GROUP LAWS AND COMPLEX MULTIPLICATION IN LOCAL FIELDS

Abstract

TITLE: Group Laws and Formal Complex Multiplication in Local Fields

AUTHOR: Michael Urda

DEPARTMENT: Mathematics

DEGREE: M.Sc.

This thesis is concerned with the study of certain objects known as group laws or as they are often called - 1-parameter formal Lie groups, and with the proof of the reciprocity law for local class fields. In part I the immediate structural consequences of definitions are presented in a straightforward manner, together with some basic results on the form of group laws (which are actually types of power series). The second section deals with results which are somewhat beyond the basic level - in particular some properties of homomorphisms are considered. Part III gives an introductory development of group laws as they pertain to algebraic number theory. Isomorphisms between group laws are considered in the fourth section. The thesis concludes with a proof of the reciprocity law for local class field theory, the preparation for which was carried out in part V - a particular construction of group laws.

Group Laws and Formal Complex Multiplication in Local Fields

by

Michael Urda

McGill University Department of Mathematics

Preface

This thesis is concerned with the study of certain objects known as group laws (which are defined over rings), or, as they are often called - one-parameter formal Lie groups, and with the proof of the reciprocity law for local class fields. In part I the immediate structural consequences of definitions are presented in a straightforward manner, together with some basic results on the form of group laws (which are actually types of power series). The second section deals with results which are somewhat beyond the basic level - in particular some properties of homomorphisms are considered. Part III gives an introductory development of group laws as they pertain to algebraic number theory - specifically, we consider group laws over a complete discrete valuation ring and examine results with respect to the residue class field. Isomorphisms between group laws are considered in the fourth section, and, a close relationship between roots of unity and such isomorphisms is revealed. The thesis concludes with a proof of the reciprocity law for local class field theory, the preparation for which was carried out in part V - a particular construction of group laws.

The study of group laws and their properties is a relatively new topic, going back to about 1950, but, related investigations were undertaken in connection with the theory of elliptic curves, for many years prior to this date. Dieudonné, in his series of papers (see Bibliography, nos. 2-9), employed infinitesimal methods (now somewhat out of vogue due to the popularity of the newer, more direct approach

of Lazard and Lubin) to obtain required results. The later papers by Lubin and Tate establish a close relationship between algebraic number theory and group laws.

Almost the entire development of this thesis is to be found in J. Lubin's papers listed in the Bibliography (nos. 13-17); the papers most frequently used were those listed in the Bibliography with reference nos. 13 and 17. My contributions are that I have supplied more detailed demonstrations of statements found therein, rearranged some proofs and constructed others for results due to Lazard (T10, T20) which were simply quoted by Lubin. In addition, T3B, and T11 are some formulations of my own.

Notation:

1/ RHS, LHS mean right-hand-side, left-hand-side respectively, of ='s.

2/ D1, D2,..., stand for definitions.

3/ T1, T2,..., represent statements with proof which are sometimes given names such as theorem, proposition, lemma, corollary, depending on their importance to the development.

4/ Rings which are commutative and have unity are often denoted by A.

5/ char A stands for the characteristic of the ring A.

6/ The word "in" stands for "an element of".

I would like to thank Mrs. Anne Liepinaitis for typing the manuscript.

Michael Urda

Montreal, 1972

Bibliography

1. I.G. Connell, "Abelian Formal Groups", Proc. of A.M.S., 17 (1966) 958-959.
2. J.Dieudonné, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caracteristique p>0", Comment.Math. Helv., 28 (1954) 87-118.
3. J. Dieudonné, "Lie groups and Lie hyperalgebras over a field of characteristic p>0", II, American J. Math., 77 (1955), 218-244.
4. J. Dieudonné, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caracteristique p>0", III, Math. Z., 63 (1955) 53-75.
5. J. Dieudonné, "Lie groups and Lie hyperalgebras over a field of characteristic p>0", IV, American J. Math., 77 (1955) 429-452.
6. J. Dieudonné, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caracteristique p>0", V, Bull. Soc. Math. France, 84 (1956) 207-239.
7. J. Dieudonné, "Lie groups and Lie hyperalgebras over a field of characteristic p>0", Amer. J. Math., 79 (1957) 331-388.
8. J. Dieudonné, "Groupes de Lie et hyperalgèbres de Lie sur un corps de caracteristique p>0", VII, Math. Ann., 134 (1957) 114-133.
9. J. Dieudonné, "Lie groups and Lie hyperalgebras over a field of characteristic p>0", VIII, Amer. J. Math., 80 (1958) 740-772.
10. S. Lang, "Algebra", Addison Wesley Publishing Co., Reading, Mass., (1967).
11. M. Lazard, "La non-existence des groupes de Lie formel non-abéliens à un parametre", C.R. Acad. Sci. Paris, 239 (1954) 942-945.
12. M. Lazard, "Sur les groupes de Lie formel à un parametre", Bull. Soc. Math. France, 83 (1955) 251-274.

13. J. Lubin, "One-parameter formal Lie groups over p-adic integer rings", Annals of Math., t.80 (1964) 464-484.

14. J. Lubin, "Finite subgroups and isogenies of one-parameter formal Lie groups", Ann. of Math., 85 (1967) 296-302.

15. J. Lubin, "Galois endomorphisms of the torsion subgroup of certain formal groups", Proc. of A.M.S., 20 (1969) 229-231.

16. J. Lubin and J. Tate, "Formal moduli for one-parameter formal Lie groups", Bull. Soc. Math. France, 94 (1966) 49-59.

17. J. Lubin and J. Tate, "Formal complex multiplication in local fields", Ann. of Math., 81 (1965) 380-387.

18. J.P. Serre, "Corps Locaux", Hermann, Paris (1962).

19. E. Weiss, "Algebraic Number Theory", McGraw-Hill Book Co., Inc., New York (1963).

20. H. Weyl, "Algebraic Theory of Numbers", Annals of Mathematics Studies no. 1, Princeton University Press, Princeton, N.J. (1940).

Contents

Preface		p. i
I	Elementary Properties of Group Laws	p. 1
II	Homomorphisms and Isomorphisms	p. 9
III	Properties of $\mathrm{Hom}_D(F,G)$ and $\mathrm{Hom}_k(F,G)$	p.15
IV	Isomorphisms between Group Laws and Properties of Power Series	p.27
V	A Construction of D-Group Laws	p.35
VI	The Reciprocity Law	p.43
Bibliography		p.iii

I Elementary Properties of Group Laws

D1 Given A, a commutative ring with unity, then $A[[T_1,\ldots,T_n]]$ represents the ring of formal power series in the n indeterminates, $T_1,\ldots,T_n$. The monomial $aT_1^{a_1}\ldots T_n^{a_n}$, $a\neq 0$, is said to have total degree $a_1+a_2+\ldots+a_n$.

D2 If F,G in $A[[T_1,\ldots,T_n]]$ then we write $F \equiv G \pmod{\deg r}$, by which is meant: any monomial occurring in F and G of total degree less than r occurs in F with the same coefficient as it occurs in G.

A power series substituted into another power series is a well-defined power series provided that the substituents have no constant term.

D3 A group law over A is any formal power series F in $A[[x,y]]$ satisfying:

1/ $F(x,y) \equiv x+y \pmod{\deg 2}$

2/ $F(F(x,y),z) = F(x,F(y,z))$, i.e. an associative law.

T1 $F(x,0) = x$ for any group law, F(similarly $F(0,y) = y$).

PROOF:

By the associative law $F(F(x,0),0) = F(x,F(0,0)) = F(x,0)$.

From the definition of group laws we may write $F(x,0) = x+b_2x^2+b_3x^3+\ldots$, and say that b_r is the first coefficient $\neq 0$ beyond the first;

then, $F(x,0) = x+b_rx^r+\ldots$;

hence, $F((x+b_rx^r+\ldots),0) \equiv x+b_rx^r+\sum_{i=r}^{\infty} b_i(x+b_rx^r+\ldots)^i \equiv x+2b_rx^r+\ldots \pmod{\deg r+1}$.

Therefore, $x+b_rx^r+\ldots = x+2b_rx^r+\ldots$, and so it follows that $b_r = 2b_r$, which implies that $b_r = 0$, contradicting our assumption that $b_r \neq 0$. Hence, there is no first coefficient of $F(x,0)$ beyond the first which is different from 0; that is, $F(x,0) = x$.

T2 If F is a group law over A then there exists $i_F(T)$ in $A[[T]]$ such that $F(T,i_F(T)) = 0$.

PROOF:

We may write $F(x,y) = x+y+a_{11}xy+(a_{12}xy^2+a_{21}x^2y)+\ldots$ using T1, and suppose we have a power series $i_F(T) = b_1T+b_2T^2+\ldots$; then we must find elements b_i so that $F(T,i_F(T)) = 0$. But, this is equivalent to solving the following sequence of equations:

$$b_1+1 = 0$$

$$b_2+a_{11}b_1 = 0$$

$$b_3+a_{11}b_2+a_{12}b_1^2+a_{21}b_1 = 0$$

$$\vdots \qquad \vdots$$

$$b_n+\sum n(i,j,k_1,k_2,\ldots,k_r,j_1,j_2,\ldots,j_r)a_{ij}b_{k_1}^{j_1},\ldots,b_{k_r}^{j_r} = 0$$

$$\vdots \qquad \vdots$$

where n's are positive integers and $\sum$ is extended over b_i's such that $i<n$. It is clear that a solution for the b_i's exists (in fact, the general formula for b_n could be obtained in terms of a_{ij}'s, $i+j\leq n$, and integers).

T3 Lazard showed that a group law defined over A, a commutative ring with unity, having no nilpotent elements (i.e. there does not exist a in A such that $a^n = 0$ for any positive integer n), must necessarily be abelian, that is $F(x,y) = F(y,x)$.

See Lazard's paper: "La non-existence des groupes de Lie formel non-abéliens à un parametre" (reference no. 11).

T3A In 1966 I.G. Connell obtained the following characterization: In order that all group laws over A be abelian it is necessary and sufficient that the ideal of nilpotent elements of A be torsion-free as an additive group.

See paper titled "Abelian Formal Groups", by I. Connell (reference no. 1).

Throughout the rest of this thesis we assume that the group laws we deal with are abelian so whenever we speak of a group law over a ring, that ring is assumed to satisfy the hypothesis of T3A.

T3B We will prove Lazard's result for fields, A, such that char A = 0.

PROOF:

It is clear that we need only show $a_{ij} = a_{ji}$ for every pair of positive integers, i,j. This is done by induction on i+j - for i=j=1 there is nothing to prove, so we can proceed and assume the inductional hypothesis, namely that $a_{ij} = a_{ji}$ for all $i+j<n$. Consider the associative law $F(F(x,y),z) = F(x,F(y,z))$, and compare the coefficients on the LHS, RHS of $xy^{i-1}z^j$, $x^jy^{i-1}z$, and $xy^{n-2}z$. For example, in the first case:

$$\begin{aligned}
\text{LHS} = {} & ((x+y+a_{11}xy+\ldots)+z) \\
& + a_{11}(x+y+a_{11}xy+\ldots)z) \\
& + (a_{12}(x+y+a_{11}xy+\ldots)z^2+a_{21}(x+y+a_{11}xy+\ldots)^2z) \\
& + (a_{13}(x+y+a_{11}xy+\ldots)x^3+a_{22}(x+y+a_{11}xy+\ldots)^2z^2+a_{31}(x+y+\ldots)^3z) \\
& + \text{etc.} \\
\text{RHS} = {} & (x+(y+z+a_{11}yz+\ldots))
\end{aligned}$$

$$+(a_{11}(x(y+z+a_{11}yz+\dots)))$$
$$+(a_{12}(x(y+z+a_{11}yz+\dots)^2+a_{21}x^2(y+z+a_{11}yz+\dots))$$
$$+(a_{13}(x(y+z+a_{11}yz+\dots)^3+a_{22}(x^2(y+z+a_{11}yz+\dots)^2)+a_{31}(x^3(y+z+a_{11}yx+\dots)))$$
$$+\text{etc};$$

we observe that $xy^{i-1}z^j$ can occur on LHS only within:

$$a_{1j}\ (x+y+\dots)z^j$$
$$a_{2j}(x+y+\dots)^2z^j$$
$$\vdots$$
$$a_{ij}(x+y+\dots)^iz^j$$

and on the RHS only within:

$$a_{11}x(y+z+\dots)$$
$$a_{12}x(y+z+\dots)^2$$
$$\vdots$$
$$a_{1,n-1}x(y+z+\dots)^{n-1}.$$

Hence, for this case we obtain $ia_{ij}+f(a_{lk}\text{'s}) = \binom{n-1}{i-1}a_{1,n-1}+g(a_{lk}\text{'s})$. And, similarly in the second case $ja_{ji}+f(a_{kl}\text{'s}) = \binom{n-1}{j-1}a_{n-1,1}+g(a_{kl}\text{'s})$.

(where $1+k<n$ and f,g are polynomials)

Therefore, $a_{ij}-a_{ji} = (\binom{n-1}{i-1}/i-\binom{n-1}{j-1}/j)a_{1,n-1} = 0$, since $i\binom{n-1}{j-1} = j\binom{n-1}{i-1}$, and $a_{1,n-1} = a_{n-1,1}$ (which is established as follows). In the latter case we get $(n-1)a_{1,n-1}+f(a_{lk}\text{'s}) = (n-1)a_{n-1,1}+f(a_{kl}\text{'s})$, where f is a polynomial and $1+k<n$; hence $a_{n-1,1} = a_{1,n-1}$.

D4 For group laws F,G over a ring, A, we put $\{f \text{ in } A[[T]]:\ f \equiv 0$

(mod deg 1) and $f(F(x,y)) = G(f(x),f(y))\} = \mathrm{Hom}_A(F,G)$, and call the individual elements A-homomorphisms from F to G. When there exists an A-homomorphism, f, from F to G, and an A-homomorphism, g, from G to F such that $f.g(T) = T = g.f(T)$, then we say that f is an A-isomorphism (similarly g).

