CURVES, JACOBIANS, AND ZETA FUNCTIONS

Introductory Course to the Summer School on

Arithmetic Geometry and Public Key Cryptography

Held in Tel Aviv University, 27.7 – 4.8.2008

by

Moshe Jarden

1. Algebraic Function Fields of One Variable

When we speak about a **function field of one variable over a field** K, we mean a finitely generated regular extension F of K of transcendence degree 1. We briefly recall the definitions of the main objects attached to F/K and their properties. See the books [Che51] or [Sti93] for details. A more comprehensive survey can be found [FrJ08, Sections 3.1-3.2].

A K**-place** of F is a place $\varphi\colon F \to \tilde{K} \cup \{\infty\}$ such that $\varphi(a) = a$ for each $a \in F$. A **prime divisor** $\mathfrak{p}$ of F/K is an equivalence class of K-places of F. Let $\varphi_\mathfrak{p}$ be a place in that class, $v_\mathfrak{p}$ the corresponding discrete valuation of F/K, and $\bar{F}_\mathfrak{p}$ the residue field. The latter field is a finite extension of K which is uniquely determined by $\mathfrak{p}$ up to K-conjugation. We set $\deg(\mathfrak{p}) = [\bar{F}_\mathfrak{p} : K]$. A **divisor** of F/K is formal sum $\mathfrak{a} = \sum k_\mathfrak{p}\mathfrak{p}$, where $\mathfrak{p}$ ranges over all prime divisors of F/K, for each $\mathfrak{p}$ the coefficient $k_\mathfrak{p}$ is an integer, and $k_\mathfrak{p} = 0$ for all but finitely many $\mathfrak{p}'s$. The **degree** of $\mathfrak{a}$ is $\deg(\mathfrak{a}) = \sum k_\mathfrak{p} \deg(\mathfrak{p})$. The divisor attached to an element $f \in F^\times$ is defined to be $\mathrm{div}(f) = \sum v_\mathfrak{p}(f)\mathfrak{p}$, where $\mathfrak{p}$ ranges over all prime divisors of F/K. This makes sense, since $v_\mathfrak{p}(f) = 0$ for all but finitely many $\mathfrak{p}$'s. Further, one attaches to f the **divisor of zeros** $\mathrm{div}_0(f) = \sum_{v_\mathfrak{p}(f)>0} v_\mathfrak{p}(f)\mathfrak{p}$ and the **divisor of poles** $\mathrm{div}_\infty(f) = -\sum_{v_\mathfrak{p}(f)<0} v_\mathfrak{p}(f)\mathfrak{p}$. If $f \notin K$, the degrees of each of these divisors is equal to $[F : K(f)]$. Hence, $\deg(\mathrm{div}(f)) = \deg(\mathrm{div}_0(f)) - \deg(\mathrm{div}_\infty(f)) = 0$. If $\mathfrak{a} = \sum k_\mathfrak{p}\mathfrak{p}$ is a divisor of F/K, we write $v_\mathfrak{p}(\mathfrak{a}) = k_\mathfrak{p}$ for each prime divisor $\mathfrak{p}$ of F/K and note that $v_\mathfrak{p}(\mathrm{div}(f)) = v_\mathfrak{p}(f)$ for each $f \in F^\times$. Given two divisors $\mathfrak{a}, \mathfrak{b}$ of F/K, we write $\mathfrak{a} \le \mathfrak{b}$ if $v_\mathfrak{p}(\mathfrak{a}) \le v_\mathfrak{p}(\mathfrak{b})$ for each prime divisor $\mathfrak{p}$ of F/K. Finally, one attaches to each divisor $\mathfrak{a}$ a finitely generated vector space $\mathcal{L}(\mathfrak{a})$ over K consisting of all $f \in F$ with $\mathrm{div}(f) + \mathfrak{a} \ge 0$ and write $\dim(\mathfrak{a})$ for $\dim(\mathcal{L}(\mathfrak{a}))$.

