8. Algebraic Schemes for Cryptosystems

The above title is a kind of pun since we will discuss the geometric objects called Algebraic Schemes which also give us algebraic schemes (in the "English" sense) for cryptosystems. All the groups discussed so far turn out to be special cases of certain groups that are introduced in this section.

The fundamental problem studied in arithmetic algebraic geometry is the solution of systems of algebraic equations. The notion of an Algebraic Scheme is the essential geometric notion that incorporates this question. We then introduce the notion of vector group schemes and the K-group of such objects. With some additional constraints these are the groups that seem to arise in many cryptographic contexts.

While we cannot hope to introduce all the algebraic geometry and commutative algebra that is necessary to study these K-groups here, we give the fundamental definitions and some important examples. We will also not give proofs as the subject is too vast to be covered here. When we apply this theory to hyper-elliptic curves in the next section we will be more precise.

8.1. **Finite rings.** We recall some basic facts about finite commutative rings with identity (and $1 \neq 0$). (The adventurous reader may like to explore which parts of this entire section can be carried over to the non-commutative case). The reader can prove these results from first principles.

(1) In any finite ring there are finitely many ideals and in particular there are finitely many maximal ideals. In other words such a ring is "semi-local".
(2) Any prime ideal in a finite ring is maximal.
(3) (Analogue of Chinese Remainder Theorem). Any finite ring is a product of finite *local* rings; i. e. finite rings which have only one maximal ideal.
(4) In a finite local ring every element is either a unit or nilpotent. Moreover, a finite local ring has p^n elements for some prime p and some integer n.
(5) The *residue field* of a finite local ring is the quotient of the ring by its maximal ideal. This is a finite field.
(6) An element of a finite local ring is a unit if and only if its image in the residue field is non-zero.

8.2. **Functors of points.** Suppose that we are given a system S of p polynomial equations in q variables. To every finite ring A we associate the set $S(A)$ of all q-tuples $(a_1, \ldots, a_q)$ of elements of A that satisfy this system of equations. This is an example of a *functor* F from finite rings to finite sets; i. e. for every ring A we associate a finite set $F(A)$ such that if $A \to B$ is a ring homomorphism then we have a natural map $F(A) \to F(B)$ so that composition of ring homomorphisms goes to composition of set maps and the identity ring homomorphism goes to the identity map.

Giving a system T that is "derived" from the system S by substituting the variables by polynomial functions of another set of r variables is a natural operation on systems of equations. The analogous notion is that of a morphism of functors (also called a *natural transformation*) $F \to G$. This is a way of giving a map $F(A) \to G(A)$ so that for any ring homomorphism $A \to B$ we get a *commutative diagram* (any element in the top left corner has the same image in the bottom right

corner independent of the route followed).

$$\begin{array}{ccc} F(A) & \to & G(A) \\ \downarrow & & \downarrow \\ F(B) & \to & G(B) \end{array}$$

Some simple examples of such functors are:

(1) To every finite ring we associate the empty set.
(2) To every finite ring we associate the singleton set.
(3) To every finite ring we associate the underlying set of the ring.
(4) To every finite ring we associate the group of units in the ring.
(5) To every finite ring we associate the collection of q tuples of elements of the ring.

Each of the above is a particular case of the following more general construction. Let R be any finitely generated ring (i. e. R is a the quotient of the ring $\mathbb{Z}[X_1, \ldots, X_q]$ of polynomials with integer coefficients by some ideal I). We have a functor (usually denoted by $\mathrm{Spec}(R)$) which associates to the finite ring A the finite set of (unital) ring homomorphisms $\mathrm{Hom}(R, A)$. This can be done by taking the rings (1) $R = 0$ (2) $R = \mathbb{Z}$ (3) $R = \mathbb{Z}[X]$ (4) $R = \mathbb{Z}[X, Y]/(XY - 1)$ and (5) $R = \mathbb{Z}[X_r \ldots, X_q]$. The associated geometric objects can conceptualised as (1) empty (2) point (3) line (4) hyperbola (5) q-dimensional *affine space* $\mathbb{A}^q$ (since that is what one will get when A is a field). A functor of the form $\mathrm{Spec}(R)$ for a finitely generated ring R is called an *affine scheme*. If R is a quotient of the polynomial ring $\mathbb{Z}[X_1, \ldots, X_q]$ by the ideal generated by polynomials $(f_1(X_1, \ldots, X_q), \ldots, f_p(X_1, \ldots, X_q))$, then it is clear that $\mathrm{Spec}(R)(A)$ is naturally identified with the subset of q-tuples of elements of A which satisfy the system of equations given by the f_i.

For those who have studied affine schemes earlier in a slightly different way we offer the following:

Lemma 17. *Let $R \to S$ be a homomorphism of finitely generated rings so that for every finite ring A the induced map $\mathrm{Hom}(S, A) \to \mathrm{Hom}(R, A)$ is a bijection. Then this homomorphism is an isomorphism.*

A slightly different example (but one which is fundamental) is the functor that associates with a ring A the collection of all $n+1$-tuples $(a_0, a_1, \ldots, a_n)$ which generate the ring A upto multiplication by units. Equivalently, one can think of all surjective A-module homomorphisms $A^{n+1} \to A$ modulo the equivalence induced by multiplication by units. This functor is denoted $\mathbb{P}^n$ and is conceptualised as the projective n-dimensional space. We use the symbol $(a_0 : a_1 : \cdots : a_n)$ to denote the equivalence class under unit multiples of the $n+1$-tuple $(a_0, d_1, \ldots, a_n)$ which gives rise to an element in $\mathbb{P}^n(A)$.

Now, if $a = (a_0 : a_1 : \cdots : a_p)$ and $b = (b_0 : b_1 : \cdots : b_q)$ are elements in $\mathbb{P}^p(A)$ and $\mathbb{P}^q(A)$ respectively, then we can form the $(p+1)\cdot(q+1)$-tuple consisting of $c_{ij} = a_j \cdot b_j$; this tuple generates the ring A as well. Clearly, when a and b are replaced by unit multiples ua and vb for some units u and v in A, the tuple $c = (c_{ij})_{i=0,j=0}^{p,q}$ is replaced by its unit multiple $(uv)c$. Thus, we have a natural transformation $\mathbb{P}^p \times \mathbb{P}^q \to \mathbb{P}^{pq+p+q}$. Moreover, one easily checks that the resulting map on sets

$$\mathbb{P}^p(A) \times \mathbb{P}^q(A) \to \mathbb{P}^{pq+p+q}(A)$$

is on-to-one for every finite ring A. This natural transformation is called the Segre embedding.

