DIRECTORATE OF DISTANCE EDUCATION

UNIVERSITY OF NORTH BENGAL

MASTERS OF SCIENCE -MATHEMATICS

SEMESTER–I

P ADIC ANALYSIS

DEMATH-1 ELEC-5

BLOCK-1

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

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 1-P ADIC ANALYSIS

Introduction to the Block

In this block we will go through Congruences And Modular Equations

Convergent series Charts And Atlases Theory of valuations-I

The P-Adic Norm And The P-Adic Numbers Theory of valuations -II

Representations of p-adic groups

Unit I Deals with Congruences And Modular Equations

Unit II Deals with Convergent series

Unit III Deals with Charts And Atlases

Unit IV Deals with Theory of valuations-I

Unit V Deals with The P-Adic Norm And The P-Adic Numbers

Unit VI Deals with Theory of valuations -II

Unit VII Deals with Representations of p-adic groups

UNIT – 1 : CONGRUENCES AND MODULAR EQUATIONS

STRUCTURE

1.0 OBJECTIVES

After studying this unit, you should be able to:

- Understandabout Congruences and modular equations, Ultrametric Spaces
- Understand about Nonarchimedean Fields
- Understand about Congruences and modular equations

1.1 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.

Congruences and modular equations, Ultrametric Spaces, Nonarchimedean Fields, Congruences and modular equations.

1.2 CONGRUECES AND MODULAR EQUATIONS

ULTRAMETRIC SPACES

We begin by establishing some very basic and elementary notions.

Definition.A metric space (X, d) is knownultrametric if the strict triangle inequalityd(x, z)<max(d(x, y), d(y, z)) for any x, y, z ∈ X is satisfied.

Remark.i.If (X, d) is ultra-metric then (Y, d |Y x Y), for any subset Y ∈ X, is ultra-metric as well.

ii.If (Xi, di), ..., (Xm, dm) are ultrametric spaces then the Cartesian product

Xi x...x Xm is ultrametric with respect to

d((xi, ..., xm), (yi, ..., ym)) := max(di(xi, yi), ..., dm(xm, ym)).

Let (X, d) be an ultrametric space in the following.

Theorem.For any three points x, y, z ∈ X such that d (x, y)=d(y, z) we have d(x, z)=max(d(x, y), d(y, z)).

Proof.We can assume that d (x, y)<d(y, z).Then

d (x, y)<d(y, z)<max(d(y, x), d(x, z))=max(d(x, y), d(x, z)).The maximum in question therefore necessarily is equal to d (x, z) so that

d (x, y)<d(y, z)<d(x, z).

We deduce that

d (x, z)<max(d(x, y), d(y, z))<d(x, z).

Let a ∈ X be a point and ∈ >0 be a positive real number.We call B ∈ (a) :={ x ≤X : d(a, x)< ∈ } the closed ball and B-(a) :={ x ≤X : d(a, x)< ∈ } the open ball around a of radius ∈ .Any subset in X of one of these two kinds is simply referred to as a ball.As the following facts show this language has to be used with some care.

Theorem.i.Every ball is open and closed in X.

ii.For b ≤B≤ (a), resp.b ≤B~ (a), we have B≤(b)=B≤(a), resp.B-(b) =B-(a).

Proof.Obviously B-(a) is open and B ∈ (a) is closed in X.We first consider the equivalence relation x ~ y on X defined by d (x, y)< ∈ .The corresponding equivalence class of b is equal to B-(b) and hence is open.Since equivalence classes are disjoint or equal this implies B-(b)=B~(a)when ever b ≤B- (a).It also shows that B- (a) as the complement of the other open equivalence classes is closed in X.

Analogously we can consider the equivalence relation x w y on X defined by d (x, y)< ∈ .Its equivalence classes are the closed balls

B≤ (b), and we obtain in the same way as before the assertion ii.for closed balls.It remains to show that B≤ (a) is open in X.But by what we have established already with any point b ≤B≤ (a) its open neighborhood B- (b) is contained in B ≤(b)= B ≤(a).

The assertion ii.in the above Theorem can be viewed as saying that any point of a ball can serve as its midpoint.By way of an example we will observe later on that also the notion of a radius is not well determined.

Theorem.For any two balls B and B' in X such that B n B'=0 we have B C B' or B' C B.

Proof.Pick a point a ≤ B n B'.As a consequence ofTheorem following four cases have to be distinguished:

1.B=B-(a), B'=B- (a),

2.B=B-(a), B'=Bs(a),

3.B=Be (a), B'=B-(a),

4.B=Be (a), B'=B- (a).

In cases 1, 2, and 4 we then obviously have B C B'.In case 3 we obtain B C B' if ∈ <5 and B' C B if ∈ = 5.

Notes

Remark.If the ultrametric space X is connected then it is empty or consists of one point.

Proof.Assuming that X is nonempty we pick a point a ≤X.then implies that X=B ≤ (a) for any ∈ >0 and hence that X={ a }.

Theorem.Let U=(Jiei U be a covering of an open subset U C X by open subsets Ui C X; moreover let ei>e2>...>0 be a strictly descending sequence of positive real numbers which converges to zero; then there is a decomposition

U=U Bj≤eJ of U into pairwise disjoint balls Bj such that:

Bj=B≤ n (j)(aj) for appropriate aj≤ X and n(j)≤ N,

Bj C Uj for some i (j)≤ I.

Proof.For a ≤ U we put

n (a) := min{ n ≤N : B ≤ n(a) C Ui for some i ∈ I }.

The family of balls J :={ B≤ n(a)(a) : a ≤ U}by construction has the properties (a) and (b) and covers U (observe that for any point a in the open set Ui we find some sufficiently big n ∈ N such that B ∈ n (a) C Ui).The balls inthis family indeed are pairwise disjoint: Suppose that B ∈ n (a1)(al) n B ∈ n(a2)

By Theorem we can assume that B ∈ n (a1) (ai) C B ∈ n(a1) (a2).then

Theorem implies that B ∈ n (a1)(ai)=B ∈ n(a1)(a2) and hence B ∈ n(a1)(ai) C B ∈ n(a1) (ai).Due to the minimality of n (ai) we must have n(ai)<n(a2), resI) ^ (1)> ∈ (2).

It follows thatB ∈ n (a1)(ai)=B ∈ n(a2)(ai)=B ∈ n(a2)(a2)

As usual the metric space X is known complete if every Cauchy sequence in X is convergent.

Theorem.A sequence (xn)neN in X is a Cauchy sequence if and only if limn — d(xn xn+1) — 0.For a subset A C X we call d (A) : — sup{ d(x, y) : x, y ∈ A}the diameter of A.

Theorem.Let B C X be a ball with ∈ : — d(B)>0 and pick any point a G B; we then have B — B- (a) or B — B ∈ (a).

Proof.The inclusion B C B ∈ (a) is obvious.By Theorem the ball B is of the form B — B- (a) or B — B>(a).The strict triangle inequality then implies ∈ — d(B)<5.If ∈ - 5 there is nothing further to prove.If ∈ <5 we have B C B ∈ (a) C B- (a) C B and hence B — B ∈ (a).

Let us consider a descending sequence of balls Bi D B2 ^5 Bn D...in X.If X is complete and if limn — TO d (Bn) — 0 then we claim that Q Bn — 0.n ∈ n If we pick points xn G Bn then (xn)n∈N is a Cauchy sequence.Put x : — limn — TO xn.Since each Bn is closed we must have x G Bn and therefore x G n nBn.

Without the condition on the diameters the intersection P|n Bn can be empty (compare the exercise further below).This motivates the following definition.

Definition.The ultrametric space (X, d) is known spherically complete if any descending sequence of balls B1 D B2 D...in X has a nonempty intersection.

Theorem.If X is spherically complete then it is complete.

ii.Suppose that X is complete; if 0 is the only accumulation point of the set d (X*X) C R+ of values of the metric d then X is spherically complete.

Proof.i.Let (xn)neN be any Cauchy sequence in X.We can assume that this sequence does not become constant after finitely many steps.Then the en := max{ d(xm, Xm+1) : m>n }

are strictly positive real numbers satisfying en>en+1 and en>d (xn, xn+1).Using Theoremii.we obtain B ∈ n (x.n)= B ∈ n (x„+i) D B ∈ n+1 (xn+i).By assumption the intersection fn B ∈ n (xn) must contain a point x.We have d (x, xn)<en for any n ∈ N.Since the sequence (en)n converges to zero this implies that x=limx^^ xn.

Notes

ii.Let B1D^B2 D...be any decreasing sequence of balls in X.Obviously we have d (B1)>d(B2)>...By our above discussion we only need to consider the case that infnd (Bn)>0.Our assumption on accumulation points implies that d (Bn) ∈ D(X*X) for any n ∈ N and then in fact that the sequence (d(Bn))n must become constant after finitely many steps.Hence there exists an m ∈ N such that 0<e := d(Bm)=d(Bm+1)=...ByTheorem we have, for any n>m and any a ∈ Bn, that Bn=B- (a) or B, n=B^a).

Moreover, which of the two equations holds is independent of the choice of a by Theorem.ii.Case 1: We have Bn=B ∈ (a) for any n>m and any a ∈ Bn.It immediately follows that Bn=Bm for any n>m and hence that P|n Bn=Bm.Case 2: There is an t>m such that B^=B-(a) for any a ∈ B^.For any n>t and any a ∈ Bn C B^ we then obtain B-(a)=B^ D Bn D B- (a) so that B^=Bn and hence P|n Bn=B^.

Exercise.Suppose that X is complete, and let B1 D B2 D...be a decreasing sequence of balls in X such that d (B1)>d(B2)>...and infnd (Bn)>0.Then the subspace Y := X\(P|n Bn) is complete but not spherically complete.

Theorem.Suppose that X is spherically complete; for any family (Bi)ie/ of closed balls in X such that B^ n Bj=0 for any i, j ∈ / we then have di/ Bi=0.

Proof.We choose a sequence (in)neN of indices in I such that:

d (Bii)>d(Bi2)>...>d (Bin)>...,

for any i ∈ I there is an n ∈ N with d (Bj)>d(Bin).

The proof of Theorem shows that Bj=Bd (B.)(a) for any a ∈ B^ Our assumption on the family (Bi)i therefore implies that:

Bh D Bl2 D...D BlnD ..., for any i ∈ I there is an n ∈ N with Bi D Bin.nBi=nBin=0.

Check your Progress-1

Discuss Congruences and modular equations

____

____

____

1.3 NONARCHIMEDEAN FIELDS

Let K be any field.

Definition.A nonarchimedean absolute value on K is a function

||: K — ► R

which satisfies:

|a|>0,

|a|=0 if and only if a=0,

|ab|=|a|.|b|,

b \<max(|a |, |b|).

Exercise.i^ 1 |<1 for any n ∈ Z.

||:Kx —>Rx is a homomorphism of groups; in particular, |1|=

|- 1|=1.

K is an ultrametric space with respect to the metric d (a, b) :=|b — a|; in particular, we have |a+b|=max(|a |, |b|) whenever |a|=|b|.

Addition and multiplication on the ultrametric space K are continuous maps.

Definition.A nonarchimedean field (K, ||) is a field K equipped with a nonarchimedean absolute value ||such that:

||is non-trivial, i. ∈ ., there is an a ∈ K with |a|=0, 1,

K is complete with respect to the metric d (a, b) :=|b — a|.

Notes

The most important class of examples is constructed as follows.We fix a prime number p.Then \a\p := p-r if a=prime with r, m, n ∈ Z and p \mn is a nonarchimedean absolute value on the field Q of rational numbers.

The corresponding completion Qp is known the field of p-adicnumbers.Of course, it is nonarchimedean as well.We note that \Qp\p=pZ U{0 }.Hence Qp isspherically complete by Theoremii.On the other hand we observe that in theultrametric space Qp we can have Be (a)=B∃(a) even if e=5.To have more examples we state) the following fact.Let K/Qp be any finite extension of fields.Then

\a\ :=K:Qpy \NormK/qp(a)\p

is the unique extension of ||p to a nonarchimedean absolute value on K.The corresponding ultrametric space K is complete and spherically complete and, in fact, locally compact.

In the following we fix a nonarchimedean field (K, \\).By the strict triangle inequality the closed unit ball

ok : = Bi(0) is a subring of K, known the ring of integers in K, and the open unit ball mK := B- (0) is an ideal in ok.Because of oK=ok \mK this ideal mK is the only maximal ideal of ok.The field ok/mK is known the residue class field of K.

Exercise.If the residue class field ok/mK has characteristic zero then K has characteristic zero as well and we have \a\=1 for any nonzero a ∈ Q C K.

ii.If K has characteristic zero but ok/mK has characteristic p>0 then we have log |p| \ a\=\ a \p log p for any a ∈ Q C K; in particular, K contains Qp.

A nonarchimedean field K as in the is known a p-adicfield.

Theorem.If K is p-adic then we have n — 1

|n|>|n!|>|p|p — 1 for any n ∈ N.

Definition.A (nonarchimedean) norm on V is a function ||||: V —>R such that for any v, w ∈ V and any a ∈ K we have:

||av||=|a|.||v||, ||v+w||<max(||v||, ||w||),

if ||v||=0 then v=0.

Moreover, V is known normed if it is equipped with a norm.

Exercise..||v||>0 for any v ∈ V and ||0|=0.

V is an ultrametric space with respect to the metric d(v, w) :=||w — v||; in particular, we have ||v+w||=max(||v||, ||w||) whenever ||v|=||w||.Addition V*V V and scalar multiplication K x V —► V are continuous.

Theorem.Let (Vi, ||.||i) and (V2, ||.||2) let two normed K-vector spaces; a linear map f : Vi —>V2 is continuous if and only if there is a constant c>0 such that

IIf (v)112<c||v|i for any v ∈ Vi.

Proof.We suppose first that such a constant c>0 exists.Consider any sequence (vn)neN in Vi which converges to some v ∈ Vi.Then(||vn — v|i)n and hence (|f (vn) — f (v)|2)n=(||f (vn — v)|2)n are zero sequences.It follows that the sequence (f (vn))n converges to f (v) in V2.This means that f is continuous.Now we assume vice versa that f is continuous.We find a 0< ∈ <1 such that Be (0) C f-i(Bi(0)).

Since ||is non-trivial we can assume that ∈ = |a|for some a ∈ K.In otherwords||v|i<|a|implies |f(v)|2<1 for any v G V\.Let now 0=v ∈ Vi be an arbitrary nonzero vector.

We find an m G Z such thatB\a\m+2<||v||i<\ a\m+1.

Setting c :=|a|- 2 we obtain 11/(v)112=\a\m •/(a-mv)||2<\ a\m<c • ||v|i.

Definition.The normed K-vector space (V, ||.||) is known a K-Banach space if V is complete with respect to the metric d(v, w) :=||w — v||.

Examples.Kn with the norm ||(a1, ..., an)||:= max1<i<\ a is a K-Banach space.

Notes

Let I be a fixed but arbitrary index set.A family (aj,)ie/ of elements in K is known bounded if there is a c>0 such that \aj \<c for any i G I.The set ∈ ^ (I) := set of all bounded families (a^)ie/ in K

with componentwise addition and scalar multiplication and with the norm ||(ai)i|U := sup\ai\ i∈/ is a K-Banach space.

With I as above let

co (l) :={ (a i)ie/ g ∈ (I) : for any ∈ >0 we have \ai \>e

for at most finitely many i G I }.

It is a closed vector subspace of ∈ ™ (I) and hence a K-Banach space in its own right.Moreover, for(ai)i∈ c0(I) we have

||(ai)i — max \ ai\.ie/

For example, c0(N) is the Banach space of all zero sequences in K.

Remark.Any K-Banach space (V, ||||) over a finite extension K/Qp which satisfies ||V||C \K\ is isometric to some K-Banach space (c0(I), ||); moreover, all such I have the same cardinality.

Let V and W be two normed K-vector spaces.From now on we denote, unless this causes confusion, all occurring norms indiscriminately by ||||.It is clear that

L (V, W) :={ / ∈ HomK(V, W) : f is continuous} is a vector subspace of HomK(V, W).the operator norm

||f ||:= sup ||f ((V)I : v ∈ V, v=0 =sup j : v ∈ V, 0<||v||<1

is well defined for any / ∈ L (V, W).

Theorem.L (V, W) with the operator norm is a normed K-vector space.Proposition.If W is a K-Banach space then so, too, is L(V, W).

Proof.Let (fn)nen be a Cauchy sequence in L(V, W).Then, on the one hand, (||fn||)n is a Cauchy sequence in R and therefore converges, of course.On the other hand, because of

IIfn+1 (v)-fn(v)||=||(fn+1 -fn) (v)||<||fn+1 -fn||1||

we obtain, for any v ∈ V, the Cauchy sequence (fn(v))n in W.By assumption the limit f (v) := limn fn(v) exists in W.Obviously we have

f (av)=af(v) for any a ∈ K.

For v, v' ∈ V we compute

f (v)+f (v')=limfn(v)+limfn(v')=lim(fn(v)+fn(v'))

n= limfn (v+v')=f(v+v').

This means that v i —>f (v) is a K-linear map which we denote by f.Since ||f (v)|=lim||fn(v) H<(lim||fn|nn

it follows from Theorem that f is continuous.Finally the inequality 11 /-fn II =sup{ : v=0

su limm jfm (v)-fn(v) I : v — 0

sup \ ||||: V 0

I IMI

<lim jfm - fn j<sup jfm+1 - fmj

m>n

shows that f indeed is the limit of the sequence (fn)n in L(V, W).

In particular,

V' :- L(V, K)

always is a K-Banach space.It is known the dual space to V.

---

1 — ^2 ai 1i .

Applying any <= ∈ co (N)' by continuity leads to

≤ (v) — ^ ai≤ (1i) .

Theorem.Let I be an index set; for any j ∈ I let 1j ∈ c0 (I) denote the family (a/)^/ with ai — 0 for i — j and aj — 1; then

co (I)' - ∈ ™(I)is an isometric linear isomorphism.

Proof.We give the proof only in the case I — N.The general case follows the same line but requires the technical concept of summability.Let us denote the map in question by i.Because of

| ∈ (ii) |<j ∈ j …jiilU — j ∈ j

it is well defined and satisfies

j ∈ j for any ∈ ∈ c0(N)'.

For trivial reasons i is a linear map.Consider now an arbitrary nonzero vector v —(ai)i ∈ c0(N).In the Banach space c0 (N) we then have the convergent series expansion

We obtain

| ∈ (v) |<supi|ai||<(1i) |<sup |<(li)|=||v||^ supi|a>|

It follows that together with the previous inequality that i in fact is an isometry and in particular is injective.For surjectivity let (ci)i G ∈ ^(N) be any vector and put ∈ :=||(cj)j||ro.We consider the linear form ∈ : Co(N —>K (ai)i 1 aicii

(note that the defining sum is convergent).Using Theorem together with the inequality

| ∈ ((fli)i)|=|^2 Oi0i \<sup |ai||ci |<sup |ai|

sup |ci|= ∈ ||(ai)i||^i

we observe that ∈ is continuous.It remains to observe that

i (∈)=(∈ (1i))i=(ci)i.

Check your Progress-2

Discuss Nonarchimedean Fields

1.4 CONGRUENCES AND MODULAR EQUATIONS

Let n ∈ Z (we will usually have n>0).We define the binary relation

Definition.If x, y ∈ Z, then x=y if and only if n |(x — y).This is often also writtenx=y (mod n) or x=y (n).

When n=0, x=y if and only if x=y, so in that case=is really just equality

Proposition The relation=is an equivalence relation on Z.

Proof.Let x, y, z ∈ Z.Clearly=is reflexive since n |(x — x)=0.It is symmetric since

if n |(x — y) then x — y=kn for some k ∈ Z, hence y — x=(-k)n and so n |(y — x).For transitivity, suppose that n |(x — y) and n |(y — z); then since x — z=(x — y)+(y — z) we have n |(x — z).

If n>0, we denote the equivalence class of x ∈ Z by [x]n or just [x] if n is understood; it is also common to use x for this if the value of n is clear from the context.From the definition,

[x]n={ y ∈ Z : y=x }={ y ∈ Z : y=x+kn for some k ∈ Z },

and there are exactly |n|such residue classes, namely

[1]n ..., [n 1]n.

Of course we can replace these representatives by any others as required.

Definition.The set of all residue classes of Z modulo n is

Z/n={ [x]n : x=0, 1, ..., n — 1 }.

If n=0 we interpret Z/0 as Z.

Consider the function

nn: Z —>Z/n; nn(x)=[x]n.

Notes

This is onto and also satisfies

n- :(a)={ x ∈ Z : x ∈ a }.

We can define addition+and multiplication x on Z/n by the formula

[x]n +[y]n=[x+y]n, [x]n X [y]n=[xy]n,

which are easily observen to be well defined, i. ∈ ., they do not depend on the choice of representatives x, y.The straightforward proof of our next result is left to the reader.

Proposition The set Z/n with the operations+and x is a commutative ring

function nn: Z —>Z/n is a ring homomorphism which is surjective (onto) and has kernel

kernn=[0]n={ x ∈ Z : x=0 }.

Now let us consider the structure of the ring Z/n.The zero is 0=[0]n and the unity is 1=[1]n.We can also ask about units and zero divisors.In the following, let R be a commutative ring with unity 1 (which we assume is not equal to 0).

Definition An element u ∈ R is a unit if there exists a v ∈ R satisfying

uv=vu=1.

Such a v is necessarily unique and is known the inverse of u and is usually denoted u-1.

Definition z ∈ R is a zero divisor if there exists at least one w ∈ R with w=0 and zw=0.There can be lots of such w for each zero divisor z.

Notice that in any ring 0 is always a zero divisor since 1/0=0=0/1.

Example.Let n=6; then Z/6={ 0, 1, ..., 5 }.The units are 1, 5 with 1 1=1 and 5 1 =5 since 52=25=1.The zero divisors are 0, 2, 3, 4 since 2x3=0.

In this example notice that the zero divisors all have a factor in common with 6; this is true for all Z/n (observe below).It is also true that for any ring, a zero divisor cannot be a unit (why?) and a unit cannot be a zero divisor.

Recall that if a, b ∈ Z then the greatest common divisor (gcd) or highest common factor (hcf) of a and b is the largest positive integer dividing both a and b.We often write gcd (a, b) for this.When a=0=b we have gcd (0, 0)=0.

Theorem.Let n>0.Then Z/n is a disjoint union

Z/n={ units}U{zero divisors }

where{units}is the set of units in Z/n and{zero divisors}the set of zero divisors.Furthermore,

z is a zero divisor if and only if gcd (z, n)>1;

u is a unit if and only if gcd (u, n)=1.

Proof.If h=gcd (x, n)>1 we have x=x0h and n=n0h, so

n0x=0.

Hence x is a zero divisor in Z/n.

Let us prove (b).First we suppose that u is a unit; let v Then uv=1 and so for some integer k,

uv — 1=kn.

But then gcd (u, n)|1, which is absurd.So gcd (u, n)=1.Conversely, ifgcd(u, n)=1 we must demonstrate that u is a unit.To do this we will need to make use of the Euclidean Algorithm.

Recollection [Euclidean Property of the integers] Let a, b ∈ Z with b=0; then there exist unique q, r ∈ Z for which a=qb+r with 0 ^ r<|b|.

Theorem (The Euclidean Algorithm) integers Qi, Ti satisfying

a=Q\b+Ti To=b=Q2T1+T2 Ti=Q3T2+T3

0=Tn -1=QN+1TN

where we have 0+Ti<Ti-1 for each i.Furthermore, we have tn=gcd(a, b) and then by back substitution for suitable s, t ∈ Z we can write

tn=sa+tb.

Example If a=6, b=5, then r0=5 and we have

6=1*5+1, so q1=1, r1=1,

5=5*1, so q2=5, r2=0.

Therefore we have gcd (6, 5)=1 & we can write 1=1* 6+(-1)* 5

Using the Euclidean Algorithm, we can write su+tn=1 for suitable s, t ∈ Z.But then su=1 and s=u-1, so u is indeed a unit in Z/n.

These proves part (b).But we also have part (a) as well since a zero divisor z cannot be a unit, hence has to have gcd(z, n)>1.

To determine the number of units and zero divisors in Z/n.We already have |Z/n|=n.

Definition.(Z/n)x is the set of units in Z/n.(Z/n)x becomes an abelian group under the multiplication x.

n

Let+(n)=|(Z/n)x|=order of (Z/n)x.By Theorem 1.8, this number equals the number of integers 0, 1, 2, ..., n — 1 which have no factor in common with n.The function+is known as the Euler+- function.

Example n=6: |Z/6|=6 and the units are 1, 5, hence +(6)=2.

Example n=12: |Z/12|=12 and the units are 1, 5, 7, 11, hence +(12)=4.

In general+(n) is quite a complicated function of n, Let a, b ∈ Z then there are unique sequences of

however in the case where n=p, a prime number, the answer is more straightforward.

Example Let p be a prime (i. ∈ ., p=2, 3, 5, 7, 11,...).Then the only non-trivial factor of p is p itself, so +(p)=p — 1.We can say more: consider a power of p, saypr with r>0.Then the integers in the list 0, 1, 2, ..., pr — 1 which have a factor in common with pr are precisely those of the form kp for 0+k+pr-1 — 1, hence there are pr-1 of these.So we have+(pr)=pr-1(p — 1).

Example When p=2, we have the groups (Z/2)x={ 1 }, (Z/22)x={ 1, 3 }=Z/2, (Z/23)x={ 1, 3, 5, 7 }=Z/2 x Z/2, and in general

(Z/2r+1)x Z/2 x Z/2r-i

for any r ^ 1.Here the first summand is{±1}and the second can be taken to be

Now for a general n we have

n=pi1 p22 … pSs

where for each i, pi is a prime with

2 ^ pi<P2<<Ps

and ri ^ 1.Then the numbers pi, ri are uniquely determined by n.We can break down Z/n into copies of Z/pri, each of which is simpler to understand.

Theorem.There is a unique isomorphism of rings

: Z/n=Z/pi1 x Z/p22 x … x Z/prss

and an isomorphism of groups

Tx :(Z/n)x ^ (Z/pi1)x x(Z/p22)x x … x (Z/pSs)x.

Thus we have

^ (n)=^(pi1)^(p22) … ^(pSs).

Proof.Let a, b>0 be coprime (i. ∈ ., gcd(a, b)=1).We will show that there is an isomorphism of rings

T: Z/ab=Z/a x Z/b.

there are u, v G Z such that ua+vb=1.It is easily checked that gcd (a, v)=1=gcd(b, u).

Define a function

T: Z/ab —>Z/a x Z/b; T([x]af ∈)=([x]a, [x]b).

This is easily observen to be a ring homomorphism.Notice that

|Z/ab|=ab=|Z/a||Z/b|=|Z/a x Z/b|

and so to show that T is an isomorphism, it suffices to show that it is onto.

Let ([y]a, [z]b) G Z/a x Z/b.

We must find an x G Z such that T ([x]ab)=([y]a, [z]b).

Now set x=vby+uaz; then

x=(1 — ua)y+uaz=[y]a

x=vby+(1 — vb)z=[z]b

hence we have T ([x]ab)=([y]a, [z]b) as required.

To prove the result for general n we proceed by induction upon s.Example Consider the case n=120.Then 120=8*3*5=2*4*3*5 and so the Theorem predicts that

Z/120=Z/8 x Z/3 x Z/5.

We will verify this.First write 120=24*5.Then gcd (24, 5)=1 since

24=4*5+4=^ 4=24 -4*5 and 5=4+1=^ 1=5 - 4,

Hence 1=5*5 -24.

Therefore we can take a=24, b=5, u= — 1, v=5 in the proof of the Theorem.Thus we have a ring isomorphism

Ti: Z/120 Z/24 x Z/5…Ti([25y - 24z]i2o)=([y]24, M5),

as constructed in the proof above.Next we have to repeat this procedure for the ring Z/24.Here we have

8=2*3+2=^ 2=8 -2 and 3=2+1=^ 1=3 - 2,

So gcd (8, 3)

Hence there is an isomorphism of rings

T2: Z/24 — ► Z/8 x Z/3; T2 ([9x - 8y]24)=([x]s, [y]3),

and we can of course combine these two isomorphism to obtain a third, namely

T: Z/120 Z/8 x Z/3 x Z/5; T ([25(9x - 8y)- 24z]i2o)=([x]s, [y]3, M5),

as required.Notice that we have

T-1 ([1]s, [1]3, [1]5)=[1]120, which is always the case with this procedure.

We now move on to consider the subject of equations over Z/n.Consider the following example.

Example.Let a, b ∈ Z with n>0.Then ax=b

is a linear modular equation or linear congruence over Z.We are interested in finding all solutions of Equation in Z, not just one solution.

If u ∈ Z has the property that au=b then u is a solution; but then the integers of form u+kn, k ∈ Z are also solutions.Notice that there are an infinite number of these.But each such solution gives the same congruence class [u+kn]n=[u]n.We can equally well consider

[a]n X=[b]n

as a linear equation over Z/n.This time we look for all solutions of Equation in Z/n and as Z/n is itself finite, there are only a finite number of these.As we remarked above, any Integer solution u gives rise to solution [u]n ; in fact many solutions give the same solution Conversely, a solution [v]n of generates the set

[v]n={ v+kn : k ∈ Z }

of solutions so there is in fact an equivalence of these two problems.

Now let try to find all solutions in Z/n.There are two cases:

the element [a]n ∈ Z/n is a unit;

the element [a]n ∈ Z/n is a zero divisor.

In case (1), let [c]n=[a]-1 be the inverse of [a]n.Then we can multiply [c]n to obtain X=[bc]n

Solution namely [bc]n! So we have completely found that X=[bc]n is the unique solution in Z/n.

namely the integers of form bc+kn, k ∈ Z.But any given solution u must satisfy [u]n=[bc]n in Z/n, hence u=bc and so u is of this form.So the solutions are precisely the integers n this form.

So exactly one solution in Z/n,

X=[a]-1[b]n

and has all integers of the form cb+kn as its solutions.

In case there can be solutions or none at all.For example, the equation

nx=1, n

can only have a solution in Z if n=1.There is also the possibility of multiple solutions in Z/n, as is shown by the example

2x=4 12

By inspection, this is observen to this congruence can also be solved by reducing it to

x=2, 6

Since if 2 (x — 2)=0 then x — 2=0, which is an example.

So if [a]n is not a unit, uniqueness is also lost as well as the guarantee of any solutions.We can more generally consider a system of linear equations

a1x=b1, a2x=b2, ..., ak x=bk,

ni n2 nfc

where we are now trying to find all integers x ∈ Z which simultaneously satisfy these congruences.The main result on this situation is the following.

Theorem (The Chinese Remainder Theorem).Let n1, n2, ..., n^ be a sequence of coprime integers, a1, a2, ..., ak a sequence of integers satisfying gcd(a, n)=1 and b1, b2, ..., bk be sequence of integers.Then the system of simultaneous linear congruences equations

a1x=b1, a2x=b2, ..., ak x=bk,

ni n2 nfc

has an infinite number of solutions x ∈ Z which form a unique congruence class

[x]niU2 •••Uk ∈ Z/n1n2 … nk

Proof.The proof uses the isomorphism

Z/ab=Z/a x Z/b

for gcd (a, b)=1 as together with an induction on k.

Example.Consider the system

3x=5, 2x=6, 7x=1.

2 3 5

Since 8=3, this system is equivalent to

5

x=1, x=0, x=3.

235

Solving the first two equations in Z/6, we obtain the unique solution x=3.Solving the simultaneous pair of congruences

x=3, x=3,

65

we obtain the unique solution x=3 in Z/30.

is often used to solve polynomial equations modulo n, by first splitting n into a product of prime powers, say n=pl1 p22 • • • pdd, and then solving modulo prkk for each k.

Theorem.Let n=pl1 p22 • • • pr (f, where the pk's are distinct primes with each rk ^ 1.Let f (X)∈ Z[X] be a polynomial with integer coefficients.Then the equation

f (x)=0

has a solution if and only if the equations

f (xi)=0, f (x2)=0, …, f (xr)i=.0,

Pl1 p22 pdd

all have solutions.Moreover, each sequence of solutions in Z/prjf of the latter gives rise to a unique solution x ∈ Z/n of f(x)=0 satisfying

x=xkVk.

VT2 Pk

Example.Solve x2 -1=0.

24

We have 24=8 • 3, so we will try to solve the pair of congruences equations

x2 — 1=0, x2 — 1=0,

1 8 2 3

with x1 ∈Z/8, x2 ∈ Z/3.Now clearly the solutions of the first equation are x1=1, 3, 5, 7; for

8

the second we get x2=1, 2.

Proposition.Let K be afield, and f (X)$\in$ K [X] be a polynomial with coefficients in K.Then for a $\in$ K,

f (a)=0 ^ f (X)=(X - a)g(X) for some g(X)$\in$ K[X].

Proof.This is a standard result in basic ring theory.

Corollary Let K be a field and let f (X) $\in$ K[X] with deg f=d>0.Then f (X) has at most d distinct roots in K.

As a particular case, consider the field Z/p, where p is a prime, and the polynomials

Xp-X, Xp-1 - 1 $\in$ Z/p[X].

Theorem (Fermat's Little Theorem).For any a $\in$ Z/p, either a=0 or (a)p-1=1 (so in the latter case a is a (p - 1)st root of 1).Hence,

Xp-X=X(X - 1) (X - 2) … (X - p - 1).

