Algebraic Number Theory
Example Sheet 1

1. A integral domain:

$xy = 0 \Rightarrow v(xy) = \infty$.

But if $x, y \neq 0$, $v(xy) = v(x) + v(y)$

and $v(x), v(y) \in \mathbb{R}$, so $v(xy) \in \mathbb{R}$ #

v extends uniquely

$K = \operatorname{Frac} A$, $x = \frac{a}{b}$, $a, b \in A$, $b \neq 0$.

Define $v(x) = v(a) - v(b)$

Well defined since $v(cd) =$

$= v(c) + v(d)$ for $c, d \in A$.

$v(x) = \infty \Leftrightarrow x = \frac{a}{b}$ & $v(a) = \infty \Leftrightarrow$

$\Leftrightarrow x = \frac{a}{b}$, $a = 0 \Leftrightarrow x = 0$.

$v(xy) = v\left(\frac{a}{b}\frac{c}{d}\right) = v(ac) - v(bd) =$

$$= \big(v(a) - v(b)\big) + \big(v(c) - v(d)\big) =$$

$$= v(x) + v(y).$$

$$v(x+y) = v\left(\frac{a}{b} + \frac{c}{d}\right) = v\left(\frac{ad+bc}{bd}\right) =$$

$$= v(ad+bc) - v(bd) \geq$$

$$\geq \min\big(v(ad), v(bc)\big) - v(bd) =$$

$$= \min\big(v(ad) - v(bd), v(bc) - v(bd)\big) =$$

$$= \min\big(v(x), v(y)\big).$$

<u>Uniqueness</u>: Any extension has to satisfy the defining equation of our extension.

2. $|x| = 0 \iff e^{-v(x)} = 0 \iff v(x) = \infty \iff$

$$\iff x = 0.$$

$$|xy| = e^{-v(xy)} = e^{-v(x) - v(y)} = |x||y|$$

$$|x+y| = e^{-v(x+y)} \leq e^{-\min(v(x),v(y))} =$$

$$= \max(|x|,|y|).$$

The converse is similar, reversing the calculations.

3. <u>x is integral over A:</u>

The subring $A[b_1,\dots,b_n] \subseteq B$ is finite over A (i.e. a f.g. A-module) by a result in lectures.

x is integral over $A[b_1,\dots,b_n]$ by assumption, so $A[b_1,\dots,b_n,x]$ is finite over $A[b_1,\dots,b_n]$ $\Rightarrow$

$\Rightarrow$ $A[b_1,\dots,b_n,x]$ is finite over A

$\Rightarrow$ x is integral$/A$, again by the same result in lectures (the converse)

$\tilde{A}$ is a ring

If $x, y \in \tilde{A}$, then $A[x,y]$ is a ~~fg~~ finite over A, so any element of $A[x,y]$ is integral over A.

In particular, $x+y$, $xy \in \tilde{A}$.

$\tilde{A}$ is integrally closed in B

If $x \in B$ & $b_1, \ldots, b_n \in \tilde{A}$ are such that $x^n + b_1 x^{n-1} + \ldots + b_n = 0$, then $x \in \tilde{A}$ by the first part of this question.

4. (i) Induction on $n \geq 2$: $\prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i$ by definition. Need converse.

$n=2$:

~~Rec~~ Write $1 = a+b$, $a \in I_1$, $b \in I_2$.

Then if $x \in I_1 \cap I_2$, $x = xa + xb \in$
$\in I_1 \times I_2$,

$n \geq 3$.

Claim: I_1 & $\bigcap_{i=2}^{n} I_n$ are coprime.

Pf: If not, $\exists$ maximal ideal m of A s.t $I_1 + \bigcap_{i=2}^{n} I_2 \subseteq m$. But then $I_1 \subseteq m$ and $I_i \subseteq m$ for some $i \geq 2$, so I_1 and I_i are not coprime #.

