Home assignment 9: p-adic numbers

Rules: This is a class assignment for the next week. Please solve as many exercises as you can, bring me what you can before the Wednesday week after. Wednesdays 17:00 we will discuss the solutions in a monitor session. Exercises with [*] are extra hard and not necessary to follow the rest. Exercises with [!] are non-trivial, fundamental and necessary for further work.

9.1 Norms and valuations

Definition 9.1. Norm on a ring A is a function $A \to \mathbb{R}^{\geqslant 0}$, denoted $r \mapsto \|r\|$, which satisfies the following conditions: $\|x+y\| \leqslant \|x\| + \|y\|$, $\|xy\| = \|x\|\|y\|$ and $\|x\| = 0 \Leftrightarrow x = 0$.

Remark 9.1. The absolute value on $\mathbb{R}$ and $\mathbb{C}$ are examples of a norm.

Definition 9.2. A discrete valuation on a ring A is a function $\nu : A \to \mathbb{Z} \cup \{\infty\}$ such that $\nu(ab) = \nu(a)\nu(b)$, $\nu(a+b) \geqslant \min(\nu(a), \nu(b))$, and $\nu(x) = \infty \Leftrightarrow x = 0$.

Exercise 9.1. Let ν be a discrete valuation on a ring. Prove that $x \to u^{-\nu(x)}$ is a norm, for any $u \in \mathbb{R}^{>1}$.

Exercise 9.2. Let $\frac{n}{m} \in \mathbb{Q}$, where n, m are coprime integers. The **the p-adic valuation** $\nu_p(\frac{n}{m})$ is equal to α if $n = p^\alpha n'$, where $\alpha > 0$ and n' is coprime with p, to $-\alpha$ if $m = p^\alpha m'$, where $\alpha > 0$ and m' is comprime with p, to 0 if m and n are coprime with p, and to ∞ if $n = 0$.

Exercise 9.3. Prove that p-adic valuation is a discrete valuation in the sense of Definition 9.2.

Remark 9.2. Clearly, the norm defines a metric on R, $d(x,y) := \|x - y\|$.

Exercise 9.4. Let R be a ring equipped with a norm. Construct the ring structure on its metric completion $\bar{R}$, compatible with the ring structure on R. Prove that $\bar{R}$ is equipped with a norm compatible with the norm on R.

Definition 9.3. The normed ring $\bar{R}$ is called **the completion of R with respect to the norm**.

Exercise 9.5. Let R be a normed ring, and $\bar{R}$ its completion. Assume that R is a field. Prove that $\bar{R}$ is also a field.

9.2 p-adic numbers

Definition 9.4. Let ν be a valuation on a ring A. **The completion of R with respect to the valuation** ν is its completion with respect to the norm $x \mapsto u^{-\nu(x)}$, for some $u > 1$.

Exercise 9.6. Prove that the completion is independent from $u \in \mathbb{R}^{>1}$.

Definition 9.5. The completion of $\mathbb{Z}$ with respect to the valuation ν_p is called **the ring of p-adic integers**, denoted $\mathbb{Z}_p$. The completion of $\mathbb{Q}$ with respect to this valuation is called **the ring of p-adic rationals**, denoted $\mathbb{Q}_p$.

Exercise 9.7. Let (X, d) be a metric space, and $\{a_i\}$ be a sequence of points in X. Suppose that the series $\sum d(a_i, a_{i-1})$ converges. Prove that $\{a_i\}$ is a Cauchy sequence. Is the converse true?

Exercise 9.8 (!). Prove that for any sequence of integers a_k, the series $\sum a_k p^k$ converges in $\mathbb{Z}_p$.

Hint. Use the previous exercise.

Exercise 9.9. Prove that $(1-p)\left(\sum_{k=0}^{\infty} p^k\right) = 1$ in $\mathbb{Z}_p$.

Exercise 9.10 (!). Prove that every integer not divisible by p is invertible in $\mathbb{Z}_p$.

Exercise 9.11 (!). Let $x \in \mathbb{Q}_p$. Prove that $x = \frac{x'}{p^k}$, where $x' \in \mathbb{Z}_p$.

9.3 Ostrowski's theorem

Exercise 9.12 (*). Prove that $\lim\limits_{n\to\infty} \sqrt[n]{n} = 1$ (here the limit is taken in $\mathbb{R}$ with the usual metric).

Definition 9.6. A norm ν on a ring R is called **non-Archimedean** if $\nu(x+y) \leqslant \max(\nu(x), \nu(y))$ for all x, y. Otherwise the norm is called **Archimedean**.

