is a prevariety, there is a diagonal $\Delta_X = \{(x, x) : x \in X\}$ and a diagonal map $i_X : X \to X \times X$ taking x to (x, x). Δ_X has the induced topology from $X \times X$. $i_X : X \to \Delta_X$ is a homeomorphism for all prevariety X.

DEF 1.3 variety

A prevariety X is called a **variety** if Δ_X is *closed* in $X \times X$.

PROP 1.4

Let X be a variety and Y a prevariety.
1. If $\varphi : Y \to X$ is a morphism, then its graph is closed in $Y \times X$.
2. If $\varphi, \psi : Y \to X$ agrees in a dense subset of Y, then $\varphi = \psi$.

Below is a useful condition for a prevariety to be a variety:

PROP 1.5

Let X be a prevariety covered by finitely many affine open sets $\bigcup_{i=1}^{m} U_i$. Then X is a variety, if and only if for all pairs $i \neq j$, $U_i \cap U_j$ is also affine, and $\mathcal{O}_X\left(U_i \cap U_j\right)$ is generated by restrictions of $\mathcal{O}_X(U_i)$ and $\mathcal{O}_X\left(U_j\right)$.

We can similarly define F-varieties. The F-rational points of X are F-morphisms $\mathbb{A}^0 \to X$.

1.3 projective varieties

We will denote everything projective by a *.

DEF 1.6 projective space

We can make $\mathbb{P}^n$ into a variety as follows. Let $U_i = \left\{(x_0, \cdots, x_n)^* \in \mathbb{P}^n : x_i \neq 0\right\}$. U_i can be given an affine structure by assuming $x_i = 1$. $U_i \cap U_j$ is also affine, so by Proposition 1.5, $\mathbb{P}^n$ is a variety.

An ideal is called **homogeneous** if it is generated by homogeneous polynomials. The closed sets of $\mathbb{P}^n$ are the zero sets of homogeneous ideals.

Usual results for affine spaces carry over:

PROP 1.7

1. $\mathcal{O}_{\mathbb{P}^n}(D^*(f)) = k[t_0, \cdots, t_n]_f^*$, the latter defined as the algebra of rational functions $\frac{g}{f^h}$, where f and g are homogeneous with $\deg g = h \cdot \deg f$.
2. $V^*(I) = \emptyset$ if and only if $\sqrt{I}$ contains the **irrelevant ideal** $(t_0, t_1, \cdots, t_n)$.
3. $V^*(I)$ is irreducible if and only if $\sqrt{I}$ is prime.

Products of $\mathbb{P}^n$ can be defined as a closed subset of some projective space. Consider $\varphi : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}$, $(x_i)^*, \left(y_j\right)^* \mapsto \left(x_i y_j\right)^*$. The image of this map defines an isomorphism $\mathbb{P}^m \times \mathbb{P}^n \to V^{m,n} \subseteq \mathbb{P}^{mn+m+n}$, where $V^{m,n}$ is a closed subset of $\mathbb{P}^{mn+m+n}$, defined by the zero set of $z_{ij}z_{kl} - z_{ik}z_{jl}$.

A **projective variety** is a closed subset of some $\mathbb{P}^n$, and a **quasiprojective variety** is an open subset of some projective variety.

1.4 dimension

If X is any irreducible affine variety, then $k[X]$ is an integral domain. Let $k(X)$ be its fraction field. For any principal open set $U = D(f)$, $k[U] = k[X]_f$, so $k(U) = k(X)$.

DEF 1.8
dimension

If X is any irreducible general variety, then for any two affine open subsets U and V, $k(U) = k(V)$ by the argument above. Therefore, we can speak of $k(X)$, and the **dimension** of X is defined as the transcendence degree of $k(X)$ over k.

For example, if X is irreducible affine, the dimension of X is the maximum number of algebraically independent elements in $k[X]$.

If Y is a proper irreducible closed subvariety of X, then $\dim Y < \dim X$. If X and Y are irreducible varieties, then $\dim X \times Y = \dim X + \dim Y$. $\dim \mathbb{A}^n = \dim \mathbb{P}^n = n$, and 0-dimensional varieties are all finite. For an irreducible polynomial f, $Z_{\mathbb{A}^n}(f)$ always has codimension 1.

1.5 a technical result

THM 1.9

Let $\varphi : X \to Y$ be a morphism of varieties. Then φX contains a non-empty open subset of its closure $\overline{\varphi X}$.

This implies that the image of any *constructible set* is constructible: a set is called constructible if it is the union of locally closed sets (the intersection of an open set and a closed set).

2

Section 2 linear algebraic groups, first properties

2.1 algebraic groups

DEF 2.1 algebraic groups

An **algebraic group** is an algebraic variety G which is also a group, such that multiplication $\mu : G \times G \to G$ and inverse $i : G \to G$ are morphisms of varieties.

If the underlying variety is affine, call G **linear**.

