Algebraic Number Theory - ex. sheet 1.

Q1. If R is Noetherian, then (by Thm 1.2) it is a PID, hence by Prop. 1.4 is a DVR.

Q2. $R \subset K$ a valuation ring which is a maximal proper subring. Want valuation v st $R = R_v = \{x \in K \mid v(x) \geq 0\}$

Let $0 \neq \pi \in m_R$. Then $\frac{1}{\pi} \notin R$ so by maximality of R, $R[1/\pi] = K$. In particular, for any $x \in K$, $\exists n \in \mathbb{N}$ with $\pi^n x \in R$

Define v by:

$$v(x) = \sup\left\{\frac{a}{b} \in \mathbb{Q},\ b>0 \ \middle|\ \pi^{-a}x^b \in R\right\}.$$

By above, if $x \in K^*$ then $v(x) \in \mathbb{R}$ exists, and $v(0) = +\infty$.

Check $v(x+y) \geq \min(v(x), v(y))$:

If $v(x), v(y) \geq \frac{a}{b}$ then $\pi^{-a}x^b, \pi^{-a}y^b \in R$.

$\therefore \forall\, 0 \leq i \leq b$, $R \ni (\pi^{-a}x^b)^i (\pi^{-a}y^b)^{b-i} = \pi^{-ab}(x^i y^{b-i})^b$

$\therefore$ (R integrally closed) $\pi^{-a}x^i y^{b-i} \in R$.

So $\pi^{-a}(x+y)^b = \sum \binom{b}{i} . \pi^{-a} x^i b^{-i} \in R$

ie, $v(x+y) \geq a/b$.

Check $v(xy) = v(x) + v(y)$:

If $v(x)+v(y) > \alpha \in \mathbb{Q}$, then can write $\alpha = \frac{a+c}{b}$,

$a/b < v(x)$ and $c/b < v(y)$, so $\pi^{-a}x^{b}$ and $\pi^{-c}y^{b} \in R$

$\Rightarrow \pi^{-(a+c)}(xy)^b \in R$

$\Rightarrow v(xy) \geq \alpha$.

$\therefore v(xy) \geq v(x) + v(y)$. Conversely, suppose that

$v(xy) > \alpha > v(x) + v(y)$, $\alpha \in \mathbb{Q}$.

Then can write $\alpha = \frac{a+c}{b}$ with $a/b > v(x)$, $c/b > v(y)$.

Then $\alpha < v(xy) \Rightarrow \pi^{-a-c}(xy)^b \in R$. (1)

$a/b > v(x) \Rightarrow \pi^{-a}x^b \notin R$, so $\pi^{a}x^{-b} \in R$. (2)

(1), (2) $\Rightarrow \pi^{-c}y^b \in R$, contradicting $c/b > v(y)$.

So v is a valuation. Obviously $R \subset R_v$, so as R is maximal, $R = R_v$.

Q3. Suppose $(x_n) \longrightarrow x \neq 0$, so $|x| = c > 0$. Then $\exists N$ s.t. $\forall n \geq N$, $|x_n - x| < c$. Now $x_n = (x_n - x) + x$

so if $n \geq N$, $|x_n| = \max\{|x_n - x|, |x|\} = c$.

So as the AV on $\hat{K}$ is given by

$|(x_n)| = \lim |x_n|$, $|(x_n)| \in |K^*|$ i.e. $|\hat{K}^*| = |K^*|$.

Q4. $F = \{ f = \sum_{n \geq 0} a_n T^{r_n} \mid a_n \in k,\ r_n \in \mathbb{Q},\ r_0 < r_1 < \dots < r_n \to \infty \}$.

Let $f, g \in F$. WLOG we can write

$$f = \sum a_n T^{r_n}, \quad g = \sum b_n T^{r_n}, \quad r_0 < \dots < r_n \to \infty$$

(adding suitable zero terms to f, g if necessary).

