Elliptic curves: what they are, why they are called elliptic, and why topologists like them, II

Wayne State University Mathematics Colloquium
February 28, 2007

Doug Ravenel

Elliptic curves

Recall that an elliptic curve E is a 1-dimensional algebraic variety with a group structure. If it is defined over the complex numbers $\mathbf{C}$, then it can be regarded as the quotient group $\mathbf{C}/\Lambda$, where Λ is the free abelian group generated by 1 and a number τ with positive imaginary part.

Elliptic curves

Recall that an elliptic curve E is a 1-dimensional algebraic variety with a group structure. If it is defined over the complex numbers $\mathbf{C}$, then it can be regarded as the quotient group $\mathbf{C}/\Lambda$, where Λ is the free abelian group generated by 1 and a number τ with positive imaginary part.

It can also be regarded as a plane cubic curve with the group structure defined by the colinear rule: the sum of any three colinear points is the identity element. The equation defining the curve can have coefficients in an arbitrary commutative ring R.

Formal group laws

After choosing a local coordinate x near the identity element, we can express the group structure locally via a power series expansion $F(x, y) \in R[[x, y]]$.

Formal group laws

After choosing a local coordinate x near the identity element, we can express the group structure locally via a power series expansion $F(x, y) \in R[[x, y]]$.

This power series must have the following three properties.

(i) $F(x, 0) = F(0, x) = x$ since $(0, 0)$ is the identity element.

(ii) $F(y, x) = F(x, y)$ since the group is Abelian.

(iii) $F(F(x, y), z) = F(x, F(y, z))$ by associativity.

Formal group laws

After choosing a local coordinate x near the identity element, we can express the group structure locally via a power series expansion $F(x, y) \in R[[x, y]]$.

This power series must have the following three properties.

(i) $F(x, 0) = F(0, x) = x$ since $(0, 0)$ is the identity element.

(ii) $F(y, x) = F(x, y)$ since the group is Abelian.

(iii) $F(F(x, y), z) = F(x, F(y, z))$ by associativity.

Such a power series is called a 1-dimensional commutative formal group law over R.

Algebraic topology

Algebraic toplogists make a living by associating algebraic structures with topological spaces and studying them. One such structure is ordinary cohomology.

Algebraic topology

Algebraic toplogists make a living by associating algebraic structures with topological spaces and studying them. One such structure is ordinary cohomology.

For a space X, $H^*(X)$ is a graded commutative ring, meaning that there are abelian groups $H^i(X)$ for $i \geq 0$ and it is possible to multiply an element in $H^i(X)$ by one in $H^j(X)$ and get one in $H^{i+j}(X)$.

Algebraic topology

Algebraic toplogists make a living by associating algebraic structures with topological spaces and studying them. One such structure is ordinary cohomology.

For a space X, $H^*(X)$ is a graded commutative ring, meaning that there are abelian groups $H^i(X)$ for $i \geq 0$ and it is possible to multiply an element in $H^i(X)$ by one in $H^j(X)$ and get one in $H^{i+j}(X)$.

Cohomology is a *contraviant functor*, which means that a continuous map $X \to Y$ induces a ring homomorphism $H^*(X) \leftarrow H^*(Y)$; the arrow gets reversed.

Bordism and cobordism

$H^*(X)$ is described as the dual of $H_*(X)$, the ordinary homology of the space X.

Bordism and cobordism

$H^*(X)$ is described as the dual of $H_*(X)$, the ordinary homology of the space X.

$H_*(X)$ is defined in terms of maps of simplicial complexes into X.

Bordism and cobordism

$H^*(X)$ is described as the dual of $H_*(X)$, the ordinary homology of the space X.

$H_*(X)$ is defined in terms of maps of simplicial complexes into X.

We get a richer version of homology by replacing simplicial complexes with complex manifolds. The resulting group is called the *complex bordism of* X and is denoted by $MU_*(X)$.

Bordism and cobordism

$H^*(X)$ is described as the dual of $H_*(X)$, the ordinary homology of the space X.

$H_*(X)$ is defined in terms of maps of simplicial complexes into X.

We get a richer version of homology by replacing simplicial complexes with complex manifolds. The resulting group is called the *complex bordism of* X and is denoted by $MU_*(X)$.

It has a cohomological version denoted by $MU^*(X)$ (the complex cobordism of X) with formal properties similar to those of $H^*(X)$.

Complex projective space

Recall that $\mathbf{C}P^n$ is the space of complex lines thru the origin in the vector space $\mathbf{C}^{n+1}$.

Complex projective space

Recall that $\mathbf{C}P^n$ is the space of complex lines thru the origin in the vector space $\mathbf{C}^{n+1}$.

A linear embedding

$$\mathbf{C}P^{n-1} \to \mathbf{C}P^n$$

is Poincaré dual to a class $x \in MU^2(\mathbf{C}P^n)$.

Complex projective space

Recall that $\mathbf{C}P^n$ is the space of complex lines thru the origin in the vector space $\mathbf{C}^{n+1}$.

A linear embedding

$$\mathbf{C}P^{n-1} \to \mathbf{C}P^n$$

is Poincaré dual to a class $x \in MU^2(\mathbf{C}P^n)$.
We have

$$MU^*(\mathbf{C}P^n) = MU^*(\text{point})[x]/(x^{n+1}),$$

Complex projective space

Recall that $\mathbf{C}P^n$ is the space of complex lines thru the origin in the vector space $\mathbf{C}^{n+1}$.

