HOMEWORK #7 – MATH 435

SOLUTIONS

Chapter 4, Section 3: #1 If R is a commutative ring and $a \in R$, let $L(a) = \{x \in R \,|\, xa = 0\}$. Prove that $L(a)$ is an ideal of R.

Solution: Indeed, we need to show that $L(a)$ is a subgroup under addition, and closed under multiplication by elements of R. First suppose that $x, y \in L(a)$. Then $xa = 0$ and $ya = 0$ so that $(x+y)a = xa + ya = 0 + 0 = 0$ which shows that $L(a)$ is closed under addition. Notice that $0a = 0$ so that $0 \in L(a)$ and finally note that if $x \in L(a)$, then $0 = -0 = -(xa) = (-x)a$ which proves that $-x \in L(a)$ as well. We have shown that $L(a)$ is a subgroup under addition.

Now we show it is closed under multiplication from elements of R. Indeed, to show this, suppose that $r \in R$ and $x \in L(a)$. Then $(rx)a = r(xa) = r0 = 0$ which shows that $rx = xr \in L(a)$ and so we have shown that $L(a)$ is an ideal as desired.

Chapter 4, Section 3: #5 If I is an ideal of R and A is a subring of R, show that $I \cap A$ is an ideal of A.

Solution: We already know that the intersection of two subgroups is again a subgroup, so $I \cap A$ is already a subgroup of A under addition. Now we show that $I \cap A$ is closed under multiplication from arbitrary elements of A. Pick $a \in A$ and $x \in I \cap A$. Then $x \in I$ and $x \in A$. Thus $ax \in I$ (since I is an ideal of R and $a \in A \subseteq R$) and $ax \in A$ (since $a, x \in A$ and A is closed under multiplication since it is a ring). Thus $I \cap A$ is a ring as desired.

Of course, $I \cap A$ need not be an ideal of R (can you find an example?).

Chapter 4, Section 3: #18 Show that $R \oplus S$ is a ring and that the subrings $\{(r, 0) \,|\, r \in R\}$ and $\{(0, s) \,|\, s \in S\}$ are ideals of $R \oplus S$ isomorphic (as rings) to R and S respectively.

Solution: First we show that $R \oplus S$ is a ring. Certainly it is closed under multiplication and addition (componentwise). Now we have other things to check.

Associativity of $+$:

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

Associativity of $\cdot$:

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

Additive identity:

$$(0, 0) + (r, s) = (0 + r, 0 + s) = (r, s) = (r + 0, s + 0) = (r, s) + (0, 0)$$

Additive inverses: Given $(r, s) \in R \oplus S$, then $(r, s) + (-r, -s) = (r - r, s - s) = (0, 0) = (-r + r, -s + s) = (-r, -s) + (r, s)$.

Distributive property:

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

We have now shown that $R \oplus S$ is a ring.

Now $\{(r, 0) \,|\, r \in R\}$ is easily seen to be a subring. Indeed, it's already a subgroup under addition and also note that $(r, 0)(a, b) = (ra, 0b) = (ra, 0)$ and likewise $(a, b)(r, 0) = (ar, b0) = (ar, 0)$ both of which are in $\{(r, 0) \,|\, r \in R\}$. Thus it is an ideal, and not just a subring. Likewise $\{(0, s) \,|\, s \in S\}$ is a subring.

Consider the map $\phi : R \to \{(r, 0) \,|\, r \in R\}$ defined by the rule $\phi(r) = (r, 0)$. This is certainly bijective. Of course

$$\phi(r + r') = (r + r', 0) = (r, 0) + (r', 0) = \phi(r) + \phi(r')$$

and

$$\phi(rr') = (rr', 0) = (r, 0)(r', 0) = \phi(r)\phi(r').$$

which shows that ϕ is a homomorphism. Thus ϕ is an isomorphism and R is isomorphic with $\{(r, 0) \,|\, r \in R\}$.

Similarly, S is isomorphic with $\{(0, s) \,|\, s \in S\}$.

Chapter 4, Section 3: #20 If I, J are ideals of R, let $R_1 = R/I$ and $R_2 = R/J$. Show that $\phi : R \to R_1 \oplus R_2$ defined by $\phi(r) = (r + I, r + J)$ is a homomorphism of R into $R_1 \oplus R_2$ such that $\ker \phi = I \cap J$.

