

## 3. LIE ALGEBRAS

Now we introduce the Lie algebra of an algebraic group. First, we need to do some more algebraic geometry to understand the tangent space to an algebraic variety at a point.

**3.1. Derivations.** Let  $A$  be a commutative  $k$ -algebra. Let  $M$  be a left  $A$ -module. A *derivation* of  $A$  in  $M$  is a linear map  $D : A \rightarrow M$  such that

$$D(ab) = aD(b) + bD(a)$$

for all  $a, b \in A$ . This implies:  $D(c \cdot 1) = 0$  for all scalars  $c \in k$ . We write  $\text{Der}(A, M)$  for the set of all derivations of  $A$  in  $M$ . It is obviously a left  $A$ -module with  $(a \cdot D)(b) = a(D(b))$ .

Now take the special case that  $M = A$ . The elements of  $\text{Der}(A, A)$  are called simply *derivations* of  $A$ . Moreover, there is a little more structure here: if  $D, D'$  are two derivations of  $A$ , then you can look at

$$[D, D'] = DD' - D'D$$

which is another linear map from  $A$  to  $A$ . It is a derivation! Indeed:

$$\begin{aligned} (DD' - D'D)(ab) &= D(aD'(b) + bD'(a)) - D'(aD(b) + bD(a)) \\ &= D(a)D'(b) + aD(D'(b)) + D(b)D'(a) + bD(D'(a)) \\ &\quad - D'(a)D(b) - aD'(D(b)) - D'(b)D(a) - bD'(D(a)) \\ &= a(DD' - D'D)(b) + b(DD' - D'D)(a). \end{aligned}$$

This gives the set  $\text{Der}(A, A)$  the structure of a *Lie algebra*.

((Aside: definition of a Lie algebra. It is a vector space  $\mathfrak{g}$  with a bilinear operation  $[\cdot, \cdot] : \mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$  satisfying anticommutativity

$$[X, X] = 0 \text{ for all } X \in \mathfrak{g},$$

and the Jacobi identity

$$[X, [Y, Z]] + [Y, [Z, X]] + [Z, [X, Y]] = 0 \text{ for all } X, Y, Z \in \mathfrak{g}.$$

Note the multiplication on a Lie algebra is usually *not* associative, and there is never a unit!!! For example for any vector space  $V$ , we have the Lie algebra  $\mathfrak{gl}(V)$  consisting of all linear endomorphisms  $X : V \rightarrow V$ , with Lie bracket  $[X, Y] = X \circ Y - Y \circ X$  being the commutator. The Lie algebra  $\text{Der}(A, A)$  constructed above is a subalgebra of  $\mathfrak{gl}(A)$ .)

**Exercise 3.1.** (4) Verify directly that for a vector space  $V$ , the set  $\mathfrak{gl}(V)$  of endomorphisms of  $V$  under the commutator satisfies the axioms of a Lie algebra (i.e. check the Jacobi identity if you never did this before!).

**3.2. Tangent space.** Let  $X$  be a closed subvariety of  $\mathbb{A}^n$ . Let  $k[X] = k[T_1, \dots, T_n]/I$  where  $I = I(X)$ . Suppose  $I$  is generated by polynomials  $f_1, \dots, f_s$ . Let  $x \in X$  and let  $L$  be a line in  $\mathbb{A}^n$  passing through  $x$ . Its points can be written as  $x + tv$  for  $v = (v_1, \dots, v_n)$  a direction vector and  $t \in k$ . The points on this line that intersect  $X$  are parametrized by the  $t$  that solve the equations

$$f_i(x + tv) = 0 \quad (1 \leq i \leq s).$$

Of course,  $t = 0$  is one such solution. Let us call  $L$  a *tangent line* and  $v$  a *tangent vector* to  $X$  at  $x$  if  $t = 0$  is a “multiple root” to these equations.

To formulate this precisely, let  $D_i$  be partial differentiation with respect to  $T_i$  (this is a derivation of the algebra  $k[T] = k[T_1, \dots, T_n]$ !). Then, we have the Taylor expansion of  $f_i(x + tv)$  at  $t = 0$ :

$$f_i(x + tv) = t \sum_{j=1}^n v_j (D_j f_i)(x) + t^2(\dots).$$

By “ $t = 0$  is a multiple root” we of course mean that the leading term of this Taylor expansion is zero, i.e.

$$\sum_{j=1}^n v_j (D_j f_i)(x) = 0$$

for all  $i = 1, \dots, s$ . The set of tangent vectors  $v$  to  $X$  at  $x$  – i.e. the *tangent space* to  $X$  at  $x$  – is precisely the set of solutions  $v$  to this equation.

