

Topics in number theory: p -adic numbers

Solutions to homework 3

Problem 1. Show that, for n in \mathbb{Z}_p and x in $2p\mathbb{Z}_p$, $|\exp(n \log(1+x)) - 1|_p = |xn|_p$. (Note $\exp(n \log(1+x))$ is the definition of $(1+x)^n$.)

Solution. If $x \in 2p\mathbb{Z}_p$ then from the proof of Proposition 4.5.8 of Gouvea (and as stated in the lecture) we have $|\log(1+x)|_p = |x|_p$. In particular, $y := n \log(1+x)$ is in $2p\mathbb{Z}_p$. We also proved that then $|\exp(y) - 1|_p = |y|_p$. Thus, $|\exp(n \log(1+x)) - 1|_p = |n \log(1+x)|_p = |xn|_p$.

Problem 2. Let $f(X) = \sum_{n \geq 1} \frac{X^n}{n^2}$. Verify that $x \mapsto f(x)$ is a function on $p\mathbb{Z}_p$, and use the corollary to Strassman's theorem to bound the number of its zeroes in the balls $p^m\mathbb{Z}_p$ ($m \geq 1$).

Solution. Note that $(\limsup |1/n^2|_p^{1/n})^{-1} = 1$ and therefore $f(x)$ is a function on $p\mathbb{Z}_p$.

Let $g_m(X) = f(p^m X) = \sum_{n \geq 1} \frac{p^{mn} X^n}{n^2}$. Let a_n denote the coefficient of X^n in $g_m(X)$ and let N be the positive integer that satisfies the condition in Strassman's theorem. Then $f(X)$ has at most N zeroes in the ball $p^m\mathbb{Z}_p$.

If $n = sp^r$ with $(p, s) = 1$, then $v_p(a_n) = msp^r - 2r$. Therefore $v_p(a_n)$ is minimal implies that $s = 1$, so $N = p^r$. Thus we need to find $r \geq 0$ such that $v_p(a_{p^r})$ is minimal.

Now $b_r := v_p(a_{p^{r+1}}) - v_p(a_{p^r}) = mp^{r+1} - 2(r+1) - mp^r + 2r = mp^r(p-1) - 2$. This is positive if $p > 3$ and $r \geq 0$, and therefore $N = p^0 = 1$ if $p > 3$.

If $p = 3$ then $b_r > 0$ for $r > 0$. Since $v_p(a_1) = m$ and $v_p(a_3) = 3m - 2$, we have $N = 3$ if $m = 1$ and $N = 1$ otherwise.

Finally, if $p = 2$ then $b_r > 0$ for $r > 1$. Since $v_p(a_1) = m$, $v_p(a_2) = 2m - 2$ and $v_p(a_4) = 4m - 4$, we have $N = 4$ if $m = 1$, $N = 2$ if $m = 2$ and $N = 1$ otherwise.

$$\text{Summarizing, we have } N = \begin{cases} 4 & \text{if } p = 2, m = 1, \\ 3 & \text{if } p = 3, m = 1, \\ 2 & \text{if } p = 2, m = 2, \\ 1 & \text{otherwise.} \end{cases}$$

Problem 3. Let $K = \mathbb{Q}_2(\sqrt{2})$, an extension of \mathbb{Q}_2 of degree 2. $|\cdot|_2$ on \mathbb{Q}_2 extends to a non-archimedean absolute value on K by the formula $|a + b\sqrt{2}| = \sqrt{|a^2 - 2b^2|_2}$ for a, b in \mathbb{Q}_2 .

- Show that K does not contain fourth roots of unity other than ± 1 .
- Show that the valuation ring of K is $\mathcal{O}_K = \{a + b\sqrt{2} \text{ with } a, b \in \mathbb{Z}_2\}$ with valuation ideal $\mathfrak{P}_K = \sqrt{2}\mathcal{O}_K$, and describe the residue field $\mathcal{O}_K/\mathfrak{P}_K$ explicitly.
- Suppose that $\zeta \in K \setminus \{1\}$ satisfies $\zeta^p = 1$ for some prime $p \neq 2$. Use the identity $(1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{p-1}) = p$, and the absolute values of ζ and $1 - \zeta$ to show that there are no non-trivial p -th roots of unity in K for any odd prime p .