T4 (Proposition) $\mathrm{Hom}_A(F,G)$ is an abelian group.
PROOF:

1/ We define the addition as follows:

for f,g in $\mathrm{Hom}_A(F,G)$ put $(f+g)(T) = G(f(T),g(T))$. We must show that f+g is again an A-homomorphism from F to G:

0// $(f+g)(T)$ is a well-defined power series since both f and g, by definition, have 0 constant term.

1// $(f+g)(F(x,y)) = G(f(F(x,y)), g(F(x,y))) =$

(definition of +)

$= G(G(f(x),f(y)),G(g(x),g(y))) =$

(f,g are A-homomorphisms)

$= G(G(f(x),f(y)),G(g(y),g(x))) =$ (G is abelian)

$= G(G(G(f(x),f(y)),g(y)),g(x)) =$ (G is associative)

$= G(G(f(x),G(f(y),g(y)),g(x)) =$ (G is associative)

$= G(f(x),G(G(f(y),g(y)),g(x))) =$ (G is associative)

$= G(f(x),G(g(x),G(f(y),G(y)))) =$ (G is abelian)

$= G(G(f(x),g(x)),G(f(y),g(y))) =$ (G is associative)

$= G((f+g)(x),(f+g)(y)) =$ (definition of +);

consequently $(f+g)(F(x,y)) = G((f+g)(x),(f+g)(y))$.

2/ As additive identity choose the zero power series, denoted $0(T)$; then $(f+0)(T) = G(f(T),0(T)) = G(f(T),0) = f(T)$ (by T1) and $(0+f)(T) = G(0(T),f(T)) = G(0,f(T)) = f(T)$ (by T1).

3/ Existence of additive inverses: let f in $\mathrm{Hom}_A(F,G)$ then we claim that $f+i_G.f = i_G.f+f = 0$; for, $(f+i_G.f)(T) = G(f(T),i_G.f(T)) =$ $= G(f(T),i_G.f(T)) = 0(T)$ by T2.

4/ Associativity of + : $(f+(g+h))(T) = G(f(T),(g+h)(T)) =$ $= G(f(T),G(g(T),h(T))) = G(G(f(T),g(T)),h(T)) =$ (by associativity of G)

$= G((f+g)(T),h(T)) =$ (definition of +)

$= ((f+g)+h)(T)$ (definition of +);

hence, $f+(g+h) = (f+g)+h$, where f,g,h in $\mathrm{Hom}_A(F,G)$.

1/ to 4/ show that $\mathrm{Hom}_A(F,G)$ is a group under +.

5/ Commutativity of +: $(f+g)(T) = G(f(T),g(T)) = G(g(T),f(T))$ since G is abelian, $= (g+f)(T)$; hence, $f+g=g+f$.

T5 (Proposition) The set of group laws over A gives rise to a category with a bi-additive composition.

PROOF:

1. The set of objects consists of group laws over A.

2. Given F,G, any two group laws, then Mor(F,G) is defined to be $\mathrm{Hom}_A(F,G)$.

3. Given 3 group laws F,G,H and homomorphisms f in $\mathrm{Hom}_A(F,G)$, g in $\mathrm{Hom}_A(G,H)$ then we define g.f to be $g.f(T) = g(f(T))$, i.e. the composed power series.

We must check that composition is well-defined, i.e. that g.f in $\mathrm{Hom}_A(F,H)$: but, $(F(x,y)) = G(f(x),f(y))$,

and, $g(G(x,y)) = H(g(x),g(y))$; we claim that $g.f(F(x,y)) = H(g.f(x),g.f(y))$, for, LHS $= g(f(F(x,y))) = g(G(f(x),f(y))) =$

$= H(g(f(x)),g(f(y))) = H(g.f(x),g.f(y)) =$ RHS.

The following axioms must be verified:

CAT1 $Hom_A(F,G),Hom_A(F',G')$ are disjoint or equal, the latter occurring only if $F=F'$, $G=G'$; this is done by specifying that homomorphisms f in $Hom_A(F,G)$ are actually triples (f,F,G).

CAT2 Given a group law, F, then define $1_F(T)$ to be T: so that if f in $Hom_A(F,G)$ $f.1_F(T) = f(T)$ implies $f.1_F = f$, and if g in $Hom_A(G,F)$ $1_F.g(T) = g(T)$ implies $1_F.g = g$.

CAT3 Given homomorphisms f in $Hom_A(F,G)$, g in $Hom_A(G,H)$, h in $Hom_A(H,I)$ of group laws F,G,H,I, then we must show that $h.(g.f) = (h.g).f$. But, this follows from the well known fact that well-defined composition of power series is associative.

To show that the category has a bi-additive composition we need: $(g_1+g_2).f = g_1.f+g_2.f$, and $g.(f_1+f_2) = g.f_1+g.f_2$ where g,g_1,g_2 in $Hom_A(G,H)$ and f,f_1,f_2 in $Hom_A(F,G)$. It suffices to show only one, the first, for example; $((g_1+g_2).f)(T) = (g_1+g_2)(f(T)) = H(g_1(f(T)), g_2(f(T)))$ $= (g_1.f+g_2.f)(T)$.

D5 We call $Hom_A(F,F)$ the set of endomorphisms of the group law F; it is denoted by $End_A(F)$.

T6 (Corollary) $End_A(F)$ is a ring with unity.

PROOF:

We already know it is an abelian group by T4. The multiplication on $End_A(F)$ is defined to be, simply, the composition of power series; it is well-defined, as was shown in T5 3. Furthermore, the multiplication is associative (see CAT3 of T5), and the unity element is clearly 1_F (see CAT2 of T5). Finally, the bi-additivity of . proved in T5 shows that this operation is distributive over +, i.e. $(f+g)h = f.h+g.h$ and $f.(g+h) = f.g+f.h$, where f,g,h in $End_A(F)$.

D6 The image of n in Z(integers) under the canonical homomorphism

$$\begin{array}{l} Z \longrightarrow End_A(F) \\ z \longrightarrow z.[1]_F \end{array}$$ is denoted by $[n]_F$.

II Homomorphisms and Isomorphisms

D7 Suppose that f in $A[[T]]$ with $f(T) = a_1T+a_2T^2+\ldots$ then the first degree coefficient of f, namely, a_1, is denoted c(f).

T7 (Proposition) The mapping $c:Hom_A(F,G)\longrightarrow A$, which is defined by: f in $Hom_A(F,G)$, $f = a_1T+a_2T^2+\ldots$, implies $c(f)=a_1$, is a group homomorphism which becomes a unitary ring homomorphism in the special case $c:End_A(F)\longrightarrow A$.

PROOF:

1/ Suppose f,g in $Hom_A(F,G)$, $f = a_1T+a_2T^2+\ldots$, $g = b_1T+b_2T^2+\ldots$ then $(f+g)(T) = G(f(T),g(T)) \equiv f(T)+g(T) \pmod{\text{deg } 2}$

$\equiv a_1T+b_1T \equiv (a_1+b_1)T \pmod{\text{deg } 2}$;

hence $c(f+g) = a_1+b_1 = c(f)+c(g)$.

2/ For the special case we again have $c(f+g) = c(f)+c(g)$ by 1/; but, also, $f.g(T) = f(g(T)) \equiv a_1b_1T \pmod{\text{deg } 2}$, so that $c(f.g) = a_1b_1 = c(f).c(g)$; and, finally, $1_F(T) = 1.T$ implies $c(1_F) = 1$.

Now we consider some properties involving group laws over two distinct rings.

D8 Let $*:A\longrightarrow B$ be a unitary homomorphism of commutative rings with unity and suppose $f(x_1,\ldots,x_n)$ is a power series over A then define a power series over B by putting $f^*(x_1,\ldots,x_n) = \sum a^*_{i_1,\ldots,i_n,j_1,\ldots,j_n} x_{i_1}^{j_1},\ldots,x_{i_n}^{j_n}$ provided that $f(x_1,\ldots,x_n) = \sum a_{i_1,\ldots,i_n} x_{i_1}^{j_1}\ldots x_{i_n}^{j_n}$.

T8 (Proposition) 1. There exists a covariant additive functor * from G_A to G_B (where G_A denotes the category of group laws over A).

2. The map $*: End_A(F) \longrightarrow End_B(F^*)$ given by $f \longrightarrow f^*$ is a unitary ring homomorphism (where * is the map in D8).

PROOF:

1. In order that a functor be defined we must associate each object of G_A with an object of G_B. This is done by taking F in $Obj(G_A)$ and mapping it onto F*; but, we should show that F* is, in fact, in G_B, i.e. that F* is a group law over B:

0/ clearly F* is a power series over B

1/ $F(x,y) \equiv x+y \pmod{\text{deg } 2}$ implies $F^*(x,y) \equiv 1^*x+1^*y \pmod{\text{deg } 2} = x+y \pmod{\text{deg } 2}$

2/ $F(F(x,y),z) = F(x,F(y,z))$ implies $F^*(F^*(x,y),z) = F^*(x,F^*(y,z))$ by taking * of LHS and RHS.

To complete the functor's definition we must associate with each f in $Hom_A(F,G)$ an element of $Hom_B(F^*,G^*)$ - this element is obviously f*. Now, we verify:

FUN1 $(1_F)^* = 1_{F^*}$; let f in $Hom_A(F^*,G^*)$, then $f.(1_F)^*(T) = f(1_F^*(T)) = f(T)$, so $f.(1_F)^* = f$ and if we put $f = 1_{F^*}$ it follows that $(1_F)^* = 1_{F^*}$.

FUN2 if f in $Hom_A(F,G)$, g in $Hom_A(G,H)$ we must show that $(g.f)^* = g^*.f^*$; let us assume $f = \sum a_i T^i$ and $g = \sum b_i T^i$, so that $(g.f)^*T = (g.f(T))^* = (\sum_k (\sum n a_i b_{j_1}^{k_1} \ldots b_{j_r}^{k_r}) T^k)^* =$ (where n is an integer depending on $i, j_1, k_1, \ldots j_r, k_r$ and the second $\sum$ also depends on these)

$= \sum_k (\sum n a_i * b_{j_1}{}^{*k_1} \ldots b_{j_r}{}^{*k_r}) T^k = g^*(f^*(T)) = g^* . f^*(T)$; this establishes the covariance of *.

The following will show that * is additive:

f,g in $\mathrm{Hom}_A(F,G)$ implies $(f+g)^* = f^*+g^*$; but, LHS $= (G(f(T),g(T)))^* =$

$= G^*(f^*(T),g^*(T)) =$ (see FUN 2 for a similiar verification), $= f^*+g^*$.

2. The fact that $*:\mathrm{End}_A(F) \longrightarrow \mathrm{End}_B(F^*)$ is a ring homomorphism has been established in 1., since, we showed that:

a/ * is additive i.e. $(f+g)^* = f^*+g^*$

b/ * is multiplicative i.e. $(f.g)^* = f^*.g^*$ (in FUN 2)

in a general setting. Of course, $(1_F)^* = 1_{F^*}$ by FUN 1.

D9 If f is in $A[[T_1,\ldots,T_n]]$, and has 0 constant term, and u, u^{-1} are in $A[[T]]$,-- we then put $f^u(T_1,\ldots,T_n) = u(f(u^{-1}(T_1),\ldots, u^{-1}(T_n)))$.

T9 (Lemma) F and G are isomorphic group laws over A if and only if there exists u(T) in $A[[T]]$ whose inverse exists and such that $G = F^u$.

PROOF:

1. Say $G = F^u$, then $uF(u^{-1}(x),u^{-1}(y)) = G(x,y)$ implies that $F(u^{-1}(x),u^{-1}(y)) = u^{-1}(G(x,y))$, which shows that u^{-1} is in $\mathrm{Hom}_A(G,F)$. Also, replacing x,y by u(x), u(y) respectively shows that $u(F(x,y)) =$ $= G(u(x),u(y))$, and so u is in $\mathrm{Hom}_A(F,G)$. Furthermore, we already know that $uu^{-1} = 1_G$, $u^{-1}u = 1_F$, so that one implication is completed.

2. If F,G are isomorphic over A then there exist f in $\mathrm{Hom}_A(F,G)$, g in $\mathrm{Hom}_A(G,F)$ such that $f.g = 1_G$, $g.f = 1_F$, so take u to be f and u^{-1} to be g; then $g(G(x,y)) = F(g(x),g(y))$ implies that $G(x,y) = f(F(g(x), g(y)))$,

i.e. $G=F^u$.

T10 (Proposition) If L is a field of characteristic zero then any group law F(overL) is isomorphic to x+y over L.

PROOF:

It suffices to show that there exists u in $L[[T]]$ which is invertible and which satisfies: $F(x,y) = u(u^{-1}(x)+u^{-1}(y))$.

