CCR Expository Report 34
An Elementary Introduction to Elliptic Curves II

Leonard S. Charlap
Raymond Coley

July 1990

Abstract

This paper is the second in a series whose purpose is to provide elementary proofs of the main results on elliptic curves with emphasis on curves over finite fields. The main results proved in this part concern rational maps between elliptic curves and Weil reciprocity. We prove that all isogenies are homomorphisms and the "Lower Star Theorem", as well as generalized Weil reciprocity.

Introduction

These notes are a continuation of [5]. Our goal in [5] was to provide elementary proofs for the results used by Schoof in [12]. In doing this we left out those parts of the basic material on elliptic curves that were unnecessary for this purpose. In these notes we would like to fill in some of those gaps.

Our main topic concerns rational maps between elliptic curves, a topic omitted in [5]. A secondary topic is Weil reciprocity which we use to further the study of the Weil pairing. Some of the results about rational maps between elliptic curves simply carry over from similar results proved in [5] about rational maps from an elliptic curve to itself. Many of the other results we present are usually proved using large amounts of commutative algebra. We have been able to find elementary proofs much in the style of [5]. A characteristic of these proofs is that although the theorems hold for more general varieties, our elementary proofs only work in the case of elliptic curves.

Unfortunately the situation is different in the case of Weil reciprocity. We have not been able to find a proof that avoids some more or less advanced notions, *i.e.*, Dedekind domains or valuation theory. We have chosen to present the required result without proof in the body of the notes and to relegate the more difficult material (and the proof) to a rather long Appendix. In this Appendix we develop the necessary theory starting from about the same level required in the rest of the notes so again you should not have to consult a lot of other books. One somewhat unsatisfactory result of this treatment is that the

theorems of the Appendix hold in such generality that they include some of the earlier results.

We would like to thank David Robbins for insightful remarks, abundant useful criticism, and unstinting encouragement. We would also like to thank Noam Elkies for a number of incisive comments and suggestions.

In Section 1, we review some results from [5] about rational mappings and make the obvious extensions to rational mappings between elliptic curves. Section 2 provides a new proof of the key result that up to translation all rational mappings between elliptic curves are homomorphisms. Section 3 reviews some elementary field theory, while Section 4 is concerned with elementary Galois theory. Section 5 covers some elementary material on the norm map. Sections 3, 4, and 5 are required in the proof of the "Lower Star Theorem". They only contain standard results and can be omitted by a knowledgeable reader. Section 6 investigates the norm map on the various fields associated to an elliptic curve, and proves the "Lower Star Theorem". Section 7 begins the discussion of Weil reciprocity. Section 8 contains standard results from valuation theory, and Section 9 completes the proof of generalized Weil reciprocity. Section 10 applies Weil reciprocity to yield a new expression for the Weil pairing.

We use the notations and assumptions of [5] except that in the Appendix we use the numbering 3.4b, for example, to refer to a theorem (or whatever) in the body of the paper. In particular, we assume that our ground field has characteristic not equal to two or three.

1 Rational Maps Between Elliptic Curves

We let k be any field (with appropriate characteristic). We let K denote its algebraic closure. Let E and E' be elliptic curves over k with equations

$$Y^2 = X^3 + AX + B$$

and

$$Y^2 = X^3 + A'X + B'$$

respectively. We let $\mathcal{O}$ and $\mathcal{O}'$ denote the respective identity elements and x, y, x', and y' the coordinate functions.

Definition 1.1. A *rational map* F from E to E' is a pair (r, s) where r and s are rational functions on E such that

$$s^2 = r^3 + A'r + B' \quad .$$

If we make the convention that $F(P) = \mathcal{O}'$ if and only if r and s are not finite at P, we see that F actually defines a map from E to E' by $F(P) = (r(P), s(P))$ since r and s must have poles at the same points, and if they do not have poles, $(r(P), s(P))$ will be a point on E'.

Remark. There is an amusing way of looking at rational maps that will actually be useful. Given the field k, we form the elliptic curve E' using the equation

$$Y^2 = X^3 + A'X + B' \quad . \tag{1}$$

Now suppose we consider the field of rational functions $K(E)$ on the curve E. Then we can use the same equation to form a new elliptic curve, which we might denote by $E'(K(E))$. Now $K(E)$ may not be algebraically closed, and by our convention, the points of $E(K(E))$ have coordinates in the algebraic closure of $K(E)$. The finite points whose coordinates lie in $K(E)$ (*i.e.*, the $K(E)-$rational points) are precisely the rational maps from E to E'. We can think of the identity of this curve, call it $\mathcal{O}_M$, as the "map" with the constant value $\mathcal{O}'$.

All of the results and proofs on rational maps in [5, Part II] carry over to the case of rational maps between elliptic curves with the obvious modifications. We state some here for ease of reference.

Proposition 1.1. A nonconstant rational mapping $F : E \to E'$ is onto.

Definition 1.2. The *ramification index of* F *at* $P \in E$ is defined by

$$e_F(P) = \mathrm{ord}_P(u' \circ F) \quad ,$$

where u' is a uniformizing variable at $F(P) \in E'$.

Proposition 1.2. Suppose that r' is a nonzero rational function on E' and $F : E \to E'$ is a nonconstant rational mapping. Let $P \in E$. Then

$$\mathrm{ord}_P(r' \circ F) = [\mathrm{ord}_{F(P)} r'] \cdot [e_F(P)] \quad .$$

Definition 1.3. Suppose that $F : E \to E'$ is a nonconstant rational mapping. We define $F^* : K(E') \to K(E)$ by $F^*(r') = r' \circ F$. We also define $F^* : \mathrm{Div}(E') \to \mathrm{Div}(E)$ to be the homomorphism with

$$F^*(\langle Q' \rangle) = \sum_{F(P)=Q'} e_F(P)\langle P \rangle \quad .$$

Proposition 1.3. $F^* : \mathrm{Div}(E') \to \mathrm{Div}(E)$ is one–to–one.

Proposition 1.4. Suppose that $F : E \to E'$ is a nonconstant rational mapping and that r' is a nonzero rational function in $K(E')$. Then

$$\mathrm{div}(F^*(r')) = \mathrm{div}(r' \circ F) = F^*(\mathrm{div}(r')) \quad .$$

Proposition 1.5. Suppose that $F_1 : E \to E'$ and $F_2 : E' \to E''$ are nonconstant rational mappings. Then

$$(F_2 \circ F_1)^* = F_1^* \circ F_2^* \quad .$$

2 Homomorphisms

In [5] we studied *endomorphisms*, while here we study *homomorphisms*.

Definition 2.4. A rational mapping from E to E' that is also a group homomorphism is called a *homomorphism*. These mappings form a group, which we denote by $\mathrm{Hom}(E, E')$.

We are also interested in an apparently more general class of mappings.

Definition 2.5. A rational mapping $F : E \to E'$ with the property that $F(\mathcal{O}) = \mathcal{O}'$ is called an *isogeny*.

Clearly every homomorphism is an isogeny. The main result of this section is to show that every isogeny is a homomorphism.

Definition 2.6. A rational map $F : E \to E'$ is said to be *even* (respectively *odd*) if $F(-P) = F(P)$ (respectively $F(-P) = -F(P)$) for all $P \in E$.

It is obvious that an even homomorphism must be the map $\mathcal{O}_M$ that sends everything into $\mathcal{O}'$. If our main result is to hold, then *all* even maps must be constant since all maps are the composition of an isogeny and a translation. This is the first part of the proof of the main theorem of this section.

Theorem 2.1. All even mappings are constant.

Proof. Let $F : E \to E'$ be even. Write $r = x' \circ F$ and $s = y' \circ F$. Then $r, s \in k(E) = k(x, y)$. Now $F(-P) = F(P)$ implies $r(-P) = r(P)$ and $s(-P) = s(P)$, so by [5, Exercise 6.8], $r, s \in k(x)$.

Hence it suffices to show that there are no nonconstant functions $r, s \in k(x)$ which satisfy

$$r^2 = s^3 + A's + B' \quad .$$

This is really just a result about rational functions of one variable and has nothing to do with the curves E and E' *per se*. We can slightly restate it as follows: If d_1, d_2, d_3 are distinct in k, and $a, b \in k(X)$ satisfy

$$b^2 = (a - d_1)(a - d_2)(a - d_3) \quad , \tag{2}$$

then a and b are constant. (Here we use X to denote an indeterminate.)

We can write a and b in the form $a = q/c^2$ and $b = p/c^3$ for $p, q, c \in k[X]$ where we assume c has minimal degree. Then (2) becomes

$$(q - d_1c^2)(q - d_2c^2)(q - d_3c^2) = p^2 \quad . \tag{3}$$

So we want to show that (3) has no solutions (with d_1, d_2, d_3 distinct in k) such that q, c, and p are not all constants.

Now we show that the $(q - d_ic^2)$ are pairwise relatively prime for $i = 1, 2, 3$. Suppose that π were a common irreducible factor of $q - d_1c^2$ and $q - d_2c^2$. Then π divides q and c^2 and so divides $q - d_3c^2$ as well. Then (3) implies that $\pi^3 | p^2$ so $\pi^4 | p^2$. Thus π^2 divides one of the $q - d_ic^2$. Since $\pi | c^2$, we have $\pi^2 | c^2$. Therefore we may conclude that $\pi^2 | q$. It now follows that $\pi^6 | p^2$ so that $\pi^3 | p$. We could therefore replace p by p/π^3, q by q/π^2 and c by c/π to obtain another representation of a and b with a c of lower degree which is a contradiction.

Now we are reduced to showing that the system

$$\begin{aligned} q - d_1 c^2 &= s_1^2 \\ q - d_2 c^2 &= s_2^2 \\ q - d_3 c^2 &= s_3^2 \end{aligned} \tag{4}$$

has no solutions where the s_i are pairwise relatively prime polynomials and q, c, s_1, s_2, and s_3 are not all constant. Subtracting and rewriting, we see that it suffices to show that the system

$$\begin{aligned} {s_1}^2 - {s_3}^2 &= t_1^2 c^2 \\ {s_1}^2 - {s_2}^2 &= t_2^2 c^2 \end{aligned} \tag{5}$$

has no solutions, s_1, s_2, s_3, which are pairwise relatively prime and s_1, s_2, s_3, and c are not all constants. In this system we are given that ${t_1}^2$ and ${t_2}^2$ (which are constants) are not equal or zero.

Assume we have such a solution and that $\max(\deg s_1, \deg s_3)$ is minimal among such solutions. Since s_1 and s_3 are relatively prime, (5) implies that we can write $s_1 - s_3 = 2f^2$ and $s_1 + s_3 = 2g^2$ for polynomials f and g which will be relatively prime and not both constant. (If f and g are both constant, then s_1 and s_3 will be constant. Hence c will be constant and so will s_2.)

We have

$$2 \cdot \max(\deg f, \deg g) \leq \max(\deg s_1, s_3) \quad .$$

Since both f and g cannot be constant, $\max(\deg f, \deg g)$ is strictly less than $\max(\deg s_1, s_3)$. Using the second equation of (5), we see that

$$f^4 - \lambda f^2 g^2 + g^4 = {s_2}^2 \tag{6}$$

and λ is not equal to ± 2 where $\lambda = 4(t_2/t_1)^2 - 2$.

If we factor (6), we get

$$(f^2 - \mu g^2)(f^2 - \mu' g^2) = {s_2}^2 \tag{7}$$

where $\mu\mu' = 1$ and $\mu + \mu' = \lambda \neq \pm 2$. In particular we see that μ and μ' are not zero or equal. Hence there are polynomials h and k such that

$$\begin{aligned} f^2 - \mu g^2 &= h^2 \\ f^2 - \mu' g^2 &= k^2 \end{aligned} \tag{8}$$

and this system is of the same form as (5) with f corresponding to s_1 and h corresponding to s_3. Now (8) implies

$$\max(\deg f, \deg h) \leq \max(\deg f, \deg g)$$

which is strictly less than $\max(\deg s_1, \deg s_3)$. As this contradicts our assumption, we are done. ∎

Now it is not difficult to prove our main result.

Theorem 2.2. All isogenies are homomorphisms.

Proof. Let $\alpha_0 : E \to E'$ be an isogeny. Define $\alpha_\pm : E \to E'$ by

$$\alpha_+(P) = \alpha_0(P) + \alpha_0(-P)$$
$$\alpha_-(P) = \alpha_0(P) - \alpha_0(-P)$$

for $P \in E$.

Then $2\alpha_0 = \alpha_+ + \alpha_-$. Since $\alpha_+(-P) = \alpha_+(P)$, we see by the previous theorem that α_+ is a constant map. Since

$$\alpha_0(\mathcal{O}) = \mathcal{O}', \quad \alpha_+(P) = \mathcal{O}' \ \forall P \in E \quad ,$$

and we have

$$2\alpha_0 = \alpha_- \quad .$$

Suppose we could show that α_- is a homomorphism. Then we would have

$$2(\alpha_0(P+Q) - \alpha_0(P) - \alpha_0(Q)) = \mathcal{O}'$$

which implies that

$$\alpha_0(P+Q) - \alpha_0(P) - \alpha_0(Q) \in E'[2]$$

for all $P, Q \in E$. Fixing Q, this is a nonsurjective map, and hence by Proposition 1.1 it is a constant function of P. Since α_0 is an isogeny, this constant must be $\mathcal{O}'$. Hence if we can show α_- is a homomorphism, then α_0 will also be one.

So now we can assume that we have an *odd* isogeny $\alpha : E \to E'$. Let $Q \in E$ and put

$$\beta_Q(P) = \alpha(P+Q) - \alpha(P-Q) \quad .$$

It is now trivial to see that $\beta_Q(-P) = \beta_Q(P)$. Hence β_Q is constant, and we get

$$\beta_Q(P) = \beta_Q(\mathcal{O}) = \alpha(Q) - \alpha(-Q) = 2\alpha(Q) \tag{9}$$

for all $P \in E$.

Claim. $\alpha(n \cdot P) = n \cdot \alpha(P)$.

The proof of the claim is by induction. It is clear for $n = 0$ or 1. Consider

$$\begin{aligned} \beta_P(n \cdot P) =& \alpha((n+1) \cdot P) - \alpha((n-1) \cdot P) \\ =& \alpha((n+1) \cdot P) - (n-1) \cdot \alpha(P) \end{aligned}$$

where the last line follows by induction. On the other hand, by (9)

$$\beta_P(n \cdot P) = 2\alpha(P) \quad .$$

Therefore

$$\alpha((n+1) \cdot P) = 2\alpha(P) + (n-1) \cdot \alpha(P) = (n+1) \cdot \alpha(P)$$

which proves the claim.

Put

$$\gamma_Q(P) = \alpha(P+Q) - \alpha(P) - \alpha(Q) \quad .$$

Suppose $m \cdot P = Q$. Then

$$\begin{aligned}\gamma_Q(P) &= \gamma_{m\cdot P}(P) \\ &= \alpha(P + m\cdot P) - \alpha(P) - \alpha(m\cdot P) \\ &= (m+1)\cdot\alpha(P) - \alpha(P) - m\cdot\alpha(P) \\ &= \mathcal{O}' \quad .\end{aligned}$$

Hence for fixed Q, $\gamma_Q(P) = \mathcal{O}'$ for all P such that $m\cdot P = Q$ for some m. Now it follows from [Corollary 7.6]ccr82299 that there are m^2 such P for each m prime to the characteristic of k. Since there are infinitely many such P, $\gamma_Q(P) = \mathcal{O}'$ for all $P, Q \in E$ which implies that α is a homomorphism. ■

Henceforth we will use the words *isogeny* and *homomorphism* interchangeably. Notice that the theorem tells us that *any* rational mapping is the composition of an isogeny and a translation. This means that to assume that a rational mapping between elliptic curves is a homomorphism is not a very strong assumption.

3 Some Field Theory

Let $\alpha : E \to E'$ be a rational map, and let x' and y' be the coordinate functions on E'. Definition 1.3 defines a map $\alpha^* : \mathrm{Div}(E') \to \mathrm{Div}(E)$. It is easy to define a map in the other direction.

Definition 3.7. Define $\alpha_* : \mathrm{Div}(E) \to \mathrm{Div}(E')$ by setting $\alpha_*(\langle P\rangle) = \langle\alpha(P)\rangle$ for the generators of $\mathrm{Div}(E)$ and extending linearly.

One of the main objectives of this part of these notes is to show that if D is a principal divisor then so is $\alpha_*(D)$. In fact, we will define a map, also denoted by α_*, from $K(E)$ to $K(E')$ such that

$$\alpha_*(\mathrm{div}(r)) = \mathrm{div}(\alpha_*(r)) \quad .$$

Note that if $\alpha(\mathcal{O}) = P'$, then $\beta = T_{-P'} \circ \alpha$ takes $\mathcal{O}$ into $\mathcal{O}'$, and β is an isogeny. Furthermore if $D \in \mathrm{Div}(E)$ and $\beta_*(D) = \mathrm{div}(r')$, then $\alpha_*(D) = \mathrm{div}(r' \circ T_{P'})$. Hence it suffices to investigate the case of α a homomorphism.

It turns out that to study this situation (and, in fact, many others) it is advantageous to adopt the somewhat more abstract point of view alluded to in the remark on [5, page 60] (see next paragraph). We will do that in this section. Most of the material is perfectly standard results from the elementary theory of fields, and so we will not give precise proofs for all of it. Good references are [1] and [17, Chapter II].

Let $K' = \alpha^*(K(E')) \subset K(E)$. K' consists of all functions in $K(E)$ of the form $r' \circ \alpha$ for some $r' \in E'$. Let $\bar{x} = x' \circ \alpha$ and $\bar{y} = y' \circ \alpha$ so $\bar{x}, \bar{y} \in K' \subset K(E)$. The idea here is to regard $K(E)$ as an extension of K'.

We show that $K(E)$ is a finite algebraic extension of K'. First observe that K' is isomorphic to $K(E')$ and hence is generated by $\bar{x}$ and $\bar{y}$ over K. Since y (respectively $\bar{y}$) satisfies an algebraic (in fact quadratic) equation over $K(x)$ (respectively $K(\bar{x})$), both $K(E)$ and K' have the same transcendence degree (namely 1) over K, *i.e.*, both $K(E)$ and K' have elements, x and $\bar{x}$ respectively, that do not satisfy any polynomial in $K[X]$ and such that $K(E)$ and K' are algebraic over $K(x)$ and $K(\bar{x})$ respectively.

Now if x were transcendental over K', then x and $\bar{x}$ would both be elements of $K(E)$ transcendental over K which are algebraically independent. This would mean that the transcendence degree of $K(E)$ over K would have to be at least two. Hence x is algebraic over K' and $K(E)$ is a finite algebraic extension of K'.

Recall that in [5], we said that α was *separable* if $e_\alpha = 1$. We want to see how this condition is reflected in the extension $K(E)$ over K'. We first need an easy and well–known lemma.

Lemma 3.1. Let M be an extension of a field L and $r \in M$ be algebraic over L. Let f be a polynomial in $L[X]$ of minimal degree with $f(r) = 0$. Then f is irreducible, and if $g \in L[X]$ satisfies $g(r) = 0$, then f divides g. Hence for $r \in M$ algebraic over L there is a unique monic (*i.e.*, leading coefficient one) irreducible polynomial $f \in L[X]$ with $f(r) = 0$.

