Solutions to Homework for M351 – Algebra I

Examples & Hwk 1:

> $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ and $(\mathbb{C},+)$ are groups. — $(\mathbb{N},+)$ is NOT a group. *Why not?* — *Is the set of irrational numbers, with $+$, a group? Explain.*

Solution: Conventions differ on whether $\mathbb{N}$ denotes the set of positive, or of non-negative, integers. If you argue the former, then $\mathbb{N}$ is not a group, because there is no neutral element. If you argue the latter, then $0 \in \mathbb{N}$ is the neutral element, but not every element has an additive inverse.

The set of irrational numbers (let's call it I) is not a group with addition, because there is no binary operation $+ : I \times I \to I$ in the first place (the sum of irrational numbers may well be rational). This problem could arise, because we restricted an already defined operation $+$ on the larger set $\mathbb{R}$ to a subset. If you define an operation $+$ from scratch to map $G \times G \to G$, then this "closedness" property is automatically taken care of.

Examples & Hwk 2:

> $(\mathbb{Z}^*,\cdot)$ is NOT a group. *Why not?* — $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$ and $(\mathbb{C}^*,\cdot)$ are groups. Here we have used the following notations for certain sets of numbers: $\mathbb{Z}^* := \mathbb{Z}\setminus\{0\}$, $\mathbb{Q}^* := \mathbb{Q}\setminus\{0\}$, $\mathbb{R}^* := \mathbb{R}\setminus\{0\}$, $\mathbb{C}^* := \mathbb{C}\setminus\{0\}$.

Solution: $(\mathbb{Z}^*,\cdot)$ is NOT a group, because the multiplicative inverse is lacking.

Examples & Hwk 3:

> Matrix groups. We denote by $GL_n(\mathbb{R})$ the set of all invertible $n\times n$ matrices with real entries, and by $SL_n(\mathbb{R})$ the set of all those $n \times n$ matrices with real entries whose determinant is 1. By $O_n(\mathbb{R})$ we denote the set of orthogonal $n\times n$ matrices with real entries. Similarly, we write $GL_n(\mathbb{Q})$ or $GL_n(\mathbb{Z})$ etc. to require that the entries be rational numbers, or integers. $+$ and $\cdot$ denote matrix addition or multiplication respectively. — $(GL_n(\mathbb{R}),\cdot)$ is a group. *Why? Which statement from Math 251 is pertinent here? Are $SL_n(\mathbb{R})$ and $O_n(\mathbb{R})$ groups? How about $GL_n(\mathbb{Q})$, $GL_n(\mathbb{Z})$, $SL_n(\mathbb{Q})$, $SL_n(\mathbb{Z})$, each together with $\cdot$?*

Solution: $GL_n(\mathbb{R})$ is a group: In order to *have* the operation within $GL_n(\mathbb{R})$ in the first place, we need that the product of invertible matrices is invertible again. Then we have the associative law from matrix algebra, the identity matrix als neutral element, and the inverse matrix as inverse in the sense of the group axioms (and, yes, the inverse of an invertible matrix is invertible). $SL_n(\mathbb{R})$ is also a group, namely a *subgroup* of $GL_n(\mathbb{R})$. We need to check only the 'closedness' properties, namely that products of matrices with determinant 1 have determinant 1 again, and inverses of determinant 1 matrices have determinant 1. (Because $\det(AB) = \det A \det B$ and $\det(A^{-1}) = (\det A)^{-1}$.)

$O_n(\mathbb{R})$ is a group, because products and inverses of orthogonal matrices are orthogonal. (Remember: If $AA^T = I$ and $BB^T = I$, then $(AB)(AB)^T = ABB^TA^T = AIA^T = AA^T = I$; and a similar calculation for the inverse.)

$GL_n(\mathbb{Q})$ and $SL_n(\mathbb{Q})$ are groups. But $GL_n(\mathbb{Z})$ is NOT a group, whereas $SL_n(\mathbb{Z})$ is. The distinction in these cases is whether the inverse matrix of a matrix from each of these sets is in the same set again. For $GL_n(\mathbb{Z})$ this clearly needn't be the case (e.g., the matrix $2I$). For $A \in SL_n(\mathbb{Z})$, the fact that A^{-1} has integer entries follows from the formula $A^{-1} = (\operatorname{adj} A)/(\det A)$, where the adjoint matrix is the transpose of the cofactor matrix.

Example & Hwk 4:

> The set $\{E, O\}$ together with addition subject to the rules $E+E = E$, $E+O = O+E = O$, $O+O = E$ is a group. *Can you recognize some simple wisdom commonly known to high school graduates that is represented by this abstract example?*

Solution: The rules encode the fact that the sum of two even numbers is even, the sum of two odd numbers is even, and the sum of an even and an odd number is odd.

Example & Hwk 5:

> Can you generalize the previous example and construct a group on a set of three elements, let's call it $\{Z, I, T\}$, with an appropriate addition, with a similar idea behind the abstract example?

Solution: Z symbolizes a number leaving the remainder **z**ero when divided by 3. I symbolizes a number leaving the remainder 1 when divided by 3. And T symbolizes a number leaving the remainder **t**wo, when divided by 3. This motivates the rules $Z + Z = Z$, $Z + I = I$, $Z + T = T$, $I + I = T$, $I + T = Z$, $T + T = I$ with a *commutative* addition. Group properties can be verified with patience. The general principle will be discussed in class later.

Example & Hwk 6:

> The set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \setminus \{0\}$, together with multiplication, is a group. *Show this. Explain why it is necessary to know that $\sqrt{2}$ is irrational in order for your proof to work.*

Solution: We view this set as a subset of $\mathbb{R}$, so we inherit the associative and commutative law and only need to check the closedness properties: $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$. Hence the product of two elements in the set is also in the set, because $ac+2bd$ and $ad+bc$ will be rational again. (Note: If I had taken $\sqrt[3]{2}$ instead, this property would have failed, or I'd have needed to take the set of all $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ instead.) Now the inverse is $(a+b\sqrt{2})^{-1} = a/(a^2-2b^2) - b/(a^2-2b^2)\sqrt{2}$. The nonvanishing of the denominator follows from the irrationality of $\sqrt{2}$.

Example & Hwk 7:

> The set of permutations of $\{1, 2, \ldots, n\}$, together with composition $\circ$, is a group, often called S_n. Remember the definition of permutations: For instance, the permutation (1347256) is the function $1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 7, 5 \mapsto 2, 6 \mapsto 5, 7 \mapsto 6$. What is the inverse of this permutation? What is $(1347256) \circ (3512647)$? What is $(3512647) \circ (1347256)$?

Solution: The problem was not concerned with the associative law, which holds generally for the composition of functions. The identity is also obvious: (1234567) in the example $n = 7$.

The inverse of (1347256) is the function that maps $1 \mapsto 1, 3 \mapsto 2, 4 \mapsto 3, 7 \mapsto 4, 2 \mapsto 5, 5 \mapsto 6, 6 \mapsto 7$ (by reversing the arrows). Listing the value table in natural order, we write this permutation as (1523674).

