RATIONAL FORMAL GROUPS

RATIONAL FORMAL GROUP LAWS

By

ROBERT BISMUTH, B.Sc.

A Thesis

Submitted to the School of Graduate Studies

in Partial Fulfilment of the Requirements

for the Degree

Master of Science

McMaster University

(March 1976)

MASTER OF SCIENCE (1976) McMASTER UNIVERSITY
(Mathematics) Hamilton, Ontario.

TITLE: Rational Formal Group Laws

AUTHOR: Robert Bismuth, B.Sc. (Hons.) (University of Wales)

SUPERVISOR: Dr. T.M.K. Davison

NUMBER OF PAGES: 102 , vii .

ABSTRACT:

This thesis is concerned with the general form of those one dimensional formal group laws over any field $\underline{A}$ which are given as rational functions over $\underline{A}$. After having determined an exact expression for any rational function which is a formal group law over $\underline{A}$, an investigation is made into the category whose objects are the rational formal group laws over $\underline{A}$, and, whose morphisms are just their formal group morphisms which are given by rational functions. The isomorphism-classes of this category are then completely determined, and, are shown to be essentially equivalent to the classes of congruent quadratic forms over $\underline{A}$, provided, of course, that the characteristic of $\underline{A}$ is different from two.

Finally, we generalize most of the results in the case of fields to the case of semi-prime rings, making a suitable definition of a rational formal group law over a semi-prime ring. In particular, we show that semi-primeness determines, and, is determined by, the general form of rational formal groups over commutative rings with unit.

PREFACE:

An attempt has been made while writing this thesis to make the material covered, and, the results produced, accessible to those readers with only a slight knowledge of the theory of rings, and, the theory of categories. For their benefit, and to make the thesis as self contained as possible, most of the specialized background, from ring and category theory, which is needed to understand the significance of formal group laws, has been included, and, can be found in the two appendices.

The first chapter introduces the concept of a formal group law, and, the few results which shall be needed in later discussions. Chapter two is the core of the thesis: it is here that the main result is proven, which is later generalized in chapter four. In chapter three, this result is then used extensively in the investigation of a certain naturally arising subcategory of the category of formal group laws over an arbitrary field.

The notation used in the thesis which differs from standard mathematical notation, will be defined as it is used.

ACKNOWLEDGEMENTS:

I wish to thank everyone with whom I came into contact in the preparation and writing of this thesis: their valuable comments and overwhelming patience have been more than welcome. In particular, the faculty and secretaries of the Department of Mathematics deserve special thanks, as, without them, I would never have been able to fully complete my work. Naturally, the greatest part of my thanks is reserved for my supervisor, Dr. T.M.K. Davison. Both his energetic enthusiasm towards mathematics, and, his deep insight, not to mention his kind patience, served to stimulate, and, to maintain my mathematical curiosity while investigating the various problems discussed in this thesis.

TABLE OF CONTENTS:

SYMBOL TABLE:

$R[[X_1,\ldots,X_n]]$	– the ring of formal power series over a ring R in the indeterminates $X_1,\ldots,X_n$.
$R[X_1,\ldots,X_n]$	– the subring of polynomials contained in the above ring.
ord( )	– the order filtration of a formal power series ring.
$\underline{A}(X)$	– the field of rational functions in the indeterminate X over the field $\underline{A}$.
$\underline{A}(X,Y)$	– the field of rational functions in two indeterminates over the field $\underline{A}$.
$\Omega(\underline{A})$	– the algebraic closure of the field $\underline{A}$.
$\underline{Fml}(R)$	– the category of all formal group laws over the ring R .
$Fg(R)$	– the category of all one dimensional formal group laws over R .
$Rat(R)$	– the category of all rational formal group laws over R .
$\underline{CAlg}\ R)$	– a category of complete R-algebras defined in §1.1 .
$\underline{FP}(R)$	– a category of formal power series rings over R , filtered with respect to the order filtration, defined in §1.1 .
$\mathbb{R}$	– the field of real numbers.
$\underline{Z}$	– the ring of integers.
$\underline{N}$	– the set of positive integers.
$\underline{N}_0$	– the set of non-negative integers.

CHAPTER 1: GENERAL THEORY OF FORMAL GROUPS.

§1.1 The Categories in Question:

Throughout this chapter, let R denote a commutative ring, with unit.

Denote by $\underline{CAlg}(R)$ the category whose objects are all the complete and Hausdorff filtered R-algebras (see Appendix B for the appropriate definitions), which contain R as a subring, and, whose morphisms are those continuous R-algebra homomorphisms satisfying:

Property 1.1.1: Given two R-algebras in $\underline{CAlg}(R)$, S and S', with filtrations ν and ν' respectively, then a continuous R-algebra homomorphism,

$$\theta : S \longrightarrow S' ,$$

is a morphism in $\underline{CAlg}(R)$ iff:

For all $s \in S$ with $\nu(s) > 0$, we have: $\nu'(\theta(s)) > 0$.

Now let $\underline{FP}(R)$ denote the full subcategory of $\underline{CAlg}(R)$ whose objects are the Formal Power Series rings over R, each considered filtered with respect to the order filtration.

Remarks: i. R itself is obiously an object of $\underline{FP}(R)$, the filtration being the discrete filtration.

ii. The objects of $\underline{FP}(R)$ are just the free, complete R-algebras on finitely many generators. Since all the morphisms here satisfy Property I.1.1, Proposition B.3.1 guarantees the universal property of free objects: a morphism is uniquely determined by the image of the generators under its action.

These remarks directly imply:

Proposition 1.1.2: i. R is a zero object for the category $\underline{FP}(R)$, and,

ii. $\underline{FP}(R)$ has all finite coproducts, in particular,

$$R((X_1,\ldots,X_n)) \amalg R((Y_1,\ldots,Y_m)) \cong R((X_1,\ldots,X_n,Y_1,\ldots,Y_m)).$$

Proof: i. Given an object of $\underline{FP}(R)$, $R\langle(X_1,\ldots,X_n)\rangle$, then we have two morphisms of $\underline{FP}(R)$:

$$i : R \longrightarrow R\langle(X_1,\ldots,X_n)\rangle ,$$

the inclusion of R, and:

$$\varepsilon : R\langle(X_1,\ldots,X_n)\rangle \longrightarrow R ,$$

the augmentation map.

Clearly, as we are dealing with R-algebra homomorphisms, the map i is unique. On the other hand, the augmentation ε is unique in view of Property 1.1.1. Hence, R is a zero object in $\underline{FP}(R)$.

ii. As we are dealing with free objects, the proof of ii. is immediate.

∎

NOTE: For the remainder of this chapter, we shall adopt the notation of Appendix B and let the symbol R_k represent the ring of formal power series in k indeterminates ($k > 0$) over R. The precise indeterminates of R_k shall be indicated only if they are not clearly indicated by context.

§1.2 Formal Group Laws over R :

Since we have shown that $\underline{FP}(R)$ has an initial object, and all finite coproducts, we may consider arbitrary cogroups in $\underline{FP}(R)$ (see Appendix A for the general background material).

Suppose that (R_n, c, η, a) is a cogroup in $\underline{FP}(R)$.

The map,

$$c : R_n \longrightarrow R_{2n} ,$$

is completely determined by the following vector of n formal power series in 2n indeterminates:

$$F(X,Y) = (F_1(X,Y),\ldots,F_n(X,Y))$$

where: X,Y are the obvious abbreviations for the indeterminates $X_1,\ldots,X_n$ and, $Y_1,\ldots,Y_n$ respectively, and, for all i, $1 \leq i \leq n$,

$$F_i(X,Y) = c(X_i) \quad .$$

Now, by Proposition B.3.3, with the obvious notation, for any $G(X) \in R_n$,

$$c(G(X)) = G(F(X,Y)) \quad ,$$

and so it follows immediately from the co-associativity of c that:

$$F(X,F(Y,Z)) = F(F(X,Y),Z) \quad ,$$

where, X,Y,Z are the abbreviations for the indeterminates of R_{3n} , $X_1,\ldots,X_n$, $Y_1,\ldots,Y_n$ and $Z_1,\ldots,Z_n$ respectively.

Since R is actually a zero object in $\underline{FP}(R)$, the map,

$$\eta : R_n \longrightarrow R \quad ,$$

must be the augmentation map, ε . Hence, the commutative diagram:

$$\begin{array}{ccc} R_n & & \\ \downarrow c & \searrow \cong & \\ R_{2n} & \xrightarrow[1 \amalg \varepsilon]{} & R_n \amalg R \end{array}$$

implies, for $1 \leq i \leq n$,

$$X_i = F_i(X_1,\ldots,X_n,\varepsilon(Y_1),\ldots,\varepsilon(Y_n)) \quad ,$$

ie. $$X_i = F_i(X_1,\ldots,X_n,0,\ldots,0) \quad .$$

With the obvious notation, this shows that,

$$F(X,0) = X \quad ,$$

and, similarly,

$$F(0,Y) = Y \quad .$$

Lastly, the antipodism map,

$$a : R_n \longrightarrow R_n \quad ,$$

is uniquely determined by the vector of n formal power series in n indeterminates,

$$T(X) = (T_1(X),\ldots,T_n(X))$$

where, for $1 \leq i \leq n$,

$$T_i(X) = a(X_i)$$

Chasing around the commutative diagram:

$$\begin{array}{ccc} R_n & \xrightarrow{\varepsilon} & R \\ {\scriptstyle c}\downarrow & & \downarrow{\scriptstyle i} \\ R_{2n} & \xrightarrow[(1,a)]{} & R_n \end{array}$$

shows us that:

$$F(X,T(X)) = 0 \qquad \text{(ie. the zero n-tuple.)}.$$

A similar arguement shows that:

$$F(T(Y),Y) = 0$$

Note: $T(X)$ is the unique vector of formal power series with this property.

Summing up the above discussion, we have shown:

Lemma 1.2.1: Given a cogroup (R_n,c,η,a) in the category $\underline{FP}(R)$, then there is a unique vector of n formal power series in 2n indeterminates over R, $F(X,Y) = (F_1(X,Y),\ldots,F_n(X,Y))$, determined by (R_n,c,η,a), satisfying: i. $F(X,0) = X$, and, $F(0,Y) = Y$; and,

ii. $F(X,F(Y,Z)) = F(F(X,Y).Z)$

Furthermore, there exists a unique vector of n formal power series in n indeterminates over R,

$$T(X) = (T_1(X),\ldots,T_n(X)),$$

such that:

iii. $F(X,T(X)) = 0$, and, $F(T(Y),Y) = 0$.

———∎———

Definition: a formal group law of dimension n over R is a vector of n formal power series over R in 2n indeterminates, $X_1,\ldots,X_n,Y_1,\ldots,Y_n$, each with zero constant term,

$$F(X,Y) = (F_1(X,Y),\ldots,F_n(X,Y)),$$

satisfying:

$$\text{i. } F(X,0) = X \text{ , and, } F(0,Y) = Y \text{ , and,}$$

$$\text{ii. } F(X,F(Y,Z)) = F(F(X,Y),Z)$$

Note: in the above, the symbols X,Y and Z are to be interpreted in the obvious fashion, as vectors of indeterminates.

If, in addition to the above, $F(X,Y)$ satisfies:

$$F(X,Y) = F(Y,X) \text{ ,}$$

then we say that the formal group law $F(X,Y)$ is commutative.

We have immediately:

Lemma 1.2.2: If $F(X,Y)$ is a formal group law of dimension n over R, then there exists a vector of n formal power series over R in n indeterminates,

$$T(X) = (T_1(X),\ldots,T_n(X)) \text{ ,}$$

such that,

$$F(X,T(X)) = 0 \text{ , and, } F(T(Y),Y) = 0 \text{ .}$$

Furthermore, such a vector $T(X)$ is unique.

Proof: Let,

$$G_i(X,Y) = X_i - F_i(X,Y) \text{ , for } i,\ 1 \leq i \leq n \text{ .}$$

Then, since:

$$F(X,0) = X \text{ , and, } F(0,Y) = Y \text{ ,}$$

$$\text{ie. } F_i(X,Y) \equiv X_i + Y_i \mod \text{degree } 2 \text{ , } 1 \leq i \leq n$$

we see that $G_i(X,Y)$ has zero constant term, when considered as a formal power series in the indeterminates $Y_1,\ldots Y_n$ over the ring:

$$R((X_1,\ldots,X_n)) \text{ .}$$

Obviously,

$$\left.\frac{\partial G_i}{\partial Y_k}\right|_{Y=0} = -\delta_{ik} \text{ , } 1 \leq i \leq n \text{ , } 1 \leq k \leq n \text{ ,}$$

so that:

$$\det\left[\left.\frac{\partial G_i}{\partial Y_k}\right|_{Y=0}\right] = (-1)^n$$

Hence, by Corollary B.4.2 (the Inverse Function Theorem), there exist n formal power series,

$$H_j(X,Y) \quad , \quad 1 \leqslant j \leqslant n \quad ,$$

such that:

$$Y_i = G_i(X,H(X,Y)) \quad , \quad 1 \leqslant i \leqslant n \quad ,$$

where, $H(X,Y)$ denotes the vector of formal power series:

$$H(X,Y) = (H_1(X,Y),\ldots,H_n(X,Y)) \quad .$$

Put: $Y_i = X_i \quad , \; 1 \leqslant i \leqslant n \; .$

Then, we have:

$$X_i = G_i(X,H(X,X)) \quad , \quad 1 \leqslant i \leqslant n \quad ,$$

$$= X_i - F_i(X,H(X,X)) \; .$$

Thus, the required result follows immediately upon taking:

$$T(X) = H(X,X)$$

Uniqueness now follows directly from the formal associativity of $F(X,Y)$.

Lemma 1.2.1, together with Lemma 1.2.2, implies: ——□——

Proposition 1.2.3: There is a bijection between the set of formal group laws of dimension n over R , and, the set of cogroup structures in the category $\underline{CAlg}(R)$ on the object R_n .

——□——

Note: Since $\underline{FP}(R)$ is a full subcategory of $\underline{CAlg}(R)$, a cogroup in $\underline{FP}(R)$ is also a cogroup in $\underline{CAlg}(R)$.

Let $F(X,Y)$ and $G(W,Z)$ be two formal group laws over R, of dimensions n and m respectively. Denote their associated cogroups (via the bijection of Proptn. 1.2.3) by:

$$C_F = (R_n, c_F, \varepsilon_n, a_F) \quad , \text{ and, } \quad C_G = (R_m, a_G, \varepsilon_m, a_G) \quad .$$

By definition, a morphism,

$$\theta : C_F \longrightarrow C_G \quad ,$$

in the category of $\underline{FP}(R)$ cogroups, is a morphism,

$$\theta \in \mathrm{Hom}_{\underline{CAlg}(R)}(R_m, R_n) \quad ,$$

for which the diagram:

$$\begin{array}{ccc} R_n & \xleftarrow{\theta} & R_m \\ {\scriptstyle C_F}\downarrow & & \downarrow{\scriptstyle C_G} \\ R_{2n} & \xleftarrow[\theta \sqcup \theta]{} & R_{2m} \end{array} \quad , \quad \text{commutes.}$$

Put:

$$f_i(X_1, \ldots, X_n) = \theta(W_i) \quad \text{for } 1 \leq i \leq m \quad ,$$

where, the $X_1, \ldots, X_n$ are the indeterminates of R_n, and, the $W_1, \ldots W_m$ those of R_m. Define a vector,

$$f(X) = (f_1(X), \ldots, f_m(X)) \quad ,$$

of m formal power series in n indeterminates over R.

Chasing around the above diagram, and recalling that the continuity of the maps involved gives, in the usual notation,

$$C_F(\theta(W)) = f(F(X,Y)) \quad , \quad \text{and,}$$

$$\theta \sqcup \theta(C_G(W)) = G(f(X), f(Y)) \quad ,$$

we see immediately that:

$$f(F(X,Y)) = G(f(X), f(Y)) \quad .$$

Conversely, given any vector,

$$g(X) = (g_1(X),\ldots,g_m(X)) \quad ,$$

of m formal power series in n indeterminates over R , each with zero constant term, satisfying:

$$g(F(X,Y)) = G(g(X),g(Y)) \quad , \qquad \text{(*)}$$

then the vector g(X) determines a unique map, in the category FP(R),

$$\theta_g : R_m \longrightarrow R_n \quad ,$$

with, for $1 \leq i \leq m$,

$$\theta_g(W_i) = g_i(X) \quad ,$$

and we have the commutative square:

$$\begin{array}{ccc} R_m & \xrightarrow{\theta_g} & R_n \\ {\scriptstyle C_G}\downarrow & & \downarrow{\scriptstyle C_F} \\ R_{2m} & \xrightarrow[\theta_g \cup \theta_g]{} & R_{2n} \end{array}$$

Hence, the vector of formal power series g(X) , determines a morphism θ_g in the category of FP(R) cogroups.

We may now define the category of all formal group laws over to be: the category Fml(R) whose objects consist of the formal group laws defined over the ring R , and, for any two formal group laws over R , F(X,Y) and G(W,Z) of dimensions n and m respectively, a morphism,

$$f : F(X,Y) \longrightarrow G(W,Z) \quad ,$$

in the category Fml(R) is a vector of m formal power series in n indeterminates, each with zero constant term, which satisfies condition (*) above.

The above discussion has shown,

Theorem 1.2.4: There is a natural isomorphism between the category of FP(R) cogroups and the category of all formal group laws over R, Fml(R).

We have the following important consequence:

Corollary 1.2.5: i. For any object S of $\underline{CAlg}(R)$, a formal group law $F(X,Y)$, of dimension n over R, defines a group structure on:

$$\mathrm{Hom}_{\underline{CAlg}(R)}(R_n,S) \quad .$$

Denoting the group operation by: $*_F$,

for $\phi,\psi \in \mathrm{Hom}_{\underline{CAlg}(R)}(R_n,S)$, $\phi *_F \psi$ is specified by:

$$\phi *_F \psi(X_i) = F(\phi(X_1),\ldots,\phi(X_n),\psi(X_1),\ldots,\psi(X_n)) \quad .$$

ii. If T is any object of $\underline{CAlg}(R)$ then, for all,

$$\gamma \in \mathrm{Hom}_{\underline{CAlg}(R)}(S,T) \quad ,$$

we have:

$$\gamma \circ (\phi *_F \psi) = (\gamma\circ\phi) *_F (\gamma\circ\psi) \quad .$$

iii. If $G(W,Z)$ is another formal group law over R, of dimension m, then, given a morphism in $\underline{Fml}(R)$,

$$f : G(W,Z) \longrightarrow F(X,Y) \quad ,$$

for all $\xi,\zeta \in \mathrm{Hom}_{\underline{CAlg}(R)}(R_m,S)$, we have,

$$(\xi *_G \zeta)\circ\theta_f = (\xi\circ\theta_f) *_F (\zeta\circ\theta_f) \quad ,$$

where θ_f is the continuous ring homomorphism associated to the morphism f (by the above Theorem).

iv. With $G(W,Z)$ as above, and, assuming $F(X,Y)$ to be commutative, $\mathrm{Hom}_{\underline{Fml}(R)}(G,F)$ has the structure of an abelian group, and, is canonically isomorphic to a subgroup of the group, $\mathrm{Hom}_{\underline{CAlg}(R)}(R_n,R_m)$.

Proof: The above Corollary follows directly from the various definitions involved, together with the elementary properties of cogroups, discussed in Appendix A.

—Q—

§1.3 Commutative Formal Group Laws:

Throughout this section let $F(X,Y)$ denote a commutative formal group law, of dimension $n>1$, over, and, denote its formal inverse by the vector,

$$T(X) = (T_1(X),\ldots,T_n(X)) \quad ,$$

of n formal power series in n indeterminates over R ,

ie. $F(X,T(X)) = 0$.

Writing,

$$\mathrm{End}_{\underline{\mathrm{Fml}}(R)}(F) = \mathrm{Hom}_{\underline{\mathrm{Fml}}(R)}(F,F) \quad ,$$

Corollary 1.2.5 immediately gives:

Proposition 1.3.1: $\mathrm{End}_{\underline{\mathrm{Fml}}(R)}$ is a ring, additive structure given by $F(X,Y)$, and, ring multiplication given by composition of morphisms. This ring has the obvious multiplicative identity given by:

$$1_F \in \mathrm{End}_{\underline{\mathrm{Fml}}(R)}(F) \quad .$$

Proof: Trivial in the light of Corollary 1.2.5. ∎

Since the ring of integers $\underline{Z}$ is an initial object in the category of all rings with identity, we have a unique ring homomorphism,

$$\underline{Z} \longrightarrow \mathrm{End}_{\underline{\mathrm{Fml}}(R)}(F) \quad ,$$

given by,

$$m \longrightarrow (m)_F \quad ,$$

where:

$$(m)_F(X) = \begin{cases} X & \text{for} \quad m = 1 \quad , \\ T(X) & \text{for} \quad m = -1 \quad , \\ F(X,(m-1)_F) & \text{otherwise.} \end{cases}$$

It now follows, immediately, that:

Proposition 1.3.2: i. For $F(X,Y)$ and $G(W,Z)$ any two commutative formal group laws over R , $\mathrm{Hom}_{\underline{\mathrm{Fml}}(R)}(F,G)$ is a left $\mathrm{End}_{\underline{\mathrm{Fml}}(R)}(G)$-module, and a right $\mathrm{End}_{\underline{\mathrm{Fml}}(R)}(F)$-module .

ii. If $f \in \mathrm{Hom}_{\underline{Fml}(R)}(F,G)$, then:

$$f \circ (m)_F = (m)_G \circ f \quad , \text{ for all } m \in \underline{Z} .$$

Note: the composition above means composition component-wise for the vectors $f(X)$ and $(m)_F(X)$.

Proof: Trivial. ∎

Remark: If the dimension of both F and G above is 1, and, R is a field of characteristic 0, then it can be shown (Fröhlich[3]) that a formal power series, $h(X) \in R((X))$ is a morphism from F to G in $\underline{Fml}(R)$ iff: for some $q \in \underline{Z}$, $q \neq \pm 1$, $h \circ (q)_F = (q)_G \circ h$, and, $h(0) = 0$.

§1.4 1-Dimensional Formal Group Laws over a Semi-Prime Ring:

In this section we shall assume that the ring R is a semi-prime ring, ie. the ring R has no nilpotent elements, or, equivalently, the intersection of all the prime ideals of R is the zero ideal.

Let $F(X,Y)$ be any arbitrary formal group law of dimension 1 over R, ie. $F(X,Y)$ is just a formal power series in two indeterminates, X and Y,

$$F(X,Y) = \sum_{i,j=0}^{\infty} a_{ij} X^i Y^j \quad ; \quad a_{ij} \in R \quad , \quad i,j \geq 0 .$$

If $t(X) \in R((X))$ is the formal inverse of $F(X,Y)$, put:

$$t(X) = -X + \sum_{i=2}^{\infty} b_i X^i \quad ; \quad b_i \in R \quad , \quad i \geq 2 .$$

Set, $I = \ker(\varepsilon)$, where,

$$\varepsilon : R((X,Y,Z)) \longrightarrow R ,$$

is the augmentation map, ie. I is just the set of formal power series in one indeterminate over R with zero constant term.

Theorem 1.4.1: $F(X,Y)$ is actually a commutative formal group law,

ie. $F(X,Y) = F(Y,X)$

Proof: (Lazard [4]) For all formal power series $u,v \in I$, define a binary operation on the set I by:

$$u * v = F(u,v)$$

Now, clearly:

$$t(u) = -u + \sum_{i=2}^{\infty} b_i (u)^i \quad , \qquad \text{——————(1)}$$

and,

$$u * t(u) = 0 \quad ,$$

so that, by virtue of the properties of $F(X,Y)$ as a formal group law, the operation $*$ defines a group structure on the set I.

Let $h(u,v)$ denote the commutator product of u with v,

ie. $h(u,v) = u * v * t(u) * t(v)$

Since the indeterminates X and Y are elements of I, we may consider $h(X,Y)$, which is clearly a formal power series in X and Y alone, say:

$$h(X,Y) = \sum_{i,j=0}^{\infty} c_{ij} X^i Y^j \qquad \text{——————(2)}$$

Obviously: $F(X,Y)$ is commutative iff $c_{ij} = 0$ for all $i,j \geq 0$,

and so, it will suffice to show that:

$$h(X,Y) = 0$$

For each $u,v \in I$, let,

$$u^v = v * u * t(v) = h(v,u) * u$$

With this notation, Hall's identity for the inner automorphisms of groups gives:

$$h(h(X,Y),Z^Y) * h(h(Y,Z),X^Z) * h(h(Z,X),Y^X) = 0 \qquad \text{——————(3)}$$

In order to analyze this relationship, first define a lexicographic ordering of the monomials of I:

given two monomials $c \cdot X^i \cdot Y^j \cdot Z^k$ and $c' \cdot X^{i'} \cdot Y^{j'} \cdot Z^{k'}$ then define:

$$c \cdot X^i \cdot Y^j \cdot Z^k < c' \cdot X^{i'} \cdot Y^{j'} \cdot Z^{k'} \quad \text{iff,}$$

$i' - i > 0$, $j' - j > 0$, $k' - k > 0$, and, $c \neq 0$, $c' \neq 0$.

