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:

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

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

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

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:
First we can see that since $0 \in \langle \pi^n \rangle$ for all n, $0 \in \bigcap_{n\geq 1}\langle \pi^n \rangle$.
Now consider a nonzero element $a \in R$. We know that a can be written as a finite product of irreducibles (proved earlier), and that π is prime, therefore irreducible, so

case 1: $\pi \nmid a,$ or
case 2: $a = \pi^s b$
Suppose there are two ways of writing a in case 2:
$a = \pi^m b = \pi^n b'$ suppose $m \geq n$, and $m, n \geq 1$
$\pi^{m-n} b = b'$ From cancellation in IDs
$\Rightarrow \pi^n b' = \pi^n(\pi^{m-n} b)$
So the two factorizations have the same number of π's

In case 1:
$\pi \nmid a$
$\Rightarrow \forall q, \pi q \neq a \Rightarrow a \notin \langle \pi \rangle$

In case 2:
$a = \pi^s b$
WLOG, assume $\pi \nmid b$
$\Rightarrow \forall q, \pi q \neq b$
$\Rightarrow \forall q, \pi^{s+1} q \neq a$
$\Rightarrow a \notin \langle \pi^{s+1} \rangle$

In all cases, for any nonzero a there exists an ideal of a power of π such that $a \notin \langle \pi^n \rangle$. So since a is not in all ideals of the form $\langle \pi^n \rangle$, $a \notin \bigcap_{n\geq 1}\langle \pi^n \rangle$. But $0 \in \bigcap_{n\geq 1}$. So $\bigcap_{n\geq 1} = 0$

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:
First we can prove that R is a UFD. We know that every element in R can be written as a product of irreducibles. Now we prove that irreducible elements generate maximal ideals:

$$\begin{aligned}
&p \in R \text{ is irreducible}\\
&\text{Suppose } <p> \subseteq <j> \subseteq R\\
&\Rightarrow p = jr\\
&p \text{ is irreducible } \Rightarrow j \text{ or } r \text{ is a unit}\\
&\text{if } r \text{ is a unit, then } <j> = <p>\\
&\text{if } j \text{ is a unit, then } <j> = R \text{ which is not an ideal}
\end{aligned}$$

So $<p>$ is a maximal ideal. Now we can prove that maximal ideals are prime ideals, and that an element generating a prime ideal is prime.

$$\begin{aligned}
&\text{Suppose } <q> \text{ is a maximal ideal and that}\\
&q = ab\\
&\text{We also assume that } q \mid ab, q \nmid a\\
&<q> \subset <q> + <a>\\
&<q> + <a> \text{ is an ideal, since the sum of ideals is an ideal}\\
&<q> + <a> = R, \text{because it is a strict superset of } <q>, \text{ and } <q> \text{ is maximal}\\
\\
&1 \in <q> + <a>\\
&\Rightarrow 1 = r_1 q + r_2 a\\
&\Rightarrow b * 1 = b * r_1 q + b * r_2 a\\
&\Rightarrow b = b r_1 q + r_2(ab)\\
&q \mid (b r_1) q, q \mid (r_2) ab\\
&\Rightarrow q \mid b r_1 q + r_2(ab) \Rightarrow q \mid b
\end{aligned}$$

So q is prime. We have shown that every irreducible element is prime in R. So every element can be written as a finite product of irreducibles, and therefore can be written as a finite product of primes. This implies that R is a UFD, which includes uniqueness of the factorizations. But since there is only one prime:

$$\begin{aligned} &r \in R \Rightarrow r = (u_0\pi)(u_1\pi)(u_2\pi)...(u_k\pi) \\ &\Rightarrow r = (u_0...u_k)\pi^k = u'\pi^k \end{aligned}$$

Now we have to prove that every element of K can be written in a similar way.

$$\begin{aligned}
&\frac{a}{b} \in K \\
&\frac{a}{b} = \frac{u_1\pi^m}{u_2\pi^n} \\
&\text{If } m \geq n: \\
&\frac{u_1\pi^m}{u_2\pi^n} = \frac{u_2\pi^n u_2^{-1}u_1\pi^{m-n}}{u_2\pi^n} \\
&= \frac{u_2^{-1}u_1\pi^{m-n}}{1} = \frac{u'\pi^{m-n}}{1} = u'\pi^{m-n}
\end{aligned}$$

$$\begin{aligned}
&\text{If } m < n: \\
&\frac{u_1\pi^m}{u_2\pi^n} = \frac{u_1\pi^m}{u_1\pi^m u_1^{-1}u_2\pi^{n-m}} \\
&= \frac{1}{u_1^{-1}u_2\pi^{n-m}} = \frac{1}{u'\pi^{n-m}} \\
&= \left(\frac{u'\pi^{n-m}}{1}\right)^{-1} \\
&= \left(u'\pi^{n-m}\right)^{-1} \text{ using the convention of writing } \frac{a}{1} = a \text{ in K} \\
&= u'\left(\pi^{n-m}\right)^{-1}
\end{aligned}$$

