Algebraic Structures- Solutions of Homework 9

written by Motke Porat

January 2018

1 Question 1.

1.1 (b):

Assume that R is a finite integral domain, so denote $R = \{r_1, ..., r_n\}$. For every $0 \neq r \in R$ we have $|rR| = |R|$, otherwise there exist $r_i, r_j \in R$ such that $r_i \neq r_j$ but $rr_i = rr_j$, so $r(r_i - r_j) = 0$ and as R has no zero divisors and $r \neq 0$, we get that $r_i - r_j = 0$, i.e., that $r_i = r_j$. So $|rR| = |R|$ which actually means that $rR = R$ (as R is finite) and therefore there exists $x \in R$ for which $rx = 1$. Therefore, every nonzero element in R has an inverse in R so R is a field.

2 Question 2.

2.1 (c):

Let $I \subset J \subset R$ where $I, J \lhd R$. **We first show that** $J/I \lhd R/I$:

- If $a + I, b + I \in J/I$, i.e., if $a, b \in J$, then
$$(a + I) - (b + I) = (a - b) + I \in J/I$$
as $J \leq R$ and hence $a - b \in J$.
- If $a + I \in J/I$ and $r + I \in R/I$, i.e., if $a \in J$ and $r \in R$, then
$$(a + I)(r + I) = ar + I \in J/I, \quad (r + I)(a + I) = ar + I \in J/I$$
as $J \lhd R$ and hence $ra, ar \in J$.

Next, define the mapping
$$\phi : R/I \to R/J \text{ by } \phi(r + I) = r + J.$$
It is easy to see that ϕ is a ring homomorphism: if $r_1, r_2 \in R$ then
$$\phi((r_1 + I) + (r_2 + I)) = \phi((r_1 + r_2) + I) = (r_1 + r_2) + J = \phi(r_1 + I) + \phi(r_2 + I)$$
and
$$\phi((r_1 + I)(r_2 + I)) = \phi(r_1r_2 + I) = r_1r_2 + J = \phi(r_1 + I)\phi(r_2 + I),$$
that $\ker \phi = J/I$:
$$r + I \in \ker \phi \iff \phi(r + I) = J \iff x + J = J \iff x \in J \iff x + I \in J/I$$
so from the first homomorphism theorem it follows that
$$(R/I)/(J/I) \approx \phi(R/I) = R/J.$$

3 Question 3.

Let R be a commutative ring with a unit $1 \neq 0$ and $I_1, ..., I_k \lhd R$.

3.1 (a):

The mapping $\phi : R \to R/I_1 \times ... \times R/I_k$ defined by $\phi(r) = (r + I_1, ..., r + I_k)$ is a ring homomorphism: For every $r_1, r_2 \in R$ we have

$$\begin{aligned}\phi(r_1 + r_2) &= ((r_1 + r_2) + I_1, ..., (r_1 + r_2) + I_k) \\ &= (r_1 + I_1, ..., r_1 + I_k) + (r_2 + I_1, ..., r_2 + I_k) = \phi(r_1) + \phi(r_2)\end{aligned}$$

and

$$\begin{aligned}\phi(r_1 r_2) &= (r_1 r_2 + I_1, ..., r_1 r_2 + I_k) \\ &= (r_1 + I_1, ..., r_1 + I_k)(r_2 + I_1, ..., r_2 + I_k) = \phi(r_1)\phi(r_2).\end{aligned}$$

We can easily see that $\ker \phi = I_1 \cap ... \cap I_k$, as

$$\begin{aligned}r \in \ker \phi &\iff (r + I_1, ..., r + I_k) = (I_1, ..., I_k) \\ &\iff r + I_1 = I_1, ..., r + I_k = I_k \iff r \in I_1, ..., r \in I_k \\ &\iff r \in I_1 \cap ... \cap I_k.\end{aligned}$$

3.2 (b):

We prove this by induction. If $k = 2$, we assume that $I_1 + I_2 = R$, therefore there exist $t_1 \in I_1$ and $t_2 \in I_2$ such that $t_1 + t_2 = 1$. Then

$$t_1 + I_2 = (t_1 + t_2) + I_2 = 1 + I_2 \quad \text{and} \quad t_2 + I_1 = (t_2 + t_1) + I_1 = 1 + I_1$$

and hence for every $r, s \in R$

$$rt_2 + st_1 + I_1 = r + I_1 \quad \text{and} \quad rt_2 + st_1 + I_2 = s + I_2,$$

which imply that

$$\phi(rt_2 + st_1) = ((rt_2 + st_1) + I_1, (rt_2 + st_1) + I_2) = (r + I_1, s + I_2)$$

and this proves that ϕ is onto $R/I_1 \times R/I_2$. The fact that $I_1 \cap I_2 = I_1 \cdot I_2$ follows from a previous exercise from the homework.

