Algebraic NT, L5

the last thm. of L in fact forgot to mention the assumption that $|a|_p \leq 1$. the proof in Koblitz's book is not so obvious, it takes more than 1 page (pp. 11-12)

theorem 2

The import of thm. 5 cannot be overstated because it enables us to replace an uncountable set $a = [(a_n)]_\sim$ by a countable set, an infinite sequence $\sum_{i=0}^{\infty} b_i p^i$ (written instead of $(b_i)_{i\geq 0}$ in the form of a formal infinite sum) with every $b_i \in \{0, 1, \dots, p-1\}$; here $c_0 = b_0$, $c_1 = b_0 + b_1 p$, $c_2 = b_0 + b_1 p + b_2 p^2$, ... thus we get the ring $\mathbb{Z}_p$ of p-adic integers: $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$ $= \{\sum_{i=0}^{\infty} b_i p^i \mid b_i \in \{0, 1, \dots, p-1\}\}$. the operations of addition (+) and multiplication ($\cdot$, or omitted) are defined in $\mathbb{Z}_p$, in the representation, in the ob-

vious way, with the carries in higher order, like we compute with decimal expansions. For example,

$$1 = 1\cdot p^0 + 0\cdot p^1 + 0\cdot p^2 + 0\cdot p^3 + \dots +$$
$$+ (p-1) = (p-1)p^0 + (p-1)\cdot p^1 + (p-1)\cdot p^2 + (p-1)\cdot p^3 + \dots$$

$$0 = 0\cdot p^0 + 0\cdot p^1 + 0\cdot p^2 + 0\cdot p^3 + \dots$$

carry +1 ↦ ↦ ↦ ...

and we see that $\sum_{i=0}^{\infty}(p-1)p^i = -1$ in $\mathbb{Z}_p$. Here we represent numbers $n \in \mathbb{N}_0$ as elements of $\mathbb{Z}_p$ by extending their p-adic expansions by 0 digits: $n \in \mathbb{N}_0 \rightsquigarrow n = b_0 p^0 + b_1 p^1 + \dots + b_q p^q$, $b_i \in \{0,1,\dots,p-1\}$, $b_q > 0$

$$= \sum_{i=0}^{\infty} b_i p^i \text{ with } b_i := 0 \text{ for } i > q.$$

More generally we can find additive inverse to any $a \in \mathbb{Z}_p$: If $a = \sum_{i=0}^{\infty} b_i p^i$, $b_i \in \{0,1,\dots,p-1\}$ and $\bar{a} := \sum_{i=0}^{\infty}(p-1-b_i)p^i$, then we see as above with $a = 1$ that $(a+\bar{a})+1 = a+(\bar{a}+1)$ and there-

Prove $-a = 1 + \bar{a}$. But here we used associativity (the addit. inverse to a of $+$) which should have been established before. Anyway, one can show that $(\mathbb{Z}_p, 0, 1, +, \cdot)$ is a comm. integral domain.

Similarly to our previous Prop. 1 we can prove

Proposition 6 $a = \sum_{i=0}^{\infty} b_i p^i$, $b_i \in \{0, \dots, p-1\}$, is a unit in $\mathbb{Z}_p \iff b_0 > 0$.

The field $\mathbb{Q}_p$ is a field of fractions of $\mathbb{Z}_p$ and we represent its elements as formal sums $a = \sum_{i=k}^{\infty} b_i p^i$, $b_i \in \{0, \dots, p-1\}$, $k \in \mathbb{Z}$, and $b_k > 0$; $0 = \sum_{i=-\infty}^{\infty} 0 \cdot p^i$.

We set $\mathrm{ord}_p(a) := k$ and $\mathrm{ord}_p(0) := +\infty$, and (for $a \in \mathbb{Q}_p$) $|a|_p := (1/p)^{\mathrm{ord}_p(a)}$, so $|0|_p = 0$. This agrees with the previously defined p-adic absolute value or, rather, norm $\|a\|_p$. From now on I will write $|a|_p$ instead of $\|a\|_p$.

*) Probably it is best to formally represent 0 by the empty sum.