Then, using the induction hypothesis and the case $n=2$,

$$\bigcap_{i=1}^{n} I_i = I_1 \cap \bigcap_{i=2}^{n} I_i = I_1 \cdot \bigcap_{i=2}^{n} I_i =$$

$$= I_1 \cdot \prod_{i=2}^{n} I_i = \prod_{i=1}^{n} I_i$$

(ii) Induction on $n \geq 2$:

$n=2$:

Write $1 = x + y$, $x \in I_1$, $y \in I_2$.

Write Φ for the map $A \longrightarrow A/I_1 \times A/I_2$

then $\Phi(x) = (0,1)$ and $\Phi(y) = (1,0)$

so if $(a,b) \in A/I_1 \times A/I_2$,

$$\Phi(ay+bx) = (a,b).$$

$\underline{n \geq 3:}$ ~~Φ~~ $A \longrightarrow \prod_{i=2}^{n} A/I_i$

is surjective by the induction hypothesis.

By the claim in part (i), I_1 & $\bigcap_{i=2}^{n} I_i$ are

coprime, so $A \longrightarrow A/I_1 \times A/\bigcap_{i=2}^{n} I_i$ is

surjective by the case $n=2$ $\Longrightarrow$

$$A \longrightarrow A/I_1 \times A/\bigcap_{i=2}^{n} I_i \longrightarrow A/I_1 \times \prod_{i=2}^{n} A/I_i$$

is surjective.

To finish (ii), note that the kernel of

$A \longrightarrow \prod_{i=1}^{n} A/I_i$ is $\bigcap_{i=1}^{n} I_i$ and use (i).

(iii) If $\mathfrak{m}_i^{e_i} + \mathfrak{m}_j^{e_j} \neq A$, then $\exists$ maximal ideal $\mathfrak{m}$ of A such that $\mathfrak{m}_i^{e_i} + \mathfrak{m}_j^{e_j} \subseteq \mathfrak{m}$. But then

$\mathfrak{m}_i^{e_i} \subseteq \mathfrak{m} \Rightarrow \mathfrak{m}_i \subseteq \mathfrak{m} \Rightarrow \mathfrak{m}_i = \mathfrak{m}$

and $\mathfrak{m}_j^{e_j} \subseteq \mathfrak{m} \Rightarrow \mathfrak{m}_j \subseteq \mathfrak{m} \Rightarrow \mathfrak{m}_j = \mathfrak{m}$

so $\mathfrak{m}_i = \mathfrak{m}_j \Rightarrow i = j$.

5. (i) One checks that it's an A-submodule of K. To show that it's a fractional ideal, we need finite generation.

Let $a \in \mathfrak{a}$, $a \neq 0$. Then $\mathfrak{a}^{-1} \subseteq (aA)^{-1} = a^{-1}A$ which is a cyclic A-module, so A Noetherian and $\mathfrak{a}^{-1} \subseteq a^{-1}A$ submodule $\Rightarrow$ $\mathfrak{a}^{-1}$ finitely generated.

(ii) Let $\mathfrak{b}_1 \supseteq \mathfrak{b}_2 \supseteq \dots \supseteq \mathfrak{a}$ be a descending chain of ideals in A. Then

$\mathfrak{b}_1^{-1} \subseteq \mathfrak{b}_2^{-1} \subseteq \dots \subseteq \mathfrak{a}^{-1}$ is an ascending chain, so it becomes stationary since $\mathfrak{a}^{-1}$ is a Noetherian A-module by (i).

To show that the original chain is descending, it then suffices to prove the following claim:

<u>Claim</u>: If $I, J \subseteq A$ are ideals and $I^{-1} = J^{-1}$, then $I = J$.

To show this, we need a lemma:

<u>Lemma</u>: $I \subseteq A$ ideal, $\mathfrak{m} \subseteq A$ maximal ideal then $(I^{-1})_{\mathfrak{m}} = (I_{\mathfrak{m}})^{-1}$

<u>Proof</u>: $(I_{\mathfrak{p}})^{-1} \supseteq (I^{-1})_{\mathfrak{p}}$ is clear.

