London Mathematical Society Student Texts. 3

Local Fields

J.W.S. CASSELS
Department of Pure Mathematics and Mathematical Statistics
University of Cambridge

CAMBRIDGE
UNIVERSITY PRESS

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York, NY 10011-4211 USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1986
Reprinted 1988, 1995

Library of Congress cataloging in publication

Cassels, J.W.S. (John William Scott)
Local Fields
(London Mathematical Society student texts; 3)
Includes bibliographies.
1. Local Fields (Algebra)
I. Title II. Series
QA247.C34 1985 512′.3 85-47934

British Library cataloguing in publication data

Cassels, J.W.S.
Local Fields
(London Mathematical Society students texts; 3)
1. Fields, Algebraic
I. Title II. Series
512′.3 QA247

ISBN 0 521 30484 9 hardcover
ISBN 0 521 31525 5 paperback

Transferred to digital printing 2003

CONTENTS

Paragraphs which can be omitted at a first reading are marked with an asterisk. But if you do skip them, then you miss some of the lollipops. The logical dependence of the chapters is given by the Leitfaden.

CHAPTER ONE: INTRODUCTION

1 VALUATIONS

These are generalizations of the ordinary absolute value on the field $\mathbb{C}$ of complex numbers. A valuation is a real valued function on a field k satisfying certain axioms. We leave formal definitions to the next Chapter, but here give more examples of valuations to illustrate some salient features.

(a) $k = \mathbb{C}$. For $a = u + iv$ with $u, v \in \mathbb{R}$, the ordinary absolute value is $|a| = \sqrt{(u^2 + v^2)}$. Then

(i) $|a| \geq 0$, with $= 0$ only for $a = 0$. (1.1(i))

(ii) $|ab| = |a||b|$. (1.1(ii))

(iii) $|a + b| \leq |a| + |b|$. (1.1(iii))

The inequality (iii) is usually called the triangle inequality.

(b) $k = k_o(T)$, where k_o is any field and T is transcendental over k_o. We first define $|\,|$ on the ring of polynomials $k_o[T]$. Let $c > 1$ be fixed arbitrarily. If

$$f = f(T) = f_o + f_1 T + \ldots + f_n T^n \quad (f_j \in k_o,\ f_n \neq 0),$$

we put

$$|f| = c^n, \qquad |0| = 0.$$

Any element h of $k_o(T)$ is of the form $f(T)/g(T)$ with $f(T), g(T) \in k_o[T]$ and $g(T) \neq 0$. We put

$$|h| = |f|/|g|.$$

Then for $f,g \in k_o(T)$ we have

(i) $|f| \geq 0$, with $= 0$ only for $f = 0$

(ii) $|fg| = |f||g|$

(iii)* $|f + g| \leq \max\{|f|,|g|\}$,

as is easily verified (do it first for $f,g \in k_o[T]$).

We call (iii)* the <u>ultrametric inequality</u>. It is clearly stronger than the triangle inequality (iii).

(c) $k = \mathbb{Q}$. Let p be a (positive) prime and let $\gamma \in \mathbb{R}$, $0 < \gamma < 1$. Any nonzero $r \in \mathbb{Q}$ can be written

$$r = p^{\rho}u/v,$$

where $\rho, u, v \in \mathbb{Z}$ and $p \nmid u$, $p \nmid v$. By unique factorization in $\mathbb{Z}$, the number ρ depends only on r. We put

$$|r|_p = \gamma^{\rho}, \quad |0|_p = 0.$$

Then

(i) $|r|_p \geq 0$ with equality only for $r = 0$ (1.2(i))

(ii) $|rs|_p = |r|_p\ |s|_p$ (1.2(ii))

(iii)* $|r + s|_p \leq \max\{|r|_p, |s|_p\}$. (1.2(iii))

Here (i), (ii) are trivial. To check (iii)* we may suppose that $r \neq 0$, $s \neq 0$ and without loss of generality that $|r|_p \geq |s|_p$. Then

$$r = p^{\rho}u/v, \quad s = p^{\sigma}x/y$$

for $\rho, \sigma, u, v, x, y \in \mathbb{Z}$ with

$$p \nmid uvxy,$$

and

$$\sigma = \rho + \tau \quad \text{with} \quad \tau \geq 0.$$

Now

$$r + s = p^{\rho}U/V,$$

where

$$V = vy \in \mathbb{Z}, \quad U = uy + p^{\tau}vx \in \mathbb{Z}.$$

Clearly $p \nmid V$. It is, however, quite possible that $p|U$ (at least when $\tau = 0$), say $U = p^{\lambda}W$, $\lambda \geq 0$, $p \nmid W$. Then

$$|r + s|_p = \gamma^{\rho+\lambda} \leq \gamma^{\rho} = \max\{|r|_p, |s|_p\}.$$

<u>Note</u>. It is usual to take $\gamma = p^{-1}$, when we have the <u>p-adic valuation</u> of $\mathbb{Q}$.