Note that $f \in \mathcal{L}(\mathfrak{a})$ if and only if $\mathrm{div}_0(f) + \mathfrak{a} \geq \mathrm{div}_\infty(f)$. Since $\mathrm{div}_0(f)$ and $\mathrm{div}_\infty(f)$ have no common prime divisors, the latter condition is equivalent to $\mathfrak{a} \geq \mathrm{div}_\infty(f)$. If $\mathfrak{a} \leq \mathfrak{b}$, then $\mathcal{L}(\mathfrak{a}) \subseteq \mathcal{L}(\mathfrak{b})$.

The Riemann-Roch theorem gives a nonnegative integer g, called the **genus** of F/K, such that if $\deg(\mathfrak{a}) > 2g-2$, then $\dim(\mathcal{L}(\mathfrak{a})) = \deg(\mathfrak{a}) + 1 - g$. In the general case $\dim(\mathfrak{a}) = \deg(\mathfrak{a}) - 1 + g + \dim(\mathfrak{w} - \mathfrak{a})$, where $\mathfrak{w}$ is a **canonical divisor** of F/K [FrJ08, Thm. 3.2.1]. To this end recall that all canonical divisors of F/K are **linearly equivalent** (i.e. differ from each other by a divisor of an element of $F^\times$), $\deg(\mathfrak{w}) = 2g-2$ and $\dim(\mathfrak{w}) = g$ [FrJ08, Lemma 3.2.2].

As an example for the application of the Riemann-Roch theorem we consider a function field F/K of genus 0 with a prime divisor $\mathfrak{p}$ of degree 1. Since $1 > 2 \cdot 0 - 2$, we have $\dim(\mathcal{L}(\mathfrak{p}) = 2$, so there exists $x \in \mathcal{L}(\mathfrak{p}) \smallsetminus K$. It satisfies $\mathfrak{p} \geq \mathrm{div}_\infty(x)$. Hence, $1 \leq [F : K(x)] \leq \deg(\mathfrak{p}) = 1$, so $F = K(x)$ is a **rational function field** over K.

2. Curves

Let F/K be a function field of one variable. By assumption, F/K is a separably generated extension, that is there exists $x \in F$ such that x is transcendental over K and $F/K(x)$ is a finite separable extension. By the primitive element theorem, there exists $y \in F$ with $F = K(x,y)$. Moreover, y can be chosen to be integral over $K[x]$. Thus, there exists a polynomial $f \in K[X,Y]$ such that $f(x,Y) = \mathrm{irr}(x, K(y))$. The assumption that F/K is regular implies that f is absolutely irredicible. It defines an absolutely irreducible affine plane curve Γ that may be defined as a functor $L \rightsquigarrow \Gamma(L)$ from the category of all field extension L of K to the category of sets given by

$$\Gamma(L) = \{(a,b) \in L^2 \mid \ f(a,b) = 0\}.$$

Writing $f(X,Y) = \sum_{i,j \leq d} a_{ij} X^i Y^j$ with $d = \deg(f)$, we may also consider the homogeneous polynomial $f^*(X_0, X_1, X_2) = \sum_{i,j \leq d} a_{ij} X_0^{d-i-j} X_1^i X_2^j$, of degree d. Associated with f^* is the projective plane curve Γ^*, where now

$$\Gamma^*(L) = \{(a_0{:}a_1{:}a_2) \in \mathbb{P}^2(L) \mid \ f^*(a_0, a_1, a_2) = 0\}.$$

Here $(a_0{:}a_1{:}a_2)$ is the equivalence class of all nonzero triples (a_1', a_2', a_3') for which there exists $c \in L^\times$ satisfying $(a_1', a_2', a_3') = (ca_1, ca_2, ca_3)$.