Assume, for a contradiction, that:

$$h(X,Y) \neq 0 \quad ,$$

ie. $c_{ij} \neq 0$ for some $i,j \geq 0$ (equation 2 above).

Let α be the smallest integer such that:

$$c_{\alpha j} \neq 0 \quad \text{for some } j \geq 0 \quad ,$$

and, let β be the smallest integer such that:

$$c_{\alpha\beta} \neq 0 \quad .$$

Obviously, $h(X,0) = h(0,Y) = 0$,

so that: $c_{0j} = c_{j0} = 0$, for all $j \geq 0$.

Hence, $\alpha \geq 1$, $\beta \geq 1$.

We shall show that the left Hand side of equation (3) contains the non-zero monomial,

$$-(c_{\alpha\beta})^{\beta+1} \cdot X^{\alpha} \cdot Y^{\alpha\beta} \cdot Z^{\beta^2} \quad ,$$

of minimal rank with respect to the ordering above.

Note that $c_{\alpha\beta} \neq 0$ implies that $(c_{\alpha\beta})^{\beta+1} \neq 0$ only because we have assumed R to be a semi-prime ring!

In this fashion, we shall obtain a contradiction to our choice of α,β and, the required result will follow immediately.

Before we can show the existence of this monomial, we first need to prove the following lemma:

Lemma: for all $i<\alpha$ and all $j \geq 0$, $c_{ij} + c_{ji} = 0$.

Proof: By equation (1) above,

$$h(Y,X) = t(h(X,Y)) = -h(X,Y) + \sum_{k=2}^{\infty} b_k \cdot (h(X,Y))^k$$

Clearly, all the monomials in the expansion of

$$\sum_{k=2}^{\infty} b_k \cdot (h(X,Y))^k \quad ,$$

have degree in X alone at least 2α.

Hence,

$$h(Y,X) \equiv -h(X,Y) \quad \text{mod degree } \alpha+1 \text{ in } X .$$

Required result is now immediate.

The proof of the Theorem now splits into two cases, depending on whether $\alpha = 1$ or not.

Case 1: Suppose that $\alpha>1$.

In the expression,

$$h(h(X,Y),Z^Y) ,$$

it is easy to see that the minimum degree found in X is α^2.

Similarly, noting that the Lemma implies that:

$$\alpha = \beta ,$$

the minimum degree in X found in the expansion of,

$$h(h(Z,X),Y^X) ,$$

is also α^2.

On the other hand, in the expansion:

$$h(h(Y,Z),X^Z) = \sum_{i,j=0}^{\infty} c_{ij} \cdot \left(\sum_{k,\ell=0}^{\infty} c_{k\ell}\, Y^k Z^\ell\right)^i (X^Z)^j ,$$

one can easily see that the term of minimal total degree is:

$$-(c_{\alpha\beta})^{\beta+1} \cdot X^{\alpha} \cdot Y^{\alpha\beta} \cdot Z^{\beta^2}$$

Since,

$$X * Y * Z \equiv X + Y + Z \quad \text{mod total degree } 2 ,$$

it is clear that the monomials of degree α in X in the expansion of the left hand side of equation (3) are just the terms of degree α in the the expansion of:

$$h(h(Y,Z),X^Z) ,$$

so that, the monomial,

$$-(c_{\alpha\beta})^{\beta+1} \cdot X^{\alpha} \cdot Y^{\alpha\beta} \cdot Z^{\beta^2}$$,

is, in fact, the monomial of minimum rank (with respect to our ordering) in the expansion of equation (3) .

Case 2: Suppose that $\alpha = 1$, ie. $\alpha^2 = \alpha$.

In view of the above remark concerning the expansion of,

$$X * Y * Z \quad ,$$

the sum of the terms of degree one in X in the expansion of equation (3) is just the sum of the monomials of degree one in X in the three expressions,

$$h(h(X,Y),Z^Y), h(h(Y,Z),X^Z), \text{ and, } h(h(Z,X),Y^X) \quad .$$

Now, by definition of the various entities,

$$h(h(Z,X),Y^X) = \sum_{i,j=0}^{\infty} c_{ij} \cdot \left(\sum_{k,\ell=0}^{\infty} c_{k\ell} Z^k X^{\ell}\right)^i \cdot F\left(\sum_{r,s=0}^{\infty} c_{rs} X^r Y^s, Y\right)^j$$

Hence the sum of the terms of degree 1 in X is simply,

$$S_1 = \sum_{j,k=1}^{\infty} c_{1j} \cdot c_{k1} \cdot Z^k \cdot Y^j \cdot X \quad , \qquad \text{——————(4)}$$

since, we know that,

$$c_{i0} = c_{0i} = 0 \quad , \quad \text{for all } i \geq 0 \quad .$$

We also have:

$$h(h(X,Y),Z^Y) = \sum_{i,j=0}^{\infty} c_{ij} \cdot \left(\sum_{\ell,k=0}^{\infty} c_{\ell k} X^{\ell} Y^k\right)^i \cdot (Z^Y)^j \quad .$$

Hence the sum of the terms of degree 1 in X, in the above expansion, is:

$$S_2 = \sum_{j,k=1}^{\infty} c_{1j} \cdot c_{1k} \cdot Y^k \cdot (Z^Y)^j \cdot X \quad . \qquad \text{——————(5)}$$

Adding together expressions (4) and (5) to determine the contribution of $h(h(Z,X),Y^X)$ and $h(h(X,Y),Z^Y)$ to the terms of degree 1 in X in the expansion of the left hand side of equation (3), and, bearing in mind the results of the Lemma, we see that:

$$S_1 + S_2 = \sum_{j,k=1}^{\infty} c_{1j} \cdot c_{1k} \cdot X \cdot Y^j \cdot ((Z^Y)^k - Z^k) \quad . \qquad \text{——————(6)}$$

For $k>1$, we have:

$$(Z^Y)^k - Z^k = F(\sum_{r,s=0}^{\infty} c_{rs} \cdot Y^r \cdot Z^s \ , \ Z)^k - Z^k \ , \qquad (7)$$

so that every monomial in the expansion (7) has degree at least 1 in Y. Hence, all the terms of equation (6) have degree at least $\beta+1$ in Y.

On the other hand,

$$h(h(Y,Z),X^Z) = \sum_{i,\ell=0}^{\infty} c_{i\ell} \cdot \left(\sum_{j,k=0}^{\infty} c_{jk} \cdot Y^j \cdot Z^k\right)^i \cdot F(\sum_{r,s=0}^{\infty} c_{rs} \cdot X^r \cdot Z^s \ , \ X)^\ell \ ,$$

has only the two terms,

$$-(c_{1\beta}) \cdot (c_{1\beta} \cdot Y \cdot Z^\beta)^\beta \cdot (c_{\beta 1} \cdot Z^\beta + 1) \cdot X$$

$$= (c_{1\beta})^{\beta+2} \cdot X \cdot Y^\beta \cdot Z^{\beta^2+\beta} - (c_{1\beta})^{\beta+1} \cdot X \cdot Y^\beta \cdot Z^{\beta^2} \ ,$$

envolving X^1 .

Therefore, the monomial of minimial rank occuring in the expansion of equation (3) is once again,

$$-(c_{\alpha\beta})^{\beta+1} \cdot X^\alpha \cdot Y^{\alpha\beta} \cdot Z^{\beta^2} \ ,$$

which is non-zero as the ring R is semi-prime, and, we have assumed:

$$c_{\alpha\beta} \neq 0 \ .$$

Thus we have arrived at a complete contradiction, and, must assume that:

$$c_{ij} = 0 \ , \text{ for all } i,j \geq 0 \ .$$

Hence, $F(X,Y)$ is a commutative formal group law . ∎

Remark: If S is any commutative ring with unit, Ian G. Connell has shown [1] that in order for all 1-dimensional formal group laws over S to be commutative, it is necessary and sufficient that the nilradical of S (ie. the intersection of all the prime ideals of S) be torsion free as an abelian group.

§1.5 Isomorphism in Fml(R) :

If F and G are any two formal group laws over R , of dimensions n and m respectively, with:

$$h : F \longrightarrow G \quad ,$$

a morphism in the category Fml(R) , then, recalling Theoren 1.2.4, h induces a ring homomorphism in the category CAlg(R) :

$$\theta_h : R_m \longrightarrow R_n \quad .$$

In particular, when $n = m$, θ_h is an endomorphism of R_n , so that, if h is an isomorphism in Fml(R) , then θ_h is an automorphism of R_n in CAlg(R) .

Conversely, given any automorphism of R_n in CAlg(R) ,

$$\theta : R_n \longrightarrow R_n \quad ,$$

writing, $X_1, \ldots, X_n$ for the indeterminates of R_n , and ; for $1 \leqslant i \leqslant n$,

$$f_i(X) = \theta(X_i) \quad , \text{ and, } f_i^{-1}(X) = \theta^{-1}(X_i) \quad ,$$

define, for F(X,Y) any formal group law over R of dimension n :

$$F'(X,Y) = f^{-1}(F(f(X),f(Y)) \quad ,$$

where f(X) and $f^{-1}(X)$ are the obvious vectors of formal power series. Trivially we have:

$$F'(X,0) = X \quad , \text{ and, } \quad F'(0,Y) = Y \quad .$$

We may show the associativity of F'(X,Y) by direct computation:

$$\begin{aligned} F'(X,F'(Y,Z)) &= f^{-1}(F(f(X),f(f^{-1}(F(f(Y),f(Z)))))) \\ &= f^{-1}(F(F(f(X),f(Y)),f(Z))) \\ &= F'(F'(X,Y),Z) \quad , \end{aligned}$$

so that, F'(X,Y) is also a formal group law over R of dimension n . Clearly, F'(X,Y) is isomorphic to F(X,Y) in the category Fml(R) .

We have shown:

Theorem 1.5.1: Given two formal group laws over R, F and G, of dimensions n and m, respectively, with a morphism in $\underline{Fml}(R)$:

$$h : F \longrightarrow G \quad ,$$

then, h is an isomorphism in $\underline{Fml}(R)$ iff the induced morphism in $\underline{CAlg}(R)$,

$$\theta_h : R_m \longrightarrow R_n$$

is an automorphism of R_n (note that if h is an isomorphism, then $n = m$).

Secondly, given any isomorphism of R_n, then we may define a new formal group lawsover R of dimension n which is isomorphic to $F(X,Y)$.

∎

NOTE: For the remainder of this thesis, only the theory of 1 dimensional formal group laws will be investigated.

Henceforth, the expression: "Formal group law over R", shall actually mean: " 1 dimensional formal group law over R ".

CHAPTER 2: RATIONAL FORMAL GROUP LAWS.

Throughout this chapter $\underline{A}$ will denote an arbitrary field.

§2.1 Definition and Basic Properties:

Let $F(X,Y)$ denote a rational function in the two indeterminates X and Y, over the field $\underline{A}$.

Definition: we shall call the rational function $F(X,Y)$ a rational formal group law over $\underline{A}$, if $F(0,0) = 0$, and, $F(X,Y)$ satisfies:

i. $F(X,0) = X$, and, $F(0,Y) = Y$, and,

ii. $F(F(X,Y),Z) = F(X,F(Y,Z))$.

From now on, let $F(X,Y)$ represent any rational formal group law over $\underline{A}$. Choose relatively prime polynomials $P(X,Y)$ and $Q(X,Y)$ over $\underline{A}$ such that:

$$F(X,Y) = \frac{P(X,Y)}{Q(X,Y)} ,$$

and write:

$$P(X,Y) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} X^i Y^j \quad , \quad n,m \geq 0$$

$$Q(X,Y) = \sum_{r=0}^{\ell} \sum_{s=0}^{k} b_{rs} X^r Y^s \quad , \quad \ell,k \geq 0 ,$$

where,

$$a_{nj} \neq 0 \quad \text{and} \quad a_{im} \neq 0 \quad \text{for some } i \text{ and } j ,$$

$$b_{\ell s} \neq 0 \quad \text{and} \quad b_{rk} \neq 0 \quad \text{for some } s \text{ and } r .$$

Clearly, the above definition tells us that,

$$P(0,0) = 0 \quad , \text{ and, } Q(0,0) \neq 0 ,$$

and, furthermore,

$$a_{10} = a_{01} = b_{00}$$

Hence, we may assume, without any loss of generality, that $Q(0,0) = 1$, so that: $a_{10} = a_{01} = 1$.

We may now associate to $F(X,Y)$ the formal power series:

$$F'(X,Y) = P(X,Y)\cdot\left(\sum_{t=0}^{\infty} (-1)^t\cdot(Q(X,Y) - 1)^t\right) .$$

Since $F(X,Y)$ is a rational formal group law, it is easy to see that $F'(X,Y)$ is a formal group law, in the sense of the previous chapter. Thus, what we shall be concerned with shall be a very special class of formal group laws over $\underline{A}$. This association of a formal group law to a rational formal group law is extreamly important, and, must always be kept in mind later, when considering the final result of this chapter, and, in particular, its generalization found in Chapter 4.

We shall now abuse our notation by letting $F(X,Y)$ denote both the rational function,

$$\frac{P(X,Y)}{Q(X,Y)} ,$$

and, the associated formal power series $F'(X,Y)$.

By Lazard's result (Theorem 1.4.1), we know that:

$$F(X,Y) = F(Y,X) ,$$

and so,

$$\frac{P(X,Y)}{Q(X,Y)} = \frac{P(Y,X)}{Q(Y,X)}$$

Thus,

$$P(X,Y)\cdot Q(Y,X) - P(Y,X)\cdot Q(X,Y) = 0 .$$

It now follows immediately that:

$$Q(X,Y) \mid Q(Y,X) ,$$

since, $P(X,Y)$ and $Q(X,Y)$ were chosen relatively prime. Similarly:

$$Q(Y,X) \mid Q(X,Y) ,$$

and, therefore, $Q(X,Y) = Q(Y,X)$.

Hence, $P(X,Y) = P(Y,X)$,

that is, $P(X,Y)$ and $Q(X,Y)$ are symmetric polynomials.

Note: the above notation shall be used throughout the remainder of this chapter.

§2.2 Degree Results:

Define a map,

$$\deg_X : \underline{A}(X,Y,Z) \longrightarrow \underline{N}_0 \quad ,$$

by:

$$\deg_X(G(X,Y,Z)) = \text{the degree in } X \text{ of } G(X,Y,Z) \quad ,$$

for any polynomial $G(X,Y,Z) \in \underline{A}(X,Y,Z)$.

Note: the degree in X of $G(X,Y,Z)$ is simply the degree of the polynomial $G(X,Y,Z)$ when considered as a polynomial in X over the ring $\underline{A}(Y,Z)$.

Obviously, $\deg_X$ is well defined as a set-map, and has the following properties:

Lemma 2.2.1: If $R(X,Y,Z)$ and $S(X,Y,Z)$ are any two polynomials in three indeterminates over $\underline{A}$, and,

$$\deg_X(R(X,Y,Z)) = r \quad , \quad \deg_X(S(X,Y,Z)) = s \quad ,$$

then: i. $\deg_X(R(X,Y,Z)\cdot S(X,Y,Z)) = r + s$, and,

ii. $\deg_X(R(S(X,Y,Z),Y,Z)) = r\cdot s$.

Proof: Trivial. ∎

We may extend $\deg_X$ to a map:

$$\mathrm{Deg}_X : \underline{A}(X,Y,Z) \longrightarrow \underline{Z} \quad ,$$

by defining,

$$\mathrm{Deg}_X\left(\frac{R(X,Y,Z)}{S(X,Y,Z)}\right) = \deg_X(R(X,Y,Z)) - \deg_X(S(X,Y,Z)) \quad .$$

It is easy to see that this does in fact define a well defined set map, and, furthermore, the mapping Deg_X has the same multiplicative property as $\deg_X$, stated in part i. of Lemma 2.2.1 (note that part ii. of the lemma is false for the map Deg_X) .

Returning now to the rational formal group law, $F(X,Y)$, we may define two new rational functions over $\underline{A}$:

$$\overline{F}(X,Y,Z) = F(F(X,Y),Z) \quad \text{, and, } \overline{G}(X,Y,Z) = F(X,F(Y,Z)) \quad .$$

By the definition of a rational formal group law, we must have:

$$\overline{F}(X,Y,Z) = \overline{G}(X,Y,Z) \quad ,$$

and so, it follows that:

$$\mathrm{Deg}_X(\overline{F}(X,Y,Z)) = \mathrm{Deg}_X(\overline{G}(X,Y,Z)) \quad . \qquad \text{——(1)}$$

Since,

$$\mathrm{Deg}_X(P(X,F(Y,Z)) = \deg_X(P(X,Y)) \quad \text{, and,}$$

$$\mathrm{Deg}_X(Q(X,F(Y,Z)) = \deg_X(Q(X,Y)) \quad ,$$

by the multiplicative property of Deg_X we have,

$$\mathrm{Deg}_X(\overline{G}(X,Y,Z)) = \deg_X(P(X,Y)) - \deg_X(Q(X,Y))$$

ie. $$\mathrm{Deg}_X(\overline{G}(X,Y,Z)) = n - \ell \quad .$$

On the other hand, computing the left hand side of equation (1) is somewhat more complicated. Put:

$$\overline{P}(X,Y,Z) = P\left(\frac{P(X,Y)}{Q(X,Y)},Z\right) \quad \text{, and, } \overline{Q}(X,Y,Z) = Q\left(\frac{P(X,Y)}{Q(X,Y)},Z\right)$$

Clearly,

$$\overline{P}(X,Y,Z) = Q(X,Y)^{-n} \cdot \left(\sum_{i=0}^{n} \sum_{j=0}^{n} a_{ij}\, P(X,Y)^i \cdot Q(X,Y)^{n-i} \cdot Z^j\right) \quad ,$$

so that, writing,

$$N(X,Y,Z) = \sum_{i=0}^{n} \sum_{j=0}^{n} a_{ij}\, P(X,Y)^i \cdot Q(X,Y)^{n-i} \cdot Z^j \quad ,$$

we have:

$$\mathrm{Deg}_X(\overline{P}(X,Y,Z)) = \deg_X(N(X,Y,Z)) - \deg_X(\, Q(X,Y)^n \,) \quad ,$$

that is, by Lemma 2.2.1,

$$\mathrm{Deg}_X(\overline{P}(X,Y,Z)) = \deg_X(N(X,Y,Z)) - n \cdot \ell \quad .$$

Similarly, we must have:

$$\mathrm{Deg}_X(\overline{Q}(X,Y,Z)) = \deg_X(D(X,Y,Z)) - \ell^2 \quad ,$$

where,

$$D(X,Y,Z) = \sum_{r=0}^{\ell} \sum_{s=0}^{\ell} b_{rs} P(X,Y)^r \cdot Q(X,Y)^{\ell-r} \cdot Z^s$$

Obviously, by the definition of the various rational functions envolved:

$$\mathrm{Deg}_X(\overline{F}(X,Y,Z)) = \mathrm{Deg}_X(\overline{P}\,X,Y,Z)) - \mathrm{Deg}_X(\overline{Q}(X,Y,Z)) \quad ,$$

ie. $$\mathrm{Deg}_X(\overline{F}(X,Y,Z)) = \deg_X(N(X,Y,Z)) - \deg_X(D(X,Y,Z)) - (n\cdot\ell - \ell^2). \quad —(2)$$

The computation of the first two terms of the right hand side of the above equation splits naturally into two cases:

First, suppose that, $n>\ell$, that is: $\deg_X(Q(X,Y)) > \deg_X(P(X,Y))$.

After a moments reflection, it becomes clear that:

$$\deg_X(N(X,Y,Z)) = n\cdot\ell \quad , \text{ and, } \quad \deg_X(D(X,Y,Z)) = \ell^2 \quad ;$$

so that, by equation (2) , we must have:

$$\mathrm{Deg}_X(\overline{F}(X,Y,Z)) = 0$$

But, by equation (1) we have already,

$$\mathrm{Deg}_X(\overline{F}(X,Y,Z)) = n - \ell \quad ,$$

and, since we have assumed that $\ell > n$, we have a contradiction !

Hence, only the second case can occur, that is, we must have: $n \geq \ell$.

If we actually have: $n>\ell$, it is not too difficult to see that:

$$\deg_X(N(X,Y,Z)) = n^2 \text{ , and, } \deg_X(D(X,Y,Z)) = n\cdot\ell \quad ,$$

therefore, equation (2) now gives:

$$\mathrm{Deg}_X(\overline{F}(X,Y,Z)) = (n - \ell)^2 \quad .$$

Equation (1) now implies that: $(n - \ell)^2 = n - \ell$,

so that, we must have: $n = \ell + 1$.

We have now shown above:

Theorem 2.2.2: For any rational formal group law, $F(X,Y) = \frac{P(X,Y)}{Q(X,Y)}$, we have:

$$\deg_X(Q(X,Y)) \leq \deg_X(P(X,Y)) \leq \deg_X(Q(X,Y)) + 1 \quad .$$

This result, together with the symmetry of $P(X,Y)$ and $Q(X,Y)$, gives:

$$P(X,Y) = \sum_{i=0}^{m} \sum_{j=0}^{m} a_{ij} X^i Y^j \text{ , and, } Q(X,Y) = \sum_{r=0}^{m} \sum_{s=0}^{m} b_{rs} X^r Y^s \text{ ,}$$

where, if $b_{rm} = 0$ for all r, $0 \leq r \leq m$, then, for some r, $b_{rm-1} \neq 0$.

Corollary 2.2.3: For all i , $0 \leq i \leq m-1$,

$$b_{0i} = a_{0i+1} \text{ , and , } b_{0m} = b_{m0} = 0 \text{ .}$$

Proof: immediate from the first property of rational formal group laws, together with the above notation. ∎

Remark: By symmetry we must have: $b_{i0} = a_{i+1,0}$ for all $0 \leq i \leq m-1$.

Corollary 2.2.4: $F(X,Y)$ is actually a polynomial over $\underline{A}$ iff for some $a \in \underline{A}$,

$$F(X,Y) = X + Y + aXY \text{ .}$$

Proof: If $F(X,Y)$ is a polynomial, then by the theorem, $\deg_X(P(X,Y)) = 1$.

Hence, $F(X,Y) = X + Y + aXY$, for some $a \in \underline{A}$.

Conversely, any polynomial: $X + Y + cXY$, $c \in \underline{A}$,

can be seen to be a rational formal group law over $\underline{A}$. ∎

§2.3 Divisibility Results:

We now wish to establish relationships between the coefficients of $P(X,Y)$ and $Q(X,Y)$, using their relative primeness. The associative property of $F(X,Y)$ states:

$$F(X,F(Y,Z)) = F(F(X,Y),Z) \text{ ,}$$

which obviously says that:

$$P(F(X,Y),Z) \cdot Q(X,F(Y,Z)) = Q(F(X,Y),Z) \cdot P(X,F(Y,Z)) \text{ .}$$

Thus, we have:

$$\left(\sum_{i=0}^{m} \sum_{j=0}^{m} a_{ij} \cdot F(X,Y)^i \cdot Z^j\right) \cdot \left(\sum_{r=0}^{m} \sum_{s=0}^{m} b_{rs} \cdot X^r \cdot F(Y,Z)^s\right) =$$

$$= \left(\sum_{t=0}^{m} \sum_{u=0}^{m} b_{tu} \cdot F(X,Y)^t \cdot Z^u\right) \cdot \left(\sum_{k=0}^{m} \sum_{\ell=0}^{m} a_{k\ell} X^k \cdot F(Y,Z)^\ell\right) \text{ .}$$

Multiplying both sides of the above equation by: $Q(X,Y)^m \cdot Q(Y,Z)^m$,

and, writing:

$$R(X,Y,Z) = \sum_{r=0}^{m} \sum_{s=0}^{m} b_{rs} X^r P(Y,Z)^s Q(Y,Z)^{m-s} ,$$

$$S(X,Y,Z) = \sum_{k=0}^{m} \sum_{\ell=0}^{m} a_{k\ell} X^k P(Y,Z)^{\ell} Q(Y,Z)^{m-\ell} ,$$

we have:

$$0 = R(X,Y,Z) \cdot \sum_{i=0}^{m} \sum_{j=0}^{m} a_{ij} P(X,Y)^i Q(X,Y)^{m-i} Z^j -$$

$$- S(X,Y,Z) \cdot \sum_{t=0}^{m} \sum_{u=0}^{m} b_{tu} P(X,Y)^t Q(X,Y)^{m-t} Z^u .$$

Trivially, $P(X,Y)$ divides the zero polynomial in $\underline{A}(X,Y)$, so that $P(X,Y)$ must divide the right hand side of the above equation. It follows immediately that $P(X,Y)$ must divide the polynomial:

$$\left(R(X,Y,Z) \cdot \sum_{j=0}^{m} a_{0j} Z^j - S(X,Y,Z) \cdot \sum_{u=0}^{m} b_{0u} Z^u \right) \cdot Q(X,Y)^m ,$$

in $\underline{A}(X,Y,Z)$. But, $P(X,Y)$ and $Q(X,Y)$ are relatively prime in $\underline{A}(X,Y,Z)$, hence:

$$P(X,Y) \nmid Q(X,Y)^m .$$

Thus,

$$P(X,Y) \mid \left(R(X,Y,Z) \cdot \sum_{j=0}^{m} a_{0j} Z^j - S(X,Y,Z) \cdot \sum_{u=0}^{m} b_{0u} Z^u \right) .$$

Now substitute: $Y=0$, in the above. Since: $P(0,Z) = Z \cdot Q(0,Z)$,

we have:

$$R(X,0,Z) = \left(\sum_{r=0}^{m} \sum_{s=0}^{m} b_{rs} X^r Z^s \right) \cdot Q(0,Z)^m , \text{ and,}$$

$$S(X,0,Z) = \left(\sum_{k=0}^{m} \sum_{\ell=0}^{m} a_{k\ell} X^k Z^{\ell} \right) \cdot Q(0,Z)^m .$$

Obviously, $P(X,0) \nmid Q(0,Z)^m$ in $\underline{A}(X,Y,Z)$, so that:

$$P(X,0) \mid \left\{ \left(\sum_{r=0}^{m} \sum_{s=0}^{m} b_{rs} X^r Z^s \right) \cdot \sum_{j=0}^{m} a_{0j} Z^j - \left(\sum_{k=0}^{m} \sum_{\ell=0}^{m} a_{k\ell} X^k Z^{\ell} \right) \cdot \sum_{u=0}^{m} b_{0u} Z^u \right\} ,$$

in $\underline{A}(X,Y,Z)$. Collecting together the various powers of X and Z , we have,

$$P(X,Y) \mid \left\{ \sum_{u=0}^{2m} Z^u \cdot \sum_{k=0}^{m} X^k \cdot \left\{ \sum_{\substack{i+j=u \\ 0 \le i,j \le m}} (a_{0j} \cdot b_{ki} - a_{ki} \cdot b_{0j}) \right\} \right\} \qquad (1) .$$

Suppose now that: $a_{m0} \neq 0$, ie. $\deg_X(P(X,0)) = m$.