If $y \in (I_{\mathfrak{p}})^{-1}$, then $\forall a \in I$, $s \in A \setminus \mathfrak{p}$,

$y\frac{a}{s} \in A_{\mathfrak{p}}$.

Write $ya/s = b/t$, $b \in A$, $t \in A \setminus \mathfrak{p}$.

then $(yt)a = bs \in A$

a was arbitrary, so $yt \in I^{-1} \Rightarrow y \in (I^{-1})_{\mathfrak{p}}$.

$\square$

We now return to the claim. Over PID's A the claim is clear: $xA = yA \iff x^{-1}A = y^{-1}A$.

We can now localise to get the claim in general:

If $I^{-1} = J^{-1}$, then $I_{\mathfrak{p}}^{-1} = J_{\mathfrak{p}}^{-1}$ $\forall \mathfrak{p}$ by the lemma, so $I_{\mathfrak{p}} = J_{\mathfrak{p}}$ $\forall \mathfrak{p}$ since $A_{\mathfrak{p}}$ is a PID. But then $I = J$ by Question 6(ii).

(iii) Suppose that we have distinct $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \supseteq \mathfrak{a}$.

Then $\mathfrak{p}_1 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3 \supseteq \ldots$

becomes stationary by (ii), so $\exists k$:

$$\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_k = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_k \cap \mathfrak{p}_{k+1}.$$

Then $\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_k \subseteq \mathfrak{p}_{k+1} \Rightarrow$

$\Rightarrow \exists i \leq k : \mathfrak{p}_i \subseteq \mathfrak{p}_{k+1} \Rightarrow \mathfrak{p}_i = \mathfrak{p}_{k+1}$ #.

6. (i) If $\mathfrak{a} \subseteq \mathfrak{p}$, then $\mathfrak{a}_\mathfrak{p} \subseteq \mathfrak{p}A_\mathfrak{p}$, so

$v_\mathfrak{p}(\mathfrak{a}) > 0$.

If $v_\mathfrak{p}(\mathfrak{a}) > 0$, then $\mathfrak{a}_\mathfrak{p} \subseteq \mathfrak{p}A_\mathfrak{p}$.

If $a \in \mathfrak{a}$, then $\frac{a}{1} \in \mathfrak{p}A_\mathfrak{p}$ so

$a = \frac{b}{s}$ for some $b \in \mathfrak{p}$, $s \in A \setminus \mathfrak{p} \Rightarrow$

$\Rightarrow as = b \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ since

$s \notin \mathfrak{p}$.

The last part follows from Q5(iii).

(ii) $\mathfrak{a} \subseteq \bigcap_{\mathfrak{m}} \mathfrak{a}_{\mathfrak{m}}$ is clear.

If $x \in \bigcap_{\mathfrak{m}} \mathfrak{a}_{\mathfrak{m}}$, then write $x = \frac{a_{\mathfrak{m}}}{s_{\mathfrak{m}}}$, $a_{\mathfrak{m}} \in \mathfrak{a}$, $s_{\mathfrak{m}} \in A \setminus \mathfrak{m}$ for every $\mathfrak{m}$.

Let I be the ideal generated by the $s_{\mathfrak{m}}$.
Then $I \not\subseteq \mathfrak{m}$ $\forall \mathfrak{m}$ $\Rightarrow$ $I = A$, so
$\exists$ $b_1, \ldots, b_r \in A$ and $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ s.t
$\sum_{i=1}^{r} b_i s_{\mathfrak{m}_i} = 1$.
Then $x = \sum_{i=1}^{r} b_i x s_{\mathfrak{m}_i} = \sum_{i=1}^{r} b_i a_{\mathfrak{m}_i} \in \mathfrak{a}$.

(iii) <u>Lemma</u>: If $I, J \subseteq A$ ideals, $\mathfrak{m} \subseteq A$ max ideal, then $(IJ)_{\mathfrak{m}} = I_{\mathfrak{m}} J_{\mathfrak{m}}$.

<u>Proof</u>: $(IJ)_{\mathfrak{m}} \subseteq I_{\mathfrak{m}} J_{\mathfrak{m}}$ is clear.

