# Chapter 1

# VALUATIONS AND PSEUDO-VALUATIONS

It is shown in abstract algebra that there are only the following two distinct types of simple extensions of a field K.

A *simple transcendental extension* of K is obtained by adjoining an indeterminate x to K and forming the field K(x) of all rational expressions in x with coefficients in K. Apart from isomorphisms there is only one such extension of K.

Next there are the *simple algebraic extensions* of K of which there may be many. These may be obtained as follows. Denote again by x an indeterminate, further by K[x] the ring of all polynomials in x with coefficients in K, and by f(x) an element of K[x] which is monic (i.e. has highest coefficient 1) and irreducible over K. The polynomials divisible by f(x) form a prime ideal $\mathfrak{p}$ in K[x]. Divide the elements of K[x] into residue classes modulo $\mathfrak{p}$ by putting two elements into the same class if their difference is in $\mathfrak{p}$. These residue classes form together the residue class ring $K[x]/\mathfrak{p}$ which, in fact, turns out to be a field. Furthermore, the residue class, $\xi$ say, that contains the polynomial x, satisfies the equation $f(\xi) = 0$. In this way K has been extended to a field $K[x]/\mathfrak{p} = K(\xi)$ in which the equation $f(\xi) = 0$ has at least one root $\xi$. Apart from isomorphisms there is again only one such extension; but different monic irreducible polynomials f(x) will generate different simple algebraic extensions.

The construction of both extension fields K(x) and $K(\xi)$ does not require that K was already imbedded in a larger field, and it uses only algebraic processes. More important for the theory of Diophantine approximations is a non-algebraic method of field extension that is based on ideas from topology.

This non-algebraic method is applied already in elementary analysis where it serves to extend the field $\Gamma$ of the rational numbers to the larger field $P$ of the real numbers. Of the different variants of this method we select the one which has the advantage of easy generalization.

Define a real number $\alpha$ as the limit

$$\alpha = \lim_{m\to\infty} a_m$$

of a convergent sequence $\{a_m\} = \{a_1, a_2, a_3, \ldots\}$ of rational numbers; here the sequence is said to be convergent or a fundamental or Cauchy sequence if

$$\lim_{\substack{m\to\infty\\ n\to\infty}} |a_m - a_n| = 0.$$

Further two fundamental sequences $\{a_m\}$ and $\{b_m\}$ have the same limit if and only if

$$\lim_{m\to\infty} |a_m - b_m| = 0,$$

and the special sequence $\{a, a, a, \ldots\}$ has the rational limit a.

In this manner the rational field $\Gamma$ becomes inbedded in the real field $P$. We may now study subfields of $P$, and in particular simple extensions $\Gamma(\alpha)$ of $\Gamma$ where $\alpha$ is any chosen element of $P$. This construction of a simple extension of $\Gamma$ naturally is completely different from that by the abstract algebraic method. It becomes now an interesting problem to decide whether $\Gamma(\alpha)$ is a transcendental or algebraic extension of $\Gamma$, or, as we say, whether $\alpha$ is a transcendental or an algebraic real number. This problem will be studied in several of the later chapters.

## 1. Valuations and pseudo-valuations.

The construction just mentioned of the real numbers depends essentially on the fact that the function $|a|$ is a *valuation* of $\Gamma$. Here a valuation w(a) of an arbitrary field K denotes any real-valued function of the elements a of K which has the following properties,

(1): $$w(0) = 0, \text{ but } w(a) > 0 \text{ if } a \neq 0;$$

(2): $$w(ab) = w(a)w(b) \qquad \text{(product equation);}$$

(3): $$w(a\mp b) \leqslant w(a) + w(b) \qquad \text{(triangle inequality).}$$

If w(a) has the properties (1) and (3), but instead of (2) satisfies the weaker relation

(2'): $$w(ab) \leqslant w(a)w(b) \qquad \text{(product inequality),}$$

then w(a) is said to be a *pseudo-valuation* of K. It is clear that every valuation is also a pseudo-valuation; but the converse need not be true.

From these definitions the following properties follow easily. *When* w(a) *is a valuation:*

$$w(\mp 1) = 1, \qquad w(-a) = w(a),$$

$$w(a) - w(b) \leqslant w(a-b) \leqslant w(a) + w(b), \qquad |w(a) - w(b)| \leqslant w(a-b),$$

$$w\left(\prod_{\nu=1}^{n} a_\nu\right) = \prod_{\nu=1}^{n} w(a_\nu), \qquad w\left(\sum_{\nu=1}^{n} a_\nu\right) \leqslant \sum_{\nu=1}^{n} w(a_\nu).$$

*When* w(a) *is a pseudo-valuation:*

$$w(\mp 1) \geqslant 1, \qquad w(-a) = w(a),$$

$$w(a) - w(b) \leqslant w(a-b) \leqslant w(a) + w(b), \qquad |w(a) - w(b)| \leqslant w(a-b),$$

$$w\left(\prod_{\nu=1}^{n} a_\nu\right) \leqslant \prod_{\nu=1}^{n} w(a_\nu), \qquad w\left(\sum_{\nu=1}^{n} a_\nu\right) \leqslant \sum_{\nu=1}^{n} w(a_\nu).$$

Here n may be any positive integer.

Each field has at least one valuation, viz. the *trivial valuation* defined by

$$w_0(a) = \begin{cases} 0 \text{ if } a = 0, \\ 1 \text{ if } a \neq 0. \end{cases}$$

For the trivial valuation the triangle inequality (3) holds in the strengthened form

$$w_0(a \mp b) \leqslant \max[w_0(a), w_0(b)].$$

This we express by saying that $w_0(a)$ *is Non-Archimedean.* More generally, any valuation or pseudo-valuation $w(a)$ of K is called *Non-Archimedean* if always

(3'): $$w(a \mp b) \leqslant \max[w(a), w(b)];$$

but $w(a)$ is said to be *Archimedean* if this inequality is not satisfied for all a and b. Thus the valuation $|a|$ of $\Gamma$ is Archimedean.

## 2. The p-adic valuations of $\Gamma$.

In addition to $|a|$ and $w_0(a)$, the rational field $\Gamma$ possesses yet infinitely many other valuations. For let p be any one of the infinitely many primes 2,3,5,.... . Denote by $|a|_p$ the function on $\Gamma$ defined as follows,

(i): $$|0|_p = 0;$$

(ii): if $a \neq 0$ is any other element of $\Gamma$, let n be the unique integer such than $p^{-n}a = \frac{r}{s}$ where both integers r and s are prime to p; then put

$$|a|_p = p^{-n}.$$

It is not difficult to prove that $|a|_p$ is a valuation of $\Gamma$, and that it is Non-Archimedean. For $|a|_p$ has the property (1); and if at least one of a and b vanishes, then properties (2) and (3') are trivially satisfied. If, however, both $a \neq 0$ and $b \neq 0$, let $\nu$ be the integer such that $p^{-\nu}b = \frac{\rho}{\sigma}$ where $\rho$ and $\sigma$ are prime to p. Now (2) follows from

$$p^{-n-\nu}ab = \frac{r\rho}{s\sigma}$$

since $r\rho$ and $s\sigma$ are prime to p. Assume further that, say $n \leqslant \nu$. Then

$$p^{-n}(a \mp b) = \frac{r\sigma \mp p^{\nu-n}s\rho}{s\sigma}$$

where $s\sigma$ is prime to p, but $r\sigma \mp p^{\nu-n}s\rho$ may still be divisible by a positive power of p, so that

$$|a \mp b|_p \leqslant p^{-n} = \max(|a|_p, |b|_p).$$

We call $|a|_p$ the p-*adic valuation* of $\Gamma$, and also say that $|a|_p$ is the p-adic *value of* a.

If q is an arbitrary prime, evidently

$$|q|_p = \begin{cases} \frac{1}{p} & \text{if } q = p, \\ 1 & \text{if } q \neq p. \end{cases}$$

This means that p-*adic valuations belonging to different primes* p *are distinct.* Therefore $\Gamma$ possesses an infinite set of distinct valuations,

$$w_0(a), \ |a|, \ |a|_p \text{ for all primes p.}$$

These valuations are related to one another by the

FUNDAMENTAL IDENTITY: $|a| \prod_p |a|_p = w_0(a)$ if $a \epsilon \Gamma$,

a formula which is equivalent to the fundamental theorem of arithmetic on the unique factorisation of integers. The product $\prod_p$ in this identity runs over all primes; note that for $a \neq 0$ all but finitely many of the factors $|a|_p$ are equal to 1.