1. First show that for any u in $L[[T]]$ which is invertible $u(u^{-1}(x)+u^{-1}(y))$ is a group law:

0/ it is clearly a power series over L

1/ it is $\equiv x+y \pmod{\deg 2}$, from inspection

2/ $u(u^{-1}(u(u^{-1}(x)+u^{-1}(y)))+u^{-1}(z))=u((u^{-1}(x)+u^{-1}(y))+u^{-1}(z))$
$= u(u^{-1}(x)+(u^{-1}(y)+u^{-1}(z)))=u(u^{-1}(x)+u^{-1}(u(u^{-1}(y)+u^{-1}(z))))$

2. Now, we claim that any group law over a field of characteristic zero (in our case L), say $F = \sum a_{ij}x^iy^j$, is determined by $a_{11},a_{12},a_{13},\ldots$; and this demonstrated, when it is shown that each a_{ij}, $i+j=n$, can be represented by a function depending only on $a_{1,n-1}$ and a_{1k}'s where $1+k<n$. Let us examine the associativity relation $F(F(x,y),z) = F(x,F(y,z))$.

$$\begin{aligned}
\text{LHS} = {} & ((x+y+a_{11}xy+\ldots)+z) \\
& + (a_{11}(x+y+a_{11}xy+\ldots)z) \\
& + (a_{12}(x+y+a_{11}xy+\ldots)z^2+a_{21}(x+y+a_{11}xy+\ldots)^2z) \\
& + (a_{13}(x+y+a_{11}xy+\ldots)z^3+a_{22}(x+y+a_{11}xy+\ldots)^2z^2+a_{31}(x+y+a_{11}xy+\ldots)^3z) \\
& + \text{etc.}
\end{aligned}$$

$$\text{RHS} = (x+(y+z+a_{11}yz+\ldots))$$

$$+(a_{11}(x(y+z+a_{11}yz+\dots))$$
$$+(a_{12}(x(y+z+a_{11}yz+\dots)^2+a_{21}x^2(y+z+a_{11}yz+\dots))$$
$$+(a_{13}(x(y+z+a_{11}yz+\dots)^3+a_{22}(x^2(y+z+a_{11}yz+\dots)^2)+a_{31}(x^3(y+z+a_{11}yz+\dots)))$$
$$+\text{etc.}$$

Compare the coefficients of $xy^{i-1}z^j$ on both sides of the equation: $xy^{i-1}z^j$ can occur on LHS only within:

$$a_{1j}(x+y+\dots)z^j$$
$$a_{2j}(x+y+\dots)^2z^j$$
$$\vdots$$
$$a_{ij}(x+y+\dots)^iz^j,$$

and on RHS only within:

$$a_{11}x(y+z+\dots)$$
$$a_{12}x(y+z+\dots)^2$$
$$\vdots$$
$$a_{1,n-1}x(y+z+\dots)^{n-1}.$$

by equating coefficients we obtain--$ia_{ij}+f_n(a_{lk}\text{'s}) = \binom{n-1}{i-1}a_{1,n-1}+g_n(a_{lk}\text{'s})$ (where f_n, g_n are some determinable polynomials and $l+k<n$). Hence, the equation we want is: $a_{ij} = (\binom{n-1}{i-1}a_{1,n-1}+g_n(a_{lk}\text{'s})-f_n(a_{lk}\text{'s}))i^{-1}$.

3. Consider all possible group laws $u(u^{-1}(x)+u^{-1}(y))$ where u runs over invertible power series, we observe that any such group law is of the form $\sum b_{ij}x^iy^j$ where $b_{11} = f_1(b_1,b_2)$

$$b_{12} = f_2(b_1,b_2,b_3)$$
$$\vdots$$
$$b_{1n} = f_n(b_1,\dots,b_{n+1})$$
$$\text{etc.},$$

where b_i are variables (coefficients of u), $b_1 \neq 0$ and $f_1(b_1,\ldots,b_{i+1})$ is a function in which b_{i+1} occurs without multipliers. (Note that since L is a field of characteristic zero all power series $\neq 0$ and having non-zero first degree term are invertible, and this allows us to call the $b_1,b_2,\ldots,b_n,\ldots$ "variables".) Let $F(x,y) = \sum a_{ij}x^iy^j$, and put $b_{1n} = a_{1n}$ for all n; this allows us to solve for the b_i in terms of the a_{1i} and still, we can consider b_1 to be a variable. By part 2. $F(x,y) = u(u^{-1}(x)+u^{-1}(y))$ with $b_1 = 1$, for example.

T11 (Corollary) Any group law, F, over a field of characteristic zero is determined by the coefficients $a_{11},a_{12},\ldots,a_{1n},\ldots$, where $F(x,y) = \sum a_{ij}x^ix^j$.

PROOF:

See proof of T10 2.

III Properties of $\mathrm{Hom}_D(F,G)$ and $\mathrm{Hom}_k(F,G)$

D10 We denote by D any complete valuation ring such that char D =0 and which is discrete; $Q(D) = L$ represents the quotient field of D, $m = dD$ is the maximal ideal of D and $k = D/m$ is the residue field with p(=prime) elements. U represents the units of D.

T12 (Theorem) 1. $c:\mathrm{Hom}_D(F,G) \longrightarrow D$ is an injective homomorphism of groups.

2. The image of c is a closed subgroup of D.

PROOF:

1. The result, T7, shows that c is already a group homomorphism, so it remains to demonstrate that c is an injection. Let f in $\mathrm{Hom}_D(F,G)$ be such that $c(f) = 0$, we claim that $f = 0$. By T10 we have $F(x,y) = u(u^{-1}(x)+u^{-1}(y))$, $G(x,y) = v(v^{-1}(x)+v^{-1}(y))$, with u,v in $L[[T]]$ (where $L = Q(D)$). But, since f is a homomorphism $f(F(x,y)) = G(f(x),f(y))$ which implies $f.u(u^{-1}(x)+u^{-1}(y)) = v(v^{-1}.f(x)+v^{-1}.f(y))$; hence, $v^{-1}(f.u)(u^{-1}(x)+u^{-1}(y)) = v^{-1}.f(x)+v^{-1}.f(y)$, and replacing x by u(x), y by u(y) yields $v^{-1}.f.u(x+y) = v^{-1}.f.u(x)+v^{-1}.fu.(y)$. This means that $v^{-1}.f.u$ is an additive power series, and so $v^{-1}.f.u$ must be a linear monomial, aT, for example.

It is clear that we may choose u,v having first coefficient equal to 1 (by the concluding remark in T 10) so that a must $b_e c(f)$, which is 0 by hypothesis. Therefore, $v^{-1}.f.u = 0$, and this obviously implies $f = 0$.

2. The proof takes four steps.

1/ $c(\mathrm{Hom}_D(F,G)) = \{a \in D:\ v.(a).u^{-1}$ in $D[[T]]$, where $(a)(T) = aT\}$.

Proof:

By the technique in 1. we can write f in $\mathrm{Hom}_D(F,G)$ in the form $v.(a).u^{-1}$ where $a = c(f)$, for particular u,v depending only on F,G. This shows that if c(f) in LHS then $c(f) = a$ in RHS, because $v.(a).u^{-1} = f$ in $\mathrm{Hom}_D(F,G)$ implies $v.(a).u^{-1}$ in $D[[T]]$, and a in D.

Conversely, suppose a in RHS, i.e. $v.(a).u^{-1}$ in $D[[T]]$ and a in D then $v.(a).u^{-1}$ in $\mathrm{Hom}_D(F,G)$:

for, $v.(a).u^{-1}(F(x,y)) = v.(a)(u^{-1}(x)+u^{-1}(y)) = v(a(u^{-1}(x))+a(u^{-1}(y)))$

$= v((a).u^{-1}(x)+(a)u^{-1}(y)) =$

$= G(v((a).u^{-1}(x)),v((a).u^{-1}(y))) =$

$= G(v.(a).u^{-1}(x),v.(a)u^{-1}(y))$.

Furthermore, $c(v.(a).u^{-1}) = a$ by definition of v and u^{-1} (see 1.), and consequently a in LHS.

2/ Associate with each a in L the element $b_i(a)$, obtained as the coefficient of T^i in $v.(a).u^{-1}$; then $b_i(a)$ is a polynomial function of a whose coefficients are in L; hence, $b_i(a)$ is a continuous function of a (using the valuation metric).

3/ Let us define $X_i = \{a$ in D: $b_i(a)$ in $D\}$, then it follows that X_i is closed in D:

Proof:

It is clear that D is closed in $L = Q(D)$ and also that $b_i(D)$ is closed in L; hence, it follows that $b_i(D) \cap D$ is closed in L(because

the intersection of two closed sets is again closed). But, this last set is precisely X_i.

$$4/\ \cap X_i = \{a \text{ in } D:\ v.(a).u^{-1} \text{ in } D[[T]]\}.$$

Proof:

Let a in $\cap X_i$, then $b_i(a)$ in D for each i, hence, $v.(a).u^{-1}$ is in $D[[T]]$ and, therefore, a in RHS.

Let a in RHS, then $v.(a).u^{-1}$ in $D[[T]]$ and clearly $b_i(a)$ in D for each i; hence, a in X_i for all i, which implies that a in LHS.

In conclusion we observe that $\cap X_i$ is closed since X_i are closed; therefore, $c(\mathrm{Hom}_D(F,G))$, which is $\cap X_i$ by 1/ and 4/, is closed in D.

In the proof of T12 1. we could have replaced D by L and obtained that $c:\mathrm{Hom}_L(F,G) \longrightarrow L$ is injective, this makes possible the following definition (extending in a sence D6).

D11 Denote by $[a]_F$ the unique L-endomorphism of F with first degree coefficient equal to a, for any a in L.

T13 $\mathrm{Hom}_D(F,G)$ is a Z_p module, where Z_p is the ring of p-adic integers.

PROOF:

Observe that $c(\mathrm{End}_D(F))$ is closed in D by T12 2., contains Z (since $c([n]_F) = n$), and hence contains the closure, Z_p, of Z in D. Hence, the injectivity of $c^{-1}:c(\mathrm{End}_D(F)) \longrightarrow \mathrm{End}_D(F)$ shows that Z_p is canonically contained in $\mathrm{End}_D(F)$.

Let a in Z_p and f in $\mathrm{Hom}_D(F,G)$, then we define the action of Z_p on $\mathrm{Hom}_D(F,G)$ as follows: $a.f = f.[a]_F$ $\quad (=[a]_G.f)$; this action

is well-defined since -

1. a.f in $\mathrm{Hom}_D(F,G)$, for, $f.[a]_F F(x,y) = f([a]_F(F(x,y))) = f(ax,ay) =$
   $= G(f(ax),g(ay)) = G(f.[a]_F(x),f.[a]_F(y))$,
2. given a there is a unique $[a]_F$.

T14 (Proposition) If f in $\mathrm{Hom}_k(F,G)$, where k is any field such that char $k = p>0$ and $f \not\equiv [0]$ then there exists $q = p^r$ such that $f(T) \equiv aT^q \pmod{\deg q+1}$, $a \neq 0$.

PROOF:

Suppose $f(T) = a_1T+a_2T^2+\ldots$, and say that n is the smallest positive integer such that $a_n \neq 0$, so $f(T) = a_nT^n+\ldots$ and $f(T) \equiv a_nT^n \pmod{\deg n+1}$. But, since f in $\mathrm{Hom}_k(F,G)$ we get $f(F(x,y)) \equiv G(f(x),f(y)) \pmod{\deg n+1}$; hence, $a_n(x+y)^n \equiv a_nx^n+a_ny^n \pmod{\deg n+1}$, which implies $(x+y)^n = x^n+y^n$.

Now, suppose there exists $m|n$ such that g.c.d.$(m,p) = 1$ and say $n = mp^r$ then $x^{p^rm}+y^{p^rm} = (x+y)^{p^rm}$. We know from elementary number theory that $x^{p^r}+y^{p^r} = (x+y)^{p^r} \pmod{p}$, so we get, putting $s = x^{p^r}$, $t = y^{p^r}$, $s^m+t^m = (s+t)^m \pmod{p}$ which implies that $\binom{m}{1} = m \equiv 0 \pmod{p}$, a contradiction. Therefore, there does not exist $m|n$ such that $(m,p) = 1$; i.e. $n = p^r$ for some positive integer r. Therefore, $f(T) \equiv a_nT^n \pmod{\deg n+1}$ and $n = p^r$.

D12 Given a group law F defined over k (a field of characteristic p) and if $0 \neq [p]_F(T) \equiv aT^{p^h} \pmod{\deg p^h+1}$, which must be the case by T14 then h is called the height of F; if $[p]_F(T) = 0$ then we say that F has infinite height (in both cases denoted height(F)).

T15 If height(F) $\neq$ height(G) then $\mathrm{Hom}_k(F,G) = 0$, where F,G are group laws over k.

PROOF:

Suppose that $0 \neq f$ in $\mathrm{Hom}_k(F,G)$, then $f(F(x,y)) = G(f(x),f(y))$ and hence $f\cdot[p]_F = f\cdot([1]_F+\ldots+[1]_F)$ (p times) $= f\cdot[1]_F+\ldots+f\cdot[1]_F = f+\ldots+f$; also $[p]_G\cdot f = ([1]_G+\ldots+[1]_G)\cdot f = [1]_G\cdot f+\ldots+[1]_G\cdot f = f+\ldots+f$; therefore, $f\cdot[p]_F = [p]_G\cdot f \neq 0$ (unless both $[p]_F$ and $[p]_G = 0$ in which case height F = height G = infinity). It is clear that this equation holds only if the leading coefficients of $[p]_F$ and $[p]_G$ have the same degree, which by T14 must be of the form p^h; hence, height (F) = height (G). The statement T15 is simply the contrapositive of the above deduction.

T16 (Proposition) 1. height $(F^*)<\infty$ implies *: $\mathrm{Hom}_D(F,G)\longrightarrow\mathrm{Hom}_k(F^*,G^*)$ is injective.

2. height $(F^*)=\infty$ does not imply *: $\mathrm{Hom}_D(F,G)\longrightarrow\mathrm{Hom}_k(F^*,G^*)$ is injective.

PROOF:

1. We will show that $f \neq 0$ implies $f^* \neq 0$. It is clear that when at least one of f's coefficients is a unit then $f^* \neq 0$, so we assume that each coefficient of f has value greater than zero. Hence, $f(T) = d^r g(T)$ where $r>0$ is some integer, d is a local uniformizer (arising from the valuation on D), and g(T) in $D[[T]]$ is such that $g^*(T) \neq 0$. Now,

$d^f\cdot g(F(x,y)) = G(d^r g(x), d^r g(y))$, since f in $\mathrm{Hom}_D(F,G)$,

$= d^r g(x)+d^r g(y)+d^{2r}P(x,y)$, since G is a group law and P(x,y) in $D[[x,y]]$.

Hence, $g(F(x,y)) = g(x)+g(y)+d^r P(x,y)$, so that $g^*(F^*(x,y)) = g^*(x)+g^*(y)$.

But, this shows that g^* in $\mathrm{Hom}_k(F^*,x+y)$, and we can easily see that height $(x+y)$ is infinite (since $[p]_{x+y} = [1]_{x+y}+\ldots+[1]_{x+y} = pT = 0$, since char $k = p$); so that $g^*=0$ by T15. Hence, we have a contradiction and our assumption (that $r>0$) is false - so $f^* \neq 0$.