Operations in $\mathbb{Q}_p$: $a = \sum_{i=k}^{\infty} b_i p^i$, $a' = \sum_{i=k'}^{\infty} b'_i p^i$, $(+,\cdot)$

with $b_i, b'_i \in \mathbb{Z}_m$ and $b_k, b'_{k'} \neq 0$. Then $c = a+a' = \sum_{i=\ell}^{\infty} b''_i p^i$ where $\ell = \min(k, k')$ and the digits $b''_i \in \mathbb{Z}_m$ are obtained from the pairwise sums $b_i + b'_i$ and carries. Similarly, the product $c = aa' = \sum_{i=k+k'}^{\infty} b'''_i p^i$ where $b'''_i = \sum_{j+j'=i} b_j b'_{j'}$ + Carries

(undefined b_j with $j < k$ are extended by 0s, same with $b'_{j'}$), the sum is in reality finite, this recipe includes the case when one or both of a, a' is 0: $a + 0 = a$, $0 + a' = a'$ and $0+0=0$), $a0 = 0a' = 00 = 0$. From this we clearly see the properties of p-adic order: If $a, a' \in \mathbb{Q}_p$ then $\mathrm{ord}_p(a+a') \geq \min(\mathrm{ord}_p(a), \mathrm{ord}_p(a'))$, with $=$ if $\mathrm{ord}_p(a) \neq \mathrm{ord}_p(a')$, and $\mathrm{ord}_p(aa') =$

$= ord_p(a) + ord_p(a')$. (for $\forall a, a' \in \mathbb{Q}_p$, including 0)

Also, $\mathbb{Z}_p$ is a local ring as ~~$\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \mid a \neq 0\}$~~

$p\mathbb{Z}_p = \{0 \cdot p^0 + b_1 p^1 + b_2 p^2 + \dots \mid b_i \in \mathbb{N}\}$

$= \mathbb{Z}_p \setminus \mathbb{Z}_p^\times$ is its only maximal ideal.

= non-units of $\mathbb{Z}_p$

Of course, $(\mathbb{Q}_p, 0, 1, +, \cdot, |\cdot|_p)$ is a non-archimedean normed field.

Here are three examples on arithmetic in $\mathbb{Q}_p$, taken from Koblitz's book (p. 15). Before giving them I mention as a reference on p-adic numbers the book by Alain M. Robert, A Course in p-adic Analysis, Springer-Verlag, New York (2000).

Examples. (Not in Koblitz): $(1-p) \cdot \sum_{i=0}^{\infty} 1 \cdot p^i =$

$= (1 \cdot p^0 + 0 \cdot p^1 + 0 \cdot p^2 + \dots) - (0 \cdot p^0 + 1 \cdot p^1 + 0 \cdot p^2 + \dots)$

$= \sum_{i=0}^{\infty} 1 \cdot p^i - \sum_{i=1}^{\infty} 1 \cdot p^i = 1 \cdot p^0 + 0 \cdot p^1 + 0 \cdot p^2 + \dots = 1.$

Thus, in $\mathbb{Q}_p$ and even in $\mathbb{Z}_p$, $\frac{1}{1-p} = (1-p)^{-1} =$

$= 1 \cdot p^0 + 1 \cdot p^1 + 1 \cdot p^2 + 1 \cdot p^3 + \dots$. This is one form

of the geometric series formula. Now kobitas examples: ($p=7$)

Multiplication:

$$3+6\cdot 7+2\cdot 7^2+\dots$$
$$\times\ 4+5\cdot 7+1\cdot 7^2+\dots$$

$$5+4\cdot 7+4\cdot 7^2+\dots$$
$$1\cdot 7+4\cdot 7^2+\dots$$
$$3\cdot 7^2+\dots$$
$$\vdots$$
$$5+5\cdot 7+4\cdot 7^2+\dots$$

Subtraction:

$$2\cdot 7^{-1}+0\cdot 7^0+3\cdot 7^1+\dots$$
$$-\ 4\cdot 7^{-1}+6\cdot 7^0+5\cdot 7^1+\dots$$
$$5\cdot 7^{-1}+0\cdot 7^0+4\cdot 7^1+\dots$$

• Kurt Hensel

Division $(1+2\cdot 7+4\cdot 7^2+\dots):(3+5\cdot 7+1\cdot 7^2+\dots)$

$$-\ 1+6\cdot 7+1\cdot 7^{2+1}+\dots$$
$$(3\cdot 7+2\cdot 7^{2+1}+\dots)$$
$$-\ (3\cdot 7+5\cdot 7^2+\dots)$$
$$4\cdot 7^2+\dots$$
$$-\ (4\cdot 7^{2+1}+\dots)$$
$$\vdots$$

$$= 5+1\cdot 7+6\cdot 7^2+\dots$$

- We are retrieving (mentally, physically it is, sadly, impossible) to elementary/grade school!!! thank you