Of particular interest is the case when a is an integer distinct from zero when evidently

$$w_0(a) = 1, \ |a| \geqslant 1, \ |a|_p \leqslant 1 \text{ for all primes } p.$$

Denote by $p_1, p_2, \ldots., p_r$ an arbitrary set of finitely many distinct primes. The fundamental identity leads then immediately to the

FUNDAMENTAL INEQUALITY: $|a| \prod_{j=1}^{r} |a|_{p_j} \geqslant 1.$

*This inequality is basic for our whole theory.*

Remark: It is shown in valuation theory[1]) how valuations of a field K can be continued into simple algebraic extensions of K. If K is the rational field, these extensions become finite algebraic number fields $\Lambda$. One finds that, apart from the trivial valuation, $\Lambda$ possesses finitely many Archimedean valuations and an enumerably-infinite set of Non-Archimedean valuations. These valuations satisfy again both a fundamental identity and a fundamental inequality very similar to those for $\Gamma$. It is therefore possible to develop a theory of Diophantine approximations over $\Lambda$ which is completely analogous to that over $\Gamma$ which is treated in these lectures. Very little new is required for the more general theory; but formulae naturally become rather more involved. For this reason I shall not deal with the more general theory except in Appendix C.

## 3. A further example.

There is yet another class of fields for which a theory of Diophantine approximations may be developed. This are the simple transcendental extensions $K = \Sigma(x)$ of an arbitrary field $\Sigma$.

Of main interest for the theory are those valuations of K that become identical with the trivial valuation when a lies in the ground field $\Sigma$. The following construction produces infinitely many of them.

Denote again by $\Sigma[x]$ the ring of polynomials in x with coefficients in $\Sigma$; let further p be any "prime", i.e., a monic irreducible polynomial in $\Sigma[x]$. Also let $\theta$ be a real constant such that $0 < \theta < 1$.

If $r \neq 0$ is an arbitrary element of $\Sigma[x]$, we shall write deg r for the degree of r and $\text{ord}_p\, r$ for the order of r at p, i.e., the largest integer g such that $p^g$ is a factor of r.

Every element $a \neq 0$ of K may now be written in a unique way as a quotient $a = \frac{r}{s}$ of two polynomials r and s in $\Sigma[x]$ that are relatively prime and where s is monic and not the zero polynomial. In terms of r and s put

[1] See e.g. the 10th chapter of Modern Algebra by van der Waerden.

$$||a|| = \begin{cases} 0 & \text{if } a = 0, \\ \theta^{\deg s - \deg r} & \text{if } a \neq 0, \end{cases} \qquad ||a||_p = \begin{cases} 0 & \text{if } a = 0, \\ \theta^{\operatorname{ord}_p r - \operatorname{ord}_p s} & \text{if } a \neq 0. \end{cases}$$

There is no difficulty in proving that these two functions of $a$ are Non-Archimedean valuations of K and that

$$w_0(a), \ ||a||, \ ||a||_p \text{ for all ``primes'' } p$$

form a system of distinct valuations. One may adapt Euclid's method for proving that there are infinitely many rational "primes" and so prove[2] that this system has infinitely many elements.

Since the polynomials in $\Sigma[x]$ satisfy the law of unique factorisation.into "primes", there is again a fundamental identity. It takes in this case the form

$$||a|| \prod_p ||a||_p^{\deg p} = w_0(a) \text{ if } a \in K,$$

where the product $\prod_p$ extends over all "primes" p. There is also a fundamental inequality: if $p_1, p_2, \ldots, p_r$ are finitely many distinct "primes" and $a \neq 0$ is an element of $\Sigma[x]$, then

$$||a|| \prod_{j=1}^{r} ||a||_{p_j}^{\deg p_j} \geqslant 1 .$$

These two properties allow to develop a theory of Diophantine approximations over $K = \Sigma(x)$ which proves to be very similar to that for $\Gamma$ treated in these lectures. Although we shall not deal with this theory, the valuations of K will occasionally be used by way of example.

## 4. Valuations and pseudo-valuations derived from given ones.

Let K be any field and w(a) any valuation or pseudo-valuation of K. If $\lambda$ is any constant such that

$$0 < \lambda < 1,$$

put

$$w^*(a) = w(a)^\lambda.$$

Then $w^*(a)$ *is likewise a valuation or pseudo-valuation of* K, *respectively*.

For that $w^*(a)$ has the properties (1) and (2) or (2') is obvious, but we still have to prove that also the triangle inequality (3) is satisfied. Now one shows easily that if x and y are non-negative real numbers, then[3])

$$(x+y)^\lambda \leqslant x^\lambda + y^\lambda.$$

Hence from the properties (1) and (3) of w(a),

[2] If $p_1, p_2, \ldots, p_r$ are finitely many distinct "primes" in $\Sigma[x]$, $p_1 p_2 \ldots p_r + 1$ is divisible by a "prime" distinct from the given ones.

[3] For fixed $x \geqslant 0$ and variable $y > 0$ the function $f(y) = (x+y)^\lambda - y^\lambda$ has the derivative $\frac{df(x)}{dy} = \lambda\{(x+y)^{\lambda-1} - y^{\lambda-1}\} < 0$. Hence f (y) assumes its maximum at y = 0, and this maximum is $f(0) = x^\lambda$.

$$w^*(a+b) = w(a+b)^\lambda \leq \{w(a) + w(b)\}^\lambda \leq w(a)^\lambda + w(b)^\lambda = w^*(a) + w^*(b),$$

as asserted.

If $w(a)$ is Non-Archimedean, this proof becomes superfluous. It is, in fact, now obvious from (3') that, if $\lambda$ is any positive constant, $w^*(a) = w(a)^\lambda$ is likewise a Non-Archimedean valuation or pseudo-valuation, respectively.—

Next let $w_1(a), \ldots, w_r(a)$, where $r \geqslant 2$, be finitely many valuations or pseudo-valuations of K. *Then the maximum*

$$w_\Sigma(a) = \max_{j=1,2,\ldots,r} w_j(a)$$

*is again a pseudo-valuation* of K.

For $w_\Sigma(a)$ trivially has the property (1). Next,

$$w_\Sigma(ab) = \max_{j=1,2,\ldots,r} w_j(ab) \leq \max_{j=1,2,\ldots,r} w_j(a) w_j(b) \leq \max_{j=1,2,\ldots,r} w_j(a) \,.\, \max_{j=1,2,\ldots,r} w_j(b) =$$

$$= w_\Sigma(a) w_\Sigma(b),$$

and so $w_\Sigma(a)$ has the property (2'). Finally,

$$w_\Sigma(a \mp b) = \max_{j=1,2,\ldots r} w_j(a \mp b) \leq \max_{j=1,2,\ldots,r} \{w_j(a) + w_j(b)\} \leq$$

$$\leq \max_{j=1,2,\ldots,r} w_j(a) + \max_{j=1,2,\ldots,r} w_j(b) = w_\Sigma(a) + w_\Sigma(b),$$

which shows that $w_\Sigma(a)$ also satisfies the triangle inequality (3).

We say that $w_\Sigma(a)$ is the *sum* of $w_1(a), \ldots, w_r(a)$, and we call $w_1(a), \ldots, w_r(a)$ the *terms* of $w_\Sigma(a)$.

If all these terms are Non-Archimedean, it is again easy to see that their sum is likewise Non-Archimedean; for now

$$w_\Sigma(a \mp b) = \max_{j=1,2,\ldots,r} w_j(a \mp b) \leq \max_{j=1,2,\ldots,r} \max\{w_j(a), w_j(b)\} =$$

$$= \max\left[\max_{j=1,2,\ldots,r} w_j(a), \max_{j=1,2,\ldots,r} w_j(b)\right] = \max\{w_\Sigma(a), w_\Sigma(b)\}.$$

Of particular interest for us is the case when all terms $w_1(a), \ldots, w_r(a)$ of $w_\Sigma(a)$ *are valuations*. This does *not* imply that $w_\Sigma(a)$ is necessarily also a valuation. For instance, in the trivial example

$$K = \Gamma, \qquad w_\Sigma(a) = \max(|a|, |a|^{\frac{1}{3}}),$$

we have

$$w_\Sigma(\tfrac{1}{2}) = (\tfrac{1}{2})^{\frac{1}{3}}, \qquad w_\Sigma(2) = 2, \qquad w_\Sigma(\tfrac{1}{2} \cdot 2) = 1 \neq (\tfrac{1}{2})^{\frac{1}{3}} \cdot 2.$$

But although $w_\Sigma(a)$ need not be a valuation, it does have two simple properties that a general pseudo-valuation need not have:

(I): *If* $n$ *is a positive integer, then for all* $a$ *in* K,

$$w_\Sigma(a^n) = w_\Sigma(a)^n.$$

(II): *If* $g \neq 0$ *is an element of* K *such that*

$$w_1(g) = \ldots = w_r(g) = w_\Sigma(g),$$

and if a is an arbitrary element of K, then

$$w_\Sigma(ag) = w_\Sigma(a)w_\Sigma(g)$$

*and more generally,*

$$w_\Sigma(ag^n) = w_\Sigma(a)w_\Sigma(g)^n \quad \textit{for all integers } n.$$

These properties follow immediately from the product equation (2) for the terms $w_j(a)$ of $w_\Sigma(a)$.

