EXERCISES 4

Please submit solutions by 3pm on Thursday 8th March to the pigeonholes in 4W (ground floor).

(W) = Warm-up; (H) = Homework; (A) = Additional.

1. (W) Let R be a commutative ring, and let $a \in R$. Show that the equation $x^2 = a$ has at most two solutions when R is an integral domain. Can you find a commutative ring R and a nonzero $a \in R$ such that $x^2 = a$ has *more than* two solutions? [Hint: experiment with rings of the form $\mathbb{Z}_n$.]

2. (W) Let R and S be rings. Show that $R \times S = \{(r, s) \mid r \in R,\ s \in S\}$ becomes a ring if we define

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{and} \quad (a, b) \cdot (c, d) = (ac, bd)$$

for $a, c \in R$ and $b, d \in S$; this ring is the *direct product* of R with S. [Hint: you require only the definition of a ring from week one to solve this problem.]

3. (H) Consider the evaluation homomorphism $\phi\colon \mathbb{R}[x] \to \mathbb{C}$ defined by setting $\phi(f) = f(i)$; this is simply Example 2.6 in the special case $R = \mathbb{C}$, $S = \mathbb{R}$ and the element $r = i = \sqrt{-1} \in \mathbb{C}$.

(1) Identify $\mathrm{Ker}(\phi)$ and prove carefully your assertion [Hint: the division algorithm!].

(2) What can we conclude from the First Isomorphism Theorem?

4. (H) Let R be a ring with 1 such that the number $|R|$ of elements in R is finite. Show that:

(1) the number of elements of R is divisible by $\mathrm{char}(R)$ [Hint: use Lemma 2.19 and apply Lagrange's theorem from Algebra 1A];

(2) if $|R| = p$ is a prime number, then $R \cong \mathbb{Z}_p$.

(3) if R is an integral domain, then it is a field. [Hint: for $0 \neq a \in R$, show that multiplication by a is a bijection from R to R.]

5. (A) Let I, J be ideals in a ring R.

(1) Prove that the set $I + J := \{a + b \in R \mid a \in I, b \in J\}$ is an ideal in R (so it's a subring and therefore a ring in its own right), and that J is an ideal in the ring $I + J$.

(2) Prove that $I \cap J := \{a \in R \mid a \in I, a \in J\}$ is an ideal in the ring I (where again we use the fact that since I is an ideal, it's a subring and therefore a ring in its own right).

(3) Prove the *second isomorphism theorem*[1], namely, that the quotient ring $I/(I \cap J)$ is isomorphic to the quotient ring $(I + J)/J$.

The course website is: `http://people.bath.ac.uk/dmjc20/Alg2B/`

[1]This may be thought of as follows. We can't take the quotient of I by J, because J needn't be a subset of I. However, there are two operations that are pretty close:

(a) one is to replace J by a smaller ideal that fits inside I and then take the quotient, i..e, consider $I/(I \cap J)$;

(b) the other is to replace I by a larger ideal that contains J and then take the quotient, i.e., consider $(I + J)/J$.

The conclusion of the second isomorphism theorem tells us that these two options give the same answer!

Solutions 4

1. (1) If $x^2 = a$ has no solution there is nothing to prove. Otherwise, suppose that $b \in R$ provides one solution. If $c \in R$ is any solution we have

$$(c - b) \cdot (c + b) = c^2 - b^2 = a - a = 0.$$

Since R is an integral domain. we have either $c = b$ or $c = -b$, so there can be at most two solutions.

(2) Consider the ring $\mathbb{Z}_8$. Then $[1]^2 = [3]^2 = [-3]^2 = [-1]^2 = [1]$ and so $x^2 = [1]$ has four solutions, namely $[1], [3], [5], [7]$.

2. The idea is to show that each defining property of a ring holds for $R \times S$ using the corresponding property of R and S.

Both R and S are non-empty, so the corresponding pair of elements defines an element of $R \times S$ and hence $R \times S$ is nonempty. The operations of addition and multiplication defined in the question give binary operations on $R \times S$, because $a + c, ac \in R$ and $b + d, bd \in S$ - this follows from the fact that addition and multiplication are binary operations on R and S.