Exercise 9.13 (*). Let ν be a norm on $\mathbb{Q}$. Prove that ν is non-Archimedean if and only if $\mathbb{Z}$ is contained in the unit ball.

Hint. Use the limit $\lim\limits_{n\to\infty} \sqrt[n]{n} = 1$. Estimate $\sqrt[n]{(\nu(x+y)^n)}$ for large n, using the estimate for binomial coefficients: $\nu(C_n^k) \leqslant 1$.

Exercise 9.14. Let ν be a non-Archimedean norm on $\mathbb{Z}$. Consider the set $\mathfrak{m} \subset \mathbb{Z}$ consisting of all integers n such that $\nu(n) < 1$. Deduce from the non-Archimedean property that $\mathfrak{m}$ is an ideal in $\mathbb{Z}$. Prove that the ideal $\mathfrak{m}$ is prime.

Exercise 9.15. Let ν be a non-Archimedean norm on $\mathbb{Q}$, and $\mathfrak{m} = \{0, \pm p, \pm 2p, \pm 3p, ...\}$ the ideal constructed above. Prove that there exists a real number $\lambda > 1$ such that $\nu(n) = \lambda^{-k}$ for every $n = p^k r$, where r is coprime with p.

Exercise 9.16. Let ν be a norm on $\mathbb{Q}$ such that $\nu(2) \leqslant 1$. Prove that $\nu(a) < \log_2(a) + 1$ for every integer $a > 0$.

Hint. Use the binary expansion of the number N.

Exercise 9.17 (*). Let ν be a norm on $\mathbb{Q}$ such that $\nu(2) \leqslant 1$. Prove that $\nu(a) \leqslant 1$ for every integer $a > 0$ (in particular, ν is non-Archimedean).

Hint. Deduce from $\lim\limits_{n\to\infty} \sqrt[n]{n} = 1$ the relation $\lim\limits_{n\to\infty} \frac{\log n}{n} = 0$. Using the previous problem, obtain $\lim\limits_{N\to\infty} \nu(a^N) \leqslant 1$.

Exercise 9.18. Let a_i be a sequence of rational numbers of the form $\frac{x}{2^n}$, which is Cauchy with respect to the usual Euclidean norm on $\mathbb{R}$. Suppose that the norm ν on $\mathbb{Q}$ is Archimedean. Prove that $\nu(a_i)$ is a Cauchy sequence.

Hint. Using the binary expansion of x, prove that

$$\nu(x/2^n) \leqslant \nu(2)^{\log_2(x)+1}/\nu(2)^n \leqslant \nu(2)^{\log_2(x+1)-n}.$$

Exercise 9.19. Show that any Archimedean norm ν on $\mathbb{Q}$ extends to a continuous function on $\mathbb{R}$ satisfying $\nu(xy) = \nu(x)\nu(y)$. Prove that ν is given by $x \mapsto |x|^\lambda$ for some constant $\lambda > 0$. Express λ in terms of $\nu(2)$.

Remark 9.3. We have obtained a complete classification of norms on $\mathbb{Q}$: every norm is either a power of a p-adic norm or a power of the usual absolute value. This classification is called **Ostrowski's theorem**.

9.4 Limits and completions

Remark 9.4. Here we give an alternative definition of p-adics. This section is independent from the previous ones.

Definition 9.7. Let $\{C_i\}$ be a set of vector spaces or abelian groups associated with the vertices of a commutative diagram $\mathcal{C}$, and $V \subset \prod_i C^i$ the set of all collections $v_i \in C_i$ such that for any map $\phi_{ij} : C^i \longrightarrow C^j$ associated with a vertex, one has $\phi_{ij}(v_i) = v_j$. The space V is called **an inverse limit** of a diagram $\{C_i\}$. The same notion is also called **limit** and **projective limit**. Inverse limit is denoted $\varprojlim$.

Exercise 9.20. Let $... \longrightarrow C_1 \longrightarrow C_2 \longrightarrow C_3 \longrightarrow ...$ be a diagram with all arrows injective. Prove that $\varprojlim C_i$ is an itersection of all C_i.

Exercise 9.21. Let $C_1 \longrightarrow C_2 \longrightarrow C_3 \longrightarrow ... \longrightarrow C_n$ be a diagram. Prove that $\varprojlim C_i = C_1$.

Exercise 9.22 (*). Find an example of a diagram $... \longrightarrow C_1 \longrightarrow C_2 \longrightarrow C_3 \longrightarrow ...$ where all spaces C_i are non-zero, and the limit $\varprojlim C_i$ vanishes.