Clearly, the degree in X of the right hand side of line (1) is at most m, thus, there exist $g_i \in \underline{A}$, $0 \leq i \leq 2m$, such that:

$$P(X,0) \cdot \sum_{i=0}^{2m} g_i Z^i = \sum_{u=0}^{2m} Z^u \cdot \sum_{k=0}^{m} X^k \cdot \left[\sum_{\substack{s+j=u \\ 0 \leq s,j \leq m}} (a_{0j} \cdot b_{ks} - a_{ks} \cdot b_{0j}) \right] \qquad (2)$$

Since,

$$P(X,0) = \sum_{r=0}^{m} a_{r0} X^r ,$$

equating coefficients of the various powers of Z in equation (2) we obtain:

$$g_i \cdot \sum_{r=0}^{m} a_{r0} X^r = \sum_{k=0}^{m} X^k \cdot \left[\sum_{\substack{s+j=i \\ 0 \leq s,j \leq m}} (a_{0j} \cdot b_{ks} - a_{ks} \cdot b_{0j}) \right] \quad \ldots$$

where: $0 \leq i \leq 2m$.

Equating coefficients in the above equation gives:

$$g_i \cdot a_{r0} = \sum_{\substack{s+j=i \\ 0 \leq s,j \leq m}} (a_{0j} \cdot b_{rs} - a_{rs} \cdot b_{0j}) ,$$

for all i,r ; $0 \leq i \leq 2m$, $0 \leq r \leq m$.

In particular, when $r=1$, we have:

$$g_i = \sum_{\substack{s+j=i \\ 0 \leq s,j \leq m}} (a_{0j} \cdot b_{1s} - a_{1s} \cdot b_{0j}) , \quad (0 \leq i \leq m),$$

and, for $i=2m$,

$$g_{2m} = \sum_{\substack{s+j=2m \\ 0 \leq s,j \leq m}} (a_{0j} \cdot b_{1s} - a_{1s} \cdot b_{0j})$$

$$= a_{0m} \cdot b_{1m} - a_{1m} \cdot b_{0m} .$$

But, by Corollary 2.2.3,

$$b_{0m} = 0 ,$$

hence,

$$g_{2m} = a_{0m} \cdot b_{1m} .$$

Thus, for any r , $0 \leq r \leq m$,

$$g_{2m} \cdot a_{r0} = \sum_{\substack{s+j=2m \\ 0 \leq s,j \leq m}} (a_{0j} \cdot b_{rs} - a_{rs} \cdot b_{0j}) ,$$

ie. $a_{0m} \cdot b_{lm} \cdot a_{r0} = a_{0m} \cdot b_{rm}$,

which proves:

Proposition 2.3.1: If $a_{m0} \neq 0$, then:

$$a_{r0} \cdot b_{lm} = b_{rm} \quad , \quad \text{for: } 0 \leq r < m \ .$$

Proof: Use the argument above, together with the symmetry of $P(X,Y)$,

ie. $a_{0m} = a_{m0}$. ——Z——

Return now to the original equation,

$$P(X,F(Y,Z)) \cdot Q(F(X,Y),Z) = Q(X,F(Y,Z)) \cdot P(F(X,Y),Z) \quad ——— (*) \ .$$

Suppose that $F(X,Y)$ is a rational formal group with:

$$\deg_X(Q(X,Y)) < \deg_X(P(X,Y)) \ .$$

Then, by Theorem 2.2.2, we have:

$$\deg_X(Q(X,Y)) = m - 1 \ .$$

ie. $b_{rm} = b_{mr} = 0$, for all r , $0 \leq r < m$.

We shall show that $Q(X,Y)$ is a constant polynomial, ie. $m = 1$.

The expansion of equation (*) is:

$$Q(Y,Z)^{-m} \cdot \left(\sum_{i=0}^{m} \sum_{j=0}^{m} a_{ij} \, X^i \, P(Y,Z)^j \, Q(Y,Z)^{m-j} \right) \cdot$$

$$\cdot Q(X,Y)^{-(m-1)} \cdot \left(\sum_{k=0}^{m-1} \sum_{\ell=0}^{m-1} b_{k\ell} \, P(X,Y)^k \, Q(X,Y)^{m-1-k} \, Z^\ell \right) =$$

$$= Q(X,Y)^{-m} \cdot \left(\sum_{r=0}^{m} \sum_{s=0}^{m} a_{rs} \, P(X,Y)^r \, Q(X,Y)^{m-r} \, Z^s \right) \cdot$$

$$\cdot Q(Y,Z)^{-(m-1)} \cdot \left(\sum_{t=0}^{m-1} \sum_{u=0}^{m-1} b_{tu} \, X^t \, P(Y,Z)^u \, Q(Y,Z)^{m-1-u} \right) \ .$$

Hence:

$$0 = Q(Y,Z) \cdot R(X,Y,Z) - Q(X,Y) \cdot S(X,Y,Z) \quad , \text{ where:}$$

$$R(X,Y,Z) = \left(\sum_{r=0}^{m} \sum_{s=0}^{m} a_{rs} \, P(X,Y)^r \, Q(X,Y)^{m-r} \, Z^s \right) \left(\sum_{t=0}^{m-1} \sum_{u=0}^{m-1} b_{tu} \, X^t \, P(Y,Z)^u \, Q(Y,Z)^{m-1-u} \right),$$

$$S(X,Y,Z) = \left(\sum_{i=0}^{m} \sum_{j=0}^{m} a_{ij} \, X^i \, P(Y,Z)^j \, Q(Y,Z)^{m-j} \right) \left(\sum_{k=0}^{m-1} \sum_{\ell=0}^{m-1} b_{k\ell} \, P(X,Y)^k \, Q(X,Y)^{m-1-k} \, Z^\ell \right).$$

Obviously, $Q(X,Y) \mid 0$ in $\underline{A}(X,Y,Z)$, and, $Q(X,Y) \nmid P(X,Y)$ in $\underline{A}(X,Y,Z)$.

Furthermore, $Q(X,Y) \mid Q(Y,Z)$ in $\underline{A}(X,Y,Z)$ iff $Q(X,Y)$ is a constant polynomial .

Suppose, for a contradiction, that $Q(X,Y)$ is not a constant polynomial,

ie. $\deg_X(Q(X,Y)) = m - 1 > 0$.

Hence equation (*) implies that:

$$Q(X,Y) \mid R(X,Y,Z)$$

Considering $R(X,Y,Z)$ as a polynomial in $Q(X,Y)$, clearly $Q(X,Y)$ must divide the constant term,

ie. $$Q(X,Y) \mid \left(\sum_{s=0}^{m} a_{ms} Z^s \right) \cdot \left(\sum_{t=0}^{m-1} \sum_{u=0}^{m-1} b_{tu} X^t P(Y,Z)^u Q(Y,Z)^{m-1-u} \right) .$$

Since, $\deg_X(P(X,Y)) = m$, there exists i , $0 < i < m$, such that: $a_{mi} \neq 0$,

ie. $\sum_{s=0}^{m} a_{ms} Z^s \neq 0$.

Clearly,

$$Q(X,Y) \nmid \sum_{s=0}^{m} a_{ms} Z^s$$

hence:

$$Q(X,Y) \mid \sum_{t=0}^{m-1} \sum_{u=0}^{m-1} b_{tu} X^t P(Y,Z)^u Q(Y,Z)^{m-1-u} .$$

Now set: $Z = X$. We have,

$$Q(X,Y) \mid \sum_{t=0}^{m-1} \sum_{u=0}^{m-1} b_{tu} X^t P(Y,X)^u Q(Y,X)^{m-1-u} .$$

We know that: $Q(X,Y) = Q(Y,X)$, and, $P(X,Y) = P(Y,X)$,

and so,

$$Q(X,Y) \mid \sum_{t=0}^{m-1} b_{tm-1} X^t$$

By symmetry, $Q(X,Y)$, is not a polynomial in X alone, therefore:

$$\sum_{t=0}^{m-1} b_{tm-1} X^t \equiv 0 ,$$

ie. $b_{tm-1} = 0$ for all $0 < t < m$.

Contradiction ! We know that $Q(X,Y)$ has degree exactly $m - 1$ in both X and Y, and we have assumed that: $m - 1 > 0$,

ie. for some t , $0 \leq t \leq m$, $b_{tm-1} = b_{m-1t} \neq 0$!

Hence we have in fact shown that $Q(X,Y)$ must be a constant polynomial.

Summing up, we have:

Proposition 2.3.2: If $F(X,Y)$ is a rational formal group law, over $\underline{A}$,

ie. $F(X,Y) = \frac{P(X,Y)}{Q(X,Y)}$, $P(X,Y)$ and $Q(X,Y)$ relatively prime,

and, $\deg_X(\ Q(X,Y)\ ) < \deg_X(\ P(X,Y)\ )$,

then, $F(X,Y)$ is actually a polynomial formal group law over $\underline{A}$,

ie. $F(X,Y) = X + Y + aXY$, for some $a \in \underline{A}$.

§2.4 Möbius Transformations and Isomorphism:

Let $\Psi_\alpha(X)$ denote the Möbius transformation:

$$\Psi_\alpha(X) = \frac{X}{1 - \alpha \cdot X} \quad , \quad \text{where: } \alpha \in \underline{A} \ .$$

Clearly, $\Psi_\alpha(X)$ defines an automorphism of $\underline{A}((X))$, under substitution of formal power series, the inverse transformation given by:

$$\Psi_\alpha^{-1}(X) = \frac{X}{1 + \alpha \cdot X} \ ,$$

and so we may consider the rational formal group law, isomorphic to $F(X,Y)$ under the morphism $\Psi_\alpha(X)$ (Theorem 1.5.1), defined by:

$$F_\alpha(X,Y) = \Psi_\alpha^{-1} \circ F(\Psi_\alpha(X), \Psi_\alpha(Y))$$

Thus, we have:

$$F_\alpha(X,Y) = \frac{F(\Psi_\alpha(X), \Psi_\alpha(Y))}{1 + \alpha \cdot F(\Psi_\alpha(X), \Psi_\alpha(Y))} \ ,$$

and so,

$$F_\alpha(X,Y) = \frac{P_\alpha(X,Y)}{Q_\alpha(X,Y) + \alpha \cdot P_\alpha(X,Y)} \ ,$$

where:

$$P_\alpha(X,Y) = (1 - \alpha X)^m \cdot (1 - \alpha Y)^m \cdot P(\Psi_\alpha(X), \Psi_\alpha(Y)) \quad , \text{ and,}$$

$$Q_\alpha(X,Y) = (1 - \alpha X)^m \cdot (1 - \alpha Y)^m \cdot Q(\Psi_\alpha(X), \Psi_\alpha(Y)) \ .$$

Put: $$\overline{Q}_\alpha(X,Y) = Q_\alpha(X,Y) + \alpha \cdot P_\alpha(X,Y) \ .$$

Clearly,

$$\overline{Q}_\alpha(0,0) \equiv 1 \quad ,$$

and, as might be expected, it is possible to show that $P_\alpha(X,Y)$ and $Q_\alpha(X,Y)$ are relatively prime polynomials over $\underline{A}$.

First, we shall need the following Lemma:

Suppose $d(X,Y)$ is a polynomial in two indeterminates over $\underline{A}$,

$$d(X,Y) = \sum_{i=0}^{k} \sum_{j=0}^{\ell} c_{ij} X^i Y^j \quad .$$

We may define a new polynomial $\overline{d}(X,Y)$ by:

$$\overline{d}(X,Y) = d(\psi_\alpha^{-1}(X),\psi_\alpha^{-1}(Y))\cdot(1 + \alpha X)^k\cdot(1 + \alpha Y)^\ell \quad .$$

Lemma 2.4.1: If,

$$\overline{d}(X,Y) = c_{00} \quad , \quad \text{then:}$$

$$d(X,Y) = c_{00}\cdot(1 - \alpha X)^k(1 - \alpha Y)^\ell \quad .$$

Proof: Given that,

$$\overline{d}(X,Y) = c_{00} \quad ,$$

obviously:

$$\overline{d}(\psi_\alpha(X),\psi_\alpha(Y)) = c_{00} \quad .$$

Hence, by the definition of $\overline{d}(X,Y)$, we have:

$$c_{00} = d(X,Y)\cdot(1 + \alpha\psi_\alpha(X))^k\cdot(1 + \alpha\psi_\alpha(Y))^\ell$$

$$= d(X,Y)\,\frac{1}{(1 - \alpha X)^k\cdot(1 - \alpha Y)^\ell}$$

Therefore,

$$d(X,Y) = c_{00}\cdot(1 - \alpha X)^k\cdot(1 - \alpha Y)^\ell \quad . \qquad \text{Q}$$

We can now prove:

Theorem 2.4.2: $P(X,Y)$ and $Q(X,Y)$ are relatively prime in $\underline{A}(X,Y)$ iff:

$P_\alpha(X,Y)$ and $Q_\alpha(X,Y)$ are relatively prime in $\underline{A}(X,Y)$ for all $\alpha\in\underline{A}$.

Proof: Assume, first, that $P(X,Y)$ and $Q(X,Y)$ are relatively prime.

Fix $\alpha \in \underline{A}$. Suppose, for a contradiction, that there exists $d_\alpha(X,Y) \in \underline{A}(X,Y)$,

$$d_\alpha(X,Y) = \sum_{i=0}^{k} \sum_{j=0}^{\ell} c_{ij} X^i Y^j \quad ,$$

such that:

$$d_\alpha(X,Y) \mid P_\alpha(X,Y) \quad \text{and} \quad d_\alpha(X,Y) \mid \overline{Q}_\alpha(X,Y) \quad , \text{ in } \underline{A}(X,Y),$$

and, $d_\alpha(X,Y)$ is not a conatant polynomial,

ie. $\deg_X(d_\alpha(X,Y)) = k > 0$, $\deg_Y(d_\alpha(X,Y)) = \ell > 0$.

It follows immediately that:

$$d_\alpha(X,Y) \mid Q_\alpha(X,Y) \quad .$$

Let $P'_\alpha(X,Y)$ and $Q'_\alpha(X,Y)$ be polynomials over $\underline{A}$ such that:

$$P_\alpha(X,Y) = P'_\alpha(X,Y) \cdot d_\alpha(X,Y) \quad , \text{ and ,}$$

$$Q_\alpha(X,Y) = Q'_\alpha(X,Y) \cdot d_\alpha(X,Y) \quad .$$

Since, by the definition of $P_\alpha(X,Y)$,

$$P_\alpha(X,Y) = (1 - \alpha X)^m \cdot (1 - \alpha Y)^m \cdot P(\Psi_\alpha(X), \Psi_\alpha(Y)) \quad ,$$

we have,

$$P_\alpha(\Psi_\alpha^{-1}(X), \Psi_\alpha^{-1}(Y)) = (1 + \alpha X)^{-m} \cdot (1 + \alpha Y)^{-m} \cdot P(X,Y) \quad ,$$

so that,

$$P(X,Y) = \overline{P}'_\alpha(X,Y) \cdot \overline{d}_\alpha(X,Y) \quad ,$$

where:

$$\overline{P}'_\alpha(X,Y) = (1 + \alpha X)^{m-k} \cdot (1 + \alpha Y)^{m-\ell} \cdot P'_\alpha(\Psi_\alpha^{-1}(X), \Psi_\alpha^{-1}(Y)) \quad , \text{ and,}$$

$$\overline{d}_\alpha(X,Y) = (1 + \alpha X)^k \cdot (1 + \alpha Y)^\ell \cdot d_\alpha(\Psi_\alpha^{-1}(X), \Psi_\alpha^{-1}(Y)) \quad .$$

Now, $P(X,Y)$ is a polynomial over $\underline{A}$, and, clearly so is $\overline{d}_\alpha(X,Y)$, therefore, $P'_\alpha(X,Y)$ must also be a polynomial over $\underline{A}$,

ie. $\overline{d}_\alpha(X,Y) \mid P(X,Y)$ in $\underline{A}(X,Y)$.

By a similar argument,

$$Q(X,Y) = \overline{Q}'_\alpha(X,Y) \, \overline{d}_\alpha(X,Y) \quad ,$$

where: $\overline{Q}_\alpha(X,Y) = (1+\alpha X)^{m-k}\cdot(1+\alpha Y)^{m-\ell}\cdot Q_\alpha(\psi_\alpha^{-1}(X),\psi_\alpha^{-1}(Y))$

But, $P(X,Y)$ and $Q(X,Y)$ are relatively prime in $\underline{A}(X,Y)$, therefore:

$$\overline{d}_\alpha(X,Y) = c \quad , \quad \text{where} \quad c\in\underline{A} \ .$$

Hence, by Lemma 2.4.1, we have:

$$d_\alpha(X,Y) = c\cdot(1-\alpha X)^k\cdot(1-\alpha Y)^\ell \ .$$

By our original assumption,

$$P_\alpha(X,Y) = P'_\alpha(X,Y)\cdot d_\alpha(X,Y) \ ,$$

which says that:

$$(1-\alpha X)^m\cdot(1-\alpha Y)^m\cdot P(\psi_\alpha(X),\psi_\alpha(Y)) = P'_\alpha(X,Y)\cdot c\cdot(1-\alpha X)^k\cdot(1-\alpha Y)^\ell \ ,$$

$$\text{ie.} \quad c\cdot P'_\alpha(X,Y) = (1-\alpha X)^{m-k}\cdot(1-\alpha Y)^{m-\ell}\cdot P(\psi_\alpha(X),\psi_\alpha(Y)) \ .$$

Now, $P'_\alpha(X,Y)$ is a polynomial over $\underline{A}$, and so,

$$(1-\alpha X)^{m-k}\cdot(1-\alpha Y)^{m-\ell}\cdot P(\psi_\alpha(X),\psi_\alpha(Y))$$

must be a polynomial over $\underline{A}$. However,

$$\deg_X(\ P(X,Y)\ ) = m \ ,$$

which implies that: $k = \ell = 0$. Contradiction !

Hence the only common divisors of $P_\alpha(X,Y)$ and $Q_\alpha(X,Y)$ in $\underline{A}(X,Y)$ are the constant polynomials, and, this is true for any value of $\alpha\in\underline{A}$.

Conversely, if $P_\alpha(X,Y)$ and $Q_\alpha(X,Y)$ are relatively prime for every value of $\alpha\in\underline{A}$, then obviously $P(X,Y)$ and $Q(X,Y)$ are relatively prime since:

$$P_0(X,Y) = P(X,Y) \quad , \text{ and ,}$$

$$Q_0(X,Y) = Q(X,Y) \ .$$

We shall now derive a simple form needed in the next section:

Lemma 2.4.3: Suppose that $F(X,Y)$ is a rational formal group law, and, for some $\alpha_0\in\underline{A}$ we have: $F_{\alpha_0}(X,Y) = X + Y + aXY$, $a\in\underline{A}$, then:

$$F(X,Y) = \frac{X + Y + (a+2\alpha_0)XY}{1-(\alpha_0^2 + a\cdot\alpha_0)XY}$$

Proof: We have: $\Psi_{\alpha_0}^{-1} \circ F(\Psi_{\alpha_0}(X), \Psi_{\alpha_0}(Y)) = X + Y + aXY$,

so that,

$$F(X,Y) = \Psi_{\alpha_0}\left(\Psi_{\alpha_0}^{-1}(X) + \Psi_{\alpha_0}^{-1}(Y) + a\cdot\Psi_{\alpha_0}^{-1}(X)\cdot\Psi_{\alpha_0}^{-1}(Y)\right)$$

$$= \frac{(1+\alpha_0 X)\cdot(1+\alpha_0 Y)}{(1+\alpha_0 X)\cdot(1+\alpha_0 Y)} \cdot \frac{\Psi_{\alpha_0}^{-1}(X) + \Psi_{\alpha_0}^{-1}(Y) + a\cdot\Psi_{\alpha_0}^{-1}(X)\cdot\Psi_{\alpha_0}^{-1}(Y)}{1 - \alpha_0\left(\Psi_{\alpha_0}^{-1}(X) + \Psi_{\alpha_0}^{-1}(Y) + a\cdot\Psi_{\alpha_0}^{-1}(X)\cdot\Psi_{\alpha_0}^{-1}(Y)\right)}$$

$$= \frac{(1+\alpha_0 Y)\cdot X + (1+\alpha_0 X)\cdot Y + aXY}{(1+\alpha_0 X)\cdot(1+\alpha_0 Y) - \alpha_0\left[(1+\alpha_0 Y)\cdot X + (1+\alpha_0 X)\cdot Y + aXY\right]}$$

$$= \frac{X + Y + (a + 2\alpha_0)\,XY}{1 - (\alpha_0^2 + a\alpha_0)\,XY}$$

□

§2.5 The General Form of a Rational Formal Group Law:

Let $\Omega(\underline{A})$ denote the algebraic closure of the field $\underline{A}$.

Before giving a general form for a rational formal group law over the field $\underline{A}$, we need two additional lemmas concerning $\Omega(\underline{A})$:

Lemma 2.5.1: For any rational formal group law $F(X,Y)$ over $\Omega(\underline{A})$, we have:

$$a_{r0}\cdot b_{1m} = b_{rm} \quad , \quad \text{for } 0 \leqslant r \leqslant m \ .$$

Proof: We shall make use of the fact that $\Omega(\underline{A})$ is not a finite field.

