On the work of V. G. Drinfeld

Vyjayanthi Chari and Dinesh Thakur

Professor Vladimir Gershnovich Drinfeld was born on 14 February 1954, in Kharkov USSR. He is currently a member of the Physicotechnical Institute of Low Temperatures, Academy of Sciences of the Ukranian SSR. He was awarded the Fields medal at the Kyoto ICM 1990 for his work on:

- Drinfeld modules leading to a decisive breakthrough in the Langlands programme,
- classification of instantons (jointly with Atiyah, Hitchin and Manin),
- reduction theory of completely integrable systems of KdV type (jointly with Sokolov),
- quantum groups.

In this article we shall concentrate on his work on Drinfeld modules and quantum groups. We hope to convey some idea of the breadth of his contributions, for while the first is of a rich purely mathematical nature, the second illustrates his abilities to abstract, systematize and put in a rigorous mathematical framework many ideas which first appeared in physics. A unifying theme in Drinfeld's work in these two areas is the viewing of commutative objects in the context of bigger non-commutative objects and exploiting the resulting variations.

The *Langlands programme* is a series of conjectures, theorems and insights aimed at understanding the absolute Galois group[1] G of Q, $F_p(t)$, their finite extensions (global fields) and their completions (local fields).

One of the main achievements in number theory, in the first part of this century, was the description of the maximal abelian quotient $G^{ab}=Gal(K^{ab}/K)$ of G in terms of the arithmetic of K. Thus, if K is a local (resp. global) field, then G^{ab} is the profinite completion of $K^\times$ (resp. of $A_K^\times/K^\times$), where A_K is the adele ring of K (essentially the product of all completions of K).

Since the description of G^{ab} is essentially the description of one-dimensional representations of G, Langlands suggested that the description of n-dimensional matrix representations should be the next step. His conjectures in an imprecise and simplified form are: (i) n-dimensional representations of G are in one to one correspondence with certain infinite dimensional representations of $GL_n(K)$ (resp. $GL_n(A_K)$) in the local (resp. global) case. Note that $GL_1(K)=K^\times$. (ii) This correspondence should identify the L-functions attached in a natural way to the representations of G and of GL_n. We omit the definition of these functions.

In fact, for the case $n=1$, $K=Q$, the second part of the conjecture already implies the quadratic and the power reciprocity laws of Legendre–Gauss–Eisenstein that usually form the core of the first graduate course in number theory. The quadratic reciprocity law tells you, for example, whether a prime q divides x^2-p for some x, given that the prime p divides y^2-q for some y.

Drinfeld proved Langlands conjectures for $n=2$ for global fields of finite characteristics, i.e. for $F_p(t)$ and its finite extensions. He also sketched a method to extend this to any n. Even though the general case is still not finished because of the formidable technical difficulties, our understanding of the situation has increased immensely by Drinfeld's work. In his proof, Drinfeld introduced fundamental objects of a new kind which he called elliptic modules but which are now referred to as Drinfeld modules. Once understood, these are very simple and natural objects, which at the same time have many deep properties that are still being studied.

We will now explain the notion of Drinfeld modules and describe some of their properties. Let K be a field of characteristic p, i.e. $px=0\ \forall x\in K$. Examples of such

Vyjayanthi Chari and Dinesh Thakur are in School of Mathematics, Tata Institute of Fundamental Research, Bombay 400 005.

fields are $F_p(t)$ and its extensions. The first thing to notice is that for such fields one has a much larger supply of additive functions. In other words, in the more familiar situation of real or complex numbers, the solutions to the equation $f(x+y)=f(x)+f(y)$ are just $f(x)=cx$, for some scalar c. In characteristic p, $f(x)=x^{p^n}$ is also a solution since the cross terms in $(x+y)^{p^n}=x^{p^n}+y^{p^n}$ are multiples of p and hence zero. It follows that $f(x)=\Sigma c_i x^{p^i}$ is also a solution. Let $R \cong End\, G_a$ be the ring of all such additive functions, the multiplication operation being just the composition of functions. This is a huge noncommutative ring.

Now let X be a smooth, projective algebraic curve over F_p, fix any point on it and let A be the space of functions on it with a pole only at this point. (See Srinivas' article on Mori's work for the terminology, page 1292 this issue). Then A is a commutative ring with the usual pointwise addition and multiplication. For example, if one takes X to be the projective line and the point to be the point at infinity, then A is $F_p[t]$. The important fact is that A can be embedded in R in various ways and a Drinfeld module is just a choice of embedding $a \in A \to f_a \in R$ such that the linear term of $f_a(x)$ is ax but $f_a(x)$ is not identically ax, for all a. The last is a non-triviality condition.