To show that $R \times S$ is an abelian group, let $a, c, e \in R$ and $b, d, f \in S$. We have that

$$\begin{aligned}
\big((a, b) + (c, d)\big) + (e, f) &= (a + c, b + d) + (e, f) \\
&= \big((a + c) + e, (b + d) + f\big) \\
&= \big(a + (c + e), b + (d + f)\big) && \text{by associativity of } + \text{ in } R \text{ and } S \\
&= (a, b) + \big((c + e, d + f)\big) \\
&= (a, b) + \big((c, d) + (e, f)\big),
\end{aligned}$$

so addition in $R \times S$ is associative. Also, since addition is commutative in both R and S, we have

$$(a, b) + (c, d) = (a + c, b + d) = (c + a, d + b) = (c, d) + (a, b)$$

so addition is commutative in $R \times S$. Also, if $0_R \in R$ and $0_S \in S$ denote the zero elements, then

$$(a, b) + (0_R, 0_S) = (a + 0_R, b + 0_S) = (a, b),$$

so (using commutativity of addition) we have that $(0_R, 0_S)$ is the zero element in $R \times S$. Given an element $(a, b) \in R \times S$, the additive inverses $-a \in R$ and $-b \in S$ satisfy

$$(a, b) + (-a, -b) = (a + (-a), b + (-b)) = (0_R, 0_S),$$

so (again using commutativity of addition) we have that $(-a, -b)$ is the additive inverse of (a, b).

Checking associativity of multiplication is more-or-less identical to associativity of addition:

$$\begin{aligned}
\big((a, b) \cdot (c, d)\big) \cdot (e, f) &= (ac, bd) \cdot (e, f) \\
&= \big((ac)e, (bd)f\big) \\
&= \big(a(ce), b(df)\big) && \text{by associativity of } \cdot \text{ in } R \text{ and } S \\
&= (a, b) \cdot \big((ce, df)\big) \\
&= (a, b) \cdot \big((c, d) \cdot (e, f)\big)
\end{aligned}$$

as required.

Finally to check the distributivity identities, note that

$$\begin{aligned}
(a,b)\cdot\big((c,d)+(e,f)\big)+(e,f) &= (a,b)\cdot(c+e,d+f) \\
&= \big(a(c+e),b(d+f)\big) \\
&= \big(ac+ae,bd+bf)\big) && \text{by distributivity in both } R \text{ and } S \\
&= (ac,bd)+(ae,bf) \\
&= (a,b)\cdot(c,d)+(a,b)\cdot(e,f),
\end{aligned}$$

and similarly for the other distributivity axiom.

[This final part is not necessary, but if you really like your rings to have a unit, note that $(a,b)\in R\times S$ is a unit iff there exists $(c,d)\in R\times S$ such that

$$(1_R,1_S)=(a,b)\cdot(c,d)=(ac,bd).$$

This is equivalent to saying that $1_R=ac$ and $1_S=bd$, which in turn is equivalent to a being a unit in R and b being a unit in S. Therefore, $R\times S$ has a unit iff both R and S have units.]

3. (1) We claim that $\mathrm{Ker}(\phi)=\mathbb{R}[x](x^2+1)$ is the ideal generated by the element $x^2+1\in\mathbb{R}[x]$. To prove this we establish that the right hand side is contained in the left hand side and vice versa. First, if $f=g(x^2+1)\in\mathbb{R}[x](x^2+1)$, then $\phi(f)=g(i)\cdot(i^2+1)=0$, so $f\in\mathrm{Ker}(\phi)$. Conversely, if $f\in\mathrm{Ker}(\phi)$, then applying division by x^2+1 yields quotient $q\in\mathbb{R}[x]$ and remainder $r=bx+a\in\mathbb{R}[x]$ such that

$$f=(x^2+1)q+bx+a.$$

Our assumption gives $0=f(i)=0\cdot q(i)+bi+a$, i.e., that $a+bi=0\in\mathbb{C}$ which forces $a=b=0$. Therefore $f=(x^2+1)q\in\mathbb{R}[x](x^2+1)$ as required. This shows that $\mathrm{Ker}(\phi)=\mathbb{R}[x](x^2+1)$.

(2) The map ϕ is surjective, because for $a+bi\in\mathbb{C}$, we have $\phi(a+bx)=a+bi$. The first isomorphism theorem tells us that the induced map

$$\overline{\phi}\colon \frac{\mathbb{R}[x]}{\mathbb{R}[x](x^2+1)}\longrightarrow\mathbb{C}$$

is an isomorphism. We'll see later in the course that a standard method to construct fields is to consider quotients of a polynomial ring $\Bbbk[x]$ by an ideal.

In this case, perhaps the result comes as no surprise because multiplying and adding in $\mathbb{C}$ is just like working with polynomial expressions in i and then identifying i^2 with -1, that is, identifying i^2+1 with 0.

