Série 3 Exercice 8

David Wiedemann

27 mars 2022

1

Indeed, let $\frac{a}{b} \in \mathbb{Q}$ in reduced form such that $\nu_p(\frac{a}{b}) = 0$. By the definition of p-adic valuation, this means that we may suppose both a and b share no common factors with p, then $\frac{b}{a}$ also shares no common factor with p and hence $\nu_p(\frac{b}{a}) = 0$, implying $\frac{b}{a} \in R_\nu$.
Finally, $\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1}$ which finally implies that $\frac{a}{b}$ is invertible in R_ν.

2

First we show that all (p^n) are distinct ideals of R, indeed suppose there exists $a, b \in \mathbb{N}$ such that $(p^a) = (p^b)$, without loss of generality suppose $a < b$.
Hence, there exists an element $\frac{x}{y} \in \mathbb{Q}$ with $\nu_p(\frac{x}{y}) \geq 0$ such that $\frac{x}{y}p^b = p^a$.
As $\mathbb{Q}$ is a field, this implies that $\frac{x}{y} = p^{a-b}$ which means $\frac{x}{y}$ has a negative valuation which contradicts our hypothesis.

Now we show that the ideals mentionned in the exercise are indeed all the ideals of R.
Let I be an non-zero ideal of R.
Define $a = \inf_{x \in I \setminus \{0\}} \{\nu(x)\}$. Since $\nu|_{I\setminus\{0\}}$ has codomain $\mathbb{N}$, this infimum exists and is attained by some element $y \in I$.
Note that we may write $y = p^a \frac{d}{c}$ where d and c are coprime to p.
By part 1, we know that $\frac{d}{c}$ is invertible, hence implying that (since I is an ideal) $p^a \in I$.

We pretend that $I = (p^a)$, to do this, we show the double inclusion.
First, note that, since by construction $p^a \in I$, we immediatly get that $(p^a) \subset I$ since (p^a) is the smallest ideal containing p^a.
Furthermore, let $x \in I$, then by definition of a, $\nu(x) \geq a$.
We may then write $x = p^{\nu(x)} \frac{d}{c} = p^a p^{\nu(x)-a} \frac{d}{c}$ where d and c are coprime to p, this implies that $x \in (p^a)$.

Hence, if I is a non-zero ideal, I is of the form p^n for some n and since these ideals are disjoint, we have characterised all of them.

3

Using the exercise of week 2, we know that $\mathbb{Z} \subset R$.
Hence consider the composition $\mathbb{Z} \overset{\iota}{\hookrightarrow} R \overset{q_R}{\longmapsto} {}^{R}\!/_{(p^n)}$ where ι is the inclusion morphism and q_R is the canonical projection morphism.
Furthermore define $q : \mathbb{Z} \to {}^{\mathbb{Z}}\!/_{(p^n)}$ to be the canonical projection.
We now pretend that $\ker(q_R \circ \iota) = \ker q = (p^n)$.

Indeed if $a \in \ker q = (p^n)$, then $p^n | a$ hence $p^n | \iota(a) \implies q_R(\iota(a)) = 0$.

Similarly, now suppose $r \in \ker(q_R \circ \iota)$, this means that $\iota(r) \in \ker q_R = (p^n)$ (where now $(p^n) \subset R$).
Hence there exists $\frac{a}{b} \in R$ (where we suppose $\gcd(a, b) = 1$ without loss of generality) such that $p^n \frac{a}{b} = \iota(r)$.
Now, since $\frac{a}{b} \in R$, $\nu(\frac{a}{b}) \geq 0$ which implies in particular that b is coprime to p.
Hence, since $\iota(r)$ is an integer, $\frac{a}{b}$ has to be an integer which implies $b = 1$.
Thus $p^n a = \iota(r) \implies p^n a = r$ (in $\mathbb{Z}$), ie. $r \in (p^n) \subset \mathbb{Z}$.

