DIRECTORATE OF DISTANCE EDUCATION

UNIVERSITY OF NORTH BENGAL

MASTERS OF SCIENCE -MATHEMATICS

SEMESTER–I

P ADIC ANALYSIS

DEMATH-1 ELEC-5

BLOCK-2

UNIVERSITY OF NORTH BENGAL

Postal Address:

The Registrar,

University of North Bengal,

Raja Rammohunpur,

P.O.-N.B.U.,Dist-Darjeeling,

West Bengal, Pin-734013,

India.

Phone: (O) +91 0353-2776331/2699008

Fax:(0353) 2776313, 2699001

Email: regnbu@sancharnet.in ; regnbu@nbu.ac.in

Wesbsite: www.nbu.ac.in

First Published in 2019

All rights reserved. No Part of this book may be reproduced or transmitted,in any form or by any means, without permission in writing from University of North Bengal. Any person who does any unauthorised act in relation to this book may be liable to criminal prosecution and civil claims for damages. This book is meant for educational and learning purpose. The authors of the book has/have taken all reasonable care to ensure that the contents of the book do not violate any existing copyright or other intellectual property rights of any person in any manner whatsoever. In the even the Authors has/ have been unable to track any source and if any copyright has been inadvertently infringed, please notify the publisher in writing for corrective action.

FOREWORD

The Self-Learning Material (SLM) is written with the aim of providing simple and organized study content to all the learners. The SLMs are prepared on the framework of being mutually cohesive, internally consistent and structured as per the university's syllabi. It is a humble attempt to give glimpses of the various approaches and dimensions to the topic of study and to kindle the learner's interest to the subject

We have tried to put together information from various sources into this book that has been written in an engaging style with interesting and relevant examples. It introduces you to the insights of subject concepts and theories and presents them in a way that is easy to understand and comprehend.

We always believe in continuous improvement and would periodically update the content in the very interest of the learners. It may be added that despite enormous efforts and coordination, there is every possibility for some omission or inadequacy in few areas or topics, which would definitely be rectified in future.

We hope you enjoy learning from this book and the experience truly enrich your learning and help you to advance in your career and future endeavours.

P ADIC ANALYSIS

BLOCK-1

BLOCK-2

BLOCK 2-P ADIC ANALYSIS

Introduction to the Block

In this block we will go through Classical linear groups over p-adic fields
Analytic Functions Over P-Adic Fields, Zeta-functions
Some elementary p-adic analysis, The Campbell-Hausdorff Formula
The Topology Of Qp, P-Adic Algebraic Number Theory

Unit VIII Classical linear groups over p-adic fields
Unit IX Analytic Functions Over P-Adic Fields
Unit X Zeta-functions
Unit XI Some elementary p-adic analysis
Unit XII The Campbell-Hausdorff Formula
Unit XIII The Topology Of Qp
Unit XIV P-Adic Algebraic Number Theory

UNIT-8: THE P-ADIC NORM AND THE P-ADIC NUMBERS

STRUCTURE

8.0 OBJECTIVES

After studying this unit, you should be able to:

- Understand about Classical linear groups over p-adic fields
- Understand about Study of gln (p)
- Understand about Study of On (p, P)
- Understand about Locally Compact Fields
- Understand about Extension to the representations of K which do not satisfy the condition (S)

8.1 INTRODUCTION

In mathematics, p-adic analysis is a branch of number theory that deals with the mathematical analysis of the functions of p-adic numbers.

Classical linear groups over p-adic fields, Study of gln (p), Study of On (p, P), Locally Compact Fields, Extension to the representations of K which do not satisfy the condition (S).

8.2 CLASSICAL LINEAR GROUPS OVER P-ADIC FIELDS

General Definitions

We shall study the following types of classical linear groups over field P or over division algebra.

GL,, (P)- The group of all non-singular n x n matrices with coefficients from P is known the general linear group

PrGLn (P) Let CLn (P) be the centre of the group GL^ (P). The group pr GLn{ P)=GLn (P)/CLn (P) is known the projective linear group.

SLn (P)-The subgroup of GLn (P) consisting of all the matrices of determinant 1 is known the special linear group or the unimodular group. It can be proved that PrSLn (P)=S Ln (P)/ C (S Ln (P)) is a simple group

Let ∈ = Pn and <p a non-degenerate bilinear form over ∈ S Pn (P)- If <p is an alternating form, then the the set of all ma- trices in GLn (P) which leave this bilinear form invariant is a group known the linear symplectic group. We shall denote the by Spn (P). This group is independent of the choice of the alternating bilinear form because any two such bilinear forms are equivalent.

If p is a symmetric non-degenerate bilinear form, then the set of elements in GLn (P) leaving p invariant is group known the linear orthogonal group.

Let P be a separable quadratic extension of P. Let ∈ ^ ∈ be the unique nontrivial automorphism of P. If (p is a non-degenerate Hermitian bilinear form over ∈ i . ∈ ., y (y, x)= (p (x, y), then the set Un (p, P) of elements of GLn (P) leaving p invariant is a group known the unitary group.

Letp be a division algebra of finite rank over P, such that P is the centre of p. GLn (P) The group SLn (P) can be defined as the kernel of the map ^ (determinant of Dieudonne) from GLn (P) to p/C where C is the commutator subgroup of P\

Let PP be the algebra of quaternions over P. In this case there exists an involution in p i . ∈ ., an anti automorphism of p of order 2. So we can define as in the group Un (p, P) which leaves invariant the bilinear form p over pn. As in can define S0n (p, P) and SVn (p, P) and prove that their projective groups are in general simple.

Suppose that P is a locally compact p-adic field. All the groups of types are locally compact, because on Mn (P) (the set of all nyn matrices with coefficients from P) we have the topology of P"1 and GLn (P) is an open subset of Mn (P) and the groups SLn (P) etc.are closed subgroups of GLn (P).

Let us assume that the rank of p over P is r. Then Mn (p) can be imbedded in Mnr (P), as p can be considered as a space of dimension nr over P, since a matrix is inversible in Mn (p) if and only if it is invertible in Mnr (P), we have

GLn (p)=GLnr (P) H Mn (p) But GLnr (P) is an open subset of Mnr (P), therefore GLn (p) is an open subset of Mn (p). Since Mn (p) is locally compact, because it hasthe same topology as the P'1, GLn (P) is locally compact. Un (<p, P) is locally compact, because it is a closed subgroup of GLn (p).

8.3 STUDY OF GLN (P)

By p we shall mean a division algebra of finite rank over P, which is a locally compact valuated field, contained in the centre of p. Let O denote the ring of integers of P

Notes

As we have already observen that O is a compact subset of p, there- fore Mn (O) which is homeomorphic to On2 is compact in Mn (P). Let GLn (O) be the set of elements Mn (O) which are invertible in Mn (O). Obviously GLn (F) contains GLn (O). Therefore

GLn (O)=GLn (p n Mn (O) n [GLn (p n Mn (O)]"1

Since O is open in p, Mn (O) is open in Mn (p. Therefore GLn (O) is open in Mn (O). Similarly GLn (O) is open in GLn (p). Moreover GLn (O) is closed in Mn (O). For, let (Xp) be a sequence of elements in GLn (O) such that Xp tends to X $\in$ Mn (O) as p tends to infinity. Because Mn (O) is compact, we can assume that X-1 has a limit Z in Mn (O). But then ZX=XZ=I, therefore Xbelongs to GLn (O). Hence GLn (O) is compact.

We define in the following some subgroups of GLn (p), which will be of use later on.

where (*) indicates that there can be some non-zero entries.

*|t $\in$ GLn (p), ai $\in$

n being a

Uniform sing parameter in P1

N = 1 1 anaij $\in$ P, aij ^ 0a1n

a i $\in$ Z Pa"

We observe immediately that T=AN and r=DN. Moreover T is a solvable group, r is solvable if Pis commutative and T (respectively r) is a semi direct product of A and N (respectively D and N).

Proposition. GLn (P)=G=TK, where K=GLn (O).

Proof. When n=1, the proposition is trivially true. Suppose that it is true for all GLs (p) for s<n - 1. We shall prove it for GLn (p). Let g= (gij) be an element of G. We can find integers (kj1)1<j<n such that

n^ gijkj1=0 for 2<i<n j=1 = a11+0 for i=1.

By multiplying on the right with a suitable element of p we can take atleast one of j to be 1. Let k= (y j be a matrix, where yi1 = ki1 for i=1, 2, .. ., n with j=1, Yjr=0 for r=2, .. ., n and the other jij are so determined that k belongs to K.

So we get But by induction hypothesis g=tk where t belongs to T and k ∈ K' the subgroups T' and K' defined in GLn-1 (P in the same way as T and K in G Thus we get

1 *k-1\/1 0 t 0 k

This implies that

= t1k1, t1 ∈ T and k1 ∈ K.

Hence our result follows:

We shall now prove an analogue of Elementary divisors theorem.

Let A be a ring with unity (but without any other condition). Let us

consider the following assertions (where module signifies left module): any finitely generated module is isomorphic to a direct sum

A/a,, where a, are left ideals with A+a\ d ... d ar

i= l ~1 ~1 ~r

Such decomposition, if it exists, is unique.

if M is a free module of finite type and N a finitely generated submodule of M, there exists a basis e1, .. ., er and r elements a1, .. .,ar of A such that ai+1 c Aaj and such that N is the direct sum of submodules Aae.

if such elements et and ai exist, the ideal Aaj are independent of the choice of the ei and ai satisfying.

if g is a m X n matrix with coefficients in A, there exists two m X m and mxn invertible matrices p and q such that d=pgq is a m X n "diagonal" matrix (i . ∈ ., dj=for i ± j) and ai=dil ∈ Aai+1.

if such matrices p and q exist, the ideals Aai are independent of the choice of p and q.

Notes

It is obvious that : consider a basis x \,..xn of M and a system of generators y1ym of N and define the matrix g by Yj=H gijXi. Then et = ∈ (q~l)ikXk is basis of Mand the ae = ∈ pikyk generate N. if a is left Noetherian then implies, for any finitely generated module is a quotient M/N, with M free of finite type and N finitely generated.

It is well known that all these six assertions are true if A is a commutative principal ideal ring. We shall now prove the following extension:

Theorem. Let A be a ring with unity (but A can be non-commutative and can have zero divisors), which satisfies the following conditions:

any left or tight ideal is two sided (equivalently Ax =xA for any x ∈ A

the set of the principal ideals is totally ordered by inclusion (hence any finitely generated ideal is principal).

Proof : the result is obviously true form n=m=1. Assume it is proved for (m - 1) X (n - 1) matrices. Let us consider the ideals A gij- : by they are all contained in one of them, and we can assume without loss of generality, that gji ∈ Ag11 for any indices i, j. Let gi1=cig11 for 2<i<m. By multiplying g on the left by a m X m matrix k where

' i 0 0-c2 10 … 0

k = -cm o …1

we get a matrix kg with (kg)11=g11 and (kg)i1=0 for i>2. Moreover, the matrix k is invertible. Similarly, using the fact that gij ∈ g11 A. We find a n X n inversible matrix h such that

g11 0 ... 0

Now, we have just to apply the induction hypothesis to g (remember that all the coefficients of g, hence of g belong to Agn).

Proof. Let ^. (respectively yf) be the canonical generator of A/a, (respectively A/bj) and x, (respectively yj) the canonical image of L (respectively y.) in M. Then y j=Y aijxi, where an ∈ A and is determined j i=1 m

completely modulo a, and therefore modulo a,. Similarly x, =Y I'ki.Yk-

~ ~ k= 1

where bkii ∈ A and is completely determined modulo b1. Let m be a maximal left ideal containing b1. We observe immediately that m is a two nn

sided ideal and Ajm is a division algebra. Since yy=Y ay=X I'ki.Yk-

we have

n ^ aij=Sky (mod in)

But this is possible only when n>m, because if Vm and Vn are two vector spaces over a division ring of dimension m and n respectively such that <p and if are two linear transformations from Vm to Vn and Vn to Vm respectively. then ^=I implies that if is an isomorphism of Vm onto a subspace of Vn. In the same way we get that m>n. Hence m=n.

If possible let us suppose that a, +bj for some i. Let us suppose that there exists an element a in at_ which does not belong to bj Consider the set aM, it is a submodule of M.

Every left principal ideal in A is a right principal ideal in A. Let xeA —>xaeAa be a map from A to Aa/aA n a,, its kernel is the set \x\xa ∈ a, }=B. Therefore we get that Aa/aA n a, is isomorphic to A/B. Moreover A/ B= (0) if and only if a belongs to a,. Now rank of aM=number of a, such that a does not belong to a,. Since a belongs to aj, a belongs to aj for j<i, therefore rank of a M<n - i. On the other hand rank of aM=number of bj, such that a does not belong to bj. Since a does not belong to bj, rank aM>n - i. Hence we arrive at a contradiction. Thus a, =bj and our result is proved.

A has no zero divisors.

Obviously, the ring O of the integers of any valuated non - commutative field satisfies.Moreover we have in this case djj= (jdf1 with y ∈ O* and 1<i<r and=0 for i>r. The diagonal n X n matrix y defined by yu=yi for

$1<i<r$ and $y_i=1$ for $i>r$ is invertible and multiplying d on the right by y^{-1} and q on the left by y, we get a decomposition g=p d q where p and q are invertible and d is a diagonal matrix whose diagonal coefficients nPi are positive powers of the uniformising parameter n with JS1<…<fir, and the fij are com- pletely determined by these conditions (we used the fact that ideal in O is generated by one and only one power of r).

Now, let us return to the group G. For any n-tuple of rational inte- gers, a= (a1, .. ., an), let da be the diagonal n X n matrix with diagonal coefficients na' and let A+ be the subset of the subgroup A consisting of the matrices da with a1<….<an.

Proposition. In each double coset KgK modulo K, there exists one and only one element of A+.

Proof. Let g= (gij) be any element of G. Multiply g by a diagonal matrix (aii), where aii=ak, a ∈ P, v (a)>0 and k is a sufficiently large integer so chosen that the matrix g=g (aii)belongs to K. Then by the above theorem there exist matrices p and q in K such that

g (aii)=g=p'dpq with dp ∈ A+

Let us take ai=Si - kv (a). Then we have g=pdaq with q, p in K and da in A+. Conversely if g belongs to Kda K. then g belongs to Kdp K. But dp is unique, therefore da is unique.

Corollary. K is a maximal compact subgroup of G.

If possible let H d K be a compact subgroup of G. Obviously there exists a ± 0 such that da belongs to H. Then

r=air 0

(da)r=0 Pa

If ai ± 0, then v (nrai ^ ±m as r ^ ±ra, which is a contradiction as 84 v is a continuous function form p to R. Hence H=K.

Let ∈ be a vector space over p. Let I be a lattice in ∈ i . ∈ ., a finitely generated O module such that its basis generate ∈ . Since I has no torsion, basis of I is a basis of ∈ . In particular if we take ∈ = PPn and I=On and if we identify G with the group of endomorphisms of E, then g ∈ K and only if g (I)=I. Moreover if we take any lattice L, then the subgroup of G which leaves L invariant is a conjugate subgroup of K.

Let H be a compact subgroup of G. Let e1, .. ., en be a basis of ∈ . Let J be an O-module generated by the elements h (ej), 1<j<n and h ∈ H. Evidently we have

J is invariant by H J ∈ I

The map h ^ h (ej) is a continuous map from H to ∈ .

But H is compact, therefore the image of H in ∈ by the map defined in is compact and hence bounded. Therefore there exists an integer k such that J c H~kI, which shows that J is finitely generated, but J ∈ I, therefore J is generated by a finite set of element which generate ∈ . Hence J is a lattice. Thus H is contained in a conjugate subgroup of K namely the subgroup of G which leaves J invariant. Hence we have proved the the following.

Corollary. Any two maximal compact subgroups ofG are conjugates and any compact subgroup of G is contained in a maximal compact subgroup ofG.

Remark. Any double coset KxK, x ∈ G, is a finite union of left cosets modulo K, because K is open and compact, therefore every double coset and left coset modulo K is open and compact.

We introduce a total ordering in Zn by the lexicographic order i . ∈ ., if a= (a1, ..., an) and jd= (S1, ...,fdn) are two elements of Zn, then we say that jd>a if jdi>a, for the least index i for which jdi ± ai.

Proposition. If NdpK n KdaK+ (p, where a fd are in Zn and da ∈ A+ then jd>a and Nda K n Kda K=da K.

Proof. Let ndp belongs to N dp Kn Kda K,

Then ndp belongs to KdaK. But ndp belongs to KdaK if and only

CX\ (Xn

if the invariant factors of ndp are n, ... n. Therefore we get that /r"' divides tP i for i=1, 2, ..., n. If a 1<jSi, our assertion is proved. If a i=1, then we multiply the matrix ndp on the right by a matrix 8.

wherenai 3in1if0 0So we getra1 00 tP2 *0 0 Jp n

It is obvious that belongs to K. Therefore ndpd is in KdaK, which means that its invariant factors. Thus tGn are the invariant factors for g, which implies that g belongs to Kn-1da - Kn-1 with obvious notations. Our assertion is trivially true forn=1. If we assume that it is true for all groups GLr (P) for r<n - 1. \\ c get a<[i. But a=ji, therefore a<g. We prove the second assertion also by induction on n. For n=1, it is trivially true. Let us assume that the results is true for all groups GLr (P) for r<n - 1. We have to show that dgnda belongs to K if nda belongs to KdaK Let us suppose that

Since nda belongs to KdaKn"1 divides an for i=2, …,n. Obviously

where X consists of integers Xj=n~ai a and g is a (n - 1 X n - 1) mat rix of the form <F] X<1, and the invariant factors of n'da- are

belongs to Kn-1 .

8.4 STUDY OF ON (P, P)

In this section we shall prove some of the results for the group G=On (p, P).The same results can be proved for other such groups of GLn (P namely SLn (P) etc. with obvious modifications. Throughout our discussion P will denote a locally compact p-adic field such that K=Op\Yp has characteristic different.

Definition. Let ∈ be a vector space of dimension n over P. A subspace F c ∈ is known isotropic with respect to (p (a bilinear form as ∈) if there exists an element x in F such that p (x, y)=0 for every y in F, in other words the bilinear form when restricted to F is degenerate.

Definition. A subspace F c ∈ is known totally isotropic with respect to p if the restriction of p to F is zero i . ∈ ., p (x, y)=0 for every x, y in F.

It is obvious from the definition that the set of totally isotropic sub-spaces of ∈ is inductively ordered. Therefore there exist maximal totally isotropic subspaces of ∈ . They are of the same dimension, which we call the index of p. If index of p=0, p is known a non-isotropic form.

Witt's decomposition. Let E1, E2 and E3 be three subspaces of E such that

E=E1 E2 E3

E1 and E3 are totally isotropic.

Ei+E3 is not isotropic.

E2 is orthogonal to Ei+E3 i . ∈ ., for x in E2, p (x, y)=o for every ye Ei+E3.

It can be proved that for the vector space ∈ = Pn, there exists a Witt decomposition and we can find a basis e1, e2, ..., er of E1, er+1, ..., er+q of E2 and er+q+1, ..., en of E3, where 2r+q=n, in such a way that <fi (ej, ej)=8, n+1-j for 1<i<r and r+q<j<n. and that is an orthogonal basis for E2. Clearly the matrix of the

rr+1, ••

bilinear form p with respect to this basis of ∈ is

and A is a q X q matrix, which is the matrix of p restricted to E2.

We shall now completely determine the restriction of p to the non - isotropic part. For simplicity we assume that r=0 and q=n. Let e1, ..., eq be an orthogonal basis of ∈ . If x= (x1, ..., xq) is a point q

of ∈ with respect to these basis. Then p (x, x)= 2 a^ with ∈ P

If for i+j is in P"y. then the vector o, ai

Notes

is an isotropic vector of p, which is not possible. Therefore aj ∈ aj (mod P*1), which implies that q<4. We shall say that two bilinear forms p and p' are equivalent if there exists a linear isomorphism of the space of p onto the space of p' and a constant c ± 0, such that p' o A=op. Then it can be proved that every non-isotropic bilinear form over ∈ is equivalent to one and only one of the following type:

q=4

xf - Cx2 - nx3+Cnx4

xf - Cx2 - Cnx3

q=2

x2 - Cx2

xf - nx2

xf - Cnxf

The O-form as where (l, C, n, C n) is a set of representatives of

P modulo Pj2 as obtained in Corollary of Hensel's Theorem.

We shall say that a basis e, en is a Witt basis for p if the relations in are satisfied and if the restriction of p to E2 has one of the above forms. It is obvious that for p or for a constant multiple fo p, we can always find a Witt besides and the matrix of p with respect to a Witt basis is independent of the choice of the Witt basis.

Proposition. If M=Mq (P) is a matrix such that M AM belongs to Mq (O) (M denotes the transpose of the matrix M and A denotes the matrix of the restriction ofp to E2), then M belongs to Mq (O).

Proof. We prove first that if for x ∈ E, p (x, x) is in O, then the co-ordinates of x are in O. Let us assume for instance that q=4. If possible

---

1 q=3

x1 - Cx2 - nx3

let v (xf)<0 and v (xf)<min (v (x2), v (x3), v (x4)). Suppose that v (xf)=a. Since v (x2 - cx2 - nx2 - cnx2)>0 we have x2 - Cx2=o (mod Y2r+1), where r=max (0, a). Therefore (n-axf)2 - s (n-ax2)2=0 (mod Y).

But this is impossible, because C is not a square in k. Thus our result is established. The other cases can be similarly dealt with.

Let M= (mjj), then M AM= (yj where yij-=p (m1i, ..., mqimqj), If MAM belongs to Mq (O) then yii belongs to O, which implies thatmri belongs to O for i, r=1, 2, ..., q. It is obvious that it is sufficient to assume that only the diagonal elements of M AM are in O.

In the following we shall be dealing with a fixed Witt basis of the space ∊ . We shall adhere to the following notations throughout our discussion.

Ko=G n K, To=G n T, N=G n N, Ao=G n A+

n 1 n-ar 0da =T«1

where a= (a1, ..., ar)

Proposition. G=T0K0

Proof. We have already proved that GLn (P)=TK. Therefore g ∊ G implies that g=tk where t and K belong to T and K respectively. We know that det (g)=±1 and det (k) belongs to O*. So det (t) belongs to O*. But det (t) is a power of n, therefore det (t)=1. Now g belongs to G if and only if gOg=O i . ∊ ., fOt=k-1'OK-1. Since k-1'Ok-1 belongs to Mn (O), tOt belongs to Mn (O). This shows that a^Sa3 and a3 and a2Aa2 belong to Mn (O). Moreover, we have 1=det t= (det a^ (det a2) (det a3) and (det a2) and (det a1). (det a3) belong to O (for, a15a3 belongs to Mn (O)). So det a2 belongs to O* implying a2 belongs to K. By above proposition we get that the matrix a2 has coefficients from O. We shall find a matrix 6 in T n K such that t6 belongs to G. Then g=tK=t66-1 K implies that 6-1 K belongs to Ko and our result will be proved. Multiply the matrix t by the matrices h and h on the right. Where We shall determine the matrices b, % and Z in such a way that belongs to G. Now th h'belongs to G if and only if (t h h)'O (t hh)=O

i . ∈ ., if and only if the following conditions are satisfied

b' sl1Sa3=S

AY+Xa-1Sa3+%'b' d1Sa3=0

a'3 Sa1bZ+d3SZ+y AY+Z' bb a\ Sa3+Z sa3=0 let us take b=S (a11 Sa3)-1. Then h belongs to K n T and the conditions reduce to

AY+X (a-1)'Sa3+%'S=0 S Z+d3 SZ+Y AY+Z' S+Z Sa3=0

So if we take SZ'=-AY- X'a^1Sa3 and sZ=V where V = a'3SZ+YAY+ZSa3, we observe that the matrix thh belongs to G. It is obvious that the matrix hh belongs to T n K.Hence we get

g=thh. (hh)-1k=t0k0, which proves our result completely.

Definition. Let I be a lattice in ∈ . The O module N (I) generated by the set of elements <p (x, y) for x, y in I is known the norm of the lattice I.

A lattice I is known a maximal lattice if it is maximal among the lattices of norm N (I). It is easy to observe that any lattice of a given norm is contained in a maximal lattice of the same norm. The lattice Io generated by the Witt basis (ei, ..., en) of ∈ is a maximal lattice of norm n

On. Let I be a lattice of norm O containing Io. Let x = ∈ xiei be any

element in I. Then ip (x, ei)=± xn+1-i for 1<i<r and r+q<i<n. r+q

let y= D xiei, since i (y, ej) is an integer for r+1<j<r+q, Xj is i=r+1

an integer for r+1<q+r. Hence x belongs to Io. Therefore Io is a maximal lattice.

Theorem. Let I1 and I2 be two maximal lattices of norm O, then there exists a Witt basis (f1, f2, ..., fn) of ∈ and r integers aj>...>ar>0, such that (r =index i)

I1 is generated by (f1, f2, .. ., fn)

I2 is generated by

$$\left(\overset{-\alpha_1}{\pi} f_1, \ldots, \overset{-\alpha_r}{\pi} f_r, f_{r+1}, \ldots, f_{r+q}, \overset{\alpha_r}{\pi} f_{r+q+1}, \ldots, \overset{\alpha_1}{\pi} f_n\right).$$

Proof. We shall prove the theorem by induction on r. When r=0, i is non-isotropic and there exists only one maximal lattice of norm O which is generated by any witt basis of ∈ . Let us assume that the theorem is true for all bilinear forms of index<r. We first prove the following result.

If I is a maximal lattice of norm O and X is an isotropic vector in I such that n-1 Xdoes not belong to I, then there exists an isotropic vector X ∈ I such that i (X, X7)=1.

If possible let us suppose that the result is not true. Let us assume that i (X, Y) belongs to Y for every Y in I. Then i (n-1 X, Y) belongs to O. Consider I=I+On-1 X. It is a lattice because / is finitely generated O module containing I. Moreover

l (Y+an-1 X, Z+jin~xX)=<p (Y, Z)+ai (n-1 X, Z)+Pi (n~lX, Y) is an integer for every a, /3 in O. Therefore norm of I' is O. But this is a

contradiction because I is a maximal lattice of norm O. Therefore there exists a vector Y in I such that <p (X, Y) belongs to O*. By multiplying Y by some inversible element of O, we get a vector Y in I such that V (X, Y')=1.

Let us take X=Y - ^ (F', Y)X. Obviously <p (X, X)=1 and <p (X, X)=O.

Now we shall prove the theorem. For every isotropic vector X ∈ I1 (respectively I2) let t (X) (respectively u (X)) denote the smallest integer

such that X (respectively nuX)X) belongs to Irrespectively IO. Such an integer exists. because I1 is an O-module of finite type and I2 gen- erates E, therefore there exists an integer t such that ntI1 c I2. Thus t (X)<t always. Let X be an isotropic vector in I1 such that n-1 X does not belong to I1. Then Y=nt (X)X belongs to I2 and n-1 Y does not belong to I2. Since n-1 X does not belong to I1, it is obvious that u (Y)=-t (X). By the above result there exists a vector X in I1 such that V (X, X')=1 and

<p (X, X')=0. This shows that n-1 X does not belong to I1. By the definition of t (X) and t (X)' we get that

V (nt (X) X, ^X,) X)=^X)+t (X)

Since v (nt (X)X, nt (X)X, nt (X)X) belongs to U, we get that

t (X)+t (X)>0.

Similarly there exists an isotropic vector Y in I2 such that V (Y, Y)=1and u (Y)+u (Y)>0.

Let Z=n''^Y') Y, then t (Z)=-u (Y)

Therefore we get

t (X)+t (Z)<0

obviously Z is isot ropic and n1Z does not belong to I1. Therefore there exists a vector Z in I1 such that v (Z Z)=1 and v (Z, Z)=0 and

t (Z)+HZ)>0

Let us suppose that the vector Xis so chosen that t (X) is of maximum value, which exists because t (X)<t for every X for some integer t.

Therefore in particular we get t (Z')<t (X). From and it follows that

t (X)+t (Z)=0 t (X)+t (Z')=0

Thus we have found two vectors X and Z in I1 such that na1 X and n-a1 Z where a1=t (X) belong to I2 and

p (Z X)=p (n~t (Z) y,nt (X)Y)=1.

Let F denote the subspace of ∈ orthogonal to the subspace of E generated by the vectors X and Z.Obviously p restricted to F is non - de- generate and its index is r - 1. Moreover I1=OX OZ F n I1, because for any a in I1 we have

a=AX+p Z+b, where A and O belong to p and b belongs to F. But p (a, X)=u, therefore it is an integer, similarly A is an integer. Thus b belongs to I1 and the assertion is proved. Similarly we have I2=Ona1 X On-a1 Z I2 n F. It can be easily sen that Ij n F (j=1, 2) is a maximal lattice of norm O. Hence by induction hypothesis there exists a Witt basis f2, f3, •••, fn-1 of F and there exist r-1 integers a2 > — ar>o such that

f1, f2, ..., fn-1 generate I1 n F.

f2, .. ., lrfr, fr+1, ..., fr+q, °n fr+q+1' °n fn-1 generate h n F.

If we take f1=Z, fn=X and a1=t (X) we get a Witt basis (f1, •••, fn) 97 of ∊ and r integers a1, ...,ar satisfying the requirements of the theorem because a2=t (fn-1)<a1.

Corollary. The group G acts transitively on the set of lattices of norm O.

The mapping g defined by

g (f)=fi, where Y=ai for 1<i<r

= O for r+1<i<r+q = 2r+q - i+1 for r+q+1<i<2r+q.

leaves O invariant. Therefore g belongs to G.

Proposition. In each double coset of G modulo Ko there exists one and only one element da of A+.

Proof. Let g be any element of G. We shall denote by g itself the automorphism of ∊ with respect to the initial Witt basis (e1, ..., en). The lattice g (Io) is obviously a maximal lattice of norm O. Therefore by the above theorem we get a Witt basis (f1, ..., fn)of ∊ such that

Io is generated by f1, ..., fn,

g (Io) is generated by g1, ..., gn where gi=f with as defined in the corollary of above theorem. Let k\ (respectively k2) be the matrix with respect to the basis e1;.. ., en) (respectively g \, g2, ... gn) of the automorphism k1 (respectively k2) defined by k1 (ei)=f (respectively k2 (gi)=g^)) for i=1, 2, ,n. We observe immediately that the matrix K1 and K2 are in Ko. Moreover the matrix of the automorphism I] —> with respect to the basis I) is d° It is obvious that

Notes

g (ei)=YuMJiSj

j = (*2)S (fa)kj fk

jk = J] (k2) (d°a)kj (kQB e7 jk, l

Thus we get g=k2 cPa k \, which means da belongs to K^gK0. The uniqueness part of the propositional follows from the uniqueness of d° in K x K for x in GLn (P).

We introduce a total ordering in Zn which is inverse of the lexicographic ordering.

Proposition. Let a and fi be two elements in Zr such that ∊ A°+. If N° K0 n K0 da K0+p then fi>a. Moreover N° da K0 n K0 dO K0 = da K0.

Proof. Since N0 d° K and K° da K are contained in N Gfi K and K da K respectively with

a'= (-a 1, — a2, .. ., -ar, 0 ... 0, ar, ar-1, .. ., a\) fi'= (— fi1, — Pa, .. ., — fir, 0 ••• 0, fir, fir — 1,.. .,Ih)

we have N dp, K n K da, K+p. Therefore fi'>a' for the lexicographic

ordering introduced in Zn.

It is obvious that fi>a for the new ordering of Zr. The other assertion follows trivially from the fact that

da K n G=da K°.

Check your Progress-1

Discuss classical linear groups over p-adic fields

____

____

____

8.5 LOCALLY COMPACT FIELDS

In this section we give certain equivalent conditions for valuated fields to be locally compact. Later on we shall completely characterise the locally compact valuated fields.

Theorem. Let K be a field with a proper valuation v. Then the following conditions are equivalent.

K is locally compact. O is compact.

K is complete, v is a discrete valuation and k is a finite field.

Proof, (a) =^ (b). Since (I'a)aerv form a fundamental system of closed neighbourhoods for 0, there exists an a such that I'a is compact. But m I'a=OXo, if Kx>)=a, therefore O=x-1 Ia is compact.

(b) =^ (a) is trivial, as O is a compact neighbourhood of 0. (a) =^ (c)K is complete because it is a locally compact commuta- tive group. For any a>0 in rv O/ Ia is compact because O is compact.

But O/Ia is a discrete space, therefore it contains only a finite num- ber of elements. In particular k=O/Y is finite field. For any p in rv, 0<p<a, we have Ia c Ip c O, therefore Ip/Ia is a nontrivial ideal of O/Ia and distinct elements give rise to distinct ideals. But O/Ia is a

finite set, therefore there exist only a finite number of p with 0<p<a, so we get that

rv has a smallest positive element

rv is Archimedian.

Thus rv is isomorphic to Z and the valuation v is discrete. (c) =^ (b). We shall prove that discreteness of the valuation v and finiteness of k implies that O is precompact, which together with the fact that K is complete implies that O is compact. Let V be any neighbourhood of 0. Since v is discrete, for some n>0 V contains Yn. We shall show by induction on n that O/ Yn is finite for n>0. The result is true for n=1; let us assume it to be true for all r<n. We have O/Yn-1 ^ O/Yn/Yn-1/Yn But O/Yn-1 is finite by induction hypothesis and Yn-1/Yn is finite because it is

Notes

isomorphic to O/Y, therefore O/Yn is finite. Hence there exist a finite number of elements x1 xr in O

such that O c |J (x^+Yn) c |J (x^+V) and since this is true for every

i=1 i=1

neighbourhood of 0, O is precompact.

Convergent Power Series

Let K be complete field with a real valuation v. Then the power series

To f (x)=X anx" with coefficients from K is said to be convergent at a

n=0

to point x of K if the series ∈ anx" is convergent. It has already been

to proved that the series anx" converges if and only if n=0

v (anx")=v (an)+nv (x) ^ to as n ^ to

From it is obvious that if take t=lim inf - (if a,,)). then the series n n

f converges for all x which v (x)>-t and does not converge for those x for which v (x)<-t and for those x for which v (x)=-t either the series converges for all x or does not converge at all. The number -t is known the order of convergence of the power series f and the set { x|v (x)>-t } or { x|v (x)>-t, if the series converges at a point x with v (x)=-t } is known the disc of convergence, which we shall denote by Df. If we consider the absolute value associated to v then the radius of convergence is

p=a-= (lim sup (| a|n)1/n }

yn^TO) and Df={ x| |x|<p } or { x| |x|<p }

The mapping x ^ f (x) from Df to K is continuous because it is a uni-

TO form limit of polynomials namely the partial sums of the series ∈ anxn in the disc { x|v (x)>-t1, for all t1>t } or in the disc { x|v (x)>-t } if the series converges on the disc. The classical results about addition and multiplication,. .. of power series can be carried over to the power series with coefficient in a complete valuated field. For instance

if f (x)=X a^nxn and g (x)=2 bnxn are two power series with Df and

Dg as their discs of convergence respectively; then if for one x in Df, ajx1 belongs to Dg for every i, f (x) also belongs to Dg and we have

g (f (x))=Z crxr, where cr=^ bq ^ ai1 ai2 ... aiq,

q=0 i]_+i2+ — +iq=r

all the series being convergent.

Remark. If k=O/Y is an infinite field, then

inf (v (aixi))=inf (v (f (/))). v (y)=v (x)

For, v (f (x))>infi (v (aixi)). We get equality, if there does not exist any two terms of the same valuation. In the exceptional case as the series

TO as the series ∈ any" is convergent, we have

f (y)=X ary+terms of higher valuation, where io<r<Jo<to.

r=io and without loss of generality we can assume that v (x)=0 and

infjv (aixi)=0. Now v (f (y))>0 if and only if 2 ary belongs to

r=io Jo r Yi . ∈ ., if and only if the polynomial ∈ arf (the image in k)=0. But

r= io k has infinite number of elements and the above polynomial not being identically zero has only a finite number of zeros, therefore there exists atleast one y for which v (f (y))=0 and v (x)=v (y). Thus in this case whenever x is in Df and f (y) belongs to Dg for all those y for which

v (x)=v (y), we have

inf v (aixi)=inf v (f (y)).

v (y)=v (x)

TO

Then f (g (x))=2 crxr with

r=0 cr=^ bq ^ avi ... avq. r=0 V1+ +Vq=r

Remark. Let A be a ring with a topology defined by a decreasing filtration (An)n>0 of ideals for which A is Hausdorff and complete space.

