Exercise 1 If $|x+y| \leq \max\{|x|, |y|\}$, then in particular

$|n \cdot 1| = |\underbrace{1+\dots+1}_{n}| \leq |1|$, so the image of $\mathbb{Z}$ is bounded in K.

Now suppose $|n \cdot 1| \leq C \ \forall \ n \in \mathbb{Z}$.

Let $x, y \in K$; we may assume $|y| \leq |x|$.

Then $|x+y|^n \leq \sum_{k=0}^{n} \binom{n}{k} |x|^{n-k} |y|^k \leq (n+1) C |x|^n$,

hence $|x+y| \leq (1+n)^{\frac{1}{n}} C^{\frac{1}{n}} |x|$.

Letting $n \to \infty$, this yields $|x+y| \leq |x| = \max\{|x|, |y|\}$.

Exercise 2 a) Say $|y| < |x|$. Then

$$|y| < |x| = |x+y-y| \leq \max\{|x+y|, |y|\}$$

and we must have $\max\{|x+y|, |y|\} = |x+y|$, otherwise $|y| < |y|$.

Hence we get

$$|x| \leq |x+y|,$$

while also $|x+y| \leq \max\{|x|, |y|\} = |x|$.

Hence $|x+y| = \max\{|x|, |y|\}$.

2)

b) Suppose x, y, z are the corners of a triangle in K. Thus its side lengths are $x-y$, $x-z$ and $y-z$.

If all these lengths are equal there is nothing to prove. If not, say $|x-z| < |x-y|$.

Then

$$|(z-x)+(x-y)| = |z-y| = \max\{|x-z|, |x-y|\} = |x-y|$$

by (a), so the triangle is isosceles

c) Let $y \in B(x,\varepsilon) = \{z \in K : |z-x| < \varepsilon\}$

We must show that $B(y,\varepsilon) = B(x,\varepsilon)$.

Let $z \in B(y,\varepsilon)$, so $|z-y| < \varepsilon$

Then either $|z-x| < |z-y| < \varepsilon$ or $|z-x| = |z-y| < \varepsilon$ since every triangle is isosceles. In either case $z \in B(x,\varepsilon)$.

Similarly $B(x,\varepsilon) \subseteq B(y,\varepsilon)$.

So $B(x,\varepsilon) = B(y,\varepsilon)$.

d) Let $S_N = \sum_{n=1}^{N} a_n$. We must show that $\lim_{N,M\to\infty} |S_N - S_M| = 0$. Say $N < M$, then

$$|S_N - S_M| = \left|\sum_{n=N+1}^{M} a_n\right| \leq \max_{n\in(N+1,M)}\{|a_n|\} = |a_{N+1}| \xrightarrow{N\to\infty} 0$$

Since $\lim_{N\to\infty} |a_n| = 0$.

Exercise 3

a) Given $v: K^* \to G$, we get a valuation on $\mathbb{Q}^*$ by: $v\circ i : \mathbb{Q}^* \xhookrightarrow{i} K^* \to G$. By Ostrowski, $v\circ i = \mathrm{ord}_p$ for some p, and $\mathrm{im}(v\circ i) = \mathbb{Z}$.

But then $v = \frac{1}{e}\mathrm{ord}_p$, where e is the ramification index of p in $K/\mathbb{Q}$.

So $G = \frac{1}{e}\mathbb{Z}$, and thus v is discrete.

b) Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

Then $p^{\frac{1}{n}} \in \bar{\mathbb{Q}}$ $\forall n$, and $\mathrm{ord}_p(p^{\frac{1}{n}}) = \frac{1}{n} \xrightarrow{n\to\infty} 0$.

So the image of ord_p extended to $\bar{\mathbb{Q}}$ is not discrete.

4) Exercise 4 a) By construction, every $x \in \mathbb{Q}_p$ is the limit of a sequence from $\mathbb{Q}$.

Let $x \in \mathbb{Z}_p$ and $1 > \varepsilon > 0$. We must find $z \in \mathbb{Z}$ such that $|x - z|_p < \varepsilon$.

First, find $N \in \mathbb{N}$ s.t. $p^{-N} < \varepsilon$.

Then we can find $\frac{a}{b} \in \mathbb{Q}$ s.t. $|x - \frac{a}{b}|_p < \varepsilon$,

Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. In fact $\frac{a}{b} \in \mathbb{Z}_p$, for if $|\frac{a}{b}|_p > 1$ then, by Exercise 2(a) we have $|x - \frac{a}{b}|_p = \max\{|x|_p, |\frac{a}{b}|_p\} = |\frac{a}{b}|_p > 1$, contradicting $|x - \frac{a}{b}|_p < \varepsilon$.

So $|\frac{a}{b}|_p \leq 1$, meaning that (assuming a, b have no common factor) $p \nmid b$.

So $\gcd(p, b) = 1$, and thus we can find $n, m \in \mathbb{Z}$ such that $np^N + mb = 1$.