By way of example, the rational field $\Gamma$ has the pseudo-valuations

$$\max(|a|_{p_1}^{\lambda_1}, \ldots, |a|_{p_r}^{\lambda_r})$$

and

$$\max(|a|^{\lambda}, |a|_{p_1}^{\lambda_1}, \ldots, |a|_{p_r}^{\lambda_r})$$

where $p_1, \ldots, p_r$ are finitely many distinct primes and $\lambda, \lambda_1, \ldots, \lambda_r$ are real constants satisfying

$$0 < \lambda \leqslant 1, \ \lambda_1 > 0, \ldots, \lambda_r > 0.$$

These pseudo-valuations of $\Gamma$ have then the properties (I) and (II).

The constructions of this section are by no means the only ones that allow to derive new valuations or pseudo-valuations from given ones, but they suffice for the purpose of these lectures. For other operations the reader is referred to a joint paper by P. Cohn and myself[4].

## 5. Bounded sequences, fundamental sequences, and null sequences.

In the next few sections we shall now generalise the method of the introduction for defining real numbers as limits of convergent sequences of rational numbers.

Let K be an arbitrary field with the valuation or pseudo-valuation w(a), and let

$$\{a_m\} = \{a_1, a_2, a_3, \ldots\}$$

be an arbitrary infinite sequence of elements of K.

Such a sequence is said to be *a bounded sequence with respect to* w(a) if there exist two positive numbers p and M such that

$$w(a_m) < M \quad \text{for all } m \geqslant p;$$

it is said to be *a fundamental sequence with respect to* w(a) if, given any $\epsilon > 0$, there is a positive number $q(\epsilon)$ such that

$$w(a_m - a_n) < \epsilon \quad \text{for all } m \geqslant q(\epsilon) \text{ and all } n \geqslant q(\epsilon);$$

and it is said to be *a null sequence with respect to* w(a) if, given any $\epsilon > 0$, there is a positive number $r(\epsilon)$ such that

$$w(a_m) < \epsilon \quad \text{for all } m \geqslant r(\epsilon).$$

[4] Nieuw Archief voor Wiskunde (3), 1 (1953), 161-198.

It is obvious that *if* $\{a_m\}$ *is a bounded, or a fundamental, or a null sequence, then*

$$\{-a_m\} = \{-a_1, -a_2, -a_3, \ldots\}$$

*is a sequence of the same kind.* The following lemmas also are easy consequences of the definitions.

(a): *Every fundamental sequence is bounded.*

For let p be an integer not less than q(1), and let $m \geqslant p$. Then

$$w(a_m) = w\{a_p + (a_m - a_p)\} \leqslant w(a_p) + w(a_m - a_p) < w(a_p) + 1, = M \text{ say.}$$

(b): *Every null sequence is a fundamental sequence.*

For let $m \geqslant r(\frac{1}{2}\epsilon)$ and $n \geqslant r(\frac{1}{2}\epsilon)$. Then

$$w(a_m) < \tfrac{1}{2}\epsilon,\ w(a_n) < \tfrac{1}{2}\epsilon,\ w(a_m - a_n) \leqslant w(a_m) + w(a_n) < \tfrac{1}{2}\epsilon + \tfrac{1}{2}\epsilon = \epsilon.$$

(c): *If* $\{a_m\}$ *is a fundamental sequence, but not a null sequence, there exist two positive numbers* s *and* N *such that*

$$w(a_m) > N \text{ for all } m \geqslant s.$$

For assume that $\{a_m\}$ is a fundamental sequence, but that there are no such numbers s and N. Then, however small $\epsilon > 0$ is chosen, there exist arbitrarily large suffixes n such that $w(a_n) < \frac{1}{2}\epsilon$. There is then also a suffix n of this kind satisfying $n \geqslant q(\frac{1}{2}\epsilon)$, and now also

$$w(a_m - a_n) < \tfrac{1}{2}\epsilon \text{ for all } m \geqslant q(\tfrac{1}{2}\epsilon).$$

Hence, for all $m \geqslant q(\frac{1}{2}\epsilon)$,

$$w(a_m) = w\{a_n + (a_m - a_n)\} \leqslant w(a_n) + w(a_m - a_n) < \tfrac{1}{2}\epsilon + \tfrac{1}{2}\epsilon = \epsilon,$$

and so $\{a_m\}$ is a null sequence.

In the next two lemmas we denote by p', M', q'(ε), and r'(ε) the numbers corresponding to p, M, q(ε), and r(ε), respectively, that belong to the second sequence $\{b_m\}$.

(d): *If* $\{a_m\}$ *and* $\{b_m\}$ *are fundamental sequences, so are*

$$\{a_m + b_m\},\ \{a_m - b_m\}, \text{ and } \{a_m b_m\}.$$

For first,

$$w\{(a_m \mp b_m) - (a_n \mp b_n)\} = w\{(a_m - a_n) \mp (b_m - b_n)\} \leqslant w(a_m - a_n) + w(b_m - b_n) < \tfrac{1}{2}\epsilon + \tfrac{1}{2}\epsilon = \epsilon$$

provided that

$$m \geqslant \max\{q(\tfrac{1}{2}\epsilon), q'(\tfrac{1}{2}\epsilon)\} \text{ and } n \geqslant \max\{q(\tfrac{1}{2}\epsilon), q'(\tfrac{1}{2}\epsilon)\}.$$

Secondly, by (a) the sequences are bounded and therefore

$$w(a_m b_m - a_n b_n) = w\{(a_m - a_n)b_m + a_n(b_m - b_n)\} \leqslant w(a_m - a_n)w(b_m) + w(a_n)w(b_m - b_n) <$$

$$< \frac{\epsilon}{2M'} M' + M \frac{\epsilon}{2M} = \epsilon$$

provided that

$$m \geq \max\left[q\left(\frac{\epsilon}{2M'}\right), q'\left(\frac{\epsilon}{2M}\right), p, p'\right] \text{ and } n \geq \max\left[q\left(\frac{\epsilon}{2M'}\right), q'\left(\frac{\epsilon}{2M}\right), p, p'\right].$$

(e): *If* $\{a_m\}$ *and* $\{b_m\}$ *are null sequences, so are* $\{a_m+b_m\}$ *and* $\{a_m-b_m\}$. *If* $\{a_m\}$ *is a null sequence, and* $\{b_m\}$ *is bounded, then* $\{a_mb_m\}$ *is a null sequence.*

The first assertion holds because

$$w(a_m \mp b_m) \leq w(a_m) + w(b_m) < \frac{1}{2}\epsilon + \frac{1}{2}\epsilon = \epsilon \text{ is } m \geq \max\left[r\left(\frac{1}{2}\epsilon\right), r'\left(\frac{1}{2}\epsilon\right)\right],$$

and the second one because

$$w(a_mb_m) \leq w(a_m)\, w(b_m) < \frac{\epsilon}{M'} M' = \epsilon \text{ if } m \geq \max\left[r\left(\frac{\epsilon}{M'}\right), p'\right] .$$

## 6. The ring $\{K\}_w$ and the ideal $\mathfrak{p}$ .

Denote by $\{K\}_w$ the set of all fundamental sequences of K with respect to the valuation or pseudo-valuation $w(a)$. On account of (d) we may then define for the elements of $\{K\}_w$ operations of addition, subtraction and multiplication by the formulae,

$$\{a_m\}+\{b_m\} = \{a_m+b_m\}, \qquad \{a_m\}-\{b_m\} = \{a_m-b_m\}, \qquad \{a_m\}\{b_m\} = \{a_mb_m\} .$$

It is easily verified that, with respect to these operations, $\{K\}_w$ satisfies the commutative, associative, and distributive laws of addition and multiplication, and that subtraction is the inverse operation to addition; further

$$\{0\} = \{0,0,0,\ldots\} \qquad \text{and} \qquad \{1\} = \{1,1,1,\ldots\}$$

are the zero and unit elements of $\{K\}_w$. Since, e.g.

$$\{1,0,0,0,\ldots\}\{0,1,0,0,\ldots\} = \{0\},$$

$\{K\}_w$ is then a commutative ring with unit element, but is neither a field nor even a domain of integrity on account of these zero divisors.