Solution. (a) If $(a + b\sqrt{2})^2 = -1$ with $a, b \in \mathbb{Q}_2$, then by expanding and noting that $\{1, \sqrt{2}\}$ is a basis for K over \mathbb{Q}_2 we see that $2ab = 0$ and $a^2 + 2b^2 = -1$. Note that -1 is not a square in \mathbb{Q}_2 (by Homework 1), and -2 is not a square in \mathbb{Q}_2 since its valuation is 1. Therefore we get a contradiction and hence -1 is not a square in K .

(b) The valuation is $v(a + b\sqrt{2}) = v_2(a^2 - 2b^2)/2$. For $a, b \in \mathbb{Q}_2$ note that $v_2(a^2)$ is even and $v_2(2b^2)$ is odd. Therefore, $v_2(a^2 - 2b^2) = \min\{v_2(a^2), v_2(2b^2)\}$. In particular, $v(a + b\sqrt{2}) \geq 0$ if

and only if this minimum is non-negative. Therefore, $a + b\sqrt{2} \in \mathcal{O}_K$ if and only if $v_2(a) \geq 0$ and $v_2(b) \geq -1/2$ (and hence $v_2(b) \geq 0$). So the valuation ring is $\{a + b\sqrt{2} \text{ with } a, b \in \mathbb{Z}_2\}$.

For the valuation ideal, it is clear that $\sqrt{2}\mathcal{O}_K \subseteq \mathfrak{P}$, since $v(\sqrt{2}\alpha) = 1 + v(\alpha)$. Conversely, $v(a + b\sqrt{2}) > 0$ if and only if $v_2(a) > 0$ and $v_2(b) > -1/2$. The latter condition is equivalent to $v_2(b) \geq 0$. Note that $v_2(a) > 0$ implies that $a \in \sqrt{2}\mathcal{O}_K$ and $v_2(b) \geq 0$ implies $b\sqrt{2} \in \sqrt{2}\mathcal{O}_K$. This shows that $\mathfrak{P} \subseteq \sqrt{2}\mathcal{O}_K$ and hence $\mathfrak{P} = \sqrt{2}\mathcal{O}_K$. The residue field $\mathcal{O}_K/\mathfrak{P}$ consists of two elements \mathfrak{P} and $1 + \mathfrak{P}$. Note that for any $a, b \in \mathbb{Z}_2$, $a + b\sqrt{2} + \mathfrak{P} = a + \mathfrak{P}$ which equals one of \mathfrak{P} or $1 + \mathfrak{P}$.

(c) If ζ in K satisfies $\zeta^p = 1$ then $v(\zeta^k) = 0$ for all $k \geq 0$. Therefore, by the previous part it follows that $\zeta^k \in 1 + \mathfrak{P}$ for all $k \geq 0$. In particular, it follows that $v(1 - \zeta^k) > 0$ for all $k \geq 0$. But by the given identity we have $v(1 - \zeta) + v(1 - \zeta^2) + \cdots + v(1 - \zeta^{p-1}) = v(p) = 0$. This is a contradiction.

Problem 4. We let $L = \mathbb{Q}_2(\sqrt{5})$ and $M = \mathbb{Q}_2(\sqrt{7})$. They are extensions of degree 2 of \mathbb{Q}_2 because 5 and 7 are not squares in \mathbb{Q}_5 . $|\cdot|_2$ on \mathbb{Q}_2 extends to a non-archimedean absolute value on each by the formula $|a + b\sqrt{D}| = \sqrt{|a^2 - Db^2|_2}$ for a, b in \mathbb{Q}_2 , and $D = 5$ or 7 .

- For α in L^\times or M^\times , define $v(\alpha)$ in $\frac{1}{2}\mathbb{Z}$ by $|\alpha| = 2^{-v(\alpha)}$. Show that $v(\alpha) = v_2(\alpha)$ if α is in \mathbb{Q}_2^\times . Moreover, show that for M , the image of v is $\frac{1}{2}\mathbb{Z}$, but that for L the image is \mathbb{Z} . (Hint: For L , first show that if a, b are in \mathbb{Z}_2^\times , then $v(a + b\sqrt{5}) = 1$.)
- Show that $X^8 - 1$ has exactly 4 roots in M , namely those of $X^4 - 1$.
- Show that for M , the valuation ring is $\mathcal{O}_M = \{a + b\sqrt{7} \text{ with } a, b \in \mathbb{Z}_2\}$ with valuation ideal $\mathfrak{P}_M = (1 + \sqrt{7})\mathcal{O}_M$, and describe the residue field $\mathcal{O}_M/\mathfrak{P}_M$ explicitly.
- Determine the valuation ring \mathcal{O}_L of L and its valuation ideal \mathfrak{P}_L , and describe the residue field $\mathcal{O}_L/\mathfrak{P}_L$ explicitly.