(d) $k = k_o(T)$, as in (b). Let $p(T)$ be an irreducible element of $k_o[T]$ and, as before, let $0 < \gamma < 1$. Every $h(T) \in k_o(T)$ can be written

$$h(T) = \{p(T)\}^{\rho} f(T)/g(T),$$

where $f(T), g(T) \in k_o[T]$ are not divisible by $p(T)$ and where $\rho \in \mathbb{Z}$ depends only on h (and, of course, p). We put

$$|h|_p = \gamma^{\rho}, \quad |0|_p = 0$$

and the reader will readily check that (i), (ii) and (iii)* hold.

The examples (b), (d) are closely related. Indeed on replacing T by T^{-1} in (b) we obtain (d) for the special polynomial $p(T) = T$.

We note also that except for (a) we always have the

ultrametric inequality (iii)*, not just the triangle inequality (iii). We shall see in Chapter 3 that (a) is indeed essentially the only valuation for which the ultrametric inequality fails.

2 REMARKS

Working with general valuations may require psychological adjustment. Consider first some consequences of the ultrametric inequality

$$|a + b| \leq \max(|a|, |b|). \tag{2.1}$$

It implies by an obvious induction that

$$|a_1 + \ldots + a_n| \leq \max_j |a_j| \tag{2.2}$$

and so (replacing a_j by $a_{j+1} - a_j$) that

$$|a_n - a_1| \leq \max_j |a_{j+1} - a_j|. \tag{2.3}$$

Let now b be a point of the "disc"

$$D = \{x : |x - a| < 1\}$$

of "centre" a. Then by (2.3)

$$|x - b| \leq \max\{|x - a|, |b - a|\} < 1,$$

for every $x \in D$. Conversely $|x - b| < 1$ implies that $x \in D$. Hence

$$D = \{x : |x - b| < 1\}.$$

Every point of the disc has an equal right to be regarded as a centre!

Again, consider the sequence (Conway and Sloane)

$$a_1 = 4, \quad a_2 = 34, \quad a_3 = 334, \ \ldots, \ a_n = 3\ldots34, \ \ldots$$

of integers. Then with respect to the 5-adic valuation we have

$$|a_m - a_n|_5 = 5^{-n} \qquad (m > n).$$

In particular, the sequence $\{a_n\}$ has the properties of what in ordinary real or complex analysis we call a <u>fundamental sequence</u> (Cauchy sequence). In this case we have

$$3a_1 = 12, \quad 3a_2 = 102, \quad 3a_3 = 1002, \ \ldots, \ 3a_n = 10\ldots02, \ldots,$$

and so

$$|3a_n - 2|_5 = 5^{-n}$$

Hence $\{a_n\}$ tends to the limit $2/3$ in a 5-adic sense. (We shall be defining these notions formally in the next Chapter).

On the other hand, fundamental sequences occur very naturally which do not have a rational limit. For example, one can find (in many ways) a sequence $\{a_n\}$ of integers such that

$$a_n^2 + 1 \equiv 0 \quad (5^n) \tag{2.4}$$

$$a_{n+1} \equiv a_n \quad (5^n) \tag{2.5}$$

for all $n \geq 1$. We take $a_1 = 2$. If a_n has already been chosen, we have to find an integer b such that

$$a_{n+1} = a_n + b5^n$$

satisfies (2.4), that is

$$(a_n + b5^n)^2 + 1 \equiv 0 \quad (5^{n+1}).$$

This is easily seen to be equivalent to

$$c_n + 2a_n b \equiv 0, \quad (5) \tag{2.6}$$

where $a_n^2 + 1 = 5^n c_n$. Since a_n is clearly not divisible by 5, we can satisfy (2.6). Hence we have an a_{n+1}, and the inductive process continues.