Then the formal power series anxn converges at x in A if and only n= 0

if anxn ^ 0 as n tends to infinity and obviously the series converges everywhere in A if and only if an tends to 0 as n tends to infinity.

8.6 EXTENSION TO REPRESENTATIONS OF K WHICH DO NOT SATISFY THE CONDITION (S).

This problem is related with the construction of other representa- tions of G: we have observen that the representation UA do not form a com- plete system. Hence, by the Gelfand-Raikov theorem, there certainly exist other irreducible unitary representations of G.

We have two indications: first the case of a real semi-simple Lie group G. It observems very likely that to any class of Cartan subgroups H of G, corresponds a series of representations of G, indexed by the char- acters of H. This has been verified in some particular cases (of.Harish- Chandra and Gelfand-Graev). In particular, assume that there exists a compact Cartan subgroup H: then in many cases (more precisely in the cases where G/K is a bounded homogeneous domain in the sense of ∊ . Cartan (K is a maximal compact subgroup)), we can get irreducible uni- tary representations of G in the following way: take a character A of H. take the unitary induced representations UA in the space HA ; this rep- resentation is not irreducible. But we have a complex-analytic structure on G/H and we can look at the subspace of HA formed by the func- tions which correspond to holomorphic functions on G/H. Then we get an irreducible representation. This is in particular true for compact semi-simple Lie groups.

On the other hand, in the case of classical linear groups over a finite field, for instance for the special linear group G with 2, 3 or 4 variables, one knows all the irreducible representations of G and one observes that to each class of Cartan subgroup H, corresponds a series of representations indexed by the characters of H. But one does not know how exactly

this correspondence works. It observems likely that the representation U (A) associated with character A of H is a sub representation of the induced representation UA, and it would be extremely interesting to get a "geometric" definition of U (A).

If one could get such a definition, it would perhaps be possible to generalize it to the algebraic simple linear groups (or at least to the classical groups) over a p-adic field.

Check your Progress-2

Discuss locally compact fields

____

____

8.7 LET US SUM UP

In this unit we have discussed the definition and example of Classical linear groups over p-adic fields, Study of gln (p), Study of On (p, P), Locally Compact Fields, Extension to the representations of K which do not satisfy the condition (S)

8.8 KEYWORDS

Classical linear groups over p-adic fields….. We shall study the following types of classical linear groups over field P or over division algebra .

Study of gln (p)….. By p we shall mean a division algebra of finite rank over P, which is a locally compact valuated field, contained in the centre of p

Study of On (p, P)….. In this section we shall prove some of the results for the group G=On (p, P) .

Locally Compact Fields….. In this section we give certain equivalent conditions for valuated fields to be locally compact

Extension to the representations of K which do not satisfy the condition (S)….. This problem is related with the construction of other representa-tions of G: we have observen that the representation UA do not form a com-plete system

8.9 QUESTIONS FOR REVIEW

Explain Classical linear groups over p-adic fields

Explain Locally Compact Fields

8.10 REFERENCE

p-adic numbers: an introduction by Fernando Gouvea

p-adic Numbers, p-adic Analysis, and Zeta-Functions, Neal Koblitz (1984, ISBN 978-0-387-96017-3)

A Course in p-adic Analysis by Alain M Robert

Analytic Elements in P-adic Analysis by Alain Escassut

8.11 ANSWERS TO CHECK YOUR PROGRESS

Classical linear groups over p-adic fields

(answer for Check your Progress-1 Q)

Locally Compact Fields

(answer for Check your Progress-2 Q)

UNIT-9: ANALYTIC FUNCTIONS OVER P-ADIC FIELDS

STRUCTURE

9.0 OBJECTIVES

After studying this unit, you should be able to:

- Understand about Analytic Functions Over P-Adic Fields
- Understand about Zeroes Of A Power Series
- Understand about Criterion For The Rationality Of Power-Series
- Understand about P-Adic Power Series
- Understand about Algebraic Extensions Of Qp
- Understand about Study Of The Algebra Of Spherical Functions
- Understand about The Zero Set Of A Linear Recurrence Sequence

9.1 INTRODUCTION

In mathematics, p-adic analysis is a branch of number theory that deals with the mathematical analysis of the functions of p-adic numbers.

Analytic Functions Over P-Adic Fields, Zeroes Of A Power Series, Criterion For The Rationality Of Power-Series, P-Adic Power Series, Algebraic Extensions Of Qp, Study Of The Algebra Of Spherical Functions, The Zero Set Of A Linear Recurrence Sequence.

9.2 ANALYTIC FUNCTIONS OVER P-ADIC FIELDS

Unless otherwise stated K will denote a completed valuated field with a real valuation v. We shall adhere to the notations adopted in part throughout our discussion.

Newton Polygon of a Power-Series

Definition. Let f (x)=2 aixi be a power-series over K. Let S be the i=0

set of points Ai= (i, v (ai)) in the Cartesian plane. The convex hull of S together with the point y=to on the ordinate axis is known the Newton Polygon of the power series f.

It is obvious that the point Ai= (i, v (ai)) lies on the line Y+v (x)X = v (aixi), where v (aix') is the intercept cut off by the line on the Y - axis. If the series is convergent at the point x=t then intercepts cut off on the axis of Y by the lines through the points Ai with the slope -v (t) tend to infinity as i tends to infinity. Moreover it can be easily proved that if (mi) is the sequence of slopes of the sides of Newton Polygon of f,

then (mi) is monotonic increasing and 1111 ….. p (f) (the order of convergence of f).

9.3 ZEROES OF A POWER SERIES

Let /'=X be a power series over K. Let p (f) =7_1, ""inf— —. We

have already proved that f is convergent for all points x in K for which v (x)>p(f). Let r be a real number greater than p (f). We shall try to

find the zeroes of f on the circle v (x)=r. Let us assume that a0 ± 0.

If there exists no side of the Newton Polygon of f with slope-r, then there exists there exists one and only term of minimum valuation in X aixi. For, if v (x)=r and a=v (aixi)=v (ajxJ) =^f v (akxk), then all the points Ak are above the line Y+rX=a and AiAJ- is a side of the Newton Polygon of slope-r. This is contrary to the hypothesis. Thus v (f (x))=v (aixi) for some i and for v (x)=r, which implies that there is no zero of f on the circle v (x)=r.

If there exists a side Ap Aq of slope-r, then there exist at least two terms of minimum valuation. Therefore there can to be a zero of f on the circle v (x)=r. Assume that p<q. Let v (x0)=r for some x0 in K and c=v (aqx0)=v (aqxq). Consider the power series

fi (y)=a-1 x-qf (xoy)=Y^ by

Obviously v (bp)=v (bq)=0, v (bi)>0 for i ± p, q and v (y)=0 whenever v (x)=r. Hence without loss of generality we can take r = 0, v (ap)=v (aq)=0, v (ai)>0 for i<o and i<p and i>q and aq=1. Therefore

f (x)=xq+...+apxp=p+...+ap) where ap+0

The polynomials X and (X~p + + ap) satisfy the requirements of

Hensel's Theorem, therefore there exists a monic polynomial g of degree q - p and a power series h, both with coefficients in O, such that

~g=X~p+...+ap, h=xp, f=gh

and the radius of convergence of h is equal to the radius of convergence of f. Let us assume that g=X~p+ … +gQ. Then go=~ep, +0. Let us further assume that K is an algebraically closed field. Then g has q – p zeroes in K which belong obviously to O*. Moreover h has no zeroes on the circle v (x)=0. Thus f has exactly q - p zeroes on the circle v (x)=0 where q - p is the length o the projection of the side of the Newton Polygon of f with slope 0. If A1, A2,. . ., Aq-p are the zeroes of

Notes

q-p f, on v (x)=0 then f=h • n (x- Ai). We have also proved that if f is a

i=1 f (x) power series and A is its zero on a circle if x)=r> p (f), then is
x- A

also a power series with the same radius of convergence. Regarding the zeroes of f inside the circle v (x)>r we prove the following.

Proposition. The power series f has a finite number of zeroes A1,. . ., Ak in the disc v (x)>r>p (f) and there exists a power series h such that

f (x) =i P| (x - Aj) • h (x) with p (f)=p (h).

1=1

Proof. We have proved that f (x) has zeroes on the circle v (x)=ri > p (f) if and only if there exists a side of the Newton Polygon of f of slope -ri. But we know that if (m^ is the sequence of slopes of sides of the Newton Polygon of f, then l™comi=-p (f). Therefore there exist only a finite number of sides of the Newton Polygon of slope -r1<-r<-p (f) i. ∈ . , there exists only a finite number of r1 such that r1>r>p (f) for which there are zeroes of f (x) on v (x)=r1. Hence the theorem follows.

If f (x)=X aid is convergent in a disc v (x)>r, then we shall say

i=0 that f (x) is analytic v (x)>r.

Proposition. If f (x) has no zeroes in the disc v (x)>r>p (f) in particular f (0)+0, then the power series /s analytic for v (x)>r.

Proof. Let us assume that f (0)=1. Since f has no zeroes in v (x)>r, there exists no side of the Newton Polygon of f of slope<-r. This

implies that>~r for every i. Considering f as a formal power

J]V (ai1)>-Ti fU=-rJ

1=1= A 1=1v (bJ)>-r.

Hence p^j> r.

Proposition. If f is an entire function (i. ∊ . , p (f)=-m) and has no zeroes, then f is a constant.

Let f (x)=Yj °j=0 aixi. As in the proof of the preceding proposition, we observe that:

v (aj)>-rJ for any r Hence, we have aj=0 for J> 1.

From these propositions, we can deduce the complete structure of entire functions:

Weierstrass' Theorem. Let K be an algebraically closed complete field with a real valuation v. Let f be an everywhere convergent power series over K. Then the zeroes of f different from zero form a se- quence (A1, A2,. . ., An,. . .,) such that v (An) is a decreasing sequence which tends to -m if the sequence (An) is infinite and we have

f (x)=a0/[~[|l - j

the infinite product being uniformly convergent in each bounded subset of K. Conversely for any sequence (An) such that v (An) is a decreasing sequence tending to -m as n tends to infinity, the infinite product is uniformly convergent in every bounded subset of K and defines an entire having zeros at the prescribed points An.

Proof. We shall prove the latter part first. Consider

1=1 / v N x 1

<pn (x)=n t1 _ j.)=2

N ^ " k=0

where akN= (- l)k V,. ' — —

1<i1 <i2<---<ik<NAi1 Ai2 Aik

clearly Kawv) >+\ v\ —)+•••+v\— T /(11=p*. Since lim i{ Ai) = \ W

\A 1 // 1 — m

-oo, lim=co. Let

Notes

k — — m k

co / \ m

- [[(l -11Xak^'where

«= s 1

i Ai, ... Ai, +lt Okn

1<i1 <12 <-<ik 1 k n — m

(obviously the series giving at is convergent and therefore the series p (x)represents an entire function. We have to show that the polynomials pn converge to p uniformly on every bounded subset of K.

Given two real numbers M and A there exists an integer q such that v (akNXk)>M for k>q, for all x with v (x)>Aand for all N, because

^ —>oo as k — » oo. This implies that for any N k

PN (x) - ^ akNxk

> M for v (x)>A

P (x) - ^ akNxk

Similarly we get

> M for v (x)>A

Since akN ^ aK as N tends to infinity, combining we get v{ (fi (x) - (fiN (k))>Mfor N sufficiently large. It can be easily proved that the Aj are the only zeroes of the function <p (x).

Let us denote by f1 the product given by (1). Take a disc v (x)>r. In this disc f (x) has only a finite number of zeroes. Let the zeroes of f in v (x)>r be 0 (k times) and A1, A2,. .. Ap. Then

where gx) has no zeroes in the disc if x)>r. Therefore - is analytic in

the disc v (x)>r. Consider — = — =n /=1 (' ~ j~) where g\ is f

analytic and has no zeroes in the disc if x)>r. Therefore — is analytic f in the disc gx)>r and has no zeroes in it. Since it is true for every r, —

is a constant function. Hence our theorem is proved.

Form the properties of the meromorphic functions:

Definition. A power series <p = ∈ aiX over a field K is said to be a

j=-m

meromorphic function in a disc v (x)>r if and only if there exist two

functions f and g analytic in the same disc such that (p= —.

In any disc v (x)>F>r, g has a finite number of zeroes, therefore g=Pg where P is a polynomial and g has no zeroes v (x)>F which means that y is analytic in if x)>F. Therefore we can can write

p = f 1

—, where /'=f — is a convergent power series in if x)>F. P g

9.4 CRITERION FOR THE RATIONALITY OF POWER-SERIES

Let F be any field and f=Y*TO=0 akX an element in F[[x]]. It can be easily proved that f is a rational function if and only if there exists a

finite sequences (qi)o<i<h of elements of F at least one of which is non-zero and an integer k such that

anPh+an+1 Qh-1+' ' '+an+hQo=0

for all integers n such that n+h>k. Let us denote by Ah+1 the determinant of the matrix (an+i+j)0<i, j<h.

Theorem The power series f is a rational function if and only if there exists integer h and no such that Ah+1=0 for all v>no.

Proof. It is obvious that the condition is necessary. We shall prove that the condition is sufficient by induction on h. When h=0, we have an=0 for n sufficiently large. Therefore f is actually a polynomial. Let us

Notes

assume that An+1=0 for n>no. Moreover we can assume that Ah ± 0 for infinitely many n, because if An=0 for n large then by induction hypothesis we get that f is a rational function. Since Ah+1=0

for n>no, Ah Ahn+2= (Ah+1). So it follows that Ah+0 for n>no. Consider the following system of linear equations

Er=an0+r*1+an0+l+r*2+•••+an0+l+rXh+1=0 for r=0, 1, 2, . ..

For any q>no the system 2 qof the h if h equations Eq, Eq+1,. .. Eq+h-1 is of rank h (because Ahq ± 0). So has a unique solution upto a constant factor. But the system <=' of the h+1 equations Eq,. . ., Eq+h is also of rank h (because Ah+1+0 and A^+1=0) and therefore 2'q and 2 q+1 on the hand and 2 'qand 2 q+1 on the other hand have the same solution.

Thus any solution of q is a solution of q+1 and any solution of no is a solution of Eq for q>no. Thus we have found a finite sequence (xi) such that ano+rx1+...+ano+h+rxh+1=0 for r>0. Hence f is a rational function.

Theorem. Let f (x)=Y> aiX be a formal power series with coefficients in Z. Let R and r be two real numbers such that Rr>1

f considered as a power series over the field of complex numbers is holomorphic in the disc |x|<R.

f considered as a power series over Op (the complete algebraic clo- sure of Qp) is meromorphic in the disc |x|<F with F>r. (where lip) is the absolute value associated to Vp). Then f is a rational function.

Proof. We can assume that R<1, because R>1 implies that f is a polynomial and we have nothing to prove. Moreover r>1, because Rr>1. Since f is meromorphic in |x|p<P, there exist two functions g and h analytic in \x\p<r such that /=f. If necessary by multiplying / by a suitable power of x we can assume that f has no pole at x=0 and hence that h is polynomial with h (0)=1. Let

By Cauchy's inequality we obtain the following

|as|<MR-s

|gs|<Nr~s

By taking R and r smaller if necessary we assume that |as |<R~s and

|gs|p<r~s for s>s0.

Let m+1

where m>k.

The equation gives an+m an+m+1 an+m+k-2 gn+m-k r2+2m

Obviously for n>so we have

IA^+1I< (m+1)! (R- (n+2m))m+1 and lAm+1lp< (r~n)m~k+1

because |an|p<1 for every n. If Am+1+0, then 1<|Am+1||Am+1|<
(m+1)!R_2m (m+1)rkn[Rr]"n (m+1)=k1[(R r)m+1 r~k]-n

Let m be so chosen that (Rr)m+1r~k>1. Then there exists an integer n0
such that for n>n0

Am+1iAm+1i<1.

This is a contradiction. Therefore Am+1=0 for n>n0. Hence f is a
rational function.

Corollary. If f is a power series over Z such that f has a non-zero radius
of convergence considered as series over the complex number field is
meromorphic in Op, then f is a rational function.

9.5 P-ADIC POWER SERIES

We consider power series

f (x)=^2 ak (x— xo)k

where x0 ∈ Qp and ak ∈ Qp for all k.

f (x) converges on B (x0, p-m) lim \ak\pp-mk=0.

k^k

In particular, f (x)=^k=0 akxk converges on Zp=B (0, 1) if and only if limk^k \ak\p=0. Consider the set of power series converging on Zp,

O :=<akxk : ak ∈ Zp for k ^ 0, lim \ak\p=0 1.

Then O is a ring under addition and multiplication of power series. Notice that O contains Zp[x].

Given power series f=^k=0 akxk, g=k=0 bkxk ∈ O and a non-negative integer m, we write f=g (modpm) if ak=bk (modpm) for all k ^ 0.

Theorem. (Strassman). Let f (x)=T=0 akxk t O be a power series of which not all coefficients are 0. Let k0 be the index such that

|ak|p ^ |ako|p for k ^ ko, |ak|p<|ako|p for k>ko.

Then f (x) has at most k0 zeros in O.

By dividing f by ako, we observe that there is no loss of generality to assume that ako=1, ak t Zp for k ^ k0, ak t pZp for k>k0.

We need some Theorems.

Theorem. Let R be a ring and g a monic polynomial in R[x]. Then for every polynomial f t R[x] there exist q, r t R[x] such that

f=qg+r, r=0 or deg r<deg g.

Proof. This is the usual division with remainder algorithm for polynomials. Since g is monic, it holds for polynomials with coefficients in an arbitrary ring R.

Theorem. Suppose that f satisfies. Then there are a monic polynomial g t Zp[x] of degree k0, and h tO, such that

f=g • h, h=1 (modp).

Proof. We prove by induction on m that for m ^ 0 there are polynomials gm, hm such that

f=gmhm (modpm+1), gm is monic, deggm=k0, hm=1 (modp), gm=gm-1 (modpm), hm=hm-i (modpm), where g-i=h-i := 0. Suppose we have constructed such polynomials. Let 0 ^ k ^ k0. Then the coefficients of Xk in g0, g1,. . ., form a Cauchy sequence, and thus, they converge to a limit in Zp. As a consequence, the polynomials gm converge to a monic polynomial g t Zp[x] of degree k0. Likewise, for every k ^ 0, the coefficients of Xk in hm form a Cauchy sequence and thus converge to a limit in Zp. We note that the degrees of the polynomials hm can increase to x>. As a consequence, the polynomials hm converge to a power series h t O. We have h=1 (modp) since hm=1 (modp) for all m. The coefficients of f— gmhm converge to the coefficients of f— gh and on the other hand to 0. Hence f=g • h.

We now come to the construction of the polynomials gm, hm. Note that holds for m=0 with g0 := ^k=0 akxk, ho=1. Assume that holds for some m ^ 0. We have to construct gm+1, hm+1 such that holds for m+1 instead of m.

We truncate f after an index k1 such that |ak\p ^ p-m-2 for k>k1, that is, we take f1 := Y^k=0 akxk. Then f=f1 (modpm+2), and thus, f1 = gmhm (modpm+1). This implies that there is a polynomial a ∈ Zp[x] such that

f1=gmhm+pm+1a.

By there are polynomials q, r ∈ Zp[X] such that

a=qgm+r, with r=0 or deg r<deg gm.

Now take

gm+1 := gm+pm+1r, hm+1 := hm+pm+1q.

Then we have the following congruences modulo pm+2:

f— gm+1hm+1=f1— (gm+pm+1r) (hm+p^^

= gm hm+pm+1a— gmhm— pm+1 (qgm+rhm)— p2m+2qr = pm+1 (a— qgm— rhm)

= pm+1 (a— qgm— r— r (hm— 1))

= 0 (modpm+2).

Hence gm+1, hm+1 satisfy with m +1 instead of m. This completes our induction step.

Proof of Theorem. Take g, h as in for x ∈ Zp we have h (x)=1 (modp), hence h (x)=0. Therefore, the zeros of f in Zp are those of g. So f has at most deg g=k0 zeros in Zp.

Check your Progress-1

Discuss Analytic Functions Over P-Adic Fields

9.6 ALGEBRAIC EXTENSIONS OF QP

The completion R of Q with respect to the ordinary absolute value has only one non-trivial algebraic extension, namely C. Further, the ordinary absolute value\•\on R has precisely one extension to C, given by |a| := \a • o|1/2=\Nc/r (o)\1/2 for a ∈ C.

In contrast, Qp has finite extensions of arbitrarily large degrees: for instance, for every positive integer d, Xd— p is irreducible in Qp[X] and thus, Qp has an algebraic extension of degree d. An interesting fact is, that for every positive integer d, Qp has up to isomorphism only finitely many extensions of degree d. We state without proofs some results on the extension of |.|p to finite extensions of Qp.

Let K be a finite extension of Qp of degree d, say. Completely similarly as for algebraic number fields, there is a ∈ K such that K=Qp (a). Let f (X)=Xd+a1Xd-1+...+ad ∈ Qp[X] be the minimal polynomial of a over Qp. Let a1,. .. , ad be the distinct zeros of f in the algebraic closure Qp of Qp. These give rise to precisely d distinct Qp-embeddings (i. ∈ . , injective homomorphisms leaving elements of Qp unchanged) of K in Qp, say a1,. .. , ad with &i (a)=ai for i=1,. . ., d.

We define the norm of K over Qp by d

Nk/qp (a)=Gj (a) for a ∈ K.

We state without proof the following result.

Theorem. Let K be a finite extension of Qp. Then |.|p can be continued in precisely one way to K, and K is complete with respect to this continuation If we denote this continuation also by |.|p, then we have

| a|p=|Nk/qp (a)|p/[K:Qp] for a ∈ K.

One can show that if Qp (a)=K and f (X)=Xd+a1Xd 1+...+ad ∈ Qp[X] is the minimal polynomial of a over Qp, then

NK/qp (a)= (— 1)dad.

More generally, if Qp (a)=K, then the degree d of f divides [K : Qp], and we have

|a|p=|ad|p/d.

Given a finite extension K of Qp, we define the ring of p-adic integers of K,

Op, K := { a ∈ K : |a|p ^ 1 }.

Then

mp, K := { a ∈ K : \a\p<1 }

is a maximal ideal of Op, K and

Op, K/mp, K

is a field, the residue class field of K.

Let d := [K : Qp]. Then the value group \K*\p := { \a\p : a ∈ K* } is a subgroup of the multiplicative cyclic group generated by p-1/d. So \K*\p is generated by p-1/eK for some positive divisor eK of d. We call eK the ramification index of K.

One can show that Op, K/mp, K is a finite extension of Zp/pZp=Fp. The degree fK := [Op, K/mp, K : Zp/pZp] is known the residue class degree of K. We state without proof the following results. Given a ∈ Op, K, we write a for the corresponding residue class in Op, K/mp, K.

Theorem. Let K be a finite extension of Qp with ramification index ∈ = eK and residue class degree f=fK. elements of Op, K such that u1,. .. , Uf

Notes

form a basis of Op, K/mp, K over Fp = Zp/pZp. Then Op, K is a free Zp-module with basis

{ n%Uj : i=0,. .. , ∊ — 1, j=1,. . ., f },

i. ∊ . , every element of Op, K can be expressed uniquely in the form

e-1 f i=0 j=1

Examples.. Let K=Q3 (/3)={ a+b/3 : a, b ∊ Q3 }, where is one of the roots of X2— 3. Notice that \/3 ∊ Q3. For \^3\2=3-1, hence \V3\3 does not belong to the value set of\ \3 on Q3. In general, we have for a, b ∊ Q3,

\a+b/3\3=\nq3 (^3)/q3 (a+b/3)\1/2=\a2— 3b2\3/2 = max (\a\3, 3-1/2\b\3).

This implies

O3, K={ a+6^3 : a, b G Z3 }, m3, K={ a+bV3 : a G 3Z3, b G Z3 }=V3O3, k,

03, k/m3, K— Z3/3Z3=F3.

This confirms that eK=2, fK=1.

Let K=Q3 (i)={ a+bi : a, b G Q3 }, where i is a root of X2+1. The polynomial X2+1 does not have roots modulo 3, so it is irreducible in Q3 [X]. We have for a, b G Q3,

|a+biI3=|a2+b2^2=max (| a|3, |b|a),

hence

O3, K={ a+bi : a, b G Z3 }, m3, K={ a+bi : a, b G 3Z3 }=3O3, K,

Or3, K/m3, K={ a+bi : a, b G F3 }=F3 (i).

This confirms that eK=1, fK=2.

We can extend |.|p to the algebraic closure Qp: given a G Qp, take any finite extension K of Qp containing a and put

|a|p := 1 NK/Qp (a)|p/[K:Qp].

gives an alternative expression which is independent of the choice of K. Qp is not complete with respect to |.|p. The completion Cp of Qp with respect to |.|p is algebraically closed.

9.7 STUDY OF THE ALGEBRA OF SPHERICAL FUNCTIONS

Let M be the unity representation of K and Let A be the algebra Lm (G): by our results, this is a commutative algebra. It observems possible to determine completely the structure of A. The representations UA likely

give all the characters A of A. The A describe a space isomorphic to a space Cr and the map a ^ (A (a)) is probably an isomorphism of A onto the algebra of polynomials on Cr which are invariant by the Weyl group of G. (It observems that a recent work by Satake (unpublished) gives a positive answer).

Computation of the "characters" of the UA.

The representations UA are "in general" irreducible. Moreover, if f is a continuous function on G, with carrier contained in K, and if f belongs to some Lm (K), then it is trivial to show that the operator Uxf if of finite rank, and hence has a trace. The same is obviously true if f is a finite linear combination of translates of such functions. But the space of those f is exactly what known the space of "regular" functions of G (space D (G)) and the map f ^ Tr Uf is a "distribution" on G. A problem is to compute more or less explicitly this distribution (which is the "character" of UA. It observems likely that, at least on the open subset of the "regular" elements g of G it is a simple function of the proper values of g (by analogy with the case of complex or real semi-simple Lie groups, of works of Harsih-Chandra and Gelfand-Naimark).

9.8 THE ZERO SET OF A LINEAR RECURRENCE SEQUENCE

Notes

The Norwegian mathematician Thoralf Skolem introduced techniques from p-adic analysis to prove results on Diophantine equations. As an example we prove a result on linear recurrence sequences.

A linear recurrence sequence in C is a sequence U={ uk }<=L0 given by a linear recurrence

un— clun-1+' ' '+ckun-k (n ^ k) with coefficients c1,. .. , ck G C and ck=0, and by initial values

uo,. . ., uk-i G C.

The linear recurrence relation satisfied by U is not uniquely determined. It is however not difficult to show that there is only one linear recurrence relation of minimal length satisfied by U. This minimal length is known the order of U.

Let be the linear recurrence of minimal length satisfied by U. Then the polynomial

fu (X) := Xk - ciXk-1 cfc

is known the companion polynomial of f.

Remark. Denote by Iu the set of polynomials a0Xm+a1 Xm-1+...+am G C[X] such that

aoUn+aiun-i+...+amun-m=0 for all n ^ m.

Then Iu is an ideal of the polynomial ring C[X] generated by fu, i. ∈ . , all polynomials in Iu are divisible by fu,

Theorem. Let f=Xk— c1Xk-1— ...— ck G C[X] with ck=0. Suppose that f factorizes over C as f= (X— «1)ei (X— at)

where a1,. . ., at are distinct, and e1,. . ., et are positive integers. let U={ un }~0 be a sequence in C. Then the following two assertions are equivalent: U satisfies un=c1un-1+c2un-2+...+ckun-k (n ^ k).

There are polynomials f1,. . ., ft G C[X] of degrees at most e1— 1,. . ., et— 1, respectively such that un=^ fh (n)a'n for n ^ 0.

Moreover, the polynomials f1,. . ., ft are uniquely determined by U.

Proof. Take a sequence U with Define the k x k-matrix

(0 1 0 \0 1 0

A 1\ ck ck-1 c1 /

For n ^ 0 let un := (un,. . ., un+k-1)T. Then un+1=Aun for n ^ 0 and thus,

un=Anu0 for n ^ 0.

Check that the characteristic polynomial of A is det (X1— A)=f (X). There is a non-singular matrix C such that A=C-1JC, where J is a Jordan Normal Form of A. We can take

Ji \J = ... V Jt j

where for h=1,. .. , t, Jh is the Jordan block of order eh associated with ah, /ah 1 \ / 1 a-1

This implies that An=C-1 JnC= (Ej (n)^ , where V / i, j=1,. . ., k

Eij (n)=J] fhij) (n)an with ∊ C[X], deg<eh— 1.

By substituting this into and taking the first coordinate, with some polynomials f1,. . ., ft of degrees at most e1— 1,. . ., et— 1, respectively.

The unicity of fi,. . ., ft. Let V be the set of sequences U satisfying Then V is a complex vector space. Its dimension is k, since any k-tuple of initial values u0,. . ., uk-1 ∊ C can be extended uniquely to a sequence U satisfying Next, let W be the set of sequences U satisfying for certain polynomials fi,. . ., ft of degrees at most e1— 1,. .. , et— 1, respectively. Also W is a complex vector space, generated by the sequences { nj0^)^=0, for h=1,. .. , t, j=0,. .. , eh— 1. Note that the number of these generators is e1+...+et=k; so W has dimension ^ k. We have just shown that V C W. Hence W must have dimension equal to k=dim V and so, V=W. This implies the equivalence Further, { nja'n }jj=0, (h=1,. . ., t, j=0,. . ., eh— 1) must form a basis of W=V. Hence any sequence in V can be expressed uniquely in the form.

Corollary. Let again f=Xk— ciXk-1 cfc= (X— ai)e1 ••• (X—
at)et ∈ C[X],

where ck=0, a1,. . ., at are distinct, and e1>0,. . ., et>0, and let U={ un }n=0 be a sequence in C. Then the following two assertions are equivalent:

U is a linear recurrence sequence with companion polynomial f.

There are polynomials f1,. . ., ft ∈ C[X] of degrees exactly e1— 1,. .. , et— 1, respectively such that

t

Un=^ fh (n)a'n for n ^ 0.

Proof. First assume that U has companion polynomial f. Then k := deg f is the length of the minimal recurrence satisfied by U. We know that Un=h=1 fh (n)an with deg f =: e'h— 1 ^ eh— 1 for h=1,. . ., t.

Then again, U satisfies a linear recurrence of length ej+...+et corresponding to the polynomial (X— a1)e'1 ... (X— at)et. So e1+... et ^ k. Hence e'h=eh for h=1,. . ., t.

Conversely, let U={ u, n } with u, n=Yfh=1 fh (n)arn where deg fh=eh— 1 for h=1,. . ., t. By Theorem 7. 1, U satisfies the companion polynomial of U divides f, so it is of the shape (X— a1)e'1 ... (X — at)et with eh ^ eh.

eh— 1, for h=1,. .. , t. Hence e'h=eh for h=1,. . ., t, and the companion polynomial of U is f.

We are interested in the zero set of a linear recurrence sequence,

Zj := { n ∈ Z>0 :, un=^ fh (n)<=0 }.

Equations of the shape Y^h=1 fh (n) n=0 are known exponential – polynomial equations.

Example. Let U be given by

/,. n+1 .. — n — 1 \

Un := 2 (2n+ (— 2)n)+ (n— 1) (—) (. =e2ni/3).

2   \. —. 1 J

By Corollary U has companion polynomial

(X— 2) (X+2) (X —.)2 (X —. — 1)2=X6+2X5— X4— 6X3— 11X2— 8X— 4,

so it is a linear recurrence sequence of order 6.

By considering n=0 (mod 6), n=1 (mod 6),. .. one verifies that

Zjj={ 0, 1 } U { n ∈ : n=5 (mod6) }

(check this). This example was specifically constructed to make it easy to com- pute the set Zj. In case that k := deg fJ ^ 3 and the a and the coefficients of the fi are algebraic numbers there exists an algorithm to determine the set ZJ which is based on lower bounds for linear forms in logarithms. But for k>3 such an algorithm is not known.

Theorem. (Skolem, Mahler, Lech). The set Zjj is either finite, or a union of a finite set and a finite number of infinite arithmetic sequences.

Under an additional hypothesis, it can be shown that there are no infinite arithmetic sequences in ZJ, and thus, that the set of solutions is finite.

Corollary. Let t ^ 2. Suppose that the polynomials fi in are nonzero, and that none of the quotients ai/aj (1 ^ i<j ^ t) is a root of unity. Then the set Zjj is finite.

Proof. Suppose that Zv contains an infinite arithmetic sequence, say { a+dm : m ∈ Z^0 }. That is,

Vm := ^ 9h (m)Pm=0 for all m ∈ Z^o,

Where gh (X)=fh (a+dX)ah, ^h=ah

If any two numbers pi, Pj were equal, we would have (ai/aj)d=1, contradicting our assumption. Hence ^1,. .. , fit are distinct. Theorem implies that the polynomials g1,. .. , gt are identically 0, hence the

Notes

polynomials $f_1,...,f_t$ are identically 0, which is again against our assumption.

To apply techniques from p-adic analysis. For this, we have to map U to a sequence in Q_p.

Denote by $\{ v_1,...,v_m \}$ the set of coefficients of the polynomials $f_1,...,f_t$ and let $K=Q(v_1,...,V_m, a_1,...,a_t)$

be the field generated by the v_i and the a_h, i. ∈ . , consisting of all expressions f/g where f, g are polynomials in the v_i and a_h with coefficients from Q. Clearly, $u_n \in K$ for all n ^ 0. Note that a priori the v_i and a_h are just complex numbers, with the $a_h=0$. So these numbers can be algebraic or transcendental.

First suppose that $v_1,...,v_m$, $a_1,...,a_t$ are algebraic, i. ∈ . , K is an algebraic number field. Similarly as one can embed K in C, one can embed K in any algebraically closed field that contains Q. So in particular, one can embed K in Q_p for any prime number p. Thus, we can map the sequence U to a sequence in Q_p with the same set of zeros, and apply techniques from p-adic analysis on Q_p.

The Chebotarev density theorem from algebraic number theory implies that there are infinitely many primes p such that K can be embedded in Q_p. Thus, by choosing the prime p appropriately, we can work also on Q_p itself instead of an algebraic extension.

Now assume that not all $v_1,...,v_m$, $a_1,...,a_t$ are algebraic. Lech showed that also in this general case, there are infinitely many primes p, such that the field K can be embedded in Q_p. We leave aside the intricate proof of this fact.

Thus, in all cases, the sequence U can be mapped to a sequence of which the coefficients of the polynomials f_h and the numbers a_h all lie in Q_p. In fact, by a careful choice of the prime p we can observe to it that

$f_h \in Z_p[X]$, $a_h \in Z$ for $h=1,...,t$.

This is what we assume henceforth.

The idea of the proof is then to define a power series

u (x) := ^ fh (x)ah

and to apply Theorem 5. 1, to get a hand on the zeros in Zp. The problem is that for this, we have to define ah as a power series and this is not always possible.

In analogy to the well-known expansion over R or C, we define

(1+ft)x=^ for @, x ∈ Zp with \ft\p ^ 1/p,

k=o ^ '

where f x^ x (x— 1) ... (x— k+1) VkJ=k!.

Notice that for x=n a non-negative integer, this coincides with the usual definition for (1+ft)n.

We show that the series converges. Choose a sequence of positive integers xn— x. Then (x")— iff) since also in the p-adic setting, polynomials are continuous. The numbers (X*) are all integers, so (k) ∈ Zp. This implies that I (X)ftk\p<\ftk\p— 0 as k— — <x>. Hence indeed, the series converges.

We want to express (1+ft)x as a power series in x. Put r := 1 if p>2, r := 2 if p =2.

Theorem. Suppose that \ft\p ^ p-r. Then there is a power series expansion

<X> (1+ft)x=^ ck xk which converges for x ∈ Zp.