Solution: First we show it is a homomorphism:

$$\begin{aligned} \phi(rr') &= ((rr') + I, (rr') + J) = (r + I, r + J)(r' + I, r' + J) = \phi(r)\phi(r') \\ \phi(r + r') &= ((r + r') + I, (r + r') + J) = (r + I, r + J) + (r' + I, r' + J) = \phi(r) + \phi(r') \end{aligned}$$

Note that $\ker \phi = \{r \in R \,|\, (r+I, r+J) = (0+I, 0+J)\} = \{r \in R \,|\, r \in I, r \in J\} = I \cap J$ as desired.

Chapter 4, Section 3: #22 Let $m, n \in \mathbb{Z}$ be two relatively prime integers, and set $I_m = m\mathbb{Z}$ and $I_n = n\mathbb{Z}$.

(a) What is $I_m \cap I_n$?

(b) Use the result of #20 to show that there is an injective homomorphism from $\mathbb{Z}/I_{mn}$ to $\mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$.

Solution: **(a)** Note that $I_m \cap I_n$ is the set of all numbers that are multiples of both m and n. Since m and n are relatively prime, this is the same as the integers which are multiples of mn as desired.

(b) It is sufficient to show that there is an isomorphism between $\mathbb{Z}/I_{mn}$ and a subring of $\mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$. We first consider the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$ from #20. Notice that the image of this map is a subring $S \subseteq \mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$. We thus have a surjective homomorphism $\psi : \mathbb{Z} \to S$ (the same map as ϕ, but just with different codomains).

Now, the kernel of ψ is the same as the kernel of ϕ (since they are really the same map in some level). Now, $\ker \psi = \ker \phi = I_m \cap I_n = I_{mn}$ by (a). Thus by the first homomorphism theorem, $\mathbb{Z}/I_{mn} = \mathbb{Z}/\ker \psi \simeq S$, and since S is a subring of $\mathbb{Z}/I_m \oplus \mathbb{Z}/I_n$ we are done.

Chapter 4, Section 4: #3,4 In example 3, show that $M = \{x(2 + i) \,|\, x \in R\}$ is a maximal ideal and that $R/M = \mathbb{Z}_{\text{mod}5}$.

Solution: I'll solve both of these at once. Obviously the second statement implies the first since $\mathbb{Z}_{\text{mod}5}$ is a field.

First consider an arbitrary element $(a+bi)+M \in R/M$. Notice I can rewrite this as:

$$\begin{aligned} & (a+bi)+M \\ = \;& (a-2b+2b+bi)+M \\ = \;& (a-2b)+b(2+i)+M \\ = \;& (a-2b)+M \\ = \;& \big((a-2b)\text{mod } 5\big)+5q+M \\ = \;& \big((a-2b)\text{mod } 5\big)+M \end{aligned}$$

where the third equality follows because $b(2+i) \in M$, the penultimate equality is simply the division algorithm, and the final equality comes because $5 \in M$.

But this means that every element $(a+bi)+M \in R/M$ can be written as one of

$$\begin{aligned} &0+M \\ &1+M \\ &2+M \\ &3+M \\ &4+M \end{aligned}$$

since those are the only possibilities of an integer modulo 5. In particular, $R/M = \{0+M, 1+M, 2+M, 3+M, 4+M\}$ but of course, some of those elements might be repeats.

We will now show that that $0+M \neq 1+M$ which at least shows that the first two have no repeats. For a contradiction, suppose they were equal, then $1 \in M$ and so $1+0i = (a+bi)(2+i) = (2a-b)+(2b+a)i$ thus $2b+a=0$ and $2a-b=1$. Thus $a=-2b$ and plugging this in we get $2(-2b)-b=1$ and so $b=-\frac{1}{5}$ which is not an integer, a contradiction.

Now, certainly for integers $a, b \in \{0,1,2,3,4\}$, we have that

$$(a+M)+(b+M) = \big((a+b)\text{mod}5\big)+5q+M = \big((a+b)\text{mod}5\big)+M$$
$$(a+M)(b+M) = \big((ab)\text{mod}5\big)+5q'+M = \big((ab)\text{mod}5\big)+M$$

where q and q' appear in the division algorithm. In particular, it follows we have a natural surjective ring homomorphism $\gamma : \mathbb{Z}_{\text{mod}5} \to R/M$ which sends a to $a+M$. But then $|R/M|$ divides 5 by Lagrange's theorem (and the corollary from the first midterm). But R/M has at least 2 elements and so $|R/M| = 5$. But then γ is clearly bijective (since it is a surjective map between two sets both of which have 5 elements) and so we have completed the proof.