1. p-adic numbers

Definition 1.1. Let K be a field. A function $|| \, || : K \to \mathbf{R}_{\geq 0}$ is called an absolute value if the following properties hold:
1) $||x|| = 0 \Leftrightarrow x = 0$.
2) $|| \, || : K^* \to \mathbf{R}^*_{>0}$ is a group homomorphism.
3) $\forall \, x, y \; ||x + y|| \leq ||x|| + ||y||$ ("the triangle inequality").

Remark. The function $||x|| = \begin{cases} 0, x=0 \\ 1, x\neq 0 \end{cases}$ is called the trivial absolute value. This one will often be excluded from consideration.

Definition 1.2. An absolute value $|| \, || : K \to \mathbf{R}_{\geq 0}$ is called nonarchimedean iff $\forall \, x, y$ $||x + y|| \leq \max(||x||, ||y||)$ ("the strict triangle inequality").

Short visit to highschool (rings).

All the rings in this section will be commutative with the identity.

A ring $\mathcal{O}$ is called local if there exists just one maximal ideal $\mathfrak{m} \subset \mathcal{O}$. Any element outside the maximal ideal in the local ring is invertible. Conversely, if in some ring $\mathcal{O}$ there exists an ideal $\mathfrak{m}$ such that all the elements outside $\mathfrak{m}$ are invertible then $\mathcal{O}$ is local and $\mathfrak{m}$ is the maximal ideal.

Suppose $\mathfrak{p} \in \mathcal{O}$ is a prime ideal. The localisation $\mathcal{O}_\mathfrak{p}$ is the set of equivalence classes of fractions $\frac{x}{y}$, $y \notin \mathfrak{p}$, $\frac{x}{y} = \frac{x_1}{y_1} \Leftrightarrow \exists u \notin \mathfrak{p} \mid u(xy_1 - x_1 y) = 0$. Since the ideal $\mathfrak{p}$ is prime this set is a ring. Let the ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p} \subset \mathcal{O}_\mathfrak{p}$ consist of all fractions with numerators in $\mathfrak{p}$. Any element outside $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is invertible hence $\mathcal{O}_\mathfrak{p}$ is a local ring and $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is its maximal ideal.

Suppose $\mathcal{O}$ contains no zero divisors (i.e. is an integral domain). Then the ideal (0) is prime, hence $\mathcal{O}_{(0)}$ exists. The ring $\mathcal{O}_{(0)}$ is called the field of fractions of $\mathcal{O}$.

Remark. $\mathbf{Z}_{(0)} = \mathbf{Q}$.

The inclusion of prime ideals $\mathfrak{p} \supset \mathfrak{p}_1$ leads to the inclusion of local rings $\mathcal{O}_{\mathfrak{p}_1} \supset \mathcal{O}_\mathfrak{p}$. Hence the field of fractions of an integral domain $\mathcal{O}$ contains all other localisations $\mathcal{O}_\mathfrak{p}$.

Example. Let $p \in \mathbf{Z}$ be a prime. The ring $\mathbf{Z}_{(p)}$ is a subring of $\mathbf{Q}$ consisting of all rational numbers such that p does not divide the denominator.

Let $\mathcal{O} \subset A$ be an inclusion of rings, $x \in A$. x is called integral over $\mathcal{O}$ iff x is a root of some monic polynomial with coefficients in $\mathcal{O}$: $x^n + \sum\limits_{i=0}^{n-1} a_i x^i = 0$. Certainly any element of $\mathcal{O}$ is integral over $\mathcal{O}$. If A contains no elements outside $\mathcal{O}$ which are integral over $\mathcal{O}$ then $\mathcal{O}$ is called integrally closed in A. An integral domain $\mathcal{O}$ is shortly called integrally closed if it is integrally closed in its own field of fractions.

Theorem-definition. Let $\mathcal{O}$ be a principal ideal domain. Then $\mathcal{O}$ is factorial (i.e. any nonzero element could be in a unique way up to multiplication by invertible elements decomposed as a product of irreducible factors). If $p \in \mathcal{O}$ is irreducible and $0 \neq x \in \mathcal{O}$ then $\mathrm{v}_p(x) \overset{\mathrm{def}}{=} \max(n \in \mathbf{Z}_{\geq 0} \, \text{such that} \, p^n \,|\, x)$. If K is the field of fractions of $\mathcal{O}$ then $\mathrm{v}_p(x)$ may be extended to K^* by the formula $\mathrm{v}_p\left(\frac{x}{y}\right) = \mathrm{v}_p(x) - \mathrm{v}_p(y)$ with values in $\mathbf{Z}$.

Proof. See any book on algebra ■

End of the visit.

Definition-Theorem 1.3. Let K be a field, $|| \, ||$ a nonarchimedean absolute value on K. Then: 1) $\mathcal{O} = \{x \in K \, , \, ||x|| \leq 1\}$ is a ring (called valuation ring), $\mathfrak{p} = \{x \in K \, , \, ||x|| < 1\}$ is a maximal ideal in $\mathcal{O}$. $\mathfrak{p} \neq (0) \Leftrightarrow || \, ||$ is nontrivial. $\forall x \in K^*$ either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.
2) $\mathcal{O}$ is a local ring, K is its field of fractions. $\mathcal{O}$ is integrally closed.
3) Let $U = \mathcal{O}^* = \mathcal{O} \setminus \mathfrak{p}$. U is a subgroup of K^*, $|| \, || : K^*/U \to \mathbf{R}^*_{>0}$ is an inclusion. The absolute value $|| \, ||$ is called discrete iff $||K^*||$ is a discrete subgroup of $\mathbf{R}^*_{>0}$ (hence trivial or infinite cyclic). $|| \, ||$ is discrete $\Leftrightarrow \mathfrak{p} \subset \mathcal{O}$ is a principal ideal.