By (2.2) we have

$$|a_m - a_n|_5 \leq 5^{-n}, \qquad (m > n)$$

so again $\{a_n\}$ is a fundamental sequence. Suppose that it has a limit $e \in \mathbb{Q}$. By (2.4) we have

$$|a_n^2 + 1|_5 \leq 5^{-n}$$

from which it easily follows that

$$|e^2 + 1|_5 = 0.$$

Hence

$$e^2 + 1 = 0 \tag{2.7}$$

by (1.2(i)). But there is no $e \in \mathbb{Q}$ satisfying (2.7).

In the next chapter we shall show that any field may be "completed" with respect to a valuation on it in the same way as the real numbers are constructed from the rationals by completing with respect to the ordinary absolute value. The completion of $\mathbb{Q}$ with respect to a p-adic valuation $|\ |_p$ is the field $\mathbb{Q}_p$ of <u>p-adic numbers</u>. The argument above will then show that $\mathbb{Q}_5$ contains a solution e of (2.7).

3 AN APPLICATION

Here we show that the bare definition of the p-adic valuation provides a natural proof of an interesting result. Nothing in this section is used later, so it can be omitted if desired. In Chapter 12 we shall, however, indicate that it is not an isolated result but, rather, has been the starting point of much recent work.

We recall that the <u>Bernoulli numbers</u> B_k are given by the formal power-series expansion

$$\frac{X}{e^X - 1} = B_0 + \frac{B_1}{1!} X + \dots + \frac{B_k}{k!} X^k + \dots . \tag{3.1}$$

Hence

$$B_o = 1, \qquad B_1 = -1/2 .$$

Further,

$$B_k = 0 \quad (k \text{ odd}, > 1), \tag{3.1 bis}$$

since

$$\frac{X}{e^X - 1} + \frac{X}{2} = \frac{X(e^{\frac{1}{2}X} + e^{-\frac{1}{2}X})}{2(e^{\frac{1}{2}X} - e^{-\frac{1}{2}X})}$$

is unchanged by the substitution $X \to -X$.

Clearly the B_k are rational. The first few values are:

$B_2 = 1/6$	$B_{12} = -691/2730$
$B_4 = -1/30$	$B_{14} = 7/6$
$B_6 = 1/42$	$B_{16} = -3617/510$
$B_8 = -1/30$	$B_{18} = 43867/798$
$B_{10} = 5/66$	$B_{20} = -174611/330$

We shall present Witt's proof of

<u>THEOREM 3.1</u> (von Staudt-Clausen). <u>Let</u> k <u>be even</u>. <u>Then</u>

$$B_k + \sum_{\substack{q \text{ prime} \\ (q-1)\,|\,k}} q^{-1} \in \mathbb{Z} . \tag{3.2}$$

For example, the only primes q such that $q - 1$ divides 2 are $q = 2, 3$. In accordance with the Theorem $B_2 + \frac{1}{2} + \frac{1}{3} = 1$. Again, when $k = 20$ the relevant primes are $q = 2,3,5,11$ and one checks that

$$B_{20} + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{11} = -528.$$

Put

$$S_k(n) = 1^k + 2^k + \ldots + (n-1)^k. \tag{3.3}$$

On comparing coefficients on both sides of

$$1 + e^X + \ldots + e^{(n-1)X} = \frac{e^{nX} - 1}{X} \; \frac{X}{e^X - 1}$$

using (3.1), we rapidly obtain the once well-known formula

$$S_k(n) = \sum_{r=o}^{k} \binom{k}{r} \frac{B_r}{k+1-r} \; n^{k+1-r} , \tag{3.4}$$

expressing $S_k(n)$ as a polynomial in n. Here $\binom{k}{r}$ is the binomial coefficient.