Exercise 3.1. Prove this lemma.

Definition 3.8. The unique monic irreducible polynomial $f \in L[X]$ with $f(r) = 0$ is called the *minimal* polynomial of r. We denote it by m_r.

Definition 3.9. We say an irreducible polynomial is *separable* if it has nonzero derivative. We say a reducible polynomial is *separable* if each of its irreducible factors is separable. A polynomial that is not separable is said to be *inseparable*.

If M is an extension of L, we say $r \in M$ is *separable over* L if m_r is separable. Otherwise we say r is *inseparable*. We say M is a *separable* extension of L if m_r is separable for each $r \in M$. Otherwise we say M is *inseparable* over L.

It is easy to see that an irreducible polynomial f is inseparable if and only if $f(X) = g(X^p)$ for some polynomial g where p is the characteristic of L. Suppose $f \in L[X]$ is inseparable so $f(X) = f_1(X^p)$ and the degree of f is divisible by p. If now f_1 is inseparable, then $f_1(X) = f_2(X^p)$ and the degree of f is divisible by p^2. Since the degree of f is finite, there is $s \geq 0$ such that $f(X) \in L[X^{p^s}]$, but $f \notin L[X^{p^{s+1}}]$. So we can write

$$f(X) = f_0(X^{p^s}) \quad ,$$

and if $\deg f = n$ and $\deg f_0 = n_0$, then

$$n = n_0 p^s \quad .$$

Definition 3.10. The integer n_0 is called the *degree of separability* of f, while p^s is called the *degree of inseparability* of f.

It is clear that if $p = 0$ then everything must be separable.

Exercise 3.2. Show that if L is perfect, then every polynomial in $L[X]$ is separable.

One can prove the converse of this exercise (in the case of positive characteristic) if one knows the following result (which we need later anyway):

Lemma 3.2. Suppose $r \in L$ and there is no $s \in L$ with $s^p = r$. Then $X^{p^e} - r$ is irreducible in $L[X]$ for all $e \geq 0$.

Proof. Let $\varphi(X)$ be a nonconstant irreducible monic factor of $X^{p^e} - r$ in $L[X]$. Let ρ be a root of φ in some extension L' of L. Then $r = \rho^{p^e}$ and

$$X^{p^e} - r = (X - \rho)^{p^e} \quad .$$

If $\psi(X)$ is any nonconstant irreducible monic factor of $X^{p^e} - r$ in $L[X]$, then $\psi(X)$ is a power of $X - \rho$, so $\psi(\rho) = 0$. Hence $\varphi | \psi$, and consequently $\varphi = \psi$. This shows that $X^{p^e} - r$ is a power of $\varphi(X)$, say $X^{p^e} - r = \varphi(X)^m$. Since $\deg(X^{p^e} - r) = p^e$, $\deg \varphi(X)$ and m must be powers of p. Hence $X^{p^e} - r = \varphi(X)^{p^t}$ for some $t \geq 0$. Let $c \in L$ be the constant term of φ. We have $r = (\pm c)^{p^t}$. Since r does not have a p^{th} root in L, we must have $t = 0$, so $X^{p^e} - r = \varphi(X)$ is irreducible in $L[X]$. ∎

Exercise 3.3. i) Suppose L is a field of characteristic $p > 0$ and that every polynomial (of positive degree) in $L[X]$ is separable. Show that L is perfect.

ii) Find a proof of the above lemma that does not use the fact that $X^{p^e} - r$ has a root in some extension. (**Hint:** Write

$$X^{p^e} - r = [\varphi(X)]^h \cdot \psi(X)$$

for appropriate φ and ψ and differentiate.)

Let M be an extension of L. We know that $r \in M$ is inseparable if $m_r'(X) = 0$. It turns out, however, that it suffices merely to have m_r' vanish at r.

Proposition 3.6. Suppose $r \in M$. Then r is inseparable over L if $m_r'(r) = 0$. Furthermore if r is inseparable over L and $g \in L[X]$ satisfies $g(r) = 0$, then $g'(r) = 0$.

Proof. $m_r'(r) = 0$ implies $m_r' = 0$ since m_r' has lower degree than m_r. Hence r is inseparable. The converse is obvious.

If $g(r) = 0$, then $g(X) = h(X) \cdot m_r(X)$. Hence $g'(r) = h(r) \cdot m_r'(r)$ since $m_r(r) = 0$. If r is inseparable, we get $g'(r) = 0$ as desired. ∎

Now suppose $g \in L[X]$ and $g(r) = 0$. Then $X - r$ divides g considered as a polynomial in $M[X]$, *i.e.*, we can write

$$g(X) = (X - r)^s g_1(X)$$

for some integer $s \geq 1$ and some $g_1(X) \in M[X]$ with $g_1(r) \neq 0$. Since r is a member of $L(r) \subset M$, we can apply the same argument to the field $L(r)$ instead of M. We get

$$g(X) = (X - r)^\sigma g_2(X)$$

for some integer $\sigma \geq 1$ and some $g_2(X) \in L(r)[X]$ with $g_2(r) \neq 0$. The above two equations imply that $\sigma = s$ and $g_1 = g_2$. Thus s depends only on $g(X)$ and the element r and not on the extension M.

Definition 3.11. We call s the *multiplicity* of the root r of g.

We have the following easy corollary which is just a restatement of the proposition.

Corollary 3.1. Suppose $r \in M$. Then r is inseparable over L if and only if r is a multiple root of m_r. Furthermore if r is inseparable over L and $g(X) \in L[X]$ satisfies $g(r) = 0$, then r is a multiple root of g.

Actually we can describe the multiplicity of the roots of an irreducible polynomial that splits completely in some extension. Suppose $f \in L[X]$ and M is an extension of L so that f factors completely in $M[X]$, *i.e.*,

$$f(X) = c_0(X - r_1)(X - r_2)\cdots(X - r_n)$$

with $r_i \in M$.

Proposition 3.7. If $f(X) \in L[X]$ is irreducible and has degree of inseparability p^s, then each linear factor in the above equation appears exactly p^s times.

Proof. We have $f(X) = g(X^{p^s})$ for some irreducible separable polynomial $g \in L[X]$. Each element ${r_i}^{p^s}$ (where the r_i are the roots of f) is a root of g and must be a simple root of g. Hence

$$g(X) = (X - {r_i}^{p^s})g_i(X)$$

where $g_i(X) \in M[X]$ and $g_i({r_i}^{p^s}) \neq 0$. Then

$$f(X) = (X - r_i)^{p^s} f_i(X)$$

where $f_i(r_i) = g_i({r_i}^{p^s}) \neq 0$. This shows that $X - r_i$ is a factor of $f(X)$ of multiplicity exactly p^s. ∎

4 Some Galois Theory

In Part I we used a theorem from Galois theory to prove the crucial Lemma 12.13. We will need that theorem here also so we will include a proof. The material of this section is standard. Our treatment follows [1].

Theorem 4.3. Let G be a finite group of automorphisms of a field M and let L be the set of points of M left fixed by all of the elements of G. Then L is a subfield of M and $[M : L]$ equals the order of G.

Proof. It is an easy exercise to see that L is a subfield of M. Let $|G| = n$ and $[M : L] = m$, and suppose $m < n$. Let $g_1, \ldots, g_n$ be the elements of G, and let $r_1, \ldots, r_m$ be a basis for M over L. Consider the following system of linear equations:

$$\begin{array}{ccccccccc}
g_1(r_1)X_1 & + & g_2(r_1)X_2 & + & \cdots & + & g_n(r_1)X_n & = & 0 \\
g_1(r_2)X_1 & + & g_2(r_2)X_2 & + & \cdots & + & g_n(r_2)X_n & = & 0 \\
\vdots & & \vdots & & \ddots & & \vdots & & \vdots \\
g_1(r_m)X_1 & + & g_2(r_m)X_2 & + & \cdots & + & g_n(r_m)X_n & = & 0 \quad .
\end{array}$$

Since there are n unknowns $X_1, \ldots, X_n$ and m equations, and we have assumed $m < n$, there is a nontrivial solution, say $x_1, \ldots, x_n$ in M. Let r be an arbitrary element of M. We can write

$$r = \sum_{i=1}^{m} a_i r_i$$

with $a_i \in L$. If we multiply the first equation by a_1, the second by a_2 and so on, and then use the fact that since $a_i \in L$, $g_j(a_i) = a_i$, and the fact that $g_j(a_i r_i) = a_i g_j(r_i)$, we get

$$\begin{array}{ccccccccc}
g_1(a_1r_1)x_1 & + & g_2(a_1r_1)x_2 & + & \cdots & + & g_n(a_1r_1)x_n & = & 0 \\
g_1(a_2r_2)x_1 & + & g_2(a_2r_2)x_2 & + & \cdots & + & g_n(a_2r_2)x_n & = & 0 \\
\vdots & & \vdots & & \ddots & & \vdots & & \vdots \\
g_1(a_mr_m)x_1 & + & g_2(a_mr_m)x_2 & + & \cdots & + & g_n(a_mr_m)x_n & = & 0 \quad .
\end{array}$$

Adding these equations, we obtain

$$g_1(r)x_1 + g_2(r)x_2 + \cdots + g_n(r)x_n = 0 \quad . \tag{10}$$

Since the automorphisms of M form a vector space over M, this equation shows that the automorphisms $g_1, \ldots, g_n$ are dependent over M. If $n = 1$, then Equation (10) is impossible since x_1 was assumed to be a nontrivial solution and g_1 is an automorphism.

Assume inductively that Equation (10) cannot hold for a set of automorphisms of size $< n$. Pick $s \in M^*$ with $g_n(s) \neq g_1(s)$. Now replace r in (10) by $s \cdot r$ and use the fact that the g_i's are automorphisms to obtain

$$g_1(s)g_1(r)x_1 + g_2(s)g_2(r)x_2 + \cdots + g_n(s)g_n(r)x_n = 0 \quad . \tag{11}$$

Divide (11) by $g_n(s)$ and subtract the result from (10). The terms with $g_n(r)$ cancel out, and we get

$$g_1(r)x_1 \left(1 - \frac{g_1(s)}{g_n(s)}\right) + \cdots + g_{n-1}(r)x_{n-1} \left(1 - \frac{g_{n-1}(s)}{g_n(s)}\right) = 0 \quad .$$

Since we have assumed $g_1(s) \neq g_n(s)$, the coefficient of $g_1(r)$ is not zero, and we have an equation of dependence for the elements of a set of automorphisms of size $n-1$ which contradicts our induction hypothesis. Hence we have shown that $m \geq n$.

Now assume $m > n$, and suppose g_1 is the identity of G. Since $m > n$, there are $n+1$ elements $r_1, r_2, \ldots, r_{n+1}$ of M which are linearly independent over L. Consider the following system of linear equations:

$$\begin{array}{ccccccccc}
g_1(r_1)X_1 & + & g_1(r_2)X_2 & + & \cdots & + & g_1(r_{n+1})X_{n+1} & = & 0 \\
g_2(r_1)X_1 & + & g_2(r_2)X_2 & + & \cdots & + & g_2(r_{n+1})X_{n+1} & = & 0 \\
\vdots & & \vdots & & \ddots & & \vdots & & \vdots \\
g_n(r_1)X_1 & + & g_n(r_2)X_2 & + & \cdots & + & g_n(r_{n+1})X_{n+1} & = & 0 \quad .
\end{array}$$

Again we have more unknowns than equations so there is a nontrivial solution. This solution cannot lie in L because then the first equation would show that the $r_1, \ldots, r_{n+1}$ would be dependent over L (recall that g_1 is the identity).

Among all the nontrivial solutions pick one with the minimal number of elements different from zero. Call it $s_1, s_2, \ldots, s_\ell, 0, 0, \ldots, 0$ where we assume the first ℓ terms are not zero. We also may assume $s_\ell = 1$. We get

$$\begin{array}{ccccccccccc} g_1(r_1)s_1 & + & g_1(r_2)s_2 & + & \cdots & + & g_1(r_{\ell-1})s_{\ell-1} & + & g_1(r_\ell) & = & 0 \\ g_2(r_1)s_1 & + & g_2(r_2)s_2 & + & \cdots & + & g_2(r_{\ell-1})s_{\ell-1} & + & g_2(r_\ell) & = & 0 \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots & & \vdots \\ g_n(r_1)s_1 & + & g_n(r_2)s_2 & + & \cdots & + & g_n(r_{\ell-1})s_{\ell-1} & + & g_n(r_\ell) & = & 0. \end{array} \tag{12}$$

Since all of the $s_1, \ldots, s_{\ell-1}$ cannot lie in L, at least one of these, say s_1, is in M but not in L. Pick some g_k with $g_k(s_1) \neq s_1$. Since G is a group, $g_k \cdot g_1, g_k \cdot g_2, \ldots, g_k \cdot g_n$ is merely a permutation of $g_1, g_2, \ldots, g_n$. Hence if we apply g_k to the system (12), we get

$$\begin{array}{ccccccccc} g_1(r_1)g_k(s_1) & + & \cdots & + & g_1(r_{\ell-1})g_k(s_{\ell-1}) & + & g_1(r_\ell) & = & 0 \\ g_2(r_1)g_k(s_1) & + & \cdots & + & g_2(r_{\ell-1})g_k(s_{\ell-1}) & + & g_2(r_\ell) & = & 0 \\ \vdots & & \ddots & & \vdots & & \vdots & & \vdots \\ g_n(r_1)g_k(s_1) & + & \cdots & + & g_1(r_{\ell-1})g_k(s_{\ell-1}) & + & g_n(r_\ell) & = & 0 \quad . \end{array} \tag{13}$$

If we subtract (13) from (12), we get

$$\begin{array}{ccccccccc} g_1(r_1) \cdot [s_1 - g_k(s_1)] & + & \cdots & + & g_1(r_{\ell-1}) \cdot [s_{\ell-1} - g_k(s_{\ell-1})] & = & 0 \\ g_2(r_1) \cdot [s_1 - g_k(s_1)] & + & \cdots & + & g_2(r_{\ell-1}) \cdot [s_{\ell-1} - g_k(s_{\ell-1})] & = & 0 \\ \vdots & & \ddots & & \vdots & & \vdots \\ g_n(r_1) \cdot [s_1 - g_k(s_1)] & + & \cdots & + & g_1(r_{\ell-1}) \cdot [s_{\ell-1} - g_k(s_{\ell-1})] & = & 0 \quad . \end{array} \tag{14}$$

This shows that $[s_1 - g_k(s_1)], [s_2 - g_k(s_2)], \ldots, [s_{\ell-1} - g_k(s_{\ell-1})]$ is a nontrivial solution to (14) which has at most $\ell - 1$ elements different from zero which contradicts the choice of ℓ. ■

5 The Norm Map

The results of this section are also standard and can be found in [17], for example.

Let M be a finite algebraic extension of a field L. Put $n = [M : L]$, the dimension of M as a vector space over L, and let $r_1, \ldots, r_n$ be a basis for M over L. For $r \in M$, let A_r be the matrix of the linear map on M given by multiplication by r with respect to the basis $r_1, \ldots, r_n$. Then the Cayley–Hamilton Theorem implies that $\det(r \cdot I - A_r) = 0$. Let $f_r(X)$ be the polynomial $\det(X \cdot I - A_r)$. We call f_r the *characteristic* polynomial of r with respect to the extension M of L. It is easy to see that f_r is independent of the choice of the basis $r_1, \ldots, r_n$. As remarked above, r satisfies f_r, however, f_r may not be

irreducible. The minimal polynomial m_r is irreducible, and by Lemma 3.2 we see that $m_r | f_r$. Now f_r is clearly monic, *i.e.*, it can be written as

$$f_r(X) = X^n + c_1 X^{n-1} + \cdots + c_{n-1} X + c_n$$

with $c_i \in L$. In fact,

$$\begin{aligned} c_1 &= -\mathrm{tr}\, A_r \text{ and} \\ c_n &= (-1)^n \det A_r \quad . \end{aligned}$$

Definition 5.12. The *norm* of r is $\mathrm{N}(r) = (-1)^n c_n = \det A_r$, and the *trace* of r is $\mathrm{Tr}(r) = -c_1 = \mathrm{tr} A_r$.

Exercise 5.4. For $r, s \in M$ and $c \in K$, show the following:

i) $\mathrm{N}(rs) = \mathrm{N}(r)\mathrm{N}(s)$.

ii) If $r \in L$, then $\mathrm{N}(r) = r^n$.

iii) $\mathrm{Tr}(r+s) = \mathrm{Tr}(r) + \mathrm{Tr}(s)$.

iv) $\mathrm{Tr}(c \cdot r) = c \cdot \mathrm{Tr}(r)$.

v) If $r \in L$, then $\mathrm{Tr}(r) = n \cdot r$.

When it is necessary to indicate the fields involved, we write

$$\mathrm{N} = \mathrm{N}_{M/L}$$

and

$$\mathrm{Tr} = \mathrm{Tr}_{M/L} \quad .$$

Now suppose Δ is a finite extension of M and let $r \in M$. We can consider r as a member of Δ and thus can consider $\mathrm{N}_{\Delta/L}(r)$ and $\mathrm{N}_{M/L}(r)$ and similarly for the two traces.

Proposition 5.8. For $r \in M$, we have

$$\mathrm{N}_{\Delta/L}(r) = \left[\mathrm{N}_{M/L}(r)\right]^m$$

and

$$\mathrm{Tr}_{\Delta/L}(r) = m \left[\mathrm{N}_{M/L}(r)\right]$$

where m is the degree of Δ over M.

Proof. Let $r_1, \ldots, r_n$ be a basis for M over L and $s_1, \ldots, s_m$ be a basis for Δ over M.

Exercise 5.5. Show that $\{r_i \cdot s_j : 1 \le i \le n \text{ and } 1 \le j \le m\}$ is a basis for Δ over L.

Order the elements of this basis by saying that $r_i \cdot s_j$ precedes $r_{i'} \cdot s_{j'}$ if $j < j'$ or if $j = j'$ if $i < i'$. Recall that A_r is the matrix of multiplication by r on M with respect to the basis $\{r_i\}$. Let C be the $mn \times mn$ matrix of multiplication by r on Δ with respect to the basis $\{r_i \cdot s_j\}$.

Exercise 5.6. Show that C is zero except for m blocks along the diagonal each containing the matrix A_r.

The lemma now follows easily. ∎

The matrix C in the above proof is the *m–fold tensor power* of A_r and we write $C = {A_r}^{(m)}$.

Corollary 5.2. Let F_r (respectively f_r) be the characteristic polynomial of r with respect to the extension Δ (respectively M) of L. Then $F_r = {f_r}^m$.

Proof. The proof follows trivially from the following equation:

$$F(X) = \det(X \cdot I - C) = \det(X \cdot I - A_r)^{(m)} \quad . \tag{15}$$

∎

This corollary allows us to prove the following interesting theorem which relates the minimal polynomial to the characteristic polynomial.

Theorem 5.4. f_r is a power of m_r; $f_r = m_r$ if and only if $M = L(r)$.