In $(1347256) \circ (3512647)$, note that the first mapping to be executed is the one to the right of the $\circ$. So this composition maps $1 \mapsto 3 \mapsto 4$, $2 \mapsto 5 \mapsto 2$, $3 \mapsto 1 \mapsto 1$, $4 \mapsto 2 \mapsto 3$, $5 \mapsto 6 \mapsto 5$, $6 \mapsto 4 \mapsto 7$ and $7 \mapsto 7 \mapsto 6$. Therefore $(1347256) \circ (3512647) = (4213576)$.

By similar reasoning, $(3512647) \circ (1347256) = (3127564)$. So, clearly, the group S_7 is not abelian.

Example & Hwk 8:

Take the following set of six rational functions $\{I, F_0, F_1, F_\infty, M, W\}$ given by $I(z) = z$, $F_0(z) = z/(z-1)$, $F_1(z) = 1/z$, $F_\infty(z) = 1-z$, $M(z) = (z-1)/z$, $W(z) = 1/(1-z)$. Don't try to understand the rationale behind the names. Use composition $\circ$ as operation. This is a group. *To help showing this, construct the group table.*

Is the set of all rational functions, together with $\circ$, a group? Give a reason for your answer. — Show that the set of those rational functions of the form $f(z) = \frac{az+b}{cz+d}$ with a, b, c, d real and $ad - bc \neq 0$ forms a group, again under the composition $\circ$ as operation.

Solution: Clearly I is a (the) neutral element. Let's calculate a few compositions, as samples: $(F_0 \circ F_1)(z) = F_0(F_1(z)) = F_0(1/z) = \frac{1/z}{1/z-1} = \frac{1}{1-z} = W(z)$, hence $F_0 \circ F_1 = W$. — $(F_1 \circ F_0)(z) = F_1(F_0(z)) = F_1(z/(z-1)) = (z-1)/z = M(z)$, hence $F_1 \circ F_0 = M$. Altogether, there are 25 such calculations (not counting those trivial cases where one term is I). The following table lists $a \circ b$, where the 1st 'factor' a is given in the left column, and the second 'factor' b is given in the top row:

$\circ$	I	F_0	F_1	F_∞	M	W
I	I	F_0	F_1	F_∞	M	W
F_0	F_0	I	W	M	F_∞	F_1
F_1	F_1	M	I	W	F_0	F_∞
F_∞	F_∞	W	M	I	F_1	F_0
M	M	F_1	F_∞	F_0	W	I
W	W	F_∞	F_0	F_1	I	M

The set of *all* rational functions, with composition, does not form a group, because, for instance, the function $z \mapsto z^2$ does not have an inverse. Or, more radically, constant functions (which are certainly rational), do not have an inverse.

To show that the set of rational functions of the form $f(z) = \frac{az+b}{cz+d}$ with a, b, c, d real and $ad - bc \neq 0$ forms a group, with composition, we only need to show the closedness properties. The neutral element $f(z) = z$ is included, with $a = d$, $b = c = 0$. (Note that multiples of (a, b, c, d) describe the same function, so I don't need to specify which number $a = d$ is.) The inverse of $z \mapsto \frac{az+b}{cz+d}$ is $w \mapsto \frac{dw-b}{-cw+a}$ because

$$\frac{d\frac{az+b}{cz+d} - b}{-c\frac{az+b}{cz+d} + a} = z\ .$$

If $f(z) = \frac{a_1z+b_1}{c_1z+d_1}$ and $g(z) = \frac{a_2z+b_2}{c_2z+d_2}$, then

$$(f \circ g)(z) = f(g(z)) = \frac{a_1\frac{a_2z+b_2}{c_2z+d_2} + b_1}{c_1\frac{a_2z+b_2}{c_2z+d_2} + d_1} = \frac{(a_1a_2 + b_1c_2)z + (a_1b_2 + b_1d_2)}{(c_1a_2 + d_1c_2)z + (c_1b_2 + d_1d_2)}$$

This is again a rational function of the prescribed form, because

$$(a_1a_2 + b_1c_2)(c_1b_2 + d_1d_2) - (a_1b_2 + b_1d_2)(c_1a_2 + d_1c_2) = (a_1d_1 - b_1c_1)(a_2d_2 - b_2c_2) \neq 0 \qquad (*)$$

Remarkably, this composition rule corresponds exactly to matrix multiplication for 2×2-matrices:

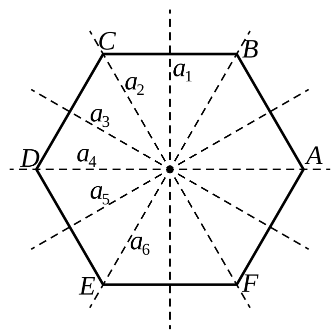
$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} (a_1a_2 + b_1c_2) & (a_1b_2 + b_1d_2) \\ (c_1a_2 + d_1c_2) & (c_1b_2 + d_1d_2) \end{bmatrix}$$

The mysterious formula $(*)$ is therefore nothing but $\det(A_1A_2) = (\det A_1)(\det A_2)$.

Example & Hwk 9:

Draw a regular n-gon, say, to be specific, a hexagon $n = 6$. Draw its six symmetry axes $a_1,\ldots,a_6$ (half of them are lines through opposite vertices, half of them are lines through midpoints of opposite sides. Let $S_1,\ldots,S_6$ be reflections of the hexagon with respect to the axes $a_1,\ldots,a_6$ respectively. Moreover, let $R_0,\ldots,R_5$ denote counterclockwise rotations about the center of the hexagon by 0, 60, 120,. . . ,300 degrees resectively. The mappings $S_1,\ldots,S_6,R_0,\ldots,R_5$, together with composition, form a group, which is called DIHEDRAL GROUP D_6. (Or similarly D_n, if you have an n-gon instead of a hexagon.)

Solution: If axis a_j arises from axis a_i by a rotation of angle α, then $S_j \circ S_i$ is a rotation by angle 2α. Order matters: $S_i \circ S_j$ is a rotation about -2α. – The composition of two rotations is a rotation by the sum of the angles (commutative). – The composition of a rotation and a reflection is again a certain reflection, and order matters: Rotating by α, then reflecting in axis a amounts to reflection in a new axis that is rotated by angle $-\alpha/2$ with respect to the old one. The converse order has the new axis rotated by $+\alpha/2$ with respect to the old one. All these facts can be seen in terms of elementary geometry, by drawing a circle about the origin, through a point being mapped under the various transformations, and adding and subtracting the appropriate angles. Each reflection is its own inverse. Inverses of rotations by α are rotations by the negative angle $-\alpha$ (or, equivalently, by $2\pi - \alpha$).



It is also possible, but more tedious, to calculate matrices for each of the linear transformations in question. This way, D_6 arises as a subgroup of the group $O_2(\mathbb{R})$. It is also possible to study the transformations by looking at how they permute the vertices of the hexagon. In this way, D_6 arises as a subgroup of the permutation group S_6.