If G is linear, let $A = k[G]$. Then $\mu : G \times G \to G$ defines an algebra homomorphism, the **comultiplication** $\Delta : A \to A \otimes A$, and $i : G \to G$ defines the **antipode** $\iota : A \to A$. Roughly speaking, Δ tells you how to split x and y apart when evaluating $f(xy)$; it turns f into $\sum f_{1i} \otimes f_{2i}$, so that $f(xy) = \sum f_{1i}(x) \cdot f_{2i}(y)$. For example, if group operation is addition and $f(x) = x^2$, then $f(x+y) = x^2 + 2xy + y^2$, so $\Delta(f) = x^2 \otimes 1 + 2x \otimes x + 1 \otimes x^2$.

The identity $e \in G$ is a map $\mathbb{A}^0 \to G$, so it corresponds to a map $A \to k$, taking f to $f(e)$. k can be embedded back to A, taking $c \in k$ to the constant function $f(x) = c$. This way we get a map, the **identity** $\varepsilon : A \to A$, which takes a function f and returns a constant function $f(e)$. This is the algebraic equivalent of the map $G \to \{e\}$.

The diagonal map $x \mapsto (x, x)$ corresponds to a map $A \otimes A \to A$, taking $f(x) \otimes g(y)$ to $(f \cdot g)(x)$. This is the **multiplication** map $m : A \otimes A \to A, f \otimes g \mapsto f \cdot g$. Using Δ, ι, ε and m, we can rewrite the group axioms as follows:

property — in G — in A

associativity

$$\begin{tikzcd}
G \arrow[drr] & \times & G \arrow[d, "\mu"'] & \times & G \arrow[d, "\mathrm{id}"'] \\
 & & G \arrow[drr] & \times & G \arrow[d, "\mu"'] \\
 & & & & G
\end{tikzcd}
\qquad
\begin{tikzcd}
A & \otimes & A & \otimes & A \\
 & & A \arrow[ull] \arrow[u, "\Delta"] & \otimes & A \arrow[u, "\mathrm{id}"] \\
 & & & & A \arrow[ull] \arrow[u, "\Delta"]
\end{tikzcd}$$

inverse

$$\begin{tikzcd}
G \arrow[d] \arrow[drr, "\Delta_G"'] \arrow[dddrr, bend left, "g \mapsto e"] & & \\
G \arrow[d, "\mathrm{id}"] & \times & G \arrow[d, "i"] \\
G \arrow[drr] & \times & G \arrow[d, "\mu"'] \\
 & & G
\end{tikzcd}
\qquad
\begin{tikzcd}
A & & \\
A \arrow[u] & \otimes & A \arrow[ull, "m"'] \\
A \arrow[u, "\mathrm{id}"] & \otimes & A \arrow[u, "\iota"] \\
 & & A \arrow[ull] \arrow[u, "\Delta"] \arrow[uuull, bend right, "\varepsilon"']
\end{tikzcd}$$

identity

$$\begin{tikzcd}
 & & G \arrow[d, equal] \arrow[dd, bend left, "\mathrm{id}"] \\
\{e\} \arrow[drr] & \times & G \arrow[d, "\mu"'] \\
 & & G
\end{tikzcd}
\qquad
\begin{tikzcd}
 & & A \arrow[d, equal] \\
\{\varepsilon\} & \otimes & A \\
 & & A \arrow[ull] \arrow[u, "\Delta"] \arrow[uu, bend right, "\mathrm{id}"']
\end{tikzcd}$$

The rules can be understood as follows. Like we said, Δ does the following thing: give me a function f and two variables x and y, I tell you how to evaluate f on $x \cdot y$. So associativity is essentially saying that, give me f and three variables x, y and z, I have two equivalent ways to evaluate $f(x \cdot y \cdot z)$: first we get to know how to evaluate $f(x \cdot y)$, and then we get to know how to evaluate $f((x \cdot y) \cdot z)$, or vice versa. Inverse is essentially saying that, given a function $f : G \to k$, first split x and y apart: $f(xy) = \sum f_{1i}(x) f_{2i}(y)$ and turn y into y^{-1}, and multiply the two part together: $\sum f_{1i}(x) f_{2i}(x^{-1})$. This is essentially $f(xx^{-1})$, and it asserts that this is equal to $f(e) = f(\varepsilon(x))$. Finally, identity is just saying that $f(e \cdot x)$ is equal to $f(x)$.

For two examples, $(k, +)$ is a linear algebraic group, called the **additive group** G_a, and $(k^\times, \cdot)$ is also a linear algebraic group, called the **multiplicative group** G_m or $\mathrm{GL}(1)$. They are examples of *connected* groups.

Other linear algebraic groups include: $\mathrm{GL}(n, \mathbb{C})$, $\mathrm{SL}(n, \mathbb{C})$, D_n (diagonal), T_n (upper-triangular), U_n (unipotent upper-triangular), O_n, SO_n and Sp_{2n}. O_n is *not* connected when $\operatorname{char} k \neq 2$.

For an example of a non-linear algebraic group: the elliptic curve is a projective variety, with an abelian group structure.