Let $\mathfrak{p}$ denote the subset of $\{K\}_w$ consisting of all null sequences.

(f): *The set* $\mathfrak{p}$ *is an ideal of* $\{K\}_w$. *If* $w(a)$ *is a valuation, then* $\mathfrak{p}$ *is a prime ideal of* $\{K\}_w$.

From (e), if $\{a_m\}$ and $\{b_m\}$ are elements of $\mathfrak{p}$, so are $\{a_m\} + \{b_m\}$ and $\{a_m\} - \{b_m\}$; if further $\{a_m\}$ belongs to $\mathfrak{p}$ and $\{b_m\}$ to $\{K\}_m$, then $\{a_m\}\{b_m\}$ is an element of $\mathfrak{p}$. Hence $\mathfrak{p}$ is an ideal.

Next assume that $w(a)$ is a valuation. It suffices to show that if $\{a_m\}$ and $\{b_m\}$ belong to $\{K\}_w$, but not to $\mathfrak{p}$, then their product likewise is not an element of $\mathfrak{p}$. By (c), the hypothesis implies that there are four positive numbers $s$, $N$, $s'$, and $N'$ such that

$$w(a_m) > N \text{ if } m \geq s \qquad \text{and} \qquad w(b_m) > N' \text{ if } m \geq s'.$$

Hence

$$w(a_mb_m) = w(a_m)w(b_m) > NN' \text{ if } m \geq \max(s,s'),$$

and hence $\{a_m\}\{b_m\}$ is not a null sequence.

When $w(a)$ is not a valuation but only a pseudo-valuation, this proof is not valid, and then $\mathfrak{p}$ need not be a prime ideal.

## 7. The residue class ring $K_w$.

If the difference $\{a_m\} - \{b_m\} = \{a_m - b_m\}$ of two fundamental sequences $\{a_m\}$ and $\{b_m\}$ lies in $\mathfrak{p}$, i.e., is a null sequence, then the two sequences are said to be *congruent modulo* $\mathfrak{p}$, and we write

$$\{a_m\} \equiv \{b_m\} \pmod{\mathfrak{p}}, \text{ or simply } \{a_m\} \equiv \{b_m\}.$$

This is in agreement with the usual notation of congruence modulo an ideal. It is also well known that such congruence is an *equivalence relation;* i.e., in the present case the following three laws hold:

$$\{a_m\} \equiv \{a_m\};$$

$$\text{if } \{a_m\} \equiv \{b_m\}, \text{ then } \{b_m\} \equiv \{a_m\};$$

$$\text{if } \{a_m\} \equiv \{b_m\} \text{ and } \{b_m\} \equiv \{c_m\}, \text{ then } \{a_m\} \equiv \{c_m\}.$$

For $\{a_m\} - \{a_m\} = \{0\}$ is a null sequence; if $\{a_m\} - \{b_m\}$ is a null sequence, so is $\{b_m\} - \{a_m\} = -(\{a_m\} - \{b_m\})$; and if $\{a_m\} - \{b_m\}$ and $\{b_m\} - \{c_m\}$ are null sequences, so is

$$\{a_m\} - \{c_m\} = (\{a_m\} - \{b_m\}) + (\{b_m\} - \{c_m\}).$$

On account of this property, we may subdivide the elements of $\{K\}_w$ into classes by putting into the same class all fundamental sequences that are congruent modulo $\mathfrak{p}$ to one given fundamental sequence. Denote by $K_w$ the set of all such *residue classes modulo* $\mathfrak{p}$; in the notation of algebra, $K_w = \{K\}_w/\mathfrak{p}$.

Let $\alpha$ and $\beta$ be two elements of $K_w$, and let, say, $\{a_m\}$ and $\{a'_m\}$ be any two fundamental sequences in the residue class $\alpha$ and $\{b_m\}$ and $\{b'_m\}$ any two fundamental sequences in the residue class $\beta$. Hence both $\{a_m - a'_m\}$ and $\{b_m - b'_m\}$ are null sequences. It follows then that also

$$\{(a_m \mp b_m) - (a'_m \mp b'_m)\} = \{a_m - a'_m\} \mp \{b_m - b'_m\}$$

and

$$\{a_m b_m - a'_m b'_m\} = \{a_m - a'_m\}\{b_m\} + \{a'_m\}\{b_m - b'_m\}$$

are null sequences, and that therefore

$$\{a_m\} + \{b_m\} \equiv \{a'_m\} + \{b'_m\}, \quad \{a_m\} - \{b_m\} \equiv \{a'_m\} - \{b'_m\}, \quad \{a_m\}\{b_m\} \equiv \{a'_m\}\{b'_m\}.$$

We have thus proved that the residue classes, $\alpha + \beta$, $\alpha - \beta$, and $\alpha\beta$ say, that contain the fundamental sequences $\{a_m + b_m\}$, $\{a_m - b_m\}$, and $\{a_m b_m\}$, respectively, remain unchanged if $\{a_m\}$ is replaced by any congruent sequence $\{a'_m\}$, and $\{b_m\}$ is replaced by any congruent sequence $\{b'_m\}$.

Hence $K_w$ admits the operations of addition, subtraction, and multiplication and so is a ring. It is also obvious, from the definitions of these operations, that addition and multiplication in $K_w$ are commutative, associative, and distributive, and that subtraction is the inverse operation to addition.

If a is any element of K, the ring $K_w$ contains the special residue class, (a) say, that is defined by the fundamental sequence $\{a\} = \{a, a, a, \ldots\}$. In particular, (0) is the zero element of $K_w$ and is identical with the set of all null sequences, and (1) is the unit element of $K_w$. Since, evidently,

$$(a) + (b) = (a+b), \qquad (a) - (b) = (a-b), \qquad (a)(b) = (ab),$$

the elements (a) of $K_w$ form a ring that is isomorphic to K. In fact, *they form a field isomorphic to* K, (K) say. For (a) is distinct from (0) if and only if $a \neq 0$, and then (a) has the inverse $(a^{-1})$ because $(a)(a^{-1}) = (1)$.

From now on we shall *not* distinguish between the element (a) of (K) and the corresponding element a of K, thus shall identify (K) with the original field K. It may then be said that *the ring* $K_w$ of all residue classes modulo $\mathfrak{p}$ *contains* K *as a subfield.* We call $K_w$ the *completion of* K *with respect to* w(a).

## 8. The completion of a field with respect to a valuation.

Of particular interest is the case when w(a) is a valuation.

(g): *If* w(a) *is a valuation of* K, *then the completion* $K_w$ *is a field.*

It suffices to show that if $\alpha$ is any element of $K_w$ distinct from zero, there exists a second element of $K_w$, $\alpha^{-1}$ say, such that $\alpha\alpha^{-1} = 1$. Let $\{a_m\}$ be an arbitrary fundamental sequence in the residue class $\alpha$; since $\alpha \neq 0$, this sequence is not a null sequence. There are then by (c) two positive numbers s and N such that

$$w(a_m) > N \text{ and hence } a_m \neq 0 \text{ if } m \geqslant s.$$

Put

$$a_m^* = 0 \text{ if } 1 \leqslant m < s, \qquad a_m^* = \frac{1}{a_m} \text{ if } m \geqslant s.$$

The new sequence $\{a_m^*\}$ is likewise a fundamental sequence because, for $m \geqslant s$ and $n \geqslant s$,

$$w(a_m^* - a_n^*) = w\left(\frac{1}{a_m} - \frac{1}{a_n}\right) = \frac{w(a_m - a_n)}{w(a_m)w(a_n)} < \frac{1}{N^2}\, w(a_m - a_n),$$

and hence

$$w(a_m^* - a_n^*) < \epsilon \text{ if } m \geqslant \max\{q(N^2\epsilon), s\},\ n \geqslant \max\{q(N^2\epsilon), s\}.$$

Denote by $\alpha^{-1}$ the residue class of $\{a_m^*\}$. Then $\alpha\alpha^{-1} = 1$, since

$$\{a_m\}\{a_m^*\} = \{a_m a_m^*\}, \text{ where } a_m a_m^* = 1 \text{ if } m \geqslant s.$$

When w(a) is only a pseudo-valuation, $K_w$ in general will not be a field, but may contain divisors of zero. One such case will soon be discussed.