With the principles above, the following group table arises for the dihedral group, D_6. In particular, it is clear that compositions of transformations from D_6 are again from D_6, that R_0 is neutral, and that inverses of transformations in D_6 are in D_6. Associativity is inherited from composition of functions in general.

$\circ$	R_0	R_1	R_2	R_3	R_4	R_5	S_1	S_2	S_3	S_4	S_5	S_6
R_0	R_0	R_1	R_2	R_3	R_4	R_5	S_1	S_2	S_3	S_4	S_5	S_6
R_1	R_1	R_2	R_3	R_4	R_5	R_0	S_2	S_3	S_4	S_5	S_6	S_1
R_2	R_2	R_3	R_4	R_5	R_0	R_1	S_3	S_4	S_5	S_6	S_1	S_2
R_3	R_3	R_4	R_5	R_0	R_1	R_2	S_4	S_5	S_6	S_1	S_2	S_3
R_4	R_4	R_5	R_0	R_1	R_2	R_3	S_5	S_6	S_1	S_2	S_3	S_4
R_5	R_5	R_0	R_1	R_2	R_3	R_4	S_6	S_1	S_2	S_3	S_4	S_5
S_1	S_1	S_2	S_3	S_4	S_5	S_6	R_0	R_5	R_4	R_3	R_2	R_1
S_2	S_6	S_1	S_2	S_3	S_4	S_5	R_1	R_0	R_5	R_4	R_3	R_2
S_3	S_5	S_6	S_1	S_2	S_3	S_4	R_2	R_1	R_0	R_5	R_4	R_3
S_4	S_4	S_5	S_6	S_1	S_2	S_3	R_3	R_2	R_1	R_0	R_5	R_4
S_5	S_3	S_4	S_5	S_6	S_1	S_2	R_4	R_3	R_2	R_1	R_0	R_5
S_6	S_2	S_3	S_4	S_5	S_6	S_1	R_5	R_4	R_3	R_2	R_1	R_0

Example & Hwk 10:

The set $O_2(\mathbb{R}) \times \mathbb{R}^2$ consists of pairs (A, a) where A is an orthogonal 2×2 matrix and a is a 2-vector. We define the multiplication by $(A, a) \odot (B, b) = (AB, Ab + a)$. Check that this is a group. It is called the isometry group of the plane, because the motivation behind the definition of $\odot$ is that (A, a) represents the mapping $x \mapsto Ax + a, \mathbb{R}^2 \to \mathbb{R}^2$.

Solution: Since the interpretation in terms of mappings was given as illustration, but not proved, we should abide by the very definition of the operation and prove in particular the associative law from it, rather than claiming inheritance from composition of mappings in general.

We use in particular that the product of orthogonal matrices is orthogonal to make sure the operation is well-defined, i.e., $(AB, Ab + a) \in O_2(\mathbb{R}) \times \mathbb{R}^2$. The neutral element is $(I, \vec{0})$, because $(I, \vec{0}) \odot (A, a) = (IA, Ia + \vec{0}) = (A, \vec{0})$. (The right neutral property can be checked similarly, but need not, since it follows together with the other group axioms as shown in class.) The inverse of (A, a) is $(A^{-1}, -A^{-1}a)$, because $(A^{-1}, -A^{-1}a) \odot (A, a) = (A^{-1}A, A^{-1}a - A^{-1}a) = (I, \vec{0})$. (A similar comment applies how we can, but need not, check right inverse property.) – To find the inverse rather than pulling out of the hat, you'd solve $(B, b) \odot (A, a) = (I, \vec{0})$ for B and b.

The associative law:

$$\Big((A,a) \odot (B,b)\Big) \odot (C,c) = (AB, Ab + a) \odot (C,c) = ((AB)C, (AB)c + (Ab + a))$$
$$(A,a) \odot \Big((B,b) \odot (C,c)\Big) = (A,a) \odot (BC, Bc + b) = (A(BC), A(Bc + b) + a)$$

By the associativity of matrix multiplication (between 2×2 matrices as well as between 2×2 and 2×1 matrices) and the associativity of vector addition, both right hand sides are equal.

Hwk 12:

Let R be any ring (with operations $+$ and $\cdot$). Define the matrix ring $M_n(R)$ as the set of all $n \times n$ matrices whose entries are in R. The addition will be componentwise, and the multiplication will also be defined as in the usual matrix algebra course: $(AB)_{ik} = \sum_{j=1}^{n} A_{ij} B_{jk}$.

Show that $M_n(R)$ is a ring, and show that it has an identity provided R has.

Solution: We denote the entries of matrix $A \in M_n(R)$ with $A_{ij} \in R$. All summations will range from 1 to n, so $\sum_i$ is an abbreviation for $\sum_{i=1}^{n}$. For didactical clarification, we denote the addition and multiplication in $M_n(R)$ by $\oplus$ and $\odot$, thus distinguishing them from the operations in R. This change in notation is not necessary.

Commutativity of $\oplus$*:* $(A \oplus B)_{ij} := A_{ij} + B_{ij}$, whereas $(B \oplus A)_{ij} := B_{ij} + A_{ij}$. These latter two expressions are equal due to commutativity of $+$ in R.

Associativity of $\oplus$*:* $((A \oplus B) \oplus C)_{ij} := (A_{ij} + B_{ij}) + C_{ij}$, whereas $(A \oplus (B \oplus C))_{ij} := A_{ij} + (B_{ij} + C_{ij})$. These two expressions are equal, due to associativity of $+$ in R.

Additive neutral: If 0 is the additive neutral in R, then the zero matrix $\mathbf{0}$ defined by $\mathbf{0}_{ij} = 0$ for each (i,j) is the additive neutral in $M_n(R)$. Indeed, $(A \oplus \mathbf{0})_{ij} = A_{ij} + \mathbf{0}_{ij} = A_{ij} + 0 = A_{ij}$.

Additive inverse: The additive inverse of A is the matrix whose entries are $-A_{ij}$. Calculation omitted (just as trivial as the preceding ones).

Distributive Laws: We only check $A \odot (B \oplus C) = (A \odot B) \oplus (A \odot C)$. The other relation, $(B \oplus C) \odot A = (B \odot A) \oplus (C \odot A)$ is proved analogously.

$$\begin{aligned}
\Big(A \odot (B \oplus C)\Big)_{ik} &\underset{(1)}{=} \sum_j A_{ij} (B \oplus C)_{jk} \underset{(2)}{=} \sum_j A_{ij} (B_{jk} + C_{jk}) \underset{(3)}{=} \sum_j A_{ij} B_{jk} + A_{ij} C_{jk} \\
&\underset{(4)}{=} \Big(\sum_j A_{ij} B_{jk}\Big) + \Big(\sum_j A_{ij} C_{jk}\Big) \underset{(5)}{=} (A \odot B)_{ik} + (A \odot C)_{ik} \underset{(6)}{=} \Big((A \odot B) \oplus (A \odot C)\Big)_{ik}
\end{aligned}$$

These equalities are justified as follows: (1) definition of matrix product; (2) definition of matrix sum; (3) distributive law in R; (4) commutative and associative laws for $+$ in R, enhanced from two to n terms by means of induction; (5) definition of matrix addition; (6) definition of matrix multiplication.