2.2 some basic results

We first state some basic results we want to prove for algebraic groups, and then proceed to their proofs.

PROP 2.2 There is a unique irreducible component G^0 containing e. G^0 is also the connected component of e. It is a normal subgroup of G of finite index, and any subgroup of finite index contains G^0.

Therefore, irreducibility of algebraic groups is equivalent to connectedness. For this reason, we say that algebraic groups are *connected* rather than *irreducible*.

Recall that in the case of topological / Lie groups, any open neighbourhood of e generates the whole group. However in Zariski topology any open set is dense (at least in that irreducible component), so things are easier here:

PROP 2.3 If G is connected, then for any two open sets U and V in G, $U \cdot V = G$.

We would like that operations on closed subgroups yield closed ones.

PROP 2.4 The kernel and image of an algebraic group homomorphism are closed subgroups. If $\varphi : G \to G'$, then $\varphi\left(G^0\right) = \varphi(G)^0$.

PROP 2.5 The subgroup generated by closed subgroups is closed and connected.

PROP 2.6 The commutator of a closed subgroup and a connected closed subgroup is connected.

We now set out to prove them.

Proof of Proposition 2.2. If X and Y are irreducible components, then $XY = \mu(X \times Y)$ and their closure are irreducible. Therefore, $X = Y = \overline{XY}$. In particular X is closed under multiplication and $X = X^{-1}$; so X is a closed subgroup. Since inner automorphisms produce homeomorphisms, $xXx^{-1} = X$, so X is normal. Its cosets are components of G so there are finitely many of them. This also shows that irreducible components are disjoint, so they are also connected components. $\square$

Proof of Proposition 2.3. Both xV^{-1} and U are open dense, so they intersect somewhere. $\square$

LEM 2.7 If H is a subgroup of G, then $\overline{H}$ is also a subgroup. If H contains a non-empty open subset of $\overline{H}$ (so H is “large enough”), then H is closed.

A non-example for this lemma would be $(\mathbb{Z},+) \subset (\mathbb{C},+)$.

Proof. If $x \in H$ then $H = xH \subseteq x\overline{H}$. Since $x\overline{H}$ is closed, $\overline{H} = x\overline{H}$. So $H\overline{H} = \overline{H}$. Now let $x \in \overline{H}$. Similar argument shows $\overline{H}$ is a closed subgroup. If H contains a non-empty open subset of $\overline{H}$, then H, as the union of translates of that open subset, is open in $\overline{H}$. So $\overline{H} = HH$ by Proposition 2.3, and $H = \overline{H}$. □

Proof of Proposition 2.4. Inverse image of a closed set $\{e\}$ is closed. $\overline{\varphi(G)}$ contains an open subset of $\varphi(G)$ (Theorem 1.9), so $\varphi(G)$ is closed. $\varphi\left(G^0\right)$ is connected and of finite index in $\varphi(G)$. □

LEM 2.8 Suppose X_i $(i \in I)$ are irreducible varieties with morphisms $\varphi_i : X_i \to G$, such that $e \in \varphi_i X_i$. Let H be generated by $\varphi_i X_i$. Let $Y_i = \varphi_i X_i$.

1. H is connected;
2. there is some $n > 0$ and $(a_1, \cdots, a_n) \in I^n$, together with $(\varepsilon_1, \cdots, \varepsilon_n) \in \{\pm 1\}^n$ such that $H = Y_{a_1}^{\varepsilon_1} \cdots Y_{a_n}^{\varepsilon_n}$.

Proof. Assume that all Y_i^{-1} occur among the Y_j's. For $a \in I^n$ let $Y_a = Y_{a_1} \cdots Y_{a_n}$; then $Y_b \cdot Y_c = Y_{b,c}$ and Y_b are irreducible subsets. Take a such that $\dim Y_a$ is maximal. □

Proof of Proposition 2.5 and Proposition 2.6. Taking φ_i the inclusion maps in the first case, and $\varphi_i(x) = xix^{-1}i^{-1}$ $(i \in K,\ X_i = H)$ in the second case. □

2.3 G-spaces

DEF 2.9 *G-spaces*

A G-**space** is a variety on which G can act.

A **homogeneous** space is a G-space where the G-action is transitive.

For $x \in X$, its **isotropy group** is $G_x = \{g \in G : gx = x\}$ and its **orbit** is $G \cdot x = \{g \cdot x : g \in G\}$.

In the case of Lie group actions on smooth manifolds, the orbits can be bad in general; for example, the action of $\mathbb{R}$ on $\mathbb{T}^2$ by $\left(x + t, x + \sqrt{2}\right)$ has orbits that are neither closed nor open. In the algebraic case, things are much simpler: it turns out that a closed orbit always exists, an essential statement in the theory of algebraic groups.

THM 2.10 *closed orbit lemma*

Orbits of lowest dimension are always closed; in particular, there exists closed orbits.