**Example 3.2.** (1) If  $X = \mathbb{A}^n$  itself, there are no  $f_i$ 's so all  $v \in k^n$  solve the equations, so the tangent space to  $\mathbb{A}^n$  at  $x$  is the vector space  $k^n$ .

(2) If  $X = V(T_1^2 + T_2^2 - 1)$  in  $\mathbb{A}^2$ , the tangent space at  $x$  is all  $v_1, v_2$  such that

$$2v_1x_1 + 2v_2x_2 = 0$$

Usually, this is just a copy of  $k$ , except in characteristic 2 when it's all of  $k^2$ . . . . Characteristic 2 goes wrong because in that case  $T_1^2 + T_2^2 - 1 = (T_1 + T_2 + 1)^2$  and we haven't written down the ideal of  $X$  correctly!

Now we want to reformulate the notion of tangent space more algebraically. Going back to the above setup, let

$$D_v = \sum_j v_j D_j,$$

another derivation of  $k[T]$ . Then  $v$  is a tangent vector to  $X$  at  $x$  if and only if  $(D_v f_i)(x) = 0$  for all  $i = 1, \dots, s$ . So the tangent space  $T_x X$  to  $X$  at  $x$  is the vector space

$$\begin{aligned} T_x(X) &:= \{v \in k^n \mid (D_v f_i)(x) = 0 \text{ for all } i = 1, \dots, s\} \\ &= \{v \in k^n \mid (D_v f)(x) = 0 \text{ for all } f \in I(X)\}. \end{aligned}$$

Let  $M_x$  denote the maximal ideal in  $k[T]$  of all functions vanishing at  $x$ . Then, if  $v$  is a tangent vector,  $D_v I(X) \subseteq M_x$ . So the linear map  $f \mapsto (D_v f)(x)$  factors to induce a well-defined linear map

$$\bar{D}_v : k[X] \rightarrow k[T]/M_x.$$

Let us let  $k_x = k[T]/M_x = k[X]/(M_x + I(X))$ . It is a  $k[X]$ -module isomorphic to  $k$ , with action  $fc = f(x)c$  for  $f \in k[X]$  and  $c \in k$ . So we get from  $v$  a derivation  $\bar{D}_v$  of  $k[X]$  in the  $k[X]$ -module  $k_x$ , i.e.  $\bar{D}_v$  satisfies

$$D(fg) = f(x)D(g) + g(x)D(f)$$

for all  $f, g \in k[X]$ . I will call such elements of  $\text{Der}(k[X], k_x)$  *point derivations* (for the point  $x$ ).

Conversely, any such point derivation  $\bar{D} \in \text{Der}(k[X], k_x)$ , can be lifted (via the map  $k[T] \rightarrow k[X]$ ) to a point derivation  $D$  of  $k[T]$  that is zero on  $I(X)$ . Now it is not hard to check that every such point derivation of the polynomial algebra is of the form  $f \mapsto (D_v f)(x)$  for some  $v \in k^n$  with  $D_v I(X) \subseteq M_x$ . We deduce that the map  $D_v \mapsto \bar{D}_v$  is an isomorphism

$$T_x(X) \rightarrow \text{Der}(k[X], k_x).$$

Let us henceforth *identify*  $T_x(X)$  with the vector space  $\text{Der}(k[X], k_x)$  of all point derivations. The advantage of this abstract definition is that it is independent of the choice of the embedding of  $X$  in  $\mathbb{A}^n$ .

Now let  $\phi : X \rightarrow Y$  be a morphism of affine varieties. We have the comorphism  $\phi^* : k[Y] \rightarrow k[X]$ , and composing with this induces a map

$$d\phi_x : T_x(X) = \text{Der}(k[X], k_x) \rightarrow T_{\phi(x)}(Y) = \text{Der}(k[Y], k_{\phi(x)}), f \mapsto f \circ \phi^*.$$

This is called the differential of  $\phi$  at  $x$ ,

If  $\psi : Y \rightarrow Z$  is another map, the chain rule gives

$$d(\psi \circ \phi)_x = d\psi_{\phi(x)} \circ d\phi_x$$

So in particular, the differential of an isomorphism is an isomorphism of the tangent spaces.

