Ringvorlesung Geometric Literacy WS06/07 **GK Leipzig**

Algebraic Geometry

Annette Huber

Contents

1 Algebraic Varieties

k an algebraically closed field. We denote $\mathbb{A}_k^n = k^n$ the *affine space* and $\mathbb{P}_k^n$ *projective space*, i.e. the set of lines through 0 in k^{n+1}. We usually write points in $\mathbb{P}_k^n$ in homogenuous coordiates $[x_0 : \cdots : x_n]$ upto a factor $\lambda \in k^*$.

Definition 1.1. *Let $S \subset k[X_1, \ldots, X_n]$ be a subset. Then the set*

$$V(S) = \{P \in \mathbb{A}_k^n \mid f(P) = 0 \textit{ for all } f \in S\}$$

is called affine variety defined by S. *Analogously let $S \subset k[X_0, \ldots, X_n]$ be a set of homogenuous polynomials. Then*

$$V(S)\{P \in \mathbb{P}^n \mid f(P) = 0 \textit{ for all } f \in S\}$$

is called projective variety defined by S.

Note that for $[x_0 : \cdots : x_n] \in \mathbb{P}^n$ the value $f(P)$ is not well-defined

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$$

if f is homogenous of degree d. However, the vanishing of $f(P)$ is well-defined.

Remark: Closed complex submanifolds of $\mathbb{CP}^n = \mathbb{P}_{\mathbb{C}}^n$ are in fact projective varieties, e.g. all compact Riemann surfaces.

Affine or projective varieties are equipped with a topology.

Definition 1.2. *Let V be an affine or projective variety. Then the* Zariski topology *on V has as closed sets the subvarieties.*

Example: Let $V = \mathbb{A}^1$ (defined by $S = \emptyset$ in $\mathbb{A}^1$) and $f \in k[X]$. Then $V(f) = \{x \in k \mid f(x) = 0$ is *finite* (unless $f = 0$). This implies that the closed sets in V are either finite or all of V. Or equivalently: the open sets are cofinite or empty. In particular all non-trivial open sets are *dense*!

We want varieties to form a category, so we need morphisms.

Definition 1.3. *Let V, W be varieties. Then a map $f : V \to W$ is called* morphism *if it is continuous and locally induced by polynomials. In the case $W = \mathbb{A}^1$ we call*

$$\mathcal{O}(V) = \mathrm{Mor}(V, \mathbb{A}^1)$$

the ring of algebraic functions on V*.*

Theorem 1.4 (Hilbert's Nullstellensatz)**.** *Let $V = V(S) \subset \mathbb{A}^n$ be an affine variety. Then*

$$\mathcal{O}(V) = k[X_1, \ldots, X_n]/I(V)$$

with

$$I(V) = \{f \in k[X_1, \ldots, X_n] \mid f(V) = 0\})\sqrt{I(S)}$$

where $I(S)$ is the ideal generated by S and $\sqrt{I}$ denotes the radical, i.e. $f \in k[X_1, \ldots, X_n]$ such that some $f^m \in I$.

Proof. Their is obviously a map

$$\pi : k[X_1, \ldots, X_n] \to \mathcal{O}(V)$$

One first proves that it is surjective. Again obivously, $\sqrt{I(S)}$ is contained in the kernel. The main part of the Theorem is to show that it is the full kernel. □

Hence the theory of affine varieties is equivelent to the theory of polyomial rings and their ideals.

In genera, a *variety* is glued from affine varieties along morphisms of varieties. For technical reasons, it is more convention to formulate this in a different language.

Definition 1.5. *A* sheaf *of rings $\mathcal{O}$ on a topological space X is an assignment*

$$U \mapsto \mathcal{O}(U)$$

(U open in X, $\mathcal{O}(U)$ a ring) togehter with

$$V \subset U \subset X \mapsto \rho_{UV} : \mathcal{O}(U) \to \mathcal{O}(V)$$

which is functorial and such that for an open covering $U = \bigcup U_i$ the sequence

$$0 \to \mathcal{O}(U) \to \prod \mathcal{O}(U_i) \to \prod \mathcal{O}(U_i \cap U_j)$$

($f \mapsto (\rho_{UU_i} f)_i$ and $(f_i)_i \mapsto (f_i - f_j)_{i,j}$) is exact.

Example:

1. Let X be a complex manifold and $\mathcal{O}(U)$ the ring of holomorphic functions on U. The map ρ_{UV} is restriction of the function to V.

2. X affine variety and $\mathcal{O}(U)$ the ring of algebraic functions on U.

Definition 1.6. *A* variety *over k is a topological space V together with a sheaf of rings $\mathcal{O}_V$ on V such there is a finite open covering $V = U_1 \cup \cdots \cup U_n$ such that $(U_i, \mathcal{O}_{U_i})$ is isomorphic to an affine variety with its sheaf of algebraic functions.*

A morphism *of varieties is a continuous map $f : V \to W$ compatible with the sheaves of rings.*

Similarly a smooth manifold can be defined as a topological space togher with a sheaf of rings which locally looks like an open disc in $\mathbb{R}^n$ together with the sheaf of smooth functions.
Remark: This is not completely correct. The morphisms of the sheaves of rings have to be *local*. This implies that f is locally induced by morphisms of affine varieties. We do not go into this.
Example: Projective varieties because $\mathbb{P}^n$ can be covered by copies of $\mathbb{A}^n$.

Properties of varieties

V is called *reducible* if $V = V_1 \cup V_2$ with $V_i \neq V$ closed subsets. It is called irreducible otherwise.

Proposition 1.7. *An affine variety V is irreducible if and only if $\mathcal{O}(V)$ is an integral domain. Any variety is a finite union of irreducible subvarieties.*

Definition 1.8. *The* dimension *of a variety V is the maximal length of a chain of closed irreducible subvarieties*

$$V_n \subset V_{n-1} \subset V_{n-2} \subset \cdots \subset V_0$$

(where $V_i \neq V_{i-1}$)

Example: The sequence

$$\mathbb{A}^n \subset \mathbb{A}^{n-1} \cong V(x_n) \subset \mathbb{A}^{n-2} \cong V(x_n, x_{n-1} \dots$$

shows that $\dim \mathbb{A}^n \geq n$. In fact it is equal to n.