Solution. (a) Note that $v(a + b\sqrt{D}) = v_2(a^2 - Db^2)/2$, so for $\alpha \in \mathbb{Q}_2^\times$ we have $v(\alpha) = v_2(\alpha^2)/2 = v_2(\alpha)$. Hence $v(\mathbb{Q}_2) = \mathbb{Z} \subseteq v(M) \subseteq \frac{1}{2}\mathbb{Z}$. Since $v(1 + \sqrt{7}) = v_2(1 - 7)/2 = 1/2$, we have $1/2 \in v(M)$. Since v is a homomorphism of groups, it follows that $v(M) = \frac{1}{2}\mathbb{Z}$.

Similarly, $v(\mathbb{Q}_2) = \mathbb{Z} \subseteq v(L) \subseteq \frac{1}{2}\mathbb{Z}$. If $a, b \in \mathbb{Z}_2^\times$, then $a^2, b^2 \in 1 + 8\mathbb{Z}_2$, so $a^2 - 5b^2 \in 4 + 8\mathbb{Z}_2$ and hence $v(a + b\sqrt{D}) = v_2(a^2 - 5b^2)/2 = 1$. For arbitrary $a, b \in \mathbb{Q}_2$, if $v_2(a) \neq v_2(b)$, then $v_2(a^2 - 5b^2) = \min\{v_2(a^2), v_2(b^2)\} \in 2\mathbb{Z}$, and hence $v(a + b\sqrt{D}) \in \mathbb{Z}$. On the other hand, if $v_2(a) = v_2(b) = m$, then writing $a = 2^m a_0$ and $b = 2^m b_0$ with a_0 and b_0 in \mathbb{Z}_2^\times , we have $v(a + b\sqrt{5}) = m + v(a_0 + b_0\sqrt{5}) = m + 1 \in \mathbb{Z}$. This proves $v(L) = \mathbb{Z}$.

(b) Since $-7 \equiv 1 \pmod{8}$ is a square modulo 8, by Hensel's Lemma -7 is a square in \mathbb{Z}_2 (proved in the class). Therefore, $\mathbb{Q}_2(\sqrt{7}) = \mathbb{Q}_2(\sqrt{-1})$ which shows that $\sqrt{-1}$ is in M , and $X^4 - 1$ has four solutions in M . On the other hand, if α in M satisfied $\alpha^4 + 1 = 0$, then $\alpha^2 = \pm\sqrt{-1} = c\sqrt{7}$ for some $c \in \mathbb{Z}_2^\times$. Let $\alpha = a + b\sqrt{7}$ with a and b in \mathbb{Q}_2 . Then $c\sqrt{7} = \alpha^2 = (a^2 + 7b^2) + 2ab\sqrt{7}$ implies that $a^2 + 7b^2 = 0$ since $\{1, \sqrt{7}\}$ is a basis for M over \mathbb{Q}_2 . If $b = 0$ then $a = 0$, and $\alpha = 0$ is no solution. If $b \neq 0$ then $a \neq 0$ and $v_2(a) = v_2(b)$, in which case $c = 2ab$ gives a contradiction since $v_2(c) = 0$ and $v_2(2ab)$ is an odd integer. Therefore, there is no α in M satisfying $\alpha^4 + 1 = 0$.

(c) Clearly, $\mathbb{Z}_2 + \sqrt{7}\mathbb{Z}_2 \subseteq \mathcal{O}_M$. Let $a, b \in \mathbb{Q}_2$ with $v_2(a) = m$, $v_2(b) = n$ and $v(a + b\sqrt{7}) \geq 0$. Then $v_2(a^2 - 7b^2) \geq 0$. If $m \neq n$ then $v_2(a^2) \neq v_2(7b^2)$ and hence $v_2(a^2 - 7b^2) = \min\{v_2(a^2), v_2(7b^2)\} \geq 0$, which implies that $m, n \geq 0$. If $m = n$ writing $a = 2^m a_0$ and $b = 2^m b_0$ with a_0 and b_0 in \mathbb{Z}_2^\times we get $v_2(a^2 - 7b^2) = 2m + v_2(a_0^2 - 7b_0^2)$. As noted earlier, a_0^2 and b_0^2 lie in $1 + 8\mathbb{Z}_2$ and hence $a_0^2 - 7b_0^2 \in 2 + 8\mathbb{Z}_2$. Therefore, $v_2(a^2 - 7b^2) = 2m + 1$. This implies that $2m + 1 \geq 0$ and hence $m \geq 0$. This proves that $\mathcal{O}_M = \mathbb{Z}_2 + \sqrt{7}\mathbb{Z}_2$.