Associativity of $\odot$*:*

$$\begin{aligned}
\Big(A \odot (B \odot C)\Big)_{il} &\underset{(1)}{=} \sum_j A_{ij} (B \odot C)_{jl} \underset{(2)}{=} \sum_j A_{ij} \Big(\sum_k B_{jk} C_{kl}\Big) \underset{(3)}{=} \sum_j \Big(\sum_k A_{ij} (B_{jk} C_{kl})\Big) \\
&\underset{(4)}{=} \sum_j \Big(\sum_k (A_{ij} B_{jk}) C_{kl}\Big) \underset{(5)}{=} \sum_k \Big(\sum_j (A_{ij} B_{jk}) C_{kl}\Big) \underset{(6)}{=} \sum_k (A \odot B)_{ik} C_{kl} \underset{(7)}{=} \Big((A \odot B) \odot C\Big)_{il}
\end{aligned}$$

These equalities are justified as follows: (1),(2) definition of matrix product; (3) distributive law in R, enhanced by induction; (4) associativity of multiplication in R; (5) commutative and associative laws for $+$ in R, enhanced from two to n terms by means of induction; (6),(7) definition of matrix multiplication.

Multiplicative neutral: If 1 is the multiplicative neutral in R (and 0 the additive neutral), then the matrix $\mathbf{1}$, given by $\mathbf{1}_{ij} = 1$ if $i = j$, and $\mathbf{1}_{ij} = 0$ if $i \neq j$, is the multiplicative neutral in $M_n(R)$. Indeed, $(A \odot \mathbf{1})_{ik} = \sum_j A_{ij} \mathbf{1}_{jk} = A_{ij}|_{j=k} = A_{ik}$, so $A \odot \mathbf{1} = A$. A similar calculation shows $\mathbf{1} \odot A = A$. Both are needed, logically.

Hwk 13:

> Let R be a ring (with operations $+$ and $\cdot$). We define operations on $R \times R$ as follows:
>
> $$(x,y)+(u,v) := (x+u, y+v)\ , \quad (x,y)\cdot(u,v) := (xu-yv, xv+yu)$$
>
> Here, as usual, $a-b$ stands for a plus the additive inverse of b.
>
> Show that this defines a ring. We are going to denote $R \times R$, when adorned with *these* operations, as $R[i]$. (This is admittedly a strange name as of yet).

Solution: The abelian group properties for the addition are immediate and follow similarly as in the previous problem. I won't write them out again.

I'll tacitly use simple properties involving $-$, which can be concluded easily from the ring axioms, usually using the distributive law, next to other axioms.

Associativity of $\cdot$ *:*

$$\Big((s,t)\cdot(x,y)\Big)\cdot(u,v) \underset{(1)}{=} (sx-ty, sy+tx)\cdot(u,v) \underset{(2)}{=} ((sx-ty)u-(sy+tx)v, (sx-ty)v+(sy+tx)u)$$
$$\underset{(3)}{=} (sxu-tyu-syv-txv, sxv-tyv+syu+txu)$$
$$(s,t)\cdot\Big((x,y)\cdot(u,v)\Big) \underset{(1)}{=} (s,t)\cdot(xu-yv, xv+yu) \underset{(2)}{=} (s(xu-yv)-t(xv+yu), s(xv+yu)+t(xu-yv))$$
$$\underset{(3)}{=} (sxu-syv-txv-tyu, sxv+syu+txu-tyv)$$

These equalities are justified as follows: (1),(2) definition of product; (3) distributive law in R; associativity of addition; associativity of multiplication.

The results coincide, due to commutativity of addition.

Distributive Laws: I'll show $\Big((s,t)+(x,y)\Big)\cdot(u,v) = (s,t)\cdot(u,v)+(x,y)\cdot(u,v)$. The other distributive law is proved analogously. (Both are needed, logically.)

$$\Big((s,t)+(x,y)\Big)\cdot(u,v) \underset{(1)}{=} (s+x, t+y)\cdot(u,v) \underset{(2)}{=} ((s+x)u-(t+y)v, (s+x)v+(t+y)u)$$
$$\underset{(3)}{=} (su+xu-tv-yv, sv+xv+tu+yu) \underset{(4)}{=} ((su-tv)+(xu-yv), (sv+tu)+(xv+yu))$$
$$\underset{(5)}{=} (su-tv, sv+tu)+(xu-yv, xv+yu) \underset{(6)}{=} (s,t)\cdot(u,v)+(x,y)\cdot(u,v)$$

These equalities are justified as follows: (1) definition of sum; (2) definition of product; (3) distributive law in R; associativity of addition; (4) commutativity of addition (and associativity again); (5) definition of sum; (6) definition of product; associativity of multiplication.

Hwk 14:

> Continuing the previous problem, show that $R[i]$ has an identity, if R has. Show also that $R[i]$ is commutative, if R is.
>
> Assume that R is a field. Must $R[i]$ necessarily be a field? If not, what condition must be satisfied in R to guarantee that $R[i]$ is a field?

Solution: $(1,0)$ is an identity: $(1,0)\cdot(u,v) = (1u-0v, 1v+0u) = (u,v)$. This is because we showed that $0a = 0$ in any ring. An analogous proof applies to the reverse order of factors. (Both are needed logically, unless R is commutative.)

If R is commutative, then $(x,y)\cdot(u,v) = (xu-yv, xv+yu)$ and $(u,v)\cdot(x,y) = (ux-vy, uy+vx)$ coincide because $ux = xu$ etc. (Commutativity of addition is also used.)

On top of the preceding properties, we now assume that R is a field, i.e., $1 \neq 0$ and every $a \neq 0$ has an inverse. Clearly, then $(1,0) \neq (0,0)$. Let's see, if every (a,b) has an inverse (except if $a=b=0$): We look for (x,y) such that $(a,b)\cdot(x,y)=(1,0)$.

First we calculate (x,y), *assuming* such an (x,y) exists. Since it is not legitimate to make this assumption, we then use the resulting formula and *prove* that it satisfies the required condition, thus proving the existence of an inverse (under conditions about to be established during the calculation).

The eqn $(a,b)\cdot(x,y)=(1,0)$ means $ax-by=1$ and $ay+bx=0$. Unless $b=0$, the second equation implies $x=-ayb^{-1}$. Plugging this into the first equation, we conclude $-aayb^{-1}-by=1$, and multiplying by $-b$, we get $(aa+bb)y=-b$. *Assuming* that $aa+bb\neq 0$, we find that $y=-b(aa+bb)^{-1}$ and then from $x=-ayb^{-1}$ that $x=a(aa+bb)^{-1}$. We omit discussion of the case $b=0$, since we have anyways only found a necessary condition for the inverse (as a motivation to come up with the formula), but must show sufficiency of the heuristically found formula.

