Solutions to Homework 9

Problem 1. Problem E in chapter 17.

Solution. (1) We will denote the ring by $\mathbb{H}$ and call it the quaternion algebra, or quaternions ($\mathbb{H}$ stands for Hamilton. Sir William Rowan Hamilton was an Irish mathematician who discovered the quaternions). Thus

$$\mathbb{H} = \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} : z, w \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C}).$$

Here $\overline{z}$ denotes the complex conjugate of z. To see that $\mathbb{H}$ is a unital ring note that the 0 matrix is in $\mathbb{H}$ and

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} - \begin{bmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{bmatrix} = \begin{bmatrix} z - z_1 & w - w_1 \\ -\overline{w} + \overline{w_1} & \overline{z} - \overline{z_1} \end{bmatrix} = \begin{bmatrix} z - z_1 & w - w_1 \\ -\overline{w - w_1} & \overline{z - z_1} \end{bmatrix} \in \mathbb{H}$$

so $\mathbb{H}$ is a subgroup of $M_2(\mathbb{C})$. Furthermore

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \cdot \begin{bmatrix} z_1 & w_1 \\ -\overline{w_1} & \overline{z_1} \end{bmatrix} = \begin{bmatrix} zz_1 - w\overline{w_1} & zw_1 + w\overline{z_1} \\ -\overline{w}z_1 - \overline{z}\overline{w_1} & -\overline{w}w_1 + \overline{z}\overline{z_1} \end{bmatrix} = \begin{bmatrix} zz_1 - w\overline{w_1} & zw_1 + w\overline{z_1} \\ -\overline{(zw_1 + w\overline{z_1})} & \overline{zz_1 - w\overline{w_1}} \end{bmatrix} \in \mathbb{H}$$

so $\mathbb{H}$ is closed under multiplication. This shows that $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$. Since the identity matrix $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is in $\mathbb{H}$, we see that $\mathbb{H}$ is a unital subring of $M_2(\mathbb{C})$. Since $\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ are in $\mathbb{H}$ and

$$\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$$

we see that $\mathbb{H}$ is not commutative.

(2) Writing $z = a + bi$, $w = c + di$, where a, b, c, d are real numbers, we have $\overline{z} = a - bi$, $\overline{w} = c - di$ and

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} = \begin{bmatrix} a + bi & c + di \\ -c + di & a - bi \end{bmatrix} = a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + c \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + d \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

(3) This is a straightforward computation.

(4) and (5) We have

$$\begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} \cdot \begin{bmatrix} \overline{z} & -w \\ -\overline{(-w)} & z \end{bmatrix} = \begin{bmatrix} z\overline{z} + w\overline{w} & -zw + wz \\ -\overline{w}\overline{z} + \overline{z}\overline{w} & \overline{w}w + \overline{z}z \end{bmatrix} = \begin{bmatrix} |z|^2 + |w|^2 & 0 \\ 0 & |z|^2 + |w|^2 \end{bmatrix}.$$

Writing $z = a + bi$, $w = c + di$, we have $|z|^2 + |w|^2 = a^2 + b^2 + c^2 + d^2$. Our computation can be rewritten as

$$(aI + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(aI - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) = (a^2 + b^2 + c^2 + d^2)I.$$

It follows that

$$(aI - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})(aI + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = (a^2 + (-b)^2 + (-c)^2 + (-d)^2)I = (a^2 + b^2 + c^2 + d^2)I.$$

If not all a, b, c, d are 0 then $a^2 + b^2 + c^2 + d^2 \neq 0$ and the inverse of $aI + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ is

$$\frac{a}{a^2 + b^2 + c^2 + d^2} I - \frac{b}{a^2 + b^2 + c^2 + d^2}\mathbf{i} - \frac{c}{a^2 + b^2 + c^2 + d^2}\mathbf{j} - \frac{d}{a^2 + b^2 + c^2 + d^2}\mathbf{k}.$$

We see that every non-zero element in $\mathbb{H}$ is invertible, i.e. $\mathbb{H}$ is a division ring (skew field).

Problem 2. a) Solve Problem F in chapter 17.

b) Let G be an abelian group written additively (so the operation is denoted by $+$ and the identity element by 0). Consider the direct product $G \times G$. It is an abelian group and we have the following four homomorphisms:

- $\pi_1 : G \times G \longrightarrow G$, $\pi_1(a, b) = a$.
- $\pi_2 : G \times G \longrightarrow G$, $\pi_2(a, b) = b$.
- $e_1 : G \longrightarrow G \times G$, $e_1(a) = (a, 0)$.
- $e_2 : G \longrightarrow G \times G$, $e_2(a) = (0, a)$.