2. Consider F^* of infinite height and G^* of finite height; in particular $F(x,y) = x+y+bxy$, b in m, the maximal ideal of D, and $G(x,y) = x+y+xy$, so height (F^*) = height $(x+y)$ is infinite whereas height $(G^*) = 1$. Put $f(T) = bT$, then $f(F(x,y)) = f(x+y+bxy) = (bx+by+b^2xy) = G(bx,by) = G(f(x),f(y))$, which means f in $\mathrm{Hom}_D(F,G)$ and yet $f^* = 0$ so * is not injective.

T17 (Proposition) If F,G are group laws over D then there exist polynomials P_i in $D[X_1,\ldots,X_n]$ and R_i in $L[X]$ where $L = Q(D)$ satisfying:

1. $R_i(X) = P_i(X,R_2(X),\ldots,R_{i-1}(X))$ when $i \neq p^r$ for some $r>0$,
2. $R_i(X) = 1/pP_i(X,R_2(X),\ldots,R_{i-1}(X))$ if $i = p^r$ for some $r>0$,
3. if f in $\mathrm{Hom}_L(F,G)$ and $c(f) = a_1$ in L then ith degree coefficient in f(T) is $R_i(a_1)$.

PROOF:

Induction on i.

Case i = 1: Let $R_1 = P_1 = X$ then 1.,2. are clearly satisfield; suppose f in $\mathrm{Hom}_L(F,G)$, $c(f) = a_1$ in L then the first degree coefficient in f(T) is a_1 and $R_1(a_1) = X(a_1) = a_1$, so 3. holds.

Case j=i: We must show that the result holds for j = i.

1. Say $i \neq p^r$, $r>0$, let $i = mq$ where $m>1$, p does not divide m and $q = p^r$.

2. Suppose $i = p^r$, $r>0$, let $i = mq$ again where $m = p$ and $q = p^{r-1}$.

Since f is a homomorphism we have $f(F(x,y)) = G(f(x),f(y))$, and we can examine the coefficients of $x^q y^{(m-1)q}$ on both sides of this equality. On the LHS we get a polynomial over D in $a_1,\ldots,a_{i-1}$, added to $\binom{mq}{q}a_i$; On the RHS we get a polynomial over D in $a_1,\ldots,a_{i-1}$, but a_i does not appear. Equating coefficients and solving for a_i we get:

a_i equal to a polynomial over D, $P_i(a_1,\ldots,a_{i-1})$ if $i \neq p^r$,

a_i equal to 1/p·(a polynomial over D), $1/p\ P_i(a_1,\ldots,a_{i-1})$ if $i = p^r$;

since $\binom{mq}{q}$ is p-adic unit if $i \neq p^r$ and is 1/p times a p-adic unit otherwise (it is sufficient to show a. $(m,p) = 1$ implies $(\binom{p^r m}{p^r},p) = 1$

b. $(\binom{pp^{p-1}}{p^{p-1}},p^2) = p$;

this is done by observing $\binom{p^r m}{p^r} = \prod_{z=0}^{p^r-1} (mp^r-z)/(p^r-z)$, in which mp^r-z, p^r-z always have the same power of p, and $\binom{p^r}{p^{r-1}} = \prod_{z=0}^{p^r-1} (p^r-z)/(p^{r-1}-z)$, in which p^r-z, $p^{r-1}-z$ always have the same power of p except when $z = 0$). This defines P_i, and now we put $R_i(X) = P_i(X,\ldots,R_{i-1}(X))$ if $i \neq p^r$

and $R_i(X) = 1/pP_i(X,\ldots,R_{i-1}(X))$ if $i = p^r$.

By the definitions of R_i, P_i 3. follows immediately.

T18 (Corollary) Suppose that f in $\mathrm{Hom}_L(F,G)$, where F,G are group laws over D, $f = a_1T+a_2T^2+\ldots$, and that $n>1$ is the smallest positive integer such that a_n is not in D, then 1. $n = p^r$ for some $r>0$

and 2. pa_n in D.

PROOF:

1. If $n \neq p^r$, $r>0$ then by T17 there are polynomials $P_1,\ldots,P_n$ over D and $R_1,\ldots,R_n$ such that $R_n(X) = P_n(X, R_2(X),\ldots,R_{n-1}(X))$ and $R_n(a_1) = a_n$. But, since n is the smallest positive integer such that

a_n is not in D it is clear that $a_1,\ldots,a_{n-1}$ are in D, so that $R_1(a_1)$, $\ldots,R_{n-1}(a_n)$ must be in D. Now $a_n = R_n(a_1) = P_n(a_1,\ldots,R_{n-1}(a_1))$ which is clearly in D, and yet a_n is not in D; this contradiction enables us to conclude that $n = p^r$.

2. We know that $P_n(a_1,R_1(a_1),\ldots,R_{n-1}(a_1))$ is in D, but this is exactly equal to pa_n since $n = p^r$.

D13 If n is an integer greater than or equal to 2 put $B_n(x,y) =$
$= (x+y)^n-x^n-y^n$, and $C_n(x,y) = B_n$ if n is not a power of a prime
$= 1/qB_n$ if n is a prime (=q) power.

T19 $C_n(x,y)$ is not zero considered as a polynomial of $K[x,y]$ where K is any field.

PROOF:

We must show that the coefficients of $C_n(x,y)$ are relatively prime.

Case a. Let $C_n = B_n = \binom{n}{1} x^{n-1}y+\ldots+\binom{n}{n-1} xy^{n-1}$, and suppose that p is a prime dividing each coefficient; it follows that p divides n and that $(x+y)^n = x^n+y^n \pmod p$. Put $p^r = q$ and $n = qm$ where $(p,m) = 1$ and p^{r+1} does not divide n, then $(x+y)^{qm} = (x^q)^m+(y^q)^m$ which implies that $(x^q+y^q)^m = (x^q)^m+(y^q)^m \pmod p$, and hence p divides m, a contradiction. Therefore, our assumption that some prime divides each coefficient is false.

Case b. Let $C_n = 1/pB_n$, p is a prime and $n = q^r$. Again, let q be a prime dividing all the coefficients of C_n then q divides p^{r-1} and so q must be p; but near the end of T17 we showed that $(\binom{p^r}{p^{r-1}}, p^2) = p$, so $q = p$ does not divide all coefficients of C_n, contradicting our

assumption; hence, the result.

The following is a result due to Lazard, we prove it for integral domains.

T20 (Proposition) Let F,G be abelian group laws over any commutative ring,A, with 1 such that $F \equiv G \pmod{\deg n}$ then there exists a in A such that $F(x,y) \equiv G(x,y)+aC_n(x,y) \pmod{\deg n+1}$.

PROOF:

This proof is valid forintegral domains, A.

1. First, we prove the result for fields, A, of characteristic zero. By comparing the coefficients of $xy^{i-1}z^j$ for the associative law, $F(F(x,y),z) = F(x,F(y,z))$, we get (where $F(x,y) = x+y+a_{11}xy+\ldots$) $ia_{ij}+f_{ij}(a_{lk}'s) = \binom{n-1}{i-1}a_{1,n-1}+g_{ij}(a_{lk}'s)$, where $1+k<n$ and f_{ij},g_{ij} are simple functions since:

on LHS $xy^{i-1}z^j$ occurs only in $a_{1j}(x+y+a_{11}xy+\ldots)z^j$

$$a_{2j}(x+y+a_{11}xy+\ldots)^2z^j$$

$$\vdots$$

$$a_{ij}(x+y+a_{11}xy+\ldots)^iz^j$$

while on RHS it occurs only in $a_{11}x(y+z+a_{11}yz+\ldots)$

$$a_{12}x(y+z+a_{11}yz+\ldots)^2$$

$$\vdots$$

$$a_{1,n-1}x(y+z+a_{11}yz+\ldots)^{n-1}.$$

Similarly for $G(x,y) = x+y+b_{11}xy+\ldots$. Hence, $i(a_{ij}-b_{ij}) = \binom{n-1}{i-1}(a_{1,n-1}-b_{1,n-1})$ since $f_{ij}(a_{lk}'s) = f_{ij}(b_{lk}'s)$ and $g_{ij}(a_{lk}'s) = g_{ij}(b_{lk}'s)$ by hypothesis. Therefore, all we need is to solve:

when $n \neq q^r$ $a_{ij}-b_{ij} = (\binom{n-1}{i-1}/i)(a_{1,n-1}-b_{1,n-1}) = \binom{n}{i}$ for each i between 1 and n-1. This is done if we put $a = (\binom{n-1}{i-1}/i\binom{n}{i})(a_{1,n-1}-b_{1,n-1})$, i.e. $a = (a_{1,n-1}-b_{1,n-1})/n$ (since $\binom{n-1}{i-1}/i = \binom{n}{i}/n$ from elementary number theory). Note that if $n = q^r$ then the above applies to yield $a = (a_{1,n-1}-b_{1,n-1})p/n$.

2. Now we prove the result for fields, A, of characteristic p = prime.

Case 1 $n \neq q^r$.

1/ p does not divide n: Here we can solve for $a_{ij}-b_{ij}$ in terms of $a_{1,n-1}-b_{1,n-1}$ as follows. Say p does not divide i then examination of coefficients (in the associative law) for $xy^{i-1}z^j$ gives $a_{ij}-b_{ij} = (\binom{n-1}{i-1}/i)(a_{1,n-1}-b_{1,n-1}$ as in 1. If p does divide i then it does not divide j = n-i and we apply the above procedure to a_{ji} (which is actually a_{ij}) and get a symmetric result. Hence, there is only one equation to solve - it is $na=(a_{1,n-1}-b_{1,n-1})$ and has the obvious solution.

2/ p does not divide n and $n = p^r m, (m,p)=1$: Since $p|n$ then comparing coefficients of $xy^p z^{n-p}$ in the associative law shows that $a_{1,n-1}-b_{1,n-1} = 0$. Comparing coefficients of $xy^{i-1}z^j$ for i not a multiple of p yields $a_{ij}-b_{ij} = 0$. So for these i,j any a will do to solve $a_{ij}-b_{ij} = \binom{n}{i}a$ since p divides $\binom{n}{i}$. Consequently we focus our attention on a_{ij} where i and hence j are multiples of p.

Consider $a_{p,n-p}, a_{2p,n-2p}, \ldots, a_{(p-1)p,n-(p-1)p}$; comparing coefficients of $x^{Lp}y^{n-(L+1)p}z^p$ (L between 1 and p-1) yields a relation between $\binom{n-p}{Lp}a_{p,n-p}$ and $\binom{n-Lp}{p}a_{Lp,n-Lp}$ and since p does not divide $\binom{n-Lp}{p}$ we can solve for $a_{Lp,n-Lp}$ in terms of $a_{p,n-p}$; this then shows

that the equations $a_{Lp,n-Lp}-b_{Lp,n-Lp} = \binom{n}{Lp}a$ all reduce to the same equation, $a_{p,n-p}-b_{p,n-p} = \binom{n}{p}a$. Similarly for $a_{p^s,n-p^s}, a_{2p^s,n-2p^s}, \ldots,$ $a_{(p-1)p^s,n-(p-1)p^s}$, $s<r$ we get only one equation actually, $a_{p^s,n-p^s}-b_{p^s,n-p^s} = \binom{n}{p^s}a$. For $s = r$ we get the same except that L is between 1 and m-1, but still only one equation results. Now, we need only consider equations dealing with $a_{p,n-p},\ldots,a_{p^r,n-p^r}$. But comparing coefficients of $x^p y^{n-p-p^2} z^{p^2}$ gives a relation between $\binom{n-p}{p^2}a_{p,n-p}$ and $\binom{n-p^2}{p}a_{p^2,n-p^2}$ which enables us to solve for $a_{p,n-p}$ in terms of $a_{p^2,n-p^2}$ since p does not divide $\binom{n-p}{p^2}$. Again we see that the first two equations become one. In a similar fashion we eliminate other equations to finally be left with only one equation, which is $a_{p^r,n-p^r}-b_{p^r,n-p^r} = \binom{n}{p^r}a$ and which can easily be solved since p does not divide $\binom{n}{p^r}$.

Case 2 $n = q^r$.

Either p divides n i.e. $p = q$ or it does not divide n. If $q \neq p$ then Case 1.1/ applies with minor alteration and finally we obtain again that there is only one equation to solve: $(n/q)a = a_{1,n-1}-b_{1,n-1}$ to which the solution is obvious. When $q = p$ we are forced to apply the technique of Case 1.2/ in which instance the only equation to solve becomes: $a_{p^{r-1},n-p^{r-1}}-b_{p^{r-1},n-p^{r-1}} = (\binom{n}{p^{r-1}}/p)a$, the solution to which is again clear.

3. We can now prove the result for arbitrary integral domains, A, with unity. Consider Q(A), the quotient field of A, and observe that F,G are elements of the set of group laws over Q(A), by the natural embedding; now, the proposition holds for Q(A) so we obtain a in Q(A)

such that $F(x,y) \equiv G(x,y)+aC_n(x,y) \pmod{\deg n+1}$. But $F(x,y)-G(x,y)$ is over A so that a must be in A also; (T19 shows that the coefficients of C_n are relatively prime so a linear combination of them equals 1).

T21 (Proposition) Let F,G be group laws over D and suppose that $F^*(x,y) \equiv H^*(x,y)+aC_r(x,y) \pmod{\deg r+1}$, a in k, $r=p^s$; then, $[p]_{F^*}(T) \equiv [p]_{H^*}(T)-aT^r \pmod{\deg r+1}$.