## 9. The limit notation.

Let again K be a field, w(a) a valuation or pseudo-valuation of K, and $K_w$ the completion of K with respect to w(a). It is convenient, and in agreement with the usual convention for the real field, to adopt the following notation.

If $\{a_m\}$ is any fundamental sequence, and if $\alpha$ is its residue class in $K_w$, then we say that $\alpha$ *is the limit of* $a_m$ *with respect to* w(a) *as* m *tends to infinity*, and we write

$$\alpha = \lim_{m\to\infty} a_m \, (w).$$

From the definition of $\alpha$, *this limit is naturally unique.* For the fundamental sequence of the special form $\{a\} = \{a, a, a, \ldots\}$ we have

$$a = \lim_{m\to\infty} a \; (w)$$

since this sequence lies in the residue class (a) which we have identified with the element a of K.

The definition of the operations in $K_w$ immediately implies that, if

$$\beta = \lim_{m\to\infty} b_m \, (w)$$

is a second limit, then

$$\alpha + \beta = \lim_{m\to\infty} (a_m + b_m)(w), \quad \alpha - \beta = \lim_{m\to\infty} (a_m - b_m)(w), \quad \alpha\beta = \lim_{m\to\infty} (a_m b_m)(w).$$

Let, in particular, w(a) be a valuation, and assume that $\beta \neq 0$ and that all $b_m$ are distinct from zero. It follows then from (g) that

$$\beta^{-1} = \lim_{m\to\infty} \frac{1}{b_m} \, (w).$$

Hence in this case also

$$\frac{\alpha}{\beta} = \alpha\beta^{-1} = \lim_{m\to\infty} \frac{a_m}{b_m} \, (w).$$

## 10. The continuation of w(a) onto $K_w$.

Let

$$\alpha = \lim_{m\to\infty} a_m(w) \, .$$

From the definition of a fundamental sequence with respect to w(a),

$$|w(a_m) - w(a_n)| \leq w(a_m - a_n) < \epsilon \text{ if } m \geq q(\epsilon) \text{ and } n \geq q(\epsilon) \, .$$

Hence $\{w(a_m)\}$ *is a convergent sequence of real numbers, and the real limit*

$$\lim_{m\to\infty} w(a_m), = W(\alpha) \text{ say,}$$

exists.

(h): $W(\alpha)$ *depends only on $\alpha$, and not on the fundamental sequence as the limit of which $\alpha$ is defined.*

For let also

$$\alpha = \lim_{m\to\infty} a'_m(w).$$

Then $\{a_m - a'_m\}$ is a null sequence and therefore

$$\lim_{m\to\infty} w(a_m - a'_m) = 0.$$

It follows then that

$$0 \leq |\lim_{m\to\infty} w(a_m) - \lim_{m\to\infty} w(a'_m)| = \lim_{m\to\infty} |w(a_m) - w(a'_m)| \leq \lim_{m\to\infty} w(a_m - a'_m) = 0,$$

whence

$$\lim_{m\to\infty} w(a_m) = \lim_{m\to\infty} w(a'_m).$$

(i): $W(a) = w(a)$ *when* a *is any element of* K.

For now $a = (a)$ is the limit of the fundamental sequence $\{a\}$ and hence

$$W(a) = \lim_{m\to\infty} w(a) = w(a).$$

(j): $W(\alpha)$ *is a pseudo-valuation of* $K_w$. *It is a valuation if* $w(a)$ *is a valuation; it is Archimedean if* $w(a)$ *is, and it is Non-Archimedean if* $w(a)$ *is.*

First, the definition of $W(\alpha)$ implies that this function vanishes only if $\alpha = 0$ and is otherwise positive. Secondly,

$$W(\alpha\beta) = \lim_{m\to\infty} w(a_m b_m) \leq \lim_{m\to\infty} w(am)w(b_m) = \lim_{m\to\infty} w(a_m) \lim_{m\to\infty} w(bm) = W(\alpha)W(\beta),$$

with equality if $w(a)$ is a valuation. Third,

$$W(\alpha\mp\beta) = \lim_{m\to\infty} w(a_m \mp bm) \leq \lim_{m\to\infty} (w(a_m) + w(b_m)) = \lim_{m\to\infty} w(a_m) + \lim_{m\to\infty} w(b_m) =$$

$$= W(\alpha) + W(\beta) .$$

When $w(a)$ is Non-Archimedean, we have instead

$$W(\alpha\mp\beta) = \lim_{m\to\infty} w(a_m \mp bm) \leq \lim_{m\to\infty} \max\{w(a_m), w(bm)\} =$$

$$= \max\{\lim_{m\to\infty} w(a_m), \lim_{m\to\infty} w(b_m)\} = \max(W(\alpha), W(\beta)),$$

and it is trivial that if $W(\alpha)$ is Non-Archimedean, so is $w(a)$.

The valuation or pseudo-valuation $W(\alpha)$ is called the *continuation of* $w(a)$ *onto the completion* $K_w$. Since $W(\alpha)$ and $w(a)$ are identical on K, and $w(a)$ has so far only been defined on K, we shall in future write $w(\alpha)$ for $W(\alpha)$ whether $\alpha$ is an element of K or of $K_w$.

## 11. The elements of K lie dense in $K_w$.

In real analysis, the limit $\alpha$ of a convergent sequence $\{a_m\}$ of rational numbers satisfies the limit relation

$$\lim_{m\to\infty} |\alpha - a_n| = 0.$$

We show now that an analogous relation holds also for K and $K_w$.

Let

$$\alpha = \lim_{m\to\infty} a_m (w) .$$

Since also

$$a_n = \lim_{m\to\infty} a_n(w) \qquad (n = 1,2,3,...),$$

it follows that

$$\alpha - a_n = \lim_{m\to\infty} (a_m - a_n)(w) \qquad (n = 1,2,3,...)$$

and hence

$$w(\alpha - a_n) = \lim_{m\to\infty} w(a_m - a_n) \qquad (n = 1,2,3,...).$$

Now, by the hypothesis,

$$w(a_m - a_n) < \epsilon \text{ if } m \geqslant q(\epsilon) \text{ and } n \geqslant q(\epsilon),$$

and therefore

$$0 \leqslant w(\alpha - a_n) = \lim_{m\to\infty} (a_m - a_n) \leqslant \epsilon \text{ if } n \geqslant q(\epsilon).$$

Since $\epsilon > 0$ may be arbitrarily small, this means that

$$\lim_{n\to\infty} w(\alpha - a_n) = 0.$$

*Thus the elements of* $K_w$ *may be approximated arbitrarily closely with respect to* $w(\alpha)$ *by the elements of* K.

## 12. Fundamental sequences in $K_w$.

The construction in §§ 5-9 of $K_w$, the completion of K with respect to w(a), is independent of the hypothesis that K is a *field* and remains valid when K is any commutative *ring*. In particular, even under this more general assumption the following properties still remain true:

Null sequences are fundamental sequences; sum and difference of two fundamental sequences are fundamental sequences; and sum and difference of two null sequences are null sequences.

Let us apply this remark to the ring $K_w$ and its valuation or pseudo-valuation $w(\alpha)$. We may form "new" fundamental sequences and null sequences consisting of elements of $K_w$ instead of K, and by means of these construct the completion, $(K_w)_w$ say, of $K_w$ with respect to $w(\alpha)$. However, as will now be proved, the "new" fundamental sequences have already limits in $K_w$ itself, and so this complicated procedure is unnecessary.

(k): *Let* $\{\alpha_m\} = \{\alpha_1, \alpha_2, \alpha_3, ...\}$ *be a fundamental sequence of* $K_w$ *with respect to* $w(\alpha)$. *There exists an element* $\alpha$ *of* $K_w$ *such that*

$$\lim_{m\to\infty} w(\alpha - \alpha_m) = 0.$$

By what was proved in § 11, we can find for each $\alpha_m$ an element $a_m$ of K such that $w(\alpha_m - a_m)$ is arbitrarily small, say

$$w(\alpha_m - a_m) < \frac{1}{m} \qquad (m = 1,2,3,...).$$

The sequence

$$\{\alpha_m - a_m\} = \{\alpha_1 - a_1, \alpha_2 - a_2, \alpha_3 - a_3, \ldots\}$$

is therefore a "new" null sequence and hence also a "new" fundamental sequence. The difference of the two fundamental sequences,

$$\{a_m\} = \{\alpha_m\} - \{\alpha_m - a_m\}$$

is therefore likewise a "new" fundamental sequence. But since its elements $a_m$ belong to K, and because $w(\alpha)$ is the continuation of $w(a)$, it follows that $\{a_m\}$ is a fundamental sequence of K with respect to $w(a)$. Let

$$\alpha = \lim_{m\to\infty} a_m(w)$$

be its limit in $K_w$. Then, by § 11,

$$\lim_{m\to\infty} w(\alpha - a_m) = 0,$$

so that $\{\alpha - a_m\}$ is a "new" null sequence. But then the difference of the two null sequences

$$\{\alpha - \alpha_m\} = \{\alpha - a_m\} - \{\alpha_m - a_m\}$$

is likewise a "new" null sequence, whence the assertion.