Proof. 1) and 3) are clear ■
2) $\mathcal{O}^* = \mathcal{O} \setminus \mathfrak{p}$ coincides with the set of all invertible elements of $\mathcal{O}$, hence $\mathfrak{p}$ is a unique maximal ideal in $\mathcal{O}$. If $x \in K$ and $x^n = \sum\limits_{i=0}^{n-1} a_i x^i$ for some $a_i \in \mathcal{O}$ then $||x|| \leq 1$ (otherwise the absolute value of the left side should have been strictly greater than the absolute value of the right side, the latter being estimated with the strict triangle inequality). Hence $\mathcal{O}$ is integrally closed ■

Theorem 1.4. Let K be a field, $|| \, ||$ a nonarchimedean absolute value on K, $x \in K$ and $x = \sum\limits_{i=0}^{n} x_i$. If all $||x_i||$ are different then $||x|| = \max\limits_i ||x_i||$.

Proof. Clear ■

Theorem 1.5. Let K be a field, $|| \; ||$ an absolute value on K. Let $I \subset K$ be the image of the standard ring homomorphism $i : \mathbf{Z} \to K$, $1 \overset{i}{\mapsto} 1$. (I is isomorphic to either $\mathbf{Z}$ or some $\mathbf{F}_p$, depending on char(K), cf. Remark 2 after the Definition 1.4). Then:
$|| \; ||$ is nonarchimedean $\Leftrightarrow \forall\, x \in I \; ||x|| \leq 1$.

Proof. $\Rightarrow$ clear. $\Leftarrow$ To prove that $||x+y|| \leq \max(||x||, ||y||)$ it suffices to prove that $\forall z \in K \; ||z|| \leq 1 \Rightarrow ||1+z|| \leq 1$. Suppose $||z|| \leq 1$. Then for any natural n $||1+z||^n = ||(1+z)^n|| = ||\sum\limits_{i=0}^{n} \binom{n}{i} z^i|| \leq n+1$ ($||\binom{n}{i}|| \leq 1$ by assumption, then use the standard triangle inequality). Hence $||1+z|| \leq (n+1)^{\frac{1}{n}}$. Since this holds for any n, $||1+z|| \leq 1$ ■

Remark. If char$(K) \neq 0$ then any absolute value on K is nonarchimedean (hometask).

Theorem 1.6. Suppose k is a field, $K = k(T)$ the field of rational fractions in one independent variable over k. Suppose $|| \; || : K \to \mathbf{R}_{\geq 0}$ is an absolute value such that its restriction on k is trivial while it is nontrivial itself. Then $|| \; ||$ is nonarchimedean & discrete and either
$||x|| = s^{-\mathrm{v}_P(x)}$ (where $s \in \mathbf{R}, s > 1, P \in k[T]$ irreducible, $\deg P \geq 1$), or
$||x|| = s^{\deg(\text{numerator}(x)) - \deg(\text{denominator}(x))}$ (where $s \in \mathbf{R}, s > 1$).

Remark. The two types of absolute values above are in fact the same. Namely, it is easy to construct an automorphism of the field K such that the composition of the absolute value of the second type with it becomes the absolute value of the first type. To check this is a hometask.

Proof of the Theorem. By the previous theorem $|| \; ||$ is nonarchimedean. First suppose that $||T|| \leq 1$. Then by strict triangle inequality $k[T] \subset \mathcal{O}$, $\mathcal{O}$ being the valuation ring defined in Definition-Theorem 1.3. If $\mathfrak{p} \subset \mathcal{O}$ is the maximal ideal then $\mathfrak{p} \cap k[T]$ which by definition consists of all $x \in k[T]$ such that $||x|| < 1$ is a prime ideal in $k[T]$. It is nonzero (otherwise $\forall x \in k[T] \; ||x|| = 1$, so $|| \; ||$ is trivial) hence generated by some irreducible polynomial $P \in k[T]$ as $k[T]$ is a principal ideal ring. If $x \in k[T]$ then $x = P^{\mathrm{v}_P(x)} y$ where $y \notin \mathfrak{p} \cap k[T]$, so $||y|| = 1$. This means that $|| \; ||$ is of the first type.
Now suppose that $||T|| > 1$. Then by Theorem 1.4. for any polynomial $||\sum\limits_{i=o}^{n} a_i T^i|| = ||T^n|| = ||T||^n$, hence $|| \; ||$ is of the second type. Clearly $|| \; ||$ is discrete in both cases ■

Theorem 1.7. (Ostrowski) Suppose $||\ ||$ is a nontrivial absolute value on $\mathbf{Q}$. Then either
$||x|| = s^{-\mathrm{v}_p(x)}$ (where $s \in \mathbf{R}, s > 1, p$ prime) or
$||x|| = |x|^\alpha$ (where $a \in \mathbf{R}, 0 < \alpha \leq 1, |\ |$ the standard absolute value).

Remark. The two types of absolute values above are totally different. In particular, the absolute value of the second type is archimedean.