Suppose we have a group homomorphism $\phi : G \longrightarrow G \times G$. Prove that $f = \pi_1\phi$ and $g = \pi_2\phi$ are endomorphisms of G and $\phi(a) = (f(a), g(a))$ for every $a \in G$.

c) We use the notation from part b). Suppose $\psi : G \times G \longrightarrow G$ is a group homomorphism. Prove that $\alpha = \psi e_1$ and $\beta = \psi e_2$ are endomorphisms of G and $\psi(a, b) = \alpha(a) + \beta(b)$ for every $(a, b) \in G \times G$.

d) Suppose that $\phi : G \longrightarrow G \times G$ is an isomorphism and $\psi : G \times G \longrightarrow G$ is the inverse of ϕ. Using the notation from parts b) and c) prove that

$$\alpha f + \beta g = 1, \quad f\alpha = 1, \quad f\beta = 0, \quad g\alpha = 0, \quad g\beta = 1.$$

Conclude that in the ring $End(G)$ α is left invertible and a right zero divisor.

e) Let G be the set of all sequences of integers, i.e. all functions $f : \mathbb{N} \longrightarrow \mathbb{Z}$. Show that G is an abelian group under the usual addition of functions. Prove that G and $G \times G$ are isomorphic. Hint: split a sequence into two sequences, one using the odd terms and the other using even terms.

Solution. a) We start with a general observation. Let X be any non-empty set and G an abelian group (written additively). Then the set $F(X, G)$ of all functions from X to G is an abelian group with addition defined by pointwise addition in G: if f, g are in $F(X, G)$ then the function $f + g$ is defined by

$$(f + g)(x) = f(x) + g(x) \text{ for any } x \in X.$$

The identity element in $F(X, G)$ is the function 0 which to any element in X assigns the identity element 0 in G: $0(x) = 0$ for all $x \in X$. For $f \in F(X, G)$, the inverse of f is the function $-f$ defined by $(-f)(x) = -f(x)$. The verification that this is indeed a group is straightforward and it is left as an exercise.

Suppose now that $X = G$. Consider the subset $End(G)$ of $F(G, G)$ which consists of all functions $f : G \longrightarrow G$ which are endomorphisms, i.e. such that $f(a + b) = f(a) + f(b)$ for any $a, b \in G$. We claim that $End(G)$ is a subgroup of $F(G, G)$. In fact, 0 is an endomorphism and if f, g are endomorphisms then

$$(f - g)(a + b) = f(a + b) - g(a + b) = f(a) + f(b) - g(a) - g(b) =$$

$$f(a) - g(a) + f(b) - g(b) = (f - g)(a) + (f - g)(b)$$

so $f - g$ is an endomorphism.

Since composition of two endomorphisms is again an endomorphism, the composition defines a binary, associative operation on $End(G)$. Let I be the identity function: $I(a) = a$ for all $a \in G$. It is clearly an endomorphism and it is the identity element for composition. To finish the verification that $End(G)$ is a ring we need to check the distributive laws: for any endomorphisms f, g, h we have

$$[(f+g)h](a) = (f+g)(h(a)) = f(h(a)) + g(h(a)) = (fh)(a) + (gh)(a)$$

so $(f+g)h = fh + gh$, and

$$[h(f+g)](a) = h((f+g)(a)) = h(f(a)+g(a)) = h(f(a)) + h(g(a)) = (hf)(a) + (hg)(a)$$

so $h(f+g) = hf + hg$. Thus $End(G)$ is indeed a unital ring.

Instead of stating the addition and multiplication tables for $End(\mathbb{Z}_4)$, which is straightforward, we will show that for any n the ring $End(\mathbb{Z}_n)$ is isomorphic with the ring $\mathbb{Z}_n$. Define the function $T : End(\mathbb{Z}_n) \longrightarrow \mathbb{Z}_n$ by $T(f) = f(1)$. We have

$$T(f+g) = (f+g)(1) = f(1) + g(1) = T(f) + T(g)$$

so T is a homomorphism of additive groups. Note that every element of $\mathbb{Z}_n$ is of the form $m \cdot 1$ for some integer m (1 generates the additive group $\mathbb{Z}_n$). Thus for an endomorphism f we have $f(m \cdot 1) = mf(1)$. Suppose that $g(1) = m$ and $f(1) = k$, where $k, m \in \{0, 1, \ldots, n-1\}$. Then $fg(1) = f(m) = f(m \cdot 1) = mf(1) = mk$. This shows that $T(fg) = T(f)T(g)$. Thus T is a ring homomorphism.