Proof. The proof roughly goes as follows. If an orbit is not closed, its boundary should be the union of other orbits and one dimension less; therefore, the orbit with minimal dimension should be a closed orbit.

An orbit is open in its closure. This is because, applying Theorem 1.9 to $g \mapsto g \cdot x$ shows that $G \cdot x$ contains a non-empty open subset U of its closure. Since $G \cdot$

x is the union of translates of U, $G \cdot x$ itself is open. Therefore, for $x \in X$, $S_x = \overline{G \cdot x} \setminus G \cdot x$ is closed. By the noetherian property there is a minimal S_x; it is a union of orbits. Suppose $y \in S_x$, then $G \cdot y \subseteq S_x$. Because S_x is closed, $\overline{G \cdot y} \subseteq S_x$, so $S_y \subsetneq S_x$, contradicting minimality. Therefore, S_x is empty, and $G \cdot x$ is a closed orbit. □

The proof also implies that an orbit is locally closed, so it can be made into a variety and hence a homogeneous G-space.

For linear algebraic groups, an especially important kind of G-actions is rational representations:

DEF 2.11 rational representation

A **rational representation** of G is a homomorphism of algebraic groups $G \to \mathrm{GL}(V)$. We also say V is a G**-module**.

Intuitively, a representation is rational if it is defined using polynomials. So for example the representation of $\mathbb{G}_a$ by $t \mapsto \begin{pmatrix} 1 & t \\ & 1 \end{pmatrix}$ is rational, but $t \mapsto \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}$ isn't.

Every finite group has a faithful representation in some $\mathrm{GL}(V)$, as follows. Right translation permutes the group elements, and therefore can be viewed as actions on $V = kG$; this action is a faithful representation. For linear algebraic groups, the case is similar; every linear algebraic group has a faithful representation in some finite-dimensional $\mathrm{GL}(V)$, via the action $k[G]$ by right translation. The gap here is that $k[G]$ is generally infinite dimensional. Therefore, we need the following lemma.

If X and G are affine, the group action $a : G \times X \to X$ defines a pullback $a^* : k[X] \to k[G] \otimes k[X]$. Given $f \in k[X]$ and $g \in G$, $a^* f$ tells us how to compute f on gx. This leads to a function $s(g)$ for every $g \in G$: $s(g)$ is a function $k[X] \to k[X]$ such that $s(g)f(x) = f(g^{-1}x)$. $s(g)$ reflects the action of G on $k[X]$.

LEM 2.12

Suppose G is a linear algebraic group acting on an affine variety X. Suppose V is a finite dimensional subspace of $k[X]$.

1. There is a finite dimensional subspace W of $k[X]$, that contains V and is stable under all $s(g)$.
2. V is stable under all $s(g)$ if and only if $a^* V \subseteq k[G] \otimes V$. If this is so, s defines a rational representation $G \times V \to V$.

Proof. To prove 1, we can assume $\dim V = 1$ and $V = kf$. Let $a^* f = \sum_{i=1}^n u_i \otimes f_i$. Then

$$(s(g)f)(x) = f(g^{-1}x) = \sum_{i=1}^n u_i(g^{-1}) f_i(x)$$

so all $s(g)f$ lies in the subspace spanned by f_i. The subspace spanned by $s(g)f$ is then finite dimensional and stable under all $s(g)$.

By a similar argument, if $a^*V \subseteq k[G] \otimes V$, then V is $s(G)$-stable. Conversely, if V is $s(G)$-stable, let $\{f_i\}$ be a basis of V and extend it to a basis $\{f_i, g_j\}$ of $k[X]$. Suppose $f \in V$ and $a^*f = \sum_i u_i \otimes f_i + \sum_j v_j \otimes g_j$. Then

$$(s(g)f)(x) = \sum_i u_i(g^{-1})f_i(x) + \sum_j v_i(g^{-1})g_i(x),$$

and our assumption says $v_i(g^{-1}) = 0$ for all g. So all v_i vanish, and $a^*V \subseteq k[G] \otimes V$. □

Now, take ρ to be the right translation: $\rho(g)f(x) = f(xg)$, then ρ defines a faithful rational representation of G in $\mathrm{GL}(k[G])$. Similarly, the left multiplication $\lambda(g)f(x) = f(gx)$ is a faithful rational representation of G. We want to extract a finite dimensional faithful representation out of it. Recall that $k[G]$ is generated (as an algebra) by finitely many elements; these elements span a finite dimensional subspace of $k[G]$, so by the previous lemma $k[G]$ has a finite dimensional subspace V that is stable under $\rho(G)$ and generate (as an algebra) the whole $k[G]$. This is the representation we want:

THM 2.13 linearization theorem

Any linear algebraic group G admits an isomorphism into some closed subgroup of some $\mathrm{GL}(n)$.