Corollary (Wilson's Theorem).For any prime p we have

(p- 1)!= -1 (mod p).

We also have the more subtle

Theorem (Gauss's Primitive Root Theorem).For any prime p, the group (Z/p)2 is cyclic of order p - 1.Hence there is an element a $\in$ Z/p of order p - 1.

The proof of this uses for example the structure theorem for finitely generated abelian groups.A generator of (Z/p)x is known a primitive root modulo p and there are exactly<p(p -1) of these in (Z/p)x.

Example : Take p = 7.Then ϕ(6) = ϕ(2)ϕ(3) = 2, so there are two primitive roots modulo 7.We have

$2^3 \underset{7}{\equiv} 1, \quad 3^2 \underset{7}{\equiv} 2, \quad 3^6 \underset{7}{\equiv} 1,$

hence 3 is one primitive root, the other must be $3^{\overline{6}} \equiv 5$

One advantage of working with a field K is that all of basic linear algebra works just as well over K.For instance, we can solve systems of

Notes

simultaneous linear equations in the usual way by Gaussian elimination.

Example : Take p = 11 and solve the system of simultaneous equations.

$$3x + 2y - 3z \equiv_{11} 1, \quad 2x + z \equiv_{11} 0,$$

i.e., find all solutions with $x, y, z \in Z/11$.
Here we can multiply the first equation by $3^{-1} = 4$, obtaining

$x + 8y - 1z \equiv_{11} 4, \; 2x + z \equiv_{11} 0,$

and then subtract twice this from the second to obtain
$x + 8y - 1z \equiv_{11} 4, \; 6y + 3z \equiv_{11} 3,$
and we know that the rank of this system is 2.The general solution is
$x \equiv_{11} 5t, \quad y \equiv_{11} 5t + 6, \quad z \equiv_{11} t$, for $t \in Z$.

Now consider a polynomial f (X) ∈ Z[X], say

f (X)= ∈ afc X k.

Suppose we want to solve the equation

f (x)=0

for some r ^ 1 and let's assume that we already have a solution x1 ∈ Z which works modulo p, i.e ., we have

f (xi) 0.

Can we find an integer x2 such that

f (x2)=0

and x2=x1? More generally we would like to find an integer xr such that

f (xr)=0

and xr=x1 ? Such an xr is known a lift of x1 modulo pr.

Example Take p=5 and f (X)=X2+1.Then there are two distinct roots modulo 5 namely 2, 3.Let's try to find a root modulo 25 and agreeing with 2 modulo 5.Try 2+5t where t=0, 1, ..., 4.Then we need

(2+5t)2+1=0,

or equivalently

20t+5=0, (25 under = symbol)

which has the solution t=1.(5 under equal to symbol)

Similarly, we have t=3 as a lift of 3.

Example Obtain lifts of 2, 3 modulo 625.

The next result is the simplest version of what is usually referred to as Hensel's Theorem.In various guises this is an important result whose proof is inspired by the proof of Newton's Method from Numerical Analysis.Theorem (Hensel's Theorem: first version).Let f (X)=Y^t=oaXk ∈ Z[X] and

suppose that x ∈ Z is a root of f modulo ps (with s ^ 1) and that f '(x) is a unit modulo p.

Then there is a unique root x' ∈ Z/ps+1 of f modulo ps+1 satisfying x'=x; moreover, x' is ps

given by the formula

x'=x —uf(x),

pS+1

where u ∈ Z satisfies uf' (x)=1, i. ∈ ., u is an inverse for f'(x) modulo p.

Proof.We have

f (x)=0, f '(x)=0,

ps, p

so there is such a u ∈ Z.Now consider the polynomial f (x+Tps) ∈ Z[T].Then

f (x+Tps)=f(x)+f'(x)Tps+••• (mod (Tps)2) by the usual version of Taylor's expansion for a polynomial over Z.Hence, for any t ∈ Z,

f (x+tps)=f (x)+f'(x)tps+(mod p2s).

An easy calculation now shows that

Notes

f (x+tps)=0 t= — uf(x)/ps.

ps+1 p

Example.Let p be an odd prime and let f (X)=Xp-1 — 1.Then Gauss's Primitive Root Theorem we have exactly p — 1 distinct (p — 1)st roots of 1 modulo p; let a=a $\in$ Z/p be any one of these.Then f' (X)= — Xp-2 and so f'(a)=0 and we can apply

Hence there is a unique lift of a modulo p2, say a2, agreeing with a1=a modulo p.So the reduction function

Pi: (Z/p2)X —>(Z/p)x; pi (b)=b

must be a group homomorphism which is onto.So for each such a1=a, there is a unique element a2 $\in$ Z/p2 satisfying ap-1=1 and therefore the group (Z/p2)x contains a unique cyclic subgroup of order p — 1 which p1 maps isomorphically to (Z/p)X.As we earlier showed that |Z/p21 has order (p — 1)p, this means that there is an isomorphism of groups

(Z/p2)X=(Z/p)X x Z/p,

by standard results on abelian groups.

We can repeat this process to construct a unique sequence of integers a1, a2,...satisfying ak=ak+1 and ak-1=1.We can also deduce that the reduction homomorphisms

pk pk

Pk: (Z/pk+1)X — (Z/pk)X

are all onto and there are isomorphisms

(Z/pk+X(Z/p)X x Z/pk.

The case p=2 is similar only this time we only have a single root of X2-1 — 1 modulo 2 and obtain the isomorphisms

(Z/2)X =0, (Z/4)X Z/2, (Z/2s)X=Z/2 x Z/2s-2 if s ^ 2.

It is also possible to do examples involving multivariable systems of simultaneous equations using a more general version of Hensel's Theorem.

Theorem (Hensel's Theorem: many variables and functions).Let

fj (Xi, X2, ..., Xn) G Z[Xi, X2, ..., Xn]

for 1 j m be a collection of polynomials and set f=(fj).Let a=(a1, ..., an) G Zn be a solution of f modulo pk.Suppose that the m x n derivative matrix

Df (a)=(f (a)

has full rank when considered as a matrix defined over Z/p.Then there is a solution a'= (a1, ..., an) G Zn of f modulo pk+1 satisfying a'=a.

Example.For each of the values k=1, 2, 3, solve the simultaneous system

f (X, Y, Z)=3X2+Y=1,

g (X, Y, Z)=XY+YZ=0.

Finally we state a version of Hensel's Theorem that applies under slightly more general conditions than the above and will be of importance later.

Check your Progress-3

Discuss Congruences and modular equations

____

____

____

1.5 LET US SUM UP

In this unit we have discussed the definition and example Congruences and modular equations, Nonarchimedean Fields, Congruences and modular equations

1.6 KEYWORDS

Congruences and modular equations…… A metric space (X, d) is known ultrametric if the strict triangle inequalityd (x, z)<max (d (x, y), d (y, z)) for any x, y, z $\in$ Xis satisfied

Nonarchimedean Fields …..A nonarchimedean absolute value on K is a function||: K — ► R

Congruences and modular equations…..If x, y $\in$ Z, then x=y if and only if n |(x — y).This is often also writtenx=y (mod n) or x=y (n)

1.7 QUESTIONS FOR REVIEW

Explain Congruences and modular equations

ExplainNonarchimedean Fields

ExplainCongruences and modular equations

1.8 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

1.9 ANSWERS TO CHECK YOUR PROGRESS

Congruences and modular equations

(answer for Check your Progress-1 Q)

Nonarchimedean Fields (answer for Check your Progress-2 Q)

Congruences and modular equations

(answer for Check your Progress-3 Q)

UNIT-2:CONVERGENT SERIES

STRUCTURE

2.0 OBJECTIVES

After studying this unit, you should be able to:

- Understand about Convergent series
- Understand about Differentiability
- Understand about Power series
- Understand about Locally analytic functions

2.1 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.

Convergent series, Differentiability, Power series, Locally analytic functions

2.2 CONVERGENT SERIES

From now on throughout the book (K, |.|) is a fixed nonarchimedean field For the convenience of the reader we collect in this section the most basic facts about convergent series in Banach spaces

Let (V, ||.||) be a K-Banach space.

Theorem.Let (vn) ne N be a sequence in V; we then have:

The series vn is convergent if and only if limn vn=0;

if the limit v := limn vn exists in V and is nonzero then ||vn||=||v|| for all but finitely many n G N;

let a : N ^ N be any bijection and suppose that the series v= =1 vn is convergent in V; then the series r =1 vCT(n) is convergent as well with the same limit v.

Proof.If v=0 then ||v||=0 and hence ||vn — v||<||v||for any sufficiently big n $\in$ N.then implies that

||vn||=|(vn — v)+v||=max(||vn — v||, ||v|)=||v||.

We fix an $\in$ >0 and choose an m $\in$ N such that

||v — ^ vn||< $\in$ for any s>m.

Then also

IK!=||(v — ^ vn) — (v — ^ vn |<max(||v — ^ v.nH, ||v — ^ vn||)<e n=1

for any s>m.Setting $\in$:= max{ a-1(n) : n<m }>m we have

{ a-1(1), ..., a-1(m)}C{1, ..., $\in$ } and hence, for any s> $\in$,

{ a(1), ..., a(s) }={ 1, ..., m}U{m, ..., ns_m} with appropriate natural numbers n>m.We conclude that

s/m \ llv — t va(n) II=II I v — t vn j — vni —...— vns_m ^n=1\ n=1 /

<max |v — t vn||, ||vn11 |, ..., llvns_m||^<e

for any s> ∈ .

The following identities between convergent series are obvious: - E^=1 avn=a • vn for any a ∈ K.

(∈ ∈ =1 Vn) + ∈ :=1 Wn)= ∈ ∈ =1^+Wn).

Theorem.LetY^ ∈ =1 an andY^ ∈ =1 vn be convergent series in K and V, respectively; then the series ∈ wn with wn := ∈ ∈ +m=n a ∈ vm is conver- gent, and

∈ ^ Wn =(^ a^ (^ Vn n=1

Proof.Let A :=supn|an|and C :=supn||vn||.The other cases being trivial we will assume that A, C>0.For any given ∈ >0 we find an N ∈ N such that

ee |an|<— and ||vn||<— for any n>N.

Then

||wn||<max |a ∈ |.||vm||<max (C max |a ∈ |A max ||vm||)<e

∈ +m=n ∈ >N m>N

for any n>2N.The series wn therefore is convergent.To establish the asserted identity we note that its left hand side is the limit of the sequence s

Ws := ^ wn=^ (l ∈ Vm n= 1 ∈ +m<s

whereas its right hand side is the limit of the sequence s s

WS := f an) (^2vn)=a ∈ Vm.

It therefore suffices to show that the differences Ws — W's converge to zero.But we have

||Ws — W'SH=II y a ∈ VmH<max |a ∈ |.||vm|| ∈ , m<s

∈ , m<s ∈ +m>s ∈ +m>s

<max (C max |a ∈ |, A max ||vm

∈ >2 2

Notes

Analogous assertions hold true for series ∈ ∈ =1 vni, ..., nr indexed by multi-indices in N...N.

Check your Progress-1

DiscussConvergent series

____
____
____

2.3 DIFFERENTIABILITY

Let V and W be two normed K-vector spaces, let U C V be an open subset, and let f : U —>W be some map.

Definition.The map f is known differentiable in the point vo ∈ U if there exists a continuous linear map

Dv 0 f : V W

such that for any ∈ >0 there is an open neighbourhood U ∈ =U ∈ (vo) C U of vo with

llf (v)- f (vo)-Dvof(v -vo)y< ∈ ||v -vo||for any v ∈ U ∈ .

We can of course assume in the above definition that the open neighbourhood U ∈ is of the form U ∈ =B^ ∈)(v0) for some sufficiently small radius 5 (∈)>0.We claim that the linear map Dv0f is uniquely determined.Fix an e'>0, and choose a basis{vj }jeJ of the vector space V.By scaling we can assume that ||vj||<5(e').We put vj :=vj+v0.Then

vj ∈ B& (∈ ,) (vo)=.

More generally, for any 0< ∈ <e' we pick a t ∈ ∈ Kx such that

|t ∈ |5 (e')<5 (∈).

Then

t ∈ (vj-vo)+vo ∈ BS(∈) (vo)=U ∈ for any j ∈ J.

It follows that

Ilf(t ∈ (vj-vo)+vo)- f (vo)-Dvof(t ∈ (vj-vo)) |< ∈ |t ∈ (vj-vo)| and f (t ∈ (vj-vo)+vo)- f (vo) hence that Dvof(vj-vo) |< ∈ |vj-vo||.

t ∈ By letting ∈ tend to zero we obtain

n tt t\ n ^ ^ i- f(t(vj-vo)+ vo)- f(vo)

Dvo f (vj)=Dvo f (vj-vo)=lim t GK x, t^o

for any j ∈ J.But as a linear map Dvo f is uniquely determined by its value on the basis vectors vj'.

The continuous linear map Dvof : V —>W is known(if it exists) the derivative of f in the point vo ∈ U.In case V=K we also write f' (ao) := Dao f (1).

Remark If f is differentiable in v0 then it is continuous in v0.

(Chain rule) Let V, Wi, and W2 be normed K-vector spaces, U C V and Ui C Wi be open subsets, and f : U —>Ui and g : Ui —>W2 be maps; suppose that f is differentiable in some v0 ∈ U and g is differentiable in f (v0); then g o f is differentiable in v0 and

Dvo (g o f) Df (v0)g ◦ Dvo f.

A continuous linear map u : V —>W is differentiable in any v0 ∈ V and Dv0u=u; in particular, in the situation of ii.we have

Dvo (u o f)=u o Dvo f.

(Product rule) Let V, W1, ..., Wm, and W be normed K-vector spaces, let U C V be an open subset with maps fi : U —>Wi, and let u : W1 x...x Wm —>W be a continuous multilinear map; sup- pose that fi, ..., fm all are differentiable in some point v0 ∈ U; then u(fi, ..., fm) : U —>W is differentiable in v0 and

Dvo (u(fi, ..., fm))=^ u(fi(vo), ..., Dvo fi, ..., fm(vo)).

Proof.These are standard arguments Let ∈ >0 and choose a 5>0 such that ∈ 2, ^llDvof\ \, 5\\Df(vo)gll<e

(here\||refers to the operator norm of course).By assumption on g we have llg (w)- g(f (vo))- Df(vo)g(w - f (wo))||<5|w - f Mil

for any w ∈ Us (f (vo)).By the differentiability and hence continuity of f in v0 there exists an open neighbourhoodU (v0) C U of v0 such that f (U(v0)) C Us(f(vo)) and

||f (v)- f M -Dvo f (v - v0) |<5|v - M for any v ∈ U(v0).In particular

llf (v)- f (v0)\=llDvo f (v - v0)+f (v)- f (v0)-Dvo f (v - v0)\

<max (lDvo f l ||v - v0||, 5||v - v0\)

for any v ∈ U (v0).We now compute

llg (f(v))- g(f(vo))- Df(v0)g o DV0 f(v -vo)y =\\g(/(v))- g(/(vo))- Df (vo)g(/(v)- f (vo))

+ Df (vo)g(f (v)- f (v0)-Dvof(v - v0))\|

max (S\\f (v)- f (v0)\ |, ||Df (vo)g\ llf(v)- f (v0)-Dvof(v - v0)\)(2)

max (5||f (v)- f (v0)\ |, ||Df (vo)g\ ^llv- v0 II)(3)

max (∈ ||Dvof \, ^2, 5\Df(vo)#ll) ' llv- v0 \ ∈ ||v - v0||

for any v ∈ U (v0).

Suppose that the vector space V=V...Vm is the direct sum of finitely many vector spaces Vp..., Vm and that the norm on V is the maximum of its restrictions to the Vp Write a vector v0 ∈ U as v0=v0, 1+...+v0, m with v0, j ∈ Vi.For each 1<i<m there is an open neighbourhood Uj C Vi of v0, i such that

Ui+...+UTO C U.

Therefore the maps

fi :Uj-^ W

vi -► f (v0, 1+...+vj+...+v0, m)

are well defined.If it exists the continuous linear map

Dvo)f :=Dvo, ^fi : Vj-^ W

is known the i-th partial derivative of f in v0.We recall that differentiability of f in v0 implies the existence of all partial derivatives together with the identity m

Dvo f = ∊ Dvo)f.i=1 f

Let us go back to our initial situation V*U —► W.

Definition.The map f is known strictly differentiable in v0 ∊ U if there exists a continuous linear map Dv0 f : V —>W such that for any ∊ >0 there is an open neighborhood U ∊ C U of v0 with

Wf (vi)- f(V2)- Dv0f(vi - V2)y<∊ ||vi - V21|for any vi, v2 ∊ U ∊ .

Exercise.Suppose that f is strictly differentiable in every point of U.Then the map

U —>L(V, W) v i —>Dv f is continuous.

Our goal for the rest of this section is to discuss the local invertibility properties of strictly differentiable maps.

Theorem.Let Bs (v0) be a closed ball in a K-Banach space V and let f : Bs (v0) —>V be a map for which there exists a 0< ∊ <1 such that

Wf (vi)- f (v2)-(vi - v2)W<eWvi- v2 W for any vi, v2 ∊ Bs (vo); then f induces a homeomorphism

Bs (vo)-=^ Bs (f (vo)).

Proof.We have

Wf (vi)- f (v2)W=Wvi- v2 W for any vi, v2 ∊ Bs (vo).

In particular, f is a homeomorphism onto its image which satisfies f (Bs(v0)) C Bs(f(v0)).It remains to show that this latter inclusion in fact is an equality.Let w $\in$ Bs (f (v0)) be an arbitrary but fixed vector.For any v' $\in$ Bs (v0) we put

v" := w+v' - f (v').

We compute

||v" - v0W<max(Wv" -v'W, ||v' - v0W)

max (Ww- f(v')W, 5)

max (Ww- f(vo)W, Wf(vo)- f(v')W, ^)

max (5, Wf(vo)- f(v')W)(5)

max (5, ||v0 -v'W)

which means that v" G Bs (v0).Hence we can define inductively a sequence (vn)n>0 in Bs(vo) by

Vn+1 := w+Vn- f (Vn).

Using weobserve that

||Vn+1 -VnII=||Vn- f (Vn)-(Vn-1 - f (Vn-1))|

= |f (Vn-1)- f (Vn)-(Vn-1 -Vn)||

<G11 Vn -Vn-111

and therefore

I Vn+1 -Vn |< $\in$ n |V1 - Vo |< $\in$ n 5

for any n>1.It follows that (Vn)n is a Cauchy sequence and, since V is complete, is convergent.Because Bs (v0) is closed in V the limit v := limn^^ vn lies in Bs(v0).By passing to the limit in the defining equation and using the continuity of f we finally obtain that f (v)=w.

Proposition (Local invertibility) Let V and W be K-Banach spaces, U C V be an open subset, and f : U —>W be a map which is strictly differentiable in the point v0 G U; suppose that the derivative Dv0 f : V -

4 W is a topological isomorphism; then there are open neighbourhoods U0 C U of V0 and U1 C W of f(V0) such that:

f : U0 -- U1 is a homeomorphism;

the inverse map g : U1 —>U0 is strictly differentiable in f (v0), and

Df (vo)g=(Dvof)-1.

Proof.We consider the map

f1 := (Dvof)-1 o f : U -^ V.

As a consequence of the chain rule it is strictly differentiable in v0 and

Dvof1=(Dvof)-1 o Dvof=idy.

Hence, fixing some 0<G0<1 we find a neighbourhoodBso(v0) C U of v0 such that the condition is satisfied.The Theorem then says that

f1 : U0 :=Bso(V0)-^ Bso(f1(v0))

is a homeomorphism.Since Dv0 f is a homeomorphism by assumption U\ := Dv0 f (B<s0 (fi(vo))) is an open neighborhood of f (v0) in W and f : U0 -^ Ui is a homeomorphism.

let e>0.We have ||(DV0f)-1||>0 since (Dv0f)-1 is bijective.Hence we find a 5>0 such that

*ll (Dvof)-1||<1 and 5|(Dvof)-1||2< ∊ .

By the strict differentiability of f in v0 we have

llf (V1)- f (V2)-Dvof(V1 - V2) |<5|v1 - V2I for any V1, V2 G Us.

Applying (Dv0 f)-1 gives

(Dvof)-1(f (v1)- f (v2))-(v1 - V2) 1<5|(Dv0f)-1y ' ||V1 - V2 1.By our choice of 5 and deduce

(Dv0f)-1(f(v1)- f(v2)) 1=|v1 - v2 1.

Combining the last two formulas we obtain

|v1 -v2 -(Dv0f)-1(f (v1)- f (v2)) 1

5|(Dv0f)-1|- |(Dv0f)-1(f(V1)- f(V2))|

5|(Dv0f)-1|2 -|f(V1)- f(V2)|

e|f (v1)- f (v2) 1

for any v1, v2 G Us.It follows that

l|g (W1)- g(W2)-(Dv0f)-1(W1 - W2) |<∈ ||w1 - W2|

for any w1, w2 G f (U0 n Us).Since f (U0 n Us) is an open neighbourhood of f (v0) in U1 this establishes ii.

which says that any continuous linear bijection between K-Banach spaces necessarily is a topological isomorphism.We also point out the trivial fact that any linear map between two finite dimensional K-Banach spaces is continuous.

Corollary Let U C Kn be an open subset and f : U —— ► Km be a map which is strictly differentiable in v0 ∈ U; suppose that Dv0 f is injective; then there are open neighbourhoods U0 C U of v0 and Ui C Km of f(v0) as well as a ball Be(0) C Km-n around zero and linearly independent vectors w \, ..., wm-n ∈ Km such that the map

Uo x Be (0) Ui (v, (al, ..., am —— n)) 1 ► f (v)+aiwi+...+am-nwm-r.is a homeomorphism.

Proof.We choose the vectors wj in such a way that

Km=im (Dv0f) Kwi...Kwm-n.

Then the linear map

u :Kn x Km-n -^ Km

(v, (al, ..., am-n)) 1 ^ (Dv0f) (v)+aiwi+...+am nwm —— r is a topological isomorphism.One checks that the map

f : U x Km-n —— ► Km

(v, (al, ..., am-n)) 1 ^ f (v)+aiwi+...+am-nwm-r is strictly differentiable in (v0, 0) with D(v0, 0)f=u.

Corollary Let U C Kn be an open subset and f : U — ► Km be a map which is strictly differentiable in v0 ∈ U; suppose that Dv0 f is surjective; then there are open neighbourhoods U0 C U of v0 and Ui C Km of f(v0) as well as a ball Be(0) C Kn-m around zero and a linear map p : Kn — ^ Kn-m such that the map

U0 Ui x Be (0) v i — ^ (f(v), p(v)- p(v0))

is a homeomorphism; in particular, the restricted map f : U0 — ► Km is open.

Proof.We choose a decomposition

Kn=ker (Dv0 f) C

and let p :Kn — ► ker(Dv0 f)=Kn-m be the corresponding projection map.Then

u :Kn — ► Km x Kn-m

v ' ►((Dv0f) (v), P(v))

is a topological isomorphism.One checks that

f : U — ► Km x Kn-m v 1 — ► (f (v), p(v)- p(v0))

is strictly differentiable in v0 with Dv0f=u.

We finish this section with a trivial observation.

A map f : X —>A from some topological space X into some set A is known locally constant if f-1(a) is open (and closed) in X for any a ∈ A.

Theorem.Implies that in our standard situation of two normed K- vector spaces V and W and an open subset U C W there are plenty of locally constant maps f : U —>W.They all are strictly differentiable in any v0 ∈ U with Dv0 f=0.

Check your Progress-2

Discuss Differentiability

2.4 POWER SERIES

Let V be a K-Banach space.By a power series f (X) in r variables

X= (X1, ..., Xr) with coefficients in V we mean a formal series

f (X)=^ Xava with va ∈ V.

Here and in the following we use the usual conventions for multi-indices

Xa := Xf1...Xaand |a|:= ai+...+ay

if a=(a1, ..., ar) ∈ NO (with N0 := N U{0 }).

For any ∈ >0 the power series f (X)=^a Xava is known ∈ - convergent

If limeH||va||=0.

Remark.If f (X) is ∈ - convergent then it also is 5-convergent for any 0<5<e.

The K-vector space

F ∈ (Kr; V) := all ∈ - convergent power series f (X)=^ Xava

a ∈ w0 is normed by ∈ :=maxe|a|||va

By a straightforward generalization of the argument for c0 (N) it is shown that F ∈ (Kr; V) is a Banach space.By the way, in case ∈ = |c|for some c ∈ Kx the map

Co (N0)-=UF|c|(Kr; K)

(»a)a — ∈ CfJX^ a

is an isometric linear isomorphism.

Remark.The vector space F ∈ (Kr; V) together with its topology only de- pends on the topology of V (and not on its specific norm).

Proof.Let ||||' be a second norm on V which induces the same topology as ||||.Applying the identity map idV we obtain two constants ci, c2>0 such that

ci||||<||||'<c2||||.

Then obviously

lim ∈ |a|||va||'=0 if and only if lim ∈ |a|||va||=0.

This means that using ||||' instead of ||leads to the same vector space F ∈ (Kr; V) but which carries the two norms |||| ∈ and |f || ∈ :=maxa ∈ |a||va||'.The above inequalities immediately imply the analogous inequalities

ci|11 ∈ <||| ∈ <C2 |11 ∈ .

By the identity map on F ∈ (Kr; V) this means that |||| ∈ and |||| ∈ induce the same topology.

Consider a convergent series

f = ∈ fi

in the Banach space F ∈ (Kr; V).Suppose that

f (X) = ∈ X ava and fi(X) — ∈ Xc

We have

llf - ∈ fi^ ∈ =II ∈ X "(Va- ∈ Vi, a)lle=max ∈ H\\Va- E

e —||/ y X (Va -/J vi, a)|| ∈ — max e' ' ||va -/J vi, a \ i=0 a i=0 i=0

This shows that

Va — ∈ Vi, a for any a ∈ NO

which means that limits in F ∈ (Kr; V) can be computed coefficient wise.

Let B ∈ (0) denote the closed ball around zero in Kr of radius ∈ .We recall that Kr always is equipped with the norm ||(ai, ..., ar)||— maxi<i<r |ai|.By Theorem3.1.i.we have the K-linear map

F ∈ (Kr; V) —>K-vector space of maps B ∈ (0) —>V f (X) — ∈ X"Va-^ f(x) : — ∈ X"Va.aa

Remark.For any x ∈ B ∈ (0) the linear evaluation map

Fe (Kr; V) V

f -^ f(x)

is continuous of operator norm<1.

Proof.We have

ll/(x)||— I ExaVa\ \<maxe|a||a

Proposition Let u : Vi x V2 — ► V be a continuous bilinear map between K-Banach spaces; then

U : F(Kr; Vi) x F(Kr; V2) F(Kr; V)

(∈ Xava, ∈ Xawa) 1 — ► ∈ Xa(∈ u(v^, w7))

a a a ft+y=a

is a continuous bilinear map satisfying

U (f, g)~(x)=u(f (x), g (x)) for any x ∈ B(0) and any f ∈ F ∈ (Kr; Vi) and g ∈ F ∈ (Kr; V2).

Proof.By a similar argument as the bilinear map u is continuous if and only if there is a constant c>0 such that

||u(vi, V2)||<c||vi|| IHI for any vi ∈ Vi, V2 ∈ V2.We therefore have

e|a||| ∈ u(v^, w7) |<c max (∈ |ft|||vft|| ∈ |y|||v71

ft+y=a ft+y=a

This shows (compare the proof of Theorem 3.2)that with f and g also U(f, g) is ∈ - convergent and that

|U (f, g)| ∈ <c|f|| ∈ NgN ∈ .

Hence U is well defined, bilinear, and continuous.The asserted identity between evaluations is an immediate generalization

Proposition F ∈ (Kr; K) is a commutative K-algebra with respect to the multiplication

(∈ baX a) (∈ CaXa) := ∈ (∈ b" CY)X a ^

a a aft+y

in addition we have

(fg)~(x)=f(x)g(x) for any x ∈ B(0)

as well as

llfg| ∈ =II f | ∈ |g| ∈

for any f, g ∈ F ∈ (Kr; K).

Proof.Apart from the norm identity this is a special case of the multiplication in K as the bilinear map.It remains to show that

W/aWe>11/|| ∈ ||0|| ∈ .

Let>denote the lexicographic order on N0, and let p and v be lexicograph- ically minimal multi-indices such that

= W/We and \cv\e[V 1=Walls, respectively.

Put A := p+v and consider any equation of the form A=0+7.

Claim: 0<p or 7<v.

Otherwise we would have 0>p and 7>v.This means that there are 1<i, j<r such that

01 — pl, ..., bi-1 — pi — 1, and 0i>[ai

as well as

Yi=vl, ..., Yj-i=vj-l, and Yj>vj.

Notes

By symmetry we can assume that i<j.We then obtain the contradiction

Ai — pi+vi<0i+Yi — Ai.

This establishes the claim.

We of course have

Ibp\e^<W/We and \c7MyI<||g|| ∈ .

But in case (0, y)=(p, v) the fact that 0<p or y<v together with the minimality property of p and v implies that

\bpM71<W/We or \CYMyI<Walls.

It follows that

\b7CY\^|A|=\ b7 \CY^<W/lie Wg We whenever 0+y=A but (0, y)=(p, v).We conclude that

e>\ ^ b7C7 \ ∈ |A|=\b^Cv \ ∈ |A|=W/|| ∈ ||g|| ∈ .7+7=A

Proposition.Let g ∈ Fs (Kr; Kn) such that ||g||s<e; then Fe(Kn; V)-^Fs(Kr; V)

f (Y) = ∈ vg -^ f o g(X) := ∈ g(X)gvg

is a continuous linear map of operator norm<1 which satisfies (f ∘ g)~(x)=f(g(x)) for any x ∈ Bs(0) C Kr.

Proof.Using the obvious identification

Fs (Kr; Kn)=n Fs (Kr; K)

g=(gi, ..., gn)

we have maxi Hg^ls= ||g||s< ∈ .The therefore implies that g (X)g ∈ Fs (Kr; K) for each 0 and nn

iig (X)glis =1 nggilis=n iigi|gi<elg|.

It follows that g (X)gvg ∈ Fs(Kr; V) for each 0 with

l|g (X)hvglis=l|g(X)glisIIvg1<elg||vg1.

Since the right hand side goes to zero by the ∈ - convergence of f the series f o g (X)=^g g(X)gvg is convergent in the Banach space Fs(Kr; V).Moreover, we have

||f o gHs<max ||g(X)gvg||s<maxelg|||vgH=||f || ∈ P P

To observe the asserted identity between evaluations we first note that by the map g indeed maps the ball Bs (0) C Kr into the ball Be(0) C Kn.(fogp(x) = ∈ (gg)~(x)vg=Eg(x) ∈ = /(g(x)).

As a consequence of the discussion the power series f o g can be computed by formally inserting g into f.

although, for any g ∈ F<s(Kr; Kn), we have inequality

suP||g(x)||<||g||a xeBs (o)

it is, in general, not an equality.This means that we can have g (B(0)) C B ∈ (0) even if ∈ <||g.Then, for any f ∈ F ∈ (Kn; V), the composite of maps f o g exists but the composite of power series f o g ∈ F<s(Kr; V)can not.

Exercise.An example of such a situation is <X>

g (X) :=Xp- X ∈ Fi(Qp; Qp) and f (Y) := ∈ Yn ∈ Fp(Qp; Qp).

Corollary (Point of expansion) Let f ∈ F ∈ (Kr; V) and y ∈ B ∈ (0); then there exists an fy ∈ F ∈ (Kr; V) such that ||fy| ∈ =|f | ∈ and

f (x)=fy(x - y) for any x ∈ B ∈ (0)=B^y).

Proof.Let e1, ..., er denote the standard basis of Kr.to the power series g(X) := X+y=Y)r=1 X^e^+y ∈ F ∈ (Kr; Kr) which satisfies ||g| ∈ < ∈ we obtain the existence of fy(X) := f (X+y) satisfying

II fy 11 ∈ <||f || ∈ and fy(x)=f (x+y) for x ∈ B ∈ (0).By symmetry we also have

llfll ∈ =ll (fy)-yIl ∈ <llfy^ ∈ .

It will be convenient in the following to use the short notation

Notes

i :=(0, ..., 1, ..., 0)

for the multi-index whose only nonzero entry is a 1 in the i-thplace.

Suppose that the power series f (X)=Y)a Xava is ∈ - convergent.Then also, for any 1<i<r, its i-th formal partial derivative

9f-(X) := ∈ Xa-i-atv0 dXi

is ∈ - convergent (since Waiva||<||va||).In case our field K has characteristic zero it follows inductively that

va=0^((A)ai ...(dfc)f ~(0) for any a.

Proposition.The map f is strictly differentiable in every point z ∈ Bs (0) and satisfies

D"f" (1)=(H) ~(z)-

Proof.Case 1: We assume that z=0, and introduce the continuous linear map

Kr —► V

(ai, ..., ar)i — ► ^2

i=i

Let 5>0 and choose a 0<5'< ∈ such that

5 By induction with respect to |a|one checks that

|xa -ya |<(5')|a|- i||x -

We now compute

llfr (x)- f(y)- D(x - y)|=

for any x, y ∈ B>(0).This proves that f is strictly differentiable in 0 with Do f=D and hence

D0i)f (1)=vi=(f)~<°>.

