2.4 The p-adic number field

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **46 (2000)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.05.2024**

2.4 THE p-ADIC NUMBER FIELD

Let p be prime. We shall use $\mathbf{Z}_p$ to represent the p-adic integers, and $\mathbf{Q}_p$ the p-adic rationals. Let $|\cdot|_p$ denote the p-adic absolute value on $\mathbf{Q}_p$, normalized so that $|p|_p = p^{-1}$. Let $\overline{\mathbf{Q}}_p$ be the algebraic closure of $\mathbf{Q}_p$. The absolute value on $\mathbf{Q}_p$ extends uniquely to $\overline{\mathbf{Q}}_p$, however $\overline{\mathbf{Q}}_p$ is not complete with respect to the absolute value. Let $\mathbf{C}_p$ be the completion of $\overline{\mathbf{Q}}_p$ with respect to this absolute value. Then the absolute value extends to $\mathbf{C}_p$, and $\overline{\mathbf{Q}}_p$ is dense in $\mathbf{C}_p$. We also have $\mathbf{C}_p$ algebraically closed. Furthermore, on $\mathbf{C}_p$ the absolute value is non-Archimedean, and so

$$|a+b|_p \le \max\{|a|_p, |b|_p\}$$

for any $a, b \in \mathbf{C}_p$. Note that the two fields $\mathbf{C}$ and $\mathbf{C}_p$ are algebraically isomorphic, and any one of the two can be embedded in the other. We denote two particular subrings of $\mathbf{C}_p$ in the following manner

$$\mathfrak{o} = \{a \in \mathbf{C}_p : |a|_p \le 1\}, \qquad \mathfrak{p} = \{a \in \mathbf{C}_p : |a|_p < 1\}.$$

Then $\mathfrak{p}$ is a maximal ideal of $\mathfrak{o}$. If $\tau \in \mathbf{C}_p$ such that $|\tau|_p \le |p|_p^s$, where $s \in \mathbf{Q}$, then $\tau \in p^s\mathfrak{o}$, and so we shall also write this as $\tau \equiv 0 \pmod{p^s\mathfrak{o}}$.

Any $n \in \mathbf{Z}$, $n > 0$, can be uniquely expressed in the form $n = \sum_{m=0}^{k} a_m p^m$, where $a_m \in \mathbf{Z}$, $0 \le a_m \le p-1$, for $m = 0, 1, \ldots, k$, and $a_k \ne 0$. For such n, we define

$$s_p(n) = \sum_{m=0}^{k} a_m,$$

the sum of the p-adic digits of n, and also define $s_p(0) = 0$. For any $n \in \mathbf{Z}$, let $v_p(n)$ be the highest power of p dividing n. This function is additive, and relates to the function $s_p(n)$ by means of the identity

$$v_p(n!) = \frac{n - s_p(n)}{p-1}, \tag{8}$$

which holds for all $n \ge 0$. Note that for $n \ge 1$ this implies that

$$v_p(n!) \le \frac{n-1}{p-1}.$$

The definition of this function can be extended to all of $\mathbf{Q}$ by taking $v_p(1/n) = -v_p(n)$.

Throughout we let $q = 4$ if $p = 2$, and $q = p$ otherwise. Note that there exist $\phi(q)$ distinct solutions, modulo q, to the equation $x^{\phi(q)} - 1 = 0$, and each solution must be congruent to one of the values $a \in \mathbf{Z}$, where $1 \le a \le q$,

$(a,p)=1$. Thus, by Hensel's Lemma, given $a \in \mathbf{Z}$ with $(a,p)=1$, there exists a unique $\omega(a) \in \mathbf{Z}_p$, where $\omega(a)^{\phi(q)}=1$, such that

$$\omega(a) \equiv a \pmod{q\mathbf{Z}_p}.$$

Letting $\omega(a)=0$ for $a \in \mathbf{Z}$ such that $(a,p) \neq 1$, we see that ω is actually a Dirichlet character, called the Teichmüller character, having conductor $f_\omega = q$. Let us define

$$\langle a \rangle = \omega^{-1}(a)a.$$

Then $\langle a \rangle \equiv 1 \pmod{q\mathbf{Z}_p}$. For $p \geq 3$, $\lim_{n\to\infty} a^{p^n} = \omega(a)$, since $a^{p^n} \equiv a \pmod{p}$ and $a^{p^n(p-1)} \equiv 1 \pmod{p^{n+1}}$.