PROOF:

A simple computation reveals that $[p]_{F^*}(T) =$

$= \sum_n (f(a_{lk}\text{'s})+\sum_{i+j=n}(\sum_{l=1}^{p-1} l^i)a_{ij})T^n$, (where f is a simple function and $1+k<n$) so that $[p]_{F^*}-[p]_{H^*} \equiv \sum_{\substack{i+j=r \\ 1\le i\le j}}(\sum_{l=1}^{p-1} l^i)(a_{ij}-b_{ij}))T^r \pmod{\deg r+1}$, since the previous $a_{lk} = b_{lk}$, $1+k<n$,

$$= (\sum_{\substack{i+j=r \\ 1\le i\le j}}(\sum_{l=1}^{p-1} l^i\binom{n}{i}))/p.aT^r.$$

But,

$$\sum_{\substack{i+j=r \\ 1\le i\le j}}(\sum_{l=1}^{p-1} l^i\binom{n}{i}) = \sum_{l=1}^{p-1}(\sum_{i+j=r} l^i\binom{n}{i}) = \sum_{l=1}^{p-1}(l+1)^i-l^i-1^i = p^{p^s}-p.$$

Hence $[p]_{F^*}(T)-[p]_{H^*}(T) \equiv ((p^{p^s}-p)/p)aT^r = -aT^r \pmod{\deg r+1}$.

IV Isomorphisms between Group Laws and Properties of Power Series

D14 Let f in $A[[T_1,\ldots,T_n]]$ for any ring, A, and consider the polynomial $p(T_1,\ldots,T_n)$ such that $p \equiv f \pmod{\deg n+1}$, we will call this p the n-bud of f and denote it by n-bud(f).

It is clear that n-bud(f) = n-bud(g) if and only if $f \equiv g \pmod{\deg n+1}$.

T22 (Theorem) Say F is a group law defined over D, height(F*) = h finite, coefficients of the q-bud of F, $(q = p^h)$, $\in U$, a subring of D such that Q(U) is an unramified extension of Q_p; then there exists a D-group law $G(x,y) \equiv x+y+aC_q(x,y) \pmod{\deg q+1}$, where a is a unit in U, such that F is U-isomorphic to G. It follows that F is D-isomorphic to G.

PROOF:

We claim there exists G(x,y) such that $G(x,y) \equiv x+y \pmod{\deg q}$ and $G^v = F$, v in $U[[T]]$, i.e. G is U-isomorphic to F. First, we know that for some integer $r \geq 2$ there is a G(x,y) such that $G(x,y) \equiv x+y \pmod{\deg r}$ with G being U-isomorphic to F (simply take r = 2 and F = G). Now, let r be the largest positive integer less than $q = p^h$ such that there is a G with $G(x,y) \equiv x+y \pmod{\deg r}$ and $G^v = F$ for some v in $U[[T]]$. Then $G(x,y) \equiv x+y+bC_r(x,y) \pmod{\deg r+1}$ by T20, b in U.

Case 1 If $r \neq p^s$ for some integer $s \geq 0$ then $C_r = cB_r$ where c is invertible in Z_p, and hence in U. Put $u(T) = T-bcT^r$ in $U[[T]]$ then $F^u(x,y) \equiv$ $\equiv F(x,y)+aB_n(x,y) \pmod{\deg n+1}$ (which can be shown by substituting), $\equiv x+y+bcB_r(x,y)+(-b)cB_r(x,y) \equiv x+y \pmod{\deg r+1}$, and we have G^u,F U-isomorphic (since $(G^u)^{u^{-1}v} = G^{(uu^{-1})v} = G^v = F$).

Case 2 If $r = p^s$ for some integer $s \geq 0$ the b is necessarily not a unit in U (suppose it were, then $[p]_{G^*}(T) \equiv -b^*T^r \pmod{\deg r+1}$ by T21, where $H^* = x+y$; hence, height$(G^*) = s < h$ contradicting the result, T15, (note: F D-isomorphic to G implies F* k-isomorphic to G*)). But, U is unramified over Q_p so $b = pc$ for some c in U; therefore, letting $u(T) = T - cT^r$ in $U[[T]]$ we obtain $G^u(x,y) \equiv x+y \pmod{\deg r+1}$. Once again, G^u is D-isomorphic to F (via $u^{-1}v$). This completes the proof of the claim since we need only apply the above process finitely many times to arrive at the last step: $G(x,y) \equiv x+y + O(x,y) \pmod{\deg q}$ where $O(x,y)$ is the zero power series and $G = F^v$ for some v in $U[[T]]$.

Hence, $G(x,y) \equiv x+y+aC_q(x,y) \pmod{\deg q+1}$, a in U, by T20. It remains to show that a is a unit; but, if it were not we would obtain $[p]_{G^*}(T) \equiv (-a)T^r + aT^r = 0 \pmod{\deg q+1}$ by T21, which says that height$(G^*) > h$, contradicting the existence of a U-isomorphism between F* and G* (making use of T15).

<u>D15</u> Let A be any ring, then $A[[T_1,\ldots,T_n]]_r$ stands for the set: $\{f$ in $A[[T_1,\ldots,T_n]]$: non-zero coefficients of f occur only for degrees $\equiv 1 \pmod{\deg r-1}\}$.

It is clear that f in $A[[T_1,\ldots,T_n]]_r$ and u in $A[[T]]_r$ invertible implies f^u in $A[[T_1,\ldots,T_n]]_r$ and u^{-1} in $A[[T]]_r$.

<u>T23</u> (Proposition) Suppose n is an integer and that p does not divide n, that w is a primitive nth root in D, and f in $D[[T]]$ is such that $f^{(n)}(T) = T$, where $f^{(n)}$ denotes the composition of f with itself n times, if, furthermore, $f(T) \equiv wT \pmod{\deg 2}$ then there is a u in $D[[T]]$ so that $f^u(T) = wT$, and where u is invertible over D.

PROOF:

1. We claim that the following implies T23: Given $f_m(T) \equiv wT \pmod{\deg m}$ then there exists $u_m(T) \equiv T+aT^m \pmod{\deg m+1}$ such that $u_m \cdot f_m \cdot u_m^{-1}(T) \equiv wT \pmod{\deg m+1}$ and u_m^{-1} in $D[[T]]$.

Proof:

Put $f_2 = f$, $f_3 = u_2 f u_2^{-1}, \ldots, (u_m u_{m-1} \cdots u_2) f (u_m u_{m-1} \cdots u_2)^{-1}, \ldots$. Then, it is clear that $u_2, u_3 u_2, u_4 u_3 u_2, \ldots$ is a Cauchy sequence since $u_{m-1} \cdots u_2 \equiv u_m u_{m-1} \cdots u_2 \pmod{\deg m}$; hence the sequence converges to a limit, u, in $D[[T]]$ (using the fact that $D[[T]]$ is complete). Now, we establish that this is the required u; for, because the sequence, $u_2, u_3 u_2, \ldots$, is invertible over D then so is its limit; also $ufu^{-1}(T) - u_{k_m} f_{k_m} u_{k_m}^{-1}(T) \equiv 0 \pmod{\deg m+1}$ for all sufficiently large k_m (by definition of u), which implies that $ufu^{-1}(T) \equiv wT \pmod{\deg m+1}$ for each m; hence, $ufu^{-1}(T) = wT$ which means that $f^u(T) = wT$.

2. Proof of the statement in 1.

Case 1 If $m \not\equiv 1 \pmod{n}$; we have $f_m(T) \equiv wT+aT^m \pmod{\deg m+1}$, say, and let us suppose that $u_m(T) = T+bT^m$, then

$f_m^{u_m}(T) \equiv u_m f_m u_m^{-1}(T) \equiv u_m f_m(T+(-b)T^m) \equiv \pmod{\deg m+1}$

$\equiv u_m(wT+w(-b)T^m+aT^m) \equiv$

$\equiv wT+w(-b)T^m+b(wT+w(-b)T^m+aT^m)^m \equiv$

$\equiv wT+(a+b(w^m-w))T^m \pmod{\deg m+1}$.

We claim that w^m-w is a unit in D; clearly $w^m-w \neq 0$, further, w^* is a primitive nth root of unity in k so $w^{*m} \neq w^*$, hence $(w^m-w)^* \neq 0$, which implies the claim. Now, simply define $b = a(w-w^m)^{-1}$ and we have u_m,

the required power series (u_m's inverse is clearly defined over D).

Case 2 $m \equiv 1 \pmod{n}$; we have , therefore, $w^m = w$. If

$f_m(T) \equiv wT+aT^m \pmod{\deg m+1}$ then

$f_m^{(2)}(T) \equiv w(wT+aT^m)+a(wT+aT^m)^m \equiv w^2T+(w+w^m)aT^m \pmod{\deg m+1}$,

$f_m^{(3)}(T) \equiv w(w^2T+(w+w^m)aT^m)+a(w^2T)^m \equiv w^3T+(w^2+w^{m+1}+w^{2m})aT^m \pmod{\deg m+1}$,

$f_m^{(4)}(T) \equiv w(w^3T+(w^2+w^{m+1}+w^{2m})aT^m)+a(w^3T)^m \pmod{\deg m+1}$

$\equiv w^4T+(w^3+w^{m+2}+w^{2m+1}+w^{3m})aT^m \pmod{\deg m+1}$,

and, in general,

$f_m^{(n)}(T) \equiv w^nT+(w^{n-1}+ w^{n+m-2}+\ldots+w^{n+im-(i+1)}+\ldots+w^{(n-1)m}aT^m \pmod{\deg m+1}$

$\equiv T+nw^{-1}aT^m \pmod{\deg m+1}$, since $m \equiv 1 \pmod{n}$.

But, $f_m^{(n)}(T) = (u_{m-1}\ldots u_2)f^{(n)}(u_{m-1}\ldots u_2)^{-1}(T) = T$ since $f^{(n)}(T) = T$, so we must have $a = 0$, and consequently $f_m \equiv wT \pmod{\deg m+1}$. In this case we can choose $u_m(T) = T$ and we get $f_m^{u_m} \equiv wT \pmod{\deg m+1}$.

T24 (Corollary) If w is a primitive (r-1)th root of unity in D, $r = p^s$, and F is a D-group law such that $[w]_F$ in $\mathrm{End}_D(F)$, then there exists G, a D-group law in $D[[x,y]]_r$ such that it is D-isomorphic to F.

PROOF:

Let $[w]_F$ be denoted by f, then by T23 there exists an invertible u in $D[[T]]$ such that $f^u(T) = wT$. Put $G = F^u$. We claim that f^u in $\mathrm{End}_D(G)$, for, clearly f^u in $D[[T]]$ and $f^u \equiv 0 \pmod{\deg 1}$; but, also

$f^u(G(x,y)) = ufu^{-1}(G(x,y)) = uf(F(u^{-1}(x),u^{-1}(y))) = uF(fu^{-1}(x),fu^{-1}(y)) =$

$= uF(u^{-1}ufu^{-1}(x),u^{-1}ufu^{-1}(y)) = G(f^u(x),f^u(y))$.

Furthermore, G(x,y) is in $D[[x,y]]$; for, otherwise, there exists a least $m \not\equiv 1 \pmod{r-1}$ such that G(x,y) has terms of degree m, then we can write $G \equiv G_1+H \pmod{\deg m+1}$, where $G_1(x,y)$ in $D[[x,y]]_r$ and H is

a form of degree m; and so,

$$wG_1(x,y)+wH(x,y) \equiv wG(x,y) \equiv f^u(G(x,y)) \pmod{\deg m+1}$$
$$\equiv G(f^u(x),f^u(y)) \equiv G_1(wx,wy)+H(wx,wy) \pmod{\deg m+1}$$
$$\equiv wG_1(x,y)+w^mH(x,y) \pmod{\deg m+1},$$

which implies that $wH = w^mH$, consequently H is 0.

We conclude this section with two interesting results: one on power series and another dealing with homomorphic group laws.

T25 (Proposition) Suppose K is an algebraically closed field with char K = $p>0$, that f in $K[[T]]_r$ ($r = p^s$) is actually a power series in T^r and that $f(T) \equiv aT^r \pmod{\deg r+1}$, $a \neq 0$, then there exists an invertible u in $K[[T]]_r$ such that $f^u(T) = aT^r$.

PROOF:

1. We claim that if there exists $f_1,\ldots,f_m,\ldots$ such that f_m in $K[[T]]_r$ is a power series in T_r for each m and $f_m(T) \equiv aT^r \pmod{\deg m}$ implies there exists u_m in $K[[T]]_r$ such that $f_{m+1} = u_m f_m u_m^{-1}$ and $u_m(T) \equiv T \pmod{\deg l_m}$ where l_m goes to infinity with m, then the result follows.

Proof:

Consider $f_1 = f, f_2 = u_1 f u_1^{-1},\ldots,f_m = (u_{m-1}\cdots u_1)f(u_{m-1}\cdots u_1)^{-1},\ldots$; we observe that $u_1, u_2u_1,\ldots,(u_m\cdots u_1),\ldots$ is a Cauchy sequence in $K[[T]]$ and since this ring is complete the sequence must have a limit, u, say, which is, in fact, in $K[[T]]_r$ by definition of the u_i's. Now, this u is the one required since $ufu^{-1}(T)-(u_{k_m}\cdots u_1)f(u_{k_m}\cdots u_1)^{-1} \equiv 0 \pmod{\deg l_{k_m}}$ for all sufficiently large l because $u-u_{k_m}\cdots u_1 \equiv 0 \pmod{\deg l_{k_m}}$ for all sufficiently large l; consequently, $ufu^{-1}(T) \equiv aT^r \pmod{\deg l_{k_m}}$ for all

sufficiently large l, which means that $f^{u}(T) = aT^{r}$.