If $T(f) = 0$ then $f(1) = 0$, so $f(m) = f(m \cdot 1) = mf(1) = 0$ for all m, i.e. $f = 0$. This means that T has trivial kernel, i.e. T is injective. Finally, for any $m \in \mathbb{Z}_n$, the function $f_m(k) = mk$ is an endomorphism of $\mathbb{Z}_n$ and $f_m(1) = m$. This shows that T is surjective. This completes our proof that T is an isomorphism of rings.

b) Composition of group homomorphisms is again a group homomorphism. Thus f and g are homomorphisms from G to G, i.e. endomorphisms of G. If $\phi(a) = (b, c)$ then $b = \pi_1(b, c) = \pi_1\phi(a) = f(a)$ and $c = \pi_2(b, c) = \pi_2\phi(a) = g(a)$. Thus $\phi(a) = (f(a), g(a))$.

c) As in part b), α and β are homomorphisms from G to G, i.e. endomorphisms of G. Now $(a, b) = (a, 0) + (0, b)$, so

$$\psi(a, b) = \psi((a, 0) + (0, b)) = \psi((a, 0)) + \psi((0, b)) = \psi(e_1(a)) + \psi(e_2(b)) = \alpha(a) + \beta(b).$$

d) We have

$$a = \psi\phi(a) = \psi(f(a), g(a)) = \alpha(f(a)) + \beta(g(a)) = (\alpha f + \beta g)(a)$$

for any $a \in G$. Thus $\alpha f + \beta g = 1$.

Also,

$$(a, b) = \phi\psi(a, b) = \phi(\alpha(a) + \beta(b)) = \phi(\alpha(a)) + \phi(\beta(b)) = (f\alpha(a), g\alpha(a)) + (f\beta(b), g\beta(b)) =$$

$$(f\alpha(a) + f\beta(b), g\alpha(a) + g\beta(b))$$

for any $a, b \in G$. This means that

$$a = f\alpha(a) + f\beta(b) \text{ and } b = g\alpha(a) + g\beta(b)$$

for any $a, b \in G$. Taking $b = 0$ we get $a = f\alpha(a)$ and $0 = g\alpha(a)$ for all $a \in G$, i.e. $f\alpha = 1$ and $g\alpha = 0$. Similarly, taking $a = 0$ we get $0 = f\beta(b)$ and $b = g\beta(b)$ for all $b \in G$. Thus $f\beta = 0$ and $g\beta = 1$.

In particular, $f\alpha = 1$ means that α is left invertible. This implies that $\alpha \neq 0$. Similarly $g \neq 0$ as $g\beta = 1$. Since $g\alpha = 0$, α is a right zero divisor.

e) Define a function $F : G \longrightarrow G \times G$ by $F(f) = (g, h)$ where $g(n) = f(2n-1)$ and $h(n) = f(2n)$ for $n = 1, 2, \ldots$. More explicitly, if we think of f as a sequence $f_1, f_2, f_3, \ldots$ then $F(f)$ is the pair of sequences $(f_1, f_3, f_5, \ldots; f_2, f_4, f_6, \ldots)$. Clearly $F(f_1 + f_2) = F(f_1) + F(f_2)$, so F is a homomorphism. Now define $H : G \times G \longrightarrow G$ by $H(g, h) = f$ where $f(n) = \begin{cases} g((n+1)/2) & \text{if } n \text{ is odd} \\ h(n/2) & \text{if } n \text{ is even} \end{cases}$. More explicitly, if g is the sequence $g_1, g_2, \ldots$ and h is the sequence $h_1, h_2, \ldots$ then $H(g, h)$ is the sequence $g_1, h_1, g_2, h_2, g_3, h_3, \ldots$. It is a straightforward verification that H is the inverse function of F. This shows that F is an isomorphism of groups.

Problem 3. Problem G in chapter 17.

Solution. (1) We check all the axioms (even though we know that $A \times B$ is a group).

A1.

$$(r_1, s_1) + (r_2, s_2)] + (r_3, s_3) = (r_1 + r_2, s_1 + s_2) + (r_3, s_3) = ((r_1 + r_2) + r_3, (s_1 + s_2) + s_3)$$

$$= (r_1 + (r_2 + r_3), s_1 + (s_2 + s_3)) = (r_1, s_1) + (r_2 + r_3, s_2 + s_3) = (r_1, s_1) + [(r_2, s_2) + (r_3, s_3)].$$

A2. We have $(r, s) + (0, 0) = (r + 0, s + 0) = (r, s) = (0, 0) + (r, s)$ so $(0, 0)$ is the zero of $A \times B$.

A3. Since $(r, s) + (-r, -s) = (r + (-r), s + (-s)) = (0, 0)$, every element has its negative.

A4. $(r, s) + (r_1, s_1) = (r + r_1, s + s_1) = (r_1 + r, s_1 + s) = (r_1, s_1) + (r, s)$.

The properties A1-A4 mean that $A \times B$ is an abelian group under $+$. Now we check that multiplication is associative:

M. $[(r_1, s_1) \cdot (r_2, s_2)] \cdot (r_3, s_3) = (r_1 \cdot r_2, s_1 \cdot s_2) \cdot (r_3, s_3) = ((r_1 \cdot r_2) \cdot r_3, (s_1 \cdot s_2) \cdot s_3) = (r_1 \cdot (r_2 \cdot r_3), s_1 \cdot (s_2 \cdot s_3)) = (r_1, s_1) \cdot (r_2 \cdot r_3, s_2 \cdot s_3) = (r_1, s_1) \cdot [(r_2, s_2) \cdot (r_3, s_3)]$.

Finally we verify the distributive laws:

D.

$$[(r_1, s_1) + (r_2, s_2)] \cdot (r_3, s_3) = (r_1 + r_2, s_1 + s_2) \cdot (r_3, s_3) = ((r_1 + r_2) \cdot r_3, (s_1 + s_2) \cdot s_3)$$

$$= (r_1 \cdot r_3 + r_2 \cdot r_3, s_1 \cdot s_3 + s_2 \cdot s_3) = (r_1 \cdot r_3, s_1 \cdot s_3) + (r_2 \cdot r_3, s_2 \cdot s_3) = (r_1, s_1) \cdot (r_3, s_3) + (r_2, s_2) \cdot (r_3, s_3)$$

and similarly

$$(r_3, s_3) \cdot [(r_1, s_1) + (r_2, s_2)] = (r_3, s_3) \cdot (r_1, s_1) + (r_3, s_3) \cdot (r_2, s_2)$$

.

(2) The ring $A \times B$ is commutative iff $(r,s)(r_1,s_1) = (r_1,s_1)(r,s)$ for any $r, r_1 \in A$ and $s, s_1 \in B$. This means that $rr_1 = r_1 r$ and $ss_1 = s_1 s$ for any $r, r_1 \in A$ and $s, s_1 \in B$ so $A \times B$ is commutative iff both A and B are commutative.

If 1_A, 1_B are the multiplicative identities of A and B respectively, that

$$(r,s)(1_A,1_B) = (r \cdot 1_A, s \cdot 1_B) = (r,s) = (1_A,1_B)(r,s)$$

so $(1_A,1_B)$ is the identity of $A \times B$. Conversely, if (x,y) is the multiplicative identity of $A \times B$ then

$$(r,s)(x,y) = (r,s) = (x,y)(r,s)$$

for any $r \in A$ and $s \in B$. In other words,

$$rx = r = xr \text{ and } sy = s = ys$$

for any $r \in A$ and $s \in B$, so x is the identity of A and y is the identity of B.

(3) We assume that neither A nor B is the trivial ring (if $A = \{0\}$ is the trivial ring then $A \times B$ and B are isomorphic).

Note first that $(r,0)$ and $(0,s)$ are left and right zero divisors in $A \times B$ for any non-zero $r \in A$, $s \in B$. since $(r,0)(0,s) = (0,0) = (0,s)(r,0)$.

Suppose that (r,s) is a left zero divisor in $A \times B$ and $r \neq 0$, $s \neq 0$. Then $(r,s)(a,b) = (0,0)$ for some $(a,b) \neq 0$. If $a \neq 0$ then r is a left zero divisor in A, and if $b \neq 0$ then s is a left zero divisor in B. Thus either r is a left zero divisor in A or s is a left zero divisor in B. Conversely, if r is a left zero divisor in A then (r,s) is a left zero divisor in $A \times B$ for any $s \in B$: there is $a \in A$ such that $a \neq 0$ and $ra = 0$ and then $(r,s)(a,0) = (0,0)$. Similarly, if if s is a left zero divisor in B then (r,s) is a left zero divisor in $A \times B$ for any $r \in A$. Thus we can summarize our discussion as follows:

$(r,s) \neq (0,0)$ is a left zero divisor in $A \times B$ if and only if $r = 0$, or $s = 0$, or r is a left zero divisor in A, or s is a left zero divisor in B.

Similarly we show that

$(r,s) \neq (0,0)$ is a right zero divisor in $A \times B$ if and only if $r = 0$, or $s = 0$, or r is a right zero divisor in A, or s is a right zero divisor in B.

(4) (r,s) is invertible in $A \times B$ if and only if $(r,s)(a,b) = (1,1) = (a,b)(r,s)$ for some $a \in A$ and $b \in B$. This is equivalent to r being invertible in A and s invertible in B. In other words, $(A \times B)^\times = A^\times \times B^\times$.

(5) We see from (3) that $A \times B$ has always zero divisors, so it can not be a domain.

Problem 4. Problem H parts 5 and 6 in chapter 17.

Solution. (5) Let us assume that R has 2 binary operations $+, \cdot$ such that R is a group under $+$, multiplication is associative and has the identity element 1 and the distributive laws hold. Then for any $a, b \in R$ we have

$$(a+b)(1+1) = a \cdot (1+1) + b \cdot (1+1) = a \cdot 1 + a \cdot 1 + b \cdot 1 + b \cdot 1 = a + a + b + b.$$

On the other hand,

$$(a+b)(1+1) = (a+b)\cdot 1 + (a+b)\cdot 1 = a+b+a+b.$$

We see that $a+a+b+b = a+b+a+b$. Cancelling a on the left and b on the right, we see that $a+b = b+a$, i.e. $+$ is commutative.

(6) Let a be a generator of A. Let B be the set of all elements of A which commute with a: $B = \{b \in A : ab = ba\}$. Clearly $a \in B$. Also $0 \in B$ and if $b, c \in B$ then $a(b-c) = ab - ac = ba - ca = (b-c)a$. This shows that $b - c \in B$. We proved that B is a subgroup of A. Since $a \in B$ and a generates A, we have $A = B$.

We proved that a commutes with every element in A. Let $C = \{u \in A : uw = wu \text{ for every } w \in A\}$ be the set of all elements in A which commute with any element in A. We just proved that $a \in C$. Clearly $0 \in C$ and if $b, c \in C$ then $s(b-c) = sb - sc = bs - cs = (b-c)s$ for every $s \in A$. This shows that $b - c \in C$. We proved that C is a subgroup of A. Since $a \in C$ and a generates A, we have $A = C$. In other words, all elements in A commute with each other, i.e. A is commutative.

Problem 5. a) Solve Problem M parts 1 and 3 in chapter 17.

b) Find two elements a, b in the ring of 2×2 matrices which are nilpotent and such that $a + b$ is not nilpotent.

Solution. a) (1) Suppose that $a^n = 0$ for some integer $n > 0$. Then

$$1 = 1 - a^n = (1-a)(1 + a + a^2 + \ldots + a^{n-1}) = (1 + a + a^2 + \ldots + a^{n-1})(1-a).$$

This means that $1 - a$ is invertible. Also, $(-a)^n = (-1)^n a^n = 0$ so $-a$ is nilpotent and therefore $1 - (-a) = 1 + a$ is invertible.

(3) Suppose $a^n = 0$ and $b^m = 0$ for some positive integers m, n and $ab = ba$. Then, by the binomial formula,

$$(a+b)^{m+n-1} = \sum_{k=0}^{m+n-1} \binom{m+n-1}{k} a^k b^{m+n-1-k}.$$

Now if $k \geq n$ then $a^k = 0$. If $k \leq n-1$ then $m + n - 1 - k \geq m$ and $b^{m+n-1-k} = 0$. We see that each summand in the above sum is 0, so $(a+b)^{m+n-1} = 0$.

b) We have

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}^2$$

so the matrices $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ are nilpotent, however the matrix

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

is not nilpotent, since

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Problem 6. Problem A parts 1,2,3 in chapter 18.

Solution. (1) Let $S = \{x+y\sqrt{3} : x, y \in \mathbb{Z}\}$. Clearly $0 = 0+0\cdot\sqrt{3} \in S$ and $1 = 1+0\cdot\sqrt{3} \in S$. Let $x + y\sqrt{3}$ and $a + b\sqrt{3}$ be two elements in S. Then

$$(x + y\sqrt{3}) - (a + b\sqrt{3}) = (x - a) + (y - b)\sqrt{3} \in S$$

so S is an additive subgroup of $\mathbb{R}$. Furthermore,

$$(x + y\sqrt{3})(a + b\sqrt{3}) = xa + 3yb + (xb + ya)\sqrt{3} \in S.$$

This completes our verification that S is a unital subgring of $\mathbb{R}$.

(2) Let $S = \{x + y\sqrt[3]{2} + z\sqrt[3]{4} : x, y, z \in \mathbb{Z}\}$. Clearly $0 \in S$ and $1 \in S$. Let $x + y\sqrt[3]{2} + z\sqrt[3]{4}$ and $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ be two elements in S. Then

$$(x + y\sqrt[3]{2} + z\sqrt[3]{4}) - (a + b\sqrt[3]{2} + c\sqrt[3]{4}) = (x - a) + (y - b)\sqrt[3]{2} + (z - c)\sqrt[3]{4} \in S$$

so S is an additive subgroup of $\mathbb{R}$. Furthermore,

$$(x+y\sqrt[3]{2}+z\sqrt[3]{4})(a+b\sqrt[3]{2}+c\sqrt[3]{4}) = (xa+2yc+2zb+(xb+ya+2zc)\sqrt[3]{2}+(xc+yb+za)\sqrt[3]{4} \in S.$$

This completes our verification that S is a unital subgring of $\mathbb{R}$.

(3) Let $S = \{x2^y : x, y \in \mathbb{Z}\}$. Clearly $0 \in S$ and $1 = 1 \cdot 2^0 \in S$. Let $x2^y$ and $a2^b$ be two elements in S. We may assume that $y \geq b$. Then $x2^y = (x2^{y-b})2^b$ and $x2^{y-b}$ is an integer, and

$$x2^y - a2^b = (x2^{y-b})2^b - a2^b = (x2^{y-b} - a)2^b \in S$$

so S is an additive subgroup of $\mathbb{R}$. Furthermore,

$$(x2^y)(a2^b) = (xa)2^{y+b} \in S.$$

This completes our verification that S is a unital subring of $\mathbb{R}$.

Problem 7. Problem C parts 8,9 in chapter 18.

Solution. (8) Clearly $f(0) = 0$ so $0 \in B$. If $s, t \in B$ then $f(s) = s$ and $f(t) = t$, so $f(s - t) = f(s) - f(t) = s - t$, i.e. $s - t \in B$. Finally, $f(st) = f(s)f(t) = st$, so $st \in B$. This proves that B is a subring of A.

(9) Let $Z = \{u \in A : uw = wu \text{ for every } w \in A\}$ be the center of A. Clearly $0 \in Z$ and if $b, c \in Z$ then $s(b-c) = sb-sc = bs-cs = (b-c)s$ for every $s \in A$. This shows that $b-c \in Z$. It follows that Z is a subgroup of A. Also, $s(bc) = (sb)c = (bs)c = b(sc) = b(cs) = (bc)s$ for every $s \in A$. Thus Z is a subring of A.

Problem 8. Problem F parts 5,7 in chapter 18.

Solution. (5) We are assuming here that A is unital and B is an integral domain. We have $f(1)^2 = f(1)f(1) = f(1 \cdot 1) = f(1)$, so $f(1)(f(1) - 1) = 0$. Since B is an integral domain, we have $f(1) = 0$ or $f(1) - 1 = 0$, i.e. $f(1) = 1$. If $f(1) = 1$ and a is invertible in A then $ab = 1 = ba$ for some $b \in A$ and $1 = f(1) = f(ab) = f(a)f(b)$ and similarly $1 = f(b)f(a)$. This means that $f(a)$ is invertible in B.

(7) Suppose that A is a field and $f : A \longrightarrow B$ a homomorphism. Suppose that $f(a) = 0$ for some $a \neq 0$, $a \in A$. Since a is invertible in A, we have $1 = aa^{-1}$ and therefore

$$f(1) = f(aa^{-1}) = f(a)f(a^{-1}) = 0.$$

It follows that $f(r) = f(r \cdot 1) = f(r)f(1) = 0$ for every $r \in A$, so the image $f(A) = \{0\}$. Equivalently, if the image of A is not $\{0\}$, then f has trivial kernel, i.e. f is injective.