Proof. Assume that we have shown that \0k/k!\p ^ 0 as k ^ <x>. Let x ∈ Zp. Then

(i+a)x=^ ~k\ x (x -1) ••• (x - k +1)

ro a k k

=akj-xj with akj- ∈ Z

k=0 j=0

Notes

^ f^ ak ^ j = 2. J Lhl akj Jxj.

j=0 \k=j ' /

Interchanging the summations is allowed by Theorem and the expressions between the parentheses converge. This yields our power series expression.

It remains to show that \, 5k/k'\p ^ 0 as k ^ x>. We first estimate \k'\p. Among { 1,. . ., k } there are precisely [k/p] multiples of p which together con- tribute [k/p] factors p to the prime factorization of k!. Further, among these integers there are precisely [k/p2] multiples of p2 which contribute another [k/p2] factors p; and so on. Thus, the maximal power of p dividing k! is

[k/p]+[k/p2]+[k/p3]+... <   -,

and so, \ak/k!\p ^ pk/ (p-1)-kr ^ 0 as k ^ <x>. This completes our proof.

We are now ready to complete. Put again r=1 if p>2 and r=2 if p=2. Further, set D=p— 1 if p>2 and D=2 if p =2. Then the unit group (Zp/prZp)* has order D. This implies that = 1 (modpr), i. ∈ . , =1+ah with \ah\p ^ p-r. We now split up Zj into residue classes modulo D, i. ∈ . , we consider the sets

Za := { m ∈ Z^0 : ua+Dm=0 } for a=0,. .. , D— 1.

Now indeed,

Ua (x) := ^ fi (a+Dx)ah+Dx=^ f (a+Dx)a<= (1+^h)x

is a power series converging on Zp with ua (m)=ua+Dm for m ∈ Z^0. By Theorem, ua (x) is either identically 0, or it has only finitely many zeros on Zp. This implies that either Za=Z^0, or is finite. As a consequence, the solution set is indeed the union of a finite set and finitely many infinite arithmetic sequences.

An important problem is to estimate the cardinality of the finite set and of the number of arithmetic sequences that occur in the set of solutions of. The following result is due to W. M. Schmidt. Let U be a linear recurrence sequence in C of order k. Let A (U) denote the cardinality of the finite set in Zjj, and B (U) the number of arithmetic sequences in Zj. Then

A (U)+B (U) ^ exp exp exp (20k).

The importance of this bound is that it depends only on k and not on any other parameter. It is very likely far from best possible. Schmidt's very difficult proof does not use p-adic analysis like above, but is based on Diophantine approximation.

We give an application to cubic Thue equations. Let f (X)=X3+aX2 + bX+c be an irreducible polynomial in Z[X] with one real root, say a1 and two complex roots a2, a3=a2. Consider the equation

F (x, y)=x3+ax2y+bxy2+cy3=1 in x, y G Z.

Let K=Q (aq). Then K is a cubic field with one real embedding and two complex embeddings. Then the unit group O*K has rank 1. That is, there is pi such that O*K={ ±nl : n G Z }. Let (x, y) be a solution of The conjugates of x— a1y are x— aiy for i=1, 2, 3. Hence 3

Nk/q (x— aq y)=JJ (x— o^y)=F (x, y)=1.

So x — a1y is a unit, i. ∊ . , x — a1y=±nn for some n G Z. Then also x — aiy=±n™ for i=1, 2, 3. We use the identity

(02— a3) (x— a1y)+ (03— a1) (x— a2 y)+ (01— «2) (x— 03 y)=0.

This implies

(a2— a3)hl'+ (a3— a1)n2+ (a1— a2)h3=°.

We leave as Exercise to prove that none of the quotients yi/yj (i=j) is a root of unity. Then by Corollary this last equation has only finitely many solutions n G Z^q. We prove in the same manner that there are only finitely many solutions n<0 by applying again, but now with n-1 instead of n and taking n' := — n>0. As a consequence, the equation F (x, y)=1 has only finitely many solutions.

Check your Progress-2

Discuss Algebraic Extensions Of Qp

____

____

____

9.9 LET US SUM UP

In this unit we have discussed the definition and example of Analytic Functions Over P-Adic Fields, Zeroes Of A Power Series, Criterion For The Rationality Of Power – Series, P-Adic Power Series, Algebraic Extensions Of Qp, Study Of The Algebra Of Spherical Functions, The Zero Set Of A Linear Recurrence Sequence

9.10 KEYWORDS

Analytic Functions Over P-Adic Fields….. stated K will denote a completed valuated field with a real valuation v

Zeroes Of A Power Series ….. Let /'=X be a power series over K. Let p (f) =7_1, ""inf— —

Criterion For The Rationality Of Power – Series….. Let F be any field and f=Y*TO=0 akX an element in F[[x]].

P-Adic Power Series…… The completion R of Q with respect to the ordinary absolute value has only one non-trivial algebraic extension, namely C .

Algebraic Extensions Of Qp ….. Study Of The Algebra Of Spherical Functions….. Let M be the unity representation of K and Let A be the algebra Lm (G): by our results, this is a commutative algebra. It observems possible

The Zero Set Of A Linear Recurrence Sequence….. The Norwegian mathematician Thoralf Skolem introduced techniques from p-adic analysis to prove results on Diophantine equations

9.11 QUESTIONS FOR REVIEW

Explain Analytic Functions Over P-Adic Fields

Explain Algebraic Extensions Of Qp

9.12 REFERENCES

p-adic numbers: an introduction by Fernando Gouvea

p-adic Numbers, p-adic Analysis, and Zeta-Functions, Neal Koblitz (1984, ISBN 978-0-387-96017-3)

A Course in p-adic Analysis by Alain M Robert

Analytic Elements in P-adic Analysis by Alain Escassut

9.13 ANSWERS TO CHECK YOUR PROGRESS

Analytic Functions Over P-Adic Fields

(answer for Check your Progress-1 Q)

Algebraic Extensions Of Qp

(answer for Check your Progress-2 Q)

UNIT-10 : ZETA-FUNCTIONS

STRUCTURE

10.0 OBJECTIVE

After studying this unit, you should be able to:

- Understand about Zeta-functions
- Understand about Fields of finite type over z
- Understand about Convergence of the product
- Understand about Zeta function of a prescheme
- Understand about Zeta function of a prescheme over fp
- Understand about Zeta function of a prescheme over fq

- Understand about Reduction to a hyper-surface
- Understand about Algebraic And Topological Properties

10.1 INTRODUCTION

In mathematics, p-adic analysis is a branch of number theory that deals with the mathematical analysis of the functions of p-adic numbers.

Zeta-functions, Fields of finite type over z, Convergence of the product, Zeta function of a prescheme, Zeta function of a prescheme over fp, Zeta function of a prescheme over fq, Reduction to a hyper-surface, Algebraic And Topological Properties

10.2 ZETA-FUNCTIONS

It is well known that the Riemann zeta function Z (s)=n (1 - P-s)-1,

P where p runs over all prime numbers, is absolutely convergent for Res >. We can generalise this definition for any commutative ring with unit element. In the case of ring of integers p is nothing but the generating element of the maximal ideal (p) and it is also equal to the number of elements in the field Z/ (p). Motivated by this we define for any commutative ring A with identity

Za (s)=f[(1 - N (M)-s)-1 /klcf57h]' “P l M

where M runs over the set of all maximal ideals of A and N (M) is the number of elements in the field A/M. But in general N (M) is not finite and even if N (M) is finite the produce (I) is not convergent, therefore we have to put some more restrictions on the ring. In the following we shall prove that if A is finitely generated over Z i. ∈ . , if there exist a finite number of elements x1, , xk in A such that the homomorphism from

$z[x_i, \ldots, X_k$ to A which sends X' to X_j is surjective, then N (M) is finite and the infinite product (I) is absolutely convergent fot Re s>dim A, where the dimension of A is defined as follows.

Definition. If A is an integral domain, the dimension of A is the tran- scendence degree (respectively transcendence degree +1) of the quotient

field of A over Z/ (p) (respectively Q) if characteristic of A is p (respectively 0). In the general case dim A is the supremum of the dimension of the rings A/Y where Y is any minimal prime ideal.

It can be proved that dimension of A is equal to the supremum of the lengths of strict maximal chains of prime ideals. Before proving the convergence of the zeta function we give some examples of finitely generated rings of over Z.

The ring Z is finitely generated over itself.

Any finite field F_q.

The ring of polynomials in a finite number of variables over F_q i, ∈ . , the ring $F_q[X_1 X_k]$

The ring $F_q[X_1, \ldots, X_r]/U$, where U is any prime ideal of $F_q[X_1, \ldots, X_r]$. This is the set of regular functions defined over F_q on the variety V defined by the ideal U affine space.

Let K be any algebraic number field. The ring of integers A in K is finitely generated over Z.

Let V be an affine variety defined over the algebraic number field K and let O c $K[X_1, \ldots, X_r]$ be the ideal of V. Then the ring of regular functions on V i. ∈ . , $K[X_1, \ldots, X_r]/O$ is not finitely gen- erated over Z.

But the ideal O is generated by the ideal O_0 = O n $A[X_1, \ldots, X_r]$ of the ring $A[X_1, \ldots, X_r]$ and we can associate to Vthe quotient ring $A[X_1; \ldots, X_r]/O$ which is obviously finitely generated over Z. It is to be noted that this ring is not intrinsic and depends on the choice of the coordinates in Kr

10.3 FIELDS OF FINITE TYPE OVER Z

We shall require the following Theorem in the course of our discussion.

Normalisation Theorem of Noether. Let K be a field. Let R and S be subrings of K containing a unit elements such that S is finitely generated over R. Then there exists an elements a+0 in R and a finite number pf element X1, . . ., Xr in S such that

X1, . . ., Xr are algebraically independent over the quotient fields of R.

Any elements of S is integer over R[a-1, X1, . . ., Xr].

Proposition. Let K be a field. Let R be a subring of K and L the quotient field of R. If K as a ring is finitely generated over R, then (K : L) is finite and there exists an element a in R such that L=R[a-1].

We first prove the following: If a field K is integral over a subring R then R is a field.

Let x be any element of R, then x-1 belongs to K and therefore satisfies an equation

Xn+a1 X"-1+•••+an=0, ai ∈ R

This implies that x-1 is a polynomial in x over R. But R[x]=R, therefore x-1 belongs to R. Hence R. Hence Ris afield Proof of proposition 1. Since K is finitely generated over R, by the normalization Theorem, there exists an element a+0 in R and a finite family (x1, . . ., xr) in K algebraically independent over L such that K is integral over R[a-1, x1;.. ., xr]. By the remark above it follows that R[a-1, x1, . .. , xr] is a field. But x1, . .. , xr are algebraically independent over L, therefore r=0 and L=R[a-1]. Since K is finitely generated and integral over L, (K : L) is finite.

Proposition. If a commutative ring A is finitely generated overZ, then WN (M) is finite for any maximal ideal M of A.

Notes

Proof. Since A is finitely generated over Z, the field K=A/M is finitely generated over Z. If characteristic of K is zero then K contains Z. Therefore by proposition (1) Q=Z (a-1) for some a ± 0 and a in Z, which is impossible. Thus characteristic of K is p and by proposition K is a finite extension of Fp, hence K is a finite field.

10.4 CONVERGENCE OF THE PRODUCT

Proposition. The infinite product Za (s) is a absolutely convergent for Re s>dim A and uniformly convergent for Re s>dim A+s for every s> 0.

Proof. We shall prove the result by induction on r=dim A. If r=0

Lai 1 Za (s) =1 - q~s

is a meromorphic function in the plane with a simple pole at s=0. Let us assume that the result is true for all those rings which are finitely generated over Z and dimension of which are less than r. Before proving the result for rings of dimension r we prove the following result.

Let A be a finitely generated ring over Z and B=A[X], the ring of polynomials in one variable over A, then Zb (s)=Za (s - 1) in a suitable domain of convergence. In fact if Za (s) is convergent for Re s>x, then Zb (s) is convergent for Re s>x+1.

If dim A=0, then A=Fq for some q and B=Fq[X]. Since he maximal ideals in B are generated by irreducible polynomials, which can be assumed to be monic, we get

Zb (s)=f[(1 - qsd (p))-1

where P runs over the set of monic irreducible polynomials over A. In order to prove the absolute convergence of Zb (s), it is sufficient to prove the convergence of the infinite series

where s=t+it

Since the number of monic polynomials of degree r is qr, we have

TO* = ∈ |q-d (P)|T <<= qr|q-r|T^ q (1 - &)r r=1

Obviously the series S is convergent if 1 - <r<0 i. ∈ . , <r>1. More- over in this domain

Zb (s) = (Q a monic polynomial inB)

Q q h- y — =y — Z — i nsk Z — i nKs~

qsk k=0qk (s-1) 1 - q1-s

Hence

ZB (s)=<=a (s - 1).

Now let the dimension of A be arbitrary and B=A[X \.

We shall denote by Spm (B) the set of maximal ideals of B. For any M in Spm (B), M n A is in Spm (A), because A/M n A, being a subring of the finite field B/M, is a field. Let n denote the mapping M ∈ Spm (B) —>M n A ∈ Spm (A). It can be easily proved that the set n-1N and Spm (A/N[X) are isomorphic, where N is any maximal ideal of A. Therefore

Zb (S)=n [1 - (N (M))-s\-1

meSpm (B)= n 11 (1 - N (m)-s)-1

neSpm (A) men-1 (n)= 0 ZA/M[X] (s)

neSpm (A)

But A/N is a finite field, therefore Za/N[X\s=Za/N (s - 1)

So we get

ZB (s)=Y\ (ZA/n (s - 1))

neSpm (A)= Y\ (1 - N (N)1-s)-1

neSpm (A)= Za (s - 1).

It follows that ZFq (s)[Xu.. ., xk\=| and Zz[Xu.. ., xK]=Zz (k- s)

where Zz is nothing but the Riemann zeta function.

Notes

Now we shall prove our main proposition. Assume that A is an integral domain.

Let K be the quotient field and R the prime ring of A.

Since A is finitely generated over R, by the normalisation Theorem we have the following:

If characteristic A=p ± 0, then there exist r elements x1; x2, . . ., xr in A such that A is integral over R[x1, . . ., xr], where x1, . . ., xr are algebraically independent over R=Fp. (ii)- If characteristic A=0, then there exits an element a in R=Z and r - 1 elements x1;.. ., xr-1 in A such that every element of A is integral over Z[a-1, x1, . .. xr-1] and the elements x1, . . ., xr-1 are algebraically independent over Q.

We get r elements in the first case and r - 1 elements in the second case because r is the dimension of A which is equal to the transcendence degree of K over Fp or transcendence degree of K over Q+1 according as the characteristic of A is non-zero or not. It can be proved that A (respectively A'=A (a-1)) is a finite module over B=Fp[x1;.. ., xr] (respectively B=Z[a-1, x1, . . ., xr-1]) and the mapping n from Spm (A) ^ Spm (B) (respectively from Spm (A') ^ Spm (B)) is onto. Let A (respectively A') be generated by k elements as a B (respectively B) module. We shall prove that n-1 (N) for any N in Spm (B) (respectively in Spm (B)) has at most k elements. Let C=A/AN. It is an algebra of rank t<k over B/N. Since n-1 (M) is isomorphic to Spm (A/AN) it is sufficient to prove that C has at most k maximal ideals. This will follow from the following.

Theorem Let A be any commutative ring with identity and (Ui1<Km a finite set of prime ideals in A such that

A=Ui+Uj for i+j

Then the mapping Q : A ^ P = n AUi is surjective

Proof. It is sufficient to prove that 1=Y ai where aj belongs to Uj for

j+i because if (t1, . .. , tm) is any element of P, then | m \

I=t'ian= (t1, . . ., tm), where ft is a representative of ti in A.

If m=2, the result is obvious i. ∈ . , 1=a1+a2 where a1 is in O2 and a2 is in O1. Let us assume that it is true for less than m ideals.

m-1 Then 1=Y Vi where Vi ∈ Oj for 1<j<m - 1 and j+i. Since

A=Oi+Om, we have 1=xi+yi for 1<i<m - 1 with xi ∈ Om and

m- 1

e Oi. Clearly Y xv+Y viYi=1.

Let us take Uj=vx for i<i<m - 1 and um=Y yvi, then

ui=1 and ui ∈ Oj for j ± i.

Let M1, M2, . . ., Mt be any finite set of distinct maximal ideals of C.

tt

Then by Theorem C/- P| M is isomorphic to C/M/ indicates the direct sum). Thus t<k.

Assume that the characteristic of A is 0. Let M be any maximal ideals of A. If a does not belong to M, then MA[a-1] is a maximal ideal in A[a-1], because A[a-1]/MA[a-1] is isomorphic to A/M. If a belongs to M, then M contains one and only one prime Pi occurring in the unique factorisation of a and the set of maximal ideals which contains pi. is isomorphic to Spm (A/piA). Therefore if a=p^1, . . ., patt, then

Za (s)=ZA[a-1] (s) n Z (s)

i=1 A/PiAyg[5

But dim A/p^A<dim A, therefore inorder to prove the convergence k[. of Za (s) it is sufficient to consider ZA[a-1] (s). We have

ZA[a-1] (s)=n n (1 - (^M)-5)-1

n Spm (S') ne-1n (n)

Since N (M)>N (M), we get

^ ^ |NMr<k Y, N«r<kUr - <r - 1)

neSpm (<=) nen-1 (M)   neSpm (5')

Therefore ZA[a-i] (s) is convergent for %s>dim A.

If characteristic A=p, then we get

^ ^ |NMr<k Yj |NNr<kZFp (r - s)

neSpm (<=) men-1 (n)   neSpm (5')

which gives the same result as above Now we have in the general case (A is not an integral domain).

10.5 ZETA FUNCTION OF A PRESCHEME

Let A be a commutative ring with unity. We shall denote by Sp (A) the set of all prime ideals of A. On Sp (A) we define a topology by classifying the sets F (O) as closed sets, where

F (O)={ Y|Y d O, Y ∈ Sp (A) }.

and O is any ideal in A. This topology is referred to as the Jacobson Zariski topology. It is obvious that in this topology a point is closed if and only if it is a maximal ideal of A. We associate with every point Y of Sp (A) a local ring A namely the ring of quotient of A with respect to the multiplicatively closed set A - Y. On O the sum of all these local rings we define a sheaf structure by giving "sufficiently many" sections. For any a, b, e, A we consider the open subset

V (b)={ Y|Y ∈ Sp (A), Y t b }.

For any Y ∈ \{ h), (-] the, fraction is an element of Y. Then V b! yb the mapping Y — » (-) gives a section S (a, b) of 0. The pair (X, ff) bY

together with the sheaf of local rings O is known an affine scheme, where X=Sp (A).

Definition. Let (X, O) be a ringed space. We say that Xis a prescheme if every point has an open neighbourhood which is isomorphic as a ringed space to Sp (A) for some ring A. Such a neighbourhood is known an affine neighbourhood.

We shall assume that the pre-scheme X satisfies the ascending chain condition for open sets, then X is quasi-compact and it can be written as the union of a finite number of affine open sets X- We shall denote by Aj the ring such that X is isomorphic to SpA). Then the ring Aj is Noetherian and has a finite number of minimal prime ideals Yjj. Each prime ideal of Aj contains a Yjj and X=SpA) is the union of the sjj=SpAj) (with Ajj)=Aj/Yjj), each Sj being a closed subset of X and the Aj being integral domains. Moreover the residue field of the local ring associated to a point x $\in$ Sj is the same for the sheaf of the scheme X and for the sheaf of the scheme Sp (Aj)

We define the dimension of X as the maximum of the dimensions of the rings A/or of the rings Aj). It can be proved that if X is irreducible (i. $\in$. if X cannot be represented as union of two proper closed subsets). then Aj=dim Aj for i+J.

A prescheme S is a finite type over Z if there exists a decomposition of S into a union of a finite number of open affine sets X such that each Aj, the ring associated to X, is finitely generated over Z. It can be proved that the same is true for any decomposition into a finite number of affine open sets. In particular, a ring A is finitely generated over Z if and only if the scheme Sp (A) is of finite tyte over Z and an open prescheme of S is also of finite type over Z.

Let S be a prescheme of finite type over Z. A point x $\in$ S is closed if and only if the residue field of the local ring of x is finite (we shall denote by N (x)) the number of elements of this field). In particular, if S=UX., then a point x $\in$ Xj is closed in S if and only if it is closed in X Now we define the Z-function of S by:

Zs (s)=f[(1 - (N (x))-s)-1

where x runs over the set of closed points of S. It is clear that if S=Sp (A), then Zs=Za- As above, we can write S as a union of a finite number of subsets Sj, each Sj being affine open subset, with

Sj=SpA), where Aj is an integral domain finitely generated over Z. Then it is obvious that:

| n <=s] |<n CsinSjnS* j ...)

Cs=u !\i<j<k ^ / n Z SinS I<j

Now we shall prove the following generalization.

The Z function of a prescheme S of finite type over Z is convergent for Re s>dim S.

Of course bis for prescheme of dimension<dim S. Then we get as in the preceding the convergence of Za for any integral domain A finitely generated over Z of dimension<dim S, and in particular the convergence of the Zst. After (I), we have just to prove this: if U (resp. F) is an open (resp. closed) subset of X=Sp (A) (with dim A < dim S), then ZUnF is convergent for Re (s)>dim S. But let G=X- U; we have:

ZunF=ZF/ZFnG

and F n G is closed in X. Hence we have just to prove the convergence of Zf. But F is defined by an ideal of A and F=Sp (A/O) and Zf = Za/o. If O={ 0 }, we have Zf=Za and if O+{ 0 } then the minimal prime ideals of A/ O give non trivial prime ideals of A and we have dim A/O<dim S : the induction hypothesis ensures the convergence of ZF.

Check your Progress-1

Discuss Zeta – functions

____

____

____

10.6 ZETA FUNCTION OF A PRESCHEME OVER F_P

Let S be a prescheme over Z of finite type. We have a canonical map from a prescheme S to Sp (Z) given by n (x)=characteristics of the residue field of local ring of x for any x in S. Suppose that n (x)=p for every x in S. In this case each Aj is of characteristic p and the canonical map from Z into Aj can be factored through Fp. In this case we say that the prescheme S is over Fp.

Let S be a prescheme of finite type over Fp. Then the residue field k (x) of the local ring associated to a closed point x is of characteristic P for every x in S. Therefore k (x)=Fpdx) where d (x) is a strictly positive integer. thus

& (s)= n (i-p~sd (xyi) ~x=xeS

Let us take t=p~s. Then

cs (s)= n (i ~^~i)=cs (t).

x=xeS

The function Zs (t) is also known a zeta function on S. It is absolutely convergent in the disc |t|<p~dim (s). we have

x=xeS k= 0 h=0

with a0=1 and an $\in$ Z. The end of these lectures will be devoted to the following theorem (Dwork's theorem):

Theorem. The function lis (t) of a prescheme S of finite type over Fp is a rational function of t.

10.7 ZETA FUNCTION OF A PRESCHEME OVER F_Q

In order to prove Dwork's theorem it is sufficient to prove it for an affine scheme and open sets of an affine scheme because of the equation.

Then we have to look at thezeta function of a ring A finitely generated over Fp. Such a ring can be considered as the quotient of Fp[X1 Xk] by some ideal O and we can associate to A the variety V defined by O in Kk where K is the algebraic closure of Fp. It can be noted that V is not necessary irreducible. We shall call Za the zeta function of the variety V.

More generally we consider a variety V over Fq, where q=pf. The variety V is completely determined by the ring

A=Fq[X1, . .. Xn\/O n Fq[X1, . . ., Xn] where O is an ideal in K[X1, .. Xn\ generated by O0=Fq[X1, . . ., Xn\ n O K being the algebraic closure of Fq. We define

Zv=Za and Zv=Za.

For every maximal ideal M of Fq[X1;... Xn\ there exists a maxi- mal ideal M in K[X1, . . ., Xn\ such that Fq[X1, . . ., Xn\ n M'=M. But

Spm (K[X1, Xn\) is isomorphic to Kn, therefore a maximal ideal M of

Fq[X1;.. ., Xn\ is determined by one point x of Kn. Moreover this point x belongs to V if and only if M d O However this correspondence be- tween the maximal ideals of Fq[X\ and the points of Kn is not one-one. So we want to find the condition when two points x and y of Kn cor- respond to the same maximal ideal of Fq[X1;.. ., Xn\=Fq[X |. Let Mx and My be the maximal ideals of K[X| corresponding to x= (x1, . . ., xn) and y= (y1, . . ., yn) respectively such that Mx n Fq[x\=My n Fq [x \. It is obvious that Fq[X\ /Mx n Fq[x\=F[x\/My n Fq[x\ is isomorphic to Fq [x1;.. ., xn\=Fqf for some f>0. We shall show that the necessary and sufficient condition that Mx n Fq[X|=My n Fq[X| is that there exists an element u in G (Fqf/Fq) such that u (x)=y. For n=1 the existence of u is trivial.

Let us assume that there exists a u in G (Fqf/Fq) such that u (xi)=yi for i=1, 2, . . ., r - 1 for<n. Let u (xj)=zj for j>r. Let P (x) be the polynomial of zr over Fq (y1, . . ., yr-1). Then P (y1, . . ., yr-1zr)=0, which gives on applying u the equation P (x1, . . ., xr-1, yr)=0. Therefore P is in My n Fq[X\ i. ∈ . , P (y1, . .. yr-1, yr)=0. Thus yr and zr are conjugate over Fq (y1, . . ., yr-1). Let t be the automorphism of K over Fq (y1, . . ., yr-1) such that T (ar)=yr. Then tou is an element of G (Fqf /Fq) such that tou (xj)=yi for i=1, 2, . . ., r. Our result follows by induction. The converse is trivial. Hence we observe that if M is a maximal ideal of Fq[X| containing O with N (M)=qf, then there exist exactly f points conjugate over Fq, in Kn n V and f= (Fq (x) : Fq) if and only if f is the smallest integer such that x belongs to (Fqf)n.

Let Nf=number of points in V n (Fqf)n

Jf=number of points in V n (Fqfqf)n - U (V n (Fqf)n)

If=number of maximal ideals of A of norm q.

We have proved that Jf=fIf. By definition of the Z- function of V we have

Zv (s)=Za (s)=n (1 - (nM)-s)-1

meSpm (A)= Y\ (1 - q-sf (M))-1

meSpm (A)

where f (M) is defined by the equation N (M)=qf (M) So we observe that we can substitute t=q~s in the zeta function (and not only t=p~s as in the general case) and get a new zeta function. Zv (s)=f[(1 - tf (M))-1=f] (1 - tf)-If=Zv, q (t)

meSpm (A) f=1

Therefore

Log Zv, q (t)=J] -If log (1 - tf) f=1

TO TO Af f=q k=1

_ y1 y1 tkf= VVTT

fn=n=1

TO= Z N- f

Thus Cv. tid) exp X N,, — , where N,, is the number of points of V

in Fq. We have already observen that this is a power series with integral coefficients.

Theorem. Zv, q (t) is a rational function oft.

Notes

We shall show that in order to prove the rationality of ZA (t) where t=q-s, it is sufficient to prove the rationality of Za (t) where t=p~s. Since ZV, q (t) and ZV (t) are both convergent in a neighbourhood of the origin, we have

ZV, q (tf)=ZV (t) with q=pf.

Let u be any f-th root of unity. Then

ZV (jUt)=ZV, q (U ftf)=ZV, q (tf)=ZV (t)

If we have U) XUW

then also , =Z, (ZLo b^k

/U Z, ZLo<Vf* _ Zto MZ^V ZLo c&pnW

Ho<k<[n/ f] bkftkf

Z0<k<[n/f] Ckftkf

Uk=0 if k ∈ 0 (mod f)

Thus we get

Z bkftkf_? (/)

0<k<[n/ f]

Bkftk ~ 0<k<[n/ f] = ∈ ctft» 0<k<[n/ f]

Hence ZVq (t) is a rational function of t.

10.8 REDUCTION TO A HYPER-SURFACE

We shall show that to prove our theorem it is sufficient to consider the zeta function of a hypersurface V defined by a polynomial P (X1Xn)

in Fp[X1, . . ., Xn]. We know that we can write V=P| Vi where each Vi

is a hyper surface. Let ∈ be any subset of { 1, 2 , r } and Ve=Pi V.

ie E

Let Nv (respectively Nve) be the number of points of V (respectively Ve) in any field FPn. We now prove that

Nv=^ (-1)1+n (∈) NVE

where n (∈) is the number of elements in ∈ .

Let any point x in V belong to k hypersurface Vj where 1<k<r. Then x appears l times in the right hand side of equation (I), where

I=r-kC00kC1 - (r-kC0kC2+r-kC^+•••+ (-1)s+1

(kCs+r-kC1kCs-1+.. . +kChr-kCs-h+.. .)+.. .

= X r- kC, X (-1)h"-'Ch

<= (_1)f-1 r-kC,

Thus I=0 or 1 according as r<k or r=k. Hence the equality is established. This proves that

Zv (,)=n^VE (,)] (-1)1+n (∈)

This proves that it is for a hypersurface.

Let V be a hypersurface defined by the polynomial P (X1, X2, . .. Xn) in Fp[X1;... Xn]. Let Bbe any subset of { 1, 2, . . ., n }. Let

Wb={ x| x ∈ V, xj=0 for i not in B }

Ub=|x|x ∈ Wb, J~[Xi=0

It is obvious that V is union of disjoint subsets Wb - Ub where B runs over all the subsets of { 1, 2, . . ., n }. Hence the zeta function of V is the product of the zeta functions of the varieties (Wb - Ub) and that will be a consequences of the following Theorem.

Theorem. Let P be a polynomial in Fp[X1, . . ., Xn]. then the zeta function of the open subset defined by n X=0 in the hyper surface W

defined by P is a rational function.

Computation of Nr

Notes

We shall adhere to the following notation throughout our discussion.

X= (X1... ., Xn+1), Xi ∈ Fp. a= (a1, . . ., an+1), ai ∈ Z.

x=xa ••• xx n+1

|a|=«1+«2+...+ n+1.

Let x be any additive character of Fpr. Then we have ^ x (UPX1, . .. , Xn))=0 if P (X1, . . ., Xn)*0

UeFpr

= p if P (X1, . . ., Xn)=0

Therefore

z z x (UP (X1, . . ., Xn))=pNr

X1 eF'pf UeFpr

where pNr= (p - 1)n+^ n+1x (Xn+1 P (x1,. . ., Xn))

Xe (F'Pr)

Let

Xn+1 P (Xi, . Xn)=^ aa X

where only a finite number of aa are nonzero. Then

X (Xn+l P)=Y\ X (aaXa).

Therefore pNr= (p - 1)n+x n X (aa, . . ., X)

XE (F'pf)n+1 a

We take the character X defined by X (t)=n <p (tp). where k= 0

1.0.1 f ∈ Rr such that /'=/ and <p (y)=F (C - \, y), C being a primitive pth root of unity. Thus from equation we get

pfNr= (pr - 1)n +^ n n ^ (ba^x<= (Ppr)n+1 a k=0 where=xh F, ∈ X*, ba=aa and ba belongs to W \. Let

G (§)=["[<p (ba§a~) and Gr (§)=f[G (^).

Then

pfNr= (p - 1)n+^ GJg)

fe (R;)n+1

We have already proved that G (^) is analytic for ^ integral. Therefore

Gr (^)=^ graP

aeZn+1

Then

pNr= (p - 1)n +2 G (<=)

fe (Rp)n+1 = (/ - 1)n+^ gra ^ T

aeZn+1 fe (Rp)n+1

(p - i)n+z &n z &

aeZn+1 i=1 V i

But 2 ^i=0 if ai ∈ 0 (mod p - 1)

= p - 1 if ai=0 (mod p - 1) Therefore

PN= (P - 1)n +2 ga (P - 1)

a= (p -1)

= (P - 1)n+^ gpra-a (P - 1)n+1

Trace and Determinant of certain Infinite Matrices

[X1, . .. , Xn+1]

power series in n+1 variables over K. Let H=Z haXa by any element

a of A. We define an operator Th on A as follows

Th (H)=HH for every H inA.

For any integer r we define an operator Ar Such that

Notes

Let K be any field and A=K

taa X* =2 ara X*.

It can be easily proved that these two operators are continuous for the topology given by the valuation on A defined earlier. Let us set rH, r=Ar o Th. It is obvious that the monomials constitute a topological basis of A and the operator rH, r has a matrix (yap) with respect to this basis, where yap=hra-p. It is trivial to observe that Thh=Th ◦ TH for any

two elements H and H of A and Arr>=Ar o A'r for any two integers r and r. Moreover we have

rH, r=ArS o THHf) — HlS-1

where Hr) (X)=H (Xr).

In order to prove the above identity it is sufficient to prove that the action of the two sides is the same on the monomials. We have TH0Ar (X3)=0 if S is not a multiple of r

Th o Ar (X'r)=T/fX^) if jS is a multiple of r

ra +jfi

with the convention that coefficient of X r=0 if r does not divide s.

Therefore

Th o Ar (Xs)=Ar=Ar o <H)

Thus

rH, r=Ar o Th o Ar o Th = Ar o Ar o TH (r) o TH = Ar2 o TH, Hr)

Let us assume that we have proved that

r' H, r=ArS o THoH (r)o... oH (rs-1)

Then

rH;1=rsH, rorH, r=AjsThoH2•••oH oa°°Th

= ArS Tho Th (2) TH (rS-1) o Ar o Th

= ArS+1 Th ∘ Trfr) O ... O Ttf (rs)

We observe immediately that r^r is an operator of the same type as rHr namely rsHr=PH O r where r=Is and H=H Hr)... Hr 1).

Theorem. Let us assume that K=O the complete algebraic closure of Qp and r=pf. Let us further assume that the coefficients ha tend to 0 as |a| tends to infinity. Then the series Tr (rH-r) = ∈ (rHr)aa giving the

, a, trace of r with respect to the basis (Xa) is convergent and we have

= ∈ m H (p")

V ' fe (R*fs)n+1 Proof. For any monomial X3 in K[[X1, . . ., X^+1]]

ThAX3)=Ar O^ haX

= ∈ harX+ a

Therefore the matrix of the operator rH, r with respect to the basis (X3) is (jap) with

TayS=hra-p and Tr (^ H, r)=Z hra-a. But ha tends to a 0 as|a|tends to infinity, therefore the series Z hm-a is convergent in a K. We have already proved that

Y^H (p)= (r - 1)n+12 hra-a

Therefore

T' (V"-')= (r_\)n+l Z H (P)

V ' pr-l =1

Hence our Theorem is proved for s=1 for s>1, r^r is of the same type as rH, r Thus our Theorem is completely established.

Corollary. psNs= (ps - 1)n+ (ps - 1) Tr rs where r=fc, p we have already proved that psns= (ps - 1)n)

fe (^,)n+1 k=0

Notes

Therefore the corollary follows from the Theorem.

Meromorphic character of ^V (t) in O

We have observen that

Zv (t)=exp n+1

Ns=^ H (-1)n-ips (i-1)+^+ M (-1)n+1-i'ps (i-1) Trr

i=0 \i' i=0 x 1 ' i=0

Therefore o ts

where A (t)=exp I - X— Tr P s=1 s

So in order to prove that ZV (t) is meromorphic in O, it is sufficient to prove that A (t) is every where convergent in O.

If r were a finite matrix, then its trace is well defined. If the order of the matrix is N, then N Tr r5=^ dSare the eigen values of r.

Moreover

A (t)=exp = det (I - tf)

If r is an infinite matrix, we define det (I - tr)=2 dmtm, where

m=0 dm= (-1) ^ ^ eajil 7i^ (1).. . 7imV (m)

1<i'1<<im o

so being the signature of any permutation o in sm. Then for r=rg, p we get

dm= (- 1)m '2 Y-i So7«1 «o (i)... Yamao (m)ai being distinct.

ai 1<i<m oes,

Let us assume that there exists a constant M such that

v (ga)>M |a|. Then

v (jap)=v (gpa-p)>M|pa -5 | > M (p|a |-| 5 I)

We consider one term of the series giving dm mm n YajYo (j) =Yj <Yajao (j)) j=1

M^p|aj|-|a^ (j) |J M (p - 1)^ a j

Now there exist only a finite number of indices ai such that their length|a|is less than some constant, therefore the series dm converges.