If ~~a~~ $a \in I$, $b \in J$, $s, t \in A \setminus \mathfrak{p}$,

then $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \in (IJ)_{\mathfrak{p}}$, so

$(IJ)_{\mathfrak{p}} \supseteq I_{\mathfrak{p}} J_{\mathfrak{p}}$. $\square$.

Now if $\mathfrak{p}, \mathfrak{q}$ are max ideals,

$$\mathfrak{p}_{\mathfrak{q}} = \begin{cases} A_{\mathfrak{q}}, & \mathfrak{q} \neq \mathfrak{p} \\ \mathfrak{q} A_{\mathfrak{q}} & \mathfrak{q} = \mathfrak{p} \end{cases}.$$

$v_{\mathfrak{q}}\left(\prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}\right) = e_{\mathfrak{q}}$ follows from this and the lemma.

<u>Last part</u>: let $\mathfrak{a} \leq A$ be an ideal and consider $\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$, this is well defined by part (i).

We then have $v_{\mathfrak{p}}(\mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a})$ $\forall \mathfrak{p}$ by the earlier part of (iii), so $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{b}_{\mathfrak{p}}$ $\forall \mathfrak{p}$.

then $\mathfrak{a} = \mathfrak{b}$ by part (ii).

7. <u>1, 2 but not 3</u>

$\mathbb{Z}[X, Y]$ is Noetherian (Hilbert basis thm) and a UFD $\Rightarrow$ integrally closed. But (X) is a prime ideal which isn't maximal.

<u>1, 3 but not 2</u>

$\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Q}(\sqrt{-3})$ is an order but not the ring of integers ($\frac{1+\sqrt{-3}}{2}$ is an algebraic integer).

<u>2, 3 but not 1</u>

Let $\overline{\mathbb{Z}}$ be the ring of algebraic integers inside $\mathbb{C}$; the field of fractions ~~is~~ is $\overline{\mathbb{Q}}$, the field of algebraic numbers.

~~Q~~ $\overline{\mathbb{Z}}$ is integrally closed (it's the integral closure of $\mathbb{Z}$ in $\overline{\mathbb{Q}}$).

If $P \overset{\neq 0}{\subseteq} \overline{\mathbb{Z}}$ is a prime ideal and $0 \neq a \in P$, then $K = \mathbb{Q}(a)$ is a number field and $P \cap \mathcal{O}_K \ni a$, so $P \cap \mathcal{O}_K$ is a maximal ideal (it's always prime).

Hence $P \cap \mathbb{Z} = (P \cap \mathcal{O}_K) \cap \mathbb{Z} = p\mathbb{Z}$ for some prime p.

The ring $\overline{\mathbb{Z}}/P$ is then integral over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (as $\overline{\mathbb{Z}}$ is integral over $\mathbb{Z}$), so it must be a field and P is maximal.

It is not Noetherian: the sequence of ideals $(2) \subseteq (2^{1/2}) \subseteq (2^{1/4}) \subseteq \ldots$

doesn't become stationary.

If it did, $(2^{1/n}) = (2^{1/2n})$ for some n

so $\exists u \in \overline{\mathbb{Z}}$ s.t. $2^{1/2n} = 2^{1/n} u \Rightarrow$

$\Rightarrow 2^{-1/n} \in \overline{\mathbb{Z}}$, but this is a contradiction.

8. ~~$v_5(4) = 0$, so~~

$\mathbb{Z}_p$ is complete under the ~~metric~~ absolute value $|x|_p = p^{-v_p(x)}$ with corresponding metric $d(x,y) = |x-y|_p$.

So $v_p(c) > 0 \Leftrightarrow |c|_p < 1$ and hence $\sum_{i=0}^{\infty} (-1)^i c^i$ converges and is an inverse to $1+c$.

2nd part: $v_5(4) = 0$, so

$v_5(4a-1) = v_5(a - 1/4)$.

$$1/4 = -\frac{1}{1-5} = -(1+5+5^2+\dots)$$

so we can take $a = -(1+5+5^2+\dots+5^9)$.