A point (a, b) of $\Gamma(L)$ (also called an **L-rational point** of Γ) is **simple** if $\frac{\partial f}{\partial X}(a,b) \neq 0$ or $\frac{\partial f}{\partial Y}(a,b) \neq 0$. Likewise, an L-rational point $\mathbf{a} = (a_0{:}a_1{:}a_2)$ is **simple** if $\frac{\partial f^*}{\partial X_i}(\mathbf{a}) \neq 0$ for at least one i between 0 and 2. The advantage of a simple point over singular (=nonsimple) points is that its **local ring**

$$O_{\Gamma^*,\mathbf{a}} = \Big\{ \frac{g(1,x,y)}{h(1,x,y)} \mid h, g \in K[X_0, X_1, X_2] \text{ are homogeneous of the same degree and } h(\mathbf{a}) \neq 0 \Big\}$$

(assuming that $a_0 \neq 0$) is a valuation ring of F. If $L = K$, then the local ring corresponds to a **K-rational place** $\varphi_{\mathbf{a}}$ (with $\mathbf{a} = \varphi_{\mathbf{a}}(1,x,y)$), so to a prime divisor $\mathfrak{p}_{\mathbf{a}}$ of degree 1.

The curve Γ^* has two more affine open subsets Γ_1, Γ_2 with coordinate rings $K\big[\frac{1}{x}, 1, \frac{y}{x}\big]$ and $K\big[\frac{1}{y}, \frac{x}{y}, 1\big]$, respectively. They have the same function field F over K as Γ. The three affine pieces $\Gamma, \Gamma_1, \Gamma_2$ together cover Γ.

The curve Γ^* has only finitely many singular points. In an attempt 'to get rid of them', we first consider the integral closure $K[x,y]'$ of $K[x,y]$ in F. It is a finitely generated ring over $K[x,y]$, so has the form $K[x_1, \ldots, x_n]$ for some $x_1, \ldots, x_n \in F$. Assuming that K is perfect (e.g. $\mathrm{char}(K) = 0$ or K is finite), then every local ring of $K[x_1, \ldots, x_n]$ is a valuation ring. Thus, $K[x_1, \ldots, x_n]$ is the coordinate ring of a smooth affine curve Δ in $\mathbb{A}^n$. Similarly, it is possible to normalize Γ_1 and Γ_2 to affine smooth higher dimensional affine curves Δ_1 and Δ_2. Finally, one patches Δ, Δ_1, and Δ_2 together to obtain a projective normalization Δ^* of Δ. The curve Δ^* has the same function field as Δ and there is a surjective morphism $\pi\colon \Delta^* \to \Delta$.

The advantage of the projective smooth model Δ^* of F/K on Δ is that every K-place φ of F gives rise to a point $\mathbf{a} \in \Delta^*(\tilde{K})$ (where $\tilde{K}$ denotes the algebraic closure of K) whose local ring is the valuation ring of φ. This gives a bijective correspondance between $\Delta^*(K)$ and the set of prime divisors of F/K of degree 1. In particular, $\Delta^*(\tilde{K})$ bijectively corresponds to the set of prime divisors of $F\tilde{K}/\tilde{K}$. It follows that the group $\mathrm{Div}(F\tilde{K}/\tilde{K})$ of divisors of $F\tilde{K}/\tilde{K}$ is isomorphic to the free additive Abelian group $\mathrm{Div}(\Delta^*)$ generated by the points in $\Delta^*(\tilde{K})$. The subgroup of all K-rational divisors of

Δ^* (i.e. those that are fixed by $\mathrm{Gal}(K) = \mathrm{Gal}(\tilde{K}/\tilde{K})$) is isomorphic to $\mathrm{Div}(F/K)$.

3. Elliptic Curves and Jacobians

As before, let F be a function field of one variable over a field K (that we assume to be perfect whenever necessary) and let C be a smooth projective model of F/K such that $C(K) \neq \emptyset$. We choose a point $\mathbf{o} \in C(K)$.