Proof. Let $V \subseteq k[X]$ be chosen as described earlier, and $\{f_1, \cdots, f_n\}$ a basis of V. Then $\rho(g)f_i = \sum_j m_{ji}(g)f_j$ for $m_{ji} \in k[G]$, and $\varphi(g) = \big(m_{ji}(g)\big)$ gives an algebraic group homomorphism $G \to \mathrm{GL}_n$; Since f_i generate $k[X]$ as an algebra, φ is injective, and $\varphi(G)$ is a closed subgroup of GL_n.

To prove that φ is actually an isomorphism onto $\varphi(G)$, we need φ^* surjective. $\varphi^* : k[\mathrm{GL}_n] = k\left[t_{ij}, \frac{1}{\det}\right] \to k[G]$ is given by $\varphi^* t_{ij} = m_{ij}$, $\varphi^* \frac{1}{\det} = \frac{1}{\det m_{ij}}$. Since $f_i(g) = \sum_j f_j(e)m_{ji}(g)$, φ^* is indeed surjective. □

2.4 Jordan decomposition

Recall that an endomorphism a of a vector space V is **semi-simple** if a is the direct sum of one-dimensional maps, i.e. a is diagonalizable, and **nilpotent** if $a^s = 0$ for some $s \in \mathbb{Z}_+$; a is called **unipotent** if $a - 1$ is nilpotent. Under a field of positive characteristic p, a is unipotent if and only if $a^{p^s} = 1$ for some $s \in \mathbb{Z}_+$. Also recall that a set of pairwise commuting matrices can be simultaneously upper-triangularized, and if they are also all semisimple they can be simultaneously diagonalized. The product, direct sum and tensor product of two semisimple (nilpotent, unipotent) matrices is semisimple (nilpotent, unipotent), and if $a \in \mathrm{End}(V)$ and $b \in \mathrm{End}(W)$ are semisimple (nilpotent) then so is $a \otimes 1 + 1 \otimes b$.

Similar to the additive Jordan decomposition $a = a_s + a_n$, we have a multiplicative version:

THM 2.14 multiplicative Jordan decomposition

Let $a \in \mathrm{GL}(V)$. Then there are unique elements $a_s, a_u \in \mathrm{GL}(V)$ such that

- $a = a_s \cdot a_u$,
- a_s is semisimple and a_u is unipotent,
- a_s and a_u commutes, and
- any a-stable subspace or the quotient of one is also a_s- and a_u-stable, and $a = a_s \cdot a_u$ interpreted in that space.

COR 2.15

If $a = a_s a_u$ and $b = b_s b_u$, then $a \oplus b = (a_s \oplus b_s) + (a_u \oplus b_u)$ and $a \otimes b = (a_s \otimes b_s)(a_u \otimes b_u)$.

The importance of multiplicative Jordan decopmosition is that it can be carried over to linear algebraic groups. Recall that every linear algebraic group can be linearized as a closed subgroup of some GL_n. We have a multiplicative Jordan decomposition there. Remarkably, this decomposition is intrinsic, i.e. not depending on the particular embedding:

THM 2.16 Jordan decomposition in algebraic groups

technically we need to specify the meaning of Jordan decomposition, in particular unipotency, in infinite dimensional spaces, in terms of *locally finite* endomorphisms; the results are pretty much the same though.

Suppose G is a linear algebraic group and $g \in G$. There are unique elements $g_s, g_u \in G$ such that

- $g = g_s g_u = g_u g_s$, and $\rho(g)_s = \rho(g_s)$, $\rho(g)_u = \rho(g_u)$, where $\rho(g)$ is the right translation in the vector space $k[G]$;
- g_s and g_u are natural, in the sense that for any algebraic group homomorphism $\varphi : G \to G'$, $\varphi(g)_s = \varphi(g_s)$ and $\varphi(g)_u = \varphi(g_u)$;

The set of unipotent elements of G, G_u, is a closed subset of G. The same need not hold for semisimple elements. Also, if $x \in G$ is an F-point, then *neither* x_s nor x_u need to be an F-point.

PROP 2.17

Suppose G is a subgroup of GL_n consisting of unipotent matrices. Then G is conjugate to a subgroup of U_n, the group of upper-triangular matrices with ones on the diagonal.

Hence, unipotent linear algebraic groups are nilpotent, and hence solvable. Another consequence is that whenever $G \to \mathrm{GL}(V)$ is a rational representation of a unipotent linear algebraic group, there is a non-zero vector in V fixed by all of G.

PROP 2.18 Kostant-Rosenlicht

Let G be a unipotent linear algebraic group and X and affine G-space. Then all orbits of G are closed.

3

Section 3

commutative algebraic groups

3.1 structure of commutative algebraic groups

We recall that every element $g \in G$ can be written as $g = g_s g_u$, and that G_u is always a closed subset of G. We now see that G splits cleanly into G_u and G_s in the case of commutative algebraic groups:

THM 3.1 Let G be a commutative linear algebraic group, and let G_s and G_u be the subset of semisimple and unipotent elements. Then G_s and G_u are *closed subgroups*, and G is the (inner) direct product $G_s \times G_u$.

If moreover G is connected, then the same holds for G_s and G_u.