4. (1) Since R is finite, the subring $\mathbb{Z}1_R$ must be finite, and Lemma 2.19 implies that $\mathbb{Z}1_R\cong\mathbb{Z}_n$ where $n=\mathrm{char}(R)>0$. It follows that $|\mathbb{Z}1_R|=n=\mathrm{char}(R)$. Since $\mathbb{Z}1_R$ is a subring of R, it is in particular a subgroup under addition, and Lagrange's theorem implies that $|R|$ is divisible by $\mathrm{char}(R)=|\mathbb{Z}1_R|$.

(2) We have $|R|\geq 2$, so $\mathbb{Z}1_R$ has at least two elements: $0_R,1_R$. Thus $|\mathbb{Z}1_R|=\mathrm{char}\,(R)$ is at least 2, and it divides the prime number $|R|$ by part (1), so $|\mathbb{Z}1_R|=|R|$. This forces $R=\mathbb{Z}1_R$, and the result follows from Lemma 2.19(2).

(3) Let R be a finite integral domain. Let $0\neq a\in R$ and consider the map $f\colon R\to R$ sending $u\mapsto ua$. To see that this map is injective, suppose $u,v\in R$ satisfy $ua=va$. The cancellation property of R implies that $u=v$ because $0\neq a$. Moreover, since R is finite, it follows that f is bijective ($|Ra|=|R|$ and $Ra\subseteq R$ implies that $Ra=R$). In partiular there exist $u\in R$ such that $ua=1$ and u is then a multiplicative inverse of a. We have thus shown that every $0\neq a\in R$ has a multiplicative inverse. Hence R is a field.

5. (1) To see that $I+J$ is an ideal in R, note that $0 = 0+0 \in I+J$, so $I+J \neq \emptyset$. Let $a_1+b_1, a_2+b_2 \in I+J$ for elements $a_1, a_2 \in I$, $b_1, b_2 \in J$. Consider also $r \in R$. Since I, J are ideals, we have that $a_1 - a_2, ra_1, a_1 r \in I$ and $b_1 - b_2, rb_1, b_1 r \in J$, we have that

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I + J,$$

and that $r(a_1 + b_1) = ra_1 + rb_1 \in I + J$ and $(a_1 + b_1)r = a_1 r + b_1 r \in I + J$. This shows that $I + J$ is an ideal of R.

To see that J is an ideal in $I + J$, we know $0 \in J$, so $J \in I + J$ is a non-empty subset. Since J is an ideal, we already know that $a, b \in J \Rightarrow a - b \in J$. Similarly, we already know that $a \in J$ and $r \in R$ implies that $a \cdot r, r \cdot a \in J$, so the same is true if we restrict attention only to those elements $r \in I + J$. Therefore J is an ideal in the ring $I + J$.

(2) To see that $I \cap J$ is an ideal in R, we have $0 \in I \cap J$, so $I \cap J \neq \emptyset$. Let $a, b \in I \cap J$ and let $r \in R$. As I, J are ideals of R, it follows that $a - b, ra, ar$ lie in both I and J, so $a - b, ra, ar \in I \cap J$. This shows $I \cap J$ is an ideal of R. The proof that $I \cap J$ is an ideal in the ring I is identical to that of part (1) above.

(3) Consider the map $\phi\colon I \to (I + J)/J$ given by $\phi(a) = a + J$.

For $a, b \in I$, we have that

$$\phi(a + b) = (a + b) + J = a + J + b + J = \phi(a) + \phi(b),$$

and that

$$\phi(a \cdot b) = a \cdot b + J = a + J + b + J = \phi(a) \cdot \phi(b),$$

so ϕ is a ring homomorphism.

Let $a \in \mathrm{Ker}(\phi) \subseteq I$. Then $\phi(a) = 0$ gives $a + J = J$, or equivalently, $a \in J$, so in fact $a \in I \cap J$. We have $I \cap J \subseteq \mathrm{Ker}(\phi)$, so $\mathrm{Ker}(\phi) = I \cap J$. The first isomorphism theorem now implies that

$$\frac{I}{I \cap J} \cong \mathrm{Image}(\phi),$$

so it remains to show that ϕ is surjective. For $a \in I$ and $b \in J$, consider $(a + b) + J \in (I + J)/J$. Then for $a \in I$, we have that

$$\phi(a) = a + J = a + b + J$$

because $b \in J$, so ϕ is surjective as required.