Proposition 1.9. *All varieties are finite-dimensional. If V is irreducible, then all maximal chains have the same length. If $k = \mathbb{C}$ and V a projective manifold, then its dimension in the above sense agrees with the dimension in the sense of complex analysis.*

Example: Consider $V(y^2 - x(x-1)^2) \subset \mathbb{A}^2$. ([Picture], nodal curve with dopple point in 0)). Varieties can have singular points.

Definition 1.10. *Let V be affine, $\mathcal{O}(V) = k[X_1, \dots, X_n]/(f_1, \dots, f_m)$. Then we define the* Jacobian *of V as*

$$\mathrm{Jac}(V) = \left(\frac{\partial f_i}{\partial X_j} \right)_{i,j}$$

V has a singularity *in $P \in V$ if* $\operatorname{rk} \mathrm{Jac}(V)(P) \neq \dim V$. *The variety is called* singular *(*non-singular*)if V has a singular (no singular) point.*

The generic value for $\operatorname{rk} \mathrm{Jac}(V)(P)$ is $\dim V$. This is another possible definition of the example. Recall that the Jacobian matrix occurs in the implicit function theorem. Over $\mathbb{R}$ or $\mathbb{C}$ the rank-condition implies that V is a manifold near P.

In our example the varietiy has dimension 1. But $\mathrm{Jac}(V) = (-2x(x-1) - (x-1)^2, 2y)$ vanishes in $(1, 0)$. This is a singularity.

Note that varieties are not Hausdorff but always (pseudo)-compact. Instead:

Definition 1.11. *Let V be a variety, $C \subset \bar{C}$ an open inclusion of irreducible curves. Let $f : C \to V$ be a morphism. By an extension $\bar{f}$ of f we mean $\bar{f} : \bar{C} \to V$ such that $\bar{f}_C = f$.*

A variety is called separated *if for all such $C \subset \bar{C}$, $f : C \to V$ the extension $\bar{f}$ is unique. V is called* proper *or* complete *if $\bar{f}$ exists and is unique.*

Example: Quasi-projective varieties (open in projective varieties) are separated. Projective varieties are proper, affine are not.

Theorem 1.12 (Hironaka). *Assume* $\operatorname{char} k = 0$ *(not necessarily $k = \bar{k}$). Let V/k be a variety. Then there is a finite sequence of blow-ups in the singular locus*

$$\pi : \tilde{V} = V_n \to V_{n-1} \to \cdots \to V_0 = V$$

such that $\tilde{V}$ is non-singular.

π is an isomorphism over the non-singular locus of V. For a singular point $P \in V$ the fibre $\pi^{-1}P$ is a projective variety.
Example: $V(y^2 - x^2(x-1) \subset \mathbb{A}^2$ has the singular point $(0,0)$. Blow-up of $\mathbb{A}^2$ in $(0,0)$: replace the point by all lines through it.

$$\tilde{A^2} = \{(x, y, [\tilde{x} : \tilde{y}]) \mid x\tilde{y} = \tilde{x}y\}$$

For $x \neq 0$, the point $[\tilde{x} : \tilde{y}]$ is uniquely determined by (x, y). Similarly for $y = 0$. For $(x, y) = (0, 0)$ the condition becomes empty and the fibre is a copy of $\mathbb{P}^1$.

In this case $\tilde{V} \subset \tilde{A^2}$ is the irreducible subvariety containing points $(x, y) \neq (0, 0)$ with the equation $y^2 = x^2(x-1)$. It contains two points above $(0, 0)$ corresponding to the two tangents to V.

2 Algebraic cycles and Intersection Theory

Literature: Fulton, Hartshorne App. A

Theorem 2.1 (Bezout). *Let C_1, C_2 be curves in $\mathbb{P}^2$ of degree n and m which have no common irreducible components. Then $C_1 \cap C_2$ consists of nm points counted with multiplicity.*

The degree of a curve is the degree of the homogenuous polynomial that defines it.
Example: By abuse of notation we work in $\mathbb{A}^2 \subset \mathbb{P}^2$. $C_1 = V(y)$, $C_2 = V(y - F(x)$. Then $C_1 \cap C_2$ is the set of zeroes of F. In this case we understand multiplicities of of zeroes. In order to understand the Theorem, we need to define multiplicities in general.

Definition 2.2. *Let V be an variety, $P \in V$. Then*

$$\mathcal{O}_P = \lim_{P \in U} \mathcal{O}(U) = \{f \in \mathcal{O}(U) \mid P \in U\} / \sim$$

where for $f_i \in \mathcal{O}(U_i)$ we have $f_1 \sim f_2$ if there is $V \subset U_1 \cap U_2$ such that $f_1 = f_2$ on V is called stalk of $\mathcal{O}$ in P. *Similarly*

$$k(V) = \lim_{U} \mathcal{O}(U)$$

If $V = V_1 \cup \cdots \cup V_n$ with proper closed subvarieties V_i, then

$$k(V) = k(V_1) \oplus \ldots k(V_n)$$

If V is irreducible, then $k(V) = Q(\mathcal{O}(V))$ the field of fractions of the integral domain $\mathcal{O}(V)$. In this case $k(V)$ is called *function field* of V.

Definition 2.3. *Let C_1, C_2 be curves in V. Then the* intersection multiplicity *in $P \in C_1 \cap C_2$ is defined as*

$$m_P(C_1, C_2) = \dim_k \mathcal{O}_{C_1,P} \otimes_{\mathcal{O}_{V,P}} \mathcal{O}_{C_2,P}$$

Example: $C_1 = V(x)$, $C_2 = V(y)$ in $\mathbb{A}^2$ and $P = (0,0)$ Then.

$$\mathcal{O}(C_1) \otimes_{\mathcal{O}(\mathbb{A}^2)} \mathcal{O}(C_2) = k[x,y]/x \otimes_{k[x,y]} k[x,y]/y \cong k$$

The intersection multiplicity is 1. $C_2 = V(y^2)$ yields

$$\mathcal{O}(C_1) \otimes_{\mathcal{O}(\mathbb{A}^2)} \mathcal{O}(C_2) = k[x,y]/x \otimes_{k[x,y]} k[x,y]/y^2 \cong k[y]/y^2$$

has dimension 2.

