p-adic numbers and applications
Lecture Notes for the Summer School for Undergraduates at ELTE, 2013

Gergely Zábrádi

3rd June 2013

These are the notes for the course 'p-adic numbers and applications' at the Summer School for undergraduates at ELTE, July 2013.

In this course we intend to advertise the usefulness and relevance of the p-adic numbers. Instead of concentrating on the proof of one particular theorem, our goal is to give an idea of 1) how things work in the p-adic world; 2) what questions can be answered using them; 3) what directions of current research there are.

The book [4] that we will mostly follow in motivating p-adics is an excellent introduction. The books [7, 12] are more advanced. The former gives a concise introduction to the theory of p-adic L-functions (and zeta-functions) and the latter contains an elementary proof of the Hasse-Minkowski theorem.

1 Why p-adic numbers?

Historically, the main motivation for the developement of algebraic number theory was the attempt to prove Fermat's Last Theorem, ie. when $n \geq 3$ is an integer then there are no integer solutions of $x^n + y^n = z^n$ with $xyz \neq 0$. This was such a problem in mathematics whose solution required the systematic study of several areas and led to the developement of arithmetic geometry, among many others.

Arithmetic algebraic geometry is the area of mathematics dealing with the rational or integer solutions of polynomial equations.

Over the last century, p-adic numbers have played a very important role in arithmetic geometry. They were introduced by Kurt Hensel in 1897 motivated by the analogies of $\mathbb{Z}$ with field of fractions $\mathbb{Q}$ and $\mathbb{C}[t]$ (complex polynomials in 1 variable) with field of fractions $\mathbb{C}(t)$. Note for instance that both $\mathbb{Z}$ and $\mathbb{C}[t]$ are unique factorisation domains, ie. any element can be decomposed (upto units uniquely) as a product of primes. While the primes in $\mathbb{Z}$ are the usual prime numbers, the primes in $\mathbb{C}[t]$ are the linear polynomials $t - \alpha$ ($\alpha \in \mathbb{C}$). Moreover, any rational number can be written as the quotient of two integers; similarly, any rational function can be—by definition—written as a quotient of two polynomials. The analogy, in fact, is much deeper. We may write each polynomial $P(t)$ in the form $P(t) = a_0 + a_1(t-\alpha) + a_2(t-\alpha)^2 + \cdots + a_n(t-\alpha)^n$ (with $a_i \in \mathbb{C}$) and each integer $m \geq 0$ in the form $m = a_0 + a_1 p + \cdots + a_n p^n$ with $a_i \in \{0, 1, \ldots, p-1\}$. The expansion in $t - \alpha$ will show, for example, whether or not the polynomial vanishes at $t = \alpha$ and if so, to which order. On the other hand, for integers this expansion tells us to what order p divides m. Moreover, in case of quotients of polynomials we can push this further. Taking $f(t) = P(t)/Q(t)$ and $\alpha \in \mathbb{C}$ we may expand

$$f(t) = a_{n_0}(t-\alpha)^{n_0} + a_{n_0+1}(t-\alpha)^{n_0+1} + \cdots = \sum_{i \geq n_0} a_i (t-\alpha)^i \ .$$

This is called the Laurent series expansion of f around α.

- We can have $n_0 < 0$ here—this happens if and only if the order of the root of $Q(t)$ at α is bigger than the order of the root of $P(t)$ at α. In complex analysis we say in this case that f has a *pole* at α of order $-n_0$.
- The expansion will not be finite. In fact, it will only be finite if $Q(t)$ is constant times a power of $t - \alpha$. One can show that the series will be convergent in a punctured neighbourhood of α, but for now we regard the expression above as a formal Laurent series, ignoring the question of convergence.

Why don't we try the same for the rational numbers? We may write both the numerator and denominator in base p and divide formally. For example, with $p = 5$ we obtain

$$\frac{35}{31} = \frac{2p + p^2}{1 + p + p^2} = 2p + 4p^2 + 3p^3 + p^4 + 4p^5 + 4p^6 + \dots \ .$$

To check that this is indeed correct we multiply both sides by $31 = 1 + p + p^2$ and use $p = 5$ to compute (expanding upto p^6)

$$\begin{aligned} (1+p+p^2)(2p + 4p^2 + 3p^3 + p^4 + 4p^5 + 4p^6 + \dots) = \\ = (2p + 2p^2 + 2p^3) + (4p^2 + 4p^3 + 4p^4) + (3p^3 + 3p^4 + 3p^5) + \\ + (p^4 + p^5 + p^6) + 4p^5 + 4p^6 + 4p^6 + \cdots = \\ = 2p + 6p^2 + 9p^3 + 8p^4 + 8p^5 + 8p^6 + \cdots = \\ = 2p + p^2 + 10p^3 + 8p^4 + 8p^5 + 8p^6 + \cdots = \\ = 2p + p^2 + 10p^4 + 8p^5 + 8p^6 + \cdots = 2p + p^2 \end{aligned}$$

This above is not precise at all (with all those dots) but at least you should get the feeling what is going on. However, it is easy to check that this can always be done and the process gives an infinite expansion

$$\frac{a}{b} = a_{n_0}p^{n_0} + a_{n_0+1}p^{n_0+1} + \dots$$

of any (positive, for now) rational number a/b with $a_i \in \{0, 1, \dots, p-1\}$. This even reflects the properties of the rational number a/b "near p" (or "locally at p"), ie. if $(a, b) = 1$ then $n_0 < 0$ if and only if $p \mid b$. You could ask what happens to the negatives? As any negative number is a product of -1 and a positive number, it suffices to expand -1:

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots + (p-1)p^n + \dots \ .$$

If we return for the moment to the case of rational functions, each $f(t) \in \mathbb{C}(t)$ can be expanded as Laurent series at each primes $t - \alpha$. However, we have seen many functions at calculus class having a Laurent (even Taylor) series expansion that are not a quotient of two polynomials, for instance e^t or $\sin t$. We may even ignore convergence and take the field $\mathbb{C}((t))$ of all formal Laurent series (with finite "tail"). The field $\mathbb{C}(t)$ of rational functions is a subfield of this. The field $\mathbb{Q}_p$ of p-adic numbers is the analogue of $\mathbb{C}((t))$, ie. the set

$$\mathbb{Q}_p = \{a_{n_0}p^{n_0} + a_{n_0+1}p^{n_0+1} + \cdots \mid a_i \in \{0, 1, \ldots, p-1\},\ n_0 \le i\}$$

of finite-tailed (= "finite to the *left*", but usually infinite to the *right*) Laurent series with the above described multiplication and addition. Note that unlike in $\mathbb{C}((t))$ we need to "carry over", e.g. $(2 + 0 \cdot p + \ldots) + ((p-1) + 0 \cdot p + \ldots) = 1 + 1 \cdot p + \ldots$. We denote by $\mathbb{Z}_p$ the subring of those elements in $\mathbb{Q}_p$ with $n_0 \ge 0$. This subset is indeed closed under addition and multiplication.

1.1 Exercises

Exercise 1.1. Suppose that $f(t) = P(t)/Q(t)$ is in lowest terms so that $P(t)$ and $Q(t)$ do not have common zeros. Show that the expansion of $f(t)$ in $t - \alpha$ is finite if and only if $Q(t) = a_m(t-\alpha)^m$ for some $0 \le m \in \mathbb{Z}$ and $0 \ne a_m \in \mathbb{C}$.

