Homework

Frederick Robinson*

11 January 2010

Contents

*I worked with Dan Stevens on these exercises

1 Chapter 7 Section 1

1.1 Problem 1

1.1.1 Question

Let R be a ring with 1.

Show that $(-1)^2 = 1$ in R

1.1.2 Answer

$$1 + (-1) = 0$$

$$\Rightarrow (-1)(1 + (-1)) = (-1)0$$

$$\Rightarrow (-1)1 + (-1)^2 = 0$$

$$\Rightarrow (-1)^2 = 1$$

1.2 Problem 7

1.2.1 Question

The *center* of a ring R is $\{z \in R \mid zr = rz \text{ for all } r \in R\}$ (i.e., is the set of all elements which commute with every element of R). Prove that the center of a ring is a subring that contains the identity. Prove that the center of a division ring is a field.

1.2.2 Answer

We will prove that the center, say Z of a ring R is a subring of R

Proof. We need to prove Z is a subgroup of the additive group in the original ring.

Towards this end we first demonstrate that Z is closed under addition. Let $x, y \in Z$. So, by the definition of Z we have $xr = rx$ and $yr = ry$ for arbitrary $r \in R$. So, $xr + yr = rx + ry \Rightarrow (x + y)r = r(x + y)$.

Now we must demonstrate that the Z is closed under additive inverses. Again take $x \in Z$. $rx = xr \Rightarrow -(rx) = -(xr)$ and by Proposition 1.2 (page 226) we have $-(rx) = -(xr) \Rightarrow r(-x) = (-x)r$. Thus, Z is closed under additive inverses as desired.

So we have demonstrated that Z is a group under addition (as defined in the ring) if it is nonempty.

Now we will show that multiplication as defined on R is closed in Z. Again, we let $x, y \in Z$. Hence, $xr = rx$ and $yr = ry$ for $r \in R$. So, $xyr = xry = rxy \Rightarrow (xy)r = r(xy)$ as desired.

It remains to show that Z is necessarily nonempty. The additive identity of R is in Z as $0r = r0 = 0$ for all $r \in R$ (Proposition 1.1 page 226). If R is a ring with identity then the identity is central for, $1r = r = r1$ for any $r \in R \Rightarrow 1 \in Z$. □

The center of a division ring is a field.

Proof. By the previous proof we know that the center of a division ring R is a ring. Moreover, for R a division ring the center Z must be a division ring since for $z \in Z, r \in R$ we have $r = z^{-1}zr = z^{-1}rz \Rightarrow rz^{-1} = z^{-1}r$.

So, since we know that Z is a division ring, and every element of Z commutes with every element of R it must be that $\forall z, z' \in Z$ we have $zz' = z'z$. Thus, Z is a commutative division ring. This is just the definition of a field though. □

1.3 Problem 8

1.3.1 Question

Describe the center of the real Hamilton Quaternions $\mathbb{H}$. Prove that $\{a + bi \mid a, b \in \mathbb{R}\}$ is a subring of $\mathbb{H}$ which is a field but is not contained in the center of $\mathbb{H}$.

1.3.2 Answer

First we work out the product of two elements of $\mathbb{H}$ in general.

$$(a + bi + cj + dk)(a' + b'i + c'j + d'k)$$

$$= (aa'-bb'-cc'-dd')+(ab'+ba'+cd'-dc')i+(ac'-bd'+ca'+db')j+(ad'+bc'-cb'+da')k$$

So, an element $(a + bi + cj + dk)$ is in the center of $\mathbb{H}$ if and only if we

have

$$ab' + ba' + cd' - dc' = a'b + b'a + c'd - d'c \Rightarrow cd' - dc' = c'd - d'c$$

$$\Rightarrow cd' = c'd$$

and

$$ac' - bd' + ca' + db' = a'c - b'd + c'a + d'b \Rightarrow -bd' + db' = -b'd + d'b$$

$$\Rightarrow db' = d'b$$

and

$$ad' + bc' - cb' + da' = a'd + b'c - c'b + d'a \Rightarrow bc' - cb' = +b'c - c'b$$

$$\Rightarrow bc' = b'c$$

for arbitrarily chosen $a', b', c', d' \in \mathbb{R}$

An element $(a + bi + cj + dk) \in \mathbb{H}$ satisfies this if and only if it is of the form $(a + bi + cj + dk) = a$ for $a \in \mathbb{R}$. Hence, the center or $\mathbb{H}$ is just the real numbers $\mathbb{R}$.