First we consider the case where $g = \mathrm{genus}(F/K) = \mathrm{genus}(C)$ is 1. Then there is a bijective correspondance, $\mathbf{p} \to [\mathbf{p} - \mathbf{o}]$ between $C(K)$ and the set of equivalence classes (modulo principal divisors) of divisors of degree 0. For example, if $\mathbf{a}$ is a divisor of degree 0, then, by Riemann-Roch, $\dim(\mathcal{L}(\mathbf{a} + \mathbf{o})) = 1$, so there exists $f \in F^\times$ with $\mathrm{div}(f) + \mathbf{a} + \mathbf{o} \geq 0$. Since the degree of the left hand side is 1, there exists $\mathbf{p} \in C(K)$ such that $\mathrm{div}(f) + \mathbf{a} + \mathbf{o} = \mathbf{p}$. In other words, $[\mathbf{a}] = [\mathbf{p} - \mathbf{o}]$. Thus, our map is indeed surjective.

The set of equivalent K-rational classes of C of degree 0 forms a group. It is therefore possible to apply the bijective correspondance of the preceding paragraph to define addition on $C(K)$ making it an additive Abelian group with $\mathbf{o}$ as the zero point. Anothe application of Riemann-Roch shows that three points $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3 \in C(K)$ lie on the same line if and only if $\mathbf{p}_1 + \mathbf{p}_2 + \mathbf{p}_3 = 0$ (in the group $C(K)$).

Another application of the Riemann-Roch theorem allows us to choose C as a projective plane curve (called an **elliptic curve**) defined by one homogeneous equation of degree 3. If $\mathrm{char}(K) \neq 2, 3$, that equation can be chosen to be

$$X_2^3 = X_0 X_1^2 + A X_0^2 X_1 + B X_0^3,$$

where $A, B \in K$ satisfy $4A^2 + 27B^3 \neq 0$ and $\mathbf{o} = (0{:}1{:}0)$. The geometric rule of addition on $C(K)$ leads to explicit formulas of addition and negation that are often used for computations.

In the general case, where $g \geq 1$, there is a smooth projective variety J (called the **Jacobian** of C) of dimension g defined over K with two morphisms $J \times J \to J$ and $J \to J$, also defined over K, making $J(\tilde{K})$ an additive Abelian group such that the first morphism gives the addition and the second one gives the negation. Thus, J

is an **Abelian variety**. In addition, there is a unique rational morphism $\gamma: C \to J$ defined over K satisfying $\gamma(\mathbf{o}) = 0$ and having the following universal property: If α is a rational map of C into an Abelian variety A defined over K such that $\gamma(\mathbf{o}) = 0$, then there exists a unique morphism map $\beta: J \to A$ such that $\alpha = \beta \circ \gamma$.

One proves that the image $\gamma(C)$ is Zariski closed in J, the map $\gamma: C(\tilde{K}) \to J(\tilde{K})$ is injective, and the set $\gamma(C(\tilde{K}))$ generates $J(\tilde{K})$. The map γ extends linearly to a homomorphism $\beta: \mathrm{Div}(C) \to J(\tilde{K})$ (that is $\beta(\sum_{i=1}^n k_i \mathbf{p}_i) = \sum_{i=1}^n k_i \gamma(\mathbf{p}_i))$. A theorem of Abel says that the restriction β_0 of β to $\mathrm{Div}_0(C)$ gives a short exact sequence:

$$0 \longrightarrow \mathrm{div}((F\tilde{K})^\times) \longrightarrow \mathrm{Div}_0(C) \xrightarrow{\beta_0} J(\tilde{K}) \longrightarrow 0.$$

Finally we note that when $g = 1$, J coincides with the elliptic curve C equipped with the addition law described above. In this case, γ is the identity map.