Write: $\underline{A}' = \Omega(\underline{A})$. Recall:

$$F_\alpha(X,Y) = \Psi_\alpha^{-1} \circ F(\Psi_\alpha(X), \Psi_\alpha(Y)) \quad , \quad \alpha \in \underline{A}' \ ,$$

and,

$$P_\alpha(X,Y) = \sum_{i=0}^{m}\sum_{j=0}^{m} a_{ij}\cdot X^i\cdot(1-\alpha X)^{m-i}\cdot Y^j\cdot(1-\alpha Y)^{m-j} \ ,$$

$$Q_\alpha(X,Y) = \sum_{r=0}^{m}\sum_{s=0}^{m} b_{rs}\cdot X^r\cdot(1-\alpha X)^{m-r}\cdot Y^s\cdot(1-\alpha Y)^{m-s} \ ,$$

with:

$$\overline{Q}_\alpha(X,Y) = Q_\alpha(X,Y) + \alpha\cdot P_\alpha(X,Y) \ .$$

Let $a_{ij}(\alpha)$ denote the coefficient of X^iY^j in $P_\alpha(X,Y)$. Then:

$$a_{ij}(\alpha) = \sum_{\substack{k+s=i \\ 0\leqslant k,s\leqslant m}} \sum_{\substack{\ell+t=j \\ 0\leqslant \ell,t\leqslant m}} (-\alpha)^{\ell+k}\cdot\binom{m-s}{k}\cdot\binom{m-t}{\ell}\cdot a_{st} \ .$$

Similarly, if $b_{ij}(\alpha)$ denotes the coefficient of X^iY^j in $Q_\alpha(X,Y)$,

$$b_{ij}(\alpha) = \sum_{\substack{u+v=i \\ 0\leq u,v\leq m}} \sum_{p+q=j} (-\alpha)^{p+u} \cdot \begin{bmatrix} m-v \\ u \end{bmatrix} \begin{Bmatrix} m-q \\ p \end{Bmatrix} \cdot b_{vq} \quad ,$$

and so, if $\overline{b}_{ij}(\alpha)$ denotes the coefficient of X^iY^j in $\overline{Q}_\alpha(X,Y)$,

$$\overline{b}_{ij}(\alpha) = b_{ij}(\alpha) + \alpha \cdot a_{ij}(\alpha)$$

Clearly,

$$a_{m0}(\alpha) = \sum_{k=0}^{m} a_{k0} \cdot (-\alpha)^k \quad ,$$

and,

$$a_{0m}(\alpha) = \sum_{\ell=0}^{m} a_{0m-\ell} \cdot (-\alpha)^{m-\ell}$$

Since: $a_{10} = a_{01} = 1$,

neither $a_{0m}(\alpha)$ nor $a_{m0}(\alpha)$ is constantly zero, when viewed as a polynomial in α. Thus, the set,

$$E = \{ \beta \in \underline{A}^1 \mid a_{m0}(\beta) = 0 \text{ , or, } a_{0m}(\beta) = 0 \}$$

is a finite set. Now, by Theorem 2.4.2, $P_\alpha(X,Y)$ and $\overline{Q}_\alpha(X,Y)$ are relatively prime polynomials, so, by Proposition 2.3.1, for all $\beta \in \underline{A}^1 \backslash E$, we have:

$$a_{i0}(\beta) \cdot \overline{b}_{lm}(\beta) = \overline{b}_{im}(\beta) \quad , \text{ for any } i \ , \ 0 \leq i \leq m \quad ,$$

ie. is a root of the polynomial:

$$b_i(\alpha) = a_{i0}(\alpha) \cdot \overline{b}_{lm}(\alpha) - \overline{b}_{im}(\alpha)$$

Hence, since $\underline{A}^1 \backslash E$ is an infinite set, for each i , $0 \leq i \leq m$, $b_i(\alpha)$ must be constantly zero, ie. the zero polynomial in $\underline{A}^1(\alpha)$.

This says:

$$a_{i0}(\alpha) \cdot \overline{b}_{lm}(\alpha) = \overline{b}_{im}(\alpha) \qquad \text{——————(*)}$$

Now,

$$a_{i0}(\alpha) = \sum_{k=0}^{m} (-\alpha)^k \cdot \begin{bmatrix} i \\ k \end{bmatrix} \cdot a_{i-k0} \quad ,$$

$$\overline{b}_{lm}(\alpha) = b_{lm}(\alpha) + \alpha \cdot a_{lm}(\alpha) \quad ,$$

$$\text{ie.}\quad \bar{b}_{1m}(\alpha) = \sum_{\substack{u+v=1\\ 0\le u,v\le m}} \sum_{\substack{p+q=m\\ 0\le p,q\le m}} (-\alpha)^{p+u}\cdot\binom{m-v}{u}\cdot\binom{m-q}{p}\cdot b_{vq} \;+$$

$$+\;\alpha\cdot\left(\sum_{\substack{k+s=1\\ 0\le k,s\le m}} \sum_{\substack{\ell+t=m\\ 0\le \ell,t\le m}} (-\alpha)^{\ell+k}\cdot\binom{m-s}{k}\cdot\binom{m-t}{\ell}\cdot a_{st}\right),$$

and, similarly,

$$\bar{b}_{im}(\alpha) = \sum_{\substack{u+v=i\\ 0<u,v<m}} \sum_{\substack{p+q=m\\ 0<p,q<m}} (-\alpha)^{p+u}\cdot\binom{m-v}{u}\cdot\binom{m-q}{p}\cdot b_{vq} \;+$$

$$+\;\alpha\cdot\left(\sum_{\substack{k+s=i\\ 0<k,s<m}} \sum_{\substack{\ell+t=m\\ 0<\ell,t<m}} (-\alpha)^{\ell+k}\cdot\binom{m-s}{k}\cdot\binom{m-t}{\ell}\cdot a_{st}\right).$$

Comparing the constant terms in equation (*) above, we see that:

$$a_{i0}\cdot b_{1m} = b_{im} \qquad \text{, for all } i\text{ , } 0 \le i \le m.$$

———Ⅱ———

Remark: This lemma is, of course, the generalization of Proposition 2.3.1 . Together with the Proposition 2.3.2 it gives the proof of the main theorem of this section, first directly implying the next lemma , which forms the heart of the main proof. The main technique used here is the special subset of the isomorphism class in $\underline{\text{Fml}}(\underline{A})$, of the rational formal group law in question, which we obtain via our simple Möbius transformations. Their importance with respect to the theory of rational formal groups is far more than accidental, as we shall see in Chapter 3, where they turn out to be fundamental objects of study when examining the isomorphism of rational formal group laws over $\underline{A}$.

Lemma 2.5.2: Let $F(X,Y)$ be any rational formal group law over $\Omega(\underline{A})$, with:

$$F(X,Y) = \frac{P(X,Y)}{Q(X,Y)} \quad , \text{ and,}$$

$$\deg_X(\, Q(X,Y)\,) = \deg_X(\, P(X,Y)\,) \quad , \text{ then:}$$

there exists another rational-formal group law, $F'(X,Y)$, over $\Omega(\underline{A})$, which satisfies:

i. $\deg_X(\, Q'(X,Y)\,) < \deg_X(\, Q(X,Y)\,)$, where:

$$F'(X,Y) = \frac{P'(X,Y)}{Q'(X,Y)} \quad , \text{ and,}$$

ii. $F(X,Y)$ and $F'(X,Y)$ are isomorphic formal group laws.

Proof: We shall show that for a suitable $\alpha\in\Omega(\underline{A})$, $F_\alpha(X,Y)$ satisfies i. and ii.

Obviously, for any $\alpha\in\Omega(\underline{A})$, $F_\alpha(X,Y)$ is isomorphic to $F(X,Y)$, hence, it suffices to find an $\alpha_0\in\Omega(\underline{A})$ such that:

$$\deg_X(\, \overline{Q}_{\alpha_0}(X,Y)\,) < \deg_X(\, Q(X,Y)\,)$$

By Lemma 2.5.1 we have:

$$a_{r0}(\alpha)\cdot\overline{b}_{1m}(\alpha) = \overline{b}_{rm}(\alpha) \quad , \text{ for } 0 \leq r \leq m \ .$$

Now,

$$\overline{b}_{1m}(\alpha) = \sum_{\substack{u+v=1 \\ 0\leq u,v\leq m}} \sum_{\substack{p+q=m \\ 0\leq p,q\leq m}} (-\alpha)^{p+u}\cdot\binom{m-v}{u}\cdot\binom{m-q}{p}\cdot b_{vq} +$$

$$+ \alpha\cdot\left(\sum_{\substack{k+s=1 \\ 0\leq k,s\leq m}} \sum_{\substack{\ell+t=m \\ 0\leq \ell,t\leq m}} (-\alpha)^{\ell+k}\cdot\binom{m-s}{k}\cdot\binom{m-t}{\ell}\cdot a_{st}\right)$$

$$= \sum_{p=0}^{m} (-\alpha)^p\, b_{1m-p} + (-\alpha)^{p+1}\cdot\binom{m}{1}\cdot b_{0m-p} +$$

$$+ \sum_{\ell=0}^{m} (-1)^{\ell}\cdot(\alpha)^{\ell+1}\cdot a_{1m-\ell} + (-1)^{\ell+1}\cdot(\alpha)^{\ell+2}\cdot\binom{m}{1}\cdot a_{0m-\ell} \ .$$

Clearly, the coefficient of α^{m+1} in $\overline{b}_{1m}(\alpha)$ is:

$$(-1)^{m+1}\cdot\binom{m}{1}\cdot b_{00} + (-1)^m\cdot a_{10} + (-1)^m\cdot\binom{m}{1}\cdot a_{01}$$

$$= (-1)^m \quad ,$$

and so, $\bar{b}_{1m}(\alpha)$ is not a constant polynomial in α.

Thus, there exists $\alpha_0 \in \Omega(\underline{A})$ such that:

$$\bar{b}_{1m}(\alpha_0) = 0$$

Hence:

$$\bar{b}_{rm}(\alpha_0) = 0 \quad , \text{ for all } 0 \leq r \leq m \quad (\text{ by Lemma 2.5.1 }),$$

and, by symmetry,

$$\bar{b}_{mr}(\alpha_0) = 0 \quad , \text{ for all } 0 \leq r \leq m \ .$$

It follows immediately that,

$$\deg_X(\bar{Q}_{\alpha_0}(X,Y)) \leq m-1 \quad ,$$

ie. $$\deg_X(\bar{Q}_{\alpha_0}(X,Y)) < \deg_X(Q(X,Y)) \ . \qquad \blacksquare$$

Theorem 2.5.3: Suppose that $F(X,Y)$ is a rational formal group law over $\Omega(\underline{A})$, then,

$$F(X,Y) = \frac{X + Y + aXY}{1 + bXY} \quad , \text{ for some } a,b \in \Omega(\underline{A}) \ .$$

Proof: Clearly, in view of Lemma 2.4.3 , it suffices to show $F(X,Y)$ is isomorphic to some polynomial formal group law by $\Psi_\alpha(X)$ for some $\alpha \in \Omega(\underline{A})$.

We have,

$$F(X,Y) = \frac{P(X,Y)}{Q(X,Y)} \quad , \text{ where: } \quad \deg_X(P(X,Y)) = m \ .$$

By Proposition 2.3.2, if,

$$\deg_X(Q(X,Y)) < m \quad ,$$

then, $F(X,Y)$ is actually a polynomial formal group law,

ie. $$Q(X,Y) = 1 \ .$$

Thus, suppose that we have:

$$\deg_X(Q(X,Y)) = m \ .$$

(Note that it is impossible, by Theorem 2.2.2, to have,

$$\deg_X(Q(X,Y)) > \deg_X(P(X,Y)) \ . \ )$$

We may now apply Lemma 2.5.2 to $F(X,Y)$, obtaining:

$$F_{\alpha_0}(X,Y) = \frac{P_{\alpha_0}(X,Y)}{\overline{Q}_{\alpha_0}(X,Y)} \quad ,$$

where: $\deg_X(\ \overline{Q}_{\alpha_0}(X,Y)\ ) < \deg_X(\ Q(X,Y)\ )$

Now, if: $\deg_X(\ P_{\alpha_0}(X,Y)\ ) > \deg_X(\ \overline{Q}_{\alpha_0}(X,Y)\ )$,

then, $F_{\alpha_0}(X,Y)$ is a polynomial formal group law (by Proposition 2.3.2), and, hence, $F(X,Y)$ is isomorphic to a polynomial formal group law.

If, however, we have

$$\deg_X(\ P_{\alpha_0}(X,Y)\ ) = \deg_X(\ \overline{Q}_{\alpha_0}(X,Y)\ ) \quad ,$$

then, writing:

$$P_0(X,Y) = P_{\alpha_0}(X,Y) \quad ,$$

$$\overline{Q_0}(X,Y) = \overline{Q}_{\alpha_0}(X,Y) \quad , \text{ and},$$

$$F_0(X,Y) = F_{\alpha_0}(X,Y) \quad ,$$

we may apply Lemma 2.5.2 to the group law $F_0(X,Y)$, obtaining:

$$(F_0)_{\alpha_1}(X,Y) = \frac{(P_0)_{\alpha_1}(X,Y)}{(Q_0)_{\alpha_1}(X,Y)}$$

By the obvious computation,

$$(F_0)_{\alpha_1}(X,Y) = F_{\alpha_0+\alpha_1}(X,Y) \quad ,$$

and so we shall write,

$$F_1(X,Y) = F_{\alpha_0+\alpha_1}(X,Y) \quad ,$$

$$P_1(X,Y) = P_{\alpha_0+\alpha_1}(X,Y) \quad , \text{ and},$$

$$Q_1(X,Y) = \overline{Q}_{\alpha_0+\alpha_1}(X,Y) \quad .$$

As before, by Proposition 2.3.2 , if,

$$\deg_X(\ P_1(X,Y)\ ) > \deg_X(\ Q_1(X,Y)\ ) \quad ,$$

then, $F_1(X,Y)$ is a polynomial formal group law.

On the other hand, if we have:

$$\deg_X(P_1(X,Y)) = \deg_X(Q_1(X,Y)) \quad ,$$

then, we may apply Lemma 2.5.2 to $F_1(X,Y)$, obtaining, in the obvious notation:

$$F_1(X,Y) = \frac{P_1(X,Y)}{Q_1(X,Y)} \quad ,$$

a rational formal group law isomorphic to $F(X,Y)$.

In this fashion, we may build up a sequence of rational formal group laws, each isomorphic to the orginal group law $F(X,Y)$:

Define: $F_0(X,Y) = F_{\alpha_0}(X,Y)$,

now, for each $k \in \underline{N}$, define:

if, $\deg_X(P_{k-1}(X,Y)) > \deg_X(Q_{k-1}(X,Y))$,

then: $F_k(X,Y) = F_{k-1}(X,Y)$,

ie. $P_k(X,Y) = P_{k-1}(X,Y)$ and, $Q_k(X,Y) = Q_{k-1}(X,Y)$;

and, if we have,

$$\deg_X(P_{k-1}(X,Y)) = \deg_X(Q_{k-1}(X,Y)) \quad ,$$

then, apply Lemma 2.5.2 to $F_{k-1}(X,Y)$, and set:

$$F_k(X,Y) = (F_{k-1})_{\alpha_k}(X,Y) \quad ,$$

$$P_k(X,Y) = (P_{k-1})_{\alpha_k}(X,Y) \quad , \text{ and,}$$

$$Q_k(X,Y) = (Q_{k-1})_{\alpha_k}(X,Y) \quad .$$

Obviously, if the sequence, $\{F_k(X,Y)\}_{k=0}^{\infty}$, of rational formal group laws, eventually becomes a constant sequence,

ie. for all $k \geq \ell$, say, $F_k(X,Y) = F_{k-1}(X,Y)$,

then, $F_\ell(X,Y)$ is actually a polynomial formal group law .

Hence, since $F_\ell(X,Y)$ is isomorphic to $F(X,Y)$ under the isomorphism given by $\Psi_\beta(X)$, where,

$$\beta = \sum_{k=0}^{\ell} a_k \quad ,$$

to prove the theorem, it suffices to show that for any rational formal group law, $F(X,Y)$, the derived sequence, $\{F_k(X,Y)\}_{k=0}^{\infty}$, is eventually constant.

Suppose, for a contradiction, that $F(X,Y)$ is a rational formal group law for which the sequence, $\{F_k(X,Y)\}_{k=0}^{\infty}$, is not eventually constant.

Let: $\deg_X(P(X,Y)) = m$.

We must have,

$$\deg_X(P_k(X,Y)) = \deg_X(Q_k(X,Y)) \quad ; \text{ for all } k \in \underline{N} \ ,$$

and also,

$$\deg_X(Q_k(X,Y)) > \deg_X(Q_{k+1}(X,Y)), \text{ for all } k \in \underline{N}$$

Hence, it follows directly that:

$$\deg_X(P_k(X,Y)) > \deg_X(P_{k+1}(X,Y)), \text{ for all } k \in \underline{N} \ .$$

But, this implies that:

$$\deg_X(P_k(X,Y)) < 0 \quad , \text{ for all } k > m \ .$$

This is impossible, since the numerator of any rational formal group law must have degree in X at least 1, and, obviously for each $k \in \underline{N}$, $F_k(X,Y)$ is a rational formal group law. Contradiction !

Therefore, for any rational formal group law, $F(X,Y)$, the derived sequence,

$$\{F_k(X,Y)\}_{k=0}^{\infty} \quad ,$$

is eventually constant.

Hence, every rational formal group law is isomorphic to a polynomial formal group law, and so, the required result now follows directly from Lemma 2.4.3

∎

Corollary 2.5.4: A rational function $F(X,Y)$ over a field $^{\circ}\underline{A}$ is a rational formal group law over $\underline{A}$ iff :

$$F(X,Y) = \frac{X + Y + aXY}{1 + bXY} \quad , \text{ for some } a,b \in \underline{A} .$$

Proof: As in the proof of Lemma 2.5.1, let,

$$\pi : \underline{A} \longrightarrow \Omega(\underline{A}) \quad ,$$

be the natural inclusion of $\underline{A}$ in its algebraic closure $\Omega(\underline{A})$, and, let:

$$\tilde{\pi} : \underline{A}((X,Y)) \longrightarrow \Omega(\underline{A})((X,Y)) \quad ,$$

be the extended inclusion.

To prove the result of the corollary, we shall make use of this embedding, applying the theorem to the image $\tilde{F}(X,Y)$ of $F(X,Y)$. This tells us that for some $a,b \in \Omega(\underline{A})$, we have:

$$\tilde{F}(X,Y) = \frac{X + Y + aXY}{1 + bXY}$$

In fact, we are dealing with the power series:

$$\tilde{F}(X,Y) = (X + Y + aXY) \cdot \left(\sum_{i=0}^{\infty} (bXY)^i \right)$$

ie. $$\tilde{F}(X,Y) = X + Y + aXY + bX^2Y + bXY^2 + ab(XY)^2 + \ldots\ldots$$

Now, suppose that we have,

$$F(X,Y) = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} a_{ij} X^i Y^j \quad , \quad a_{ij} \in \underline{A} \text{ for all } i,j \geq 0 .$$

By the definition of $\tilde{\pi}$ we have,

$$\tilde{F}(X,Y) = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \pi(a_{ij}) \cdot X^i \cdot Y^j \quad ,$$

so that:

$$(X + Y + aXY) \cdot \left(\sum_{i=0}^{\infty} (bXY)^i \right) = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \pi(a_{ij}) \cdot X^i \cdot Y^j$$

Comparing coefficients we see that:

$$\pi(a_{11}) = a \quad , \quad \text{and} \quad , \quad \pi(a_{21}) = b \quad .$$

Define a new rational formal group law:

$$G(X,Y) = \frac{X + Y + a_{11}XY}{1 + a_{21}XY}$$

Clearly, we have:

$$\tilde{G}(X,Y) = \tilde{F}(X,Y)$$

But, the map $\tilde{\pi}$ is an injection ! Hence:

$$F(X,Y) = G(X,Y) \quad ,$$

$$\text{ie.} \quad F(X,Y) = \frac{X + Y + a_{11}XY}{1 + a_{21}XY} \quad .$$

□

CHAPTER 3: THE RATIONAL CATEGORY.

§3.1 The definition:

Throughout this chapter let $\underline{A}$ denote an arbitrary field.

Let $Fg(\underline{A})$ denote the category whose objects are all the formal groups over the field $\underline{A}$, and, whose morphisms are the formal group homomorphisms defined in Chapter 1. Now, a morphism of $Fg(\underline{A})$ is given by a formal power series over $\underline{A}$, and so we define a rational morphism of formal group laws to be a morphism of $Fg(\underline{A})$ given by a formal power series over $\underline{A}$ which is actually a rational function over $\underline{A}$. The logical choice for the category of rational formal group laws over $\underline{A}$ is therefore the subcategory of $Fg(\underline{A})$, $Rat(\underline{A})$ say, whose objects are the rational formal group laws over $\underline{A}$, and, morphisms the rational morphisms of $Fg(\underline{A})$ between them.

The category $Rat(\underline{A})$ is not, in general, a full subcategory of the category $Fg(\underline{A})$:

Lemma 3.1.1: If $\underline{A}$ is a field of characteristic 0, then, the additive formal group law,

$$F_a(X,Y) = X + Y \quad ,$$

and the multiplicative formal group law,

$$F_m(X,Y) = X + Y + XY \quad ,$$

are isomorphic objects of the category $Fg(\underline{A})$, the isomorphisms given by: $\phi_a : F_a \longrightarrow F_m$ the formal power series:

$$\phi_a(X) = \sum_{n=1}^{\infty} \frac{X^n}{n!} \quad , \quad (\text{ie. } \phi_a(X) = e^X - 1),$$

$\phi_m : F_m \longrightarrow F_m$ the formal power series:

$$\phi_m(X) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{X^n}{n} \quad , \quad (\text{ie. } \phi_m(X) = \log(X + 1)).$$

Remarks: i. Neither $\phi_m(X)$ nor $\phi_a(X)$ is a rational function over a field of characteristic 0.

ii. This Lemma generalizes to state:

Over a field of characteristic 0 all commutative formal group laws are isomorphic to the additive group law, and furthermore, if the isomorphism is given by the power series:

$$\phi(X) = \sum_{i=0}^{\infty} a_i X^i \quad , \text{ and, } \quad \psi(X) = \sum_{j=1}^{\infty} b_j X^j \quad ,$$

with: $a_1 = 1$,

then, $b_1 = 1$, and , the two power series are unique.

A proof of this may be found in Fröhlich [3] .

§3.2 Rational Isomorphism:

Having defined the category $\mathrm{Rat}(\underline{A})$, one certainly would like to be able to state the necessary and sufficient conditions for two objects of $\mathrm{Rat}(\underline{A})$ to be isomorphic.

Suppose that $F(X,Y)$ and $G(X,Y)$ are two rational formal group laws over $\underline{A}$. Let $f(X)$ and $g(X)$ be two power series over $\underline{A}$, which are actually rational functions. Suppose that:

$$f : F \longrightarrow G \quad , \text{ and,}$$

$$g : G \longrightarrow F \quad ;$$

in $\mathrm{Rat}(\underline{A})$.

By Theorem 1.5.1 , these two maps both produce endomorphisms of the power series ring $\underline{A}((X))$. Denote each of the respective endomorphisms by:

$$\theta_f : \underline{A}((X)) \longrightarrow \underline{A}((X)) \quad , \text{ and,}$$

$$\theta_g : \underline{A}((X)) \longrightarrow \underline{A}((X)) \quad .$$

The same Theorem also shows that $f(X)$ and $g(X)$ produce inverse isomorphisms in $\mathrm{Rat}(\underline{A})$ iff θ_f and θ_g are inverse automorphisms of the power series ring.

In the obvious fashion, we may now define two automorphisms, $\tilde{\theta}_f$ and $\tilde{\theta}_g$, of the field of rational functions over $\underline{A}$ in terms of the maps θ_f and θ_g,

Let $H(X) = \frac{R(X)}{S(X)}$ be any rational function over $\underline{A}$, $R(X)$ and $S(X)$ polynomials over $\underline{A}$. Then, define:

$$\tilde{\theta}_f(H(X)) = \frac{\theta_f(R(X))}{\theta_f(S(X))} \quad , \text{ and,}$$

$$\tilde{\theta}_g(H(X)) = \frac{\theta_g(R(X))}{\theta_g(S(X))}$$

Clearly both the maps $\tilde{\theta}_f$ and $\tilde{\theta}_g$ are well defined, and, furthermore, are inverse automorphisms of the field of rational functions $\underline{A}(X)$. Also, by the definition of the maps θ_f and θ_g, they both fix the base field $\underline{A}$. Hence $\tilde{\theta}_f$ and $\tilde{\theta}_g$ are actually members of the Galois Group of the simple transcendental extention $\underline{A}(X)$ of $\underline{A}$.

It now follows from elementary Galois Theory that, for some $\alpha, \beta, \gamma \in \underline{A}$,

$$\tilde{\theta}_f(X) = \frac{\beta X}{\gamma - \alpha X} \quad , \text{ and,}$$

$$\tilde{\theta}_g(X) = \frac{\gamma X}{\beta + \alpha X} \quad .$$

But, since:

$$\tilde{\theta}_f(X) = \theta_f(X) = f(X) \quad , \text{ and,}$$

$$\tilde{\theta}_g(X) = \theta_g(X) = g(X) \quad ,$$

we have,

$$f(X) = \frac{\beta X}{\gamma - \alpha X} \quad , \text{ and,} \quad g(X) = \frac{\gamma X}{\beta + \alpha X} \quad .$$

(For a proof that the elements of the Galois group of $\underline{A}(X)$ over $\underline{A}$ are just the Möbius transformations over $\underline{A}$, see Van der Waerden [10] pages 217-18.)

Summing up, we have shown:

Theorem 3.2.1: If $F(X,Y)$ and $G(X,Y)$ are any two rational formal group laws over a field $\underline{A}$, then $F(X,Y)$ is isomorphic to $G(X,Y)$ in the category $\mathrm{Rat}(\underline{A})$ iff there exists $\alpha,\beta,\gamma \in \underline{A}$, such that the Möbius transformation,

$$f(X) = \frac{\beta X}{\gamma - \alpha X} \quad , \beta \neq 0 \ ,$$

maps $F(X,Y)$ to $G(X,Y)$ in $\mathrm{Rat}(\underline{A})$.

We have now reduced the problem of necessary and sufficient conditions for isomorphism in $\mathrm{Rat}(\underline{A})$ to the question of the existence of a Möbius transformation. First let us determine necessary conditions for the existance of an ismorphism between two rational formal groups, in the category $\mathrm{Rat}(\underline{A})$:

Suppose that $F(X,Y)$ and $G(X,Y)$ are two rational formal group laws over $\underline{A}$, which are isomorphic under the map induced by:

$$\Phi(X) = \frac{\beta X}{\gamma - \alpha X} \ ,$$

ie. $\Phi : F \longrightarrow G$ in $\mathrm{Rat}(\underline{A})$.