2. We prove the statement in 1. Let $f_m(T) \equiv aT^r+bT^m \pmod{\deg m+1}$; we want $f_{m+1} = u_m f_m u_m^{-1}$ so we must define u_m in such a way that $u_m f_m u_m^{-1} \equiv aT^r \pmod{\deg m+1}$ and $u_m(T) \equiv T \pmod{\deg m}$, u_m in $K[[T]]_r$. If $b = 0$ then we can take u_m to be the identity. For $b \neq 0$ we must have $m \equiv r \pmod{r^2-r}$ since m must be a multiple rn, of r and then n must be $\equiv 1 \pmod{r-1}$; clearly $n>1$, and if we consider any $u_m(T) \equiv T+cT^n \pmod{\deg n+1}$ then

$$f_m^{u_m}(T) = u_m f_m u_m^{-1}(T) \equiv u f_m(T-cT^n) \equiv u(a(T-cT^n)^r+b(T-cT^n)^m) \equiv$$
$$\equiv u(a(T-cT^n)^r+bT^m) \equiv a(T-cT^n)^r+bT^m+c(a(T-cT^n)^r+bT^m)^n \equiv$$
$$\equiv aT^r-ac^rT^{nr}+bT^m+ca^nT^{rn} \pmod{\deg m+1},$$

(using the facts that $(x+y)^r = x^r+y^r \pmod{p}$, $p^s = r$, char K = p),

$$\equiv aT^r+(-ac^r+b+a^nc)T^m \pmod{\deg m+1}.$$

Now, we want this to be $\equiv aT^r \pmod{\deg m+1}$, so we need only choose c satisfying $-ac^r+b+a^nc = 0$ (which is permissible since K is algebraically closed) to obtain the result, $u_m(T)$ being simply $T+cT^n$.

T26 (Corollary) With the hypothesis as in T25, then, there is a v in $K[[T]]_r$ such that $f^{v}(T) = T^r$.

PROOF:

Just put $w(T) = bT$ where b is any (r-1)th root of a, then let $v = w \cdot u$ where u is obtained from T25. Now we get

$$f^v(T) = f^{w\cdot u}(T) = (f^u)^w = (aT)^w = w(a)w^{-1}(T) =$$
$$w(a)(b^{-1}(T))^r = w(ab^{-r}T^r) = bab^{-r}T = aa^{-1}T = T.$$

T27 (Proposition) Let F,G be L-group laws where L is a field with char L = 0, f in $L[[T]]$ satisfy:

$f(F(x,y)) \equiv F(f(x),f(y)) \pmod{\deg n}$,

$f(G(x,y)) \equiv G(f(x),f(y)) \pmod{\deg n}$,

$c(f) \neq 0$, $c(f) \neq$ any root of 1,

then, $F \equiv G \pmod{\deg n}$.

PROOF:

By T10 we can obtain u,v in $L[[T]]$ such that $c(u) = c(v) = 1$ and $F^u(x,y) = x+y$, $G^v(x,y) = x+y$. It follows that both f^u and f^v are linear (mod deg n) since: $f^u(F^u(x,y)) = ufu^{-1}.uF(u^{-1}(x),u^{-1}(y)) =$

$= ufF(u^{-1}(x),u^{-1}(y)) \equiv uF(fu^{-1}(x),fu^{-1}(y)) \pmod{\deg n}$

$\equiv uF(u^{-1}f^u(x),u^{-1}f^u(y)) = F^u(f^u(x),f^u(y)) \pmod{\deg n}$;

hence $f^u(x+y) \equiv f^u(x)+f^u(y) \pmod{\deg n}$, $n \geq 3$, which can happen only if f^u is linear (mod deg n); therefore, $f^u(T) \equiv bT \pmod{\deg n}$ and since $c(u) = c(u^{-1}) = 1$ then b must be a. Similarly we can obtain $f^v(T) \equiv aT \pmod{\deg n}$. Hence, $v.u^{-1}(aT) \equiv v(f(u^{-1}(T))) \equiv \pmod{\deg n}$

$\equiv av.u^{-1}(T) \pmod{\deg n}$.

Now, we claim that any series with first degree coefficient not equal to 0 or a root of 1 commuting with a linear monomial over a field of characteristic zero must itself be linear.

Proof:

Say $g(T) \equiv bT+dT^r \pmod{\deg r+1}$, $r<n$ and that $a.g(T) = g(aT) \pmod{\deg n}$, $a \neq 0$; then,

$abT+adT^r \equiv abT+da^rT^r \pmod{\deg r+1}$, hence , $d(a^r-a) = 0$, which implies that $d = 0$ (since $a^r \neq a$). Consequently, $v.u^{-1}(T) \equiv bT \pmod{\deg n}$; further, it is clear that $b = 1$ according to the definitions of u and v.

Finally, we observe that $F(x,y) = u(u^{-1}(x)+u^{-1}(y)) \equiv$

$$\equiv v(v^{-1}(x)+v^{-1}(y)) = G(x,y) \pmod{\deg n},$$

(since $u \equiv v \pmod{\deg n}$).

V A Construction of D-Group Laws

D16 Suppose we have a complete discrete valuation ring, D, with prime element, d, such that p = (D:d(D)) is the number of elements in the residue class field, and Q(D) is the quotient field, which is, hence, complete with respect to the valuation (that is, the situation of D10) then we denote by D_d the subset$\subset D[[T]]$ consisting of all f's such that $f(T) \equiv dT \pmod{\text{deg } 2}$ and $f(T) \equiv T^p \pmod{d}$.

In order to carry out the intended construction we must consider a preliminary result concerning power series.

T28 (Lemma) Let f,g in D_d and say $l(X_1,\ldots,X_n) = \sum_{i=1}^{n} a_i X_i$ is a linear form over D, then there exists h in $D[[X_1,\ldots,X_n]]$ such that

$h(X_1,\ldots,X_n) \equiv l(X_1,\ldots,X_n) \pmod{\text{deg } 2}$ and

$f(h(X_1,\ldots,X_n)) = h(g(X_1),\ldots,g(X_n))$.

PROOF:

To make the notation less burdensome put $X = (X_1,\ldots,X_n)$ and $g(X) = (g(X_1),\ldots,g(X_n))$.

1. We claim that the congruences $h_r(X) \equiv l(X) \pmod{\text{deg } 2}$ and $f(h_r(X)) \equiv h_r(g(X)) \pmod{\text{deg } r+1}$ have a unique (mod deg r+1) solution $h_r(X)$ in $D[[X_1,\ldots,X_n]]$.

Case r =1: Simply take $h_1(X) = l(X)$.

Case r≥1: We assume the result for any r≥1.

Case r+1: We must exhibit a solution h_{r+1} to the system -

$h_{r+1}(X) \equiv l(X) \pmod{\text{deg } 2}$,

$f(h_{r+1}(X)) \equiv h_{r+1}(g(X)) \pmod{\text{deg } r+2}$.

Let us write $h_{r+1} = h_r + dif_r$ for some dif_r in $D[[X_1,\ldots,X_n]]$; then,

$f(h_r(X)+dif_r(X)) \equiv (h_r(X)+dif_r(X))(g(X)) \pmod{\deg r+2}$,

hence, $f(h_r(X))+f(dif_r(X))+h_r(X)dif_r(X)(\ldots) \equiv$

$\equiv h_r(g(X))+dif_r(g(X)) \pmod{\deg r+1}$,

therefore, $f(dif_r(X))+h_r(X)dif_r(X)(\ldots) \equiv dif_r(g(X)) \pmod{\deg r+1}$, (using the induction hypothesis). But, the last congruence can be satisfied only if $dif_r(X) \equiv 0 \pmod{\deg r+1}$; because, if $a \not\equiv 0$ is a coefficient of a term of lowest degree, $t \leq r$, appearing in $dif_r(X)$ then we must have $da = d^t a$, so that t must be 1 (since d is prime), which implies that $dif_r(X)$ has a linear term, in contradiction to the required congruence: $1(X) \equiv h_r(X) \equiv h_{r+1}(X) \pmod{\deg 2}$. It follows necessarily that $h_{r+1} = h_r + dif_r$ where $dif_r \equiv 0 \pmod{\deg r+1}$. Consequently, $f(h_{r+1}(X)) \equiv f(h_r(X)+d(dif_r(X)) \pmod{\deg r+2}$, and $h_{r+1}(g(X)) \equiv h_r(g(X))+d^{r+1}(dif_r(X)) \pmod{\deg r+2}$ require that we take $dif_r(X) = \dfrac{f(h_r(X))-h_r(g(X))}{d^{r+1}-d} \pmod{\deg r+2}$.

It is clear that the coefficients of $dif_r(X)$ (and hence $h_{r+1}(X)$) are in D since $f(h_r(X))-h_r(g(X)) \equiv (h_r(X))^p-h_r(X^p) \equiv 0 \pmod{d}$, using the fact that d divides p; so that d does, in fact, divide the numerator of $dif_r(X)$.

2. To complete the demonstration of existence it sufficies to remark that $D[[X_1,\ldots,X_n]]$ is complete, so that the limit of the Cauchy sequence, $h_1(X), h_2(X), \ldots$, exists in $D[[X_1,\ldots,X_n]]$; if we call this limit $h(X)$, clearly $h(X) \equiv 1(X) \pmod{\deg 2}$ and $f(h(X)) = h(g(X))$.

3. The uniqueness of h(X) follows from the form of the existence

proof 1. and 2. which indicates that the sequence, $h_1, h_2, \ldots,$ is uniquely determined and, hence, determines (uniquely) h since we are dealing with a Hausdorff topology.

We are now in a position to make the following definition.

D17 Given f in D_d denote by $F_f(X,Y)$ the unique solution of:
$F_f(X,Y) \equiv X+Y \pmod{\deg 2}$ and $f(F_f(X,Y)) = F_f(f(X),f(Y))$.
Given a in D and f,g in D_d denote by $[a]_{f,g}(T)$ the unique solution of:
$[a]_{f,g}(T) \equiv aT \pmod{\deg 2}$ and $f([a]_{f,g}(T)) = [a]_{f,g}(g(T))$.

T29 (Theorem) Let f,g,h in D_d and a,b in D then we have:

1. $F_f(X,Y) = F_f(Y,X)$
2. $F_f(F_f(X,Y),Z) = F_f(X,F_f(Y,Z))$
3. $F_f([a]_{f,g}(X),[a]_{f,g}(Y)) = [a]_{f,g}(F_g(X,Y))$
4. $[a]_{f,g}([b]_{g,h}(T)) = [ab]_{f,h}(T)$
5. $[a+b]_{f,g}(T) = F_f([a]_{f,g}(T),[b]_{f,g}(T))$
6. $[d]_{f,f}(T) = f(T), \quad [1]_{f,f}(T) = T.$

PROOF:

The method of proof is the same in each case; we simply demonstrate that the LHS, RHS are both solutions to a problem of the type found in T28, and since we know there is exactly one such solution, the LHS and RHS must be the same. Corresponding to each equation is listed the problem to which it belongs, and then the verifications are carried out.

1/ a/ $G(X,Y) \equiv X+Y \pmod{\deg 2}$

b/ $f(G(X,Y)) = G(f(X),f(Y))$.

By definition, $F_f(X,Y)$ is a solution to this problem and also,

a/ $F_f(Y,X) \equiv Y+X = X+Y \pmod{\deg 2}$

b/ LHS = $f(F_f(Y,X)) = F_f(f(Y),f(X)) = RHS$

which show that $F_f(Y,X)$ is a solution to 1/.

2/ a/ $G(X,Y,Z) \equiv X+Y+Z \pmod{\deg 2}$

b/ $f(G(X,Y,Z)) = G(f(X),f(Y),f(Z))$.

a/ $F_f(F_f(X,Y),Z) \equiv F_f(X+Y,Z) \equiv (X+Y)+Z \pmod{\deg 2}$

b/ LHS = $f(F_f(F_f(X,Y,),Z)) = F_f(fF_f(X,Y),f(Z))$

$= F_f(F_f(f(X),f(Y)),f(Z)) = RHS;$

hence, the LHS of 2. is a solution for 2/.

a/ $F_f(X ,F_f(Y,Z)) \equiv F_f(X,Y+Z) \equiv X+(Y+Z) \pmod{\deg 2}$

b/ LHS = $f(F_f(X,F_f(Y,Z))) = F_f(f(X),f(F_f(Y,Z)))$

$= F_f(f(X),F_f(f(Y),f(Z))) = RHS;$

so, the RHS of 2. is a solution for 2/.

3/ a/ $G(X,Y) \equiv aX+aY \pmod{\deg 2}$

b/ $f(G(X,Y)) = G(g(X),g(Y))$.

a/ $F_f([a]_{f,g}(X),[a]_{f,g}(Y)) \equiv [a]_{f,g}(X)+[a]_{f,g}(Y) \equiv aX+aY \pmod{\deg 2}$

b/ LHS = $f(F_f([a]_{f,g}(X),[a]_{f,g}(Y))) = F_f(f([a]_{f,g}(X)),f([a]_{f,g}(Y)))$

$= F_f([a]_{f,g}(g(X),[a]_{f,g}(g(X)))) = RHS;$

so, LHS of 3. is a solution of 3/.

a/ $[a]_{f,g}(f_g(X,Y)) \equiv aF_g(X,Y) \equiv a(X+Y) \pmod{\deg 2}$

b/ LHS = $f([a]_{f,g}(F_g(X,Y)) = [a]_{f,g}(g(F_g(X,Y)))$

$= [a]_{f,g}(F_g(g(X),g(Y))) = RHS$

which mean that RHS of 3. is solution to 3/.

4/ a/ $G(T) \equiv (ab)T \pmod{\deg 2}$

b/ $f(G(T)) = G(h(T))$.

a/ $[a]_{f,g}([b]_{g,h}(T)) \equiv a([b]_{g,h}(T)) \equiv a(bT) \pmod{\deg 2}$

b/ LHS $= f([a]_{f,g}([b]_{g,h}(T))) = [a]_{f,g}(g([b]_{g,h}(T)))$

$= [a]_{f,g}([b]_{g,h}(h(T))) =$ RHS;

that is, LHS of 4. solves 4/.

a/ $[ab]_{f,h}(T) \equiv (ab)T \pmod{\deg 2}$

b/ LHS $= f([ab]_{f,h}(T)) = [ab]_{f,h}(h(T)) =$ RHS;

showing that RHS of 4. solves 4/.