Case : Let z ∈ B ∈ (0) be an arbitrary point.We find a power series fz (X)=Y)a Xava(z) in F ∈ (Kr; V) such that

f (x)=fz(x — z) for any x ∈ B ∈ (0).

Using the chain rule together with the first case we observe that f is strictly differentiable in z with

DZf (1)= Dfz(1)= Vi(z).

Since fz (X) can be computed by formally inserting X+z into f (X) we have ∈ XaVa(z)= ∈ (X+z)aVa

and hence

vi (z)= ∈ za--a.iva=^f)(z).

By the map

f : B ∈ (0) — ^ V dxi

x —^ DX f (1)

is well defined and satisfies

df(df dxi \dX.

Corollary (Taylor expansion) If K has characteristic zero then we have

f (X)= ∈ x∀ori-tar(()a'...(if-)∀rf) (°).

Corollary.(Identity theorem for power series) If K has characteristic zero then for any nonzero f ∈ F ∈ (Kr; V) there is a point x ∈ B ∈ (0) suchthat f (x)=0.

In fact much stronger results.In particular, the assumption on the characteristic of K is superfluous.But this requires a different method of and subsequent comment).In any case the map

F ∈ (Kr; V) —>strictly differentiable maps B ∈ (0) —>V is injective and commutes with all the usual operations as considered above.We therefore will simplify notations in the following and write very often f for the power series as well as the corresponding map.

Proposition (Invertibility for power series) Let f (X) ∈ F ∈ (Kr; Kr) such that f(0)=0, and suppose that D0f is bijective; fix a 0<5<2

llfllII (D f)-1l2; then 5<||f || ∈ , and there is a uniquely determined g(Y) ∈ Fs(V°Kr) such that

g (0)=0, ||g|i<e, and f o g(Y)=Y ;

in particular, the diagram

Bs (0) g

B ∈ (0) f ^ B\\f y, (0)

is commutative.

Proof.Case 1: We assume that D0f=idKr.Let

f=(fi, ..., fr) and fi(X)=^di, aXa.

Since f (0)=0 we have aito=0.Moreover, the matrix of D0f in the standard basis of Kr is equal toBut we are in the special case that this matrix is the identity matrix.Hence a%g=0 for i=j and ai }i=1.We therefore observe that

fi (X)=Xi+^ ai, aXa.

|a |>2

It follows in particular that

11/II.>e

and hence

e2 5<II/li, il(A>/)-ili2 I/1.∀ ∈ ∀B/'

In case 1 of the proof we have computed that

11/(x)-/(y)-(x - y)II< -2^||x -yII for any x, y ∈ B&(0).

As 5<1 this is the condition.We therefore conclude that

/: Bs (0)- Bs (0) is a homeomorphism.Furthermore, for|a |>2 we have

Iai, j|5|a|<11/1|.(.)H<11/1|.(.)2=5(5 f)<5.

Hence it follows from that

In a next step we establish the existence of a formal power series

g = (gi, ..., gr) with

gi (Y) = ∈ ^ |y |>i

such that

/(g(Y))=Y.

First of all let us check that formally inserting any such g into/is a well-defined operation.We formally compute

/ i(g(Y))= ∈ ^agi(Y)ai...gr (Y)ar

|a |>I = ∈ ai, a (∈ bij>YS)ai (∈ br, « YS)°"

|a |>1 |g |>i |g |>i

E (Eai'abi, y(i) '...' bi, d (ai)b2, g(ai+i) '...' br, g (ai+-+ar))

IyI>i...

where in the last expression the multi-indices in the inner sum run over all a, 3(1), ..., /3(a\+...+ar)such that |a |, |3(1) |, ..., |3(a+...+ar) |>1 and

3 (1)+...+3 (ai)+3 (ai +1)+...+3 (ai+a2)+...+3 (ai+...+ar)= y.

Because of |3(v) |>1 this condition enforces |a |<|y|so that these inner sums in fact are finite.We now set

Y=fi (g(Y))

and compare coefficients.For y=i we obtain

1=^ ai, ∈ b ∈ , i=bi, i. ∈ =1

Notes

For y=i we have

0 — ^ ^ ai, ab 1, 7(1) •...— bi, Y+ai, aC (a, y)

...2<|a |<|7|

where C (a, y) is a (finite) sum of products of the form

bi, 7 (i) •...• br, p (ai+...+ar)with |3(v) |>1 and ^ 3(v)=y.

In particular,

^ |3(v)|=|Y|and |3(v) |>1.

Since the number of summands |3(v)|is equal to |a |>2 it follows that |3(v) |<|y|.We observe that on the right hand side of the equation

bi, Y=-^2 afi«C(a, y)

2<M<T

only coefficients b ∈ , g appear with |3 |<|y|.This means that the coefficients 3ia can be computed recursively from these equations.Hence g exists and is uniquely determined.In addition we check inductively that

|bi, Y|<()H-i

holds true.For |y|=1 we have ^i, 1=0 or 1 and the inequality is trivial.If |Y|>2 then the induction hypothesis implies

|C (a, y)I<max|6i, y(i)|•...• \br, p (ai+...+ar)l

max(|f \(l^(1)l-1)+...+(l^(Qa+...+ar)|- i)

...^ e2

Jt|-M

V e2) Hence we have

\bi, y\<max \ai, a\ \C(a, Y) |<max |C(a, Y)|

2<|« |<|y|2<|« |<|y| ∈ |a|

<max (^T ∈)l7l-H=max (^)|a|— 2 (f)17, -1

2<|a |<|7l ∈ |a|e2 ' 2<|a |<|7|V||f lie e2

Jt|— 1

(the last identity since ∈ <||f || ∈).We deduce that

|bi, 7|5|y|<(5fk)|y|— k.

Because of 5<1 this shows that g is 5-convergent with ||g|^<5.But bi, i=1 then implies that ||g||s=5.Altogether we have shown so far that:

f is 5-convergent with ||f ||s=5;

there is a uniquely determined 5-convergent g with

g (0)=0, ||g||s=5<e, and f o g(Y)=Y.

Using that f o g=id so that

Bs (0)^ Bs (0)

are homeomorphisms which are inverse to each other.But we also conclude that g o f (X) exists as a 5-convergent power series as well and satisfies (g o f)~=g o f=id.The identity theorem then implies that

g o f (X)= X.

Case 2: Let Dof be arbitrary bijective.If (aj)i, j is the matrix of (Do f) 1 in the standard basis of Kr then the operator norm is given by

||(Dof)-1||=max|aj|.

Viewed as a power series (D0f)-1 is e'-convergent for any e'>0 with ll(Dof)-1||, '=e' max|ai, j|=e'||(Dof)-1||.

In the following we put e' :=||(Dof)_iy.Then ||(D0f)-1|| ∈ '=e, and from obtain

fo := f o (Dof)-1 GF, (Kr; Kr) and ||fo||, <||f || ∈ .

Any 5 as in the assertion then satisfies

e2 _ e'2 ^ e'2

Notes

<, B (Dof)-1||2=||f||, <

Obviously fo (0)=0, and Dofo=idKr by the chain rule.So we can apply the first case to fo and obtain a uniquely determined go G F (Kr; Kr) such

that

go (0)=0, HgoHs=5, and fo o go(Y)=Y

as well as

e'2, e

5<||fo |, , <e' ||(Dof)-1 |<|fo" ∈ '<lf H ∈

by.We define

g := (Dof)-1 o go G F(Kr; Kr).

Then g (0)=0 and

f (g(Y))=f ((Dof)-1 o go(Y))=f o (Dof)-1(go(Y))=fo(go(Y))=Y.In addition, implies

||g|U<||(Dof)-1|5=5|(Dof)-1 |< ∈ .

The unicity of g easily follows from the unicity of go.

Proposition Let u : V — ► W be a continuous linear map between K-Banach spaces; then

F ∈ (Kr; V) —>F ∈ (Kr; W) f (X)= Xava — u o f (X) := Xau(va) is a continuous linear map of operator norm<||u||which satisfies u o f (x)=u(f (x)) for any x ∈ Be(0).

Check your Progress-3

Discuss Power Series

2.5 LOCALLY ANALYTIC FUNCTIONS

Definition.A function f : U —>V is known locally analytic if for any point x0 ∈ U there is a ball B ∈ (x0) C U around x0 and a power series F ∈ F ∈ (Kr; V) such that

f (x)=F (x — x0) for any x ∈ B ∈ (x0).

The set Can (U, V) := all locally analytic functions f : U —>V

is a K-vector space with respect to pointwise addition and scalar multi-plication.For fi, f2 ∈ Can(U, V) and xo ∈ U let Fi ∈ F ∈ i(Kr; V) such that fi(x)=Fi(x — x0) for any x ∈ B ∈ i(x0).Put ∈ := min(ei, e2).Then Fi+F2 ∈ Fe (Kr; V) and

(fi+f2) (x)=(Fi+F2) (x — xo) for any x ∈ B ∈ (xo).

The vector space Can (U, V) carries a natural topology which we will discuss later on in a more general context.

Example.We have F ∈ Can (B ∈ (0), V) for any F ∈ F ∈ (Kr; V).

Proposition.Suppose that f : U —>V is locally analytic; then f is strictly differentiable in every point x0 ∈ U and the function x — —>Dxf is locally analytic in Can(U, L(Kr, V)).

Proof.Let F ∈ Fe (Kr; V) such that

f (x)=F(x — x0) for any x ∈ B ∈ (x0).

From and the chain rule we deduce that f is strictly differentiable in every x ∈ Be (x0) and

Dxf((ai, ..., ar))= xo^(1)=ai(JX)~(x — xo).

Let

H (x>= xa, , „.

For any multi-index a we introduce the continuous linear map La : Kr — - V

(ay..., ar) 1 - a1v1, a+...+arvr, a.

Because of ||La||<maxi ||vi;Q, ||we have

Notes

G (X) := XaLa ∈ Fe(Kr; L(Kr, V))

A and Dxf=G (x — xo) for any x ∈ Be(xo).

Remark If K has characteristic zero then, for any function f : U —> V, the following conditions are equivalent:

f is locally constant;

f is locally analytic with Dxf=0 for any x ∈ U.

Proof.This is an immediate consequence of the Taylor formula.

We now give a list of more or less obvious properties of locally analytic functions.

For any open subset U' C U we have the linear restriction map

Can (U, V) — Can(U', V) f -- f |U'.

For any open and closed subset U' C U we have the linear map

Can (U', V) Can(U, V)

f -f(x) :=|0(X) T

otherwise known extension by zero.

If U=(JieI Ui is a covering by pairwise disjoint open subsets then

Can (U, V) ^ n Can(Ui, V)

iei

f -^ (f |Ui)i.

For any two K-Banach spaces V and W we have

Can (U, V © W) ^ Can(U, V) Can(U, W) f 1 — ► (prv of, prw of).

In particular n

∀ian (TT isn\ ~T~[/∀tan/

Can (U, Kn) ^ JJ Can(U, K).

For any continuous bilinear map u : Vi x V2 —>V between K-Banach spaces we have the bilinear map

Can (U, Vi) x Can(U, V2) — ► Can(U, V) (f, g) 1 — ► u(f, g)

Can (U, V) is a module over Can(U, K).

For any continuous linear map u : V —>W between K-Banach spaces we have the linear map

Can (U, V) — ► Can(U, W)

f 1 — ► u o f

Theorem.Let U' C Kn be an open subset and let g ∈ Can (U, Kn) such that g(U) C U'; then the map

Can (U', V) Can(U, V) f -^ f ∘ g

is well defined and K-linear.

Proof.Let x0 ∈ U and put y0 := g(x0) ∈ U'.We choose a ball Be (y0) C U' and a power series F ∈ Fe(Kn; V) such that

f (y)=F(y -yo) for any y ∈ B ∈ (yo).

We also choose a ball Bs (x0) C U and a power series G ∈ F(Kr; Kn) such that

g (x)=G(x — x0) for any x ∈ Bs(x0).

Observing that

||G - G(0)ys'<T-IIG - G(0)ys for any 0<8'<8 8

we can decrease 8 so that

||G - y0 Hs=||G - G(0)|s< ∈

(and, in particular, g(Bs(x0)) C Be(y0)) holds true.It then follows fromthat F o (G - y0) ∈ Fs(Kr; V) and

(F o (G - y0))~(x - x0)=F(G(x - x0)- y0)

$= F(g(x) - y0)$

$= f(g(x))$

for any $x \in Bs(x0)$.

The last result can be expressed by saying that the composite of locally analytic functions again is locally analytic.

Proposition (Local invertibility) Let U C Kr be an open subset and let f ∈ Can(U, Kr); suppose that Dx0f is bijective for some x0 ∈ U; then there are open neighbourhoods U0 C U of x0 and Ui C Kr of f(x0) such that:

i.f : U0 -^ Ui is a homeomorphism;

ii.the inverse mapg : U\ —>U0 is locally analytic, i. ∈ ., g ∈ Can(U, Kr).

Proof.According we find open neighbourhoods U0 C U of x0 and U1 C Kr of f (x0) such that

f : U0 — U U1 is a homeomorphism.

We choose a ball B ∈ (x0) C U0 and a power series F ∈ F ∈ (Kr; Kr) such that

f (x)=F(x — xo) for any x ∈ B ∈ (x0).

The power series F1 (X) := F(X) — f (x0) ∈ F ∈ (Kr; Kr) satisfies F1(0)=0.Moreover, D0F1=Dx0 f is invertible.we therefore find, for a sufficiently small 0<5<e, a power series G1(Y) ∈ Fs (Kr; Kr) such that

G1 (0)=0, ||G1||a<e, and F1 o G1(Y)=Y.

In particular, G1 : Bs(0) —>B ∈ (0) is locally analytic.Hence the composite

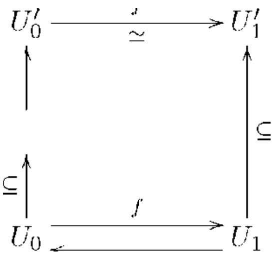
g : U1 := Bs(f (xo)) — — — — — — U Bs(0) — — U B^0) — — — ^ B ∈ (x0)

is locally analytic and satisfies

f o g (y)=f (G1(y — f (x0))+x0)=F (G1(y — f (x0)))

= F1 (G1 (y — f (x0)))+f (x0)=y — f (x0)+f (x0)=y

for any y ∈ U1.By further decreasing 5 we can assume that U1 C U1, and by setting U0 := g(U1) we obtain the commutative diagram



c

B ∈ (x0)

g in which the two lower horizontal arrows both are locally analytic and are inverse to each other.

There are "locally analytic versions".

We have done so already and we will systematically continue to call a

map f : U — u U' between open subsets U C Kr and U' C Kn locally

f c analytic if the composite U —u U' — u Kn is a locally analytic function.

For any h *eG* the maps

∈ $_h$ *: G*G and r_h *: G G*

g — -hg g*i* — -gh

are locally analytic isomorphisms (of manifolds).

By symmetry we only need to consider the case of the left multiplication ∈ $_h$.This map can be viewed as the composite

G —- G *x* G G

g^1 — -(h, g).

Obviously have ∈ $_h$ o ∈ $_h$–**i** = ∈ $_{hh}$-*i* = ∈ $_e$=id_G and then also ∈ $_h$–**i** o ∈ $_h$=id_G.It follows that ∈ - ⁝ = ∈ $_h$–**i** is locally analytic as well.

Check your Progress-4

Discuss Locally analytic functions

____
____
____

2.6 LET US SUM UP

In this unit we have discussed the definition and exampleofConvergent series, Differentiability, Power series, Locally analytic functions

2.7 KEYWORDS

Convergent series…..(K, |.|) is a fixed nonarchimedean field

Differentiability….Let V and W be two normed K-vector spaces, let U C V be an open subset, and let f : U —>W be some map

Power series…..Let V be a K-Banach space.By a power series f (X) in r variables X= (X1, ..., Xr) with coefficients in V we mean a formal series

Locally analytic functions…..Let U C Kr be an open subset and V be a K-Banach space

2.8 QUESTIONS FOR REVIEW

Explain Convergent series

Explain Differentiability

Explain Power series

Explain Locally analytic functions

2.9 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

2.10 ANSWERS TO CHECK YOUR PROGRESS

Convergent series	(answer for Check your Progress-1 Q)
Differentiability	(answer for Check your Progress-2 Q)
Power series	(answer for Check your Progress-3 Q)
Locally analytic functions	(answer for Check your Progress-4 Q)

UNIT - 3:CHARTS AND ATLASES

STRUCTURE

3.0 OBJECTIVES

After studying this unit, you should be able to:

Learn, Understand about Charts And Atlases

Learn, Understand about The Tangent Space

3.1 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.

Charts And Atlases, The Tangent Space

3.2 CHARTS AND ATLASES

Let M be a Hausdorff topological space.

Definition.A chart for M is a triple (U, p, Kn) consisting of an open subset U C M and a map p : U —>Kn such that:

p (U) is open in Kn,

p :U p(U) is a homeomorphism.

Two charts (U1, p1, Kn1) and (U2, p2, Kn2) for M are known compatible if both maps 2° – 1

Pi (Ui n U2K " P2(Ui n U2) ^lO^-1

are locally analytic.

We note that the condition in part ii.of the above definition makes sense since p1 (U1 n U2) is open in Kni.If (U, p, Kn) is a chart then the open subset U is known its domain of definition and the integer n>0 its dimension.Usually we omit the vector space Kn from the notation and simply write (U, p) instead of (U, p, Kn).If x is a point in U then (U, p) is also known a chart around x.

Theorem.Let (Uj, pi, Kni) for i=1, 2 be two compatible charts for M; if U1 n U2=0 then n1=n2.

Proof.Let x ∈ U1 n U2 and put xi := pi(x).We consider the locally analytic maps

f :=^2 o^-1

p1 (U1 n U2K " p2(U1 n U2).

g :=^lo^-1

They are differentiable and inverse to each other, and x2=f (xi).Hence, by the chain rule, the derivatives

DX1 f

K™i ^ K™2

Dx2 g

are linear maps inverse to each other.It follows that n1=n2.

Definition.An atlas for M is a set A={ (Ui, ^i, Kni) }i^I of charts for M any two of which are compatible and which cover M in the sense that M=IJieI Ui.

Two atlases A and B for M are known equivalent if AuB also is an atlas for M.

Notes

An atlas A for M is known maximal if any equivalent atlas B for M satisfies B C A.

Remark.The equivalence of atlases indeed is an equivalence relation.

In each equivalence class of atlases there is exactly one maximal atlas.

Proof.Let A, B, and C be three atlases such that A is equivalent to B and B is equivalent to C.Then A is equivalent to C if we show that any chart (U1, ip1)in A is compatible with any chart (U2, ip2) in C.By symmetry it suffices to show that the map ip2 o ^-1 : ip1(U1 n U2) — ► ^2(U1 n U2) is locally analytic in a sufficiently small open neighbourhood of ^1 (x) for any point x ∈ U1 n U2.Since B covers M we find a chart (V, f) around x in B.By assumption (V, f) is compatible with both (U1, <p1) and (U2, ^>2).Then^1(U1 n V n U2) is an open neighbourhood of ^1(x) in ^1 (U1 n U2) on which the map<p2 ∘ ^-1 is the composite of the two locally analytic maps<p2 ∘ f>~1 and 'f o ^-1.Hence it is locally analytic.

If the given equivalence class consists of the atlases Aj for j ∈ J then A :=Uj ∈ JAj is the unique maximal atlas in this class.

Theorem If A is a maximal atlas for M the domains of definition of all the charts in A form a basis of the topology of M.

Proof.Let U C M be an open subset.We have to show that U is the union of the domains of definition of the charts in some subset of A, or equivalently that for any point x ∈ U we find a chart (Ux, ipx) around x in A such that

Ux C U.Since A covers M we at least find a chart (U'x, <p'x) around x in A.We put Ux :=U'x n U and ^x := ^X|Ux.Clearly (Ux, ^>x) is a chart around x for M such that Ux C U.We claim that (Ux, <px) is compatible with any chart (V, f) in A.But we do have the locally analytic maps

po^Xy1

^x (ux n VK " f (ux n V)

<f'xOp 1

which restrict to the locally analytic maps

po^y1

^x (Ux n V) : " f (Ux n V).

fxOp

Hence B := Au{(Ux, p>x)}is an atlas equivalent to A.The maximality of A then implies that B C A and a fortiori (Ux, p>x) ∈ A.

Definition. An atlas A for M is known n-dimensional if all the charts in A with nonempty domain of definition have dimension n.

Remark Let A be an n-dimensional atlas for M; then any atlas B equivalent to A is n-dimensional as well.

Proof.Let (V, f) be any chart in B and choose a point x ∈ V.We find a chart (U, p>) in A around x.Since A and B are equivalent these two charts have to be compatibledimension u.

Definition.A (locally analytic) manifold (M, A)(over K) is a Hausdorff topological space M equipped with a maximal atlas A.The manifold is known n-dimensional (we write dim M=n) if the atlas A is n-dimensional.

By abuse of language we usually speak of a manifold M while considering A as given implicitly.A chart for M will always mean a chart in A.

Example.Kn will always denote the n-dimensional manifold whose maxi- mal atlas is equivalent to the atlas{(U, C, Kn) : U C Kn open }.

Remark Let (U, p>, Kn) be a chart for the manifold M; if V C U is an open subset then (V, p>|V, Kn) also is a chart for M.

Proof.This was shown in the course

Let (M, A) be a manifold and U C M be an open subset.Then

Au :={ (V, 0, Kn)eA : V C U },

by an atlas for U.We claim that Au is maximal.Let (V0, 00) be a chart for U which is compatible with any chart in Au.To observe that (V0, 00) ∊ AU it suffices, by the maximality of A, to show that (V0, 00) is compatible with any chart (V, 0) in A.That implies (Vn U, 0|Vn U) is a chart in A and hence in AU.By assumption (V0, 00) is compatible with (Vn U, 0|Vn U).Since V0 n V C Vn U the compatibility of (V0, 00)with (V, 0) follows trivially.The manifold (U, AU) is known an open submanifold of (M, A).

As a nontrivial example of a manifold we discuss the d-dimensional projective space Pd (K) over K.We recall that Pd (K)=(Kd+1 \{ 0 })/ ~ is the set of equivalence classes in Kd+1 \{ 0}for the equivalence relation

(a^ ..., a^+i)(ca1, ..., cad+1) for any c ∊ Kx.

As usual we write [a1 :...: ad+1] for the equivalence class of (a1, ..., ad+1).With respect to the quotient topology from Kd+1 \{ 0}the projective space Pd(K) is a Hausdorff topological space.For any 1<j<d+1 we have the open subset

Uj :={ [a1 :...: ad+1] ∊ Pd(K) : |a^ |<|aj|for any 1<i<d+1 }

together with the homeomorphism

<Pj : Uj-A B1(0) C Kd

[«1 :...: ad+1] — (^.....j • j • ' W1)

The (Uj, >pj, Kd) are charts for Pd(K) such that IJjUj=Pd(K).We claimthat they are pairwise compatible.For 1<j<k<d+1 the composite

f : V :={ x ∊ B1 (0) : |xfe_11=1}— -a Uj n Uk-A{y ∊ ∊ 1(0) : |yj|=1} is given by

f (X1, ..., xd)=(-_^, ..., __j-1, -L -, __L ., ..., Pk-1, , ..., JOsL.).

J v 17 ' d ^_k-l' ' _k-l ' _k-l' _k-l' '_k-l' _k-l' ' _k-l'Let a ∊ V be a fixed but arbitrary point and choose a 0< ∊ <1.Then B ∊ (a) C V.We consider the power series

F (X) :=wrE(-ak-T)"Xn-i

T?(Y\-T?(Y\\(Xi+ai) if 1 - i<j or k - i - d, Fi(X) • — (X) •<..

[(Xi-1+ai-i) if J<i<k.

Because of |ak-1|— 1 we have F • — (F1, ..., Fd) ∈ F ∈ (Kd; Kd).For x ∈ Be(a) we compute

F.(x _ a) — V f - xfe-i-afe-i W — _J 1 — _W_

T t ak_i E__/ V a, k — i' ak-1 1+ xk-1 ak-1 xk-1

n>0 ak-1

and then

f (x) — F(x — a).

Hence f ist locally analytic.In case j>k the argument is analogous.The above charts therefore form a d-dimensional atlas for Pd (K).

Exercise.Let (M, A) and (N, B) be two manifolds.Then

AxB •— {(U x V), p x ^, Km+n) • (U, p, Km) ∈ A, (V, ^, Kn) ∈ B }

is an atlas for M x N with the product topology.We call M x N equipped with the equivalent maximal atlas the product manifold of M and N.

Let M be a manifold and ∈ be a K-Banach space.

Definition.A function f • M —> ∈ is known locally analytic if f o p-1 ∈ Can(p(U), ∈) for any chart (U, p) for M.

Remark Every locally analytic function f • M —> ∈ is continuous.

Let B be any atlas consisting of charts for M; a function f • M —> ∈ is locally analytic if and only if f o p-1 ∈ Can(p(U), ∈) for any (U, p) ∈ B.

The set Can (M, ∈) := all locally analytic functions f : M —>E

is a K-vector space with respect to pointwise addition and scalar multiplication.It is easy to observe that a list of properties completely

Notes

analogous to the one given in section holds true.In a later section we will come back to a more detailed study of this vector space.

Let now M and N be two manifolds.The following result is immediate.

Theorem. For a map g : M —>N the following assertions are equivalent: g is continuous and f o g ∈ Can (g-1(V), Kn) for any chart (V, f, Kn) for N; for any point x ∈ M there exist a chart (U, >, Km) for M around x and a chart (V, f, Kn) for N around g(x) such that g(U) C V and f o g o p-1 ∈ Can(p(U), Kn).

Definition.A map g : M —>N is known locally analytic if the equivalent conditions are satisfied.

Theorem. If g : M —>N is a locally analytic map and ∈ is a K-Banach space then

C an (N, ∈) — ► C an(M, ∈) f f o g is a well-defined K-linear map

With L —o- M — U N also g o f : L — ► N is a locally analytic map of manifolds.

Example. For any open submanifold U of M the inclusion map U —U M is locally analytic.

Let g : M —>N be a locally analytic map; for any open submanifold V C N the induced map g-1(V) — U V is locally analytic.

The two projection maps

pi- ! : M x N — ► M and pr2 : M x N — ► N are locally analytic.

For any pair of locally analytic maps g : L —>M and f : L —>N the map

(g, f) : L M x N

x 1 — ► (g(x), f (x))

is locally analytic.

For the remainder of this section we will discuss a certain technical but useful topological property of manifolds.First let X be an arbitrary Hausdorff topological space.

Let X=Ui ∈ i Ui and X=IJ Vj be two open coverings of X.The second one is known a refinement of the first if for any j ∈ J there is an i ∈ I such that Vj- C Ui.

An open covering X=(JieI Ui of X is known locally finite if every point x ∈ X has an open neighbourhoodUx such that the set{i ∈ I : Ux n Ui=0}is finite.

The space X is knownparacompact, resp.strictly paracompact, if any open covering of X can be refined into an open covering which is locally finite, resp.which consists of pairwise disjoint open subsets.

Remark.Any ultrametric space X is strictly paracompact.

Any compact space X is paracompact.

Proposition For a manifold M the following conditions are equivalent:

M is paracompact; M is strictly paracompact the topology of M can be defined by a metric which satisfies the strict triangle inequality.

Proof.We suppose that M is paracompact.From general topology we recall the following property of paracompact Hausdorff spaces.Let A C U C M be subsets with A closed and U open.Then there is another open subset V C M such that

A c V c V c U.

Step 1: We show that the open and closed subsets of M form a basis of the topology.Given a point x in an open subset U C M we have to find an open and closed subset W C M such that x ∈ W C U we can assume that U is the domain of definition of a chart (U, <p, Kn) for M.As reknown above there is an open neighbourhood V C M of x such that V C U.We then have the vertical homeomorphisms

V=—>V=— ^ U M

p (V) ~>y(V) ~>^>(U) ~>Kn.

Since ^>(V) is open in Kn there is a ball B := B ∈ (<p(x)) C ^>(V) around<^(x).We put W := ^>- 1(B) C V.Clearly x ∈ W C U.The ball B is open and hence B is open in V and M.But the ball B also is closed in Kn.Hence W is closed in V and therefore in M.This finishes.

Let now M=Uiej Ui be a fixed but arbitrary open covering.We can assume after refinement, that any Ui is the domain of definition of some chart for M.By the first step we can even assume, after a further refinement, that each U is open and closed in M and is the domain of definition of some chart for M.In particular, each Ui has the topology of an ultrametric space.By assumption we can pick a locally finite refinement (Vj)j^j of (Ui)ie/.So we have the locally finite open covering

M= |Jj ∈ JVj, and for each j ∈ J there is an i(j) ∈ I such that Vj C Ui(j).

Step 2: We construct a covering M=(Jj ∈ J Wj by open and closed subsets Wj C M such that Wj C Vj for any j ∈ J.For this purpose we equip J with a well-order<(recall that this is a total order on J with the property that each nonempty subset of J has a minimal element - by the axiom of choice such a well-order always exists).We now use transfinite induction to find open and closed subsets Wj C M such that

Wj C Vj for any j ∈ J, and

M=(Uj<fc Wj) U (Uj>fc Vj) for any k ∈ J.

We fix a k ∈ J and suppose that the Wj for j<k are constructed already.Claim: M=(U]<k Wj) U (Uj>k Vj).

Let x ∈ M.Since the covering (Vj)j is locally finite the set

{ j ∈ J : x ∈ Vj- }={ ji<...<jr }

is finite.If jr>k then x ∈ Vjr C Uj>k Vj.If jr<k then x ∈ Vj for uny j>jr and the induction hypothesis (property (b) for jr) implies x ∈ 1Jj<jrWj C (Jj<k Wj.This establishes the claim.

We observe that the closed subset

W := M \((|J Wj) U (|J Vj))

j<k j>k

of M satisfies W C Vk C Um.

Claim: Let (X, d) be an ultrametric space; for any subsets A C U C X with A closed and U open there exists an open and closed subset V C X such that

A C V C U.

For any subset D C X and any x ∈ X we put

d (x, D) := inf d(x, y).

The strict triangle inequality implies that the function d(., D) on X is continuous and that

D (e) :={ x ∈ X : d(x, D) = ∈ },

for any ∈ >0, is open in X.Moreover, D(0)=D.The closed subsets A and B := X \ U of X satisfy A n B=0.By the continuity of the functions d(., A) and d(., B) the subsetV :={ x ∈ X : d(x, A)<d(x, B) }

Therefore is open in X and satisfies A C V C U.Similarly V' :={ x ∈ X : d(x, A)>d(x, B)}is open in X.It follows that V as the complement in X of the open subset V' U (Ue>o(A (∈) n B (∈) ^ is closed.This establishes theclaim.We apply this claim to W Q Vk Q U.(k) and obtain an open and closedsubset Wk Q Uj(k) such that W Q Wk Q Vk.With U.(k) also Wk is open and closed in M.As W Q Wk the index k.It remains to show that the Wj for j G J actually cover M.Let x G M.As argued before the set{j G J : x G Vj }={ ji<...<jr}is finite.Then x G Vj for any j>jr.The property (b) for the index jr therefore implies that x G Uj<jrWj.This finishes step 2.

Step 3: At this point we have constructed a locally finite refinement (Wj)jeJ of our initial covering which consists of open and closed subsets Wj Q M.

Claim: W'L :=UjeLWj, for any subset L Q J, is open and closed in M.

Obviously W'L is open.To observe that its complement M \W'L is open as well let x G M \ W'L be any point.In particular, x G Wj for any j ∈ L.Since the covering (Wj)j is locally finite we find an open

Notes

neighbourhood Ux Q M of x such that the set{j G L : Ux 0 Wj=0 }={ j1, ..., js}is finite.Then Ux \(Wj1 U...U Wjs)is an open neighbourhood of x in M \ W'L.This establishes the claim.

We finally define a new index set P by

P := all nonempty finite subsets of J, and for any L G P we put

Wl :=(f|Wj)\(U Wj)=(f|Wj)\W'JXl.

jeL jeJ\L jeL

Clearly any WL is contained in some Wj.By the above claim each WL is open and closed in M.To check thatM=U WlLePholds true let x G M be any point.Then x G WL for the finite set L := {j G J : x G Wj }.Moreover, the WL are pairwise disjoint: Let L1=L2 be two different indices in P.By symmetry we can assume that there is a j G L1 \L2.Then WLl Q Wj and WL2 Q M \Wj.It follows that (WL)LePis a refinement of our initial covering by pairwise disjoint open subsets.Thisproves that M is strictly paracompact.

We start with an open covering of M by domains of definition of charts for M.By assumption we can refine it into a covering M=Uei Ui by pairwise disjoint open subsets.According to each Ui also is the domain of definition of some chart for M.In particular, the topology of Ui can be defined by a metric d!i which satisfies the strict triangle inequality.We put

di (x, y) :=i+dfri) for any x, y G Ui.

Obviously we have di (x, y)=di(y, x) and di(x, y)=0 if and only if x=y.To observe that di satisfies the strict triangle inequality we compute

d.(x z)=di(x, z)<max (di(x, y), di(y, z))

A, ' l+di(x, z) — 1+max (d'i(x, y), d'i(y, z))

/di (x, y) di(y, z)\

= max' iV ' iV ' '

.1+di (x, yR 1+di(y, z).