Now we prove that $\{a + bi \mid a, b \in \mathbb{R}\}$ is a subring of $\mathbb{H}$ which is in particular a field

Proof. The elements of $\mathbb{H}$ of the form $a + bi$ for $a, b \in \mathbb{R}$ form a group under

addition since $(a+bi)+(a'+b'i) = ((a+a')+(b+b')i)$ for $a,b,a',b' \in \mathbb{R}$ and $((a+a')+(b+b')i)$ is of the desired form. Moreover, given $a+bi$ we have that $a+bi+(-a-bi)=0$

Now we prove that the set of all $a+bi$ is closed under the ring product. Let $a,b,a',b' \in \mathbb{R}$. Then $(a+bi)(a'+b'i) = (aa'-bb')+(ab'+ba')i$ which is of the desired form.

So the subset in question is indeed a ring. Moreover we can show that it is a field. It contains the identity since 1 is of the form $a+bi$ (note that this proves also that it is nonempty). It is commutative since $(a+bi)(a'+b'i) = (aa'-bb')+(ab'+ba')i = (a'a-b'b)+(a'b+b'a)i = (a'+b'i)(a+bi)$. Lastly it is closed under multiplicative inverse since given $a+bi$ we see that $(a+bi)(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i) = 1$ and both $\frac{a}{a^2+b^2}$ and $\frac{b}{a^2+b^2}$ are in $\mathbb{R}$. □

$\{a+bi \mid a,b \in \mathbb{R}\}$ is not contained in the center of $\mathbb{H}$ since by a previous proof, the center of $\mathbb{H}$ consists exactly of those elements of form a for some $a \in \mathbb{R}$

1.4 Problem 11

1.4.1 Question

Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.

1.4.2 Answer

Let R be an integral domain with $x^2 = 1$ for some $x \in R$. We will prove that $x = \pm 1$

Proof. So, $x(x+1) = x^2 + x = 1 + x = x + 1$. There are two cases.

Case 1: $x + 1 \neq 0$

In this case x is the identity for $x + 1$. Since identities are unique $x = 1$

Case 2: $x + 1 = 0$

So $x = -1$ □

1.5 Problem 13

1.5.1 Question

An element x in R is called *nilpotent* if $x^m = 0$ for some $m \in \mathbb{Z}^+$

(a) Show that if $n = a^k b$ for some integers a and b then ab is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$

(b) If $a \in \mathbb{Z}$ is an integer, show that the element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n is also a divisor of a. In particular, determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ explicitly.

(c) Let R be the ring of functions from a nonempty set X to a field F. Prove that R contains no nonzero nilpotent elements.

1.5.2 Answer

(a) Let $n = a^k b$ for some integers a and b. We will show that ab is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$

Proof. $(ab)^k = a^k b^k = (a^k b)b^{k-1} = nb^{k-1} \equiv 0(mod\ n)$ □

(b) Let $a \in \mathbb{Z}$. We will show that the element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n is also a divisor of a.

Proof. We begin by showing ($\Rightarrow$) that $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if every prime divisor of n is also a divisor of a.

If we assume every prime divisor of n is also a divisor of a we have $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}$ and $a = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_m^{\beta_m} \cdot (l)$ for $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots \beta_m, l \in \mathbb{N}\backslash 0$ and $p_1, \ldots, p_m$ distinct primes.

Let $A = max\{\alpha_1, \ldots, \alpha_m\}$. We have then that $a^A = (p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_m^{\beta_m} \cdot (l))^A = p_1^{A\beta_1} \cdot p_2^{A\beta_2} \cdot \ldots \cdot p_m^{A\beta_m} \cdot (l^A)$ and since each β_i is at least 1 we can express this as $a^A = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m} \cdot p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_m^{\gamma_m} \cdot (l^A) = n \cdot p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_m^{\gamma_m} \cdot (l^A) \equiv (0 \mod n)$. Thus, a is nilpotent.