For each positive integer d we can associate to $a = (a_0 : a_1 : \cdots : a_p)$ the $\binom{p+d}{d}$ tuple of all monomials of degree exactly d with the entries from a. For example, if $d = 2$ then we take the $\binom{p+2}{2}$-tuple consisting of $b_{ij} = a_i a_j$. As above this gives a natural transformation of functors $\mathbb{P}^p \to \mathbb{P}^{\binom{p+d}{d}-1}$. For each finite ring A the resulting map on sets

$$\mathbb{P}^p(A) \to \mathbb{P}^{\binom{p+d}{d}-1}(A)$$

is one-to-one. This natural transformation is called the d-tuple Veronese embedding.

The two examples above are special cases of projective subschemes defined as follows. Let $F(X_0, \ldots, X_p)$ be any *homogeneous* polynomial in the variables $X_0, \ldots, X_p$ (in other words all the monomials in F have the same degree). While the value of F at a $p+1$-tuple $(a_0, \ldots, a_p)$ can change if we multiply the latter by a unit, this multiplication does nothing if the value is 0. Thus, the set

$$V(F)(A) = \{(a_0 : a_1 : \cdots : a_p) | F(a_0, \ldots, a_p) = 0\}$$

is well-defined. More generally, we can define, for any finite collection $F_1, \ldots, F_n$ of homogeneous polynomials in the same $p+1$ variables

$$V(F_1, \ldots, F_n)(A) = \{(a_0 : a_1 : \cdots : a_p) | F_i(a_0, \ldots, a_p) = 0; \forall i\}$$

Such sub-functors of $\mathbb{P}^p(A)$ are called projective schemes. To emphasise the point, a functor is a projective scheme if it is naturally isomorphic to one of the functors of the form $V(F_1, \ldots, F_n)$ for some homogeneous polynomials F_i in the set of $p+1$ variables X_i. In particular, the Segre embedding is given by the system of all equations of the form $Z_{ij} Z_{kl} = Z_{il} Z_{kj}$. For any monomial of degree $2d$ and two ways of writing it as a product of monomials of degree d, we obtain a quadratic equation satisfied by the elements of the Veronese embedding; this system of equations defines the Veronese embedding.

There is also a natural way of thinking of *affine* schemes in terms of subfunctors of $\mathbb{P}^n$ for a suitable n. As we saw above any affine scheme is a subscheme of $\mathbb{A}^q$, so it is enough to exhibit $\mathbb{A}^q$ as a subfunctor of $\mathbb{P}^n$ for a suitable n. Now it is clear that if $(a_1, \ldots, a_q)$ is *any* q-tuple, then the collection $(1, a_1, \ldots, a_q)$ generates the ring A so that this defines an element $(1 : a_1 : \cdots : a_q)$ of $\mathbb{P}^q(A)$. Conversely, if $(a_0 : a_1 : \cdots : a_q)$ is an element of $\mathbb{P}^q(A)$, such that a_0 is a unit then this is the same as $(1 : a_1/a_0 : \cdots : a_q/a_0)$, which in turn corresponds to the point $(a_1/a_0, \ldots, a_q/a_0)$ in $\mathbb{A}^q$.

A generalisation of the above is the notion of a quasi-projective scheme. In addition to the homogeneous polynomials F_i considered above let $G_1(X_0, \ldots, X_p)$, $\ldots$, $G_m(X_0, \ldots, X_p)$ be homogeneous polynomials *of the same degree*. We define a quasi-projective scheme

$$\begin{aligned} V(F_1, \ldots, F_n; G_1, \ldots, G_m)(A) = \big\{ & (a_0 : a_1 : \cdots : a_p) \big| \\ & F_i(a_0, \ldots, a_p) = 0; \forall i \\ & \text{and} \\ & (G_1(a_0, \ldots, a_p), \ldots, G_m(a_0, \ldots, a_p)) \text{ generate the ring } A \big\} \end{aligned}$$

Note that, we need to make sense of linear combinations of the G_i's and hence it is essential that they are all of the same degree. As before we will be interested in

the underlying functor rather than its given representation as a subfunctor defined by the "equations" F_i and the "inequations" G_j.

One can go further and define the notion of an *abstract* algebraic scheme but for our purposes the notion defined above of a quasi-projective scheme (of finite type over integers or of "arithmetic" type) will suffice.

Let $F_1,\ldots,F_n$ be a collection of equations which define a projective scheme and d be no smaller than the maximum of their degrees. It is clear that the same projective scheme is defined by the larger collection of the form $F_j \cdot M$ where j varies between 1 and n and M varies over *all* monomials of degree $d - \deg(F_j)$. Thus we can always assume that a projective scheme is defined by homogeneous equations of the same degree.

The complement of the subscheme of $V(F_1, \ldots, F_n)$ is *not* the functor that assigns to each A the set-theoretic complement $\mathbb{P}^p(A) \setminus V(F_1, \ldots, F_n)(A)$, but in fact, when F_i's have the same degree it is the quasi-projective scheme $V(0; F_1, \ldots, F_n)(A)$. The reason for this choice becomes clear as we study schemes more. For the moment it is enough to note that if A is the ring $\mathbb{F}_p[\epsilon] = \mathbb{F}_p[X]/(X^2)$, then the element $(1 : \epsilon : \cdots : \epsilon)$ is in the set-theoretic complement of $(1 : 0 : \cdots : 0)$ in $\mathbb{P}^p(A)$ but is *not* in the scheme-theoretic complement that we have defined above.