9. $x \in \mathbb{Q} \Rightarrow (a_n)_n$ periodic

We can assume $x \neq 0$. Multiplying by powers of p ~~and~~, WLOG $v_p(x) = 0$. Then, adding integers, we may assume that $-1 \leq x < 0$.

This might make $v_p(x) > 0$, if so divide by $p^{v_p(x)}$; we then have $-1 \leq x < 0$ and $v_p(x) = 0$.

Write $x = \frac{a}{b}$, $a < 0$, $b \geq 1$, $(b, p) = 1$. Then $\exists k$ s.t

$p^k \equiv 1 \mod b$ so $\exists c > 0$: ~~[illegible]~~

$p^k - 1 = bc$

then $x = \frac{a}{b} = \frac{ac}{bc} = \frac{-ac}{1-p^k}$

Set $N = -ac \geq 0$. then $N \leq p^k - 1$ since

since $x \geq -1$. Write $N = n_0 + n_1 p + \ldots + n_{k-1} p^{k-1}$

then $x = \frac{N}{1-p^k} = n_0 + n_1 p + \ldots + n_{k-1} p^{k-1} +$

$+ n_0 p^k + n_1 p^{k+1} + \ldots + n_{k-1} p^{2k-1} +$

$+ \ldots$

is periodic.

<u>Converse</u>:

WLOG $x \in \mathbb{Z}_p$. Have

$x = x_0 + x_1 p + \ldots + x_{\ell-1} p^{\ell-1} + y_0 p^{\ell} + y_1 p^{\ell+1} + \ldots$

$+ \ldots + y_{m-1} p^{\ell+m-1} + y_0 p^{\ell+m} + \ldots$

Then set $b = x_0 + x_1 p + \dots + x_{\ell-1} p^{\ell-1}$,

$c = y_0 + y_1 p + \dots + y_{m-1} p^{m-1}$,

we have $x = b + c \dfrac{p^\ell}{1-p^m} \in \mathbb{Q}$.

10. $\underline{\mathbb{Z}_7}$: Put $x = -3$:

$$(-3)^3 - 3(-4) + 4 = -14 \equiv 0 \quad (7)$$

$\rightsquigarrow$ factorization

$$x^3 - 3x + 4 = (x+3)\underbrace{(x^2 - 3x - 1)}_{\text{irreducible in } \mathbb{F}_7[x]} \mod 7$$

So $\exists$ at most one root in $\mathbb{Z}_7$, and Hensel's Lemma lifts -3 to a root.

$\underline{\mathbb{Z}_3}$: No roots mod 9.

$\underline{\mathbb{Z}_5}$: No roots mod 5.

$\underline{\mathbb{Z}_2}$: $x^3 - 3x + 4 \equiv x(x-1)^2 \mod 2$.

Hensel's Lemma $\Rightarrow$ $\exists!$ root x in $\mathbb{Z}_2$ with

$x \equiv 0 \mod 2$.

Are there any roots $\equiv 1 \mod 2$?

$x^3 - 3x + 4$ has no roots mod 4 which

are congruent to 1 or 3, so there

can't be any such root.

We conclude that ~~Therefore~~ $\exists!$ solution in $\mathbb{Z}_2$.

$\underline{11}$. $$\binom{1/2}{n} = \frac{1/2(1/2-1)\dots(1/2-n+1)}{n!} =$$

$$= 2^{-n}\frac{1(1-2)(1-4)\dots(1-2n+2)}{n!} =$$

$$= 2^{-n}(-1)^{n-1}\frac{1.3.5\dots(2n-3)}{n!} =$$

$$= 2^{-n}(-1)^{n-1}\frac{(2n-3)!}{n!\,2.4\dots(2n-4)} =$$

$$= 2^{-n}(-1)^{n-1}2^{2-n}\frac{(2n-3)!}{n!\,(n-2)!} =$$

$$= 2^{2-2n}(-1)^{n-1}\frac{1}{2n-2}\binom{2n-2}{n}$$

It follows that

$$v_p\binom{1/2}{n} = v_p\left(\frac{1}{2n-2}\right) + v_p\left(\binom{2n-2}{n}\right) \geq$$

for $p \neq 2$.

$$\geq -v_p(\cancel{2}n-1) \qquad \text{~~since~~}$$

Hence $v_p\binom{1/2}{n} \geq -v_p(n-1) \geq -\log_p(n-1)$.