It follows that

$$B_k = \lim_{n \to o} n^{-1} \; S_k(n). \tag{3.5}$$

With the ordinary definition of limit $n \to 0$ for positive integers n, this is a nonsense. If, however, we choose a prime p and work with the p-adic valuation $| \; |_p$, then it makes perfectly good sense; for example n can run through the sequence

$$p, \; p^2, \; p^3, \; \ldots, \; p^m, \; \ldots \quad . \tag{3.6}$$

We therefore compare $p^{-m-1} \; S_k(p^{m+1})$ and $p^{-m} \; S_k(p^m)$. Every integer j in

$$0 \leqslant j < p^{m+1}$$

is uniquely of the form

$$j = up^m + v \qquad (0 \leqslant u < p, \quad 0 \leqslant v < p^m).$$

Hence

$$S_k(p^{m+1}) = \sum_j j^k$$

$$= \sum_u \sum_v (up^m + v)^k$$

$$\equiv p \sum_v v^k + kp^m \sum_u u \sum_v v^{k-1} \quad (p^{2m})$$

on expanding by the binomial theorem. Here $\sum_v v^k = S_k(p^m)$. Further,

$$2 \sum_u u = p(p-1) \equiv 0 \quad (p).$$

Hence

$$S_k(p^{m+1}) \equiv pS_k(p^m), \quad (p^{m+1}) \tag{3.7}$$

where for $p = 2$ we have used the hypothesis that k is even.

On dividing by p^{m+1}, we can write (3.7) as

$$|p^{-m-1} S_k(p^{m+1}) - p^{-m} S_k(p^m)|_p \leq 1.$$

By the consequence (2.3) of the ultrametric inequality (1.2(iii)), it follows that

$$|p^{-\ell} S_k(p^\ell) - p^{-m} S_k(p^m)|_p \leq 1 \tag{3.8}$$

for any positive integers ℓ, m. Put $m = 1$ and let ℓ tend to infinity in the conventional sense, so $p^\ell \to 0$ in the p-adic sense. Then

$$|B_k - p^{-1} S_k(p)|_p \leq 1 \tag{3.9}$$

by (3.5).

Now

$$S_k(p) = \sum_0^{p-1} j^k$$

$$\equiv \begin{cases} -1 & \text{if} \quad (p-1)|k \quad (p) \\ 0 & \text{otherwise.} \end{cases} \tag{3.10}$$

Hence and by (3.9),

$$\left.\begin{array}{lll} |B_k + p^{-1}|_p \leq 1 & \text{if} & (p-1)\,|\,k \\ |B_k|_p \leq 1 & & \text{otherwise} \end{array}\right\} . \tag{3.11}$$

Put

$$W_k = B_k + \sum_{\substack{q \text{ prime} \\ (q-1)\,|\,k}} q^{-1} \tag{3.12}$$

If p is any prime, we have

$$W_k = (B_k + p^{-1}) + \sum_{q \neq p} q^{-1} \tag{3.13(i)}$$

or

$$W_k = B_k + \sum_q q^{-1} \tag{3.13(ii)}$$

according as p is, or is not, a q. In both cases (3.11) implies

$$|W_k|_p \leq 1, \quad (\text{all primes } p) \tag{3.14}$$

on using the consequence (2.2) of the ultrametric inequality. But (3.14) implies that the rational number W_k has no primes in its denominator, i.e. $W_k \in \mathbb{Z}$, as asserted.

Notes

§3 Theorem 3.1 was announced briefly by Clausen (1840). This prompted the paper of von Staudt (1840), who said he had known the result for some time. Witt's proof seems to have entered the folklore without being published by him. See also Chapter 12, §5.

Exercises

1. Let p be a prime and s a positive integer. Show that

$$|s|_p \geq s^{-1},$$

for the p-adic valuation, with equality precisely when s is a power of p.

2. Let $k \geq 4$ be even and $p \neq 2,3$. Show that

$$|p^{-m} S_k(p^m) - B_k|_p \leq p^{-2m+\varepsilon}$$

for all $m \geq 1$, where $\varepsilon = 1$ if $(p-1)|(k-2)$ and $\varepsilon = 0$ otherwise.

[Note. A numerical example is $p = 5$, $k = 4$, $m = 1$, so $\varepsilon = 0$. Then $S_4(5) = 354$, and

$$5^{-1} S_4(5) - B_4 = 425/6.$$

Hint. By (3.4)

$$|p^{-m} S_k(p^m) - B_k|_p \leq \max_{r=0}^{k-1} \left|\frac{B_r}{k+1-r}\right|_p p^{m(r-k)}$$

Now estimate the $|B_r|_p$ by (3.1 bis) and Theorem 3.1, and use Exercise 1.]

3. For positive integer m let N_m be the integral part of $(1+\sqrt{3})^{2m+1}$. Show that $|N_m|_2 = 2^{-m-1}$.