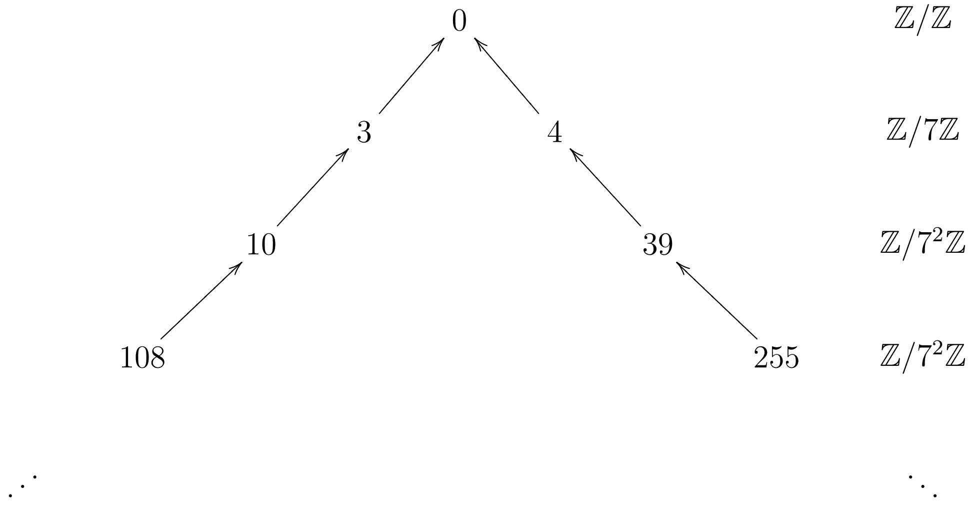
Exercise 1.2. Consider a p-adic number $x = a_0 + a_1 p + \cdots + a_n p^n + \ldots$. What is the expansion of $-x$?

Exercise 1.3. Show that $\mathbb{Q}_p$ is indeed a field.

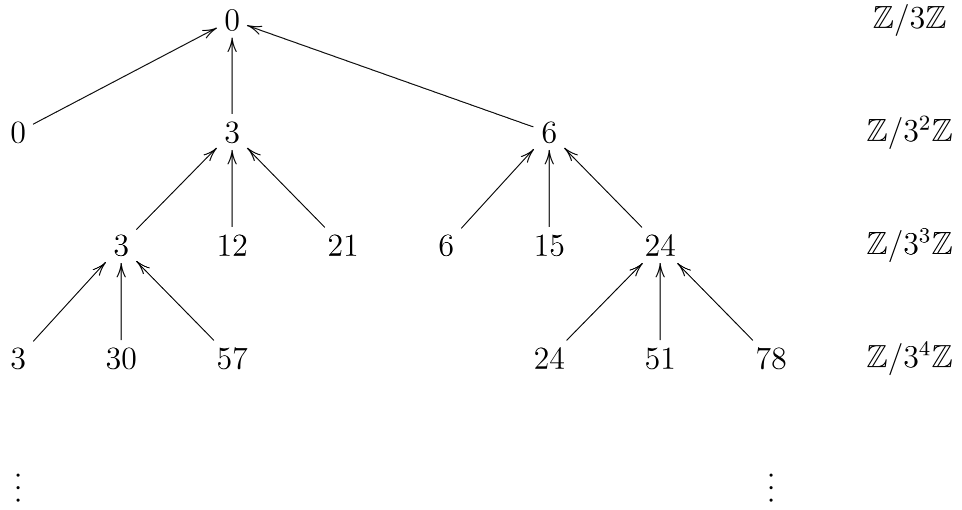
Problem 1.4. Prove that the p-adic expansion of an element in $\mathbb{Q}_p$ is eventually periodic if and only if the element is rational (ie. lies in $\mathbb{Q}$). *Hint:* Mimic the proof of the analogous statement in $\mathbb{R}$

2 Solving equations in $\mathbb{Q}_p$

We would like to illustrate how solving equations in the p-adics is related to solving equations modulo p^n. For example, take $p = 7$ and consider the equation $x^2 = 2$. Solve it first mod 7, we find right away that $x \equiv \pm 3 \pmod 7$ is a solution. Then proceed to mod 7^2 and look for the solution in the form $x = 3 + 7x_1$ (or $x = -3 + 7x_1$). $(3+7x_1)^2 = 9 + 42x_1 + 49x_1^2 \equiv 9 + 42x_1 \pmod{49}$, so we need $9 + 42x_1 \equiv 2 \pmod{49}$, that is $x_1 \equiv 1 \pmod 7$. Note that in this second step we only need to solve a *linear* equation, not quadratic any more. Now we go on to 7^3 and look for the solution in the form $x = 3 + 1 \cdot 7 + 7^2 x_2$. By a similar calculation we obtain $x_2 \equiv 2 \pmod 7$. And so forth we obtain a solution $x = 3 + 7 + 2 \cdot 7^2 + \cdots \in \mathbb{Q}_7$ of the equation $x^2 = 2$. (In particular we see that $\mathbb{Q} \subsetneq \mathbb{Q}_7$.) Similarly, we will also find a solution of the form $x = 4 + 5 \cdot 7 + \cdots \in \mathbb{Q}_7$ starting with the solution $-3 \equiv 4 \pmod 7$. As $\mathbb{Q}_7$ is a field, we have found all the solutions. All this worked out pretty well because 7 does not divide the discriminant of the polynomial $x^2 - 2$. The tree of solutions in $\mathbb{Z}_7$ looks like



What happens if the prime p does divide the discriminant of our equation? Let us have a look at the equation $x^2 = 9$ in $\mathbb{Q}_3$. Modulo 3 this has only one double root, $x \equiv 0 \pmod 3$. So we are looking for the solution in the form $x = 3x_1$ and $(3x_1)^2 \equiv 9 \equiv 0 \pmod 9$ is satisfied trivially for any $x_1 = 0, 1, 2$, therefore we have 3 solutions of $x^2 = 9$ in $\mathbb{Z}/9\mathbb{Z}$, namely $0, 3$, and 6. Now we look at the equation mod $3^3 = 27$. $(3x_1)^2 \equiv 9 \pmod{27}$ has solutions $x_1 \equiv 1, 2 \pmod 3$. Hence we have $\{x \in \mathbb{Z}/27\mathbb{Z} \mid x^2 = 9\} = \{3, 6, 12, 15, 21, 24\}$. In other words, the solutions $x \equiv 3, 6 \pmod 9$ can be lifted to a solution mod 27 in three ways, but the solution $x \equiv 0 \pmod 9$ cannot be lifted. By proceeding further, it is not hard to see that we will always have either 3 or 0 lifts of each solution mod 3^n to a solution mod 3^{n+1} for all $n \geq 1$ and the tree


0
0
3
6
3
12
21
6
15
24
3
30
57
24
51
78
$\mathbb{Z}/3\mathbb{Z}$
$\mathbb{Z}/3^2\mathbb{Z}$
$\mathbb{Z}/3^3\mathbb{Z}$
$\mathbb{Z}/3^4\mathbb{Z}$

of solutions have 2 infinite branches (and many finite) contending to the fact that there are only 2 solutions (namely $x = \pm 3$) in $\mathbb{Q}_3$.

2.1 Exercises

Exercise 2.1. Give a rigorous proof that the above process gives you a solution of $x^2 = 2$ in $\mathbb{Q}_7$.

Exercise 2.2. Prove that $x^2 + 1 = 0$ has a solution in $\mathbb{Q}_5$, but not in $\mathbb{Q}_7$. Can you describe the primes p for which this equation has a solution in $\mathbb{Q}_p$?

Problem 2.3. Show that if $f(x) \in \mathbb{Z}[x]$ is a *monic* polynomial and p is a prime then all the solutions of $f(x) = 0$ in $\mathbb{Q}_p$ lie in fact in $\mathbb{Z}_p$. *Hint:* Prove by contradiction and try and compute the first nonzero term of $f(\alpha)$ for $\alpha \in \mathbb{Q}_p \setminus \mathbb{Z}_p$.

Problem 2.4. Prove that the field $\mathbb{Q}_p$ is not algebraically closed for any prime number p. Can you construct an irreducible polynomial over $\mathbb{Q}_p$ of any given degree $0 < n \in \mathbb{Z}$?

Problem 2.5. Verify that the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ is strict for any prime number p. *Hint:* You could argue by noting that the cardinality of $\mathbb{Q}_p$ is bigger than the cardinality of $\mathbb{Q}$, but there is also an algebraic argument.