Moreover we get v (dm)>M (p - 1) inf ^ a j where infimum is taken

over all the sequence a1, . .. , am. Let pm=inf 2|aj |. Now let us

order the sequence of indices a ∊ Zn+1 in such a way that|ai |<| ai+1 |,

then we have pm = ∊ I ai|and we observe immediately that

lim — =V* ai=co m^<tt m

Therefore tends to infinity as m tends to infinity. Hence we get

the following Theorem.

Theorem If an element G = ∊ gaX satisfies the condition

aeZn+1 (C) v (ga)>MI a |

then the series det (/ - tr) with r=rG is well defined as an element of Q[[t.]] and is an every where convergent power series in Q.

It is evident from the above discussion that if we prove that

The function G defined by=n<p (aa^a) satisfies the condition (C)

/ ~ Is Tr rs \

The formal power series exp - and det (I - /T) are \ s=1 s) identical.

Then A (t) is every where convergent in O which implies that <=v (t) is meromorphic in O. when r is a finite matrix.

Let rh denote the matrix of first h rows and columns of r.

Then et (I - tTh)=exp -^ s=1 = ∊ df

where= (- 1)m 2 7h vm ... 7^, •, being an element of m.

Notes

<i1 <i2<... <im<h { m'

Therefore m'•= - ∈ f Vm=0

We shall show that dm converges to dm and Tr rsh tends to Tr rs as h tends to infinity. We have

dm - dm= (-1) ^ ^ d1 a^ (1) ... «m«^ (m) 1 a,, &em

Obviously v (dm-dfy tends to infinity as h tends to infinity. Similarly /Tr rs – Tr rsh=v 1-a2 - a1 ^ gpa1 -a2 a1 •••as <h

tends to infinity as h tends to infinity. In order to prove that the function G satisfies it is sufficient to prove that each term ^ (aa^a) of

the product satisfies. We have

<p (t)=F (Z - 1, t)

But F (Y, t)=Am (Y)tm with Am (Y)=YmBm (Y) and Bm (Y) belongs

m=o to O[[Y]]. Therefore

v (aan = ∈ (Z - 1)mBm (Z - 1) (a«Za)m

m=0 a h<^- i=0

Thus hp=0 if p+am

- (Z ~ l>Bpja (Y - 1)aa- which shows that

'=(' 1)W |a| p - 1 \p - 1 |a|/

Because Bp/a (Z - 1)^" is of positive valuation. Hence G satisfies.

We have proved that Zv (t) is convergent in a disc |t|<S<1 as a series of complex numbers and is meromorphic in the whole of Q, therefore by the Criterion of rationality proved earlier we obtain that Zv (t) is a rational function of t.

10.9 ALGEBRAIC AND TOPOLOGICAL PROPERTIES

We recall the definitions of the valuation ring

o={ x G K|v (x)>0 }={ x G K ||x|<1 },

the units

u={ x G K|v (x)=0 }={ x G K||x|=1 } and the corresponding maximal ideal

m={ x G K|v (x)>0 }={ x G K||x|<1 }.

We have observen that Z_p := B\ (0)=o_p, i. ∈ . the open unit ball in Q_p is the valuation ring. This ring o_p is a local ring with maximal ideal m=Z_p\Zp = { x G Zp||x|$_p$<1 }={ x G Zp|xo=0 }={ x=pEP=o xi+ip^1 }=pZp.

Remark. The map tp_p : Z_p ^ Z, a=i=$_0$ $a_i p^i$ ^ a_0, defines an

epimorphism from Z_p to F_p=Z/z and is known the reduction map modulo p. Furthermore the kernel of p_p is ker p_p={ x G Z_p|x_0=0 }=pZ_p, thus, from the fundamental theorem of homomorphisms, we observe that

^{Zp}/=F=^{Z} /. $^{p/}$pZ_p=^{f}p=/pZ.

Remark. For the valuation ring, units and maximal ideal, we have the following set equalities:

Zp n Q={ f G Q|p t b }=Op,

pZ_p n Q={ f G Q|p t b A p|a }=m_p and

^{Z}p $^{n\ Q}$=$^{Z/}$pZ_p $^{n\ Q}$=$^{\{}$ f $^{G\ Q\ 1}$ p$^{t\ ab\ \}}$=^{u}p=$^{Op/}$$m_p$.

Proposition. The valuation ring o_p=Z_p is a principal ideal domain, with the principal ideals {0} and $p^n Z_p$ for all n G N.

Proof. As Z_p C Q_p, it is an integral domain.

Now let a={ 0 } be an ideal in o_p and consider an element a G a\{ 0 } of maximal absolute value. Such an element can be found, since the value set is discrete. Furthermore let n be the p-adic order of a, then a

Notes

$= \in \bullet p^n$, for a unit $\in$ G u_p, thus $p^n = \in^{-1} \bullet$ a G a, which means that $(p^n)=p^n o_p$ C a.

Conversely, for each a G a we have $|a|_p=p^{-m}<p^{-n}$, thus $a=<=p^m = <=p^n p^{m-n}$ g $p^n o_p$, therefore a C $p^n o_p$.

Remark. As $o_p=Z_p$ is an integral domain, Q_p can be considered as its quotient field Quot (Z_p) and $Q_p=Z_p[p^{-1}]$. For a G $Z_p \backslash \{0\}$, $a=<=p^n$, for a unit $\in$ G u_p, it is easy to observe that a^{-1} G $p^{-n}Z_p$.

We have observen that we can write each $x \in Q_p$ as $x=p^m x$, with $m \in Z$ and $x \in Z_p$.

Proposition. The balls $p^n Z_p$, for all $n \in Z$, constitute a neighbour- hood basis of 0, which covers all of Q_p.

Proof. $B_1(0)=Z_p$ C Q_p is clopen, thus it is an open neighbourhood of 0. The map $Q_p \wedge Q_p$, $x \wedge px$ is a homeomorphism, thus $p^n Z_p$ is an open neighbourhood of 0. Now from the p-adic representation it follows that $Q_p=U_{neZ} p^n Z_p$ and those $p^n Z_p$ actually are a neighbourhood basis for 0, as for any arbitrary open set U around 0, there exists a $n_0 \in Z$ such, that B_p-no (0) C U.

Remark. Once again we have a strong connection between the topological and algebraic properties of p-adic numbers, as for an element $x \in Q_p$ we can consider $v_p(x)$ as the largest number, such that $x \in p^{Vp(x)} Z_p$.

Example. Consider $x=x_{-5}p^{-5}+x_{-4}p^{-4}+... +x_{-1}p\sim^2+xo+x_1p + x_2p^3+...$, $x_{-5}=0$, then it is clear that $x \in p^{-5}Z_p$, but $x \in p^{-4}Z_p$, as from $x=p^{-4}(x_{-5}p^{-1}+x_{-4}+x_{-3}p+... +x_0p^4+x_1p^5+...)=p^{-2}x$

we observe that $x \in Z_p$ and thus $v_p(x)=-5$.

Remark. For $n \in N$ and $x, y \in Q_p$ we have

$y \in B_p$-n (x) ^ x— $y \in p^n Z_p$ and we write $x =_p n\ y$, or even shorter $x =_n y$.

Definition. A Hausdorff[1] space is a topological space in which each pair of distinct points of X have disjoint neighbourhoods.

Proposition. Every metric space (X, d) is a Hausdorff space.

Proof. We have to show that the topology induced by the metric d is Haus- dorff. Let x, $y \in X$ be two distinct points, that is, d (x, y)=0 and consider the open balls B_x := Bd (x, y) (x) and B_y := Bd (x, y) (y). Those are obviously open sets in X and to observe that they are disjoint, we assume there exists a $z \in B_x$ n B_y, but that means that d (x, z)<^{d} $^{(x}2^{y}$ and d (y, z)<^{d} $^{(x}f^{y}\wedge$, thus d (x, z)+d (z, y)<d (x, y), which is a contradiction to the triangle inequality.

Example. The converse of the above remark is not true, for example consider the set of all ordinal numbers with the discrete order topology.

Proposition. Let X be a Hausdorff space. Suppose that Y C X and that a is a limit point of A. Then each neighbourhood of a contains infinitely many points of A.

Corollary. In a Hausdorff space the limit of a sequence is uniquely defined. This astonishing fact is not true for general topological spaces.

Proposition. The p-adic field Q_p is a totally disconnected Haus- dorff space.

Proof. As a metric space Q_p is a Hausdorff space and since its metric is an ultrametric, Q_p is totally disconnected.

Definition. A metric space (X, d) is known compact, if and only if for each open cover of X there exists a finite subcover of X. The metric space is known locally compact, if and only if every $x \in X$ has a compact neighbourhood.

Notes

Proposition. The set of all the the balls in Q_p is countable.

Proof. For any arbitrary ball B_r (x) with radius r, we know that there exists an integer z $\in$ Z, such that $r=p^{-z}$. With write $x=i=_{-m}\ x_ip^i$. Now if we take the z-th partial sum z_0 of this series, we easily observe that $z_0 \in B_p$-z (a) and this, together with the fact that the set of possible radii is countable the proposition.

Proposition. The field Q_p is locally compact with compact valuation ring Z_p.

Proof. Using the uniqueness of the p-adic expansion and the pigeonhole principle, we can construct a sequence of subsequences, proving that Zp is sequentially compact, thus as a metric space, compact. Let (a_n) be a sequence in Z_p and for each n write $a_n=°=_0\ a^{(n}{}^\wedge p^i$, then, by the pigeonhole principle, we can find an element $b_0 \in \{0, \ldots, p— 1\}$, with $a0^{n)}=b_0$, for infinitely many n. This yields a subsequence of (a_n), namely (a_{bon}), whose terms all have b_0 as first digit in their p-adic expansion. Repeating this construction inductively we obtain the desired sequence of subsequences of (a_n), $((a_{bkn})_n)_k$ with (a_{bkn}) being a subsequence of $(a_{bk}+_{in})_n$, as well as a p-adic integer $b=°=_0\ b_kp^k$ such, that every term of $(a_{bkn})_n$ has the same k+1-first digits as b. It is then clear that the sequence of the diagonals (a_{bkk}) is a subsequence of (a_n) which converges to b, which proves that Z is sequentially compact, as desired. As $Z_p=o_p=$Bi (0)$=B_p$ (0), it is evident that every ball in Q_p is compact, thus Q_p is locally compact.

Check your Progress-2

Discuss Zeta function of a prescheme over fp & fq

____

____

____

10.10 LET US SUM UP

In this unit we have discussed the definition and example of Zeta – functions, Fields of finite type over z, Convergence of the product, Zeta function of a prescheme, Zeta function of a prescheme over fp, Zeta function of a prescheme over fq, Reduction to a hyper – surface, Algebraic And Topological Properties

10.11 KEYWORDS

Zeta – functions…. Let R and S be subrings of K containing a unit elements such that S is finitely generated over R .

Fields of finite type over z….. The infinite product Za (s) is a absolutely convergent for Re s>dim A and uniformly convergent for Re s>dim A+s for every s> 0.

Convergence of the product….. Let A be a commutative ring with unity. We shall denote by Sp (A)the set of all prime ideals of A .

Zeta function of a prescheme….. Let S be a prescheme over Z of finite type. We have a canonical map from a prescheme S to Sp (Z)

Zeta function of a prescheme over fp In order to prove Dwork's theorem it is sufficient to prove it for an affine scheme and open sets of an affine scheme because of the equation.

Zeta function of a prescheme over fq….. We shall show that to prove our theorem it is sufficient to consider the zeta function of a hypersurface V defined by a polynomial P (X1Xn)

Reduction to a hyper – surface….. Algebraic And Topological Properties….. We recall the definitions of the valuation ring o={ x G K|v (x)>0 }={ x G K ||x|<1 },

10.12 QUESTIONS FOR REVIEW

Explain Zeta-functions

Explain Zeta function of a prescheme over fp & fq

10.13 REFERENCES

p-adic numbers: an introduction by Fernando Gouvea

p-adic Numbers, p-adic Analysis, and Zeta-Functions, Neal Koblitz (1984, ISBN 978-0-387-96017-3)

A Course in p-adic Analysis by Alain M Robert

Analytic Elements in P-adic Analysis by Alain Escassut

10.14 ANSWERS TO CHECK YOUR PROGRESS

Zeta-functions

(answer for Check your Progress-1 Q)

Zeta function of prescheme over fp & fq

(answer for Check your Progress-2 Q)

UNIT-11 : ELEMENTARY FUNCTIONS

STRUCTURE

11.0 OBJECTIVES

After studying this unit, you should be able to:

- Understand about Elementary Functions
- Understand about An Auxiliary Function
- Understand about Semi Simple Lie Groups
- Understand about Lie Groups
- Understand about The Universal Enveloping Algebra
- Understand about The Concept Of Free Algebras

11.1 INTRODUCTION

In mathematics, p-adic analysis is a branch of number theory that deals with the mathematical analysis of the functions of p-adic numbers.

Elementary Functions, An Auxiliary Function, Semi Simple Lie Groups, Lie Groups, The Universal Enveloping Algebra, The Concept Of Free Algebras

11.2 ELEMENTARY FUNCTIONS

We consider the convergence of the exponential logarithmic and binominal series in this section. We assume that the field K is of characteristic 0 and the real valuation v on Q induces a p-adic valuation.

The exponential series c{ x)=2 —. Converges in the disc if x)>n=0 n! and in the domain of convergence if ∈ (x) - 1)=v (x). Let n=p - 1

a0+a1 p+•••+arpr where pr<n<pr+1 and 0<aj<p - 1. One can easily prove that

n~ Sn P~ 1 r

where Sn=X at Therefore

i=0) _ "I+Sn p - 1 n (p - 1)

Sn /log n \ ^ (ii) -1

But < i-l.

Hence the

p - 1\log p) n p - 1

for if x)= The latter part of the assertion is trivial. We

p – 1 observe immediately that ∈ (x+y) = ∈ (x). ∈ (y) and ∈ (x) has no zeroes in the domain of convergence.

™ k, yk

We define log (1+y)=2 (-1)— as a formal power series over k=1 k K.

We shall show that the series log (1+y) converges for v (y)>0 and

v (log (l+/))=v (y) for if/) > we have

p – 1 log n i (-1)nyn \ But v (n)< therefore 4' (tends to infinity as n — » oo when

log p n

ever v (y)>0. On the other hand v (n)=0 if (n, p)=1, therefore the

series is not convergent for if /)<0. For n>1 and if /) > p - 1 it can

((-1)n-1yn \

easily proved that d I>if/), which proves our last assertion.

Moreover for if x)> — - — we have the equalities p - 1

e (log (1+x))=1+x

log (∈ (x))=x

Let

G=\ x|x ∈ K, v (x) > p – 1

be subgroups of K+ (the additive group of K) and K* respectively. The mapping x ^ ∈ (x) is an isomorphism of G onto G', the inverse of which is the mapping 1+x ^ log (1+x). In fact the mapping 1+y ^ log (1+7) is a homomorphism of the group 1+Yfo (H begin the complete algebraic closure of K) into the subgroup of H+, where v (y)>0. It is not

an isomorphism because it ^ is a p-th root of unity, then v (C~1) = -

P – 1 and log Z=0.

We define (1+Y)Z=2 h (m, Z) Ym = ∈ (Zlog (1+Y)) where

m=0 ui 7\ Z (Z- I)- (Z- m+I) .. .

Notes

h (m, Z)=   as a formal power series in the van- m!

ables Y and Z over K. Since h (m, Z) is a polynomial in Z, we can substitute for Z any element of K to get a power series in the one variable Y.

Proposition. For any element t in K the power function (1+x) defined

above is analytic for v (x) >   (respectively for v (x)>-v (t)-{   )

p - 1   p - 1

ifv (t)>0 (respectively if v (t)<0) Moreover if t belongs Zp, then (1+x)t is analytic for v (x)>0.

Proof. When v (t)<0

m- 1

v (h (m, t))=m (v (t)) - v (m\)>mv (t) -

p - 1

Therefore   = (/ (p 3_ Hence (1+x)' is analytic

m   p – 1 in ifx)> — - if/). Similarly one can prove the convergence when p – 1 v (t)>0.

Let t be in Zp. Then h (m, t) is a p-adic integer.

Suppose that v (m!)+1=a, then there exists an element km in Z such that

t=km (mod pk)

Therefore

t (t - 1) ... (t - m+1)=km (km— 1)

h (m, t)=h (km, m) (mod p).

But h (km, m) is a rational integer, therefore v (h (m, t))>0. From this our assertion follows easily.

11.3 AN AUXILIARY FUNCTION

Throughout our discussion Fq shall denote a finite field consisting of q elements. Let us consider the infinite product

ppP— jpm

F (Y, T)= (1+Y)t (1+Yp) P (1+O Pm

The product is well defined as formal power series in two variables Y and T over Q. Clearly is convergent in QF (Y T) as a power series over Q[T]

TO

F (Y, T) = ∈ Bm (T)Ym, d (Bm (T))

∈ am (Y)Tm,

we obtain m=0where am (Y) is a power series, the terms being of degree>m. Theorem. The coefficients of F (T, Y) are p-adic integersTheorem. If F is an element of Q

(F (Y, Z))P

if only if the coefficients of ^ ^ are in pZD

F (Yp, Zp) p

Proof of Theorem. Let us suppose that F (Y Z)=1 - X a2, Y'Zj then

i+j>0 ^ (F (YZ))p r r u G= —— — — -=F\ xF2

where F (Yp, Zp)r

Fi=1 - p ^ ai/ZJ+•••+ (P) (-1)r ^ aiJYiZJ \i+J>0

If G=1+2 t>ijYiZj, then

i+j>0

bij=- paij+ (terms of the form pX polynomials in a with rational integers coefficients with

Notes

$$r + s < i + j) + \sum_{k=1}^{\infty} \sum a_{i_1, j_1} \ldots a_{ik, jk}$$

i1+...+ik=i' j1+...+jk=j'

F2=1+2 2 a, jYpiZPj

k=1 \i+j>0

ir+jr>0

+ (-1)p Yt ap1j1ai2 j2 ... aikjki1+...+ik=f

j1+...+jk=j

ir+jr>0

where the last two sums appear only if i and j are divisible by p and in this case pi'=i, pj=j.

Assume that bij belongs to pZp for i+j>0. We shall prove that ay are in Zp by induction. Obviously a00 is in Zp. Assume that ars $\in$ Zp for r+s<i+j; then in the formula giving bij all the terms except perhaps - paij. But a - ap belongs to pZp if a belongs to Zp, therefore paij belongs to pZp and aij belongs Zp. The other part of the assertion is trivial

TPm __ r[Pn -1

(1+Y)pt n (1+YpB) Pm' m=1

T^— Tpm -1

(1+Yp)tp n (1+Ypm) pm m=2

(1+Y)p '' (1+Yp)

a+^bkYk

k=1wherebkarep-adicintegers. Moreover m

1+p<= bkYk = $\in$ h (m, T)pm $\in$ bkY

m=0 v (pm) m - 1 F (Y, T) p

But — >in > 0, therefore— —— — - - 1 has its

m! p- 1 F (Yp, Tp)

coefficients in pZp. Thus by Theorem the coefficients of F (Y, T) are p-adic integers.

One deduces that F (y, t) is analytic for v (t)>0 and v (y)>0, because if v (t)>0, then v (Bm (t))>0 because Bm (t) is a

polynomial with coefficients from Zp. Therefore the series Yj Bm (t)ym

m= 0converges for v (y)>0.

Factorisation of additive characters of a Finite Fields

jx|x ∈ np=n, xP=xj. We have the canonical map from

R2 to Fps namely the restriction on the canonical homomorphism of t

onto kO. In order t prove that thi s map i s bijective, it i s sufficient to prove that is surjective ; because both Rs and Fps have ps elements. If x ± 0 is in Fps, then xp-1 -1=0 and x is a simple root of the polynomial Xp-1 - 1. Therefore by Hensel's Theorem there exists an element a belonging to O such that a=x and apS-1 - 1=0, which proves that a is in R2 and the mapping is onto. Infact the canonical homomorphism of OO onto kO when restricted to R=U R2 is an isomorphism onto kO. Finally s= 1

Hensel's Theorem shows that R1 is contained in Qp.

Let Us=Qp (Rs). Clearly Us is a Galois extension of Qp and the Galois group is cyclic generated by the automorphism a : p ^ pp, where p is a primitive ps - 1 th root of unity. Moreover Us is an un- ramified extension of Qp, because [Us; Qp]=[Fps; Fp]. If we take TO

U=Us,

then the completion of U is the maximum unramified extension of Qp in O and a is known the Frobenius automorphism of U. If t is an elements is R2, then

Tr t=t+tp+•••+tps-1

Us / Qp

belongs to Zp. Thus the function (1+Y)Tr ^ is analytic for v (y)>0. Let t be the representative of t ∈ Fp2 in R2. If y belongs y belongs to YO then (1+y)Tr ^ belongs to O. We shall choose y in such a way that mapping t ^ (1+y)Tr ^ is a character of the additive group of Fps. Obviously for any u and v in Fps we have

(u+v)'=U+V (mod YO)

Tr (U+C)=Tr U+tr V (mod YO)

= Tr U+Tr V (mod pZp)

because Tr U is a p-adic integer. Therefore

(1+y)tr (u+v) '= (1+y)Tr U (1+y)Tr V (1+y)a,

where a belongs to pZp. Let us take 1+y=Z where Zp=1 and Z+1. It follows that (1+y)a=1. Thus the mapping u ^ ZTr U is a character of Fps. We shall show that it is a non -trivial character. Firstly, Za=1 if

and only if a belongs to pZp proved that a already belongs to Zp. For by

choice of y we have v (y) = > 0 and p - 1

Za= (1+y)a=1+ay+•••+h (m, a)ym+•••

Since a is p-adic integer, v (h (m, a)>0 and hence v (h (m, a)ym >

2 2 2 for in>2, (a+y)a+1 if if ay) < - Therefore if ay) > p - 1

which implies that a belongs to pZp. But the p - 1

canonical image of Tr U in Fp is the trace of u as an element of Fps over Fp, therefore there exists as least one U such that Tr U is not in pZp. Hence the mapping u ^ ZTr U is a non-trivial character of Fps. By definition of the product F (Y, T) we have

ilF - F (y, l/)= (l+yf P"

U pm+1--upm

F (y, i/p)= (1+yfp ... (1+ym) -P"

^pm+s-i - ^pm+s-i

F (y, iYpS 1)= (1+yf^ X ... (1+y^) P"

Since Up=U, by multiplying these identities we get

s-1

xTr U

Y\F (y, Up)= (1+y)T

Thus ZTr=n f (U) where ip (T)=F (Z - 1, T), is the splitting of

additive characters of Fps which we shall require later.

Check your Progress-1

Discuss Elementary & Auxiliary Functions

11.4 SEMI SIMPLE LIE GROUPS

Let G be a semi simple Lie group worth a faithful representation. We state here two theorems the proof of which could be found.

Theorem. The group G has a maximal compact subgroup and all the maximal compact subgroup are conjugates.

Theorem Suppose that K is maximal compact subgroup of G, then there exists a connected solvable T of G such that G=TK.

We shall prove the following theorem about completely irreducible representation of G.

Theorem. Every irreducible representation M of K is contained atmost dim (M) times in every completely irreducible representation of G.

Proof. The finite dimensional irreducible representations of G is a vector H is a complete system of representations of L (G). Let x ^ px be a representation of G in a vector space H.

Notes

We call the function d (x)={ pxa, a') where a belongs to H and a' belongs to H* (the con- jugate space of H), a coefficient of the representation. Let V denote the vector space generated by all coefficients of all finite dimensional irreducible representations of G.

Since every finite dimensional repre- sentation of G is completely reducible, V contains all the coefficients of all finite dimensional representations of G. Let p1 and p2 be two finite dimensional irreducible representations of G. Then we have

{ p\a1, aj) (p2xa2, af,)={ p\ <8> p2xa1 <g> a2, aj <8> af,)

showing that V is an algebra. Moreover V is a self adjoint algebra, be- cause if d (x)={ pa, al) is in V, then Q (x)={ pxa, a!) is also in V. Since G has a finite dimensional faithful representation, Vseparates points i. ∈ . , if d (x)=d (d) for every d in V, then x=x\ Thus Stone- Weierstrass' approximation theorem every continuous function on G can be approxi- mated uniformly on every compact subset by elements of V.

Hence if f is anon-zero elements of L (G), then f f (x)gx)dx=0 for every element

g of C (G) (the set of all continuous functions on G), because

P f=f pxf (x)dx and<pxa, a'>f (x)dx=0

for every a in H and a' in H* and p. Therefore f must be =0

The representations of G induced by all characters of T form a complete system for L (G)

Let p be a finite dimensional irreducible representation of G and let

V   t 1

p= (p)) be the representation contragradient to p. By Lie's theorem the restriction of p to T has an invariant subspace of dimension 1, which implies that there exists a vector tf+0 in E* (the conjugate space V of the representation space ∈ of, p) such that p (t)=t=x (t)t for every t ∈ T. Consider the mapping a ∈ E— "ascd~l, where p (x) =< pxa, t >. Since

p (tx) =< ptxd, t >=< pxa, prt~lf >= x~l (t)<pxa, t >= x~1 (tja (x),

p (x) is covariant by left translation. Obviously the map a— p is continuous. Let Ux~l be the representation of G induced by ^x-1. The mapping a— p is a morphism of representations p and Ux-1, because

"py a (x)= (px pya, b>=P (xy)=Ux-1 (a).

The mapping a —>a is not zero. If a ± 0, then (pxa) generates the whole space ∈ because p is irreducible, therefore for atleast on x in G (pxa, t>+0 ^ p+0. Let f be a non-zero element of L (G). If Uf 1=0. For every x then pf=0 for every p which means the f=0 This is a contradiction, hence our result is proved.

We shall show that if x is a character of T, then M occurs at- most dim (M) times in Ux. Clearly Ux/^ (restriction of UtoK) =UX/KnT gut the space of this representation is the space of continuous functions f on K such that

f (tk)=x (t) f (k) for t ∈ K n T.

Therefore U/KnT is a sub representation of the right regular representation of K. Hence (Cx)m c Lm (K) which is a space of (dimM)2. Thus M occurs at most dim (M) times in U.

11.5 LIE GROUPS

Definitions and foundations

Definition.A Lie group G (over K) is a manifold (over K) which also carries the structure of a group such that the multiplication map

m=mG : G x G — - G (g, h) — - gh

is locally analytic.

Notes

In the following let G be a Lie group, and let ∈ e G denote the unit element.

Theorem. For any h ∈ G the maps

<=h : G G and rh : G G

g — - hg g i — - gh

are locally analytic isomorphisms (of manifolds).

Proof. By symmetry we only need to consider the case of the left multipli- cation <=h. This map can be viewed as the composite

G — - G x G G

g1 — - (h, g).

The left arrow is locally analytic by Example 8. 5. 4) and the right arrow by assumption. Hence the map <=h is locally analytic. We obviously have <=h o <=h-i=<=hh-i=<=e=idG and then also <=h-i o <=h=idG. It follows that ∈ - :=<=h-i is locally analytic as well.

Corollary. For any two elements g, h ∈ G the map

Tg (<=hg-i): Tg (G) — Th (G)

is a K-linear isomorphism; in particular,

Te (<=g): Te (G) Tg (G)

is an isomorphism for any g ∈ G.

Corollary. Every Lie group is n-dimensional for some n>0.

Proof. We have dim G=dimK Te (G)=dimK Tg (G) for any g G G.

Examples. Kn and more generally any ball B<= (0) (as ran open sub-manifold of Kn) with the addition is a Lie group.

Kx and more generally B- (1) and B<= (1) for any 0 < ∈ < 1 (as open submanifolds of K) with the multiplication (observe that ab— 1 = (a— 1) (b— 1)+ (a— 1)+ (b— 1)) are Lie groups.

GLn (K) viewed as the open submanifold in Kn defined by "det=0" with the matrix multiplication is a Lie group.

Let g, h G G. We know from Remark 9. 10. ii. that the map T (pr:) x T (pr2) : T{ g>h) (G x G) — U Tg (G) x Th (G)

is a K-linear isomorphism. In order to describe its inverse we introduce the maps

ih : G —>G x G and jg : G —>G x G

x i —> (x, h) x i —> (g, x)

which are locally analytic. We have

pU o ih=idG and pr2 o ih=constant map with value h

and hence

T (pri) o T (ih)=T (idG)=idT (G)

and

T (pr2) o T (ih)=T (constant map)=0.

This means that the composed map

Tg (G) — U T (gh) (G x G) T (pri)xT (pr2) : Tg (G) x Th (G) sends t to (t, 0). Analogously the composed map

Th (G) — U T (gh) (G x G) T (pr —) X T (pr2 U Tg (G) x Th (G)

sends t to (0, t). We conclude that

Tg (ih)+Th (jg) : Tg (G) x Th (G) T{ g, h) (G x G)

(tl, t2) ' ► Tg (ih) (tl)+ Th (jg) (t2)

is the inverse of T^h) (pri) x T^^).

Theorem. T (g, h) (G x G) ^ *Tgh (G)

T (pr1)x'r (pr2)'==~"-^^^ ^^TArh)+Th (lg)

Tg (G) x Th (G)

is commutative for any g, h G G.

Proof. We compute

T (g, h) (m) ∘ (T (g, h) (pr1) x T (g, h) (pr2))-1=T (g, h) (m) 0 (Tg (ih)+Th (jg))

= Tg (m O ih)+Th (m o jg) = Tg (rh)+Th (lg)

Because of i2=idG it suffices to show that the map i is locally analytic. To do so we use the bijective locally analytic map

g : G x G —► G x G

(x, y) i —► (xy, y).

We claim that the tangent map T (g, h) (g), for any g, h G G, is bijective.

T (g, h) (G x G) T (9, h)M, T (gh, h) (G x G)

T (pri)xT (pr2)

Tgh (G) x Th (G)

in which the lower horizontal arrow is given by

(ti, t2) 1 —► (Tg (rh) (ti)+Th (lg) (t2), t2)

is commutative. Suppose that (t1, t2) lies in the kernel of this latter map. Then t2=0 and hence 0=Tg (rh) (ti)+Th (lg) (t2)=Tg (rh) (ti). The analog for the right multiplication implies that t1=0. This lower horizontal map and therefore T (g, h) (g) are injective. But all vector spaces in the diagram have the same finite dimension. Our claim that T (g, h) (p) is bijective follows. We now can apply the criterion for local invertibility and we conclude that the inverse ^-1 is locally analytic as well. It remains to note that i is the composite ^GxG G

is commutative. This reduces us to showing the special case in our assertion. We consider the diagram

Te (G) T (e, ∈) (G X G) T (Pri)XT^>Te (G) X Te (G)

T (e, ∈) (G X G) T (Pri)XT (Pr2^ Te (G) X Te (G)Te (G)

In the proof of Prop. 13. 6 we have observen that the map pT1 (x, y)= (xy-1, y) is locally analytic and that the central square in the above diagram is com- mutative. The top triangle is commutative. The commutativity of the bottom triangle is trivial. It remains to observe that passing from top to bottom along the left, resp. right, hand side is equal to Te (i), resp. to the multiplication by -1.

Corollary. For every n ∈ Z the map

fn : G g 1 — ► g"

is locally analytic, and Te (fn) coincides with the multiplication by n.

Proof. Case 1: For n=0 the map f0 is the constant map with value ∈ and Te (fo)=0.

Case 2: Let n>1. We can view fn as the composite

G G x. .. x G ^ (g,. . ., g)

(gl,. . ., gn) 1 ► gl. .. gn.

Both maps are locally analytic, the left diagonal map and the right multiplication map by assumption. Hence in the diagram

Te (G x. .. x G)

Te (mult)

Te (G) m T (pri)

Te (G) X. .. X Te (G)

the top, resp. bottom, composed map is equal to Te (fn), resp. the multiplication by n. But this diagram is commutative, the left triangle for trivial reasons and the right triangle as a consequence.

Case 3: Let n< — 1. Since fn=f-n o i

Te (fn)=Te (f-n) o Te (i)= (— n id) o (— id)=n id.

already indicates that the tangent space Te (G) in the unit element of G plays a distinguished role. We want to investigate this in greater detail.

Proposition.

rT : Te (G) x G — ^ T (G) and lT : G x Te (G) — ^ T (G)

(t, g) 1► Te (rg) (t) (g, t) 1^ Te (lg) (t)

are locally analytic isomorphisms (of manifolds)

Te (G) X G

G X Te (G)

is commutative.

Proof. By symmetry it suffices to discuss the map rT. We choose a chart c= (U, p, Kn) for G around ∊ . the map

Qc : kn Te (G) v I —. [c, v]

is a K-linear isomorphism. We equip Te (G) with the unique structure of a manifold such that dc becomes a locally analytic isomorphism of manifolds. This structure does not depend on the choice of the chart c. Of course, we then view Te (G) x G as the product manifold of Te (G) and G. The inclusion map Te (G) T (G) is locally analytic since it can be viewed as the composite of the locally analytic maps

Te (G) — I. Kn — I — u x Kn -. pG1 (U)— T (G).

We recall that tc ((g, v))=[c, v] ∊ Tg (G) is locally analytic by the construc- tion of T (G) as a manifold. Let

Co : G T (G) g -. 0 ∊ Tg (G)

denote the "zero vector field", i. ∊ . , the zero vector in the vector space r (G, T (G)). that the composed locally analytic map

Te (G) x G -*"1: T (G) x G -1 —. t (G) x T (G)

<---) —, -)- : t (g x G)— T (G)

sends (t, g) to Te (rg) (t)+Tg (le) (0)=Te (rg) (t) and hence coincides with rT. This shows that the map rT is locally analytic. It is easy to check that the map

T (G) —. Te (G) x G ^ 1 .

(TPG <t) (rPG <t)-1) (t), PG (t))

is inverse to rT. Its second component pg is locally analytic It therefore remains to prove that the map

f : T (G) -. Te (G)

t 1. TPG<t) (rPG<t)-1) (t)

is locally analytic. we compute that the composed locally analytic map

T (G) ld — : T (G) X G -X-1» T (G) x G X-X-1 T (G) x T (G)

(T (p, ,)xr (pr,)) -. : t (g x g) — l t (G)

sends t to TPG (t) (rPG (t)-1) (t). It follows that the left vertical composite in the commutative

T (G) -=T (G)

is locally analytic. Since tc is an open embedding we conclude that the right vertical composite is locally analytic. With the lower oblique arrow therefore also the upper oblique arrow f is locally analytic.

Corollary. The maps

r (G, T (G)) C an (G, Te (G)) r (G, T (G))

<=f (g) := lT ((g, f (g))) f

Cf (g) := rT ((f (g), g))

are isomorphisms of K-vector spaces.

Proof. The maps ∈ i — 1 pr2 o (lT)-1 o<= and ∈ i — 1 pr1 o (rT)-1 o<=, respectively, are inverses.

In Can (G, Te (G)) we have, for any t ∈ Te (G), the constant map constt (g) := t.

We put

<=t (g) := <=constt (g)=Te (lg) (t) and <=f (g) := <=ronstt (g)=Te (rg) (t).

Definition. A vector field ∈ <= T (G, T (G)) is known left invariant, resp right invariant, if ∈ (g)=Te (lg) (<= (∈)), resp. ∈ (g)=Te (rg) (<= (∈)), holds true for any

g ∈ G.

Corollary. The maps

Te (G) —>{ ∈ G r (G, T (G)) : ∈ is left invariant }

t <=t

and

Te (G) — ► { ∈ G r (G, T (G)) : ∈ is right invariant } t— <=[

are K-linear isomorphisms.

Proof. The map ∈ i — > ∈ (∈) is the inverse in both cases.

Let ∈ be a K-Banach space. With any vector field ∈ on G we had asso-ciated the K-linear map

D : Can (G, ∈) — ► Can (G, ∈)

f (f)=df ∘ ∈ .