<u>Claim:</u> $v_p\left(\binom{1/2}{n}\right) \not\to \infty$ as $n \to \infty$.

for $p \neq 2$.

<u>Use:</u>

If $m = \sum_{i=0}^{k} a_i p^i \in \mathbb{Z}_{\geq 1}$, $a_i \in \{0, \dots, p-1\}$,

then $$v_p(m!) = \frac{m - \sum_{i=0}^{k} a_i}{p-1}$$

Proof: Induction on m.

$m=1$ clear.

$m \Rightarrow m+1$:

Assume that $a_0, \ldots, a_\ell = p-1$ but $a_{\ell+1} \neq p-1$

(possibly $\ell = -1$, i.e. $a_0 \neq p-1$, and possibly $\ell = k$), for $m = \sum a_i p^i$.

$$\text{Then } m+1 = \left(\sum_{i=0}^{\ell} (p-1)p^i + \sum_{i=\ell+1}^{k} a_i p^i \right) + 1 =$$

$$= (a_{\ell+1}+1)p^{\ell+1} + \sum_{i=\ell+2}^{k} a_i p^i$$

So

$$v_p((m+1)!) = v_p(m+1) + v_p(m!) =$$

$$\frac{m - \left[(\ell+1)(p-1) + \sum_{i=\ell+1}^{k} a_i\right]}{p-1} + (\ell+1)$$

$$= \frac{m+1 - \left[a_{\ell+1}+1 + \sum_{i=\ell+2}^{k} a_i\right]}{p-1}$$

using the induction hypothesis

Proof of claim:

~~Set~~ For $n-2=p^k$, $n=p^k+2$, $2n-3=2p^k+1$.

Then $v_p\left(\binom{1/2}{n}\right) = v_p\left(\frac{(2n-3)!}{n!\,(n-2)!}\right) =$

$$= v_p\left((2n-3)!\right) - v_p(n!) - v_p\left((n-2)!\right) =$$

$$= \frac{2p^k+1-3}{p-1} - \frac{p^k+2-3}{p-1} - \frac{p^k-1}{p-1} =$$

$$= 0 \not\to \infty \text{ as } k \to \infty.$$

So, all in all, if $p \neq 2,3,5$, the terms of $1+\sum_{n=1}^{\infty}\binom{1/2}{n}15^n$ do not tend to 0 p-adically, so the series diverges.

If $p=3,5$, we have

$$v_p\left(\binom{1/2}{n}15^n\right) = n - v_p\left(\binom{1/2}{n}\right) \geq$$

$$\geq n - \log_p(n-1) \to \infty$$

as $n \to \infty$ (and are ≥ 0 thn) so the series converges.

Set $\alpha = 1 + \sum_{n=1}^{\infty} \binom{1/2}{n} 15^n$

to be the limit.

Then one computes $\alpha^2 = 16$ (the relevant identities for binomial coefficients hold:

$$\sum_{k=0}^{m} \binom{x}{k}\binom{y}{m-k} = \binom{x+y}{m}$$

since they hold for all $x, y \in \mathbb{Z}_{\geq 1}$ and $\mathbb{Z}_{\geq 1} \subseteq \mathbb{Z}_p$ is dense, and both sides are polynomials in x and y, hence etc.)

But $\alpha \equiv 1 \bmod 3$ in $\mathbb{Z}_3$, so $\alpha = 4$ in $\mathbb{Z}_3$, and $\alpha \equiv 1 \bmod 5$ in $\mathbb{Z}_5$, so $\alpha = -4$ in $\mathbb{Z}_5$.

12(i) $x = y^2$ in $\mathbb{Z}_p \Rightarrow x = y^2 \bmod p$, giving one implication.