= max (di(x, y), di(y, z)).

Here we have used the simple fact that t>s>0 implies t (1+s)=t+ts>

t ^ s 1+t>1+s*

s+st=s (1 +1) and hence v+r>1+-.For trivial reasons we have di — di.

On the other hand

di=^ 1 — di

and hence, for 0< ∈ — 1,

di (x, y) if x, y G Ui for some i G I, otherwise.

di (x, y) — ∈ if di(x, y).

This shows that the metrics di and di define the same topology on Ui.We note that

di (x, y)<1 for any x, y G Ui.

We now define

d : M x M —

(x, y) —

This is a metric ond.The strict triangle equality

d (x, z) — max(d(x, y), d(y, z))

only needs justification if not all three points lie in the same subset Ui.But then the right hand side is>1 whereas the left hand side is — 1.We claim that this metric d defines the topology of M.First consider any ball B ∈ (x) with respect to d in M.If ∈ >1 then Be (x)=M, and if ∈ <1 then Be(x) is open in some Ui.Hence Be (x) is open in M.Vice versa let V C M be any open subset and let x G V.We choose an i G I such that x G Ui.Then Vn Ui is an open neighbourhood of x in Ui.Hence, for some 0< ∈ <1, the ball Be(x) with respect to d (or equivalently di) is contained in V n Ui C V.

Corollary.Open submanifolds and product manifolds of paracompact manifolds are paracompact.

Check your Progress-1

DiscussCharts And Atlases

3.3 THE TANGENT SPACE

Let M be a manifold, and fix a point a $\in$ M.We consider pairs (c, v) where

c=(U, ip, Km) is a chart for M around a andv $\in$ Km.

Two such pairs (c, v) and (c', v') are known equivalent if we have

Dv (a) (P' 0 P-1) (v)=v'.

It follows from the chain rule that this indeed defines an equivalence relation.

Definition.A tangent vector of M at the point a is an equivalence class [c, v] of pairs (c, v) as above.

We define

Ta (M) := set of all tangent vectors of M at a.

Theorem. Let c=(U, p, Km) and c'=(U', p', Km) be two charts for M around a; we then have:

The map

dc : Km — Ta(M) v l —>[c, v]

is bijective.

Of, 1 o 0c : Km -l Km is a K-linear isomorphism.

Proof.The dimensions of two charts around the same point necessarily coincide.

i.Surjectivity follows from

[c'', v'']=[c, Dv, , (a)(p o p''-1) (v'')].

If [c, v]=[c, v'] then v'=Dv(a) (p o p-1) (v)=v.This proves the injectivity.ii.From [c, v]=[c', D^(a) (p' o p-1) (v)] we deduce that

Off, 1 ∘ °c=Dv (a) (p' ∘ p-1).

The set Ta (M), has precisely one structure of a topo- logical K-vector space such that the map Oc is a K-linear homeomorphism.Because this structure is independent of the choice of the chart c around a.

Definition. The K-vector space Ta (M) is known the tangent space of M at the point a.

Remark.The manifold M has dimension m if and only if dimKTa (M)=m for any a ∈ M.

Let g : M —>N be a locally analytic map of manifolds.we find charts c=(U, t, Km) for M around a and c=(V, , f, Kn) for N around g(a) such that g(U) C V.The composite

Ta (g) : Ta(M) — — u Km ^(a) — og0--1); Kn — U T^N)

is a continuous K-linear map.We claim that Ta (g) does not depend on the particular choice of charts.Let d=(U', <p') and c'=(V', f) be other chartsaround a and g(a), respectively.Using the identity in the proof as well as the chain rule we compute

Oc ∘ Dv (a)(^ ∘ g ∘ T-1) ∘ ^c''1

= Oc ∘ D^{ g{ a)0 O ^-1) O D^a)^ ∘ g ∘ T-1) ∘ Dv{ a) (Tr ∘ T''1)-1 ∘ Of, 1 =Occ O Dv, (a) (f' O g O t'-1) o Of1.

Definition. Ta (g) is known the tangent map of g at the point a.

Remark.Ta (idM)=idra(M).

Theorem.For any locally analytic maps of manifolds L —U M — U N we have

Ta (g O f)=Tf(a)(g) O Ta(f) for any a ∈ L.

Proposition (Local invertibility) Let g : M — u N be a locally analytic map of manifolds, and suppose that Ta(g) : Ta(M) — U Tg(a) (N) is bijectivefor some a ∈ M; then there are open neighbourhoods U C M of a and V C N of g(a) such that g restricts to a locally analytic isomorphism

g : U — U V of open submanifolds.

Proof.We find charts c=(U', p, Km) for M around a and c=(V', ,Kn) for N around g(a) such that g(U') C V'.We consider the locally analytic function

p (U') U' V' — ^(V') C Kn.

By assumption the derivative

Dv (a)(∘ γ ∘ P-1)=0-1 ∘ T»(g) o 0C

is bijective therefore implies the existence of open neighbourhoods W0 C p (U') of p(a) and W1 C ^(V') of -f(g(a)) such that

0 o g o p-1 : W0 W1

is a locally analytic isomorphism.Hence

g : U := p-1(Wo) — V := 0-1(W0

is a locally analytic isomorphism as well (observe the subsequent exercise).

Exercise.Let (U, p, Km) be a chart for the manifold M; then p : U p(U) is a locally analytic isomorphism between the open submanifolds U of M and p(U) of Km.

Let M be a manifold, ∈ be a K-Banach space, f ∈ Can(M, ∈), and a ∈ M.If c=(U, p, Km) is a chart for M around a then f op-1 ∈ Can(p(U), ∈).Hence daf : Ta(M) Km D-a-U°- E

[c, v] i Dv{ o) (f ∘ p-1) (v)

is a continuous K-linear map.If c'=(U', p', Km) is another chart around a then

D^(o) (f o p-1) o ^-1=D^(o) (f o p-1) o D^(o) (p' o p-1)-1 o 0-1 =D^'(o) (f o p'-1) o 1.

This shows that d0f does not depend on the choice of the chart c.

Definition.d0f is known the derivative of f in the point a.

Remark For ∈ = Kr viewed as a manifold and for the chart c0= (Kr, id, ∈) for ∈ we have

Ta (f)=eco O daf.

Obviously the map

Can (M, ∈) — ▶ L(Ta(M), ∈)

f daf is K-linear.

Let u : E1 x E2 —> ∈ be a continuous bilinear map between K-Banach spaces; if f ∈ Can(M, Ei) for i=1, 2 then u(fi, f2) ∈ Can(M, ∈) and

da (u(fi, f2))=u(fi(a), daf2)+u(dafi, f2(a)) for any a ∈ M.

For g ∈ Can (M, K) and f ∈ Can(M, ∈) we have

da (gf)=g(a) daf+dag f (a) for any a ∈ M.

Proof It is a straightforward consequence of that the function u(f1, f2) is locally analytic Let c=(U, ip) be a chart of M around a.Using the product rule in we compute

da (u(f1, f2)) ([c, vD=Dv(a)(u(f1, f2) ∘ p-1) (v)

= Dif (a)(u(fl ∘ P-\ f2 ∘ p-1)) (v)

= u (f1 O p-1(p(a)), Dv{ a) (f2 ∘ p-1) (v))

+ u (DV(a) (f 1 O P-1) (v), f2 O p-1(p(a)))

= u (f1 (a), daf2([c, v]))+ u(daf 1([c, v]), f2(a)).

This is a special case of the first assertion.

Let c=(U, p, Km) be a chart for M.On the one hand, by definition, we have dap for any a ∈ U; in particular

dap : Ta(M) Km

is a K-linear isomorphism.On the other hand viewing f=(f 1, ..., fm) asa tuple of locally analytic functions f i : U —.K we have

daf=(da<Pi, ..., da<Pm).

This means that{dafi }1<i<m is a K-basis of the dual vector space Ta(M)'.Let

{ (Idk) (a) }1<i<m denote the corresponding dual basis of Ta(M),

dafi{ {d j (a))=Sij for any a ∈ U

where Sij is the Kronecker symbol.For any f ∈ Can (M, ∈) we define the functions

f : U —.E

a daf(() (a)).

Theorem. Jf ∈ Can (U, ∈) for any 1<i<m, and

daf=^2 dafi • §2 (a) for any a ∈ U.

Proof.We have

J2 (a)=Ds'a)(f ∘ f-1) ∘ tfc"1(() (a))

= Ds'a)(f ∘ f-1) (ei)

where e1, ..., em denotes the standard basis of Km.Hence Jf is the composite

U -U f (U) "Dx — ') : L(Km, ∈) i. ∈ .

The function in the middle is locally analytic Clearly, Di —.D (ei) is a continuous K-linear map.Hence the composite of the right two maps is locally analytic by the property.That the full composite df is locally analytic.

Let

t = ∈ Ci (ss) (a) ∈ Ta(M)

be an arbitrary vector.By the definition of the dual basis we have ci= We now compute

daf (t)=^ ci daf(() (a))=^ te(t) • (a)

In a next step we want to show that the disjoint union

T (M) := U Ta(M)

a ∈ M

in a natural way is a manifold again.We introduce the projection map

PM : T(M)-u M

t1 — u a if t ∈ Ta (M).

Hence Ta (M)=pM1(a).

Consider any chart c=(U, <p, Km) for M.The map

Tc : U x Km -U pM1(U)

(a, v)i — u [c, v] viewed in Ta(M)

is bijective.Hence the composite

pc : pM1(U)--U U x Km — U Km x Km=K2m

is a bijection onto an open subset in K2m.The idea is that

ct :=(PM1(U), ^c, K2m)

should be a chart for the manifold T (M) yet to be constructed.Clearly we have

T (M)= U Pm(U).

c= (T^)

Let c=(V, -0, Km) be another chart for M such that U n V=0.The composed map

p (U n V) x Km --U pm1(u n V)=pm1(u) n pM1(v)-U 0(U n V) x km

is given by

(x, v)i — o p-1 (x), Dx(^ o p-1) (v)).

The first component ^ o p-1 of this map is locally analytic on p (Un V) since M is a manifold.The second component can be viewed as the composite

p (U n V) x Km — L(Km, Km) x Km — Km (x, v)i — (Dx(^ o p-1), v) (u, v) I — u(v).

The left function is locally analytic.The right bilinear map is continuous.Hence the composite is locally analytic.This shows that, once ct and cT are recognized as charts for T(M) with respect to a topology yet to be defined, they in fact are compatible, and hence that the set{ct : c a chart for M}is an atlas for T(M).

We have shown in particular that the composed map T T —1

(U n V) X Km ipj }(u n V)-! (U n V) x Km is a homeomorphism.

Definition.A subset X C T (M) is known open if t-1 (X np~f }(U)) is openin U x Km for any chart c=(U, tp, Km) for M.

This defines the finest topology on T (M) which makes all composed mapsU x Km p-M (U) T(M) continuous.

Theorem. The map tc : U x Km — pM1(U) is a homeomorphism with respect to the subspace topology induced by T(M) on p~f[(U).

The map pM is continuous.

The topological space T (M) is Hausdorff.

Proof.The continuity of tc holds by construction.Let Y C U x Km be an open subset.We will show that tc (Y) is open in T(M), i. ∈ ., that t-1(tc(Y) npM1(V)) is open in V x Km for any chart c=(V, ^, Kn) for M.

We can of course assume that U n V=0 so that n=m.Clearly the subset Y n((U n V) x Km) is open in (U n V) x Km.By the subset

a-V^y n((U n V) x Km)))=t-V^y) n p^(U n V))

= Tc∀ Vc (Y) n PM1(U) n Pm1(V)) =Tc∀ Vc(Y) n PM1(V))

is open in (U n V) x Km and therefore in V x Km.

The above reasoning for Y=U x Km shows that tc (Y)='pM }(U) is open in T(M) where U is the domain of definition of any chart for M.It then follows from that pM is continuous.

Let s and t be two different points in T (M).Case 1: We have pM (s)= pM(t).Since M is Hausdorff we find open neighbourhoods U C M of pM (s) and V C M of pM(t) such that UnV=0.then pM1 (U) and pM1(V) are open neighbourhoods of s and t, respectively, such that pM1(U) n pM1(V) =pM1(U n V)=0.Case 2: We have a :=pM(s)=pM(t).We choose a chart c=(U, < , Km) for M around a.The two points s and t lie in the open subset pM1 (U) of T(M).But the subspace pM1 (U) is homeomorphic, via the map tc, to the Hausdorff space U x Km.Hence pM1 (U) is Hausdorffand s and t can be separated by open neighbourhoods in pM1(U) and a fortiori in T(M).

The particular says that ct indeed is a chart for T (M).Altogether we now have established that{cT : c a chart for M}is an atlas for T(M).We always view T (M) as a manifold with respect to the equivalentmaximal atlas.

Definition. The manifold T (M) is known the tangent bundle of M.

Remark.If M is m-dimensional then T (M) is 2m-dimensional.

Theorem.The map pM : T(M) —>M is locally analytic.

Proof.Let c=(U, < ∈ >, Km) be a chart for M.It suffices to contemplate thecommutative diagram

T (M) ^ pM1 (U)

Ac (pM1(U))=A(U) x Km K2m

Let g :M PM>N be a locally analytic map of manifolds.We define the map

T (g) : T(M)-u T(N)

by

T (g)\Ta(M) := Ta(g) for any a ∈ M.

In particular, the diagram

T (M) T(N)

PM PN

M>N

is commutative.

Proposition The map T (g) is locally analytic.

For any locally analytic maps of manifolds L —U M — u N we have

T (g ∘ f)= T(g) o T(f).

Proof We choose charts c=(U, <p, Km) for M and c=(V, ^, Kn) for N such that g(U) C V.The composite

T (U) X Km - — -U pM(U) — — — U pNl(V) — — U ^(V) x Kn is given by

(x, v)i — U (^ O g O ^-l(x), Dx(^ O g O ^-l) (v)).

It is locally analytic by the same argument as for.

Remark.If U C M is an open submanifold then T (C) induces an isomorphism between T(U) and the open submanifoldf }(U).

ii.For any two manifolds M and N the map

T (prl) x T(pr2) : T(M x N) — T(M) x T(N) is an isomorphism of manifolds.

Now let M be a manifold and ∈ be a K-Banach space.For any f ∈ Can (M, ∈) we define

df : T(M) — ► E

t 1>dPM (t)f (t) •

Theorem.We have df ∈ Can (T(M), ∈).

Proof.Let c=(U, p, Km) be a chart for M.

The composed map

p (U) x Km - — U p~M\U) f E

is given by

(x, v)i — ► Dx(f o p-1) (v) and hence is locally analytic by the same argument.

Theorem. Let g : M —>N

be a locally analytic map of manifolds; for any f ∈ Can (N, ∈) we have

d (f o g)=df o T(g) •

Exercise. The map

d : Can(M, ∈) — ► Can(T(M), ∈)

f -u df

is K-linear.

Remark. If K has characteristic zero then a function f ∈ Can (M, ∈) is locally constant if and only if df=0.

Proof. Let c=(U, <p) be any chart for M.As can be observen from the proof ofpM1

x ∈ p (U).By the latter is equivalent to f o p -1 being locally constant on p(U) which, of course, is the same as f being locally constant on U.

Definition. Let U C M be an open subset; a vector field f on U is a locally analytic map f : U —>T(M) which satisfies pM o f=id^.

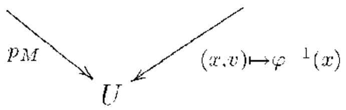
We define

r (U, T(M)) := set of all vector fields on U.

r (u, T(m))=r(u, T(u)).

Suppose that U is the domain of definition of some chart c=(U, y>, Km) forM.Because of the commutative diagram

Pm (U) g — ^(U) x Km



the map

Can (U, Km) — r(U, T(M))

/ 1 — ►{f(a) := /(a)))=Tc(a /(a))

is bijective.The left hand side is a K-vector space.On the right hand side this vector space structure corresponds to the pointwise addition and scalar multiplication of maps which makes sense since each Ta (M) is a K-vector space.The latter we can define on any open subset U C M.For any c ∈ K and {, n ∈ r(U, T(M)) we define

(c i) (a) := c {(a) and ({ +n) (a) :={ (a)+n(a).

Obviously the result are again maps ? : U — ► T(M) satisfying pM◦ ?=id^ But since U can be covered by domains of definition of charts for M the above discussion actually implies that these maps are locally analytic again.We observe that

r (U, T(M)) is a K-vector space.

We have the bilinear map

r (M, T(M)) x Can(M, ∈) — ► Can(M, ∈)

({, /) — D(/) := d/ ∘{.

Theorem. Let u : E1 x E2 — ► ∈ be a continuous bilinear map between K-Banach spaces; for any{ ∈ r(M, T(M)) and / ∈ Can(M, Ej) we have

D (u(/1, /2))=u(D(/1), /2)+u(/1, D(/2)).

Corollary For any vector field ∈ ∈ r(M, T(M)) the map Dg : Can(M, K) — ► Can(M, K)

is a derivation, i. ∈ .:

Dg is K-linear,

Dg (fg)=Dg(f)g+fDg(g) for any f, g ∈ Can(M, K).

Proposition. Suppose that M is paracompact; then for any derivation D on Can (M, K) there is a unique vector field ∈ on M such that D=Dg.

The proof requires some preparation.In the following we always assume M to be paracompact.At first we fix a point a ∈ M.A K-linear map A : Can(M, K) —>K will be known an a-derivation if

A (fg)=A(f)g(a)+f(a)A(g) for any f, g ∈ Can(M, K).

The a-derivations form a K-vector subspace

Der,, (M, K)

of the dual vector space Can (M, K)*.

Theorem. Suppose that M is paracompact, and let A be an a-derivation; if f ∈ Can(M, K) is constant in a neighbourhood of the point a then A(f)=0.

Proof. Case 1: We assume that f vanishes in the neighbourhood U C M of a.we can assume that U is open and closed in M.Then the function

if x ∈ U,

g (x) :=|o if x ∈ U

Notes

lies in Can (M, K) and satisfies gf=f.It follows that

A (f)=A(gf)=A(g)f(a)+g(a)A(f) =0.

Case 2: We assume that f is constant on M with value c.Let 1M denote the constant function with value one on M.Then f=c1m and hence

A (f)=cA(1M)=cA(1M 1M)=cA(1M)+cA(1M)=2cA(1M)=2A(f)

which means A (f)=0.

Case 3: In general we write

f=f (a)lM+(f - f (a)lM)

and use the K-linearity of A together with the first two cases.

As a consequence of the product rule we have the K-linear map

(10) Ta(M) — ^ Der,,(M, K)

t1 — ► At (f) :=daf(t).

The*mapi =ig* : G — ► G l

g^1 — ► g

is a locally analytic isomorphism (of manifolds).

Because of $i^2=id_G$ it suffices to show that the mapi 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* GG, is bijective.

T (*g, h*) (G *x* G)$^{T(9, h)M}$, T*(gh, h*) (G *x* G)

T (*pr*i) x T (*p*r2)

Tg_h (G) x T*h*(G)

in which the lower horizontal arrow is given by

$(ti, t2)^{1}$ — ►(Tg(rh) (ti) +Th(lg) (t2), t2)

is commutative.Suppose that (t_1, t_2) 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 t_1=0.We observe that 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 $\wedge^{-1}$ is locally analytic as well.It remains to note thati is the composite

Check your Progress – 2

DiscussThe Tangent Space

____

____

____

3.4 LET US SUM UP

In this unit we have discussed the definition and exampleofCharts And Atlases, The Tangent Space

3.5 KEYWORDS

Charts And Atlases….A chart for M is a triple (U, p, Kn) consisting of an opensubset U C M and a map p : U —>Kn

The Tangent Space…..M be a manifold, and fix a point a ∊ M consider pairs (c, v)

3.6 QUESTIONS FOR REVIEW

Explain Charts And Atlases

Explain The Tangent Space

3.7 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

3.8 ANSWERS TO CHECK YOUR PROGRESS

Charts And Atlases (answer for Check your Progress-1 Q)

The Tangent Space (answer for Check your Progress-2 Q)

UNIT-4:THEORY OF VALUATIONS-I

STRUCTURE

4.0 OBJECTIVES

After studying this unit, you should be able to:

- Understand about Theory of valuations-I
- Understand about Locally convex k-vector spaces
- Understand about Valuation rings and places

4.1 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.

Theory of valuations-I, Locally convex k-vector spaces, Valuation rings and places

4.2 THEORY OF VALUATIONS-I

Proposition. If M is paracompact then is an isomorphism.

Proof. We fix a chart c=(U, p, Km) for M around a point a and write p=(p1, ..., pm).Since M is paracompact that U is open and closed in M.

Then each pi extends by zero to a function Pi $\in$ Can (M, K).In the discussion

daP=(daPl, ..., daPm) : Ta(M) — Km

is an isomorphism, and we had introduced the K-basis t := gf- (a) of Ta(M).

Injectivity: Let t $\in$ Ta (M) such that At(f)=0 for any f $\in$ Can(M, K) In particular

0=At (pii)=da Pi!(t)=daPi(t) for any 1<i<m.

This means dap (t)=0 and hence t=0.

Surjectivity: From the injectivity which we just have established we deduce that the Ati are linearly independent in Dera (M, K).It therefore suffices to write an arbitrarily given A $\in$ Dera (M, K) as a linear combination of the At..In fact, we claim that

A= $\in$ A (pi!) At i= 1

holds true.Let f $\in$ Can (M, K).We find an open and closed neighbourhood V C U of a such that p (V)=Be(p(a)) and a power series F(X)= caXa $\in$ F(Km; K) such that

f (x)=F(p(x) — p(a)) for any x $\in$ V.

We can write m

f (x)=Y1 ca(^(x)- ^(a)r=f (a)+-cpi(a))gi(x) a i= 1 for any x ∈ V where the gi ∈ Can (V, K) are appropriate functions satisfying gi(a)=Ci (recall that i=(0, ..., 1, ..., 0)).We know that dF

DV (a) (f ∘ ^-1) (ei)=dx (0)=Ci

where e1, ..., em denotes, as usual, the standard basis of Km.We thereforeobtain

gi (a)=Ci=Dv{ a) (f ∘ ^-1) (ei)=daf(9c(ei)).

By the construction of the ti we have 9c (ei)=ti.It follows that

gi (a)=daf(ti).

On the other hand we extend each gi by zero to a function gi! ∈ Can (M, K).The function m

f -F(^H -&(a))gH

is constant (with value f (a)) in a neighbourhood of a.we compute

A (f)=A(F(^ - Vi(a))gn)

M = F A (<Pi! -<Pi (a))gi(a)

M = F A (^i!) daf (ti)

M = F A (^i!) Ati (f).

Since f was arbitrary this establishes our claim.

First of all we note that the relation between derivations and a-derivations on Can (M, K) is given by the formula

D (f) (a)=df(C(a))=daf(∈ (a))=A?(a) (f).

Therefore if Dg=0 then Ag (a)=0 for any a G M.Then implies that{(a)=0 for any a G M, i. ∈ ., that ∈ =0.This shows that the ∈ in our assertion is unique if it exists.For the existence we first fix a pointa G M and consider the a-derivation A (f) := D(f) (a).By there is a tangent vector ∈ (a) G Ta(M) such that A=Ag(a).For varying a G Mthis gives a map ∈ : M —>T(M) which satisfies pM ∘ ∈ =idM.It remains to show that ∈ is locally analytic, since D=Dg then is a formal consequence.So let c=(U, <p, Km) be a chart for M.In the proof we have observen thatm

D (f) (a)=^ D(Fi!)(a) ' Aec(ei) (f).

It follows that

m ∊ (a)=^ D(pa) (a) Qc(ei)=dc((D(pn) (a), ..., D(pm\) (a))).

Using the commutative diagram

vi —>(a, v)

Km U x Km

dc=^Ta (M)^ Vm(U)

we rewrite this as

∊ (a)=Tc(a, (D(pu) (a), ..., D(<pmO(a))).

This means that under the identification discussed after the definition of vector fields we have

∊ |U= ∊ /with f :=(D(^), ..., D(pm!)) G Can (U, Km).

Hence ∊ is locally analytic.

Theorem. For any derivations B, C, D : Can(M, K) — ► Can(M, K) we have:

[B, C] := B o C — C o B again is a derivation;

[,] is K-bilinear;

[B, B]=0 and [B, C]=-[C, B];

(Jacobi identity) [[B, C], D]+[[C, D], B]+[[D, B], C]=0.

Proof. These are straightforward completely formal computations.

Definition.A K-vector space g together with a K-bilinear map

[,] : g x g — ► g

which is antisymmetric (i. ∈ ., [z, z]=0 for any z ∈ g) and satisfies the Jacobi identity is known a Lie algebra over K.

If M is paracompact then we can define the Lie product [∈ , n] of two vector fields ∈ , n ∈ r(M, T(M)) by the requirement that

D[?>n] — D? 0 DnDn ∘ Df holds true.This makes r (M, T(M)) into a Lie algebra over K.

Proposition. Suppose that M is paracompact, and let ∈ be a K-Banach space and ∈ , n ∈ r(M, T (M)) be two vector fields; on C an(M, ∈) we then have

D[?>n] — D? 0 DnDn 0 Df *

Proof.Let f ∈ Can (M, ∈).We have to show equality of the functions

DK, n](/)=df ∘ [C, n]and

(D? ∘ Dn -Dn ∘ De) (f)=d(Dn(f)) ∘ ∈ - d(D?(f)) ∘ n

— d (df o n) o ∈ - d(df o ∈) o n*

This, of course, can be done after restriction to the domain of definition U of any chart c=(U, <p, Km) for M.Since M is paracompact we furthermore need only to consider charts for which U is open and closed in M.Let =(^i, ** *, <pm) and denote, as before, by ∈ Can(M, K) the extension by zero of<fi.We now make use of the following identifications.If ? denotesthe restriction to U of any of the vector fields ∈ , n, and [∈ , n] then, asdiscussed after the definition of vector fields

PM1 (U) P(U) x Km

? x^ (x, γ(x))

u=^ ^ (U)

Pm (U) 1 f(U) x Km.

These identifications reduce us to proving the equality of the following two functions of x ∈ ip (U) given by

Notes

Dx (f o ^-1) (g[s, n](x)) and

Dx (df o n o ^-1) (g(x))- Dx(df o ∈ o ^-1) (g^(x))

= Dx (D.(f ∘ ^-1) (gn(.)))(γ(x))- Dx(D.(f ∘ ^-1) (γ(.)))(gv(x)), respectively.

By viewing D.(f o ^>- 1), resp.gn(.) and g%(.), as functions from ^>(U) into L(Km, ∈), resp.into Km, wecan apply the product rule for the continuous bilinear map

L (Km, ∈) x Km — ► ∈ (u, v) l —>u(v)

to both summands in the last expression for and rewrite it as

= [Dx (D.(f o ^-1)) (g(x))\(gv(x))+Dx(f o v-1)iDxgv(g(x))]

- [Dx(D.(f o ^-1) (gn(x))](g(x))- Dx(f o ^-1)[Dxg(gv(x))].

To simplify this further we establish the following general

Claim: For any open subset V C Km, any point x ∈ V, any vectors v=(v1, ..., vm) and w=(w1, ..., wm) in Km, and any function h ∈ Can(V, ∈) we have

Dx (D.h (v)) (w)=Dx(D.h (w)) (v).

Note that the function D.h (v) is the composite

V — U ∈ (k m, ∈) ∈ .

We expand h around the point x into a power series

h (y)=H(y - x).

we then have

m dH Dyh (v)= ∈ vidY- x)

and

m dH Dx{ D.h{ v)){ w)= ∈ viDx(dY(.-x)) (w)

mm O O

= ∈ vi ∈ wj (dYj dYH) (0)

i=1 j=1 ^

m m o o

= ∈ Wj ∈ vi(dvi ag H) (0)

j=1 i=1 i j

= Dx (D.h (w)) (v).

Applying this claim to weobserve that the expression for the function simplifies to

Dx (f ∘<f-1)[Dxgv(g(x))-Dxg(gv(x))].

Comparing this with we are reduced to showing that the identity

g^, v] (x)=Dxgv(g(x))-Dxg(gv(x))

holds true in Can (^>(U), Km).But in case ∈ = K our assertion and the whole computation above holds by construction.In particular we have

Dx (Aii ∘ A-1) (g[e, n](x))=Dx(Aii ∘ A-1)[Dxg^(γ(x))-Dxγ(gv(x))] for any 1<i<m.Since

Dx (^i! O ^-1): Km K (v1, ..., vm) I ► vi

the identity follows immediately.

Remarks. The identity shows that Can (V, Km), for any open subset V C Km, is a Lie algebra with respect to

[f, g] (x) :=Dxf(g(x))-Dxg(f(x)).

The identity can be made into a definition of which one then can show that it is compatible with any change of charts for M.In this way a Lie product [∈ , n] can be obtained and can be proved even for manifolds which are not paracompact.

The topological vector space Can (M, ∈),

Notes

Throughout this section M is a paracompact manifold and ∈ is a K-Banach space.Following that Can (M, ∈) in a natural way is a topological vector space.

To motivate the later construction we first consider a fixed function f G Can (M, ∈).Since, M is strictly paracompact we find a family of charts (Uj, pj, Kmj), for j G J, for M such that the Uj are pairwise disjoint and M=(JjeJUj.According to Remark the function f is locally analytic if and only if all f o pj1 :pj(Uj) —>E, for j G J, are locally analytic.For each pj (Uj) we find balls B ∈ jv(xj, v) C Kmj and power series Fj, v G F ∈ jv(Kmj; ∈) such that

By refined into a covering by pairwise disjoint balls Bsja (yj, a).Consider a fixed a.We find a v such that (yj, a) C B ∈ jv(xj, v).In fact we then have

Bmin (Sj, a, ej, v) (yj, a)=BSj, a (yj, a) C B ∈ j, v (xj, v)=B ∈ j, v (yj, a).

Hence we can assume that Sj, a<Sj, u.Using we can change Fj, v into a power series Fj, a G Fsj a (Kmj; ∈) such that

f o p-1 (x)=Fj, a(x -yj, a) for any x G Bs^ (yj, a).

We put Uj, a :=pj-1(Bsj a(yj, a)).The (Uj, a, Pj, Kmj) again are charts for M such that the Uj, a cover M and are pairwise disjoint.

Resume: Given f G Can (M, ∈) there is a family of charts (Ui, pi, Kmi), for i G I, for M together with real numbers ei>0 such that:

M= |JieI Ui, and the Ui are pairwise disjoint;

ifi (Ui)=B ∈ i(xi) for one (or any) Xi ∈ fi(Ui);

there is a power series Fi ∈ F ∈ i (Kmi; ∈) with

f o ff1 (x)=Fi(x - Xi) for any x ∈ fi(Ui).

We note that by the existence of Fi as well as its norm ||Fiyei is independent of the choice of the point xi.

Let (c, $\in$) be a pair consisting of a chart c=(U, f, Km) for M and a real number $\in$ >0 such that f(U)=B $\in$ (a) for one (or any) a $\in$ f(U).As aconsequence of the identity theorem for power series the K-linear map

F $\in$ (Km; $\in$) — ► Can(U, $\in$)

F 1 — ► F (A(.)-a)

is injective.Let F (Cy $\in$) ($\in$) denote its image.It is a K-Banach space withrespect to the norm

||f ||=||F| $\in$ if f (.)=F (f(.)-a).

By the pair (F(c, $\in$) ($\in$), |||) is independent of the choice of the point a.

Definition. An index for M is a family I={ (ci, ei) }ie/ of charts ci= (Ui, (pi, Kmi) for M and real numbers ei>0 such that the above conditions (a) and (b) are satisfied.

For any index I for M we have

Fi (E) :=nF(a, $\in$ i) ($\in$) C ^Can(Ui, $\in$) =Can(M, $\in$).iei iei

Our above resume says that

C an (M, $\in$) =y Fi ($\in$)

where I runs over all indices for M.Hence Can (M, $\in$) is a union of direct products of Banach spaces.This is the starting point for the construction of a topology on Can (M, $\in$).

But first we have to discuss the inclusion relations between the subspaces Fi (E) for varying I.Let I={ (ci=(Ui, fi, Kmi), ef) }iei and J={ (dj= (Vj, ^j, Knj), Sj) }jej be two indices for M.

Definition.The index I is known finer than the index J if for any i $\in$ I there is a j $\in$ J such that:

(i) Ui C Vj,

Notes

ii)there is an a ∈ ^(Uf and a power series Fi, j ∈ F ∈ i(Kmi; Knj) with \\Fi, j — Fi, j(O)!^<Sj and

fj o ^"1 (x)=Fi, j(x — a) for any x ∈ Ti(Uf).

We observe that if the condition (ii) holds for one point a ∈ ^i(Ui) then it holds for any other point b ∈ ^i(Ui) as well.This follows from which implies that Gi, j (X) := Fi, j (X+b — a) ∈ F ∈ i(Kmi; Knj) with f j o ^"1 (x)=Gi, j(x — b) for any x ∈ Ti(Ui)

and

\ \Gi, j — Gi, j (0) 11 ∈ i=II (Fi, j — Fi, j (0)) (X+b — a)+Fi, j (0) — Gi, j (0)| ∈ i

<maX(\ (Fi, j — Fi, j (0)) (X+b — a)| ∈ i, Sj)

= max(\ Fi, j — Fi, j (0) II ∈ i, Sj)

= Sj.