If ∈ is left or right invariant what consequence does this have for the map D^? K-linear

G x Can (G, ∈) — ► Can (G, ∈)

(h, f)— hf (g) := f (h-1g)

of the group G on the vector space Can (G, ∈)

as well as a right K-linear action by "right translation"

Can (G, ∈) x G — ► Can (G, ∈)

(f, h) fh (g) := f (gh-1).

Theorem. If ∈ G r (G, T (G)) is right, resp. left, invariant then we have

D? (fh)=D? (f)h, resp. D? (hf)=hD? (f),

for any f G Can (G, ∈) and h G G. In the case ∈ = K the converse holds true as well.

Proof. By symmetry we only consider the "right" case. First we suppose that ∈ is right invariant, i. ∈ . , ∈ (g)=Te (rg) (<= (∈)). It follows that

T (rh-l) 0 ∈ (g)=Tg (rh-l) 0 Te (rg) (<= (∈))=Te (rgh-) (<= (∈))
= ∈ (gh-1).

We now compute

Dg (f h) (g)=dfh o ∈ (g)=d (f o rh-i) o ∈ (g)

= df 0 T (rh-i) 0 ∈ (g)

= df o ∈ (gh-1)=Dg (f) (gh-1)

= Dg (f)h (g)

where for the second line If vice versa Dg satisfiesthe asserted identity (for some ∈) then we have

df 0 T (rh-i) 0 ∈ (g)=Dg (fh) (g)=Dg (f)h (g)=Dg (f) (gh-1)=df 0 ∈ (gh-1)

for any f and any g, h. We rewrite this as

df 0 T (rh-i) 0 ∈ (gh)=df 0 ∈ (g).

With ∈ also

<=h (g) := T (rh) 0 ∈ (gh-1) is a vector field on G. Hence we obtain the identity

Dgh=Dg for any h ∈ G.

Notes

Later on we will observe that G is paracompact. In the case ∈ = K the map ∈ ^ Dg therefore is injective. It follows that <=h=<=, i. ∈ . , that

T (rh) 0 ∈ (gh-1) = ∈ (g) holds true for any g, h ∈ G. In particular, for g=h we obtain

T (rg) (<= (∈)) = ∈ (g) for any g ∈ G which means that ∈ is right invariant.

The Lie product of vector fields is characterized by the identity

Dg 0 Dn Dn 0 Dg— D[g, n]

Corollary. If the vector fields f and n on G both are left or right invariant then so, too, is the vector field [f, n].

we observe that for any s, t ∈ Te (G) there are uniquely determined tangent vectors [s, t]i and [s, t]r in Te (G) such that

f[s, t]t=[fs, ft] and f[S, t]r=[fr, ft].

Then

(Te (G), [,]i) - — -+ (r (G, T (G)), [,])

And (Te (G), [,]r) (r (G, T (G)), [,])

are injective maps of Lie algebras. Is there a relation between the two Lie products [,]i and [,]r on Te (G)? For any f ∈ r (G, T (G)) also

f (g) := Tg-i (i) ∘ f (g-1)

is a vector field on G. This provides us with an involutory K-linear automorphism

L : r (G, T (G)) — ► r (G, T (G)).

Remark. Il Te (G) ^ * r (G, T (G)) -1

Te (G) - r (G, T (G))

is commutative.

Proof. we compute

' (f!) (»)=T (i) ◦ { t (9-1 }=T (i) ◦ T (lg-i) (t)=-T (rg) (t)=-ft (g).

Theorem. Any vector fields f and n on G satisfy

[4f, 4n]=1f, n].

Proof. we compute

DT (/) (g)=d/ o= df oT (i) { (g-1)=d (/ oi) o{ (g-1)=D (/oi) (g-1). This amounts to the identity

DT (/) o 1=D (/ o l).

We continue computing

(Ui? o Din) (/) (g)=D (Din (/) o l) (g-1)

= D? (Dn (/ o l)) (g-1)

= (D? o Dn) (/ o l) (g-1)

and consequently

D[i ?, in] (/) (g)=[Dtf, Dtn] (/) (g)

= [D?, Dn] (/ o l) (g-1)

= D[?, n] (/ o l) (g-1)

= Di[«, n] (/) (g).

Corollary. We have

[s, t]r= — [s, tjz for any s, t ∈ Te (G). Proof. Compute CMr=[<=, Cf]=[— { !, — Cf]=[{ -s, { -t]

= [^c1 ^c1]=Hc1 c1]=L{ \

[{ s, stJ l{ s, stJ { [s, t]i

= C-Mi.

From now on we simplify the notation by setting [s, t] := [s, t]r and Dt := Dq-for any s, t ∈ Te (G). We then have the identity

D[s, t]=Ds o Dt— Dt o Ds

Definition. Lie (G) := (Te (G), [,]) is known the Lie algebra of G. We obviously have

dimK Lie (G)=dim G.

The guiding question for the rest of this book is how much information the Lie algebra Lie (G) retains about the Lie group G. The answer requires several purely algebraic concepts which we discuss in the next few sections.

Definition. Let Gi and G2 be two Lie groups over K; a homomorphism of Lie groups f : Gi —>G2 is a locally analytic map which also is a group homomorphism.

Definition. If (gi, [,]i) and (g2, [,]2) are two Lie algebras over K then a homomorphism (of Lie algebras) a : gi —>g2 is a K-linear map which satisfies

[a (x), a (y)]2=a ([x, y]i) for any x, y $\in$ gi.

We write HomK ((gi; [,]i), (g2, [,]2)) for the set of all homomorphisms of Lie algebras a : gi —>g2.

Exercise. For any homomorphism of Lie groups f : Gi —>G2 the map Lie (f) := Te (f) : Lie (Gi) —>Lie (G2) is a homomorphism of Lie algebras.

Check your Progress-2

Discuss Semi Simple Lie Groups & Lie Group

11.6 THE UNIVERSAL ENVELOPING ALGEBRA

In this section K is allowed to be a completely arbitrary field.

Exercise. i. Let A be an associative K-algebra with unit. Then (A, [,]a) with [x, y]A := xy - yx

is a Lie algebra over K. In the case of a matrix algebra A=Mnxn (K) the corresponding Lie algebra is denoted by gln (K).

ii. If the field K is nonarchimedean then we have gln (K)=Lie (GLn (K)).

How general are the Lie algebras in this exercise? Obviously (A, [,]a) can have Lie subalgebras which do not correspond to associative subalge- bras. We want to show that any Lie algebra in fact arises as a subalgebra of an associative algebra. A K-linear map a : g —>A from a Lie algebra g into a associative algebra A, of course, will be known a homomorphism if it satisfies

a ([x, y])=a (x)a (y)— a (y)a (x) for any x, y ∈ g.

At this point we need to recall the following general construction from mul- tilinear algebra. Let ∈ be any K-vector space. Then

T (∈) := n>0E n where E0n := E E (n factors)

is an associative K-algebra with unit (note that E00=K). The multiplica- tion is given by the linear extension of the rule

(Vi . .. Vn) (Wi . .. Wm) := Vi . .. Vn Wi <g). .. Wm.

This algebra T (∈) is known the tensor algebra of the vector space ∈ . It has the following universal property.

Any K-linear map a : ∈ —>A into any associative K-algebra with unit A extends in a unique way to a homomorphism of K-algebras with unit a : T (∈) —>A. In fact, this extension satisfies

a (vi... Vn)=a (vi) . .. a (vn).

Let g be a Lie algebra over K. Viewed as a K-vector space we can form the tensor algebra T (g). In T (g) we consider the two sided ideal J (g) generated by all elements of the form

x y— y x— [x, y] for x, y ∈ g.

Note that x y— y x ∈ g whereas [x, y] ∈ g0i. Then

U (g) := T (g)/J (g)

is an associative K-algebra with unit and e : g — ► U (g) x i —>x+J (g)

is a homomorphism.

Definition. U (g) is known the universal enveloping algebra of the Lie algebra This construction has the following universal property. Let a : g — ► A be any homomorphism into any associative K-algebra with unit A. It extends uniquely to a homomorphism a : T (g) —>A of K-algebras with unit. Because of

a (x y - y x - [x, y])=a (x)a (y) - a (y)a (x) - a ([x, y])=0 we have J (g) C ker (a).

Hence there is a uniquely determined homomorphism of K-algebras with unit

a : U (g) —>A with a o ∈ = a,

is commutative.

The tensor algebra T (∈) has the increasing filtration

To (∈) C Ti (∈) C. .. C Tm (∈) C. ..

defined by

Tm (∈) := 0<,,<mE n.

The Tm (∈) do not form ideals in T (∈). But they satisfy

Ti (∈) • Tm (∈) C Ti+m (∈) for any l, m>0.

Correspondingly we obtain an increasing filtration

Uo (g) C Ui (g) C. .. C Um (g) C. ..

in U (g) defined by

Um (g) := Tm (g)+J (g)/J (g)

and which satisfies

Ui (g) • Um (g) C Ui+m (g) for any l, m>0.

For example, we have U0 (g)=K 1 and U\ (q)=K 1 + ∈ (g). We define

gr^ U (g) := m>o grm U (g) with grm U (g) := Um (g)/Um-i (g)

(and the convention that U-1 (g) := { 0 }). Because of the K-bilinear maps

gr1 U (g) X grm U (g) ► gr1+m U (g)

(y+Ui-i (g), z+Um-i (g)) I — ► yz+Uz+m-i (g)

are well defined. Together they make gr, U (g) into an associative K-algebra with unit.

Theorem. (Poincare-Birkhoff-Witt) The algebra gr^ U (g) is isomorphic to a polynomial ring over K in possibly infinitely many variables Xi and, in particular, is commutative. More precisely, let { xi }iei be a K-basis of g; then

K[{ Xi }i€/] gr^ U (g)

Xi i — ^ ∈ (xi)+Uo (g) G gri U (g)

is an isomorphism of K-algebras with unit.

Corollary. The map ∈ : g —>U (g) is infective.

Because of this fact the map ∈ usually is viewed as an inclusion and is omitted from the notation. We observe that g indeed is a Lie subalgebra of an associative algebra.

Corollary. Let d := dimK g<to; if xi,. . ., xd is an (ordered) K - basis of g then { xil . .. xim : m>0, 1<ii <. .. <im<d } is a K-basis of U (g).

Proof. The Theorem Poincare-Birkhoff-Witt implies that, for any m>0, the set

{ xil . .. xim+Um- i (g) : 1<ii <. .. <im<d }

is a K-basis of Um (g)/Um-i (g) (recall the convention that the empty pro- duct, in the case m=0, is equal to the unit element).

Notes

This last corollary obviously remains true, by choosing a total ordering of a K-basis of g, even if g is not finite dimensional.

Let t : gi —>g2 be a homomorphism of Lie algebras. Applying the universal property gives a homomorphism of K-algebras with unit

U (t) : U (gi) — ► U (g2)

g2 is commutative. We want to apply this in two specific situations. First let g1 and g2 two Lie algebras. Obviously, g1 x g2 again is a Lie algebra with respect to the componentwise Lie product. There are the corresponding monomorphisms of Lie algebras

Theorem. K-bilinear map

U (gi) x U (g2) — ► U (gi x g2)

(a, b) i — ^ U (ii) (a) U (i2) (b).

By the universal property of the tensor product it induces the map in the assertion as a K-linear map. The latter is bijective by a straightforward application. Since we have

[ii (x), i2 (y)]=[(^ (0, y)]= ([x, 0], [0, y])= (0, 0)

for any x ∈ gi and any y ∈ g2 it follows easily that U (ii) (a) and U (i2) (b), for any a ∈ U (gi) and any b ∈ U (g2), commute with one another. This implies that the asserted map is a homomorphism and hence an isomorphism of K-algebras with unit.

We point out that under the isomorphism in the above Theorem the elements

x C 1+1 C y<—> (x, y)

correspond to each other. Secondly, for any Lie algebra g the diagonal map

A : g — ► g x g

x l —> (x, x)

is a homomorphism of Lie algebras. We obtain the commutative diagram

Ag

g x g

c

U (g x U (g) g)

U (g) U (g). U (A)

Definition. The composed map U (g) —>U (g) CK U (g) in the lower line of the above diagram is denoted (by abuse of notation) again by A and is known the diagonal (or comultiplication) of the algebra U (g).

We note that for x $\in$ g C U (g) we have

A (x)=x 1+1 x.

11.7 THE CONCEPT OF FREE ALGEBRAS

In this section K again is an arbitrary field. We will discuss the following problem. Let A be a specific class (or category) of K-algebras. We have in mind the following list of examples:

ComK := all commutative and associative K-algebras with unit;

AssK := all associative K-algebras with unit;

LieK := all Lie algebras over K;

- AlgK := all K-algebras, i. $\in$. , all K-vector spaces A equipped with a K-bilinear "multiplication" map A x A —>A.

We suppose given a finite set X=[X \,.. ., Xd }, and we ask for an algebra AX in the class A together with a map X —>AX which have the following universal property: For any map X —>A from the set X into any algebra A in the class A there is a unique homomorphism Ax — ► A of algebras in A such that the diagram

Notes

$$\begin{tikzcd} X \arrow[rr] \arrow[dr] & & A \\ & \mathfrak{A}_X \arrow[ur] & \end{tikzcd}$$

is commutative. If it exists AX is known the free A-algebra on X.

The case ComK: The polynomial ring Ax := K[Xi,. . ., Xd] over K in the variables X1,. .. , Xd has the requested universal property.

The case Assk: As we have reknown in section 14 the tensor algebra

Ax := Asx := T (Kd)

of the standard K-vector space Kd together with the map

X — ► Kd C T (Kd)

Xi i —>i-th standard basis vector ei

satisfies the requested universal property. It sometimes is useful to view Asx as the ring of all "noncommutative" polynomials

P (Xi,.. ., Xd)= ^ 0 (i1,. ..)im)Xi1 . .. Xim

(i1,. . ., im)

with coefficients a (i1t. ., im) G K where the sum runs over finitely many tu- ples (i1,. . ., im) with entries from the set { 1,. . ., d } (including possibly the empty tuple). The multiplication is determined by the rule that the variables commute with the coefficients but not with each other. The algebra Asx in a natural way is graded by As^n) := Kd K. .. K Kd (n factors) which means that

Asx= ra>oAsXn) with AsXX ' AsXm) C AsX+m") for any l, m>0.

The case Algx: Here we have to preserve the information about the order in which the multiplications in a "monomial" Xi1 . .. Xim are per- formed (and we have to omit the unit element). This can be done in the following way. We inductively define sets X (n) for n>1 by X (1) := X and

X (n) := disjoint union of all X (p) x X (q) for p+q=n, and we put

Mx := disjoint union of all X (n).

The obvious inclusion maps X (m) x X (n) — Y X (m+n) combine into a "multiplication" map

px : Mx x Mx — ► Mx.

We now form the K-algebra

Ax := the K-vector space on the basis Mx

in which the multiplication is given by the linear extension of the map px. There are the obvious inclusions X C Mx C Ax.

Let y : X —>A be any map into any K-algebra A. We inductively extend to a map : Mx —>A by

Y : X (n) ^ X (p) x X (q) —>A

(x, y) 1 — ^ Y (x)Y (y).

This extension by construction is multiplicative in the sense

Mx x Mx ^ Mx X

Ax x Ax • > Ax

is commutative. Hence it further extends by linearity to a homomorphism of K-algebras

Y : Ax — ► A.

We stress that the algebra Ax is graded by

Ax := the K -vector space on the basis X (n),

i. ∈ . , we have

Ax= ^hAx^ with Ax A{ X c Aix+m) for any l, m>1.

The case LieK: In AX we consider the two sided ideal JX which is generated by all expressions of the form aa and (ab)c+ (bc)a+ (ca)b for a, b, c G AX.

Then

Lx := Ax/Jx with [a+Jx, b+Jx] := ab+Jx

is a Lie algebra over K.

Let y : X — ► g be any map into any Lie algebra g over K. As discussed above it extends to a homomorphism of K-algebras : Ax — ► g. We obviously have

Jx ^ ker ().

Hence there is a uniquely determined homomorphism of Lie algebras : LX —>g

is commutative.

Exercise. i. We have JX= nenJX n A^ and hence

LX= ^nL^ with [Lx, Lx^] ^ LX+m) for any l, m>1 if we define L^ := /JXnAX (i. ∈ . , the Lie algebra LX is graded).

The set X is (more precisely, maps bijectively onto a) K-basis of LX1.

The set { [Xi, Xj] : i<j } is a K-basis of.

The inclusion map X — X Asx extends uniquely to a homomorphism of Lie algebras

: Lx — x (Asx, [,]asx).

By the universal property of the universal enveloping algebra this map further extends uniquely to a homomorphism of associative K-algebras with unit : U (Lx) -x Asx.

Check your Progress-3

Discuss Universal Enveloping Algebra & Free Algebra

11.8 LET US SUM UP

In this unit we have discussed the definition and example of Elementary Functions, An Auxiliary Function, Semi Simple Lie Groups, Lie Groups, The Universal Enveloping Algebra, The Concept Of Free Algebras

11.9 KEYWORDS

Elementary Functions

An Auxiliary Function

Semi Simple Lie Groups

Lie Groups

The Universal Enveloping Algebra

The Concept Of Free Algebras

11.10 QUESTIONS FOR REVIEW

Explain Elementary Functions….. We consider the convergence of the exponential logarithmic and binominal series in this section

Explain An Auxiliary Function …. Throughout our discussion Fq shall denote a finite field consisting of q elements

Explain Semi Simple Lie Groups….. Let G be a semi simple Lie group worth a faithful representation. We state here two theorems the proof of which could be found .

Explain Lie Groups…. A Lie group G (over K) is a manifold (over K) which also carries the structure of a group such that the multiplication map

Explain The Universal Enveloping Algebra….. In this section K is allowed to be a completely arbitrary field .

Explain The Concept Of Free Algebras….. In this section K again is an arbitrary field. We will discuss the following problem. Let A be a specific class (or category) of K-algebras

11.11 REFERENCES

p-adic numbers: an introduction by Fernando Gouvea

p-adic Numbers, p-adic Analysis, and Zeta-Functions, Neal Koblitz (1984, ISBN 978-0-387-96017-3)

A Course in p-adic Analysis by Alain M Robert

Analytic Elements in P-adic Analysis by Alain Escassut

11.12 ANSWERS TO CHECK YOUR PROGRESS

Elementary Functions (answer for Check your Progress-1 Q)

An Auxiliary Function (answer for Check your Progress-1 Q)

Semi Simple Lie Groups (answer for Check your Progress-2 Q)

Lie Groups (answer for Check your Progress-2 Q)

The Universal Enveloping Algebra (answer for Check your Progress-3 Q)

The Concept Of Free Algebras(answer for Check your Progress-3 Q)

UNIT-12: THE CAMPBELL-HAUSDORFF FORMULA

STRUCTURE

12.0 OBJECTIVES

After studying this unit, you should be able to:

- Understand about The Campbell-Hausdorff Formula
- Understand about The Convergence Of The Hausdorff Series
- Understand about Formal Group Laws

12.1 INTRODUCTION

In mathematics, p-adic analysis is a branch of number theory that deals with the mathematical analysis of the functions of p-adic numbers.

The Campbell-Hausdorff Formula, The Convergence Of The Hausdorff Series, Formal Group Laws

Notes

12.2 THE CAMPBELL – HAUSDORFF FORMULA

Again K is an arbitrary field and X={ X1, . .. , Xd } is a fixed finite set. We recall that the free associative K-algebra with unit AsX on X is graded:

AsX=n>oAsX^ and AsX AsXX Q AsX+m') for any l, m>0.

Therefore

Asx := n AsX'1 n> 0

with the multiplication

n(an)n (bn)n := (aibn — i\n i=0

also is an associative K-algebra with unit (containing AsX as a subalgebra). It is known the Magnus algebra on X. Similarly as for AsX it is useful to view Asx as the ring of all "noncommutative" formal power series over K in the variables X1, . .. , Xd. In Asx we have the two sided maximal ideal

mx := { (n)n ∈ Asx : ao=0 }.

Theorem. i. AsX={ (an)n ∈ AsX : a0=0 }. "t" x

ii. 1+mX is a subgroup of AsX.

Proof. i. The map

AsX — ^ K (an)n 1 v a0

is a homomorphism of K-algebras with unit. The group of multiplicative units Asx therefore must be contained in the complement of the kernel of this map. Vice versa let a= (an)n ∈ Asx be an element such that a0=0. We have

a=a0 • (1— u) where u := (0, -a-1 • ai, . .. , -a-1 • an+1, . ..).

Since um ∈ { 0 } x.. . x { 0 } x n>m AsX the sum ^m>0 um is well defined in Asx. For b := a-1 • (^2m>0 um) we then obtain ab=ba=1.

ii. This is obvious Note that 1+mx is the kernel of the homomorphism of groups

AsX — ► K x (an)n 1 ^ a0.

In the last proof we have used a special case of the following general principle. For each m>0 let u (m) ∈ { 0 } x.. . x { 0 } x n>m AsX be some

element. Then the sum ^m>0 u (m) ∈ Asx is well defined. In particular, for any u ∈ mx we have the well defined homomorphism of K-algebras with unit

eu : K[[T]] — ^ Asx F (T) — ^ F (u).

Proposition If the field K has characteristic zero then the maps exp : mx —>1+mx and log : 1+mx —>mx

u — • ∈ n 1+u — ^ ∈ (— i)n+1 un n>0 n>1

are well defined and inverse to each other.

Proof. exp (u)=eu (exp (T)) and log (1+u)=e« (log (1+T)) the maps in the assertion are well defined. Applying eu to the identities

exp (log (1+T))=1+T and log (exp (T))=T in the ring Q[[T]] shows that they are inverse to each other.

Exercise. If a, b ∈ mx commute with each other (multiplicatively) then we have

exp (a+b)=exp (a) exp (b).

we can view Lx as the Lie, subalgebra of Asx "generated" by the elements X \,. .. , Xd. Moreover, we have

Lx=Lx) Lx2).. . Asx=K AsX) AsX).. .

We now define

Lx := ^ L^ C mx C Asx. n> 1

Theorem. LX is a Lie subalgebra of AsX.

Proof. Let a= (an)n and b= (bn)n be any two elements of LX. We have to show that ab— ba ∈ LX holds true. For any m>1 we put

a (m) := (0, ai, . .. , am, 0, . ..), v (m) := (0, . .. , 0, am+i, am+2, . ..),
b (m) := (0, bi, . .. , bm, 0, . ..), u (m) := (0, . .. , 0, bm+i, bm+2, . ..).

Then a (m), b (m) ∈ LX and hence a (m)b (m)— b (m)a (m) ∈ LX. Moreover

ab— ba= (a (m)+v (m)) (b (m)+u (m))— (b (m)+u (m)) (a (m)+v (m)) =
a (m)b (m)— b (m)a (m)+ (0, . .. , 0, cm+i, . ..).

It follows that for n<m we have

n-th component of ab— ba=n-th component of a (m)b (m)— b (m)a (m) ∈ Lln). Since m was arbitrary we conclude that ab— ba ∈ LX.

Since U (LX)=AsX can view the comultiplication A of U (Lx) as a homomorphism of K-algebras with unit

A : Asx — ► Asx Ask.

It satisfies A (Xj)=Xj 1+1 Xj for any 1<i<d. Since the Xi, . .. , Xd form a K-basis of AsX) it follows that

A (AsXX C AsXi) K AsX0)+AsX0) K AsXi)

and then inductively that

A (4s<=>) C [, 4s™ AsX"] l+m=n

for any n>0. This makes it possible to extend A to the homomorphism of K-algebras with unit

A : 4sx=n 4sXn) —>4sx k4sx := n [4s{ X +k 4s^]

n>0 l, m>0 = n [4sX K 4sX">]

n>0 l+m=n (an)n 1 4 (yA (an)n.

Theorem. If the field K has characteristic zero then we have Lx={ a ∈ 4sx : A (a)=a 1+1 a }.

Proof. Let a= (an)n ∈ 4sx be any element. We have A (a)=a+1+1 a if and only if A (an)=an +1+1 an for any n>0. Latter is equivalent to an ∈ Lx n As□□□=L^ for any n>0 which exactly is the condition that a ∈ Lx.

Theorem. (Campbell-Hausdorff) Suppose that K has characteristic zero; then the map

exp : Lx — 4 { b ∈ 1+mx : A (b)=b <g> b }

is a well defined bijection; moreover, the right hand side is a subgroup of 1+m x.

Proof. The second part of the assertion follows immediately from A being a ring homomorphism. Since Lx C mx the map exp is defined on Lx and is injective. For the subsequent computations we observe that the componentwise construction of the ring homomorphism A implies that A commutes with the maps exp and log. First let a ∈ L x. Then A (a) = a 1+1 a, and we compute

A (exp (a))=exp (A (a))=exp (a 1+1 a)

= exp (a 1) exp (1+a)

= (exp (a) 1) (1+exp (a))

= exp (a) exp (a).

This shows that exp (a) indeed lies in the target of the asserted map. Vice versa let b ∈ 1+mX such that A (b)=b 0 b. We can define a := log (b) ∈ mX so that b=exp (a). We compute

A (a)=A (log (b))=log (A (b))

= log (b 0 b)=log ((b 0 1) (1 0 b))

= log (b 0 1)+log (1 0 b)

= log (b) 0 1+1 0 log (b)

= a 0 1+1 0 a.

Hence implies that a $\in$ LX. We observe that the asserted map is surjective.

Corollary. Suppose that the field K has characteristic zero; then LX equipped with the multiplication

a 0 b := log (exp (a) exp (b))

is a group whose neutral element is the zero vector 0 and such that — a is the inverse of a.

Proof. Since exp (0)=1 the neutral element for 0 must be the zero vector 0. Furthermore, since a and — a commute with respect to the usual multi- plication in AsX we have exp (a) exp (— a)=exp (— a) exp (a)=exp (0)=1. Hence a 0 (— a)= (— a) 0 a=log (1) =0.

Definition. For the field K=Q and the two-element set { Y, Z } we call

H (Y, Z) := Y 0 Z $\in$ L{ Y, Z } c as{ y, z } the Hausdorff series (in Y and Z).

As alluded to earlier we should view H (Y, Z) as a noncommutative formal power series in the variables Y, Z with coefficients in the field Q. We have

exp (Y) exp (Z)=1+W with W=^ Y+ ZS

r+s>1 H (Y, Z) — $\in$ (-1)

(-1)m+i/^~^ y r ZM m m V / ^ r! s! / m>1 r+s>1

(-1)m+1 TTY^. Zfi

/ / -* m/ j H rg si!

n>1 r+s=nm= 1 ri+.. . +rm =r i=1

si+.. . +sm=s ri+si>1, . .. , rm+sm>1

Here and in the following the product sign Hm=1 always has to be under- stood in such a way that the corresponding multiplications are carried out in the order of the enumeration i— 1, . .. , m. It is convenient to use the abbreviations

Hrs : — V V T]Y^ ZSL

r, s Z_^ m Z_^ H ri! si!

m= 1 ri+.. . +rm =r i= 1

si+.. . +sm=s ri+si>1, . .. , rm+sm>1

and

Hn : — ^ ^ Hr, s r+s=n

We note that Hr, s is a sum of noncommutative monomials of degree r in Y and s in Z. As a sum of noncommutative monomials of total degree n the element Hn lies in As{ yZ }. We have

H— Hn or, more formally, H— (Hn)n. n> 1 (n)

From the theory we know that Hn ∈ L{ Yz } for each n>1 but this is not visible from the above explicit formula.

Examples. H1, 0— Y, H0, 1— Z, and H1— Y+Z.

Hr, 0— H0, r— 0 for any r>2 (observe, for example, that Hr, 0 is the term of degree r in log (exp (Y))— Y).

H2— H2, 0+H11+Ho, 2— H11— YZ - 1 (YZ+ZY)— 1 [Y, Z].

If g is any Lie algebra over (any) K then the K-linear map

ad (z) : g — ► g

f 1 — ► ^ f],

for any z ∈ g, is a derivation in the sense that

ad (z) ([f, y])=[ad (z) (f), y]+[f, ad (a) (y)] for any f, y ∈ g holds true.
This is just a reformulation of the Jacobi identity in g.
Proposition(Dynkin's formula) For r+s>1 we have

Hr, s=r+s (K, s+Ks)

Notes

with H'r s defined as

m — 1 <=Dm-1 ∈ ((IPdYP ∘ -sp, ∘ -ppz)

m>1 ri+.. . +rm=r i=1

si+.. . +sm_i =s — 1 ri+si>1, . .. , rm_i+sm_i>1

and m — 1

Hg := ∈ 0)0 ∈ (Il^o ^ (Y) •

m>1 ri+.. . +rm_i=r — 1 i=1

si+.. . +sm_i=s ri+si>1, . .. , rm_i +sm_i>1

Remark. Suppose that K has characteristic zero; then we have

a 0 b=H (a, b) for any a, b ∈ LX •

Proof. The above explicit computations including Dynkin's formula were completely formal and therefore are valid for any a, b (instead of Y, Z). The expression H (a, b), of course, has to be calculated componentwise in AsX using the observation.

The exploitation of these "universal" considerations is based upon the following technique. For any finite dimensional K-vector space V let

Map (V x V; V) := K-vector space of all maps f : V x V —► V.

We pick a K-basis e1, . .. , ed of V.

Definition. A map f : V x V —>V is known polynomial (of degree (r, s)) if there are (homogeneous) polynomials Pi (X1, . .. , Xd, Y1, . .. , Yd) over K (of degree r in X1, . .. , Xd and degree s in Yi, . .. , Yd), for 1<i<d, such that

f (5^aiei, ^kiei)=^2 Pi (ai, . .. , ad, bi, . . . , bd)ei for any ai, bi G K.

In Map (V x V; V) we have the vector subspace Pol (V x V; V) of all polynomial maps. It decomposes into

Pol (V x V; V)= „>o Pol„ (V x V; V)= „>o r+s=n Polr, s (V x V; V) where Polr, s (V x V; V) denotes the subspace of all polynomial maps of degree (r, s) and Pol,, (V x V; V) := r+s=,, Polr, s (V x V; V) is the subspace of all polynomial maps of total degree n.

Theorem. Given any f G Polr, s (V x V; V) and gi G Pol1i, mi (V x V; V) for i=1, 2 the map (v, w) i — ► f (gi (v, w), g2 (v, w)) lies in Polrii+si2, rmi+sm2 (V x V; V)'

Corollary. The property of a map f : V x V —>V of being polynomial

(of a certain degree) does not depend on the choice of the K-basis of V.

Suppose now that the vector space V is a Lie algebra g of finite dimension d := dimK g. Then also the vector space Map (g x g; g) is a Lie algebra with respect to the Lie product

[f, g] (hy) := [f (xy)].

Corollary Pol (g x g; g) is a Lie subalgebra of Map (g x g; g); more precisely,

We identify the two-element set { Y, Z } with the subset of Pol (g x g; g) consisting of the two projection maps pr^ : g x g —>g by sending Y to pr1 and Z to pr2. By the universal property of free Lie algebras this extends uniquely to a homomorphism of graded Lie algebras

0 : L{ y, z } — ► Pol (g x g; g).

It satisfies

e ([Y, a]) (y, z)=[y, ∈ (a) (y, 3)] and 0 ([Z, a]) (y, z)=[z, ^ (a) (y, 3)] for any a ∈ L{ Y, Z }.

We define

Pow (g x g; g) := Poln (g x g; g) n>0

as a K-vector space. The elements of Pow (g x g; g) can be viewed (if K is infinite, and after the choice of a K-basis of g) as d-tuples of usual formal power series in the variables Y1, . .. , Yd, Z1, . .. , Zd with coefficients in K. As a consequence of the Lie product on Pol (g x g; g) extends by

[(fn)n, (gn)n] := ([fl, 9m])n l+m=n

to a Lie product on Pow (g x g;g). Being graded 0 extends to the K-linear map 0 : L{ y, z } — ► Pow (g x g; g)

(fn)n I ► (0 (fn))n.

Using the trick obtain for any m ∈ N, with the notations in this proof, that

0 ([a, b])=0 ([a (m), b (m)])=[0 (a (m)), 0 (b (m))]

= [0 (a), 0 (b)] mod ^ Poln (g x g; g) n>m

for any a, b ∈ L{ y, z }. Since m is arbitrary this means that 0 also is a homomorphism of Lie algebras.

From now on we assume for the rest of this section that the field K has characteristic zero. We put

H := Hg := § (H) ∈ Pow (g x g; g).

More precisely, we have

H=^ Hr, s with Hr, s := 9 (Hr, s) ∈ Polr, s (g x g; g). r+s>1

Using Dynkin's formula in Prop. 16. 7 implies that

Hr, s=r+s (H'r>s+H<=s)

With H 1, 0=pr1; H0, 1=pr2, and

H 1, 1 : g x g

(y, z) 1 — ► 2 [y> 3] 2

H (a, H (b, c))=H (H (a, b), c), H (a, 0)=H (0, a)=a, and H (a, -a)=0

for any a, b, c ∈ L{ y, z }. In order to use this we reinterpret the evaluation of H in a and b in the following way.

Let a, b ∈ L{ y, z } be any two elements. By the universal property of free Lie algebras there is a unique homomorphism of Lie algebras mapping Y to a and Z to b. By construction it satisfies

ea, b (LPz }) C { 0 }x.. . x{ 0 }x n 4n;z }

for any m>1 and therefore extends, by the observation before the K-linear map

ba, b : L{ Y, Z } > L{ Y, Z }

(cn)n 1 ' ^ ^ <=a, b (cn). The same reasoning as for 0 shows that ea, b in fact is a homomorphism of Lie algebras. On the other hand of course, ea>b is the restriction of a corresponding unique homomorphism of associative K-algebras with unit

<=a, b : As{ Y, Z } ► As{ Y, Z }.

Viewing an element in As{ y, z } as a noncommutative polynomial G (Y, Z) it is clear that

Ca, b (G)=G (a, b)

holds true. It follows that

ba, b (H)=^ €a, b (Hn)=^ Hn (a, b)=H (a, b).

There is an analogous construction for the Lie algebra Pow (g x g;g). Quite generally, given any g1, g2 ∈ Map (V x V; V) there is the homomor- phism (of Lie algebras in case V=g)

Map (V x V; V) — ► Map (V x V; V)

f 1 — ► f (gi, g2) (v, w) := f (gi (v, w), g2 (v, w)).

If g1, g2 ∈ Pol (V x V; V) then says that it restricts to

Pol (V x V; V) — ► Pol (V x V; V)

and satisfies

f (gi, g2) ∈ Polrni+sn2 (V x V; V)

if f ∈ Polr, s (V x V; V) and gi ∈ PoU, (V x V; V).

Hence for g \, g2 in

Pow0 (g x g; g) := { 0 } x Poln (g x g; g)

we obtain, by the usual componentwise procedure, a homomorphism of Lie algebras

Pow (g x g; g) — ► Pow (g x g; g) f — ► f (gi, g2).

Indeed, this is just a reformulation of the fact that a formal power series without constant term can be inserted into any formal power series. We note that pri (gi, g2)=gi.

As before let now a, b G L[y, z] be any two elements. Then 0 (a), 9 (b) lie in Pow0 (g x g; g) Hausdorff series H G L{ y, z } and various choices for the elements a and b. For a := Y and b :=— Y we have 0 (a)=pr1 and 0 (b)= — pr1 and we obtain from that

- H (Y, — Y) "^Hf (pri, — pri).

Since H (Y, — Y)=0 by the assertion i. follows. For a := Y and b := 0 we similarly obtain

Hi ^ H (Y, 0)

H > tf (pri, 0).

Again we have H (Y, 0)=Y and hence H/ (pr1, 0)=pr1 which is the assertion ii. The last assertion iii. comes symmetrically from the choice a := 0 and b := Y.