Higher dimensional intersection theory

Definition 2.4. *Let V be a variety. Let $Z^p(V)$ the group of formal $\mathbb{Z}$-linear combinations of irreducible subvarieties of codimension p. Elements of $Z^p(V)$ are called* p-cylces*, the generators* primitive p-cycles.

Two primitive cycles $\Gamma_1, \Gamma_2 \subset V$ intersect *properly* if all irreduble components W of $\Gamma_1 \cap \Gamma_2$ have codimension equal to $\operatorname{codim} \Gamma_1 + \operatorname{codim} \Gamma_2$.
Remark: For curves in $\mathbb{P}^2$ this means that they have no component in common as in Bezout's theorem.

Serre has given a definition of an intersection multiplicity $m_W(\Gamma_1, \Gamma_2)$ for such cycles. This yields a partially defined map

$$Z^p(V) \times Z^q(V) \to Z^{p+q}(V)$$

By imposing an appropriate equivalence relation $A^p(V) = Z^p(V)/\sim$ this implies an *intersection pairing*

$$A^p(V) \times A^q(V) \to A^{p+q}(V)$$

Definition 2.5. $\Gamma_0, \Gamma_1 \in Z^p(V)$ *are* rationally equivalent *if there is a cycle $\Gamma \in Z^p(V \times \mathbb{P}^1)$ such that $\Gamma \cap V \times \{0\} = \Gamma_0$ and $\Gamma \cap V \times \{1\} = \Gamma_1$.*

Proposition 2.6 (Chow's moving lemma)**.** *Let V be smooth quasi-projective and $\Gamma_1, \Gamma_2 \in Z^p(V)$. Then there is $\Gamma_1' \sim \Gamma_1$ such that Γ_1' intersects Γ_0 properly. The induced* intersection pairing

$$A^p(V) \times A^q(V) \to A^{p+q}(V)$$

is well-defined.

The graded ring $A^*(V)$ is called *Chow ring.*

Example: For $0 \leq p \leq n$ we have $A^p(\mathbb{P}^n) \cong \mathbb{Z}$ generated by $\mathbb{P}^{n-p} \subset \mathbb{P}^n$. Let C_1, C_2 be irreducible curves in $\mathbb{P}^2$. Then $[C_i] \in A^1(\mathbb{P}^2) \cong \mathbb{Z}$ is given by the degree. Under the intersection pairing

$$A^1(\mathbb{P}^2) \times A^1(\mathbb{P}^2) \to A^2(\mathbb{P}^2), \qquad ([C_1], [C_2]) \mapsto \deg C_1 \cdot \deg C_2$$

Warning: Even for projective curves $C/\mathbb{C}$ the group $A^p(C)$ is not finitely generated in general!

Riemann-Roch

Definition 2.7. *Let X be a variety. A* vector bundle *V on X is a map $p : V \to X$ such that $X = \bigcup U_i$ and*

$$p^{-1}U_i \cong U_i \times \mathbb{A}^n \to U_i$$

and the transition maps on $U_i \cap U_j$ respect the fibres and are linear on the fibres.

Let X be smooth irreducible. Let $L \to X$ be a line bundle, ie. a vector bundle with fibre dimension $n = 1$. We want to define the *chern class*

$$c_1(L) \in A^1(X)$$

A trivialization of L over a covering U_i induces transition maps

$$f_{ij} : U_i \cap U_j \times \mathbb{A}^1 \to U_i \cap U_j \times \mathbb{A}^1 \qquad (x, 1) \mapsto (x, \tilde{f}_{ij}(x))$$

with $\tilde{f}_{ij} \in \mathcal{O}(U_i \cap U_j)^*$. These $\tilde{f}_{ij}$ have to satisfy a cocycle condition for triple intersections. We can assume U_i affine.

We fix one index i_0 and put

$$f_j \in \tilde{f}_{i_0 j} \in \mathcal{O}(U_{i_0} \cap U_j) \subset k(U_j) = Q(\mathcal{O}(U_j))$$

hence $f_j = P_j/Q_j$ with $P_j, Q_j \in \mathcal{O}(U_j)$. Then

$$\mathrm{Div}(f_j) = \mathrm{Div}(P_j) - \mathrm{Div}(Q_j) \in Z^1(U_j)$$

where $\mathrm{Div}(f)$ denotes the subvariety of U_j defined by f (with multiplicities of components). These glue to define a cycle in $Z^1(X)$. It is in fact well-defined in $A^1(X)$.

Recall that in the case X a curve, $A^1(X)$ consists of formal linear combinations of points.

Theorem 2.8 (Riemann-Roch)**.** *Let C be a complete smooth irreducible curve and L a line bundle on C with $D = c_1(L)$. Then*

$$\dim_k H^0(C, L) - \dim_k H^1(C, L) = \deg D + 1 - g$$

where g is the genus of C.

The cohomology in the statement is cohomology of coherent sheaf. In particular $H^0(C, L)$ is the group of global sections $s : C \to L$ of L. We have $H^1(C, L) \cong H^0(C, K \otimes L^\vee)^\vee$ for the canonical bundle on C. This reformulation is often usefull.

Higher dimensional Riemann-Roch

Let X be smooth irreducible variety. The first Chern class generalizes to higher Chern classes

$$c_p : \mathrm{VB}/X \to A^p(X)$$

characterised by the following property: We denote $c_t(V) = \sum c_p(V)t^p \in A^*(X)$

1. $c_t(L) = 1 + c_1(L)t$ for line bundles
2. For $f : X' \to X$ we have $c_p(f^{-1}V) = f^{-1}c_p(V)$
3. c_t is multiplicative on short exact sequences of vector bundles.

The behaviour of c_t under $\otimes$ is complicated. Instead we formulate in terms of the *Chern character*

$$\mathrm{ch} : \mathrm{VB}/X \to A^*(X)$$

with $\mathrm{ch}_n = \frac{1}{n!}P_n(c_1, \ldots, c_n)$ implicity defined by

$$P_n - c_d P_{n-1} + c_2 P_{n-2} \pm +(-1)^n n c_n = 0$$

The Chern character is compatible with $\oplus$ and $\otimes$.

