WHAT IS...

a Shtuka?

David Goss

Shtuka is a Russian word colloquially meaning "thing". Spelled *chtouca* in the French literature, a mathematical shtuka is, roughly speaking, a special kind of module with a Frobenius-linear endomorphism (as explained below) attached to a curve over a finite field. Shtukas came from a fundamental analogy between differentiation and the p-th power mapping in prime characteristic p. We will follow both history and analogy in our brief presentation here, with the hope that the reader will come to some appreciation of the amazing richness and beauty of characteristic p algebra.

Additive Polynomials

Let L be a field in characteristic p (so L is some extension field of the finite field $\mathbb{F}_p = \mathbb{Z}/(p)$). The binomial theorem implies that the p-th power mapping $\tau(x) := x^p$ satisfies $\tau(\alpha+\beta) = \tau(\alpha)+\tau(\beta)$ for α and β in L (the coefficients of the mixed terms are 0 in L); thus $\tau^j(\alpha+\beta) = \alpha^{p^j}+\beta^{p^j} = \tau^j(\alpha)+\tau^j(\beta)$ for any $j \geq 0$. We view the mappings $x \mapsto \tau^j(x)$ as operators on L and on its field extensions. A *polynomial in* τ is an expression $p(\tau) := \sum_{j=0}^m c_j\tau^j$ with $\{c_j\} \subseteq L$; so $p(\tau)(x) = \sum_{j=0}^m c_j x^{p^j}$. Like τ and τ^j for $j \geq 0$, the function $x \mapsto p(\tau)(x)$ is an additive map. Thus its kernel, the roots of $p(\tau)(x)$ in a fixed algebraic closure $\bar{L}$ of L, is a finite-dimensional $\mathbb{F}_p$-subspace of $\bar{L}$. The set of polynomials in τ, denoted $L\{\tau\}$, is a left L-vector space and forms a ring under *composition*; notice that $\tau \cdot (c\tau) = c^p\tau^2$, so this ring is not commutative in general. The analogy with the ring of complex differential operators in one variable, which becomes clear with a little thought, motivated much early work of O. Ore, E. H. Moore, and others.

Drinfeld Modules

To define a Drinfeld module we need an algebra A which will play the same role in the characteristic p theory as the integers $\mathbb{Z}$ play in classical arithmetic. For simplicity of exposition we now set $A = \mathbb{F}_p[T]$, the ring of polynomials in one indeterminate T. Let L be as above. A *Drinfeld A-module* ψ of rank d over L [Dr1] is an $\mathbb{F}_p$-algebra injection $\psi\colon A \to L\{\tau\}$ such that the image of $a \in A$, denoted $\psi_a(\tau)$, is a polynomial in τ of degree d times the degree of a with $d > 0$. Note that ψ is uniquely determined by $\psi_T(\tau)$ and therefore d is a positive integer. Moreover, there is a homomorphism $\imath$ from A to L defined by setting $\imath(a)$ equal to the constant term of the polynomial $\psi_a(\tau)$. Drinfeld modules are similar to elliptic curves in that they possess division points (= zeroes of $\psi_a(\tau)(x)$ for $a \in A$), Tate modules, and cohomology. Moreover, like elliptic curves, Drinfeld modules arise analytically (i.e., over the complete field $\mathbb{F}_p((1/T))$) from "lattices" via an exponential function (which is an entire $\mathbb{F}_p$-linear function $e(\tau) = \sum_{j=0}^\infty b_j\tau^j$).

A Bit of Algebraic Geometry

For simplicity again, we now assume that L is an algebraically closed field. Consider the projective line $\mathbb{P}^1$ over L. An *affine open subspace* U of $\mathbb{P}^1$ is $\mathbb{P}^1$ minus a finite *nonempty* collection of points. There is a large ring $\Gamma(U)$ of rational functions with no poles in U. A *locally free sheaf* of rank d on $\mathbb{P}^1$ over L is an assignment of a free $\Gamma(U)$-module of rank d to *each* affine open subspace U in a way which is consistent with respect to the restriction of one affine open subspace to another. Notice that the rational functions with no poles anywhere on $\mathbb{P}^1$ are the elements of L, and there are far too

David Goss is professor of mathematics at The Ohio State University. His email address is `goss@math.ohio-state.edu`.

few of these to classify locally free sheaves. There is, however, a very clever dictionary between the locally free sheaves and certain *graded* modules which arise from homogeneous coordinates (see, e.g., §II.5 of R. Hartshorne's book *Algebraic Geometry*).

Shtukas

In his study of the Korteweg de Vries equation, I. M. Krichever found a remarkable dictionary between certain sheaves on curves and subalgebras of $\mathbb{C}[[t]][d/dt]$ (see, e.g., [M1]). The analogy between τ and d/dt inspired V. G. Drinfeld to look for a similar construction involving Drinfeld modules; the resulting sheaves will give us the shtuka. Let our field L now be equipped with a Drinfeld module ψ of degree d. We make $M := L\{\tau\}$ into a module over $L \otimes_{\mathbb{F}_p} \mathbb{F}_p[T] \simeq L[T]$ as follows: Let $f(\tau) \in M$, $l \in L$, and $a \in A = \mathbb{F}_p[T]$; we then put

$$l \otimes a \cdot f(\tau) := lf(\psi_a(\tau))$$

(so that elements of $\mathbb{F}_p[T]$ always act via the ψ-action). Using a right division algorithm, one shows readily that M is a free $L[T]$-module of rank d. However, M is much richer than $L[T]^d$ because M also has the left action of τ via multiplication in $L\{\tau\}$. This action is *Frobenius-linear*, as $\tau(l \cdot m) = l^p \cdot \tau(m)$ for $l \in L$ and $m \in M$.