Finally, let $X \subset \mathbb{P}^p$ be a quasi-projective scheme, and let $F_1,\ldots, F_n$ be a bunch of homogeneous polynomials of the same degree. The intersection $X \cap V(F_1, \ldots, F_n; 1)$ is clearly a subscheme of X and such subschemes are called *closed* subschemes of X. The intersection $X \cap V(0; F_1, \ldots, F_n)$ is also a subscheme of X and such subschemes are called open subschemes of X. More generally, the intersection of $V(D_1, \ldots, D_m; E_1, \ldots, E_n)$ and $V(F_1, \ldots, F_k; G_1, \ldots, G_l)$ is the scheme

$$V(D_1, \ldots, D_m, F_1, \ldots, F_k; \{E_i \cdot G_j\})$$

The "Hilbert Basis theorem" asserts that the intersection of *any* (not necessarily finite) collection of closed subschemes is a closed subscheme.

One very useful example of a closed subscheme is the subscheme $\mathbb{P}^p \subset \mathbb{P}^p \times \mathbb{P}^p$, which is the diagonal; this is a closed subscheme of the scheme $\mathbb{P}^p \times \mathbb{P}^p$ defined by the conditions $X_iY_j = X_jY_i$ for $0 \leq i, j \leq p$. For any $p < q$ we can exhibit $\mathbb{P}^p$ as the closed subscheme of $\mathbb{P}^q$ given by $X_i = 0$ for $p < i \leq q$.

Like the case of set-theoretic complement, the set-theoretic union of closed subschemes is in general not a closed subschemes. For example the smallest closed subscheme of $\mathbb{P}^2$ that contains $L = V(X_1)$ and $M = V(X_2)$ is easily seen to be $V(X_1X_2)$; but it is possible for the product of two elements of a finite ring to be 0 without either of them being zero. Thus we can *define* the *scheme-theoretic* union of a collection of closed subschemes to be the smallest closed subscheme that contains the set-theoretic union (the set-theoretic union defines a subfunctor); such a scheme exists by Hilbert's basis theorem. From now on when we use the term union of schemes we shall always mean the scheme theoretic union.

A closed subscheme $Y \subset X$ is said to be a proper closed subscheme if for some finite ring A, the subset $Y(A) \subset X(A)$ is a proper subset. A scheme is said to be *reducible* if it can be written as the union of two distinct (but not necessarily disjoint!) proper closed subschemes. For example $V(X_1X_2)$ in $\mathbb{P}^2$) is the union of the two lines $V(X_1)$ and $V(X_2)$. Now even a proper closed subscheme $Y \subset X$ can be "essentially" all of X; for example consider the closed subscheme $Y = V(X_2^2)$ of the scheme $X = V(X_2^3)$. For any *finite field* F, we have $Y(F) = X(F)$. A scheme X is said to be *reduced* if it has no proper closed subscheme Y such that

$Y(F) = X(F)$ for all finite fields F. Note that the scheme $V(X_1X_2)$ is reduced but not irreducible, while $V(X_1^2)$ is irreducible but not reduced. Hilbert's Basis theorem can also be used to show that any scheme X has a closed subscheme Y so that Y is reduced and $Y(F) = X(F)$ for finite fields F. As a consequence of the Lasker-Noether Primary Decomposition theorem any scheme can be written as the union of a finite collection of irreducible closed subschemes; moreover, the underlying reduced schemes of these closed subschemes are uniquely determined. For example, consider the scheme $L = V(X_1^2, X_1X_2)$ in $\mathbb{P}^2$. One can show that that L is the union of the closed subschemes $M = V(X_1)$ and $N = V(X_1^2, X_1X_2, X_2^2)$. But L can also be written as the union of M and $K = V(X_1^2, X_0X_2, X_1X_2, X_2^2)$; moreover N and K are distinct schemes.

8.3. **Morphisms of schemes.** We have already discussed natural transformations. However, not all natural transformations of functors are "morphisms"; which we now define. It is in fact easier to first define the notion of a "multi-valued" morphism or *correspondence*.

Let $L = V(F_1, \ldots, F_n; G_1, \ldots, G_m)$ be a quasi-projective scheme in $\mathbb{P}^p$ and $K = V(D_1, \ldots, D_k; E_1, \ldots, E_l)$ be a quasi-projective scheme in $\mathbb{P}^q$. As before we can and do assume that the collections $\{D_i\}$, $\{E_i\}$, $\{F_i\}$ and $\{G_i\}$ have constant degrees. Let X_i's be the $p+1$ variables for $\mathbb{P}^p$ and Y_j be the $q+1$ variables for $\mathbb{P}^q$. If d_1 is the degree of the D_t's then the bi-homogeneous polynomials of the form $D_t \cdot M$ where M is a monomial of degree d_1 in the variables X_i can be written as polynomials in the variables $Z_{ij} = X_iY_j$ (by choosing some arbitrary pairing of X's with Y's for each term). Let $\{\tilde{D}_t\}$ denote the resulting collection of polynomials in Z_{ij} as M varies over all possible monomials in the X's and F_t's vary. We have similar collections $\{\tilde{E}_t\}$, $\{\tilde{F}_t\}$ and $\{\tilde{G}_t\}$. One then checks quite easily that $L(A) \times K(A)$ is the subset of $\mathbb{P}^{pq+p+q}(A)$ defined by the conditions:

(1) The equations $Z_{ij}Z_{kl} - Z_{il}Z_{kj} = 0$ hold.
(2) All the $\tilde{D}_t$'s and the $\tilde{F}_t$'s vanish.
(3) The evaluation of the collection $\{\tilde{E}_i \cdot \tilde{G}_j\}$ results in a tuple that generates the ring A.

In particular, this is also a quasi-projective scheme.

Thus, when X and Y are quasi-projective schemes, then so is $X \times Y$. Hence, for a sub-functor Z of $X \times Y$ it makes sense say that it is a subscheme; or more specifically a closed or open subscheme. In particular, if W is a subscheme (resp. closed or open subscheme) of Y, we see that $X \times W$ is a subscheme (resp. closed or open subscheme) of $X \times Y$. Similarly, for subschemes of X. Another useful closed subscheme is $\Delta_X \subset X \times X$, the diagonal subscheme, which is defined by intersecting $X \times X$ with the diagonal subscheme of $\mathbb{P}^q \times \mathbb{P}^q$ when X is given a a subscheme of $\mathbb{P}^q$.