This result shows that every "new" fundamental sequence $\{\alpha_m\}$ differs only by a "new" null sequence $\{\alpha - \alpha_m\}$ from a "new" fundamental sequence of the special form $\{\alpha\} = \{\alpha, \alpha, \alpha, \ldots\}$ where $\alpha \epsilon K$. Thus the completion $(K_w)_w$ of $K_w$ is isomorphic to, and may be identified with, $K_w$. We may also write

$$\alpha = \lim_{m\to\infty} \alpha_m(w),$$

just as is done in real analysis. Then these "new" limits satisfy the same rules as did the limits of fundamental sequences $\{a_m\}$ of K. It is for these reasons that $K_w$ was called the completion of K with respect to the valuation or pseudo-valuation $w(a)$.

## 13. Equivalence of valuations and pseudo-valuations.

Let again K be a field, and let $w(a)$ and $w'(a)$ be two distinct valuations or pseudo-valuations of K. We say that $w(a)$ *and* $w'(a)$ *are equivalent and write* $w(a) \sim w'(a)$ *if every null sequence of* K *with respect to* $w(a)$ *is also a null sequence with respect to* $w'(a)$, *and vice versa.*

This definition implies that also *every fundamental sequence of* K *with respect to* $w(a)$ *is a fundamental sequence with respect to* $w'(a)$, *and vice versa.* For assume $\{a_m\}$ were a fundamental sequence with respect to $w(a)$, but not with respect to $w'(a)$. There would then evidently exist an infinite sequence of pairs of suffixes

$$(m_1, n_1),\ (m_2, n_2),\ (m_3, n_3), \ldots$$

such that

$$\lim_{k\to\infty} m_k = \lim_{k\to\infty} n_k = \infty,$$

and that further

$$\{a_{m_1}-a_{n_1},\ a_{m_2}-a_{n_2},\ a_{m_3}-a_{n_3},\ldots\}$$

is a null sequence with respect to $w(a)$, but not with respect to $w'(a)$, against the hypothesis.

It follows that equivalent valuations or pseudo-valuations $w(a)$ and $w'(a)$ generate *identical* and not only isomorphic completions of K: $K_w=K_{w'}$. From the standpoint of valuation theory alone there would then be no need to distinguish between such equivalent valuations or pseudo-valuations.

Two equivalent valuations $w(a)$ and $w'(a)$ can be proved to be connected by an identity

$$w'(a) = w(a)^{\lambda}$$

where $\lambda$ is a positive constant. Such a simple relation need not hold between two equivalent pseudo-valuations. For instance, in the case of the rational field $\Gamma$,

$$|a| \text{ and } \max(|a|,\ |a|^{\frac{1}{3}})$$

are equivalent. This trivial example also shows that a valuation may well be equivalent to a pseudo-valuation.

## 14. The valuations and pseudo-valuations of $\Gamma$.

The relation $w(a)\sim w'(a)$ is an equivalence relation in the algebraic sense. We may therefore subdivide all valuations and pseudo-valuations of a given field K into equivalence classes, and then the problem arises of determining all distinct equivalence classes.

A. Ostrowski was the first to determine a full system of nonequivalent valuations of any finite algebraic number field[5]), and I did the same for the classes of non-equivalent pseudo-valuations of such a field[6]).

For our purpose the most important case is that of the rational field $\Gamma$. Then the result is that *every valuation of* $\Gamma$ *is equivalent to one of the valuations*

$$w_0(a),\ |a|,\ \text{and}\ |a|_p$$

*where* p *runs over all primes* $p = 2, 3, 5,\ldots$; *and every pseudo-valuation of* $\Gamma$ *which is not already equivalent to one of these valuations must be equivalent to a pseudo-valuation of the form*

$$w_1(a) = \max(|a|_{p_1}^{\lambda_1},\ldots,\ |a|_{p_r}^{\lambda_r}) \quad\text{or}\quad w_2(a) = \max(|a|^{\lambda},\ |a|_{p_1}^{\lambda_1},\ldots,|a|_{p_r}^{\lambda_r}).$$

Here $p_1,\ldots, p_r$ are finitely many distinct primes, with $r \geqslant 2$ in the case of $w_1(a)$ and $r \geqslant 1$ in that of $w_2(a)$; and $\lambda, \lambda_1,\ldots, \lambda_r$ are constants satisfying

$$0 < \lambda \leqslant 1,\ \lambda_1 > 0,\ldots,\ \lambda_r > 0.$$

An alteration of these constants has only the effect of replacing $w_1(a)$ or $w_2(a)$ by an equivalent pseudo-valuation, and so, from the standpoint of valuation theory, it would suffice to put

[5] Acta math. 41 (1919), 271-284.

[6] Acta math. 67 (1936), 51-80.

$$\lambda = \lambda_1 = \ldots = \lambda_r = 1.$$

However, for the later applications to Diophantine approximations, a different choice of these constants is of advantage.

For let $g \geqslant 2$ be an arbitrary integer, and let

$$g = p_1^{e_1} \ldots p_r^{e_r}$$

be its factorisation into a product of powers of different primes $p_1, \ldots, p_r$ with exponents $e_1, \ldots, e_r$ that are positive integers. Fix now $\lambda_1, \ldots, \lambda_r$ such that $|g|_{p_1}^{\lambda_1} = \ldots = |g|_{p_r}^{\lambda_r} = \frac{1}{g}$, i.e., take

$$\lambda_1 = \frac{\log g}{e_1 \log p_1}, \ldots, \lambda_r = \frac{\log g}{e_r \log p_r},$$

and put

$$|a|_g = \max\left(|a|_{p_1}^{\frac{\log g}{e_1 \log p_1}}, \ldots, |a|_{p_r}^{\frac{\log g}{e_r \log p_r}}\right)$$

and

$$|a|_{g^*} = \max\left(|a|, |a|_{p_1}^{\frac{\log g}{e_1 \log p_1}}, \ldots, |a|_{p_r}^{\frac{\log g}{e_r \log p_r}}\right) = \max(|a|, |a|_g).$$

We call $|a|_g$, and $|a|_{g^*}$ *the* g*-adic and the* g**-adic pseudo-valuations*, respectively, and also speak of the g-adic and g*-adic values of a.

The definition of $|a|_g$ implies that

$$|ag^n|_g = g^{-n} |a|_g$$

for all a in $\Gamma$ and all integers n. This is easily verified and is also contained in the property (II) of § 4.

If $g' \geqslant 2$ is a second integer, it is obvious that $|a|_g$ and $|a|_{g'}$ are equivalent if and only if g and g' have the same prime factors $p_1, \ldots, p_r$ and differ only in their exponents; and just the same holds for $|a|_{g^*}$ and $|a|_{g'^*}$. Furthermore,

$$|a|_g = |a|_p$$

if g is a positive integral power of the single prime p.

In these lectures, $P$ will denote the real field, i.e., the completion of $\Gamma$ with respect to $|a|$; and similarly $P_p$, $P_g$, and $P_{g^*}$ will stand for the completions of $\Gamma$ with respect to $|a|_p$, $|a|_g$, and $|a|_{g^*}$, respectively. Then $P_p$, $P_g$, and $P_{g^*}$ are the *field of* p*-adic numbers*, and the *rings of* g*-adic and* g**-adic numbers*, respectively. This field and these two rings were introduced by K. Hensel[7]) in 1892 and have proved of fundamental importance in many branches of mathematics.

We shall study the elements of $P_p$, $P_g$, and $P_{g^*}$ in detail in the next

[7] Hensel's little book *Zahlentheorie* (Berlin 1913), which gives an elementary introduction to the theory of p-adic and g-adic numbers, may be particularly recommanded on account of its many examples of actual computations with such numbers.

chapter; and they will form both the object and a tool in most of the later work.