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:

Proof of (i):

let $\alpha = u_1\pi^{n_1}, \beta = u_2\pi^{n_2}$
We are considering the elements as being in K, but u_1, u_2 are units in R and $\alpha, \beta \in R$
Assume that $n_1 < n_2$
$u_1\pi^{n_1} + u_2\pi^{n_2} = u_3\pi^{n_3}$ from 3.

Suppose that $n_3 < n_1$ (This will show a contradiction)
$u_1\pi^{n_1} + u_2\pi^{n_2} = u_3\pi^{n_3}$
$= \pi^{n_1}(u_1 + u_2\pi^{n_2-n_1}) = \pi^{n_1}u_3\pi^{n_3-n_1}$
$= u_1 + u_2\pi^{n_2-n_1} = u_3\pi^{n_3-n_1}$
Note that $n_3 - n_1 < 0$
$= u_1 + u_2\pi^{n_2-n_1} = u_3\left(\pi^{n_1-n_3}\right)^{-1}$
The expression on the left side is an element of R from closure
This implies the right side is in R (its not)
But we need to check that $u_3\left(\pi^{n_1-n_3}\right)^{-1}$ can't be in R
If $u_3\left(\pi^{n_1-n_3}\right)^{-1} \in R$, then it can be written $u_1\pi^b, b \geq 0$
$\Rightarrow u_1\pi^b * u_3\left(\pi^{n_1-n_3}\right) = 1$
$\Rightarrow A * u_1\pi^b * u_3\left(\pi^{n_1-n_3}\right) = A$
This contradicts the unique factorization of A in R
Because of the contradiction we can conclude that $n_3 \geq \min(n_1, n_2)$

Proof of (ii):

$$
\begin{aligned}
&\text{let } \alpha = u_1\pi^{n_1}, \beta = u_2\pi^{n_2} \\
&\alpha\beta = u_1\pi^{n_1}u_2\pi^{n_2} \\
&= u_1u_2\pi^{n_1}\pi^{n_2} = u_1u_2\pi^{n_1+n_2} \\
&= u'\pi^{n_1+n_2} \\
&\Rightarrow v(\alpha\beta) = n_1 + n_2 = v(\alpha) + v(\beta)
\end{aligned}
$$

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:
Proof of (i):

$$
\begin{aligned}
&u \in R \text{ is a unit} \\
&\Rightarrow uu^{-1} = 1 \\
&\Rightarrow v(u) + v(u^{-1}) = v(1) = 0 \\
&u, u^{-1} \in R \Rightarrow v(u), v(u^{-1}) \geq 0 \\
&\Rightarrow v(u) = 0, v(u^{-1}) = 0
\end{aligned}
$$

$$
\begin{aligned}
&\text{Now assume } v(b) = 0 \text{ for some } b \in R \\
&b^{-1} \in K = \frac{1}{b} \\
&\Rightarrow b * \frac{1}{b} = 1 \text{ in K} \\
&\Rightarrow v(b) + v(\frac{1}{b}) = v(1) = 0 \\
&v(b) = 0 \Rightarrow v(\frac{1}{b}) = 0 \\
&\text{since } v(\frac{1}{b}) \geq 0,\ \frac{1}{b} = b^{-1} \in R \\
&\text{So } b \text{ has a multiplicative inverse in } R \Rightarrow b \text{ is a unit}
\end{aligned}
$$

Proof of (ii):
We assumed that the function $v(\alpha)$ takes values other than 0 and ∞, so for some

$\alpha \in K, v(\alpha) \neq 0$. We need to show that there exists an element in R with the same property.

$$\alpha \in K, v(\alpha) = c, c \neq 0$$
if $c > 0$, then $c \in R$ by definition of R, and we are done)
if $c < 0$, then $c^{-1} \in K$
$$c * c^{-1} = 1$$
$$v(c * c^{-1}) = v(1) = 0$$
$$v(c) + v(c^{-1}) = 0$$
$$v(c^{-1}) = -v(c)$$
$$\Rightarrow v(c^{-1} > 0)$$
So $c^{-1} \in R$ and we are done

Proof of (iii):

$$r \in R, v(r) > 0$$
The multiplicative inverse of r in K is $\frac{1}{r}$
$\frac{1}{r} * r = 1$ In K
$$\Rightarrow v(\frac{1}{r} * r) = v(1)$$
$$\Rightarrow v(\frac{1}{r}) + v(r) = 0$$
$$\Rightarrow v(\frac{1}{r}) = -v(r)$$

Proof of (iv):
First we can show that all of the elements in the image of v are divisible by c. Then we can show that for each multiple of c, ac, with $a, c \in \mathbb{Z}$, there exists an element t s.t. $v(t) = ac$.