Proof. Let $\deg m_r = s$ and let f_1 be the characteristic polynomial of r considered as an element of $L(r)$. Now $[L(r) : L] = s$, so $\deg f_1 = s$ also. By Lemma 3.2, $m_r | f_1$, so $m_r = f_1$ which proves $f_r = m_r$ if $M = L(r)$. Now Corollary 5.2 above proves f_r is a power of m_r. Corollary 5.2 even shows that $f_r = [m_r]^m$ where $m = [M : L(r)]$, so if $f_r = m_r$ then $m = 1$ and $M = L(r)$. ∎

Proposition 5.9. Let $L \subset M \subset \Delta$ be a tower of extensions as above. Let $r \in \Delta$. Then

$$\mathrm{N}_{M(r)/L}(r) = \left[\mathrm{N}_{M/L} \circ \mathrm{N}_{M(r)/M}\right](r) \quad .$$

Proof. By the above theorem, the minimal polynomial of r with respect to the extension $M(r)$ over M is the same as the characteristic polynomial. Suppose $\deg m_r = s$. Then it is clear that $\{1, r, r^2, \ldots, r^{s-1}\}$ is a basis for $M(r)$ over M. In fact, if we write

$$m_r(X) = X^s + c_1 X^{s-1} + \cdots + c_{s-1} X + c_s \quad ,$$

then

$$A_r = \begin{pmatrix} 0 & 1 & 0 & \cdot & \cdot & \cdot \\ 0 & 0 & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ -c_s & -c_{s-1} & \cdot & \cdot & -c_2 & -c_1 \end{pmatrix} \quad .$$

Now as in the proof of Proposition 3.6 we can get the matrix C of multiplication by r with respect to the extension $M(a)$ over L as follows: Suppose $[M : L] = n$. Let B_c be the matrix corresponding to multiplication by any element $c \in M$ for the extension M over L. So B_c is an $n \times n$ matrix, A_r is an

$s \times s$ matrix, and C is an $ns \times ns$ matrix. To get C, replace each 0 (respectively 1) in A_r by the $n \times n$ zero (respectively identity) matrix, and replace c_i by the matrix B_{c_i}.

Expanding the determinant of A_r, we get

$$\mathrm{N}_{M(r)/L}(r) = \det B_{(-1)^s c_s} \quad .$$

Since

$$c_s = (-1)^n \mathrm{N}_{M(r)/M}(r) \quad ,$$

the proposition follows. ∎

Corollary 5.3. Let M be a finite algebraic extension of L and Δ a finite algebraic extension of M. Then

$$\mathrm{N}_{\Delta/L} = \mathrm{N}_{M/L} \circ \mathrm{N}_{\Delta/M} \quad .$$

The other roots of the minimal polynomial, m_r, of r are called the *conjugates* of r. They may or may not be in M. If M contains the conjugates of each of its elements, we say M is a *normal* extension of L.

Elements that are conjugates are closely related as the next theorem will show. First we need a lemma.

Lemma 5.3. Let $\sigma : L \to L'$ be an isomorphism between two fields. Let $f(X) \in L[X]$ be irreducible, and set $g = \sigma(f)$, *i.e.*, apply σ to the coefficients of f. Let r (respectively s) be a root of f (respectively g) in some extension field. Then σ can be extended to an isomorphism from $L(r)$ to $L'(s)$.

Proof. Since r is algebraic over L, every element in $L(r)$ is of the form $h(r)$ for some $h(X) \in L[X]$. Furthermore if we take h to have degree $\leq n-1$ where $n = \deg f$, then h is unique (since $f = m_r$). Now we map $h(r) \in L(r)$ into $[\sigma(h)](s) \in L'(s)$, and it is not hard to see that this is an isomorphism. ∎

It should be clear from this lemma that if M is algebraic over L, and r and r' are conjugate over L, then there is an isomorphism : $L(r) \to L(r')$ taking r into r' and fixing L. We can, however, do better if M is normal over L. If M is normal over L, we can extend this isomorphism to all of M.

Theorem 5.5. If M is a finite normal extension of L and $r, r' \in M$ are conjugate over L, then there is a automorphism of M taking r into r' which leaves L fixed.

Proof. Let $r_1, r_2, \ldots, r_m \in M$ generate M over L. Let

$$F(X) = \prod_{i=1}^{m} m_{r_i}(X) \in L[X] \quad .$$

F is monic, and its roots generate M. Since M is normal over L, $F(X)$ factors completely in $M[X]$. Let $\deg F = n$. We are going to prove the following somewhat more general result: Suppose we are given an isomorphism $\sigma : L_1 \to L_2$ between two fields. Further suppose we have monic polynomials $F_1(X)$ and $F_2(X)$ in $L_1[X]$ and $L_2[X]$ respectively with $\sigma(F_1) = F_2$. Further suppose for $i = 1, 2$ there are fields M_i which are generated by the roots of F_i and in which

F_i factors completely *i.e.*, into linear factors. Then τ can be extended to an isomorphism from M_1 to M_2.

First we show our result follows from the more general result. Let $\sigma : L(r) \to L(r')$ be the isomorphism given by the lemma using m_r and $m_{r'}$ as the irreducible polynomials. Hence $\sigma(r) = r'$ and σ leaves L fixed. Since $F(X) \in L[X]$, $\sigma(F) = F$. Now we are in the situation of our more general result with $L_1 = L(r)$, $L_2 = L(r')$, and $F_1 = F_2 = F$.

The proof of the more general result is by induction on n. The case $n = 1$ is trivial. For the inductive step, let G_1 be a factor of F_1 which is irreducible over L_1. Then $G_2 = \sigma(G_1)$ will be a factor of F_2 irreducible over L_2. Pick a root $s_1 \in M$ of G_1 and a root $s_2 \in M$ of G_2. Now apply the lemma again using G_1, G_2, s_1, and s_2 to get an extension of σ to $\tau : L_1(s_1) \to L_2(s_2)$ with $\tau(s_1) = s_2$. We can write $F_1(X) = (X - s_1)F_3(X)$ and $F_2(X) = (X - s_2)F_4(X)$. Now $F_3(X) \in L_1(s_1)[X]$ and $F_4[X] \in L_2(s_2)[X]$, and since $\tau(s_1) = s_2$, $\tau(F_3) = F_4$. Also F_3 and F_4 are monic and of degree $n-1$. Now F_3 factors completely in M_1, and M_1 is generated by the roots of F_3 over $L_1(s_1)$, and F_4 factors completely in M_2 and M_2 is generated by the roots of F_4 over $L_2(s_2)$. Hence by induction, we get an extension of τ to an isomorphism $\rho : M_1 \to M_2$. Since τ is an extension of σ, we have proved the more general result.

Since in our case, $\sigma(r) = r'$ and σ leaves L fixed, we are done. ∎

There is at least one case where we know that the extension is normal, namely the situation of Theorem 4.3. In fact, in this case the extension is also separable. An extension which is both normal and separable is said to be *Galois*.

Theorem 5.6. *M is a Galois extension of L if and only if L is the fixed field of a group of automorphisms of M.*

Proof. Assume L is the fixed field of a group G of automorphisms of M. Let $g_1, g_2, \ldots, g_n$ be the elements of the group G. Let r be an arbitrary element of M. We will show that the minimal polynomial of r has distinct roots all of which are in M. Let $r, r_2, r_3, \ldots, r_m$ be the set of distinct elements in the sequence $g_1(r), g_2(r), \ldots, g_n(r)$. Since G is a group of automorphisms, the elements $r, r_2, r_3, \ldots, r_m$ are permuted by the elements of G. Consider the polynomial

$$f(X) = (X - r)(X - r_2)\cdots(X - r_m) \quad .$$

Since an automorphism in G merely permutes the factors of f, the coefficients of f are left fixed by all of the automorphisms in G. Hence $f(X) \in L(X)$. Clearly $f(r) = 0$ so if we can show that f has minimum degree among those polynomials in $L[X]$ with r as a root then f will be the minimal polynomial of r, and we will be half done. Suppose g is any polynomial in $L[X]$ with r as a root. Applying an automorphism in G to the equation $g(r) = 0$, we get $g(r_i) = 0$ for some i, in fact, for each i. Thus the degree of g must be at least m, the degree of f, and we are half done.

Now assume M is Galois over L and let $g_1, g_2, \ldots, g_n$ be the automorphisms of M which fix L. It is easy to see that the g_i form a group. If $r \in M$ is left fixed by all of the g_i, then by Theorem 5.5, r can have no conjugates in M and hence since M is separable over L, r must be in L. Therefore L is the fixed field of the g_i. ∎

In this situation, the group of automorphisms of M that fix L is called the *Galois* group of M (or M over L).

Let us assume $M = L(r)$ and that M is normal. Then we can write

$$m_r(X) = \prod_{i=1}^{m}(X - r_i)$$

where $r_1 = r$ and the other r_i's are the conjugates of r and are in M.

Theorem 3.3 tells us that $m_r = f_r$ in this case. Therefore we get

$$\mathrm{N}(r) = \prod_{i=1}^{n} r_i \tag{16}$$

and

$$\mathrm{Tr}(r) = \sum_{i=1}^{n} r_i \quad .$$

If r is separable over L, then the $r_1, \ldots, r_n$ are distinct by Corollary 3.1. If r is inseparable over L, and if n_0 is the degree of separability of m_r, and p^s is its degree of inseparability, then by Proposition 3.7,

$$f_r(X) = \prod_{i=1}^{n_0}(x - r_i)^{p^s} \quad ,$$

so r has n_0 distinct conjugates. Hence the above two equations yield

$$\mathrm{N}(r) = \left(\prod_{i=1}^{n_0} r_i\right)^{p^s} \tag{17}$$

and

$$\mathrm{Tr}(r) = p^s \cdot \left(\sum_{i=1}^{n_0} r_1\right) = 0 \quad .$$

We restate the last equation in a proposition.

Proposition 5.10. If M is a finite extension of L and $r \in M$ is inseparable over L, then $\mathrm{Tr}_{M/L}(r) = 0$.

6 The Norm Map (Continued)

Now suppose we are given an isogeny $\alpha : E \to E'$ between elliptic curves E and E', and we put $K' = \alpha^*(K(E')) \subset K(E)$. We would like to compute the norm $\mathrm{N} = \mathrm{N}_{K(E)/K'}$. We will show that

$$[\mathrm{N}(r)](P) = \prod_{\alpha(Q)=\alpha(P)} r(Q)^{e_\alpha} \tag{18}$$

where $P \in E$, $r \in K(E)$ and e_α is the ramification index of α.

Now this is very close to Equation (17) which says that $\mathrm{N}(r)$ is the product of the conjugates of r over K'. We have to identify the conjugates of the rational function r with the translates of r by points in E that get sent into $\mathcal{O}'$ by α. We also must show that the ramification index of α is p^s, the degree of inseparability of m_r, the minimal polynomial of r over K'. (It is not hard to see that this degree is independent of r so we can call it the degree of inseparability of the extension $K(E)$ of K'.) Incidentally, this will also clear up a loose end from Section 3 where we wanted to know how the separability of α was reflected in the extension of K'. Obviously the answer must be that the extension is separable, but we have not proved it as yet.

Let $\mathcal{S} = \ker \alpha \subset E$, and consider the group of translations

$$T_{\mathcal{S}} = \{T_P : P \in \mathcal{S}\} \quad .$$

Then $T_{\mathcal{S}}$ is a finite group of automorphisms of E. $T_{\mathcal{S}}$ also acts on $K(E)$ by

$$T_P(r) = T_P{}^*(r) = r \circ T_P \quad .$$

Now suppose $r \in K'$, so $r = r' \circ \alpha$ for some $r' \in K[E']$. Then

$$[T_P(r)]\,(Q) = r'(\alpha(Q+P)) = r'(\alpha(Q)) = r(Q) \quad ,$$

so $T_{\mathcal{S}}$ leaves K' fixed. Set

$$L = \{r \in K(E) : T_P(r) = r,\ \forall P \in \mathcal{S}\} \quad .$$

Then Theorem 4.3 tells us that $K(E)$ is a finite algebraic extension of L of degree $m = |\mathcal{S}|$, and Theorem 5.6 tells us that this extension is Galois.

The idea of our proof of (18) is that N is the composition of the norm from $K(E)$ down to L with the norm from L down to K'. We will show that there is an elliptic curve C with $K(C) = L$ such that the map α factors through C. The point is that since $K(E)$ is Galois over L, the factor from E to C should be "nice", while the factor from C to E' should be very "special".

We have

$$\begin{array}{c} K(E) \\ | \\ L \\ | \\ K' \end{array} \quad .$$

Let

$$\begin{aligned} \tilde{x} &= \left[\mathrm{Tr}_{K(E)/L}\right](x) \\ \tilde{y} &= \left[\mathrm{Tr}_{K(E)/L}\right](y) \quad , \end{aligned}$$

so

$$\tilde{x} = \sum_{P \in \mathcal{S}} T_P(x)$$
$$\tilde{y} = \sum_{P \in \mathcal{S}} T_P(y) \quad .$$

Note that $\tilde{x}$ (respectively $\tilde{y}$) has a pole of multiplicity 2 (respectively 3) at each point of $\mathcal{S}$ and no other poles.

Proposition 6.11. $\tilde{x}$ and $\tilde{y}$ generate L.

Proof. Clearly $\tilde{x}$ and $\tilde{y}$ are in L. Let $r \in L$, and suppose r is even, *i.e.*, $r(-P) = r(P)$. If we multiply r by a suitable power of

$$\prod_{\substack{P \notin \mathcal{S} \\ r(P)=\infty}} (\tilde{x} - \tilde{x}(P)) \quad ,$$

we will get an even rational function r_1 which is in L and whose poles are only on $\mathcal{S}$.

Now r_1 even implies that $\mathrm{ord}_{\mathcal{O}}(r_1)$ is even. Say $\mathrm{ord}_{\mathcal{O}}(r_1) = 2a$. If we subtract a suitable scalar multiple of $\tilde{x}^a$ from r_1, we will get an even function in L whose only poles are on $\mathcal{S}$ and whose multiplicity at $\mathcal{O}$ is at most $2a-2$. If we continue in this fashion, we get

$$r_1 = p(\tilde{x}) + g$$

where p is a polynomial, and g is in L with no poles off $\mathcal{S}$ and with $g(\mathcal{O}) = 0$. But $g \in L$ implies $g(P) = g(\mathcal{O})$ for any $P \in \mathcal{S}$. Thus g has no poles at all, so g is zero, and r_1 and r are in $K(\tilde{x})$.

Now suppose $r \in L$ is odd. Then $\tilde{y}r$ is even, so $\tilde{y}r \in K(\tilde{x})$ and $r \in K(\tilde{x}, \tilde{y})$. Since every rational function is the sum of an even function and an odd function, we are done. ∎

Theorem 6.7. There is an elliptic curve C such that

i) $K(C)$ is isomorphic to L, and

ii) there are homomorphisms $\beta : E \to C$ and $\gamma : C \to E'$ such that

1) $\alpha = \gamma \circ \beta$,
2) $\ker \beta = \ker \alpha$,
3) $e_\beta = 1$,
4) $\ker \gamma = \{\tilde{\mathcal{O}}\}$ where $\tilde{\mathcal{O}}$ is the identity element of C, and
5) $e_\gamma = e_\alpha$.

Proof. $\tilde{y}^2$ is even so $\tilde{y}^2 \in K(\tilde{x})$. Furthermore it is easy to see that $\mathrm{ord}_{\mathcal{O}}\tilde{y}^2 = 6$. Therefore

$$\tilde{y}^2 = f(\tilde{x}) \tag{19}$$

for some cubic polynomial f. If we can show that the polynomial f has three distinct roots, then we can let C be the elliptic curve defined by (19). Then part i) will follow from Proposition 6.11 above.

Suppose $f(k) = 0$ for some $k \in K$. Let $N = |\{P \in E : \tilde{x}(P) = k\}|$. By (19), $\tilde{x}(P) = k$ implies $\tilde{y}(P) = 0$.

Hence if $\tilde{x}$ takes the value k at both P and Q in E, then both $\tilde{x}$ and $\tilde{y}$ take the same values at P and Q. Therefore by Proposition 6.11 α must take the same value at each of the points with $\tilde{x}(P) = k$, *i.e.*, α maps N points of E to the same point of E'. Thus we must have

$$N \leq |\ker \alpha| \quad .$$

On the other hand, $\tilde{x}$ is invariant under $T_{\mathcal{S}}$ so

$$\tilde{x}(P+Q) = \tilde{x}(P) \ \forall Q \in \mathcal{S} \quad .$$

Hence $\tilde{x}$ takes the value k at least $|\mathcal{S}|$ times, *i.e.*, $N \geq |\ker \alpha|$ so

$$N = |\ker \alpha| \quad . \tag{20}$$

Consider the set

$$\mathcal{R} = \{P \in E : \tilde{y}(P) = 0\} \quad .$$

If $\tilde{y}$ is zero at P, then $\tilde{x}(P) = k$ for some root k of f. If we let M be the number of these roots, then (20) tells us that $|\mathcal{R}| = M \cdot |\ker \alpha|$, *i.e.*, $\tilde{y}$ is zero at precisely $M \cdot |\ker \alpha|$ points of E.

Since α is surjective, we can find a point $P \in E$ such that $2 \cdot \alpha(P) = \mathcal{O}'$, but $\alpha(P) \neq \mathcal{O}'$. Consider the set

$$P + \mathcal{S} = \{P + Q : Q \in \mathcal{S}\} \quad .$$

Let $P + Q \in P + \mathcal{S}$. Then $-(P+Q) = P + R$ where $R = -2 \cdot P - Q$, and

$$\alpha(R) = -2 \cdot \alpha(P) - \alpha(Q) = \mathcal{O}'$$

so $R \in \mathcal{S}$, *i.e.*, $-(P+Q) \in P + \mathcal{S}$. Now

$$\tilde{y}(P) = \sum_{Q \in \mathcal{S}} y(P+Q), \text{ and}$$
$$y(-(P+Q)) = -y(P+Q)$$

so $\tilde{y}(P) = 0$ for any $P \in E$ with $\alpha(P) \in E'[2] - \{\mathcal{O}'\}$.

We know there are three nontrivial points in $E'[2]$. Since α is surjective, α maps $|\ker \alpha|$ points into each one. So by the above, $\tilde{y}$ is zero at at least $3 \cdot |\ker \alpha|$ points. Hence f has at least 3 roots, and since f is cubic, it must have distinct roots, and i) follows.

It should be clear by now that $\tilde{x}(P) = \tilde{x}(Q)$ and $\tilde{y}(P) = \tilde{y}(Q)$ implies that $P - Q \in \mathcal{S}$ so C can be considered as the quotient group $E/\mathcal{S}$. We take $\beta : E \to C$ to be the canonical projection, *i.e.*,

$$\beta(P) = (\tilde{x}(P), \tilde{y}(P)) \quad .$$

Then since $\tilde{x} = x' \circ \alpha, \tilde{y} = y' \circ \alpha \in L = K(C)$, we can define γ by

$$\gamma(\tilde{P}) = (\tilde{x}(P), \tilde{y}(P))$$

for any $P \in E$ with $\beta(P) = \tilde{P}$. Since $\alpha(P) = (\tilde{x}(P), \tilde{y}(P))$, we see that $\alpha = \gamma \circ \beta$ and 1) follows. Also since $C = E/\mathcal{S}$, 2) and 4) are clear.

We have considered $\tilde{x}$, and $\tilde{y}$ as functions on E. Of course, they can also be considered as functions on C. In fact, they are the coordinate functions on C. With this "abuse of terminology" we see that $\tilde{x} \circ \beta = \tilde{x}$ where the first $\tilde{x}$ is a function on C, and the second is a function on E. In any case this equation shows that $e_\beta = 1$ and 3) follows. Since $e_\alpha = e_\beta \cdot e_\gamma$, we get 5). ∎

We have now split up the map α into a map β that has a kernel but no ramification and a map γ that has ramification but no kernel. One of the results we want from all this is that if α is separable (*i.e.*, $e_\alpha = 1$), then $K(E)$ is a separable extension of K'.

Proposition 6.12. Let $\alpha : E \to E'$ be an injective homomorphism. Then α is an isomorphism if and only if $e_\alpha = 1$ or $K(E)$ is separable over K'.

Proof. Let $\bar{x} = \alpha^*(x')$, and $\bar{y} = \alpha^*(y')$ where x' and y' are the coordinates on E'. Recall $K' = \alpha^*(K(E')) \subset K(E) = K(x, y)$. Since $\bar{x}$ is an even function on E, $\bar{x} \in K(x)$.

Claim. If we consider $\bar{x}$ as a function of x, it takes each value of K exactly once. Suppose $k, l \in K$ and $\bar{x}(k) = \bar{x}(l)$. Let $P, Q \in E$ with $x(P) = k$ and $x(Q) = l$. Then

$$\alpha(P) = (\bar{x}(P), \bar{y}(P)) = (\bar{x}(Q), \pm\bar{y}(Q)) = \pm\alpha(Q) \quad .$$

By replacing Q with $-Q$ we can assume that $\alpha(P) = \alpha(Q)$. Since α is injective by hypothesis and surjective by Proposition 1.1, the claim follows.

Since $\alpha(P) = \mathcal{O}'$ implies $P = \mathcal{O}$, we see that $\bar{x}$ has no finite poles. Hence $\bar{x}$ is a polynomial.

Exercise 6.7. Let p be the characteristic of K. Show that

$$\bar{x} = (ax + b)^{p^r} \tag{21}$$

for some $a, b \in K$ and $r \geq 0$.

Now x' has a pole of multiplicity 2 at $\mathcal{O}' \in E'$ so $\bar{x}$ has a pole of multiplicity $2e_\alpha$ at $\mathcal{O}$. The above equation shows that we must have $e_\alpha = p^r$.

If $K(E)$ is separable over K', then $ax + b \in K(E)$ must have a minimal polynomial with nonzero derivative. Now $\bar{x} \in K'$. Thus $X^{p^r} - \bar{x} \in K'[X]$ and (21) says that $ax + b$ is a root of it. Since $\bar{x} = \alpha^*(x')$, if $\bar{x}$ had a p^{th} root in K', x' would have a p^{th} root in $K(E')$ which is absurd. Thus by Lemma 3.2, $X^{p^e} - \bar{x}$ is irreducible. The only way this can happen is for r to be zero. Hence $K(E)$ separable implies $e_\alpha = 1$, and it suffices to show that if $e_\alpha = 1$ then α is an isomorphism.

If $e_\alpha = 1$, then $\bar{x} = ax + b$ so $x \in K'$. Now $\bar{y}$ is an odd function, and since $\alpha^{-1}(\mathcal{O}') = \{\mathcal{O}\}$, $\bar{y}$ also has no finite poles. Hence $\bar{y} = yh$ with $h \in K[x]$. Since $e_\alpha = 1$, $\text{ord}_\mathcal{O}(\bar{x}) = -2$. Since $\bar{y}^2 = \bar{x}^3 + A'\bar{x} + B'$, $\text{ord}_\mathcal{O}(\bar{y}) = -3$ and $\text{ord}_\mathcal{O}(h) = 0$. This implies that h is a nonzero constant.

Therefore $e_\alpha = 1$ yields

$$\bar{x} = ax + b \text{ and } \bar{y} = cy$$

for some $a, b, c \in K$ and since $\alpha(P) = (\bar{x}(P), \bar{y}(P))$, α is manifestly an isomorphism. ∎

Corollary 6.4. Let $\alpha : E \to E'$ be a homomorphism. Then α is separable (*i.e.*, $e_\alpha = 1$) if and only if $K(E)$ is a separable extension of K'.

Proof. Write $\alpha = \gamma \circ \beta$ as in Theorem 6.7. Then if α is separable, so is γ. Also if $K(E)$ is separable over K', so is $K(C)$. In either case the proposition tells us that γ is an isomorphism, and we can assume $\alpha = \beta$. Since Theorem 5.6 says that $K(E)$ is Galois over $K(C)$, and Theorem 6.7 says that $e_\beta = 1$, we are done. ∎

Corollary 6.5. Let $\alpha : E \to E'$ be a homomorphism. If α has trivial kernel, then after a suitable change of coordinates, we get $\alpha(x, y) = (x^{p^r}, y^{p^r})$, and $e_\alpha = p^r$ for some $r > 0$.

Proof. This is really a corollary of the proof of the proposition. Equation (21) tells us that after composing with an isomorphism, $\bar{x} = x' \circ \alpha = x^{p^r}$. Since $\bar{y}$ is an odd function, we can write $\bar{y} = yh$ where h is a function of x alone. It is easily seen that h has no finite poles and thus is a polynomial . Since $\bar{y}^2 = \bar{x}^3 + A'\bar{x} + B'$, we get

$$\begin{aligned} y^2h^2 &= x^{3p^r} + A'x^{p^r} + B' \\ &= s(x)^{p^r} + (A' - A^{p^r})x^{p^r} + (B' - B^{p^r}) \end{aligned}$$

where $s(x) = x^3 + Ax + B$. Now $y^2 = s(x)$ so s divides $C^{p^r}x^{p^r} + D^{p^r} = (Cx + D)^{p^r}$ where we have put $A' - A^{p^r} = C^{p^r}$ and $B' - B^{p^r} = D^{p^r}$. Hence s must divide $Cx + D$ for $C, D \in K$ which is absurd. Therefore we must have $C = D = 0$, and it follows that $\bar{y} = y^{p^r}$. The part about the ramification index follows from the definition. ∎

To summarize what we have proved in this section so far, we see that a homomorphism between elliptic curves can be factored into a separable part and a factor that looks like (x^{p^r}, y^{p^r}) (such maps are called *purely inseparable*). We will use this result to prove the formula for the norm by breaking it up into two easier cases.

Theorem 6.8. Let $\alpha : E \to E'$ be a homomorphism, and $K' = \alpha^*(K(E'))$ $\subset K(E)$. Let $\mathrm{N} = \mathrm{N}_{K(E)/K'}$, and $r \in K(E)$. Then

$$[\mathrm{N}(r)](P) = \prod_{\alpha(Q)=\alpha(P)} r(Q)^{e_\alpha}$$

for $P \in E$.

Proof. This theorem is now a consequence of the previous results. Theorem 6.7 says that $\alpha = \gamma \circ \beta$ where β is separable and γ is purely inseparable. Corollary 5.3 tells us that the corresponding norm is also a composition. In the separable case Theorem 5.6 together with the proof of Theorem 6.7 says that the Galois

group of $K(E)$ over $\beta^*(K(C))$ is $T_S(\approx \ker\beta)$ so the conjugates (over $\beta^*(K(C))$) of a rational function r are the functions $T_P(r)$ for $P \in \ker\beta$. In the purely inseparable case by Corollary 6.5, $\gamma = (x^{p^r}, y^{p^r})$ for some $r > 0$, and $e_\alpha = p^r$. Our result now follows. ∎

There are a number of important consequences of this theorem.

Definition 6.13. Let $\alpha : E \to E'$ be an isogeny. Define

$$\alpha_* : \mathrm{Div}(E) \to \mathrm{Div}(E')$$

by setting

$$\alpha_*(\langle P\rangle) = \langle \alpha_*(P)\rangle$$

and extending linearly.

We also define $\alpha_* : K(E) \to K(E')$ by

$$\alpha_*(r) = N(r) \circ \alpha^{-1}$$

where $r \in K(E)$, and

$$N = N_{K(E)/\alpha^*(K(E'))} \quad ,$$

i.e., $N(r) = r' \circ \alpha$ for some $r' \in K(E')$, and $\alpha_*(r) = r'$.

Theorem 6.9 "Lower Star". Let $\alpha : E \to E'$ be an isogeny. For $r \in K(E)$,

$$\alpha_*(\mathrm{div} r) = \mathrm{div}(\alpha_*(r)) \quad .$$

Proof. It follows immediately from Theorem 6.8 that

$$[\alpha_*(r)]\,(P') = \prod_{\alpha(Q)=P'} r(Q)^{e_\alpha}$$

for $P' \in E'$. While the theorem follows by simply unraveling this equation, it is perhaps easier to understand if we do our usual trick of breaking it up into the separable and purely inseparable cases.

In the separable case ($e_\alpha = 1$), we get

$$\begin{aligned}\mathrm{div}(\alpha_*(r)) &= \sum_{P'\in E'} \sum_{\alpha(Q)=P'} \mathrm{ord}_Q(r)\langle P'\rangle \\ &= \sum_{Q\in E} \mathrm{ord}_Q(r)\langle \alpha_*(Q)\rangle \\ &= \alpha_*(\mathrm{div}(r)) \quad .\end{aligned}$$

Now in the purely inseparable case ($\ker\alpha = \mathcal{O}$), we can assume $\alpha(x,y) = (x^{e_a}, y^{e_a})$, so

$$[\alpha_*(r)]\,(P') = r(P)^{e_a}$$

where $P \in E$ is the unique point with $\alpha(P) = P'$. Hence

$$[\alpha_*(r) \circ \alpha]\,(P) = r(P)^{e_\alpha}$$

so

$$\mathrm{ord}_P\,(\alpha_*(r)\circ\alpha) = e_\alpha \cdot \mathrm{ord}_P(r) \quad .$$

On the other hand, by Proposition 1.2

$$\mathrm{ord}_P\,(\alpha_*(r)\circ\alpha) = [\mathrm{ord}_{P'}\alpha_*(r)]\,e_\alpha \quad ,$$

and we see that

$$\mathrm{ord}_{P'}(\alpha_*(r)) = \mathrm{ord}_P(r) \quad .$$

Finally

$$\begin{aligned}\mathrm{div}(\alpha_*(r)) &= \sum_{P'\in E'} \mathrm{ord}_{P'}(\alpha_*(r))\langle P'\rangle \\ &= \sum_{P\in E} \mathrm{ord}_P(r)\langle\alpha_*(P)\rangle \\ &= \alpha_*(\mathrm{div}(r)) \quad .\end{aligned}$$

■

Exercise 6.8. i) Show $\alpha_*\circ\alpha^*$ acts as multiplication by $\deg\alpha$ on $\mathrm{Div}(E')$.

ii) If $\beta : E' \to E''$ is another rational mapping, then $(\beta\circ\alpha)_* = \beta_*\circ\alpha_*$.

7 Weil Reciprocity

Let $D = \Sigma n_P\langle P\rangle$ be a divisor on E. We define the *support* of D to be the set of points $P \in E$ such that $n_p \neq 0$.

Definition 7.14. Let r be a rational function on E and D a divisor on D, and suppose div$r$ and $D = \Sigma n_P\langle P\rangle$ have disjoint supports. Then we can define

$$r(D) = \prod_{P\in E} f(P)^{n_P} \quad .$$

Exercise 7.9. Let $\alpha : E \to E'$ be a rational map. Prove the following two equations in the sense that if one side is well–defined, then so is the other and they are equal:

i) $r(\alpha^*(D')) = [\alpha_*(r)](D')$ for $r \in K(E)$ and $D' \in \mathrm{Div}(E')$.

ii) $r'(\alpha_*(D)) = [\alpha^*(r')](D)$ for $r' \in K(E')$ and $D \in \mathrm{Div}(E)$.

Now Weil reciprocity can be stated very simply. Suppose r and s are rational functions on E whose divisors have disjoint supports. Then

$$r(\mathrm{div}s) = s(\mathrm{div}r) \quad . \tag{22}$$

Unfortunately we have not been able to find a simple proof. r and s cannot both be polynomials since all polynomials have a pole at $\mathcal{O}$, but if they were monic polynomials, and if they were both functions of one variable, then (22) would

say that the product of the values of r on the zeros of s equals the product of the values of s on the zeros of r (up to sign). This is well–known to be true. It is merely the fact that the resultant of two polynomials is symmetric. Weil reciprocity can be thought of as the generalization of this to three rational functions of two variables, namely r, s, and the polynomial $y^2 - x^3 - Ax - B$ which defines the elliptic curve E.

The usual method of proof of this result is to first prove it on the projective line $\mathbb{P}_1$ where it is easy, and then to use the "Lower Star" theorem to pull the result back to the elliptic curve considering one of our rational functions as a rational mapping between E and $\mathbb{P}_1$. For us, this approach has the difficulty that $\mathbb{P}_1$ is not an elliptic curve so our proof of the "Lower Star" Theorem is not valid. The difficulty is that rational maps to $\mathbb{P}_1$ are not all homomorphisms. One might think that since $\mathbb{P}_1$ is such a simple object, the proof should be easier in this case, but we have not been able to find any proof except the very general one which works for maps between any two smooth curves.

We have decided to adopt a slightly different approach. There is a generalization of Weil reciprocity that essentially removes the requirement that div$f$ and div$g$ have disjoint supports. We will state this theorem and then do enough valuation theory to state the main result from the valuation theory we need. We will sketch the proof of the valuation theoretic result in an Appendix. A reference is [13, Chapter III, Section 1], especially page 45. We would like to thank Noam Elkies for pointing out this generalization.

We begin with a definition. We assume $f, g \neq 0$ in what follows.

Definition 7.15. Let E be an elliptic curve and $f, g \in K(E)$. For $P \in E$ we set

$$\langle f, g \rangle_P = (-1)^{mn} \left[\frac{f^n}{g^m} \right] (P)$$

where $m = \mathrm{ord}_P f$ and $n = \mathrm{ord}_P g$. We call $\langle f, g \rangle_P$ the *local symbol* of f and g. The local symbol is sometimes called the *tame symbol*.

The following exercises are all quite easy.

Exercise 7.10.

i) Let $h = \frac{f^n}{g^m}$. Show that $\mathrm{ord}_P h = 0$ so that the above definition makes sense.

ii) $\langle f, g \rangle_P = 1$ unless f or g has a pole or zero at P.

iii) If $1 - g$ has a zero at P and $\mathrm{ord}_P f \neq 0$, then $\langle f, g \rangle_P = 1$.

iv) Suppose $\mathrm{ord}_P f = 0$, then $\langle f, g \rangle_P = f(P)^n$.

v) $\langle f, hg \rangle_P = \langle f, g \rangle_P \cdot \langle f, h \rangle_P$, and $\langle fh, g \rangle_P = \langle f, g \rangle_P \cdot \langle h, g \rangle_P$ for any $h \neq 0$.

vi) $\langle f, g \rangle_P \cdot \langle g, f \rangle_P = 1$.

vii) $\langle -f, f \rangle_P = 1$.

viii) $\langle 1 - f, f \rangle_P = 1$.

Now we can state our main result which is sometimes called the "Product Formula".

Theorem 7.10 "Generalized Weil reciprocity": For $f, g \in K(E)$, we have

$$\prod_{P \in E} \langle f, g \rangle_P = 1 \quad .$$

Proof. We consider g as a map from E to $\mathbb{P}_1$. If g is a constant mapping, say $g(P) = t \in K$, then $\langle f, g \rangle_P = 1/t^m$ where $m = \mathrm{ord}_P f$ so

$$\prod_{P \in E} \langle f, g \rangle_P = t^{-\sum \mathrm{ord}_P f} = t^0 = 1 \quad .$$

Thus we can assume g is not a constant mapping. Note that $g^*(K(\mathbb{P}_1)) = K(g) \subset K(E)$. Thus if $t \in \mathbb{P}_1$, the local symbol $\langle \ \rangle_t$ defines a "local symbol", $\langle \ \rangle_\tau$ on pairs of functions in $K(g)$ by

$$\langle r \circ g, s \circ g \rangle_\tau = \langle r, s \rangle_t \quad ,$$

where $r, s \in K(\mathbb{P}_1)$. If $I : \mathbb{P}_1 \to \mathbb{P}_1$ is the identity map, then $g^*(I) = g$, a fact which will be useful. The theorem will follow from the following two lemmas:

Lemma 7.4. For all $t \in \mathbb{P}_1$, we have

$$\prod_{g(Q)=t} \langle f, g \rangle_Q = \langle N_{K(E)/K(g)} f, g \rangle_\tau \quad . \tag{23}$$

Lemma 7.5. For rational functions r on $\mathbb{P}_1$, we have

$$\prod_{t \in \mathbb{P}_1} \langle r, I \rangle_t = 1 \quad .$$

The theorem then follows by applying Lemma 7.5 to the function $r = g_*(f) = N_{K(E)/K(g)} f \circ g^{-1}$ and using Lemma 7.4. ∎

So we are left with the proofs of the two lemmas. The second one is not hard, and we give its proof here.

Proof. We can write a rational function on $\mathbb{P}_1$ as

$$r = a \prod_{t \in \mathbb{P}_1} (I - t)^{n_t}$$

where $n_t = \mathrm{ord}_t r$. Since the local symbol $\langle r, I \rangle_t$ is multiplicative in r, we are reduced to the case $r = (I - t)$. Suppose $t = 0$, *i.e.*, $r = I$. By ii) of the above exercise, $\langle I, I \rangle_s = 1$ for $s \neq 0, \infty$. It is easy to compute $\langle I, I \rangle_0 = -1$ and $\langle I, I \rangle_\infty = -1$, and this case follows.

Now suppose $t \neq 0$. Here we have $\langle I - t, I \rangle_s = 1$ for $s \neq 0, t, \infty$. Again it is easy to compute $\langle I - t, I \rangle_0 = -t$, $\langle I - t, I \rangle_t = 1/t$, and $\langle I - t, I \rangle_\infty = -1$, and we are done. ∎

The proof of Lemma 7.4 is much more difficult and requires some preparation even to point out where the difficulty lies. We give this preparation in the

next section. We can, however, show that Weil reciprocity is a consequence of Generalized Weil reciprocity.

Corollary 7.6. Let $r, s \in K(E)$ have divisors with disjoint supports, *i.e.*, they have zeros and poles at different points of E. Then

$$r(\mathrm{div}s) = s(\mathrm{div}r) \quad . \tag{24}$$

Proof. By the theorem,

$$\prod_{P \in E} \langle r, s \rangle_P = 1 \quad .$$

Now $\langle r, s \rangle_P = 1$ except where r or s has a pole or zero. If r has a pole or zero at P (and hence s does not), then

$$\langle r, s \rangle_P = s(P)^{-\mathrm{ord}_P r} \quad ,$$

while if s has a zero or pole at P

$$\langle r, s \rangle_P = r(P)^{\mathrm{ord}_P s} \quad .$$

Since

$$r(\mathrm{div}s) = \prod_{P \in E} r(P)^{\mathrm{ord}_P s} \quad ,$$

we see that the Generalized Reciprocity Formula says that

$$r(\mathrm{div}s) \cdot s(-\mathrm{div}r) = 1$$

which is the desired result. ∎

8 A Bit of Valuation Theory

If we examine Equation (23), we see that on the right we have a *global* object, while on the left side we have a product of *local* objects. We will first look at the norm $N_{K(E)/K(g)}$ and show how this can be written as a product of "local norms". To see where these "local norms" come from, we must examine the relationship between the order, ord_t, at $t \in \mathbb{P}_1$ and the orders, ord_Q at the points $Q \in E$ with $g(Q) = t$. Again it is advantageous to adopt a more abstract view if only to relate to the standard texts. By the way, references for this section are [11, Chapter 3] and [14, Chapters I and II].

The orders mentioned above are examples of discrete valuations.

Definition 8.16. Let K be any field. A *discrete valuation* on K is a mapping $v : K^* \to \mathbb{Z}$ such that

$$\begin{aligned} v(xy) &= v(x) + v(y) \\ v(x+y) &\geq \min(v(x), v(y)) \quad . \end{aligned}$$

We say v is *trivial* if $v(x) = 0$ for all $x \in K^*$.

The next example is very important for what follows.

Example 8.1. Let E be an elliptic curve over a field k. It is easy to see that ord_P is a valuation on the field $k(E)$ for any point $P \in E$. What is not so easy to see is that if k is algebraically closed, these are the only valuations on $k(E)$ that are trivial on k, the subfield of constant rational functions. This is essentially due to a famous theorem of Hilbert called the "Nullstellensatz". We indicate here how this comes about with proofs deferred to the Appendix. Let v be a discrete valuation on $k(E)$ which is trivial on k. We want to find a point $P \in E$ such that $v = \mathrm{ord}_P$. Let $A = \{r \in k(E) : v(r) \geq 0\}$. We want to think of A as being the rational functions which are finite at our desired point P.

Exercise 8.11. Show that A is a *discrete valuation ring* or *DVR*, *i.e.*, A is a pid with a unique (nonzero) prime (or maximal) ideal $\mathfrak{m}$. Show that $\mathfrak{m} = \{r \in k(E) : v(r) > 0\}$.

The field $A/\mathfrak{m}$ is called the *residue field* of A. The form of the Nullstellensatz we use is the following:

Theorem 8.11 (Weak Hilbert Nullstellensatz). Let A be a ring which is finitely generated over a field k. Let $\mathfrak{m}$ be any maximal ideal of A. Then $A/\mathfrak{m}$ is an algebraic extension of k.

See the Appendix for an indication of the proof. In our case since k is assumed to be algebraically closed, we get $A/\mathfrak{m} = k$.

There are two cases, corresponding to the cases where the desired point P is finite or infinite. First suppose $v(x) \geq 0$ where x is the usual coordinate function.

Exercise 8.12. Show that this implies that $v(y) \geq 0$ also.

So we have $x, y \in A$. Let $\pi : A \to A/\mathfrak{m}$ be the canonical projection, and put $a = \pi(x)$ and $b = \pi(y)$ so $a, b \in k$. It is easy to see that $P = (a, b)$ is a point on our curve E. We want to show that $v(r) = \mathrm{ord}_P r \ \forall r \in k(E)$.

First note that $\pi(x) = a = x(P)$ and $\pi(y) = b = y(P)$ so $\pi(r) = r(P) \ \forall r \in k(E)$, *i.e.*, π is the evaluation map at P. Hence

$$\mathfrak{m} = \{r \in A : r(P) = 0\} \quad .$$

Now if $r \notin A$, $v(1/r) < 0$ so $(1/r) \in \mathfrak{m}$ and $(1/r)(P) = 0$. Hence r is not finite at P, and we see that A is the ring of rational functions which are finite at P.

Observe that v can be computed from A. Since A is a pid, we can pick a generator u of $\mathfrak{m}$.

Exercise 8.13. If $r \in A$ is not zero, show that we can write $r = u^d s$ with $d \in \mathbb{Z}$ and s invertible.

Now it is not hard to see that $v(r) = d$ and that u is a uniformizer at P so $\mathrm{ord}_P r = d$ too.

If $v(x) < 0$, then we take $P = \mathcal{O}$. We leave the details of this case to the "interested reader".

Closely related to discrete valuations are absolute values. In fact McCarthy's valuations are Serre's absolute values.

Definition 8.17. Let K be any field. An *absolute value* on K is a real–valued function $x \mapsto |x|$ on K which satisfies the following conditions:

i) $|x| \geq 0$ and $|x| = 0$ if and only if $x = 0$,

ii) $|xy| = |x| \cdot |y|$,

iii) $|x + y| \leq \max(|x|, |y|)$.

Exercise 8.14.

i) Let v be a discrete valuation on K and $a \in \mathbb{R}$ be between 0 and 1. Set $|x| = a^{v(x)}$. Show $|\ |$ is an absolute value on K.

ii) Show $|-x| = |x|$.

iii) Suppose $|x| > |y|$. Show $|x + y| = |x|$.

It is *not* true that every absolute value on K comes from a discrete valuation, however we make the following additional assumptions on our absolute values which will insure that they come from a discrete valuation. **We assume that $|K^*|$, the set of absolute values of all elements of K^*, is a discrete subset of $\mathbb{R}^*$.**

Exercise 8.15. Let $|\ |$ be an absolute value on K. Show that there is $\lambda > 0$ in $\mathbb{R}$ such that $v(x) = \lambda \cdot \exp(|x|)$ is a discrete valuation on K.

Remark. The terminology regarding valuations, absolute values and the like is a mess. Various books use different names for the same concepts, and the same names for different concepts. There are actually *four* concepts which are more or less equivalent, valuations, absolute values, valuation rings, and places. We have already seen valuations and absolute values. If R is a subring of a field K we say R is a *valuation ring* for K if $x \in K$ and $x \notin R$ implies $x^{-1} \in R$. A *place* of K is a "homomorphism" from K into the set consisting of the elements of some field F and another element called "∞". By this we mean that the intuitive algebraic rules regarding ∞ are followed, *e.g.*, $x \pm \infty = \infty, 1/0 = \infty, 0 \cdot \infty$ is undefined, *etc.*

If we have a valuation v, we get a valuation ring by setting

$$R = \{x \in K : v(x) \geq 0\} \quad .$$

Let $\mathfrak{m} = \{x \in R : v(x) = 0\}$. We get a place by mapping $x \in R$ into $R/\mathfrak{m}$ and if $x \in K$ is not in R we map it to ∞.

The notion of valuation is confused because some people consider valuations whose values lies in more general groups than others. There are various characterizations of all of these concepts that correspond to *discrete* valuations, *e.g.*, in a valuation ring corresponding to a discrete valuation the ideal $\mathfrak{m}$ is *principal*.

In addition, there are different versions of rule iii) in the definition of absolute value. If one merely requires the triangle inequality

$$|x + y| \leq |x| + |y|$$

we get a somewhat more general notion. The ones we consider are called *ultrametric* by the French and *non–archimedean* by everybody else. Roughly

speaking, the only other ones (the archimedean ones) are the usual absolute values on the reals and the complexes. [4] is a good place to try and get this all straightened out.

We have tried to avoid valuation rings and places, and have used mostly valuations in the body of these notes and absolute values in the Appendix.

Let $|\ |$ be an absolute value on K. Recall the construction of the real numbers from the rational numbers. One can copy that construction on K to get the *completion* $\hat{K}$. One defines cauchy sequences and limits just as in the rational case. Thus $\hat{K}$ is an extension field of K in which every cauchy sequence converges. The following exercise is not difficult although it is a little fussy:

Exercise 8.16. If $\sigma : K \to L$ is an isomorphism of fields with absolute values, then we say σ is *analytic* if $|x|_K = |\sigma(x)|_L$. Suppose L is an extension of K which happens to be complete. Show there is an analytic isomorphism from $\hat{K}$ to a subfield of L which is the identity on K, *i.e.*, $\hat{K}$ is analytically K–isomorphic to a subfield of L. In particular, this shows that if K' is a complete extension of K such that every element of K' is the limit of some cauchy sequence of elements of K, then K' is analytically K–isomorphic to $\hat{K}$.

Exercise 8.17. Let E be an elliptic curve and $P \in E$. Let

$$A = \{r \in k(E) : r(P) < \infty\} \quad .$$

Let $\hat{A}$ be the completion of A with respect to the valuation $\mathrm{ord}_{P'}$. Show that $\hat{A}$ is isomorphic to $k[[u]]$, the ring of formal power series in a uniformizer u at P. (This situation is investigated in the case $P = \mathcal{O}$ in [15, Chapter IV].)

If L is an extension of K and K has a valuation (and an associated absolute value), then there may be many ways to extend the valuation on K to L. In the finite separable case they are classified by the following theorem:

Theorem 8.12. Let $L = K(x)$ be a finite separable extension of K, and let v be a valuation on K. Let m_x be the minimal polynomial of x. Suppose m_x factors into r nonconstant irreducible factors when considered as a polynomial in $\hat{K}[X]$. Then v has exactly r distinct extensions to L.

Furthermore, if we let V be an extension of v to L which corresponds to the factor f of m_x in $\hat{K}[X]$, and let $\hat{L}$ be the completion of L with respect to V, then there is $\hat{x} \in \hat{L}$ with $\hat{L} = \hat{K}(\hat{x})$ and f is the minimal polynomial of $\hat{x}$ over $\hat{K}$.

The purely inseparable case is handled by the following:

Proposition 8.13. Let L be a purely inseparable extension of K. Then any valuation on K has a unique extension to L.

We defer the proof of Theorem 8.12 to the Appendix. Note that the hypothesis that L be generated by a single element over K is not a restriction since every finite separable extension is generated by a single element (see any algebra book, say [10, page 185]). For the proof of the proposition we note that if L is a purely inseparable extension of K, then there is an integer $e > 0$ with the property that $x^{p^e} \in K$ for all $x \in L$. This enables us to write a formula for the extension of a valuation on K to L. We leave the details as an exercise. As in Section 5, we can put the theorem and the proposition together to cover the case of an arbitrary finite extension. We can now use these results to prove the desired result concerning the norm.

Theorem 8.13. Let L be a finite extension of K. Let v be a valuation on K, and let $v_1, v_2, \ldots, v_r$ be the various extensions of v to L. Let $\hat{K}$ be the completion of K and $\hat{L}_i$ be the completion of L with respect to v_i. Then for all $y \in L$ we have

$$N_{L/K}(y) = \prod_{i=1}^{r} N_{\hat{L}_i/\hat{K}}(y) \quad .$$

Proof. First we assume that L is a separable extension so we can write $L = K(x)$ for some $x \in L$. By the results of Section 5, $N_{L/K}(x)$ is plus or minus the constant term of m_x. This constant term is the product of the constant terms of its factors in $\hat{K}[X]$ which, in turn, are plus or minus the various $N_{\hat{L}_i/\hat{K}}(x)$. Hence the theorem holds for the particular element x.

Fix $y \in L^*$. (If $y = 0$, the result is trivial.) Consider the fields $K(y \cdot (x + z))$ where z runs through K. Since v is a nontrivial valuation, K must have infinitely many elements. Since L is separable over K, there are only finitely many fields between L and K ([10, page 185] again). Hence for some distinct $z, z' \in K$ we have $K(y \cdot (x + z)) = K(y \cdot (x + z'))$. Call this intermediate field K'. We must have $y \cdot (z - z') \in K'$. Since $z - z' \in K^*$, we must have $y \in K'$. Thus $y \cdot (x + z) \in K'$ so $yx \in K'$, and since $y \neq 0$, we must have $x \in K'$. Therefore $L = K(y \cdot (x + z))$. Since $z \in K$, we also have $L = K(x + z)$. Hence we have the theorem for the particular elements $y \cdot (x + z)$ and $x + z$ of L. Finally we get

$$\begin{aligned} N_{L/K}(y) &= \frac{N_{L/K}(y \cdot (x+z))}{N_{L/K}(x+z)} \\ &= \frac{\prod_{i=1}^{r} N_{\hat{L}_i/\hat{K}}(y \cdot (x+z))}{\prod_{i=1}^{r} N_{\hat{L}_i/\hat{K}}(x+z)} \\ &= \prod_{i=1}^{r} \frac{N_{\hat{L}_i/\hat{K}}(y \cdot (x+z))}{N_{\hat{L}_i/\hat{K}}(x+z)} \\ &= \prod_{i=1}^{r} N_{\hat{L}_i/\hat{K}}(y) \quad . \end{aligned}$$

This finishes the separable case.

As usual we can now consider a field M with M separable over K and L purely inseparable over M. In the purely inseparable case Equation (17) shows that $N(x) = x^{p^e}$ where $p^e = [L : M]$. It is not hard to show that the degree does not change under completion with respect to any valuation on M (and its unique extension to L). We again leave the details as an exercise. ∎

9 Completion of the Proof of Weil Reciprocity

We now complete the proof of generalized Weil reciprocity by proving Lemma 7.4. We had an elliptic curve E and rational functions $f, g \in K(E)$. We considered g as a rational mapping to the projective line $\mathbb{P}_1$. Then for $t \in \mathbb{P}_1$ we

wanted to prove the following formula:

$$\prod_{g(Q)=t} \langle f,g\rangle_Q = \langle N_{K(E)/K(g)} f, g\rangle_\tau$$

where $\langle\ \rangle_\tau$ is defined by

$$\langle r\circ g, s\circ g\rangle_\tau = \langle r,s\rangle_t \quad .$$

Let $K_g = \widehat{K(g)}$ be the completion of this field with respect to the valuation $\mathrm{ord}_\tau(h\circ g) = \mathrm{ord}_t h$ for $h \in K(\mathbb{P}_1)$. Then ord_τ extends uniquely to K_g.

Now if $v, w \in K_g$, the local symbol $\langle v,w\rangle_\tau$ can be defined as the limit of the local symbols in $K(g)$. It is easy to see that the values of the local symbols will converge because the difference of two functions that are close in this metric must have a zero at t. This "completed" local symbol is still multiplicative in v and w. Similarly for $Q \in E$, we can extend the local symbol to $K_Q = \widehat{K(E)_Q}$, the completion of $K(E)$ with respect to the valuation ord_Q.

Proposition 1.2 tells us that $\mathrm{ord}_Q = e\cdot \mathrm{ord}_\tau$ on $K(g)$ where $e = e_g(Q)$ is the ramification index of g at $Q \in E$. Consider the extensions of the valuation $e\cdot\mathrm{ord}_\tau$ on K_g to K_Q. The following theorem describes the situation completely.

Theorem 9.14. Let L be a field which is complete with respect to some valuation v, and let M be a finite extension of L. Then there is a unique extension of v to M. In fact, if $x \in M$, then

$$v(x) = (1/d)v(N_{M/L}x)$$

where $d = [M : L]$.

This result is a translation of Theorem 3.4 in the Appendix. We know that ord_Q is an extension of $e\cdot\mathrm{ord}_\tau$. Hence if we write $d = [K_Q : K_g]$ and $N_Q = N_{K_Q/K_g}$, then

$$\mathrm{ord}_Q(r) = (e/d)\mathrm{ord}_\tau(N_Q r) \text{ for } r \in K_Q \quad .$$

We now show $e = d$ where $e = e_g(Q)$ and $d = [K_Q : K_g]$. In fact, we will show that $1, f, f^2, \ldots, f^{e-1}$ forms a basis for K_Q as a vector space over K_g. First assume $t = g(Q) = 0$ so $e = \mathrm{ord}_Q g$. Let $r \in K_Q$ and $a_0 = r(Q)$. Suppose

$$\mathrm{ord}_Q(r - a_0) = h_1 = k_1 e + \ell_1 \text{ with } 0 \le \ell_1 < e \quad .$$

Then we can write $r - a_0 = s_1 f^{\ell_1} g^{k_1}$ where $s_1(Q) = a_1 \neq 0$. We now set $r_1 = a_0 + a_1 f^{\ell_1} g^{k_1}$, and $\mathrm{ord}_Q(r - r_1) = h_2 > h_1$. We can set $h_2 = k_2 e + \ell_2$ and continue this process producing a sequence of functions $\{r_i\}$ which converges to r and is of the form

$$r_i = q_0(g) + q_1(g)f + \cdots + q_{e-1}(g)f^{e-1}$$

where each q_j is a polynomial. This proves our result ($e = d$) in this case. If $g(Q) \neq 0, \infty$, substitute $g - g(Q)$ for g in the above construction. If Q is a pole of g, use $1/g$ for g. Hence we have shown that

$$\mathrm{ord}_Q(r) = \mathrm{ord}_\tau(N_Q r) \text{ for } r \in K_Q \quad . \tag{25}$$

Theorem 8.13 tells us that

$$N_{K(E)/K(g)}f = \prod_{g(Q)=t} N_Q f \quad .$$

Thus the right–hand side on our equation satisfies

$$\langle N_{K(E)/K(g)}f, g\rangle_\tau = \prod_{g(Q)=t} \langle N_Q f, g\rangle_\tau \quad ,$$

and it suffices to prove the following:

Claim. $\langle f, g\rangle_Q = \langle N_Q f, g\rangle_\tau$.

Since everything in sight is multiplicative, we can assume that f is a uniformizer at Q. *i.e.*, $\mathrm{ord}_Q f = 1$. On the other hand if $\mathrm{ord}_Q g = 0$, then

$$\langle f, g\rangle_Q = g(Q)^{-\mathrm{ord}_Q f} = 1/t \quad ,$$

while

$$\langle N_Q f, g\rangle_\tau = t^{-\mathrm{ord}_\tau N_Q f} = 1/t$$

since $\mathrm{ord}_\tau N_Q f = \mathrm{ord}_Q f = 1$ by (25). Hence we can assume $\mathrm{ord}_Q g \neq 0$ or that $t = 0$ or ∞.

Since $g = g^*(I)$, we must have $\mathrm{ord}_\tau g = \pm 1$. Suppose $\mathrm{ord}_\tau g = 1$. By the definition of the local symbol

$$\begin{aligned}\langle N_Q f, g\rangle_\tau =& -\frac{(N_Q f)\circ g^{-1}}{I}(t)\\ =& \frac{N_Q f}{g}(Q)\end{aligned}$$

where the expression $N_Q f(Q)$ must be interpreted with a grain of salt since $N_Q f$ lies in the completion of $K(g)$ and thus may not be a proper function. As we have remarked above, however, there are functions in $K(g)$ near $N_Q f$, and if they are near enough, they all have the same value which we take for $N_Q f(Q)$.

On the other hand, $\mathrm{ord}_Q g = e \cdot \mathrm{ord}_t I = e$ so

$$\langle f, g\rangle_Q = (-1)^e \frac{f^e}{g}(Q) \quad . \tag{26}$$

Therefore in this case it suffices to show that the function $N_Q f/f^e$ takes the value $(-1)^{e-1}$ at the point Q. If we have $t = \infty$, then a similar argument shows that it suffices to prove the exact same thing.

Let the minimal polynomial of f over K_g be given by

$$m_f(X) = X^e + a_1 X^{e-1} + \cdots + a_e$$

where the a_i are in K_g. By the definition of the norm and the proof of Theorem 5.4, we get that $a_e = (-1)^e N_Q f$. Now consider the equation $m_f(f) = 0$, *i.e.*,

$$f^e + a_1 f^{e-1} + \cdots + a_e = 0 \quad . \tag{27}$$

If $a_i \neq 0$, then

$$\begin{aligned} \mathrm{ord}_Q(a_i f^{e-i}) &= \mathrm{ord}_Q a_i + \mathrm{ord}_Q f^{e-i} \\ &= e \cdot \mathrm{ord}_\tau a_i + e - i \\ &\equiv -i \pmod{e} \quad . \end{aligned}$$

Hence the nontrivial monomials of Equation (27) all have distinct orders at Q except possibly for f^e and a_e. Thus the only way for all of the monomials to sum to 0 is for $\mathrm{ord}_Q f^e$ to equal $\mathrm{ord}_Q a_e$. Also since

$$\mathrm{ord}_Q(f^e + a_e) \geq \mathrm{ord}_Q f^e = \mathrm{ord}_Q a_e \quad ,$$

all of the other monomials must have higher order at Q, *i.e.*,

$$\mathrm{ord}_Q f^e = \mathrm{ord}_Q a_e < \mathrm{ord}_Q(a_i f^{e-i}) \text{ for } 1 \leq i \leq e-1 \quad .$$

Hence since

$$\begin{aligned} \mathrm{ord}_Q(f^e + a_e) &= \mathrm{ord}_Q(-a_1 f^{e-1} - a_2 f^{e-2} - \cdots - a_{e-1} f \\ &\geq \min_{1 \leq i \leq e-1} \{a_i f^{e-i}\} \\ &> \mathrm{ord}_Q f^e = \mathrm{ord}_Q a_e \quad , \end{aligned}$$

after dividing by f^e, we get

$$\mathrm{ord}_Q(1 + a_e/f^e) > \mathrm{ord}_Q 1 = 0 \quad .$$

This tells us that

$$\frac{a_e}{f^e}(Q) = -1$$

so

$$\frac{N_Q f}{f^e} Q = (-1)^{e-1} \quad ,$$

and we have finished the proof of Lemma 7.4 and of generalized Weil reciprocity.

10 The Weil Pairing

We end these notes with an application of generalized Weil reciprocity to the Weil pairing. The definition given in [5] of the Weil pairing is essentially the one given in [15, page 96]. In Exercise 3.16 on page 108, Silverman gives an alternative definition which involves functions of much lower degree. In [8] a similar definition is used, but it is slightly incorrect. In this section we give the correct version of the definition in [8] and prove it is equivalent to the one in [5].

Let E be an elliptic curve over an algebraically closed field K. Pick $N > 0$ such that N is prime to the characteristic of K. Let $P, Q \in E[N]$, the subgroup of E of N–torsion points. Suppose $P, Q \neq \mathcal{O}$ and $P \neq Q$. Fix $P', Q' \in E[N^2]$ such that

$$P = N \cdot P' \text{ and } Q = N \cdot Q' \quad .$$

Pick functions f_P and $g_P \in K(E)$ such that

$$\begin{aligned} \mathrm{div} f_P &= N\langle P\rangle - N\langle \mathcal{O}\rangle \\ \mathrm{div} g_P &= [N]^*(\langle P\rangle - \langle \mathcal{O}\rangle) \\ &= \langle P' + E[N]\rangle - \langle E[N]\rangle \end{aligned} \tag{28}$$

where $[N]$ is the rational mapping multiplication by N. Pick f_Q and g_Q similarly. Since we have only specified the divisors of these functions there is some freedom in their choice, and we may assume that

$$\begin{aligned} {g_P}^N &= f_P \circ [N], \text{ and} \\ {g_Q}^N &= f_Q \circ [N] \end{aligned} \tag{29}$$

where $[N]$ is multiplication by N. Then in [5] (and in [15]), the Weil pairing was defined by

$$w(P,Q) = \frac{g_Q \circ \tau_P}{g_Q}$$

where τ_P is translation by S. Recall that the function on the right–hand side of the above equation is multiplication by an N^{th} root of unity, and by an "abuse of terminology" we define $w(P,Q)$ to be this root.

The next theorem gives the correct version of the definition in [8].

Theorem 10.15. Let $P, Q \in E[N]$. Then

$$w(P,Q) = (-1)^N \frac{f_P(Q)}{f_Q(P)} \cdot \frac{f_Q}{f_P}(\mathcal{O}) \quad .$$

Proof. Let h be any rational function with

$$\mathrm{div} h = (N-1)\langle Q'\rangle + \langle Q' - Q\rangle - N\langle \mathcal{O}\rangle \quad .$$

By Generalized Weil reciprocity, we have

$$\prod_{S \in E} \langle g_P, h\rangle_S = 1 \quad .$$

The only nontrivial contributions in the above product come from $S = Q', Q'-Q$ and the zeros and poles of g_P.

First consider $S = Q'$ and $Q' - Q$,

$$\begin{aligned} \langle g_P, h\rangle_{Q'} &= {g_P}^{N-1}(Q') \text{ and} \\ \langle g_P, h\rangle_{Q'-Q} &= g_P(Q' - Q) \text{ so} \\ \langle g_P, h\rangle_{Q'} \cdot \langle g_P, h\rangle_{Q'-Q} &= \frac{g_P(Q'-Q)}{g_P(Q')} \cdot {g_P}^N(Q') \\ &= \frac{g_P(S)}{g_P(S+Q)} \cdot f_P \circ [N](Q') \\ &= \frac{f_P(Q)}{w(P,Q)} \end{aligned}$$

where we have put $S = Q' - Q$ and used (29).

Now let

$$H(S) = \prod_{T \in E[N]} h(S+T)$$

so

$$\begin{aligned}
\mathrm{div}H &= \sum_{T \in E[N]} \mathrm{div}(h \circ \tau_T) = \sum_{T \in E[N]} {\tau_T}^*(\mathrm{div}h) \\
&= \sum_{T \in E[N]} (N-1)\langle Q' - T\rangle + \langle Q' - Q - T\rangle - N\langle -T\rangle \\
&= (N-1)\langle Q' + E[N]\rangle + \langle Q' - Q + E[N]\rangle - N\langle E[N]\rangle \\
&= N\langle Q' + E[N]\rangle - N\langle E[N]\rangle \\
&= [N]^*(N\langle Q\rangle - N\langle \mathcal{O}\rangle) \\
&= \mathrm{div}(f_Q \circ [N]) \quad .
\end{aligned}$$

Since we had the usual freedom in the choice of h, we can assume

$$H = f_Q \circ [N] = {g_Q}^N$$

by (29).

We now consider the zeros of g_P.

$$\begin{aligned}
\prod_{\mathrm{ord}_S g_P > 0} \langle g_P, h\rangle_S &= \prod_{T \in E[N]} \frac{1}{h(P'+T)} \\
&= \frac{1}{H(P')} \\
&= \langle g_P, H\rangle_{P'} \quad .
\end{aligned}$$

For the poles of g_P, we have

$$\begin{aligned}
\prod_{\mathrm{ord}_S g_P > 0} \langle g_P, h\rangle_S &= \langle g_P, h\rangle_{\mathcal{O}} \cdot \prod_{T \in E[N] - \mathcal{O}} h(T) \\
&= (-1)^{1 \cdot N} \frac{{g_P}^{-N}}{h^{-1}}(\mathcal{O}) \cdot \prod_{T \in E[N] - \mathcal{O}} h(T) \\
&= (-1)^{1 \cdot N} \frac{{g_P}^{-N}}{H^{-1}}(\mathcal{O}) \\
&= \langle g_P, H\rangle_{\mathcal{O}} \quad .
\end{aligned}$$

Putting this all together, we get

$$\begin{aligned}
1 &= \left[\langle g_P, h\rangle'_Q \cdot \langle g_P, h\rangle_{Q'-Q}\right] \cdot \langle g_P, H\rangle_{P'} \cdot \langle g_P, H\rangle_{\mathcal{O}} \\
&= \frac{f_P(Q)}{w(P,Q)} \cdot \frac{1}{H(P')} \cdot (-1)^N \frac{H}{{g_P}^N}(\mathcal{O}) \\
&= \frac{f_P(Q)}{w(P,Q)} \cdot \frac{1}{f_Q(N \cdot P')} \cdot (-1)^N \frac{f_Q \circ [N]}{f_P \circ [N]}(\mathcal{O}) \\
&= \frac{1}{w(P,Q)} \cdot \frac{f_P(Q)}{f_Q(P)} \cdot (-1)^N \frac{f_Q}{f_P}(\mathcal{O}) \quad .
\end{aligned}$$

■

If you examine the choices made for f_P, f_Q, g_P, and g_Q, you will see that f_P and f_Q are really completely arbitrary (with the given divisor) so we can pick them so that

$$\frac{f_Q}{f_P}(\mathcal{O}) = 1 \quad .$$

For this choice the Weil pairing can be written

$$w(P,Q) = (-1)^N \frac{f_P(Q)}{f_Q(P)} \quad .$$

This has appeared a number of times in the literature incorrectly, without the $(-1)^N$, *e.g.*, [8].

APPENDIX

1. The Nullstellensatz

In Section 8 we used a famous theorem due to Hilbert called the "Nullstellensatz". This theorem has a number of forms, and the one we used is usually called the "weak" Nullstellensatz. The Nullstellensatz is a basic theorem for the study of algebraic geometry, and most books on elementary algebraic geometry contain a proof. One way to state it is that a maximal ideal of polynomials in many variables with coefficients in an algebraically closed field have a common zero. A straightforward proof of this version can be found in [9]. Another elementary proof is in [6]. We follow the treatment in [7].

In our situation we have a field k and a ring R which is finitely generated over k, *i.e.*, $R = k[x_1, x_2, \ldots, x_n]$. Now to make the theorem interesting, the x_i must be transcendental over k, but they may not be algebraically independent over k, *i.e.*, R may not be the polynomial ring in n variables over k. The theorem tells us that if we divide R by a maximal ideal $\mathfrak{m}$, the residue field $R/\mathfrak{m}$ *is* algebraic over k. So roughly speaking, $\mathfrak{m}$ must contain all of the transcendence.

The proof proceeds by first showing that $A = R/\mathfrak{m}$ contains a subring B which is a polynomial ring over k in perhaps fewer than n variables, and that A is integral over B, *i.e.*, every element of A satisfies a monic polynomial with coefficients in B. This result is called Noether's Normalization Theorem. Before we get to its proof, we need some elementary results concerning integral elements.

Proposition 1.1. Let B be a subring of a ring A and let $\alpha \in A$. The following properties are equivalent:

i) α is integral over B.

ii) $B[\alpha]$ is finitely generated as a B-module where $B[\alpha]$ is the subring of A generated by B and α.

iii) There exists a subring $B_1 \subset A$ with $B \subset B_1$ and $\alpha \in B_1$ such that B_1 is finitely generated as a B-module.

Proof. i) $\Rightarrow$ ii) Since α is integral over B, there exists $F(X) \in B[X]$ such that

$$F(X) = X^n + b_1 X^{n-1} + \cdots + b_n \quad ,$$

and $F(\alpha) = 0$. Hence

$$\alpha^n = -\sum_{i=1}^{n} b_i \alpha^{n-i}$$

so $B[\alpha]$ is generated by $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ as a B-module.

ii) $\Rightarrow$ iii) is trivial.

iii) $\Rightarrow$ i). Let $b_1, b_2, \ldots, b_n \in B_1$ be a set of generators for B_1 as a B-module. Since $\alpha \in B_1$, $\alpha b_i \in B_1$ for $i = 1, 2, \ldots, n$ so there are elements $\beta_{i,j} \in B$ such that

$$\alpha b_i = \sum_{j=1}^{n} \beta_{i,j} b_j \text{ for } i = 1, 2, \ldots, n \quad . \tag{30}$$

Let F be the polynomial defined by

$$F(X) = \det(X \cdot I_n - [\beta_{i,j}])$$

where I_n is the $n \times n$ identity matrix, and $[\beta_{i,j}]$ is the obvious thing. Equation (30) implies that $F(\alpha)b_i = 0$ for $i = 1, 2, , n$. Hence $F(\alpha) = 0$. Since the coefficients of F are in B and F is clearly monic, this shows α is integral over B. ■

Now we give a few corollaries.

Corollary 1.1. If $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$ are integral over B, then $B[\alpha_1, \alpha_2, \ldots, \alpha_n]$ is finitely generated as a B-module and is integral over B, *i.e.*, every element of $B[\alpha_1, \ldots, \alpha_n]$ is integral over B.

Proof. The proof is by induction on n. For $n = 1$, this is i) $\Rightarrow$ ii) of the proposition. Assume the desired result holds for $n - 1$. Then $B_1 = B[\alpha_1, \ldots, \alpha_{n-1}]$is finitely generated over B so

$$B_1 = \sum_{i=1}^{s} \beta_i B$$

for some s and some $\beta_i \in B_1$. Since α_n is integral over B,

$$B[\alpha_n] = \sum_{j=0}^{m-1} {\alpha_n}^j B$$

for some m. Hence

$$\begin{aligned} B[\alpha_1, \ldots, \alpha_n] &= B_1[\alpha_n] \\ &= \sum_{j=0}^{m-1} {\alpha_n}^j B_1 \\ &= \sum_{i,j} {\alpha_n}^j \beta_i B \end{aligned}$$

which is a finitely generated B-module. ■

Corollary 1.2. Let $B_A = \{\alpha \in A : \alpha \text{ is integral over } B\}$. Then B_A is a subring of A.

Proof. Take $\alpha, \beta \in B_A$. By Corollary 1.1, $B[\alpha, \beta]$ is integral over B so $\alpha \pm \beta$ and $\alpha\beta$ which are members of $B[\alpha, \beta]$ are integral over B. ■

Corollary 1.3. If A is integral over B and B is integral over C, then A is integral over C.

We leave this proof as an exercise since it is an easy consequence of Corollary 1.3.

Corollary 1.4. If $\alpha \in A$ and α is integral over B_A, then $\alpha \in B_A$.

This proof is an easy consequence of the previous corollary.

Now we can prove the Normalization Theorem.

Theorem 1.1 (Noether's Normalization Theorem). Let A be an integral domain which is finitely generated over a field, *i.e.*, $A = k[x_1, x_2, \ldots, x_n]$. Then there are elements $y_1, y_2, \ldots, y_r \in A$ such that

i) the subring $B = k[y_1, \ldots, y_r]$ is isomorphic (as an algebra over k) to the ring of polynomials in r variables, *i.e.*, $y_1, y_2, \ldots, y_r$ are algebraically independent over k, and

ii) A is integral over B.

Proof. The proof is by induction on n. If $n = 0$ there is nothing to prove. Let $X_1, X_2, \ldots, X_n$ be indeterminates, and $R = k[X_1, \ldots, X_n]$. Define a surjective k-homomorphism $\varphi : R \to A$ by $\varphi(X_i) = x_i$ for $i = 1, 2, \ldots, n$. Since A is an integral domain, $\mathfrak{p} = \ker \varphi$ is a prime ideal of R. If $\mathfrak{p} = 0, A = R$, and we are done. Let $F \in \mathfrak{p} - 0$. If $F \in K$, then $F \cdot F^{-1} = 1 \in \mathfrak{p}$ so $\mathfrak{p} = R$, and $A = 0$, and we are done. Thus we can assume F is nonconstant. We use

Lemma 1.1. Let R be a polynomial ring, $k[X_1, \ldots, X_n]$, over a field k, and let F be a nonconstant polynomial in R. Then there exist integers $m_2, m_3, \ldots, m_n \geq 0$ such that R is integral over the subring $S = k[F, G_2, G_3, \ldots, G_n]$ where G_i is the polynomial

$$G_i = X_i - {X_1}^{m_i} \quad ,$$

and

Lemma 1.2. Let U be a subring of some ring V and $\mathfrak{a}$ an ideal of V. Then $U/\alpha \cap U$ can be identified with a subring of V/α. If V is integral over U, then V/α is integral over $U/\alpha \cap U$.

By Lemma 1.1, R is integral over S so $R/\mathfrak{p}$ is integral over $A_1 = S/S \cap \mathfrak{p}$ by Lemma 1.2. Since $F \in S \cap \mathfrak{p}$, the subring $A_1 \subset R/\mathfrak{p}$ is generated mod $(S \cap \mathfrak{p})$ over k by the G_i for $i = 2, 3, \ldots, n$. By the induction hypothesis applied to A_1 there are $y_1, y_2, \ldots, y_r \in A_1$ such that $y_1, y_2, \ldots, y_r$ are algebraically independent over k, and A_1 is integral over $B = k[y_1, \ldots, y_r]$. By Corollary 1.3 since $A = R/\mathfrak{p}$ is integral over A_1 and A_1 is integral over B, A is integral over B. ∎

Lemma 1.2 is easy, and we leave the proof as an exercise. Lemma 1.3 is not so easy. It is due to Nagata and the proof follows.

Proof. Clearly if we adjoin X_1 to S, we can get the rest of the X_i's so $R = S[X_1]$. If we can show that X_1 is integral over S for an appropriate choice of $m_2, m_3, \ldots, m_n$, then by Proposition 1.1, R will be integral over S, and we will be done.

Let $m_2, m_3, \ldots, m_n > 0$ and put

$$G_i = X_i - {X_1}^{m_i} \text{ for } i = 2, 3, \ldots, n \quad .$$

Let T be an indeterminate over S so $S[T]$ is the polynomial ring in one variable over S. Recall that $F \in R$ so F is a polynomial in n variables. Define $H(T) \in$

$S[T]$ by

$$H(T) = F(T, G_2 + T^{m_2}, \ldots, G_n + T^{m_n}) - F(X_1, \ldots, X_n) \quad .$$

Then $H(X_1) = 0$. Hence to show that X_1 is integral over S, it suffices to show that we can pick $m_2, m_3, \ldots, m_n$ such that the leading coefficient of H is independent of $G_2, G_3, \ldots, G_n$ since then this leading coefficient will have to be a constant (*i.e.*, in k), and we can divide it out.

Let $m_1 = 1$, and let δ be the total degree of F. Now F is a linear combination of monomials

$$M_\alpha(X_1, \ldots, X_n) = {X_1}^{\alpha_1} {X_2}^{\alpha_2} \cdots {X_n}^{\alpha_n}$$

where $\alpha = (\alpha_1, \ldots, \alpha_n)$ with $\alpha_i \geq 0$. That is

$$F(X_1, \ldots, X_n) = \sum_{|\alpha| < \delta} a_\alpha M_\alpha(X_1, \ldots, X_n)$$

with $|\alpha| = \Sigma_{i=1}^n \alpha_i$ and $a_\alpha \in k$. Hence

$$\begin{aligned} H(T) &= \sum_{|\alpha| < \delta} a_\alpha M_\alpha(T^{m_1}, G_2 + T^{m_2}, \ldots, G_n + T^{m_n}) - F(X_1, \ldots, X_n) \\ &= \sum_{|\alpha| < \delta} a_\alpha \cdot \left(T^{\Sigma_{i=1}^n \alpha_i m_i} + H_\alpha(T) \right) - F(X_1, \ldots, X_n) \end{aligned}$$

where the $H_\alpha(T) \in S[T]$ are such that

$$\deg_T H_\alpha(T) < \sum_{i=1}^n \alpha_i m_i \quad ,$$

i.e., we have collected the factors in M_α which contain just powers of T and the remaining terms (the H_α) have lower degree in T. Hence the only way that the leading coefficient of H can involve any X_i's is that some of the $T^{\Sigma_{i=1}^n \alpha_i m_i}$ cancel for different α's. So if we pick $m_2, m_3, \ldots, m_n$ so the $\Sigma_{i=1}^n \alpha_i m_i$ are all different for all α with $|\alpha| < \delta$, we will be done. There are many possibilities; $m_i = (\delta + 1)^{i-1}$ works, for example. ∎

Now we can easily prove the main result of this section.