PROP 3.2 Let G be a connected linear algebraic group of dimension one. Then G is commutative, and either $G = G_s$ or $G = G_u$.

In the latter case, if $\operatorname{char} k = p > 0$, then the elements of G have order dividing p.

3.2 diagonalizable groups and tori

DEF 3.3 rational character

Let G be a linear algebraic group. A homomorphism of algebraic groups $\chi : G \to \mathbb{G}_m$ is called a **rational character**.

The set of rational characters is denoted by $X^*(G)$. It has a natural abelian group structure, which we write *additively*. Characters are regular functions on G so lie in $k[G]$, and they are linearly independent in $k[G]$.

A homomorphism of algebraic groups $\lambda : \mathrm{G}_m \to G$ is called a **cocharacter**. The set of cocharacters is dentoed by $X_*(G)$, and it also have an abelian group structure, also written additively.

DEF 3.4
diagonalizable
tori

G is called **diagonalizable** if G is isomorphic to some closed subgroup of D_n, the group of diagonal matrices. G is called an (algebraic) **torus** if it is isomorphic to some D_n.

For example, if $G = \mathrm{D}_n$, then χ_i which takes x to the i-th element off the diagonal of x is a character. Monomials in χ_i serves as a basis for $k[\mathrm{D}_n]$, so they are all characters. As a result, $X^*(G) \cong \mathbb{Z}^n$. A homomorphism $\mathrm{G}_m \to \mathrm{D}_n$ is always of the form $x \mapsto \mathrm{diag}(x^{a_1}, \cdots, x^{a_n})$, so $X_*(\mathrm{D}_n) \cong \mathbb{Z}^n$.

THM 3.5

The following conditions are equivalent:

- G is diagonalizable;
- $X^*(G)$ is a finitely generated abelian group, and its elements form a k-basis of $k[G]$;
- any rational representation of G is a direct sum of 1-dimensional such representations.

In this case, $k[G]$ is isomorphic to the group algebra of $X^*(G)$, and if $\operatorname{char} k = p > 0$, then $X^*(G)$ doesn't have p-torsion.

To recall, if M is a finitely generated abelian group, then its group algebra $k[M]$ is the k-algebra with basis $e(m)$ ($m \in M$), with multiplication $e(m) \cdot e(n) = e(m+n)$. We have $k[M_1 \oplus M_2] \cong k[M_1] \otimes_k k[M_2]$. Define homomorphisms $\Delta : e(m) \mapsto e(m) \otimes e(m)$, $\iota : e(m) \mapsto e(-m)$ and $e : e(m) \mapsto 1$. Assume M has no p-torsion if $p = \operatorname{char} k > 0$. For example, if $M = \mathbb{Z} / d\mathbb{Z}$ where $p \nmid d$, then $k[M] \cong k[t] / \left(t^d - 1\right)$.

The $e(\cdot)$ is used solely to prevent confusing operations in M and in $k[M]$.

PROP 3.6

- $k[M]$ is always an affine algebra, and there is a diagonalizable linear algebraic group $\mathcal{G}(M)$ with $k\left[\mathcal{G}(M)\right] = k[M]$, such that Δ, ι and e are exactly the comultiplication, antipode and identity;
- There is a canonical isomorphism $M \cong X^*\left(\mathcal{G}(M)\right)$;
- If G is a diagonalizable group, then there is a canonical isomorphism $\mathcal{G}(X^*(G)) \cong G$.

Since $\mathcal{G}(\mathbb{Z}^n) = \mathrm{D}_n$ and $\mathcal{G}(\mathbb{Z} / d\mathbb{Z})$ is finite, we proved that

COR 3.7

A diagonalizable group is a direct product of a torus and a finite abelian group of order prime to $p = \operatorname{char} p$. It is a torus if and only if it is connected.

PROP 3.8
rigidity of
diagonalizable groups

Let G and H be diagonalizable groups and X a connected affine variety. If there is a morphism of varieties $\varphi : X \times G \to H$, such that for any given $x \in X$, $\varphi(x, -)$ is a homomorphism of algebraic groups, then φ is independent of x.

This proposition essentially says that homomorphisms between diagonalizable groups are *rigid*, or cannot be deformed; in other words, $\mathrm{Hom}(G, H)$ behaves like a *discrete* set, think $\mathbb{Z}^n$. As an application, recall the centralizer and the normalizer of a subgroup. They are both closed subgroups of G, and $Z_G(H) \trianglelefteq N_G(H)$.

COR 3.9 If H is a diagonalizable subgroup of G, then $N_G(H)^0 = Z_G(H)^0$ and $N_G(H) / Z_G(H)$ is finite.

Now suppose T is a torus. For $\chi \in X^*(T)$ and $\lambda \in X_*(T)$ the map $a \mapsto \chi(\lambda(a))$ is a character $\mathbb{G}_m \to \mathbb{G}_m$, and such a map can only some monomial $a \mapsto a^d$. We set $\langle \chi, \lambda \rangle = d$. This defines a *perfect* pairing between $X^*(T)$ and $X_*(T)$; in particular $X_*(T)$ is free abelian. The map $a \otimes \lambda \mapsto \lambda(a)$ defines a canonical isomorphism between abelian groups $k^\times \otimes X_*(G) \cong T$.