Proof of the Theorem. First suppose that $\forall a \in \mathbf{Z}\ ||a|| \leq 1$. Then by Theorem 1.5. $||\ ||$ is nonarchimedean. Now one should proceed as in the first case of Theorem 1.6 using $\mathbf{Z}$ instead of $k[T]$. This leads to the absolute value of the first type.
Now suppose $\exists a \in \mathbf{Z}$ such that $||a|| > 1$. One may suppose $a > 1$. Let b be an arbitrary integer such that $b > 1$. Let us prove that $||b|| > 1$. Suppose the opposite is true. Write down a in b-ary system: $a = \sum\limits_{i=0}^{m} a_i b^i,\ 0 \leq a_i < b$. Then $m \leq \frac{\log a}{\log b}$. We have supposed $||b|| \leq 1$, so $||a|| \leq (m+1) \max\limits_i ||a_i|| \leq (m+1) \max\limits_i a_i < (m+1)b$ (as $||a_i|| \leq a_i$ by the triangle inequality). One may conclude that $||a|| < \left(\frac{\log a}{\log b} + 1\right) b$. Now consider a^n instead of a for some positive integer n, the inequality changing to $||a|| < \left(\left(\frac{n \log a}{\log b} + 1\right) b\right)^{\frac{1}{n}}$. While n tends to infinity the right part of this inequality tends to 1 hence $||a|| \leq 1$ which contradicts the assumption. So $||b|| > 1$ for all integers b exceeding 1.
Now let us use again the expansion $a = \sum\limits_{i=0}^{m} a_i b^i,\ 0 \leq a_i < b$. Since $\forall i\ \ a_i < b$ and $||b|| > 1$ the triangle ineqality leads to $||a|| < (m+1)\, b\, ||b||^{\frac{\log a}{\log b}}$. Changing a to a^n, n arbitrary large, one gets $||a|| < ||b||^{\frac{\log a}{\log b}} ((m+1)b)^{\frac{1}{n}}$, hence $||a|| \leq ||b||^{\frac{\log a}{\log b}}$.
Exchanging a with b one may get the ineqality $||b|| \leq ||a||^{\frac{\log b}{\log a}}$ in the same way, so $||a||^{\frac{1}{\log a}}$ does not depend on a which means that for any nonzero rational x $||x||$ is given by the formula $||x|| = |x|^\alpha$, $|\ |$ being the standard absolute value, α some real number.
It remains to check when this formula does in fact define an absolute value. Certainly it suffices to check whether the triangle inequality does hold. If $\alpha < 0$ it never holds (try $y = -x + \epsilon,\ \epsilon \to 0$). If $\alpha > 0$ then the statement $\forall x, y\ |x+y|^\alpha \leq |x|^\alpha + |y|^\alpha$ is equivalent to the statement $\forall z$ such that $0 < z \leq 1\ \ (1+z)^\alpha \leq 1 + z^\alpha$. The derivative of the function $(1+z)^\alpha - 1 - z^\alpha$ is nonzero inside the segment $0 < z < 1$ hence the triangle inequality is equivalent to the condition $2^\alpha - 2 \leq 0 \Leftrightarrow \alpha \leq 1$ ■

Remark. If K is a field, $|| \, ||$ an absolute value on K, then the distance function $d(x,y) = ||x-y||$ defines a structure of metric space on K.

Very short visit to highschool (metric spaces).

A sequence $\{x_i\}$ of elements of the metric space X is called fundamental or Cauchy sequence if $\lim\limits_{i,j \to \infty} d(x_i, x_j) = 0$.

A metric space $\widehat{X}$ is called the completion of the metric space X if X is a dense subspace of $\widehat{X}$ and $\widehat{X}$ is complete (by definition this means that any Cauchy sequence of elements of $\widehat{X}$ converges). All the completions of X are isomorphic (as metric spaces) to each other. In fact, it is easy to prove that they are isomorphic to one given by the following standard construction.
Consider the set of all Cauchy sequences with elements in X. Define the equivalence relation on this set as follows: $\{x_i\} \sim \{y_j\}$ if $\lim\limits_{k \to \infty} d(x_k, y_k) = 0$. Then $\widehat{X}$ is a quotient set by this equivalence relation.

If X is a metric space, the base of its standard topology is given by the open balls $\{x \in X \mid d(x, x_0) < r\}$.

Any continuous map $f : X \to Y$ where Y is a complete metric space could be in a unique way extended to $\widehat{X}$ with the formula $f(\{x_i\}) = \lim\limits_{i \to \infty} f(x_i)$.

End of the visit.

Theorem 1.8. Let K be a field, $|| \, ||$ an absolute value on K, $d(x,y) = ||x-y||$ corresponding metric. Then
1) $" + ", " \cdot " : K \times K \to K$, $"x \mapsto -x" : K \to K$, $"x \mapsto x^{-1}" : K \diagdown 0 \to K$, $|| \, || : K \to \mathbf{R}$ are all continuous in the topology defined by d (topology of the product being used on $K \times K$, usual topology on $\mathbf{R}$).
2) Let $\widehat{K}$ be the completion of the metric space K. Then the set $\widehat{K}$ with operations above (extended by continuity) is a field.
3) The absolute value $|| \, ||$ extended to $\widehat{K}$ by continuity is the absolute value on $\widehat{K}$. It is nonarchimedean iff it is nonarchimedean on K. If this is the case then the sets of values of $|| \, ||$ on K and on $\widehat{K}$ coincide.