Definition 2.9. *$K_0(X)$ ist the Grothendieck group of vector bundles on X. It is the abelian group generated by (isomorphism classes of) vector bundles on X with relations*

$V \sim V_1 + V_2$ *if there is a short exact sequence* $0 \to V_1 \to V \to V_2 \to 0$

In fact,

$$\mathrm{ch} : K_0(X)_{\mathbb{Q}} \to A^*(X)_{\mathbb{Q}}$$

is an isomorphism of vector spaces.

Theorem 2.10 (Grothendieck-Riemann-Roch)**.** *Let $f : X \to Y$ be a proper map of smooth varieties. Then the diagram*

$$\begin{array}{ccc} K_0(X) & \xrightarrow{\mathrm{Td}_X \mathrm{ch}} & A^*(X)_{\mathbb{Q}} \\ {\scriptstyle f_*}\downarrow & & \downarrow{\scriptstyle f_*} \\ K_0(Y) & \xrightarrow[\mathrm{Td}_Y]{} & A^*(Y)_{\mathbb{Q}} \end{array}$$

commutes where $\mathrm{Td}_X \in A^*(X)$ *is the* Todd class*.*

The classical case follows with Y a point and X a smooth proper curve.

3 Schemes

Affine varieties are defined by polnomial equations over $k = \bar{k}$. Affine schemes do the same over general rings.

Let A be a commutative ring with 1.

Definition 3.1.

$$\mathrm{Spec} A = \{\mathfrak{p} \subset A \mid \mathfrak{p} \textit{ prime ideal } \}$$

If $\mathfrak{a} \subset A$ is an ideal, then

$$V(\mathfrak{a}) = \{\mathfrak{p} \in \mathrm{Spec} A \mid \mathfrak{a} \subset \mathfrak{p}\}$$

Using the $V(\mathfrak{a})$ as closed sets, we have a topology on $\mathrm{Spec} A$ as in the case of varieties.
Example:

1. $A = k[X_1, \dots, X_n]$ with $k = \bar{k}$. By Hilbert's Nullstellensatz we have bijection

   $$\{\mathfrak{m} \subset A \mid \mathfrak{m} \text{ maximal ideal }\} \leftrightarrow \{(X_1 - a_1, \dots, X_n - an) \mid (a_1, \dots, a_n) \in k^n\}$$

   The left hand side is contained in Spec$A$. Moreover, $V(\mathfrak{a})$ in the sense of varieties is given by the $V(\mathfrak{a}) \cap \{\mathfrak{m}\}$. Moreover, for a prime ideal $\mathfrak{p}$, the variey $V(\mathfrak{p})$ is irreducible. This means

   $$\mathrm{Spec}A = \{\text{irreducible subvarieties of } \mathbb{A}^n\}$$

   The Zarsiki-topologies agree.

2. $A = \mathbb{Q}[X]/X^2 + 1 = \mathbb{Q}(i)$ is a field, i.e., Spec$\mathbb{Q}[X]/X^2 + 1 = \{0\}$ has only point point. It is the subscheme of $\mathbb{A}^1_{\mathbb{Q}}$ defined by $X^2 + 1$, i.e., $V(X^2+1) \subset \mathrm{Spec}\mathbb{Q}[X]$. On the other hand $V(X^2+1)$ over $\bar{Q}$ consists of two points, corresponding to $\pm i$.

3. Spec$\mathbb{Z} = \{\eta = 0\} \cup \{(p) \mid p \text{ prime number }\}$ because $\mathbb{Z}$ is a principal ideal domain. Any ideal $\mathfrak{a} = (a)$ with $a \in \mathbb{Z}$ defines

   $$V(\mathfrak{a}) = \{\mathfrak{p} \mid \mathfrak{a} \subset \mathfrak{p}\} = \{p \mid p \mid a\}$$

   the prime divisors of a. Hence $V(\mathfrak{a})$ is either finite or all of Spec$\mathbb{Z}$. If $U \subset \mathrm{Spec}\mathbb{Z}$ is open, non-empty, then its complement does not contain η. Hence $\{\eta\}$ is dense!

In general: If $\{\mathfrak{p}\} \subset \mathrm{Spec}A$ is closed, then $\mathfrak{p}$ is a maximal ideal.

Note that we have topological space but it carries little information. E.g. for all fields Spec$k$ is just one point. The interesting part of the information is put in a sheaf of rings.

Lemma 3.2. *The sets of the form*

$$U_f = \{\mathfrak{p} \in \mathrm{Spec}A \mid f \notin \mathfrak{p}\} = \mathrm{Spec}A \setminus V(f)$$

for $f \in A$ form a basis of the topology. We have

$$U_f = \mathrm{Spec}A_f \qquad A_f = \{\frac{a}{f^n} \mid a \in A, n \in \mathbb{N}\}/\sim$$

Proposition 3.3. *There is a unique sheaf of rings $\mathcal{O}$ on* Spec$A$ *with $\mathcal{O}(U_f) = A_f$.*

In particular, $\mathcal{O}(\mathrm{Spec}A) = A$.

Definition 3.4. *A* scheme *is a topological space X together with a sheaf of rings $\mathcal{O}_X$ such that $X = \bigcup_{i \in I} U_i$ is an open covering such that*

$$(U_i, \mathcal{O}\mid_{U_i}) = (\mathrm{Spec}A_i, \mathcal{O}) \textit{ for all } i \in I\}$$

Example:

1. k a field. $\mathrm{Spec}k = \{*\}$ with $\mathcal{O}(\mathrm{Spec}k) = k$.

2. V an affine variety over $k = \bar{k}$. Let $\tilde{V}$ be the set of irreducible subvarieties of V. It contains V because points are 0-dimensional subvarieties. For $\tilde{U} \subset \tilde{V}$ put $\mathcal{O}(\tilde{U}) = \mathcal{O}(\tilde{U} \cap V)$. This is $\mathrm{Spec}k[X_1, \dots, X_n]/I(V)$.