4. Zeta Functions

The Riemann zeta function is defined for each complex number s with $\mathrm{Re}(s) > 1$ by the convergent series:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Its relation to number theory goes over the Euler product:

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}},$$

where p ranges over all prime numbers. The zeta function satisfies a functional equation that extends the definition of $\zeta(s)$ to a meromorphic function in the whole complex plane. One of the most intriguing open questions in Mathematics is the Riemann Hypothesis: If $\zeta(s) = 0$ and $\mathrm{Re}(s) \geq 0$, then $|s| = \frac{1}{2}$. The Riemann Hypothesis has legion of applications.

Likewise one defines a zeta function for a function field F of genus g over a finite field K of q elements.

$$\zeta_{F/K}(s) = \sum_{\mathfrak{a} \geq 0} \frac{1}{N\mathfrak{a}^s},$$

where $\mathrm{Re}(s) > 1$, $\mathfrak{a}$ ranges over all nonnegative divisors of F/K, and $N\mathfrak{a} = q^{\deg(\mathfrak{a})}$. The Euler product in this case has the form:

$$\zeta_{F/K}(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N\mathfrak{p}^{-s}},$$

where $\mathfrak{p}$ ranges over all prime divisors of F/K.

It is usefull to make a change of variables $t = q^{-s}$ in order to get a Zeta function:

$$Z(t) = \sum_{\mathfrak{a} \geq 0} t^{\deg(\mathfrak{a})}$$

that converges for $|t| < q^{-1}$. If we write A_n for the number of nonnegative divisors of F/K of degree n, we may rewrite $Z(t)$ as a power series:

$$Z(t) = \sum_{n=0}^{\infty} A_n t^n.$$

In particular, A_1 is the number of prime divisors of F/K of degree 1. We set $N = A_1$.

It turns out that $Z(t)$ is a rational function:

$$Z(t) = \frac{L(t)}{(1-t)(1-qt)},$$

where $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g} \in \mathbb{Q}[t]$. Here $a_0 = 1$ and $a_1 = N - (q+1)$. Thus, $Z(t)$ has two poles at $t = 1$ and $t = q^{-1}$. The zeros of $Z(t)$ are the zeros of $L(t)$. Writing their inverses as $\omega_1, \ldots, \omega_{2g}$, we find that $L(t) = \prod_{i=1}^{2g}(1 - \omega_i t)$. One version of the Rieman Hypthesis for F/K asserts that

$$|\omega_i| = \sqrt{q}, \qquad i = 1, \ldots, 2g. \tag{1}$$

It was proved by André Weil in 1948 and reproved with elementary methods by Bombieri [FrJ08, Chapter 4]. Condition (1) is equivalent to the statement that the zeros of $\zeta_{F/K}(s)$ lie on the line $\mathrm{Re}(s) = \frac{1}{2}$. Thus, the Riemann Hypothesis holds for $\zeta_{F/K}$. Another extremely important consequence of (1) follows from the observation that $a_1 = -\sum_{i=1}^{2g} \omega_i$:

$$|N - (q+1)| \leq 2g\sqrt{q}. \tag{2}$$

As an application of (2) consider an absolutely irreducible polynomial $f \in \mathbb{F}_q[X,Y]$ of degree d. Let Γ be the affine plane curve defined by $f(X,Y)=0$. Then

(3) $$q+1-(d-1)(d-2)\sqrt{q}-d \le |\Gamma(\mathbb{F}_q)| \le q+1+(d-1)(d-2)\sqrt{q}.$$

It follows that if q is sufficiently large (in fact, if $q > (d-1)^4$), then $\Gamma(\mathbb{F}_q) \neq \emptyset$. Consequently, if M is an infinite extension of $\mathbb{F}_q$, then M is PAC, that is every absolutely irreducible variety defined over M has an M-rational point.