A *correspondence* from X to Y is a closed subscheme of $X \times Y$. For any natural transformation $f : X \to Y$ the graph Γ_f is the subfunctor of $X \times Y$ which gives for each finite ring A the graph of $f(A) : X(A) \to Y(A)$. We say that f is a *morphism* if Γ_f is a closed subscheme of $X \times Y$. In other words, a morphism is a natural transformation which is also a correspondence. Alternatively, if $Z \subset X \times Y$ is a correspondence so that the projection $Z(A) \to X(A)$ is a bijection for all finite rings A, then Z is the graph of a morphism.

Now it follows easily that the identity natural transformation $X \to X$ is a morphism with the diagonal as the associated correspondence. Moreover, each of the projections $X \times Y \to X$ and $X \times Y \to Y$ is a morphism. It is also clear that if $W \subset X$ is a subscheme then the intersection of $W \times Y$ with Γ_f gives the graph of the restriction of $f : X \to Y$ to W; as a result this restriction is also a morphism. If $Z \subset X \times Y$ is the graph of a morphism then the projection $Z \to X$ is a morphism; its graph in $Z \times X \subset X \times Y \times X$ is the intersection of the diagonal of the extreme terms (consisting of (x, y, x)) with $Z \times X$. The map $Z(A) \to X(A)$ is a bijection; let $g : X \to Z$ be the inverse natural transformation. The graph of g in $X \times Z \subset X \times X \times Y$ is the intersection of $\Delta_X \times Y$ with $X \times Z$. Thus g is also a morphism. In other words, there are morphisms $Z \to X$ and $X \to Z$ with composition either way being identity. Thus $Z \to X$ is an *isomorphism*.

Now, let $f : X \to Y$ be a morphism and $g : Y \to Z$ be another morphism. Let W be the intersection of $\Gamma_f \times Z$ with $X \times \Gamma_g$ in $X \times Y \times Z$. Under the above isomorphism $X \to \Gamma_f$, we can identify W as a subscheme of $X \times Z$. It clear that $W(A)$ is the graph of the composite natural transformation $g \circ f$. Thus, morphisms can be *composed*.

Let $f : X \to Y$ be a morphism and $W \subset Y$ be a subscheme. Then, we have a subscheme of Γ_f given by its intersection with $X \times W$. Since $\Gamma_f \to X$ is an isomorphism, we obtain a subscheme of X as well; this scheme is usually denoted $f^{-1}(W)$ and called the inverse image of W under f. In some cases it may happen that Γ_f is *contained* in $X \times W$ so that $f^{-1}(W) = X$. In this case we say that the morphism f factors through or lands inside W.

The theorem of Chevalley asserts that there is a smallest subscheme W of Y so that f factors through W; we can refer to W as the *categorical image* of f. Note that it may not be true that $W(A)$ is the image of $X(A)$ in $Y(A)$ even for *one* non-zero finite ring A.

Given morphisms $X \to W$ and $X \to Z$ we easily check that the natural transformation $X \to W \times Z$ is a morphism. Given morphisms $X \to S$ and $Y \to S$, we obtain the compositions $a : X \times Y \to X \to S$ and $b : X \times Y \to Y \to S$. Thus we a morphism $X \times Y \to S \times S$. The inverse image of the diagonal is denoted $X \times_S Y$ and is called the *fibre product* of X and Y over S. For any morphisms $Z \to X \times Y$ such that the resulting composites with a and b are equal, we see that the morphism actually lands in the subscheme $X \times_S Y$.

One important example of a correspondence is the subscheme Z of $\mathbb{P}^{p+q} \times \mathbb{P}^q$ defined by the conditions $X_i Y_j = X_j Y_i$ for $0 \leq i, j \leq q$. Let U be the open subscheme of $\mathbb{P}^{p+q}$ given by $U = V(0; X_0, X_1, \ldots, X_q)$. For $(a_0 : \cdots : a_{p+q})$ in $U(A)$, the tuple $(a_0, \ldots, a_q)$ generates the ring A, thus we see that we see that $((a_0 : \cdots : a_{p+q}), (a_0 : \cdots : a_q))$ gives an element of $\mathbb{P}^{p+q}(A) \times \mathbb{P}^q(A)$ which clearly lies in $Z(A)$. Conversely, if $((a_0 : \cdots : a_{p+q}), (b_0 : \cdots : b_q))$ lies in $Z(A)$ *and* $(a_0, \ldots, a_q)$ generate the ring A, then the above equations show that there is a unit u in A so that $b_i = u a_i$ (apply the Chinese Remainder theorem for finite rings!). Thus, the projection $Z(A) \to \mathbb{P}^{p+q}(A)$ is a bijection over $U(A)$ and gives a morphism $U \to \mathbb{P}^q$. This morphism is called the *projection* on $\mathbb{P}^{p+q}$ *away* from the linear subscheme (or subspace!) $V(X_0, \ldots, X_q)$; more generally, we can refer to the above correspondence as the projection correspondence.

A natural generalisation of this is to consider a collection $F_0, \ldots, F_q$ of homogeneous polynomials of the same degree in variables $X_0, \ldots, X_p$; we can then take the

subscheme Z of $\mathbb{P}^p \times \mathbb{P}^q$ defined by the equations

$$F_i(X_0, \ldots, X_p)Y_j = F_j(X_0, \ldots, X_p)Y_i$$

for $0 \leq i, j \leq q$. We can take U to be the open subscheme defined by $U = V(0; F_0, \ldots, F_q)$. The correspondence Z restricts to a morphism $U \to \mathbb{P}^q$. The scheme Z is referred to as the *blow-up* of $\mathbb{P}^p$ along the closed subscheme $Y = V(F_1, \ldots, F_q)$ and is sometimes denoted $\tilde{\mathbb{P}}^p_Y$.