The discussion leading to the commutative can easily be generalized to the three-element set { U, Y, Z } and the Lie algebra

Pow (g x g x g; g)

of d-tuples of formal power series over K ind variables. We leave the details to the reader. This leads to the homomorphism of Lie algebras

: L{ u, y, z } — ► Pow (g x g x g; g)

which sends U, Y, and Z to pr1, pr2, and pr3, respectively. For any choice of elements a, b ∈ L{ U, Y, Z } we obtain, analogously the commutative - Y, Z Ho, i -

L{ Y, Z } ^ L{ U, Y, Z }

Pow (g x g; g) ; ; 5- Pow (g x g x g; g). f (0 (a), 0 (b))

Theorem Suppose that K has characteristic zero; we then have

(pri, ld (pr2, pr3))=!L (lL (pri, pr2), pr3).

Proof. Apply to the Hausdorff series H ∈ L{ Y, Z } and the two choices a := U, b := H (Y, Z) and a := H (U, Y), b := Z, respectively

12.3 THE CONVERGENCE OF THE HAUSDORFF SERIES

We fix a Lie algebra g of finite dimension d over a field K of characteristic zero. We also pick a K-basis ∈ \,. .. , ed of g.

Definition. The elements 7kj ∈ K, for 1<i, j, k<d, defined by the equations d[ei, ej]=Yij ek

are known the structure constants of g with respect to the basis { ei }1<i<d. If we define the Lie product [,]' on Kd by

(23) \{ vi, . .. , Vd), (Wi, . .. , Wd) }'= (^2 Yij VWj,. .. ^7ij- nwj)

i, j i, j

then the isomorphism g=Kd becomes an isomorphism of Lie algebras. Using this same isomorphism we also can view the element

H=Hg ∈ Pow (g x g; g)

as a d-tuple

H (Y, Z) := Hg (Y, Z)= (H (i) (Y, Z), . .. , H (d) (Y, Z))

of formal power series H (i) (Y, Z) over K in the variables Y= (Yi, . .. , Yd) and Z= (Z1, . .. , Zd). That

H (i) (Y, Z)=Yi+Zi+2 ^ YjkYjZk+.. .. j, k

Theorem. i. H (Y, 0)=Y, H (0, Z)=Z. ii H (Y, -Y)=0.

iii. H (U, H (Y, Z))=H (H (U, Y), Z).

From now on let (K, ||) be a nonarchimedean field of characteristic zero. Via the linear isomorphism g=Kd we can view g as a manifold over K (but which structure does not depend on the choice of the basis).

Let us suppose at this point that there is an ∈ > 0 such that

H (Y, Z) G F<= (Kd x Kd; Kd) and ||H| | ∈ < e

(where Kd is equipped with the usual maximum norm). We then consider the open submanifold

G := B (0) C Kd=g.

Obviously

G x G<= G<=

(g, h) i — ► gh := H (g, h)

is a well defined locally analytic map.

gi0=0gi=gi, gi (-gi)=0, and gi (g2gs)= (gig2)g3

for any gi, g2, g3 G C<=.

Proposition. C<= is a d-dimensional Lie group over K whose neutral element is the zero vector 0 and such that — g is the inverse of g G G<=.

If two ∈ > e'>0 satisfy then G<= of course is an open subgroup G<=.

Definition. { G<= }<= is known the Campbell-Hausdorff Lie group germ of the Lie algebra g.

What is the Lie algebra of G<= We have the "global" chart c := (G<=, C, Kd) for the manifold G<= and correspondingly the locally analytic isomorphism

rc : G<= x Kd — ^ T (G<=)

(g, v) 1 ^ M] G Tg (G<=)

as well as the linear isomorphism

Can (G<=, Kd) — ^ r (G<=, T (G<=))

/ 1 ^ C/ (g)=Tc (g, f (g))=[c, f (g)] G Tg (G<=).

we know that the Lie product of vector fields corresponds on the left hand side to the Lie product

[fh Mg)=Dg/i (/2 (g)) - Dgf2 (/i (g)).

On the other hand the Lie product on Lie (G<=)=T0 (G<=) is induced via the inclusion

To (Ge) -^ r (G<=, T (Ge))

t 1 ► Ct (g)=T0 (rg) (t)

by the Lie product of vector fields. By the construction of the tangent map T0 (rg)

Proposition. Lie (G<=)=g as Lie algebras.

Proof. By the above discussion it suffice to show that

[,]'=[,]"

holds true. To further compute the Lie product [,]" we start from the identity

rg (h)=H (h, g).

Since, H does not contain monomials of degree (0, s) in (Y, Z) with s>2 we can write

H (i) (Y, Z)=Zi+Y, P (i, j) (Z)Yj+terms of degree>2 in Y.

we deduce that

D, aH, i) (Y, g) ^ t (^

Dor'g P — W — i t, j=<P (i. j) (gti, j °Yj |y=o

and hence that

fv (g)=D0 (rg) (v)= (Y vj P (i, j) (g), . .. , Y vj P (d. j) (g))

for any v= (vi, . .. , vd) ∈ Kd. To derive the function fv in 0 we must derive the P (i. j) (Z) in Z and subsequently set Z=0. By can write

p (i. j) (Z)=tij+2<= YjfcZfc+terms of degree>2 in Z

where tij denotes the Kronecker symbol. It follows that

d^i. j) (Z)=i y i SZk iz=0 2 'jk

and hence that

Dofv= (2 ∈ jvj)i, k

And (d d)

D0fv (w)= (2 ∈ Yjkvjwk, . .. , 21] Yjkvj wj)

j, k= 1 j, k= 1 = 1 [v, w]'

for any v= (v1, . .. , vd), w= (w1, . .. , wd) G Kd. We conclude that [v, w]''=Dofv (w) - Dofw (v)=2[v, w]' - 2[w, v]'=[v, w]'.

Having observen the interesting consequences of a possible convergence of the Hausdorff series we now must address the main question of this section whether satisfying exists.

Using the isomorphism g=Kd any element f G Pol (g x g; g) can be viewed as a d-tuple f of polynomials in the variables Y and Z and hence, in particular, as an element f G F<= (Kd x Kd; Kd) for any ∈ > 0. Since the polynomials in Hr, s := Hr, s are homogeneous of total degree r+s we have

|| H 11 11 H II er+s

\\Hr, s\ \ ∈ — ||Hr, s||1e.

Suppose that there is a 0<e0<1 such that

\Hr, s\1 < ∈ - (r+s-1) for any r+s>1.

It follows that for any 0 < ∈ < e0 we have

||Hr, s| | ∈ = \Hr, s\1er+s<||Hr, s||1e0+s-1e < ∈ for any r+s>1

and

lim ||Hrs| | ∈ < ∈ lim \Hrs\1er+s-1

r+s^ro — r+s^ro —

= ∈ +lim |Hr, s|ie0+s-1 (%)r+s-i

r+s^TO 0< ∈ lim (—)r+s-i

r+s^TO o

As

H=^ Hr, s r+s>1

we conclude that for any 0 < ∈ < e0.

The coefficients of the Hausdorff series H are explicitly known and their absolute values therefore can easily be estimated. But in order to translate this knowledge into an estimate for the norms ||Hr, s||i we need a particularly well behaved basis of the K-vector space L{ YZ }.

The free K-algebra A{ Y, z } by construction has the K-basis M{ y, z } = Ura> 1{ Y, Z } (n). For any x G M{ YZ } we let ex denote its image in the factor algebra L{ Y, Z }. These ex obviously generate L{ YZ } as a K-vector space. Hence there exist subsets B C M{ Y, Z } such that { ex }xeB is a K-basis of L{ y, Z }. In the following we have to make a particularly clever choice of such a subset B. But first we note that also the free associative K-algebra with unit As{ Y, Z } has an obvious K-basis which is the set Mon{ YZ } of all noncommutative monomials in Y and Z. All of this is valid over an arbitrary field K. Since our K is nonarchimedean we can introduce the oK-submodules

As{ Y, Z } := ^ 0K^

^GMon { y, z }

of As{ y, z } and

L{ "ya, Z } := L{ y, z } n As{ Y^, Z }

of L{ Y, Z }.

Proposition i. (K arbitrary) There is a subset B C M{ YZ } such that we have

{ ex }x€B is a K-basis of L{ Y, z },

{ Y, Z } C B, and

for any x G B\{ Y, Z } there are x', x" G B with x=x'x" and, in particular, ex=[ex /, ex«].

ii. (K nonarchimedean) There is a subset B C M{ YZ } as in i. and such that

L{ Y, z }=^ 0kex ' x€B

We now define the constant e0 by

|p|p-1 ∈ - 1 if K is p-adic for some p,

e-1   otherwise

where

e1 := max (1, max 1yk|) i, j, k

We note that 0<e0<1. The constant e1 has the property that l|[/, g]||i<e1^/||1NgN1 for any f, g ∈ Pol (g x g;g).

Theorem. Let { ex }xeB be any K-basis of L{ Y, Z } then have

N^ (ex)|1<en-1 for any x ∈ B (n) := B n { Y, Z } (n).

Proof. We proceed by induction with respect to n. For x=Y we have d (eY)=pr1 and hence d (eY)= (Y1, . .. , Yd) so that Hd (eY)|1=1=e1. The case x=Z is analogous. Any x ∈ B (n) with n>2 can be written as

x=x'x" with x' ∈ B (l), x" ∈ B (m), and l+m=n.

Since l, m<n we can apply the induction hypothesis to x' and x" and obtain

l|0 (e*)N1=ll^ ([ex', ex"])||1=P (ex'), 0 (eT/')]||1

e1|^ (ex/) N1 H0 (ex") N1 e1e1-1em-1=ef-1.

Proposition. For any 0 < ∈ < e0 we have H ∈ F ∈ (Kd x Kd; Kd) and

on n. u. f or any 0<c<e0 we have h ∈ f ∈ (Kd v lTd\

IHL < ∈ .

Proof. As discussed it suffices to show that

|Hr, s|1 < ∈ - (r+s-1) for any r+s>1.

We fix n := r+s>1. We also pick a basis { ex }xeB as

Hr, s— ^ ^ cxex. Since Hr, s G L{ Y, z } we in fact have

Hr, s —

where B (n)— B n { Y, Z } (n).

then implies that

llHVIi<max |cx|||0 (ex)||i<si-1 max |cx |.

xGB (n) xGB (n)

In order to estimate the |cx| we have to distinguish cases. But we emphasize that this is a question solely about the Hausdorff series (and not the Lie algebra g) and therefore, in principle, can be treated over the field Q.

Case 1: K is not p-adic for any p. Since Q C K we can choose the basis already over the field Q. Then all coefficients cx lie in Q. we have |cx|— 0 or 1 and hence |Hr, s|1<^n — 1— eo (n-1).

Case 2: K is p-adic for some p. we have Qp C K and

_ log |p| |a|— |a|- logP for any a G Qp.

Hence we can assume without loss of generality that (K, ||)— (Qp, ||p), and we choose B as in We want to show that n — 1

max |cx|p<pp — 1. xGB (n)

Since the left hand side is an integral power of p this amounts to showing that

plCx G Zp : — 0qp for any x G B (n) where l is the unique integer such that

i<1 <i+1.

By our particular choice of the set B this is equivalent to

plHr, s G Ljyz } and hence to plHr, s G A^^Z }. The explicit form of the coefficients of Hr, s then reduces us to showing that

| mn dc. |p<1, or equivalently, |^J|ri!si!|p>p — l

whenever 1<m<n, r1+.. . +rm=r, s1+.. . +sm=s, and ri+si>1. But implies

|m n ri!si!|p>p — p — 1 ((m — 1)+ (ri+S1-1)+.. . +(rm+Sm-1))

n — 1 = p — p — 1.

Since the left hand side is an integral power of p it indeed must be>p — l.

Check your Progress-1

Discuss The Campbell-Hausdorff Formula & Convergence

12.4 FORMAL GROUP LAWS

Let K be any field of characteristic zero. We fix a natural number d, and let R := K[[Y1, . .. , Yd, Z1, . .. , Zd]\ denote the ring of formal power series over K in the variables Y= (Y1, . .. , Yd) and Z= (Z1, . .. , Zd).

Definition. A formal group law (of dimension d over K) is a d-tuple F = (F1, . .. , Fd) of power series Fi ∈ R such that we have:

F (Y, 0)=Y and F (0, Z)=Z,

F (U, F (Y, Z))=F (F (U, Y), Z).

We observe that the condition (i) implies that

Fi (Y, Z)=Yi+Zi+terms of degree>1 both in Y and Z.

Hence the two sides in the condition (ii) are well defined.

Examples. 1) Fi (Y, Z)=Yi+Zi.

F (Y, Z)=Y+Z+YZ (for d=1).

F := for a finite dimensional Lie algebra g over K (and some choice of K-basis of g).

The last example has a converse. Let F be any formal group law. We have

Fi (Y, Z)=Yi+Zi+^ cjkYj Zk+terms of degree>3.

We define a bilinear map : Kd x Kd — ► Kd by

bp ((vl, . .. , Vd), (wl, . .. , Wd)) := ^ c1k vj wk, . .. ^ cdk vj wk),

and we put

[v, w]f := (v, w)— 6f (w, v) for v, w ∈ Kd.

Theorem [,]f satisfies the Jacobi identity.

Proof. We observe that [,]f is a Lie product on Kd. In the case of the formal group law it follows from the that [,]h« coincides (up to the isomorphism g=Kd) with the Lie product on g.

Next we discuss a observemingly very different construction of a formal group law from a finite dimensional Lie algebra g over K by using the universal enveloping algebra U (g). We have the following list of K-linear maps:

(multiplication) m=mg : U (g) 0K U (g) —>U (g),

(unit) ∈ = eg : K —>U (g) sending a to a 1,

(comultiplication) A=Ag : U (g)— (— >U (g x g)=U (g) 0K U (g),

Notes

(counit) c=cs : U (g)=T (g)/J (g) -g °=K.

Of course, the maps m and ∈ satisfy the axioms for a (noncommutative) associative K-algebra with unit, and A and c are homomorphisms of K-algebras with unit. In addition, the maps A and c have the following properties:

(counit property) (c C id) o A=id= (id 0 c) o A ;

(coassociativity) (id 0 A) o A= (A 0 id) o A ;

(cocommutativity) U (g) A U (g) 0K ^ (g) x y^y X " U (g) 0K U (g)

is commutative.

They easily follow, by applying the universal property of U (g), from the corresponding properties of the diagonal map A : g —>g x g. We now consider the K-linear dual

U (g)* :=HomK (U (g), K) together with the K-linear map

y : U (g)* Ok U (g)* — U [U (g) Ok U (g)]* --U U (g)*. li O I2 1 — ► [x O y u li (x) ^ (y)]

Proposition. (U (g)*, y, c) is a commutative and associative K-algebra with unit.

In order to determine the algebra U (g)* explicitly we pick an (ordered) K-basis e1, . .. , ed of g. We know from the Poincare-Birkhoff- Witt theorem that the

e« := On '.. . ' OdT for a= («i, . .. , «d) ∈ N

form a K-basis of U (g).

Proposition The map

U (g)* -U K[[Ui, . .. , Ud]]

I -u Fe (U) := ∈ l (ea)Ua «end

is an isomorphism of K-algebras with unit onto the ring of formal power series over K in the variables U={ Up.. . , Ud }.

Proof. The fact that { ea }a is a K-basis of U (g) immediately implies that the asserted map is a K-linear isomorphism. The unit element c of U (g)* is the projection map onto Ke0=K which is mapped to Fc=1. For the multiplicativity we first recall that

A (e?)=A (efc)m= (efc O 1+1 O efc)m

m= EC?) (ek O 1) (1 O em-')0m-iek m= ∈ ("?)ek O e?-i

for any 1<k<d and any m>0. By induction one deduces that (30) A (ea) = ∈ e^ O eY for any a ∈ NO f3+j=a

holds true. We now compute

F^ (<=1, <=2){ lD = ∈ Kh, h){ ea)Ua = ∈ (^i ^) (A (e«))Ua

= EE fi (e«)<2 (e, -)US+1"

a ^+7=a

= (∈ ^i (e^)U ^) (∈ ^2 (e7)UY)

= F, 1 (U)F, 2 (U).

By dualizing the multiplication map

U (g X g)=U (g) U (g) — U U (g) we obtain a K-linear map

U (g)* — -U U (g x g)*.

Applying to both sides (with (e1, 0), . .. , (ed, 0), (0, e1), . .. , (0, ed) as an ordered K-basis for g x g) we can view the latter as a K-linear map

K [[Ui, . .. , Ud]] - — U K [[Y1, . .. , Yd, ZiZd]]=R.

We define F (i) := m* (Ui) ∈ R and Fg := (F (i), . .. , F{ d)).

At this point we have to recall a few basic facts about formal power series rings. First of all, the formal power series ring K[[Ui, . .. , Ur]] has a unique maximal ideal mu which is the ideal generated by Ui, . .. , Ur. This is an immediate consequence of the fact that any formal power series F over K with F (0)=0 is invertible.

Definition. i. A commutative ring with unit is known local if it has a unique maximal ideal.

ii. A homomorphism of local rings is known local if it maps the maximal ideal into the maximal ideal.

Consider two formal power series rings K[[U \,. .. , Ur]] and K[[Vi, . .. , Vs]]. For any F= (Fi, . .. , Fr) G my x.. . x my the map

<=f : K [[Ui,. .. , Ur]] K [[Vi, . .. , Vs]]

G - — ► G (F) := G (Fi, . .. , Fr)

is a well-defined local homomorphism of local rings. We have <=f (Ui)=Fi.

Theorem Let ∊ : K[[Ui, . .. , Ur]] —>K[[Vi, . .. , VS]] be any homomorphism of K-algebras with unit which is local; we then have

<==<=f with Fi := ∊ (Ui).

Proof. Since ∊ is local we have Fi G my so that <=f is well defined. Both <= and <=f are homomorphisms of K-algebras with unit. Hence the identities <= (Ui)=<=f (Ui) imply that

<= (G)=<=f (G) for any polynomial G G K [Ui, . .. , Ur].

We now write an arbitrary formal power series G G K[[Ui, . .. , Ur]] as

G=^ Gn n> 0

where Gn is a homogeneous polynomial of degree n. In particular, Gn lies in mU. Since ∊ is local we obtain ∊ (Gn) G m^. Therefore the element

Y, ∊ (Gn) G K[[Vi, . .. , Vs]] n>0

is well defined. We have

<= (G) — ∊ (Gn) = ∊ (G0)+.. . +<= (Gk)+<= (Gn)— YY ∊ (Gn)

= ∈ (Y Gn)— Y ∈ (Gn)

G mV+i

for any k>0. Since P|k>0 mV+i={ 0 } we conclude that

<= (G)=Y ∈ (Gn).

The same reasoning, of course, applies to ef• Hence

e (G) = ∈ (Gn)=eF (Gra)=eF (G)

TnJ— / J ^b'x^n) Proposition i. m* is a local homomorphism.

ii. m*=epe.

is a formal group law.

[,]pe coincides (up to the isomorphism g=Kd given by the basis e \,. .. , ed) with the Lie product on g.. FG is a formal group law.

ii- [,]fg c coincides, modulo the isomorphism Of1 : g=Te (G) Kd, with the Lie product on g.

Proof, i. Because of <^ (∈) =0 we have

FG c (v, 0)=v and FG, c (0, w)=w for any v, w ∈ B<= (0).

Again using the identity theorem this translates into the identities of formal power series

Fg, c (Y, 0)=Y and Fg, c (0, Z)=Z.

In particular, the formation of

Fg, c (U, Fg, c (Y, Z)) and Fg, c (Fg, c (U, Y), Z)

is well defined. For sufficiently small d>0 these formations commute with the evaluation in any points u, v, w ∈ B (0). But by the associativity of the multiplication in G we have

FG, c (u, FG, c (v, w))=FG, c (FG, c (u, v), w) for any ^ F w ∈ BS (0). By a third application of Cor. 5. 8 this translates into the identity of formal power series

FGtM, FGtC (Y, Z))=FGtC (FGtM, Y), Z).

Theorem. The Lie group G has a family { H\a\ }\a\ of open subgroups indexed by the sufficiently big |a| ∈ |K| which forms a fundamental system of open neighbourhoods of ∈ e G and such that each H|a| is isomorphic, via <P> to* (0), FG, c)- |a|

Proof. With ∈ > 0 as above we put e0 := ||FG)C||<=, and we choose any |a|>max (1, -2) (so that, in particular, ^ < ∈). We claim that

||fg>cII^<H holds true. Let FG, c (Y, Z)=Y+Z+^ va, gYaZ3 with va, g ∈ Kd. \a \, \3\>1

We have |va, 3||<e0e-\a\-\3\ and hence

IIZgJ I1I=max (Ia, \aItjK ! |v,,, 31)

max (-p-r, max e0(t4-)\a \+\ 3\)

H M, \3\>i \-\-

max(\ -\, eo("--)2)

R.

By possibly enlarging the lower bound for |a| we can make exactly the same

argument for the power series expansion of the map g i —>g-1 on G in a

Sufficiently small neighbourhood of <^ (∈) =0. The family

H\a\ := T-1(B_x_(0)) then has the required properties.

\ \ M

Corollary. Every Lie group is paracompact.

Proof. We find an open subgroup H C G which as a manifold is isomorphic to a ball B- (0). Any coset gH, for g ∈ G, then is isomorphic, as a manifold, to B- (0) as well. By the ultrametric space B- (0) and therefore any coset gH is strictly paracompact. As a disjoint union of cosets gH the Lie group G also is strictly paracompact.

Remark. If Ge is the Campbell-Hausdorff Lie group germ of a Lie algebra g then we have

H0=F gs, c for the chart c := (Ge, C, Kd).

In the present situation of a Lie group G and with the choice of the K-basis of g which corresponds to the standard basis of Kd under the isomorphism 0-1 : g - —+Kd we now have the three formal group laws

H0, F0, and Fg, c

whose Lie products

[, }Hg=[, }Fg=[, }fg, c

coincide and coincide with the Lie product on g.

In order to compare formal group laws we need the following concept.

Definition. Let F and F be formal group laws over K of dimension d and d', respectively. A formal homomorphism : F —>F is a d!-tuple = (1, . .. , d') of formal power series G K [[U1, . .. , Ud } } such that . (0)=0 and

(F (Y, Z))=F' ((Y), (Z)).

The formal group laws F and F are known isomorphic if d=d' and if there are formal homomorphisms : F —>F and ' : F —>F such that (' (U))=U= ' ((U)).

We write Hom (F, F') for the set of all formal homomorphisms : F — > F', and we consider the linear map

Hom (F, F') — ► HomK (Kd, Kd')

* /9 i (U)\:= (\J t).. . _ dU3 |u=0 ' J

Theorem. The map Hom (F, F') -i HomK ((Kd, [, }f), (Kd', [, }<=))

i — ► is well defined and bijective; in particular, the formal group laws F and F_ are isomorphic if and only if the corresponding Lie products [, }f and [,]F' are isomorphic.

Notes

Corollary. The three formal group laws H_g, and FGc are mutually isomorphic.

Proposition. Let Gi and G2 be two Lie groups over K and let Ci = (Ui, ^i, Kdi), for i=1, 2, be a chart for Gi around the unit element ei ∈ Gi such that ^i (ei)=0; for any formal homomorphism : FGl C1 —>FG2 C2 there is an ∈ > 0 such that ∈ FS (Kdl; Kd2).

Proof. In a first step we consider the special case that Gi= (K, +) is the additive group of the field K and the chart is ci= (K, id, K). The FG1, Cl = Y+Z. We abbreviate d := d2 and F := Fg2 C2 • The formal homomorphism is a d-tuple of formal power series in one variable U which satisfies

(0)=0 and (Y+Z)=F ((Y), F (Z)).

Deriving the last identity with respect to Z and then setting Z equal to zero leads to dF

F' (U)=^ (F (U), 0) • F' (0).

We define

dF G (Y) := ^ (Y, 0) • F' (0) and obtain the system of differential equations

F' (U)=G ((U)) withΦ(0)=0.

We write

G (Y) = ∈ Ya (Ma • ' (0)) with Ma ∈ MdXd (K)

And (U) = ∈ Un ^ with Wn= (Wn, i, . .. , Wn, d) ∈ Kd.

Our system of differential equations now reads

EUnwnr1 = ∈ (∈ UmWrnr)ai •.. . • (∈ Umwmr)ad (Ma • ' (0))

n> 0 and m>i

Wn+1 = ∈ (∈ n) (M S' (0))

a€n0 mi. i+.. . +md. ad =n i, j

for n>0, where the second summation runs over all \a\-tuples

By comparing coefficients we obtain the equations

(m1, 1, ..., m1, ai, m2, 1, ..., m2, a2, ..., md, 1, ..., md, ad)

of integers>1 whose sum is equal to n. Since each mi 1i. n!m — f is an integer it follows that

||wn+1 II<max{ (n\wmijA)-\\Ma•f' (0)|| : a ∈ N0, mM+.. -+md>ad=n } i,
j

< max{ (n Ikmij||)-||Ma||-||f' (0)|| : a ∈ Nd, mM+.. . +md, «d=n }.

.. "m, ;. i, j

we have observen that

l|F|| i<A 11 ia<M

holds true for any sufficiently big \a\ ∈ \K \. This implies the existence of some \a\>1 such that

\\Ma\I<\a\|a| for any a ∈ Nd.

We claim that

||wn+1|<\a\n || ' (0)|r+1 for any n>0.

The case n=0 is obvious form w1=f' (0). We now proceed by induction with respect to n. Since 1<mgj<n the induction hypothesis gives

Ikmij iK^n--1 -||f'

We deduce

II IK, . , ||<\nj"-|a |.||<=' (0)||' i, j

and therefore

IK+1|<max \a\n-|a| - || ' (0)||n - \a\H - ||f' (0)||=\a\n - || ' (0)||n+1

Conclude that there are appropriate e0, e1>0 such that , w. — r ||<UUi" for any n>1. n!

It follows thatΦG F (K; Kd) for any 0 < ∈ < ∈ - 1.

We now consider the general case, and we fix a K-basis y1, . .. , fdl of g1 (where gi := Lie (G^)). For any f G g1 we can apply to the homomorphism of Lie algebras and obtain a unique formal homomorphism

— x : F (K, +), id*FG1, c1

such that

— X (0)=O (1)=0Ci1 (f).

We introduce the homomorphism of Lie algebras

G := dc2 ° ∘ □cl : Q1*Q2.

The unicity implies in addition that we must have — CT (x) (U)= — (— x (U)).

By the special case which we have treated already we find an ∈ > 0 such that

— x. G F (K; Kdl) and — <T (x.) G F (K; Kd2) for any 1<i<d1.
Hence, for sufficiently small ∈ > 0, the maps G1

fi ((ai, . .. , adl)) :=^-l (Φr1 UlU.. . ^-1 (^d (ad1)) Kdl D Be (0)

f2 ((al, . .. , adl)) :=G2 l (-LCT (rl) (al))^.. . ^G2 l (^CT (rd) (adl))

G2are well defined and locally analytic. we observe that the tangent map at 0 of the upper map is equal to (a1, . .. , adl) i —>a1x1+.. . +adlXd1 which is a bijection. Hence by the upper map can be inverted as a locally analytic map in a sufficiently small open neighbourhood V1 C U1 of e1 ∈ G1. Because of the resulting composed locally analytic map f2 ∘ f-1 : V1 — ► Be (0) — ► G2 has as its power series expansion (with respect to the charts <p1\V1 and <^2) around ^1 (e1) =0.

Check your Progress-2

Discuss Formal Group Laws

12.5 LET US SUM UP

In this unit we have discussed the definition and example of The Campbell-Hausdorff Formula, The Convergence Of The Hausdorff Series, Formal Group Laws

12.6 KEYWORDS

The Campbell-Hausdorff Formula….. K is an arbitrary field and X={ X1, . .. , Xd } is a fixed finite set

The Convergence Of The Hausdorff Series ….. We fix a Lie algebra g of finite dimension d over a field K of characteristic zero. We also pick a K-basis ∈ \,. .. , ed of g.

Formal Group Laws ….. Let K be any field of characteristic zero. We fix a natural number d, and let R := K[[Y1, . .. , Yd, Z1, . .. , Zd]\ denote the ring of formal power series over K in the variables Y= (Y1, . .. , Yd) and Z= (Z1, . .. , Zd).

12.7 QUESTIONS FOR REVIEW

Explain The Campbell-Hausdorff Formula & Convergence

Explain Formal Group Laws

12.8 REFERENCES

p-adic Numbers, p-adic Analysis, and Zeta-Functions, Neal Koblitz (1984, ISBN 978-0-387-96017-3)

A Course in p-adic Analysis by Alain M Robert

Analytic Elements in P-adic Analysis by Alain Escassut

12.9 ANSWERS TO CHECK YOUR PROGRESS

The Campbell-Hausdorff Formula (answer for Check your Progress-1 Q)

Convergence Formal Group Laws (answer for Check your Progress-2 Q)

UNIT-13: THE TOPOLOGY OF QP

STRUCTURE

13.0 OBJECTIVES

After studying this unit, you should be able to:

- Understand about The Topology Of Qp
- Understand about Topology Associated With Valuation
- Understand about Approximation Theorem
- Understand about Completion Of A Field With Valuation
- Understand about Infinite Series In A Complete Field

13.1 INTRODUCTION

In mathematics, p-adic analysis is a branch of number theory that deals with the mathematical analysis of the functions of p-adic numbers.

The Topology Of Qp, Topology Associated With Valuation, Approximation Theorem, Completion Of A Field With Valuation, Infinite Series In A Complete Field

13.2 THE TOPOLOGY OF QP

We will now discuss continuous functions on Q_p and related topics. We begin by introducing some basic topological notions.
Let $\alpha \in Q_p$ and $\delta > 0$ be a real number.

Definition :The *open disc centred at* α *of radius* δ is

$$D(\alpha; \delta) = \{\gamma \in Q_p : |\gamma - \alpha|_p < \delta\}.$$

The *closed disc centred at* α *of radius* δ is

$$D(\alpha; \delta) = \{\gamma \in Q_p : |\gamma - \alpha|_p ™ \delta\}.$$

Clearly

$$D(\alpha; \delta) \subseteq D(\alpha; \delta).$$

Such a notion is familiar in the real or complex numbers; however, here there is an odd twist.

Proposition. *Let* $\beta \in D(\alpha; \delta)$. *Then*

$$D(\beta; \delta) = D(\alpha; \delta)$$

Hence every element of $D(\alpha; \delta)$ *is a centre. Similarly, if* $\beta^{j} \in D(\alpha; \delta)$, *then*

$$D(\beta^{j}; \delta) = D(\alpha; \delta).$$

Proof. This is a consequence of the fact that the p-adic norm is non-Archimedean. Let $\gamma \in D(\alpha; \delta)$; then

$$\begin{aligned} |\gamma - \beta|_p &= |(\gamma - \alpha) + (\alpha - \beta)|_p \\ &™ \max\{|\gamma - \alpha|_p, |\alpha - \beta|_p\} \\ &< \delta. \end{aligned}$$

Thus $D(\alpha; \delta) \subseteq D(\beta; \delta)$. Similarly we can show that $D(\beta; \delta) \subseteq D(\alpha; \delta)$ and therefore these two sets are equal. A similar argument deals with the case of closed discs.

Let $X \subseteq Q_p$ (for example, $X = Z_p$).

Definition : The set

$$D_X(\alpha; \delta) = D(\alpha; \delta) \cap X$$

is the *open ball of radius* δ *in* X *centred at* α. Similarly,

$D_X(\alpha;\delta) = D(\alpha;\delta) \cap X$

is the *closed ball in* X *of radius* δ *centred at* α.

We will now define a continuous function. Let f: X —>Qp be a function.

Definition :We say that f is *continuous at* $\alpha \in X$ if

$\forall\varepsilon>0\exists\delta>0$ such that $\gamma \in D_X(\alpha;\delta) \Longrightarrow f(\gamma) \in D(f(\alpha);\varepsilon)$.
If f is continuous at every point in X then we say that it is continuous on X. Example :Let $f(x) = \gamma_0 + \gamma_1 x + \cdot\cdot\cdot + \gamma_d x^d$ with $\gamma_k \in Q_p$ be a polynomial function. Then as in real analysis, this function is continuous at every point. To observe this, we can either use the old proof with $|\ |_p$ in place of $|\ |$, or the following p-adic version.

Let us show that f is continuous at α. Then
$|f(x) - f(\alpha)|_p = |x-\alpha|_p : {}^{d}_{n=1}\gamma_n(x^{n-1}+\alpha x^{n-2}+\cdot\cdot\cdot+\alpha^{n-1})_p$
If we also assume that $|x|_p < |\alpha|_p$, then

$|f(x)-f(\alpha)|_p$ ™ $|x-\alpha|_p \max\{\alpha^{n-1}\gamma_n \ldots\ldots 1$ ™ n ™ d}

™ $|x-\alpha|_p B$,

say, for some suitably large $B \in R$ (in fact it needs to be at least as big as all the numbers $\alpha^{n-1}\gamma_n$ *with*1^{TM} n^{TM} *d*)

But if $\varepsilon > 0$ $\left(\textit{and without loss of generality}, \varepsilon < |\alpha|_p\right)$ *we can take*
$\delta = \varepsilon/B$. If $|x-\alpha|_p < \delta$, we now have

$|f(x) - f(\alpha)|_p < \varepsilon$.
Example. Let the power series anxn have radius of convergence r>0.

Then the function f: D 0; r —>Qp for which

f x = n= 1

is continuous by a similar proof to the last one.

It is also the case that sums and products of continuous functions are continuous as in real analysis.

Notes

What makes p-adic analysis radically different from real analysis is the existence of non-trivial locally constant functions which we now discuss. First recall the following from real analysis.

Recollection Let f: (a, b) —>R be a continuous function. Suppose that for every x $\in$ (a, b) there is a t>0 such that (x -1, x +1) C (a, b) and f is constant on (x -1, x +1), i. $\in$. , f is locally constant. Then f is constant on (a, b).

We can think of (a, b) as a disc of radius (b - a)/2 and centred at (a+b)/2. This suggests the following definition in Qp.

Definition. Let f: X —>Qp be a function where X C Qp. Then f is locally constant on X if for every a $\in$ X, there is a real number 5a>0 such that f is constant on the open disc Dx (a; 5a). \t r\nx

This remark implies that there are no interesting examples of locally constant functions on open intervals in R; however, that is false in Qp.

Example. Let X=Zp, the p-adic integers. From Theorem 2. 29, we know that for a $\in$ Zp, there is a p-adic expansion

a=ao+ai p + + a,,pn + ,

where an $\in$ Z and 0 ^ an ^ (p— 1). Consider the functions

fn: Zp — t Zp; fn (a)=an,

which are defined for all n ^ 0. We claim these are locally constant. To observe this, notice that fn is unchanged if we replace a by any ft with |ft— a|p<1/pn; hence fn is locally constant.

We can extend this example to functions fn: Qp — t Qp for n $\in$ Z since for any a $\in$ Qp we have an expansion

a=a-r p-r + + ao+aip + + anpn +

and we can set fn (a)=an in all cases; these are still locally constant functions on Qp. One important fact about such functions is that they are continuous.

Proposition. Let f: X — t Qp be locally constant on X. Then f is continuous on X.

Proof. Given a ∈ X and ∈ > 0, we take 5=5a and then f is constant on DX (a; 5a).

This result is also true in R.

Example. Let us consider the set Y=D (0; 1) C Zp. Then we define the characteristic function of Y by

f1 if a ∈ Y,

Xy: Zp t Qp; Xy (a)=\ , if a ∈ Y.

This is clearly locally constant on Zp since it is constant on each of the open discs D (k; 1) with 0 ^ k ^ (p— 1) and these exhaust the elements of Zp. This can be repeated for any such open ball D (a; 5) with 5>0.

Another example is provided by the TeichmUller functions. These will require some work to define. We will define a sequence of functions with the properties stated in the next result.

Proposition. There is a unique sequence of locally constant, hence continuous, functions wn: Zp — t Qp, satisfying

(T1) wn (a)p=wn (a) for n ^ 0,

(T2) a=^ Wn (a)pn.

Proof. First we define the TeichmUller character w: Zp — t Qp which will be equal to w0. Let a ∈ Zp; then the sequence (apn) is a sequence of p-adic integers and we claim it has a limit. To observe this, we will show that it is Cauchy and use the fact that Qp is complete

has a unique p-adic expansion

a=a0+a1p+a2p+... with ak ∈ Z and 0 ^ ak ^ (p— 1). In particular,

|a— ao|p<1.