Hence applying the universal property of the quotient ring, we get an induced morphism as such :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{q_R \circ \iota} & {}^{R}\!/_{(p^n)} \\ {\scriptstyle q}\downarrow & \nearrow_{\exists! \varphi} & \\ {}^{\mathbb{Z}}\!/_{(p^n)} & & \end{array}$$

We pretend that it is now sufficient to show that $q_R \circ \iota$ is surjective to show that ϕ is indeed an isomorphism.
Before showing that $q_R \circ \iota$ is surjective, we show how this implies ϕ is an isomorphism.
Indeed, if $q_R \circ \iota$ is surjective, then

$${}^{R}\!/_{(p^n)} \simeq \operatorname{Im} q_R \circ \iota \underbrace{\simeq}_{\text{by first isom. theorem}} {}^{\mathbb{Z}}\!/_{\ker q_R \circ \iota} \underbrace{\simeq}_{\text{since } \ker q_r \circ \iota = (p^n)} {}^{\mathbb{Z}}\!/_{(p^n)}$$

We now show that $q_R \circ \iota$ is surjective.
Let $[p^i \frac{a}{b}] \in {}^{R}\!/_{(p^n)}$, where, again, we assume $\frac{a}{b}$ is in reduced form and shares no factors with p.

To show this, we must find an integer $d \in \mathbb{Z}$ such that

$$\frac{a}{b}p^i - d = kp^n, \quad k \in R$$

where by abuse of notation, we regard d as included in R.
Indeed, then $q_R(\frac{a}{b}p^i) = q_R(d)$ which will imply that $q_R \circ \iota$ is surjective.
Using that p^n and b are coprime, choose x and d integers such that $xp^n + db = ap^i$, such x and d always exist because of Bezout's theorem.
Now set $k = \frac{x}{b}$, note that $k \in R$ since b is coprime to p.
It is now immediatly verified that

$$\frac{a}{b}p^i - d = kp^n$$

Since

$$ap^i = kp^n b + db = xp^n + db$$

Hence $\frac{a}{b}p^i$ has a representative in $\mathbb{Z}$ which in turn implies that $q_R \circ \iota$ is surjective, concluding our proof.

4

To show this, we proceed by contradiction.
So suppose there exist two different prime numbers $p \neq q$ such that $R_p \simeq R_q$.
Note that an isomorphism of rings induces a bijection between the set of ideals which respects inclusion.
To declutter this proof, I prove this at the end of the document.
So let $\psi : R_p \to R_q$ be the isomorphism we assume to exist, using part 2, we know that all ideals of R_p are of the form (p^n).
Furthermore, we notice that these ideals are nicely ordered :

$$(p) \supsetneq (p^2) \supsetneq \dots$$

Applying ϕ to this chain yields a chain of ideals in R_q

$$\phi((p)) \supsetneq \phi((p^2)) \supsetneq \dots$$

Using the result cited above, this immediatly implies that $\psi((p^i)) = (q^i)$.
In particular, (p) is a maximal ideal and ϕ takes maximal ideals to maximal ideals, hence we get that $\phi(p) = (q)$.
Since R_p and R_q are supposed isomorphic, we would need to have that $R_p/(p) \simeq R_q/(q)$ are isomorphic.
Indeed, consider $q_q \circ \psi : R_p \to R_q/(q)$ the composition of the isomorphism with the canonical quotient map and $q_p : R_p \to R_p/(p)$ since $(p) = \psi^{-1}((q))$ and $q_q \circ \psi$ is surjective, we conclude by the first isomorphism theorem that

$R_{p\diagup(q)} \simeq R_{q\diagup(q)}$.
Using part 3, this would imply that $\mathbb{Z}\diagup(q) \simeq \mathbb{Z}\diagup(p)$ which is a contradiction, since they are not even in bijection as sets.

We now show the result cited at the beginning of part 4.
So let $\phi : A \to B$ be an isomorphism of rings and let $I \subset A$ be an ideal, then $\phi(I)$ is an ideal since :

— Clearly $\phi(I)$ is an additive subgroup since $\phi(0) = 0 \in \phi(I)$ and $\phi(a) + \phi(b) = \phi(a + b) \in \phi(I)$.

— Let $\lambda \in B$ and $\phi(a) \in \phi(I)$, then $\lambda\phi(a) = \phi(\phi^{-1}(\lambda))\phi(a) = \phi(\underbrace{\phi^{-1}(\lambda)a}_{\in I}) \in \phi(I)$.

This correspondence is clearly a bijection between the ideals of A and B since ϕ is a bijection and the correspondence obviously preserves inclusions since maps of set preserve inclusions.
In particular, if m is a maximal ideal, then $\phi(\mathrm{m})$ is maximal since if $B \supsetneq J \supsetneq \phi(\mathrm{m})$, then $A \supsetneq \phi^{-1}(J) \supsetneq \mathrm{m}$.