Theorem 1.2 (Weak Hilbert Nullstellensatz). Let R be a ring which is finitely generated over a field k. Let $\mathfrak{m}$ be any maximal ideal of R. Then $R/\mathfrak{m}$ is an algebraic extension of k.

Proof. Since R is finitely generated over k, so is $A = R/\mathfrak{m}$, and since A is a field, it certainly is an integral domain so the Normalization Theorem 1.1 applies. Thus there are elements $y_1, y_2, \ldots, y_r \in A$, algebraically independent over k such that A is integral over $B = k[y_1, \ldots, y_r]$. If $r > 0$, then since A is really a field $\eta = {y_1}^{-1} \in A$. Hence η is integral over a polynomial ring, namely B. Therefore η satisfies

$$\eta^m + F_1 \eta^{m-1} + \cdots + F_m = 0$$

for some $F_i \in B = k[y_1, \ldots, y_r]$. If we multiply by ${y_1}^m$, we get

$$1 + F_1 y_1 + \cdots + F_m {y_1}^m = 0$$

which contradicts the fact that the $y_1, y_2, \ldots, y_m$ are algebraically independent over B. Therefore $r = 0$, and A is algebraic over k. ∎

2. Newton's Polygon

In Section 8 we needed to know the different ways a valuation v on a field K could be extended to a finite separable extension $L = K(x)$. The answer turned out to depend on the factorization of the minimal polynomial, m_x, over the completion of K. In the next sections we indicate the proof of this result (Theorem 8.12).

As you may expect, the main difficulty is to find *one* extension of v to L. There are a number of approaches to this problem. One is to assume that K is complete. Then it is not hard to show that if an extension exists, it must satisfy

$$v(x) = (1/e)v(N_{L/K}x) \ \forall x \in L \tag{31}$$

where e is the degree of L over K. One can then use this formula to *define* the extension, and it remains to show the extension is, indeed, a valuation on L. This can be done by means of Hensel's Lemma (see [2] or [16], for example) or by using "Newton's Polygon", (see [4]). The incomplete case then follows easily. Another way is to look at the associated valuation ring of v, and use Zorn's Lemma to find a valuation ring of L which extends it (see [3] or [11]).

All of these methods have the advantage (or disadvantage) of working for more general valuations than discrete ones. The treatment in [14] applies only to discrete valuations, but avoids the use of difficult lemmas. This treatment makes heavy use of the notion of integrality and develops some of the theory of Dedekind Domains to get at the extension results. Although in some abstract sense, Serre's approach may be the "best" for our purpose, we have decided to use Cassels's treatment because it is more elementary and computational in spirit.

Let K be a field with a valuation v. Let $|\ |$ be the associated absolute value, *i.e.*, $|x| = a^{|v(x)|}$ for some $a \in [0,1]$. We are first interested in extending the absolute value to the field $K(X)$. Fix $C > 0$. For

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in K[X]$$

define

$$\|f\| = \|f\|_C = \max_j C^j |a_j| \ .$$

For $h = f/g \in K(X)$, put $\|h\| = \|f\|/\|g\|$.

Exercise 2.1. Show that $\|\ \|$ is an extension of the absolute value $|\ |$ to $K(X)$. (Hint: The only nontrivial part is to show that $\|fg\| \geq \|f\|\|g\|$. This can be done by a careful examination of the coefficient of X^{I+J} in fg where I is given by $\|f\| = \|a_I X^I\|$ and $\|a_i X^i\| < \|f\|$ if $i < I$, and similarly for J and g.)

Until we say otherwise, assume that K is complete with respect to $|\ |$. Let us also assume that $a_0 \neq 0$ and $a_n \neq 0$, *i.e.*, X does not divide f and the degree of f is precisely n. To get the *Newton Polygon*, $\Pi(f)$, we consider the points in $\mathbb{R}^2$ defined by

$$P(j) = (j, \ln|a_j|) \text{ for } a_j \neq 0 \quad .$$

Then $\Pi(f)$ is the upper boundary of the convex hull of the $P(j)$. Every $P(j)$ lies on or below $\Pi(f)$. $P(0)$ and $P(n)$ are the beginning and end of $\Pi(f)$ which consists of line segments, say σ_s for $1 \leq s \leq r$ for some r. Say σ_s joins $P(m_{s-1})$ and $P(m_s)$. We get a sequence of indices

$$0 = m_0 < m_1 < \cdots < m_r = n \quad .$$

The slope of σ_s is

$$\gamma_s = \frac{\ln|a_{m_s}| - \ln|a_{m_{s-1}}|}{m_s - m_{s-1}} \quad ,$$

and we must have

$$\gamma_1 > \gamma_2 > \cdots > \gamma_r \quad .$$

Definition 2.1. We say f is of *type* $(\ell_1, \gamma_1; \ell_2, \gamma_2; \ldots; \ell_r, \gamma_r)$ where $\ell_1 = m_1$ and $\ell_s = m_s - m_{s-1}$ for $s > 1$. We will usually abbreviate this by saying f is of type $(*)$.

If $r = 1$, we say f is *pure*.

So a polynomial is pure if its first and last coefficients are "bigger" than any of the rest. If a polynomial is of type (ℓ, γ) (and hence pure), then its degree must be ℓ, and $\gamma = (1/\ell)\ln|a_n/a_0|$.

Suppose f is of type $(*)$. We want to see how the Newton Polygon is related to the norm $\|\ \|_C$. Consider the boundary of the convex hull of the points $\{(j, \ln C^j|a_j|)\}$. Call it $\Pi_C(f)$. Let $\gamma_{C,s}$ be the corresponding slopes. Then it is an easy computation to see that

$$\gamma_{C,s} = \gamma_s + \ln C \quad .$$

Fix an index s and consider the absolute value $\|\ \|_C$ where $C = \exp(-\gamma_s)$. Then it follows from the above equation that $\|f\|_C = \|a_j X^j\|_C$ for two j's, namely $j = m_{s-1}$ and m_s, *i.e.*, $\Pi_C(f)$ has a segment of slope zero if and only if $\ln C$ is one of the γ_s's. On the other hand, if $\ln C$ is distinct from the γ_s's, then this $(\|f\|_C = \|a_j X^j\|_C)$ can only happen for precisely one value of j. Furthermore if $C = \exp(-\gamma_s)$, then it follows that

$$\left\| f(X) - \sum_{m_{s-1} \leq j \leq m_s} a_j X^j \right\|_C < \|f\|_C \quad . \tag{32}$$

If one can establish inequalities of this type for particular values of C, then one gets the slopes of the lines in the Newton Polygon.

It is also easily seen that if we take $C = \exp(-\gamma)$, then f is pure of type (ℓ, γ) if and only if

$$\|f\|_C = \|a_0\|_C = \|a_\ell x^\ell\|_C \quad . \tag{33}$$

(In this case $C = |a_0/a_N|^{1/N}$ where $N = \deg f$.)

Example 2.1. Let us take

$$f(X) = 6 + 14X^3 - 20X^5 + 29X^8 - 23X^9 + 11X^{11} + 4X^{12} - X^{13} \quad .$$

Its Newton Polygon is illustrated in Figure 1. We have

$$m_0 = 0, m_1 = 3, m_2 = 5, m_3 = 8, m_4 = 9, m_5 = 11, m_6 = 12, m_7 = 13 \quad ,$$

while the slopes are

$$\gamma_1 = 0.28, \gamma_2 = 0.18, \gamma_3 = 0.12, \gamma_4 = -0.23, \gamma_5 = -0.37, \gamma_6 = -1.01, \gamma_7 = -1.39 \quad .$$

Figure 2 shows $\Pi_C(f)$ for $C = \exp(\gamma_2)$ and Figure 3 shows $\Pi_C(f)$ for $C = \exp(\gamma_3)$. In each of these cases one can see the expected flat segments.

Exercise 2.2. Suppose $f, g \in K[X]$ are both pure with slope γ. Then fg is also pure with slope γ.

A slightly more elaborate result is

Proposition 2.2. Suppose that f is of type $(*)$ and that g is pure of type (ℓ, γ) where $\gamma < \gamma_r$. Then fg is of type $(\ell_1, \gamma_1; \ldots; \ell_r \gamma_r; \ell, \gamma)$.

Proof. Suppose

$$g(X) = b_0 + b_1 X + \cdots + b_N X^N \quad .$$

Take $C = \exp(-\gamma_s)$ for some s with $1 < s < r$. Then $\gamma_s > \gamma_r$ so $\gamma < \gamma_s$, so if we put $C_g = \exp(-\gamma)$, we get $C_g > C$. By Equation (33) we get $\|g\|_C = |b_0| > \|b_N\|_C$. Thus

$$\|g(X)\|_C > \|g(X) - b_0\|_C \quad .$$

This and (32) imply

$$\left\| f(X)g(X) - b_0 \sum_{m_{s-1} \le j \le m_s} a_j X^j \right\|_C < \|fg\|_C \quad . \tag{34}$$

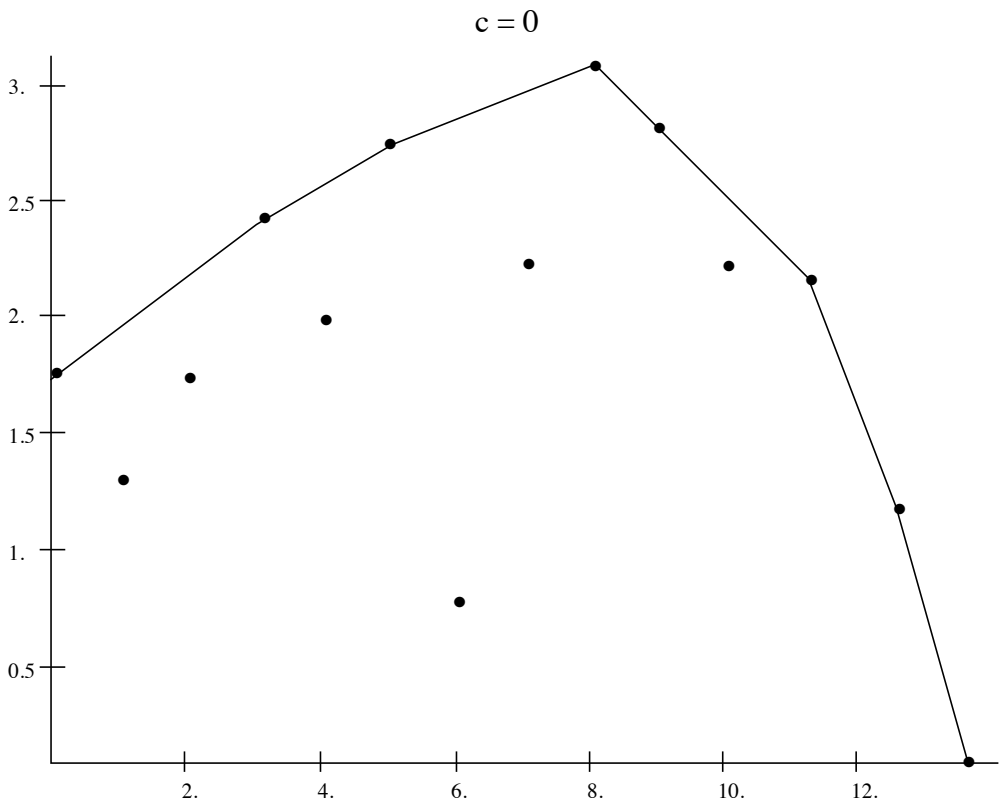

Figure 1

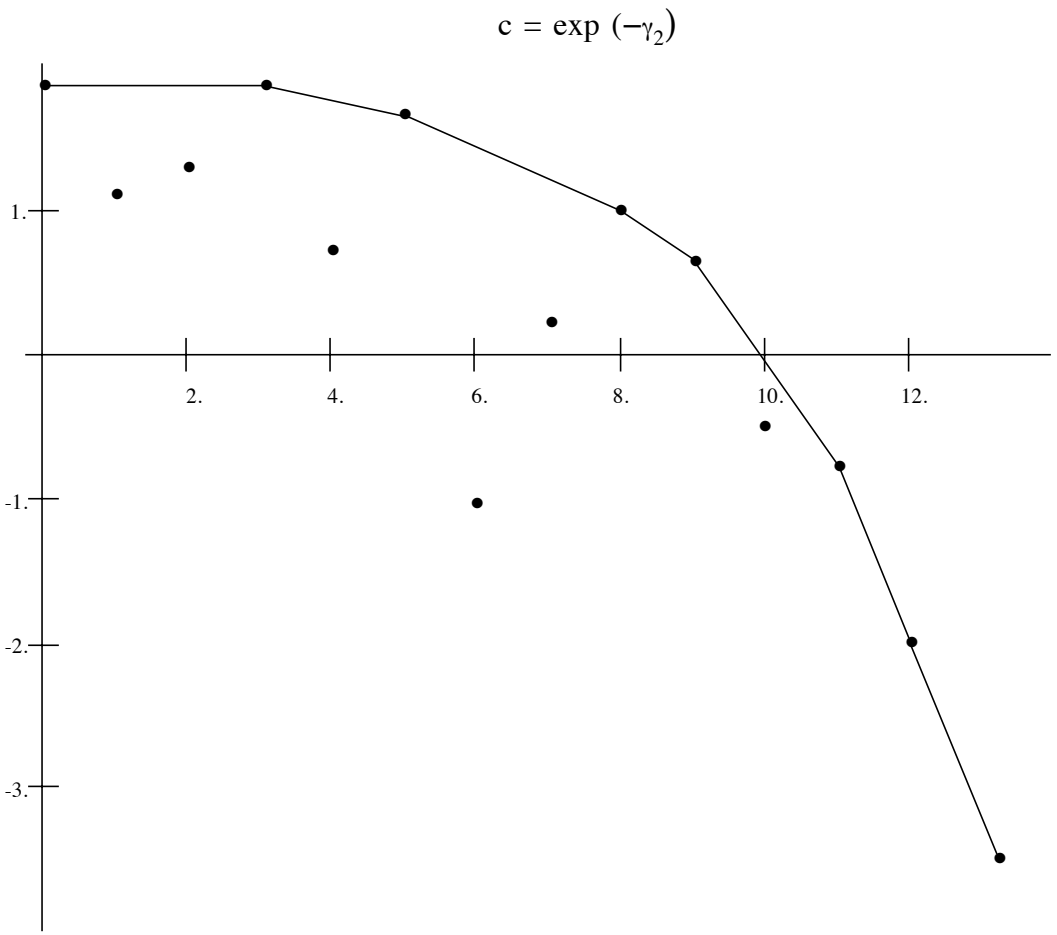

Figure 2

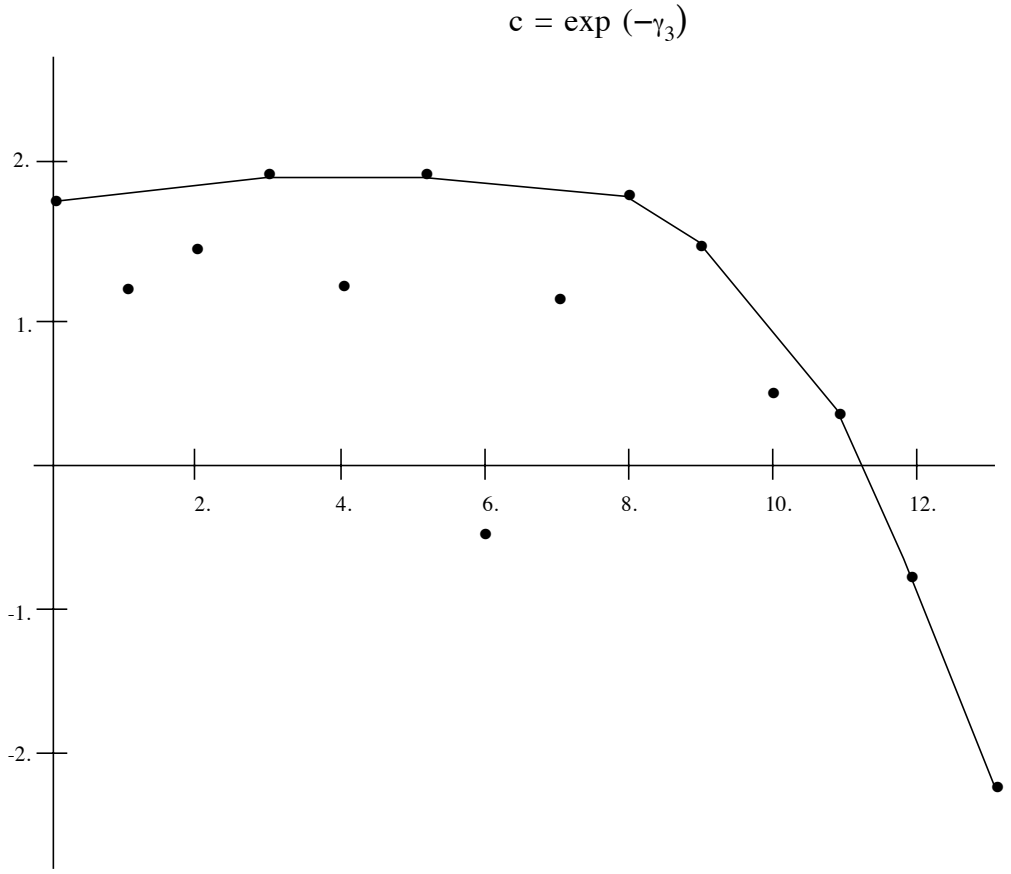

Figure 3

Similarly,

$$\|f(X)g(X) - a_n X^n g(X)\|_{C_g} < \|fg\|_{C_g} \quad .$$

Now, it is not difficult to see that, Equation (34) says that the first r line segments of the Newton Polygon of fg must have slope γ_j for $j = 0, 1, \ldots, r$ and the last equation says that the last line segment must have slope γ. ■

Now we would like to state the main result that we need concerning the Newton Polygon.

Theorem 2.3 ("Newton"). Let K be complete, and let

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in K[X]$$

with $a_0 \neq 0$ and $a_n \neq 0$. Suppose N with $0 < N < n$ such that

$$\begin{aligned} \|a_N X^N\| &= \|f\| \quad , \\ \|a_j X^j\| &< \|f\| \text{ for } j > N \end{aligned}$$

where $\| \ \| = \| \ \|_C$ for some C. Then there are $g, h \in K[X]$ with $\deg g = N$ and $\deg h = n - N$ and $f = gh$.

The proof of this result is very much in the spirit of the proof of Hensel's Lemma.