Proof. 1) Hometask $\blacksquare$
2) Taking of the limit commutes with substraction and with multiplication hence one may define the algebraic operations on Cauchy sequences componentwise. The only problem is to define the inverse element on $\widehat{K}$ (as the domain of the definition of this operation on K does not contain zero). So one needs to prove that $\forall x \in \widehat{K}, x \neq 0$ there exists a sequence $\{x_i \in K, x_i \neq 0\}$ such that $x = \lim\limits_{i\to\infty} x_i$. Consider an arbitrary sequence $\{x_i\} \in K$ tending to x. This cannot contain the infinite number of zero's (otherwise it could tend only to zero) so some its tail consists of nonzero elements and still tends to x.
3) If $x = \{x_i\}$ and $y = \{y_i\}$ are the elements of $\widehat{K}$ then $||xy|| = ||\{x_iy_i\}|| = \lim\limits_{i\to\infty} ||x_iy_i|| = \lim\limits_{i\to\infty} ||x_i||||y_i|| = \lim\limits_{i\to\infty} ||x_i|| \lim\limits_{i\to\infty} ||y_i|| = ||x||||y||$. If $x = \{x_i\}$ and $||x|| = 0$ then $\{x_i\}$ represents $0 \in \widehat{K}$ by definition. For the same token $||x + y|| \leq ||x|| + ||y||$ if this holds componentwise. The last statement is also correct if $||x|| + ||y||$ is changed to $\max(||x||, ||y||)$. Clearly $\forall x \in \widehat{K} \exists x_0 \in K$ such that $||x - x_0||$ is arbitrarily small. If $|| \; ||$ is nonarchimedean then by Theorem 1.4 $||x_0|| = \max(||x||, ||x_0 - x||) = ||x||$ hence the sets of values of $|| \; ||$ on K and on $\widehat{K}$ coincide $\blacksquare$

Remark. If $|| \; ||$ is archimedean then Theorem 1.4 is not true so the sets of values above may be different.

Definition-Theorem 1.9. Let K be a field, $|| \; ||_1$ and $|| \; ||_2$ two absolute values on K. They are called equivalent (notation $|| ||_1 \sim || ||_2$) if $|| ||_2 = || ||_1^t, t > 0$. Then $|| ||_1 \sim || ||_2 \Leftrightarrow$ both define the same topology on K.

Proof. $\Rightarrow$ clear. $\Leftarrow$ The condition $||x|| < 1$ is of topological nature ($||x|| < 1 \Leftrightarrow \lim\limits_{n\to\infty} x^n = 0$) hence $||x||_1 < 1 \Leftrightarrow ||x||_2 < 1$. Let $x, y \in K$ be any two nonzero elements. The set $\{m, n \in \mathbf{Z} \,|\, ||x^m y^n||_i < 1\}$ does not depend on i. The condition $||x^m y^n||_i < 1$ is equivalent to the condition $m \log ||x||_i + n \log ||y||_i < 0$ hence the two vectors $(\log ||x||_1, \log ||y||_1)$ and $(\log ||x||_2, \log ||y||_2)$ are proportional with positive coefficient, taking the exponent ends the proof $\blacksquare$

Definition 1.10. 1)The completion of the field $\mathbf{Q}$ with respect to the absolute value $||x||_p = s^{-\mathrm{v}_p(x)}$ is called the field of p-adic numbers (notation $\mathbf{Q}_p$).
2) The ring $\mathbf{Z}_p \subset \mathbf{Q}_p$ ($x \in \mathbf{Z}_p \overset{\text{def}}{\Leftrightarrow} ||x||_p \leq 1$) is called the ring of p-adic integers.

Remark 1. The completion of the field $\mathbf{Q}$ with respect to the absolute value $||x||_\infty = |x|^\alpha$ $(0 < \alpha \leq 1)$ is the field of reals $\mathbf{R}$.

Remark 2. Equivalent absolute values define the same sets of Cauchy sequences, corresponding equivalence relations being also the same. Hence the concept of $\mathbf{R}$ (resp. $\mathbf{Q}_p$) does not depend on the choice of α (resp. s).
Example. Consider the absolute value $||x||_T = s^{-\mathrm{v}_T(x)}$ on the field $K = k(T)$. Then the completion of K with respect to this absolute value is isomorphic to the field $k\{T\}$ of formal Laurent power series with coefficients $a_i \in k$ of the form $\sum\limits_{i=m}^{\infty} a_i T^i$ (i.e series with no more then finite number of terms of negative degree). For the proof see hometask.

Theorem 1.11. Let K be a field, $||\ ||$ a nonarchimedean absolute value on K. Suppose $||\ ||$ defines a structure of a complete metric space on K. Consider an infinite series $\sum\limits_{i=1}^{\infty} x_i$, $x_i \in K$. $\sum\limits_{i=1}^{\infty} x_i$ converges $\Leftrightarrow \lim\limits_{i\to\infty} ||x_i|| = 0$.

Proof. $\Rightarrow$ clear. $\Leftarrow$ One needs to check that $y_n \overset{\text{def}}{=} \{\sum\limits_{i=1}^{n} x_i\}$ is a Cauchy sequence. In fact, $||y_m - y_n|| = ||\sum\limits_{i=n+1}^{m} x_i|| \leq \max\limits_{i=n+1}^{m} ||x_i||$ which by assumption tends to zero while m and n both tend to infinity ■

Remark . Of course the last theorem is not true if $||\ ||$ is archimedean. In fact, in that case only $||\sum\limits_{i=n+1}^{m} x_i|| \leq \sum\limits_{i=n+1}^{n} ||x_i||$ is guaranteed. The sum to the right may be large besides each particular $||x_i||$ is small (depending on the number of the terms i.e. on $m-n$).