Writing,

$$\Phi^{-1}(X) = \frac{\gamma X}{\beta + \alpha X} \ ,$$

it follows that:

$$F(X,Y) = \Phi^{-1} \circ G(\Phi(X),\Phi(X)) \qquad (*)$$

Now by Theorem 2.5.3 for some $a,b,a',b' \in \underline{A}$, we have:

$$F(X,Y) = \frac{X + Y + a'XY}{1 - b'XY} \quad , \text{ and,}$$

$$G(X,Y) = \frac{X + Y + aXY}{1 - bXY} \ .$$

Substituting for Φ and Φ^{-1} in equation (*), we see that:

$$F(X,Y) = \frac{\gamma \cdot G\left(\frac{\beta X}{\gamma - \alpha X}, \frac{\beta X}{\gamma - \alpha X}\right)}{\beta + \alpha \cdot G\left(\frac{\beta X}{\gamma - \alpha X}, \frac{\beta Y}{\gamma - \alpha Y}\right)}$$

$$F(X,Y) = \frac{\gamma\left((\gamma - \alpha Y)\beta X + (\gamma - \alpha X)\beta Y + a\beta^2 XY\right)}{\beta\left((\gamma - \alpha X)(\gamma - \alpha Y) - b\beta^2 XY\right) + \alpha\left((\gamma - \alpha Y)\beta X + (\gamma - \alpha X)\beta Y + a\beta^2 XY\right)}$$

$$= \frac{\gamma\cdot(\gamma X + \gamma Y + (a\beta - 2\alpha)XY)}{\gamma^2 - (b\beta^2 - a\alpha\beta + \alpha^2)XY}$$

$$= \frac{X + Y + \gamma^{-1}\cdot(a\beta - 2\alpha)\cdot XY}{\gamma - \gamma^{-1}\cdot(b\beta^2 - a\alpha\beta + \alpha^2)XY}$$

But,

$$F(X,Y) = \frac{X + Y + a'XY}{1 - b'XY}$$

so that, we may assume that: $\gamma = 1$,

in which case, we have:

$$a' = a\beta - 2\alpha \quad , \text{ and,}$$

$$b' = b\beta^2 - a\alpha\beta + \alpha^2$$

Now, if the characteristic of the field $\underline{A}$ is 2, then:

$$a' = a\beta$$

However, if $\underline{A}$ is a field of characteristic not 2, then:

$$\alpha = \frac{a\beta - a'}{2} \quad ,$$

so that, substituting we have:

$$b' = b\beta^2 - a\left(\frac{a\beta - a'}{2}\right)\beta + \left(\frac{a\beta - a'}{2}\right)^2 \quad ,$$

ie. $$4b' = 4b\beta^2 - 2a^2\beta^2 + 2aa'\beta + a^2\beta^2 - 2aa'\beta + (a')^2$$

Hence, we have:

$$4b' - (a')^2 = \beta^2(4b - a^2)$$

Conversely, with $F(X,Y)$ and $G(X,Y)$ the formal group laws above, and, $\underline{A}$ any field of characteristic not 2, sufficient conditions for isomorphism in the category $\mathrm{Rat}(\underline{A})$ are immediately produced from the above arguement: if there exists a $\beta \in \underline{A}$ such that:

$$4b' - (a')^2 = \beta^2(4b - a^2) \quad ,$$

then, clearly the Möbius transformation,

$$\phi(X) = \frac{\beta X}{1 - \left[\frac{a\beta - a'}{2}\right]X} \quad ,$$

gives an isomorphism between $F(X,Y)$ and $G(X,Y)$ in the category $\mathrm{Rat}(\underline{A})$.

Define the Discriminant of a rational formal group law $F(X,Y)$,

$$F(X,Y) = \frac{X + Y + aXY}{1 - bXY} \quad ,$$

to be the square class associated to $(4b - a^2)$, if $(4b - a^2) \neq 0$, and, define it to be 0 otherwise.

$$\text{ie.} \quad \mathrm{disc}(F(X,Y)) = \begin{cases} (4b - a^2)\cdot(\underline{A}^{\times})^2 & , \text{ if } 4b - a^2 \neq 0 \ , \\ 0 & , \text{ if } 4b - a^2 = 0 \ . \end{cases}$$

Summing up the above discussion, we have shown:

Theorem 3.2.3: Two rational formal group laws over a field $\underline{A}$ have the same discriminant when they are isomorphic in the category $\mathrm{Rat}(\underline{A})$. If in addition, the characteristic of $\underline{A}$ is different from 2, then we have:

Two rational formal group laws are isomorphic in the category $\mathrm{Rat}(\underline{A})$ iff they have the same discriminant.

Suppose for the remainder of this Chapter, that the characteristic of $\underline{A}$ is different from 2.

With $F(X,Y)$ as above, we have the first consequence of Theorem 3.2.3:

Proposition 3.2.4: In the category $\mathrm{Rat}(\underline{A})$ we have:

i. $F(X,Y)$ is isomorphic to the additive group law,

$$F_a(X,Y) = X + Y \quad ,$$

iff $4b - a^2 = 0$.

ii. $F(X,Y)$ is isomorphic to the multiplicative group law,

$$F_m(X,Y) = X + Y + XY \quad ,$$

iff $a^2 - 4b$ is a non-zero square in $\underline{A}$.

iii. The additive group law is never isomorphic to the multiplicative group law.

Proof: First note that:

$$\text{disc}(\, F_a(X,Y)\,) = 0 \quad , \text{ and,}$$

$$\text{disc}(\, F_m(X,Y)\,) = (-1)\cdot(\underline{A}^{\times})^2 \quad ,$$

and so, parts i. and ii. follow immediately from Theorem 3.2.3 .

Part iii. is clearly true. ∎

If we have:

$$\frac{\underline{A}^{\times}}{(\underline{A}^{\times})^2} = \{1\} \quad ,$$

then we say that the field $\underline{A}$ is quadratically closed .

Note: since the characteristic of $\underline{A}$ is not 2, this is equivalent to every quadratic polynomial over $\underline{A}$ splitting over $\underline{A}$.

Corollary 3.2.5: $\underline{A}$ is quadratically closed iff there are exactly two isomorphism classes in the category $\text{Rat}(\underline{A})$.

Proof: Suppose first that $\underline{A}$ is quadratically closed.

Then, for any $a,b \in \underline{A}$ such that $a^2 - 4b \neq 0$,

$a^2 - 4b$ is a square in $\underline{A}$.

Hence, for such a,b , by theorem 3.2.4, writing:

$$F(X,Y) = \frac{X + Y + aXY}{1 - bXY} \quad ,$$

we have:

$F(X,Y)$ is isomorphic to $F_m(X,Y)$ in $\text{Rat}(\underline{A})$.

Thus the only two isomorphism classes in $\text{Rat}(\underline{A})$ are the additive class and the multiplicative class.

Conversely, suppose that there are only two isomorphism classes in the category $\mathrm{Rat}(\underline{A})$. Then, for all $a,b \in \underline{A}$,

$$a^2 - 4b \quad \text{is a square in } \underline{A}.$$

Choosing the particular case when : $a = 0$,

this implies that for all $b \in \underline{A}$, $-4b$ is a square in $\underline{A}$.

Since 4 is a square in $\underline{A}$, we must have that $-b$ is a square in $\underline{A}$.

Hence, the field $\underline{A}$ is quadratically closed.

§3.3 The Relationship to Quadratic Forms:

As we shall only be considering binary quadratic forms over the field $\underline{A}$, since confusion will be impossible, we shall refer to them as simply quadratic forms. Note: all forms considered will be non-degenerate.

If we disregard, for the moment, the isomorphism class of the additive group law, then we have shown that there exists a one to one correspondence between the isomorphism classes of the category $\mathrm{Rat}(\underline{A})$ and the elements of the square class group of the field $\underline{A}$. It is well known that there is a close connection between the classes of congruent quadratic forms over $\underline{A}$ and the elements of the square class group of $\underline{A}$. The immediate question to answer is : what possible connection is there between the isomorphism classes of $\mathrm{Rat}(\underline{A})$ and the set of all congruence classes of quadratic forms over $\underline{A}$?

Let $F(X,Y)$ be any rational formal group law over $\underline{A}$,

$$\text{ie.} \qquad F(X,Y) = \frac{X + Y + aXY}{1 - bXY} \quad , \text{ for some } a,b \in \underline{A} .$$

Then, we may associate to $F(X,Y)$ the two by two matrix over $\underline{A}$:

$$M(F) = \begin{pmatrix} 1 & \frac{a}{2} \\ \frac{a}{2} & b \end{pmatrix}$$

Of course, the matrix $M(F)$ defines a quadratic form over $\underline{A}$, and, in this

fashion we may associate a quadratic form to the rational formal group law $F(X,Y)$. Since we are excluding the isomorphism class of the additive group law from our discussion, we have:

$$\det(M(F)) = b - \frac{a^2}{4} \neq 0 \quad ,$$

so that we do in fact have a non-degenerate quadratic form.

Clearly this correspondence defines a well defined set map from the set of all rational formal group laws over $\underline{A}$ to the set of all quadratic forms over $\underline{A}$. We can show immediately that this map is injective:

Theorem 3.3.1: Let $F(X,Y)$ and $G(X,Y)$ be any two rational formal group laws over $\underline{A}$. Then, we have:

$F(X,Y)$ is isomorphic to $G(X,Y)$ in the category $\mathrm{Rat}(\underline{A})$ iff the quadratic forms associated to the matrices $M(F)$ and $M(G)$ are congruent.

Proof: First suppose that we are given two isomorphic rational formal group laws,

$$F(X,Y) \quad \text{and} \quad G(X,Y) \quad .$$

Then, there must exist a Mobius transformation,

$$\phi(X) = \frac{\beta X}{1 - \alpha X} \quad , \beta \neq 0 \quad ,$$

such that:

$$F(X,Y) = \phi^{-1}(G(\phi(X),\phi(Y)))$$

Put:

$$M(\phi) = \begin{pmatrix} 1 & -\alpha \\ 0 & \beta \end{pmatrix}$$

and, write:

$$G(X,Y) = \frac{X + Y + aXY}{1 - bXY} \quad , \text{and,} \quad F(X,Y) = \frac{X + Y + a'XY}{1 - b'XY} \quad .$$

Since Φ is an isomorphism, we have previously shown that:

$$a' = a\beta - 2\alpha \quad , \text{ and,}$$

$$b' = \alpha^2 - a\alpha\beta + b\beta^2$$

We also have:

$$M(\phi)^t \cdot M(G) \cdot M(\phi) = \begin{pmatrix} 1 & 0 \\ -\alpha & \beta \end{pmatrix} \begin{pmatrix} 1 & \frac{a}{2} \\ \frac{a}{2} & b \end{pmatrix} \begin{pmatrix} 1 & -\alpha \\ 0 & \beta \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \frac{a\cdot\beta}{2} - \alpha \\ \frac{a\cdot\beta}{2} - \alpha & \alpha^2 - a\alpha\beta + \beta^2 \cdot b \end{pmatrix}$$

Hence,

$$M(F) = M(\phi)^t \cdot M(G) \cdot M(\phi) \quad ,$$

and, since $\beta \neq 0$, we have:

$$\det(M(\phi)) \neq 0 \quad \longrightarrow$$

so that the associated quadratic forms are congruent.

Suppose, on the other hand, that the quadratic forms associated to the matrices $M(F)$ and $M(G)$ are congruent. Then, there exists a two by two matrix B , with,

$$\det(B) \neq 0 \quad ,$$

such that:

$$M(F) = B^t \cdot M(G) \cdot B$$

Hence,

$$\det(M(F)) = \det(B)^2 \cdot \det(M(G)) \quad ,$$

ie. $$\det(M(F)) \equiv \det(M(G)) \mod (\underline{A}^\times)^2 \quad .$$

But,

$$\det(M(F)) = b' - \frac{(a')^2}{4} \quad , \text{ and, } \det(M(G)) = b - \frac{a^2}{4} \quad ,$$

so that:

$$\det(M(F)) \equiv \operatorname{disc}(F(X,Y)) \mod (\underline{A}^\times)^2 \quad , \text{ and,}$$

$$\det(M(G)) \equiv \operatorname{disc}(G(X,Y)) \mod (\underline{A}^\times)^2 \quad .$$

It now follows immediately that:

$$\text{disc}(F(X,Y)) \equiv \text{disc}(G(X,Y)) \mod (\underline{A}^{\times})^2 ,$$

and so, by Theorem 3.2.3, $F(X,Y)$ and $G(X,Y)$ are isomorphic in the category $\text{Rat}(\underline{A})$.

Of course, in general, this map is far from being a bijection of sets. One has only to examine the field of p-adic numbers, for any prime p, to see that there are twice the number of classes of congruent quadratic forms as there are elements in the square class group (see Serre [8]). However, in the case of finite fields, the situation is somewhat different.

If M is a two by two matrix associated to the quadratic form $f(x,y)$, then we may define the classical discriminant to be the element of the square class group given by:

$$\text{Disc}(f(x,y)) = \det(M)\cdot(\underline{A}^{\times})^2 .$$

Clearly, by what we have seen in the above proof of the last Theorem, two quadratic forms over $\underline{A}$ have the same classical discriminant when they are congruent. For the above correspondence to be bijective, it is necessary and sufficient that any two quadratic forms having the same classical discriminant be congruent.

If $\underline{A}$ is a finite field, then this condition is met, and, so any quadratic form over $\underline{A}$ will be congruent to one derived from a rational formal group law. The proof of this result can be found in Serre [8] .

Furthermore, if $\underline{A}$ is a finite field, then, the square class group of $\underline{A}$ has exactly two elements:

Suppose that $\underline{A} = \mathbb{F}_q$, where $q = p^n$, for some prime $p \neq 2$.

Define a group homomorphism on the multiplicative group $\underline{A}$,

$$\phi : \underline{A}^{\times} \longrightarrow \{-1,+1\} ,$$

given by:

$$\phi(a) = a^{\frac{q-1}{2}} \quad , \quad \text{for all } a \in \underline{A} \ .$$

Now, for each $a \in \underline{A}$, there exists $y \in \Omega(\underline{A})$ such that: $y^2 = a$.

Hence, we must have:

$$y^{q-1} = \pm 1$$

If $y^{q-1} = 1$, then, since $\underline{A}$ is the splitting field of the polynomial:

$$X^q - X \quad ,$$

it follows that $y \in \underline{A}$.

On the other hand, if for some $a \in \underline{A}$ we have: $\phi(a) = 1$,

then,

$$y^2 = a \quad \text{implies that} \quad y^{q-1} = 1 \quad ,$$

showing that: $\ker(\phi) = (\underline{A}^\times)^2$

Furthermore, the map ϕ is actually surjective since the polynomial,

$$\phi(X) - 1 \quad ,$$

has at most $\frac{q-1}{2}$ roots in the field $\underline{A}$.

Hence, we have the following short exact sequence of groups and homomorphisms:

$$\{1\} \longrightarrow (\underline{A}^\times)^2 \longrightarrow \underline{A}^\times \longrightarrow \{-1,+1\} \longrightarrow \{1\} \quad ,$$

$$\text{ie.} \quad \frac{\underline{A}^\times}{(\underline{A}^\times)^2} = \{-1,+1\} \ .$$

This discussion directly gives:

Theorem 3.3.2: If $\underline{A}$ is any finite field, then, there are only 3 isomorphism classes of rational formal group laws over $\underline{A}$, in the category $\mathrm{Rat}(\underline{A})$, which have obvious representatives:

$F_a(X,Y) = X + Y$, $F_m(X,Y) = X + Y + XY$, for b a non-square,

$$F_b(X,Y) = \frac{X + Y}{1 - bXY}$$

Proof: Immediate from the above.

§3.4 Some Endomorphism Rings in $\underline{Rat}(\underline{A})$:

So far we have only considered the problem of isomorphism in the category $\underline{Rat}(\underline{A})$. Naturally, one would wish to have some information concerning the structure of the Hom-sets of $\underline{Rat}(\underline{A})$, and, to do this it is necessary to consider the endomorphism rings of the additive and multiplicative group laws,

$$F_a(X,Y) = X + Y \quad , \text{ and } , \quad F_m(X,Y) = X + Y + XY \quad .$$

Note: by Proposition 1.3.1 , we know that the sets $\mathrm{End}_{\underline{Fg}(\underline{A})}(F_a)$ and $\mathrm{End}_{\underline{Fg}(\underline{A})}(F_m)$ are rings, since $\underline{Fg}(\underline{A})$ is a full subcategory of $\underline{Fml}(\underline{A})$, and so, it is obvious that the sets $\mathrm{End}_{\underline{Rat}(\underline{A})}(F_a)$ and $\mathrm{End}_{\underline{Rat}(\underline{A})}(F_m)$ are rings with unit, since composition of rational functions yields rational functions.

Before determining these endomorphism rings, note that it is easy to show that, for any $n \in \underline{Z}$:

$$(n)_{F_a}(X) = n \cdot X \quad , \text{ and } ,$$

$$(n)_{F_m}(X) = (X + 1)^n - 1 \quad .$$

Proposition 3.4.1: Suppose that $\phi(X)$ is a rational function over $\underline{A}$, then:

i. if $\underline{A}$ has characteristic zero ,

$$\phi(X) \in \mathrm{End}_{\underline{Rat}(\underline{A})}(F_a) \text{ iff } \phi(X) = a \cdot X \quad , \text{ for some } a \in \underline{A} \ ,$$

ii. if the characteristic of $\underline{A}$ is p , an odd positive prime,

$$\phi(X) \in \mathrm{End}_{\underline{Rat}(\underline{A})}(F_a) \text{ iff :}$$

$$\phi(X) = \textstyle\sum_{i=0}^{n} a_i \cdot X^{p^i} \text{ for some } a_i \in \underline{A} \quad .$$

Proof: First consider the case when the characteristic of $\underline{A}$ is zero.

Suppose that $\phi(X) \in \mathrm{End}_{\underline{Rat}(\underline{A})}(F_a)$, then, we must have (see §1.3) :

$$\phi \circ (n)_{F_a} = (n)_{F_a} \circ \phi \quad , \text{ for all } n \in \underline{Z} \ .$$

ie. $\phi(nX) = n\cdot(\phi(X))$

Hence, $\phi(X) = a\cdot X$, for some $a\in\underline{A}$.

Conversely, it is obvious that: $\phi(X) = a\cdot X\in End_{Rat(\underline{A})}(F_a)$ for all $a\in\underline{A}$.

Now assume that the characteristic of $\underline{A}$ is p, an odd positive prime. Suppose that the rational function, $\phi(X)$, is an endomorphism of the additive group law, in $Rat(\underline{A})$. Then, we see that:

$$\phi(X + Y) = \phi(X) + \phi(Y) \quad ,$$

since: $\phi(F_a(X,Y)) = F_a(\phi(X),\phi(Y))$.

Put:

$$\phi(X) = \sum_{i=1}^{\infty} a_i\cdot X^i \quad , \qquad a_i\in\underline{A} \quad .$$

(Recall: $\phi(X)$, while being a rational function over $\underline{A}$, must also be representable as a formal power series.)

We must have:

$$\sum_{i=1}^{\infty} a_i\cdot(X + Y)^i = \sum_{j=1}^{\infty} a_j\cdot X^j + \sum_{k=1}^{\infty} a_k\cdot Y^k \quad .$$

This implies that:

$$a_i\cdot\binom{i}{\ell} = 0 \quad , \text{ for all } i\geq 2 \text{ , and all } 0 < \ell < i \quad .$$

Obviously, if $i \neq p^n$, $n>0$, there exists ℓ, $0 < \ell < i$, such that,

$$\binom{i}{\ell} \neq 0$$

Hence, if $i \neq p^n$, for some $n\geq 0$, then: $a_i = 0$,

so that, writing: $b_j = a_{pj}$, for $j\geq 0$,

$$\phi(X) = \sum_{j=0}^{\infty} b_j\cdot X^{pj} \quad .$$

If $\phi(X)$ is to be a morphism in the category $Rat(\underline{A})$, then it must be a rational function, that is, there exist polynomials $p(X)$ and $q(X)$, and:

$$\phi(X) = \frac{p(X)}{q(X)}$$

Thus: $p(X) = \phi(X) \cdot q(X)$,

and so, writing,

$$p(X) = \sum_{r=1}^{\ell} c_r \cdot X^r \quad , \text{ and } , \quad q(X) = \sum_{s=0}^{m} d_s \cdot X^s \quad ,$$

we have:

$$\sum_{r=1}^{\ell} c_r \cdot X^r = \left(\sum_{j=0}^{\infty} b_j X^{p^j} \right) , \left(\sum_{s=0}^{m} d_s \cdot X^s \right)$$

Choose $k \in \underline{N}_0$ such that:

$$p^k + m > \ell \quad , \text{ and } , \quad p^{k+1} - p^k > m$$

Clearly this choice of k ensures that the the coefficient of X^{p^j+m} in the expansion of the right hand side of the above equation is:

$$b_j d_m \quad ,$$

whenever we have: $j > k$.

Since we may assume, with out loss of generality that: $d_m \neq 0$,

it follows immediately that:

$$b_j = 0 \quad , \text{ for all } j>k \quad ,$$

since the degree of the left hand side is ℓ .

Hence:

$$\phi(X) = \sum_{j=0}^{k} b_j \cdot X^{p^j}$$

Conversely, given any polynomial,

$$\phi'(X) = \sum_{j=0}^{n} b'_j \cdot X^{p^j} \quad ,$$

since,

$$(X + Y)^{p^t} = X^{p^t} + Y^{p^t} \quad , \text{ for all } t \in \underline{N}_0 \quad ,$$

ϕ' obviously determines an endomorphism of the additive group law .

Remarks: We have shown above that if the characteristic of the field $\underline{A}$ is zero, then:

$$\text{End}_{\text{Rat}(\underline{A})}(F_a) = \text{End}_{\text{Fg}(\underline{A})}(F_a)$$

Furthermore, $\mathrm{End}_{\mathrm{Rat}(\underline{A})}(F_a)$ is a field, in this case, isomorphic to $\underline{A}$.

Note that none of these comments are true for the case when $\underline{A}$ has characteristic an odd positive prime. Here all we can note is that $\mathrm{End}_{\mathrm{Rat}(\underline{A})}(F_a)$ is a non-commutative ring, with unit.

Before computing the rational endomorphism ring of the multiplicative group law, we shall need to prove the following Lemma:

Lemma 3.4.2: Let $q(X)$ be a polynomial over the algebraically closed field $\Omega(\underline{A})$, with constant term 1. Then:

$q(X)$ satisfies the functional equation,

$$q((X+1)^n - 1) = q(X)^n \quad ,$$

for all $n \in \underline{N}_0$, iff:

$$q(X) = 1 \quad , \text{ or, } \quad q(X) = (X+1)^m \quad , \text{ for some } m \in \underline{N} \; .$$

Proof: Suppose that $q(X)$ is a polynomial over $\Omega(\underline{A})$, with constant term 1, and, we have:

$$q((X+1)^n - 1) = q(X)^n \quad , \text{ for all } n \in \underline{N}_0 \; .$$

Since this equation is trivially satisfied if $q(X) \equiv 1$, we shall assume that $q(X)$ is a non-constant polynomial.

Thus, there exists at least one $x_0 \in \Omega(\underline{A})$ such that:

$$q(x_0) = 0 \quad ,$$

and so, for each $n>0$, we must have:

$$q((x_0+1)^n - 1) = 0 \; .$$

But, $q(X)$ is a polynomial, so that, the expression,

$$(x_0+1)^n - 1 \quad ,$$

must only assume a finite number of distinct values in $\Omega(\underline{A})$.

Thus, there exist integers m and m', with, $m'>m>0$, such that:

$$(x_0 + 1)^m - 1 = (x_0 + 1)^{m'} - 1 \quad ,$$

ie. $$(x_0 + 1)^m = (x_0 + 1)^{m'} \quad .$$

Assume, for a contradiction, that: $x_0 \neq -1$.

Then, we may divide both sides of the above equation by $(x_0 + 1)^m$:

$$1 = (x_0 + 1)^{m'-m} \quad .$$

But, $m'-m$ is a positive integer, and so, we have:

$$q((x_0 + 1)^{m'-m} - 1) = 0 \quad ,$$

ie. $$q(0) = 0 \quad .$$

We now have a contradiction, since $q(X)$ has constant term 1 !

Therefore the only possible root of $q(X)$ is: $x_0 = -1$.

Hence, we must have:

$$q(X) = (X + 1)^k \quad , \text{ for some } k \in \underline{N} \quad .$$

Conversely, for any $n \in \underline{N}_0$, the polynomial:

$$(X + 1)^n \quad ,$$

obviously satisfies the required functional equation, and, has constant term 1 .

