Chapter 16

The p-adic numbers

16.1. The p-adic norm

Exercise 16.1.1. Prove the product formula for all non-zero rational numbers r.

Exercise 16.1.2.† A circle in $\mathbb{C}$ takes the form $B(a;r) := \{x : |x-a| \le r\}$ where a is the center of the circle and r is its radius. We define a p-adic circle to be $B_p(a;r) := \{x : |x-a|_p \le r\}$.

(a) Prove that if $b \in B_p(a;r)$, then $B_p(a;r) = B_p(b;r)$. (In other words, every point inside a p-adic circle can be taken to be its center.)

(b) Prove that if two circles $B_p(a;r)$ and $B_p(A;R)$, with $r \le R$, have a point b in common, then $B_p(a;r) \subset B_p(A;R)$. (That is, two p-adic circles are either disjoint or one is contained in the other.)

16.2. p-adic expansions

Exercise 16.2.1. (a) Prove that the p-adic expansion of any non-zero rational number a/n with $(a,n) = 1$ is eventually periodic.

(b) Show that if $p \nmid n$, then the length of the period divides $\mathrm{ord}_n(p)$.

Exercise 16.2.2. Suppose that $(r_k)_{k\ge1}$ is any sequence of rationals such that for any $\epsilon > 0$, if k and ℓ are sufficiently large, then $|r_k - r_\ell|_p < \epsilon$. Prove that the r_k tend to a limit with a p-adic expansion.

16.3. p-adic roots of polynomials

Exercise 16.3.1. Show that if $f(x) \in \mathbb{Z}[x]$ has no repeated roots, then there are only finitely many primes p for which there exists an integer a_p with $f(a_p) \equiv f'(a_p) \equiv 0 \pmod p$.

Exercise 16.3.2. Prove that if odd prime p does not divide a, then there are exactly $1 + (\frac{a}{p})$ square roots of $a \pmod p$.

Exercise 16.3.3. (a) If prime $p \nmid a$, show that the sequence $a_n = a^{p^n}$ converges in the p-adics.

(b) Show that $\alpha := \lim_{n\to\infty} a_n$ is a $(p-1)$st root of unity and that all solutions to $x^{p-1} - 1$ in $\mathbb{Z}_p$ can be obtained in this way.

(c) Conclude that $i := \lim_{n\to\infty} 2^{5^n}$ is a square root of -1 in $\mathbb{Q}_5$.

16.4. p-adic factors of a polynomial

Exercise 16.4.1. Assume $g(x) \in \mathbb{C}[x]$ and $\alpha \in \mathbb{C}$ with $\alpha \neq 0$.
(a) Prove that $\|(x-\alpha)g(x)\| = \|(\overline{\alpha}x - 1)g(x)\|$ and $M((x-\alpha)g(x)) = M((\overline{\alpha}x-1)g(x))$.
(b) If $|\alpha| \leq 1$ whenever $f(\alpha) = 0$, prove that $M(f) \leq \|f\| \leq M(f)\left(\sum_{i=0}^{n}\binom{n}{i}^2\right)^{1/2}$, where f has degree n. (We note that $\sum_{i=0}^{n}\binom{n}{i}^2 = \binom{2n}{n} \leq 2^{2n}$.)
(c) Deduce that if f has degree n, then $M(f) \leq \|f\| \leq 2^n M(f)$.
(d) Suppose that $g(x) \in \mathbb{Z}[x]$ divides $f(x) \in \mathbb{Z}[x]$. Prove that $M(g) \leq M(f)$.
(e) Deduce that if g has degree d, then $\|g\| \leq 2^d\|f\|$.

16.5. Possible norms on the rationals

Exercise 16.5.1. Prove that $|1| = |-1| = 1$.

16.6. Power series convergence and the p-adic logarithm

Exercise 16.6.1. Let p be a given prime.
(a) Prove that $\sum_{n\geq 0} z^n/a_n$ converges when $|z|_p < p^{-\tau}$, where $\tau = \limsup_{n\to\infty} v_p(a_n)/n$.
(b) Deduce that $\sum_{n\geq 1} z^n/n$ converges if $|z|_p < 1$. (In $\mathbb{C}$ this also converges inside $|z| < 1$.) Exercise 3.10.1(b) states that $v_p(n!) = \frac{n - s_p(n)}{p-1}$ where $s_p(n)$ is the sum of the digits of n when written in base p.
(c) Deduce that $\sum_{n\geq 1} z^n/n!$ converges if $|z|_p < p^{-1/(p-1)}$.

Exercise 16.6.2. Suppose that $|1-a|_p, |1-b|_p < p^{-1/(p-1)}$.
(a) Prove that $|1-ab|_p < p^{-1/(p-1)}$.
(b) Deduce that $\exp_p(ab) = \exp_p(a)\exp_p(b)$.

Exercise 16.6.3. Suppose that $v_p(x) > 0$.
(a) Prove that if $p^k \leq m < p^{k+1}$, then $v_p(x^m/m) \geq p^k v_p(x) - k$, for each integer $k \geq 0$.
(b) Suppose that $v_p(x) \geq 2r/p^r$ for some integer $r \geq 1$. Deduce that $v_p(x^m/m) \geq k$ for all $m \geq p^k$, whenever $k \geq r$.

Exercise 16.6.4. Prove that $\sum_{m\geq 1} 2^m/m = 0$ in the 2-adics.

Exercise 16.6.5. Assume that $|a-1|_p, |b-1|_p < 1$.
(a) Prove that $\lim_{k\to\infty} a^{p^k} = 1$.
(b) Deduce that $\log_p(ab) = \log_p(a) + \log_p(b)$.
(c) Deduce that if $a = b^n$, then $\log_p(a) = n\log_p(b)$.
(d)† Suggest an algorithm for the discrete log problem in the p-adics.

Exercise 16.6.6. Assume that $\alpha, \beta \in \mathbb{Z}_p$.
(a) Prove that $\log_p(-\alpha) = \log_p(\alpha)$.
(b) Prove that $\log_p(\alpha\beta) = \log_p(\alpha) + \log_p(\beta)$.

16.7. The p-adic dilogarithm

Exercise 16.7.1. (a) Prove that the sum defining $\mathcal{L}_k(x)$ converges for all $x \in \mathbb{C}$ with $|x|_\infty \leq 1$ for all $k \geq 2$, and for $|x|_p < 1$ in the p-adics.
(b) Establish that $\mathcal{L}_k(x) + \mathcal{L}_k(-x) = 2^{1-k}\mathcal{L}_k(x^2)$ when $|x|_p < 1$.

Exercise 16.7.2. Let $p = 2$ and $|z-1|_2 < 1$.
(a) Prove that $\mathcal{L}_2(1-z) + \mathcal{L}_2(1+z) = \frac{1}{2}\mathcal{L}_2(1-z^2) + C$ for some constant C.
(b) Prove that $C = 0$ using (16.7.1).
(c) Deduce (again) that $\mathcal{L}_2(2) = 0$.

Exercise 16.7.3. Prove that if $|x|_p, |y|_p < 1$, then

$$\mathcal{L}_2(x) + \mathcal{L}_2(y) - \mathcal{L}_2(xy) - \mathcal{L}_2\left(\frac{x(1-y)}{1-xy}\right) - \mathcal{L}_2\left(\frac{y(1-x)}{1-xy}\right) = \log_p\left(\frac{1-x}{1-xy}\right)\log_p\left(\frac{1-y}{1-xy}\right).$$