We now switch to another construction of p-adic numbers which we later prove to be equivalent to one developed above.

Alt-Definition 1.12. For $i > 1$ let $\phi_i : \mathbf{Z}/(p^i) \to \mathbf{Z}/(p^{i-1})$ be the standard residue map. Define the set $\mathbf{Z}_p$ by the formula $\mathbf{Z}_p \overset{\text{def}}{=} \lim\limits_{\leftarrow}\{\mathbf{Z}/(p^i), \phi_i\}$. By definition this means that the element $x \in \mathbf{Z}_p$ is a sequence $\{{}_ix \in \mathbf{Z}/(p^i), 1 \leq i < \infty\}$ such that $\forall i > 1$ $\phi_i({}_ix) = {}_{i-1}x$. Such construction is called "projective limit".

Theorem 1.13. 1) $\mathbf{Z}_p$ carries the natural structure of the commutative ring with 1.

2) The standard ring homomorphism $\mathbf{Z} \to \mathbf{Z}_p, 1 \mapsto 1$ sends $n \in \mathbf{Z}$ to $\{_i x \equiv n \pmod{p^i}\}$. It is injective.
3) Let ϵ_i be the projection of $\mathbf{Z}_p$ on its i-th component. Then ϵ_i is surjective and $\ker(\epsilon_i) = p^i \mathbf{Z}_p$.
4) $u \in \mathbf{Z}_p$ is invertible $\Leftrightarrow {}_1u \neq 0 \Leftrightarrow p \nmid u$ in $\mathbf{Z}_p$.
5) $\forall$ nonzero $x \in \mathbf{Z}_p$ $\exists! u \in \mathbf{Z}_p$ invertible and $n \in \mathbf{Z}$ nonnegative such that $x = p^n u$.

Proof. 1) Ring operations may be defined componentwise. Since all of them commute with taking the residue, $\mathbf{Z}_p$ becomes a ring, $\{1 \mod p^i\}$ being the identity ■
2) Clear ■
3) Suppose $a \in \mathbf{Z}/(p^i)$. Choose $\widetilde{a} \in \mathbf{Z} \subset \mathbf{Z}_p$ such that $\widetilde{a} \mod p^i$ equals a. Then $\epsilon_i(\widetilde{a}) = a$. Clearly $\epsilon_i(p^i \mathbf{Z}_p) = 0$. Suppose $x \in \mathbf{Z}_p$, $\epsilon_i(x) = 0$. Then for $j > i$ the component ${}_jx \mod p^j$ of x is divisible by p^i and the quotient is uniquely defined mod p^{j-i}. Set $y = \{_n y\} : {}_n y \overset{\text{def}}{=} \frac{{}_{n+i}x}{p^i} \mod p^n$, then $p^i y = x$ ■
4) By the previous point ${}_1u \neq 0 \Leftrightarrow p \nmid u$ in $\mathbf{Z}_p$. Clearly ${}_1u \neq 0 \Leftrightarrow \forall i \ {}_iu$ is invertible in $\mathbf{Z}/(p^i)$(hometask)$\Leftrightarrow$ u is invertible in $\mathbf{Z}_p$ ■
5) By 3) $p^i | x$ in $\mathbf{Z}_p \Leftrightarrow \forall j \leq i \ {}_jx = 0$. Now one may use 4) ■

Alt-Definition 1.14. Suppose $x \in \mathbf{Z}_p$. $\mathrm{v}_p(x) \overset{\text{def}}{=}$ the number n from 2.13 5).

Alt-Definition-Theorem 1.15. 1) $\mathbf{Z}_p$ is an integral domain (i.e. has no zero divisors).
2) Let $\mathbf{Q}_p$ be the field of fractions of $\mathbf{Z}_p$. Extend v_p to $\mathbf{Q}_p \setminus 0$ by the formula $\mathrm{v}_p(z = \frac{x}{y}) = \mathrm{v}_p(x) - \mathrm{v}_p(y)$. $\mathrm{v}_p(z)$ does not depend on the choice of $x, y \in \mathbf{Z}_p$. $\mathrm{v}_p : \mathbf{Q}_p^* \to \mathbf{Z}$ is a group homomorphism.
3) Let $|| \ z \neq 0||_p \overset{\text{def}}{=} s^{-\mathrm{v}_p(z)}$ for some $s \in \mathbf{R}$, $s > 1$; $|| \, 0||_p = 0$. Then $|| \ ||_p$ is a nonarchimedean absolute value on $\mathbf{Q}_p$.

Proof. 1) Clearly p is not a zero divisor in $\mathbf{Z}_p$ hence $\mathbf{Z}_p$ has no zero divisors by Theorem 1.13 5) ■
2) Easy consequence of the decomposition in 2.13. 5) ■
3) It suffices to check that $\forall z_1, z_2 \in \mathbf{Q}_p$ $\mathrm{v}_p(z_1 + z_2) \geq \min(\mathrm{v}_p(z_1), \mathrm{v}_p(z_2))$. Here we formally suppose that $\mathrm{v}_p(0) = +\infty$. This is a hometask ■

Theorem 1.16. The field $\mathbf{Q}_p$ as defined above enjoys all the properties of $\mathbf{Q}_p$ as defined in Definition 1.10. "This" $\mathbf{Z}_p$ coincides with "that" $\mathbf{Z}_p$. The absolute values $|| \ ||_p$

here and there are the same for the same s.