Theorem. If I is finer than J then we have Fj (E) C Fj (∈).

Proof. Let f ∈ Fj (E).We have to show that f |Ui ∈ F(Ci, ∈ i) (∈) for any i ∈ I.In the following we fix an i ∈ I.

We have ^i (Ui)=B ∈ i(a).By assumption we find a j ∈ J and an Fi, j ∈ F ∈ i (Kmi; Knj) such that

Ui C Vj,

\ \Fi, j — Fi, j (0)| ∈ i<Sj, and

fj o ^∀1 (x)=Fi, j(x — a) for any xTi(Ui).

We put

b := f j o ^-_1(a)=Fi, j(0) ∈ f j(Vj).

Since f ∈ Fj (E) we also find a Gj ∈ F (Knj; ∈) such that

f o f-1 (y)=Gj(y — b) for any y ∈ f j (Vj)=(b).

As a consequence of then the power series

Fi :=Gj o (Fi, j — Fi, j(0)) ∈ F ∈ i(Kmi; ∈)

exists and satisfies

Fi (x - a)=Gj(Fi, j(x - a)- b)=f o f-1(fj o p-1(x))=f ∘ p-1(x) for any x ∈ pi(Ui).

The relation of being finer only is a preorder.If the index I is finer than the index J and J is finer than I one cannot conclude that I=J.

But it does follow that Fx (E)=Fj (∈) which is sufficient for our purposes

Theorem. For any two indices J1 and J2 for M there is a third index I for M which is finer than J1 and J2.

Proof. Let J1={ ((Ui, pi, Kni), ef) }ieI and J2={ ((Vj, fj, Kmj), Sj) }jj.We have the covering

m=y Ui n Vji, j

by pairwise disjoint open subsets.For any pair (i, j) ∈ I x J the function

fj o p-1 : pi(Ui n Vj) — ► Kmj

is locally analytic.Hence we can cover pi (Ui n Vj) by a family of balls Bi, j, k=(ai, j, k) such that/3i, j, k<min(ei, Sj), and

there is a power series Fi, j, k ∈ Fpijk (Kni; Kmj) with

fj o p-1 (x)=Fi, j, k (x - ai, j, k) for any x ∈ Bi, j, k.

Using the fact that

\ \Fi, j, k - Fi, j, k (0)||«<- fj\\Fi, j, k - Fi, j, k (0)||ft, j, k for any 0<a<fi, j, k

together with we can, after possibly decreasing the fj, , j, k, assume in addition that

\ \Fi, j, k — Fi, j, k(0)lift, j, k<Sj.

Notes

After a possible further refinement based on (compare the argu- ment for the resume at the beginning of this section) we finally achieve that the Bi, j, k are pairwise disjoint.We put

Wi, j, k := A-(Bi, j, k)

and obtain the index I :={ ((W^-.k, <fi, Kni), A.j^)}i, j, k for M.By construction I is finer than J2.

Moreover, observing that ^io^"1 : ^i(Wi, j -, k) — M Kni is the inclusion map and that ^i, j, k<ei we observe that I is finer than J1 for trivial reasons.

Given any index I for M we consider Fx (∈) =HieI F(Ci, ∈ i) (∈) from now on as a topological K-vector space with respect to the product topology of the Banach space topologies on the F(Ci, ∈ i) (∈).Obviously Fx (E) is Hausdorff.But it is not a Banach space if I is infinite.Suppose that the topology of Fx (E) can be defined by a norm.The corresponding unit ball B1 (0) is open.By the definition of the product topology there exist finitely many indices i1, ..., ir ∈ I such that

n F (a, si) (∈) x{ 0 }x...x{ 0 }C ∈ 1(0).

i=ii,..., ir

As a vector subspace the left hand side then necessarily is contained in any ball B ∈ (0) for ∈ >0.The intersection of the latter being equal to{0}it follows that I is finite.

Theorem If I is finer than J then the inclusion map Fj (E) — M Fx (∈) is continuous.

Proof. For any i ∈ I there exists, by assumption, a j(i) ∈ J such that the conditions (i) and (ii) in the definition of "finer" are satisfied.The inclusion map in question can be viewed as the map

n ∈ « .,) (∈) -m n F(ci.«i)(∈)

(fj)j 1 M (fj(i)\Ui)i.

Hence it suffices to show that each individual restriction map

F (d(i), 0(i)) (∈) -M F(ci, ei) (∈)

is continuous.But we even know from Prop.5.4 that the operator norm of this map is<1.

We point out that, for I finer than J, the topology of Fj (∈) in general is strictly finer than the subspace topology induced by Fx (∈).

In the present situation there is a certain universal procedure to construct from the topologies on all the Fx (E) a topology on their union Can(M, ∈) = UjFx (∈).Since this construction takes place within the class of locally convex topologies we first need to review this concept in the next section.

Check your Progress-1

Discuss Theory of valuations-I

____

____

____

4.3 LOCALLY CONVEX K-VECTOR SPACES

This section serves only as a brief introduction to the subject.The reader who is interested in more details is referred to LetE be any K-vector space.

Definition.A (nonarchimedean)seminorm on ∈ is a function q : ∈ —>R such that for any v, w ∈ E and any a ∈ K we have:

q (av)=|a| q(v),

q (v+w)<max(q(v), q(w)).

It follows immediately that a seminorm q also satisfies:

q (0)=|0| q(0)=0;

q (v)=max(q(v), q(-v))>q(v — v)=q(0)=0 for any v ∈ E;

q(v+w)=max(q(v), q(w)) for any v, w ∈ E such that q(v)=q(w) — q(v — w)<q(v) — q(w)<q(v — w) for any v, w ∈ E.

Let (qi)iei be a family of seminorms on ∈ .We consider the coarsest topology on ∈ such that:

All maps qi : ∈ —>R, for i ∈ I, are continuous,

all translation maps v+.: ∈ —>E, for v ∈ E, are continuous.

It is known the topology defined by (qi)iei.For any finitely many qi1, ..., qir and any w ∈ E and ∈ >0 we define

B ∈ (qii, ..., qir; w) :={ v ∈ E : qir(v — w), ..., qir(v — w)< ∈ }.

The following properties are obvious:

B ∈ (qii, ..., qir; w)=B^q^; w) n...n B ∈ (qir; w);

B ∈ i (qii; wi) n B ∈ 2 (qi2; w2)=UwBmin(∈ i, ∈ 2) (qii, qi2; w) where w runs over all points in the left hand side;

B ∈ (qii, ..., qir; w)=w+B^, ..., qir ;0);

a B ∈ (qii, ..., qir; w)=Bjtt| ∈ (qii, ..., qir; aw) for any a ∈ Kx.

Theorem. The subsets Be (qil, ..., qir; w) form a basis for the topology on ∈ defined by (qi)ie/•

Proof. The B ∈ (q^, ..., qir; w), do form a basis for a (unique) topology T' on ∈ .On the other hand let T denote the topology defined by (qi)iei.We first show that T' C T.It suffices to check that B ∈ (qi; 0) G T for any i G I and ∈ >0.As a consequence we certainly have that

B-(qi; w) :={ v G ∈ : qi(v - w)<5}G T

for any w G ∈ and 5>0.But we observe that

Be (qi; 0)=B- (qi;0) U |J B- (qi; w).

qi (w)= ∈

To conclude that actually T'=T holds true it now suffices to show that T' satisfies.The continuity property follows immediately from To establish for T' we have to show that q-1((a, 3)) G T' for any i G I and any open interval (a, 3) C R.Because of we can assume that 3>0.Let w G q-1((a, 3)) be any point.Case 1: We have qi (w)>0.Choose any 0< ∈ <qi (w).It then follows from (v) that Be(qi; w) C q-1(qi(w)) C q-1((a, 3)).Case 2: We have qi (w)=0.Choose any 0< ∈ <3.We obtain Be (qi; w) C qt_1([0, e]) C q-1((a, 3)) since necessarily a<0 in this case.

Theorem. ∈ is a topological K-vector space, i. ∈ ., addition and scalar multiplication are continuous, with respect to the topology defined by (qi)iei.

Proof. From the following inclusions:

B ∈ (qii, ..., qir; w1)+B ∈ (qii, ..., qir; w2) C B ∈ (qii, ..., qir; w1+w2);

Bs (a) B|a|- i ∈ (qii, ..., qir; w) C B ∈ (qii, ..., qir; aw) provided 5<|a| and 5 max(q^(w), ..., qir(w))<e;

Bs (0) B ∈ (qii, ..., qir; w) C B ∈ (qii, ..., qir; 0) provided 5<1 and 5 max(qii(w), ..., qir(w))< ∈ .

Exercise. The topology on ∈ defined by (qi)iei is Hausdorff if and only if for any vector 0=v G ∈ there is an index i G I such that qi(v)=0.

Definition.A topology on a K-vector space ∈ is known locally convex if it can be defined by a family of seminorms.A locally convex K-vector space is a K-vector space equipped with a locally convex topology.

Obviously any normed K-vector space and in particular any K-Banach space is locally convex.

Remark. Let{Ej }jeJ be a family of locally convex K-vector spaces; then the product topology on ∈ :=njejEj is locally convex.

Proof. Let (qj, i)i be a family of seminorms which defines the locally convextopology on Ej.Moreover, letprj : ∈ —>Ej denote the projection maps.Using one checks that the family of seminorms (j o prj)i, j defines the product topology on ∈ .

Exercise Let{ Ej }jeJ be a family of locally convex K-vector spaces and let ∈ :=njeJEj with the product topology; for any continuous semi- norm q on ∈ there is a unique minimal finite subset Jq C J such that

q(n Ej x{0}x...x{0 }) ={ 0 }.jeJ \Jq

For our purposes the following construction is of particular relevance.Let ∈ be a any K-vector space, and suppose that there is given a family {Ej }jeJ of vector subspaces Ej C ∈ each of which is equipped with a locally convex topology.

Theorem. There is a unique finest locally convex topology T on ∈ such that all the inclusion maps EjE, for j ∈ J, are continuous.

Proof. Let Q be the set of all seminorms q on ∈ such that q|Ej is continuous for any j ∈ J, and let T be the topology on ∈ defined by Q.It follows immediately from that all the inclusion maps Ej —m (E, T) are continuous.On the other hand, let T' be any topology on ∈ defined by a family of seminorms(qi)iei such that Ej — M (E, T') is continuous forany j ∈ J.Obviously we then have (qi)ieI C Q.This implies, using again that T' C T.

The topology T on ∈ in the above Theorem is known the locally convex final topology with respect to the family{Ej }jeJ.Suppose that the family {Ej }jeJ has the additional properties:

- ∈ = UjeJEj;

the set J is partially ordered by<such that for any two j1, j2 ∈ J there is a j ∈ J such that j1<j and j2<j;

whenever j1<j2 we have Ej1 C Ej2 and the inclusion map Ej1 —Ej2 is continuous.

In this case the locally convex K-vector space (E, T) is known the locally convex inductive limit of the family{Ej }jeJ.

Theorem.A K-linear map f : ∈ —> ∈ into any locally convex K- vector space ∈ is continuous (with respect to T) if and only if the restrictionsf |Ej, for any j ∈ J, are continuous.

Proof. It is trivial that with f all restrictions f |Ej are continuous.Let us therefore assume vice versa that all f |Ej are continuous.Let (qi)ieI be a family of seminorms which defines the topology of ∈ .Then all seminorms qi := qi ∘ f, for i ∈ I, lie in the set of seminorms Q which defines the topologyT of ∈ .It follows that

f-1 (B ∈ (q_ii, ..., qir; f (w))=Be(qii, ..., qir; w)

is open in ∈ .Because of that f is continuous.

Theorem. Let{Ej }jeJ be a family of locally convex K-vector spaces and let ∈ :=njeJEj with the product topology; suppose that each Ej has the locally convex final topology with respect to a family of locally convex K-vector spaces{Ej, k }keIj and that Ej=IJkEj, k; for any k=(kj)j ∈ I := rije j1 j we put Ek :=nje J Ej, kj with the product topology; then the topology of ∈ is the locally convex final topology with respect to the family{Ek }keI.

Proof. By the locally convex topology of Ej is defined by the set Qj of all seminorms q such that q|Ej, k is continuous for any k ∈ Ij.Let prj : ∈ —>Ej denote the projection maps.By the topology of ∈ is defined by the set of seminormsQ :=IJjeJ{ qoprj : q ∈ Qj }.For any q ∈ Qj and any k ∈

Hence the restriction of any seminorm in Q to any Ek is continuous.This means that the locally convex final topology on ∈ with respect to the family{Ek }k is finer than the product topology.Vice versa, let q be any seminorm on ∈ such that q\Ek, for any k G I, is continuous.We have to show that q is continuousfor any k G I, a unique minimal finite subset Jq, k ∈ J such that the restriction q\Ek factorizes into

e— - — -nj j

In particular, q\Ej, kj — 0 for any j G Jq, k.We claim that the set

Jq • — |^J Jq, k kei

is finite.We define ∈ —(∈ j)j G I in the following way.If j G Jq we choosea k G I such that j G Jq, k and we put ∈ j •— kj; in particular, q\Ej^ — q\Ej, kj — 0.For j G J \Jq we pick any ∈ j G Ij.By construction we haveJq ∈ Jq, |so that Jq necessarily is finite.This means that the seminorm q on ∈ factorizes into R.

It follows that

q (v)<max (q\Ej) o prj(v) for any v G ∈ .jeJq

Since each q\Ej is continuous by assumption we conclude that q is continuous.

The topological vector space Can (M, ∈),

As in section we let M be a paracompact manifold and ∈ be a K-Banach space.We have observen that

C an (M, ∈) — y Fi (∈)

where I runs over all indices for M.Each Fi (E) by Remark is locally convex as a product of Banach spaces.We can and always will view Can (M, ∈) as the locally convex inductive limit of the family {Fi (∈) }i(where I<J if J is finer than I).All our earlier constructions involving Can (M, ∈) are compatible with this topology.In the following we briefly discuss the most important ones.

Proposition For any a ∈ M the evaluation map

5a : Can(M, ∈) — ► E

f 1 — ► f (a)

is continuous.

Proof. It suffices, to show that the restriction 5a\FI (E) is continuous for any index I for M.Let I={ (ci=(Ui, ifi, Kmi), ei) }iei.There is a unique i ∈ I such that a ∈ Ui.Then ^i (Ui)=B ∈ i(^i(a)), and we have the Fi (∈) ^*E

F ^F (0)

F (Ci, Si) (∈) Fsi(Kmi; ∈).

F (ifi(.)-ifi (a))^F

The left vertical projection map clearly is continuous.The lower horizontal map is a topological isomorphism by construction.By Remark the right vertical evaluation map is continuous of operator norm<1.

Corollary. The locally convex vector space Can (M, ∈) is Hausdorff.

Proof. Let f=g be two different functions in Can (M, ∈).We find a point a ∈ M such that f (a)=g(a).Since ∈ is Hausdorff there are open neighbourhoodsVfof f (a) and Vg of g(a) in ∈ such that Vf n Vg=0.Using we observe that Uf := 5-1(Vf) and Ug := 5-1(Vg) are open neighbourhoodsof f and g, respectively, in Can(M, ∈) such that Uf n Ug=0.

Remark. With M also its tangent bundle T (M) is paracompact.

Proof. Since M is strictly paracompact by we find a family of charts{ci=(Ui, ^i, Kmi) }ie/ for M such that the Ui are pairwise disjoint and M=IJi Ui.Then the ci, T=(pM1(Ui), AgCi, K2mi) form a family of charts for T(M) such that T(M) is the disjoint union of the open subsets P~M (Ui).Each pM1 (Ui) being homeomorphic to an open subset in K2mi carries the topology of an ultrametric space.Topology of T (M) can be defined by a metric which satisfies the strict triangle inequality.Hence T (M) is paracompact.

Proposition. The map d : Can(M, ∈) — ► Can(T(M), ∈) is continuous.

For any locally analytic map of paracompact manifolds g : M —>N the map

Can (N, ∈) — ► Can(M, ∈) f -^ f ∘ g

is continuous.

For any vector field f on M the map D^ : Can(M, ∈) —>Can(M, ∈) is continuous.

Proof. We have to show that d|Fi (E) is continuous for any index I={ (ci=(Ui, pi, Kmi), ei) }iei for M.Let f ∈ Fi (E).We have the commutative diagrams

(x, v)^Dx(f o^r1) (v)

PM

Ui -*Ti (Ui)

We also have power series Fi ∈ FSi (Kmi; ∈) such that

f O p- !(x)=Fi(x - ai) for any x ∈ Pi(Ui)=B ∈ i(a).

From the proof we recall the formula

mi d F

Dx (f ∘ p-1) (v)=vjdxt.(x- ai)

j=1 j

for any x ∈ pi (Ui) and any v=(v1;..., vmi) ∈ Kmi.We now cover Kmi by pairwise disjoint balls B ∈ i (w((i)) where w((i)=(w^l, ..., w^.) runs over an appropriate family of vectors in Kmi, and we put

m'i d F

Gik (Xi, ..., Xmi, Y1, ..., Ymi) :=+wg) ^ G F* (K2mi; ∈).

Then

df 0 fiX (x, v)=Dx(f 0 P- 1) (v)=Gi, k(x - ai, v -wg) for any (x, v) G pi(Ui) x B ∈ i(wg)=B ∈ i(apwg).This means that df G FJ (E) C Can(T(M), ∈) for the index

J :={ ((Pig (BSi(ai, wki))), fi, Ci, K2mi), Si) }i, k.

In other words we have the commutative diagram Can (T(M), ∈) … Fj (∈) Since the vertical inclusion maps are continuous by construction this reducesus to showing the continuity of the lower horizontal map Fi (∈) —>Fj (∈).But this easily follows from the inequalities

ii.We only sketch the argument and leave the details to the reader.Let X={ ((Ui, pi, Kni), ei) }ie/ be an index for N.We refine the covering M= Ui g-1(Ui) into a covering M=(JjeJ V which underlies an appropriate index J={ ((Vj, , Kmj), Sj) }jeJ and such that, for any i G I and j G J with Vj C g~1(Ui), there is a power series Gi, j G Fs(Kmj; Kni) with s, <Si andPi o g o ^j (x)=Gi, j(x -aj) for any x G ^j(Vj)=Bs, (aj).In this situation we have the commutative diagram

Can (N, ∈) — //g>Can(M, ∈)

where the lower horizontal arrow in terms of power series is given by the maps

Fe.(Kni; ∈) ~^FS.(Km; ∈)

F i — ► F o (Gi, j - Gi, j (0))

Proposition. For any covering M=Uie /Ui by pairwise disjoint open subsets Ui we have

C an (M, ∈) =^ C an(Ui, ∈) ieias topological vector spaces.

Proof.Using one checks that in the construction of Can (M, ∈) as a locally convex inductive limit it suffices to consider indices for M whose underlying covering of M refines the given covering M=(Ji Ui.Then the assertion is a formal consequence

In this and the next chapter we give a short account of the classical 1 theory of valuated fields.Unless otherwise stated by a ring we mean a commutative ring with the unit element 1 and without zero divisors.

Definition. Let A be a ring and r a totally ordered commutative group [1].A valuation v of the ring A is a mapping from A* (the set of non-zero elements of A) into r such that

(I) v(xy)=v(x)+v(y) for every x, y in A*.

(II) v(x+y)>inf (v(x), Vy)) for every x, y in A*.

We extend v to A by setting v (0)=to; where to is an abstract element added to the group r satisfying the equation

to+to=a+to=to+a=to for a in r.

We assume that a<to for every a in r.The valuation v is said to be improper if v (x)=0 for all x in A*, otherwise v is said to be proper.

The following are immediate consequences of our definition.

v (1)=0.For, v(x.1)= v(x)=v(x)+v(1), therefore v(1)=0

If for x in A, x 1 is also in A, we have v(x 1)=-v(x), because 2 v(1)=v(xx-1)=v(x)+v(x~l)=0

If x is a root of unity, then v(x)=0.In particular v(- 1)=0, which implies that v(-x)=v(x)

n in Z (the ring of integers)

v (n)=v(1++ 1)>inf(v(1))=0.

If for x, y in A v(x) ± v(y), then v(x+y)=inf(v(x), v(y)).Let us assume that v (x)>v(y) and v(x+y)>v(y).Then v (y)=v(x+y - x)>>inf(v(x+y), v(-x))>v(y), which is impossible.

If Xj belongs to A for i=n, 1, 2, ..., n, then one can prove by induction

on n that v (∊ xf)>inf (v(xi)) and that the equality holds if

i=1 1<i<n

there exists only one j such that v (xj)=inf (v(xi)).In particular if

1<I<n

Yj xi=0 (n>2) then v(xi)=v(xj)=inf (v(xk)) for at least one pair

j=1 1<k<n

of unequal indices i and j.For, let xi be such that v(xi)<v(xj) for i ± l.

Then v (xi)>inf (v(xk))=v(xj), which proves that v(xi)=v(x,).

1<k<n k±i J J

Proposition. Let A be a ring with a valuation v.Then there exists one and only one valuation w of the quotient field K of A which extends v.

It is observen immediately that ii |- j=v(x)- v(y) for x, y in A.

So without loss of generality we can confine ourselves to a field.The

image of K* (the set of non-zero elements of field K) by v is a subgroup of r which we shall denote by rv

Proposition. Let K be a field with a valuation v.Then

The set O={ x\x ∈ K, v(x)>0}is a subring of K, which we shall call the ring of integers of K with respect to the valuation v.

The set Y={ x|x ∈ K, v(x)>0}is an ideal in O known the ideal of valuation v.

O*=O -Y={ Xx ∈ K, v(x)=0}is the set of inversible elements of O

O is a local ring (not necessarily Noetherian) and Y is the unique maximal ideal of O.

We omit the proof of this simple proposition.The field k=O/Y is known the residual field of the valuation v.

It is obvious form the proposition 2 that the valuation v of K which is a homomorphism form K* to r can be split up as follows

K* -U K*/O* -U rv-U r.

Notes

where v1 is the canonical homomorphism, v2 the map carrying an element xO* to v(x) and (v3) the inclusion map of rv into r.

Definition. Two valuations v and v of a field K are said to be equivalent if there exists an order preserving isomorphism u of rv onto T'v such that v=u o v.

From the splitting of the homomorphism v it is obvious that a valuation of a field K is completely characterized up to equivalence by any one of O, or Y.

A valuation of a field K is said to be real if rv is contained in R (the field for real numbers).Since any subgroup of R is either discrete i.e ., isomorphic to a subgroup of integers or dense in R, either rv is contained in Z or rv is dense in R.In the former case we say that v is a discrete valuation and in the latter non-discrete.Moreover v is com- palely determined up to a real constant factor, because if v and V are two non-discrete equivalent valuations of K, the isomorphism of rv onto r'v can be extended to R by continuity, which is nothing but multiplication by a element of R.If v and V are discrete and equivalent, the assertion is trivial.If rv=z we call v a normed discrete valuation.

Definition. Let K be a field with a normed discrete valuation v.In K we can find an element n with v (n)=1.The element n is known a uniform sing parameter for the valuation v.

Let K be a field with a normed discrete valuation v and O+(0) an ideal in O.Let a=inf (v(x)).Such an a exists because v (x)>0 xeO for every x in O.Moreover there exists an element x0 in O such that v(x0)=a, because the valuation is discrete.Then O=Ox0=On a For, x.x belongs to G ∈ >v (x)>v(xq) ∈ >K —)>0 ∈ >x/xq belongs x0.x to G ∈ >v belongs to Gxo.Since v{ —)=v(xq)- a\fn)=0, we get na that x0 is in Ona, conversely na belongs to Ox0 is obvious.Therefore O=Ona.In particular Y=On.In general let v be any valuation of a field K.Let O be any ideal of O and Ho={ a\a ∈ r, such that there exists x in O with v(x)=a }.Then the map O ^ Ho is a 1 - 1 correspondence between the set of ideals O in O and the subsets Ho of rv having the property that if a belongs to Ho and S belonging to rv is such that S>a, then S belongs to Ho.In particular if rv is contained in R, then the ideals of O are of one of the two kinds

I'a={ x|x $\in$ O, v(x)>a }

Ia={ x\x $\in$ O, v(x)>a} for any a>0.

Examples. Let Q be the field of rational numbers.For any m in Q we have m=± p0^ parruniquely, where a1, ..., ar are in Z and p1, ..., pr are distinct primes.If v is any valuation of Q,

we have v (m)=r

X ajv (pj).Therefore it is sufficient to define a valuation for primes in

j=1 Z.We note that for a valuation v there exists at most one p for which v (p)>0.If possible let us suppose that there exist two primes p1 and p2 such that v (pt)>0 for i=1, 2.

Since (p1, p2)=1, there exist two integers a and b such that ap1+ bp2=1.This implies that 0=v (1)>inf(v(ap1)), v(bp2))>0, whichis impossible.Thus our assertion is proved, If there does not exist any prime p for which v(p)>0, then v is improper.

For a prime p we define vp (p)=1 and vp(m)=a, where a is the highest power of p dividing m.It is easy to verify that this is a valuation of Q and any valuation of Q for which v (p)>0 is equivalent to this valuation.It is a discrete normed valuation of Q.One can take p as a uniform sing parameter and prove that the residual field is isomorphic to Z/(p)

Let K be any field, K((x)) the field of formal power series over

TO K.For any element f (x)= $\in$ arxr of K((x)) we define v(f(x))=t, r=m if at is the first non-zero coefficient in f(x).One an easily verify that v is a normed discrete valuation of K((x)).The ring of integers of the valuation is the ring of formal power series with non-negative exponents and the ideal is the set of those elements in the ring of integers for which the constant term is zero.One can take x as a uniform sing parameter.

Check your Progress-2

Discuss Locally convex k-vector spaces

____

____

____

4.4 VALUATION RINGS AND PLACES

This section is added for the sake of completeness.The results men tioned here will not be used in the sequel.

Remark.Let K be a field with a valuation v and ring of integers 0.7 Then for any x in K, either x belongs to O or x-1 belongs to O.

Motivated by this we define

A subring A of a field K is known a valuation ring of K if for any x in K either x belongs to A or x-1 belongs to A.

In general a ring A is said to be a valuation ring if it is a valuation ring for its quotient field.

4.5 LET US SUM UP

In this unit we have discussed the definition and exampleofTheory of valuations – I, Locally convex k-vector spaces, Valuation rings and places

4.6 KEYWORDS

Theory of valuations–I…..M is paracompact then is an isomorphism

Locally convex k-vector spaces…..A (nonarchimedean) seminorm on ∈ is a function q : ∈ —>Rsuch that for any v, w ∈ E and any a ∈ K

Valuation rings and places

4.7 QUESTIONS FOR REVIEW

Explain Theory of valuations-I

Explain Locally convex k-vector spaces

4.8 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

4.9 ANSWERS TO CHECK YOUR PROGRESS

Theory of valuations-I (answer for Check your Progress-1 Q)

Locally convex k-vector spaces (answer for Check your Progress-2 Q)

UNIT-5 :THE P-ADIC NORM AND THE P-ADIC NUMBERS

STRUCTURE

5.0 OBJECTIVES

After studying this unit, you should be able to:

- Understand about The P-Adic Norm And The P-Adic Numbers
- Understand about P-Adic Numbers And P-Adic Integers
- Understand about Completions

5.1 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 P-Adic Norm And The P-AdicNumbers, P-Adic Numbers And P-Adic Integers, Completions

5.2 THE P-ADIC NORM AND THE P-ADIC NUMBERS

Let R be a ring with unity 1=1 R.

Definition.A function

N: R —► R+={ r ∈ R : r ^ 0 }

is known a norm on R if the following are true.

(Na) N(x) =0 if and only if x=0.

(Nb) N(xy)=N(x)N(y)∀x, y ∈ R.

(Nc) N(x+y) ^ N(x)+N(y)∀x, y ∈ R.

Condition (Nc) is known the triangle inequality.

N is known a seminorm if (Na) and (Nb) are replaced by the following conditions in algebra and analysis.

(Na') N(1)=1.

(Nb') N(xy)<N(x)N(y)∀x, y ∈ R.

A (semi)norm N is known non-Archimedean if (Nc) can be replaced by the stronger statement, the ultra-metric inequality:

(Nd) N(x+y) ^ max{ N(x), N(y) }∀x, y ∈ R.

If (Nd) is not true then the norm N is said to be Archimedean.

Exercise: Show that for a non-Archimedean norm N, (Nd) can be strengthened to (Nd') N(x+y) ^ max{ N(x), N(y) }∀x, y ∈ R with equality if N(x)=N(y).

Example Let R C C be a subring of the complex numbers C.Then setting N (x)=|x |, the usual absolute value, gives a norm on R.In particular, this

Notes

applies to the cases R=Z, Q, R, C.This norm is Archimedean because of the inequality

|1+1|=2>|1|=1.

(ii) Let I=[0, 1] be the unit interval and let

C (I)={ /: I —>R : f continuous }.

Then the function |f |(x)=|f(x)|is continuous for any / ∈ C(I) and hence by basic analysis,

3x/ ∈ I such that |f |(x/)=sup{ |f |(x) : x ∈ I }.

Hence we can define a function

N: C (!) R+; N (f)=|f |(x,),

which turns out to be an Archimedean seminorm on C (I), usually known the supremum seminorm.This works upon replacing I by any compact set X C C.

Consider the case of R=Q, the ring of rational numbers a/b, where a, b ∈ Z and b=0.Suppose that p ^ 2 is a prime number.

Definition. If 0=x ∈ Z, the p-adic ordinal (or valuation) of x is

ordp x=max{ r : pr|x}^ 0.

For a/b ∈ Q, the p-adic ordinal of a/b

ordp a=ordpa —ordp b.b

Notice that in all cases, ordp gives an integer and that for a rational a/b, the value of ordp a/b is well defined, i. ∈ ., if a/b=a'/b' then

ordpa —ordp b=ordp a' — ordp b'.

We also introduce the convention that ordp 0=to.

Proposition. If x, y ∈ Q, theordp has the following properties:

ordp x=to if and only if x=0;

ordp (xy)=ordp x+ordp y;

ordp (x+y) ^ min{ ordp x, ordp y}with equality if ordp x=ordp y.

Proof.Let x, y

a c be non-zero rational numbers.Write x=pr-and y=ps -, where a, b, c, d

∈ Z with p \ a, b, c, d

r a c x +y =p (b+d)

b d

and r, s ∈ Z.Now if r=s, we have

a cN b+d/ (ad+bc)

r pr bd

which gives ordp (x+y) ^ r since p \ bd.

Now suppose that r=s, say s>r.Then

x+y=pr (a+p'-r d)

r (ad+ps-r bc)

= p bd.

Notice that as s — r>0 and p \ ad, then

ordp (x+y)=r=min{ ordp x, ordp y }.

The argument for the case where at least one of the terms is 0.

Definition. For x ∈ Q, let the p-adic norm of x be given by

(p-ordp x if x=0, lxlp=\I p ^=0 if x=0.

Proposition. The function ||p: Q —>R+ has the properties

|x|p=0 if and only if x=0;

Mp=Wy^;

|x+y|p ^ max{|x|p, |y|p }, with equality if |x|p=|y|p.Hence, ||p is a non-Archimedean norm on Q.

Let p be a prime and n ^ 1.Then from the p-adic expansion

n=no+nip+ +ngpg with 0 ^ n ^ p — 1, we obtain the number

ap (n)=no+ni +…..+ng.

Example. Then p-adic ordinal of n! is given by

ordp (n!) = |n!|p=p-(n-ap(n)) (p-i).

Proof.Observe the exercises.

Now consider a general norm N on a ring R.

Definition. The distance between x, y ∈ R with respect to N is

dw (x, y)=N(x — y) ∈ R+.

It easily follows from the properties of a norm that (Da)dN(x, y)=0 if and only if x=y;

(Db) dw(x, y)=dw(y, x)Vx, y ∈ R;

(Dc) dN(x, y) ^ dN(x, z)+dN(z, y) if z ∈ R is a third element.

Moreover, if N is non-Archimedean, then the second property is replaced by (Dd)dN(x, y) ^ max{ dN(x, z), dN(z, y)}with equality if dN(x, z)=dN(z, y).

Proposition.(The Isosceles Triangle Principle).Let N be a non-Archimedean norm on a ring R.Let x, y, z ∈ R be such that dN(x, y)=dN(z, y).Then dw (x, y)=max{ dw(x, z), dw(z, y) }.

Hence, every triangle is isosceles in the non-Archimedean world.

Now let (an)nyi be a sequence of elements of R, a ring with norm N.

n — ap(n)

dp (n!)=p — 1 :

Definition. The sequence (an) tends to the limit a ∈ R with respect to N if

Ve>0 3M ∈ N such that n>M =^ N (a — an)=dN(a, an)< ∈ .

We use the notation

lim (N)an=a n^^

Which is reminiscent of the notation in Analysis and also keeps the norm in mind.

Definition. The sequence (an) is Cauchy with respect to N if

Ve>03M ∈ N such that m, n>M =^ N (am — an)=dN(am, an)<e.

Proposition. If lim (N)an exists, then (an) is Cauchy with respect to N.

n^tt

Proof.Let a=lim (N)an.Then we can find a M\ such that

n^tt n>M\ =^ N(a — aU)<^.