As seen in part (a), $v(1 + \sqrt{7}) = 1/2$ and hence by Proposition 5.4.5, $\mathfrak{P}_M = (1 + \sqrt{7})\mathcal{O}_M$. Given $\alpha = a + b\sqrt{7} \in \mathcal{O}_M$, with a and b in \mathbb{Z}_2 , we have $\alpha = (a - b) + b + b\sqrt{7}$ and therefore $\alpha + \mathfrak{P}_M = (a - b) + \mathfrak{P}_M$. Moreover, since $2\mathbb{Z}_2 \subseteq \mathfrak{P}_M$, we see that $(a - b) + \mathfrak{P}_M$ equals \mathfrak{P}_M or

$1 + \mathfrak{P}_M$. Thus, $\mathcal{O}_M/\mathfrak{P}_M$ has two elements, 0 and 1 being distinct representatives. [Note that, with $I = \mathcal{O}_M(1 + \sqrt{7}) \subseteq \mathfrak{P}_M$, $2\mathbb{Z}_2 \subseteq I$ since $2 = (-1/3 + \sqrt{7}/3)(1 + \sqrt{7})$. So the same argument using I instead of \mathfrak{P}_M shows that I is a maximal ideal of \mathcal{O}_M , which proves directly that $I = \mathfrak{P}_M$.]

(d) Let $\alpha = (1 + \sqrt{5})/2$. Since $v(\alpha) = v_2(1/4 - 5/4)/2 = 0$ we have $\alpha \in \mathcal{O}_L$. Thus $\mathbb{Z}_2 + \alpha\mathbb{Z}_2 \subseteq \mathcal{O}_L$. Note that every element of \mathcal{O}_L can be written as $a + b\alpha$ with $a, b \in \mathbb{Q}_2$. Consider such an element with $v_2(a) = m$ and $v_2(b) = n$. Therefore, from part (a), $v(a) = m$ and $v(b\alpha) = n$. Thus, if $m \neq n$ then it follows from the non-archimedean property that $m, n \geq 0$. On the other hand, if $m = n$ then writing $a = 2^m a_0$ and $b = 2^m b_0$ with a_0, b_0 in \mathbb{Z}_2^\times , we get $v(a + b\alpha) = m + v(a_0 + b_0\alpha)$. And $v(a_0 + b_0\alpha) = v(a_0^2 + a_0 b_0 - b_0^2) = 0$ since $a_0^2, a_0 b_0$ and b_0^2 are all in $1 + 2\mathbb{Z}_2$. Thus, it follows that $m \geq 0$. This proves that $\mathcal{O}_L = \mathbb{Z}_2 + \alpha\mathbb{Z}_2$.

By Proposition 5.4.5 it follows that $\mathfrak{P}_L = 2\mathcal{O}_L$ (and this can also be seen directly as above by considering when $v(a + b\alpha) > 0$). Note that $v(\alpha) = v(1 \pm \alpha) = 0$ and hence $\alpha, 1 \pm \alpha$ are not in \mathfrak{P}_L . It is therefore clear that $\mathfrak{P}_L, 1 + \mathfrak{P}_L, \alpha + \mathfrak{P}_L$ and $(1 + \alpha) + \mathfrak{P}_L$ are disjoint. On the other hand, if $a + b\alpha \in \mathcal{O}_L$ with a and b in \mathbb{Z}_2 , then either a or $a - 1$ is in $2\mathbb{Z}_2 \subseteq \mathfrak{P}_L$ and similarly either b or $b - 1$ is in \mathfrak{P}_L . Therefore $(a + b\alpha) + \mathfrak{P}_L$ reduces to one of the four classes mentioned above. Thus, $\mathcal{O}_L/\mathfrak{P}_L$ is a field with four elements.