3. $\mathcal{C} = \mathrm{Spec}\mathbb{Z}[X,Y]/Y^2 = X(X-1)(X+1)$ is an example of an arithmetic surface. The elements of $\mathcal{C}$ fall in two classes:

$$\begin{aligned} \mathcal{C}_p &= \{\mathfrak{p} \in \mathcal{C} \mid p \mid \mathfrak{p}\} \qquad p \text{ prime number} \\ \mathcal{C}_\eta &= \{\mathfrak{p} \in \mathcal{C} \mid \text{there is no } p \text{ in } \mathfrak{p}\} \end{aligned}$$

   Then

$$\begin{aligned} \mathcal{C}_p &\cong \mathrm{Spec}\mathbb{F}_p[X,Y]/Y^2 = X(X-1)(X+1) \\ \mathcal{C}_\eta &\cong \mathrm{Spec}\mathbb{Q}_p[X,Y]/Y^2 = X(X-1)(X+1) \end{aligned}$$

   By base-change to $\bar{\mathbb{F}}_p$ and $\bar{\mathbb{Q}}$ we are in the situation of varieties. They are non-singular with exception of $p = 2$, when there is a simple double point.

Strange effects occur in schemes which are not allowed in varieties.

1. $\mathrm{Spec}k[X,Y]/X^2$ is homeomorphic to $\mathrm{Spec}k[X]$ because $V(X) = V(X^2)$ as sets. However, they are not isomorphis as schemes. There may be nilpotent elements in $\mathcal{O}$.

2. $\mathrm{Spec}k[[X]] = \{\eta = 0, \xi = (X)\}$. The point η is dense, ξ is closed. We visualize this scheme as an open disc with ξ the center and η any other point (with varying "any").

Properties of Schemes

Let S be a scheme.

Definition 3.5. *The category* Sch_S *of schemes over S has as objects morphisms of schemes $f : X \to S$ and as morphisms commutative diagrams $F : X \to X'$ such that $f'F = f$.*

A morphism $f : X \to S$ is called *separated* when for all $C \subset \bar{C}$ of irreducible 1-dimensional schemes and all diagrams

$$\begin{array}{ccc} C & \longrightarrow & X \\ \big\downarrow & & \big\downarrow \\ \bar{C} & \longrightarrow & S \end{array}$$

the lift $\bar{f} : \bar{C} \to X$ is unique. f is called *proper* if $\bar{f}$ exists and is unique. f is called *flat* if for all $P \in X$ the morphism

$$\mathcal{O}_{S,f(P)} \to \mathcal{O}_{X,P}$$

is flat, i.e. the functor $\cdot \otimes_{\mathcal{O}_{S,f(P)}} \mathcal{O}_{X,P}$ is exact.

As in the case of varieties, separated corresponds to Haussdorff in the case of manifolds. Proper corresponds to proper, i.e., preimages of compact sets are compact. Flatness is unintuitive. It implies for example that that the fibre-dimension of f is constant.

Example: $f : V \to \mathrm{Spec}k$ for a field k is always flat.

The morphism $f : X \to S$ is *smooth* if f is flat and all geometric fibres

$$\begin{array}{ccc} X_{\bar{P}} & \longrightarrow & X \\ \big\downarrow & & \big\downarrow \\ \bar{P} & \longrightarrow & S \end{array}$$

(with $\bar{P} = \mathrm{Spec}\bar{k}$ with $\bar{k}$ a algebraically closed field) are smooth in the sense of varieties (Jacobi-criterion). **Example:** Our arithmetic surface $\mathcal{C}$ is smooth over $\mathrm{Spec}\mathbb{Z} \setminus \{(2)\}$

4 Moduli problems

Definition 4.1. *Fix a scheme X/S (i.e, $f : X \to S$). For $T \to S$ let*

$$X(T) = \mathrm{Mor}_S(T, X)$$

Example: Let $S = \mathrm{Spec}\mathbb{Q}$, $X = \mathrm{Spec}\mathbb{Q}[X,Y]/F$ and $T = \mathrm{Spec}K$ where $K/\mathbb{Q}$ is a field extension. Then

$$\begin{aligned} X(T) &= \{\mathrm{Spec}K \to \mathrm{Spec}\mathbb{Q}[X,Y]/F \mid \text{ over } \mathrm{Spec}\mathbb{Q}\} \\ &= \{K \leftarrow \mathbb{Q}[X,Y]/F \mid \mathbb{Q}\text{-linear}\} \\ &= \{(a,b) \in K^2 \mid F(a,b) = 0\} = V(F) \subset K^2 \end{aligned}$$

the set of solutions of F in K.

Proposition 4.2 (Yoneda-Lemma). *X is uniquely determined by the functor*

$$X(\cdot) : \mathrm{Sch}_S \to \mathrm{Mengen}$$

This is quite formal and holds for all categories. An object is characterized by a univeral property.

Example: Given X/S and Y/S we want to define $X \times_S Y$. Note that set-theoretically $\mathbb{A}^1 \times \mathbb{A}^1 \neq \mathbb{A}^2 = \mathrm{Spec} k[X, Y]$. Instead:

$$X \times_S Y(T) = X(T) \times_{S(T)} Y(T)$$

fibre product of sets. This means:

Given a pair of maps $f : T \to X$ and $g : T \to S$ compatible with the projection to S, there is a unique map $T \to X \times_S Y$ making the diagram commute. The uniqueness of $X \times_S Y$ is garanteed by the Yoneda-Lemma. The existence has to be checked. If follows from the existence of tensor products. **Example:** A *group scheme* is a pair of maps

$$\mu : G \times_S G \to G \qquad e : S \to G$$

such that $G(T)$ with $\mu(T) : G(T) \times G(T) \to G(T)$ is a group with neutral element $e(T) \in G(T)$.

1. The general linear group: GL_n with $\mathrm{GL}_n(\mathrm{Spec} A)$ invertible $n \times n$-matrices with coefficients in A.

2. If $A/\mathrm{Spec}\mathbb{C}$ is a proper group scheme, then it is abelian. (Abelian variety). It is of the form $\mathbb{C}^g/\Lambda$ for a lattice Λ.