Define $f + g = \sum (a_n + b_n) T^{r_n} \in F$

Consider the set $S = \{ r_i + r_j \mid i, j \geq 0 \}$

- as $(r_n) \to \infty$, can write $S = \{ s_n \mid n \geq 0 \}$ with

$s_0 < s_1 < \dots < s_n \to \infty$, and for any n,

$I_n = \{ (i, j) \mid r_i + r_j = s_n \}$ is finite.

Then define $fg = \sum c_n T^{s_n}$

where $c_n = \sum_{(i,j) \in I_n} a_i b_j$.

Then F is a ring under $+$ and $\times$. For inverses:

clearly any T^r is invertible, so STP

$$f = \sum a_n T^{r_n}, \quad r_n = 0,\ a_n = 1$$

is invertible; but $f^{-1} = \sum_{m \geq 0} (1 - f)^m \in F$.

It's routine to check v is a valuation.

Obviously $v(F^*) = \mathbb{Q}$, and R_v is the set of f with $r_n < 0 \Rightarrow a_n = 0$. Finally, F is complete w.r.t. v: let (f_i) be a Cauchy sequence. Replacing by a subsequence, may assume $v(f_i - f_j) > i$ if $j > i$.

Then if $r \le i$, the coefficient of T^r in f_i equals that in f_j for all $j \geq i$. Let this common coefficient be a_r. So $a_r = 0$ for all but finitely many $r \le i$.

Then $(f_i) \longmapsto \sum a_r T^r \in F$

Q5 (i) Chinese remainder thm: $\mathbb{Z}/M^n\mathbb{Z} \simeq \prod \mathbb{Z}/p_i^{nr_i}\mathbb{Z}$.

where $M = \prod p_i^{r_i}$.

$\therefore \varprojlim \mathbb{Z}/M^n\mathbb{Z} = \prod_i \varprojlim \mathbb{Z}/p_i^{nr_i}\mathbb{Z}$

and $\varprojlim \mathbb{Z}/p^{nr}\mathbb{Z} = \mathbb{Z}_p$ as long as $r > 0$.

(ii) $\hat{\mathbb{Z}} \xrightarrow{\varphi} \prod_p \mathbb{Z}_p$ by $(x_n)_n \longmapsto ((x_{p^r})_r)_p$.

is a homomorphism.

If $\varphi(x) = 0$ then $x = (x_n)$, $x_{p^r} = 0$ $\forall$ prime powers p^r.

So if $n = \prod p_i^{r_i}$, then as $\pi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p_i^{r_i}\mathbb{Z}$

maps x_n to $x_{p_i^{r_i}}$, we have

$$(x_n \bmod p_i^{r_i}) = 0 \quad \forall i \quad \Rightarrow \quad x_n = 0.$$

by C.R.T.

$\therefore \varphi$ injective. For surjectivity: let $(y_p) \in \prod_p \mathbb{Z}_p$.

and let $x_{p^r} = (y_p \bmod p^r) \in \mathbb{Z}/p^r\mathbb{Z}$. By CRT, for

every $n = \prod p_i^{r_i}$ $\exists!\, x_n \in \mathbb{Z}/n\mathbb{Z}$ s.t. $x_n \bmod p_i^{r_i} = x_{p_i^{r_i}}$.

and $(x_{p^{r+1}} \bmod p^r) = x_{p^r} \Rightarrow (x_{nd} \bmod n) = x_n \quad \forall n, d.$

so $x = (x_n) \in \hat{\mathbb{Z}}$ with $\varphi(x) = (y_p)_p$.

(iii) Let $d(x,y) = \max\left(|x-y|_2, |x-y|_3\right)$.

Obviously d is a metric. Claim completion of $\mathbb{Q}$ w.r.t d

is $\mathbb{Q}_2 \times \mathbb{Q}_3$ with metric $\hat{d}((x,x'),(y,y'))$

$$= \max\left(|x-y|_2, |x'-y'|_3\right)$$

$x, y \in \mathbb{Q}_2$
$x', y' \in \mathbb{Q}_3$.