In other words, we have associated to each $a \in A$, a linear function $f_a(x)$ such that

$$f_{a+b}(x)=f_a(x)+f_b(x), f_{ab}(x)=f_a(f_b(x)). \qquad (*)$$

This should be compared with the classical situation, where to $k \in Z$, one associates an endomorphism of the multiplicative group $F_k(x)=x^k$.

As an illustration, for $A=F_p[t]$, one can choose f_t to be any nonlinear polynomial $f_t(x)=\sum_{i=0}^{n} c_i x^{p^i}$, with $c_0=t$. Since t is a generator of A, using $(*)$ one knows f_a for any a. If $c_n \neq 0$, n is called the rank of the Drinfeld module. The rank one situation is closest to the classical multiplicative group situation described above. The simplest case[2] is $f_t(x)=tx+x^p$ and then we have $f_{t^2}(x)=f_t(f_t(x))=t^2x+(t+t^p)x^p+x^{p^2}$. As an analogue of kth roots of unity, which are solutions of $F_k(x)=x^k=1$, one has 'ath roots of unity' viz. solutions of $f_a(x)=0$. Note that 0 is the identity for addition and 1 for multiplication. Adjoining these to $F_p(t)$, one gets extensions analogous to the cyclotomic extensions $Q(\zeta_k)$, which contain any finite extension of Q with abelian Galois group, thus making contact with Langlands programme for $n=1$.

As an analogue of the exponential function e^z, which is just a normalized function satisfying $F_k(e^z)=e^{kz}$, one has the entire function $e(z)$ satisfying $f_a(e(z))=e(az)$ and normalized to have linear term z. As an analogue of $2\pi iZ$, which is the solution set of the equation $e^z=1$, one has the kernel of $e(z)$, i.e. the solution set of $e(z)=0$, which is an A-module (or lattice) of rank n. In particular, in the rank one case, one has the analogue of $2\pi i$. In the rank two case, one gets a rank two lattice, so this case corresponds to elliptic curves mentioned in Srinivas' article on Mori's work.

The coefficients of f_a, considered as functions of lattices corresponding to Drinfeld modules f, give examples of analogues of modular forms. Drinfeld modules are also intimately connected to the arithmetic of special values of the zeta function, the L functions, analogues of gamma functions, Bessel functions, Gauss sums and so on.

In general, one studies the rank n case to make contact with GL_n. (Note that the change of base of the rank n lattice corresponds to a matrix in GL_n.) For those readers who are familiar with somewhat more advanced concepts of mathematics the punchline that connects Drinfeld modules to the Langlands programme is: on certain cohomology of varieties parametrizing Drinfeld modules of rank n, one finds representations of the Galois group and GL_n naturally paired as required in Langlands conjectures.

We hope that these examples and analogies indicate how this simple looking but mathematically rich object unifies many concepts.

The same parameter (also called moduli) varieties of Drinfeld modules which were used for attacking the Langlands conjectures were later used to produce good error correcting codes: a very important application in today's world which is heavily dependent on communicating huge amounts of data with as few errors as possible. This illustrates the time-tested fact that fundamental abstract objects which pure mathematicians study for their intrinsic interest eventually lead to important applications outside mathematics.

We now turn to Drinfeld's work on a new and exciting subject—quantum groups.

In his talk at the ICM in Berkeley in 1986, Drinfeld introduced the term quantum group and defined it to be a Hopf algebra deformation of the universal enveloping algebra of a Lie algebra. A large class of quantum groups is known, in fact Drinfeld and Jimbo independently introduced one for each complex simple Lie group. The first examples of what are now called quantum groups were discovered in 1978–79 and studied extensively by the mathematical physicists of the Leningrad school, notably, Sklyanin, Fadeev and others. These examples arose in their theory of the quantum inverse scattering method. The basic relation in their theory is described by solutions of a family of algebraic equations called the Yang–Baxter Equation (YBE):

$$R^{12}(u-v)\,R^{13}(u-w)\,R^{23}(v-w)$$
$$=R^{23}(v-w)\,R^{13}(u-w)\,R^{12}(u-v).$$

Here $R(u)$ is an element of *End* $(V\otimes V)$ for some vector space V, u is a complex variable, the equation takes place in *End* $(V\otimes V\otimes V)$, and R^{ij} means R in the i,j positions and one elsewhere. The Yang–Baxter equations had appeared earlier in the work of Baxter on exactly solvable lattice models. Many solutions of the YBE had been obtained by these people and others, although their arguments were sometimes long and complicated or of a heuristic nature. Drinfeld's theory helps to make these ideas concrete and allows one to generate solutions of the YBE in the representation categories of quantum groups. His work along with articles of Jimbo shaped the area and has generated a lot of research by many mathematicians.