For our purposes we shall need to make a slight extension of the definition of the Teichmüller character ω. If $t \in \mathbf{C}_p$ such that $|t|_p \leq 1$, then for any $a \in \mathbf{Z}$, $a+qt \equiv a \pmod{q\mathfrak{o}}$. Thus we define

$$\omega(a+qt) = \omega(a)$$

for these values of t. We also define

$$\langle a+qt \rangle = \omega^{-1}(a)(a+qt)$$

for such t.

Fix an embedding of the algebraic closure of $\mathbf{Q}$, $\overline{\mathbf{Q}}$, into $\mathbf{C}_p$. We may then consider the values of a Dirichlet character χ as lying in $\mathbf{C}_p$. For $n \in \mathbf{Z}$ we define the product $\chi_n = \chi\omega^{-n}$ in the sense of the product of characters. This implies that $f_{\chi_n} \mid f_\chi q$. However, since we can write $\chi = \chi_n\omega^n$, we also have $f_\chi \mid f_{\chi_n} q$. Thus f_χ and f_{χ_n} differ by a factor that is a power of p. In fact, either $f_{\chi_n}/f_\chi \in \mathbf{Z}$ and divides q, or $f_\chi/f_{\chi_n} \in \mathbf{Z}$ and divides q.

Let $\mathbf{Q}_p(\chi)$ denote the field generated over $\mathbf{Q}_p$ by all values $\chi(a)$, $a \in \mathbf{Z}$. In this context we can state the following, found in [13] (pp. 14–15).

LEMMA 2.2. *In the field $\mathbf{Q}_p(\chi)$, for all $n \in \mathbf{Z}$, $n \geq 0$,*

$$B_{n,\chi} = \frac{1}{n+1} \lim_{h\to\infty} \frac{1}{p^h f_\chi} \left(B_{n+1,\chi}\left(p^h f_\chi\right) - B_{n+1,\chi}(0) \right).$$

From this we can obtain

LEMMA 2.3. *Let $\tau \in \mathbf{C}_p$. In the field $\mathbf{Q}_p(\chi, \tau)$, for all $n \in \mathbf{Z}$, $n \geq 0$,*

$$B_{n,\chi_n}(\tau) = \lim_{h\to\infty} \frac{1}{p^h f_\chi} \sum_{a=1}^{p^h f_\chi} \chi_n(a)(a+\tau)^n .$$

Proof. By applying Lemma 2.2 to (4), we obtain

$$B_{n,\chi} = \lim_{h\to\infty} \frac{1}{p^h f_\chi} \sum_{a=1}^{p^h f_\chi} \chi(a)a^n .$$

Therefore, by (2),

$$\begin{aligned} B_{n,\chi_n}(\tau) &= \sum_{m=0}^{n} \binom{n}{m} \tau^{n-m} \lim_{h\to\infty} \frac{1}{p^h f_{\chi_n}} \sum_{a=1}^{p^h f_{\chi_n}} \chi_n(a)a^m \\ &= \lim_{h\to\infty} \frac{1}{p^h f_{\chi_n}} \sum_{a=1}^{p^h f_{\chi_n}} \chi_n(a) \sum_{m=0}^{n} \binom{n}{m} \tau^{n-m} a^m . \end{aligned}$$

Since f_χ and f_{χ_n} differ by a factor that is a power of p, we must have

$$B_{n,\chi_n}(\tau) = \lim_{h\to\infty} \frac{1}{p^h f_\chi} \sum_{a=1}^{p^h f_\chi} \chi_n(a)(a+\tau)^n,$$

and the proof is complete. □

2.5 p-ADIC FUNCTIONS

Let K be an extension of $\mathbf{Q}_p$ contained in $\mathbf{C}_p$. An infinite series $\sum_{n=0}^{\infty} a_n$, $a_n \in K$, converges in K if and only if $|a_n|_p \to 0$ as $n \to \infty$. Let $K[[x]]$ be the algebra of formal power series in x. Then it follows that a power series

$$A(x) = \sum_{n=0}^{\infty} a_n x^n,$$

in $K[[x]]$, converges at $x = \xi$, $\xi \in \mathbf{C}_p$, if and only if $|a_n \xi^n|_p \to 0$ as $n \to \infty$. Therefore whenever a power series $A(x)$ converges at some $\xi_0 \in \mathbf{C}_p$, then it must converge at all $\xi \in \mathbf{C}_p$ such that $|\xi|_p \leq |\xi_0|_p$. The following result, for double series in K, can be found in [8].