Clearly $(\mathbb{Q}_2 \times \mathbb{Q}_3, \hat{d})$ is complete, and the

diagonal map $\mathbb{Q} \hookrightarrow \mathbb{Q}_2 \times \mathbb{Q}_3$ is an isometry, Let $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_3$; then $\exists (x_n), (y_n)$

sequences in $\mathbb{Z}$ with $v_2(x_n - x), v_3(y_n - y) \geq n$.

By CRT $\exists z_n \in \mathbb{Z}$ with $z_n \equiv \begin{cases} x_n & \text{mod } 2^n \\ y_n & \text{mod } 3^n \end{cases}$

$\Rightarrow (z_n) \to x$ 2-adically $\Rightarrow (z_n, z_n) \to (x, y)$
$\qquad\quad \to y$ 3-adically $\qquad$ in $(\mathbb{Q}_2 \times \mathbb{Q}_3, \hat{d})$.

If $(x, y) \in \mathbb{Q}_2 \times \mathbb{Q}_3$, $\exists m$ st $(6^m x, 6^m y) \in \mathbb{Z}_2 \times \mathbb{Z}_3$

– so $\exists$ $z_n \in \mathbb{Z}$ with $(z_n, z_n)_n \to (6^m x, 6^m y)$

$\Rightarrow \left(\frac{1}{6^m} z_n, \frac{1}{6^m} z_n\right)_n \to (x, y)$.

$\square$

Q6. (i) Suppose $|x - y| < |x - z| < |y - z|$.

$$y - z = (x - z) + (y - x)$$

$\Rightarrow |y - z| \leq \max(|x - z|, |y - x|)$ – contradiction.

(ii) Let $y \in \overline{B}_r(x)$. Then $|y - x| \leq r$.

So if $|y - z| \leq r$, $|z - x| \leq \max(|z - y|, |y - x|) \leq r$.

$\Rightarrow \overline{B}_r(y) \subset \overline{B}_r(x)$ ie. $|x - y| \leq y \Rightarrow \overline{B}_r(y) = \overline{B}_r(x)$.

In partic, $\forall y \in \overline{B}_r(x)$, $B_r(y) \subset \overline{B}_r(x)$ ie. $\overline{B}_r(x)$ is open.

Q7. <u>Suppose R compact.</u>

i) K is complete: any Cauchy seq. (x_n) in K is bounded

say $|x_n| \leq C$. Choose $y \in K^*$ with $|y| \geq C$.

Then $|x_n/y| \leq 1$ i.e. $x_n' = x_n/y \in R$. R compact

$\Rightarrow R$ complete $\Rightarrow (x_n') \to x' \in R \Rightarrow (x_n) \to y.x' \in K$.

ii) v is discrete, $k = R/m_R$ finite:

Let $\pi \in m_R \setminus 0$. Then $\pi R \subset R$ is open,

so by coset decomp. $R = \coprod_{a \in R/\pi R} a + \pi R$, R compact

$\Rightarrow R/\pi R$ finite. This means k is finite.

If $x, y \in R$ with $0 \leq v(x) < v(y) < v(\pi)$ then

$x + \pi R \neq y + \pi R$ (by Δ inequality)

So $v(K^*) \cap [0, v(\pi))$ is finite $\Rightarrow v$ discrete.

In other direction: if K is complete & discretely valued,

$R \cong \varprojlim R/\pi_K^n R$; $R/\pi_K R$ finite $\Rightarrow R/\pi_K^n R$ finite $\forall n$

$\Rightarrow \varprojlim$ compact

[OR: K complete, $R \subset K$ closed $\Rightarrow R$ complete.

v = disc. valuation, AV $|\cdot|$ $\Rightarrow R = \coprod_{a \in R/\pi^n R} a + \pi^n R$

union of finite # of balls of radius $|\pi|^n$. So R totally bounded, hence compact.]

Q8. (i) Let $X = \varprojlim X_n \xrightarrow{pr_n} X_n$.

If all $\pi_n : X_n \to X_{n-1}$ are surjective, then by axiom of choice pr_n is surjective $\forall n$.