For any functor F on the category of finite rings we can introduce a new functor T_F which associates to a finite ring A the set $F(A[\epsilon])$ where $A[\epsilon]$ denotes the finite ring $A[T]/(T^2)$. The morphism $A[\epsilon] \to A$ that sends ϵ to induces a natural transformation of functors $T_F \to F$. Now, if $F = \mathbb{P}^p$ is the projective space then $T_{\mathbb{P}^p}(A)$ consists of equivalence classes of $p+1$-tuples

$$(a_0 + b_0\epsilon, \ldots, a_p + b_p\epsilon) \simeq (ua_0 + (a_0 b + ub_0)\epsilon, \ldots, ua_p + (a_p b + ub_0)$$

where u is a unit in A and $(a_0, \ldots, a_p)$ generate the ring A (this is enough to ensure generation of $A[\epsilon]$ by the above $p+1$-tuple). The elements $s_{ij} = a_i a_j$ and $t_{ij} = b_i a_j - a_j b_i$ are invariants associated with the equivalents class upto simultaneous multiplication by a unit u in A. Thus, if we consider the equivalence classes (under multiplication by units in A) of pairs $(S; T)$ where S is a symmetric matrix and T an anti-symmetric matrix; then the equations satisfied by S and T are

$$s_{ij}s_{kl} - s_{ik}s_{jl} = 0 \tag{1}$$

$$t_{ij}s_{kl} + t_{jk}s_{il} + t_{ki}s_{jl} = 0 \tag{2}$$

Moreover, the entries s_{ij} of S generate the ring A. Conversely, a pair of matrices (S, T) satisfying the two equations and the condition that the entries of S generate the ring can be seen to arise in from an element $\mathbb{P}^p(A[\epsilon])$.

Proof. Let us assume that A is a finite local ring (the other cases follow from the Chinese Remainder Theorem). In this case, at least one of the entries s_{ij} must be a unit (since a sum of nilpotent elements is nilpotent). The equation $s_{ij}s_{ij} = s_{ii}s_{jj}$ shows that s_{ii} must also be a unit. Let us then define $a_k = s_{ik}/s_{ii}$ and $b_k = t_{ki}$. The equation $s_{jk}s_{ii} = s_{ij}s_{ik}$ implies that $s_{jk} = a_j a_k$ as required. Moreover, the equation

$$t_{jk}s_{ii} = t_{ji}s_{ki} - t_{ki}s_{ji}$$

shows us that $t_{jk} = b_j a_k - b_k a_j$ as required. □

The collection of equivalence classes of pairs $(S; T)$ under multiplication by units in A can be identified with $\mathbb{P}^{p^2+2p}$. Thus $T_{\mathbb{P}^p}$ is naturally isomorphic to the quasi-projective scheme

$$V(S_{ij}S_{kl} - S_{ik}S_{jl}, T_{ij}S_{kl} + T_{jk}S_{il} + T_{ki}S_{jl}; S_{ij})$$

This quasi-projective scheme is the *Zariski Tangent Scheme* of $\mathbb{P}^p$. More generally, for any quasi-projective scheme X given as a subscheme of $\mathbb{P}^p$ one can show that the functor T_X is naturally isomorphic to a subscheme of $T_{\mathbb{P}^p}$. In other words, T_X is also a quasi-projective scheme; this scheme is called the Zariski Tangent scheme of X. Moreover, the natural transformation $T_X \to X$ (given by the natural map $X(A[\epsilon]) \to X(A)$) is a morphism of schemes. This gives an important example of a vector space scheme; a notion that we will introduce in the next section.

8.4. **Relativisation and categorical constructions.** Now that we have constructed morphisms it follows that quasi-projective schemes form a *category*. One standard construction is that of the *slash* category associated with an object S which is denoted by $/S$. The objects in this category are morphisms $X \to S$. The morphisms are commutative diagrams

$$\begin{array}{ccc} X & \to & Y \\ & \searrow \quad \swarrow & \\ & S & \end{array}$$

The products in this category are provided by fibre products. Geometrically, we conceptualise the objects $X \to S$ as families of spaces parametrised by S. Note that there is a natural and unique morphism from any scheme X to the scheme $\nVdash$ (which we have called a point or $\mathrm{Spec}(\mathbb{Z})$ or $\mathbb{A}^0$ or $\mathbb{P}^0$ above in different places!). Thus schemes are in fact naturally parametrised by $\mathrm{Spec}(\mathbb{Z})$.

For any morphism $T \to S$ we can "re-parametrise" or perform base change by associating $X \times_S T \to T$ with $X \to S$. One checks that this gives a functor from the slash category $/S$ to the slash category $/T$.

For example, let N be any integer and consider the rings $\mathbb{Z}/N\mathbb{Z}$ and $\mathbb{Z}[1/N]$. The schemes over $\mathrm{Spec}(\mathbb{Z}/N\mathbb{Z})$ are the schemes *"modulo N"*. The schemes over $\mathrm{Spec}(\mathbb{Z}[1/N])$ are schemes *"outside N"*. In particular, we can take $N = p$ a prime to get schemes over $\mathrm{Spec}(\mathbb{F}_p)$ or schemes of characteristic p. We occasionally see statements like "the following is true outside characteristic 2 and 3"; this can be interpreted as a statement about schemes over $\mathrm{Spec}(\mathbb{Z}[1/6])$.

For many algebraic object that can be defined diagram-theoretically, there are associated types of objects in the category $/S$. For example we can define a group as a set G with maps $\mu : G \times G \to G$ for multiplication, $\iota : G \to G$ for inverse and $e : 1 \to G$ which maps the singleton set to the identity element of G. These satisfy various commutative diagrams which ensure that multiplication is associative, the product of an element and its inverse is identity and the identity multiplied with anything is identity.

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{1\times\mu} & G \times G \\ {\scriptstyle \mu\times 1}\downarrow & & \downarrow{\scriptstyle \mu} \\ G \times G \times G & \xrightarrow{1\times\mu} & G \times G \end{array} \qquad \begin{array}{ccccc} G & \xrightarrow{\Delta} & G \times G & \xrightarrow{1\times\iota} & G \times G \\ & \searrow & & & \downarrow{\scriptstyle \mu} \\ & & 1 & \xrightarrow{e} & G \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{1\times e} & G \times G \\ {\scriptstyle 1}\searrow & & \downarrow{\scriptstyle \mu} \\ & & G \end{array}$$

Thus we can define a group scheme over S as a morphism $G \to S$ with morphisms in $/S$; $\mu : G \times_S G \to G$ and $\iota : G \to G$ and $e : S \to G$ which satisfy the same commutative diagrams. One example is the scheme $\mathbb{G}_m = \mathrm{Spec}(\mathbb{Z}[X, Y]/(XY - 1))$ which is called the multiplicative group of units since it associates to every finite ring A the group of units in A.