**Lemma 3.3.** *Let  $\phi$  be an isomorphism of an affine variety  $X$  onto an open subvariety of an affine variety  $Y$ . Then,  $d\phi_x$  is an isomorphism of  $T_x(X)$  onto  $T_{\phi(x)}(Y)$ .*

*Proof.* It suffices to consider the special case that  $X$  is equal to the principal open subset  $D(f)$  of  $Y$  for some  $f \in k[Y]$  with  $f(x) \neq 0$ . So  $k[X] = k[Y]_f$ . Then this amounts to showing that  $\text{Der}(k[Y], k_x) \cong \text{Der}(k[Y]_f, k_x)$ . Restriction of functions gives a map  $\text{Der}(k[Y]_f, k_x) \rightarrow \text{Der}(k[Y], k_x)$ . We construct an inverse map as follows: given  $D \in \text{Der}(k[Y], k_x)$ , Define

$$D(g/f) = (f(x)D(g) - g(x)D(f))/f(x)^2,$$

which makes sense as  $f(x) \neq 0$ . □

The lemma allows us to define the tangent space at a point  $x$  in an *arbitrary* variety as follows. Let  $x \in X$ , and pick affine open neighbourhoods  $U, V$  of  $x$  with  $x \in U \subseteq V$ . By the lemma,  $T_x(U) \cong T_x(V)$  (canonically). So let us define  $T_x(X)$  to be  $T_x(U)$ , giving us a well-defined vector space up to canonical isomorphism. For a morphism  $\phi : X \rightarrow Y$  of arbitrary varieties, it is easy to make sense of the differential

$$d\phi_x : T_x(X) \rightarrow T_{\phi(x)}(Y)$$

too (exercise!).

**Exercise 3.4.** (5) Let  $X, Y$  be algebraic varieties,  $x \in X, y \in Y$ . Prove that  $T_{(x,y)}(X \times Y) \cong T_x(X) \oplus T_y(Y)$  as vector spaces

**3.3. Separability.** Now we are going to prove some slightly technical algebraic results about derivations. Recall that for a  $k$ -algebra  $A$  and an  $A$ -module  $M$ , we wrote  $\text{Der}(A, M)$  for the  $k$ -linear derivations of  $A$  on  $M$ . Let us now denote this by  $\text{Der}_k(A, M)$  since we are going to look at what happens when the field changes.

Let  $m : A \otimes_k A \rightarrow A$  be the multiplication. Let  $I = \ker m$ , the ideal generated by all  $a \otimes 1 - 1 \otimes a$  ( $a \in A$ ). Define the *module of differentials*  $\Omega_{A/k}$  be

$$\Omega_{A/k} = I/I^2.$$

This is an  $A \otimes A$ -module annihilated by  $I$ , hence it is an  $A$ -module since  $A \cong A \otimes A/I$ . Let  $da$  denote the image of  $a \otimes 1 - 1 \otimes a$  in  $\Omega_{A/k}$ . Note the map  $d : a \mapsto da$  is a derivation of  $A$  in the  $A$ -module  $\Omega_{A/k}$ :

$$ad(b) + d(a)b = a(b \otimes 1 - 1 \otimes b) + (a \otimes 1 - 1 \otimes a)b + I^2 = ab \otimes 1 - 1 \otimes ab + I^2 = d(ab).$$

The  $da$  for  $a \in A$  generate  $\Omega_{A/k}$  as an  $A$ -module. You should think of  $\Omega_{A/k}$  as the *universal module for derivations of  $A$* :

**Theorem 3.5.** *Suppose  $M$  is an  $A$ -module and  $D : A \rightarrow M$  is a derivation. Then there exists a unique  $A$ -module homomorphism  $\phi : \Omega_{A/k} \rightarrow M$  such that  $D = \phi \circ d$ , i.e. the map*

$$\text{Hom}_A(\Omega_{A/k}, M) \xrightarrow{\sim} \text{Der}_k(A, M), \quad \phi \mapsto \phi \circ d$$