Moduli spaces of elliptic curves

Aim:

Definition 4.3. *Let the functor*

$$M : \mathrm{Sch}/\mathrm{Spec}\mathbb{Z} \to \mathrm{Sets}$$

be given by

$$M(T) = \{\mathcal{E} \to T\}/\sim$$

Theorem 4.4. *(Roughly speaking) M is the functor of points of a scheme over* $\mathrm{Spec}\mathbb{Z}$*, i.e., there is X such that $X(T) = M(T)$.*

Definition 4.5. *Let $k = \bar{k}$ be an algebraically closed field. A smooth complete curve E/k is called* elliptic *if it has genus* 1 *(cf. Riemann-Roch).*

Equivalently, it is defined by an equation of degree 3 in $\mathbb{P}^2$. **Example:** $y^2 = x(x-1)(x+1)$ (if $2 \neq 0$ in k).

Over the complex numbers, an elliptic curve is nothing but a compact Riemann surface of genus 1. It has always the form $\mathbb{C}/\Gamma$ for some lattice Γ. This representation shows that there is an abelian group law on E. For general k, pick a point $0 \in E$. Then there is an geometrically defined group law on E. It works as follows. Let E be given by a equation of degree 3.

1. Let $P, Q \in E$. Let L be the line through P, Q. It intersects E in a third point H.

2. Let L' be the line through 0 and H. It intersects E in a third point $P + Q$.

The hard part is associativity. The group law depends on the choice of 0, but it is well-defined up to translation.

Definition 4.6 (2nd version)**.** *Let $k = \bar{k}$. An* elliptic curve *is a curve E of genus* 1 *together with the choice of a point $0 \in E$.*

Let T be a scheme. An elliptic curve *$\mathcal{E}$ over T (sometimes* family of elliptic curves *is an T-scheme $f : \mathcal{E} \to T$ such that f is flat and such that all geometric fibres are elliptic curves together with a section $0 : T \to \mathcal{E}$ of f.*

This induces a group law $\mathcal{E} \times_T \mathcal{E} \to \mathcal{E}$ with unit section 0.

We want to determine elliptic curves over a given T up to isomorphism. We start with $M(\mathbb{C})$, the set of isomorphism classes of elliptic curves over $\mathbb{C}$.

$$M(\mathbb{C}) = \{\mathbb{C}/\Gamma \mid \Gamma \subset \mathbb{C} \text{ lattice } \}/\sim$$

Let $\Gamma = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Then multiplication by ω_1^{-1} induces an isomorphism

$$\mathbb{C}/\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \to \mathbb{C}/\mathbb{Z} + \mathbb{Z}\frac{\omega_2}{\omega_1}$$

i.e, we can choose $\Gamma = \mathbb{Z} + \mathbb{Z}\tau$ with $\tau \in \mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im} z > 0\}$.

Proposition 4.7. *Let $\tau, \tau' \in \mathbb{H}$. Then*

$$\mathbb{C}/\mathbb{Z} + \tau\mathbb{Z} \cong \mathbb{C}/\mathbb{Z} + \tau'\mathbb{Z}$$

if and only if

$$\tau' = \gamma\tau = \frac{a\tau + b}{c\tau + d} \textit{ with } \}\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

E.g. $\tau \mapsto \tau + 1$ is given by the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. This means

$$M(\mathbb{C}) = \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$$

Problem: M cannot be given by a scheme. Suppose M is represented by Y. Then

$$\mathrm{id} \in \mathrm{Mor}(Y, Y) = Y(Y) = M(Y)$$

corresponds to a universal elliptic curve. Its pull-back to $Y_{\mathbb{C}}$ should be given by

$$\mathbb{H} \times \mathbb{C}/\mathrm{SL}_2(\mathbb{Z}) \rtimes \mathbb{Z}^2$$

where $(\gamma, z)(\tau, z) = (\gamma\tau, z + \gamma)$: For fixed τ this is $\mathbb{C}/\mathbb{Z} + \tau\mathbb{Z}$. However, for $\tau = i$ this does not work globally.... TODO

Rigidification

Let $N \geq 1$, E an elliptic curve. We denote

$$E[N] = \text{ kernel of multiplication by } N$$

with respect to the group law on E. This is the *N-torsion* of E.
Example: Let $E = \mathbb{C}/\mathbb{Z} + \tau\mathbb{Z}$. Then

$$E[N] = \frac{1}{N}\mathbb{Z} + \frac{\tau}{\mathbb{Z}}/\mathbb{Z} + \tau\mathbb{Z} \cong (\mathbb{Z}/NZ)^2$$

We define new moduli problems:

$$M_N(T) = \{(\mathcal{E} \to T, \alpha) \mid \ \mathcal{E} \text{ elliptic curve}, \alpha : (\mathbb{Z}/N)^2_T \cong \mathcal{E}[N]\}/\sim$$

The choice of α is called *level-N-structure*.

Theorem 4.8. *Let $N \geq 3$. Then M_N is represented by a flat curve $Y_N \to \mathrm{Spec}\mathbb{Z}$. It is smooth outside $p \mid N$. The curve Y_N has a canonical compactification $X_N \to \mathrm{Spec}\mathbb{Z}$ such that X_N is proper and flat.*

The Y_N and X_N are called *moduli curves.*
Example: $Y_N(\mathbb{C}) = \mathbb{H}/\Gamma(N)$ with

$$\Gamma(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma = \mathrm{id} \mod N\}$$

and $X(N) = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}/\Gamma(N)$. This adds finitely many points to $Y(N)$, the *cusp.*

Why is this useful? We can say more about varieties/schemes defined by moduli problems that about varieties defined directly by equations. **Example:** Let $N = mm'$. This induces $\beta : \mathbb{Z}/m \cong m'\mathbb{Z}/N\mathbb{Z} \subset \mathbb{Z}/N\mathbb{Z}$ and hence $\beta^* : M_N(T) \to M_m(T)$ by operating on the level structures: $\alpha \mapsto \alpha\beta$. This is a transformation of functors, hence it induces a morphism of schemes $\beta^* : Y_N \to Y_m$. Over $\mathbb{C}$ this is

$$\mathbb{H}/\Gamma(N) \to \mathbb{H}/\Gamma(m)$$

induces by the inclusion $\Gamma(N) \subset \Gamma(m)$. Many interesting maps between moduli curves are induced by this type of morphism. They induce interesting operations on cohomology, in particular the *Hecke operators.*

Theorem 4.9 (Wiles et al., Conjecture of Shimura-Taniyama-Weil)**.** *If $E/\mathbb{Q}$ is an elliptic curve, then there is a covering map*

$$X_{N,\mathbb{Q}} \to E$$

for some explicit N.