If m, n>M\, then N(a — am)< ∈ / 2 and N(a — aU)< ∈ /2, hence by making use of the inequality from (Nc) we obtain

N (am — an)=N ((am — a)+(a — au))

^ N (am — a)+N(a — an)

∈ ∈ <2+2= ∈ .

Exercise: Show that in the case where N is non-Archimedean, the inequality

N (am — an)<^

Consider the case of R=Q, the rational numbers, with the p-adic norm |\p.

Example :.Take the sequence $a_n = 1 + p + p^2 + \cdots + p^{n-1}$.Then we have

$$\begin{aligned} |a_{n+k} - a_n|_p &= p^n + p^{n+1} + \dots\dots + p^{n+k-1} \\ &= p^n(1 + p + p^2 + \dots\dots + p^{k-1}) \end{aligned}$$

For each ε > 0, we can choose an M for which p^M “ 1/ε, so if n > M we have

$$|a_{n+k} - a_n|_p < \frac{1_{TM}}{P^M}\varepsilon$$

This shows that (a_n) is Cauchy.
In fact, this sequence has a limit with respect to $|\ |_p$.Take a = 1/(1 − p) ∈ Q; then we have

$a_n = \left(p^n - 1\right)/\left(p-1\right)$ hence,

$$a^n - \frac{1}{(1-p)^p} = \frac{p^n}{(p-1)_p} = \frac{1}{p^n}$$

So for $\varepsilon > 0$, *we have*

$$= a^n - \frac{1}{(1-p)^p} < \varepsilon$$

whenever n > M (as above).

From now on we will write $\lim^{(p)}$ in place of $\lim^{(N)}$.So in the last example, we have

$$\lim_{n\to\infty}(p)(1+p+......+p^{n-1}) = \frac{1}{(1-p)}$$

Again consider a general norm N on a ring R.

Definition : A sequence (a_n) is called a *null sequence* if it is complete with respect to N. $\lim\limits_{n\to\infty}^{(N)} an = 0$

Of course this assumes the limit exists! This is easily seen to be equivalent to the the fact that in the real numbers with the usual norm $|\ |$, $\lim_{n\to\infty}$N (a_n) = 0.

Example In the ring Q together with p-adic norm ||p, we have an=pn.Then

|pn|p=4t ^ 0 as n ^p pn

so lim (p)an=0.Hence this sequence is null with respect to the p-adicnorm.

n^<^

Example with an=(1+p)pn — 1.Then for n=1,

|ai|p=1 (1+ P)p — 1|

1j p+•••+(^ — 1)pp 1+pp

since for 1 ^ k ^ p — 1,

ordp(k1=1

Hence |a1|p=1/p2.

For general n, we proceed by induction upon n, and show that

|an|p=pn+i.

Hence we observe that as n ^ rc>, |an|p ^ 0, so this sequence is null with respect to the p-adic norm ||p.

Example.R=Q, N=||, the usual norm.Consider the sequence (an) whose nth term is the decimal expansion of \/2 up to the n-th decimal place, i. ∈ ., a1=1.4, a2=1.41, a3=1.414, etc.

Then it is well known that V2 is not a rational number although it is real, but(an) is a Cauchy sequence.

The last example shows that there can be holes in a normed ring, i. ∈ ., limits of Cauchy sequences need not exist.The real numbers can be thought of as the rational numbers with all the missing limits put in.

Let R be a ring with a norm N.Define the following two sets:

CS (R, N)=the set of Cauchy sequences in R with respect to N,

Null (R, N)=the set of null sequences in R with respect to N.

So the elements of CS (R, N) are Cauchy sequences (an) in R, and the elements of Null(R, N) are null sequences (an).Notice that

Null (R, N) C CS(R, N).

We can add and multiply the elements of CS (R, N), using the formulae

(an)+(bn)=(an+bn), (an) X (bn)=(anbn),

since it is easily checked that these binary operations are functions of the form

+, x : CS(R, N) x CS(R, N) CS(R, N).

Claim: The elements 0cs=(0), 1cs=(1r) together with these operations turn CS(R, N) into a ring (commutative if R is) with zero 0CS and unity 1CS.Moreover, the subset Null(R, N) is a two sided ideal of CS(R, N), since if (an) $\in$ CS(R, N) and (bn) $\in$ Null(R, N), then

(anbn), (bnan) $\in$ Null(R, N)

as can be observen by calculating lim (N)anbn and lim(N)bnan.

n^tt n^tt

We can then define the quotient ring CS (R, N)/Null(R, N); this is known the completion of R with respect to the norm N, and is denoted RN or just R if the norm is clear.We write{an}for the coset of the Cauchy sequence (an).The zero and unity are of course{0R}and{1R}respectively.The norm N can be extended to RN as the following important result shows.

Theorem. The ring RN has sum+and product x given by

{ an }+{ bn }={ an+bn{ an}X{bn }={ anbn },

and is commutative if R is.Moreover, there is a unique norm N on RN which satisfies ?V({ a })=N(a) for a constant Cauchy sequence (an)=(a) with a $\in$ R; this norm is defined by

^ ({ cn })=lim N(Cn) n^tt

as a limit in the real numbers R.Finally, N is non-Archimedean if and only if N is.

Proof.We will first verify that N is a norm.Let{an } $\in$ R.We should check that the definition of ?V({ an }) makes sense.For each $\in$ >0, we have an M such that whenever m, n>M then N(am, an)< $\in$ .To proceed further we need to use an inequality.

Claim:

|N (x) — N(y)|^ N(x — y) for all x, y $\in$ R.

Proof. By (Nc),

N (x)=N ((x — y)+y) ^ N(x — y)+N(y)

implying

N (x) — N (y) ^ N(x — y).

Similarly,

N (y) — N (x) ^ N(y — x).

Since N(— z)=N(z) for all z ∈ R (why?), we have

|N (x) — N(y)|^ N(x — y).

This result tells us that for ∈ >0, there is an M for which whenever m, n>M we have

|N(am)- N(a, n) |<e,

which shows that the sequence of real numbers (N(an)) is a Cauchy sequence with respect to the usual norm ||.By basic Analysis, we know it has a limit, say

∈ =limN (an).

n^tt

Hence, there is an M' such that M'<n implies that

| ∈ -N(an) |< ∈ .

So we have shown that fV ({ an })= ∈ is defined.

We have

W ({ an })=0 lim N(an)=0

n^tt

(an) is a null sequence {an }=0,

proving (Na).Also, given{ an}and{bn }, we have

N ({ an }{ bn })=N({ anbn })=lim N(anbn) n^tt

= limN (an)N(bn) n^tt

= limN (an)lim N(bn) n^tt n^tt

= W ({ an })W({ bn }),

which proves (Nb).Finally,

W ({ an }+{ bn })=lim N(an+bn) n^tt ^ lim (N(an)+N(bn)) n^tt

= limN (an)+lim N(bn) n^tt n^tt

= N ({ an })+N ({ bn }),

which gives (Nc).Thus N is certainly a norm.We still have to show that if N is nonArchimedean then so is N.We will use the following important Theorem.

Theorem Let R be a ring with a non-Archimedean norm N.Suppose that (an) is a Cauchy sequence and that b $\in$ R has the property that b=lim(N^an.Then there is an M such n^tt

that for all m, n>M,

N (am — b)=N (an — b)

so the sequence of real numbers (N(an — b)) is eventually constant.In particular, if(an) is not a null sequence, then the sequence (N(an)) is eventually constant.

Proof.Notice that

|N (am — b) — N(an — b)|^ N(am — an),

so (N(an — b)) is Cauchy in R.Let t=limn^^ N (an — b); notice also that t>0.Hence there exists an M1 such that n>M1 implies

N (an — b)>2 Also, there exists an M2 such that m, n>M2 implies

t

N (am — an)<^,

since (an) is Cauchy with respect to N.Now take M=max{ M1, M2}and consider m, n>M.Then

N (am — b)=N ((an — b)+(am — an))

= max{ N(an — b), N(am — a, n) }

= N (an — b)

since N (an — b)> ∈ /2 and N(am — an)<t/2.

Let{an }, {bn}have the property that

N ({ am })=N({ bm });

furthermore, we can assume that neither of these is{0 }, since otherwise the inequality in (Nd) is trivial to verify.By the Theorem with b=0 we can find integers M', M" such that

n>M' =^ N (an)=N({ an })

and

n>M" =^ N (bn)=N({ bn }).

Thus for n>max{ M', M" }, we have

N (an+bn)=max{ N (an), N (bn) }

= max{ fV({ an }), fV({ bn }) }.

This proves (Nd) for N

Definition.A ring with norm N is complete with respect to the norm N if every Cauchy sequence has a limit in R with respect to N.

Example. The ring of real numbers (resp.complex numbers)is complete with respect to the usual norm ||.

Definition. Let R be a ring with norm N, and let X C R; then X is dense in R if every element of R is a limit (with respect to N) of elements of X.

Theorem. Theorem: *Let* R *be a ring with norm* N. *Then* $\hat{R}$ *Moreover,* R *can be identified with a dense subring of* $\hat{R}$.

Proof. First observe that for a ∈ R, the constant sequence (a_n) = (a) is Cauchy and so we obtain the element {a} in $\hat{R}$; this allows us to embed R as a subring of $\hat{R}$ (it is necessary to verify that the inclusion $R \longleftrightarrow \hat{R}$ preserves sums and products). We will identify R with its image without further comment; thus we will often use a ∈ R to denote the element {a} ∈ $\hat{R}$.

It is easy to verify that if (a_n) is a Cauchy sequence in R with respect to N , then (a_n) is also a Cauchy sequence in $\hat{R}$ with respect to $\hat{N}$. Of course it may not have a limit in R, but it *always* has a limit in $\hat{R}$, namely the element {a_n} by definition of $\hat{R}$.

Now suppose that (an) is Cauchy sequence in R with respect to the norm N Then we must show that there is an element a ∈ R for which

$$\lim_{m\to\infty}{}^{(N)} \alpha_m = \alpha -----(1)$$

Notice that each am is in fact the equivalence class of a Cauchy sequence (amn) in R with respect to the norm N, hence if we consider each amn as an element of R as above, we can write

$$\lim_{m\to\infty}{}^{(N)} a_{nm} = \alpha_n -----(2)$$

We need to construct a Cauchy sequence (cn) in R with respect to N such that{ cn }= $\lim_{m\to\infty}{}^{(N)} \alpha m$

Then a={ cn}is the required limit of (an).

Now for each m, there is an Mm such that whenever n>Mm,

N (am -amn)< $\frac{1}{m}$

For each m we now choose an integer k (m)>Mm; we can even assume that these integers are strictly increasing, hence k (1)<k(2)< <k(m)< .

We define our sequence (cn) by setting cn=ank(n).We must show it has the required properties.

Definition. The ring of p-adic numbers is the completion Q of Q with respect to N=||p; we will denote it Qp.The norm on Qp will be denoted ||p.

Definition. The unit disc about 0 ∈ Qp is the set of p-adic integers,

Zp={ a ∈ Qp : |a|p ^ 1 }.

Proposition. The set of p-adic integers Zp is a subring of Qp.Every element of Zp is the limit of a sequence of (non-negative) integers and conversely, every Cauchy sequence in Q consisting of integers has a limit in Zp.

Example. Find

$(1/3 + 2 + 2 \cdot 3 + 0 \cdot 3^2 + 2 \cdot 3^3 + \cdots) + (2/3^2 + 0/3 + 1 + 2 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \cdots)$.

The idea is start at the left and work towards the right.Thus if the answer is

$$\alpha = a_{-2}/3^2 + a_{-1}/3 + a_0 + a_1 3 + \cdots,$$
$$a_{-2} = 2, \quad a_{-1} = 1, \quad a_0 = 2 + 1 = 0 + 1 \cdot 3 \underset{3}{\equiv} 0,$$

then $a_1 = 2 + 1 = 0 + 1 \cdot 3 \underset{3}{\equiv} 2$

where the 1 is carried from the 3^0 term.Continuing we get

$$a_2 = 0 + 1 + 1 = 2, \; a_3 = 2 + 1 = 0 + 1 \cdot 3 \underset{3}{\equiv} 0,$$

and so we get

$$\alpha = 2/3^2 + 1/3 + 0 + 2 \cdot 3 + 2 \cdot 3^2 + 0 \cdot 3^3 + \cdots$$

as the sum to within a term of 3-adic norm smaller than $1/3^3$.

Notice that the p-adic expansion of a p-adic number is unique, whereas the decimal expansion of a real need not be.For example

0.999 •••=1.000 •••=1.

We end this section with another fact about completions.

Theorem. Let R be field with norm N.Then R is a field.In particular, Qp is a field.

Proof. Let{an}be an element of R, not equal to{0 }.Then N ({ an })=0.Put

$\in$ =N ({ an })=lim N(an)>0.n^<^

Then there is an M such that n>M implies that N (an)> $\in$ /2 (why?), so for such an n we have an=0.

So eventually an has an inverse in R.

Now define the sequence (bn) in R by bn=1 if n ^ M and bn=a-1 if n>M.Thus this sequence is Cauchy and

lim (N)anbn=1, n^^

which implies that

{ an }{ bn }={ 1 }.

Thus{an}has inverse{bn}in RR

Check your Progress-1

Discuss The P-Adic Norm And The P-Adic Numbers

5.3 P-ADIC NUMBERS AND P-ADIC INTEGERS

In everything that follows, p is a prime number.The completion of Q with respect to |• |p is known the field of p-adic numbers, notation Qp.

The continuation of |• |p to Qp is also denoted by |• |p.This is a non-archimedean absolute value.Convergence, limits, Cauchy sequences and the like will all be with respect to |• |p.

Theorem.The value set of $|\cdot|_p$ on Q_p is{0}U{pm • m ∈ Z }.

Proof.Let x ∈ Qp, x=0.Choose a sequence{xk}in Q converging to x.For k sufficiently large we have xk=0 and thus, |xk|p=pmk for some mk ∈ Z.Clearly, |x|p=limk^^ pmk=pm for some m ∈ Z.

The ring of p-adic integers is defined by

Zp •={x ∈ Qp • |x|p ^ 1 }.

This is indeed a ring, since for any two x, y ∈ Zp we have \x-y\p ^ max(\x\p, \y\p) ^1, and \xy\p ^ 1.Hence x — y ∈ Zp and xy ∈ Zp.

The group of units, i. ∈ ., invertible elements of Zp is equal to

Zp={ x ∈ Qp : \x\p=1 }.

Notice that Zp contains Z, but also all numbers in Q with p-adic absolute value ^ 1, these are the rational numbers of the form a/b with a, b ∈ Z and b not divisible by p.Further, the group Z* contains all rational numbers with p-adic absolute value 1, these are the numbers of the form a/b with a, b ∈ Z and p \ ab.

For x, y ∈ Qp and m ∈ Z we write x=y (modpm) if (x — y)/pm ∈ Zp.Thus,

x=y (modpm)\x — y\p ^ p-m.

For p-adicnumbers, "very small" means "divisible by a high power of p", and two p-adic numbers x and y are p-adically close if and only if x — y is divisible by a high power of p.

The above definition applies also to rational numbers of the form a/b with a, b ∈ Z and p \ b since these are contained in Zp.It is not difficult to show that if ai, a2, bi, b2 are integers with p{ bib2 and m is a positive integer, then

ai=a2 (modpm), bi=b2 (modpm) =^ ^ (modpm).

b\ b2

Theorem. For every a ∈ Zp and every positive integer m there is a unique am ∈ Z such that

a=am (mod pm), 0 ^ am<pm.

Hence Z is dense in Zp.

Proof. There is a rational number a/b (with coprime a, b ∈ Z) such that \a — (a/b)\p ^ p-m since Q is dense in Qp.At most one of a, b is divisible by p and it cannot be b since \a/b\p ^ 1.Hence there is an integer am with bam=a (mod pm)and 0 ^ am<pm.Thus, a=a/b=am (modpm).This shows the existence of am.It is unique, since any residue class mod pm contains only one integer from{0, ..., pm — 1 }.

We prove some algebraic properties of the ring Zp.

Theorem.(i) The non-zero ideals of Zp are pmZp(m=0, 1, 2,...).In particular, pZp is the only maximal ideal of Zp.

(ii)Zp/pmZp=Z/pmZ.In particular, Zp/pZp=Fp.

Proof.(i).let I be a non-zero ideal of Zp and choose a ∈ I for which |a|p is maximal.Let |a|p=p-m.Then p-ma ∈ Zp, hence pm ∈ I.Further, for ft ∈ I we have |ftp-m|p ^ 1, hence ft ∈ pmZp.So I C pmZp.This implies I=pmZp.

(ii).The homomorphism Z/pmZ ^ Zp/pmZp: residue class of a mod pmZ residue class of a mod pmZp is injective since pmZp if Z=pmZ.It is also surjective in view.So it is an isomorphism.

We now show that every element of Zp has a "Taylor series expansion, " and every element of Qp a "Laurent series expansion" where instead of powers of a variable X one takes powers of p.

Theorem.(i) Every element of Zp can be expressed uniquely as^2kL0 bkpk with bk ∈ { 0, ..., p — 1}for k ft 0 and conversely, every such series belongs toZp.

(ii) Every element of Qp can be expressed uniquely as ^2fc=-ko bkpk with k0 ∈ Z and bk ∈ { 0, ..., p — 1}for k ft — k0 and conversely, every such series belongs to Qp.

Proof.(i).First observe that a series fc=0 bkpk with bk ∈ {0, ..., p — 1}converges in Qp.Further, it belongs to Zp, since |fc=0 bkpk|p ^ maxk^o|bkpk|p ^ 1.

Let a ∈ Zp and let{am }^=1 be the sequence.Write these integers in their p-adicexpansion.Since am+1=am (modpm)for m ft 1, we

have ai=b0, a2=b0+bip, a3=b0+bip+b2p2, ..., am=b0+bip+ hbm-ipm-1

where b0, bi,... ∈ { 0, ..., p — 1 }.It follows that

$$\alpha = \lim_{m\to\infty} \sum^{m} b_k p^k = \sum^{\infty} b_k p^k$$

This expansion is unique since the integers am are uniquely determined.

(ii).As above, any series fc=-ko bkpk with bk ∈ { 0, ..., p — 1}convergesin Qp.Let a ∈ Qp with a=0.Suppose that |a|p=pko.Then ft :=pkoa hasIft|p=1, so it belongs to Zp.Now multiply the p-adic expansion of ft with

Corollary Zp is uncountable.

Proof. Apply Cantor's diagonal method.

We use the following notation:

a=0.6061...(p) if a=Y, T=o bfc 'Pk,

a=6-ko 6-1.6061...(p) if a=Y!k=_ko bkPk with ko<0.

We can describe various of the definitions given above in terms of p-adic ex- pansions.For instance, for a ∈ Qp we have |a|p=p-m where a=ff=m 6kpk with 6k ∈ { 0, ..., p — 1}for k ^ m and 6m=0.next, if a=cf=0 akpk, P=Sfc=0 6 kPk ∈ Zp with ak, 6k ∈ { 0, ..., p — 1 }, then

a=P (modpm)ak=6k for k<m.

Notes

For p-adic numbers given in their p-adic expansions, one has the same additionwith carry algorithm as for real numbers given in their decimal expansions, except that for p-adic numbers one has to work from left to right instead of right to left.Likewise, one has subtraction and multiplication algorithms for p-adic numbers which are precisely the same as for real numbers apart from that one has to work from left to right instead of right to left.

We describe an algorithm to compute the digits of the p-adic expansion of a ∈ Zp.Let

a=^ 6kpk=0.606162 ...(p)

with 6k ∈ { 0, ..., p — 1 }.Define

ak :=^ 6mpm-k=0.6k6k+16k+2...(p)m=k

Then the p-adic integers ak and digits 6k can be computed inductively as follows: a0 := a;

For k=0, 1, ..., determine 6k such that ak=6k (mod p) and 6k ∈ { 0, ..., p — 1 }, and compute ak+1 :=(ak — 6k)/p.

Theorem.Let a=fc=-ko 6kpk with 6k ∈ { 0, ..., p — 1}for k p — k0.Then

a ∈ Q{6k }fc=_ko is ultimately periodic.

Proof.

=^ Without loss of generality, we assume that a ∈ Zp(if a ∈ Qp with \a\p=pko, say, then we proceed further with :=pk°a which is in Zp).

Suppose that a=A/B with A, B ∈ Z, gcd(A, B)=1.Then p does not divide B (otherwise \a\p>1).Let C := max(\A \, \B\).Let{ak } ∈ =0 be the sequence defined above.Notice that ak determines uniquely the numbers bk, bk+1,....

Claim.ak=Ak/B with Ak ∈ Z, \Ak \ ^ C.

This is proved by induction on k.For k=0 the claim is obviously true.Suppose the claim is true for k=m where m ^ 0.Then am bm (Am bmB)/p

am+1 7^.

pB

Since am=bm (mod p) we have that Am — bmB is divisible by p.So Am+1 := (Am — bmB)/p ∈ Z.Further,

\Am+11<C+(p — 1)B<C.

This proves our claim.

Now since the integers Ak all belong to{ — C, ..., C }, there must be indices l<m with Ai=Am, that is, ai=am.But then, bk+m-1=bk for all k ^ l, proving that{bk }^=0 is ultimately periodic.

Example.We determine the 3-adic expansion of — ^= — | 3-3.We start with the 3-adic expansion of —|.Notice that |=2a (mod 3) for a ∈ Z.

k 0 12 3 4

a, — 2 — 4 _ 3 _1 — 2

"k 5 5 5 5 5

bk 2 1 0 1 2

It follows that the sequence of 3-adic digits{bk } ∈ =0 of — |is periodic with period 2, 1, 0, 1 and that 2 _

— 5 =

= 0.21012101...(3).

Hence

2

=210.12101210 ...(3).

135 v 7

Conversely, we can recover the rational number from its expansion.Check that if \x\p<1 then 1+x+x2+ =1/(1 — x).Thus,

210.12101210 ...(3)

= 2 x 3-3+1 x 3-2+0 x 3-1 +

+ (1 x 30+2 x 31+1 x 32+0 x 33)(1+34+38+) 5 16 2

= 27+1 — 34= — 135.

5.4 COMPLETIONS

An absolute value preserving isomorphism between two fields K^K2 with absolute values|.|i, |.|2, respectively, is an isomorphism<p : K1 ^ K2 such that |<^(x)|2=|x|1 for x ∈ K1.

Let K be a field, |.|a non-trivial absolute value on K, and{ak } ∈ =0 a sequence in K.

We say that{ak } ∈ =0 converges to a with respect to|.|iflimk^^ |ak — a|=0.Further, {ak } ∈ =0 is known a Cauchy sequence with respect to|.|if limm, ra^^ |am an|0.

Notice that any convergent sequence is a Cauchy sequence.

We say that K is complete with respect to|.|if every Cauchy sequence w.r.t .|.|in K converges to a limit in K.For instance, R and C are completew.r.t.the ordinary absolute value.

By mimicking the construction of R from Q, one can show that every field K with an absolute value can be extended to an essentially unique field K, such that K is complete and every element of K is the limit of a Cauchy sequencefrom K.

Theorem. Let K be a field with absolute value|.|.There is an up to absolute value preserving isomorphism unique extension field K of K, known the completion of K, having the following properties:

I |can be continued to an absolute value on K, also denoted|.|, such that K is complete w.r.t .|.|;

K is dense in K, i. ∊ ., every element of K is the limit of a sequence from K.

Proof. We give a sketch.Cauchy sequences, limits, etc.are all with respectto 1 |.

The set of Cauchy sequences in K with respect to |- |is closed under termwise addition and multiplication{an }+{ bn}:={ an+bn }, {an}{bn}:={ an bn }.With these operations they form a ring, which we denote by R.It is not difficult to verify that the sequences{an}such that an ^ 0 with respect to|.|form a maximal ideal in R, which we denote by M.Thus, the quotient R/M is a field, which is our completion K.

We define the absolute value |a|of a ∊ K by choosing a representative {an}of a, and putting |a|:= limn^^ |an |, where now the limit is with respect to the ordinary absolute value on R.It is not difficult to verify that this is well-defined, that is, the limit exists and is independent of the choice of the representative{an }.

We can view K as a subfield of K by identifying a ∊ K with the element of K represented by the constant Cauchy sequence{a }.In this manner, the absolute value on K constructed above extends that of K, and moreover, every element of K is a limit of a sequence from K.So K is dense in K.One showsthat K is complete, that is, any Cauchy sequence{an}in K has a limit in K, by taking very good approximations bn ∊ K of an and then taking the limit of the bn.

Finally, if K' is another complete field with absolute value extending that on K such that K is dense in K' one obtains an isomorphism from id to K' as follows: Take a ∊ K.Choose a sequence{ak}in K converging to a; this is necessarily a Cauchy sequence.Then map a to the limit of{ak}in K'.

Corollary. Assume that | |is a non-archimedean absolute value on K.Then the extension of|.|to K is also non-archimedean.

Proof. Let a, b ∈ K.Choose sequences{ak }, {bk}in K that converge to a, b, respectively.Then taking the limit of |ak+bk|^ max(|ak |, |bk|) gives |a+b|^ max(|a |, |b|).

Ostrowski proved that any field complete with respect to an archimedean absolute value is isomorphic to R or C.As a consequence, any field that can be endowed with an archimedean absolute value is isomorphic to a subfield of C.On the other hand, there is a much larger variety of fields with a non-archimedean absolute value.

It is possible to define notions such as convergence, continuity, differentia-bility, etc.for complete fields with a non-archimedean absolute value similarly as for R or C, and this leads to non-archimedean analysis.One of the striking features of non-archimedean analysis is the following very easy criterion for convergence of series.

Theorem. Let K be a field complete w.r.t.a non-archimedean absolute value|.|.Let{ak } ∈ =0 be a sequence in K.Then fc=o ak converges in K if and only if limk^^ ak=0.

Proof. Suppose that a := ^0 ak converges.Then

n n— 1

an "y]ak y] ak ^ a — a=0.

k=0 k=0

Conversely, suppose that ak ^ 0 as k ^<x>.Let an := n=0 ak.Then for any integers m, n with 0<m<n we have

|an am|1 ∈ ak|^ max(|am+1 |, ..., |an|) ^ 0 as m, n ^ ^.k=m+1

So the partial sums an form a Cauchy sequence, hence must converge to a limit in K.

Corollary.Let K be a field complete w.r.t.a non – archimedean absolute value|.|.Then the sequence{ak } ∈ =0 converges in K if and only if lim (ak — ak — 1)=0.k^^

Proof. Apply Theorem to the series Jk=0 bk where b0 := a0 and bk := ak — ak — 1 for k ^ 1.

Theorem. Let again K be a field complete w.r.t.a non-archimedean absolute value|.|.Then every series Jk=0 ak convergent in K w.r.t .|.|is unconditionally convergent, i. ∈ ., neither the convergence, nor the value of the series, are affected if the terms ak are rearranged.

Proof. Let a be a bijection from Z^0 to Z^0.We have to prove that

Efc=0 aCk)= _0 ak, or equivalently, that SM ^ 0 as M ^ ro, where

c.y^M n _ y^M n

SM •=2_^k=0 ak k=0 a^ (fc)-

Let e>0.There is N such that |ak |< ∈ for all k ^ N.Choose N ∈ such that {a(0), ..., a(N ∈)}contains{0, ..., N }.Then for every M>N ∈ , Sm contains only terms ak with k>N and aa(k) with a(k)>N.Hence each term in SM has absolute value< ∈ and therefore, by the ultrametric inequality, |SM |< ∈ .This proves our Theorem.

For interchanging two infinite summations we have the following criterion:

Theorem. Let K be a field complete w.r.t.a non-archimedean absolute value |- |.Let{amn }^n=0 be a double sequence such that limmax(TO, ra)^TO amn=0.Then both the expressions

co \ 00/00

J] I J] amnI, J] (J] am

m=0 \n=0/n=0 \m=0

converge and are equal.

Check your Progress-2

Discuss P-Adic Numbers And P-Adic Integers

___

___

___

5.5 LET US SUM UP

In this unit we have discussed the definition and exampleofThe P-Adic Norm And The P-Adic Numbers, P-Adic Numbers And P-Adic Integers, Completions

5.6 KEYWORDS

The P-Adic Norm And The P-Adic Numbers….A functionN: R — ► R+={ r ∈ R : r ^ 0 }is known a norm on R

P-Adic Numbers And P-Adic Integers…..The completion of Q with respect to |• |p is known the field of p-adic numbers, notation Qp.

Completions…..An absolute value preserving isomorphism between two fields K^K2 withabsolute values |.|i, |.|2, respectively, is an isomorphism<p : K1 ^ K2

5.7 QUESTIONS FOR REVIEW

Explain The P-Adic Norm And The P-Adic Numbers

Explain P-Adic Numbers And P-Adic Integers

5.8 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

5.9 ANSWERS TO CHECK YOUR PROGRESS

The P-Adic Norm And P-Adic Numbers

(answer for Check your Progress-1 Q)

P-Adic Numbers And P-Adic Integers

(answer for Check your Progress-2 Q)

UNIT -6 :THEORY OF VALUATIONS-II

STRUCTURE

6.0 OBJECTIVES

After studying this unit, you should be able to:

- Understand about Theory of valuations–II
- Understand about Complete algebraic closure of a p-adic field
- Understand about Valuations of non-commutative rings

6.1 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.

Theory of valuations–II, Residual degree and ramification index, Complete algebraic closure of a p-adic field, Valuations of non-commutative rings

6.2 THEORY OF VALUATIONS -II

Hensel's Theorem

In this section we give a proof of Hensel's Theorem and deduce certain corollaries which will be used quite often in the following.In this section by a ring we mean a commutative ring with unity It can have zero divisors

Definition. Let A be a ring.Two elements x and y in A are said to be strongly relatively prime if and only if Ax+Ay=A i.e.if and only if there exist two elements u and v in A such that ux+vy=1.

In particular if k[x] is the ring of polynomials over a filed k then any two elements in k[x] are strongly relatively prime if and only if they are coprime in the ordinary sense.

It is obvious that if xand y are two strongly relatively prime elements in a ring A, then for any z in A x divides yz implies that x divides z.

Theorem Let P and P be two polynomials with coefficients in a ring A such that P is monic and P and P are strongly relatively prime.Let us assume that degree P=d (P)=s and d(P)=s.Then for every polynomial Q in A[x] there exists one and only one pair of polynomials U and V such that

Q=UP+VP with d (V)<s and for every t>S, d(Q)<t+s if and only if d(U)<t.

Proof. The existence of one pair U and Vsuch that Q=UP+VP is trivial.If d (V)>s, we write V=AP+Bwhere d(B)<s, which is possible because P is a monic polynomial, so we get

q=(U+A).P+BP'withd (B)<s.

Thus we can assume in the beginning itself that d(V)<s.If possible let there exists another pair U and V' such that

Q=UP+VP, d(V')<s.

Then

UP+V'P=UP+VP implies that (U - U')P=(V' - V)P.

But P and P are strongly relatively prime, therefore P divides V' - V.Since d (V - V)<s, V' - V=0.This implies that P (U- U)=0.As Pis monic we must have U=U.Let d (Q)<t+s.Then d (UP)= d(Q - VP).But d (V)<s and d(P)=s<t, therefore d(UP)<t+s, which implies that d(U)<t because Pis a monic polynomial of degrees.It is obvious that d(V)<t(t>s) implies that d(Q)<t+s.

Definition. Let A be a ring, the intersection of all the maximal ideals is known the radical of A and shall be denoted by r(A).

It can be easily proved that any element x of A belongs to r (A) if and only if 1-xy is invertible for all y ∈ A.

Theorem. Let A be a ring O an ideal in A contained in r (A).Then two polynomials P and P in A[x] ane of which (say P) is minic are strongly relatively prime if and only if P and P (the images of P and P in A/ O[x]) are strongly relatively prime.

Proof.P and P are strongly relatively prime implies Pand P are strongly relatively prime is obvious. Suppose that d (P)=s and d(P)=s.Then d (P)=d(P)=s, because Pis monic.Let ∈ ={f\ f ∈ A[x], d(f)<s+t, for some t>s }.Then ∈ is a module of finite type over A.Let ∈ = ∈ /OE, since P and P are strongly relatively prime in A/O[x], E' is generated by the polynomials XuP and XvP for 0<u<s.For, byTheorem 1 for every polynomials Q in ∈ there exists one only one pair of polynomials U and Fin A/ O[X] such that

Q=UP+FP d (V)<t+s.

But d(Q)<t+s, therefore d(U)<t.Thus

U=^ ax X\ 0<u<t

V=^ bMXL, 0<v<s ^=0

and Q= ∈ ax (XxP)+ ∈ (XP).

X=0 ^=0

By a simple corollary of Nakayama's Theorem (For proof observeAlgebre by N.Bourbaki) which states that if ∈ is a module of finite type over a ring A and q and ideal in r(A) then if (a1, ..., an) generate ∈ module qE, they generate ∈ also, we get XuP and XvP for 0<u<t and 0<v<s constitute a set of generators for ∈ .Therefore because 1 belongs to ∈ .Hence P and P are strongly relatively prime in A[X].

Let A be a ring with a decreasing filtration of ideals (On)n>0, defin- ing a topology on A for which A is a complete Hausdorff space.If

TO

f (X)=X anXn is a power series over A converging everywhere in A

then Xn(f)=sup (i)

(Xn(f)<to, because an ^ 0 as n ^ to) is an increasing function of n i. ∈ ., Xn(f)<Tn+1(f) and f(x) is a polynomial if and only if Xn(f) is constant for n sufficiently large.