By def^n of inv. limit topology, pr_n is cts. for discrete top. on X_n. So $X_n = pr_n(X)$ is compact $\Rightarrow X_n$ finite.

(ii) X_n all finite: $X_n' = \bigcap_{m \geq n} \mathrm{im}(X_m \to X_{m-1} \to \dots \to X_n)$, with the composite labelled $\pi_{m,n}$

As X_n is finite, the sequence of sets $\pi_{m,n}(X_m)$ stabilises: ie $\exists m(n)$ st. $\forall m \geq m(n)$ $\pi_{m,n}(X_m) = X_n'$.

But then $\pi_n(X_n') = \pi_{m,n-1}(X_m)$ for every $m \geq m(n)$.

So $\pi_n(X_n') = X_{n-1}'$.

Obviously $\varprojlim X_n' \subset \varprojlim X_n$; and if $(x_n) \in \varprojlim X_n$

then $x_n = \pi_{m,n}(x_m) \in \pi_{m,n}(X_m)$ for all m

$\Rightarrow x_n \in X_n'$,

Q9. (i) $H \subset X$ open sgp. $\Rightarrow$ $H \supset pr_n^{-1}(1)$ for some n.

As $pr_n^{-1}(1) = \ker(pr_n : X \to X_n)$, it has finite index, hence so does H.

Let $H \subset X$ be closed of finite index. Then $X = \coprod_{i=1}^{n} x_i H$ say, $x_1 = e$. Each $x_i H$ is closed. So

$H = X \setminus \coprod_{i \neq 1} x_i H$ is open.

(ii) $X = \mathbb{F}_p^{\mathbb{N}} \cong \varprojlim_n \mathbb{F}_p^n$ $\quad \pi_n : \mathbb{F}_p^n \longrightarrow \mathbb{F}_p^{n-1}$

$(x_1, \ldots, x_n) \longmapsto (x_1, \ldots, x_{n-1})$.

Let $Y = \mathbb{F}_p^{(\mathbb{N})} = \{(a_n) \in \mathbb{F}_p^{\mathbb{N}} \mid \text{all but fin. many } a_n = 0\}$.

- Y is <u>dense</u> (as $Y \overset{pr_n}{\twoheadrightarrow} \mathbb{F}_p^n \ \forall n$).
- Zorn's lemma $\Rightarrow$ $Y \subset V \subset X$, $\dim_{\mathbb{F}_p}(X/V) = 1$.

Q10: If $p = 3$ or 5:

- $\binom{1/2}{n} \in \mathbb{Z}_p$, so $\underbrace{1 + \sum \binom{1/2}{n} 15^n}_{x_p}$ is cvgt. in $\mathbb{Z}_p$
- $x_p \equiv 1 \pmod p$
- $\left(1 + \sum \binom{1/2}{n} x^n\right)^2 = 1 + x$ as formal power series

$$\left(1 + \sum \binom{1/2}{n} x^n\right)^2 = 1 + x + \sum_{n \geq 2} \left(\sum_{k=0}^{n} \binom{n}{k} \binom{1/2}{k} \binom{1/2}{n-k} \right) x^n$$

<u>ie.</u> $c_n = 0 \quad \forall n \geq 2$.

$\therefore x_p^2 = 1 + 15 + \sum_{n \geq 2} c_n 15^n = 16$. $\therefore x_3 = 4, \ x_5 = -4$.

Q 11 $f(x) \equiv 0 \ (p^n)$, $v_p(f'(x)) = m$, $2m < n$

Find x' with $x' \equiv x \mod p^{n-m}$, $f(x') \equiv 0 \ (p^{n+1})$

$n-m > m \Rightarrow v_p(f'(x')) = m$ & can repeat.

Put $x' = x + p^{n-m} z$.

$$f(x') = f(x) + p^{n-m} z f'(x) + \sum_{r \geq 2} p^{(n-m)r} \cdot z^r \cdot \frac{f^{(r)}(x)}{x!}$$

$f \in \mathbb{Z}_p[T] \Rightarrow \dfrac{f^{(r)}(T)}{r!} \in \mathbb{Z}_p[T]$ $\left(\left(\frac{d}{dT}\right)^r (T^N) = r! \binom{N}{r} T^{N-r} \right)$

Let $f'(x) = p^m a$, $a \in \mathbb{Z}_p^\times$.

