COMPLEX MULTIPLICATION: LECTURE 13

Example 0.1. If we let $C = \mathbb{P}^1$, then $k(C) = k(t) = k(C^{(q)})$ and the $\phi^*(t) = t^q$, thus the extension $k(C)/\phi^*(k(C))$ is of the form $k(t^{1/q})/k(t)$ which as you may recall from the first couple of lectures is in some sense the most basic inseparable extension.

Normally, separability is not a desirable property if one is interested in Galois theory. However in our situation, inseparability plays a crucial role due to the next corollary which in some sense says that the Frobenius is the only map which can cause any sort of inseparability phenomenon. This gives a useful characterisation of the Frobenius which will be necessary later.

Corollary 0.2. *Let $\psi : C_1 \to C_2$ be a morphism of fields, then ϕ factors uniquely*

$$\lambda \circ \phi : C_1 \to C_1^{(q)} \to C_2$$

where ϕ is the q^{th} power frobenius and λ is a separable map. In particular if Ψ is purely inseparable, then λ is an isomorphism.

Proof. Let K be the separable closure of $\psi^*(k(C_2)$ in $k(C_1)$. Then $k(C_1)/K$ is purely inseparable of some degree q say. Thus $k(C)^q \subset K$, but $\phi^* k(C_1^{(q)}) = k(C)^q$ and is of degree q, thus by comparing degrees we have $K = \phi^* k(C)_1^{(q)})$. Thus we have the tower of fields $k(C_1)/\phi^* k(C_1^{(q)})/\psi^*(k(C_2)$ which by **??** gives us the required factorisation.

When Ψ is purely inseparble, $\phi^*(k(C_1^{(q)})) = \psi^*(C_2)$, and so λ is an isomoprhism. □

Finally let $k = \mathbb{F}_q$ the finite field with q elements. In this case, if $C \subset \mathbb{P}^n$ is defined over k then I is generated by $f_1, ..., f_m$ whose coefficients are in $\mathbb{F}_q$, hence $f_i^{(q)}$ and so $C^{(q)} = C$, so that ϕ becomes a morphism from C to itself.

Explicitly, $\phi(x_0 : ... : x_n) = (x_0^q : ... : x_n^q)$ and $f_i(x_0^q, ...x_0^q) = f_i(x_0, ..., x_n)^q$ since f has coefficients in in $\mathbb{F}_q$, so the image is contained in C.

0.1. Differentials.

In this section we discuss the differentials on a curve. From the point of view of geometry, this plays the role in traditional calculuss of linearisation, eg. tangent spaces and differential forms. However in the algebraic setting it also gives a useful criterion for determining when a map is separable.

Definition 0.3. Let C be a curve, the space of meromorphic differentials Ω_C of C is the $\overline{k}(C)$ vector spaces spanned by symbols dx for $x \in \overline{k}(C)$ subject to the following three conditions:

i) $dx = 0$ for $x \in \overline{k}$
ii) $d(x + y) = dx + dy$ for $x, y \in \overline{k}(C)$
iii) $d(xy) = xdy + ydx$ for $x, y \in \overline{k}(C)$

This is the algebraic analogue of differential forms. More precisely, a meromorphic differential is a section of the sheaf of differential forms. This means it is an assignment to each point of the curve a point in the cotangent space at the point. Moreover this assignment is in a sense ”smooth.”

If $\psi : C_1 \to C_2$ is a non-constant map of curves, the pullback ψ^* induces a map of differentials also denoted

$$\psi^* : \Omega_{C_2} \to \Omega_{C_1}$$

given by

$$\psi^*(dx) = d\psi^*(x)$$

Proposition 0.4. *Let C be a curve.*
i) Ω_C is 1 dimensional vector space over $\overline{k}(C)$.
ii) For $x \in \overline{k}(C)$, dx is basis for Ω_C if and only if $\overline{k}(C)/\overline{k}(x)$ is separable

Proof. [Matsumura] 27 A,B □

An important consequence of this proposition is that a map of curves is separable if and only if the induced map on differentials is non-zero. Before proving it though here is an example to illustrate why the result is true.

Example 0.5. Let $C = \mathbb{P}^1$, then $\overline{k}(C) = \overline{k}(t)$. Then the symbol dt generates Ω_C by the above proposition (one can also see this directly, using the chain rule for differentation, that $df = f'dt$ where f' is the formal derivative of f with respect to t). Then the q frobenius $\phi : C \to C^{(q)} = C$ induces the pullback $\phi^* : f \mapsto f^q$ on function fields. Then

$$\phi^* dt = d\phi^* t = dt^q = qdt^{q-1} = 0$$

since we are in characteristic p.

In some sense, a non-separable is of the form $x \mapsto x^q$, so differentiating will give 0 since it turns the exponenets q into multiplication by$q$.