Deformations of Lie algebras[3] are familiar in both mathematics and physics. For example, the Heisenberg Lie algebra with generators p, q, c and the single relation

$$[p,q]=hc,$$

where c is central and h is a parameter, is a non-abelian Lie algebra which 'tends to an abelian Lie algebra as h tends to 0'.

However, simple Lie algebras do not admit non-trivial deformations in the category of Lie algebras. To circumvent this, Drinfeld and Jimbo independently introduced the idea of deforming them in the category of Hopf algebras. A Hopf algebra over a commutative ring R is an associative algebra A over R together with algebra homomorphisms $\Delta : A\to A\otimes A$ (the comultiplication) and $\varepsilon : A\to C$ (the counit), and an algebra anti-homomorphism $S: A\to A$ (the antipode). These must satisfy some conditions which we omit, except for the one on coassociativity: $\Delta\otimes id.\Delta = id\otimes\Delta.\Delta$. (In fact, for the rest of the article we shall ignore the existence of the counit and the antipode.) The Hopf algebra is commutative if A is a commutative algebra and cocommutative if $\Delta = P.\Delta$ where $P: A\otimes A\to A\otimes A$ is the permutation of the two factors. Many examples of commutative (resp. cocommutative) Hopf algebras were known, for instance: the algebra $F(G)$ of functions on a finite group, with comultiplication being given by $\Delta(f)(g,h)=f(gh)$ (resp. the universal enveloping algebra[4] Ug of a Lie algebra g, with $\Delta(x)=x\otimes 1+1\otimes x$, for any $x\in g$). We are now ready to give Drinfeld's definition of a quantum group. Quantum groups provide a large class of non-commutative, non-cocommutative Hopf algebras.

Definition. *Let g be a Lie algebra. Then a quantization of g is a Hopf algebra A, defined over the algebra $\mathbb{C}[[h]]$ of formal power series in an indeterminate h, such that $A/hA\cong Ug$ as Hopf algebras over $\mathbb{C}$. Moreover, A is required to be complete and topologically free as a $\mathbb{C}[[h]]$-module.*

By a quantum group we shall mean a quantization of a Lie algebra; the term is also applied to other closely related concepts. Notice that A is obviously a non-commutative algebra if g is non-commutative.

At this stage, let us give the simplest examples of quantum groups.

Example 1. Let g be the two-dimensional Lie algebra spanned by elements H, X with $[H,X]=2X$. Let $A=Ug\hat{\otimes}\mathbb{C}[[h]]$ as an algebra[5]. The assignment

$$\Delta_h(H)=H\otimes 1+1\otimes H,\ \Delta_h(X)=X\otimes e^{hH}+1\otimes X$$

defines a comultiplication on A. It is easy to see that A is a quantization of Ug.

Example 2. Let $g=sl_2(\mathbb{C})$ be the Lie algebra of 2×2 complex matrices of trace 0. The following elements are the standard basis for g:

$$X^+=\begin{pmatrix}0&1\\0&0\end{pmatrix},\ X^-=\begin{pmatrix}0&0\\1&0\end{pmatrix},\ H=\begin{pmatrix}1&0\\0&-1\end{pmatrix}.$$

The bracket relations are $[H,X^\pm]=\pm 2X^\pm$, $[X^+,X^-]=H$. As in example 1, take A to be the space $Ug\hat{\otimes}\mathbb{C}[[h]]$ but, this time the algebra relations are modified, the change is:

$$[X^+,X^-]=\frac{e^{hH}-e^{-hH}}{e^h-e^{-h}}.$$

The comultiplication is unchanged for H and on the other generators is:

$$\Delta_h(X^-)=X^-\otimes 1+e^{-hH}\otimes X^-,$$

$$\Delta_h(X^+)=X^+\otimes e^{hH}+1\otimes X^+.$$

Similar quantizations exist for any simple Lie algebra. These were introduced independently by M. Jimbo.

We will now explain Drinfeld's theory of quantization which gives an indication of how to arrive at the above formulas. Assume that A is a quantization of g and let Δ_h be the comultiplication. Then, the map $\delta: A\to A\otimes A$ defined by

$$\delta(a)=\frac{\Delta_h(a)-P\cdot\Delta_h(c)}{h},$$

factors to a map also written as δ from g to $g\otimes g$. This map defines a 1-cocycle on g, i.e. $\delta([x,y])=[x\otimes 1+1\otimes x,\delta(y)]-[y\otimes 1+1\otimes y,\delta(x)]$ and the dual of δ defines a Lie algebra structure on g^*. The fact that δ is a 1-cocycle suggests that one should consider the special case where δ is a coboundary, i.e. $\delta(x)=[x\otimes 1+1\otimes x,r]$ for some $r\in g\otimes g$. Note that, if g is a finite-dimensional complex semisimple Lie algebra, all 1-cocycles are of this form. Belavin and Drinfeld describe all $r \in g \otimes g$ for g semisimple, so that the associated δ^* defines a Lie algebra structure on g^*.