Proof. In the proof we refer to $\mathbf{Z}_p, \mathbf{Q}_p$ and v_p as defined in 1.14 -1.15.
Step 1. $\mathbf{Z}_p$ is a complete metric space. We will costruct a limit for any Cauchy sequence directly. Let x_j be a Cauchy sequence of p-adic integers, each x_j represented by the sequence of components $\{{}_ix_j \in \mathbf{Z}/(p^i)\}$. Consider the rectangular table:

$$\begin{array}{lllll}
\cdots & {}_4x_1 & {}_3x_1 & {}_2x_1 & {}_1x_1 \\
\cdots & {}_4x_2 & {}_3x_2 & {}_2x_2 & {}_1x_2 \\
\cdots & {}_4x_3 & {}_3x_3 & {}_2x_3 & {}_1x_3 \\
\cdots & & & &
\end{array}$$

So there is the i-th component (which is an element of $\mathbf{Z}/(p^i)$) of the j-th p-adic number on the intersection of the i-th (to the left) column with the j-th row.
Since x_j is a Cauchy sequence $\forall i \;\; \exists n$ such that if $j_1, j_2 > n$ then ${}_ix_{j_1} = {}_ix_{j_2}$. The last equality holds because $||x_{j_1} - x_{j_2}||_p$ is small. Hence any column of the table above stabilizes, i.e $\forall i \;\; {}_ix_j$ is constant starting from some j. It is easy to check that the row consisting of these constants is a p-adic number and that the Cauchy sequence we have started from converges to this number (hometask) ■
Step 2. $\mathbf{Z}$ is a dense subset of $\mathbf{Z}_p$. Indeed, suppose $x = \{{}_ix\} \in \mathbf{Z}_p$. For each i choose $\widetilde{{}_ix} \in \mathbf{Z}$ such that $\widetilde{{}_ix} \equiv {}_ix \mod p^i$. Then the sequence $x_1 = \{\cdots \widetilde{{}_1x} \mod p^2, \widetilde{{}_1x} \mod p\}$, $x_2 = \{\cdots \widetilde{{}_2x} \mod p^2, \widetilde{{}_2x} \mod p\}$, $x_3 = \{\cdots \widetilde{{}_3x} \mod p^2, \widetilde{{}_3x} \mod p\}$ $\ldots$ of images of integers $\widetilde{{}_ix}$ in the ring $\mathbf{Z}_p$ under the standard inclusion $\mathbf{Z} \to \mathbf{Z}_p$ converges to the p-adic number x ■
Step 3. $\mathbf{Q}$ is dense in $\mathbf{Q}_p$. Hometask. ■
Step 4. As a set, $\mathbf{Q}_p = \{0\} \cup \bigcup\limits_{i=-\infty}^{\infty} p^iU$, where $U = \mathbf{Z}_p^* \overset{\text{(as a set)}}{=} \mathbf{Z}_p \diagdown p\mathbf{Z}_p$. This is clear from 1.13.5) ■
Step 5. $\mathbf{Q}_p$ is a complete metric space. Indeed, consider a Cauchy sequence x_j of elements of $\mathbf{Q}_p$. Then either $x_j \to 0$ or there exist $i, j_0 \in \mathbf{Z}$ such that $\forall j \geq j_0 \; x_j \in p^iU$. This is an easy corollary of the strict triangle inequality (apply Theorem 1.4 to $x_{j_1} - x_{j_2}$). Since $U = \mathbf{Z}_p \diagdown p\mathbf{Z}_p$ U is closed in $\mathbf{Z}_p$ hence complete, so any p^iU is complete whence the statement ■
Step 6. The restriction of v_p to $\mathbf{Q}$ coincides with v_p as defined in the ring theory high school visit. Indeed, this holds for $\mathrm{v}_p|_{\mathbf{Z}}$ by Theorem 1.13.5) therefore holds for $\mathrm{v}_p|_{\mathbf{Q}}$. This ends the proof of the Theorem ■

Remark. It is easy to prove that $\mathbf{Z}_p$ is a compact metric space (see hometask). It follows from step 3 of the previous theorem that $\mathbf{Q}_p$ is therefore locally compact.

Theorem 1.17. Consider the special set of absolute values on $\mathbf{Q}$: $|| \, ||_\infty = | \, |$, for each p $|| \cdot ||_p = p^{-\mathrm{v}_p(\cdot)}$. Suppose $x \in \mathbf{Q}$. Then ("the product formula")
$||x||_\infty \prod\limits_p ||x||_p = 1$.

Proof. Hometask. ■

Now we are going to study the structure of the multiplicative group $\mathbf{Q}_p^*$. Clearly $\mathbf{Q}_p^* = p^{\mathbf{Z}} \times U$ (see Theorem 1.13 5)). It remains to study U.

Definition-Theorem 1.18. Let $U_n = 1 + p^n\mathbf{Z}_p \subset U$. Then U_n is a subgroup, $\epsilon_n|_U : U \to (\mathbf{Z}/(p^n))^*$ is a surjective group homomorphism, $\ker(\epsilon_n|_U) = U_n$.