<u>Converse:</u> Consider $T^2 - x \in \mathbb{Z}_p[T]$.

$x \not\equiv 0 \bmod p$, so $T^2 - x$ has distinct roots mod p ($p \neq 2$), and has a root by assumption.

Hensel's Lemma $\Rightarrow T^2 - x$ has a root in $\mathbb{Z}_p$.

<u>Last part:</u> If $x \in \mathbb{Q}_p^\times$, write $x = p^n u$, $n \in \mathbb{Z}$, $u \in \mathbb{Z}_p^\times$.

Then x square in $\mathbb{Q}_p^\times \Leftrightarrow$

$\Leftrightarrow$ n even and u is a square in $\mathbb{Z}_p^\times$

$\Leftrightarrow$ n even and $u \bmod p$ is a square in $\mathbb{F}_p^\times$.

(ii) Let $a, b \in \mathbb{Q}_p^\times \setminus (\mathbb{Q}_p^\times)^2$

<u>Claim</u>: $\mathbb{Q}_p(\sqrt{a}) = \mathbb{Q}_p(\sqrt{b}) \Leftarrow$

$\Leftrightarrow \quad a \equiv b \mod (\mathbb{Q}_p^\times)^2$.

<u>Pf</u>: ($\Rightarrow$) : $\mathbb{Q}_p(\sqrt{a}) = \mathbb{Q}_p(\sqrt{b}) \Rightarrow$

$\Rightarrow \sqrt{a} = x + y\sqrt{b}$ for some $x, y \in \mathbb{Q}$.

Looking at traces $\Rightarrow x = 0$, so

$a = (\sqrt{a})^2 = y^2 b$.

($\Leftarrow$) : If $a = y^2 b$, then ~~...~~ $(y\sqrt{b})^2 = a$

so $\mathbb{Q}_p(\sqrt{a}) = \mathbb{Q}_p(\sqrt{b})$ $\square$

So $\#\left\{\begin{matrix}\text{distinct quadratic} \\ \text{ext'ns of } \mathbb{Q}_p\end{matrix}\right\} = \#\left(\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2\right) - 1$

(number of non-zero elements in $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$)

Have $\mathbb{Q}_p^\times \cong \langle p \rangle \times \mathbb{Z}_p^\times$ so

$p^n u \longleftrightarrow (p^n, u)$

$$(\mathbb{Q}_p^\times)^2 \cong \langle p^2 \rangle \times (\mathbb{Z}_p^\times)^2 \implies$$

$$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \cong \underbrace{\frac{\langle p \rangle}{\langle p^2 \rangle}}_{\cong \mathbb{Z}/2\mathbb{Z}} \times \frac{\mathbb{Z}_p^\times}{(\mathbb{Z}_p^\times)^2}$$

Now $\dfrac{\mathbb{Z}_p^\times}{(\mathbb{Z}_p^\times)^2} \xrightarrow[\text{reduction mod } p]{\sim} \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2$

by part (i), and $\# \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2 = 2$

since $\mathbb{F}_p^\times$ is cyclic, so

$$\# \left(\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \right) = 4 \implies$$

$\implies \exists$ 3 distinct quadratic extn's of $\mathbb{Q}_p$.

$\underline{p=2}$: Claim holds for $p=2$ with the same proof, so need to compute $\#(\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2)$

Again $\mathbb{Q}_2^\times \cong \langle 2 \rangle \times \mathbb{Z}_2^\times$, so

$$\#\left(\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2\right) = 2 \cdot \#\left(\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2\right).$$

<u>Claim:</u> $x \in \mathbb{Z}_2^\times$ is a square $\iff$ it is a square mod 8.

<u>Pf:</u> $\Rightarrow$ is clear

$\Leftarrow$: We use Newton-Raphson as in the proof of Hensel's Lemma. Set $a_1 = 1$,

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$$

for $n \geq 1$ where $f(T) = T^2 - x$

We claim that

1) $a_n \in \mathbb{Z}_2$,

2) $v_2(f'(a_n)) = v_2(f'(a_1))$

3) $v(f(a_n)) \geq 2v(f'(a_n)) + 2^{n-1}$

for all $n \geq 1$. For $n = 1$ this is clear.