Now we show ($\Leftarrow$) that if $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent then every prime divisor of n is also a divisor of a.

Assume that $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent. Then, $\exists A$ such that $a^A = nl$ for some $l \in (Z)^+$. However this is only possible if every prime divisor of n is also a divisor of a. For, assume not, then there is some divisor m of n that is not a divisor of a. But, this is a contradiction as a^A is divisible only by those primes which divide a.

So we have shown that the element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n is also a divisor of a as desired. □

The nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$ are precisely those whose representatives have the same prime divisors as 72 by the preceding proof.

Since $72 = 2^3 \cdot 3^2$ the representatives in $[0, 72]$ are just $6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72$, and so the nilpotent elements are $\bar{6}, \bar{12}, \bar{18}, \bar{24}, \bar{30}, \bar{36}, \bar{42}, \bar{48}, \bar{54}, \bar{60}, \bar{66}, \bar{72}$

(c) Let R be the ring of functions from a nonempty set X to a field F. We shall prove that R contains no nonzero nilpotent elements.

Proof. Suppose towards a contradiction that R contains a nonzero nilpotent element, say $f : X \to F$. So $f \neq 0$ and $f^k = 0$ for some $k \in \mathbb{N}$. However, this implies that for each $x \in X$ we have $f(x)^k = 0$, as the additive identity in R is that function which takes each $x \in X$ to 0. Since f is nonzero we can choose this $f(x)$ to be nonzero.

So, $f(x) \in F$ is nonzero and nilpotent. This is however a contradiction, for it implies that $f(x)^{k-1} \cdot f(x) = 0 \Rightarrow f(x)$ is a zero divisor. But, fields have no zero divisors. □

1.6 Problem 14

1.6.1 Question

Let x be a nilpotent element of the commutative ring R (cf. the preceding exercise).

(a) Prove that x is either zero or a zero divisor.

(b) Prove that rx is nilpotent for all $r \in R$.

(c) Prove that $1 + x$ is a unit in R.

(d) Deduce that the sum of a nilpotent element and a unit is a unit.

1.6.2 Answer

(a) We shall show that x is either zero or a zero divisor.

Proof. Since x is nilpotent, $\exists k \in \mathbb{N}$ such that $x^k = 0$. There are two cases.

Case 1: $k = 1$

$x^1 = 0 \Rightarrow x = 0$

Case 2: $k \neq 1$

$x \cdot x^{k-1} = 0$. This is just the definition for x being a zero divisor though as $x^{k-1} \neq 0$ for k minimal. □

(b) We prove that rx is nilpotent for all $r \in R$.

Proof. Since x is nilpotent there is some $k \in \mathbb{N}$ such that $x^k = 0$. Moreover, since R is commutative we have that $(rx)^k = r^k x^k = r^k \cdot 0 = 0$. Hence, rk is nilpotent. □

(c) Now we show that $1 + x$ is a unit in R.

Proof.

$$(1+x)(1-x+x^2-x^3+\ldots\pm x^{k-1}) = 1-x+x^2-x^3+\ldots\pm x^{k-1}+x-x^2+x^3-x^4+\ldots\pm x^k$$

$$= 1 + x^k$$

$$= 1$$

So, $1 + x$ is a unit in R is desired. □

(d) Deduce that the sum of a nilpotent element and a unit is a unit.

Proof. Let $x, a \in R$ with x nilpotent and a a unit. Then we have

$$\begin{aligned} a^{-1}(x + a) &= a^{-1}x + a^{-1}a \\ &= a^{-1}x + 1 \end{aligned}$$

Which is a unit as, we know by part b that rx is a nilponent element, and adding the identity to a nilponent element yields a unit by c. Moreover the fact that multiplying $(x+a)$ by a^{-1} yileds a unit proves that $(x+a)$ is a unit because

$$\left(a^{-1}(x + a)\right)^{-1} a^{-1}(x + a) = 1 \Rightarrow \left(\left(a^{-1}(x + a)\right)^{-1} a^{-1}\right)(x + a) = 1$$

□

1.7 Problem 17

1.7.1 Question

Let R and S be rings. Prove that the direct product $R \times S$ is a ring under componentwise addition and multiplication. Prove that $R \times S$ is commutative if and only if both R and S are commutative. Prove that $R \times S$ has an identity if and only if both R and S have identities.

