Introduction to Drinfeld Modules

9 Sept 2013

1) Motivations:

1.1) Lattices in $\mathbb{C}$:

$\Lambda \subset \mathbb{C}$ is a lattice if it is a discrete subgroup of $(\mathbb{C}, +)$.

$\Lambda \mathbb{R} \cong \mathbb{R}$ or $\mathbb{R}^2$

$\mathbb{R}$: rank 1 $\Rightarrow \Lambda = \omega \mathbb{Z}$

$\mathbb{R}^2$: rank 2 $\Rightarrow \Lambda = \omega_1 \mathbb{Z} + \omega_2 \mathbb{Z}$, $\{\omega_1, \omega_2\}$ lin. indep. over $\mathbb{R}$.

1.2) Rank 1 case: let $\Lambda = 2\pi i \mathbb{Z}$

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & \mu_n \cong \frac{\Lambda}{n\Lambda} = \frac{\mathbb{Z}}{n\mathbb{Z}} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \Lambda & \to & \mathbb{C} & \xrightarrow{\exp} & \mathbb{G}_m(\mathbb{C}) & \to & 1 \\
 & & \downarrow n & & \downarrow n & & \downarrow \varphi_n & & \\
0 & \to & \Lambda & \to & \mathbb{C} & \to & \mathbb{G}_m(\mathbb{C}) & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \frac{\Lambda}{n\Lambda} & & 0 & & 1 & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}$$

$n \in \mathbb{Z}$

$\varphi_n(x) = x^n$

$\exp(nz) = \varphi_n(\exp(z))$

Remarks: 1) $\varphi : \mathbb{Z} \longrightarrow \mathrm{End}\, \mathbb{G}_{m,\mathbb{C}}$

$n \longmapsto \varphi_n \quad (x \mapsto x^n)$

ring homomorphism, gives $\mathbb{Z}$-module structure on $\mathbb{G}_m$.

2) $\ker \varphi_n = \mu_n = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}$

leads to interesting number theory:

Let $K_n = \mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n)$, $\mu_n = \langle \zeta_n \rangle$

$$\mathrm{Gal}(K_n/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(\mu_n) = (\mathbb{Z}/n\mathbb{Z})^*$$

$$\sigma \longmapsto (\zeta_n \mapsto \zeta_n^a \ , \ [a] \in (\mathbb{Z}/n\mathbb{Z})^*)$$

Surjectivity is equivalent to irreducibility of

$$\Phi_n(x) = \prod_{(a,n)=1} (x - \zeta_n^a) \in \mathbb{Z}[X]$$

Theorems: The ring of integers of K_n is $\mathcal{O}_n = \mathbb{Z}[\zeta_n]$

Let $p \in \mathbb{Z}$ be prime. p ramifies in K_n iff $p \mid n$

If $p \nmid n$ then p splits into $|(\mathbb{Z}/n\mathbb{Z})^*|/f$ primes in $\mathcal{O}_n$ each of degree f, where f is the smallest positive integer s.t. $p^f \equiv 1 \bmod n$.

Kronecker-Weber Theorem: Every Abelian extension of $\mathbb{Q}$ lies in some $\mathbb{Q}(\zeta_n)$.

1.3) Rank 2 case: $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$

$$\wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$$ Weierstrass $\wp$-function

converges uniformly on compact subsets in $\mathbb{C} \setminus \Lambda$

Λ-periodic

$$\wp_\Lambda'(z) = -2 \sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^3}$$

$\wp_\Lambda$ satisfies a D.E.

$$(\wp_\Lambda'(z))^2 = 4\wp_\Lambda^3(z) - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda)$$

where $$g_2(\Lambda) = 60 \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^4}$$

$$g_3(\Lambda) = 140 \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^6}$$

} Eisenstein Series

$$\Delta(\Lambda) = g_2^3(\Lambda) - 27 g_3^2(\Lambda) \neq 0$$

For every $z \in \mathbb{C} \setminus \Lambda$, $(x, y) = (\wp_\Lambda(z), \wp_\Lambda'(z))$ satisfies

$$E: y^2 = 4x^3 - g_2 x - g_3$$

Elliptic curve

$$\wp : \mathbb{C} \longrightarrow E(\mathbb{C})$$
$$z \longmapsto \begin{cases} (\wp_\Lambda(z), \wp_\Lambda'(z)) & \text{if } z \notin \Lambda \\ \mathcal{O} \text{ point at } \infty & \text{if } z \in \Lambda. \end{cases}$$

$\forall n \in \mathbb{Z}$:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \Lambda & \to & \mathbb{C} & \to & E(\mathbb{C}) & \to & 0 \\
 & & \downarrow n & & \downarrow n & & \downarrow [n] & & \\
0 & \to & \Lambda & \to & \mathbb{C} & \to & E(\mathbb{C}) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \Lambda/n\Lambda & & 0 & & 0 & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}$$

$$0 \to E[n] \cong \Lambda/n\Lambda \cong (\mathbb{Z}/n\mathbb{Z})^2$$

Once again, $\mathbb{Z} \to \mathrm{End}(E)$, $n \longmapsto [n]$ turns E into a $\mathbb{Z}$-module.