Definition 9.8. A diagram $\mathcal{C}$ is called **cofiltered** if for any two vertices C_i, C_j, there exists a third vertex C_k, and sequences of arrows leading from C_k to C_i and to C_j.

Exercise 9.23. Let $\mathcal{C}$ be a commutative diagram of vector spaces C_i, with all C_i equipped with a ring structure, and all arrows ring homomorphisms. Suppose that the diagram $\mathcal{C}$ is cofiltered. Prove that $\varprojlim C_i$ admits a structure of a ring, such that the natural maps $\varprojlim C_i \longrightarrow C_i$ are ring homomorphisms.

Definition 9.9. Let G be a topological group. A sequence $\{g_i\} \subset G$ is called **a Cauchy sequence** if for any neighbourhood of $U \ni e$ of unity there exists $g \in G$ such that gU contains almost all elements of $\{g_i\}$. Cauchy sequences $\{a_i\}, \{b_i\} \subset G$ are **equivalent** if the sequence $a_1, b_1, a_2, b_2, ...$ is Cauchy. **Completion** of a topological group is the set of all equivalence classes of Cauchy sequences.

Exercise 9.24. Define the following topology on the completion $\bar{G}$ of a topological group G. The base of open sets in $\bar{G}$ is obtained from the open sets $U \subset G$, with an open set $\bar{U} \subset \bar{G}$ defined as the set of all sequences $\{a_i\}$ such that almost all a_i belong to U. Define the multiplicative structure on $\bar{G}$ by $\{a_i\}\{b_i\} = \{a_i b_i\}$. Prove that a completion $\bar{G}$ of a topological group G is a topological group.

Exercise 9.25. Consider a map from a topological group G to its completion $\bar{G}$, taking $g \in G$ to the sequence $g, g, g, g, ...$ Prove that this defines a homomorphism $G \longrightarrow \bar{G}$ of topological groups, and G is dense in $\bar{G}$.

Definition 9.10. Let $I \subset R$ be an ideal in a ring. Define **the I-adic topology** on R with the base of open sets given as $a + I^k \subset R$, for all $a \in R$ and $k \in \mathbb{Z}^{>0}$. Define **I-adic completion** of R as the completion of $\frac{R}{\cap_k I^k}$ in this topology.

Exercise 9.26 (!). Prove that I-adic completion $\bar{R}$ of R is equipped with a ring structure in such a way that the natural map $R \longrightarrow \bar{R}$ is a homomorphism. Prove that $\bar{R}$ is isomorphic to the inverse limit $\lim\limits_{\leftarrow} R/I^k$.

Exercise 9.27. Define **the p-adic norm on** $\mathbb{Z}$ as the map $\nu_p : \mathbb{Z} \longrightarrow \mathbb{Q}$ taking $x \in \mathbb{Z}$ to p^{-n}, where n is the maximal number such that x is divisible by p^n in $\mathbb{Z}$. Consider the topology associated with the ideal (p) as in Definition 9.10, called **the p-adic topology**. Prove that the completion of $\mathbb{Z}$ with respect to the norm ν_p is equal to the completion of $\mathbb{Z}$ with respect to the p-adic topology.

Exercise 9.28. Let p be a prime number. Define **the ring $\mathbb{Z}_p$ of p-adic numbers** as $\lim\limits_{\leftarrow} \mathbb{Z}/p^k\mathbb{Z}$.

a. Prove that any power series $\sum_{i=0}^{\infty} a_i p^i$ converges in $\mathbb{Z}_p$, for any $a_i \in \mathbb{Z}$. Prove that any element in $\mathbb{Z}_p$ can be obtained as a sum of such series.

b. Prove that $\mathbb{Z}_p$ is a local ring, and every $x \in \mathbb{Z}_p$ which is not divisible by p is invertible in $\mathbb{Z}_p$.

Exercise 9.29 (*). Let G be a group, and $\mathfrak{S}$ the set of all normal subgroups of finite index. **Profinite topology** on G is topology with the base of open sets given by all gS, where $g \in G$ and $S \in \mathfrak{S}$. **Profinite completion** is the completion of the quotient $\frac{G}{\bigcap_{S \in \mathfrak{S}} S}$ with respect to this topology. Prove that the profinite completion of G is $\lim\limits_{\leftarrow} G/S$, where the limit is taken over all $S \in \mathfrak{S}$.

Exercise 9.30 (*). Prove that the profinite completion of a group is compact and Hausdorff.

Exercise 9.31 (*). Prove that the profinite completion of $\mathbb{Z}$ is $\prod_p \mathbb{Z}_p$, where the product is taken over all prime numbers.

Exercise 9.32. Prove that this definition of p-adics is equivalent to the one given in Section 2.