The module M possesses a gradation given by the degree (in τ) of an element $f(\tau)$. The action of $L[T]$ given above clearly preserves this gradation. Define $M_j := \{f(\tau) \in M \mid \deg_\tau f(\tau) \le j\}$, $\mathcal{M} := \oplus_{j=0}^{\infty} M_j$, and $\mathcal{M}[1] := \oplus_{j=0}^{\infty} M_{j+1}$. Both $\mathcal{M}$ and $\mathcal{M}[1]$ are graded modules over the graded ring constructed from $L[T]$ in the same fashion as $\mathcal{M}$, and they fit into the dictionary mentioned in the preceding section. Thus both $\mathcal{M}$ and $\mathcal{M}[1]$ give rise to locally free sheaves of rank d on $\mathbb{P}^1$ over L, which we denote by $\mathfrak{M}$ and $\mathfrak{M}'$ respectively. The mapping which injects M_j into M_{j+1} gives an injection λ of $\mathfrak{M}$ into $\mathfrak{M}'$. Moreover, multiplication by τ gives an injection of $\mathfrak{M}$ into $\mathfrak{M}'$ which is Frobenius linear over each affine open subspace. We encapsulate all this by

$$\mathfrak{M} \xhookrightarrow{\lambda} \mathfrak{M}' \xhookleftarrow{\tau} \mathfrak{M}. \tag{1}$$

Diagram (1) **is** the "shtuka associated to ψ". The cokernel of λ gives rise to trivial modules on affine open subspaces *not* containing the point $\infty \in \mathbb{P}^1$, and the cokernel of τ also gives rise to trivial modules on affine open subspaces not containing a point lying over the prime $\ker \iota$ of A. These are naturally called the "pole" and the "zero" of the shtuka.

When $d = 1$, the locally free sheaves are called "line-bundles", and they come from divisors. Using the Riemann-Roch Theorem and a result of Drinfeld, one can show that the shtuka actually arises from a function on $\mathbb{P}^1$ over L [Th1]. For instance, the function associated to the rank 1 Drinfeld module C given by $C_T(\tau) := \tau$ is just T itself!

While we have worked here with $A = \mathbb{F}_p[T]$, in fact *all* of the above goes through readily when A is replaced by the affine algebra of an arbitrary smooth projective curve X over a finite field minus a fixed closed point. All of the salient issues are touched on in the simple case sketched here. The collection of those algebraic functions on X with poles of finite order forms a field k called the "function field of X". Such function fields are the analogs in finite characteristic of "number fields" defined by adjoining to the rational numbers $\mathbb{Q}$ a finite number of roots of polynomials with rational coefficients. Modern number theory is concerned with the properties of *both* types of fields.

The general notion of a shtuka, which has been crucial to the work of Drinfeld and L. Lafforgue on the Langlands conjectures for k (see [L1] and its references), is just the abstraction of (1) to families $U \times X$ where U is a scheme in characteristic p (see, e.g., [L1]). Moreover, it is possible to describe which shtukas arise from Drinfeld modules (see, e.g., [M1]).

τ-Sheaves

Over the affine line inside $\mathbb{P}^1$ over L, both $\mathfrak{M}$ and $\mathfrak{M}'$ reduce to M itself. The $L[T,\tau]$-module M is called by G. Anderson the "motive of ψ" in *analogy* with the classical theory of motives, and its abstraction to families is called "τ-sheaves". It turns out that τ-sheaves are the correct notion with which to describe characteristic-p-valued L-functions (D. Wan–Y. Taguchi, G. Böckle–R. Pink, F. Gardeyn, G. Böckle) and to study special values of characteristic-p-valued Γ-functions (G. Anderson–W. D. Brownawell–M. Papanikolas). Moreover, τ-sheaves are naturally associated to characteristic-p-valued cusp forms (G. Böckle), much as one associates elliptic curves (and other classical motives) to elliptic cusp forms. Shtukas, and τ-sheaves, are such fundamental ideas that the process of mining their riches is really just beginning!

References

[Dr1] V. G. Drinfeld, Elliptic modules, *Math. Sbornik* **94** (1974), 594–627; English transl., *Math. USSR Sbornik* **23** (1976), 561–92.

[L1] G. Laumon, La correspondence de Langlands sur les corps de fonctions (d'après Laurent Lafforgue), *Sém. Bourbaki* **873** (1999–2000).

[M1] D. Mumford, An algebro-geometric construction of commuting operators and solutions to the Toda lattice equation, *KdV* equation and related nonlinear equations, *International Symposium on Algebraic Geometry (Kyoto, 1977)* (M. Nagata, ed.), Kinokuniya, Tokyo, 1978, pp. 115–53.

[Th1] D. Thakur, Shtukas and Jacobi sums, *Invent. Math.* **111** (1993), 557–70.

Comments and suggestions may be sent to `notices-whatis@ams.org`.