Homework 16 - MATH 791

Will Thomas

Throughout this assignment, R is an integral domain. The first three problems show that we can construct a field containing R in the exact manner that the rational numbers are constructed from the integers. Recall, that formally speaking, the rational numbers are the set of equivalence classes of ordered pairs (a,b) of integers (with $b \neq 0$) such that (a,b) is equivalent to (c,d) if and only if $ad = bc$. Of course, we denote the equivalence class of an ordered pair (a,b) as a/b

Problem 1:
Let Q denote the set of ordered pairs (a,b) with $a,b \in R$ and $b \neq 0$. For $(a,b),(c,d) \in Q$, define $(a,b) \sim (c,d) \iff ad = bc \in R$. Show that $\sim$ is an equivalence relation.
Solution:
To show equivalence we need:
Reflexive:

$$(a,b) \sim (a,b) \forall a,b \in R$$

$$(a,b) \sim (a,b) \iff ab = ba$$

We know that since all ID's are commutative rings that this must hold.
Symmetric:

$$\forall a,b \in R, (a,b) \sim (b,a)$$

$$(a,b) \sim (b,a) \iff ab = ab$$

Trivially holds
Transitivity:

$$(a,b) \sim (c,d) \wedge (c,d) \sim (e,f) \implies (a,b) \sim (e,f)$$

$$(a,b) \sim (c,d) \implies ad = bc, \ (c,d) \sim (e,f) \implies cf = de$$

Multiplying both sides by ef we get $adef = bcef$ which using that fact that this is an ID, we can use commutativity and cancellation to reach

$$af(de) = be(cf) \implies af = be \iff (a,b) \sim (e,f)$$

$\therefore$ This is an equivalence relation

Problem 2:
Let K denote the set of equivalence classes under the equivalence relation in 1.
Temporarily using $[(a,b)]$ to denote the equivalence class of (a,b), defined addition and multiplication of elements in K as follows:

$$[(a,b)] + [(c,d)] := [(ad+bc, bd)]; \ [(a,b)] \cdot [(c,d)] = [(ac, bd)]$$

Show that addition and multiplication in K are well defined.
Solution:
Addition:
To show well-defined, let us take $(a, b) \sim (c, d) \in K$ and $(e, f) \in K$ and show that

$$[(a, b)] + [(e, f)] \sim [(c, d)] + [(e, f)]$$

$$[(a, b)] + [(e, f)] = [(af + be, bf)], \ [(c, d)] + [(e, f)] = [(cf + de, df)]$$

We want to show that $[(af + be, bf)] \sim [(cf + de, df)]$

$$[(af + be, bf)] \sim [(cf + de, df)] \iff adf^2 + bdef = bcf^2 + bdef$$

We can cancel out the $bdef$ and then apply the fact that $(a, b) \sim (c, d) \implies ad = bc$ to solve this problem.

$\therefore$ Addition is well-defined

Multiplication:
To show well-defined, let us take $(a, b) \sim (c, d) \in K$ and $(e, f) \in K$ and show that

$$[(a, b)] \cdot [(e, f)] \sim [(c, d)] \cdot [(e, f)]$$

$$[(a, b)] \cdot [(e, f)] = [(ae, bf)], \ [(c, d)] \cdot [(e, f)] = [(ce, df)]$$

We want to show that $[(ae, bf)] \sim [(ce, df)]$

$$[(ae, bf)] \sim [(ce, df)] \iff adef = bcef$$

We can cancel out the ef and then apply the fact that $(a, b) \sim (c, d) \implies ad = bc$ to solve this problem.

$\therefore$ Multiplication is well-defined

Problem 3:
Show that K is a field under the operations above and that the set of elements in K of the form $[(a, 1)]$ is a subring of K isomorphic to R. The field K is called the *quotient field* of R or *fraction field* of R.
Solution:
To show K is a field, we need to show that $+, \cdot$ and commutative, associative, have identities and inverses, and that $\cdot$ distributes over $+$.
The commutativity and associativity are fairly obvious from the definition and the fact that the underlying ring R is a ID.
The additive identity will be $[(0, 1)] + [(a, b)] = [(a, b)]$ and the multiplicative identity will be $[(1, 1)] \cdot [(a, b)] = [(a, b)]$