From this equation, we suspect, claim (and then prove):

Thm: If R is a field such that $aa+bb\neq 0$ for any a,b other than $(a,b)=(0,0)$, then $R[i]$ is a field, and the inverse of (a,b) is $(a(aa+bb)^{-1},-b(aa+bb)^{-1})$.

Proof: The formula makes sense since $aa+bb\neq 0$. We check:

$$\begin{aligned}
&(a,b)\cdot\Big(a(aa+bb)^{-1},-b(aa+bb)^{-1}\Big)\\
&\quad=\Big(aa(aa+bb)^{-1}-b(-b)(aa+bb)^{-1},a(-b)(aa+bb)^{-1}+ba(aa+bb)^{-1}\Big)\\
&\quad=\Big((aa+bb)(aa+bb)^{-1},(-ab+ba)(aa+bb)^{-1}\Big)=(1,0)
\end{aligned}$$

Note: The condition (1) '$aa+bb\neq 0$ unless $a=b=0$' in a field R is equivalent to the condition (2) '$xx+1=0$ has no solution'. The conclusion (1) $\Rightarrow$ (2) is trivial. The converse 'not(1) $\Rightarrow$ not(2)' is true because, for a pair $(a,b)\neq(0,0)$, either $x_1=ab^{-1}$ or $x_2=ba^{-1}$ is defined (maybe both); and if $aa+bb=0$ then whichever of x_1,x_2 is defined solves the equation $x^2+1=0$.

We now show the converse of our theorem:
Thm: If R is a field in which the equation $aa+bb=0$ has solutions other than $(0,0)$, then $R[i]$ is NOT a field, but actually has zero divisors.

Proof: According to the note, this field R contains some x such that $xx+1=0$. Then however, the element $(1,x)\in R[i]$ has no inverse. This is because $(1,x)\cdot(1,-x)=(1\cdot 1-x(-x),1(-x)+x1)=(1+xx,0)=(0,0)$. If $(1,x)$ had an inverse, then multiplying $(1,x)(1,-x)=(0,0)$ with this inverse would imply $(1,x)=(0,0)$, a contradiction.

Hwk 15:

> Continuing the previous problem, let R be a commutative ring with identity 1. In $R[i]$, we'll denote the element $(0,1)$ with the special symbol i. (You start getting an idea where $R[i]$ got its name from.) Calculate $i\cdot i$ (too easy...).
>
> I claim that, for the case $R=\mathbb{R}$, the field of real numbers, you should be at least vaguely familiar with $\mathbb{R}[i]$ under a different name. Which one? Set up a complete translation dictionary (it has only a few lines) that translates the notation set up in Problem 4 into the more familiar one.
>
> Show that $\mathbb{R}[i]$ is a field.

Solution: Since x^2+1 has no solutions in $\mathbb{R}$, we have just showed that $\mathbb{R}[i]$ is a field. With $i:=(0,1)$, we calculate $i\cdot i=(-1,0)$, the negative of the multiplicative identity in $\mathbb{R}[i]$. So we have found an $i\in R[i]$ satisfying $i^2=-1$. (*This* 1 denotes an element of $\mathbb{R}[i]$ rather than of $\mathbb{R}$.

We know $\mathbb{R}[i]$ under the name $\mathbb{C}$ as the field of complex numbers.

The real numbers a correspond to the complex numbers $(a,0) \in \mathbb{R}[i]$, which are usually denoted as $a \in \mathbb{C}$. This re-use of notation causes no confusion, since the product of complex numbers a and b, i.e., $(a,0)\cdot(b,0) = (ab,0)$ does equal to the (real) product ab, interpreted as a complex number. So the result is the same, whether you interpret the product in ab as a product in $\mathbb{R}$ or in $\mathbb{R}[i]$, and a similar remark applies to the sum $a+b$.

This way, $\mathbb{R}$ becomes a *subset*, actually a subring of $\mathbb{R}[i] = \mathbb{C}$.

The equation $(a,b) = (a,0)\cdot(1,0) + (b,0)\cdot(0,1)$ allows to write (a,b) as $a\cdot 1 + b\cdot i$, or $a+bi$.

The problem has therefore given an *explicit construction* of $\mathbb{C}$, beginning with $\mathbb{R}$. A similar comment applies to $R[i]$ for any ring R.

Hwk 16:

> I claimed in class that the power set $\mathcal{P}(M)$ (which is the set of all subsets of M), together with the operations $A+B := (A\setminus B)\cup(B\setminus A)$ and $A\cdot B := A\cap B$ is a commutative ring with identity. Prove the distributive law (as far as not done in class yet) and the associativity for $+$.

Solution: (1) Let's prove the distributive law $A(B+C) = AB + AC$, which, in set theoretic language, means $A\cap((B\setminus C)\cup(C\setminus B)) = ((A\cap B)\setminus(A\cap C))\cup((A\cap C)\setminus(A\cap B))$

(1.1) First we prove the inclusion '$\subseteq$': So let $x \in A\cap((B\setminus C)\cup(C\setminus B))$. So $x\in A$. Moreover $x \in B\setminus C$ or $x\in C\setminus B$. So x is in exactly one of the sets B, C. — Suppose $x\in B$. Then $x\notin C$. Since $x\in A$ also, we have $x\in A\cap B$. We clearly have $x\notin A\cap C$, since $x\notin C$. Hence $x\in((A\cap B)\setminus(A\cap C))$. The conclusion $x\in((A\cap B)\setminus(A\cap C))\cup((A\cap C)\setminus(A\cap B))$ is immediate. — If instead $x\in C$, then $x\notin B$, and the same conclusion follows similarly through $x\in(A\cap C)\setminus(A\cap B)$.

(1.2) Next we prove the converse inclusion '$\supseteq$': So assume $x\in((A\cap B)\setminus(A\cap C))\cup((A\cap C)\setminus(A\cap B))$. This means $x\in(A\cap B)\setminus(A\cap C)$ or $x\in((A\cap C)\setminus(A\cap B)$. — Suppose first that the former is the case. Then $x\in A\cap B$, but $x\notin A\cap C$. In particular from the first statement $x\in A$, and $x\in B$. From the second statement $x\notin A\cap C$ we conclude, since we know already that $x\in A$, that x cannot also be in C. So $x\in B\setminus C$, and a fortiori $x\in(B\setminus C)\cup(C\setminus B)$. Since also $x\in A$, the conclusion follows. — The other case, namely $x\in((A\cap C)\setminus(A\cap B))$, is handled analogously.

We have shown one distributive law. The other one doesn't need to be proved, since the commutative law for $\cap$ holds.

(2) There is another way to prove the same thing: Rather than nesting case distinctions as in the previous proof, we can start with eight cases right away, depending on whether x is or is not in A, B, C, respectively. We then draw conclusions for each case in which set x is or is not. If the results coincide for two sets in all eight cases, then we have proved equality of the said two sets. The cases can be handled in tabular form.