We say that E is *modular.*

Corollary 4.10 (Fermat's last theorem)**.** *$x^n + y^n = z^n$ has no solutions in $\mathbb{N}$ for $n \geq 3$.*

The theory of moduli curves generalizes to Shimura varieties belonging to other reductive groups than $\mathrm{GL}_2(\mathbb{R})$.

There are many other examples of moduli problems:

1. subvectorbundles of $\mathbb{A}^n \to \mathrm{Spec}\mathbb{Z}$. This gives Grassmannian varieties. Consider the special case of sub-line-bundels of $\mathbb{A}^{n+1}$

$$G(\mathrm{Spec}k) = \{ \text{ lines in } k^{n+1} \text{ through } 0\} = \mathbb{P}^n(k)$$

All Grassmannian exist, are smooth and projective.

2. Moduli spaces of smooth complete curves of higher genus form a moduli space (again after rigidification). The moduli problem is compactified by "stable curves".

3. vector bundels on a scheme S: the moduli problem has good properties when restricting to "semi-stable" ones.

4. Fix X and consider the moduli problem of p-cycles in X.

There is a standard machine to treat moduli problems.

1. First consider the situation over a field k.

2. Then pass to *nilpotent thickenings* $k[t]/t^n$. The spectrum of this ring has just one point, but an non-trivial structure sheaf. This step should be treated by induction on n. Usually the step $1 \to 2$ is the essential one.

3. Information for all thickenings is equivalent to information over $k[[t]]$.

4. Show that it comes from $k[t]$

5. Glue.

5 Weil Conjectures

Literature: Hartshorne App. C, Deligne Weil I, II.

Let p be a prime, recall $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We fix $V/\mathbb{F}_p$ a variety, i.e. a reduced scheme of finite type over $\mathbb{F}_p$. Roughly: V is a set of points in $\bar{\mathbb{F}}_p^n$ defined by equations in $\mathbb{F}_p[X_1, \dots, X_n]$. For all $k \geq 1$ Let $\mathbb{F}_{p^k}$ be the unique field with p^k elements. Then

$$V(\mathbb{F}_{p^k}) = V \cap \mathbb{F}_{p^k}^n$$

the set of solutions of the equations in the finite field, is a finite set. More formally,

$$V(\mathbb{F}_{p^k}) = \mathrm{Mor}_{\mathbb{F}_p}(\mathrm{Spec}\mathbb{F}_{p^k}, V)$$

We denote

$$|V(\mathbb{F}_{p^k})| = \nu_k(V)$$

Definition 5.1. *The Zeta-function of V is defined by*

$$\log Z(V,t) = \sum_{k \geq 1} \frac{\nu_k(V)}{k} t^k \in \mathbb{Q}[[t]]$$

This makes $Z(V,t)$ a well-defined rational power-series. **Example:** Let $V = \mathbb{P}^1$. Then

$$\nu_k(\mathbb{P}^1) = \#\mathbb{P}^1(\mathbb{F}_{p^k}) = \frac{(p^k)^2 - 1}{p^k - 1} = p^k + 1$$

Hence

$$\begin{aligned} Z(t) &= \exp(\sum_{k\geq 1}(p^k+1)\frac{t^k}{k} \\ &= \exp(sum\frac{p^k t^k}{k})\exp(\sum\frac{t^k}{k}) \\ &= \exp(-\log(1-pt))\exp(-\log(1-t)) = \frac{1}{(1-pt)(1-t)} \end{aligned}$$

This is striking: $Z(t)$ is a rational function.

Theorem 5.2 (Grothendieck, Deligne, Weil Conjectures)**.** *Let V be a smooth projective variety of dimension n over $\mathbb{F}_p$.*

1. *(rationality) $Z(V,t) \in \mathbb{Q}(t)$ is a rational function.*
2. *(functional equation) $Z(V, 1/p^n t) = \pm p^{nE/2} t^E Z(V,t)$ where E is the self-intersection number of V, i.e. the degree of $\Delta.\Delta$ where Δ is the diagonal of $V \times V$.*
3. *(Riemann hypothesis)*

   $$Z(V,t) = \frac{P_1 P_3 \dots p_{2n-1}}{P_0 P_2 \dots P_{2n}}$$

   with $P_i \in \mathbb{Z}[t]$ integral polynomials such that

   $$P_i(T) = \prod_j (1 - \alpha_{ij} t$$

   with $\alpha_{ij} \in \bar{\mathbb{Q}}$ with absolute value $p^{i/2}$ for any embedding of $\bar{\mathbb{Q}} \to \mathbb{C}$. We always have $P_0 = 1 - t$, $P_{2n} = 1 - p^n t$.
4. *If V is defined as fibre of a flat family $\mathcal{V} \to \mathrm{Spec}\mathbb{Z}$, then $\deg P_i = b_i$ where b_i is the i-th Betti-number of the compact manifold $\mathcal{V}_{\mathbb{C}}$, i.e. the dimension of its i-the singular cohomology group.*

Example: The case $V = \mathbb{P}^1$ was the above computation. Now let $V = E$ be an elliptic curve, i.e., of genus 1. Then $b_0 = b_2 = 1$ and $b_1 = 2$. By the Weil conjectures

$$Z(E, t) = \frac{(1-\alpha)(1-\beta)}{1-t)(1-pt)}$$

with $|\alpha| = |\beta| = p^{1/2}$. This means

$$(1-\alpha t)(1-\beta t) = (1-t)(1-pt)\exp(\sum \frac{\nu_k(E)}{k} t^k)$$

The coefficient of t is

$$\nu_1(E) - p - 1 = -\alpha - \beta \Rightarrow |\#E(\mathbb{F}_p) - (p+1)| = |\alpha + \beta| \leq 2\sqrt{p}$$

