Introduction to Algebraic Number Theory
Lecture 32

Andrei Jorza
Typeset by Matt Cole

13 Geometry

So far we have considered number fields $K/\mathbb{Q}$ and their rings of integers $\mathcal{O}_K$. We have seen that $\mathcal{O}_K$ is a Dedekind domain, and we've explored the unique factorization of ideals, ramification theory, and counting prime ideals in $\mathcal{O}_K$. But we could instead consider $K/\operatorname{Frac}\mathbb{F}_q[x]$, where $q = p^r$, p prime. K is significant because the set of functions on smooth projective curves over $\mathbb{F}_q$ embeds into K. Crucially, we can define a ring of integers $\mathcal{O} \subset K$ which is a Dedekind domain.

In the next nine lectures, we'll cover smooth and projective curves, their function fields, and elliptic curves.

(13.1) Varieties.

Let K be a field.

Definition 1. The *affine space of dimension n over K* is $\mathbb{A}_k^n = \{(x_1, \dots, x_n) \in K^n\}$.
The *projective space of dimension n over K* is $\mathbb{P}_k^n = \{(x_0 : \dots : x_n) \in K^{n+1} \backslash \{0 : \dots : 0\}\} \,/\, K^\times$.

Definition 2. An *affine variety* is the zero locus $V(I)$ of a prime ideal $I \subset K[x_1, \dots, x_n]$.
A *projective variety* is the zero locus $V(I)$ of a prime ideal $I \subset K[x_0, \dots, x_n]$ generated by a homogeneous polynomial.

Definition 3. Let $I = (f_1, \dots, f_n) \subset K[x_0, \dots, x_n]$. $p \in V(I)$ is *smooth* if the Jacobian $(\frac{\partial f_i}{\partial x_j}(p))$ has rank equal to $\dim V := \operatorname{trans\,deg} K(V)/K$, where $K(V) := K[x_1, \dots, x_n]/I$ is the field of functions on V.

Definition 4. $m_p := \{f \in K(V) \mid f(p) = 0\}$, an ideal. $K(V)_p := \{\frac{f}{g} \mid f, g \in K(V),\, g(p) \neq 0\}$.

Proposition 5. *If V is smooth at p, then $K(V)_p$ has m_p as its unique maximal ideal, and every ideal is m_p^n for some n.*

Example 6. Let $V_1 = (y^2 = x^3 + x)$, $V_2 = (y^2 = x^3 + x^2)$, and $p = (0, 0)$. We compute

$$\begin{aligned} K(V_1) &= K[x,y]/(y^2 - x^3 - x); \\ m_p &= \{f(x,y) \mid f \text{ has no constant term}\} = (x,y); \\ m_p^2 &= (x,y)(x,y) = (x^2, xy, y^2) = (x^2, xy, x^3 + x) = (x^2, xy, x) = (x); \\ m_p^{n+1} &= (x^n). \end{aligned}$$

$$\begin{aligned} K(V_2) &= K[x,y]/(y^2 - x^3 - x^2); \\ m_p &= (x,y); \\ m_p^2 &= (x^2, xy, x^3 + x^2) = (x^2, xy). \end{aligned}$$

So in the case of V_2, $m_p \supsetneq (x) \supsetneq m_p^2$.

Definition 7. Let V be smooth at p and $f \in K(V)$. We define $\text{ord}_p(f) = n$ if $f \in m_p^n \setminus m_p^{n+1}$.

Example 8. If V_1 is as in the example above, $x \in K(V_1)$ has $\text{ord}_p(x) = 2$, and $y \in K(V_1)$ has $\text{ord}_p(y) = 1$.

Definition 9. Let V be smooth at p. $f \in K(V)_p$ is a *uniformizer* if $\text{ord}_p(f) = 1$.

Definition 10. A *curve* C is a projective variety of dimension 1.

Example 11. The variety given by $y^2 z = x^3 + xz^2$ is a curve.

Theorem 12. *Let C be a curve smooth at p and let t be a uniformizer at p. Then $K(C)/K(t)$ is a finite separable extension.*

Example 13. Let $C: \ y^2 = x^3 + x$ with $t = y$. Then $K(C)/K(t)$ is a cubic extension.

Think of t as the variable from the Implicit Function Theorem. Also, note that $K(t)$ is like $\mathbb{Q}$, and $K(C)$ is like a number field.

(13.2) Maps between Varieties

Let C_1, C_2 be smooth projective curves.

Definition 14. A *morphism* $f : C_1 \to C_2$ is a map $f = (f_1, \ldots, f_m)$, $f_i \in K(C_1)$, s.t. $\forall p \in C_1$ we get $f(p) \in C_2$ well-defined.

Example 15. The map

$$\begin{aligned} (y^2 z = x^3 + xz^2) &\to \mathbb{P}^1 \\ (x,y,z) &\mapsto (y,z) \end{aligned}$$

is a morphism.

Theorem 16. *Let $f : C_1 \to C_2$ be a morphism on smooth projective curves C_1, C_2. Then f is either constant or surjective.*

Definition 17. Let $f : C_1 \to C_2$ be a morphism. If f constant, define $\deg f = 0$. If f surjective, we have $f^* : K(C_2) \to K(C_1)$ given by $f^*h(p) = h(f(p))\,\forall p \in C_1, h \in K(C_2)$. f^* is injective, so we can say $\deg f := [K(C_1) : f^*K(C_2)]$.

Example 18. The morphism

$$\begin{aligned}(y^2 = x^3 + x) &\to \mathbb{P}^1 \\ (x, y) &\mapsto (y)\end{aligned}$$

has $\deg(y) = 3$.

Fact: $\deg f$ is the number of points of C_1 mapping to a generic point of C_2.