Proof. We already know that ϵ_n is a surjective ring homomorhism. Hence if $x \in \mathbf{Z}_p$ is invertible then $\epsilon_n(x) \in \mathbf{Z}/(p^n)$ is invertible. Conversely if $\epsilon_n(x)$ is invertible then $p \nmid \epsilon_n(x)$ (f hometask) hence x is invertible in $\mathbf{Z}_p$, so $\epsilon_n|_U : U \to (\mathbf{Z}/(p^n))^*$ is surjective. $\ker(\epsilon_n|_U) = U_n$ by definition ■

Theorem 1.19. (The Teichmüller decomposition). $U = T \times U_1$, $T \overset{\text{def}}{=} \{x \in U$ such that $x^{p-1} = 1\}$ being a cyclic group of p-1 elements.

Proof. We postpone the proof to the end of the next theorem.

Remark. If $p = 2$ then $U = U_1$ and T is a trivial group.

Theorem 1.20. (Hensel's Lemma) Suppose $f \in \mathbf{Z}_p[t]$, f' its derivative, $n \in \mathbf{Z}_{>0}$ a positive integer. Suppose $x \in \mathbf{Z}_p$ is some p-adic integer such that $\mathrm{v}_p(f'(x)) = 0$ and $f(x) \equiv 0 \bmod p^n$. Then $\exists y \in \mathbf{Z}_p$ such that
1) $f(y) \equiv 0 \bmod p^{n+1}$
2) $\mathrm{v}_p(f'(y)) = 0$
3) $y \equiv x \bmod p^n$

Proof. Let us search for $y = x + p^n z$, $z \in \mathbf{Z}_p$. By the Taylor formula $f(y) = \sum\limits_{i=0}^{\deg f} \frac{f^{(i)}(x)}{i!}(p^n z)^i$.

Since for any monomial x^j and for any $i \leq j$ $\frac{(x^j)^{(i)}(x)}{i!} = \binom{j}{i}x^{j-i}$ the coefficients $\frac{f^{(i)}(x)}{i!}$ are p-adic integers hence $f(y) = f(x) + p^n z f'(x) + p^{2n}a$ for some $a \in \mathbf{Z}_p$. By assumption $f(x) = p^n b$ for some $b \in \mathbf{Z}_p$, $f'(x) = c$ for some $c \in U$. Choose z such that $b + zc \equiv 0 \bmod p$, since c is invertible this is possible. Then 1) holds. 3) holds automatically by the choice of y. 2) also holds (use the Taylor formula for $f'(y)$) ■

Proof of the Theorem 1.19. The equation $x^{p-1} - 1 = 0$ has $p - 1$ different solutions $\bmod p$. By Hensel's Lemma each of these solutions could be lifted to the solution of the same equation in $\mathbf{Z}_p$. Clearly they all are different and form a subgroup in U which is cyclic by the general Theorem as a finite subgroup of the multiplicative group of the field ■

Definition-Theorem 1.21. Suppose $\alpha \in \mathbf{Z}_p$, $\alpha \equiv 1 \bmod p$. The function $\exp_\alpha : \mathbf{Z}_p \to \mathbf{Z}_p$ is defined as follows. Suppose $z \in \mathbf{Z}_p$, $z = \{{}_iz \in \mathbf{Z}/(p^i)\}$. For each i choose $\widetilde{{}_iz} \in \mathbf{Z}_{\geq 0}$ such that $\widetilde{{}_iz} \equiv {}_iz \bmod p^i$. Then $\exp_\alpha(z)$ (or α^z) $= \lim\limits_{i \to \infty}\{\alpha^{\widetilde{{}_iz}}\}$. The map $\exp_\alpha$ is a group homomorphism from the additive group of the ring $\mathbf{Z}_p$ to the subgroup U_1 of its group of units U.

Proof. If a p-adic number equals 1 mod p^k then its p-th power equals 1 mod p^{k+1} by the binomial formula, hence for any integer y such that $p^i|y$ $\alpha^y \equiv 1 \bmod p^{i+1}$. Therefore $\{\alpha^{\widetilde{{}_iz}}\}$ is a Cauchy sequence (for $i > j$ both large $||\alpha^{\widetilde{{}_iz}} - \alpha^{\widetilde{{}_jz}}||_p = ||\alpha^{\widetilde{{}_jz}}||_p||\alpha^{\widetilde{{}_iz}-\widetilde{{}_jz}} - 1||_p = ||\alpha^{\widetilde{{}_iz}-\widetilde{{}_jz}} - 1||_p$, the latter being close to zero as $p^j|(\widetilde{{}_iz} - \widetilde{{}_jz})$), hence α^z exists. We still need to prove that α^z does not depend on the choice of integers $\widetilde{{}_iz}$, which is a hometask.
Suppose z_1 and z_2 are two elements of $\mathbf{Z}_p$ and the integers $\widetilde{{}_iz_1}$ *and* $\widetilde{{}_iz_2}$ are chosen. Let $z = z_1 + z_2$. One may choose $\widetilde{{}_iz} = \widetilde{{}_iz_1} + \widetilde{{}_iz_2}$. Then $\alpha^{\widetilde{{}_iz}} = \alpha^{\widetilde{{}_iz_1}}\alpha^{\widetilde{{}_iz_2}}$ hence the homomorphism property holds for the Cauchy sequences componentwise and therefore holds for their limits. Since α is in U_1 it is clear that the image of $\exp_\alpha$ is in U_1 ■

Theorem 1.22. 1) If $p \neq 2$ and $\alpha \not\equiv 1 \bmod p^2$ then $\exp_\alpha$ defines an isomorphism $\mathbf{Z}_p \to U_1$.
2) If $p = 2$ and $\alpha \equiv 5 \bmod 8$ then $\exp_\alpha$ defines an isomorphism $\mathbf{Z}_p \to U_2$.