It is clear that, while $|a|$ and $|a|_{g^*}$ are Archimedean, $|a|_p$ and $|a|_g$ are Non-Archimedean. This was proved for $|a|_p$ in §4 and so follows for $|a|_g$ from the definition.

It is sometimes convenient to define $|a|_g$ also in the excluded case when $g = 1$, by putting $|a|_1 = w_0(a)$.

## 15. Independent pseudo-valuations.

The g-adic ring $P_g$ and the g*-adic ring $P_{g^*}$ can be decomposed into finitely many field $P$ and $P_p$, as was already proved by Hensel[7]). We shall prove this decomposition as a special case of a more general theorem on pseudo-valuations.

Denote by K a field, by $w_1(a),\dots, w_r(a)$ finitely many valuations or pseudo-valuations of K, and by

$$\delta_{hk} = \begin{cases} 1 \text{ if } h = k, \\ 0 \text{ if } h \neq k \end{cases}$$

the well-known Kronecker symbol. Then $w_1(a),\dots, w_r(a)$ *are said to be independent* if there exists for each suffix $h = 1, 2,\dots, r$ an infinite sequence $\{d_m^{(h)}\} = \{d_1^{(h)}, d_2^{(h)}; d_3^{(h)},\dots\}$ in K such that

$$\lim_{m\to\infty} w_k(d_m^{(h)} - \delta_{hk}) = 0 \qquad (k = 1,2,\dots,r),$$

or, what is the same, that

$$\delta_{hk} = \lim_{m\to\infty} d_m^{(h)} (w_k) \qquad (k = 1,2,\dots,r).$$

From this definition, it is immediately clear that, if

$$w_1'(a) \sim w_1(a),\dots, w_r'(a) \sim w_r(a),$$

then also $w_1'(a),\dots, w_r'(a)$ are independent.

By way of example, let us consider the rational field $\Gamma$. Here the following result holds.

(1): *If* $p_1,\dots, p_r$ *are finitely many distinct primes, then the valuations*

$$|a|, |a|_{p_1},\dots, |a|_{p_r}$$

*and hence also the valuations*

$$|a|_{p_1},\dots, |a|_{p_r}$$

*are independent.*

First, the sequence

$$\{d_m^{(0)}\}, \text{ where } d_m^{(0)} = \frac{(p_1p_2\dots p_r)^m}{(p_1p_2\dots p_r)^m + 1},$$

is easily seen to have the limits 1 with respect to $|a|$ and 0 with respect to $|a|_{p_1},\dots,|a|_{p_r}$, respectively. Secondly, select for each suffix $h = 1, 2, \dots, r$ a positive integer $a_h$ such that

$$p_h^{a_h} > p_1 p_2 \dots p_r.$$

Then it is not difficult to verify that the sequence

$$\{d_m^{(h)}\}, \text{ where } d_m^{(h)} = \frac{(p_1 p_2 \dots p_r)^m}{(p_1 p_2 \dots p_r)^m + p_h^{a_h m}},$$

has the limit 1 with respect to $|a|_{p_h}$, but is a null sequence with respect to $|a|$, as well as with respect to all $|a|_{p_k}$ where $k \neq h$.

If $g_1 \geqslant 2, \dots, g_r \geqslant 2$ are finitely many integers which are relatively prime in pairs, one shows by a similar proof that also

$$|a|,\ |a|_{g_1},\dots,\ |a|_{g_r}$$

and hence also

$$|a|_{g_1},\dots,\ |a|_{g_r}$$

are independent.

## 16. The decomposition theorem.

Let again K be a field, and let $w_1(a), \dots, w_r(a)$, where $r \geqslant 2$, be finitely many *independent* valuations or pseudo-valuations of K. As in § 4, we put

$$w_\Sigma(a) = \max[w_1(a),\dots, w_r(a)]$$

and further write

$$w_\Sigma^{(h)}(a) = \max_{\substack{1 \leqslant k \leqslant r \\ k \neq h}} w_k(a) \qquad (h = 1,2,\dots,r).$$

These functions are likewise valuations or pseudo-valuations of K, and $w_\Sigma(a)$ is, what we call the *sum* of $w_1(a),\dots, w_r(a)$.

The following lemma gives the justification for the term of "independent" valuations or pseudo-valuations.

(m): *Let $\alpha_1 \epsilon K_{w_1}, \dots, \alpha_r \epsilon K_{w_r}$ be arbitrary elements of the completions of* K *with respect to* $w_1(a),\dots, w_r(a)$, *respectively. Then there exists an infinite sequence* $\{a_m\}$ *in* K *such that, simultaneously,*

$$\lim_{m\to\infty} a_m = \alpha_h(w_h) \qquad (h = 1,2,\dots,r).$$

First, $\alpha_1,\dots,\alpha_r$ are defined as the limits

$$\alpha_h = \lim_{m\to\infty} a_m^{(h)}(w_h) \qquad (h = 1,2,\dots,r)$$

of certain infinite sequences $\{a_m^{(1)}\},\dots,\{a_m^{(r)}\}$ in K. Secondly, by the definition of independence, there also exist r infinite sequences $\{d_m^{(1)}\},\dots,\{d_m^{(r)}\}$

in K satisfying

$$\lim_{m\to\infty} d_m^{(h)} = \delta_{hk}(w_h) \qquad (h,k = 1,2,\dots,r).$$

In particular, each such sequence $\{d_m^{(h)}\}$ is a null sequence with respect to all $w_k(a)$ where $k \neq h$, and so it is a null sequence also with respect to $w_\Sigma^{(h)}(a)$.

There exists then, for each h, an infinite sequence of strictly increasing suffixes $m_{h1}, m_{h2}, m_{h3}, \dots$ such that

$$w_\Sigma^{(h)}\left(d_{m_{hl}}^{(h)}\right) w_\Sigma^{(h)}\left(a_l^{(h)}\right) < \frac{1}{l} \qquad \text{for all } l.$$

Thus

$$\lim_{l\to\infty} w_\Sigma^{(h)}\left(d_{m_{hl}}^{(h)}\, a_l\right) = 0,$$

and hence, from the definition of $w_\Sigma^{(h)}(a)$,

$$\text{(A):} \qquad \lim_{l\to\infty} d_{m_{hl}}^{(h)}\, a_l^{(h)} = 0\ (w_k) \qquad (h,k = 1,2,\dots,r;\ h \neq k).$$

On the other hand[8]),

$$\lim_{l\to\infty} d_{m_{hl}}^{(h)} = \lim_{m\to\infty} d_m^{(h)} = 1\ (w_h) \quad (h = 1,2,\dots,r),$$

so that

$$\text{(B):} \quad \lim_{l\to\infty} d_{m_{hl}}^{(h)}\, a_l^{(h)} = \lim_{l\to\infty} d_{m_{hl}}^{(h)} \lim_{l\to\infty} a_l^{(h)} = 1.\alpha_h = \alpha_h(w_h) \quad (h = 1,2,\dots,r).$$

On combining (A) with (B), it follows that the new sequence $\{a_m\}$ where

$$a_l = \sum_{h=1}^{r} d_{m_{hl}}^{(h)}\, a_l^{(h)} \qquad (l = 1,2,3,\dots)$$

has the required limits $\alpha_1, \dots, \alpha_r$ with respect to $w_1(a), \dots, w_r(a)$, respectively.

We finally prove the following *decomposition theorem* which establishes the connection between the completions $K_w, K_{w_1}, \dots, K_{w_r}$ of K.

(n): *There is a one-to-one correspondence*

$$\alpha \longleftrightarrow (\alpha_1, \dots, \alpha_r)$$

[8]. Let $\{b_m\}$ be a fundamental sequence with respect to w(a), and let $\{b_{m_l}\}$, where $m_1 < m_2 < m_3 < \dots$, be an infinite subsequence of $\{b_m\}$. Then $\{b_1 - b_{m_1}, b_2 - b_{m_2}, b_3 - b_{m_3}, \dots\}$ evidently is a null sequence with respect to w(a), whence

$$\lim_{m\to\infty} b_m = \lim_{l\to\infty} b_{m_l}(w).$$

*between the elements* $\alpha$ *of* $K_{w_\Sigma}$ *and the ordered sets* $(\alpha_1,\dots,\alpha_r)$ *of one element in each of* $K_{w_1},\dots,K_{w_r}$ *such that, if*

$$\alpha \longleftrightarrow (\alpha_1,\dots,\alpha_r) \quad\text{and}\quad \beta \longleftrightarrow (\beta_1,\dots,\beta r),$$

*then also*

$$\alpha+\beta \longleftrightarrow (\alpha_1+\beta_1,\dots,\alpha_r+\beta_r),\ \alpha-\beta \longleftrightarrow (\alpha_1-\beta_1,\dots,\alpha_r-\beta_r),\ \alpha\beta \longleftrightarrow (\alpha_1\beta_1,\dots,\alpha_r\beta_r).$$

*This correspondence is defined by*

$$\alpha = \lim_{m\to\infty} a_m(w_\Sigma), \qquad \alpha_h = \lim_{m\to\infty} a_m(w_h) \quad (h = 1,2,\dots,r),$$

*where* $\{a_m\}$ *is a sequence in* K *which is a fundamental sequence with respect to all of* $w_1(a),\dots,w_r(a)$, *and* $w_\Sigma(a)$.