By Fermat's Little in Z we have a=ao,

hence |a0— a0 |p<1. Making use of the fact that inequality, we obtain

^ 1 together with the triangle

|ap— a0lp= (a— ao) (ap 1+ap 2ao + + ap

^ |a— ao|p<1.

Thus we have

|aP— a|P=| (aP— ap)+ (ap— ao)+ (ao— a)|^ max{ |ap— ap|p, |ap— ao|p, |ao— a|p }< 1.

We will show by induction upon n ^ 0 that Clearly this is true for n=0 by the above. Suppose true for n. Then

aPn+1=aPn+p,

where |P|p<1/pn. Raising to the power p gives

apn+2= (apn+p)p

= apn+1+papn (p-1)p+...+^ ^ apnk pp-k+...+pp,

where all of the terms except the first in the last line have||p less than 1/pn+1. Applying the p-adic norm gives the desired result for n+1.

Now consider apn. Then

apn= (apn— apn 1)+ (apn 1— ap" 2)+...+ (ap— a)+an- 1

a+^ (apk+1— apk).

Clearly the difference apn+1— apn is a null sequence & the sequence (apn) is Cauchy as desired.

Now we define the Teichmuller function or character,

w: Zp —>Qp; w (a)=lim (p)ap".

n^tt

This function satisfies

|a— w (a)|p<1, w (a)p=w (a).

The inequality follows while the equation follows from the fact that

(lim (p)ap^p=lim (p) (apn)p

Vn^tt J n^tt

= lim (p) (apn+1).

n^-tt

We now set w0 (a)=w (a) and define the wn by recursion using

fa - (wo (a)+wi (a)p + + wn (a)pn)\

wn+i (a)=w ^ pn+i   )

For a $\in$ Zp, the expansion

a=wo (a)+wi (a)p +   + wnpn +

is known the Teichmiiller expansion of a and the wn (a) are known the Teichmuller digits of a. This expansion is often used in place of the other p-adic expansion. One reason is that the function w is multiplicative. We sum up the properties of w in the next proposition.

Proposition. The function w: Zp —>Qp is locally constant and satisfies the conditions

w (aP)=w (a)w (P),

|w (a+p) - w (a) - w (P)|p<1.

Moreover, the image of this function consists of exactly p elements of Zp, namely the p distinct roots of the polynomial Xp— X.

Proof. The multiplicative part follows from the definition, while the additive result is an easy exercise with the ultrametric inequality. For the image of w, we remark that the distinct numbers in the list 0, 1, 2, ..., p— 1 satisfy

|r - s|p=1.

If r=s, then

|w (r) - w (s)|p=1

Hence, the image of the function w has at least p distinct elements, all of which are roots in Qp of Xp - X. As Qp is a field, there are not more than p of these roots. So this polynomial factors as

Xp - X=X (X - w (1)) (X - w (2)) ... (X - w (p - 1)) and the p roots are the only elements in the image of w.

Example. For the prime p=2, the roots of X2 - X are 0, 1. In fact, the Teichmuller expansion is just the p-adic expansion.

Example. For the prime p=3, the roots of X3 - X are 0, ±1. So we replace the use of 2 in the p-adic expansion by that of -1. Let us consider an example.

Setting a=1/5, we have 5=-1 and so w (5)=-1 since

|5 - (-1)|3<1-

Hence w (1/5)=-1 too, so w0 (1/5)=-1. Now consider

(1/5) - (-1) =1=2 3 15 5,

and notice that 2=-1, hence w1 (1/5)=w (2/5)=1. Next consider

(2/5) - 1 -3 -1

3=T5=T",

giving w2 (1/5)=w (— 1/5)=1. Thus

1= (— 1)+1 3+1 32+•••

5

where we have stopped at the term in 32 and ignored terms of 3-norm less than 1/32.

Example. If p=5, there are three roots of X5— X in Z, namely 0, ±1 and two more in Z5 but not in Z. On the other hand, (Z/5)x= (2) as a group. Thus, we can take w (2)=7 say, to be generator of the group of (5— 1)=4-th roots of 1 in Z5. So the roots of X5— X in Z5 are w (0)=0, w (1)=1, w (2)=y, w (3)=y3, w (4)=y2.

Suppose that we wish to find the Teichmuller expansion of 3 up to the term in 52. Then we first need to find an integer which approximates y to within a 5-norm of less than 1/52. So let us try to find an element of Z/53 which agrees with 2 modulo 5 and is a root of X4=1. We can use Hensel's Theorem to do this.

We have a root of X4— 1 modulo 5, namely 2. Set f (X)=X4— 1 and note that f' (X)=4X3. Now f' (2)=4 8=2 and we can take u=3. Then x=2— 3f (2)= — 43=7 is a root of f (X)

5   5   25

modulo 25. Repeating this we obtain

7— 3f (7)=7— 75= — 68=57

which is a root of the polynomial modulo 125. We now proceed as before.

This method always works and relies upon the same ideas as Hensel's Theorem.

Theorem (Hensel's Theorem). Let f (X) $\in$ Zp[X] be a polynomial and let a $\in$ Zp be a p-adic number for which

|f (a)|p<1 |f' (a)|p=1.

Define a sequence in Qp by setting a0=a and in general

an+1=an— (f' (an))-lf (an).

Then each an is in Zp and moreover

|f (an) |p<pn.

Hence the sequence (an) is Cauchy with respect to||p and

f (lim (p)an)=0.

n^^

Notes

Proof. The proof is left to the reader who should look at the earlier version of Hensel's Theorem mentioned above. We remark that the definition of an+1 can be modified to

an+i=an— (f ' (a))-1f (an).

One reason for using only a rather than an is that it can reduce the amount of calculation needed when using this formula.

Example. Let f (X)=Xp-1— 1. Then from our earlier discussion of u we know that there are (p— 1) roots of 1 in Zp. Suppose that we have an a such that|a— 7\p<1 for one of these roots 7. By an easy norm calculation, \f (a)\p<1. So we can take the sequence defined which converges to a root of f (X), i. ∊ . , a (p— 1)-st root of 1 in Zp.

We now prove another general fact about locally constant functions on Zp.

Theorem. Let f: Zp —>Qp be locally constant. Then the image of f,

im f=f (Zp)={ f (a) : a ∊ Zp },

is a finite set.

Proof. For each a ∊ Zp there is a real number 5a>0 for which f is constant on the open disc D (a; 5a). We can assume without loss of generality that

1

nda

5a= — —

with da ^ 0 an integer. Now for each a there is an integer na such that

|a— na\p <pda

and so f (na)=f (a). we also have

D (a; 1/pda)=D (na; 1/pda).

In fact we can assume that na satisfies

0 ^ na ^ pda+1— 1,

since adding a multiple of pda+l to na does not change the open disc D (na; 1/pda). Now

Zp=|J D (fc;1/pdk) k=0

and f is constant on each of these open discs. But also

pd0+l-1

Zp=J D (fc;1/pd^. k=0

Now take d=max{ dk : 0 ^ k ^ pdo+1— 1 }

and observe that for each k in the range 0 ^ k ^ pdo+1— 1, f is locally constant on the disc D (k;1/pdj. Hence

Zp=J D (k; 1/p^,

where f is constant on each of these discs. Since there is only a finite number of these discs, the image of f is the finite set

f (Zp)={ f (k) : 0<k<pd— 1 }.

A similar argument establishes a closely related result.

Theorem (The Compactness of Zp). Let A C Zp and for each a ∈ A let 5a>0. If Z=U D (a; 1/pSa),

aG A then there is finite subset A C A such that

Z=U D (a;1/p*a). aGA'

A similar result holds for each of the closed discs D (fi; t) where t fi 0 is a real number.

We leave the proof as an exercise. In fact these two results are equivalent in the sense that each one implies the other.

The next result is a direct consequence.

Theorem (The Sequential Compactness of Zp). Let (an) be a sequence in Zp. Then there is a convergent subsequence of (an), i. ∈ . , a sequence (fin) where fin=as (n) with s : N —>N a strictly increasing sequence and which converges. A similar result holds for each of the closed discs D (fi; t) where t fi 0 is a real number.

Proof. We have

Zp=U D (k; 1).

Hence, for one of the numbers 1 fi k fi p, say al, the disc D (al;1) has an ∈ D (al;1) for infinitely many values of n. Then

D (ai;1)=U D (k; 1/p)

and again for one of the numbers 1 fi k fi p2, say a2, we have an ∈ D (a2; 1/p) for infinitely many values of n. Continuing in this way we have a sequence of natural numbers an for which D (an; 1/p"-1) contains am for infinitely many values of m. Moreover, for each n,

D (an;1/p"-1) C D (an;1/pn).

Now for each n fi 1, choose s (n) so that as (n) ∈ D (an;1/pn-^. We can even assume that s (n)<s (n+1) for all n. Hence we have a subsequence (fin) with fin=as (n) which we must still show has limit. But notice that

|fin+l - fin|p<pn,

since both of these are in D (an+l; 1/p"). Hence the sequence (fin) is null and so it has a limit in Zp.

Recall the notion of uniform continuity:

Definition Let f: X — ^ Qp be a function. Then f is uniformly continuous on X if Ve>035>0 such that Va, fi ∈ X, with |a— fi|p <5 then |f (a)— f (fi)|p < ∈ .

Clearly if f is uniformly continuous on X then it is continuous on X. In real or complex analysis, a continuous function on a compact domain is uniformly continuous. This is true p-adically

Theorem. Let t>0, a ∈ Qp and f: D (a; t) —>Qp be a continuous function. Then f is uniformly continuous.

Definition. Let f: X —>Qp be a function. Then f is bounded on X if

3b ∈ R such that Vx ∈ X, |f (x)|p ^ b.

Again we are familiar with the fact that a continuous function defined on a compact set is bounded.

Theorem. Let f: D (a; t) —>Qp be a continuous function. Then f is bounded, i. ∈ . , there is a b ∈ R such that for all a ∈ D (a; t), |f (a)|p ^ b.

Again the proof is a modified version of that in classical analysis.

Now let us consider the case of a continuous function f: Zp —>Qp. Zp is compact, so f is bounded. Then the set

Bf={ b ∈ R : Va ∈ Zp, |f (a)|p<b }

is non-empty. Clearly Bf C R+, the set of non-negative real numbers. As Bf is bounded below by 0, this set has an infimum, inf Bf ^ 0. An easy argument now shows that

sup{ |f (a)|p : a ∈ Zp }=inf Bf.

We will write bf for this common value.

Theorem. Let f: Zp —>Qp be a continuous function. Then there is an ao ∈ Zp such that bf=|f (ao)|p.

Proof. For all a ∈ Zp we have |f (a)|p ^ bf. By definition of supremum, we know that for any ∈ > 0, there is a a ∈ Zp such that

|f (a)|p>bf - ∈ .

For each n, take an an ∈ Zp such that

|f (an) |p >bf- n

and consider the sequence (an) in Zp there is a convergent subsequence (^n)= (as (n)) of (an), where we can assume that s (n)<s (n+1). Let a'=lim (p)as (n). Then for each n we have

bf >\f (as (n)) |p >bf - S (n) and so \f (as (n))\ ^ bf as n ^ to. Since f (a')\p - \f (as (n))\p<nlim \f (a' - as (n)) \,,=0

we have bf=|f (a')|p.

Definition. Let f: Zp —>Qp be continuous. The supremum seminorm of f is P Consider the set of all continuous functions Zp —>Qp,

C (Zp)={ /: Zp —>Qp : / continuous }.

This is a ring with the operations of pointwise addition and multiplication, and with the constant functions 0, 1 as zero and unity. The function || ||p: C (Zp) —>R+ is in fact a non-Archimedean norm on C (Zp).

Theorem. C (Zp) is a ring with non-Archimedean seminorm || |p. Moreover, C (Zp) is complete with respect to this seminorm.

Now recall the notion of the Fourier expansion of a continuous function /: [a, b] —>R; this is a convergent series of the form

E°° / 2pix. 2nx

an cos + sin

V n n

n=l N

which converges uniformly to / (x). In p-adic analysis there is an analogous expansion of a continuous function using the binomial coefficient functions

n _ (x\ _ x (x - 1) ... (x - n+1)

Cn (x)— I I — j .

We recall that these are continuous functions Cn: Zp —>Qp which actually map Zp into itself

Theorem. Let / ∈ C (Zp). Then there is a unique null sequence (an) in Qp such that the series

^ ^ anCn (x)

converges to / (x) for every x $\in$ Zp. Moreover, this convergence is uniform in the sense that the sequence of functions

n^ amCm $\in$ C (Zp)

is a Cauchy sequence converging to / with respect to|| p.

The expansion in this result is known the Mahler expansion of / and the coefficients an are the Mahler coefficients of /. We need to understand how to determine these coefficients. Consider the following sequence of functions /[n]: Zp —>Qp:

/ [0] (x)=/ (x)

/ [1] (x)— / [0] (x+1) - / [0] (x)

/ [2] (x)— / [1] (x+1) - / [1] (x)

/ [n+1] (x)— /[n] (x+1) - / [n] (x)

/[n] is known the n-th difference function of /.

Proposition. The Mahler coefficients are given by

= f [n] (0) (n>0).

Proof. (Sketch) Consider

f (0)=^ a,,C,, (0)

Now by Pascal's Triangle,

Cn (x+1) - Cn (x)=Cn- l (x).

Then

f [1] (x)=f [0] (x+1) - f[0] (x)

^]an+lCn (x)

n=0

and repeating this we obtain

f [m+1] (x)=f [m] (x+1) - f [m] (x)

^ ^ an+mCn (x).

n=0

Thus we have the desired formula

f [m] (0)=am.

The main part is concerned with proving that an ^ 0 and we will not give it here.

The functions Cn have the property that

IICnllp=1.

To observe this, note that if a ∈ Zp, we already have |Cn (a)|p ^ 1. Taking a=n, we get Cn (n)=1, and the result follows. Of course this means that the series ^ anCn (a) converges for all a ∈ Zp if and only if an ^ 0.

Example. Consider the case of p=3 and the function f (x)=x3. Then

So we have

x3=C1 (x)+3C2 (x)+6C3 (x).

In fact, for any polynomial function of degree d, the Mahler expansion is trivial beyond the term in Cd.

The following formula for these an can be proved by induction on n.

n /x

(4. 3) /M (0)= (-1)k (k)f (n - k).

k=0 ^ '

Example. Take p=2 and the continuous function f: Z2 —>Q2 given by

f (n)= (-l)n if n ∈ Z.

Then

and in general

f |0] (0)=1, f W (0)=0, f 131 (0)=-1, f M (0)= (-1)n (n= (— 2)n.

Therefore

f (x) = ∈ (-2)nCn (x).

n=0

Of course, this is just the binomial series for (1— 2)x in Q2.

The exponential and logarithmic series. In

real and complex analysis the exponential

and logarithmic power series X n

exp (X)=5 ib, X n

log (X) = ∈ (-1)"-13

are of great importance. We can view each of these as having coefficients in Qp for any prime p. The first issue is to determine the p-adic radius of convergence of each of these series. Further details on this material can be found in [5].

the p-adic radii of convergence of the p-adic power series

1 (1)n-1

expp (X) = ∈ nX", logp (X)=r L-n_X"

n=0 n=1

are p-1/ (p-1) and 1 respectively.

Theorem. There are p-adic continuous functions expp: D (0;p1/ (p-1)) —>Qp and logp: D (1; 1/p) —>Qp, where for x ∈ D (0; p1/ (p-1)) and y ∈ D (1; 1/p),

expp (x)= n,

n=0 n!

logp (y)= (-1)n-1 (1 - y)n n=1

Furthermore, for x1, x2 ∈ D (0;p-1/ (p-1)) and y1, y2 ∈ D (1; 1),

expp (x1+x2)=expp (x1) expp (x2), logp (y1y2) =ogp (y1)+logp (y2).

A useful variation on the exponential function is the Artin-Hasse exponential function, given by a power series

Ep (X)=^ (1 - Xn)-^n)/n,

p\n

where the product is taken over natural numbers n not divisible by p, and p is the Mobius function for which p (1)=1 and if n>1,

E P (d)=o.

d|n

For example, for any prime q and r g 1,

(— 1 if r=1,

p (qr)=I ,

I 0 if r>1.

Using the Binomial Expansion, it is easy to observe that Ep (X) is a power series whose coefficients lie in Zp C Qp, hence its radius of convergence is at least 1.

There is a factorisation

exp (X)=n (1— Xn)-^n)/n, ng 1

and so the exactly the factors of exp (X) which do not involve powers of p in the denominators of coefficients of powers of X. Another useful formula is

Ep (X)=exp (Lp (X)),

Where Lp (X) = ∈ ^ X p"

Notice that if p is odd, this is part of the series log (X), namely the terms involving exponents of X which are powers of p.

Summary. This ends our discussion of elementary p-adic analysis. We have not touched many important topics such as differentiability, integration and so on. For these discussion of p-adic integration, T-function and Z-function.

The world of p-adic analysis is in many ways very similar to that of classical real analysis, but it is also startlingly different. I hope you have enjoyed this sampler. We will now move on to consider something more like the complex numbers in the p-adic context.

Check your Progress-1

Discuss The Topology Of Qp

13.3 TOPOLOGY ASSOCIATED WITH VALUATION

Proposition. A ring A is a valuation ring if and only if the set of principle of A is totally ordered by inclusion.

Proof. Let A be a valuation ring. Let Ax and Ay be two proper principle

x ideals of A. Consider z=- belonging to K the quotient field of A.

Since A is a valuation ring, either z or z-1 belongs A. But this implies that either Ax c Ay or Ay d Ax.

Therefore the set of principal ideals y

is totally ordered conversely let x=where y and z belong to A and z

x+0, be an element of K which is not in A. x $\in$ A implies that y does not belong to Az. But the set of principle ideals of A is totally ordered, therefore we get Az c Ay implying z=ay for some a in A. But a=x-1, therefore A is a valuation ring.

Corollary. A valuation ring is a local ring.

If possible let M1+M2 be two maximal ideals in a valuation ring A. M1+M2 implies that there exists x1 $\in$ M1, x1 & M2 and x2 $\in$ M2, x2 & Mi.

x1 & M2 Ax1 is not contained in M2 which implies that Ax1 is not contained in Ax1. Similarly x2 not belonging to M1 implies that Ax1. But this is impossible, therefore M1=M2.

Proposition. A ring A is a valuation ring if and only if A is the ring of a valuation of its quotient field K determined upto an equivalence.

Proof. Let M be the unique maximal ideal of the valuation ring A and A*=A/M. For x, y in K* we define x>y if and only if x belongs to Ay. It is easy to verify that this relation among the elements of K* induces a total order in the group K*/A* and the canonical homomorphism K* onto K*/A* is a valuation of K for which the ring of integers is A. The ring of integers of a valuation is a valuation ring has already been proved.

Let k be a fields. By kU m we mean the set of elements of k together with an element m. We extend the laws of k to (not everywhere defined) laws in k U m in this way

m+a=a+m=m for a in k*

mx a=a Xm=mxm=m, for a in k*

0 x m and m+m are not defined.

Let K be a field with a valuation v and let k=O/ Y be the residual fields of v. Then the canonical homomorphism p of O onto k extended to K by setting p (x)=m for x not in O gives rise to a map of K onto k U m known a place of K.

In general, we define

A place of a field K is a mapping p form K to k U m such that

(i) p (a+b)=p (a)+p (b)

(ii) P (ab)=p (a)p (b)

for a, b in K and whenever the right hand side is meaningful.

It is easy to prove that O=p-1 (K) is a valuation ring with the maximal ideal Y=p-1 (0).

Thus there exists a 1 -1 correspondence between the set of valuation rings and the set of inequivalent places of a field (Two places p1 and p2 of a field K carrying K into k U m and k U m) respectively are said to be equivalent if there exists an isomorphism a of k onto k such that p2=a o p1, with a (m)=m.

Let K be a field with a valuation v. For any a>0 in rv consider the ideal

Ia={ x|x ∈ K, v (x)>a }

Then there exists one and only topology on K for which

Ia for different a in rv form a fundamental system for neighbourhoods of 0.

K is a topological group for addition.

We observe immediately that the operation of multiplication in K is continuous in topology. Ia for any a>0 in rv is an open subgroup and hence a closed subgroup of K. Thus the residual field k is discrete for 10 the quotient topology. The topology of K is discrete if and only if the valuation vis improper (if rv={ o }). In particular K with a discrete and proper valuation is not discrete as a topological space. The topology of K is always Hausdorff, because if x ± 0, then x does note belong to Ia with a=v (x), therefore U Iaa>0= (0) which proves our assertion. aer v

Remark. If v is not improper, then the ideals I'a for a>o in rv also constitute a fundamental system of neighbourhoods of 0 for the topology of K. For, I'a and for a>o Ia contains I'2a.

Remark. Let A be a ring a with a decreasing filtration by ideals i. ∈ . there exists a sequence (An)n>0 of ideals such that An d An+1 and

AnAm c Am+n. Then there exists one and only one topology for which A is an additive topological group and (An)n>o constitute a fundamental system of neighbourhoods of 0. A is a topological ring this topology.

Let M be any ideals of a ring A. Then A can be made into a topo- logical ring by taking An=Mn. We call the topology defined by M on A the M-adic topology. In particular the ring of integers of a field K which a real valuation v has the M- adic topology for every M={ x/v (x)>a>0 } We shall speak of this topology of K as the M-adic topology.

If the valuation v is discrete and normed. We can take a=1 and M=Y.

Remark. If K is a field with a real valuation v, then the Y-adic topology completely characterises the valuation upto a constant factor, because x belongs to Y if and only if xn tends to zero as n tends to infinity.

13.4 APPROXIMATION THEOREM

For the sake of simplicity we confine ourselves in this section to real valuations though analogous results could be prove for any valuation. In this section we deal with the question whether there exists any connection between various inequivalent valuations of a field. We first prove:

Theorem. Let K be a field with two valuations v1 and v2. Then v1 and v2 are inequivalent if an only if O1, the ring of integers of v1, is not contained in O2, the ring of integers of v2.

Proof. If O1 c O2, then K - O1 contains K - O2 implying Y2 c Y1 c O1 c O2. Therefore Y2 is a prime ideal in O1. Assume Y2+Y, then there exists xin Y1 which does not belong to Y2. Since Y2 is an ideal in Of, there exists a>0 in rv1 such that Y2 contains Ia. Let v^x)=S.

Then for large enough q we have

v1 (xq)=qv1 (x)=qS>a,

which means that xq belongs to Y2, but Y2is a prime ideal, therefore x belongs to Y2. Hence our assumption is wrong.

Therefore Y2=Y1 and v1 is equivalent to v2. The converse is obvious.

Theorem. Let Kbe a field with v1, . . ., v,, (n>2) proper valuations such that vi is inequivalent to vj for i ± j. Then there exists an element z in K such that v1 (z)>0, v2 (z)<0 and vi (z)+0 for i=1, 2, . . ., n.

Proof. We shall prove the results by induction on n. When n=2, v1 inequivalent to v2implies that O1 is not contained in O2. Therefore there exists x in O1 and not in O2. Moreover O2 not contained in O1 implies that Y1 is not contained in Y2.

Therefore there exists y in Y1 and not in Y2. Then z=xy is the required element.

When n>2. By induction there exists an element x in K such that v1 (x)>0, v2 (x)<0 and vi (x)+0 for i=1, 2, . . ., n- 1. If vn (x)+0, we have nothing to prove. If vn (x)=0, we take an element y with vn (y)+0. Let z=yX, s a positive integer. Then for sufficiently large s, z fulfills the requirements of the Theorem.

Theorem. Let K be a field with v1, . . ., vr proper valuations such that vi is inequivalent to vj for i+j. Let Kj be the field K with topology r

defined by vi andp the canonical map from K ^ Kj=P i. ∈ . p (a) =i=1

(a, a, . . ., a). Thenp (K)=D is dense in P.

Equivalently stated if a1, . .. , ar are any r elements in K, then for every a1, . . ., ar in R there exists an element x in K such that 13

v (x - aj)>ai for i=1, 2, . . ., r.

Proof. The theorem is trivial for r=1. Let us assume that it is true in case the number of valuations is less then r.

By there exists an elements x in K such that v1 (x)>xn

0, vr{ x)<0 and Vj (x) ^ 0 for 1<i<r, then yn=tends to 1+0 in K1,

to 1 in Kr and to 0 or 1 in others as n tends to infinity. Let the notation be so chosen that p (yn)— (0, 0, . . ., 0, 1, . . ., 1) as n tends to infinity, 0 occurring in 5 places where 1<5<r - 1. Now D is a subspace of P over K, therefore lt Xp (jn)=lt p (xyn)= (0, . .. 0, X, . .. , X) n — n — r

and (0, 0, . . ., 0, x, x, . . ., x) is in D. Consider the product]~I K, by

i=5+1 r induction assumption the diagonal of n K which is imbedded in D is i=5+1 dense in the product which implies that (0, . . ., 0, a5+1, . . ., ar) belongs to D for ai in K, 5+1<i<r. Similarly (a1, a2, . . ., a5, 0, . . ., 0) belongs to D. But D is a vector space over K, therefore (a1, a2, . . ., ar) is in D.

Hence n K=D. i=1

Corollary. Under the assumptions of the theorem for aj ∈ rvj (j = 1, 2, . . ., r) there exists x in K such that vj (x)=a j.

For aj in rvj, there exists aj ∈ K such that v (aj)=aj. By approximation theorem there exists an element x in K such that v (x - aj)>aj. By definition we have v (x)=v (x - aj+aj)=inf v ((x - aj), v (aj)) = v (aj)=aj.

13.5 COMPLETION OF A FIELD WITH VALUATION

Let K be a field with a valuation v. Since K is a commutative topological group for the topology defined by v, it is a uniform space. Let K denote the completion K. The composition laws of addition and multiplication can be extended by continuity to K, for which K is a topological ring. In fact K is a topological field, because if O is a Cauchy filter on K converging to a+0, then O-1 (the image of O by the map x— x-1 in K) is a Cauchy filter. For O not converging to 0 implies that there exists a>0 in rv and a set A in O such that v (x)<a for every x in A. Since O is a Cauchy filter, for every jd in rv, there exists a set B in O contained in A such that

v (x - y)>2a+f3 for x, y in B.

Then v (x-1 - y-1)=v (x-1y-1 (y- x))=-v (x) - v (y)+v (y- x)>-a - a+2 a +13

which implies that O-1 is a Cauchy filter converging to a-1 in K. The valuation v can also be extended to be valuation v of K, in fact it is a continuous representation of K* onto rv considered as a discrete topo-logical group, so v can be extended as a continuous representation v of K* in r and we get v (x+y)>inf (v (x), v (y)) by continuity. Moreover 15

Ok (the ring of integers of K)=Ok=Ok, since Ok is open in K and_K is hence in K, Ok n K=Ok is dense in Oy, this implies that Ok ^ Ok. But Ok ^ Ok, therefore our result is proved. More generally

4=|x|v (x)>a, x ∈ = Ia=|x|v (x)>a, x ∈ Kj

In particular Yk=YK. We have YK=Ok n Yy, so we can identify Ok/yk with a subset of Oyly, and Ok/yk is dense in Oy/y^- But Orl% is discrete, therefore Or / Yy=Ok l yk.

Remark. Let Kbe a field with a real valuation v, with v we associate a map from K to R. We defined for any x in K the absolute value|x| = a-v (x), where a is a real number>1. The map || satisfies the following properties

| x=0 if and only if x=0

|xy|=| x |y| |x+y<sup (| x |, |y|)<|x|+|y |.

The absolute value of elements of K, which defines the same topol- ogy on K as the valuation v.

By Qp we shall always denote the completions of the field Q for p-adic valuation and by Zp the ring of integers in Qp. For the absolute value associated to the p-adic valuation. We take a=p so that |x|p = p-vp (x)

13.6 INFINITE SERIES IN A COMPLETE FIELD

Let K be a complete field for a real valuation v. Since every Cauchy sequence in K has a limit in K, the definition of convergence of infinite series and Cauchy criterium can be given in the same way as in the case of real numbers. However in this case we have the following.

Theorem. A family (u)iej of an infinite number of elements of K is summable if and only if u tends to 0 following the filter of the comple- ments of finite subsets of I.

Proof. The condition is clearly necessary. Conversely for any a in rv we can find a finite subset J of I such that for i not in J, v (ui)>a, then for i1, . . ., ir not in J we have ijt1u«) >a which is nothing but

Cauchy Criterium. Hence the family is summable.

Corollary. Let Y un be infinite series of elements of K Then the following conditions are equivalent.

un is convergent.

un is commutatively convergent. un tends to 0 as n tends to infinity.

Application. Let K be a complete field for a normed discrete real valuation v, n a uniformising parameter for K, R a fixed system of representatives in O for the elements of the residual field K. Then the series Y rqnq, where rq belongs to R is convergent to an element x in K and q= m

Conversely every x in K can be represented in this form in one and only one way. The series is convergent because v (rqnq)>q for q ± 0 and therefore tends to infinity as q tends to infinity. Conversely by multiplying with a suitable power of n we can take x in O, then there exists a unique r0 ∈ R such that x=r0 (mod Y).

This implies that (x - r0)n 1 is in O. Therefore there exists unique r1 in R such that

(x - x0)n-1=r1 (mod Y). or x=r0+r1n (mod Y2).

Proceeding in this way we prove by induction that

x=ro+rm•••+rmnm (mod Ym+1)

TO

Now it is obvious that the series ∈ rmnm, is convergent and that x = r=0

TO

X rqnq. The uniqueness of the series is obvious from the construction.

q=0

In particular if, K=Qp then any x in Qp can be represented in the

TO

form X rqpq, where rq ∈ { 0, 1, 2.. ., p - 1 }. q=m

Check your Progress-2

Discuss Topology Associated With Valuation

13.7 LET US SUM UP

In this unit we have discussed the definition and example of The Topology Of Qp, Topology Associated With Valuation, Approximation Theorem, Completion Of A Field With Valuation, Infinite Series In A Complete Field

13.8 KEYWORDS

The Topology Of Qp…. We will now discuss continuous functions on Qp and related topics. We begin by introducing some basic topological notions .

Topology Associated With Valuation…. A ring A is a valuation ring if and only if the set of principle of A is totally ordered by inclusion.

Approximation Theorem…. For the sake of simplicity we confine ourselves in this section to real valuations though analogous results could be prove for any valuation .

Completion Of A Field With Valuation….. Let K be a field with a valuation v. Since K is a commutative topological group for the topology defined by v, it is a uniform space

Infinite Series In A Complete Field….. Let K be a complete field for a real valuation v. Since every Cauchy sequence in K has a limit in K

13.9 QUESTIONS FOR REVIEW

Explain The Topology Of Qp

Explain Topology Associated With Valuation

13.10 REFERENCES

p-adic numbers: an introduction by Fernando Gouvea

p-adic Numbers, p-adic Analysis, and Zeta-Functions, Neal Koblitz (1984, ISBN 978-0-387-96017-3)

A Course in p-adic Analysis by Alain M Robert

Analytic Elements in P-adic Analysis by Alain Escassut

13.11 ANSWERS TO CHECK YOUR PROGRESS

The Topology Of Qp (answer for Check your Progress-1 Q)

Topology Associated With Valuation (answer for Check your Progress-2 Q)

UNIT-14 : P-ADIC ALGEBRAIC NUMBER THEORY

STRUCTURE

14.0 OBJECTIVES

After studying this unit, you should be able to:

- Understand about P-Adic Algebraic Number Theory
- Understand about First Introduction To P-Adic Numbers
- Understand about P-Adic Numbers

- Understand about Visualization Of P-Adic Numbers
- Understand about Calculating With P-Adic Numbers
- Understand about An Algebraic Construction Of The P-Adic Numbers
- Understand about Quadratic Residues In P-Adic Numbers
- Learn, Understand about Roots Of Unity

14.1 INTRODUCTION

In mathematics, p-adic analysis is a branch of number theory that deals with the mathematical analysis of the functions of p-adic numbers.

P-Adic Algebraic Number Theory, First Introduction To P-Adic Numbers, P-Adic Numbers, Visualization Of P-Adic Numbers, Calculating With P-Adic Numbers, An Algebraic Construction Of The P-Adic Numbers, Quadratic Residues In P-Adic Numbers, Roots Of Unity

14.2 P-ADIC ALGEBRAIC NUMBER THEORY

In this section we will discuss a complete normed field Cp, which contains Qp as a subfield and has the property that every polynomial f (X) $\in$ Cp[X] has a root in Cp; furthermore the norm||p restricts to the usual norm on Qp and is non-Archimedean. In fact, Cp is the smallest such normed field, in the sense that any other one with these properties contains Cp as a subfield. We begin by considering roots of polynomials over Qp.

Let f (X) $\in$ Qp[X]. Then in general f need not have any roots in Qp.

Example. For a prime p, consider the polynomial X2— p. If a $\in$ Qp were a root then we would have a2=p and so |a|p2=1/p. But we know that the norm of a p-adic number has to have the form 1/pk with k ∈ Z, so since |a|p=p-1/2 this would give a contradiction.

Theorem. There exists afield Q^lg containing Qp as a subfield and having the following properties:

every a ∈ Q^lg is algebraic over Qp;

every polynomial f (X) ∈ Q^lg [X] has a root in Qplg.

Moreover, the norm||p on Qp extends to a unique non-Archimedean norm N on Q^lg satisfying

N (a)=|a|p

whenever a ∈ Qp. This extension is given by

N (a)=| minQp, a (0)|p1/d where d=degQp (a)=degminQp, a (X) is the degree of the minimal polynomial of a over Qp.

The minimal polynomial minQp, a (X) of a over Qp is the monic polynomial in Qp[X] of smallest positive degree having a as a root and is always irreducible. We will denote by||p the norm on Qplg given in

|a|p=|minQp, a (0)|p1/d.

Let us look at some elements of Qplg. Many examples can be found using the next two results.

Theorem. Let r=a/b be a positive rational number where a, b are coprime. Then the polynomial Xb— pa ∈ Qp[X] is irreducible over Qp and each of its roots a ∈ Q^lg has norm |a|p=p-a/b.

Corollary. If r=a/b is not an integer, then none of the roots of Xb— pa in Q^lg are in Qp.

Proof. We have \a\p=p a/b which is not an integral power of p. But we know that all elements of Qp have norms which are integral powers of p, hence a </ Qp.

The Eisenstein test of the next result provides an important criterion for finding irreducible polynomials over Qp.

Notes

Theorem (The Eisenstein test). Suppose that the polynomial

f (X)=Xd+ad-iXd-1+...+aiX+ao ∈ Zp[X]

satisfies the conditions

\ak\p<1 for each k in the range 0 ^ k ^ d— 1,

\ao\p=1/p.

Then f (X) is irreducible over Qp.

Example. Consider the polynomial

f1 (X)=Xp-i+Xp-2+...+X+1.

Notice that

Xp— 1= (X— 1)fi (X)

and so f1 (X) is the polynomial whose roots are all the primitive p-th roots of 1. Now consider the polynomial g1 (X)=f1 (X+1). Then

Xgi (X)= (X+1)p— 1=x p+<= (pyk

and so

g1 (X)= Xp-1+pT (p)xk-1.

k= 1 X '

Each of the binomial coefficients ^p^ for 1 ^ k ^ p— 1 is divisible by p; also ^p^=p, hence it is not divisible by p2. By the Eisenstein test, g1 (X) is irreducible over Qp and an easy argument also shows that f1 (X) is irreducible. Thus the primitive roots of 1 in are roots of the irreducible polynomial f1 (X) and have degree (p— 1) over Qp. If Zp is a root of f1 (X), then \Zp\p=1. The remaining roots are of the form (p with 1 ^ r ^ p— 1.

The roots of g1 (X) have the form (p— 1 for 1 ^ r ^ p— 1 and g1 (0)=p, so

Icp— 1|p=p-1/ (p-1).