Similarly a ring R is a set with maps $\mu : R \times R \to R$ for multiplication, $\alpha : R \times R \to R$ for addition, $- : R \to R$ for negation, $0 : 1 \to R$ for the zero element and $1 : 1 \to R$ for the multiplicative identity. The various laws of associativity, distributivity, commutativity (of addition) and additive and multiplicative identity can again be formulated in terms of commutative diagrams. We can use such diagrams to define the notion of a ring scheme. One important example is that of $\mathbb{G}_a = \mathrm{Spec}(\mathbb{Z}[X])$ called the additive group or the structure ring, since it associates to each finite ring A the ring A itself with its natural structure.

We can similarly define the notion of group scheme actions on a scheme and modules schemes over a ring scheme. One important example is that of vector space

schemes, which are group schemes that are also modules over the ring scheme $\mathbb{G}_a$. These are so called because, if $V \to S$ is a vector space scheme over S and k is a finite field, then the collection of all elements of $V(k)$ that map to a fixed element in $S(k)$ acquire the natural structure of a vector space over k. We can form a natural vector space scheme out of $\mathbb{A}^q$; we denote this scheme by $\mathbb{V}^q$. Clearly, $\mathbb{V}^q \times S \to S$ is a vector space scheme over S for any S. Another example of a vector space scheme the scheme T_S considered above. This is called the (Zariski) *Tangent scheme* of S.

Some other important examples of vector space schemes are as follows. Let $H = V(0; X_0, X_1, \ldots, X_p)$ be the complement of the point $(0 : \cdots : 0 : 1)$ in $\mathbb{P}^{p+1}$. The projection way from this point gives a morphism $H \to \mathbb{P}^p$. This is a vector space scheme with "zero section" given by $\mathbb{P}^p \to H$ which maps $(a_0 : \cdots : a_p)$ to $(a_0 : \cdots : a_p : 0)$. For any i between 0 and p we have sections $\mathbb{P}^p \to H$ given by sending $a_0 : \cdots : a_q)$ to $(a_0 : \cdots : a_q : a_i)$. Considering the set $\mathbb{P}^p(A)$ as equivalence classes of surjective A-module homomorphisms $A^{p+1} \to A$, it is clear that the kernel of this homomorphism is independent of the chosen representative of the equivalence class. This defines a sub-vector space scheme of $\mathbb{V}^{p+1} \times \mathbb{P}^p \to \mathbb{P}^p$. Another vector space scheme over $\mathbb{P}^p$ consists of the subscheme of $\mathbb{V}^{p+1} \times \mathbb{P}^p$ which is defined by $V_i X_j = V_j X_i$; this vector space scheme is denoted L.

If $V \to S$ is a vector space scheme then for any morphism $T \to S$ it is clear that $V \times_S T \to T$ is one as well. In particular, vector space schemes can be *restricted* to subschemes. The restriction of the vector group scheme denoted H over $\mathbb{P}^{\binom{p+d}{d}-1}$ to the Veronese embedding of $\mathbb{P}^p$ is denoted $H_d \to \mathbb{P}^p$.

8.5. **The category of vector space schemes.** One can easily "relativise" the notion of a homomorphism of modules to define the notion of a homomorphism of vector space schemes.

The inverse image of the zero section under such a homomorphism a sub-vector space scheme of the domain of the homomorphism. This, defines the *kernel* of a homomorphism of vector space scheme. The image of a homomorphism $E \to F$ of vector space schemes over S is also a sub-vector space scheme. In particular, we see that the notion of *exact sequences* of vector space schemes can be defined by saying the the image of one morphism is the kernel of the next.

In fact these objects form an *abelian* category. In order to do this we need The Coherence theorem for vector space schemes:

(1) For any vector space scheme $V \to S$ there is an embedding $S \subset \mathbb{P}^p$ and an integer m and an injective homomorphism of vector space schemes $V \to H^{\oplus m}$; here by abuse of notation we use H to denote the restriction of the vector space scheme $H \to \mathbb{P}^p$ defined earlier.
(2) Given *any* homomorphism $V \to H_d^{\oplus m}$, there is a homomorphism $H_d^{\oplus m} \to H_{d+e}^{\oplus n}$ for some e and n so that the image of V is the kernel of the latter homomorphism.

Now a homomorphism $H_d \to H_{d+e}$ can be identified with a homogeneous polynomial of degree e. Thus, the coherence theorem can be used to give a concrete definition of vector space schemes in terms of $n \times m$ matrices of homogeneous polynomials of degree e. Another application is the construction of cokernels. Given $V \subset W$ a sub-vector space scheme, we can write W as a sub-vector space scheme of $H_d^{\oplus n}$ and find a homomorphism $H_d^{\oplus n} \to H_{d+e}^{\oplus m}$ so that V is the kernel. Then W/V is clearly identified with the image of W in $H_{d+e}^{\oplus m}$.

For example let $\mathbb{P}^{n-1}$ be considered as the closed subscheme of $\mathbb{P}^n$ defined by a single linear equation $X_n = 0$. The vector space scheme $\mathbb{V}^1 \times \mathbb{P}^{n-1}$ can be extended by zero to give a vector space scheme on $\mathbb{P}^n$ which we denote by $(\mathbb{V}^1 \times \mathbb{P}^{n-1})_{\mathbb{P}^n}$. We also have the morphism $\mathbb{V}^1 \times \mathbb{P}^n \to H$ given by the 1×1 matrix with entry X_n. One easily sees that this gives an exact sequence of vector space schemes

$$0 \to (\mathbb{V}^1 \times \mathbb{P}^{n-1})_{\mathbb{P}^n} \to \mathbb{V}^1 \times \mathbb{P}^n \to H \to 0$$

More generally, this can be done with any linear polynomial in the X_i's that gives a surjective linear map $\mathbb{Z}^{n+1} \to \mathbb{Z}$. The corresponding subscheme is isomorphic is again $\mathbb{P}^{n-1}$.

An irreducible (or atomic) object in an abelian category is defined as one which has no non-trivial sub-objects Ideally we would like to write every vector space scheme as a sum of irreducibles. However, it turns out that this is not possible. A compromise solution is to "semi-simplify" the operation as per a construction due to Grothendieck.