Next, assume that it is true for k and prove it for $k+1$: let $I_1, ..., I_{k+1} \lhd R$ such that $I_i + I_j = R$ for every $i \neq j$. Denote $I = I_1 \cdot ... \cdot I_k$, so $I + I_{k+1} = R :$ as $I_i + I_{k+1} = R$ for every $i = 1, ..., k$, there exist $x_i \in I_i$ and $y_i \in I_{k+1}$ for $i = 1, ..., k$ such that $x_i + y_i = 1$. Then

$$1 = (x_1 + y_1) \cdot ... \cdot (x_k + y_k) = x_1 \cdot ... x_k + y \in I + I_{k+1} \implies I + I_{k+1} = R$$

as y is a sum of products of $y_1, ..., y_k$ which are all in I_{k+1}. From the induction hypothesis we know that $I = I_1 \cdot ... \cdot I_k = I_1 \cap ... \cap I_k$ and from the first part and the homomorphism theorem we know that

$$R/I \approx R/I_1 \times ... \times R/I_k.$$

From what we proved for $k = 2$ we know that

$$\phi : R \to R/I \times R/I_{k+1} \approx R/I_1 \times ... \times R/I_{k+1}$$

is onto $R/I \times R/I_{k+1}$ and from the first part we know that

$$\ker \phi = I \cap I_{k+1} = I_1 \cap ... \cap I_{k+1}$$

and hence (once again) from the homomorphism theorem, we get that

$$R/(I_1 \cap ... \cap I_{k+1}) \approx R/I_1 \times ... \times R/I_{k+1}.$$

3.3 (c):

Let $I_j = (n_j) = n_j\mathbb{Z}$. As $gcd(n_i, n_j) = 1$ for all $i \neq j$, it follows that $I_i + I_j = \mathbb{Z}$ for all $i \neq j$, therefore from previous part of the question: the mapping

$$\phi : \mathbb{Z} \to \mathbb{Z}/(n_1) \times ... \times \mathbb{Z}/(n_k)$$

is an epimorphism (onto), so for every $a_1, ..., a_k \in \mathbb{Z}$ there exists $x \in \mathbb{Z}$ for which

$$\phi(x) = (a_1 + (n_1), ..., a_k + (n_k)) \Longrightarrow x \equiv a_1\,(mod\, n_1), ..., x \equiv a_k\,(mod\, n_k).$$

3.4 (d):

For every $1 \leq i \leq k$, denote

$$f_i(x) = a_0^{(i)} + ... + a_d^{(i)} x^d.$$

From part (c) we know that for every $1 \leq t \leq d$ there exists $a_t \in \mathbb{Z}$ for which

$$a_t \equiv a_t^{(i)}\,(mod\, n_i), \quad \forall 1 \leq i \leq k.$$

Therefore, if we let $f(x) = a_0 + ... + a_d x^d$, then

$$f(x) \equiv f_i(x)\,(mod\, n_i), \quad \forall 1 \leq i \leq k.$$

4 Question 4.

4.1 (b):

An ideal $I = (a)$ is prime if and only if a ia prime in R. Recall that if $\alpha = a + b\sqrt{-1}$ then $\overline{\alpha} = a - b\sqrt{-1}$ and $|\alpha|^2 = a^2 + b^2 \in \mathbb{N} \cup \{0\}$.

- $2 = (1 + \sqrt{-1})(1 - \sqrt{-1})$ so $2 \mid (1 + \sqrt{-1})(1 - -1])$ but $2 \nmid 1 + \sqrt{-1}$ and $2 \nmid 1 - \sqrt{-1}$, since $|2|^2 = 4$ and $|1 \pm \sqrt{-1}|^2 = 2$. So 2 is not prime.
- If $1 + \sqrt{-1} \mid \alpha\beta$ where $\alpha = a + b\sqrt{-1}$ and $\beta = c + \sqrt{-1}d$, then

  $$2 = |1 + \sqrt{-1}|^2 \mid |\alpha|^2 |\beta|^2 \Longrightarrow 2 \mid |\alpha|^2 \text{ or } 2 \mid |\beta|^2$$

  without loss of generality assume that $2 \mid |\alpha|^2 = a^2 + b^2$, so either a, b are odd or a, b are even: If