*is an isomorphism.*

*Proof.* Define a linear map  $\psi : A \otimes A \rightarrow M$  by  $\psi(a \otimes b) = bD(a)$ . You check that for arbitrary elements  $x, y \in A \otimes A$ ,

$$\psi(xy) = m(x)\psi(y) + m(y)\psi(x),$$

hence  $\psi$  vanishes on  $I^2$ . Therefore it induces a map  $\phi : \Omega_{A/k} \rightarrow M$  which is actually an  $A$ -module map, such that  $\phi(da) = \psi(a \otimes 1 - 1 \otimes a) = D(a)$  (here I have used that  $D(1) = 0$  which follows from the derivation rule). For uniqueness, you use the fact that the  $da$  generate  $\Omega_{A/k}$  as an  $A$ -module.  $\square$

The theorem gives a universal property for the pair  $(\Omega_{A/k}, d)$  which (as usual) characterizes it up to a unique  $A$ -module isomorphism. To give some examples of the structure of the  $A$ -module  $\Omega_{A/k}$ , we need:

**Exercise 3.6.** (6) Let  $A = k[T_1, \dots, T_n]/(f_1, \dots, f_s)$ . Let  $t_i$  be the image of  $T_i$  in  $A$ . Show that the  $dt_i$  generate  $\Omega_{A/k}$  as an  $A$ -module, and moreover, the kernel of the  $A$ -module homomorphism

$$A^n = \bigoplus_{i=1}^n Ae_i \rightarrow \Omega_{A/k}, e_i \mapsto dt_i$$

is the submodule  $K$  of  $A^n$  generated by  $\sum_{i=1}^n (D_i f_j(t))e_i$  for  $j = 1, \dots, s$ . (Hint: show that the  $A$ -module  $A^n/K$  satisfies the universal property in the theorem.)

Using the exercise, you can work out lots of examples:

**Example 3.7.** (1) The first example is the case  $A = k[T_1, \dots, T_n]$  itself.

In this case,  $\Omega_{A/k}$  is the *free*  $A$ -module on basis  $dT_1, \dots, dT_n$ .

(2) Let  $A = k[T_1, T_2]/(T_1^2 - T_2^3)$ , let  $t_i$  be the image of  $T_i$ . Then  $\Omega_{A/k} \cong Ae_1 \oplus Ae_2/(2t_1e_1 - 3t_2^2e_2)$ . This is not a free  $A$ -module!

(3) Let  $A$  be an integral domain with quotient field  $E$ . Then,  $\Omega_{E/k} \cong E \otimes_A \Omega_{A/k}$ . Proof: We have the derivation  $d : A \rightarrow \Omega_{A/k}$  which induces a derivation  $\bar{d} : E \rightarrow E \otimes_A \Omega_{A/k}$ . Let us check that  $E \otimes_A \Omega_{A/k}$  together with  $\bar{d}$  has the correct universal property to be  $\Omega_{E/k}$ . Take an  $E$ -module  $M$  and a derivation  $\bar{D} : E \rightarrow M$ . Its restriction to  $A$  gives us  $D : A \rightarrow M$ , hence there is a unique  $A$ -module homomorphism  $\phi : \Omega_{A/k} \rightarrow M$  with  $D = \phi \circ d$ . Hence since  $M$  is an  $E$ -module, there is a unique  $E$ -module homomorphism  $\bar{\phi} : E \otimes_k \Omega_{A/k} \rightarrow M$  with  $\bar{D} = \bar{\phi} \circ \bar{d}$ . We are done.

(4) Suppose that  $E = k(x_1, \dots, x_n)$  is a finitely generated field extension of  $k$ . By (3) and (1),  $\Omega_{E/k}$  is the  $E$ -vector space spanned by  $dx_1, \dots, dx_n$ . In particular, it is a finite dimensional vector space over  $E$ .

((Aside: Before proceeding, I want to recalling some definitions and theorems from field theory. Let  $E \subseteq F$  be a field extension. It is a *separable* field extension if either  $\text{char } E = 0$  or else  $\text{char } E = p > 0$  and the  $p$ th powers of elements  $x_1, \dots, x_n \in F$  linearly independent over  $E$  are again linearly independent over  $E$ . In the case of finite dimensional field extensions, i.e. if  $\dim_E F < \infty$ , this is equivalent to the more familiar notion from Galois theory: the minimal polynomials  $m_x$  of all  $x \in F$  over  $E$  do not have multiple roots, i.e. satisfy  $m'_x(x) \neq 0$ .