If V is a T-space, then we have a (locally finite) representation s of T in $k[V]$. For a regular character χ, let $k[V]_\chi$ denote its eigenspace:

$$k[V]_\chi = \{f \in k[V] : s(t) \cdot f = \chi(t) \cdot f, \forall t \in T\}.$$

The subspaces $k[V]_\chi$ form an $X^*(G)$-grading of $k[V]$:

$$k[V] = \bigoplus_{\chi \in X^*(G)} k[V]_\chi, \; k[V]_\chi k[V]_\psi \subseteq k[V]_{\varphi+\psi}.$$

If φ is a morphism $\mathbb{G}_m \to Z$ we write $\lim_{a\to 0} \varphi(a) = z$ if φ extends to a morphism $\tilde{\varphi} : \mathbb{A}^1 \to Z$ with $\tilde{\varphi}(0) = z$. If $\varphi'(a) = \varphi(a^{-1})$ then we write $\lim_{a\to\infty} \varphi(a) = \lim_{a\to 0} \varphi'(a)$. If V is a T-space and λ is a cocharacter, let $V(\lambda)$ be the set of $v \in V$ such that $\lim_{a\to 0} \lambda(a) \cdot v$ exists. Then $V(-\lambda)$ is the set of v such that $\lim_{a\to\infty} \lambda(a) \cdot v$ exists.

Intuitively, $\lambda(a) \cdot V$ defines a one-parameter family of morphisms $V \to V$, and $V(\lambda)$ is those points which "converges" as $a \to 0$. For example, if $\lambda : a \mapsto \begin{pmatrix} a^2 & \\ & a^{-1} \end{pmatrix}$, then $\lambda(a) \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a^2 x \\ a^{-1} y \end{pmatrix}$, so $V(\lambda)$ is the x-axis and $V(-\lambda)$ is the y-axis. Intuitively $V(\lambda)$ are the components without negative exponents, and $V(-\lambda)$ are those without positive exponents.

LEM 3.10 V_λ is closed in V, and $V(\lambda) \cap V(-\lambda)$ is the set of fixed points under action of λ.

3.3 additive functions

DEF 3.11 **additive function** An **additive function** on a linear algebraic group G is a homomorphism of algebraic groups $f : G \to \mathbb{G}_a$. The additive functions form a subspace $\mathcal{A}(G)z$ of $k[G]$. If G is an F-group then $\mathcal{A}(F)$ denotes the F-vector space of additive functions defined over F.

Assume that $\operatorname{char} k = p > 0$ and F is perfect, i.e. $F^p = F$. Define a ring R as a "twisted" polynomial ring: the underlyinngn abelian group is $F[t]$, while the multiplication is

$$\left(\sum a_i t^i\right)\left(\sum b_j t^j\right) = \sum a_i\left(\varphi^i b_j\right) t^{i+j}$$

where $\varphi : x \mapsto x^p$ is the Frobenius isomorphism.

Left and right ideals in R are all principal and R is left and right noetherian. Therefore, every finitely generated left- or right-R-module is a direct sum of cyclic modules, either free or torsion. $\mathbb{A}(F)$ can then be seen as a left R-module, by

$$\left(\sum a_i t^i\right) \cdot f = \sum a_i f^{p^i}.$$

If $p = 0$ then $R = F$ and $\mathbb{A}(F)$ is an R-module.

As an example, the additive F-functions on G_a^n are the additive polynomials in $F[t_1, \cdots, t_n]$. The only such polynomials are linear combinations of monomials of the form $t_i^{p^j}$, which form a free R-module with basis t_i.

LEM 3.12 Let G be an F-group.

1. If G is connected, then the R-module $\mathbb{A}(F)$ is torsion free.
2. If $f_1, \cdots, f_s$ are elements of $\mathbb{A}(F)$ that are linearly independent over R, then they are algebraically independent over k.

3.4 elementary unipotent groups

DEF 3.13 elementary vector groups

Say a unipotent linear algebraic group G is **elementary** if it is abelian and, if $\operatorname{char} k = p > 0$, its elements have order dividing p. G is a **vector group** if it is isomorphic to some G_a^n.

THM 3.14 The following propertie of a linear algebraic group G are equivalent:

1. G is elementary unipotent;
2. $\mathbb{A}(G)$ is a finitely generated R-module and generate as an algebra the whole $k[G]$;
3. G is a vector group if $p = 0$, or the product of a vector group and some $(\mathbb{Z} / p\mathbb{Z})^n$ if $p > 0$.

With all the notions introduced, Proposition 3.2 implies that every connected linear algebraic group must be toral or elementary unipotent. Therefore,

COR 3.15 A connected linear algebraic group of dimension one is isomorphic to either G_a or G_m.