Morphisms between elliptic curves, E_{Λ_1} and E_{Λ_2}: $c \in \mathbb{C}$, $c\Lambda_1 \subset \Lambda_2$

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \Lambda_1 & \to & \mathbb{C} & \to & E_{\Lambda_1}(\mathbb{C}) & \to & 0 \\
 & & \downarrow c & & \downarrow c & & \downarrow [c] & & \\
0 & \to & \Lambda_2 & \to & \mathbb{C} & \to & E_{\Lambda_2}(\mathbb{C}) & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \Lambda_2/c\Lambda_1 & & 0 & & 0 & &
\end{array}$$

$$0 \to \ker[c] \cong \Lambda_2/c\Lambda_1$$

Endomorphisms of E: $\mathrm{End}(E) \cong \{c \in \mathbb{C} \mid c\Lambda \subset \Lambda\}$

$$= \begin{cases} \mathbb{Z} & \text{or} \\ \text{an order } R \text{ in a quadratic imaginary } K/\mathbb{Q} \end{cases}$$

(E has complex multiplication)

$$j(E) := 1728 \frac{g_2^3}{\Delta}$$ j-invariant

$$E_1 \cong E_2 \iff j(E_1) = j(E_2)$$

Complex Multiplication: Suppose E has CM, $\mathrm{End}(E) = R$ is an order in the quad. imag. field K. Then:

1) $j(E)$ is an algebraic integer

2) $K(j)$ is the ring class field of R,
$\mathrm{Gal}(K(j)/K) \cong \mathrm{Pic}(R)$

3) E can be defined over a number field k, assume $\mathrm{End}_{\bar{k}}(E) = \mathrm{End}_k(E)$, then

$$\mathrm{Gal}(k(E[4])/k) \hookrightarrow (R/4R)^*$$

1.4) Arithmetic of Elliptic Curves

Suppose F is a number field, E/F elliptic curve

Then:

Mordell-Weil Theorem: $E(F)$ is finitely generated

$$E(F) \cong E_{tor}(F) \times \mathbb{Z}^r \quad \text{← rank, very mysterious}$$

($E_{tor}(F)$: finite)

Merel Theorem: $\forall\, m \geq 1$ $\exists\, B = B(m) > 0$ such that for every elliptic curve E defined over a number field F with $[F:\mathbb{Q}] = m$, $|E_{tor}(F)| \leq B$.

$$Gal\left(F(E[n])/F\right) \hookrightarrow Aut_{\mathbb{Z}} E[n] \cong GL_2(\mathbb{Z}/n\mathbb{Z})$$

$$E[n] = \ker([n]: \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda) \cong \frac{1}{n}\Lambda/\Lambda \cong (\mathbb{Z}/n\mathbb{Z})^2$$

Serre's Theorem: Suppose E does not have CM. Then $\exists\, B = B(E,F)$ such that the index of

$$Gal(F(E[n])/F) \text{ in } GL_2(\mathbb{Z}/n\mathbb{Z})$$

is at most B.

(We would like B to depend only on $[F:\mathbb{Q}]$, which case we would get the following strong form of Merel's Theorem:

$$|E_{tor}(F)| \ll \left([F:\mathbb{Q}] \log\log [F:\mathbb{Q}]\right)^{\gamma} \qquad \gamma = \begin{cases} 1 & \text{CM} \\ \frac{1}{2} & \text{non-CM} \end{cases}$$

$$\left(n \log\log(n)\right)^{\gamma}$$

2) Magic Mirror : Analogy between Number Fields and Function Fields

2.1) Notations : $\mathbb{F}_q$ finite field

$\mathbb{F}_q(T)$ rational function field

$F/\mathbb{F}_q(T)$ finite extension (Global Function Field)

Pick a place ∞ of F

$A := \{x \in F \mid x \text{ regular away from } \infty\}$

$= \bigcap_{p \neq \infty} \mathcal{O}_p$ ($\mathcal{O}_p$ valuation ring of the place p)

Dedekind domain, finite class number, finite unit group

Standard Example : $F = \mathbb{F}_q(T)$, $\infty \leftrightarrow \frac{1}{T}$, $A = \mathbb{F}_q[T]$

Philosophy : Replace $\mathbb{Z}$ by A everywhere.

Let F_∞ be the completion of F at ∞ ($\sim \mathbb{R}$)

Std example : $A = \mathbb{F}_q[T]$, $F_\infty = \mathbb{F}_q(\!(\frac{1}{T})\!)$

$C_\infty := \widehat{\overline{F}_\infty}$ completion of an algebraic closure of F_∞ is again algebraically closed.