Corollary 0.6. *A morphism of curves is separable if and only if*

$$\psi^* : \Omega_{C_2} \to \Omega_{C_1}$$

is non-zero (equivalently injective).

Proof. Note since k was perfect, we have $k(C_1)/\psi^* k(C_2)$ is separable if and only if $\overline{k(C_1)}/\psi^*\overline{k}(C_2)$ is separable. Let $y \in \overline{k}(C_2)$ such that dy generates Ω_{C_2}, in other words $\overline{k}(C_2)/\overline{k}(y)$ is separable. Then

$$\Psi^* \text{ injective } \Leftrightarrow \psi^* dy = d\psi^* \text{is a basis for } \Omega_{C_1}$$

$$\Leftrightarrow \overline{k}(C_1)/\psi^* y \text{is separable}$$

$$\Leftrightarrow \overline{k}(C_1)/\psi^*\overline{k}(C)_2 \text{is separable}$$

where the last equivalence follows from the fact that $\overline{k}(C_2)/\overline{k}(y)$ is separable. □

0.2. **Intersection multiplicities and Bezout's theorem.** Let M be a module over a ring R. A chain of length l in M is a sequence of submodules

$$M_0 \subsetneq M_1 \subsetneq ... \subsetneq M_l$$

Definition 0.7. The length of M is the length of the longest chain of submodules of M. When this is an integer we say M is of finite length.

The above allows to make an algebraic definition of intersection multiplicity in the algebraic setting.

Let $C_1, C_2 \subset \mathbb{A}^2$ defined by the equations f_1, f_2 be two curves which intersect at a point P, the intersection multiplicity at P, denoted by $I_P(C_1, C_2)$, is defined to be the length of the $\overline{k}[x,y]_P$ module $\overline{k}[x,y]_P/(f_1, f_2)$.

Example 0.8. Let $k = \overline{k}$ and let C_1 be the curve in $\mathbb{A}^2$ given by the equation $y^2 = x^3 + x$ and C_2 the line $ax - by = 0$. Let $P = (0,0)$, one computes that the tangent line at P of C_1 is given by the line $x = 0$, hence one would expect the intersection multiplicity to be > 1 if $b = 0$ and 1 otherwise.

Suppose $b \neq 0$, then we define $c = a/b$ so that $y = cx$. Then $\overline{k}[x,y]_P/(f_1, f_2)$ is isomorphic to $k[x]_P/(x^3 - cx^2 + x) = k[x]_P/(x(x^2 - cx + 1))$. Since polynomials with non-zero constant term are invertible in $k[x]_P$, we see that $x^2 - cx + 1$ is a unit in $\overline{k}[x,y]_P$, hence

$$\overline{k}[x,y]_P/(f_1, f_2) \cong \overline{k}[x]/(x) \cong \overline{k}$$

and this module clearly has length 1.

If however $b = 0$, we have $\overline{k}[x,y]_P/(f_1, f_2) \cong \overline{k}[y]_P/(y^2)$ which has the chain of length 2

$$0 \subsetneq (y) \subsetneq \overline{k}[y]_P/(y^2)$$

Thus this definition agrees with geometric intuition of lines with the same tangent space intersecting with a larger multiplicity.

Now if $C_1, C_2 \subset \mathbb{P}^2$ are two curves defined by homogeneous f_1, f_2 and $P \in C_1 \cap C_2$, by taking open affine covers and dehomogenising we can apply the above definition and define the intersection multiplicity $I_P(C_1, C_2)$; it is independent of the affine chart chosen.

Theorem 0.9. *(Bezout's theorem) Let $C_1, C_2 \subset \mathbb{P}^1$ be two curves over k defined by f_1 and f_2 of degrees n_1 and n_2 respectively. Then $C_1 \cap C_2$ is finite and we have*

$$\sum_{P \in C_1 \cap C_2} I_P(C_1, C_2)$$

Proof. [Hartshorne] I 7.8 □

1. Elliptic curves

In this section, we study elliptic curves from the point of view of algebraic geometry. Over $\mathbb{C}$ elliptic curves and complex tori are the same thing, and our first order business will be to show that the group structure can be defined algebraically. This is a hugely important result as it provides the mechanism which forces the torsion points to generate algebraic extensions and moreover this definition can be generalised to an elliptic curves over any field K. Important special cases are when K is a number field or when K is a finite field; these cases are related by reducing an elliptic curve mod$p$.

1.1. **Elliptic curves over general fields.**

Let us begin with the general definition of an elliptic curve.

Definition 1.1. Let K be a field. An elliptic curve over K is a pair $(E, 0)$ where E is a non-singular projective curve of genus 1 together with a point $0 \in E(K)$.

An isomorphism $\phi : E \to E'$ of elliptic curves is a ismorphism of algebraic curves such that $\phi(0) = 0'$.