A linear embedding

$$\mathbf{C}P^{n-1} \to \mathbf{C}P^n$$

is Poincaré dual to a class $x \in MU^2(\mathbf{C}P^n)$.
We have

$$MU^*(\mathbf{C}P^n) = MU^*(\mathrm{point})[x]/(x^{n+1}),$$

and the ring $MU^* := MU^*(\mathrm{point})$ is known.

More complex projective spaces

Similarly

$$
\begin{aligned}
&MU^*(\mathbf{C}P^m \times \mathbf{C}P^n) \\
&\quad = \; MU^*[x \otimes 1, 1 \otimes x]/(x^{m+1} \otimes 1, 1 \otimes x^{n+1})
\end{aligned}
$$

More complex projective spaces

Similarly

$$\begin{aligned} & MU^*(\mathbf{C}P^m \times \mathbf{C}P^n) \\ & \quad = \ MU^*[x \otimes 1, 1 \otimes x]/(x^{m+1} \otimes 1, 1 \otimes x^{n+1}) \end{aligned}$$

We can regard $\mathbf{C}^{m+1}$ and $\mathbf{C}^{n+1}$ and the spaces of polynomials over $\mathbf{C}$ of degrees $\leq m$ and $\leq n$ respectively.

More complex projective spaces

Similarly

$$\begin{aligned} & MU^*(\mathbf{C}P^m \times \mathbf{C}P^n) \\ = \; & MU^*[x \otimes 1, 1 \otimes x]/(x^{m+1} \otimes 1, 1 \otimes x^{n+1}) \end{aligned}$$

We can regard $\mathbf{C}^{m+1}$ and $\mathbf{C}^{n+1}$ and the spaces of polynomials over $\mathbf{C}$ of degrees $\leq m$ and $\leq n$ respectively.

Polynomial multiplication leads to a map

$$\mathbf{C}P^m \times \mathbf{C}P^n \to \mathbf{C}P^{m+n}.$$

A new formal group law

Letting $m, n \to \infty$ leads to a map

$$\mathbf{C}P^{\infty} \times \mathbf{C}P^{\infty} \to \mathbf{C}P^{\infty}$$

A new formal group law

Letting $m, n \to \infty$ leads to a map

$$\mathbf{C}P^\infty \times \mathbf{C}P^\infty \to \mathbf{C}P^\infty$$

inducing

$$\begin{array}{ccc}
MU^*(\mathbf{C}P^\infty \times \mathbf{C}P^\infty) & \longleftarrow & MU^*(\mathbf{C}P^\infty) \\
\| & & \| \\
MU^*[[x \otimes 1, 1 \otimes x]] & & MU^*[[x]] \\
& & \\
G(x \otimes 1, 1 \otimes x) & \longleftarrow\!\!\shortmid & x
\end{array}$$

A new formal group law

Letting $m, n \to \infty$ leads to a map

$$\mathbf{C}P^\infty \times \mathbf{C}P^\infty \to \mathbf{C}P^\infty$$

inducing

$$\begin{tikzcd} MU^*(\mathbf{C}P^\infty \times \mathbf{C}P^\infty) \arrow[d, equal] & MU^*(\mathbf{C}P^\infty) \arrow[l] \arrow[d, equal] \\ MU^*[[x \otimes 1, 1 \otimes x]] & MU^*[[x]] \end{tikzcd}$$

$$G(x \otimes 1, 1 \otimes x) \longleftarrow\!\!\shortmid\; x$$

$G(x, y)$ is a formal group law over MU^*.

Quillen's theorem

By a theorem of Quillen, the formal group law G has the following unversal property: Any formal group law F over a ring R is induced from G via a homomorphism

$$\theta : MU_* \to R.$$

Quillen's theorem

By a theorem of Quillen, the formal group law G has the following unversal property: Any formal group law F over a ring R is induced from G via a homomorphism

$$\theta : MU_* \longrightarrow R.$$

An elliptic curve over R with a choice of local coordinate determines a formal group law over R and therefore a homomorphism as above.

Elliptic cohomology

This leads to a new functor

$$X \mapsto MU^*(X) \otimes_\theta R$$

from spaces to R-algebras.

Elliptic cohomology

This leads to a new functor

$$X \mapsto MU^*(X) \otimes_\theta R$$

from spaces to R-algebras.

In favorable cases this functor has formal properties similar to those of ordinary cohomology and is known as *elliptic cohomology*.

Elliptic cohomology

This leads to a new functor

$$X \mapsto MU^*(X) \otimes_\theta R$$

from spaces to R-algebras.

In favorable cases this functor has formal properties similar to those of ordinary cohomology and is known as *elliptic cohomology*.

In some cases R can be interpreted as a ring of modular forms, which makes this of interest to number theorists.

Elliptic cohomology

Witten, Segal, Stolz and Teichner have conjectures about the geometric interpretation of this functor which make it of interest to mathematical physicists.

Elliptic cohomology

Witten, Segal, Stolz and Teichner have conjectures about the geometric interpretation of this functor which make it of interest to mathematical physicists.

When R is a ring of modular forms, θ assigns one to each complex manifold.

Elliptic cohomology

Witten, Segal, Stolz and Teichner have conjectures about the geometric interpretation of this functor which make it of interest to mathematical physicists.

When R is a ring of modular forms, θ assigns one to each complex manifold.

This modular form has a q-expansion with integer coefficients.

Elliptic cohomology

Witten, Segal, Stolz and Teichner have conjectures about the geometric interpretation of this functor which make it of interest to mathematical physicists.

When R is a ring of modular forms, θ assigns one to each complex manifold.

This modular form has a q-expansion with integer coefficients.

In 1986 Witten conjectured (correctly) that this information is related to the index of the Dirac operator on the free loop space of the manifold.