First, we note that it is obvious from the definition of $w_\Sigma(a)$ that a sequence $\{a_m\}$ in K which is a fundamental sequence with respect to each of $w_1(a),\dots,w_r(a)$ is also a fundamental sequence with respect to $w_\Sigma(a)$, and vice versa; similarly, if the sequence is a null sequence with respect to each of $w_1(a),\dots,w_r(a)$, then it is also one with respect to $w_\Sigma(a)$, and vice versa. Now, by lemma (m), the arbitrary elements $\alpha_1 \epsilon K_{w_1},\dots,\alpha_r \epsilon K_{w_r}$ can be defined as limits

$$\alpha_h = \lim_{m\to\infty} a_m(w_h) \qquad (h = 1,2,\dots,r)$$

of the *same* sequence $\{a_m\}$ in K, and then the limit

$$\alpha = \lim_{m\to\infty} a_m(w_\Sigma)$$

defines an element $\alpha$ of $K_{w_\Sigma}$. Conversely, if $\alpha$ is given as the limit with respect to $w_\Sigma(a)$ of such a sequence $\{a_m\}$, then the limits of $\{a_m\}$ with respect to $w_1(a),\dots,w_r(a)$ likewise exist and define elements $\alpha_1,\dots,\alpha_r$ of $K_{w_1},\dots,K_{w_r}$, respectively.

*The relation* $\alpha \longleftrightarrow (\alpha_1,\dots,\alpha_r)$ *is independent of the special sequence* $\{a_m\}$ *used in the definition of* $\alpha, \alpha_1,\dots,\alpha_r$. For if

(C): $$\lim_{m\to\infty} a_m = \lim_{m\to\infty} a'_m(w_h) \qquad (h = 1,2,\dots,r),$$

then $\{a_m - a'_m\}$ is a null sequence with respect to each of $w_1(a),\dots,w_r(a)$ and hence also with respect to $w_\Sigma(a)$; therefore

(D): $$\lim_{m\to\infty} a_m = \lim_{m\to\infty} a'_m(w_\Sigma).$$

Conversely, (D) implies again (C).

The formulae for $\alpha+\beta$, $\alpha-\beta$, and $\alpha\beta$ finally follow at once from the rules for limits proved in § 9.

If $\alpha \longleftrightarrow (\alpha_1,\dots,\alpha_r)$, $\alpha_1,\dots,\alpha_r$ are called the *components* of $\alpha$.

All the completions $K_{w_1},\dots,K_{w_r}$, and $K_{w_\Sigma}$ are extensions of K, and every element a of K lies simultaneously in each of these r+1 rings or fields. For such and only for such elements the correspondence relation takes the simple form

$$a \longleftrightarrow (a,a,\ldots,a).$$

In particular,

$$0 \longleftrightarrow (0,0,\ldots,0) \quad \text{and} \quad 1 \longleftrightarrow (1,1,\ldots,1)$$

are the zero element, and the unit element, of $K_{w_\Sigma}$.

We note that, since $r \geqslant 2$, $K_{w_\Sigma}$ *is not a field* because by

$$\alpha\beta = 0, \text{ where } \alpha \longleftrightarrow (1,0,\ldots,0),\ \beta \longleftrightarrow (0,1,\ldots,0),$$

$K_{w_\Sigma}$ contains non-trivial *zero divisors.* This also implies that $w_\Sigma(a)$ cannot be equivalent to a valuation since then $K_w$ would be a field.

In the special case when $w_1(a),\ldots, w_r(a)$ are valuations, the completions $K_{w_1},\ldots, K_{w_r}$ (but, of course, not $K_{w_\Sigma}$) are fields. If now

$$\alpha \longleftrightarrow (\alpha_1,\ldots,\alpha_r),\ \beta \longleftrightarrow (\beta_1,\ldots,\beta_r), \quad \text{and} \quad \beta_1 \neq 0,\ldots,\beta_r \neq 0,$$

$\alpha$ is divisible by $\beta$, with the quotient

$$\frac{\alpha}{\beta} \longleftrightarrow \left(\frac{\alpha_1}{\beta_1},\ldots,\frac{\alpha_r}{\beta_r}\right).$$

The for us must important case of the decomposition theorem concerns the g-adic and the g*-adic numbers. If $g$ has the distinct prime factors $p_1,\ldots, p_r$, the correspondence

$$\alpha \longleftrightarrow (\alpha_1,\ldots,\alpha_r)$$

relates the g-adic number $\alpha$ to the ordered set of one $p_1$-adic number $\alpha_1$, one $p_2$-adic number $\alpha_2$, etc., and one $p_r$-adic number $\alpha_r$; g*-adic numbers

$$\alpha^* \longleftrightarrow (\alpha_0,\alpha_1,\ldots,\alpha_r)$$

in addition have also a real component $\alpha_0$.

The components $(\alpha_0)$, $\alpha_1,\ldots,\alpha_r$ of $\alpha$ or $\alpha^*$ are independent of one another and may be any numbers in the corresponding fields (P), $P_{p_1},\ldots, P_{p_r}$. It is thus in general impossible to deduce from properties of one of the components any properties of the other components.

## 17. Convergent infinite series.

Let again K be an arbitrary field with the valuation or pseudo-valuation w(a). As in real analysis, it is convenient to introduce the notion of a *convergent series.*

The infinite series

$$\sum_{m=1}^{\infty} a_m = a_1+a_2+a_3+\ldots, \quad \text{where } a_m \epsilon K \text{ for all } m,$$

*is said to be convergent with respect to* w(a) *to the sum* $\alpha$ if

$$\left\{\sum_{k=1}^{m} a_k\right\} = \{a_1, a_1+a_2, a_1+a_2+a_3,\ldots\}$$

is a fundamental sequence with respect to w(a) of limit $\alpha$, and it is otherwise called *divergent.* From this definition, *the series converges if and only if, given any* $\epsilon > 0$, *there is a positive number* $q(\epsilon)$ *such that*

$$w\left(\sum_{k=1}^{m} a_k - \sum_{k=1}^{n} a_k\right) = w(a_{n+1} + a_{n+2} + \dots + a_m) < \epsilon$$

for all integers m, n satisfying $m > n \geqslant q(\epsilon)$.

Since

$$w(a_{n+1} + a_{n+2} + \dots + a_m) \leqslant w(a_{n+1}) + w(a_{n+2}) + \dots + w(a_m),$$

the series $\sum_{m=1}^{\infty} a_m$ certainly converges if the series of real numbers

$$\sum_{m=1}^{\infty} w(a_m)$$

converges; but the converse need not even be true in real analysis where $w(a) = |a|$.

On taking m=n+1, it is also obvious that $\sum_{m=1}^{\infty} a_m$ cannot be convergent unless

$$\lim_{m\to\infty} a_m = 0\ (w);$$

but, just as in real analysis, this condition is not in general sufficient for convergence. There is, however, one important case when it is *sufficient,* viz. that when w(a) is *Non-Archimedean.* For now

$$w(a_{n+1} + a_{n+2} + \dots + a_m) \leqslant \max[w(a_{n+1}), w(a_{n+2}), \dots, w(a_m)].$$

and so, if $\{a_m\}$ is a null sequence with respect to w(a), the righthand side is smaller than $\epsilon$ for all $m > n \geqslant r(\epsilon)$.

In the following chapter these simple remarks on convergent series will be applied to series for p-adic, g-adic, and g*-adic numbers.

Final remark: The sketch of valuation theory given in this chapter has been strictly limited to those facts that are to be applied later. For further study of this interesting and important theory the following texts may be referred to:

E. Artin, Algebraic numbers and algebraic functions I, Princeton 1951.
H. Hasse, Zahlentheorie, Berlin 1949.
O. F. G. Schilling, Theory of valuations, Math. Surveys IV, Amer. Math. Soc. 1950.
H. Weyl, Algebraic theory of numbers, Princeton 1940.