1.7.2 Answer

To prove that $R \times S$ is a ring under componentwise addition and multiplication we must prove first that it is a nonempty subgroup under addition, then that it is closed under multiplication.

Let (r, s) and (r', s') be elements of $R \times S$

Proof.

$$(r, s) + (r', s') = (r + r', s + s')$$

Thus, the group is closed under addition by closure of addition on R, S. Moreover we have closure under additive inverses as $(r, s) + (-r, -s) = (0, 0)$ for any r, s. Lastly we know that the group is nonempty for it contains at least the element $(0, 0)$ as each of the groups R, S have additive identities.

The group is closed under multiplication since R, S are closed under multiplication that is $(r, s)(r', s') = (rr', ss')$ and $(rr', ss') \in R \times S$ by closure of R, S under multiplication. □

$R \times S$ is commutative if and only if R, S are both commutative

Proof. Let $r, r' \in R$ and $s, s' \in S$.

First we prove ($\Rightarrow$) that $R \times S$ is commutative if R and S are both commutative.

$$(r, s)(r', s') = (rr', ss') = (r'r, s's) = (r', s')(r, s)$$

Now we prove ($\Leftarrow$) that if $R \times S$ is commutative then both R and S are commutative. For if $R \times S$ commute then in particular the elements of form $(\bar{r}, s)$ and $(r, \bar{s})$ (for $\bar{r}$ and $\bar{s}$ fixed elements of R and S respectively) commute with every other element. This implies that S and R respectively are commutative as $(r, \bar{s})(r', \bar{s}) = (r', \bar{s})(r, \bar{s}) \Rightarrow rr' = r'r$ and $(\bar{r}, s)(\bar{r}, s') = (\bar{r}, s')(\bar{r}, s) \Rightarrow ss' = s's$

Thus we have established that $R \times S$ is commutative if and only if R and S are both commutative as desired. □

We next prove that $R \times S$ has identity if and only if both R and S have identity.

Proof. We first prove ($\Rightarrow$) that $R \times S$ has identity if R and S both have identity.

$(1_R, 1_S)$ is the identity of $R \times S$ as for arbitrary $r \in R, s \in S$ we have $(1, 1)(r, s) = (r, s) = (r, s)(1, 1)$

Now we prove that if $(\hat{r}, \hat{s})$ is the identity in $R \times S$ then $\hat{r}$ and $\hat{s}$ are the identities in R and S respectively

Given arbitrary $r \in R, s \in S$ we have $(\hat{r}, \hat{s})(r, s) = (\hat{r}r, \hat{s}s) = (r, s) = (r\hat{r}, s\hat{s}) = (r, s)(\hat{r}, \hat{s})$ so it follows that $\hat{r}$ and $\hat{s}$ are identities in R and S respectively as claimed. □

1.8 Problem 18

1.8.1 Question

Prove that $\{(r, r) \mid r \in R\}$ is a subring of $R \times R$.

1.8.2 Answer

$\{(r, r) \mid r \in R\}$ is a subring of $R \times R$.

Proof. This set forms an additive group since given $r, r' \in R$ we have $(r, r) + (r', r') = (r+r', r+r')$ and $r+r' \in R$ by closure of R under addition. Moreover $R \times R$ is closed under additive inverses since $(r, r) + (-r, -r) = (0, 0)$ and $-r$ is in R for each r by closure of R under additive inverses. Also we know that $R \times R$ is nonempty since R contains 0 by group properties, implying that $(0, 0) \in R \times R$

It remains to confirm that $R \times R$ is closed under the multiplication operation. So, similar to the above we observe that this follows from the same property of R. That is, $(r, r)(r', r') = (rr', rr')$ and rr' is in R by closure of R under multiplication.

Finally we note that throughout the above each sum, inverse, product is of the desired form: (r, r) for $r \in R$. Hence, we have shown that (r, r) is a subring of $R \times R$ as desired. $\square$