Proof. We first suppose $p \neq 2$. Consider the composite map $\delta_i = \epsilon_{i+1} \circ \exp_\alpha$ $\mathbf{Z}_p \overset{\exp_\alpha}{\to} U_1 \overset{\epsilon_{i+1}}{\to} (\mathbf{Z}/(p^{i+1}))^*$. By the first line of the proof of 1.21 $p^i\mathbf{Z}_p \subset \ker \delta_i$, hence δ_i defines a homomorphism $\mathbf{Z}_p/(p^i) \to (\mathbf{Z}/(p^{i+1}))^*$ for which we will use the same notation δ_i. The image of δ_i is contained in the subgroup $(\mathbf{Z}/(p^{i+1})^*)_1$ consisting of the residues equal to

1 mod p. The order of this subgroup equals p^i because $\phi(p^{i+1}) = p^i(p-1)$, so just p^i invertible residues mod p^{i+1} have a particular residue mod p. The order of $\mathbf{Z}_p/(p^i)$ also equals p^i hence it suffices to prove that δ_i is injective to conclude it is an isomorphism. For $p = 2$ one needs to define $\delta_i = \epsilon_{i+2} \circ \exp_\alpha$ and to consider the subgroup $(\mathbf{Z}/(p^{i+2})^*)_1$ consisting of the residues equal to 1 mod 4. This is also of order p^i.
Let $z \in \mathbf{Z}_p, z \not\equiv 0 \mod p^i$. Choose $\tilde{z} \in \mathbf{Z}$, $\tilde{z} \equiv z \mod p^i$. Then $\delta_i(z) = \delta_i(\tilde{z})$. By the choice of z $\tilde{z} = p^k u$ for some $k < i$ and u not divisible by p. So $\alpha^{\tilde{z}} = \alpha^{p^k u} = (\alpha^u)^{p^k}$. It is clear that in both cases of the Theorem α^u satisfies the same conditions as α does. So to prove that δ_i is injective (hence an isomorphism) it remains to prove that for $k < i$ $\alpha^{p^k} \not\equiv 1 \mod p^{i+1}$. This could be done by induction, using the following Lemma.

Lemma. If $p \nmid u$, $p \neq 2$ and $v \geq 1$ or $p = 2$ and $v \geq 2$ then $\mathrm{v}_p((1 + p^v u)^p - 1) = v + 1$.

Proof. By the binomial formula $(1 + p^v u)^p = \sum\limits_{i=0}^{p} \binom{p}{i} p^{iv} u^i$. The first term is 1, v_p(second term) is $v + 1$. If $i \geq 3$ then $iv > v + 1$ hence v_p (forth and later terms) $> v + 1$. If $i = 2$ then $iv + \mathrm{v}_p\left(\binom{p}{i}\right) > v + 1$ by the conditions of the Lemma ■

End of the proof of the Theorem. $\mathbf{Z}_p$ is a projective limit of its quotient groups $\mathbf{Z}/(p^i)$. Correspondingly if $p \neq 2$ then U_1 is a projective limit of its quotient groups $(\mathbf{Z}/(p^{i+1})^*)_1$ while if $p = 2$ then U_2 is a projective limit of its quotient groups $(\mathbf{Z}/(p^{i+2})^*)_1$. The maps δ_i are isomorphisms on the quotient groups and it is easy to check that they commute with the standard residue maps (i.e. $\delta_{i-1} \circ \phi_i = \phi_{i+1} \circ \delta_i$ for $p \neq 2$ and $\delta_{i-1} \circ \phi_i = \phi_{i+2} \circ \delta_i$ for $p = 2$). Hence the map $\exp_\alpha$ of the projective limits is an isomorphism ■

Theorem 1.23. If $p \neq 2$ then $\mathbf{Z}_p^* \simeq T \times \mathbf{Z}_p$. If $p = 2$ then $\mathbf{Z}_p^* \simeq \{\pm 1\} \times \mathbf{Z}_p$.

Proof. This follows immediately from theorems 1.19 and 1.22 ■

Definition 1.24. log: $U_1 \to \mathbf{Z}_p$ $\log(1 + x) \overset{\text{def}}{=} \sum\limits_{i=1}^{\infty} (-1)^{i-1} \frac{x^i}{i}$.

exp: ($p\mathbf{Z}_p \to U_1$ if $p \neq 2$; $p^2\mathbf{Z}_p \to U_2$ if $p = 2$) $\exp(z) \overset{\text{def}}{=} \sum\limits_{i=0}^{\infty} \frac{z^i}{i!}$.

Remark. Since $\mathrm{v}_p(i!) = \frac{1}{p-1}(i$ - sum of the digits of i in the p-based system) (to prove is a hometask) the definition above is correct.

Theorem 1.25. If $p \neq 2$ then $U_1 \overset{\log}{\cong} p\mathbf{Z}_p$. If p=2 then $U_2 \overset{\log}{\cong} p^2\mathbf{Z}_p$.

Proof. It is wellknown that the formal power series in the Definition 2.24 are inverse to each other. Since in $\mathbf{Q}_p$ every convergent power series converges absolutely the same is true for the functions they define ■