∎

We may now look at the ring $\mathrm{End}_{\mathrm{Rat}(\underline{A})}(F_m)$:

Proposition 3.4.3: Suppose that $\phi(X)$ is a rational function over $\Omega(\underline{A})$. Then:

$$\phi(X) \in \mathrm{End}_{\mathrm{Rat}(\Omega(\underline{A}))}(F_m) \text{ iff } \phi(X) = (n)_{F_m} \quad , \text{ for some } n \in \underline{Z} \quad .$$

Proof: Let $\phi(X)$ be a rational function over $\Omega(\underline{A})$, with $p(X)$ and $q(X)$ two polynomials over $\Omega(\underline{A})$, relatively prime; and, such that:

$$\phi(X) = \frac{p(X)}{q(X)}$$

Suppose that $\phi(X)$ is an endomorphism of the multiplicative group law,

$$F_m(X,Y) = X + Y + XY \quad .$$

By definition, we must be able to express $\phi(X)$ as a formal power series in X with zero constant term. Hence, we have that: $p(0) = 0$ and, we may assume, with out loss of generality that: $q(0) = 1$.

As $\phi(X)$ is an endomorphism of the multiplicative group law, we have:

$$\phi \circ (n)_{F_m} = (n)_{F_m} \circ \phi \quad , \text{ for all } n \in \underline{Z} \ ,$$

so that $\phi(X)$ must satisfy, for each $n \in \underline{N}$, the functional equation:

$$\phi((X + 1)^n - 1) = (\phi(X) + 1)^n - 1 \ .$$

This immediately gives us:

$$p((X + 1)^n - 1) = q((X + 1)^n - 1) \cdot \left[\left(\frac{p(X)}{q(X)} + 1 \right)^n - 1 \right] \ ,$$

ie $0 = p((X + 1)^n - 1) \cdot q(X)^n - q((X + 1)^n - 1) \cdot \left[(p(X) + q(X))^n - q(X)^n \right]$.

Thus, $q((X + 1)^n - 1)$ must divide the right hand side of the above equation. But, since $p(X)$ and $q(X)$ are relatively prime,

$$q((X + 1)^n - 1) \mid p((X + 1)^n - 1) \ ,$$

unless: $q(X) \equiv 1$.

Suppose that $q(X) \not\equiv 1$, then it follows that:

$$q((X + 1)^n - 1) \mid q(X)^n \ .$$

Obviously, both $q((X + 1)^n - 1)$ and $q(X)^n$ have the same degree, for any $n \in \underline{N}$. Thus, for each $n \in \underline{N}$, there exists $k_n \in \Omega(\underline{A})$ such that:

$$q(X)^n = k_n \cdot q((X + 1)^n - 1) \ . \qquad (*)$$

Writing,

$$q(X) = \sum_{i=0}^{\ell} b_i \cdot X^i \ ,$$

we have, for each $n \in \underline{N}$,

$$q((X + 1)^n - 1) = \sum_{i=0}^{\ell} b_i \cdot ((X + 1)^n - 1)^i \ ,$$

showing that the constant term of $q((X + 1)^n - 1)$ is just: $b_0 = 1$.

On the other hand, the constant term of $q(X)^n$ is simply ; $b_0^n = 1$.

Equation (*) above implies:

$$k_n \cdot b_0 = b_0^n \quad ,$$

ie. $k_n = 1$, for all $n \geq 1$.

It follows that:

$$q((X + 1)^n - 1) = q(X)^n \quad , \text{ for all } n \geq 1 \ ,$$

and so, applying Lemma 3.4.2 , we see that:

$$q(X) = (X + 1)^{\ell} \quad , \text{ for some } \ell \in \underline{N}_0 \ .$$

The proof now splits into two cases: when $\phi(X)$ is a polynomial, and, when $\ell > 0$.

Case i. Suppose that $\ell = 0$, that is, $\phi(X)$ is a polynomial,

$$\phi(X) = p(X) \ .$$

We may write the multiplicative group law in a slightly different way:

$$F_m(X,Y) = (X + 1) \cdot (Y + 1) - 1 \ .$$

With this in mind, since $p(X)$ is an endomorphism of $F_m(X,Y)$ one must have:

$$p((X + 1) \cdot (Y + 1) - 1) = (p(X) + 1) \cdot (p(Y) + 1) - 1 \ .$$

Setting $Y = -1$, we immediately have:

$$p(-1) = (p(X) + 1) \cdot (p(-1) + 1) - 1 \ ,$$

from which it immediately follows that:

$$p(X) = 0 \quad , \text{ or } , \quad p(-1) = -1 \ .$$

If $p(X) = 0$, then:

$$\phi(X) = (0)_{F_m}(X) \ .$$

Suppose that: $p(X) \neq 0$, that is: $p(-1) = -1$.

Let $a \in \Omega(\underline{A})$ be a root of the polynomial: $p(X) + 1$.

Then, it follows that:

$$p((X + 1) \cdot (a + 1) - 1) = -1 \ .$$

Hence, $(X + 1) \cdot (a + 1) - 1$ must be a constant polynomial, ie. $a = -1$.

Therefore, for some $\ell \in \underline{N}$,

$$p(X) + 1 = (X + 1)^{\ell}$$

that is:

$$\phi(X) = (\ell)_{F_m}(X)$$

Case ii. Suppose now that $\phi(X)$ is not a polynomial, ie. $\ell \neq 0$. Since $\phi(X)$ is an endomorphism of $F_m(X,Y)$, for each $n \in \underline{N}_0$, we may define:

$$\phi_n(X) = F_m(\phi(X),(n)_{F_m}) \quad ,$$

ie.
$$\phi_n(X) = \left(\frac{p(X)}{(X+1)^{\ell}} + 1\right) \cdot (1 + (X+1)^n - 1) - 1$$

$$= \left(\frac{p(X)}{(X+1)^{\ell}} + 1\right) \cdot (X+1)^n - 1 \quad ,$$

which is clearly an endomorphism of $F_m(X,Y)$.

Consider the case when $n = \ell$.

Obviously,

$$\phi_{\ell}(X) = (X+1)^{\ell} + p(X) - 1 \quad ,$$

and, since $\phi_{\ell}(X)$ is an endomorphism, Case i above implies that there exists $t \in \underline{N}_0$ such that:

$$\phi_{\ell}(X) = (X+1)^t - 1 \quad .$$

Hence:

$$p(X) = (X+1)^t - (X+1)^{\ell} \quad .$$

Clearly, we must have: $t \leq \ell$, and so:

$$\phi(X) = \frac{(X+1)^t \cdot (1 - (X+1)^{\ell - t})}{(X+1)^{\ell}} \quad .$$

But, we have assumed that $p(X)$ and $q(X)$ are relatively prime, and so, it follows that: $t = 0$

Hence, we have shown:

$$\phi(X) = (-\ell)_{F_m}(X) \quad .$$

We have now demonstrated the necessity in our proposition, clearly the sufficiency is trivial.

∎

Corollary 3.4.4: If $\phi(X)$ is a rational function over $\underline{A}$, then:

$$\phi(X) \in \mathrm{End}_{\mathrm{Rat}(\underline{A})}(F_m) \text{ iff } \phi(X) = (n)_{F_m}(X) \text{ , for some } n \in \underline{Z} \; .$$

Proof: Obvious, since the category $\mathrm{Rat}(\underline{A})$ is a subcategory of the category $\mathrm{Rat}(\Omega(\underline{A}))$.

∎

Remarks: We have shown that for any field $\underline{A}$, the ring of endomorphisms of the multiplicative group law is isomorphic to the ring of integers. This is completely unlike the case when we considered the additive group law, and, is somewhat simpler, as the result is not complicated by consideration of the characteristic of the field in question.

§3.5 The Morphisms of $\mathrm{Rat}(\underline{A})$:

We have already mentioned that $\mathrm{Rat}(\underline{A})$ is a subcategory of the category $\mathrm{Rat}(\Omega(\underline{A}))$. Bearing this in mind, the morphisms of the larger category will be used to gain some information concerning those of the smaller category.

Suppose that $F(X,Y)$ and $G(X,Y)$ are two rational formal group laws over the field $\Omega(\underline{A})$, and, $h(X)$ is a rational function over $\Omega(\underline{A})$ giving a morphism in the category $\mathrm{Rat}(\Omega(\underline{A}))$,

$$h : F(X,Y) \longrightarrow G(X,Y) \quad .$$

By Corollary 3.2.5, we know that there exist two non-zero Möbius transformations over $\Omega(\underline{A})$,

$$m(X) = \frac{\beta X}{1 - \alpha X} \quad , \text{ and, } \quad m'(X) = \frac{\beta' X}{1 - \alpha' X} \quad ,$$

such that one of the following four statements is true:

i. $F(X,Y)$ and $G(X,Y)$ are both isomorphic to the additive group law,

ii. $F(X,Y)$ and $G(X,Y)$ are both isomorphic to the multiplicative group law,

iii. $F(X,Y)$ is isomorphic to the additive group law, and, $G(X,Y)$ is isomorphic to the multiplicative group law, and, lastly,

iv. statement iii. holds, but, with the roles of $F(X,Y)$ and $G(X,Y)$ interchanged,

where, in each case, the isomorphisms are given by $m(X)$ and $m'(X)$, respectively.

Clearly we need only examine the first three cases above to compute $h(X)$.

Case i. Suppose that $F(X,Y)$ and $G(X,Y)$ are both isomorphic to the additive group law. We have the following commutative square:

$$\begin{array}{ccc} F(X,Y) & \xrightarrow{\quad h \quad} & G(X,Y) \\ {\scriptstyle m}\downarrow & & \downarrow{\scriptstyle m'} \\ F_a(X,Y) & \xrightarrow{\quad \phi \quad} & F_a(X,Y) \end{array}$$

where $\phi(X)$ is the endomorphism of $F_a(X,Y)$ induced by $h(X)$,

ie. $\phi(X) = m' \circ hom^{-1}(X)$.

Hence, we have:

$$h(X) = (m')^{-1} \circ \phi \circ m(X) \quad .$$

The computation of $h(X)$ now splits into two cases:

Suppose that the characteristic of $\Omega(\underline{A})$ is zero. Then, we have:

$$\phi(X) = c \cdot X \quad , \text{ for some } c \in \Omega(\underline{A}) \quad .$$

By simple computation, it follows that:

$$h(X) = \frac{c\beta X}{\beta' + (\alpha'\beta c - \alpha\beta') \cdot X} \quad ,$$

and so we see that, in this case, the only possible morphisms between $F(X,Y)$ and $G(X,Y)$ are isomorphisms, or, in the case when $c = 0$,

the zero morphism.

If the characteristic of $\Omega(\underline{A})$ is not zero, then we no longer have this nice a result. For, if $\Omega(\underline{A})$ has characteristic p, an odd positive prime, then, for some $n \in \underline{N}_0$, and, some $a_i \in \Omega(\underline{A})$, $0 \leq i \leq n$:

$$\phi(X) = \sum_{i=0}^{n} a_i \cdot X^{p^i} \quad ,$$

so that,

$$h(X) = (m')^{-1} \circ \phi(m(X)) \quad ,$$

$$\text{ie.} \quad h(X) = \frac{\sum_{j=0}^{n} a_j \cdot (1 - \alpha X)^{p^m - pj} \cdot (\beta X)^{pj}}{\beta'(1 - \alpha X)^{p^n} + \alpha' \left[\sum_{i=0}^{n} a_i \cdot (1 - \alpha X)^{p^n - p^i} \cdot (\beta X)^{p^i} \right]}$$

Unfortunately, this expression for $h(X)$ does not simplify in general. If, however, $n = 0$, then, either $h(X)$ is an isomorphism, or, the zero morphism.

Case ii. Suppose that we have the following commutative diagram in the category $\mathrm{Rat}(\Omega(\underline{A}))$:

$$\begin{array}{ccc} F(X,Y) & \xrightarrow{\quad h \quad} & G(X,Y) \\ {\scriptstyle m}\downarrow & & \downarrow{\scriptstyle m'} \\ F_m(X,Y) & \xrightarrow{\quad \phi \quad} & F_m(X,Y) \end{array}$$

where, as before,

$$\phi(X) = m' \circ h(m^{-1}(X)) \quad ,$$

is the induced endomorphism of $F_m(X,Y)$.

In this case, regardless of the characteristic of $\Omega(\underline{A})$,

$$\phi(X) = (X + 1)^n - 1 \quad , \text{ for some } n \in \underline{Z} \quad ,$$

by Proposition 3.4.3 .

We can immediately see that, if $n > 0$, then:

$$h(X) = \frac{((\beta - \alpha) \cdot X + 1)^n - (1 - \alpha X)^n}{\beta'(1 - \alpha X)^n + \alpha' \left[((\beta - \alpha) \cdot X + 1)^n - (1 - \alpha X)^n \right]} \quad ,$$

in particular, when $n = 1$, we have an isomorphism in $\mathrm{Rat}(\underline{(A)})$.

On the other hand, if $n<0$, then:

$$h(X) = \frac{(1 - \alpha X)^{-n} - ((\beta - \alpha)\cdot X + 1)^{-n}}{\beta'((\beta - \alpha)\cdot X + 1)^{-n} + \alpha'\left((1 - \alpha X)^{-n} - ((\beta - \alpha)\cdot X + 1)^{-n}\right)} ,$$

giving an isomorphism when $n = -1$.

Clearly, if $n = 0$, then we have the zero morphism.

Note that for $n \neq 0$ the above expressions do not in general simplify.

Case iii. Suppose that we have in fact a morphism,

$$\phi : F_a(X,Y) \longrightarrow F_m(X,Y) ,$$

given by the composition:

$$\phi(X) = m'oh(m(X))$$

We must have, for any $n\epsilon\underline{Z}$:

$$\phi o(n)_{F_a} = (n)_{F_m} o\phi ,$$

that is, $\phi(X)$ must satisfy the functional equation:

$$\phi(n\cdot X) = (\phi(X) + 1)^n - 1$$

Now, there exist polynomials $p(X)$ and $q(X)$ over $\Omega(\underline{A})$ such that:

$$\phi(X) = \frac{p(X)}{q(X)} ,$$

with, $p(X)$ and $q(X)$ relatively prime, and, $q(0) = 1$.

The above functional equation states that, for all $n\epsilon\underline{Z}$,

$$\frac{p(nX)}{q(nX)} = \left(\frac{p(X)}{q(X)} + 1\right)^n - 1 ,$$

so that:

$$q(X)^n\cdot p(nX) = q(nX)\cdot\left((p(X) + q(X))^n - q(X)^n\right) .$$

Suppose that $n>0$, then, it follows immediately from the above that:

$$q(X) \mid q(nX)\cdot\left(\sum_{i=1}^{n}\binom{n}{i}\cdot p(X)^i\cdot q(X)^{n-i}\right) ,$$

and so, since $p(X)$ and $q(X)$ are relatively prime, we may conclude:

$$q(X) \mid q(nX) \quad .$$

Clearly: $q(0) = q(n \cdot 0)$, and, $\deg_X q(X) = \deg_X q(nX)$,

whenever n is not equal to the characteristic of $\Omega(\underline{X})$.

Therefore, $q(X) \equiv 1$,

that is, $\phi(X)$ is actually a polynomial over $\Omega(\underline{A})$.

Now suppose that $n<0$, with, the characteristic of $\Omega(\underline{A})$ is different from $|n|$. We must have:

$$\phi(nX) = (\phi(X) + 1)^n - 1$$

If $\phi(X)$ is a non-constant polynomial, then, $\phi(nX)$ is also non- constant. But, $(\phi(X) + 1)^n - 1$ is certainly not a polynomial over $\Omega(\underline{A})$!

Hence, $\phi(X) \equiv 0$.

Therefore, in this case, the only morphism between $F(X,Y)$ and $G(X,Y)$ in the category $\mathrm{Rat}(\Omega(\underline{A}))$ is the zero morphism.

Summing up these discussions, we have:

Theorem 3.5.1: If $F(X,Y)$ and $G(X,Y)$ are any two rational formal group laws over $\Omega(\underline{A})$, then:

i. if $F(X,Y)$ is isomorphic in $\mathrm{Rat}(\Omega(\underline{A}))$ to $G(X,Y)$, then there exists a group isomorphism between, $\mathrm{Hom}_{\mathrm{Rat}(\Omega(\underline{A}))}(F,G)$, and either $\mathrm{End}_{\mathrm{Rat}(\Omega(\underline{A}))}(F_a)$ or $\mathrm{End}_{\mathrm{Rat}(\Omega(\underline{A}))}(F_m)$, depending upon which of the two isomorphism classes of $\mathrm{Rat}(\Omega(\underline{A}))$ both $F(X,Y)$ and $G(X,Y)$ lie in ;

ii. if $F(X,Y)$ and $G(X,Y)$ lie in different isomorphism classes in $\mathrm{Rat}(\Omega(\underline{A}))$, then:

$$\mathrm{Hom}_{\mathrm{Rat}(\Omega(\underline{A}))}(F,G) = \{0\} \quad .$$

Proof: i. We in fact demonstrated that we have an injective set map in the previous discussion. The fact that this mapping is bijective is trivial. We may conclude that it is in fact a group isomorphism directly from statement iii of Corollary 1.2.5 .

ii. Obvious from the discussion.

∎

Remark: The isomorphism of abelian groups in part i above allows us to define the structure of a ring with unit on the abelian group:

$$\mathrm{Hom}_{\mathrm{Rat}(\Omega(\underline{A}))}(F,G)$$

In view of statement ii , we may conclude that all the hom-sets of the category $\mathrm{Rat}(\Omega(\underline{A}))$ are in fact rings.

Statement i of the above theorem, together with the previous discussion, does give some information concerning, but, obviously not precisely determining, the set, $\mathrm{Hom}_{\mathrm{Rat}(\underline{A})}(F,G)$, for rational formal group laws $F(X,Y)$ and $G(X,Y)$ over the field $\underline{A}$. However, the second part of the theorem does give a complete result:

Corollary 3.5.2: If $F(X,Y)$ and $G(X,Y)$ are two rational formal group laws over $\underline{A}$ which are not isomorphic in the category $\mathrm{Rat}(\Omega(\underline{A}))$, then:

$$\mathrm{Hom}_{\mathrm{Rat}(\underline{A})}(F,G) = \{0\}$$

Proof: Obvious by considering:

$$\mathrm{Hom}_{\mathrm{Rat}(\underline{A})}(F,G) \subseteq \mathrm{Hom}_{\mathrm{Rat}(\Omega(\underline{A}))}(F,G)$$

∎

Remark: this corollary shows that the two distinct theories of rational formal group laws over the algebraic closure of a field translates to give two distinct theories of rational formal group laws over the field in question, since, we have:

if $F(X,Y)$ and $G(X,Y)$ are two non-isomorphic formal group laws in the category $\mathrm{Rat}(\underline{A})$, then, they do not lie in the same isomorphism class in $\mathrm{Rat}(\Omega(\underline{A}))$ iff one is isomorphic to the additive group law in $\mathrm{Rat}(\underline{A})$.

CHAPTER 4: RATIONAL FORMAL GROUP LAWS OVER COMMUTATIVE RINGS.

For this chapter, let R denote an arbitrary commutative ring with non-zero unit, and, any subrings considered of any ring, will contain the unit.

§4.1 Preliminary Definitions:

For an arbitrary commutative ring, R, it is impossible to define a rational formal group law over R in the manner set out in §2.1, since, one cannot speak of the field of rational functions defined over R. However, it is possible to circumvent this problem and define a suitable set of objects for study, which, in the case when R is a field, precisely coincides with the set of all rational formal group laws over R, as defined in §2.1.

With this in mind, and, since the only rational functions, which were investigated in Chapter 2, were those to which there were, in an obvious fashion, associated formal power series, we shall make the following definitions:

Let $f(X)$ be a formal power series in one indeterminate over R. We shall call $f(X)$ a rational formal power series if there exist polynomials $p(X)$ and $q(X)$ over R, relatively prime, with $q(0)$ a unit of R, such that:

$$f(X) = \frac{p(X)}{q(0)} \cdot \left(\sum_{n=0}^{\infty} (-1)^n \cdot \left(\frac{q(X)}{q(0)} - 1 \right)^n \right) .$$

Clearly, $p(X)$ and $q(X)$ are uniquely determined by $f(X)$, up to a unit of R.

Similarly, define a rational formal power series in two indeterminates to be a formal power series over R, $F(X,Y) \in R_2$, for which there exist relatively prime polynomials $P(X,Y)$ and $Q(X,Y)$, with $Q(0,0)$ a unit of R, such that:

$$F(X,Y) = \frac{P(X,Y)}{Q(0,0)} \cdot \left(\sum_{n=0}^{\infty} (-1)^n \cdot \left(\frac{Q(X,Y)}{Q(0,0)} - 1 \right)^n \right) .$$

Again, the polynomials $P(X,Y)$ and $Q(X,Y)$ are uniquely determined by $F(X,Y)$, up to a unit of R.

Define a Rational Formal Group Law over R to be a rational formal power series (in the sense immediately above) which is a formal group law over R .

Notation: if $F(X,Y)$ is a rational formal group law over R , and,

$$F(X,Y) = \frac{P(X,Y)}{Q(0,0)} \cdot \left(\sum_{n=0}^{\infty} (-1)^n \cdot \left(\frac{Q(X,Y)}{Q(0,0)} - 1 \right)^n \right) ,$$

for suitable polynomials $P(X,Y)$ and $Q(X,Y)$ over R , we shall write:

$$F(X,Y) = \frac{P(X,Y)}{Q(X,Y)} ,$$

and, shall assume, without loss of generality, that $Q(0,0) = 1$. Clearly, with this assumption,

$$P(X,Y) = X + Y \quad \text{mod total degree 2} .$$

Remark: one can easily see that this definition of a rational formal group law over R coincides with that given in §2.1 , for the case when R is a field.

§4.2 The General Form of Rational Group Laws:

The main result demonstrated in this section will be the generalization of Theorem 2.5.3, and its Corollary. This will follow almost directly from the following four lemmas:

Throughout the following discussion we shall fix this notation:

Let,

$$\mathbb{F} = \prod_{i \in I} \mathbb{F}_i ,$$

be any product of fields, $\mathbb{F}_i$, indexed by the set I .

The natural projections,

$$p_i : \mathbb{F} \longrightarrow \mathbb{F}_i \quad , \text{ for all } i \in I ,$$

give rise to ring surjections:

$$\tilde{p}_i : \mathbb{F}((X,Y)) \longrightarrow \mathbb{F}_i((X,Y)) \quad , \quad i \in I$$

If $F(X,Y) \in \mathbb{F}([[X,Y]])$, then define:

$$F_i(X,Y) = p_i(F(X,Y)) \quad , \quad i \in I \ .$$

Lemma 4.2.1: If $F(X,Y)$ is a rational formal group law over $\mathbb{F}$, then, for any $i \in I$, $F_i(X,Y)$ is a rational formal group law over $\mathbb{F}_i$.

Proof: Clearly, if $F(X,Y)$ is a rational formal power series over $\mathbb{F}$, then, $F_i(X,Y)$ is a rational formal power series over $\mathbb{F}_i$.

Hence it suffices to show that, for all $i \in I$, $F_i(X,Y)$ is a formal group law over $\mathbb{F}_i$, whenever $F(X,Y)$ is a formal group law over $\mathbb{F}$. But, this last statement is immediate, since the ring operations are defined component-wise in $\mathbb{F}$.

Lemma 4.2.2: If $F(X,Y)$ is a rational formal group law over $\mathbb{F}$, there exist $a,b \in \mathbb{F}$ such that:

$$F(X,Y) = (X + Y + aXY) \cdot \left(\sum_{n=0}^{\infty} (-1)^n \cdot (bXY)^n \right) \ .$$

Proof: Let $F(X,Y)$ be any rational formal group law over $\mathbb{F}$,

$$F(X,Y) = \sum_{k,j=0}^{\infty} a_{kj} \cdot X^k \cdot Y^j \ .$$

By the previous lemma, for each $i \in I$, $F_i(X,Y)$ is a rational formal group law over $\mathbb{F}_i$. But, each $\mathbb{F}_i$ is a field, so that, by Corollary 2.3.4, there exist $a_i, b_i \in \mathbb{F}_i$ such that:

$$F_i(X,Y) = (X + Y + a_i XY) \cdot \left(\sum_{n=0}^{\infty} (-b_i XY)^n \right) \ .$$

Hence, for all $i \in I$, we have:

$$p_i(a_{kj}) = 0 \quad , \text{ unless } k = j \ , \ k = j-1 \ , \text{ or } j = k-1 \ ,$$

and, furthermore, for all $k \in \underline{N}$,

$$p_i(a_{kk}) = p_i(a_{11}) \cdot p_i(a_{12}) \ ,$$

$$p_i(a_{kk-1}) = p_i(a_{k-1k}) = p_i(a_{12})^{k-1} \quad , \text{ and}$$

$$p_i(a_{00}) = 0 \ , \ p_i(a_{10}) = p_i(a_{01}) = 1 \ .$$

The required result now follows immediately. ——E——

Lemma 4.2.3: Given a subring S of $\mathbb{F}$, and, a rational formal group law $F(X,Y)$ over S, then, there exist $a,b \in S$ such that:

$$F(X,Y) = (X + Y + aXY) \cdot \left(\sum_{n=0}^{\infty} (-bXY)^n \right)$$

Proof: $F(X,Y)$ is obviously a rational formal group law over $\mathbb{F}$, so that, by the previous lemma, there exist $a,b \in \mathbb{F}$ such that:

$$F(X,Y) = (X + Y + aXY) \cdot \left(\sum_{n=0}^{\infty} (-bXY)^n \right) \ ,$$

ie. $$F(X,Y) = X + Y + aXY - bX^2Y - bXY^2 - abX^2Y^2 + \ldots$$

Hence, we must have $a,b \in S$, since $F(X,Y)$ is a formal power series over S. ——E——

Finally, we have:

Lemma 4.2.4: If R is a semi-prime ring, then R is actually a subring of a product of fields.