For a finitely generated extension  $E \subseteq F$ , there is a theorem that shows that  $E \subseteq F$  is separable and only if  $E$  is a finite dimensional separable extension of  $E(t_1, \dots, t_n)$  for algebraically independent  $t_i \in F$ .)

Now for the remainder of the section, we will be concerned with the following situation: we are given finitely generated field extensions  $k \subseteq E, F$  of  $k$  with  $E \subseteq F$ . There is an exact sequence

$$0 \longrightarrow \text{Der}_E(F, F) \longrightarrow \text{Der}_k(F, F) \longrightarrow \text{Der}_k(E, F).$$

The first map is the obvious inclusion (clearly  $E$ -linear maps are  $k$ -linear). The second map is induced by restriction of functions from  $F$  to  $E$ . Note that any  $D \in \text{Der}_E(F, F)$  maps elements of  $E \subset F$  to zero, and conversely, any  $f \in \text{Der}_k(F, F)$  that maps elements of  $E$  to zero is  $E$ -linear because  $D(ef) = eD(f)$ . So the kernel of the second map, which obviously consists of all  $k$ -derivations from  $F$  to  $F$  that map  $E$  to zero, is exactly the image of the first map, checking exactness.

Hence applying the isomorphism in 3.5, we have an exact sequence

$$0 \longrightarrow \text{Hom}_F(\Omega_{F/E}, F) \longrightarrow \text{Hom}_F(\Omega_{F/k}, F) \longrightarrow \text{Hom}_E(\Omega_{E/k}, F).$$

Note moreover by adjointness of tensor and hom that

$$\text{Hom}_F(F \otimes_E \Omega_{E/k}, F) \rightarrow \text{Hom}_E(\Omega_{E/k}, F)$$

as  $F$ -vector spaces. Putting all this together, we obtain an exact sequence

$$0 \longrightarrow \text{Hom}_F(\Omega_{F/E}, F) \longrightarrow \text{Hom}_F(\Omega_{F/k}, F) \longrightarrow \text{Hom}_F(F \otimes_E \Omega_{E/k}, F)$$

of finite dimensional  $F$ -vector spaces. Dualizing we get

$$F \otimes_E \Omega_{E/k} \xrightarrow{\alpha} \Omega_{F/k} \xrightarrow{\beta} \Omega_{F/E} \longrightarrow 0.$$

This is going to be fundamental, so let us make sure we understand the maps explicitly. The first map  $\alpha$  sends  $1 \otimes d_{E/k}a$  to  $d_{F/k}a$  (viewing  $a \in E$  as an element instead of  $F$ ). The second map  $\beta$  is induced by the derivation  $d_{F/E} : F \rightarrow \Omega_{F/E}$  according to the universal property of  $\Omega_{F/k}$ .

**Lemma 3.8.** *If  $F$  is a finite dimensional separable extension of  $E$  then  $\alpha$  is injective.*

*Proof.* By the above discussion, this is equivalent to the map  $\text{Der}_k(F, F) \rightarrow \text{Der}_k(E, F)$  induced by restricting functions from  $F$  to  $E$  being surjective. Equivalently: any  $k$ -derivation from  $E$  to  $F$  can be extended to a derivation from  $F$  to  $F$ . It suffices to prove this in the case that  $F = E[T]/(f(T))$  where

$$f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$$

and (this is what separability means)  $f'(x) \neq 0$ , where  $x$  is the image under the quotient map of  $T$  in  $F$ .

Let  $D : E \rightarrow F$  be a derivation. To extend  $D$  to a derivation  $\bar{D}$  from  $F$  to  $F$ , we just need to decide what  $\bar{D}x$  should be: then the derivation formula means there is no choice for defining  $\bar{D}$  applied to any other element of  $F = E[x]$ . To decide on  $\bar{D}x$ , we need – for well-definedness – that  $\bar{D}f(x) = 0$ , i.e.

$$\bar{D}f(x) = f'(x)\bar{D}x + \sum (Da_i)x^i = 0.$$

Since  $f'(x) \neq 0$ , we can solve this equation for  $\bar{D}x$  in the field  $F$  so it is possible to extend...  $\square$

**Lemma 3.9.** *Let  $F = E(x)$ . Then,  $\dim_F \Omega_{F/E} \leq 1$ . Moreover,  $\Omega_{F/E} = 0$  if and only if  $F$  is a finite dimensional separable extension of  $E$ .*

*Proof.* There are two cases: when  $x$  is algebraic and when  $x$  is transcendental over  $E$ . In the transcendental case,  $\Omega_{F/E} = F \otimes_{E[x]} \Omega_{E[x]/E}$ , and  $\Omega_{E[x]/E}$  is the free  $E[x]$  module of rank one. So  $\dim_F \Omega_{F/E} = 1$ .