Proof. The hypothesis implies that there is a $\Delta < 1$ such that

$$\left\| f(X) - \sum_{j=0}^{N} a_j X^j \right\| = \Delta \|f\| \quad .$$

We are now going to recursively define two sequences of polynomials, $g_0, g_1, \ldots$ and $h_0, h_1, \ldots$ which converge to g and h respectively. These sequences will satisfy the following conditions:

$$\begin{aligned} \deg g_i &= N \quad , \\ \deg h_i &\leq n - N \quad , \\ \|f - g_i\| &\leq \Delta \|f\| \quad , \\ \|h_i - 1\| &\leq \Delta \quad . \end{aligned}$$

If we define δ_i by

$$\|f - g_i h_i\| = \delta_i \|f\| \quad ,$$

then δ_i measures how far off $g_i h_i$ is from the true factorization $f = gh$. We want $\lim_{i \to \infty} \delta_i = 0$. In any case our conditions on g_i and h_i tell us that $\delta_i \leq \Delta$. We will arrange it so that $\delta_{i+1} \leq \Delta \delta_i$, and since $\Delta < 1$, this will insure convergence.

We get started with

$$\begin{aligned} g_0(X) &= \sum_{j=0}^{N} a_j X^j \quad , \\ h_0(X) &= 1 \quad . \end{aligned}$$

Thus we start with $\delta_0 = \Delta$.

Now suppose we have g_i and h_i, and we want g_{i+1} and h_{i+1}. In order to conserve indices, we write $G = g_i$ and $H = h_i$ and

$$G(X) = b_0 + b_1 X + \cdots + b_N X^N \quad .$$

Since $\|f\| = \|a_N X^N\|$ and $\|f - G\| < \|f\|$, we must have $\|a_N X^N\| = \|b_N X^N\|$. Now if $\|b_i X^i\| > \|b_N X^N\|$, then we would have $\|f - G\| \geq \|(a_i - b_i)X^i\| = \|b_i X^i\| > \|a_N X^N\| = \|f\|$ which is a contradiction. Hence we have $\|G\| = \|b_N X^N\|$.

Let $D = f - GH$ and divide D by G obtaining $Q, R \in K[X]$ with $D = QG + R$ and $\deg Q \leq n - N$ and $\deg R < N$.

Claim. $\|Q\| \leq \delta_i$ and $\|R\| \leq \delta_i \|f\|$.

We have $\|D\| = \delta_i \|f\|$ and $\|G\| = \|f\|$ so if we can prove $\|Q\| \cdot \|G\| \leq \|D\|$, the first part of the claim will follow. Let $c_0, c_1, \ldots, c_{n-N}$ be the coefficients of Q. They are determined by the linear equations

$$b_N c_{n-N-j} + b_{N-1} c_{n-N-j+1} + \cdots + b_{N-j} c_{n-N} = d_{n-j} \tag{35}$$

where d_{n-j} is the coefficient of X^{n-j} in D, and j runs from 0 to $n - N$. We show

$$\|c_{n-N-j} X^{n-N-j}\| \cdot \|G\| \leq \|D\| \tag{36}$$

by induction on j. For $j = 0$, we get $b_N c_{n-N} = d_n$. Since we know that $\|G\| = C^N |b_N|$ and $\|D\| \geq C^n d_n$, the desired result follows (with equality) for $j = 0$.

Now assume we know (36) for $j-1$. Then we know that all of the terms in (35) except for the first one have absolute value $\leq |d_{n-j}|$. If the $|b_n c_{n-N-j}| > |d_{n-j}|$, this would contradict the fact that the absolute value of the whole sum $= |d_{n-j}|$. Hence we get inequality (36), and the first part of the claim follows.

The second part of the claim follows easily from the first part and the equation $D = QG + R$.

Now set $g_{i+1} = G + R (= g_i + R)$ and $h_{i+1} = H + Q (= h_i + Q)$. It is trivial to see that g_{i+1} and h_{i+1} satisfy the degree condition. The norm conditions follow from the claim, and it remains to show that $\delta_{i+1} \leq \Delta \delta_i$. We have

$$\begin{aligned}
\delta_{i+1}\|f\| &= \|f - g_{i+1} h_{i+1}\| \\
&= \|f - (G + R)(H + Q)\| \\
&= \|(f - GH) - RH - QG - RQ\| \\
&= \|D - (D - R) - RH - RQ\| \\
&= \|R(H - 1) + RQ\| \\
&\leq \max(\|R\| \cdot \|H - 1\|, \|R\| \cdot \|Q\|) \\
&\leq \max(\Delta \delta_i \|f\|, {\delta_i}^2 \|f\|) \\
&\leq \Delta \delta_i \|f\|
\end{aligned}$$

as desired. ∎

Remark. In the factorization $f = gh$ we can assume (if we so desire) that $h(0) = 1$ and that $\|h - 1\| < 1$ because we can replace h by $[h(0)]^{-1}h$.

The form in which we use the theorem is the following:

Corollary 2.5. An irreducible polynomial in $K[X]$ is pure.

Proof. Suppose f is not pure. Let

$$C = -\exp\left(\frac{1}{n}\ln\left|\frac{a_n}{a_0}\right|\right) \quad .$$

Picking this C insures that $\|a_0\| = \|a_n X^n\|$, *i.e.*, we can think of the line between P_0 and P_n in the Newton Polygon $\Pi(f)$ as being horizontal. Since the slopes of the line segments in $\Pi(f)$ always decrease, we can find an index N such that P_N is the rightmost "largest" of the P_i's. Then it is easy to see that with this C and N, f satisfies the hypothesis of the theorem, and so cannot be irreducible. ■

The next corollary is also sometimes referred to as "Newton's Theorem".

Corollary 2.6. Suppose that K is complete and that $f \in K[x]$ is of type $(*)$, *i.e.*, type $(\ell_1, \gamma_1; \ell_2, \gamma_2; \ldots; \ell_r, \gamma_r)$. Then f factors

$$f = g_1 \cdot g_2 \cdots g_r$$

where g_s is pure of type (ℓ_s, γ_s).

Proof. Write $f = \Pi h_\lambda$ as a product of irreducible polynomials. By Corollary 2.5 each h_λ is pure. If more than one of the h_λ's have the same slope, then by Exercise 2.2 their product is pure with the same slope. Continuing in this fashion, we can write

$$f = \prod_{\lambda=1}^{M} g_\lambda$$

for some M, and say g_λ is pure of type $(q_\lambda, \delta_\lambda)$ and $\delta_1 > \delta_2 > \cdots > \delta_M$. By Proposition 2.2 and a little induction, the type of Πg_λ must be $(q_1, \delta_1; q_2, \delta_2; \ldots; q_M, \delta_M)$ which must be the type of f. Hence $M = r$ and $q_i = \ell_i$ and $\delta_i = \gamma_i$ for $1 \le i \le r (= M)$. ■

Remark. There is another corollary of our theorem which tells us that f factors if we have a "good enough" approximate factorization. This says roughly that if $\delta = \|f - GH\|$ is less than $|R(G,H)|^2$ where $R(G,H)$ is the resultant of G and H, then $f = gh$ where $\deg g = \deg G$ and $\deg h = \deg H$. For a proof see [4, page 105].

3. Extensions of Valuations

Using the results of the previous section it is now relatively easy to show that we can extend a valuation (or absolute value) from a complete field to a finite extension.

Theorem 3.4. Let K be a field which is complete with respect to an absolute value $|\ |$, and let L be an extension of K of degree n. Define a map $\|\ \| : L \to \mathbb{R}$ by

$$\|x\| = |N_{L/K}x|^{1/n}$$

for $x \in L$. Then $\| \ \|$ is an absolute value on L which extends $| \ |$.

Proof. If $x \in K$, then by Proposition 5.8b, $N_{L/K}x = x^n$ so $\|x\| = |x|$ and $\| \ \|$ extends $| \ |$. Let $x, y \in L$. By Exercise 5.3b, $N_{L/K}xy = N_{L/K}x \cdot N_{L/K}y$ so $\|xy\| = \|x\| \cdot \|y\|$. We now want to show that $\|x + y\| \leq \max(\|x\|, \|y\|)$. Suppose $\|y\| \leq \|x\|$. Then if $z = y/x$, we have $\|z\| \leq 1$, it suffices to show that $\|z + 1\| \leq 1$. Let f_z and m_z be the characteristic and minimal polynomials of z respectively. Then by Theorem 5.4b $f_z = {m_z}^r$ for some $r > 0$. Write

$$f_z(X) = X^n + a_1 X^{n-1} + \cdots + a_0 \quad .$$

Then $|a_0| = |\pm N_{L/K}z| \leq 1$ since $\|z\| \leq 1$. Now by Corollary 2.5, since m_z is irreducible, it is pure. By Exercise 2.2, f_z is thereby pure. Hence $|a_i| \leq |a_0| \leq 1$.

Exercise 3.3. Show that $N_{L/K}(1 + z) = (-1)^n f_z(-1)$.

Therefore

$$\|1 + z\| = |f_z(-1)|^{1/n} \quad ,$$

and this is ≤ 1 since the coefficients of f_z have absolute value ≤ 1. ∎

We can now show that this extension of a valuation on a complete field is unique, but the proof really has little to do with the preceding material. The idea is that a finite extension L of K is a finite dimensional vector space over K, and a finite dimensional vector space over a complete field has a unique topology. Instead of using topology directly, we introduce the familiar notion of a norm on a vector space.

Definition 3.2. Let V be a vector space over a field K with valuation $| \ |$. A real valued function $\| \ \|$ on V is called a *norm* if the following conditions hold $\forall \vec{a}, \vec{b} \in V$ and $c \in K$:

i) $\|\vec{a}\| \geq 0$ and $\|\vec{a}\| = 0$ if and only if $\vec{a} = 0$.

ii) $\|\vec{a} + \vec{b}\| \leq \|\vec{a}\| + \|\vec{b}\|$.

iii) $\|c\vec{a}\| = |c| \cdot \|\vec{a}\|$.

Remark.

i) This "norm" is, of course, different from the "norm" from an extension down to the base field, but this is the usual terminology. The context usually makes clear which one is intended.

ii) A norm on V induces in the usual way a metric and thereby a topology on V. It should be clear that a norm on V lets us define cauchy sequences of points of V, and hence what it means for V to be complete.

Definition 3.3. Let $\| \ \|_1$ and $\| \ \|_2$ be norms on V. Then they are said to be *equivalent* if there are $C_1, C_2 \in \mathbb{R}$ such that $\|\vec{a}\|_1 \leq C_2\|\vec{a}\|_2$ and $\|\vec{a}\|_2 \leq C_1\|\vec{a}\|_1$.

Remark. It can be shown that equivalent norms induce the same topology on V.

Here is the main result for this situation.

Theorem 3.5. Suppose K is complete with respect to $|\ |$ and the V is a finite dimensional vector space over K. Then any two norms on V are equivalent, and V is complete with respect to any norm.

Proof. Let $\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n$ be a basis for V over K. For $\vec{a} \in K$ write

$$\vec{a} = a_1\vec{e}_1 + \cdots + a_n\vec{e}_n$$

where $a_i \in K$. We define a canonical norm on V by

$$\|\vec{a}\|_0 = \max_i |a_i| \quad .$$

It is easy to see that $\|\ \|_0$ is a norm and that V is complete with respect to it. Hence it suffices to show that any norm on V is equivalent to $\|\ \|_0$.

Let $\|\ \|$ be any norm on V. We must establish two inequalities. One is easy.

$$\begin{aligned} \|a\| &= \Big\| \sum_i a_i\vec{e}_i \Big\| \\ &\leq \sum_i |a_i| \cdot \|\vec{e}_i\| \\ &\leq C_0\|\vec{a}\|_0 \end{aligned}$$

where

$$C_0 = \sum_i \|\vec{e}_i\| \quad .$$

It remains to show that there is $C \in \mathbb{R}$ such that

$$\|\vec{a}\|_0 \leq C\|a\| \quad \forall \vec{a} \in V \quad . \tag{37}$$

Suppose not. We derive a contradiction by induction on the dimension n of V. Then $\forall \varepsilon > 0$ there is $\vec{b} = \vec{b}(\varepsilon) \in V$ such that

$$\|\vec{b}\| < \varepsilon\|\vec{b}\|_0 \quad .$$

By the definition of $\|\ \|_0$ we can assume that there is such a $\vec{b}$ with $\|\vec{b}\|_0 = |b_n|$. (Permute the $\vec{e}_i$ if necessary.) Now replace $\vec{b}$ by ${b_n}^{-1} \cdot \vec{b}$ so $\vec{b} = \vec{c} + \vec{e}_n$ where $\vec{c}$ is in the subspace W of V spanned by $\vec{e}_1, \ldots, \vec{e}_{n-1}$. In other words if (37) is false, we can find a sequence $\{\vec{c}_i\}$ of elements of W such that

$$\lim_{i\to\infty} \|\vec{c}_i + \vec{e}_n\| = 0 \quad .$$

By the triangle inequality,

$$\|(\vec{c}_i + \vec{e}_n) - (\vec{c}_j + \vec{e}_n)\| \leq \|\vec{c}_i + \vec{e}_n\| + \|\vec{c}_j + \vec{e}_n\|$$

so

$$\lim_{i,j\to\infty} \|\vec{c}_i - \vec{c}_j\| = 0 \quad .$$

Since the dimension of W is less than the dimension of V, by induction we get $\vec{c} \in W$ such that

$$\lim_{i \to \infty} \|\vec{c}_i - \vec{c}\| = 0 \quad .$$

This implies

$$\|\vec{c} + \vec{e}_n\| = \lim_{i \to \infty} \|\vec{c}_i + \vec{e}_n\| = 0 \quad .$$

But $\vec{e}_n$ is certainly not in W so $\vec{c} + \vec{e}_n \neq 0$ and we get our contradiction. Hence $\| \|_0$ and $\| \|$ are equivalent. ∎

Now we can easily prove the uniqueness of the extension of a valuation on a complete field.

Corollary 3.7. Let K be a field which is complete with respect to an absolute value $| |$, and let L be a finite extension of K. Then there is a unique extension of $| |$ to L, and L is complete with respect to this extension.

Proof. Theorem 2.4 tells us that there is an extension. If we regard L as a finite dimensional vector space over K, then it is trivial to see that the extension of the absolute value defines a norm on L. If we had two extensions of the absolute value to L, then by the theorem they would be equivalent as norms on L.

Exercise 3.4. Show that any two equivalent norms on L which agree on K are identical.

The statement about the completeness of L follows immediately from the completeness of the norm on L. ∎

We need one more trivial fact before we can prove the required result concerning extensions in the noncomplete case.

Proposition 3.3. Let K be a complete field with respect to an absolute value. Then there is a unique extension of the absolute value to $\bar{K}$, the algebraic closure of K.

Proof. Let $a \in \bar{K}$. We know that a is algebraic over K so the extension $K(a)$ is finite over K. By Corollary (2.7) the absolute value on K extends uniquely to $K(a)$ and hence uniquely to $\bar{K}$. ∎

We can now prove Theorem 8.12b. We restate it here in a slightly different form.

Theorem 3.6. Let $L = K(x)$ be a finite separable extension of K and let $| |$ be an absolute value on K. Let $\bar{K}$ be the completion of K with respect to $| |$. Let m_x be the minimal polynomial of x. Suppose

$$m_x = \varphi_1 \varphi_2 \cdots \varphi_r$$

is the factorization of m_x into (nonconstant) irreducibles in $\bar{K}[X]$.

Then the φ_i's are distinct. Let $L_i = \bar{K}(y_i)$ where y_i is a root of φ_i. Then there is a monomorphism

$$I_i : L = K(x) \hookrightarrow L_i = \bar{K}(y_i)$$

which extends the monomorphism $K \hookrightarrow \bar{K}$ under which $x \mapsto y_i$. We know that the absolute value $| |$ extends uniquely to $\bar{K}$ and thence since $\bar{K}$ is complete, uniquely to $\bar{K}(y_i) = L_j$. Using the monomorphism I_i, this defines an extension

of $|\ |$ to L which we denote by $|\ |_i$. Then the absolute values $|\ |_1, |\ |_2, \ldots, |\ |_r$ are precisely all of the extension of $|\ |$ to L. Furthermore L_i is the completion on L with respect to $|\ |_i$.

Proof. (As Cassels' remarks, the proof is shorter than the statement.) Let $\|\ \|$ be any extension of $|\ |$ to L, and let $\bar{L}$ be the completion of L with respect to it. Then we have $\bar{K} \subset \bar{L}$ and $x \in L \subset \bar{L}$. By Corollary 2.7 $\bar{K}(x)$ is complete so we must have $\bar{K}(x)$ isomorphic to $\bar{L}$ say by I. Clearly I leaves K fixed. Let $y = I(X)$, and let m_y be the minimal polynomial for y over $\bar{K}$. Since $m_x(x) = 0$, and $I(m_x) = m_x$ since $m_x \in K[X]$, we have $m_x(y) = 0$ so $m_y | m_x$. Hence m_y is one of the φ_i's as desired.

Going in the other direction, let y_i be a root of φ_i. Then $m_x(y_i) = 0$ so the extensions $K(x) = L$ and $k(y_i) \subset \bar{k}(y_i) = L_i$ are isomorphic, and we are reduced to the above situation.

It remains to show that the φ_i are distinct. If not, m_x and $m_x{}'$ would have a common factor in $\bar{K}[X]$. Now we can determine this common factor by the euclidean algorithm, so it must lie in $K[X]$, but this contradicts the fact that m_x is irreducible and separable. ∎

References

[1] Emil Artin. Galois theory, *Notre Dame Mathematical Lectures*, 2, 1957.

[2] Emil Artin. *Algebraic Numbers and Algebraic Functions*, Nelson, London, 1968.

[3] Nicolas Bourbaki. *Commutative Algebra*, Hermann, Paris, 1972.

[4] J. W. S. Cassels. *Local Fields*, Cambridge Press, 1986.

[5] Leonard S. Charlap and David P. Robbins. An elementary introduction to elliptic curves, CRD Expository Report No. 31, December 1988. IDA-CCR Log No. 82299.

[6] William Fulton. *Algebraic Curves*, W. A. Benjamin, 1969.

[7] Shigeru Iitaka. *Algebraic Geometry*, Springer-Verlag, 1982.

[8] Burt S. Kaliski. Elliptic curves and cryptography: A pseudorandom bit generator and other tools, MIT/LSC/TR-411, 1988. Cambridge.

[9] Keith Kendig. *Elementary Algebraic Geometry*, Springer-Verlag, 1977.

[10] Serge lang. *Algebra*, Addison-Wesley, 1965.

[11] Paul J. McCarthy. *Algebraic Extensions of Fields*, Blaisdell, 1966.

[12] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.*, 44:483–494, 1985.

[13] Jean-Pierre Serre. *Groupes Algébriques et Corps de Classes*, Hermann, 1959. Paris.

[14] Jean-Pierre Serre. *Local Fields*, Springer-Verlag, 1979.

[15] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[16] Edwin Weiss. *Algebraic Number Theory*, McGraw-Hill, 1963.

[17] Oscar Zariski and Pierre Samuel. *Commutative Algebra*, Van Nostrand, 1958.

Keywords

`curve, elliptic, isogeny, map, pair, rational, reciprocity, Weil`