The Grothendieck K-group of a scheme S is the quotient of the free group generated by isomorphism classes of vector space schemes over S by the relations of the form $[V] = [U] + [W]$ when $0 \to U \to V \to W \to 0$ is an exact sequence. Quillen has generalised this construction to define the groups K_i for any exact category. Grothendieck's K group then becomes K_0. The K_0 group of vector space schemes over S is denoted $G_0(S)$.

For any closed subscheme T of S, we have a vector space scheme on S obtained by extending by zero the vector space scheme $\mathbb{V}^1 \times T$; we use the symbol $[T]$ to denote the corresponding element of $G_0(S)$. From the above exact sequence we see that for any linear subscheme $M \cong \mathbb{P}^{n-1}$ in $\mathbb{P}^n$ we have the equation $[M] = [\mathbb{P}^n] - [H]$ in $G_0(\mathbb{P}^n)$. Now the right hand side is *independent* of the linear equation chosen so that $[M]$ becomes independent of the specific linear subspace M.

8.6. **Vector Bundles and regular schemes.** Most of the examples of vector space schemes that we have seen so far are *vector bundles*; these are vector space schemes that are "locally" isomorphic to $\mathbb{V}^n$ for some fixed n. In other words, $E \to X$ is a vector bundle if there is a collection of open subschemes $U_i \subset X$ such that $\cup U_i(A) = X(A)$ for every finite local ring and $E \times_X U_i$ is isomorphic to $\mathbb{V}^n \times U_i$ as a vector space scheme over U_i for every i. A collection of open sets satisfying the first property is referred to as an *open cover* of X. The vector bundle $\mathbb{V}^q \times X$ is called the *trivial* vector bundles on X. The number n is called the *rank* of the vector bundle.

Recall, that L was defined as the subscheme of $\mathbb{V}^{p+1} \times \mathbb{P}^p$ consisting of pairs of tuples $(b_0, \ldots, b_p; a_0 : \cdots : a_p)$ such that $a_i b_j = a_j b_i$ for all i and j between 0 and p. An open cover of $\mathbb{P}^p$ is given by the open subschemes $U_i = V(0; X_i)$. We see easily that $L \times_{\mathbb{P}^p} U_i$ is given by the equations $b_j = (a_j/a_i)b_i$ since a_i is a unit. Thus the map from $\mathbb{G}_a \times U_i$ to $L \times_{\mathbb{P}^p} U_i$ given by

$$(c; a_0 : \cdots : a_p) \mapsto ((a_0/a_i)c, \ldots, (a_p/a_0)c; a_0 : \cdots : a_p)$$

gives an isomorphism. Thus L is a vector bundle of rank 1 or a *line bundle*. Recall also that H was defined as the subscheme of $\mathbb{P}^{p+1}$ which is the complement of the point $(0 : \cdots : 0 : 1)$. The morphism $H \to \mathbb{P}^p$ is the projection away from this point and the zero-section is $V(X_{p+1})$. For each i between 0 and p we have a natural

homomorphism $s_i : \mathbb{G}_a \times \mathbb{P}^p \to H$ given by

$$(c; a_0 : \cdots : a_p) \mapsto (a : 0 : \cdots : a_p : c \cdot a_i)$$

Note that this is an isomorphism outside the *hyperplane* $V(X_i)$; in other words this is an isomorphism on $U_i = V(0; X_i)$. Thus H is also a line bundle.

The automorphisms of the vector space $\mathbb{V}^n$ are given as the closed subscheme GL_n of $\mathbb{A}^{n^2+1}$ consisting of $((X_{ij})_{i,j=1}^n, T)$ such that $\det((X_{ij}))T = 1$. For any scheme X, any automorphism of the vector space scheme $\mathbb{V}^n \times X$ corresponds naturally to a morphism $g : X \to \mathrm{GL}_n$. Moreover, it is clear that GL_n is a group scheme.

Now let E be a vector bundle over a scheme X, $\{U_i\}$ be an open cover of X and ϕ_i be the isomorphism of vector space schemes $\phi_i : E \times_X U_i \to \mathbb{V}^n \times U_i$. For any i and j it is clear that we get a morphism $\phi_{ij} : U_i \cap U_j \to \mathrm{GL}_n$ by comparing the two isomorphisms of $E \times_X (U_i \cap U_j)$ with $\mathbb{V}^n \times (U_i \cap U_j)$. These morphisms satisfy $\phi_{ij} \cdot \phi_{jk} = \phi_{ik}$ on $U_i \cap U_j \cap U_k$. Conversely, it is clear that we can use such a collection of morphisms $\phi_{ij} : U_i \cap U_j \to GL_n$ to construct a vector bundle on X by *patching* together the vector bundles $\mathbb{V}^n \times U_i$. More generally, we can easily show that for any vector space scheme V on X, the group scheme GL_n operates on $V^{\oplus n}$. Thus we can use the ϕ_{ij} to patch together $V^{\oplus n} \times_X U_i$ to obtain a vector space scheme. This vector space scheme is denoted $E \otimes V$ and is called the tensor product of E with V. It is clear that $\mathbb{V}^1 \otimes V = V$. One can show that $H_n = H^{\otimes n}$ and $H \otimes L = \mathbb{V}^1 \times \mathbb{P}^p$.

As before we define the K-group of vector bundles of a scheme S as the quotient $K_0(S)$ of the free abelian group on isomorphism classes of vector bundles by the subgroup generated by relations of the form $[V] + [U] - [W]$ where $0 \to V \to W \to U \to 0$ is an exact sequence of vector bundles. Note that any vector bundle is a vector space scheme and an exact sequence of vector bundles is also an exact sequence of vector space schemes. Thus we have a natural homomorphism $K_0(S) \to G_0(S)$. When S is a *regular* scheme this is an isomorphism; usually one gives a definition of regular schemes in terms of ring theory and proves the equivalence, but we could equally well use this as a definition. As a particular case we have the "Jacobian criterion" which says that a scheme is regular if the Zariski tangent vector space scheme is a vector bundle; note however that this is *not* in general necessary. For example the subscheme of $\mathbb{A}^2$ defined by $XY = p$ for some prime p is regular but its Zariski tangent space is not a vector bundle.