In the algebraic case, let  $f$  be the minimal polynomial of  $x$  over  $E$ . Then  $\Omega_{F/E} = F \otimes_{E[x]} \Omega_{E[x]/E}$ . But by the exercise,  $\Omega_{E[x]/E}$  is the  $E[x]$ -module  $E[x]/(f'(x))$ . If  $E \subseteq F$  is not separable, then  $f'(x) = 0$  and we again get that  $\Omega_{F/E}$  is one dimensional. Finally, if it is separable,  $f'(x) \neq 0$  and

$$\Omega_{F/E} \cong F \otimes_{E[x]} E[x]/(f'(x)) = 0$$

since it is generated by  $1 \otimes 1 = f'(x)^{-1} f'(x) \otimes 1 = f'(x)^{-1} \otimes f'(x) = 0$ .  $\square$

Here (at last) is the main point:

**Theorem 3.10.** *Let  $F = E(x_1, \dots, x_m)$  be a finitely generated field extension.*

- (i)  $\dim_F \Omega_{F/E} \geq \text{tr.deg.}_E F$ .
- (ii) *Equality holds if and only if  $F$  is a separable extension of  $E$ .*

*Proof.* Proceed by induction on  $d = \dim_F \Omega_{F/E}$ .

Consider first the case  $d = 0$ , so  $\Omega_{F/E} = 0$ . To get (i) and (ii), we just need to show that need to show that  $F$  is a finite dimensional separable extension of  $E$ . For this, we use induction on the number of generators  $m$  of  $F$  over  $E$ , the case  $m = 1$  being 3.9. Now suppose  $m > 1$ . Set  $E' = E(x_m)$ , so  $F = E'(x_1, \dots, x_{m-1})$ . Using the exact sequence

$$F \otimes_{E'} \Omega_{E'/E} \xrightarrow{\alpha} \Omega_{F/E} \xrightarrow{\beta} \Omega_{F/E'} \longrightarrow 0$$

we see that  $\Omega_{F/E'} = 0$  hence by induction  $F$  is a finite dimensional separable extension of  $E'$ . So by 3.8,  $\alpha$  is injective, whence  $\Omega_{E'/E} = 0$  and  $E'$  is a finite dimensional separable extension of  $E$ . Thus,  $F$  is a finite dimensional separable extension of  $E$ .

Now suppose  $d > 0$ . Pick  $x \in F$  with  $d_{F/E}x \neq 0$ . We have the exact sequence

$$F \otimes_{E'} \Omega_{E'/E} \xrightarrow{\alpha} \Omega_{F/E} \xrightarrow{\beta} \Omega_{F/E'} \longrightarrow 0$$

where  $E' = E(x)$ . Since  $\alpha(1 \otimes d_{E'/E}x) = d_{F/E}x \neq 0$ ,  $\Omega_{E'/E} \neq 0$ . So by 3.9,  $\dim_{E'} \Omega_{E'/E} = 1$  which means that  $\alpha$  is injective. So  $\dim_F \Omega_{F/E} = \dim_F \Omega_{F/E'} + 1$ . By induction,

$$\dim_F \Omega_{F/E} \geq \text{tr.deg.}_{E'} F + 1.$$

Since

$$\text{tr.deg.}_E F = \text{tr.deg.}_{E'} F + \text{tr.deg.}_E E' \leq \text{tr.deg.}_{E'} F + 1,$$

we get

$$\dim_F \Omega_{F/E} \geq \text{tr.deg.}_E F,$$

which is (i). With a little further argument along the same lines, you get (ii) ...  $\square$

As a corollary, we obtain the *differential criterion for separability*:

**Corollary 3.11.** *Assume that  $E \subseteq F$  are finitely generated extensions of  $k$  (which is algebraically closed). Then,  $F$  is a separable extension of  $E$  if and only if the natural map  $\text{Der}_k(F, F) \rightarrow \text{Der}_k(E, F)$  is surjective.*