Dictionary:

Number Fields:		Function Fields	
$\mathbb{Z}$		A	$\mathbb{F}_q[T]$
$\mathbb{Q}$		F	$\mathbb{F}_q(T)$
$\lvert\cdot\rvert$	$\longleftrightarrow$	$\lvert\cdot\rvert_\infty$	$\lvert a\rvert_\infty = q^{\deg a}$
$\mathbb{R}$		F_∞	$\mathbb{F}_q((\frac{1}{T}))$
$\mathbb{C}$		$\mathbb{C}_\infty$	

Big difference: $[\mathbb{C}:\mathbb{R}] = 2 \rightarrow$ lattices of rank $r \leq 2$ in $\mathbb{C}$

$[\mathbb{C}_\infty : F_\infty] = \infty \rightarrow$ get lattices of any rank r in $\mathbb{C}_\infty$.

What we are aiming for is:

$$\begin{array}{ccccccccc}
 & & 0 & & & & 0 & & \\
 & & \downarrow & & & & \downarrow & & \\
 & & \Lambda & & & & \varphi[a] \cong \Lambda/a\Lambda \cong \left(A/aA\right)^r & & \\
 & & \downarrow & & & & \downarrow & & \\
0 & \to & \Lambda & \to & \mathbb{C}_\infty & \xrightarrow{e_\Lambda} & G_a(\mathbb{C}_\infty) & \to & 0 \qquad a \in A \\
 & & \downarrow a & & \downarrow a & & \downarrow \varphi_a & & \varphi_a \in \mathrm{End}_{\mathbb{F}_q}(G_a) \\
0 & \to & \Lambda & \to & \mathbb{C}_\infty & \xrightarrow{e_\Lambda} & G_a(\mathbb{C}_\infty) & \to & 0 \\
 & & \downarrow & & & & \downarrow & & \\
 & & \Lambda/a\Lambda & & & & 0 & & \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array}$$

$$\boxed{e_\Lambda(az) = \varphi_a(e_\Lambda(z))}$$

Here $\Lambda \subset \mathbb{C}_\infty$ discrete A-submodule of rank r in $\mathbb{C}_\infty$ (lattice)

We get a ring homomorphism

↙ endomorphisms as $\mathbb{F}_q$-modules

$$\varphi : A \longrightarrow \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_a(\mathbb{C}_\infty))$$
$$a \longmapsto \varphi_a$$

called a Drinfeld Module.

$\varphi_a(x) = ax + g_1(a)x^q + \cdots + g_d(a)x^{q^d}$

It gives $\mathbb{G}_a$ a new A-module structure:

$$a \cdot x := \varphi_a(x)$$

To Do:

- Understand $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_a(\mathbb{C}_\infty)) = \mathbb{C}_\infty[\tau_q]$
- define e_Λ

3.1) Additive Polynomials:

R commutative $\mathbb{F}_q$-algebra

Def: A polynomial $f(x) \in R[x]$ is additive if

$$f(x+y) = f(x) + f(y) \quad \text{in } R[x,y]$$

Examples:
- ax
- x^p $\qquad (x+y)^p = x^p + y^p$
- sums and compositions of additive polynomials are again additive.

Def: $\tau_p(x) = x^p$, $\tau_p^i(x) := x^{p^i}$

subset, not subring

$$R[\tau_p] := \left\{ \left(\sum_{i=0}^{n} a_i \tau_p^i \right)(x) \;\middle|\; a_0, \dots, a_n \in R \right\} \subseteq R[x]$$

$$= \left\{ \sum_{i=0}^{n} a_i x^{p^i} \;\middle|\; a_0, \dots, a_n \in R \right\}$$

This forms a (usually non-commutative) ring under addition and composition.

The elements of $R[\tau_p]$ are additive.

Theorem: $f \in R[x]$ is additive iff $f \in R[\tau_p]$.

Proof: $\Leftarrow$ is clear.

$(\Rightarrow)$: Suppose $f = \sum f_i x^i \in R[x]$ is additive.

$f(0) = 0$, so $f_0 = 0$.

$$\frac{\partial f}{\partial x}(x+y) = \frac{\partial}{\partial x} f(x+y) = \frac{\partial}{\partial x}(f(x)+f(y)) = \frac{\partial f}{\partial x}(x) \in R[x]$$

is independent of y.

But

$$\frac{\partial f}{\partial x}(x+y) = \sum_{i=1}^{n} f_i \cdot i \cdot (x+y)^{i-1}$$

$\Rightarrow$ $i \cdot f_i = 0$ for all $i \geq 1$

$\Rightarrow$ $f_i = 0$ whenever $p \nmid i$

$\Rightarrow$ $f(x) = f_1 x + g(x^p)$ for some $g(x) \in R[x]$.

$$f(x+y) = f_1(x+y) + g((x+y)^p) = f_1 x + f_1 y + g(x^p + y^p)$$

$$f(x+y) = f(x) + f(y) = f_1 x + g(x^p) + f_1 y + g(y^p)$$

$\Rightarrow g(x^p+y^p) = g(x^p) + g(y^p) \Rightarrow g$ is additive.

If $\deg_x f \le 1$, then $g=0$ and $f = f_1 x \in R[\tau_p]$

If $\deg_x f > 1$, then $\deg_x(g) = \frac{1}{p}\deg_x(f) < \deg_x f$

by induction on $\deg_x$, $g \in R[\tau_p]$

so $f = f_1 x + g(x^p) \in R[\tau_p]$. $\square$