We redo the proof of the distributive law: Compare the columns marked by arrows.

$x\in$	$A?$	$B?$	$C?$	$B\setminus C$	$C\setminus B$	$B+C$	$A(B+C)$	AB	AC	$AB+AC$
	y	y	y	n	n	n	n	y	y	n
	y	y	n	y	n	y	y	y	n	y
	y	n	y	n	y	y	y	n	y	y
	y	n	n	n	n	n	n	n	n	n
	n	y	y	n	n	n	n	n	n	n
	n	y	n	y	n	y	n	n	n	n
	n	n	y	n	y	y	n	n	n	n
	n	n	n	n	n	n	n	n	n	n
							$\uparrow$			$\uparrow$

(3) For the associative law, it seems more transparent to use the second method with eight up-front cases, so we only use this method for the proof. To simplify the table, note that $x \in A+B$, if and only if x is in exactly one, but not both of A, B.

$x \in$	$A?$	$B?$	$C?$	$A+B$	$(A+B)+C$	$B+C$	$A+(B+C)$
	y	y	y	n	y	n	y
	y	y	n	n	n	y	n
	y	n	y	y	n	y	n
	y	n	n	y	y	n	y
	n	y	y	y	n	n	n
	n	y	n	y	y	y	y
	n	n	y	n	y	y	y
	n	n	n	n	n	n	n
					$\uparrow$		$\uparrow$

Hwk 17:

Suppose, in a ring, the extra property $a \cdot a = a$ is verified for *every* a. (The previous problem is an example where this happens.) Show generally, that a ring satisfying that extra property is automatically commutative: Since this is a bit tricky, I give you the steps (the steps how I did it; I wouldn't claim with certainty that there cannot be another, shorter way):

(a) Show that $b+b=0$ for every b. You do this by calculating $(b+b)\cdot(b+b)$ in two different ways.
(b) Show that $bcb = cbc$ for every b, c. You do this by calculating $(b\cdot c - c\cdot b)\cdot(b\cdot c - c\cdot b)$ in two different ways.
(c) Conclude $b\cdot c = c\cdot b$ from part (b) by appropriate multiplications and by again using $a\cdot a = a$.

Each step needs to be justified by explicit reference to the ring axioms (or to consequences thereof that were proved in class).

Solution: (a) By using the distributive law twice, we conclude $(b+b)\cdot(b+b) = b\cdot(b+b)+b\cdot(b+b) = (b\cdot b+b\cdot b)+(b\cdot b+b\cdot b)$. Using the property $a\cdot a = a$ for $a := b$, this simplifies to $(b+b)+(b+b)$. On the other hand, using the property $a\cdot a = a$ with $a = b+b$, we conclude $(b+b)\cdot(b+b) = b+b$. Comparing the two, we have found $(b+b)+(b+b) = (b+b)$ for every b. Subtracting $(b+b)$, we find $b+b=0$.

To simplify language, let's refer to $a\cdot a = a$ as the idempotence property. Let's also omit the $\cdot$ for multiplication.

(b) $(bc-cb)(bc-cb) = (bc-cb)$ by the idempotence property. Now let's evaluate the same expression using the distributive law for $-$ (which is an easy consequence of the distributive law for $+$[1]): $(bc-cb)(bc-cb) = (bc-cb)(bc)-(bc-cb)(cb) = ((bc)(bc)-(cb)(bc))-((bc)(cb)-(cb)(cb))$. Using the associativity of multiplication and then the idempotence, this simplifies to $((bc)(bc) - c(bb)c) - (b(cc)b - (cb)(cb)) = (bc-cbc)-(bcb-cb)$.

As noted in the footnote, $+$ and $-$ are the same in this ring, due to (a). Equating the two results and using associativity of $+$, we conclude $bc+cb = bc+cbc+bcb+cb$, and adding appropriate inverses, we get $0 = cbc+bcb$. Hence $cbc = -(bcb) = bcb$.

[1]We have seen $a0 = 0$ in class. From $a(-c)+ac = a(-c+c) = a0 = 0$, it follows that $a(-c) = -(ac)$. Now $a(b-c) = a(b+(-c)) = ab+a(-c) = ab+(-ac) = ab-ac$. – In this particular example however, we do not need the distributiv law for $-$, because $b+b=0$ implies $b=-b$, so $+$ and $-$ are actually the same operation.

(c) Multiplying $cbc = bcb$ with b from the right and using associativity of multiplication, we get $(cb)(cb) = (bc)(bb)$. By idempotence, $cb = bcb$. Similarly, multiplying $cbc = bcb$ by c from the right yields $cbc = bc$. Combining these two results with $cbc = bcb$, we get $cb = bc$.

You may wonder how I found this solution. Well, I said 'if $bc = cb$ is really true, that means $bc - cb = 0$. So let me see if I can 'simplify' $bc - cb$ to 0, using ring axioms and the idempotence property. So I started $bc - cb = (bc - cb)^2 = bcbc - bccb - cbbc + cbcb = bc - bcb - cbc + cb$. That didn't help too much, but I tried the same with $bc + cb$, began to multiply the obtained equations with b or c from either side, until I eventually discovered the $a + a = 0$ property.

Hwk 18:

> Show: A ring with exactly 3 elements, $\{0, a, b\}$ must be commutative. *Hint: First show* $a + a = b$.

Solution: We know that $0 + a$, $a + a$ and $b + a$ must be the elements $0, a, b$ in some order. Since $0 + a = a$, there are only two choices left for $a + a$, namely 0 and b. But if $a + a$ were 0, then $a + b$ would have to be b (the other results being 'taken' already). But this would imply $a = 0$, a contradiction. So we must have $a + a = b$.

The commutative law comes in three cases, two of which are trivial: $a0 = 0 = 0a$ and $b0 = 0 = 0b$. We only have to show $ab = ba$: Indeed,

$$ab = a(a + a) = aa + aa = (a + a)a = ba$$

Hwk 19:

> In the ring $\mathbb{Z}$, find the gcd of 43728 and 15360 ('the' gcd: so make it a positive number), and express this gcd in the form $43728k + 15360\ell$ with integers k, ℓ.