This is the *Hasse bound.*

Grothendieck's Ansatz

Let $\bar{V} = V \times \bar{\mathbb{F}}_p$, ie, we consider the equations over the algebraic closure. But as the equations are in fact over $\mathbb{F}_p$, there is the *Frobenius map*

$$\mathrm{Fr} : \bar{V} \to \bar{V} \qquad (x_1, \ldots, x_n) \mapsto (x_1^p, \ldots, x_n^p)$$

Recall that $x \mapsto x^p$ is a field automorphism of $\bar{F}_p$. Hence Fr is well-defined and bijective on $\bar{V}$. We have $x^p = x \leftrightarrow x \in \mathbb{F}_p$. Hence

$$\bar{V}^{\mathrm{Fr}} = V(\mathbb{F}_p), \qquad \bar{V}^{\mathrm{Fr}^k} = \nu_k(V)$$

Grothendieck's idea was to use the Lefschetz fixed point theorem to count the number of fixed points. In order to formulate such a theorem we need a suitable cohomology theory.

Definition 5.3. *A* Weil cohomology theory *is sequence of functors*

$$H^i : \mathrm{Var}/\bar{F}_p \to K\textit{-vector spaces}$$

where K is some field of characteristic zero which behaves like singular cohomology of complex manifolds.

By this we mean in particular:

1. All $H^i(\bar{V})$ are finite dimensional, they vanish for $i > 2\dim \bar{V}$.
2. There is a cup product $H^i(\bar{V} = \times H^j(\bar{V}) \to H^{i+j}(\bar{V})$.

3. If $\bar{V}$ is smooth and proper, then $H^{2n}(\bar{V}) \cong K$ and $H^i(\bar{V}) \times H^{2n-i}(\bar{V}) \to K$ is a perfect pairing., i.e., H^{2n-i} is dual to H^i.

4. There is a Lefschetz fix point formula. For $\bar{V}$ smooth proper, $f : \bar{V} \to \bar{V}$ a morphism with isolated fix points of multiplicity one (in $\Delta.\Gamma_f \subset \bar{V} \times \bar{V}$), then
$$\#\bar{V}^f = \sum(-1)^i \mathrm{Tr}(f^* : H^i(\bar{V}) \to H^i(\bar{V}))$$

Hence
$$\nu_k(V) = \#\bar{V}^{\mathrm{Fr}^k} = \sum(-1)^i \mathrm{Tr}(\mathrm{Fr}^k \mid H^i(\bar{V}))$$
This implies
$$\begin{aligned} Z(t) &= \exp(\sum_k \sum_i (-1)^i \mathrm{Tr}(\mathrm{Fr}^k \mid H^i(\bar{V}) \frac{t^k}{k}) \\ &= \prod_i \exp\left(\sum_k \mathrm{Tr}(\mathrm{Fr}^k \mid H^i(\bar{V})) \frac{t^k}{k}\right)^{(-1)^i} \\ &= \prod_i \det(1 - \mathrm{Fr}^{-1} t \mid H^i(\bar{V}))^{(-1)^{i+1}} \end{aligned}$$
Put $P_i = \det(1 - \mathrm{Fr}^{-1} | H^i) \in K[T]$. Then
$$Z(T) = \frac{P_1 \dots P_{2n-1}}{P_0 \dots p_{2n}} \in \mathbb{Q}[[t]] \cap K[t] = \mathbb{Q}(t)$$
This shows rationality. Poincaré duality implies the functional equation.

By a remark of Serre, $K = \mathbb{Q}$ is impossible. Instead we use $K = \mathbb{Q}_l$ for $l \neq p$ a prime.

Definition 5.4. *Take a rational number an write it as $l^r a/b$ with $a, b \in \mathbb{Z}$ prime to l. Then*
$$|l^r a/b|_l = l^{-r}$$
defines an absolute value on $\mathbb{Q}$. The field of l-adic numbers $\mathbb{Q}_l$ is the completion with respect to this absolute value.

Theorem 5.5 (Grothendieck et al.)**.** *Etale cohomology with coefficients in $\mathbb{Q}_l$ is a Weil cohomology theory.*

Theorem 5.6 (Deligne)**.** *The above P_i satisfy the Riemann hypothesis.*
$$P_i = \prod(1 - \alpha_j t) \qquad |\alpha_j| = p^{i/2}$$

This easily implies that $P_i \in \mathbb{Z}[t]$ and by definition $\deg P_i = \dim H^i(\bar{V})$. The Betti numbers turn up because for $\mathcal{V} \to \mathrm{Spec}\mathbb{Z}$ flat, proper with $V = \mathcal{V} \times \mathbb{F}_p$ smooth

$$H^i_{et}(\bar{V}) \cong H^i_{sing}(\mathcal{V}_{\mathbb{C}}, \mathbb{Q}_l)$$

Alternatively one can use crystalline cohomology with K an extension of $\mathbb{Q}_p$. This is an imitation of de Rham cohomology. Dwork has proved the first half of the Weil conjectures in this setting.

The basic idea of étale cohomology is to generalize the notion of sheaves to sheaves on generalized topologies. We replace open sets by unramfied covers. The intersection of open sets is replaces by fibre products of covers. In the setting of manifolds we have the implicit function theorem and this defines the same category of sheaves as with open set. However, for varieties it is different. Etale cohomology is nothing but sheaf cohomology for the étale topology.
Literature: Tamme, Introduction to étale cohomology.
Milne: Etale cohomology
Freitag, Kiehl: Etale cohomology and the Weil conjectures
Remark: Deninger tries to use a similar strategy to attack the Riemann hypothesis. $\zeta(s)$ corresponds to $\mathrm{Spec}\mathbb{Z}$ which has dimension 1, hence

$$\zeta(s) = \frac{p_1}{p_0 p_2}$$

such that the zeroes of p_1 are the expected zeroes of ζ with real part 1/2.

First problem: would need an infinite dimensional theory $p_1 = \det(1 - ? \mid H^1(?))$