*Proof.* As above,  $\text{Der}_k(F, F) \rightarrow \text{Der}_k(E, F)$  is surjective if and only if the map

$$\alpha : F \otimes_E \Omega_{E/k} \rightarrow \Omega_{F/k}$$

from 3.8 is injective. Consider the exact sequence

$$F \otimes_E \Omega_{E/k} \xrightarrow{\alpha} \Omega_{F/k} \xrightarrow{\beta} \Omega_{F/E} \longrightarrow 0.$$

Since  $k$  is algebraically closed, every extension of  $k$  is separable, so by the theorem  $\dim_F F \otimes_E \Omega_{E/k} = \dim_E \Omega_{E/k} = \text{tr.deg.}_k E$ ,  $\dim_F \Omega_{F/k} = \text{tr.deg.}_k F$ . Hence,  $\alpha$  is injective if and only if

$$\dim_F \Omega_{F/E} = \text{tr.deg.}_k F - \text{tr.deg.}_k E = \text{tr.deg.}_E F.$$

By the theorem, this is if and only if  $E \subseteq F$  is separable.  $\square$

**3.4. Simple points.** We are nearly ready to prove a fundamental geometric theorem. We still need a little more linear algebra...

Suppose that  $A$  is an integral domain. Let  $F$  be its field of fractions, and let  $A_f$  be its localization at a non-zero  $f \in A$ . View  $A_f$  as a subalgebra of  $F$ . I want to think about finitely generated  $A$ -modules given by generators and relations. Let  $R = (r_{i,j})$  be an  $s \times n$  matrix with entries in  $A$ . Consider the  $A$ -module

$$M_A(R) := \bigoplus_{j=1}^n Ae_j / \langle \sum_{j=1}^n r_{i,j}e_j \mid i = 1, \dots, s \rangle.$$

So this is the quotient of the free  $A$ -module of rank  $n$  by the relations given by the rows of the matrix  $R$ . For example, if  $R$  is the matrix

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

then  $M_A(R)$  is the free  $A$ -module of rank  $(n - r)$ . If we have an invertible  $s \times s$ -matrix  $Y$  with entries in  $A$ , then the change of basis argument gives that  $M_A(YR) \cong M_A(R)$ . Similarly, if  $Z$  is an invertible  $n \times n$ -matrix,  $M_A(RZ) \cong M_A(R)$ . Now, by linear algebra, we can find invertible matrices  $Y$  and  $Z$  with entries in  $F$  such that

$$R = Y \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} Z,$$

where  $r$  is the rank of  $R$ . Putting all entries of  $Y$  and  $Z$  over a common denominator, we may assume that  $Y, Z$  with entries in  $A_f$  for some  $0 \neq f \in A$ . Obviously, the localization  $M_A(R)_f := A_f \otimes_A M_A(R)$  of the  $A$ -module  $M_A(R)$  at  $f$  is the  $A_f$ -module given by the same generators and relations, i.e.

$$M_A(R)_f = M_{A_f}(R).$$

Now we see that  $M_A(R)_f$  is a free  $A_f$ -module of rank  $(n - r)$ .

Now let us put everything together. Assume that  $X$  is an irreducible affine variety. Recall for  $x \in X$  that we write  $k_x$  for the  $k[X]$ -module  $k[X]/M_x$ . This is equal to  $k$  as a vector space with action  $a.c = a(x)c$ . The tangent space to  $X$  at  $x$  is the vector space

$$\begin{aligned} T_x(X) &= \text{Der}_k(k[X], k_x) \cong \text{Hom}_{k[X]}(\Omega_{k[X]/k}, k_x) \\ &\cong \text{Hom}_k(k_x \otimes_{k[X]} (k_x \otimes_{k[X]} \Omega_{k[X]/k}, k). \end{aligned}$$

We write  $\Omega_X$  instead of  $\Omega_{k[X]/k}$  and for a  $k[X]$ -module  $M$  we write  $M(x)$  for the vector space  $k_x \otimes_{k[X]} M = M/M_x M$ . So according to the above isomorphism,  $\Omega_X(x) \cong T_x(X)^*$ . For this reason,  $\Omega_X$  can be called the *cotangent space* to  $X$  at  $x$ .