3 Precise definition of $\mathbb{Q}_p$

Definition 3.1. *Let K be a field. We call a function $|\cdot|\colon K \to \mathbb{R}^{\geq 0}$ an absolute value (or multiplicative valuation) on K, if it satisfies*

(1) $|x| = 0 \iff x = 0$;

(2) $|xy| = |x||y|$;

(3) $|x + y| \leq |x| + |y|$ *(triangle inequality).*

The absolute value $|\cdot|$ induces a metric $d(x, y) := |x - y|$ on K. This way K becomes a metric space, in particular, there is a topology on it.

Example 3.2. *The* trivial *absolute value: $|x| = 1$ if $x \neq 0$ and $|0| = 0$.*

Definition 3.3. *We say that the two absolute values $|\cdot|_1$ and $|\cdot|_2$ on K are* equivalent*, if they induce the same topology.*

Proposition 3.4. *$|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if there exists a real number $s > 0$ such that $|x|_1 = |x|_2^s$ for all $x \in K$.*

Proof. The implication $\Leftarrow$ is trivial. Conversely, note that $|x|_i < 1$ holds if and only if the powers of x tend to zero in the absolute value $|\cdot|_i$ $(i = 1, 2)$. Hence if $|\cdot|_1$ and $|\cdot|_2$ induce the same topology then $|x|_1 < 1 \iff |x|_2 < 1$. Applying this to $x = a/b$ and $x = b/a$ we obtain $|a|_1 \leq |b|_1 \Leftrightarrow |a|_2 \leq |b|_2$ $(a, b \in K)$. In particular, if one of $|\cdot|_1$ and $|\cdot|_2$ is trivial then so is the other. Therefore we may assume that there exists a $y \in K$ such that $|y|_1 > 1$ (whence $|y|_2 > 1$), so we choose $0 < s := \log_{|y|_2} |y|_1 \in \mathbb{R}$ so that we have $|y|_1 = |y|_2^s$. Now for any $0 \neq x \in K$ there is an $\alpha = \alpha(x) \in \mathbb{R}$ with $|x|_1 = |y|_1^\alpha$. We choose the sequence $(\frac{m_i}{n_i})_{i\in\mathbb{N}}$ $(m_i, n_i \in \mathbb{Z},\ n_i \neq 0)$ of rational numbers so that $\lim_{i\to\infty} \frac{m_i}{n_i} = \alpha + 0$. We obtain $|x|_1 = |y|_1^\alpha < |y|_1^{m_i/n_i}$, hence $|x^{n_i}|_1 < |y^{m_i}|_1$, whence $|x^{n_i}|_2 < |y^{m_i}|_2$, ie. $|x|_2 < |y|_2^{m_i/n_i}$. Letting $i \to \infty$ we deduce $|x|_2 \leq |y|_2^\alpha$. The inequality $|x|_2 \geq |y|_2^\alpha$ is proven in a similar fashion, so we have $|x|_1 = |y|_1^\alpha = |y|_2^{s\alpha} = |x|_2^s$ for all $0 \neq x \in K$ (and, of course, also for $x = 0$). □

Definition 3.5. *We say that the absolute value* $|\cdot|$ non-archimedean *if the set* $\{|n\cdot 1|\colon n\in\mathbb{Z}\}\subseteq\mathbb{R}$ *is bounded. Otherwise* $|\cdot|$ *is archimedean.*

Remark. The above definition is equivalent to saying that the ring homomorphism $f\colon\mathbb{Z}\to K$, $f(1)=1$ has bounded image in K if and only if $|\cdot|$ is non-archimedean.

Example 3.6. *1. The trivial absolute value is non-archimedean.*

2. The usual absolute value (that we denote by $|\cdot|_\infty$ *in this note) on* $\mathbb{R}$ *(or on* $\mathbb{C}$*, or on any subfield* $K\leq\mathbb{C}$*) is archimedean.*

3. Let p *be a prime. The* p*-adic absolute value* $|\cdot|_p$ *on* $\mathbb{Q}$ *is defined by* $|\frac{a}{b}p^n|_p=p^{-n}$ *where* $p\nmid a,b\in\mathbb{Z}$ *(and* $|0|_p=0$*). This is non-archimedean, since whenever* $\frac{a}{b}p^n\in\mathbb{Z}$ *we have* $n\geq 0$ *and* $|\frac{a}{b}p^n|_p=p^{-n}\leq 1$.

Proposition 3.7. *The absolute value* $|\cdot|$ *is non-archimedean if and only if the so called* ultrametric *inequality holds:*

$(3')$ $|x+y|\leq\max(|x|,|y|)$.

Moreover, if $|\cdot|$ *is non-archimedean then* $\{|n\cdot 1|,n\in\mathbb{Z}\}$ *is not only bounded, but bounded by* 1.

Proof. If $(3')$ holds then we have $|n\cdot 1|\leq|1|=1$. On the other hand, for $0<k\in\mathbb{Z}$, $|x|\geq|y|$ and $|n\cdot 1|\leq C$ for some $0<C\in\mathbb{R}$ then we have

$$|x+y|^k=|(x+y)^k|=|\sum_{j=0}^{k}\binom{k}{j}x^jy^{k-j}|\leq\sum_{j=0}^{k}|\binom{k}{j}\cdot 1||x|^j|y|^{k-j}\leq\sum_{j=0}^{k}C|x|^k=(k+1)C|x|^k\ .$$

Taking k^{th} root and letting $k\to\infty$ the statement follows. □

Theorem 3.8 (Ostrowski)**.** *On* $\mathbb{Q}$ *any nontrivial absolute value* $|\cdot|$ *is equivalent to either the real* $|\cdot|_\infty$ *or the* p*-adic* $|\cdot|_p$ *absolute value for some prime* p*. These valuations are pairwise inequivalent.*

Proof. Case 1: $|\cdot|$ is non-archimedean. If we have $|p|=1$ for all primes p then the absolute value is trivial (see Exercise 3.1). So we may take a prime p such that $\|p\|<1$. Therefore the set $A:=\{a\in\mathbb{Z}\colon\|a\|<1\}$ contains p and is an ideal in $\mathbb{Z}$ as it is closed under addition by $(3')$ and also by multiplication by any integer because of (2) (see Proposition 3.7). On the other hand, $1\notin A$ so we have $A=(p)$ as (p) is a maximal ideal in $\mathbb{Z}$. Hence for $p\nmid a,b\in\mathbb{Z}$ we have $|a|=|b|=1$ and $|\frac{a}{b}p^n|=|p|^n=|\frac{a}{b}p^n|_p^s$ where $s:=\log_{1/p}|p|$.

Case 2: $|\cdot|$ is archimedean. Let $1<m,n\in\mathbb{Z}$ be arbitrary.