Induction step:

1) $$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)} \in \mathbb{Z}_2$$

using 1) + 3) for n.

2) $$f'(a_{n+1}) - f'(a_n) = 2(a_{n+1} - a_n) =$$

$$= -2 \frac{f(a_n)}{f'(a_n)}, \quad \text{so}$$

$$v_2(f'(a_{n+1}) - f'(a_n)) \geq v_2(f(a_n)) -$$

$$- v_2(f'(a_n)) \geq$$

$$\geq v_2(f'(a_n)) + 1$$

by 3) for n, so

$$v_2(f'(a_{n+1})) = v_2(f'(a_n)) = v_2(f'(a_1))$$

using 2) for n.

3) $$f(a_{n+1}) = f(a_n) + (a_{n+1} - a_n) f'(a_n) +$$

$$+ (a_{n+1} - a_n)^2 =$$

$$= \frac{f(a_n)^2}{f'(a_n)^2}, \quad \text{so}$$

$$v_2(f(a_{n+1})) = 2v_2(f(a_n)) - 2v_2(f'(a_n)) \geq$$

$$\geq 2v_2(f'(a_n)) + 2^n =$$

$$= 2v_2(f'(a_{n+1})) + 2^n$$

using 3) for n to get the inequality and 2) for n+1 to get the last equality.

This implies that a_n converges to a root of f, i.e a square root of x.

Therefore $\mathbb{Z}_2^\times / (\mathbb{Z}_2^\times)^2 \cong (\mathbb{Z}/8)^2 \cong$

$$\cong \mathbb{Z}/2 \times \mathbb{Z}/2$$

$\Rightarrow$ we have 7 distinct quadratic ext's of $\mathbb{Q}_2$.

13. <u>Valuations on $\mathbb{Q}$:</u>

v normalised valuation on $\mathbb{Q}$.

Then $\{x \in \mathbb{Q} \mid v(x) \geq 0\} \supseteq \mathbb{Z}$,

since $v(1) = 0 \Rightarrow v(n) \geq 0 \ \forall n$.

Therefore $I = \{x \in \mathbb{Z} \mid v(x) > 0\}$ is a

prime ideal of $\mathbb{Z}$. ($I \neq 0$ since

v is non-trivial) $\Rightarrow I = p\mathbb{Z}$ for some

prime p. v normalised $\Rightarrow$ must have

$v(p) = 1$ and $v(p^n x) = n$ if $(x, p) = 1$,

so $v = v_p$.

<u>Note:</u> The argument show the following:

If A is a PID, v a normalised valuation

on $K = \operatorname{Frac} A$ such that $v(x) \geq 0 \ \forall x \in A$,

then $v = v_\pi$ for some prime $\pi \in A$.

Valuations on $\mathbb{F}_p(T)$

Let v be a normalised valuation ~~of~~ on $\mathbb{F}_p(T)$.

Two cases:

1) $v(T) \geq 0$:

then $v(f(T)) \geq 0 \;\; \forall f \in \mathbb{F}_p[T]$.

By the note, we must have $v = v_g$ for some irreducible $g \in \mathbb{F}_p[T]$.

2) $v(T) < 0$:

then $v\left(\frac{1}{T}\right) > 0 \implies$

$\implies v(f) \geq 0 \;\; \forall f \in \mathbb{F}_p[\frac{1}{T}] \subseteq \mathbb{F}_p(T)$

By the note, $v = v_g$ for some irreducible $g \in \mathbb{F}_p[{}^1/_T]$. But $v\left(\frac{1}{T}\right) > 0$ and ${}^1/_T$ is irreducible in $\mathbb{F}_p[{}^1/_T]$, so

$v = v_{1/T}$.

We can describe this valuation on $\mathbb{F}_p[T]$ by

$v_{1/T}(h(T)) = -\deg h$, for $h \in \mathbb{F}_p[T]$.