$\exists r_0 \in R$ s.t. $v(r_0) = c$

Suppose there is an element $r \in R$ s.t. $c \nmid v(r)$

$v(r) = qc + r', 0 < r' < c$ or

$v(r) = q(v(r_0)) + r', 0 < r' < c$

Consider the elements of K, r, $\frac{1}{r_0}$

let $b = r * \frac{1}{r_0} * \frac{1}{r_0} * ... * \frac{1}{r_0}$

Where there are q terms of $\frac{1}{r_0}$

$v(b) = v(r * \frac{1}{r_0} * \frac{1}{r_0} * ... * \frac{1}{r_0})$

$\Rightarrow v(b) = v(r) - v(r_0) - ... - v(r_0)$

$\Rightarrow v(b) = v(r) - qv(r_0) = r'$

$r' > 0,$ so $b \in R$. but $r' < c$, and $c := \min\{v(r) \mid r \in R\}$

This is a contradiction, so every number in the image of v must be divisible by c

Now we have to show that each multiple of c is in the range of v, with K as the domain.

For each value qc when $q \geq 0$:

$r_0 * r_0 * ... * r_0 \in K$ with q terms of r_0

$v(r_0 * r_0 * ... * r_0) = q * v(r_0) = qc,$ So there exists an element r in K s.t. $v(r) = qc$

If $q < 0$:

$\frac{1}{r_0} * \frac{1}{r_0} * ... * \frac{1}{r_0} \in K$ with q terms of $\frac{1}{r_0}$

$v(\frac{1}{r_0} * \frac{1}{r_0} * ... * \frac{1}{r_0}) = |q| * v(\frac{1}{r_0}) = |q| * (-v(r_0)) = q * v(r_0) = qc$

So there exists an element $r = \frac{1}{r_0} * \frac{1}{r_0} * ... * \frac{1}{r_0}$ in K s.t. $v(r) = qc$

So if an element is in $c\mathbb{Z}$, then that element is in $im(v)$, and if an element is not in $c\mathbb{Z}$, then it is not in $im(v)$. This proves the sets are equal.

Proof of (v): To prove that R is a DVR, we show that for each prime $p \in R$, $v(p) = v(\pi) \Rightarrow p = u\pi$. So $\langle p \rangle = \langle \pi \rangle$.

Let p be a prime in R
$\Rightarrow p$ is irreducible, so $p = ab \Rightarrow a$ or b is a unit
$\Rightarrow v(p) = v(a) + v(b)$ So one term on the right is nonzero

We know from part (iv) that for all $r \in R$, $c \mid v(r)$
And the image of v with R as the domain is $c\mathbb{Z}^+$
$c \mid v(p)$
$\Rightarrow v(\pi) * q = v(p)$
$\Rightarrow v(\pi) + ... + v(\pi) = v(p)$
But p is irreducible, so only one of the q summands on the left is nonzero (by induction)
$\Rightarrow v(\pi) = v(p)$

Now we have to prove that $v(\pi) = v(p) \Rightarrow \pi = up$, with $u \in R$ a unit
$v(\pi) = v(p)$
$v(\pi) - v(p) = 0$ From this point we can switch to the context of the field F :
$= v(\pi) + v(\frac{1}{p}) = 0$ From (iii)
$\Rightarrow v(\pi * \frac{1}{p}) = 0$
$\Rightarrow \pi * \frac{1}{p} = u$ where u is a unit in R
$\Rightarrow \pi * \frac{1}{p} * \left(\frac{1}{p}\right)^{-1} = u * \left(\frac{1}{p}\right)^{-1}$
$\Rightarrow \pi = u * p$ All of these elements are in R
$\Rightarrow \pi \mid p, p \mid \pi \Rightarrow \langle p \rangle \subseteq \langle \pi \rangle, \langle \pi \rangle \subseteq \langle p \rangle,$
$\Rightarrow \langle \pi \rangle = \langle p \rangle$

So R is a DVR with uniformizing parameter p.