Lemma 3.9. *We have* $|m|^{1/\log m}=|n|^{1/\log n}$*. (Here* log *denotes, say, the natural logarithm, in fact the base doesn't matter.)*

Proof. Write m in base n, ie. $m=\sum_{i=0}^{r}a_in^i$ where $0\leq a_i<n$ $(0\leq i\leq r)$. So we have $n^r\leq m$, whence $r\leq\frac{\log m}{\log n}$ and $|a_i|\leq a_i|1|=a_i\leq n$. Therefore we compute

$$|m|=|\sum_{i=0}^{r}a_in^i|\leq\sum_{i=1}^{r}|a_i||n|^i\ . \tag{1}$$

Note that $|n| \leq 1$ implies $|m| \leq nr \leq \frac{n \log m}{\log n}$. Applying this to m replaced by m^k and taking k^{th} root we obtain $|m| \leq \sqrt[k]{\frac{kn \log m}{\log n}}$. Letting $k \to \infty$ we get an upper bound for $|m|$ independent of m which contradicts to the assumption $|\cdot|$ being archimedean. So we have $|n| > 1$, and using (1) we compute

$$|m| \leq \sum_{i=0}^{r} |a_i||n|^i \leq |n|^r \sum_{i=0}^{r} |a_i| \leq |n|^r n(r+1) \leq |n|^{\log m/\log n} n(1 + \frac{\log m}{\log n}) \ .$$

Substituting m^k into m, taking k^{th} root, and letting $k \to \infty$ we obtain $|m| \leq |n|^{\log m/\log n}$. The statement follows by interchanging m and n. □

Put $s := \frac{\log |n|}{\log n}$ for some fixed $1 < n \in \mathbb{Z}$. By the above Lemma $0 < s$ and s does not depend on the choice of n. So we have $|m| = e^{s \log m} = m^s = |m|_\infty^s$ for all $1 < m \in \mathbb{Z}$. The statement follows for all nonnegative rational numbers by taking quotients and by Exercise 3.1 for negative rationals. □

Definition 3.10. *The field K is said to be* complete *with respect to the absolute value $|\cdot|$ if any Cauchy sequence is convergent.*

Example 3.11. *Both $\mathbb{R}$ and $\mathbb{C}$ are complete with respect to $|\cdot|_\infty$, but $\mathbb{Q}$ is only complete with respect to the trivial absolute value.*

In the following we are going to show that any field K with an absolute value $|\cdot|$ can be embedded isometrically as a subfield into a complete field. We define

$$R := \{(a_n)_n \in K^{\mathbb{N}} \colon \forall \varepsilon > 0 \exists N \in \mathbb{N} \text{ s. t. } |a_n - a_m| < \varepsilon \text{ for all } m, n \geq N\}$$

as the ring of Cauchy sequences in K. This is indeed a ring with respect to the pointwise addition and multiplication. Note that K can be embedded into R diagonally, ie. we have a ring homomorphism $\iota \colon K \hookrightarrow R$ defined by $\iota(c) := (c)_n$. Let $I_0 \subset R$ be the set of those sequences that are identically 0 except for finitely many terms. This set is an ideal in R. Let $R_0 := R/I_0$ the quotient. We may think of R_0 as the ring of equivalence classes of Cauchy sequences with respect to the equivalence relation $(a_n)_n \sim (b_n)_n$ if $a_n = b_n$ for all but finitely many $n \in \mathbb{N}$.

Proposition 3.12. *R_0 is a local ring. Its unique maximal ideal consists of the those Cauchy sequences that converge to 0 ("zero sequences").*

Remark. In case you just heard this expression for the first time a commutative ring R is said to be a *local ring* if it has a unique maximal ideal.

Proof. Let $M \subset R$ be the set of zero sequences. It is clear that $I_0 \subset M$ and M is an ideal in R. On the other hand, if $(a_n)_n$ is a Cauchy sequence with $a_n \not\to 0$ then $1/a_n$ makes sense if n is large enough and is also a Cauchy sequence. This shows that the equivalence class of $(a_n)_n$ is invertible in R_0. Therefore M is indeed the unique maximal ideal of R containing I_0, or equivalently, M/I_0 is the unique maximal ideal in R_0 by Exercise 3.4. □

Definition 3.13. *Let K be a field with an absolute value $|\cdot|$. We define $\hat{K} := R/M$ to be the* completion *of K wrt. $|\cdot|$. Note that this is indeed a field as M is a maximal ideal in R.*

Note that the composite map $K \overset{\iota}{\hookrightarrow} R \to \hat{K} = R/M$ is still injective: if $0 \neq c \in K$ the the constant c sequence does not tend to 0 hence does not lie in M. So from now on we identify K with its image in $\hat{K}$. We still need to verify that $\hat{K}$ is indeed complete in order to justify the term "completion". (In fact we also need the universal property of $\hat{K}$ for being the completion, ie. any ismoetric field homomorphism $\varphi\colon K \to F$ into a valued field F factors through $\hat{K}$.) For this we first need to extend $|\cdot|$ from K to $\hat{K}$. Since the topology on K is defined so that the map $|\cdot|\colon K \to \mathbb{R}$ is continuous, it takes any Cauchy sequence in K to a Cauchy sequence in $\mathbb{R}$. As $\mathbb{R}$ is complete, we may define $|(a_n)_n|$ as a limit $\lim_{n\to\infty} |a_n|$. So we obtain a valuation R and M is the set of elements with valuation 0 by definition. Therefore the absolute of $(a_n)_n \in R$ only depends on its class in $R/M = \hat{K}$. This way we obtain an absolute value on $\hat{K}$ which we still denote by $|\cdot|$. We leave the proof of the fact that $\hat{K}$ is indeed complete and has the required universal property to the reader as an exercise (see Exercises 3.6 and 3.7).

Definition 3.14. *The field $\mathbb{Q}_p$ of p-adic numbers is the completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$.*

3.1 Exercises

Exercise 3.1. Show that if $|\cdot|$ is any absolute value on the field K then we have $|1| = 1$ and $|-x| = |x|$.

Exercise 3.2. Show that in an ultrametric space all triangles are isosceles.

Exercise 3.3. Show that the absolute value $|\cdot|_p$ on $\mathbb{Q}$ satisfies the axioms $(1) - (3)$.

Problem 3.4. Show that a commutative ring R is local if and only if it contains an ideal $I \lhd R$ such that all the elements in $R \setminus I$ are invertible in R.

Exercise 3.5. Verify the axioms $(1) - (3)$ for the absolute value $|\cdot|$ on $\hat{K}$ if $\hat{K}$ is the completion of a valued field $(K, |\cdot|)$.

Problem 3.6. The field $\hat{K}$ is complete wrt. $|\cdot|$. *Hint:* We need to show that any Cauchy sequence of Cauchy sequences converges to a Cauchy sequence. You can construct the limit sequence as taking the ${n_i}^{\text{th}}$ term of the i^{th} sequence for n_i large enough (depending on i and the actual sequnce). It is a usual elementary argument in first year analysis how to choose these n_i.

Exercise 3.7. Verify the universal property of $\hat{K}$, ie. all $\varphi\colon K \to F$ isometric field embeddings factor through $\hat{K}$ uniquely. Also show that K is dense in $\hat{K}$. *Hint:* Take a complete field F with respect to the absolute value $|\cdot|$ and an isometric embedding $\varphi\colon K \to F$ of K as subfield of F. Extend φ to R as $\tilde{\varphi}((a_n)_n) := \lim_n \varphi(a_n)$. Since $(a_n)_n$ is a Cauchy sequence and F is complete, this makes sense. The kernel of $\tilde{\varphi}$ is exactly M, in particular it factors through $\hat{K} = R/M$.

Problem 3.8. Show that the field $\mathbb{Q}_p$ of p-adic numbers constructed in the previous section is indeed the completion of $\mathbb{Q}$ wrt. the absolute value $|\cdot|_p$.

Exercise 3.9. Let $(K, |\cdot|)$ be a—not necessarily complete—non-archimedean valued field. We define $\mathcal{O}_K := \{a \in K \colon |a| \leq 1\}$ to be the *ring of integers* in K. Show that this is indeed a subring, moreover, a local ring with maximal ideal $\mathcal{M}_K := \{a \in K \colon |a| < 1\}$. The field $\mathcal{O}_K/\mathcal{M}_K$ is called the residue class field of K. *Hint:* Use Exercise 3.4 and note that the elements with absolute value 1 are invertible in $\mathcal{O}_K$.

Exercise 3.10. Show that the ring of integers in $\mathbb{Q}_p$ is $\mathbb{Z}_p$.

Exercise 3.11. Show that the image of $|\cdot|_p \colon \mathbb{Q}_p \to \mathbb{R}$ is the same as the image of its restriction to $\mathbb{Q}$, namely $\{0\} \cup p^{\mathbb{Z}} \subset \mathbb{R}$.

Problem 3.12. What is the region of convergence of the Taylor series of $\log(1+x)$ and $\exp(x)$ at 0 in $\mathbb{Q}_p$?

4 Towards irreducibility criteria for polynomials over $\mathbb{Q}$

Exercise 4.1. *a*) Show that the polynomial $x^5 - 2x^2 + 6x - 10 \in \mathbb{Q}[x]$ is irreducible.

b) Show that the polynomial $x^2 + 1 \in \mathbb{Q}[x]$ is irreducible.

We note that the above polynomial in *a*) satisfies Eisenstein's criterion for $p = 2$ as 2 divides all the coefficients except for the leading term and 4 does not divide the constant term. In fact, in this proof we only used the prime 2 so the same proof works over $\mathbb{Q}_2$, as well. On the other hand, the polynomial in *b*) is irreducible even over $\mathbb{R}$, so, in particular, it is irreducible over $\mathbb{Q}$. What is the common in these examples?

In fact, Eisenstein's criterion is really a statement over $\mathbb{Q}_p$, not over $\mathbb{Q}$. Whenever a polynomial in $\mathbb{Q}[x]$ is irreducible over some $\mathbb{Q}_p$ or over $\mathbb{R}$ we may deduce its irreducibility over $\mathbb{Q}$, so the method is basically the same in the two examples, but we used different completions.

Over $\mathbb{R}$ it is easy to describe all the irreducible polynomials. These are the linear polynomials, and those quadratics that do not have a root in $\mathbb{R}$. What about $\mathbb{Q}_p$? Can we describe all the irreducible polynomials? The answer is yes, and we need Newton polygons for that. This will provide us with new irreducibility criteria—similar to Eisenstein's—over $\mathbb{Q}$. However, our job is a little bit harder than over $\mathbb{R}$, as the algebraic closure of $\mathbb{Q}_p$ is not a quadratic extension of $\mathbb{Q}_p$, not even a finite extension.

Exercise 4.2. Show that the polynomial $x^5 - 2x^4 + 4 \in \mathbb{Q}[x]$ is irreducible.

"Solution". This is not an Eisenstein polynomial for $p = 2$ (nor for any other prime) as 4 divides the constant term. What next? The idea is to have a look at the 2-adic absolute values of the roots of this polynomial. Assume we decompose this polynomial $x^5 - 2x^4 + 4 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)$ over a larger field $\mathbb{Q} < \mathbb{Q}_2 \leq K$ and put $c_i := -\log_2 |\alpha_i|_2 \in \mathbb{R}$ $(1 \leq i \leq 5)$. Then we have $\prod_{i=1}^5 \alpha_i = -4$ hence $\sum_{i=1}^5 c_i = -\log_2 |-4|_2 = 2$. Moreover we compute $|\alpha_i^5|_2 = \frac{1}{2^{5c_i}}$ and $|2\alpha_i^4| = \frac{1}{2^{4c_i+1}}$. Since in the ultrametic world all triangles are isosceles, we have $5c_i = 4c_i + 1$ or $\min(5c_i, 4c_i + 1) = 2$ by the ultrametric inequality. Note that $5c_i \geq 4c_i + 1$ is impossible as otherwise $\alpha_i^5 - 2\alpha_i^4 = -4$ would be divisible by 2^5 which is nonsense. Therefore we have $c_i = 2/5$ for all $1 \leq i \leq 5$. Now assume that $x^5 - 2x^4 + 4 = g(x)h(x)$ with monic nonconstant $g, h \in \mathbb{Q}_p[x]$. Then $g(x)$ is a product of

some $x-\alpha_i$ $(1 \leq i \leq 5)$. Therefore $g(0)$ is a product of some of the α_i (upto sign) therefore its 2-adic absolute value is $|g(0)| = |\alpha_i|^{\deg g} = 2^{2\deg g/5}$. However, $g(0) \in \mathbb{Q}_p$, so its absolute value is an integer power of 2. So $5 \mid \deg g$ gives us a contradiction as neither g nor h is constant. Therefore $x^5 - 2x^4 + 4$ is irreducible over $\mathbb{Q}_p$ hence also over $\mathbb{Q}$. □

The problem with the above solution is that we have not quite defined the p-adic absolute value of an element of an extension of $\mathbb{Q}_p$. Let alone showing it satisfies the ultrametric inequality. So we are going to do this in the sequel in a precise way.

4.1 Hensel's Lemma

There are various forms of Hensel's Lemma. We are going to prove the version that is needed for extending absolute values from K to a finite field extension as this is needed for Newton polygons. It is in some sense the precise generalization of our observations concerning the solutions of $x^2 = 2$ in $\mathbb{Q}_7$. Let K be a complete non-archimedean field with respect to the valuation $|\cdot|$, denote by $\mathcal{O} = \mathcal{O}_K = \{x \in K \mid |x| \leq 1\}$ its ring of integers, by $\mathfrak{p} = \{x \in K \mid |x| < 1\}$ its maximal ideal, and by $k = \mathcal{O}/\mathfrak{p}$ its residue field. We say that a polynomial $f(x) \in \mathcal{O}[x]$ is *primitive* if $f(x) = a_0 + a_1x + \cdots + a_nx^n$ with $|f| := \max_{0\leq i\leq n}(|a_i|) = 1$.

Theorem 4.1 (Hensel's Lemma). *Let $f(x) \in \mathcal{O}[x]$ be a primitive polynomial and suppose that $\overline{f}(x) := f(x) \pmod{\mathfrak{p}} \in k[x]$ can be written as $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ with $(\overline{g}(x), \overline{h}(x)) = 1$ in $k[x]$. Then there exist primitive polynomials $g(x), h(x) \in \mathcal{O}[x]$ such that $f(x) = g(x)h(x)$, $\overline{g}(x) = g(x) \pmod{\mathfrak{p}}$, $\overline{h}(x) = h(x) \pmod{\mathfrak{p}}$, and $\deg g = \deg \overline{g}$.*

Proof. Put $d := \deg f$, $m := \deg \overline{g}$. Then we have $d - m \geq \deg \overline{h}$. (Note that we only have $\deg \overline{f} \leq d$ as some of the coefficients in $f(x)$ might reduce to zero moduló $\mathfrak{p}$.) At first we lift $\overline{g}$ and $\overline{h}$ arbitrarily by choosing $g_0, h_0 \in \mathcal{O}[x]$ such that

$$\overline{g} = g_0 \pmod{\mathfrak{p}}\ , \quad \overline{h} = h_0 \pmod{\mathfrak{p}}$$

and $\deg g_0 = \deg \overline{g}$, $\deg h_0 = \deg \overline{h} \leq d-m$. Since we have $(\overline{g}, \overline{h}) = 1$, there exist polynomials $a(x), b(x) \in \mathcal{O}[x]$ with $a(x)g_0(x) + b(x)h_0(x) \equiv 1 \pmod{\mathfrak{p}}$. So all the coefficients of both $f(x) - g_0(x)h_0(x)$ and $a(x)g_0(x) + b(x)h_0(x) - 1$ are in the maximal ideal $\mathfrak{p}$. Let π be the coefficient with biggest absolute value in these polynomials (in particular, we have $|\pi| < 1$). We are going to construct g and h in the form

$$\begin{aligned} g(x) &= g_0(x) + \pi p_1(x) + \cdots + \pi^n p_n(x) + \dots \\ h(x) &= h_0(x) + \pi q_1(x) + \cdots + \pi^n q_n(x) + \dots \end{aligned}$$

such that $\deg p_i < m$ and $\deg q_i \leq d - m$. We construct these polynomials inductively. Let $n \geq 1$ and assume we have constructed

$$\begin{aligned} g_{n-1}(x) &= g_0(x) + \pi p_1(x) + \cdots + \pi^{n-1} p_{n-1}(x) \\ h_{n-1}(x) &= h_0(x) + \pi q_1(x) + \cdots + \pi^{n-1} q_{n-1}(x) \end{aligned}$$

such that $|f - g_{n-1}h_{n-1}| \leq |\pi|^n$. Put $f_n(x) := \frac{f(x) - g_{n-1}(x)h_{n-1}(x)}{\pi^n} \in \mathcal{O}[x]$. We define $p_n(x)$ to be the residue in the Euclidean division of $b(x)f_{n-1}(x)$ by $g_0(x)$, ie. we have $b(x)f_{n-1}(x) = Q_n(x)g_0(x) + p_n(x)$ with some $Q_n \in \mathcal{O}[x]$ and $\deg p_n < \deg g_0 = m$. Note that one can indeed take the euclidean division as the leading coefficient of $g_0(x)$ does not lie in $\mathfrak{p}$ hence it is invertible in $\mathcal{O}$. Now we define $q_n(x) \in \mathcal{O}[x]$ to be the polynomial we obtain by ommiting all the nonzero coefficients of $h_0(x)Q_n(x) + a(x)f_n(x)$ with valuation $\leq |\pi|$ so that we have $|q_n - h_0Q_n - af_n| \leq |\pi|$. On the other hand, we have

$$h_0p_n + g_0(h_0Q_n + af_n) = (h_0b + g_0a)f_n \equiv f_n \pmod{\pi} ,$$

so $\deg q_n \leq \deg f_n - \deg g_0 \leq d - m$ as we clearly have $\deg(h_0p_n) \leq d$. Moreover, if we put $g_n = g_{n-1} + \pi^n p_n$ and $h_n = h_{n-1} + \pi^n h_n$ then we compute

$$\begin{aligned} f - g_nh_n = f - g_{n-1}h_{n-1} - \pi^n(g_{n-1}q_n + h_{n-1}p_n) - \pi^{2n}p_nq_n \equiv \\ \equiv \pi^n(f_n - g_{n-1}q_n - h_{n-1}bf_n + h_{n-1}Q_ng_0) \equiv \\ \equiv \pi^n(f_n - q_0h_0Q_n - g_0af_n - h_0bf_n + h_0Q_ng_0) \equiv 0 \pmod{\pi^{n+1}} \end{aligned}$$

as we have $g_{n-1} \equiv g_0 \pmod{\pi}$ and $h_{n-1} \equiv h_0 \pmod{\pi}$. The result follows noting that the sums $g(x) = g_0(x) + \sum_{i=1}^{\infty} \pi^i p_i(x)$ and $h(x) = h_0(x) + \sum_{i=1}^{\infty} \pi^i q_i(x)$ both converge to *polynomials* by the bounds on the degree. For these polynomials we have $f(x) = g(x)h(x)$. □

Corollary 4.2. *If $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ is* irreducible *then we have $|f| = \max(|a_0|, |a_n|)$.*

Proof. We prove by contradiction and may assume without loss of generality that $|f| = 1$ (ie. $f(x) \in \mathcal{O}[x]$ primitive). Let $0 < r < n$ be the smallest index such that $|a_i| = 1$. Then $f(x)$ decomposes as $x^r(a_r + \cdots + a_nx^{n-r}) \equiv f(x) \pmod{\mathfrak{p}}$. We obtain a contradiction using Hensel's Lemma. □

4.2 Extending valuations

Let K be a complete nonarchimedean field as above. Our goal in this section is to prove the following

Theorem 4.3. *Let L/K be a finite field extension. Then the valuation $|\cdot|$ extends uniquely to an ultrametric valuation on L. The extension is given by $|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}$ for $\alpha \in L$ where $n = |L : K|$ the degree and $N_{L/K}(\alpha)$ is the* norm *of α, ie. the determinant of the multiplication by α as a K-linear map $L \to L$.*

Remark. Note that in case of the archimedean field $\mathbb{R}$ the extension of $|\cdot|_\infty$ to $\mathbb{C}$ is indeed given by $|\alpha|_\infty = \sqrt{|N_{\mathbb{C}/\mathbb{R}}(\alpha)|_\infty} = \sqrt{|\alpha \cdot \overline{\alpha}|}$.

Proof. Let us show the uniqueness first assuming that $\sqrt[n]{|N_{L/K}(\cdot)|}$ is a nonarchimedean absolute value. Suppose we have another extension $|\cdot|'$ to L. Denote by $\mathcal{O}_L = \{\alpha \in L \mid |\alpha| \leq 1\}$ and by $\mathcal{O}'_L = \{\alpha \in L \mid |\alpha|' \leq 1\}$ the rings of integers with respect to the two absolute values and by $\mathfrak{p}_L = \{\alpha \in L \mid |\alpha| < 1\}$ and by $\mathfrak{p}'_L = \{\alpha \in L \mid |\alpha|' < 1\}$ the maximal ideals. Assume that α lies in $\mathcal{O}_L \setminus \mathcal{O}'_L$ and let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ be α's minimal polynomial. Note that the norm $N_{L/K}(\alpha)$ is a power of a_0 (upto sign). Since $\alpha \in \mathcal{O}_L$, we have $|N_{L/K}(\alpha)| \leq 1$ therefore we also have $|a_0| \leq 1$. By Corollary 4.2 we deduce that a_i is in $\mathcal{O}_K$ for all $0 \leq i \leq d-1$. On the other hand, $\alpha \notin \mathcal{O}'_L$ whence $|\alpha|' > 1$ and $|1/\alpha|' < 1$. This means that $1 = |1|' = |-a_{d-1}\alpha^{-1} - \cdots - a_0\alpha^{-d}|' < 1$ by the ultrametric inequality. This is a condradiction, so we obtain $\mathcal{O}_L \subseteq \mathcal{O}'_L$. Moreover, $\mathfrak{p}'_L \cap \mathcal{O}_L$ is a prime ideal in $\mathcal{O}_L$ therefore it equals $\mathfrak{p}_L$. Hence we have $\mathfrak{p}_L \subseteq \mathfrak{p}'_L$. All in all we obtain $|\alpha| \leq 1 \Rightarrow |\alpha|' \leq 1$ (by $\mathcal{O}_L \subseteq \mathcal{O}'_L$) and also $|\alpha| > 1 \Rightarrow |1/\alpha| < 1 \Rightarrow |1/\alpha|' < 1 \Rightarrow |\alpha|' > 1$ (by $\mathfrak{p}_L \subseteq \mathfrak{p}'_L$) showing that $|\cdot|$ and $|\cdot|'$ are equivalent.

So it remains to show that $\alpha \mapsto |\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}$ is indeed a nonarchimedean valuation on L. Axioms (1) and (2) are obviously satisfied, so we only need to check (3′). Choose $\alpha, \beta \in L$ and assume (as we may) that $|\beta| \leq |\alpha| \leq 1$. So the statement of (3′) means that we also have $|\alpha + \beta| \leq 1$, in other words we are reduced to proving that $\mathcal{O}_L = \{\alpha \in L \mid N_{L/K}(\alpha) \in \mathcal{O}_K\}$ is a subring (in particular, closed under addition) in L. By Corollary 4.2 $\mathcal{O}_L$ is exactly the set of those elements in L whose monic minimal polynomial has coefficients in $\mathcal{O}_K$, ie. the *integral closure* of $\mathcal{O}_K$ in L which is known to be a subring (this is the way one proves that the algebraic integers form a ring). Since the proof is simple, we include it here:

Lemma 4.4. *Let B be an integral domain, $A \leq B$ be a subdomain, and $b_1, \dots, b_k \in B$ arbitrary. The elements b_i ($1 \leq i \leq k$) all have monic minimal polynomials over A (ie. they are* integral *over A) if and only if the subring $A[b_1, \dots, b_k] \leq B$ generated by $b_1, \dots, b_k$ over A is finitely generated as a module over A.*

Remark. Note that being finitely generated as a subring is much weaker than being finitely generated as a module over A. In the former we may multiply the generators together but in the latter we can only multiply the generators by constants in A.

