Homework 18 - MATH 791

Will Thomas

The problems in this homework set deal with a special kind of PID. Let R be a principal ideal domain with the property that, given any two prime elements, π_1 and π_2, $\langle \pi_1 \rangle = \langle \pi_2 \rangle$, i.e., up to a unit multiple, there is just one prime element, say $\pi \in R$. Such a ring is called a *discrete valuation ring*, denoted DVR, and $\pi \in R$ is called a *uniformizing parameter*.

Problem 1:
Fix a prime $p \in \mathbb{Z}$. Let R denote the set of rational numbers whose denominators is not divisible by p. First show that R is a subring of $\mathbb{Q}$, and then show that R is a DVR with uniformizing parameter p.
Solution:
First we need to show that R is a subring of $\mathbb{Q}$. R inherits associativity and distributivity from $\mathbb{Q}$, so we only need to show that $(R, +)$ is a group and that R is closed under multiplication.
Closure of $(R, +)$ under composition:

$$\begin{aligned}
&\frac{a_1}{a_2}, \frac{b_1}{b_2} \in R \\
&p \nmid a_2, p \nmid b_2 \\
&\frac{a_1}{a_2} + \frac{b_1}{b_2} = \frac{a_1 b_2 + b_1 a_2}{a_2 b_2}
\end{aligned}$$

Because $\mathbb{Z}$ is a UFD, we use the contrapositive of one of the requirements of a prime to say that $p \nmid a_2, p \nmid b_2 \Rightarrow p \nmid a_2 b_2$.

$$\Rightarrow \frac{a_1 b_2 + b_1 a_2}{a_2 b_2} \in R$$

Closure of $(R, +)$ under inverses:

$$\begin{aligned}
&\frac{a_1}{a_2} \in R \\
&\left(-\frac{a_1}{a_2}\right) = \frac{-a_1}{a_2} = \frac{a_1}{-a_2} \in R
\end{aligned}$$

Closure of R under multiplication:

$$\begin{aligned}
&\frac{a_1}{a_2}, \frac{b_1}{b_2} \in R \\
&\frac{a_1}{a_2} * \frac{b_1}{b_2} = \frac{a_1 b_1}{a_2 b_2} \\
&p \nmid a_2, p \nmid b_2 \Rightarrow p \nmid a_2 b_2 \\
&\Rightarrow \frac{a_1}{a_2} * \frac{b_1}{b_2} \in R
\end{aligned}$$

Also R contains the multiplicative identity $\frac{1}{1}$.
Now we need to show that R is a DVR with uniformizing parameter p.
Since primes can't be units, they must be elements of R without a multiplicative inverse.
An element has no multiplicative inverse iff it is a multiple of p.

$\frac{a_1 p}{a_2} \in R, p \nmid a_2$

We assume WLOG that $p \nmid a_1$

If $\frac{a_1 p}{a_2}$ had an inverse $\frac{x_1}{x_2}$:

$\frac{a_1 p}{a_2} * \frac{x_1}{x_2} = \frac{a_1 p x_1}{a_2 x_2} \in \left[\left(\frac{1}{1}\right)\right]$

$p \nmid x_2, p \nmid a_2 \Rightarrow p \nmid a_2 x_2$

But $p \mid p a_1 x_1$

So p divides the numerator but not the denominator

$\Rightarrow \frac{a_1 p}{a_2} * \frac{x_1}{x_2} \notin \left[\left(\frac{1}{1}\right)\right]$

So a multiple of p does not have an inverse

If an element in R is not a multiple of p, then it has an inverse

$\frac{a_1}{a_2} \in R, p \nmid a_1, \nmid a_2$

$\Rightarrow \frac{a_1}{a_2} \frac{a_2}{a_1} = 1, \frac{a_2}{a_1} \in R$

So for any non-unit prime $\frac{pa_1}{a_2}$:

$$p \mid \frac{pa_1}{a_2}$$
$$\frac{pa_1}{a_2} * \frac{a_2}{a_1} = p \Rightarrow \frac{pa_1}{a_2} \mid p$$
$$\Rightarrow \langle \frac{pa_1}{a_2} \rangle = \langle p \rangle$$

Problem 2:
Let R be a DVR with uniformizing paramter $\pi \in R$. Show that $\bigcap_{n\geq 1}\langle \pi^n \rangle = 0$.
Solution:

Admitted

Problem 3:
Let R be a DVR with uniformizing parameter $\pi \in R$. Show that every element in R can be written uniquely as $u\pi^n$ for some $n \geq 0$ and $u \in R$ a unit. Conclude that if K dnotes the quotient field of R, then every element in K can be written uniquely in the form $u\pi^n$ for some $n \in \mathbb{Z}$ and $u \in R$, a unit.
Solution:

Admitted

Problem 4:
Let R be a DVR with uniformizing parameter $\pi \in R$, and quotient field K. Define $v : K \to \mathbb{Z} \cup \{\infty\}$ by $v(0) = \infty$ and for $\alpha \neq 0, v(\alpha) = n$, where $\alpha \in K$ and $\alpha = u\pi^n$, as in 3. Show that for all $\alpha, \beta \in K$:

(i) $v(\alpha + \beta) \geq min\{v(\alpha), v(\beta)\}$

(ii) $v(\alpha\beta) = v(\alpha) + v(\beta)$

Observe that $R = \{a \in K \mid v(a) \geq 0\}$
Solution:

Admitted

Problem 5:
Let K be a field. Suppose $v : K \to \mathbb{Z} \cup \{\infty\}$ is a function such that for all $\alpha, \beta \in K$:

(i) $v(\alpha) = \infty \iff \alpha = 0$

(ii) $v(\alpha + \beta) \geq min\{v(\alpha), v(\beta)\}$

(iii) $v(\alpha\beta) = v(\alpha) + v(\beta)$

Such a function is called a *discrete valuation* on K. We assume that v takes values other than 0 and ∞. Set $R := \{\alpha \in K \mid v(\alpha) \geq 0\}$. Prove that R is DVR by the following steps below:

(i) Show that $u \in R$ is a unit $\iff v(u) = 0$. Hint: First show $v(1) = 0$.

(ii) Show there exist element $r \in R$, with $v(r) > 0$.

(iii) Prove that if $r \in R$, and $v(r) > 0$, then as an element of K, $v(\frac{1}{r}) = -v(r)$.

(iv) Suppose $c := \min\{v(r) \mid r \in R \text{ and } v(r) > 0\}$. Show that the image of v is $c\mathbb{Z}$.

(v) Show that if $\pi \in R$ and $v(\pi) = c$, then R is a DVR with uniformizing parameter π.

Solution: