1. (DF7.2.10) Consider the following elements of the integral group ring $\mathbb{Z}S_3$

$$\alpha = 3(1\,2) - 5(2\,3) + 14(1\,2\,3) \quad \text{and} \quad \beta = 6(1) + 2(2\,3) - 7(1\,3\,2)$$

(where (1) is the identity of S_3). Compute the following elements:

(a) $\alpha + \beta$, **(b)** $2\alpha - 3\beta$, **(c)** $\alpha\beta$, **(d)** $\beta\alpha$, **(e)** α^2

We have:

(a) $\alpha+\beta = (3(1\,2)-5(2\,3)+14(1\,2\,3))+(6(1)+2(2\,3)-7(1\,3\,2)) = \boxed{6(1) + 3(1\,2) - 3(2\,3) + 14(1\,2\,3) - 7(1\,3\,2)}$

(b) $2\alpha - 3\beta = \alpha + \alpha + (-\beta - \beta - \beta) = (6(1\,2) - 10(2\,3) + 28(1\,2\,3)) - (18(1) + 6(2\,3) - 21(1\,3\,2)) = \boxed{-18(1) + 6(1\,2) - 16(2\,3) + 28(1\,2\,3) + 21(1\,3\,2)}$

(c) $\alpha\beta = [3(1\,2) - 5(2\,3) + 14(1\,2\,3)][6(1) + 2(2\,3) - 7(1\,3\,2)] = 18(1\,2)(1) + 6(1\,2)(2\,3) - 21(1\,2)(1\,3\,2) - 30(2\,3)(1) - 10(2\,3)(2\,3) + 35(2\,3)(1\,3\,2) + 84(1\,2\,3)(1) + 28(1\,2\,3)(2\,3) - 98(1\,2\,3)(1\,3\,2)$
$= \boxed{-108(1) + 81(1\,2) - 21(1\,3) - 30(2\,3) + 90(1\,2\,3)}$

(d) $\beta\alpha = [6(1) + 2(2\,3) - 7(1\,3\,2)][3(1\,2) - 5(2\,3) + 14(1\,2\,3)] = 18(1)(1\,2) - 30(1)(2\,3) + 84(1)(1\,2\,3) + 6(2\,3)(1\,2) - 10(2\,3)(2\,3) + 28(2\,3)(1\,2\,3) - 21(1\,3\,2)(1\,2) + 35(1\,3\,2)(2\,3) - 98(1\,3\,2)(1\,2\,3)$
$= \boxed{-108(1) + 18(1\,2) + 63(1\,3) - 51(2\,3) + 84(1\,2\,3) + 6(1\,3\,2)}$

(e) $\alpha^2 = [3(1\,2) - 5(2\,3) + 14(1\,2\,3)][3(1\,2) - 5(2\,3) + 14(1\,2\,3)] = 9(1\,2)(1\,2) - 15(1\,2)(2\,3) + 42(1\,2)(1\,2\,3) - 15(2\,3)(1\,2) + 25(2\,3)(2\,3) - 70(2\,3)(1\,2\,3) + 42(1\,2\,3)(1\,2) - 70(1\,2\,3)(2\,3) + 196(1\,2\,3)(1\,2\,3)$
$= \boxed{34(1) - 70(1\,2) - 28(1\,3) + 42(2\,3) - 15(1\,2\,3) + 181(1\,3\,2)}$

In Section 7.3, rings are assumed to have a $1 \neq 0$.

2. (DF7.3.13) Prove that the ring $M_2(\mathbb{R})$ contains a subring isomorphic to $\mathbb{C}$.

Proof. Observing that

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

construct the set

$$S = \left\{ r_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + r_2 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : r_1, r_2 \in \mathbb{R} \right\}.$$

It is clear that this set is a nonempty subset of $M_2(\mathbb{R})$; what remains is to show is that this set under the same operations as $M_2(\mathbb{R})$ is a subring, and that this subring is isomorphic to $\mathbb{C}$.

For arbitrary $r_1, r_2, r_3, r_4 \in \mathbb{R}$, we have

$$\left(r_1 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + r_2 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right) - \left(r_3 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + r_4 \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right) = \begin{pmatrix} r_1 & -r_2 \\ r_2 & r_1 \end{pmatrix} - \begin{pmatrix} r_3 & -r_4 \\ r_4 & r_3 \end{pmatrix}$$

$$= \begin{pmatrix} r_1 - r_3 & -(r_2 - r_4) \\ r_2 - r_4 & r_1 - r_3 \end{pmatrix} = (r_1 - r_3) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + (r_2 - r_4) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and

$$\left(r_1\begin{pmatrix}1&0\\0&1\end{pmatrix}+r_2\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right)\left(r_3\begin{pmatrix}1&0\\0&1\end{pmatrix}+r_4\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right)$$
$$=r_1r_3\begin{pmatrix}1&0\\0&1\end{pmatrix}^2+r_1r_4\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}+r_2r_3\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}+r_2r_4\begin{pmatrix}0&-1\\1&0\end{pmatrix}^2$$
$$=(r_1r_3-r_2r_4)\begin{pmatrix}1&0\\0&1\end{pmatrix}+(r_1r_4+r_2r_3)\begin{pmatrix}0&-1\\1&0\end{pmatrix}.$$

Observe that the difference of two elements of S is in S, and the product of two elements of S is also in S. It follows that S is a subring of $M_2(\mathbb{R})$.

To show that this subring is isomorphic to $\mathbb{C}$ we exhibit the map $\varphi\colon S\to\mathbb{C}$ given by

$$\varphi\left(r_1\begin{pmatrix}1&0\\0&1\end{pmatrix}+r_2\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right)=r_1+r_2i\quad(r_1,r_2\in\mathbb{R}),$$

so that in particular we have that the identity matrix maps to $1+0i$ and the matrix $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ maps to $0+1i$. We show that this map is an isomorphism of rings. The operations of addition and multiplication are preserved: For arbitrary $r_1,r_2,r_3,r_4\in\mathbb{R}$, we have

$$\varphi\left((r_1+r_3)\begin{pmatrix}1&0\\0&1\end{pmatrix}+(r_2+r_4)\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right)=(r_1+r_3)+(r_2+r_4)i$$
$$=(r_1+r_2i)+(r_3+r_4i)=\varphi\left(r_1\begin{pmatrix}1&0\\0&1\end{pmatrix}+r_2\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right)+\varphi\left(r_3\begin{pmatrix}1&0\\0&1\end{pmatrix}+r_4\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right)$$

and

$$\varphi\left((r_1r_3-r_2r_4)\begin{pmatrix}1&0\\0&1\end{pmatrix}+(r_1r_4+r_2r_3)\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right)=(r_1r_3-r_2r_4)+(r_1r_4+r_2r_3)i$$
$$=(r_1+r_2i)(r_3+r_4i)=\varphi\left(r_1\begin{pmatrix}1&0\\0&1\end{pmatrix}+r_2\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right)\varphi\left(r_3\begin{pmatrix}1&0\\0&1\end{pmatrix}+r_4\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right).$$

The map $\varphi^{-1}\colon\mathbb{C}\to S$ given by

$$\varphi^{-1}(r_1+r_2i)=r_1\begin{pmatrix}1&0\\0&1\end{pmatrix}+r_2\begin{pmatrix}0&-1\\1&0\end{pmatrix}$$

is easily checked to be a two-sided inverse for φ. We have that $\varphi\varphi^{-1}$ is the identity map on $\mathbb{C}$ and that $\varphi^{-1}\varphi$ is the identity map on S. It follows that φ is a bijection, and so φ is an isomorphism of rings. Hence S is isomorphic to $\mathbb{C}$ as desired. □

3. (DF7.3.22) Let a be an element of the ring R.

(a) Prove that $\{x \in R \mid ax = 0\}$ is a right ideal and $\{y \in R \mid ya = 0\}$ is a left ideal (called respectively the right and left *annihilators* of a in R).

Proof. Fix an element $a \in R$. The sets $I = \{x \in R \mid ax = 0\}$ and $J = \{y \in R \mid ya = 0\}$ are subrings:

Observe I is a nonempty subset of R since $0 \in I$; we have $a0 = 0$. Let $x, y \in I$. Then $a(x - y) = ax - ay = 0 - 0 = 0$, so that $x - y \in I$. Thus I is closed under subtraction (so I is a subgroup of R). Similarly, $a(xy) = (ax)y = 0y = 0$, so that $xy \in I$; we have that I is closed under multiplication. Hence I is a subring of R.

Observe J is a nonempty subset of R since $0 \in J$; we have $0a = 0$. Let $x, y \in J$. Then $(x - y)a = xa - ya = 0 - 0 = 0$, so that $x - y \in J$. Thus J is closed under subtraction (so J is a subgroup of R). Similarly, $(xy)a = x(ya) = x0 = 0$, so that $xy \in I$; we have that I is closed under multiplication. Hence I is a subring of R.

To show that I is a right ideal of R, we check that I is closed under right multiplication by elements of R. Let $r \in R$ be arbitrary, and take any element $x \in I$. We have $a(xr) = (ax)r = 0r = 0$, so that $xr \in I$. It follows that I is a right ideal of R.

We use an almost identical argument to show that J is a left ideal of R: Let $r \in R$ be arbitrary, and take any element $y \in J$. Then $(ry)a = r(ya) = r0 = 0$, so that $ry \in J$. Thus J is closed under left multiplication by elements in R, so that J is a left ideal of R. $\square$

(b) Prove that if L is a left ideal of R then $\{x \in R \mid xa = 0 \text{ for all } a \in L\}$ is a two-sided ideal (called the left *annihilator* of L in R).

Proof. Let L be a left ideal of R as given. We show that the left annihilator of L in R, given by $I = \{x \in R \mid xa = 0 \text{ for all } a \in L\}$ is a subring. First, I is a nonempty subset of R since $0 \in I$: $0a = 0$ for any $a \in L$. Let $x, y \in I$. Then for any $a \in L$, we have $(x - y)a = xa - ya = 0 - 0 = 0$, so that $x - y \in I$; similarly $(xy)a = x(ya) = 0$, so that $xy \in I$. Hence I is a subring of R.

We check that I is closed under left and right multiplication by elements of R. Let $r \in R$ be arbitrary. Then for any $x \in I$ and any $a \in L$, we have $(rx)a = r(xa) = r0 = 0$ and $(xr)a = x(ra) = xa' = 0$, where $ra = a' \in L$ because L is a left ideal of R. It follows that rx and xr are elements of I, so that I is closed under left and right multiplication by elements of R.

Hence I, the left annihilator of L in R, is a two-sided ideal of R. $\square$

4. (DF7.3.34) Let I and J be ideals of R.

(a) Prove that $I + J$ is the smallest ideal of R containing both I and J.

Proof. Let I and J be ideals of R.

We check that $I + J = \{a + b \mid a \in I, b \in J\}$ is an ideal of R. It is clear that $I + J$ is a subring of R: We have $0 \in I + J$, since $0 \in I$ and $0 \in J$, and $0 + 0 = 0$. For any $a, a' \in I$ and any $b, b' \in J$ we have $(a + b) - (a' + b') = (a - a') + (b - b') \in I + J$ since $a - a' \in I$ and $b - b' \in J$. We also have

$(a+b)(a'+b') = a(a'+b') + b(a'+b') \in I + J$ since $a(a'+b') \in I$ and $b(a'+b') \in J$ since I and J are ideals. Thus $I + J$ is a subring of R.

For any $r \in R$ we have $r(a+b) = ra + rb \in I + J$, and $(a+b)r = ar + br \in I + J$, since $ar, ra \in I$ and $br, rb \in J$ due to I and J being ideals of R. Thus $I + J$ is an ideal of R.

Let K be any ideal of R containing I and J. Observe that K is an additive subgroup of R; it follows that for any $a \in I$ and any $b \in J$, we have $a, b \in K$, so that $a + b \in K$. Hence $I + J \subseteq K$. Since K was an arbitrary ideal containing I and J, it follows that $I + J$ is the smallest ideal of R containing I and J. □

(b) Prove that IJ is an ideal contained in $I \cap J$.

Proof. Ler I and J be ideals of R.

We check that $IJ = \{\sum_{i=1}^{n} a_i b_i \mid \text{for any } a \in I, b \in J, n \in \mathbb{Z}^+\}$ (set of finite sums of elements of the form ab for $a \in I, b \in J$) is an ideal of R. Of course, $0 \in I$ and $0 \in J$ so that $(0)(0) = 0 \in IJ$. Let $a_1b_1 + \cdots + a_nb_n$ and $a'_1b'_1 + \cdots + a'_mb'_m$ $(n, m \in \mathbb{Z}^+)$ be elements of IJ. Then

$$(a_1b_1 + \cdots + a_nb_n) - (a'_1b'_1 + \cdots + a'_mb'_m) = a_1b_1 + \cdots + a_nb_n + (-a'_1)b'_1 + \cdots + (-a'_m)b'_m,$$

which is clearly an element of IJ. Without loss of generality, take $m \leq n$, so that we can write $a'_1b'_1 + \cdots + a'_mb'_m = a'_1b'_1 + \cdots + a'_nb'_n$ where if $m < n$, $a'_i = b'_i = 0$ for $m + 1 \leq i \leq n$ (i.e., add zero terms if needed). Observe that because I and J are ideals, that $a_ib_i \in I$ and $a'_ib'_i \in J$ for $1 \leq i \leq n$. Then

$$(a_1b_1 + \cdots + a_nb_n)(a'_1b'_1 + \cdots + a'_nb'_n) = \sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} (a_ib_i)(a'_jb'_j)$$

is a finite sum of elements of the form required to be in IJ. Hence IJ is a subring of R.

For any $r \in R$, we have $r(a_1b_1 + \cdots + a_nb_n) = (ra_1)b_1 + \cdots + (ra_n)b_n \in IJ$ and $(a_1b_1 + \cdots + a_nb_n)r = a_1(b_1r) + \cdots + a_n(b_nr) \in IJ$ since $ra_i \in I$ and $b_ir \in J$ for $1 \leq i \leq n$ due to I and J being ideals of R. Hence IJ is an ideal of R.

With I and J being ideals, it follows that for any $a \in I$ and $b \in J$, the element ab can be viewed as an element of I and also as an element of J; that is, $ab \in I \cap J$. Therefore, for any element $a_1b_1 + \cdots a_nb_n \in IJ$, viewing every term as an element of I yields that this element is in I. Similarly, view every term as an element of J to see that this element is in J. Hence $a_1b_1 + \cdots a_nb_n \in I \cap J$, so that $IJ \subseteq I \cap J$. □

(c) Give an example where $IJ \neq I \cap J$.

In $\mathbb{Z}$, the ideal $(2) = 2\mathbb{Z}$ may be squared to obtain

$$(2)(2) = \left\{ \sum_{i=1}^{n} (2a_i)(2b_i) \mid \text{for any } a_i, b_i \in \mathbb{Z}, n \in \mathbb{Z}^+ \right\}$$

(finite sums of products of even numbers), but because we can factor out 4 from these finite sums, we have that $(2)(2) = 4\mathbb{Z}$. But $4\mathbb{Z}$ is properly contained in $2\mathbb{Z} \cap 2\mathbb{Z} = 2\mathbb{Z}$ (as $2 \notin 4\mathbb{Z}$, but every multiple of 4 is divisible by 2).

(It is clear that $2\mathbb{Z}$ is an ideal: We have that $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, is a subring of $\mathbb{Z}$ since products of even integers are even, and is an ideal of $\mathbb{Z}$ since the product of an even integer with any other integer is also even.)

(d) Prove that if R is commutative and if $I + J = R$ then $IJ = I \cap J$. (Note that R contains 1 as a global assumption.)

Proof. Let R be commutative and let I, J be ideals of R with $I + J = R$. The containment $IJ \subseteq I \cap J$ follows from a previous result. We show that $I \cap J \subseteq IJ$. To that end, take any element $c \in I \cap J$, so that $c \in I$ and $c \in J$.

Since R contains 1, it follows that there are elements $a \in I$ and $b \in J$ with $a + b = 1$. Then

$$c = c(a + b) = ca + cb = ac + cb,$$

which is a finite sum, and with $a, c \in I$ and $c, b \in J$, we have that $c = ac + cb \in IJ$.

Thus $I \cap J \subset IJ$, from which it follows that $IJ = I \cap J$. $\square$