5/ a/ $G(T) \equiv (a+b)T \pmod{\deg 2}$

b/ $f(G(T)) = G(g(T))$.

a/ $[a+b]_{f,g}(T) \equiv (a+b)T \pmod{\deg 2}$

b/ LHS $= f([a+b]_{f,g}(T)) = [a+b]_{f,g}(g(T))=$RHS;

therefore, LHS of 5. is a solution to 5/.

a/ $F_f([a]_{f,g}(T),[b]_{f,g}(T)) \equiv [a]_{f,g}(T)+[b]_{f,g}(T) \equiv a+b \pmod{\deg 2}$

b/ LHS $= f(F_f([a]_{f,g}(T),[b]_{f,g}(T))) = F_f(f([a]_{f,g}(T)),f([b]_{f,g}(T)))$

$= F_f([a]_{f,g}(g(T)),[b]_{f,g}(g(T))) =$ RHS;

so, RHS of 5. is a solution to 5/.

6/ a/ $G(T) = dT$ and b/ $f(G(T)) = G(f(T))$; a/ $G(T) = T$ and b/ $f(G(T)) = G(f(T))$.

Here, the verifications are completely trivial.

T30 (Corollary) 1. F_f is an abelian group law.

2. The map $A \longrightarrow End_A(F_f)$ given by $a \longrightarrow [a]_{f,f}$ is an injective ring homomorphism.

3. The isomorphism class for F_f depends only on d and not on f in D_d.

4. A group law, G, over D is in the isomorphism class of F_f if and only if there exists g in $End_D(G)$ with $g^* = $ Frobenius and $f'(0) = d$ (where Frobenius$(T) = T^p$).

PROOF:

1. The fact that F_f is a group law follows from T29 2., and it is necessarily abelian by T29 1.

2. The given map preserves multiplication by T29 4., addition by T29 5. (putting f = g in these equations) and hence is a ring homomorphism; it is injective because $[a]_{f,f} = 0$ implies $aT \equiv 0 \pmod{\deg 2}$ which implies that $a = 0$.

3. This is demonstrated by observing that we have a canonical isomorphism between F_f and F_g given by $[1]_{f,g}$:
First, 3. of T29 shows that $[a]_{f,g}$ in $Hom_D(F_f,F_g)$ so that $[1]_{f,g}$ in $Hom_D(F_f,F_g)$; similarly $[1]_{g,f}$ in $Hom_D(F_g,F_f)$; and clearly $[1]_{f,g}[1]_{g,f} = [1] = [1]_{g,f}\cdot[1]_{f,g}$; which means that $[1]_{f,g}$ is an isomorphism between F_fF_g. Hence, once we choose a prime, d, in D, then, given any f,g in D_d, we immediately obtain an isomorphism between F_f and F_g.

4. If G is isomorphic to F_f via u(T) then we observe that $u^{-1}fu$ is the required g (it satisfies the required properties, which are direct translations of D16, because f does).

Conversely, if there exists a g with the given properties then G is, in fact, one of the F_h's by the uniqueness in T28; in particular it is F_g, and we know by 3. that F_g is isomorphic to F_f.

D18 Let K be an algebraic extension of Q(D), then we denote the maximal ideal in the ring of integers in K by M(K).

T31 (Corollary) M(K) has a D-module structure which depends on any given f in D_d.

PROOF:

Consider $x_1, x_2, \ldots$ in M(K) and a formal power series, G, in $D[[X_1, \ldots, X_n]]$ with 0 constant term, if we substitute x_i for X_i we get an infinite series which converges with respect to the given valuation since the value of terms increases steadily as the series progresses (see, for example, E. Weiss for a proof in one variable, reference no. 19, p. 35-36). We apply this result as follows. Define $x+y = F_f(x,y)$, and $ax = [a]_{f,f}(x)$; the series on the RHSs converge to some unique elements in M(K), so that the operations are well-defined.

To check the rules required for a module it is sufficient to observe that replacing the indeterminates by elements does not change the equalities in T29, so we have:

a/ T29 1. and 2. gives commutativity and associativity

b/ the zero element is obviously the zero power series

c/ additive inverses are obtained through the analogue to T2

d/ the remaining module properties are obtained by T29 3.,4.,5.,6.

D19 The D-module obtained from M(K) by way of T31 is written $M_f(K)$.

T32 (Proposition) 1. $Q(D) \subset K_1 \subset K$ implies $M_f(K_1) \subset M_f(K)$, for algebraic extensions of Q(D).

2. If further, $K|K_1$ is an algebraic extension of fields with a K_1-fixing automorphism, g, then g induces an automorphism of $M_f(K)$.

PROOF:

1. We simply observe that an element in K_1 with positive value has positive extended value.

2. It is clear that g, being an automorphism of K, is a continuous function on Q(D) (under the valuation topology). We must show that g restricted to $M_f(K)$ is a module homomorphism: but, since the operation,+, and the action, juxtaposition, are defined using convergent series with coefficients in D, and, hence, left fixed, and because g is continuous means we have $g(\sum a_{ij}x^iy^j) = \sum g(a_{ij}x^iy^j)$ for convergent series; then it follows that $g(F_f(x,y)) = F_f(g(x),g(y))$ and $g([a]_{f,f})(x) = [a]_{f,f}(g(x))$.

Of course, it is clear that the image of g restricted to $M_f(K)$ is exactly $M_f(K)$ because, given any algebraic extension of fields, $K|Q(D),Q(D)$ complete with respect to the given valuation then the extended value of the image (under a Q(D)-fixing automorphism of K) of an element is exactly the extended value of the element (see, for example, E. Weiss, reference no. 19, Corollary 2.2.12 p.51).

VI The Reciprocity Law

D20 We denote by $Q(D)_s$, a fixed separable algebraic closure of $Q(D)$ in an algebraic closure, $\overline{Q(D)}$.

D21 Given f in D_d and an integer $m \geq 1$, $V_{f,m}$ stands for the D-submodule of $M_f(Q(D)_s)$ consisting of elements, v, such that $d^m v = 0$.

T33 It is clear that if f,g are in D_d, then we have: v in $V_{f,m}$ if and only if $[1]_{g,f}(v)$ in $V_{g,m}$.

PROOF:

If v is in $V_{f,m}$ then $d^m v = 0$ where v is in $M(Q(D)_s)$ and so $[1]_{g,f}(v)$ is in $M(Q(D)_s)$; furthermore, $[1]_{g,f}$ has a factor ,v, so that $d^m([1]_{g,f}(v))$ has a factor $d^m v$, which means it is 0.

If $[1]_{g,f}(v)$ is in $V_{g,m}$ then $d^m[1]_{g,f}(v) = 0$, i.e. $[d^m]_{g,f}(v) = 0$; hence, $[1]_{f,g}[d^m]_{g,f}(v) = 0$ so that $d^m v = 0$; furthermore, $[1]_{f,g}[1]_{g,f}(v) = v$ is in $M(Q(D)_s)$. This means that v is in $V_{f,m}$.

We observe that $Q(D)(V_{f,m}) \mid Q(D)$ is clearly separable and is also normal (since v in $V_{f,m}$ implies that $d^m v = 0$ implies that $d^m \bar{v} = 0$ implies that $\bar{v}$ is in $V_{f,m}$, so that the conjugate of every element in $V_{f,m}$ is in $V_{f,m}$) and hence Galois.

D22 According to T33 the field extension $Q(D)(V_{f,m}) \mid (Q(D))$ depends only on d, not on f in D_d so we can denote it by $L_{d,m} \mid Q(D)$ and write its Galois group, $\mathrm{Gal}\,(Q(D)(V_{f,m}) \mid Q(D))$, as $\mathrm{Gal}_{d,m}$. Furthermore, we put $V_f = \bigcup_{m=1}^{\infty} V_{f,m}$, $L_d = Q(D)(V_f)$ and let $\mathrm{proj\ lim}\ \mathrm{Gal}_{d,m}$ denote the projective limit of the $\mathrm{Gal}_{d,m}$.

T34 (Theorem) Given any prime, d, in D, f in F_d then the following statements are valid:

1. $M_f(Q(D)_s)$ is a divisible D-module

2. $V_{f,m}$ and D/d^mD are isomorphic D-modules for every integer $m \geq 1$

3. V_f and $Q(D)/D$ are isomorphic D-modules

4. If t is in proj lim $Gal_{d,m}$ then there exists a unique unit, u, in D satisfying $tv = [u]_{f,f}(v)$ for each v in V_f

5. We have an isomorphism from proj lim $Gal_{d,m}$ onto the group of units

6. d is a norm for the extension $Q(D)(V_{f,m}) \mid Q(D)$ for each $m \geq 1$,

PROOF:

For the first three parts we can assume that the f with which we are dealing has the basic form T^p+dT; this is because there exists a standard isomorphism $[1]_{f,g}$ between the modules $M_f(Q(D)_s)$ and $M_g(Q(D)_s)$ and since the isomorphic image of a divisible module is again divisible.

1. We must show that $ax = b$ is solvable for x in $M_f(Q(D)_s)$, given any a in D and b in $M_f(Q(D)_s)$. Since d is a prime for D we need only consider solving $dT = b$, i.e. $T^p+dT = b$; but, the polynomial T^p+dT-b has all its roots in $\overline{Q(D)}$ because $\overline{Q(D)}$ is algebraically closed, and, in fact, they must be in $M(\overline{Q(D)})$, for, otherwise the value of b would be negative contradicting the fact that b is in $M(Q(D)_s)$. Furthermore, the roots are distinct because $f'(T) = pT^{p-1}+d = d$, which clearly has no roots in $M(\overline{Q(D)})$; this means that the roots of $f(T) = b$ are separable over Q(D) and so are in $Q(D)_s$, this being the fixed separable closure. Consequently we have that the roots of $f(T) = b$ are in $M(Q(D)_s)$, i.e. $M_f(Q(D)_s)$ is

divisible.

We observe that $V_{f,1}$ consists of the roots of the equation $f(T) = T^p+dT = 0$ and so has exactly p elements and is, consequently, one-dimensional as a vector space over the residue class field, D/dD (for, any r in $V_{f,1}$ is a basis of $V_{f,1}$ over D/dD because a'r = ar implies (a'-a).r = 0 for a',a in D/dD which implies r = 0 since d does not divide a'-a (meaning that this is a unit in D/dD)).

2. We have that for each m $V_{f,m}$ is a torsion D-module which is surely finitely generated since it is finite and by the structure theorem for finitely generated torsion modules (over principal ideal domains) it is the direct sum of $D/d^{n_1}D, D/d^{n_2}D, \ldots, D/d^{n_r}D$ (e.g. see Lang p.390, reference no. 10); but we know that here $d: V_{f,m} \longrightarrow V_{f,m}$ has kernel $V_{f,1}$, which is a one-dimensional vector space over D/dD so we must have r = 1 (otherwise ker d would not be one-dimensional). Hence, $V_{f,m}$ and D/d^nD are isomorphic as D-modules; then $d^m(1+d^nD) = 0$ implies that $d^m+d^nD = 0$ implies that $m \geq n$; on the other hand we have $d^{m-1}(a+d^nD) \neq 0$ for some $a+d^nD$ since $V_{f,m} \neq 0$ i.e. $d^{m-1}a$ is not in d^nD which implies that $n \geq m-1$; consequently $m \geq n \geq m-1$ so n = m and we have the desired isomorphism between $V_{f,m}$ and D/d^mD.

3. To establish the isomorphism we observe that a divisible torsion module over a discrete valuation ring, D, has the form $\bigoplus_{c_1} Q(D) \bigoplus_{c_2} (Q(D)/D)$ where c_1, c_2 are certain cardinals, and in our case this takes the form $M_f(Q(D)_f) = \bigoplus_{c_1} Q(D) \bigoplus_{c_2} (Q(D)/D)$. But, the torsion part of this module is exactly $V_f = \bigoplus_{c_2} (Q(D)/D)$; further, since ker d,

$d: V_f \longrightarrow V_f$ is one-dimensional over D/dD then $c_2 = 1$, otherwise ker d would not be one-dimensional.

4. Using T32 we can see that each t in proj lim $\mathrm{Gal}_{d,m}$ induces an automorphism of V_f, the union of all $V_{f,m}$'s. But, for $V_f \approx Q(D)/D$ as modules over a complete valuation ring, D, the only automorphisms are of the form $v \longrightarrow uv$ where u is a unit of D; this establishes the existence of the unique unit.

5. To show that the map $t \longrightarrow u$ is a homomorphism we need only observe that:

$t_1+t_2 \longrightarrow$ the unique u such that $(t_1+t_2)(v) = [u]_{f,f}(v)$, and

$$(t_1+t_2)(v) = t_1(v)+t_2(v) = [u_1]_{f,f}(v)+[u_2]_{f,f}(v) = ([u_1]_{f,f}+[u_2]_{f,f})(v)$$
$$= [u_1+u_2]_{f,f}(v);$$

consequently, $t_1+t_2 \longrightarrow u_1+u_2$, where $t_1 \longrightarrow u_1$ and $t_2 \longrightarrow u_2$.

The map is injective because for any u in U, the units of D, $u \equiv 1 \pmod{d^m D}$, i.e. multiplication by a unit is the identity on $D/d^m D \approx V_{f,m}$ if and only if t is the identity on $Q(D)(V_{f,m})$ for each m. Since u = 1 satisfies the former condition the injectivity of the map follows. As a further consequence of the latter equivalence we have the induced injection: $\mathrm{Gal}_{d,m} \longrightarrow U/(1+d^m D)$.

Surjectivity is obtained as follows: First, we show that the order of $\mathrm{Gal}_{d,m}$ is p^m-p^{m-1}; for, $Q(D)(V_{f,m})$ contains the roots of the polynomial $f^m(X) = f(f(\ldots(f(X))\ldots)) = X^{p^m}+\ldots+d^m X$; hence, it contains the roots of $f^m(X)/f^{m-1}(X) = \dfrac{f(f^{m-1}(X))}{f^{m-1}(X)} = (f^{m-1}(X))^{p-1}+d$, which clearly has degree p^m-p^{m-1}; further, a simple application of Eisenstein's criterion

shows that the polynomial is irreducible over $Q(D)$ so that p^m-p^{m-1} is the degree of the field extension $Q(D)(V_{f,m})|Q(D)$; hence, the order of its Galois group, $Gal_{d,m}$, equals this number. Next, we observe that $U/(1+d^mD)$ has order p^m-p^{m-1} (see, for example, Weiss p. 19, reference no. 19). These two facts demonstrate surjectivity.

