ALGEBRA 2B (MA20217)

PROBLEM SHEET 6 WITH SOLUTIONS

1 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 called the direct product of R and S).

Solution: *We simply check all the conditions.*

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

$$\begin{aligned}\big((a,b)+(c,d)\big)+(e,f) &= (a+c,b+d)+(e,f)\\ &= \big((a+c)+e,(b+d)+f\big)\\ &= \big(a+(c+e),b+(d+f)\big)\\ &= (a,b)+\big((c+e,d+f)\big)\\ &= (a,b)+\big((c,d)+(e,f)\big),\end{aligned}$$

where the third line comes from associativity of addition in R and S, 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 $R \times S$.

Next,

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

so $(0_R,0_S)$ is the zero element in $R\times S$ (in particular $R\times S \neq \varnothing$).

Then, 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 $(-a,-b)$ is the additive inverse of (a,b).

Checking associativity of multiplication is more or less identical to associativity of addition and we don't need to repeat it.

To check the distributivity laws, note that

$$\begin{aligned}(a,b)\cdot\big((c,d)+(e,f)\big)+(e,f) &= (a,b)\cdot(c+e,d+f)\\ &= \big(a(c+e),b(d+f)\big)\\ &= \big(ac+ae,bd+bf)\big)\\ &= (ac,bd)+(ae,bf)\\ &= (a,b)\cdot(c,d)+(a,b)\cdot(e,f),\end{aligned}$$

where again the third line comes from distributivity in R and S, and similarly for right multiplication.
Finally, $(1_R, 1_S) \cdot (a, b) = (1_R \cdot a, 1_R \cdot b) = (a, b)$ so $(1_R, 1_S)$ is the multiplicative identity for $R \times S$.

2 H Let R be a commutative ring, and let $a \in R$. Show that if R is an integral domain then the equation $x^2 = a$ has at most two solutions in R. Find a commutative ring R and an element $a \in R$ such that $x^2 = a$ has more than two solutions.

Solution: *If $x^2 = a$ has no solution there is nothing to prove. Otherwise, suppose that $b \in R$ provides one solution, i.e. that $b^2 = a$. 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, this implies either $c = b$ or $c = -b$, so there can be at most two solutions, namely $\pm b$.
In $\mathbb{Z}/8$, we have $1^2 = 3^2 = 5^2 = 7^2 = 1$, so we can do it, even with $a \neq 0$. Another way to do it is to take any commutative ring R and consider $R[s, t]/\langle s^2, t^2 \rangle$, where $\langle s^2, t^2 \rangle = s^2 R + t^2 R = \{\lambda s^2 + \mu t^2 \mid \lambda, \mu \in R\}$ is the ideal generated by s^2 and t^2: then $0^2 = s^2 = t^2 = 0$.

3 H Consider the evaluation homomorphism $\varphi \colon \mathbb{R}[t] \to \mathbb{C}$ defined by setting $\phi(f) = f(i)$. Identify $\operatorname{Ker}(\phi)$: using the division algorithm, prove carefully that your answer is correct.
What does the First Isomorphism Theorem tell us in this case?

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

$$0 = f(i) = 0 \cdot q(i) + bi + a$$

so $a + bi = 0 \in \mathbb{C}$, i.e. $a = b = 0$. Therefore $f = (t^2 + 1)q \in (t^2 + 1)\mathbb{R}[t]$, as required.
The map φ is surjective, because for $a + bi \in \mathbb{C}$, we have $\varphi(a + bt) = a + bi$. The first isomorphism theorem tells us that the induced map

$$\overline{\varphi} \colon \mathbb{R}[t]/(t^2 + 1)\mathbb{R}[t] \longrightarrow \mathbb{C}$$

is an isomorphism.

4 W Prove that if I and J are ideals in a ring R, then $I+J$, IJ and $I \cap J$ are ideals in R and $IJ \subseteq I \cap J \subseteq I+J$.

Solution: *$I+J = \{a+b \mid a \in I,\ b \in J\}$ is closed under addition because $(a+b)+(a'+b') = (a+a')+(b+b') \in I+J$. It is closed under multiplication by $r \in R$ because $r(a+b) = ra+rb \in I+J$*
$IJ = \{\sum_{i=1}^{k} a_i b_i \mid k \in \mathbb{N},\ a_i \in I,\ b_i \in J\}$ is closed under addition by definition. It is closed under multiplication by $r \in R$ because

$$r \cdot \left(\sum_{i=1}^{k} a_i b_i \right) = \sum_{i=1}^{k} r a_i b_i$$

and $ra_i \in I$ because $a_i \in I$, and $b_j \in J$ so the right-hand side is in IJ.
$I \cap J$ is closed under addition and multiplication by $r \in R$ because I and J are both closed under addition and multiplication by $r \in R$.
If $c = \sum_{i=1}^{k} a_i b_i \in IJ$ then $a_i b_i \in I$ and $a_i b_i \in J$ so $ca \in I \cap J$ so $IJ \subseteq I \cap J$.
If $c \in I \cap J$ then $c = c + 0 \in I+J$, so $I \cap J \subseteq I+J$.

5 A Let R be a finite ring, i.e. the number $|R|$ of elements of R is finite. Show that $|R|$ is divisible by $\operatorname{char} R$. Deduce that if $|R| = p$ is prime, then $R \cong \mathbb{Z}/p\mathbb{Z}$.
By considering the map $m_a \colon R \to R$ given by $m_a(b) = ab$, or otherwise, show that a finite integral domain is a field.

Solution: *The additive subgroup P of R generated by 1_R is of order* $\operatorname{char} R$ *so* $\operatorname{char} R$ *divides $|R|$ by Lagrange's theorem. If $|R| = p$ is prime then $|R| > 1$ so $0_R \neq 1_R$: hence $|P| \geq 2$ and so, since $|P|$ divides $|R|$ which is prime, we have $P = R$. But $P \cong \mathbb{Z}/p\mathbb{Z}$ by the map $1_P \mapsto 1$.*
Let R be a finite integral domain. Let $0 \neq a \in R$ and consider the map $m_a \colon R \to R$ sending $b \mapsto ab$. This map is injective: for if $b, c \in R$ satisfy $ab = ac$ then $b = c$ because R is anm integral domain. But then, since R is finite, it follows that m_a is bijective, so in particular there exists $d \in R$ such that $ad = 1$, so d is then a multiplicative inverse of a. We have thus shown that every nonzero $a \in R$ has a multiplicative inverse: that is, that R is a field.

GKS, 22/3/24