Proof: If we have a prime ideal P of R, then the residue ring, R/P, is an integral domain. Let $\mathbb{F}_P$ denote its field of fractions. For each prime ideal P, we have a natural ring homomorphism,

$$\Pi_P : R \longrightarrow \mathbb{F}_P \ ,$$

given by the natural projection and inclusion maps:

$$R \longrightarrow R/P \longrightarrow \mathbb{F}_P$$

Hence, there exists a ring homomorphism,

$$i : R \longrightarrow \prod_{P \in \mathrm{Spec}(R)} \mathbb{F}_P$$

Suppose we have $r \in R$, and, $i(r) = 0$

Then, by the definition of the map i , for all $P \in \mathrm{Spec}(R)$,

$$r \equiv 0 \mod P$$

But, R is assumed to be semi-prime, therefore, $r = 0$.

Hence the map i is an injection, so that, R is indeed a subring of a product of fields.

∎

We may now consider the generalization of Corollary 2.5.4 :

Theorem 4.2.5: i. If R is a semi-prime ring, and, $F(X,Y)$ is a rational formal group law over R , then, there exist $a,b \in R$ such that:

$$F(X,Y) = (X + Y + aXY) \cdot \left(\sum_{n=0}^{\infty} (-bXY)^n \right) ;$$

ii. R is a semi-prime ring iff all polynomial rational formal group laws have the form:

$$X + Y + aXY \quad , \text{ for some } a \in R .$$

Proof: Statement i. of the theorem clearly follows directly from Lemma 4.2.3 applied to R , in view of Lemma 4.2.4 .

Clearly, if R is a semi-prime ring, and, $F(X,Y)$ is a rational formal group law over R , then, by i. $F(X,Y)$ is a polynomial group law iff

$$F(X,Y) = X + Y + aXY \quad , \text{ for some } a \in R .$$

(Note: it is easy to show that all such polynomials define formal group laws over R .)

To show the converse of statement ii., suppose that R is not a semi-prime ring. Then, there must exist $a , b \in R$, $b \neq 0$, such that:

$$b^k = 0 \quad , \text{ for some } k \in \underline{N} .$$

Assume, with loss of generality that $k = 2$

Consider the rational formal power series:

$$G(X,Y) = (X + Y) \cdot \left(\sum_{n=0} (bXY)^n \right)$$

Since, $b^n = 0$ for all $n>k$, we have:

$$G(X,Y) = X + Y + aXY + bX^2Y + bXY^2 + abX^2Y^2 \quad .$$

Direct computation will show that $G(X;Y)$ is a formal group law. Hence, if R is not semi-prime, then all the polynomial formal group laws over R do not have the form:

$$X + Y + aXY \quad , \text{ for some } a \in R \quad .$$

∎

§4.3 The General Rational Category:

As in section 3.1, let $Fg(R)$ denote the category of all formal group laws over R (ie. one dimensional formal group laws) and, all formal group law morphisms. Consider the subcategory of $Fg(R)$ whose objects consist of all rational formal group laws over R, and, whose morphisms are simply those morphisms of $Fg(R)$ which are given by rational formal power series in one indeterminate. Clearly, in the case when R is a field, this is just the category $Rat(R)$, as defined in §3.1. Hence, call this category, for any R, the category $Rat(R)$ of all rational formal group laws over R.

To establish analogous results to those found in §3.2, we must first consider the following proposition, together with its corollaries:

Recall first the notation of the previous section as regards the product of fields,

$$\mathbb{F} = \overline{\prod_{i \in I}} \mathbb{F}_i$$

Let $h(X) \in \mathbb{F}((X))$, with: $h(X) = \sum_{j=0}^{\infty} c_j X^j$

Define, for each $i \in I$:

$$h_i(X) = \sum_{j=0}^{\infty} p_i(c_j) \cdot X^j$$

Suppose that $h(X)$ is a rational formal power series over $\mathbb{F}$, with $h(0) = 0$ then, for any pair of rational formal group laws, $F(X,Y)$ and $G(X,Y)$ over $\mathbb{F}$,

Proposition 4.3.1: $h(X)$ defines a morphism in $\mathrm{Rat}(\mathbb{F})$,

$$h : F(X,Y) \longrightarrow G(X,Y) \quad ,$$

iff, for all $i \in I$, we have a morphism in $\mathrm{Rat}(\mathbb{F}_i)$:

$$h_i : F_i(X,Y) \longrightarrow G_i(X,Y) \quad .$$

Proof: If in the category $\mathrm{Rat}(\mathbb{F})$ we have:

$$h : F(X,Y) \longrightarrow G(X,Y) \quad ,$$

then, for all $i \in I$, (recalling the definition of the map $\tilde{p}_i$),

$$\tilde{p}_i(h(F(X,Y))) = \tilde{p}_i(G(h(X),h(Y))) \quad ,$$

so that,

$$h_i(F_i(X,Y)) = G_i(h_i(X);h_i(Y)) \quad .$$

Hence, $h_i(X)$ defines a morphism from $F_i(X,Y)$ to $G_i(X,Y)$ in the category $\mathrm{Rat}(\mathbb{F}_i)$.

Conversely, if for each $i \in I$,

$$h_i : F_i(X,Y) \longrightarrow G_i(X,Y) \quad ,$$

in $\mathrm{Rat}(\mathbb{F}_i)$, then one can easily see that:

$$h : F(X,Y) \longrightarrow G(X,Y) \quad ,$$

in the category $\mathrm{Rat}(\mathbb{F}_i)$.

Corollary 4.3.2: if $h(X)$ defines an isomorphism in the category $\mathrm{Rat}(\mathbb{F})$ between $F(X,Y)$ and $G(X,Y)$, then, for some $\alpha, \beta \in \mathbb{F}$,

$$h(X) = \beta X \cdot \left[\sum_{n=0}^{\infty} (\alpha X)^n\right] \quad ,$$

and, furthermore, β is a unit of $\mathbb{F}$.

Proof: Let $h^{-1}(X)$ denote the inverse isomorphism of $h(X)$ in $\mathrm{Rat}(\mathbb{F})$. By the previous proposition, for each $i \in I$, $h_i(X)$ and $h_i^{-1}(X)$ must be inverse isomorphisms in $\mathrm{Rat}(\mathbb{F}_i)$. Since each $\mathbb{F}_i$ is a field, Theorem 3.2.1 implies that, for each $i \in I$, there exist $\alpha_i, \beta_i \in \mathbb{F}_i$

such that:

$$h_i(X) = \beta_i X\left(\sum_{n=0}^{\infty} (\alpha_i X)^n\right) \quad , \text{ and, since } \beta_i \neq 0,$$

$$h^{-1}(X) = \beta_i^{-1} \cdot X \cdot \left(\sum_{n=0}^{\infty} (-\beta_i^{-1} \cdot \alpha_i \cdot X)^n\right) \quad .$$

If follows immediately that:

$$h(X) = \beta X \cdot \left(\sum_{n=0}^{\infty} (\alpha X)^n\right) \quad ,$$

where α and β are those unique elements of $\mathbb{F}$ with:

$$p_i(\alpha) = \alpha_i \quad , \text{ and, } \quad p_i(\beta) = \beta_i \quad , \text{for all } i \epsilon I \ .$$

Obviously, β is a unit of $\mathbb{F}$, since $p_i(\beta) \neq 0$ for all $i \epsilon I$.

Suppose now that S is a subring of the product $\mathbb{F}$. Then, if $F(X,Y)$ and $G(X,Y)$ are rational formal group laws over S, with $h(X)$ a rational formal power series over S, giving an isomorphism between $F(X,Y)$ and $G(X,Y)$ in the category $\mathrm{Rat}(S)$, there exist $\alpha, \beta \epsilon \mathbb{F}$, β a unit of $\mathbb{F}$ such that:

$$h(X) = \beta X \cdot \left(\sum_{n=0}^{\infty} (\alpha X)^n\right) \quad ,$$

If $h^{-1}(X)$ denotes the inverse isomorphism of $h(X)$ in $\mathrm{Rat}(S)$, then,

$$h^{-1}(X) = \beta^{-1} \cdot X \cdot \left(\sum_{n=0}^{\infty} (-\beta^{-1} \cdot \alpha \cdot X)^n\right) \quad ,$$

which implies that both β and β^{-1} are elements of the ring S, and so, we must have $\alpha \epsilon S$.

In view of this remark, we now have the generalization of Theorem 3.2.1:

Theorem 4.3.3: If R is any semi-prime commutative ring, the isomorphisms in the category $\mathrm{Rat}(R)$ are given by rational formal power series of the form:

$$\beta X \cdot \left(\sum_{n=0}^{\infty} (\alpha X)^n\right) \quad , \text{ for } \alpha, \beta \epsilon R \text{ , and, } \beta \text{ a unit.}$$

Proof: Since by Lemma 4.2.4 we can consider R as a subring of a product of fields, the required result follows from the preceding comment.

Note: Such rational formal power series are merely an extension of the notion of a Möbius transformation.

For the rest of this section R will be assumed to be a semi-prime ring.

If $R^\times$ denotes the multiplicative group of units of R, then, we may define the square class group of R to be the quotient group:

$$R_s = \frac{R^\times}{(R^\times)^2}$$

Let $F(X,Y)$ be a rational formal group law over R. Then, by Theorem 4.2.5, there exist $a,b \in R$ such that:

$$F(X,Y) = \frac{X + Y + aXY}{1 - bXY}$$

Define the discriminant of the rational formal group law $F(X,Y)$ to be:

$$\operatorname{disc}(F(X,Y)) = \begin{cases} (4b - a^2)(R^\times)^2 & \text{if } 4b \neq a^2 \\ 0 & \text{if } 4b = a^2 \end{cases}, \text{ or,}$$

Note: this agrees with the discriminant defined in §3.2, when R is a field.

We have:

Theorem 4.3.4: If two rational formal group laws over R are isomorphic in $\mathrm{Rat}(R)$, then they must have the same discriminant.

Proof: Imbed R into the product of fields given in the proof of Lemma 4.2.4. The theorem is easily seen to be true for this product of fields, since, it is true for each component of the product (this is actually Theorem 3.2.3). The required result will now be immediate.

∎

Corollary 4.3.5: There are at least two isomorphism classes in the category $\mathrm{Rat}(R)$.

Proof: Simply note that: $\operatorname{disc}(F_a(X,Y)) = 0$, and, $\operatorname{disc}(F_m(X,Y)) = -1$. The theorem now shows us that these two group laws are not isomorphic.

∎

§4.4 Concluding Remarks:

Unfortunately, the structure of semi-prime commutative rings is, in general too complicated to permit any further generalizations of the results of chapter three, utilizing the methods which we have developed. Indeed, these methods are far too 'coarse' for the general situation. However, they do allow us to deal with the case of an arbitrary product of fields fairly adequately: one can see quite easily, that, given any product of fields $\mathbb{F}$, none of whose characteristic is two, the discriminant invarient completely determines the isomorphism classes of the category $\mathrm{Rat}(\mathbb{F})$. We may even carry on to examine the hom-sets and endomorphism rings of $\mathrm{Rat}(\mathbb{F})$ by piecing together what is already known for each of the components of the product. Clearly, this becomes so complex that it is not worth considering here in full detail.

APPENDIX A: SOME CATEGORY THEORY.

The symbol $\underline{A}$ shall denote an arbitrary category in this appendix.

§A.1 Group Objects in $\underline{A}$:

Suppose that the category $\underline{A}$ has all finite products, and, has a final object, T, denoting the terminal map from any object A to T by: t_A .

An object A of $\underline{A}$ is a group object of $\underline{A}$, if there exist morphisms of $\underline{A}$,

$$\mu : A \times A \longrightarrow A \quad ,$$

$$i : A \longrightarrow A \quad , \text{ and,}$$

$$\gamma : T \longrightarrow A \quad ,$$

such that the following diagrams commute:

A.1.1: (Associativity)

$$\begin{array}{ccc} A \times A \times A & \xrightarrow{\mu \times 1} & A \times A \\ {\scriptstyle 1 \times \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ A \times A & \xrightarrow{\mu} & A \end{array}$$

A.1.2: (Unit)

$$\begin{array}{ccc} A \times T & \xrightarrow{1 \times \gamma} & A \times A \\ & \searrow^{\cong} & \downarrow{\scriptstyle \mu} \\ & & A \end{array} \quad \text{, and,} \quad \begin{array}{ccc} A \times T & \xrightarrow{\gamma \times 1} & A \times A \\ & \searrow^{\cong} & \downarrow{\scriptstyle \mu} \\ & & A \end{array}$$

A.1.3: (Inverse)

$$\begin{array}{ccc} A & \xrightarrow{(1,i)} & A \times A \\ {\scriptstyle t_A}\downarrow & & \downarrow{\scriptstyle \mu} \\ T & \xrightarrow{\gamma} & A \end{array} \quad \text{, and,} \quad \begin{array}{ccc} A & \xrightarrow{(i,1)} & A \times A \\ {\scriptstyle t_A}\downarrow & & \downarrow{\scriptstyle \mu} \\ T & \xrightarrow{\gamma} & A \end{array}$$

We define an $\underline{A}$-group to be the quadruple (A, μ, γ, i)

If in addition, the diagram,

$$\begin{array}{ccc} A \times A & \xrightarrow{\tau} & A \times A \\ & {\scriptstyle \mu}\searrow \quad \swarrow{\scriptstyle \mu} & \\ & A & \end{array}$$

(where τ is the twisting map)

commutes, then, we say that the $\underline{A}$-group (A,μ,γ,i) is abelian.

Given two $\underline{A}$-groups, (A,μ,γ,i) and (A',μ',γ',i') then define an $\underline{A}$-group morphism,

$$\theta : (A,\mu,\gamma,i) \longrightarrow (A',\mu',\gamma',i') \quad ,$$

to be a morphism of $\underline{A}$,

$$\theta : A \longrightarrow A' \quad ,$$

for which the diagram:

$$\begin{array}{ccc} A \times A & \xrightarrow{\theta\times\theta} & A' \times A' \\ \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \mu} \\ A & \xrightarrow{\theta} & A' \end{array} \quad , \text{ commutes.}$$

We may now define a category, $\mathrm{Grp}(\underline{A})$, whose objects are the $\underline{A}$-groups and morphisms the $\underline{A}$-group morphisms defined above.

Since, we have an equivalence of sets:

$$\mathrm{Hom}_{\underline{A}}(B,A) \times \mathrm{Hom}_{\underline{A}}(B,A) \equiv \mathrm{Hom}_{\underline{A}}(B,A\times A) \quad ,$$

for any two objects A,B of $\underline{A}$, when A is the group object discussed above, we may define a binary operation on the set $\mathrm{Hom}_{\underline{A}}(B,A)$ in the following manner:

for all $\phi,\psi \in \mathrm{Hom}_{\underline{A}}(B,A)$ define: $\phi * \psi = \mu \circ (\phi,\psi)$,

where, (ϕ,ψ) is the unique morphism, determined by ϕ and ψ :

$$(\phi,\psi) : B \longrightarrow A \times A$$

Clearly the operation $*$ is well defined as a set map, and, in light of the associative property of the morphism μ given in diagram A.1.1 , the operation $*$ is easily seen to be associative. Furthermore, diagrams A.1.2 show that the composite morphism,

$$B \xrightarrow{t_B} T \xrightarrow{\gamma} A \quad ,$$

is a neutral element of $\mathrm{Hom}_{\underline{A}}(B,A)$, with respect to $*$. Finally, the last set of diagrams implies that, for each $\phi \in \mathrm{Hom}_{\underline{A}}(B,A)$, we have:

With (A,μ,γ,i) an $\underline{A}$-group, we can easily show,

Proposition A.1.1: i. For any object B of $\underline{A}$, $\mathrm{Hom}_{\underline{A}}(B,A)$ is a group, and,

ii, if C is any other object of $\underline{A}$, and, there is a morphism: $\phi : C \longrightarrow B$, in $\underline{A}$,

then, ϕ induces a group homomorphism,

$$\overline{\phi} : \mathrm{Hom}_{\underline{A}}(B,A) \longrightarrow \mathrm{Hom}_{\underline{A}}(C,A) ,$$

given by:

$$\overline{\phi}(\psi) = \psi \circ \phi \quad , \text{ for all } \psi \in \mathrm{Hom}_{\underline{A}}(B,A) .$$

∎

Corollary A.1.2: A group object in the category $\underline{A}$ gives rise to a contravarient functor from $\underline{A}$ to the category of all groups.

Remark: A morphism of $\underline{A}$-groups can easily be seen to give rise to a natural transformation between the associated functors. Thus, the category $\mathrm{Grp}(\underline{A})$ is actually a subcategory of the category of all contravarient functors from $\underline{A}$ to the category of all groups.

§A.2 Cogroup Objects in $\underline{A}$:

Suppose now that $\underline{A}$ has all finite coproducts, and, an initial object, I. If A is any object of $\underline{A}$, then denote the initial map from I to A by: i_A.

We shall now define the categorical dual of the notion of a group object, which is called a cogroup object. Thus, a cogroup object in $\underline{A}$ is an object A of $\underline{A}$, together with morphism,

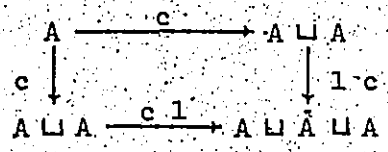
$$c : A \longrightarrow A \sqcup A ,$$

$$a : A \longrightarrow A \quad , \text{ and,}$$

$$\eta : A \longrightarrow I$$

for which the following diagrams commute:

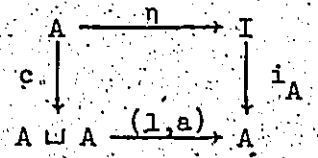
A.2.1: (Coassociativity)



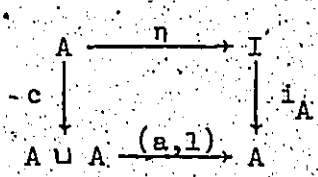
A.2.2: (Counit)

,and,

A.2.3: (Antipodism)



,and,



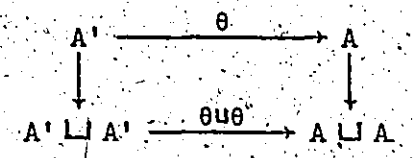
Clearly, a cogroup object (A,c,η,a) in the category $\underline{A}$ defines a group object in the dual category $\underline{A}^*$. In view of this, the natural definition for a morphism of $\underline{A}$-cogroups,

$$\theta : (A,c,\eta,a) \longrightarrow (A',c',\eta',a') \quad ,$$

would be a morphism of $\underline{A}$,

$$\theta : A' \longrightarrow A \quad ,$$

for which the diagram,



commutes.

With this definition, we have the category $\mathrm{CoGrp}(\underline{A})$ of $\underline{A}$-cogroups and their morphisms.

Clearly, by applying Proposition A.1.1 to the category $\underline{A}^*$, we immediately have, for any cogroup object (A,c,η,a) of $\underline{A}$:

Proposition A.2.1: i. For any object B of $\underline{A}$, the set $\mathrm{Hom}_{\underline{A}}(A,B)$ has a group structure, given by the cogroup structure on A;

ii. if C is any other object of $\underline{A}$, with a morphism,

$$\zeta : B \longrightarrow C ,$$

then, ζ induces a group homomorphism,

$$\overline{\zeta} : \mathrm{Hom}_{\underline{A}}(A,B) \longrightarrow \mathrm{Hom}_{\underline{A}}(A,C) ,$$

in the obvious fashion. ∎

Corollary A.2.2: Any $\underline{A}$-cogroup determines a covarient functor from $\underline{A}$ to the category of all groups.

Remarks: For further information concerning group and cogroup objects, with special emphasis on formal group laws, see Dieudonnée [2].

APPENDIX B: SOME RING THEORY.

Throughout this appendix we shall let R denote an arbitrary commutative ring, with unit.

§B.1 Formal Power Series Rings:

Let M_n denote the set of n-tuples of non-negative integers, $n \in \underline{N}_0$,

ie. if $I \in M_n$, then, $I = (i_1, \ldots, i_n)$, $i_j \in \underline{N}_0$, $1 \leq j \leq n$.

For $I, J \in M_n$, with,

$$I = (i_1, \ldots, i_n) \quad \text{and} \quad J = (j_1, \ldots, j_n) ,$$

define:

$$I \leq J \quad \text{iff} \quad i_k \leq j_k \quad \text{for all} \quad 1 \leq k \leq n ,$$

and,

$$I + J = (i_1 + j_1, \ldots, i_n + j_n) .$$

Thus, the set M_n has a natural order relation, and, a binary operation defined on it.

Let R_n denote the set of set maps from M_n to the underlying set of R .

For all $I \in M_n$, and, for all set maps,

$$f : M_n \longrightarrow R \quad , \text{ and, } \quad g : M_n \longrightarrow R ,$$

define: $f + g : M_n \longrightarrow R$,

by: $(f + g)(I) = f(I) + g(I)$,

and, define: $f \cdot g : M_n \longrightarrow R$,

by: $$(f \cdot g)(I) = \sum_{\substack{J+K=I \\ J,K \in M_n}} f(J) \cdot g(K)$$

Clearly, the set map $f + g$ is well defined, and, since the summation involved is finite, so is the map $f \cdot g$.

It is an easy exercise to show that these two binary operations defined on the set R_n satisfy the ring axioms, and, furthermore, define the structure of

a commutative ring with unit. The set R_n together with this ring structure is called the ring of formal power series in n arbitrary indeterminates over the ring R.

If $X_1,\ldots,X_n$ is any collection of indeterminates, then we may write an element f of R_n in the usual formal fashion:

$$f(X_1,\ldots,X_n) = \sum_{I\in M_n} f_I \cdot X^I \quad ,$$

where, if $I = (i_1,\ldots,i_n)$,

$$f_I = f(I) \quad , \text{ and,}$$

the symbol, X^I is to be interpreted to mean:

$$X^I = X_1^{i_1}\cdot X_2^{i_2}\cdot\ldots\cdot X_n^{i_n}$$

We may now define the ring operations in the following formal manner:

$$(f+g)(X_1,\ldots,X_n) = \sum_{I\in M_n} (f_I + g_I)\cdot X^I \quad ,$$

and,

$$(f\cdot g)(X_1,\ldots,X_n) = \sum_{I\in M_n} \left(\sum_{\substack{J+K=I \\ J,K\in M_n}} f_J \cdot g_K\right)\cdot X^I \quad ,$$

where f and g are any two elements of R_n.

The above formal notation, and the choice of the indeterminates $X_1,\ldots,X_n$, defines the ring of formal power series in the n indeterminates $X_1,\ldots,X_n$, which shall be denoted by:

$$R((X_1,\ldots,X_n))$$

We have immediately-

Lemma B.1.1: If $Y_1,\ldots,Y_n$ is any other collection of indeterminates, then, the rings $R((X_1,\ldots,X_n))$ and $R((Y_1,\ldots,Y_n))$ are isomorphic.

∎

It is extremely convenient to work with formal power series in a specified set of indeterminates; however, it is extremely tedious to continually state the specific indeterminates in question. With this in mind, unless the indeterminates envolved are not clear from the context in which they are employed, we shall abuse our notation and write R_n for any ring of formal power series over R in a specified set of n indeterminates.

Now, if $f(X_1,\ldots,X_n) \in R_n$, we call f_I, $I \in M_n$, the coefficient of the term: X^I.

The constant term of a formal power series over R, $f(X_1,\ldots,X_n)$ is the coefficient: f_0, (here 0 denotes the zero n-tuple.).

We may define an inclusion map, which is obviously a ring homomorphism,

$$i : R \longrightarrow R_n \quad ,$$

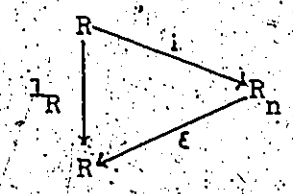
by mapping every element r of R to the unique formal power series defined by: $f_0 = r$, and, $f_I = 0$ for $I \neq 0$.

On the other hand, we may define the augmentation map,

$$\varepsilon_n : R_n \longrightarrow R \quad ,$$

which sends every formal power series $f(X_1,\ldots,X_n)$ of R_n to its constant term, $f_0 \in R$. Again, we obviously have a ring homomorphism.

The following diagram of ring homomorphisms clearly commutes:



Lemma B.1.2: i. Clearly: $(R_n)_m = R_{n+m} = (R_m)_n$, and,

ii. If: $\varepsilon'_m : (R_n)_m \longrightarrow R_n$, and, $\varepsilon'_n : (R_m)_n \longrightarrow R_m$, are the two augmentations, then: $\varepsilon_m \circ \varepsilon'_m = \varepsilon_{n+m} = \varepsilon_m \circ \varepsilon'_n$.