Taking the projective limit of both sides of the isomorphism between $Gal_{d,m}$ and $U/(1+d^mD)$ yields the required isomorphism between proj lim $Gal_{d,m}$ and U, since both groups are compact.

6. Since v in $V_{f,m}$ is a root of the Eisenstein polynomial $(f^{m-1}(X))^{p-1}+d$ then, clearly, $Q(D)(V_{f,m}) = Q(D)(v)$ so d is the norm of an element in the extension $Q(D)(V_{f,m})|Q(D)$.

D23 We let the maximal unramified extension of $Q(D)$ be represented by T and denote the Frobenius automorphism of T over $Q(D)$ by $Frob(T|Q(D))$.

L_d is totally ramified over $Q(D)$ and since T is unramified then $L_d \cap T = Q(D)$. Now, because one of $L_d|Q(D)$ and $T|Q(D)$ is Galois (in fact, both are) and $L_d \cap T = Q(D)$ it follows that L_d is linearly disjoint from T. Hence, we have $Gal(L_dT|Q(D)) = Gal(L_d|Q(D))Gal(T|Q(D))$, and this together with the facts that $Gal(L_d|Q(D))\ Gal(T|Q(D)) = 1$ and that both these subgroups are normal in $Gal(L_dT|Q(D))$ enables us to deduce that:

$$Gal(L_dT|Q(D)) = Gal(L_d|Q(D)) \times Gal(T|Q(D)).$$

We can now make the following definition.

D24 Put $r_d: Q(D)^* \longrightarrow Gal(L_dT|Q(D))$, for each prime, d, in D, defined as that homomorphism such that:

1. For each u in U, $r_d(u)$ is the identity on T, and on L_d is the inverse of t (t being the element corresponding to u under the map established by T34 part 5).

2. On L_d $r_d(d)$ is the identity, while on T it is precisely $\mathrm{Frob}(T|Q(D))$.

So, if $a = ud^m$ is an arbitrary element of $Q(D)^*$ then

$r_d(a) = (\mathrm{Frob}(T|Q(D)))^m$ on T, and

$r_d(u)(v) = \left[u^{-1}\right]_{f,f}(v)$ for all v in V_f.

T35 (Lemma) If the ring of integers of T is denoted B and we write $\underline{B}$ for the completion of B, then there exists, u in U and any f in F_d, g in F_w, $w = ud$, a power series over $\underline{B}$, $H(X) \equiv eX \pmod{\deg 2}$ where e is some unit satisfying:

1. $\mathrm{Frob}(T|Q(D))(H(X)) = H(\left[u\right]_{f,f}(X))$
2. $H(F_f(X,Y)) = F_g(H(X),H(Y))$
3. $H(\left[a\right]_{f,f}(X)) = \left[a\right]_{g,g}(H(X))$, for all a in D.

PROOF:

Essential to the proof is the well-known result that the endomorphism, $\mathrm{Frob}(T|Q(D))-1$, is onto the additive group of $\underline{B}$ and onto the multiplicative group of units in $\underline{B}$ (according to Serre p.209 reference no. 18).

First, we find a series H(X) satisfying 1. Say a is a unit in $\underline{B}$ satisfying $\mathrm{Frob}(T|Q(D))(e) = eu$ (one such certainly exists by the opening remark), then for $H_1(X) = \left[e\right]_{f,f}(X)$ we have

$$\mathrm{Frob}(T|Q(D))(H_1(X)) = \left[\mathrm{Frob}(T|Q(D))(e)\right]_{f,f}(X) = \left[eu\right]_{f,f}(X)$$
$$= \left[e\right]_{f,f}(\left[u\right]_{f,f}(X)) = H_1(\left[u\right]_{f,f}(X)).$$

Now, let us assume that we have

$$\mathrm{Frob}(T|Q(D))H_r(X) \equiv H_r([u]_{f,f}(X)) \quad (\text{mod deg } r+1),$$

proceeding by induction we must find b in $\underline{B}$ so that $H_{r+1}(X)$, defined by $H_r(X)+bX^{r+1}$, satisfies:

$$\mathrm{Frob}(T|Q(D))(H_{r+1}(X)) \equiv H_{r+1}([u]_{f,f}(X)) \quad (\text{mod deg } r+2).$$

If we put $b = ae^{r+1}$ then a must satisfy:

$$\begin{aligned}\mathrm{Frob}(T|Q(D))(H_{r+1}(X)) &= \mathrm{Frob}(T|Q(D))(H_r(X)+bX^{r+1}) \\ &= \mathrm{Frob}(T|Q(D))(H_r(X))+\mathrm{Frob}(T|Q(D))(bX^{r+1}) \\ &= \mathrm{Frob}(T|Q(D))(H_r(X))+\mathrm{Frob}(T|Q(D))(b)X^{r+1}\end{aligned}$$

and this must be

$$\begin{aligned}&\equiv H_{r+1}([u]_{f,f}(X)) \quad (\text{mod deg } r+2) \\ &\equiv H_r([u]_{f,f}(X))+b([u]_{f,f}(X))^{r+1} \quad (\text{mod deg } r+2).\end{aligned}$$

Hence, $\mathrm{Frob}(T|Q(D))(H_r(X))-H_r([u]_{f,f}(X)) \equiv$

$b([u]_{f,f}(X))^{r+1}-\mathrm{Frob}(T|Q(D))(b)X^{r+1}$ (mod deg r+2); so that $c = a(ue)^{r+1}-\mathrm{Frob}(T|Q(D))(a)\mathrm{Frob}(T|Q(D))(e^{r+1})$, where c is the coefficient of X^{r+1} on LHS of the last congruence. That is,

$$c/(\mathrm{Frob}(T|Q(D))(e))^{r+1} = a-\mathrm{Frob}(T|Q(D))(a).$$

But, we know that $\mathrm{Frob}(T|Q(D))-1$ is surjective on the additive group of $\underline{B}$ so it is possible to choose a in this fashion, and, hence to determine $b = ae^{r+1}$ as required. This allows us to define $H = \lim H_r$, and this H is the required series satisfying 1.

Now, (simplifying the notation for Frobenius in the obvious way, by omitting $(T|Q(D))$) observe that $h = \mathrm{Frob}(H)fH^{-1} = H[u]_{f,f}fH^{-1} =$

$$\begin{aligned}&= Hf[u]_{f,f}H^{-1} = H[d]_{f,f}[u]_{f,f}H^{-1} = \\ &= H[du]_{f,f}H^{-1} = H[w]_{f,f}H^{-1},\end{aligned}$$

and that the coefficients of h are in D since, they are clearly in $\underline{B}$,

and $\quad \mathrm{Frob}(h) = \mathrm{Frob}(H[w]_{f,f}H^{-1}) = \mathrm{Frob}(H)\mathrm{Frob}([w]_{f,f})\mathrm{Frob}(H^{-1})$

$= \mathrm{Frob}(H)f[u]_{f,f}\mathrm{Frob}(H^{-1}) = \mathrm{Frob}(H)fH^{-1} = h$

(because from 1. we have $\mathrm{Frob}(H)(\mathrm{Frob}H^{-1}) = H([u]_{f,f}\mathrm{Frob}(H^{-1}))$ so $H^{-1} = [u]_{f,f}(\mathrm{Frob}(H^{-1})))$, meaning that the coefficients must also be in $Q(D)$.

We can also say that h is in F_w since

$h(X) \equiv ewe^{-1}X \equiv wX \pmod{\deg 2}$ and,

$h(X) \equiv \mathrm{Frob}(H)(f(H^{-1}(X))) \equiv \mathrm{Frob}(H)((H^{-1}(X))^p) \pmod{d}$

$\equiv \mathrm{Frob}(H)(\mathrm{Frob}(H^{-1})(X^p)) \equiv X^p \pmod{d}$

by definition of the Frobenius. Furthermore, we can replace H by $[1]_{g,h}(H)$ in the above and 1. remains valid, but, now we have $g = \mathrm{Frob}HfH^{-1}$ $= H[w]_{f,f}H^{-1}$.

To verify 2. we need only show that $F(X,Y) = H(F_f(H^{-1}(X),H^{-1}(Y)))$ satisfies the defining properties of $F_g(X,Y)$. Clearly,

$F \equiv X+Y \pmod{\deg 2}$, and also,

$$H(F_f(H^{-1}((g(X)),H^{-1}(g(Y))) = H(F_f([w]_{f,f}H^{-1}(X),[w]_{f,f}H^{-1}(Y))) =$$
$$= H[w]_{f,f}(F_f(H^{-1}(X),H^{-1}(Y))) =$$
$$= gH(F_f(H^{-1}(X),H^{-1}(Y)))$$

Furthermore, F is defined over D since, the proof of T28 shows that the F satisfying the two defining conditions must, in fact, be defined over D.

In a similar fashion we have $H^{-1}[a]_{g,g}(H(X)) = [a]_{f,f}(X)$. For, clearly $H[a]_{f,f}(H^{-1}(X)) \equiv aX \pmod{\deg 2}$ and also,

$$g(H[a]_{f,f}H^{-1}(X)) = (H[w]_{f,f}H^{-1})(H[a]_{f,f}H^{-1}(X)) =$$
$$= H[w]_{f,f}[a]_{f,f}H^{-1}(X) =$$

$$= H[a]_{f,f}[w]_{f,f}H^{-1}(X) =$$
$$= H[a]_{f,f}H^{-1}(H[w]_{f,f}H^{-1}(X)) =$$
$$= H[a]_{f,f}H^{-1}(g(X)).$$

This shows that 3. is valid, and, consequently, the proof is complete.

T36 (Theorem) The field, L_dT, and the homomorphism, r_d, are the same no matter what prime, d, is chosen.

PROOF:

Given a separable algebraic extension, K, of Q(D), contained in $Q(D)_s$ we again denote by $\underline{K}$ a completion of K, which is contained in the fixed completion, $\underline{Q(D)_s}$, of $Q(D)_s$. For a Galois extension, $K|Q(D)$, the automorphisms of K over Q(D) have unique extensions to $\underline{K}$ over Q(D) because they are continuous and $\underline{K}$ is complete; so we can proceed as follows. If d and $w = ud$ (for u in U) are any two primes$\in$D, which give rise to the two series, f in F_d, $g \in F_w$, then we must show that 1/ $L_dT = L_wT$ and 2/ $r_d = r_w$.

1/ T35 2. shows that H is in $\mathrm{Hom}_{\underline{B}}(F_f, F_g)$, and H is, in fact, an isomorphism because $H'(0) = e$ is a unit so that $H^{-1}(X)$ is well-defined over $\underline{B}$. This fact and T35 3. allow us to deduce that the map $v \longrightarrow H(v)$ is an isomorphism of the torsion submodule, V_f, of $M_f(\underline{Q(D)_s})$ onto that of $M_g(\underline{Q(D)_s})$, denoted by V_g. Consequently,

$$V_g = H(V_f) \subset \underline{T(V_f)} = \underline{TL_d}, \text{ and}$$
$$V_f = H^{-1}(V_g) \subset \underline{T(V_g)} = \underline{TL_w}.$$

These two sequences imply that $\underline{TL_w}$ is contained in and contains $\underline{TL_d}$, so equality is established. Now, we simply observe that $TL_d = TL_w$ since both equal the unique separable algebraic closure of Q(D) in $\underline{TL_d}$.

2/ To show that $r_d = r_w$ we need only prove that $r_w(w) = r_d(w)$ since this implies that all homomorphisms, r_d, coincide on the prime, w, so they must be equal on $Q(D)^*$ (which is generated as a group by such primes, w). On T, $r_d(w)$ and $r_w(w)$ are both equal to $\text{Frob}(T|Q(D))$ so it remains to show that the automorphisms have the same effect on L_w. However, $r_w(w)$ is the identity on $L_w = Q(D)(V_g)$ and since L_w is generated by all H(v) for v in V_f we need only verify that $r_d(w)(H(v)) = H(v)$, for all v in V_f. But, $r_d(w) = r_d(u)r_d(d)$, where $r_d(d)$ is $\text{Frob}(\underline{T}|Q(D))$ on $\underline{T}$ and takes v onto v in V_f, while $r_d(u)$ is trivial on $\underline{T}$ and takes v onto $[u^{-1}]_{f,f}(v)$, v in V_f. Now, H has coefficients in $\underline{T}$ so we can say that

$$\begin{aligned} r_d(w)(H(v)) &= (r_d(d)r_d(u))(H(v)) = \\ &= r_d(d)H(r_d(u)(v)) = \\ &= r_d(u)H([u^{-1}]_{f,f}(v)) \end{aligned}$$

and this is, by 1. of T35 $= H([u]_{f,f}([u^{-1}]_{f,f}(v))) = H(v)$.

T37 (Corollary) 1. The reciprocity law homomorphism for $L_dT|Q(D)$ is r_d, i.e. $r_d(a) = (a, L_dT|Q(D))$, for a in $Q(D)^*$.

2. L_dT is, in fact, the maximal abelian extension of Q(D).

PROOF:

1. To show that r_d is the reciprocity law homomorphism, s, we must demonstrate that $s(a) = (a, L_dT|Q(D))$ satisfies: $s(d) = r_d(d) = r(d)$ where $r = r_d$ for all d by T36, because the primes, d, generate $Q(D)^*$. We observe that s(d) is the identity on L_d since d is a norm from $L_{d,m}$ for each m (according to T34 6.) and s(d) is $\text{Frob}(T|Q(D))$

so the equality is proved.

2. $L_dT|Q(D)$ is a maximal abelian extension since L_dT contains T, the maximal, unramified extension of $Q(D)$ and r_d restricted to U is injective (because u in U and $r_d(u) = 1$ on L_d and hence on $L_{d,m}$ for each m, then $u \equiv 1 \pmod{d^m}$ for each $m \geq 1$ so that u must be 1).

****