One can then ask the converse question: Given a δ satisfying the conditions above, can one obtain a corresponding quantization of g? Drinfeld has proved an existence theorem for quantizations of Lie algebras. The explicit forms of these quantizations do not seem to have been worked out in all cases. The underlying principle for explicit descriptions is the following. As a space take $A = Ug \hat{\otimes} \mathbb{C}[[h]]$. Notice that if A is to be a quantization of g then the comultiplication of A should be related to the one on Ug by

$$\Delta_h = \Delta + h\delta + \ldots \text{ (ref. 6).}$$

Ideally, one would like the higher order terms to be zero, so one first tries to perturb the obvious multiplication on A to make A into a Hopf algebra. (There are examples of such quantum groups but the limitations of space do not allow us to go into it.) If this fails, then one tries to keep the algebra structure unchanged and only change Δ. This is the case in example 1. In example 2, however both the algebra structure and Δ are changed, but one can check that these changes are natural and that they are more or less forced by the fact that the linear term in Δ_h is $h\delta$.

To relate this to solutions of the Yang–Baxter equation, Drinfeld introduced the notion of a universal Yang–Baxter operator. This is an invertible element $\mathcal{R}$ in $A \hat{\otimes} A$ satisfying:

$$\mathcal{R}^{12}\mathcal{R}^{13}\mathcal{R}^{23} = \mathcal{R}^{23}\mathcal{R}^{13}\mathcal{R}^{12},$$

where A is the quantum group associated to a simple Lie algebra as in example 2. Now, let $\rho : A \to End(V)$ be any representation of A in a finite-dimensional linear space V. Then, $\rho(\mathcal{R}) \in End(V \otimes V)$ satisfies the Yang–Baxter equation. Explicit formulas are known for $\mathcal{R}$ at least for some g. An alternate way of calculating $\rho(\mathcal{R})$ is to view it as an intertwining operator for the two actions of A on $V \otimes V$ given by Δ_h and $P.\Delta_h$. This in fact was the original approach of the Leningrad school, although the mathematical justification is only after Drinfeld. One should point out here that the solutions obtained from the quantum groups considered in this article are constant solutions of the YBE. Drinfeld also constructed quantum groups which gave rise to rational and trigonometric solutions of the YBE.

His most recent work in this area is a classification theorem for quantum groups. In his talk at the ICM 1990, Manin compares this theorem to the '. . . the first theorems of Lie establishing the relations between Lie algebras and local Lie groups.'

Drinfeld introduced Drinfeld modules and solved a substantial part of the Langlands programme when he was just 20 years old and completed the GL_2 case when he was 24. Drinfeld's work on Langlands conjectures, quantum groups, p-adic uniformizations etc. illustrate his mastery over powerful and involved techniques. On the other hand, his one page proof (jointly with Vladut) giving a sharp asymptotic upper bound for the number of points of a curve defined over a finite field of order p^{2^n}, uses only high school algebra applied nicely to well-known results. He also gave a one page proof of the fact that any rotation invariant finitely additive measure on the two or three dimensional sphere is proportional to Lesbesgue measure by using a clever combination of known results.

It has been a pleasure for us to write this report on Drinfeld and we hope that we have succeeded in communicating to you an idea of Drinfeld's contributions.

1. By the absolute Galois group of K, we mean the Galois group of the separable closure of K over K.
2. This is called a Carlitz module after the American Mathematician Carlitz who essentially studied it in the thirties.
3. A Lie algebra g over a field k is a vector space over k equipped with a skew bilinear map $g \times g \to g$ satisfying the Jacobi identity, $[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0$. The Lie algebra is called abelian if $[x,y] = 0$ for all $x, y \in g$. The space of $n \times n$ matrices with complex entries is a Lie algebra with $[A, B]$ being defined to be $AB - BA$, for any two matrices A, B.
4. The enveloping algebra of a Lie algebra is the associative algebra obtained by taking the quotient of the tensor algebra by the two-sided ideal generated by $x \otimes y - y \otimes x - [x, y]$, for all $x, y \in g$.
5. Here and elsewhere, the hat on the tensor product will mean that we are taking completions, for instance A is the space of formal infinite sums $\sum_{n=0}^{\infty} x_n h^n$, for arbitrary elements $x_n \in Ug$.
6. Notice that if $\delta \neq 0$ then the resulting Hopf algebra is not co-commutative thus providing examples of non-commutative, non-cocommutative Hopf algebras as asserted earlier.