Solution: We do repeated division with remainder (Euclidean algorithm):

$a = q \cdot$	$b +$	r	
$43728 = 2 \cdot$	$15360 +$	13008	(1)
$15360 = 1 \cdot$	$13008 +$	2352	(2)
$13008 = 5 \cdot$	$2352 +$	1248	(3)
$2352 = 1 \cdot$	$1248 +$	1104	(4)
$1248 = 1 \cdot$	$1104 +$	144	(5)
$1104 = 7 \cdot$	$144 +$	96	(6)
$144 = 1 \cdot$	$96 +$	48	(7)
$96 = 2 \cdot$	$48 +$	0	

The gcd is the last nonzero remainder, 48. We now express 48 as a linear combination of the corresponding a and b, beginning in line (8), backward line by line until the first one:

$$\begin{aligned}
48 &\underset{(7)}{=} \mathbf{144} - 1 \cdot \mathbf{96} \\
&\underset{(6)}{=} \mathbf{144} - 1 \cdot (\mathbf{1104} - 7 \cdot \mathbf{144}) = 8 \cdot \mathbf{144} - 1 \cdot \mathbf{1104} \\
&\underset{(5)}{=} 8 \cdot (\mathbf{1248} - 1 \cdot \mathbf{1104}) - 1 \cdot \mathbf{1104} = 8 \cdot \mathbf{1248} - 9 \cdot \mathbf{1104} \\
&\underset{(4)}{=} 8 \cdot \mathbf{1248} - 9 \cdot (\mathbf{2352} - 1 \cdot \mathbf{1248}) = 17 \cdot \mathbf{1248} - 9 \cdot \mathbf{2352} \\
&\underset{(3)}{=} 17 \cdot (\mathbf{13008} - 5 \cdot \mathbf{2352}) - 9 \cdot \mathbf{2352} = 17 \cdot \mathbf{13008} - 94 \cdot \mathbf{2352} \\
&\underset{(2)}{=} 17 \cdot \mathbf{13008} - 94 \cdot (\mathbf{15360} - 1 \cdot \mathbf{13008}) = 111 \cdot \mathbf{13008} - 94 \cdot \mathbf{15360} \\
&\underset{(1)}{=} 111 \cdot (\mathbf{43728} - 2 \cdot \mathbf{15360}) - 94 \cdot \mathbf{15360} = \underline{\underline{111 \cdot \mathbf{43728} - 316 \cdot \mathbf{15360}}}
\end{aligned}$$

So if you think it's not so straightforward to write the gcd as a linear combination, you are right: it is *straightbackward!*

Hwk 20:

In this problem, we'll see that the division algorithm can be mimicked in the ring $\mathbb{Z}[i]$, which consists of the numbers $a+bi$ where $a, b \in \mathbb{Z}$ and i is the imaginary unit. You may view this ring either as a subring of $\mathbb{C}$, or as an instance of the class of rings constructed in Problem 5.

Given $a = a_1 + a_2 i \in \mathbb{Z}[i]$ and $b = b_1 + b_2 i \in \mathbb{Z}[i]$ with $b \neq 0$, we want to find $q = q_1 + q_2 i \in \mathbb{Z}[i]$ and $r = r_1 + r_2 i \in \mathbb{Z}[i]$ such that $a = qb + r$ and r "smaller" than b. We cannot require "$0 \leq r < b$" because we do not have an order in the ring $\mathbb{Z}[i]$; a statement "$0 \leq r < b$" would be meaningless. Instead we will use the absolute value of complex numbers and require that $|r|$ is smaller than $|b|$, or, equivalently: $r_1^2 + r_2^2 < b_1^2 + b_2^2$.

Given $a = a_1 + a_2 i \in \mathbb{Z}[i]$ and $b = b_1 + b_2 i \in \mathbb{Z}[i] \setminus \{0\}$, let $\vartheta = \vartheta_1 + i\vartheta_2 \in \mathbb{C}$ be the exact quotient $\vartheta = a/b$. Let q_1 be an integer closest possible to ϑ_1 (there may be several equally good choices) and let q_2 be an integer closest possible to ϑ_2. Let r be the remainder making $a = qb + r$ true

(a) To make sure you understand the principle, find q and r according to the prescription of the preceding paragraphs in the case $a = 517 + 213i$, $b = 11 + 25i$. Check that $r_1^2 + r_2^2$ is indeed less than $b_1^2 + b_2^2$.

(b) Write out explicitly what $a = \vartheta b$ means for a_1, a_2, b_1, b_2 and ϑ_1, ϑ_2. — Write out explicitly what $a = qb + r$ means for $a_1, a_2, b_1, b_2, q_1, q_2, r_1, r_2$. — What does your prescription about the choice of q imply about the size of $q_1 - \vartheta_1$, $q_2 - \vartheta_2$?

(c) Express r_1 and r_2 in terms of $b_1, b_2, q_1 - \vartheta_1, q_2 - \vartheta_2$ and conclude that $r_1^2 + r_2^2 < b_1^2 + b_2^2$.

Solution:

$$\vartheta = \frac{517 + 213i}{11 + 25i} = \frac{(517 + 213i)(11 - 25i)}{(11 + 25i)(11 - 25i)} = \frac{11012 - 10582i}{11^2 + 25^2} = \frac{11012 - 10582i}{746} = 14.76 - 14.18i$$

By going to the *nearest* integer respectively, we have $q = 15 - 14i$. From this, we calculate $r = (517 + 213i) - (15 - 14i)(11 + 25i) = 2 - 8i$. So in this case indeed, $|r|^2 = 68 < |b|^2 = 746$.

According to the rounding rule for general principle case, we note that $|q_1 - \vartheta_1| \leq \frac{1}{2}$ and $|q_2 - \vartheta_2| \leq \frac{1}{2}$.

From $a = \vartheta b$, i.e., $a_1 = \vartheta_1 b_1 - \vartheta_2 b_2$ and $a_2 = \vartheta_1 b_2 + \vartheta_2 b_1$, and from $a = qb + r$, i.e., $a_1 = q_1 b_1 - q_2 b_2 + r_1$ and $a_2 = q_1 b_2 + q_2 b_1 + r_2$, we conclude $r = (\vartheta - q)b$, i.e., $r_1 = (\vartheta_1 - q_1)b_1 - (\vartheta_2 - q_2)b_2$ and $r_2 = (\vartheta_1 - q_1)b_2 + (\vartheta_2 - q_2)b_1$.

Don't try to move the inequalities in here yet: You wouldn't get anything useful. Squaring and adding (the mixed terms cancel) yields

$$r_1^2 + r_2^2 = \Big((\vartheta_1 - q_1)^2 + (\vartheta_2 - q_2)^2\Big)(b_1^2 + b_2)^2 \leq (\frac{1}{4} + \frac{1}{4})(b_1^2 + b_2^2) < b_1^2 + b_2^2$$

So indeed, the outlined algorithm yields an integer division in which the remainder is smaller than the divisor.

Hwk 21:

In many rings that are not fields, it can happen that $ab = 0$ for certain $a \neq 0$ and $b \neq 0$. The next problem gives a whole lot of examples, this one wants you merely to show:

In any ring, if $ab = 0$, but $a \neq 0$ and $b \neq 0$, then neither a nor b has a multiplicative inverse.

Solution: If a had an inverse a^{-1}, then multiplying $ab = 0$ from the left with a^{-1} would give $b = 0$. Similarly, if b had an inverse, multiplying $ab = 0$ with it from the right would yield $a = 0$.

Note: It makes no sense to talk of a multiplicative inverse, unless the ring has a 1. But that's fine for the problem: If the ring has no 1, then the claim is vacuously true.