If $z = ma \in \mathbb{Z}$, we then have:

$$\begin{aligned} |\tfrac{a}{b} - z|_p &= |\tfrac{a}{b} - ma|_p \\ &= |\tfrac{a}{b}|_p \, |1 - mb|_p \\ &\leq |1 - mb|_p \\ &= |np^N|_p \leq p^{-N} < \varepsilon. \end{aligned}$$

Hence we get:

$$|x-z|_p = \left|(x-\tfrac{a}{b})+(\tfrac{a}{b}-z)\right|_p$$

$$\leq \max\left\{|x-\tfrac{a}{b}|_p, |\tfrac{a}{b}-z|_p\right\} < \varepsilon.$$

b) In fact any ultrametric space X is totally disconnected. By Ex. 2 (c), any two balls in X are either disjoint, or one is contained in the other. It follows that the complement of an open ball B in X is $X \setminus B = \bigcup_{\substack{B_\alpha \text{ open} \\ \text{ball s.t.} \\ B \cap B_\alpha = \emptyset}} B_\alpha$. Hence B is open and closed.

It follows that the only connected sets are singletons: indeed, if $x, y \in Y \subseteq X$, $x \neq y$, then let $\varepsilon = |x-y| > 0$. Then $Y' = B(x,\varepsilon) \cap Y$ is open & closed in Y, with $y \notin B(x,\varepsilon) \cap Y$. So the complement Y'' of Y' in Y is open & nonempty, with $Y = Y' \cup Y''$. Hence Y is disconnected.

6) Exercise 5 Let $f(X) = (X^2-2)(X^2-17)(X^2-34)$.

Since neither 2, 17 nor 34 is a square in $\mathbb{Q}$, f has no root in $\mathbb{Q}$. But of course 2, 17 and 34 have a square root in $\mathbb{R} = \mathbb{Q}_\infty$.

To check that f has a root in $\mathbb{Q}_p$ $\forall$ p, we check that either 2, 17 or 34 is a square mod p $\forall$ p. and then appeal to Hensel's lemma.

Let p be any prime, and suppose $\left(\frac{2}{p}\right) = \left(\frac{17}{p}\right) = -1$

Then $\left(\frac{34}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{17}{p}\right) = 1$. So at least one of 2, 17 and 34 is a square mod p.

For $p \neq 2, 17$ this root is simple and thus lifts to $\mathbb{Q}_p$. So it remains to check $p = 2, 17$.

$p = 17$. $X^2 - 2$ has a simple root in $\mathbb{F}_{17}$, namely 6.

$p = 2$. Claim: 17 has a square root in $\mathbb{Q}_2$. To show this, we use Newton's lemma (Thm. 7.32 in Milne).

Let $f(X) = X^2 - 17 \in \mathbb{Z}_2[X]$, $a_0 = 1 \in \mathbb{Z}_2$.

Then $|f(a_0)|_2 = \frac{1}{16} < |f'(a_0)|_2^2 = \frac{1}{4}$, so by Newton's lemma $\exists$ root of f in $\mathbb{Z}_2$.

Exercise 6

a) We define, for $y = 1+x \in U_p^1 = 1 + p\mathbb{Z}_p$,

$$\log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n} \in \mathbb{Z}_p.$$

Similarly, for $x \in \mathbb{Z}_p$, define

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \in U_p^1$$

We need to see when $\log(1+x)$ and $\exp(x)$ converges.

For $\log(1+x)$: We use the nonarchimedean convergence criterion, so that we need only check that $\left|\frac{x^n}{n}\right|_p \xrightarrow{n\to\infty} 0$, or, equivalently, $\operatorname{ord}_p\left(\frac{x^n}{n}\right) = n \operatorname{ord}_p(x) - \operatorname{ord}_p(n) \xrightarrow{n\to\infty} \infty$. Since $x \in \mathbb{Z}_p$, $\operatorname{ord}_p(x) \geq 1$, hence $n \operatorname{ord}_p(x) \geq n$, and thus $\lim_{n\to\infty} (n \operatorname{ord}_p(x) - \operatorname{ord}_p(n)) = \infty$.

So $\log(1+x)$ converges $\forall x \in \mathbb{Z}_p$.

8)

For exp: We proceed similarly as above.

Check that $\operatorname{ord}_p\left(\frac{x^n}{n!}\right) \geq n \operatorname{ord}_p(x) - \frac{n}{p-1}$

to get that $\exp(x)$ converges $\Leftrightarrow \operatorname{ord}_p(x) > \frac{1}{p-1}$

$$\Leftrightarrow |x|_p < p^{-\frac{1}{p-1}}$$

This happens $\forall\, x \in \mathbb{Z}_p$ as long as $p \neq 2$.

Thus, by general properties of log & exp, these define inverse isomophisms $U_p^1 \cong \mathbb{Z}_p$ for $p \neq 2$.

For $p=2$, we want to show $1+2\mathbb{Z}_2 \cong \{\pm 1\} \times (1+4\mathbb{Z}_2)$.

Now, by the case for exp above, exp converges on $4\mathbb{Z}_2$. So we get an isomorphism $(1+4\mathbb{Z}_2) \cong \mathbb{Z}_2$.