Assume that  $k[X] = k[T_1, \dots, T_n]/\langle f_1, \dots, f_s \rangle$ . Let  $R$  be the the  $s \times n$  matrix  $(D_j f_i(t))$ . So,  $\Omega_X \cong M_{k[X]}(R)$ . Then you see that

$$T_x(X)^* \cong \Omega_X(x) = M_{k[X]}(R)(x) = M_k(R(x)),$$

where  $R(x)$  is the matrix obtained by evaluating entries at  $x$ .

- Lemma 3.12.**
- (i)  $\dim_{k(X)} M_{k(X)}(R) = \dim X$ .
  - (ii)  $\dim T_x(X) \geq \dim X$  with equality for all  $x$  lying in a non-empty open subset of  $X$ .
  - (iii) If  $x \in X$  is a point such that  $\dim_k T_x(X) = \dim X$ , then there is  $f \in k[X]$  with  $f(x) \neq 0$  such that  $M_{k[X]}(R)_f$  is a free  $k[X]_f$ -module of rank  $\dim X$  with basis given by  $\dim X$  out of the images of the  $e_i$ .

*Proof.* (i) Since  $k$  is algebraically closed,  $k(X)$  is a separable extension of  $k$ . So 3.10 tells us that  $\dim X = \dim_{k(X)} \Omega_{k(X)/k}$ . But  $\Omega_{k(X)/k} \cong k(X) \otimes_{k[X]} \Omega_X \cong M_{k(X)}(R)$ .

(ii) We have shown that  $\dim X = \dim_{k(X)} M_{k(X)}(R) = n - \text{rank}(R)$  and  $\dim T_x(X) = \dim M_k(R(x)) = n - \text{rank}(R(x))$ . So we need to show that  $\text{rank}(R) \geq \text{rank}(R(x))$  with equality for  $x$  lying in a non-empty open subset of  $X$ . Let  $r = \text{rank}(R(x))$ . Then there is an  $r \times r$ -minor of the matrix  $R(x)$  with non-zero determinant. This is the determinant of the corresponding  $r \times r$  minor of  $R$  evaluated at  $x$ , so  $R$  has an  $r \times r$  minor with non-zero determinant too. Hence,  $\text{rank } R \geq r$ .

Now suppose that  $\text{rank } R = s$ . Then there is an  $s \times s$  minor of  $R$  with non-zero determinant. Let  $a_1, \dots, a_t$  be all such non-zero determinants. If  $a_i(x) \neq 0$ , then  $R(x)$  also has an  $s \times s$  minor with non-zero determinant, hence  $\text{rank } R(x) = s$ . We deduce that the set of all points  $x$  such that

$\text{rank } R(x) = s$  is the union of the principal open sets  $D(a_i)$ , a non-empty open subset of  $X$ .

(iii) In view of (i), the rank of the matrix  $R$  is  $r = n - \dim X$ . Some  $r \times r$ -minor of  $R(x)$  has non-zero determinant; reordering if necessary, we can assume that  $\det((r_{i,j}(x))_{1 \leq i,j \leq r}) \neq 0$ . Set  $f = \det((r_{i,j})_{1 \leq i,j \leq r})$ , so  $f(x) \neq 0$ . On localizing at  $f$ , the matrix  $R$  becomes equivalent to

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

by linear algebra. □

Now let  $X$  be an arbitrary irreducible variety. Call a point  $x \in X$  a *simple point* if  $\dim T_x(X) = \dim X$ . Here is the main theorem:

**Theorem 3.13.** (i) *If  $x$  is a simple point, there is an affine open neighbourhood  $U$  of  $x$  such that  $\Omega_U$  is a free  $k[U]$ -module on basis*

$$dg_1, \dots, dg_{\dim X}$$

*for suitable  $g_i \in k[U]$ .*

- (ii) *The simple points of  $X$  form a non-empty open subset of  $X$ .*  
 (iii) *For any  $x \in X$ ,  $\dim T_x X \geq \dim X$ .*

*Proof.* Obviously it is enough to treat the case that  $X$  is affine, when it follows from the lemma. □

Call an irreducible variety  $X$  *smooth* if all its points are simple points.

**Exercise 3.14.** (7) Suppose that  $X$  is an affine variety and  $\Omega_X$  is a free  $k[X]$ -module. Show that  $X$  is smooth.