The additive inverses will be $[(a,b)] + [(a,-b)] = [(-ab+ab=0,1)]$, the multiplicative inverse will be $[(a,b)] \cdot [(b,a)] = [(ab,ab)] \sim [(1,1)]$ as $[(ab,ab)] \sim [(1,1)] \iff ab = ab$ which is obviously true, thus $[(ab,ab)] \in [(1,1)]$ so it is the identity.
For distributivity,
$[(a,b)] \cdot ([(c,d)] + [(e,f)]) = [(acf + ade, bdf)] = [((ad+bc), bd)] + [((af+be), bf)]$
$= [(a,b)] \cdot [(c,d)] + [(a,b)] \cdot [(e,f)]$
To show that the subring is isomorphic, we can use the First Isomorphism theorem and define $\phi : K \to R$ by $\phi([(a,b)]) = a$.

$$\ker(\phi) = \{[(a,b)] \in K \mid \phi([(a,b)]) = 0\}$$

$$\ker(\phi) = \{[(0,b)] \in K\}$$

To show this is a ring homomorphism

$$\forall [(a,b)], [(c,d)] \in K, \phi([(a,b)][(c,d)]) = \phi([(a,b)])\phi([(c,d)])$$

$$\phi([(a,b)][(c,d)]) = \phi([ac,bd]) = ac = \phi([(a,b)])\phi([(c,d)])$$

Similarly for addition

$$\forall [(a,b)], [(c,d)] \in K, \phi([(a,b)] + [(c,d)]) = \phi([(a,b)]) + \phi([(c,d)])$$

$$\phi([(a,b)] + [(c,d)]) = \phi([(ad+bc, bd)]) = ad + bc = a + c$$

And since we are only taking elements such that the second element is 1, that means $a1 + 1c = a + c = \phi([(a,b)]) + \phi([(c,d)])$
It is fairly straightforward that ϕ is surjective

$$\therefore \text{The subring of } K \text{ formed by } [(a,1)] \text{ is isomorphic to } R$$

Remark:
Henceforth we will write the elements of K as a/b, rather than $[(a,b)]$ and an element $a \in R$ either as a or $a/1$ and regard R as a subring of K. Note then that $a/b + c/d = (ad+bc)/bd$ and $a/b \cdot c/d = ac/bd$ as expected

Problem 4:
Let L be a field containing R. Show that L contains K (or at least an isomorphic copy of K). Thus in this sense, K is the smallest field containing R.
Solution:
If L is a field containing R, let us assume for contradiction that $\exists k_1/k_2 \in K$ that is not in L
We have two cases, either $k_1/k_2 \in R$ which means it is in $L \rightarrow\leftarrow$
So we must be in the case where $k_1/k_2 \notin R \iff k_2 \neq 1$. If $k_1/k_2 \in K \iff k_2/k_1 \in K$ also. Yet by a similar argument as above, $k_2/k_1 \notin R \iff k_1 \neq 1$

Additionally, since K is made of equivalence classes, we know that $k_1 \nmid k_2 \wedge k_2 \nmid k_1$. This is to say that k_1 and k_2 are relatively prime.
Since we proved the Isomorphism earlier, we know that $k_1/1 \in R \wedge k_2/1 \in R$, and since L is a *field* containing R, that means it must have multiplicative inverses
$\implies 1/k_1 \in L \wedge 1/k_2 \in L$. We can then show that $k_1/1 \cdot 1/k_2 = k_1/k_2 \in L$

$$\therefore \text{No element in } K \text{ cannot be in } L$$

$$\therefore K \text{ is the smallest field containing } R$$

Problem 5:

Let A be an $m \times n$ matrix with entries in R satisfying $m < n$. Set $x := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and $0 := \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Use standard facts from linear algebra to show that the homogeneous system of equations $A \cdot x = 0$ has infinitely many solutions over R
Solution:
First let us enumerate A as $A := (a_{ij})$ for $i < m$ and $n < j$

$$A \cdot x = \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n \end{pmatrix} = 0$$

Let us start by just finding the solutions for the top row, $a_{11}x_1 + \cdots + a_{1n}x_n = 0$. If $n = 1$ then that means that $m < n \implies m = 0$ so that is ill-posed.
Instead $n \geq 2$, so $a_{11}x_1 + a_{12}x_2 = 0$ then we know that $a_{11}x_1 = -a_{12}x_2$. We can then claim WLOG that $a_{12} = a' \cdot x_1 \cdot x_2^{-1}$

$$a_{11}x_1 = -a'x_1 \implies a_{11} = -a'$$

Since a_{11} is left arbitrary, this means that it can be any element in R, and R is infinite

$$\therefore A \cdot x = 0 \text{ has infinitely many solutions}$$