We shall denote by f the image of f in A/O1[X].

Hensel's Theorem.Let A be a ring with a decreasing filtration of ideals (On)n>0.Let A for this topology be a complete Hausdorffspace.If

TOf (X)=D anXn is an everywhere convergent power series over A and if

n=0there exist two polynomial fi and f an A/O1 [X] such that

fi is monic of degree 5fi and f are strongly relatively prime

f=fif then there exists one and only pair (g, h) such that

g is a monic polynomial of degree 5 in A[X] and g=fi.

h is everywhere convergent power series over A and h=if.

f=gh Moreover An (h)=An(f)- 5.If f is a polynomial then h is a polynomial and g and h are strongly relatively prime.

Proof. Exi5tence We construct two sequences of polynomials (gn) and (hn) an A[X] by induction on n such that

(a)gn is monic of degree s, gn=fi and gn+1=gn(mod On+i)for n>0 (S)hn=f, hn+1=hn(mod On+i) and d(hn)=An+l(f)- 5 (y) f=gnhn(mod On+i), n>0 5-1

For n=0, we take go= ∈ arXr+Xs if

r=0 5-1 t

fi=^ grX+X5 and ho=^ buX" if

r=0 u=0 0=^ buXu, with t=d(0)=d(f)- s=A1 (f)- s.

Let us assume that we have constructed the polynomials g1, g2 • • • gn-1 and h1, ..., hn-1 satisfying the conditions (a), (S), and (y) By gn-1 and hn-1 are strongly relatively prime modulo Oq for every integer q>1, becausegn-1 and hn-1 are strongly relatively prime

in A/O1[X]=A/O i [X] and O1/Oq is contained in r(A/Oq), everyq O1 /Og element of O1/Og being nil potent.Therefore there exist polynomials Xn and Yn in A (X) such that

f -gn-1 hn-1=Yngn-1+Xnhn-1 (mod On+1) and d(Xn)<s.

But by induction assumption f -gn-1 hn-1=0 (mod On) therefore 0=Yngn-1+Xnhn-1 (mod On).Thus from the uniqueness part we get Xn=0 (mod On) and Yn=0(On).We take gn=gn-1+Xn and hn=hn-1+Yn obviously the polynomials gn and hn satisfy the conditions (a), (S) and (y).Hence we get two sequences of polynomials (gn) and (hn).The respective coefficients of (gn) and (hn) converge as n tends to infinity because of the condition gn+1=gn(mod On+1) and hn+1=hn(mod On+1).Therefore limgn=g is a monic polynomial n^ro of degree s and limhn=b is power series over A which converges even— erywhere in A, because h=hn(mod On+1).We observe immediately that f=gh h=0 and g=(p.Moreover An(h)=d(hn)=An(f)- s, because h=hn(mod On+1) =^ An+1(h)=An+1 (hn)=d(hn)<An+1 (f)- s but f=gh implies that An+1 (f)<s+An+1 (h), therefore we get our result.If fis a polynomial then An(f) is constant for n sufficiently large implying An(h) is constant for n large, therefore h is a polynomial.Since gn and hn are strongly relatively prime modulo On+1, there exist by Theorem polynomials an and bn such that

1=angn+bnhn (mod On+1), where d(bn)<s and d(an)<d(hn)=An+1(f)- s.

Similarly we have polynomials an+1 and bn+1 such that

1=an+1gn+1+bn+lhn+l (mod On+2) where d(bn+0<5 and d(an+0<d(hn+0=AnM f)- s.

Combining these two we get

(an+1 - an)gn+(bn+1 - bn)hn=0 (mod On+1)

Hence by uniqueness if we get an+1=an (mod On+1) and bn+1=bn (mod On+1).Since d (bn)<s for every n, we get that lim bn=b is a polynomial, moreover lim an=a is everywhere convergent power series in A; a is a polynomial if f is a polynomial.Hence we get 1=ag+bh (mod On+1) for every n>1, which implies that g and h are strongly relatively prime in A [[A]].

Uniqueness If possible let us suppose that there exists another pair (g, H) satisfying the requirements of the Theorem.Let V=h -h and U=g - g.Since g=g=(p and h=h=if, U is in O[X] and V is in O1[[A]].

Let us assume that Ubelongs to On[X] and Vbelongs to On[[X]] for

all n<m, m>1.We have

f=gh=g H=(U+g) (V+h)=UV+Uh+gV+gh

which implies that -UV=Uh+gV.But UV is in O2n-2[[X]](2n - 2> n, as n>1), therefore

Uh+gV=0 (mod On)

Let pn be the canonical homomorphism from OnA[[X]] onto A/On [[A]].Obviously we have

Pn(U)pn(h)+pn(g)pn(V)=0, d(U)<S

But pn(h) and pn(g) are strongly relatively prime in AOn[[X]], be- cause they are so in A/O1[[X]] and O1/On is contained in r(A/On), therefore by uniqueness part we get from

pn (U)=0 andpgV)=0

This means that V=h — h=0 (mod On) and U=g — g=0 (mod On) for every n.But nOn=0, because A is a Hausdorff space, therefore U=0 and V=0.Hence the uniqueness of g and h is established.

Corollary 1.Let K be a complete filed for a real valuation v.

Let f (X) =

TO

Y anXn be an every-where convergent powerseries with coefficient from

n= 0

O.Let p and(be two polynomials in O/Y[X]=k[X] such that

p is monic of degree s.

p and(are strongly relatively prime in k[X]

f (image of f in k[X])= p

Then there exists one and only one pair g and h such that

g $\in$ O [X], g is monic of degree s and g=p

h $\in$ O[X], h converges everywhere in O and h=f=gh.

and the radius of convergence of h is the same as that of f.If f is a polynomial, then h is a polynomial.Moreover g and h are strongly relatively prime.

s — 1 t —

Proof. Suppose that p=Y arX+Xs and (=Y b>uXu.

r=o u=0

s-1 t

Let p0=Z arXr+Xs, ifi0u= ∈ auXu.

r= 0 u= 0

for every n.Let a=inf v (bn), a is obviously strictly positive.Let

={x"/x ∈ O, v(x)>a }, then (On)n>0, On=O((defines a decreasingfiltration on O.Obviously p0 and (0 (images of p and (in O/O[X]) are strongly relatively prime modulo O1 and p0 and (0 satisfy all the requirements of Hensel's Theorem, therefore there exists one and only one pair (g, h) such thatg is monic polynomial of degree 5 and g=p◦

h is an every where convergent powerseries in O, h=g0 and

An(f) – 5 f=gh

Form the choice of p0 and g0 it is obvious that this pair (g, h) satisfies the conditions of the corollary.If possible let there exist another pair (g, h') satisfying the conditions stated in the corollary.Let g'=g-g, h"=h- h Since g' and h" are in Y[x], there exists a'>0 such that g' and h" are in O' [[x]] where O{ ={ x|x ∈ O, v(x)>a' }.

Let us take in Hensel's Theorem instead of O the ideal O1 and the filtration defined by (On) where On=On.But then have two pairs (g, h) and (g, h) satisfying the conditions (a), (b), (c) of the Theorem, which is not possible, therefore g=g and h=h.

If f is a polynomial, the result about radius of convergence is obvious. Let us assume that f is not a polynomial, then An(f) tends to infinity

as n tends to infinity.It has already been proved that tf=lim, inf Since v is a real valuation, for any i we can find an integer k such

that (A-- 1)a<gag<ka, =>Agf).Therefore ^i 2k (f)

Corollary. Let K be a complete valuated field with a real valuation v and f a polynomial in O [X].Then if a in k is a simple root of f, there exists one and only one element a in O such that a is a simple root of f and a=a.

Proof. Since a is a simple root of f, we have f(X)=(X-a) f(X) where f(a)=0.Moreover (X - a) and f(X) are strongly relatively prime in k[X \, (X - a) being a prime element.Therefore form corollary 1, we have in one and only one way f(X)=(X - a)h(X), where h=if and a=a.Moreover a is a simple root of f because

h (a)=h(a)=f(a)=0.

In particular if K is a locally compact field such that characteristic k+2, then we shall show that K*/(K*)2 is a group of order 4.

K locally compact implies that vis discrete and k is a finite.Let n be 34 a uniformising parameter and let C ∈ O*=O -Y be an element such that C is not a square in k, such an element exists because k*/(k*)2 is of order 2.Then it can be observen that 1, C, n, Cn represent the distinct cosets in K*/(K*)2 and any element in K* is congruent to one of them modulo (K*)2.

Extension of Valuations -Transcendental case

In order to prove that a valuation of a field can be extended to an extention field it is sufficient to consider the following two cases: When the extension field is an algebraic extension.When the extension field is a purely transcendental extension.

Proposition 1. Let L=K (X) be a purely transcendental extension of a field K with a valuation v, let r' be any totally ordered group containing rv.Then for ^ in r' there exists one and only one valuation of L extending v such that

$$w_{\xi}\left(\sum_{j=0} a_j x^j\right) = \inf_{0\le j\le n}\left(v(a_j) + j\xi\right)$$

Proof. It is sufficient to verify that w% satisfies the axioms of a valuation for K[X\.

The axioms a% (P)=m P=0 and w%(P+Q)> inf(w%(P), w%(Q)) can be easily verified.

To prove w% (PQ)=w%(P) +

w%(Q), where P= ∈ ajXJ, j=0

Q=Y biXi and PQ+0, we write P=Pi+P2, Q=Qi+Q2, Pi

being the sum of all terms ajXJ of P such that w% (P)=v(aj)+j% and Qi being the sum of those terms biXi of Q for which w%(Q)=v(bi)+i%.Let jo and ko be the degree of Pi and Qi respectively.If Pi Qi=Y CrXr, then we have

w% (Pi Qi)=v(Cjo+ko)+%(jo+ko)

= v (ajo)+%jo+v(bko)+%ko=w% (Pi)+w% (Qi).

Now

w% (PQ)=w%(Pi Qi+Pi Q2+QiP2+P2 Q2)=W%(Pi Qi), because the valuation of the other terms is greater than w%(Pi Qi).This implies that

w% (PQ)=w%(Pi Qi)=w%(Pi)+w%(Qi)=w%(P)+w%(Q).

Corollary. There exists one and only one valuation w of K (X) such that

w extends v.

w (X)=0.

The class X of X in kw is transcendental over kv.

The valuation w is the valuation w% for %=0 and kw is a purely transcendental extension of degree i over kv.It is obvious that wo (i. ∈ .w% for %=0)satisfies (i) and that kwo=kv(Xn).If Xfwere algebraic over kv, then there exists a polynomial

P (Y)=Y ajYj such that at least one aj ± 0 and P(X)=0, which means that P (X)=X ajXJ is in Yw, where at least one aj is not in Yv and all

aj are in Ov.But this is impossible because w (P(X))=inf v(aj)=0.

Conversely let w be a valuation of K (X) satisfying.Let P =m

Z aiXi be a polynomial over K.We have to prove that w (P)=inf v(ai).

Let P=Z a^X1 be a polynomial over K.We can assume without loss

of generality that aj are in Yv and at least one of them is not in Yy, then inf v(a1)=0.If w (P)>0, then P=0 in kw, which implies, that X is

algebraic over kv, which is a contradiction.But we know that

therefore w (P)=inf v(a1).

Check your Progress-1

DiscussTheory of valuations–II

____

____

____

6.3 RESIDUAL DEGREE AND RAMIFICATION INDEX

Let L be a field and K a subfield of L.Let wbe a valuation of L and vthe restriction of w on K.Since Yw n K=Yv, the filed kv can be imbedded in the field kw.We shall say the dimension of kw over kv the residual degree of w with respect to v or of L with respect to K.We shall denote it by f (w, v).

The index of the group rv in rw is known the ramification index of w with respect to v or of L with respect to K and is denoted by $\in$ (w, v).

If no confusion is possible, we shall denote f(w, y) by f(L, K) and $\in$ (w, v) by $\in$ (L, K).

If $\in$ (w, v)=1, then L is said to be an unramified extension of K.

If f (w, v)=1, L is said to be totally ramified extension of K.

Since the group of values and residual field of K are the same as that of K we have ∈ (L, K) = ∈ (L, K) and f(L, K)=f(L, K)

Proposition. Let L be a filed with a valuation w and let K be a field contained in L and v the restriction of w on K.Then ∈ (L, K) f(L, K)< (L : K)=n, where (L : K) is dimension of L over K.

Proof. If n is infinite, the result is trivial.Let us assume that n is a finite number.Let r< ∈ and s<f be two positive integers, then we can find r elements X1,.._L, Xr in L* such that w(Xi) ∈ w(Xj)(mod r v) for i ± j and s elements Y1,...Ys in kw such that they are linearly independent over kv.Let Y1,...Ys be a system of representatives for Y1,...Ys in O*.Then the elements (XiYj, i=1, ..., r; j=1, 2,...s)are linearly independent over K.If they are not linearly independent, then there exists elements aij in K not all 0 such that

Z *ilXiYl=0

Let a=inf w (aijXiYj), obviously a is finite and belongs to Tw.

Therefore w (akjXkYi)=a for some k and l.We have

w (aijXjYj)=w(ajj)+w(X)+w(Yj)

= w (akl)+w(Xk)+w(Yl) if w(aijXiYj)=a for some i and j.

But w (Yj)=w(Yi)=0, therefore we get w(Xi)=w(Xk)(mod rv), which is possible only if i=k.Thus we get

aklXkYl+^ akjXkYj=0 (mod O') j*l

where O'={ X/X ∈ L, w(X)>a }

Multiplying the congruence with a— X-1 we get

Yl+^ a- akjYj=0 (mod Yw).j*l

Therefore

Notes

Y+^ (a~lakJ)Yj=0, where a' }akJ are in kv.j*l

But this is impossible, because Y1 Ys are linearly independent over

kv, therefore(XiYj) are linearly independent over K.Since (L : K)=n, the number of linearly independent vectors in L over K cannot be greater than n.

Hence ef<n.

Corollary If L is algebraic over K, then kw is algebraic over kv and rl/rk is a torsion group of order<(L : K).

The assertion is trivial when (L : K) is finite.When (L : K) is infinite we can write L=IJ Li and kL=Uku, where Li is a finite

Algebraic extension of K.

Then rL/rk is the union of the quotient groups rp/rk for i in I and therefore it is a torsion group.

Corollary Suppose that L is algebraic over K, then w is improper if and only if v is improper-.vimproper implies that rv={ 0 }.Therefore by corollary rw is a torsion group.But rw is a totally ordered and abelian group, therefore it consists of identity only.

Corollary. Let (L : K) be finite.Then w is discrete if and only v is discrete.vdiscrete implies that rv is isomorphic to Z and (L : k) finite implies rw/rv is of finite order.Moreover rw is Archimedian, because if a and S are in rw, then na and nfi where n=order rw/rv, are in rv; therefore there exists an integer q such that qna>nfi, which shows that qa>fi.There exists a smallest positive element in rw.For, eachcoset of rw/rv has a smallest positive element, the smallest among them is the smallest positive element forw.Hence rw is isomorphic to z.

Corollary If the valuation v on K is discrete, K is complete and (L : K) is finite, then ef=(L : K).

Proof. Let n be a uniformising parameter in L.Let Y1, ..., Yf be a basis of kw over kv and Y1;..., Yf their representatives in O*w.Let R denote a system of representatives of kv in OW

Then any element Xin Ow can be written in the form ai Yj modulo

YW with a ∈ R in one and only one way.Let L' be vector space over K generated by (Yinj) for i=1, 2, ..., f and j=0, 1, 2, ..., ∈ - 1.

Since L' is a finite dimensional vectorspace over a complete field K, L' is complete (for proof observeEspacesVectorielsTopologiques by N.Bourbaki)and therefore closed in L.

But L' is dense in L, because for every element X in L and an integer n there exists an element Xn is L' such that v(X -Xn)>n ∈ .For sufficiently small n the result is obviously true.

Let us assume that it is true for all integers r<n.Since n ∈ is in rv, there exists an element U in K such that w(U)=v(U)=ne.Therefore U-1 (X-Xn) belongs to Ow and we have

U-1 (X -Xn)=^ ajoYj(mod YW=Own)

This means that n-1[(U-1(X-Xn)- ∈ iaioYi] belongs to OW, therefore (U 1 (X -Xn)- ^ aio Yi)=^ an Yi (mod YW)

Proceeding in this way we obtain

U-1 (X-Xn)= ∈ aioYi+•••+ ∈ aie-1 Yne-1 (mod YW)

H Haij-Yi^.j=0 i '

Then w (X - Xn+1)>(n+1) ∈ .Thus L' is dense in L and therefore L'=L.So n=(L : K)<ef.But we know that ef<n, therefore

n = ∈ f.

Locally compact Fields

Proposition.If K is a locally compact filed of characteristic o with a discrete valuation v, then K is a finite extension of Qp where p is characteristic of the residual field k.

Proof.Since characteristic K=0, K contains Q the field of retinal numbers.We observe immediately that v is proper, because if v is improper then Q is contained in k which is a finite field by theorem in §7.1 and this is impossible.The restriction of v to Q is vp for some p because p adic valuations are the only proper valuations on Q and this p is the characteristic of k.We have already proved in §7.1 that K is complete, therefore K contains Qp.The valuation v on K is discrete, thereforerv is isomorphic to Z, but rvp is also isomorphic to Z and is contained in rv, therefore=(Tv : rvp) is finite.Moreover f=(kv : kvp) is also finite, because kv is a finite filed.Hence (K : Qp) = ∊ f is finite.

Proposition. Let K be complete filed for a real proper valuation v such that characteristic K=characteristic k.k and all its sub fields are perfect.Then there exists a subfield F c O which is a system of representatives’ ofk in O.Moreover if v is discrete then K is isomorphic to k((x)).

Proof. Let O be the family of subfields S of O such that the restriction of p, the canonical homomorphism from O onto k to S is an isomor- phism onto a subfield of k.The family O ±<p, because the prime fields contained in O and k are the same.Obviously O is inductively ordered by inclusion, therefore by Zorn's Theorem it has a maximal element F.We shall prove that k=p (F).The field k is algebraic over p (F).If possible let there exist an element xin k transcendental over p (F).Let p (x)=x, where x is in O, then x is transcendental over F.It is obvious that F (x) is isomorphic to p(F) (x), which contradicts the maximality of F, therefore k is algebraic over p(F).Suppose that p (F), then there ex- ists one element x in k and not in p(F).Since p (F) is a perfect field, x is a simple root of an irreducible monic polynomial Plover p(F).Let

P=Xs+as-1 Xs-1++ ao=(X- x) Q, where Q is some polynomial

over p (F) and Q(x)+0.

By Corollary fo Hensel's Theorem we obtain that the polynomial P=Xs+as-1 Xs-1+ +a0 has a simple root x in O such that p (x)= x and Q is an irreducible polynomial.Therefore F (x) is isomorphic to F[X]/(P).But p (F) (x) is isomorphic to p(F)[X]/(P) therefore we observe that p is still an isomorphism from F(x) onto p(F) (x).But this is impossible, because F is a maximal element of O.Thus our theorem is proved.

Corollary.A non-discrete locally compact valuated field of characteristic p>o is isomorphic to a field of formal power series over a finite field.

Since a locally compact valuated field K is complete, its valuation is discrete and k is finite, our corollary follows from the theorem.

Extension of a Valuation to an Algebraic Extension (Case of a Complete Field)

Theorem. If L is an algebraic extension of a complete field K with a real valuation v, then there exists one and only valuation w on L extend- ing v.

Proof. If v is improper w is necessarily improper.So we assume that v is a proper valuation.Suppose that L is a finite extension of K.If there exists a valuation w on L extending v, then w is unique, because on L any valuation defines the same topology as that of KL:K) and the topology on L determines the valuation upto a constant factor and in this case the constant factor is also determined because the restriction of the valuation to K is v.

Let L be a Galois extension of K.Then if w is a valuation on L extending v, wo a for any a in G(L/K)(the Galois group of L over K) is also a valuation extending v.Therefore by uniqueness of the extension w (x)=Woa(x) for every x in L.This shows that

v (N(x))=w((x))=y wo a(x)=no w(x)

L/K V V

where (L : K)=n.

Thus

w (x)=- v(N(x)).

n l/k

Now suppose that L is any finite extension of K of degree n.We define a mapping w on L by and prove that it satisfies the axioms for a valuation.It is well known that (Bourbaki, algebra chapter V, that if L is the separable closure of K is L, and if p is the characteristic exponent of K (i. ∈ ., p=1 if characteristic K=0 and p= characteristic K+0), then

n=(L : K)=qpe

with q=(L' : K) and pe=(L : L').Moreover L is a purely inseparable extension of L', and for each K-isomorphism a (1<i<q) of L', in an algebraic closure O of K there exists one and only one K-isomorphism of L which extends ai.This extended isomorphism will also be denoted by ai.Then

rA pe

Nl/k (x)=[n a i(x)

It is easy to prove that w (x)=m if and only if x=0 and w(xy)= w(x)+w(y) for x, y in L.To prove that w (x+y)>inf(w(x), w(y)), it is sufficient to prove that w(a)>0 implies that w(1+a)>0 for any a in L.We know that if P(X)=Xr+ar-1 Xr-1+•••+ao is the monic irreducible polynomial of a over K, then N^a=(a0)? and P(\- X) is the irreducible polynomial of 1+a.Thus

LIK^+=+Sr_1+" '+(~iyao) }r=bo

So to prove our result we have to show that bo is in O when ao is

v (ao)n/r

in G, because w(a)= — -.This will follow from the following

theorem, which completely proves our theorem.

Theorem. Let K be complete field with a real valuation v and x any element of an algebraic extension of K.If f (X)=Xr+ar-iXr-1 +ao is the minimum polynomial of x over K, then ao belonging to O implies that all the coefficients of f(X) are in O.

Proof. If possible suppose that all at are not in O, then v(aj)<0 for some j, 0<j<r.Let -a=inf v(aj), a>0 and j the smallest index such that v(aj)=-a.We have o<j<r.Since a belongs to rv, there exists an element C in K such v (C)=a.Consider the polynomial g=Cf (X)=CXk+ +CajXj+ +C0a.Because of the choice of j, g= +rjXj, where rj=caj ± 0.Therefore g has Xj as a factor which is a monic polynomial and if g=Xjif, thenXj and ^ satisfy the requirements of Corollary of Hensel's Theorem, which gives that g is reducible, which is a contradiction.Hence all aj are in O.

When L is infinite algebraic extension of K, we can express L=U Li where each Li is a finite algebraic extension of K and the family ieI

{ LfifcI is a directed set by the relation of inclusion.We define the valuation w for any x in L as w (x)=w/x) if x is in Li and is the extension of v on Li.It is obvious that w is the unique valuation on L extending v.

General Case

We shall study now how a valuation of an incomplete field can be extended to its algebraic extension.

Let K be field with a valuation v and L an algebraic extension of K.If w is a valuation of L extending v, we can look at the completion L of L.L contains L and K, so it contains a well defined composite extension Mw of L and K.Then there exist one and only one maximal ideal mw in L K such that the canonical mapping from L K ^ Mw gives

an isomorphism from L<g>K/mw onto Mw.So we get a map (p from

the set of the valuation w extending v to the set of the maximal ideals of

L<g>K.Conversely if we start from a maximal ideal M in L<g>K, then

K K the corresponding composite extension M=L<g>K/M is an algebraic extension of K and there one and only one valuation wm of M which extends v and the restriction of wM to L gives a valuation of L extending v.So we get a map 0 from the set of the maximal ideals of L K (or of the classes of complete extensions)to the set of the valuations of L extending v.

Moreover the completion L of L with respect to wm is exactly M 48 and the composite extension of L and K contained in L is M.So we have fi o 0=I (identity map)

Now we have also 0 o fi=I, for if w is any valuation of Lthen the valuation wmw is necessarily the same as w by the uniqueness of the extension to M of the valuation v of K.

Hence there exists a correspondence between the set of valuations on L extending v and the set of inequivalent composite extensions of L and K.

In particular if (L : K)=n<m, then any composite extension of L and K is complete which means that L=L<g>K/M, where M is someK

maximal ideal of L<g>K.

K

Suppose L is an algebraic extension of an incomplete valuated field K with a valuation v.Let (w)ei be the set of valuations on L extending v.We shall denote by Li the field L with the valuation w, , by e, the ramification index ∈ (L, : K) = ∈ (L, : K) by C the residual degree f(L, : K)=f(Li: K) and by n the dimension of L, over K.

Theorem. IfL is a finite extension of degree n of a field K with a real valuation v, then there exist, only finitely many different valuations (Wj) on L extending v.Moreover we have En<n and the sequence

0 ^ r (L<g>K) ^ L<g>K ^ O Li ^ 0 is exact.

Proof. We observe that wi is not equivalent to wj for i ± j, because wi equivalent to wjmeans that they differ by a constant factor and since their restriction to K is same, we have wi=wj

The number of different valuations (wi) on L extending v is finite because the number of inequivalent composite extensions of L and K is finite.To prove that the sequence is exact, we have to show that the mapping p : L K ^ n Li is surjective.By the approximation theorem of valuations p (L) is dense in n Li, therefore p(L K) is dense in n Lb where p is the canonical map from L ^ n Li.But p (L K) is a finite dimensional vector space over K therefore it is complete.Hence p (L K)=n Li i. ∈ ., p is onto.Obviously dim n Lj<dim L K over

K, which means that ∈ ni<n.

Corollary. If K or L is separable over K, then we haveEni=n.

K or L separable over K implies that r (K<g>L)=0 therefore p is an isomorphism.

6.4 COMPLETE ALGEBRAIC CLOSURE OF P-ADIC FIELD

Proposition. Let K be a complete field with a real valuation v and O the algebraic closure of K.Then O the completion of O by the valuation extending v is algebraically closed.

We shall denote the extended valuation also by v.

Proof. To prove that O is algebraically closed we have to show that any irreducible polynomial f (X) in O[X] has a root in O.Without loss of

generality we a can assume that f (X) is in Of [X] and leading coefficient of f(X) is 1.Suppose that f (X)=Xr+ar-1Xr-1+ +a0 then for every

integer m there exists a polynomial g>m (X)=Xr+lm)Xr-1++ l ∈ m) in

Of[X] such that for every xin Of-1,

v(f(x) -<pm(x)>rm Let<fim(X) = r

(X-ajm), ajm are in Of as g>m(X) is in Of [X].Then

<fim+1 (ajm)=<fim+1(ajm)- f (ajm)+f (ajm)- 9m(ajm) implies that v(<pm+1(ajm))>rm

or ^ v (ajm- atm+1)>rm.

Therefore there exists a root atm+1 of<pm+1 (X) such that v(ajm-a?m+i)>m.

Notes

So we get a sequence j^m (X)J of polynomials converging to f and

a sequence of elements jjSmJ converging to S in O and each j3m is a root of (fim(X).Since polynomials are continuous functions, we have lim f (Sm)=f (S)

But limf (Sm)=0, because given integer N>0, for m>N we

have v(f (Sm))=v(f (Sm)- ^m(Sm))>rm>N.

Hence S is a root of f (X).

One can easily prove that the residual field of O is the algebraic closure of the residual field of K.In particular if K=Qp, then the residual field of O i. ∈ ., kf is algebraic closure of Z/(P).Thus kf=uFi, where each F is a finite extension of Z/(P)

6.5 VALUATIONS OF NON-COMMUTATIVE RINGS

We define a valuation of a non-commutative ring A without zero divisors containing the unit element in the same way as of a commutative ring.Almost all the results proved so far about valuated can be carried over to division rings with valuations with obvious modifications.WE mention the following facts far illustration.

Let L be a division ring with a valuation v.Then

The set Ol= \x/x ∈ L, v(x)>0>is a non-commutative ring, which

we call the valuation ring of L with respect to the valuation v.

YL=t x/x ∈ L, v(x)>0>is the unique two sided maximal ideal of Ol.

Any ideal in Ol is a two sided ideal.For, v(x-1yx)=-v(x)+v(y)+ v(x)>0 for x in L and y in Ol which means that x-1yx belongs to Ol, therefore yx=xz for some z in Ol.Hence Olx=xOl.

The ideals of Ol are any one of the two kinds

$$I_\alpha = \{x | v(x) > \alpha \geq 0\}$$

$$I'_\alpha = \{x | v(x) \geq \alpha > 0\}$$

The division ring L is locally compact non-discrete division ring for the valuation v if and only if v is a discrete valuation, L is complete and O/ YL is finite Regarding the extension of valuations to an extension divisionring we prove the following.

Theorem. Let P be a division algebra of finite rank over a complete valuated field P with a valuation v such that P is contained in the center of P.Then there exists one and only one valuation w of P which extends

v.

Proof. Existence We define N (x)=determinant of the endomorphism

pxy ^ xy of P, for any x in P.

We shall prove that n(x)=-\{ N(x) is a valuation of P if r is the

r PP rank of p over P.The axioms w (x)=m if and only if x=0 and w(xy)=w(x)+w(y) are obviously true.

To prove w (x+y)>inf(w(x), w(y)) it is sufficient to prove that w(x)>0 implies w(1+y)>0.Let F=P (x) F is clearly a field contain- ing P and p is a vector space over F by left multiplication.The mapping px is an F endomorphism.We know that if U is any F-endomorphism

and Up the P-endomorphism defined by U, then det Up=N (det U)

F/P and we have det px=(x) (P:F) if px is considered as an F-endomorphism.Therefore we have

w{ x)=~{ P \ F)=v(N (x)).

r F/P Now w (x)>0 vv(N(x))>0 =^ v(N(1+x))>0, because we F/P F/P

have proved this for commutative case.Hence wis a valuation on P Uniqueness Since P is complete and P is of finite rank r over P, any valuation defines the same topology on P as that of Pr.But the topol- ogy determines the valuation upto a constant factor, If w1 and w2 are two valuations of p extending v then w1=Cw2 for some C in P.But restriction of w1 to w2 to P is v, therefore C=1 and w-1=w2.

Check your Progress-2

Discuss Residual degree and ramification index

____
____
____

6.6 LET US SUM UP

In this unit we have discussed the definition and exampleofTheory of valuations–II, Residual degree and ramification index, Complete algebraic closure of a p-adic field, Valuations of non-commutative rings

6.7 KEYWORDS

Theory of valuations–II …..In this section we give a proof of Hensel's Theorem and deduce certain corollaries

Residual degree and ramification index…..Let L be a field and K a subfield of L.Let wbe a valuation of L and vtherestriction of w on K

Complete algebraic closure of a p-adic field…..K be a complete field with a real valuation v and Othe algebraic closure of K.Then O the completion of O by the valuationextending v is algebraically closed.

Valuations of non-commutative rings…..a valuation of a non-commutative ring A without zero divisorscontaining the unit element in the same way as of a commutative ring

6.8 QUESTIONS FOR REVIEW

Explain Theory of valuations–II

Explain Residual degree and ramification index

6.9 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

6.10 ANSWERS TO CHECK YOUR PROGRESS

Theory of valuations–II (answer for Check your Progress-1 Q)

Residual degree and ramification index

(answer for Check your Progress-2 Q)

UNIT -7 : REPRESENTATIONS OF P-ADIC GROUPS

STRUCTURE

7.0 OBJECTIVES

After studying this unit, you should be able to:

- Understand about Representations of p-adic groups
- Understand about Some elementary p-adic analysis
- Understand about Representations of Locally Compact Groups
- Understand about Irreducible Representations
- Understand about Measures on Homogeneous spaces
- Understand about Induced Representations

7.1 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.

Representations of p-adicgroups, Some elementary p-adic analysis, Representations of Locally Compact Groups, Irreducible Representations, Measures on Homogeneous spaces, Induced Representations

7.2 REPRESENTATIONS OF P-ADIC GROUPS

We prove here an analogue of the theorem about the representations of semisimple Lie Groups in chapter of this part.We shall give the proof of the theorem for the general linear group GLn (P)=G, though the same theorem could be proved for other classical linear groups with obvious modifications.Let A denote a character of T which is trivial on N.Since A is isomorphic to T/N, A can be considered as a character of A.Let us assume that UAf=0 for every A in A* (the group of characters of A) and f ∈ L(G) such that f+0.We first try to find the condition under which our assumptions are valid.Let be an element of CA (the space of the induced representation of A).Then<p (tx)=(p(t))i A(t)<p(x) for x ∈ G and t ∈ T.Moreover

UAf (p (∈) =J<p(y) f(y)dy=0, because Uf=0

Since X the support of f is a compact set, it intersect only a finite number of double cosets modulo K.Let

S=S (f)=|a|da ∈ A+, ^ nK da K+ a=a(f)=min{J3 ∈ S (f) }.

The set S is a finite non-empty set because f ± 0.Therefore a exists.For any da in A+ the coset K da K is a finite union of left cosets modulo K, the representatives for which could be found in T, because G=TK.Let Ia be the set of left cosets C modulo K such that Kda K= 100 U C, where C=t(C)K, t(C) ∈ T.But we know that T=Na, therefore CeIa

t (C)=n(C)dY(C) where n(C) and dy(C) belong to Nand A respectively.Since n(C)dY(C) belongs to Kda K proposition implies that y(C)>a, Thus we get that K da K=m U n(C) K, y(C)>a and if y(c)=a, Ce Ia then C=da K and we can take t(c)=da.Let us assume that the right invariant Haar measure on G is such that its restriction to K is normalisedi.e ., ∈ dk=1.Then for any left coset C=t (C)K, we have

f f(g)dg=A(t(C)) f f(t(C)k) dk Jg Jk

and the equation gives

f y(y) f(y) dy=zz A(t(C)) f<fi(t(C)k) f(t(C)k)dk

Jg peS Celp Jk

= a(t(C)) f Ak) f(t(C)k) dk

p C Jk

with<r (t)=[<5(r)A(t)]2 and where ^0 denotes the restriction of (p to K.

We have shown earlier that p° (tx)=A(t) p0(x) for t ∈ TnK=NnK, but A(N)=1, therefore the space CA is independent of A.Moreover there is only one term corresponding to p=a in the summation, since for others y(c)>a.Separating the term for p=a

we get UAp (e)=o- (da)2A(da)fR<p°(k) f(da k)dk+ ∈ Qy(f, <p)A(dy) with

y>a Qy (f, <p)=J] (rWQ)* f tp0(k) f(t(C)k)dk

CeIfiy (C)=a jK

It is obvious that Qy(f, p) is independent of A.For every y ∈ Z", the mapping dy ∈ A —>xY ∈ A** given by xY(A)=A(dy)is an isomorphism of the groups A and A**.But the characters of an abelian group are linearly independent, therefore QY(f, p)=0 for every y and in particular Qa(f, p)=0.Thus we obtain

|<p(k) f(dak)dk=0, for every (p with<p(nk)=<p(k) for n ∈ Nn K.

The equation is true for left and right translations of f by elements of Kbecause Ui „=UiJ=UXUi=0 and

x1 = Uf* ∈ x=ufuA=0.

So if g (x)=f(k-1 x)for k in K, we have Uxg=0.Obviously S (f)= S (g) and a(f)=a(g).Let K'a=K n da K d-1 and Ka=K n d-1 K da be two subgroups of K.Now

f p (k) f(da(d-1 hda k))dk=f p(d-1 hda k) f(dak)dk=0

Thus the function k ^ f (da k) is orthogonal to all the functions p in CA=C and their left translates by the elements of Ka, where p is invariant on the left by the elements of N n K.

Theorem. For every a ∈ Zn such that da ∈ A+, the subgroup Ka contains N n K where N is the group consisting of the transpose of elements of N.

Proof

By definition

with a1<a2<, ..., <an.

Let h be an element n of K.

Then (da hd- l)ij=na~ajhjj which shows that the groups Ka consist of matrix h in K such that na~ajhjj is integral.If we take h ∈ N' n K, obviously h belongs to Ka.Thus Ka contains N nK.This Theorem shows that the groups Ka and K'a are sufficiently big.

In addition to the above assumption about f, let us further assume that f belongs to Lm(G) where M is some irreducible representation of K.Clearly M is a subrepresentation of left regular representation of K in L2 (K).Let ∈ c L2 (K) be an invariant subspace of the left regular representation a of K such that a when restricted to ∈ is of class M.Therefore ∈ c Lm (K).Define F (k)=f(da k).We can assume that F P 0.Since F is transformed following ML by the right regular representation of K, F belongs to Lm(K).But F is orthogonal to all the functions p in C invariant on the left by the elements of N nK, the left translates of p by the elements of K and the right translates of p by the elements of K.Hence if M satisfies the condition (S)i. ∈ .The smallest subspace of ∈ invariant by N' and which contains elements invariant on the left by the elements of N n K is ∈ .Then F is orthogonal to Lm (K), because Lm(K) is generated by the right translates of ∈ .But this is a contradiction, because F ∈ Lm(K).Thus we get the following

Theorem. The representations UA for A ∈ A* form a complete system of representations of the algebra Lm (G) if the irreducible representation M satisfies the condition (S).

Corollary. If M satisfies (S) then M occurs atmost(dim M) times in any completely irreducible representation of G.

Since UA for any A in A* when restricted to K is a sub representation of the left regular representation of K, C cLm(K) which is a subspace of dimension (dim M)2, thus M is contained at most (dim M) times in UA.

Corollary. The identity representation of K occurs at most once in any completely irreducible representation of G.

This follows from Corollary as the identity representation satisfies the condition (S).If M is the identity representation of K, then the algebra Lm(G) is commutative.

The algebra Lm(G) has complete system of representations of dim 1.Therefore if x and y are any two elements of Lm(G), then UA(x y)= UA(y x) for every A ∈ A*, because UA is of dimension 1.Therefore UA (xy-yx)=0 for every A in A*.But this is possible only if xy-yx=0 i.e ., the algebra Lm(G) is commutative.

Finally we try to find out what are the various representations of K which satisfy the condition (S).It is obvious that a representation which satisfies the condition (S) when restricted to Nn K contains the identity 104 representation of N n K.It is not known whether there exist or not representations of K which when restricted to Nn K contain the identity representation but which do not satisfy the condition (S).However in this connection we have the following result.

Theorem. Every irreducible representation M of K which comes from a representation of GLn (O/Y) and the restriction of which to N n K contains the identity representation of N n K satisfies the condition (S).

It can be easily proved that GLn (O/ Y) is isomorphic to K/H, where H is a normal subgroup K consisting of the matrices (iJ-+aj where aij belongs to Y.Therefore a representation of GLn (O/Y) gives rise to a representation of K.

Remark.We have proved that in the case of real or complex general linear group the representations induced by the unitary characters of T form a complete system of representations of algebra L (G).But in the case of general linear groups over p-adic fields the representations induced by the characters of A do not form a complete system.In fact the algebra L (K) is a sub-algebra of L(G), because K is open and com- pact in G.Therefore if the representations UA form a complete system for L (G), their restrictions to K will form a complete system of representations of L(K).But the restriction of UA to K is a representation of K induced by the unit character of N n K, therefore by Frobenius reciprocity theorem the irreducible representations of K which occur in Ux are precisely those which when restricted to Nn K contain the identity representation.But there exist representations of K for which this property is not satisfied.

SomeProblems For any classical group, we have found a maximal compact sub- group K.If G is the general linear group, it is easy to observe that: any maximal compact subgroup is conjugate to K by an inner automorphism; any compact subgroup is contained in a maximal compact subgroup.(For, let H be a compact subgroup of GL(n, P) let ei, ..., en be the canonical basis of F".

Let I0 be the O-module generated by the ei and let I be the O-module generated by the h ei for h ∈ H: because H is compact, the coordinates of the h.ei are bounded and there is an integer n>0 such that I c n-nI0.Hence I is a lattice and H is contained in the maximal compact subgroup K1 formed by the g ∈ G such that g.I=I.Moreover, if g ∈ G is such that g.Io=I, then K1=gKg-1.) But for the other types of classical groups, it is not known if the results are true or not.Actually, one cannot hope that is true: already in SL(n, P), we have only:

(i bis) any maximal compact subgroup is conjugate to K by an (not necessarily inner) automorphism.

It observems possible that there exist several but a finite number of classes of maximal compact subgroups: for instance, it observems unlikely that the maximal compact subgroup K' of the orthogonal group 0(n, P) which leaves invariant a maximal lattice of norm P is conjugate to K.But perhaps, any maximal compact subgroup of 0(n, P) is conjugate to K or to K'.

It can be noted that are not both true in the projective

group G=PGL(2, P): a maximal compact subgroup K is the canonical image of GL(2, 0) in G; the determinant defines a map d from G to the quotient group F*/(F*)n and the image of any conjugate of K is

contained in the image D of 0* in P/(P*)2.Now, let u be the image of |1 0) in G: we have u2=1 and d(u) ∈ D.Hence, u generates a compact subgroup which is not contained in any conjugate of K.

It observems very likely that our results about classical groups are valid for any semi-simple algebraic linear group over P (at least if char P=0).The general meaning of the subgroups N, D, T r is clear: N is a maximal unipotent, D is a maximal decomposed torus (a decomposed torus is an algebraic group isomorphic to (P*)r), which normalised N.Then D can be written as D=A.U, where A ~ Zr and U ~ (0*)r and we have T=a.N.The subgroup r is the normaliser of N.It can be proved (A.Borel, unpublished)that D and N exist in any such G (at least if the base field P is perfect) and are unique, upto an inner automorphism.Now the problems are:

Define a maximal compact subgroup K;

prove that G=T.K;

prove that G=K.a.K and define △+ (which is certainly related with the Weyl group and the Weyl chambers);

prove the key Theorem about the intersection Nda K n KdpK.For the simplest idea is to take a lattice I in the vector space in which G acts, and to put K={ g|g ∈ G, g.I=I }.Then we get a compact subgroup.But it is obvious that K will be maximal and satisfy only if I is conveniently chosen.

Assume that char P=0: then we can consider the Lie algebra G of G and the adjoint representation.Then we can choose a lattice I in G such that [I, I] c I (in other words, I is a Lie algebra over 0);such a lattice always exists: take a basis G and multiply it by a suitable power of n in such a way that the constants of structure become integral.Now there exist such lattices which are maximal, because [I, I] c I implies that I is a lattice of norm c 0 for the Killing form of G.As this form is non-degenerate, it is impossible to get an indefinitely growing sequence of such lattices.Hence we can choose such a maximal lattice I and put K={ g\g ∈ G, g.I=I }.

But let us look at the compact case: it can be shown that G is com- pact if any only if the Lie algebra G has no nilpotent elements.In this case, we should have K=G'.So we are led to the following conjectures:

Conjecture.there is a unique lattice in G which is a maximal Lie subalgebra over 0;

Conjecture.the set I if the X ∈ G such that the characteristic poly-nomial of the operator ad X has its coefficients in 0, is a Lie subalgebra over 0;

Conjecture.(A.Weil): any algebraic simple compact group over a locally compact P-adic field of characteristic zero is (up to finite groups) the quotient of the multiplicative group of a division algebra Q over P by its center.It is easy to prove that the Lie algebra G is the quotient of the Lie algebra Q by its center and the X ∈ I are exactly the images of the integers of Q.It is obvious that because any Lie subalgebra over 0 is contained in I.Moreover, is true for the classical groups: we have only for

Notes

compact groups the groups PGLi(P) ~ P/center and the orthogonal and unitary groups for an anisotropic form..

Then if one can prove one of the above conjectures, one can hope to generalize these results to any semi-simple group by an argument by induction on the dimension of a maximal nilpotent subalgebra of G.

7.3 SOME ELEMENTARY P-ADIC ANALYSIS

In this chapter we will investigate elementary p-adicanalysis, including concepts such as convergence of sequences and series, continuity and other topics familiar from elementary real analysis, but now in the context of the p-adic numbers Qp with the p-adic norm ||p.

Let a={ an } $\in$ Qp.we know that for some M,

|a|P= —, 1 lppordpaM '

which is an integral power of p.So for t $\in$ Z an inequality of form

Proposition.(an) is a Cauchy sequence in Qp if and only if (an+1 — an) is a null sequence.

Next we will now consider series in Qp.Suppose that (an) is a sequence in Qp.For each n we can consider the n-th partial sum of the series an,

Sn=ai+a2+ +an.

Definition If the sequence (sn) in Qp has a limit

S=lim (p)sn n^^

we say that the series an converges to the limit S and write

$\in$ an=S.

S is known the sum of the series an.If the series has no limit we say that it diverges.

In real analysis, there are series which converge but are not absolutely convergent.For example, the series XX — 1)"/n converges to — ln2 but ^1/n diverges.Our next result shows that this cannot happen in Qp.

Proposition. The series a" in Qp converges if and only if (an) is a null sequence.

Proof. If ^ an converges then by Proposition the sequence of partial sums (sn) is Cauchy since sn+isn — an is a null sequence.Conversely, if(an) is null, then observe that the sequence(sn) is Cauchy and hence converges.

So to check convergence of a series ^ an in Qp it suffices to investigate whether

lim (p)an — 0.

This means that convergence of series in Qp is generally far easier to deal with than convergence of series in the real or complex numbers.

Example.The series ^ 1/n diverges in Qp since for example the subsequence

P" — 1

J" i 1

np+1

of the sequence (1/n) has |P"|p — 1 for every n.

As a particular type of series we can consider power series (in one variable x).Let x ∈ Qp and let (a") be a sequence.Then we have the series ^ a"X".As in real analysis, we can investigate for which values of x this converges or diverges.

Example.Take a" — 1 for all n.Then

lim<P)x"! — 0 if|X|P<1

"^^ I ^ 1 otherwise.

So this series converges if and only if |x|p<1.Of course, in R the series ^ x" converges if |x |<1, diverges if |x |>1, diverges to +^ if x — 1 and oscillates through the values 0 and — 1 if x — — 1.

Example.For the series nxn, we have

\nxn\p= \n\p\xn\p<\ x\pn which tends to 0 in R if \x\p<1.So this series certainly converges for every such x.

Just as in real analysis, we can define a notion of radius of convergence for a power series in Qp.For technical reasons, we will have to proceed with care to obtain a suitable definition.We first need to recall from real analysis the idea of the limit superior (lim sup) of a sequence of real numbers.

Definition.A real number ∈ is the limit superior of the sequence of real numbers (an) if the following conditions are satisfied:

(LS1) For real number ∈ 1>0,

3M1 ∈ N such that n>M1 =^ ∈ + ∈ 1>an.

(LS2) For real number ∈ 2>0 and natural number M2,

m>M2 such that am> ∈ — ∈ 2.

We write

∈ =lim sup an

if such a real number exists.

If no such ∈ exists, we write

lim sup an=to.

It is a standard fact that if the sequence (an) converges then lim sup an exists and

lim sup an=liman.

n n^tt

In practise, this gives a useful method of computing lim sup an in many cases.

Now consider a power series ^ anxn where an ∊ Qp.

Then we can define the radius of convergence of ^ anxn by the formula

r=1 -r-.

limsup \an\p /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)thenYlanxn converges (or diverges) for all x ∊ Qp with \x\p=r.

Example.Show that the radii of convergence of the p-adic series

(-1)n-1xn

expP (x)=n.' logp (x) =

n=0 n=1

are p-1/(p-1) and 1, respectively.

|1/(n0lp/n=p(n-ap(n))/n(p-1)=p(1-ap(n)/n) (p-1)

and

limsup |1/(n!)|p/n=p1/(p-1), so the radius of convergence of expp(x) is p-1/(p-1).

Also,

|1/n|P/n=pordp(n)/n

and

limsup |1/n|1/n=1,

hence the radius of convergence of logp (x) is 1.

Check your Progress-1

Discuss Theory of valuations–IIs

____

____

____

7.4 REPRESENTATIONS OF LOCALLY COMPACT GROUPS

In this section we give a short account of some definitions and results about the representations of locally compact groups.We assume the fundamental theorem on the existence and uniqueness (upto a constant factor) of right invariant Haar measure on a locally compact groups.For simplicity we assume that the locally compact groups in our discus- sion are unimodular i.e ., the Haar measure is both right and left invariant.By L(G) we shall denote the space of continuous complex valued functions with compact support and by L(G, K), where K is some compact set of G, the set of elements of L(G) whose support is contained in K.Obviously we have L (G)=U L(G, K) and L(G, K) is a Banach space under the norm f=sup|f(x)|.

The space L (G) can be provided with a topology by taking the direct limit of the topologies of L(G, K).This topology makes L (G) a locally convex topological vector space.

Let G be a locally compact group and H a Banach space

Definition.A continuous representation U of G in H is a map x ^Uxe Hom(H, H) such that

(i)Uxy=Ux ◦ Uy for X; y in G.

(ii) The map H x G ^ Hdefined by (a, x) ^ Ux a is continuous.

Definition. Let H be a Hilbert space.The representation U is said to be Unitary if Ux is a unitary operator on H for every x in H.

Let M (G) be the space of measures on G with compact support.The space M (G) is an algebra for the convolution product defined by

$$\mu * \nu(f) = \int \int f(xy)\, d\mu(x)\, d\nu(y)$$

The space L (G) can be imbedded into M(G) by the map f ^ p f= f(x)dx.It is infact a subalgebra of M (G) because p f*pg=p f*g where

$$f * g(x) = \int f(xy^{-1}) g(y) dy.$$

Moreover if v is any element of M (G), then p f*v belongs to L(G), because for any g $\in$ L(G) we have

(p f*v) (g)=JJ g(xy)f (x)dxdv(y)

= J dv (y)J g(x) f (xy 1)dx.

= ph (g) where h(x)=f (xy-1)dv(y)

Thus we define the convolution of a measure p and function f $\in$ L (G) by setting

Let U be a representation of G in H.Then U can be extended to M (G) by setting

Up (a)=Uxadp(x)(for a $\in$ H, p $\in$ M(G)

Now let H be a Hibert space and U a Unitary representation.

Then if p and v are any two elements in M (G), we have

(UvU^a, b)=J<Ux Up a, b) dv(x)

= J<Upa, Ux-1 b)dv(x)

= J dv (x)J<UyaUx-1 b)dp(y)

= J<UxUya, b)dv(x)dp(y)

This means that Up*v=Up o Uvi.e .,

U is a representation of the algebra M (G).It can be easily verified that map p ^ Up is a continuous representation of the algebra M (G).Moreover

(U*pa, b>=(Upb, a)

= J (Uxa, b)dp(x~l)

This shows that Up=Up, wheredp(x)=dp(x-1).

Thus the operator Up,,, p on H isHermitian.

In particular we get a representation of L (G) in H given by f ^Up f=Uf, where Uf(a)=Ig Uxaf(x)dx.

We can also get a representation of M (G) by considering regular representations of G i. ∊ ., representations G by right or left translations in G in any function space connected with G with some convenient topology, for instance the space L(G) or L2(G)(the space of square integrable functions).

We shall denote by ux the left regular representations and by tx the right regular representations of G i.e ., for any function f on G we have

^x(f)(y)=f(x-1y), Tx(f)(y)=f(yx) we have for any p in M(G)

M f)= P*f

v v — 1

tp (f)=f*p where dp(x)=dp(x 1)

Let K be a compact group, M an equivalence class of (unitary)ir-reducible representations of K.For any x belonging to G, let Mx= (CM(x)) be the matrix of Mx with respect to some basis of the representation space.Let tm be the dimension of M and xm=H CM

i=1 ii

Character of M.For any two irreducible unitary representations of K we have the following orthogonally relation, CM*CM if M+M

C«.C%=- Ls^Ctf

where the value of the convolution product at the unit element ∈ of G is given by CM*C*f (e)=f C% ∈ y)dx.

When we write (1) and (2) in terms of characters we get

Xm*XM'=0 if M+M

xm *xm= —xm

tm

Obviously we have

(tmxm)*CM=CM*xmtm=CM

Let Lm (K) be the vector space generated by the coefficients CM, where Mis the complex conjugate representation of M.If f is in L2 (G),

then by Peter-Weyl's theorem, f= ∈ hjNCfj.Further if rmym*f=f, i, j, N j

then we have f=Y* ^nMCff, which means that f belong to Lm(K).Conversely if f belongs to Lm (K), then f=X ^uMCM.Therefore

i, j ij rMXM*f=f Hence f ∈ L2 (G) is in Lm(K) if and only if rMXM*f=f- In this paragraph we give another interpretation of the space Lm(K).

Definition. Let M be an irreducible unitary representation of K and U any representation of K in a Banach space H.

We say that an element a ∈ H is transformed by U following M, if a is contained in a finite dimensional invariant subspace F of H such that the restriction of U to F is direct sum representations of the equivalence class of M.

Let HM=Hm={ a | ∈ H, a transformed by U following M }.It is 59 easy to verify that Hm is a vector space.

Notes

Proposition. Lm (K) is exactly the subspace of L2(K) formed by the elements which are transformed following M (respectively following M)by the left (respectively right) regular representation of K.

Proposition. If U is a representation of K in H, thenEm=UrM^M is a continuous projection from H ^ Hm.

In order to prove the proposition 1 and 2 prove the following results.

Suppose that y belongs to Lm (K), then<y=Z /f/Cft For

ij 'J

veif, we have (kf)(7)=cjj(x~ly)=J] cJj(x-l)Cfj(y)

k = w.

So the space Ej generated by Cij, •••, Crj(rM=r) is invariant by u and the restriction of u to Ej is of class M.Therefore Lm (K), which

U is direct sum of the Ej, is contained in (L2(G)).

M

If p belongs to Lm (K) and a belongs to H, then we show that Upa belong to Hm.

We have

UxUpa=Uex*paP=UJopa where sx is the Dirac measure at the point x, and f Uybdsx (y)=Uxb.jK

This shows that p ∈ Lm (K) ^ Up a ∈ H is a morphism of representation j and U.Hence Upa is transformed by U following M.

If a belongs to Hm, thenEMa=a.Since a belongs to some finite dimensional invariant subspace F of H and the restriction of U to F is the direct sum of representation of class M, we can find a basis (eJk) of F such that UxeJk= ∈ CM(x)eik

Let a=X djjejj.Then 'J

E^a)= rM I AJkCfk(x)eikxm(x)dx

J j = rm Yu (2 AJk f cfj^d.x)dx)eik

i, k J ^ \Ajkeik=a•

Moreover

f mCM (x)xm(x-1)dx=rMXM*CM (∊) =Sj

In particular if p belongs to L2 (G) it is transformed by j following M, then

°~rMXM<P=rmxm*P=P

Therefore p belongs to Lm (K).

Clearly the results imply proposition 1.

EmEm=m m u^2xm*xm

= UrMXM=EM,

the proposition is proved by result

Similarly we prove that Em • Em=0 for M P M.Thus we get a family of projections Em with Em (H)=Hm.The sum X Hm is direct and is dense in H.It is sufficient to prove that if a' is a continuous linear form on H, which is zero on every Hm, then{a, a')=o for every a ∊ H.Let us put p (x)={ Uxa, a!).Then

$$\langle \varphi, C_{ij}^{M} \rangle = \int C_{ij}^{\overline{M}}(y) \langle U_y a, a' \rangle dy.$$

{ Uga, a') with g=Cfj

But Uga' belongs to Hm, therefore we get that p is orthogonal to all the coefficients CM for any M, so p=0.

In particular if U is unitary (for instance the regular representation in L2(K)), then the Em are orthogonal projections and His exactly Hilbertian sum of the closed subspaces Hm.

Let G be a locally compact group, K a compact subgroup of G.Sup- pose that U is a continuous representation of G in H and M an equiv- alence class of unitary representation of K.By HM=Hm we shall mean the vector subspace of H consisting of elements which are trans- formed by the restriction of U to K following M.As in the above case Em=UrwcM's a projection of Hto Hm- Let

Lm (G)-|/1 / ∈ L(G), f*rMXM ~ rmxm*/" — /j

It is easy to prove that Lm(G) is a subalgebra of L(G) and the map- ping /rmxm**rhxmis a projection from L(G) to Lm(G).

If f belongs to Lm (G) and a belongs to H, then is in Hm.If b belongs to H'M, thenUf(a)=UrM(a)XM,, f=EM Ufa ^ Ufa is in HM.If b belongs to Hm, then

Ufb=U _ Em>b=UfEMEM b=0

f*mxM

This shows that U is a representation of Lm(G) in Hm and Uf= EmUfEm.Moreover for f ∈ Lm (G)

f (j)=rM f f(k 1 y)xm(k)dk.

In particular if M is the identity representation, thenxm is constant and f is in Lm(G) if and only if

f (y)=mf f (ky)dk=rm ^ f (yk)dk

kk^ f (hyk)=f(fyk)=f(y).

Such functions are known spherical function on G with respect to K.They can be considered as functions on G/K which are left invariant, provided we write G/K={ K, aK, }

7.5 IRREDUCIBLE REPRESENTATIONS

In this section we study how we can get some information about the representation of a group G by studying the representation of the algebra

LM (G).

Definition.A representation U of a group G in a vector space V is said to be algebraically irreducible if there exists no proper invariant subspace of V.

Definition.A representation U of a topological group G in a locally convex space ∈ said to be topologically irreducible if there exists no proper closed invariant subspaces of ∈ .

Definition.A representation U of a topological group G in a Ba- nach space H is said to be completely irreducible if U (L(G)) is dense in Hom(H, H) in the topological of simple convergence i. ∈ ., given an operator T on H and element a1; a2, , ap in H, there exists for every e>0 an element f in L(G) such that

||(Uf- T) ai ||<e for i=1, 2, •••, p.

It is obvious that F is a proper closed invariant subspace of H.Let a ± 0 be any element of F, then for every b in H there exists a T ∈ Hom(H, H) such that T(a)=b.But by definition for every s>0 there exists an element f in L (G) such that ||Ufa - T(a)||<s.This means that F is dense in H which is a contradiction because F was assumed to be a closed proper subspace of H.

The definitions are equivalent for unitary representation by Von Neumann and all the three representation are equivalent for finite dimension representations.The proof can be found in.The definition implies.

Theorem. If U is a completely irreducible representation of G in a Ba- nach space H, then the representation UM of Lm(G) is H(M) is also completely irreducible.

Proof. Suppose that T belongs to Hom (H(M), H(M)).Extend T to Hby setting T=T on H (M) and O on E~M (0).Obviously T is continuous on H.

Since U is completely irreducible, T can be approximated by Uf for f in L(G)i. ∈ ., T=limUf{.Therefore

EmTEm=limEmU^Em

= lim farwCM

Hence in HM, T=limUrM^M, fi, rM^M

where rMXM* fi*rmxm is in Lm (G).Thus UM is completely irreducible.

Let U be a unitary irreducible representation of G in a Hilbert space H.By coefficient of U we means positive definite function{Uxa, a) on G.We state without proof the following theorem about the coefficients of unitary representations.

Theorem. If two irreducible unitary representations have same non- zero coefficient associated to them, they are equivalent.

We have observen that the representation U can be extended to the space M (G) and the operator Up*p for anyp in M(G) is Hermitian.In partic-ular if we take p=MXMdk, we have p=p.There fore Up,,.p=Em is Hermitian.

Moreover for any fin L (G) and a in Hm

{ Ufa, a)={ UfEMa, EMa)={ EMUfEMa, a)

={Uf0 a, a)

where fo=ruXu* f*rMXM belongs to Lm (G).Thus if we know nonzero coefficient associated to UM, we know coefficient associated to U as a representation of L(G), which determines coefficient of U as a representation of G.Thus a unitary irreducible representation of G is completely characterised by its restriction UM to Lg (G) if UM is not zero.

Definition.A set O of representations of an algebra A in a vector space is said to be complete if for every nonzero f in A there exists U ∈ O such that U f+O.

Proposition. If there exists a complete set O of representations of an algebra A which are of dimension<K (K a fixed integer), then every

completely irreducible representation of A in a Banach space is of dimension<k.

We first prove a Theorem due to Kaplansky.Let A be any algebra.For x\, , xp in A we define [x \, , xp]=X ea x^1...x^p where Sp is

P the set of all permutations u on 1, 2, , p and is the signature of<x.Obviously if dim A<p, then [x1, , xp]=o for all x1; x2, , xp in A.In particular we take A=Mn (C), algebra of n x n matrix with coefficient from C, the field of complex numbers, We define

r (n)=inf(p)such that [X1> >Xp]=Xi ∈ Mn(C)-

Clearly r (n)<n2+1.We shall prove that r (n+1)>r(n)+2.

We have r (n)- 1 elements X1, X2, Xr-1 in Mn(C)(r=r(n)) such that [X1, , Xr-1]*0, Let Ekh be the canonical basis of Mn(C).Then

[X1, , Xr-1]=^ AkhEkh.

Since [X1, , Xr-1]*0, there exists k0 and h0 such that Ak0h0*0.Let Xi be the matrix obtained by adding a row and a column of zeros to X-.Then

[Xu , Xr- 1 Eho, n+1 En+1, n+1]=[Xu , X^] Eho, n+1 En+1 n+1 =^ \AkhEkhEh<on+1

h, k = ^ ^ Akh0 Ek, n+1*0-

Thus r (n+1)>r(n)+2.

Now we prove the proposition.Suppose that r (k)=r and U is a complete irreducible representation of dim>K in a Banach space H.Let F be a subspace of H of dim k+1.Since r (k+1)>r(k), there exist operators [A1, ..., Ar] in Hom(F, F) such that [A1, ..., Ar]*0.We extend each Ai to the whole space H by defining Ai to be zero on F', where F' is any closed subspace such that H is the topological direct sum of F and F.Suppose that A1=limUft, where ∈ A.We have

0*[A1, •••, Ar] =Yj An,...A^ r=lim[U/i A2, •••, Ar].

&eSr

Therefore there exists f1 in A such that Repeating this process we obtain that there exist elements f1, ,

fr in A such that

U[fj, •••, fr]=[Ufl, • • •, Up]+0.But this is a contradiction because [f1, • • •, fr]=0 if [fj, • • •, fr] ± 0, then there exists a V in O such that

V[fb -, fr](al ^ 0 ^

[Vfl, • • •, Vr](a)+0.But r>rk and dimV<k, therefore [Vj, • • •, Vp]=0.Hence dim U<k.

Corollary.Let G be a locally compact group, K a compact subgroup, M a class of irreducible unitary representations of K in a Banach space H.If there exists a system O of representations of G in a Banach space such that (i) for every U in O, the representation UM of Lm(G) is of dim<p dim M.Equivalently M occurs atmost p times in each U.

The representations UM for U in O form a complete system of representation of algebra Lm (G).

Then M occurs atmost p times in any completely irreducible representation of G.

MEASURES ON HOMOGENEOUS SPACES

Let G be a locally compact group, dx the right invariant Haar measure and A(x) the modular function on G i. ∈ ., d(yx)=A(y)dx.Let T be a closed subgroup of G.We shall denote by the elements of r by d% and the Haar measure and the modular function on r.It is well known that there exists a right invariant Haar measure on G/T if and only if A(^)=8(^).In general it is possible to find a quasi-invariant measure on G/r.In order to show the existence, one shows that there exists a 8(^) strictly positive continuous function p on G such that p(x)=for every x in G and ^ in r.Then the measure p (x)dx gives rise to a measure dp(x) on G/r such that for any f in L(G) we havewhere depends only on the cosets of a* modulo T.Thus p (x) is a P(x) quasi-invariant measure on G/r.The details could be found in.

INDUCED REPRESENTATIONS

Let L be a representation of T in Hilbert space H.We shall define two types of induced representation on G given by L.

Assume that L is unitary.Let HL be the spaces of functions f on G such that

f is measurable with values in H.

f (x)=[p()]1/2 L f(x), for ? ∈ r.

f (p(x))-1 ||f(x)||2 dx<to.

Since the function (p(x))-1 ||f(x)||2 is invariant on the left by r, it can be considered as a function on G/r.Thus we define

II f ll2= f (p(x))-1 ||f(x) y2 dp(x)

It can be proved that HL is a Hilbert space with the scalar product

<f, g>, =f (P(x))-1<f(x), g(x))dp(x).

Let UL be the map from G to HL such that

ULf (y)=f(xy)

Obviously UL is continuous.Since we have

II tff y2=J (p(x))-1 y f(xy) y2 dp(x)

= J (P(xy~l))~l II f(x) II2 Pp^)dp{ x) =n f ii2

It follows that UL is unitary.We say that UL is the unitary representation induced by L.

Let L be any representation of r.Let us suppose that there exists a compact subgroup K of G such that G=TK.Let CL be the space of functions f such that

f is continuous with values in H.

f ({ x)=(p({))2Lf(f(x)) former.

We define ||f ||=sup ||f(x)||.Clearly CL with this norm is a x∈K

Banach space.Again right translation by elements of G give rise to a representation of G in GL.We denote this also by UL.

Let f ^ restriction of f to K=f0 be the map from the CL to C (K) (the set of continuous functions on K with values in H).The image of CL by this map is the set of elements f0 ∈ C (K) which satisfy condition above for all ∈ in r n K and x is K.But p (∈)=1, because p is a positive real character of K n r, therefore f0(∈ x)=f0(x).Through the space CL is identified with a subspace of C (K) yet the representation UL cannot be defined on this subspace.However the restriction of UL to K and the representation induced by the restriction of L to r n K are identical.

If L is unitary then f belongs to HL if and only if f0 belongs to L2 (K).We can choose p in such a way that p (xk)=p(x) for k ∈ K.Since the group K/Kn r is compact homogeneous space, there exits one and only one invariant Haar measure on it.But K/K n r is isomorphic to G/r therefore with the above choice of p, the quasiinvariant measure on G/r gives rise to the invariant measure on K/K n r.

Check your Progress-2

DiscussResidual degree and ramification index

____

____

____

7.6 LET US SUM UP

In this unit we have discussed the definition and exampleofTheory of valuations–II, Residual degree and ramification index, Complete algebraic closure of a p-adic field, Valuations of non-commutative rings

7.7 KEYWORDS

Theory of valuations–II …..We prove here an analogue of the theorem about the representations of semisimple Lie Groups

Residual degree and ramification index…..In this chapter we will investigate elementary p-adicanalysis, including concepts such as convergence of sequences and series, continuity

Complete algebraic closure of a p-adicfield …..In this section we give a short account of some definitions and results about the representations of locally compact groups

Valuations of non-commutative rings…..In this section we study how we can get some information about therepresentation of a group G by studying the representation of the algebraLM (G).

7.8 QUESTIONS FOR REVIEW

Explain Theory of valuations–II

Explain Residual degree and ramification index

7.9 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

7.10 ANSWERS TO CHECK YOUR PROGRESS

Theory of valuations–II (answer for Check your Progress-1 Q)

Residual degree and ramification index

(answer for Check your Progress-1 Q)