In fact the tensor product construction makes $K_0(S)$ into a ring and $G_0(S)$ a module over this ring.

8.7. **Action of correspondences.** If $0 \to V \to W \to U \to 0$ is an exact sequence of vector space schemes over a scheme X and if $Y \to X$ is a morphism then the *pull-back* sequence of vector space schemes

$$0 \to V \times_X Y \to W \times_X Y \to U \times_X Y \to 0$$

is *not* in general exact. We say that $Y \to X$ is *flat* if this is so. However, if V is a vector bundle then the pull back sequence of vector space schemes *is* exact regardless of the nature of the morphism $Y \to X$. Thus we have a homomorphism $K_0(X) \to K_0(Y)$ for any morphism $Y \to X$ and a homomorphism $G_0(X) \to G_0(Y)$ when $Y \to X$ is flat. An important property of tensor products is that the

homomorphism $K_0(X) \to K_0(Y)$ is a ring homomorphism and when $X \to Y$ is flat the homomorphism $G_0(X) \to G_0(Y)$ is a homomorphism of $K_0(X)$ modules.

Now, let X be a closed subscheme of $Z = \mathbb{P}^n \times Y$. We want to construct a homomorphism $G_0(X) \to G_0(Y)$. This can be done in two steps (provided we prove that the construction is independent of the factorisation). The first step is to consider a vector space scheme on X as a vector space scheme on Z (of which it is a closed subscheme). We have already seen how to do this by "extending by zero"; it is moreover clear that this preserves exact sequences. Thus we obtain a natural homomorphism $G_0(X) \to G_0(Z)$.

Hilbert's syzygy theorem can be used to describe $G_0(\mathbb{P}^n \times Y)$ in terms of $G_0(Y)$ as follows. For any integer n we have a line bundle H^n on $\mathbb{P}^n$ as described above; let W be any vector space scheme on Y. We have a vector space scheme $H_k \boxtimes W$ on $\mathbb{P}^n \times Y$ obtained as

$$H_k \boxtimes W = (H_k \times Y) \otimes (\mathbb{P}^n \times W)$$

Let V be any vector space scheme on $\mathbb{P}^n \times Y$, the syzygy theorem asserts that there is a a sequence of positive integers $k_0, \ldots, k_n$ and a sequence of vector space schemes W_n on Y which fit into an exact sequence

$$0 \to V \to H_{k_0} \boxtimes W_0 \to \cdots \to H_{k_n} \boxtimes W_n \to 0$$

Thus $G_0(\mathbb{P}^n \times Y$ is generated by $G_0(Y)$ as a module over $K_0(\mathbb{P}^n)$. Moreover, to define the homomorphism $G_0(\mathbb{P}^n \times Y \to G_0(Y)$ it is enough to define the image of terms of the form $H_k \boxtimes W$ (and check for consistency).

Consider the exact sequence which was introduced above

$$0 \to (\mathbb{V}^1 \times \mathbb{P}^{n-1})_{\mathbb{P}^n} \to \mathbb{V}^1 \times \mathbb{P}^n \to H \to 0$$

By tensoring this with W and H_{k-1} we get an exact sequence on $\mathbb{P}^n \times Y$

$$0 \to (H_{k-1}|_{\mathbb{P}^{n-1}}) \boxtimes W \to H_{k-1} \boxtimes W \to H_k \boxtimes W \to 0$$

This allows us to write the class of $H_k \boxtimes W$ in $G_0(\mathbb{P}^n \times Y$ as

$$[H_k \boxtimes W] = [H_{k-1} \boxtimes W] - [H_{k-1}|_{\mathbb{P}^{n-1}} \boxtimes W]$$

The second term on the right hand side can be thought of as an element of $G_0(\mathbb{P}^{n-1} \times Y)$. By induction we can thus reduce the problem of defining the image of $[H_k \boxtimes W]$ in $G_0(Y)$ to that of defining the image of $[(\mathbb{V}^1 \times \mathbb{P}^m) \boxtimes W]$. The image of the latter is just $[W]$. The consistency of this definition can be checked by the theory of "cohomology" and higher direct images. Thus we have a homomorphism $G_0(\mathbb{P}^n \times Y) \to G_0(Y)$ and more generally for any closed subscheme X of $\mathbb{P}^n \times Y$ we have $G_0(X) \to G_0(Y)$.

Now let X be a projective scheme (i. e. a closed subscheme of $\mathbb{P}^n$), and let Y be any scheme. Let $Z \subset X \times Y$ be a correspondence from X to Y (i. e. Z is a closed subscheme of $X \times Y$). We obtain a homomorphism $K_0(X) \to K_0(Z)$; additionally, when $Z \to X$ is flat we obtain a homomorphism $G_0(X) \to G_0(Z)$. By using the sequence of closed inclusions $Z \subset X \times Y \subset \mathbb{P}^n \times Y$ we also have a homomorphism $G_0(Z) \to G_0(Y)$. Thus we see that for any correspondence from a projective scheme X to a scheme Y we obtain a homomorphism $K_0(X) \to G_0(Y)$ and when the correspondence is flat over X we get a homomorphism $G_0(X) \to G_0(Y)$. In particular, correspondences from a regular scheme X to itself act as automorphisms of $G_0(X) = K_0(X)$. This is a very useful tool in analysing the structure of $K_0(X)$ for such schemes.

8.8. **Cryptosystems.** As seen earlier algebraic cryptosystems rely on explicit manipulations with finite abelian groups. All the finite abelian groups that have been used as cryptosystems so far are specific K-groups of schemes with minor modifications. Thus it would seem that a useful way of diversifying the collection of groups available for cryptosystems would be to study all K-groups of schemes. This is difficult because there is (so far) no way to explicitly bound the generators of such groups—indeed the fact that these groups are finitely generated is no yet proved! In computational applications we would also need explicit ways of representing elements and reducing sums of such elements to the representative ones. While the description of every element in terms of matrices using the "syzygy" approach described above is possible much more work needs to be done to make K-groups of all schemes computationally approachable. However, in the case of some specific schemes this can be done. This is what we explore in the next section.