  $$2 \mid a, b \Longrightarrow 2 \mid \alpha \Longrightarrow 1 + \sqrt{-1} \mid \alpha$$

as $1+\sqrt{-1} \mid 2$; otherwise, we have

$$2 \mid a+1, b+1 \Longrightarrow 2 \mid (a+1)+(b+1)\sqrt{-1} \Longrightarrow 2 \mid \alpha + (1+\sqrt{-1})$$

and as $1+\sqrt{-1} \mid 2$ we have that $1+\sqrt{-1} \mid \alpha + (1+\sqrt{-1})$ and hence

$$1+\sqrt{-1} \mid \alpha.$$

In any case $1+\sqrt{-1} \mid \alpha$ so $1+\sqrt{-1}$ is prime.

- If $3 \mid \alpha\beta$ then $9 \mid |\alpha|^2|\beta|^2$ which implies (and that is enough in this case) that $3 \mid |\alpha|^2$ or $3 \mid |\beta|^2$, assume without loss of generality that $3 \mid |\alpha|^2 = a^2+b^2$. Simple observation is that both $3 \mid a$ and $3 \mid b$: in $\mathbb{Z}_3$ we have $\overline{0}^2 = \overline{0}, \overline{1}^2 = \overline{1}$ and $\overline{2}^2 = \overline{1}$, therefore if the sum of two squares a^2+b^2 is divisible by 3, i.e., is equal to $\overline{0}$ in $\mathbb{Z}_3$, then the only option is that $\overline{a} = \overline{b} = \overline{0}$ in $\mathbb{Z}_3$, i.e., that both a and b are divisible by 3. Therefore we have

$$3 \mid a, b \Longrightarrow 3 \mid \alpha = a + b\sqrt{-1}$$

and 3 is prime.

5 Question 5.

Let $R = \mathbb{Z}[\sqrt{-5}]$ and $I = (2, 1+\sqrt{-5}) = 2R + (1+\sqrt{-5})R$.

5.1 (a):

Assume that I is generated by some $x \in R$, so $x = a + b\sqrt{-5}$ for some $a, b \in \mathbb{Z}$. Then

$$\begin{aligned}(2, 1+\sqrt{-5}) = (x) &\Longrightarrow 2, 1+\sqrt{-5} \in (x) \Longrightarrow x \mid 2, 1+\sqrt{-5} \\ &\Longrightarrow \|x\|^2 \mid \|2\|^2, \|1+\sqrt{-5}\|^2 \Longrightarrow (a^2+5b^2) \mid 4, 6 \\ &\Longrightarrow a^2+5b^2 = 1 \text{ or } a^2+5b^2 = 2.\end{aligned}$$

If $a^2+5b^2 = 1$ then $a = \pm 1$ and $b = 0$, which imply that $1 \in I$ and hence that there exist $r, s \in R$ such that

$$1 = 2r + (1+\sqrt{-5})s \Longrightarrow 1-\sqrt{-5} = 2(1-\sqrt{-5})r + 6s \Longrightarrow 2 \mid 1-\sqrt{-5}$$

and that is clearly a contradiction. Therefore we must have $a^2+5b^2 = 2$ and this equation has no solution $a, b \in \mathbb{Z}$ so once again it is a contradiction $\Longrightarrow I$ is not generated by any element in R.

6 Question 7.

We have the isomorphism $\phi : \mathbb{H} \to M_{2\times 2}(\mathbb{C})$ defined by

$$\phi(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

and clearly there is the mapping $\varphi : \mathbb{C} \to M_{2\times 2}(\mathbb{R})$ defined by

$$\varphi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

that is a monomorphism (a $1-1$ homomorphism); therefore one can define the mapping $\varphi_2 : M_{2\times 2}(\mathbb{C}) \to M_{2\times 2}(M_{2\times 2}(\mathbb{R})) \approx M_{4\times 4}(\mathbb{R})$ by

$$\varphi_2\left(\begin{pmatrix} z_1 & z_2 \\ z_3 & z_4 \end{pmatrix}\right) = \begin{pmatrix} \varphi(z_1) & \varphi(z_2) \\ \varphi(z_3) & \varphi(z_4) \end{pmatrix}$$

which is also a monomorphism; Finally, we get the mapping $\psi = \varphi_2 \circ \phi : \mathbb{H} \to M_{4\times 4}(\mathbb{R})$ given by

$$\psi(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$$

and as ϕ is an isomorphism and φ_2 is a monomorphism, we get that ψ is a monomorphism.