Let $z \in \mathbb{Z}$ with $-az \equiv \dfrac{f(x)}{p^n} \mod p$.

$v_p(p^{(n-m)r}) = (n-m)r > n$ if $r \geq 2$.

$$\therefore f(x') \equiv f(x) + azp^n \mod p^{n+1}$$
$$\equiv 0 \mod p^{n+1}.$$

$\square$

Q 12 (a) v extends to a complete valn. of any finite extension of K.

(b) $g(X) = cf(dX) = \sum_{i=0}^{n} b_i X^i$ say

$b_i = c d^i a_i$.

So the Newton polygon of g (regarded as a PL function $[0,n] \to \mathbb{R}$) is the NP of f plus the linear function $i \mapsto v(c) + i v(d)$.

So slopes & lengths of NP of g are $(s_j + v(d), \ell_j)$

and if $f(x)=0$, $v(x) = -s$ then $g(d^{-1}x) = 0$, $v(d^{-1}x) = -(s+v(d))$.

So result holds for $f \iff$ it holds for g.

& taking $d = -1/(\text{largest root of } f)$, $c = f(0)^{-1}$

have WLOG $f = \prod (1+\alpha_i T)$, $\alpha_n = 1$, $0 \neq \alpha_i \in \mathcal{O}_K$.

(c) Say $f = (1+T)g$, all roots of g in $\mathcal{O}_K \setminus 0$.

and $g = b_0 + b_1 T + \dots + b_{n-1} T^{n-1}$, $b_i \in \mathcal{O}_K$, $b_0 = 1$

Then $f = \sum_{i=0}^{n} a_i T^i$, $a_i = b_i + b_{i-1}$ $1 \leq i \leq n-1$
$a_0 = 1$. $a_n = b_{n-1}$.

Slopes of NP of g are all ≥ 0. So if $(k, v(b_k))$ (for $k \geq 1$) is a vertex of NP of g, $v(b_{k+1}) > v(b_k)$ and so $v(a_{k+1}) = v(b_k)$. In general, $v(a_{k+1}) \geq \min(v(b_k), v(b_{k+1}))$

Also, if 0 is not a slope of NP of g, then $v(a_1) > 0 = v(a_0)$ so $v(b_1) = v(a_0)$.

Want to show NP of f = NP of g shifted to the right by one. So are reduced to:

Let $0 = v_0, v_1, \dots, v_n \in \mathbb{R}_{\geq 0}$.

P = convex hull of $\{(-1,0), (0,v_0), \dots, (n,v_n)\}$.

Let $w_0, \dots, w_{n-1}, w_n = v_n$ st. $\forall k \in \{0, \dots, n-1\}$

$w_k \geq \min(v_k, v_{k+1})$

$=$ " if (k, v_k) is a vertex of P.

Then the convex hull of $\{(-1,0), (i,w_i)_{0 \leq i \leq n}\}$ equals P.

If we replace v_i with v_i', where (i, v_i') lies on the P, then (w_i) still satisfy the inequalities. So WLOG may assume (k, v_k) lies on P for all k.

But then $w_k \geq v_k$ for all k, and $w_k = v_k$ if (k, v_k) is a vertex, so conclusion is obvious.

(i) f irr/K. Let x_i = {roots of f} (in some ext^{n} field). Then $K(x_i) \cong K(x_j)$ so (by uniqueness of extns of AVs) $v(x_i) = v(x_j)$, and so NP has only one slope.

(ii) Let $g \mid f$, $\deg g = d$. Then g has d roots, all with $v_K(x) = m/n$. So $g(0)$ has valuation md/n, which is not an integer unless $d = 0$ or n <u>ie</u>. $g = 1$ or f

(NP of Eisenstein poly has 1 slope, $\frac{1}{n}$.)