Theorem. Let d ^ 1. Then the polynomial

fd (X)=f1 (Xpd-1)

is irreducible over Qp and its roots are the primitive p -th roots of 1 in Qp. If (pd is such a primitive root, any other has the form Zpd where 1 ^ k ^ pd— 1 and k is not divisible by p. Moreover, we have

I Zpd I=1,

|Zpd— l|p=p-<P-"pd-1.

Proof. This is proved by applying the Eisenstein test to the polynomial

gd (X)=fd (X+1),

which satisfies the conditions required and has gd (0)=p.

Corollary. If p is an odd prime, then 1 is the only p-th power root of 1 in Qp. If p=2, the only square roots of 1 in Q2 are ±1.

What about other roots of 1? We already know that there all the (p— 1)-st roots of 1 are in Qp; let us consider the d-th roots of 1 for any d> 1 not divisible by p. We begin by considering the case where d has the form d=pr— 1.

Proposition. For each r ^ 1, a primitive (pr— 1)-st root of 1, ∊ say, has degree r over Qp and has minimal polynomial

minQP, c (x)= n (x — zpt)-

0ytgr-1

Moreover, | ∊ | p= | ∊ — 1|p=1.

Now suppose that d is any natural number not divisible by p and ∊ is any d-th root of 1. Then for some m we have

pm=1;

we denote the smallest such m greater than 0 by md. Then for any primitive (pmd— 1)-th root of 1, Zpmd -i say, we can take

<==z t (pmd-i)/md <==Zpmd-i,

Notes

where t is an integer coprime to (pmd— 1)/md. This uses the fact that the group of roots of Xn— 1 in Qplg is always cyclic by a result from the basic theory of fields. From this it is possible to deduce

Proposition. Let d>0 be a natural number not divisible by p. Then any primitive d-th root of 1, <=, has degree over Qp dividing md. Furthermore,

| ∈ | p=1, ^— Mp=1- Corollary 5. 11. <= ∈ Qp if and only if md=1.

Theorem. Let <= ∈ Qplg be a primitive d-th root of 1. Let d=d0pf where d0 is not divisible by p. Then <= ∈ Qp if and only if one of the following conditions holds:

• p is odd, t=0 and md=1,

• p=2 and d=2.

Definition. Let a ∈ Qplg. Then a is ramified if |a|p is not an integral power of p, otherwise it is unramified. Let ∈ (a) be the smallest positive natural number such that ae (a) is unramified; then ∈ (a) is known the ramification degree of a.

Example. Let n be a square root of p. Earlier we saw that |n|p=p-1/2, hence n is ramified. In fact we have ∈ (a)=2.

This example generalises in an obvious way to roots of the polynomials Xb— pa

Now we can consider Qplg together with the norm||p in the light of. It is reasonable to ask if every Cauchy sequence in Qplg has a limit with respect to||p.

Proposition. There are Cauchy sequences in Q^lg with respect to||p which do not have limits. Hence, Q^lg is not complete with respect to the norm||p.

We can form the completion of Qplg and its associated norm which are denoted

Cp=Q?g, , , !!,,.

Proposition. If 0=a ∈ Cp, then

|a|p=p' where t ∈ Q.

Proof. We know this is true for a ∈ Qpg. if

a=lim (p)an

with an ∈ Qpg, then for sufficiently large n,

|a|p=|an|p.

Next we can reasonably ask whether an analogue of the Fundamental Theorem of Algebra holds in Cp.

Theorem. Cp is algebraically closed in the sense that every non-zero polynomial f (X) ∈ Cp[X] has a root in Cp. By construction, Cp is complete with respect to the norm||p.

Again, Of course we have now obtained a complete normed field containing Qp which is algebraically closed and this is the p-adic analogue of the complex numbers. It is helpful to compare the chains of fields

Q C R C C, Q C Qp C Qalg c Cp,

which are the sequences of fields we need to construct in order to reach the fields C and Cp in the real and p-adic worlds. This field Cp is the home of p-adic analysis proper and plays an important role in Number Theory and increasingly in other parts of Mathematics. We will confine ourselves to a few simple observations on Cp.

Consider a power series anxn where an G Cp. Then we can define the radius of convergence exactly as in Chapter 3, using the formula

r =limsup K|p1/n

Proposition. The series anxn converges if \x\p<r and diverges if \x\p>r, where r is the radius of convergence. If for some x0 with \x0\p=r the series anx converges (or diverges) thenYl anxn converges (or diverges) for all x with \x\p=r.

Example. Consider the logarithmic series (1 - x)n

logp (x)= — 5

n= 1

We showed that the radius of convergence is 1 for this example. Consider what happens when x=Zp, a primitive root of 1 as above. Then \ZP— 1\p=p1/ (p-1), so logp (ZP) is defined. Now by the multiplicative formula for this series,

logp ((Cp)p)=P logp (Cp^

and hence

P logp (Cp)=logp (1)=o.

Thus logp (Zp)=0. Similarly, for any primitive pn-th root of 1, Zpn say, we have that logp (Zpn) is defined and is o.

Example. Consider the exponential series

OO n

expp (x)=5 n. n=0 '

the radius of convergence was shown to be p-1/ (p-1). Suppose a G Cp with \a\p=p-1/ (p-1). Then

n= pordp n/ (p-1) n!

By considering the terms of the form apn/ (pn!), we obtain

v -. n= pn/ (p-1)= P-1/ (p-1)

which diverges to as n ^ rc>. So the series ^ an/n! diverges whenever\a \p=p In Cp we have the unit disc

Op={ a G Cp :\a \p ^ 1 }.

Proposition. The subset Op c Cp is a subring of Cp.

The proof uses the ultrametric inequality and is essentially the same as that for Zp c Qp. We end with yet another version of Hensel's Theorem, this time adapted to use in Cp.

Theorem. (Hensel's Theorem: Cp version). Let f (X) ∈ Op[X]. Suppose that Op and d>0 is a natural number satisfying the two conditions 1, , 1

|f (a)|p<', f' (a), p=pd.

Setting ai=a— f (a) f' (a)-1, we have

|f (ai)|p ^ p2d+3.

14.3 FIRST INTRODUCTION TO P-ADIC NUMBERS

In all that follows, p will stand for a prime number. N, Z, Q, R and C are the sets of respectively the natural numbers (i. ∈ . non negative integers), integers, rational numbers, reals and complex numbers.

In some— but not all— of what follows, we assume the reader is familiar with the notions of "group", "ring" and "field". We assume throughout that the reader knows the basic facts about the b-adic representation (i. ∈ . representation in base of integers and reals

Note: I did not aim here at writing a completely rigorous document, but only an easily understandable introduction for those who do not have any idea of what a p-adic is.

First definition

We will call p-adic digit a natural number between 0 and p— 1 (inclusive) A p-adic integer is by definition a sequence $(a_i)_{ieN}$ of p-adic digits. We write this conventionally as

$\ldots a_i \ldots a_2\ a_i\ a_0$

(that is, the a_i are written from left to right). If n is a natural number, and

n=ak-i ak-2 •• • ai ao

is its p-adic representation (in other words $n = \in - 0\ a_i p^i$ with each a_i a p – adic digit) then we identify n with the p-adic integer (a_i) with $a_i=0$ if $i>k$. This means that natural numbers are exactly the same thing as p-adic integer only a finite number of whose digits are not 0. Also note that 0 is the p-adic integer all of whose digits are 0, and that 1 is the p-adic integer all of whose digits are 0 except the right-most one (digit 0) which is 1.

If a= (aj) and fl= (bi) are two p-adic integers, we will now define their sum. To that effect, we define by induction a sequence (cj) of p-adic digits and a squence (+) of elements of { 0, 1 } (the "carries") as follows:

- $<=_0$ is 0.
- cj is $a+b_i+<=_i$ or $a_i+b_i+<=_i$— p according as which of these two is a p-adic digit (in other words, is between 0 and p— 1). In the former case, $<=_i$+i=0 and in the latter, $<=_{i+}$i=1.

Under those circumstances, we let a+fl= (cj) and we call a+fl the sum of a and fl. Note that the rules described above are exactly the rules used for adding natural numbers in p-adic representation. In particular, if a and fl turn out to be natural numbers, then their sum as a p-adic integer is no different from their sum as a natural number. So 2+2=4 remains valid (whatever p is— but if p=2 it would be written ... 010+... 010=... 100).

Here is an example of a 7-adic addition:

• • • 2 5 14 13 +
• • • 1 2
1 0 2

~ 4 0 2 5 1 5

This addition of p-adic integers is associative, commutative, and verifies a + 0=a for all a (recall that 0 is the p-adic integer all of whose digits are 0).

Subtraction of p-adic integers is also performed in exactly the same way as that of natural numbers in p-adic form. Since everybody reading this is assumed to have gone through first and second grade, we will not elaborate further :-).

Note that this subtraction scheme gives us the negative integers readily: for example, subtract 1 from 0 (in the 7-adics):

$$\begin{array}{r} \cdots 000000 \\ - \quad \cdots \underline{00000\,1} \\ \cdots 666666 \end{array}$$

(each column borrows a 1 from the next one on the left). So $-1=\ldots 666$ as 7-adics. More generally, -1 is the p-adic all of whose digits are $p-1$, -2 has all of its digits equal to $p-1$ except the right-most which is $p-2$, and so on. In fact, (strictly) negative integers correspond exactly to those p-adics all of whose digits except a finite number are equal to $p-1$.

It can then be verified that p-adic integers, under addition, form an abelian group. We now proceed to describe multiplication. First note that if n is a natural number and a a p-adic integer, then we have a naturally defined $na=a+\ldots+a$ (n times, with $0a=0$ of course). If n is negative, we let, of course, $na=-((-n)a)$. This limited multiplication satisfies some obvious equalities, such as $(m+n)a=ma+na$, $n(a+fl)=na+nfl$, $m(na)=(mn)a$, and so on (for those with some background in algebra, this is not new: any abelian group is a Z-module). Note also that multiplying by $p=\ldots 0010$ is the same as adding a 0 on the right. Multiplying two p-adic integers on the other hand requires some more work. To do that, we note that if a_0, ai, $a_2, \ldots$ are p-adic integers, with ai ending in (at least) one zero, a_2 ending in (at least) two zeroes, and so on, then we can define the sum of all the a^, even though they are not finite in number. Indeed, the last digit of the sum is just the last digit of a_0 (since a_1, $a_2, \ldots$ all end in zero), the second-last is the second-last digit of a_0+a_1 (because a_2, a_3, ... all end in 00), and so on: every digit of the (infinite) sum can be calculated with just a finite sum. Now we suppose that we want to multiply a and fl= (bi) two p-adic integers. We then let $a_0=b_0a$ (we know how to define this since b_0 is just a natural number), $a_1=pb_1a$, and so on: $a_i=p^ib_ia$. Since a_i is a p-adic integer multiplied by p^i, it ends in i zeroes, and therefore the sum of all the a_i can be defined.

This procedure can sound complicated, but, once again, it is still exactly the same as we have all learned in grade school to multiply two natural numbers. Here is an example of a 7-adic multiplication:

5 3 3 1 2 6

0 0 0 0 0

1 4 1 3

4 1 3

26

3

3 1 0 4 2 6

(of course, it is relatively likely that I should have made some mistake somewhere). We now have a set of p-adic integers, which we will call Z_p, with two binary operations on it, addition and multiplication. not do it— that Z_p is then a commutative ring (for those who don't know what that means, it means that addition is associative and commutative, that zero exists and satisfies the properties we wish it to satisfy, that multiplication is associative and commutative, and distributive over addition, and that 1 exists and satisfies the properties we wish it to satisfy (namely 1a=a for all a)).

Now, how about division? First, the bad news: division of p-adics is not performed in the same way as division of integers or reals. In fact, it can't always be performed. For example, 1/p has no meaning as a p-adic integer— that is, the equation pa =1 has no solution— since multiplying a p-adic integer by p always gives a p-adic integer ending in

0. There is nothing really surprising here: 1/p can't be performed in the integers either.

However, what is mildly surprising is that division by p is essentially the only division which cannot be performed in the p-adic integers. This statement (in technical terms "Z_p is a local ring") will not be made precise for the moment; however, we give a concrete example. Suppose p is odd (in other words, p=2). And let a be the p-adic integer all of whose digits are equal to (p— 1)/2 except the last one which is (p+1)/2. By performing 2a (in other words, a+a), it is clear that every digit will be zero except the last one which is 1. So 2a=1, in other words a=1/2.

For example, with our usual example of p=7 we show that the number a=... 333334 is the number "one half' by adding it to itself:

• • • 3 3 3 3 3 4 +

• • • 3 3 3 3 3 4

• • • 0 0 0 0 0 1

Thus, in the 7-adic integers, "one half' is an integer. And so are "one third" (... 44445), "one quarter" (... 1515152), "one fifth" (... 541254125413), "one sixth" (... 55556), "one eighth" (... 0606061), "one ninth" (... 3613613614), "one tenth" (... 462046205), "one eleventh" (... 162355043116235504312) and so on. But "one seventh", "one fourtneenth" and so on, are not 7-adic integers.

We now give a way to calculate the inverse (and therefore the quotient) of p-adic integers. Suppose a is a p-adic integer ending in zero (such numbers are known small for reasons we will describe later). Then $a^{\%}$ ends in at least i zeros. Therefore, as we have observen, we can calculate /3=1+a+a^5+••• even though it has an infinite number of terms. Multiplying this by (1— a) and expanding out (we shall admit that all the appropriate properties of addition are preserved when dealing with infinite sums) we find that (1— a)^=1— a+a— a^2+a^2 =1.

Therefore we are able to calculate the inverse of 1— a, which can be, as is easy

Any p-adic integer ending in 1. To summarize: p-adic integers ending in 0 have no inverse; those ending in 1 can be inverted with the formula described above. To inverse a p-adic integer a ending in a digit d other than 0 and 1, we find the (unique) digit f such that df is congruent to 1 mod p (i . ∈ . is equal to 1 plus a multiple of p). In that case, fa ends in 1 so can be inverted, and we then have 1/a=f/ (fa). To find f for small values of p, I have no better advice than checking successively all digits. Perhaps computer scientists can suggest an altogether faster method for inverting p-adics.

Up to now we have only described p-adic integers, and not p-adic numbers. We now proceed to define the latter. The relation between the set (ring) Z_p of p-adic integers and the set (field) Q_p of p-adic numbers is the same as between the set (ring) Z of integers and the set (field) Q of rationals. Namely, the second is obtained by taking quotients of an element of the first by a non zero element of the same— or, which amounts to the same, by adding new inverses to some elements of the first. In the case of the rationals, an inverse has to be added to every prime number p. In our case, however, we are fortunate, and adding an inverse to p only will suit our needs. We therefore proceed to do that.

We now define a p-adic number to be a Z-indexed sequence $(a_i)_{ieZ}$ of p-adic digits such that a=0 for sufficiently small i (explicitly: there exists i_0 ∈ Z such that a=0 for i<i_0). Such numbers are also written from right to left, with a "p-adic dot" after decimal 0. So our condition says: there are a finite number of non zero digits on the right of the p-adic point. We consider p-adic integers as p- adic numbers by identifying $(a_i)_{ieN}$ with $(a_i)_{ieZ}$ where a=0 for i<0, in other words by adding zeros to the right of the point. If a= (a^) is a p-adic number such that a=0 for i<i_0 (and we can certainly suppose i_0<0 so we do) then the p-adic number a' obtained by shifting every decimal of a by -io places to the left is a p-adic integer. We write $a=a'p^{i0}$ (or $a=a'/p^{-i0}$).

P-Adic numbers can then be added as follows: if $a=a'p^1$ with a' a p-adic intger, and $P=P'p^7$ ditto, and suppose moreover $^{i}<^{j}<0$, then we let a + P= $(a'+P'p^{j-t})p^{\%}$— note that $a'+P'p^{j-i}$ is indeed a p-adic integer. This is just a complicated way of saying that we add as usual, starting from the furthest (rightmost) column where there is a non zero digit. Multiplication is easier: under the same notations (except that the condition i<j is no longer necessary) we let $aP=a'P'p^{i+j}$. This says that we multiply "as usual", ignoring the p-adic dot, and then we place the dot in the "obvious" place where it should be.

The set Q_p of p-adic numbers, with this addition and multiplication, forms a field— in other words, all the properties of a ring are satisfied, and moreover every nonzero element has a multiplicative inverse.

Check your Progress-1

Discuss P-Adic Algebraic Number Theory

14.4 P-ADIC NUMBERS

Absolute values

The p-adic absolute value |-|p on Q is defined as follows: if a ∈ Q, a=0 then write a=pmb/c where b, c are integers not divisible by p and put |a|p=p-m; further, put |0|p=0.

Example. Let a= — 2-7385-3. Then |a|2=27, |a|3=3-8, |a|5=53, |a|p=1 for p ^ 7.

We give some properties:

|ab|p=|a|p|b|p for a, b ∈ Q;

|a+b|p ^ max (| a|p, |b|p) for a, b ∈ Q (ultrametric inequality). Notice that the last property implies that

|a+b|p=max (| a|p, |b|p) if |a|p=|b|p.

Notes

It is common to write the ordinary absolute value |a|=max (a, — a) on Q as |a|ro, to call ro the 'infinite prime' and to define Mq := U { primes }.

Then we have the important product formula:

^ \a\p=1 for a G Q, a=0.

Absolute values on fields.

We define more generally absolute values on fields. Let K be any field. An absolute value on K is a function \-\ : K ^ R^0 with the following properties:

\ab\=|a| \b\ for a, b G K;

|a+b\ ^ \a\+\b\ for a, b G K (triangle inequality); \a\=0 a=0.

Note that these properties imply that \1\=1. The absolute value\ \is known non-trivial if there is a G K with \a\={ 0, 1 }.

The absolute value\ \is known non-archimedean if the triangle inequality can be replaced by the stronger ultrametric inequality

\a+b\ ^ max (\a \, \b\) for a, b G K.

An absolute value not satisfying the ultrametric inequality is known archimedean.

If K is a field with absolute value\ \and L an extension of K, then an extension or continuation of \-\ to L is an absolute value on L whose restriction to K is\ \.

The ordinary absolute value\ \on Q is archimedean, while the p-adic absolute values are all non-archimedean.

Let K be any field, and K (t) the field of rational functions of K. For a polynomial f G K[t] define \f \=0 if f=0 and \f \=edeg f if f=0. Further, for a rational function f/g with f, g G K[t] define \f/g\=\f \/\g \. Verify that this defines a non-archimedean absolute value on K (t).

Two absolute values\ \i, \ \2 on K are known equivalent if there is a>0 such that \x\2=\x\a for all x G K. We state without proof the following result:

Theorem (Ostrowski). Every non-trivial absolute value on Q is equivalent to either the ordinary absolute value or a p-adic absolute value for some prime number p.

Valuations. In algebra and number theory, one quite often deals with val-uations instead of absolute values. A valuation on a field K is a function v : K ^ R U { to } such that for some constant c>1, c-v (• defines a non- archimedean absolute value on K. That is,

v (x)=to x=0;

v (xy)=v (x)+v (y) for x, y ∈ K;

v (x+y) ^ min (v (x), v (y)) for x, y ∈ K.

The valuation is known non-trivial if there is a ∈ K* with v (a)=0. The set v (K*) is an additive subgroup of R. The valuation v is known discrete if v (K*) is a discrete subgroup of R. A normalized discrete valuation is one for which v (K *)=Z.

14.5 VISUALIZATION Of P-ADIC NUMBERS

Our visual perception, whether due to high exposure from a young age or simply because of the biological properties of our brain I do not know, is based on standard Euclidean geometry. I doubt the physical universe is Euclidean in its geometry, but it is very clear that humankind relies on Euclidean geometry to perceive the universe. So strong is this reliance that even in the setting of p-adic topology, which clearly is not Euclidean, we have found a way to picture it using Euclidean geometry - as a matter of fact, we even used a language borrowed from Euclidean geometry and topology, such as balls and spheres, to talk about p-adic topology. However, the landscape created by p-adic topology is completely different to our intuition, thus, for example, as we have

Notes

already observen, the notions of open and closed balls becomes meaningless.

The goal of this section is to visualize the p-adic integers within our familiar framework of Euclidean geometry.

It is interesting to note that the topology on Z_p is inherently fractal, that is, Z_p is homeomorphic to the Cantor set and Q_p is homeomorphic to a finite disjoint union of Cantor sets. Consider the open set C_0 := [0, 1] and delete the middle third, obtaining the compact set C\=[0, |] U [|, 1]. Iterating on this construction we get a decreasing sequence of nested compact subspaces of the unit interval Co, where each C_n consists of 2^n closed intervals of length 3^{-n}.

Definition. A topological space that is homeomorphic to a complete metric space with a countable dense subset is known a Polish space, that is, a Polish space is a separable, completely metrizable topological space. .

Remark. Note that Polish spaces are not necessarily metric spaces, they admit many different complete metrics which then induce the same topology. A polish space with an unique metric is known a Polish metric space.

Example R^n, C^n, [0, 1], Zf and Q^n are Polish spaces.

Definition / Remark Let C_A **:= U**iez **(2i, 2i+1)** and for n $\in$ N inductively define C_n=C_{n-1} fl ($3^{-n}C_A$), then the set C := f|$i=_0$ C_i, the so known Cantor[6] set, is uncountably infinite and compact.

Now consider the 3-adic expansion of a natural number x=Y °$=_0$ x_i3^i, then the construction of Ci corresponds to removing those x $\in$ C_0 with x_0=1, the construction of C_2 corresponds to removing those x with x_i=1 and so on. In iteration we observe that the Cantor set C consists of elements that admit a 3-adic expansion of the form: ^°$=_i$ o_i3^{-i}, with $a_i \in$ { 0, 2 }. This doubling of the binary representation leads to the following

Remark. The Cantor set is homeomorphic to the Cantor space (C, ||) with the discrete topology. The Cantor space is a perfect, totally dis connected, uncountably infinite, compact Polish space. The actual homeo- morphism is given by the above construction using the ternary numeral system.

Proposition. The sets (Z_2, $||_2$) and (C, ||) are homeomorphic. A homeomorphism is given by p : Z_2 ^ C, $Yi=_0$ $x_i 2^i$ ^$Yi=_0$ $(2x_i)3^{-(i+1)}$

The case of an odd prime number is analog to the even case, we just need a more general

Definition. Let p ∈ P be arbitrarily chosen, C_A=$U_i$ez[2i, 2i+1] and C^p := [0, 1]. We define, by induction, Cn := $C^p{}_{n-i}$ f $((2p— 1)^{-n}C_A)$ and the p-Cantor set C^p is then defined as C^p := p|i_0 C^p.

Remark For a fixed n ∈ N, the set Cn consists of ^{n} disjoint open sets of length each $(2p— 1)^{-n}$. The p-Cantor set is obtained by dividing thosedisjoint sets into 2p— 1 subintervals of equal length and then deleting every second open interval.

Proposition The p-Cantor set is compact and uncountably infinity.

If we once again consider the (2p — 1)-adic expansion of a natural number x, then, completely analog to the even case, we observe that x ∈ C^n if and only if in its (2p— 1)-adic expansion, each x_n is even, which leads to the following

Remark. The Cantor sets C^p are homeomorphic to the Cantor spaces (C^p, ||) with the discrete topology. The Cantor spaces are perfect, totally disconnected, uncountably infinite, compact Polish spaces. The ac- tual homeomorphisms are given by the above construction using the (2p— 1)- ary numeral system.

Theorem. There is a homeomorphism between the metric spaces (Zp, ||p) and (C, ||), given by

p : Zp ^ C^{p}

ro ro

x=^Xip' ^ ^ (2xf) (2p— 1)$^{-(i+1)}$.

i=0 i=0

Definition. A closed metric space (X, d) is known perfect if it has no isolated points, that is, if it is equal to the set of its own limit points.

Proposition. Every uncountable Polish space contains a subset that is homeomorphic to C. In particular, every totally disconnected, perfect and compact metric space is homeomorphic to the Cantor set. A complete topological characterization of Cantor spaces is given by Brouwer[7] in the following sense: any two compact Hausdorff spaces with countable open bases are homeomorphic.

Summarizing the above discussion, we obtain the following, rather surprising

The p-adic fields Z_2 and Z_p are homeomorphic

14.6 CALCULATING WITH P-ADIC NUMBERS

The addition in Q_p is very straightforward:

Proposition. For x, y ∈ Q_p, x=J2 (=$_{-m}$ x%p%, y=J2i=$_{-n}$ y%P% and w. l. o. g. m>n we have

x ± y=Y (x% ± y%)p\

%=-m

where y%=0, for all i ∈ { -m, .. ., — n— 1 }.

Example. Take x =1 ∈ Q_p, then y=Yf=o (p— 1)p^n solves x+y=0.

Proposition. For x= (=$_{-m}$ x%p% and y=J2%=$_{-n}$ y%p% elements in Q_p we define

xy := Y ^{Z}%P%, %=-m-n

where ^{z} — $_m$ — n— ^{x}-m^y — nj ^{z}-m-n+l— ^{x}-m^y-n+^{x}-m^y — n+l ^{and} ^{z}-m-n — j Y=o x_{-m}+j_-%y_{-n}+% (compare this with the well-known Cauchy product for sequences).

Exercise Show that p ∈ Z_p has no multiplicative inverse in Z_p.

Exercise. Write a=... $a_2a_1a_0$ ∈ Z_p, then show that a admits a multiplicative inverse in Z_p if and only if a_0=0.

This is obviously completely different from the situation we are used to in Z, nevertheless Z_p is still not a field.

Remark PARI / GP[8] by H. Cohen[9], a computer algebra system with the main aim of facilitating number theory computations, has an inbuild support for p-adic numbers. One can create a p-adic number by simply typing: x=x+O (p^k), where k is the desired precision.

Example. Consider x=$_{6701}$9$_{3865}$ ∈ Q_{13}, using PARI we observe that |x| $_{13}$=13^{-5} yo9o8 $_{13}$=13^5, thus x ∈ Z_{13}, but x=x 13^5=^0_ ∈ Z_{13}.

Proposition A p-adic number x ∈ Q_p has a finite p-adic represent- ation, if and only if x=pn, for z ∈ Z, n ∈ N and p ∈ P.

Proof. Write

n n z

x=^ xip=p~^{m} ^ xip~$^{m+l}$= —, z ∈ Z,

i=-m i=-m^{p} as desired.

Conversely, if x=p^{-m}y, y ∈ N, then we can write y in the basis p and m.

get y=yip^{1}, as desired.

Proposition. Consider an arbitrary p-adic number x= G Q_p,

i=-m

then x G Q, if and only if there exist N, k G N such, that $x_n+_k=x_n$, for all n>N, that is, if x becomes periodic.

14.7 AN ALGEBRAIC CONSTRUCTION OF THE P-ADIC NUMBERS

Definition A projective system is a sequence (X_n, p_n) of sets and so known transition maps p_n : X_n 7 X_{n-1}. The projective limit of this sequence is a set X with maps $^{r}f_n$: X 7 X_n such, that $^{r}f_n=p_n$ o $^{r}f_{n+1}$ and satisfying the following condition: for each set Y and maps f_n : Y 7 X_n with $f_n=p_n$ o f_{n+1}, there is a unique factorization f of the f_n through the set X, that is $f_n={}^{r}f_n$ o f : Y 7 X 7 X_n.

Remark. A projective system can be represented by a diagram:

^{p}n+1 \r ^{p}n V V ^{P}°v v ... ----^{7} ^{X}n * ^{X}n-1 7 ... ^{X}

Proposition For every projective system (X_n, p_n) there exists a unique projective limit limX_n := (X, tf_n) C f X_n.

Proof. To observe that a limit actually exists, consider the set

X := { (Xn)|Pn (Xn+l)=Xn Vn>0 } C JJ Xn.

n=0

Then, by definition, for each $x \in X$ we have $p_n (n_{n+l} (x))=n_n (x)$, where the $n_n : X_n$ 7 X_n are the canonical projection maps. Thus the restrictions ${}^r f_n$ of those projections to X fulfill p_n o ${}^r f_{n+l}={}^r f_n$ and it is clear that (X, tf_n) is an upper bound for the given sequence.

Now we still have to prove that (X, tf_n) has the required universal prop-erty. To observe this, consider another tuple (X,if_n) satisfying the desired condition. We have to show that there is a unique factorization of ${}^r f_n$ b if_n, alas by the universal property of the product of sets and the projection maps, we know that there exists a unique map g : X 7 **fl**f=$_0$ X_n such, that the following diagram

n Xn n=0 ^{n}n

Chosing g= (^'$_n$) finishes the proof, as then im g C X and we can define the factoring function f, as in the definition, by restricting the codomain of g, that is, f : X ^ X, x ^ g (x).

The uniqueness follows again from the universal property.

Note that a projective limit neet not to be of the same kind as the sets (or groups, or rings or spaces) of the projective sequence. For example, in general, the projective limit of a sequence of fields is usually only a ring. Another example is that the projective limit of finite abelian groups need not to be finite. However in certain situations we can still save a lot of information from our spaces.

Proposition. For a projective system (X_n, p_n) of topological spaces and continuous maps, the projective limit is closed in nio X_n, if the X_n are Hausdorff spaces.

Proof. This follows immediately from the Hausdorff property, i. $\in$. we can find disjoint open neighbourhoods of Xi and p (x_{i+1}), thus it is easy to observe that ni=$_0$ X_i\X is open.

Now we return to the actual matter at hand, the construction of p-adic numbers. There is a natural, or canonical, surjective homomorphism En : $^Z/_p n_Z$ ^ $^Z/_p n\text{-}i_Z$ with ker <p=p^{n-1}Z and the sequence

$-^{Z}/p\text{-}z\ ^{Z}/p\text{-}iz \cdots ^{Z}/p2_{Z}\ ^{Z}/p_{Z}$, forms a projective system.

Definition. The ring of p-adic integers Z_p is defined as the projective limit of the above system.

Thus by definition, an element of Z_p=\jm (^{Z}/pnz, p_n) is a sequence a= (. . . ,a_n, .. ., a_1), with:

an $\in$ $^{Z}/_{p}$nz and En (an)=an-1 if n>2.

The ^{Z}/pnz, with the discrete topology, are compact topological spaces, thus by Tikhonov[10], their cartesian product is compact as well (in the product topology), for a proof of Tikhonov's theorem. Thus, as a closed subspace of a compact space, Z_p is a totally disconnected compact space.

In English: Z_p is closer to Z/nz than it is to Z/n+iz. Since Z_p is an integral domain the following definition makes sense.

Definition. The field of p-adic numbers Q_p is the field of fractions of Zp.

Proposition. Q_p is isomorphic to Q_p

Proof. This immediately follows from the universal property of the field of fractions of an integral domain.

Proposition. The following sequence is exact:

$$0 \ y\ ^{Z}p \longrightarrow ^{Z}p \longrightarrow ^{Z/}p^{n}Z\ \ y\ 0$$

ZZ With other words, Z/nZ is isomorphic to Z/nZ.

Proposition. An element a G Z_p lies in u_p if and only if p\a. Furthermore, each element a G Z_p can be written as $a=<=p^n$, with $\in$ G u_p.

14.8 QUADRATIC RESIDUES IN P-ADIC NUMBERS

An element a=Yli=$_0$ $a_i p^i$ ∈ Z is a square, if and only if a_0 is a quadratic residue modulo p.

Proof. If (y)=1, then, by Hensel's first Theorem, we know that X^2— a has a zero in Z*. Conversely, if a_0 is a quadratic residue modulo p, then there exists no b =$b_i p^i$ with $b^2 =_p a_0$.

With this ideas, we can classify the squares in Q_p:

Theorem. For an arbitrary prime p=2, we have

a ∈ Q_p is a square a=p^{2n} • <=^{2},

where n ∈ Z and <= ∈ Zp. The quotient group ^{q}p/q*2 has order 4 and, if we

fix an u ∈ u_p=Zp with= — 1, then the set { 1, p, u, up } is a complete system of representatives.

Proof. We have to consider the polynomial f (x)=x^2— a. For b ∈ Q_p with f (b)=0 it holds that ord_p (b^2)=2 • ord_p (b)=ord_p (a). We know that b can be written as b=$p^{ordp (b)}$ • <=, <= ∈ Zp, thus a=b^2=$p^{2ordp (b)}$ • <=^{2}. Now if conversely we have a=p^{2n} • <=^{2}, then b=p^n • ∈ .

The quadratic residues modulo p form a subgroup of (^/pZ)

Theorem. An element a ∈ Z2 is a square in Z_2, if and only if a $=_8$ 1. The factor group ^{q}/q*2 has order 8 and a complete system of representatives is given by { ±1, ±5, ±2, ±10 }.

Proposition. An element x ∈ Q is a square, if and only if it is a square in Q_p for all p ∈ P U { ^ }.

Proof. Arbitrarily chose x=± **]l**$_p$ e_P $p^{ordp (x)}$, x=0, then x is a square in Q^=R if and only if x>0 and it is a square in Q_p if and only if it can be written as x=p^{2n} with n ∈ Z and <= ∈ u_p, thus v_p (x) ∈ 2Z for all p ∈ P, which means that x is a square in Q .

14.9 ROOTS OF UNITY

Definition. Let K be a field. An element $Z \in K$ is known a n-th root of unity, for $n \in N$, if $Z^n=1$. If additionally $Z^m=1$, for $m \in N$ with $0<m<n$, then Z is known a primitive n-th root of unity.

Now if $Z \in Q_p$ with $Z^n=1$ for an $n \in N$, then $|Z|_p=1$, which means that all p-adic roots of unity are elements of u_p. Once again Hensel's Theorems give a complete answer to the question when p-adic roots of unity actually exist and what they look like.

Theorem. Let $p \in P$ be arbitrarily chosen and $n \in N$ such, that gcd (p, n)=1, then there exists a n-th p-adic root of unity in Q_p, if and only if n| (p— 1). If a n-th root of unity exists, it is automatically a (p— 1)-th root of unity as well and the set of all (p— 1)-th roots of unity is a subgroup of u_p with index p— 1.

Check your Progress-2

Discuss P-Adic Numbers

____

____

____

14.10 LET US SUM UP

In this unit we have discussed the definition and example of P-Adic Algebraic Number Theory, First Introduction To P-Adic Numbers, P-Adic Numbers, Visualization Of P-Adic Numbers, Calculating With P-Adic Numbers, An Algebraic Construction Of The P-Adic Numbers, Quadratic Residues In P-Adic Numbers, Roots Of Unity

14.11 KEYWORDS

P-Adic Algebraic Number Theory…. In this section we will discuss a complete normed field Cp, which contains Qp as a subfield and has the property

First Introduction To P-Adic Numbers…. In all that follows, p will stand for a prime number. N, Z, Q, R and C are the sets of respectively the natural numbers (i. ∈ . non negative integers), integers, rational numbers, reals and complex numbers.

P-Adic Numbers…. The p-adic absolute value |-|p on Q is defined as follows: if a ∈ Q, a=0 then write a=pmb/c

Visualization Of P-Adic Numbers… Our visual perception, whether due to high exposure from a young age or simply because of the biological properties of our brain I do not know, is based on standard Euclidean geometry .Calculating With P-Adic Numbers…. The addition in Q_p is very straightforward:An Algebraic Construction Of The P-Adic Numbers…. A projective system is a sequence (X_n, p_n) of sets and so known ransition maps p_n : X_n 7 X_{n-1}Quadratic Residues In P-Adic Numbers ….. An element a=Yli=$_0$ $a_i p^i$ ∈ Z is a square, if and only if a_0 is a quadratic residue modulo p .Roots Of Unity…. Let K be a field. An element Z ∈ K is known a n-th root of unity

14.12 QUESTIONS FOR REVIEW

Explain P-Adic Algebraic Number Theory

Explain P-Adic Numbers

p-adic numbers: an introduction by Fernando Gouvea

14.13 REFERENCES

p-adic Numbers, p-adic Analysis, and Zeta-Functions, Neal Koblitz (1984, ISBN 978-0-387-96017-3)

A Course in p-adic Analysis by Alain M Robert

Analytic Elements in P-adic Analysis by Alain Escassut

14.14 ANSWERS TO CHECK YOUR PROGRESS

P-Adic Algebraic Number Theory

(answer for Check your Progress-1 Q)

P-Adic Numbers

(answer for Check your Progress-2 Q)