4

Section 4
derivations, differentials, Lie algebras

4.1 derivations and tangent spaces

DEF 4.1 derivation

Suppose R is a commutative ring, A an R-algebra and M a left A-module. An R-**derivation** is an R-linear map $D : A \to M$ satisfying the Leibniz rule: $D(ab) = aD(b) + bD(a)$. The set of derivations is denoted $\mathrm{Der}_R(A, M)$, and form a left A-module.

If $\varphi : A \to B$ is a homomorphism of R-algebras and N is a B-module, pullback along φ gives $\varphi_0 : \mathrm{Der}_R(B, N) \to \mathrm{Der}_R(A, N)$ with kernel $\mathrm{Der}_A(B, N)$.

DEF 4.2 tangent spaces

Let X be an affine variety. If $x \in X$, define the **tangent space** $T_x X$ to be the k-vector space of derivations $\mathrm{Der}_k(k[X], k_x)$, where $k_x = k[X] / \mathfrak{m}_x$ is isomorphic to k as a ring, and viewed as a $k[X]$-module via $f \mapsto f(x)$.

If $\varphi : X \to Y$ is a morphism of affine algebraic varieties, then $\varphi^* : k[Y] \to k[X]$ pulls back to a map $\varphi_0^* : T_x X \to T_{\varphi x} Y$, denoted $\mathrm{d}\varphi_x$ and called the **differential** of φ at $x \in X$.

LEM 4.3 alternative definitions of tangent spaces

The following descriptions of tangent spaces are equivalent:

1. As the space of derivations $\mathrm{Der}_k(k[X], k_x)$.
2. As the dual of $\mathfrak{m}_x / \mathfrak{m}_x^2$, by noticing derivations vanish on $\mathfrak{m}_x^2$.
3. As $\mathrm{Der}_k(\mathcal{O}_x, k)$, where $\mathcal{O}_x = \mathcal{O}_{X,x}$ is the stalk of the sheaf of regular functions at x and $k \cong \mathcal{O}_x / \mathcal{M}_x$ is the residue field of $\mathcal{O}_x$. This description works for general varieties.
4. As the projective limit $\varprojlim T_x U$ for affine open charts $U \ni x$. This description works for general varieties.

basically, the infinitesimal / local variant of the first description

The third description tells us that if $\varphi : X \to Y$ is an isomorphism of X onto an affine open subvariety of Y, then $\mathrm{d}\varphi_x$ is an isomorphism.

DEF 4.4 smoothness

Say X is **smooth** at x, or x is a **simple point** of X, if $\dim T_x X = \dim X$. X is **smooth** or **non-singular** if X is smooth at all points, or all points of X are simple.

4.2 differentials, separability

Suppose R is a commutative ring and A a commutative R-algebra. Let $m : A \otimes_R A \to A$ be the algebra multiplication map, and $I = \ker m$. I is generated by elements of the form $a \otimes 1 - 1 \otimes a$, and $A \otimes A / I \cong A$.

DEF 4.5

The **module of differentials** $\Omega_{A/R}$ is defined as I / I^2. This is an $A \otimes A$-module, but it's annihilated by I, so we may and shall view it as an A-module, by $a \cdot v = (a \otimes 1) \cdot v$.

If A is the ring of functions over a space X, then I represent all functions of the form $f(x) - f(y)$, and I / I^2 decodes the first-order behaviour of such functions. Denote by $\mathrm{d}a$ or $\mathrm{d}_{A/R}a$ the image of $a \otimes 1 - 1 \otimes a$ in $\Omega_{A/R}$, then d is a derivation in $\mathrm{Der}_R(A, \Omega_{A/R})$.

$\Omega_{A/R}$ is the universal module of R-derivations of A, in the sense that it is the unique (up to isomorphism) A-module with a derivation d such that for every A-module M the map $\Phi : \mathrm{Hom}_A(\Omega_{A/R}, M) \to \mathrm{Der}_R(A, M)$, $\varphi \mapsto \varphi \circ \mathrm{d}$ is an isomorphism of A-modules.

If $\varphi : A \to B$ is an R-algebra homomorphism, there is a unique homomorphism of A-modules $\varphi^0 : \Omega_{A/R} \to \Omega_{B/R}$ with $\varphi^0 \circ \mathrm{d}_{A/R} = \mathrm{d}_{B/R} \circ \varphi$. In this sense, the above mentioned map Φ is natural.

LEM 4.6

If A is a quotient of a polynomial algebra over R, say $A = R[t_1, \cdots, t_m] / (f_1, \cdots, f_n)$, then $\mathrm{d}t_i$ generate $\Omega_{A/R}$ as an A-module.

If $\varphi : A^m \to \Omega_{A/R}$, $\varphi(e_i) = \mathrm{d}t_i$, then $\ker \varphi$ is the submodule generated by $\sum_{i=1}^m \left(\frac{\mathrm{d}}{\mathrm{d}t_i} f_j(\boldsymbol{t}) \right) e_i$.