The proof of the Lemma: $\Rightarrow$: Induction on k. The case $k = 0$ is trivial. Now by induction, the ring $R = A[b_1, \dots, b_{k-1}]$ is finitely generated as a module over A, say by the generators $x_1, \dots, x_t$. We are going to show that the set $\{x_j b_k^i \mid 1 \leq j \leq t, 0 \leq i \leq d-1\}$ generate $A[b_1, \dots, b_k]$ as a module over A where d denotes the degree of the minimal polynomial $f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0 \in A[x]$ of b_k over A. Indeed, any element in $A[b_1, \dots, b_k] = R[b_k]$ can be written as a polynomial in b_k with coefficients in R. The coefficients can be written as an A-linear combination of $x_1, \dots, x_t$ and the polynomial can be reduced to having degree $< d$ by euclidean division by f as $f(b_k) = 0$ and f is monic.

$\Leftarrow$: Suppose that $A[b_1, \dots, b_k]$ is finitely generated as a module over A, say by generators $x_1, \dots x_t$. Then we may take the matrix $M_i \in A^{t \times t}$ of the multiplication by b_i in the basis $x_1, \dots, x_t$. Note that the matrix M_i is not unique as we may have "relations" between the x_j's. However, it certainly exists since the $x_1, \dots, x_t$ form a generating system. By the theorem of Cayley and Hamilton, b_i is the root of its own characteristic polynomial which is monic and has coefficients in A. Therefore the minimal polynomial of b_i over A exists and is also monic as it divides the characteristic polynomial. □

4.3 Newton polygons

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Q}_p[x]$ be a polynomial. The Newton polygon of f is the (boundary of the) lower convex hull of the points

$$\{(-n, -\log_p |a_n|), \dots, (-i, -\log_p |a_i|), \dots, (0, -\log_p |a_0|)\} \subset \mathbb{Z}^2 \subset \mathbb{R}^2$$

on the euclidean plane. That is, take the intersection of all the closed half-planes containing these points and lying above some nonvertical line. We say that the multiplicity of the slope

$a/b \in \mathbb{Q}$ is m if we have a segment in the Newton polygon with slope a/b and horizontal width m. The polynomial f has exactly n slopes if counted with multiplicities.

Example 4.5. *The Newton polygon of the polynomial* $x^3+px^2+px+p^3$ *has vertices* $(-3,0)$, $(-1,1)$, *and* $(0,3)$*. It has slopes* $1/2$ *with multiplicity* 2 *and* 2 *with multiplicity* 1*.*

The *additive valuation* of $\alpha \in \overline{\mathbb{Q}_p}$ is by definition $-\log_p|\alpha|_p$. Note that α belongs to a finite extension K of $\mathbb{Q}_p$ and we extended $|\cdot|_p$ to K in the previous section.

Theorem 4.6. *The multiset of slopes of the Newton polygon of f equals the multiset of the additive valuations of the roots of f in* $\overline{\mathbb{Q}_p}$*.*

Proof. We introduce the ρ-norm (Gauss-norm) on $\mathbb{Q}_p[x]$ for each real number $\rho > 0$ by putting $\|a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0\|_\rho := \max_{1\leq i\leq n}(|a_i|_p\rho^i)$. The *width* of f under the ρ-norm is the difference between the maximum and minimum values of i for which $\max_i(|a_i|_p\rho^i)$ is achieved. Note that the multiplicity of the slope a/b in the Newton polygon of f is nothing else but the width of f under the ρ-norm with $\rho = p^{-a/b}$. The statement follows from the following

Lemma 4.7. *For $f(x), g(x) \in \mathbb{Q}_p[x]$ and $\rho > 0$ we have $\|fg\|_\rho = \|f\|_\rho\|g\|_\rho$ (ie. $\|\cdot\|_\rho$ is multiplicative). Moreover, the width of fg under the ρ-norm equals the sum of the widths of f and g.*

Proof. Denote by m_f and M_f the minimum and maximum values of i for which $\max_i(|a_i|_p\rho^i)$ is achieved. The integers m_g, m_{fg}, M_g, and M_{fg} are defined similarly. If we write $g(x) = b_kx^k + \cdots + b_0$ then we have

$$f(x)g(x) = \sum_i \left(\sum_{j+l=i} a_jb_l \right) x^i \ .$$

In the sum $\sum_{j+l=i} a_jb_l$ each summand has absolute value at most $\|f\|_\rho\|g\|_\rho\rho^{-i}$ with equality if and only if $|a_j| = \|f\|_\rho\rho^{-j}$ and $|b_l| = \|f\|_\rho\rho^{-l}$. This cannot occur for $i < m_f + m_g$ and for $i = m_f + m_g$ it occurs only for $j = m_f$ and $l = m_g$. So we have $m_{fg} = m_f + m_g$ and the multiplicativity of $\|\cdot\|_\rho$ also follows. The equality $M_{fg} = M_f + M_g$ is deduced the same way. Therefore the width is indeed additive. □

Corollary 4.8. *If the Newton polygon of a polynomial $f(x) \in \mathbb{Q}[x]$ wrt. some prime p (ie. considered as a polynomial in $\mathbb{Q}_p[x]$) is just one line with the only lattice points at the two ends then $f(x)$ is irreducible.*

Newton polygons have many more modern applications, too, e.g. in the theory of p-adic differential equations. To read more have a look at [6].

4.4 Exercises

Exercise 4.3. Show that all the $p-1^{\text{st}}$ roots of unity are contained in $\mathbb{Q}_p$. *Hint:* Try and factor the polynomial $x^{p-1}-1$ using Hensel's Lemma.

Problem 4.4. Compute $|1-\varepsilon_m|_p$ for any positive integer m and prime p where ε_m is a primitive m^{th} root of unity. *Hint:* At first do it if $(m,p) = 1$ or m is a power of p. For this compute the Newton polygon of a suitable polynomial having $1-\varepsilon_m$ as a root. Finally, write $\varepsilon_m = \varepsilon_{p^h}\varepsilon_j$ where $(j,p) = 1$ and $1-\varepsilon_m = (1-\varepsilon_{p^h}) + \varepsilon_{p^h}(1-\varepsilon_j)$.

Exercise 4.5. Give more details of the proof of Theorem 4.6. Verify that the width of f under the ρ-norm is equal to the multplicity of the slope $-\log_p \rho$ in the Newton polygon of f. What is the Newton polygon of the linear polynomial $x - \alpha$?

Exercise 4.6. Give a proof of Corollary 4.8.

Problem 4.7. Show that if Newton polygon of the polynomial $f(x) \in \mathbb{Q}_p$ has two different slopes then f cannot be irreducible. *Hint:* Use the uniqueness of the extension of the absolute value to finite extensions of $\mathbb{Q}_p$ in order to show that the Galois group $\mathrm{Gal}(K/\mathbb{Q}_p)$ acts on any Galois-extension K via isometries. If all the roots of f are Galois-conjugates then they have the same absolute value.

5 Applications, research directions, and further reading

If you do not intend to become a number theorist, you may ask why learn the p-adics as they are so different from the "real world". This is, in fact, not quite true. However, let us discuss the most important applications of p-adic methods in Number Theory first, together with a view what the main research directions are. The list below does not intend to be exhaustive—it certainly reflects the interest and the (limited) knowledge of the author.

5.1 Hasse's local-global principle

The most important application of the p-adics numbers are through the so-called *local-global* (or Hasse) principle. Roughly speaking the idea is that—as you may have noticed—it is easier to decide whether or not polynomial equations have roots in the fields $\mathbb{R}$ and $\mathbb{Q}_p$ for varying p than deciding it over $\mathbb{Q}$. Clearly, if there are no roots in $\mathbb{Q}_p$ for some p or in $\mathbb{R}$ then there can be no roots in $\mathbb{Q}$ either. The question is up to what extent is the converse true. Unfortunately, this is not always the case. For example, the equation $3x^3 + 4y^3 + 5z^3 = 0$ has a solution in $\mathbb{R}$ and $\mathbb{Q}_p$ for *all* primes p, but not in $\mathbb{Q}$. However, for homogeneous polynomials of degree 2 the local global principle holds. This is the theorem of Hasse and Minkowski (for a detailed and elementary proof see the book [12] by Serre).