5. l-adic Representations

Consider an Abelian variety A of dimension g over a field K. Let n be a positive integer with $\mathrm{char}(K) \nmid n$. Then $A_n(\tilde{K}) = \{\mathbf{a} \in A(\tilde{K}) \mid n\mathbf{a} = 0\}$ is an Abelian group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$. In particular, for each prime number $l \neq \mathrm{char}(K)$ and every positive integer i, we have $A_{l^i}(\tilde{K}) \cong (\mathbb{Z}/l^i\mathbb{Z})^{2g}$. The map $\mathbf{a} \mapsto l\mathbf{a}$ is an epimorphism of $A_{l^{i+1}}(\tilde{K})$ onto $A^{l_i}(\tilde{K})$. Thus, we may pass to a limit to get $T_l = T_l(A) = \varprojlim A_{l^i} \cong \mathbb{Z}_l^{2g}$. The free $\mathbb{Z}_l$-module T_l is called the **Tate-module** of A. Tensoring with $\mathbb{Q}_l$ gives a vector space $V_l = T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ over $\mathbb{Q}_l$ of dimension $2g$.

Now note that $\mathrm{Gal}(K)$ leaves each $A_{l^i}(\tilde{K})$ invariant. The action of $\mathrm{Gal}(K)$ commutes with multiplication by l, so it induces an action of $\mathrm{Gal}(K)$ on T_l. Choosing a $\mathbb{Z}_l$-basis of T_l, this action leads to the l-adic representation

$$\rho_l\colon \mathrm{Gal}(K) \to \mathrm{GL}_{2g}(\mathbb{Z}_l)$$

of $\mathrm{Gal}(K)$ associated with A.

Next we turn our attention to the case where K is the field $\mathbb{F}_q$ of q elements. Let φ_q be the Frobenius automorphism of $\tilde{\mathbb{F}}_q$ defined by $\varphi_q(x) = x^q$. As in Section 3, we consider an absolutely irreducible curve C defined over $\mathbb{F}_q$ of genus $g > 0$ having an $\mathbb{F}_q$ rational point $\mathbf{o}$. Let J be the Jacobian variety of C. Then φ_q acts on $C(\tilde{\mathbb{F}}_q)$ and on $J(\tilde{\mathbb{F}}_q)$. The latter action makes φ_q an endomorphism of J defined over $\mathbb{F}_q$. As such $J(\mathbb{F}_q) = \mathrm{Ker}(\mathrm{id}_J - \varphi_q)$ and $|J(\mathbb{F}_q)| = \deg(\mathrm{id}_J - \varphi_q)$ [Mum74, p. 180, Thm. 4].

Considering φ_q as an element of $\mathrm{Gal}(\mathbb{F}_q)$, hence also as an element $\mathrm{Aut}(V_l)$, we have for each prime number l relatively prime to q the characteristic polynomial of

$\rho_l(\varphi_q)$:

$$\chi(t) = \chi_C(t) = \det(\mathrm{id} \cdot t - \varphi_q)$$

It is a monic polynomial of degree $2g$ with coefficients in $\mathbb{Z}_l$. Indeed, $\chi(t)$ does not depend on l and its coefficients are in $\mathbb{Z}$. Moreover, $\chi_l(1) = \det(\mathrm{id}_J - \varphi_q) = |J(\mathbb{F}_q)|$.

Finally let $L(t)$ be the nomerator of the Zeta function descdribed in Section 6. It turns out that $L(t) = t^{2g}\chi(\frac{1}{t})$, so $L(1) = |J(\mathbb{F}_q)|$.

References

[Che51] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable,* Mathematical Surveys VI, AMS, Providence, 1951.

[FrJ08] M. D. Fried and M. Jarden, *Field Arithmetic, Third Edition, revised by Moshe Jarden,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2008.

[Mum74] D. Mumford, *Abelian Varieties,* Oxford University Press, London, 1974.

[Sti93] H. Stichtenoth, *Algebraic Function Fields and Codes,* Springer-Verlag, Berlin, 1993.