Proof: These results follow immediately from the above definitions.

Let $I^{(n)} = \ker(\varepsilon_n)$, that is, $I^{(n)}$ is the ideal of R_n consisting of those formal power series with zero constant term.

If $f(X_1,\ldots,X_n), g(X_1,\ldots,X_n) \in I^{(n)}$ then, it now makes sense to define the composite:

$$f\circ g(X_1,\ldots,X_n) = f(g(X_1,\ldots,X_n),\ldots,g(X_1,\ldots,X_n)) \quad ,$$

which is clearly a formal power series in n indeterminates over R with zero constant term, i.e. $I^{(n)}$ is closed with respect to composition of formal power series.

Notation:

From now on, where there is no possibility of confusion, we shall denote a formal power series in n indeterminates over R , $f(X_1,\ldots,X_n)$ by:

$$f(X) \quad ,$$

and, a given vector of m formal power series,

$$(g_1(X_1,\ldots,X_n),\ldots,g_n(X_1,\ldots,X_n)) \quad ,$$

shall be denoted by:

$$g(X) = (g_1(X),\ldots,g_n(X)) \quad .$$

Only where it becomes necessary to distinguish between these two concepts shall we use the complete notation.

B.2 Ring Filtrations:

Define $\underline{N}^*$ to be the set: $\underline{N}_0 \cup (\infty)$.

There is an obvious order relation defined on this set, given by:

for all $a,b \in \underline{N}^* \cap \underline{N}_0$, define $a \leq b$ in the usual way, and,

for all $a \in \underline{N}^*$, define $a \leq \infty$.

Now let S denote any commutative ring.

Define a filtration ν on the ring R to be a set map,

$$\nu : R \longrightarrow \underline{N}^* \quad ,$$

satisfying:

i. $\nu(0) = \infty$,

ii. $\nu(a - a') \geq \inf(\nu(a),\nu(a'))$, for all $a,a' \in R$, and,

iii. $\nu(a \cdot a') \geq \nu(a) + \nu(a')$.

The filtration ν of R is said to be Haundorff if it also satisfies:

iv. $\nu(a) = \infty$ iff $a = 0$, for all $a \in R$,

in which case we may define a metric,

$$d : R \times R \longrightarrow \mathbb{R} \quad ,$$

given by:

$$d(a,a') = 2^{-\nu(a-a')} \quad ,$$

and, with respect to this topology, it is an easy exercise to show that R is a Haundorff topological ring.

Let $A = (a_n)_{n=0}^{\infty}$ be any sequence of elements of R .

We say that an element a of R is a limit of the sequence A with respect to the filtration ν iff:

$$\lim_{n\to\infty} (a_n - a) = \infty \quad ,$$

in which case we write:

$$\lim_{n\to\infty}{}_{\nu}\, a_n = a \quad .$$

Note that if ν is Haundorff, then all limits are unique.

Lemma B.2.1: For any two sequences $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$ in R ,

i. $\lim_{n\to\infty}{}_{\nu} (a_n + b_n) = \lim_{n\to\infty}{}_{\nu}\, a_n + \lim_{n\to\infty}{}_{\nu}\, b_n$, and,

ii. $\lim_{n\to\infty}{}_{\nu} (a_n \cdot b_n) = \left(\lim_{n\to\infty}{}_{\nu}\, a_n\right) \cdot \left(\lim_{n\to\infty}{}_{\nu}\, b_n\right)$.

Proof: These results follow directly from the properties of ν .

The sequence A is called a Cauchy sequence with respect to the filtration ν iff:

$$\lim_{n\to\infty} \nu\,(a_{n+1} - a_n) = 0$$

A filtration ν of the ring B is said to be a complete filtration of B, if it is Hausdorff, and, every Cauchy sequence in B has a limit in B.

We shall now outline a general construction for complete filtrations:

Suppose there exist R-modules $(B_k)_{k=0}^{\infty}$ such that:

$$B \cong \prod_{k=0}^{\infty} B_k$$

(Note: this implies that B is actually an R-Algebra.)

If $a\in B$, then let $a(k)$ denote its k^{th} component in the above product, and, write, $a^{(n)}$ for the element of B given by:

$$a^{(n)}(k) = \begin{cases} 0 & \text{for } k\geq n \\ a(k) & \text{for } k<n \end{cases}.$$

Define, for all $r\in\underline{N}_0$,

$$I_r = \left\{a\in B \mid a(k) = 0 \text{ for all } k<r\right\}, \text{ and,}$$

$$P_r = \left\{a\in B \mid a(k) = 0 \text{ for all } k\geq r\right\}.$$

Clearly, we have:

Lemma B.2.2: For each $r\in\underline{N}_0$, i. I_r is an ideal of B, and,

ii. B is isomorphic to: $I_r \oplus P_r$.

Suppose now that we have:

$$I_r \cdot I_t \subseteq I_{r+t}, \text{ for all } r,t\in\underline{N}_0,$$

and, define:

$$\nu(a) = \sup_{a\in I_r} r = \inf_{a(k)\neq 0} k.$$

Proposition B.2.3: i. ν is a complete filtration of S, and,

ii. for all $a \in S$, $\lim_{n\to\infty} \nu(a^{(n)} - a) = 0$.

Proof: i. By our construction of the set map ν, and, our assumption on the ideals I_r, ν is obviously a ring filtration.

Clearly ν is a Hausdorff-filtration, so it is only necessary to show that all Cauchy sequences in S with respect to ν have limits in S.

Let $(a_n)_{n=0}^{\infty}$ be a Cauchy sequence in S. Then, since,

$$\lim_{n\to\infty} \nu(a_{n+1} - a_n) = 0 \quad ,$$

for each $k \in \underline{N}_0$, there exists a non-negative integer, n_k, such that:

$$a_\ell(k) = a_{n_k}(k) \quad , \text{ for all } \ell \geq n_k \quad .$$

Let a be the element of S given by:

$$a(k) = a_{n_k}(k) \quad , \text{ for all } k \geq 0 \quad .$$

Clearly, for $n > n_k$,

$$\nu(a - a_n) > k \quad , \text{ for all } k \geq 0 \quad ,$$

and, by construction, the sequence $K = (n_k)_{k=0}^{\infty}$ is either increasing, or, eventually constant. It follows immediately that:

$$\lim_{n\to\infty} \nu(a_n - a) = 0 \quad .$$

ii. By the definition of ν and of $a^{(n)}$, it follows immediately that,

$$\lim_{n\to\infty} \nu(a^{(n)} - a) = 0 \quad .$$

———□———

We shall now return to a discussion of the rings of formal power series over the ring R:

Consider the case in the above construction when $S = R_n$, for some n. Define $R_n(k)$ to be the R-module of homogenious polynomials of total degree k, contained in R_n.

Thus, if we define, for any $I = (i_1,\ldots,i_n)\in M_n$,

$$|I| = \sum_{j=1}^{n} i_j \quad ,$$

then, $f(X)\in R_n(k)$ iff:

$$f(X) = \sum_{\substack{|I|=k \\ I\in M_n}} r_I \cdot X^I \quad .$$

Clearly, we have:

$$R_n \cong \prod_{k=0}^{\infty} R_n(k) \quad ,$$

with, in the above notation:

$$f(X)(k) = \sum_{\substack{|I|=k \\ I\in M_n}} r_I \cdot X^I \quad , \text{ for all } f(X)\in R_n \ , \ k\in \underline{N}_0$$

so that, for $r\in \underline{N}_0$,

$$I_r = \left\{ f(X)\in R_n \mid r_I = 0 \text{ for all } |I|<r \right\} \quad , \text{ and,}$$

$$P_r = \left\{ f(X)\in R_n \mid r_I = 0 \text{ for all } |I|\geq r \right\} \quad .$$

By the previous discussion, we may define a complete filtration on R_n by:

$$\operatorname{ord}(f(X)) = \sup_{f(X)\in I_r} r \quad .$$

This is called the order filtration of the ring R_n .

Note: if we formally consider R to be the ring of formal power series over R in zero indeterminates, R_0 , then, in this case the order filtration is the discrete filtration.

Lemma B.2.h: for the ring R_n , $I_r \cdot I_t = I_{r+t}$, for all $r,t\in \underline{N}_0$.

Proof: Trivial! .

Notation: For any two formal power series, $f(X)$ and $g(X)$, in n indeterminates, we shall write: $f(X) \equiv g(X)$ mod (total) degree r ,

for: $f(X) \equiv g(X) \mod I_r$, where $r\in \underline{N}_0$.

Remark: From now on, the rings of formal power series over R will always be considered filtered with respect to the order filtration.

B.3 Continuous Ring Homomorphisms and the Order Filtration:

Let S and S' be two commutative rings, with filtrations ν and ν' respectively. Define, for all $m \in \underline{N}_0$,

$$\Lambda_m = \{ s \in S \mid \nu(s) \geq m \} \quad , \text{ and,}$$

$$\Lambda'_m = \{ s \in S' \mid \nu'(s) \geq m \} \quad .$$

Suppose that we have a ring homomorphism,

$$\theta : S \longrightarrow S' \quad .$$

The mapping θ is said to be continuous with respect to ν and ν' if we have: for all $m \in \underline{N}_0$, there exists an $\ell \in \underline{N}_0$ such that:

$$\theta(\Lambda_\ell) \subseteq \Lambda'_m \quad .$$

We say that θ is bicontinuous if θ is an isomorphism of rings, and, both θ and θ^{-1} are continuous.

Suppose now that S is a commutative ring with unit, and, S contains R as a subring (here we assume that the unit of S and R coincide). Let S be complete with respect to some filtration ν.

We have immediately:

Proposition B.3.1: Given elements $a_1, \ldots, a_n$ of S, with:

$$\nu(a_i) \geq 1 \quad , \quad \text{for all } i,\ 1 \leq i \leq n \quad ,$$

then, there exists a unique continuous ring homomorphism,

$$\theta : R_n \longrightarrow S \quad ,$$

such that θ is the identity on R, and,

$$\theta(X_i) = a_i \quad , \quad \text{for all } i,\ 1 \leq i \leq n \quad .$$

Proof: Suppose that $f(X) \in R_n$, then, writing, $f(X) = \sum_{I \in M_n} f_I \cdot X^I$,

$$f^{(q+1)}(X) - f^{(q)}(X) = \sum_{|I|=q} f_I \cdot X^I \quad , \quad q \in \underline{N}_0 \ .$$

If $I = (i_1, \ldots, i_n) \in M_n$, then write:

$$a^I = a_1^{i_1} \ldots a_n^{i_n} \ .$$

For any $q \in \underline{N}_0$, we have:

$$f^{(q+1)}(a_1, \ldots, a_n) - f^{(q)}(a_1, \ldots, a_n) = \sum_{|I|=q} f_I \cdot a^I \ .$$

Since $v(a_i) \geq 1$, for $1 \leq i \leq n$, we have:

$$v(a^I) \geq |I| \ ,$$

so that,

$$v(f^{(q+1)}(a_1, \ldots, a_n) - f^{(q)}(a_1, \ldots, a_n)) \geq q \ .$$

Thus, it follows immediately that:

$$\lim_{q \to \infty} v\,(f^{(q+1)}(a_1, \ldots, a_n) - f^{(q)}(a_1, \ldots, a_n)) = 0 \ ,$$

ie. the sequence $(f^{(q)}(a_1, \ldots, a_n))_{q=0}^{\infty}$ is a Cauchy sequence in S.

Since v is a complete filtration of S, we may define a set map:

$$\theta : R_n \longrightarrow S \ ,$$

by:-

$$\theta(F(X)) = \lim_{q \to \infty} v\, f^{(q)}(a_1, \ldots, a_n) \quad , \text{ for all } f(X) \ R_n \ .$$

In view of Lemma B.2.1, we see that θ is a ring homomorphism, and, by its very construction, θ is obviously continuous. Clearly, θ is the identity map on the subring R.

The uniqueness of θ follows directly from continuity:

suppose we have a continuous ring homomorphism,

$$\theta' : R_n \longrightarrow S \ ,$$

fixing R, and, such that: $\theta'(X_i) = a_i$, for $1 \leq i \leq n$, then, by continuity:

$$\lim_{q\to\infty} \nu\, f^{(q)}(a_1,\ldots,a_n) = \theta'(f(X)) \quad .$$

Hence: $\theta' \leq \theta$.

———K———

Remark: In the above proof, the symbol, $f^{(q)}(X)$, is to be interpreted in the sense of Section B.2, ie. $f^{(q)}(X)$ is a polynomial over R of total degree at most $q-1$, such that:

$$f(X) \equiv f^{(q)}(X) \mod \text{degree } q \quad .$$

Consider now the case when: $R = R_m$, for some $m \in \mathbb{N}$.

Suppose that we have a continuous ring homomorphism,

$$\theta: R_n \longrightarrow R_m \quad , \text{ fixing the subring } R \ ,$$

with the following property:

Property B.3.2: For all $f(X) \in R_n$ with $\mathrm{ord}_X(f(X)) \geq 1$, we have:

$$\mathrm{ord}_Y(\theta(f(X))) \geq 1 \quad .$$

Denoting the indeterminates of R_n by $X_1,\ldots,X_n$, and, those of R_m by $Y_1,\ldots,Y_m$, the previous proposition states that θ is completely determined by the n formal power series in m indeterminates:

$$g_i(Y_1,\ldots,Y_m) = \theta(X_i) \quad , \text{ for } 1 \leq i \leq n \ ,$$

and, we must have:

$$\theta(f(X)) = \lim_{q\to\infty} f^{(q)}(g_1(Y),\ldots,g_n(Y)) \quad .$$

Since, by Property B.3.2, $\mathrm{ord}_Y(g_i(Y)) \geq 1$, for $1 \leq i \leq n$, the $g_i(Y)$ must have zero constant term, and, so by the remarks of Section B.1 we may consider:

$$f\circ g(Y) = f(g_1(Y),\ldots,g_n(Y)) \quad ,$$

which is a formal power series in the ring R_m .

Proposition B.3.3: With the above notation: $\theta(f(X)) = f\circ g(Y)$,

$$\text{ie. } \lim_{q\to\infty} f^{(q)}(g_1(Y),\ldots,g_n(Y)) = f(g_1(Y),\ldots,g_n(Y)) \quad .$$

Proof: The statement is obviously true if $F(X)$ is actually a polynomial. Hence, by the continuity of θ the statement of the proposition is true for any $f(X) \in R_n$.

NOTE: This Proposition actually says the following:

Any vector of n formal power series over R in m indeterminates- each with zero constant term, determines, and, is uniquely determined by a continuous ring homomorphism,

$$\theta : R_n \longrightarrow R_m ,$$

which satisfies Property B.3.2 above.

§B.4 The Inverse Function Theorem:

We now assume that all continuous ring homomorphisms that we shall consider between rings of formal power series over R shall satisfy Property B.3.2 .

Consider the ideals in R_n and R_m ,

$$I^{(n)} = \ker(\varepsilon_n) \quad , \text{ and, } \quad I^{(m)} = \ker(\varepsilon_m) \quad .$$

If $f(X) \in I^{(n)}$, denote by $\overline{f}(\overline{X})$, its image under the canonical surjection:

$$I^{(n)} \longrightarrow \frac{I^{(n)}}{(I^{(n)})^2}$$

Hence, if we have: $f(X) = \sum_{i=1}^{n} a_i \cdot X_i + f_0(X)$, where: $\operatorname{ord}_X(f_0(X)) \geq 2$, then:

$$\overline{f}(\overline{X}) = \sum_{i=1}^{n} a_i \cdot \overline{X}_i \quad ,$$

so that, writing:

$$D(R_n) = \frac{I^{(n)}}{(I^{(n)})^2} \quad ,$$

$D(R_n)$ is a free R-module of the generators: $\overline{X}_1, \ldots, \overline{X}_n$.

Clearly, for any continuous ring homomorphism,

$$\theta : R_n \longrightarrow R_m \quad ,$$

we have:

$$\theta(I^{(n)}) \subseteq I^{(m)} \quad , \text{ and,}$$

$$\theta((I^{(n)})^2) \subseteq (I^{(m)})^2 \quad ,$$

so that, θ induces an R-module homomorphism:

$$D(\theta) : D(R_n) \longrightarrow D(R_m) \quad .$$

Furthermore, if we have two continuous ring homomorphisms,

$$\theta : R_n \longrightarrow R_m \quad , \text{ and,}$$

$$\Psi : R_m \longrightarrow R_p \quad ,$$

it is clear that:

$$D(\Psi \circ \theta) = D(\Psi) \circ D(\theta) \quad .$$

Let $X_1,\ldots,X_n$ be the determinates of R_n, and, let $Y_1,\ldots,Y_n$ be those of R_m. Writing, for $1 \leq i \leq n$,

$$\theta(X_i) = \sum_{k=1}^{m} c_{ik} \cdot Y_k + g_i(Y) \quad , \text{ where } \operatorname{ord}_Y(g_i(Y)) \geq 2,$$

we have,

$$D(\theta)(\overline{X}_i) = \sum_{k=1}^{m} c_{ik} \cdot \overline{Y}_k \quad ,$$

giving the matrix representation:

$$D(\theta) = (c_{ik})_{\substack{1 \leq i \leq n \\ 1 \leq k \leq m}} \quad .$$

Adopting the usual partial derivative notation, we see that:

$$c_{ik} = \left(\frac{\partial \theta(X_i)}{\partial Y_k} \right)_{Y = 0} \quad , \text{ for } 1 \leq i \leq n \text{ , and, } 1 \leq k \leq m.$$

Now suppose that we have an R-module homomorphism,

$$\phi : D(R_n) \longrightarrow D(R_m) \quad ,$$

given by:

$$\phi(\overline{X}_i) = \sum_{k=1}^{m} c_{ik} \cdot \overline{Y}_k \quad , \text{ for } 1 \leq i \leq n \quad .$$

By Proposition B.3.1, there exists a continuous ring homomorphism,

$$E(\phi) : R_n \longrightarrow R_m \quad ,$$

with:

$$E(\phi)(X_i) = \sum_{k=1}^{m} c_{ik} \cdot Y_k \quad , \quad \text{for } 1 \leq i \leq n \ .$$

Clearly, we have the following properties of the association E :

i. $D(E(\phi)) = \phi$, and,

ii. for any other R-module homomorphism,

$$\phi' : D(R_m) \longrightarrow D(R_p) \quad ,$$

we have:

$$E(\phi' \circ \phi) = E(\phi') \circ E(\phi) \quad .$$

We now have the necessary machinery , and, notation to state and prove the Inverse Function Theorem:

Theorem B.4.1: Suppose that we are given a continuous ring homomorphism,

$$\Theta : R_n \longrightarrow R_n \quad ,$$

Then, Θ is a bicontinuous ismorphism iff $D(\Theta)$ is an isomorphism of R-modules.

Proof: Clearly we need only prove the sufficiency of the condition.

Let $X_1, \ldots, X_n$ be the indeterminates of R_n .

Suppose we are given a continuous ring homomorphism,

$$\Theta : R_n \longrightarrow R_n \quad ,$$

for which, the R-module homomorphism , $\phi = D(\Theta)$, is an automorphism of the R-module $D(R_n)$.

Define:

$$\overline{\phi} = E(\phi) \quad .$$

Since, ϕ is an automorphism of $D(R_n)$, it is easy to see that $\overline{\phi}$ is a bicontinuous automorphism of R_n .

Obviously,

$$D(\Theta\circ\phi^{-1}) = 1_{D(R_n)} \quad ,$$

so that it suffices to show that $\Theta\circ\phi^{-1}$ is an isomorphism. Hence, with out loss of generality, we may assume that:

$$\phi = D(\Theta) = 1_{D(R_n)}$$

For $1 \leq i \leq n$, writing,

$$h_i(X) = \Theta(X_i) \quad ,$$

we see that:

$$h_i(X) \equiv X_i \quad \text{mod degree } 2 \quad .$$

Fix i, $1 \leq i \leq n$, and, define:

$$\Theta(X) = (h_1(X),\ldots,h_n(X)) \quad .$$

For each $\ell\in\underline{N}$ we shall now construct, by induction on ℓ, a polynomial $g_i^{(\ell)}(X)$ of total degree at most $\ell-1$, with the two properties that:

a. $X_i \equiv g_i^{(\ell)}(\Theta(X))$ mod degree ℓ, and,

b. $g_i^{(\ell)}(X) \equiv g_i^{(\ell+1)}(X)$ mod degree ℓ .

Define,

$$g_i^{(1)}(X) = X_i \quad ,$$

both of which clearly satisfy both a. and b. above.

Now suppose that we have constructed $g_i^{(k)}(X)$ satisfying both a. and b. above, for all $k<\ell$. In particular:

$$X_i \equiv g_i^{(\ell)}(\Theta(X)) + \sum_{|J|=\ell} c_J\cdot X^J \quad \text{mod degree } \ell+1 \quad ,$$

and, so, in view of our above remarks concerning Θ,

$$X_i \equiv g_i^{(\ell)}(\Theta(X)) + \sum_{|J|=\ell} c_J\cdot \Theta(X)^J \quad \text{mod degree } \ell+1 \quad .$$

Define:

$$g_1^{(\ell+1)}(X) = g_1^{(\ell)}(X) + \sum_{|J|=\ell} c_J \cdot X^J \quad ,$$

which clearly satisfies both a. and b. above.

Thus, for each i, we have constructed a sequence of polynomials,

$$\left\{ g_1^{(\ell)}(X) \right\}_{\ell=0}^{\infty} \quad ,$$

which, by property b. above, is a Cauchy sequence with respect to the order filtration. For $1 \leq i \leq n$, define:

$$g_i(X) = \lim_{\ell \to \infty} g_1^{(\ell)}(X) \quad .$$

It follows immediately from property a. above that, for each i,

$$X_i = g_i(\theta(X)) \quad ,$$

and, by the definition of θ,

$$g_i(\theta(X)) = \theta(g_i(X)) \quad .$$

Now define a continuous ring homomorphism,

$$\psi : R_n \longrightarrow R_n \quad ;$$

by:

$$\psi(X_i) = g_i(X) \qquad \text{for } 1 \leq i \leq n \quad .$$

We see immediately that:

$$\theta \circ \psi = 1_{R_n} \quad .$$

Obviously, since,

$$D(\theta) = 1_{D(R_n)} \quad ,$$

we must have:

$$D(\psi) = 1_{D(R_n)} \quad ,$$

and so, we may apply the above construction to ψ, obtaining a continuous ring homomorphism,

$$\chi : R_n \longrightarrow R_n \quad ,$$

with:

$$\Psi o \chi = 1_{R_n}$$

Therefore: $\chi = (\Theta o \Psi) o \chi = \Theta$,

showing that Θ and Ψ are inverse continuous isomorphisms of R_n .

———∎———

Corollary B.4.2: Given n formal power series,

$$f_i(X_1,\ldots,X_n) \in R_n \quad , \quad 1 \leqslant i \leqslant n \quad ,$$

each with zero constant term, then:

$$\det\left(\left.\frac{\partial f_i}{\partial X_i}\right|_{X=0} \right)$$

is a unit of R iff there exists n formal power series,

$$g_i(X_1,\ldots,X_n) \in R_n \quad , \quad 1 \leqslant i \leqslant n \quad ,$$

each with zero constant term, such that:

$$X_i = f_i(g_1(X),\ldots,g_n(X)) \quad \text{for} \quad 1 \leqslant i \leqslant n$$

Proof: A direct interpretation of Theorem B.4.1 in light of the remark after Proposition B.3.3 .

———∎———

BIBLIOGRAPHY:

[1] Connell, Ian G. "Abelian Formal Groups", Proceedings of the American Mathematical Society, Vol. 17, No. 4 , 1966 , 958-959 .

[2] Dieudonnée, Jean A. Introduction to the Theory of Formal Groups. Marcel Dekker Inc., New York, 1973 .

[3] Fröhlich, A. "Formal Groups", Lecture Notes in Mathematics, No. 74, Springer-Verlag, Berlin, 1968 .

[4] Lazard, M. "La non-existence des groupes de Lie formels non-abéliens à un parametre", Comptes Rendus de l'Académie des Sciences, Vol 239, Paris, 1954 , 942-945

[5] Lazard, M. "Sur les groupes de Lie formels à un parametre", Bulletin de la Société Mathématique de France , Vol. 83, 1955 , 251-274 .

[6] Lazard, M. "Commutative Formal Groups", Lecture Notes in Mathematics, No. 443 , Springer-Verlag, New York, 1975 .

[7] Manin, Yu. I. "The Theory of Commutative Formal Groups over Fields of Finite Characteristic", Russian Mathematical Surveys, Vol. 18 , 1963 , 1-83 .

[8] Serre, J-P. Cours d'Arithmétique. Press Universitaires de France, Paris, 1970 .

[9] Serre, J-P, Lie Algebras and Lie Groups. W.A. Benjamin Inc., Reading Mass. 1966 .

[10] van der Waerden, B.L. Algebra. Vol. 1 , Frederick Ungar Publishing Co., New York, 1970 .