There exist certain methods how to "measure" the failure of the Hasse principle. For elliptic curves this is done by the Tate-Shafarevich group which in this case fully accounts for the failure of the principle. The Tate-Shafarevich conjecture asserts that this group is always finite over for elliptic curves over finite extensions of $\mathbb{Q}$. This is one of the most important open problems in arithmetic geometry. The conjecture of Birch and Swinnerton-Dyer (a millenium prize problem) would imply this and the conjecture has been tested for many numerical examples. There is also some very important theoretical evidence in favour of this conjecture—for instance, the known cases of the BSD conjecture. To read more about elliptic curves Silverman's book [13] is an excellent introduction.

5.2 Langlands programme

L-functions play a very important role in Number Theory. These are certain generalizations of the Riemann ζ-function $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ ($\mathrm{Re}(s) > 1$). For example, the proof of Dirichlet's Theorem on primes in arithmetic progression is proven using L-functions. The

Riemann ζ-function itself (especially the set of its roots) is very much related to the distribution of primes in $\mathbb{Z}$. Further, according to the conjecture of Birch and Swinnerton-Dyer, the L-function of an elliptic curve should vanish to the order of the rank of the curve.

L-functions play the role of the connection between Galois representations and automorphic forms. One can attach L-functions to both types of objects. However, while on the Galois-side it is very natural to write the L-function as Euler product over the primes (for example, we have $\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$), this is not so obvious on the automorphic side. On the other hand, the functional equation and the analytic continuation of L-functions to the whole complex plane—note that a priori $\zeta(s)$ is only defined if $\mathrm{Re}(s) > 1$—is quite standard (well, this is Tate's thesis, in fact), but not at all on the Galois side. In fact, the only method known to show the analytic continuation is via *modularity*, ie. showing that the L-function in question is the L-function of some automorphic form. The Langlands program is the philosophy that one should try to match Galois-representations to automorphic forms having the same L-function. There are not too many known results in this direction. The case when the Galois representation is 1-dimensional, is completely understood via class field theory. The case of Galois-representations coming from elliptic curves was settled by Wiles (and Taylor) when proving Fermat's Last Theorem. More recently, there are other modularity results using Serre's conjectures and the p-adic Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$ by Colmez. So one can—rather surprisingly—use p-adic methods to prove the analytic continuation of certain complex functions!

If you are interested in this, you should start out by reading class field theory first for which I recommend the books [11] and [9].

5.3 Algebraic geometry

It should be obvious by now that the p-adic numbers are useful when trying to find (or proving that there are no) rational points on algebraic varieties. However, there are several other applications of the p-adics in algebraic geometry. For instance, it is sometimes useful to complete the local ring of a variety at a point, as complete discrete valuation rings have better properties than those that are not complete. Another very important application is in étale cohomology. The étale cohomology is a cohomology theory in algebraic geometry that has better properties if the coefficients are taken from a finite ring. However, for certain applications, it is necessary to have coefficients with characteristic zero. Therefore one takes the projective limit with coefficients in $\mathbb{Z}/p^n\mathbb{Z}$ to obtain coefficients in $\mathbb{Z}_p$. If you want to learn more on algebraic geometry the best reference is [5].

5.4 Group theory

Profinite groups are inverse limits of finite groups. They are naturally compact topological spaces in the inverse limit topology of the finite sets equipped with the discrete topology. For example infinite Galois groups are profinite, but profinite groups also show up as automorphism groups of certain (infinite) rooted trees. The additive group $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ is a profinite group, moreover, it is a *pro-p* group, ie. an inverse limit of finite p-groups. Moreover, it is the unique (upto isomorphism) infinite pro-p group topologically generated by a single element. A pro-p group G is said to have finite rank if all its closed subgroups can be topologically generated by a bounded number of elements. All pro-p groups of finite rank are closed subgroups of $\mathrm{GL}_n(\mathbb{Z}_p)$ for n large enough. If you wish to learn more on pro-p groups, the bible is the book [3].

Another application of the p-adic numbers is in modular representation theory of finite groups. This is because the natural objects to which one can lift up representations in characteristic p to characteristic 0 are complete local integral domains, such as $\mathbb{Z}_p$. For more information on modular representation theory see the book [10].

5.5 Dynamical systems

The main result of the groundbreaking paper [1] is the following. We say that a complex number $a \in \mathbb{C}$ is preperiodic for the polynomial $f(z) \in \mathbb{C}[z]$ if the set

$$\{a, f(a), f(f(a)), \ldots, f(\ldots(f(a))\ldots), \ldots\}$$

is finite. Fix a positive integer $d > 1$ and complex numbers $a, b \in \mathbb{C}$. The set of parameters $c \in \mathbb{C}$ such that both a and b are preperiodic for $f(z) = z^d + c$ is infinite if and only if $a^d = b^d$. Note that the statement is completely elementary and only concerns complex polynomials. However, the proof requires non-trivial methods in non-archimedean analytic geometry (in the sense of Berkovich [2]).

5.6 Algebraic topology

The (still open) Hilbert-Smith conjecture states that if a locally compact group G acts effectively (ie. faithfully) on a topological manifold M then G is a Lie-group. Because of known structural results on locally compact groups the conjecture can be reduced to the case $G \cong \mathbb{Z}_p$ the additive group of the p-adic integers. In other words it would be enough to show that $\mathbb{Z}_p$ cannot act faithfully on a topological manifold M.

The ring $\mathbb{Z}_p$ of p-adic integers is one of the easiest examples of a complete discrete valuation ring (the other one being $k[[t]]$, k field). These are very important in the theory of formal groups which not only show up in algebraic geometry and number theory, but also in algebraic topology. The book [8] is a good introduction to the theory of formal groups.

5.7 Physics

The geometry of space-time at small distances seems to be non-archimedean—at least according to some physisists. For instance, the p-adic numbers show up in quantum mechanics, quantum field theory, and string theory, too. I am not an expert on this, so if you are interested, you should consult the book [14] for a start.

References

[1] M. Baker and L. DeMarco. Preperiodic points and unlikely intersections. *Duke Mathematical Journal*, **159**(1):1–29, 2011.

[2] V. Berkovich. *Spectral theory and analytic geometry over non-Archimedean fields*, volume **33** of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, RI, 1990.

[3] J. D. Dixon, M. P. F. du Sautoy, A. Mann, and D. Segal. *Analytic pro-p groups.* Cambridge University Press, Cambridge, 1999.

[4] F. Q. Gouvêa. *p-adic Numbers, An Introduction.* Springer, Heidelberg, 1997.

[5] R. Hartshorne. *Algebraic Geometry*, volume **52** of *Graduate Texts in Mathematics.* Springer, 1977.

[6] K. S. Kedlaya. *p-adic Differential Equations*, volume **125** of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, 2010.

[7] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-functions*, volume **58** of *Graduate Texts in Mathematics.* Springer, 1984.

[8] M. Lazard. *Commutative formal groups*, volume **443** of *Lecture Notes in Mathematics.* Springer, Berlin, New York, 1975.

[9] J. Neukirch. *Class Field Theory*, volume **280** of *Grundlehren der mathematischen Wissenschaften.* Springer, Heidelberg, 1986.

[10] P. Schneider. *Modular Representation Theory of Finite Groups.* Springer, London, 2013.

[11] J.-P. Serre. *Local Fields*, volume **67** of *Graduate Texts in Mathematics.* Springer, New York, 1980.

[12] J.-P. Serre. *A course in arithmetic.* Springer, New York, 1993.

[13] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume **106** of *Graduate Texts in Mathematics.* Springer, 1986.

[14] V. S. Vladimirov. *p-adic Analysis and Mathematical Physics.* World Scientific, Singapore, 1994.