Now, 2-adic units are $\equiv 1$ or $-1 \bmod 4$. So we get an exact sequence

$$1 \longrightarrow \underbrace{(1+4\mathbb{Z}_2)}_{\cong U_2^2} \longrightarrow \mathbb{Z}_2^* \longrightarrow \underbrace{\mu_2}_{\cong (\mathbb{Z}/4)^*} \longrightarrow 1$$

which splits since $U_2^2 \cap \mu_2 = \{1\}$

Hence $\mathbb{Z}_2^* \cong \mu_2 \oplus U_2^2$.

b) By Hensel's lemma we know that $\mu_{p-1} \subseteq \mathbb{Q}_p$; i.e., that $\mathbb{Q}_p$ contains prime-to-p-roots of unity. So it remains to see if $\mathbb{Q}_p$ contains p^{th} root of unity.

- For $p \neq 2$, this is not the case, since then the p^{th} cyclotomic polynomial $\Phi_p(x)$ is irreducible over $\mathbb{Q}_p$ (same proof as over $\mathbb{Q}$ applies).

  Hence $\mu(\mathbb{Q}_p) = \mu_{p-1}$ if p is odd.

- For $p = 2$ we see from a) that $\mu_2 \subseteq \mathbb{Q}_2$.

c) First, p-adic valuation gives an exact sequence

$$1 \longrightarrow \mathbb{Z}_p^* \longrightarrow \mathbb{Q}_p^* \xrightarrow{ord_p} \mathbb{Z} \longrightarrow 0$$

which splits since $\mathbb{Z}$ is free.

Hence $\mathbb{Q}_p^* \cong \mathbb{Z} \oplus \mathbb{Z}_p^*$, and the second statement follows from the first.

10)

To show $\mathbb{Z}_p^* \cong \mu_{p-1} \oplus U_p^1$, note that reduction mod p gives an exact sequence

$$1 \longrightarrow U_p^1 \longrightarrow \mathbb{Z}_p^* \longrightarrow \mathbb{F}_p^* \longrightarrow 1$$

$$\mathbb{F}_p^* \cong \mu_{p-1}$$

Since $\mu_{p-1} \cap U_p^1 = \{1\}$, this yields $\mathbb{Z}_p^* \cong \mu_{p-1} \oplus U_p^1$.

d) By c), any $x \in \mathbb{Q}_p^*$ can be written uniquely as $x = \zeta p^n y$, $\zeta \in \mu_{p-1}$, $y \in U_p^1$, $n \in \mathbb{Z}$.

Since any element of U_p^1 is a square (the Taylor expansion of $\sqrt{1+t}$ converges in $\mathbb{Q}_p$ for $p \neq 2$), this defines an isomorphism

$$\mathbb{Q}_p^* / \mathbb{Q}_p^{*2} \xrightarrow{\cong} \mathbb{Z}/2\{u\} \oplus \mathbb{Z}/2\{p\}, \text{ for}$$

$u \neq 1 \in \mathbb{F}_p^* / \mathbb{F}_p^{*2}$

e) As in d) any $x \in \mathbb{Q}_2^*$ can be written uniquely as $x = 2^n u$, $u \in U_2^1$

$= \pm 2^n u'$, $u' \in U_2^2$,

so x is a square $\Leftrightarrow$ n is even and u is a square in U_2^1.

Now, for u to be a square in $\mathbb{Z}_2$ we need $a_0 \in \mathbb{Z}_2$ s.t.

$$|f(a_0)| < |f'(a_0)|^2 = \frac{1}{4}, \quad f(X) = X^2 - u.$$

$$\Leftrightarrow \quad \mathrm{ord}_2(a_0^2 - u) = 8^k$$

$$\Leftrightarrow \quad u \equiv a_0^2 \bmod 8$$

$\Leftrightarrow$ u is a square mod 8.

Representatives for $(\mathbb{Z}/8)^*$ are $\{\pm 1, \pm 5\}$, and only 1 is a square of these.

Hence a set of representatives for $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ is

$\{\pm 1, \pm 2, \pm 5, \pm 10\}$

12) Alternatively: For $x \in \mathbb{Q}_2^*$, write again $x = \pm 2^n u$, $u \in U_2^2 = 1 + 4\mathbb{Z}_2$.

Now $\sqrt{1+t} = 1 + \frac{1}{2}t - \frac{1}{8}t^2 + \cdots$ converges in $\mathbb{Q}_2 \iff t \equiv 0 \bmod 8$.

Hence any element of $U_2^3 = 1 + 8\mathbb{Z}_2$ is a square, and $x = \pm 2^n u$ is a square $\iff$ it's positive, n even, and u maps to 0 in U_2^2/U_2^3.

Now $U_2^2/U_2^3 \cong \mathbb{F}_2$, since the map

$$U_2^2 \longrightarrow \mathbb{F}_2$$
$$1 + 4y \longmapsto y$$

has kernel U_2^3.

Therefore $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \cong \mathbb{Z}/2\{-1\} \oplus \mathbb{Z}/2\{2\} \oplus \mathbb{Z}/2\{5\}$.