For the definition of genus see Silverman [AEC] Chapter II Section 4

Normally we just speak of an elliptic curve E, with the given point 0 understood. This is a somewhat abstract definition, however it follows from the Riemann Roch theorem that every elliptic curve can be written as a plane cubic curve. More precisely we could just as well have defined an elliptic curve as follows.

Definition 1.2. An elliptic curve over K, is the projectisation of a curve in $\mathbb{A}^2_K$ defined by the equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, ..., a_6 \in K$, such that the curve is smooth.

Let us briefly explian why the two definitions are equivalent. Given an elliptic curve in the sense of 1.1, the Riemann Roch theorem gives an embedding of E into $\mathbb{P}^2$ of the form given in 1.2, which sends the point 0 to the point $(0 : 1 : 0)$ at ∞. Conversely given a equation of the form in 1.2 which defines a smooth curve, one shows that this curve is of genus 1 and the point at ∞ gives the point $0 \in E(K)$.

An equation of the above form which represents an elliptic curve E is called a *Weierstrass* equation for E. One should note that it is possible that an elliptic can be represented by more than one Weierstrass equation, however any two Weierstrass equations can be related via a simple change of variables as in the proposition below.

Proposition 1.3. *Let E be an elliptic curve over K*

i)Any two Weirstrass equations are related by a linear change of variable given by:

$$x = ux' + r$$
$$y = u^3y' + su^2x' + t$$

where $u, r, s, t \in \overline{K}, u \neq 0$.

ii) If char$K \neq 2, 3$ there exists a Weierstrass equation for E of the form

$$y^2 = x^3 + a_4x + a_6$$

Exercise: Show that the planar curve defined by an equation $y^2 = x^3 + a_2x^2 + a_4x + a_6$ is smooth (and hence corresponds to an elliptic curve) if and only if the cubic equation $x^3 + a_2x^2 + a_4x + a_6$ has distinct roots.

Given a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for an elliptic curve E, we also define the following associated quantities.

$$b_2 = a_1^2 + 4a_2,$$
$$b_4 = 2a_4 + a_1a_3,$$
$$b_6 = 4a_3^3 + a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$
$$\Delta = -b_2^2b_8 - b_4^3 - 27b_6^2 + 9b_2b_4b_6$$
$$j = \frac{(b_2^2 - 24b_4)^2}{\Delta}$$

Δ is the *discrimianant* of the equation and j is known as the j-invariant (we will relate this to the complex j-function in a moment).

These become much simpler when if char$K \neq 2, 3$ and the equation is given in the form of 1.3 ii). However even though we are really only interested in elliptic curves over number fields, the proofs of many results reslies on the studying elliptic curves over finite fields, including ones with characteristic 2 and 3. Thus we make the following convention that all results will be stated for general Weierstrass equations, however if it makes the proofs substantially shorter, we will assume char$K \neq 2, 3$ and refer the reader to the Appendix in Silverman "AEC" for proofs of the general case.

The following Proposition tells how these quantities behave under change of variables as in 1.3 i).

Proposition 1.4. *i) Under the change of variable*

$$x = ux' + r$$
$$y = u^3y' + su^2x' + t$$

we have

$$u^{12}\Delta' = \Delta, \; j = j'$$

ii) A curve defined by a Weierstrass equation is non-singular if and onyl if Δ' is non-zero.

Proof. i) Appendix of [AEC], or an exercise for masochists.

ii) Note that by part i), $\Delta' \neq 0$ iff $\Delta' \neq 0$ so suffices to check for one Weierstrass representation. When char$K \neq 2, 3$, this follows from the exercise above since in this case Δ is just a multiple of the discriminant of the cubic polynomial. The general case is another calculation, see Proposition 1.4 a) of [AEC]. □

For example, let E_τ be a complex torus over $\mathbb{C}$ defined by the lattice Λ_τ. The Weierstrass $\wp$ function defines a bijection between E_τ and the curve defined by

$$y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

This defines a elliptic curve (also denoted E_τ) over $\mathbb{C}$, and we obtain a Weierstrass equation by making the substitution $y = 2y'$. Under this bijection 0 is sent to the point at ∞. In this case the quantities above simplify and we have

$$b_2 = 0, \; b_4 = g_2(\tau)/2, \; b_6 = g_3(\tau), \; b_8 = -g_2(\tau)^2/16$$

and one easily calculates that

$$\Delta = g_2(\tau) - 27g_3(\tau)^3 = \Delta(\tau)$$
$$j = 1728\frac{g_2(\tau)}{\Delta(\tau)} = j(\tau)$$

Thus the j-function evaluated on τ is the j-invariant of the associated elliptic curve of $\mathbb{C}/\Lambda_\tau$.

The j-invariant is then a well-defined invariant of the set of isomorphism classes of elliptic curves over any field. We can say a little more.