Hwk 22:

> Let me introduce a name: In a ring, whenever $a \neq 0$ and $b \neq 0$ satisfy $ab = 0$, then a and b are called *zero divisors*. In this problem, you'll find zero divisors in various rings:
>
> (a) The ring $C^0[0, 1]$ of continuous, real-valued functions on the interval $[0, 1]$, with the usual addition and multiplication of functions. (The proof of the ring properties is straightforward, you are not required to write it out here.) Find a pair of zero divisors. *If you find this difficult, then the most likely source of your difficulty is that you are shying away from piecewise defined functions.*
>
> (b) In the ring $M_2(\mathbb{Z}) = \mathbb{Z}^{2\times2}$ of 2×2 matrices with integer entries, find a pair of zero divisors.
>
> (c) In the direct sum $\mathbb{Z} \oplus \mathbb{Z}$, find a pair of zero divisors.
>
> (d) In the ring $\mathcal{P}(M)$ described in Problem 16, where $M = \{\Box, \Diamond, \star, \triangle\}$, find a pair of zero divisors.
>
> (e) Bonus problem: How many pairs of zero divisors does the commutative ring in (d) have, *not* counting pairs (A, B) and (B, A) as different?

Solution: (a) Let $f(x) := (1 - 2x)_+ = \max\{1 - 2x, 0\}$ and $g(x) := (2x - 1)_+ = \max\{2x - 1, 0\}$. Then $f(x)g(x) = 0$ for each x, since the first factor vanishes when $x \geq \frac{1}{2}$ and the second factor vanishes when $x \leq \frac{1}{2}$. Neither f nor g is 0 (i.e., the constant-zero function, which is the additive neutral in this ring). But the product fg is the 0 function (namely is identically 0).

(b) $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

(c) $(a, 0) \cdot (0, b) = (a \cdot 0, 0 \cdot b) = (0, 0)$.

(d) Remember that the 0 in this ring is the empty set $\emptyset$. $A = \{\Box, \Diamond\}$ and $B = \{\star\}$ are an example of zero divisors.

(e) The questions is how many pairs of disjoint nonempty subsets of a set of 4 elements can one find? A and B both single element sets has $\binom{4}{2} = 6$ possibilities. A a set with a single element and B a two element set has $4 \cdot 3 = 12$ possibilities. A a single element set and B with three elements has 4 possibilities. A and B each two elements has 3 possibilities. Altogether 25 pairs.

Hwk 23:

> Show that in a ring with identity that has more than one element, the multiplicative identity is automatically different from the additive identity.

Solution: Note that the additive identity 0 is defined exclusively in terms of + axioms, whereas the multiplicative identity 1 is defined exclusively in terms of $\cdot$ axioms. It seems impossible to establish any relation between the two without using an axiom that connects + and $\cdot$. This is the distributive law.

We use the property $a0 = 0$ for all a, which follows from the distributive law: $a0 = a(0+0) = a0+a0$, hence $a0 = 0$. We prove the contrapositive, namely: If in a ring R with identity it holds $1 = 0$, then R has only one element. Indeed, if $0 = 1$ then $0 = a0 = a1 = a$, so each element a would equal zero.

Hwk 24:

> In a ring with identity (not necessarily commutative!), assume that the elements a and b each have a multiplicative inverse; we'll call them a^{-1} and b^{-1} respectively. Show that ab has a multiplicative inverse as well, and give a 'formula' for it, in terms of a^{-1} and b^{-1}.

Solution: It is a good motivation, but a questionable (at best) proof to start with $x(ab) = 1$ and solve for x, via right multiplication with b^{-1} and then a^{-1}. This argument only shows: *If* ab *has an inverse, it can only be* $b^{-1}a^{-1}$. But the existence of an inverse must be shown, not assumed!

So we simply claim and prove by direct calculation that $b^{-1}a^{-1}$ is inverse to ab. Both order of factors must be checked because in a ring, right inverse does NOT imply left inverse.

$$\begin{aligned}(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b = b^{-1}1b = b^{-1}b = 1\\ (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1\end{aligned}$$

Hwk 25:

> Let A be any subset of $[0,1]$ (think of finitely many numbers between 0 and 1). Within the ring $C^0[0,1]$ (defined in 22a above), consider the set
>
> $$C^0_A[0,1] := \{f \mid f(x) = 0 \text{ for all } x \in A\}$$
>
> Show that $C^0_A[0,1]$ is a subring of $C^0[0,1]$.

Solution: We have to show that if $f, g \in C^0_A[0,1]$, then $fg, f+g, -f \in C^0_A[0,1]$, and that the zero function is in $C^0_A[0,1]$ (this latter is trivial). In other words, we have to show: if $f(x) = 0 = g(x)$ for all $x \in A$, then $f(x)g(x), f(x)+g(x), -f(x) = 0$ for all $x \in A$. This is trivial, b/c $0 \cdot 0$, $0+0$ and -0 equal 0. *Note: A simple theorem in the book states that it is sufficient to show that $f-g$ and fg are in the ring if f and g are. A proof that uses this result is just as easy as the one given here.*

Hwk 26:

> Warning / Surprise: If R is a ring with identity 1_R and S is a subring not containing the element 1_R, then S might still have an identity 1_S different from 1_R. In that case, by the uniqueness of the identity, 1_S could not serve as a multiplicative identity in R. In this problem, you'll see two examples:
>
> (a) Take the ring $\mathbb{Z} \oplus \mathbb{Z}$. Give its multiplicative identity. Show that the ring $\mathbb{Z} \oplus \{0\} = \{(a,0) \mid a \in \mathbb{Z}\}$ is a subring of $\mathbb{Z} \oplus \mathbb{Z}$. Show that it does have a multiplicative identity, and exhibit it.
>
> (b) In the ring $\mathcal{P}(M)$, where $M = \{\square, \lozenge, \star, \triangle\}$, what is the multiplicative identity? Show that $\mathcal{P}(N)$, where $N = \{\square, \star, \triangle\}$, is a subring. What is its multiplicative identity?

Solution: (a) The multiplicative identity in $R \oplus R$ is $(1_R, 1_R)$. The closure properties of $\mathbb{Z} \oplus \{0\}$ are obvious: $(a,0)(b,0) = (ab,0)$, $(a,0)+(b,0) = (a+b,0)$, and $-(a,0) = (-a,0)$. So $\mathbb{Z} \oplus \{0\}$ is indeed a subring. The original identity $(1_R, 1_R)$ is not contained in this ring. However, $(1_R, 0)$ is an identity in $\mathbb{Z} \oplus \{0\}$ because $(1_R,0)(a,0) = (a,0) = (a,0)(1_R,0)$ for all $(a,0)$.

(b) In $\mathcal{P}(M)$, the multiplicative identity is M because $M \cap A = A \cap M = A$ for every $A \subseteq M$. For $N \subset M$, $\mathcal{P}(N)$ is a subset of $\mathcal{P}(M)$, because $x \in \mathcal{P}(N)$ means $x \subseteq N$, which implies $x \subseteq M$ and hence $x \in \mathcal{P}(M)$. Clearly, if $A, B \subseteq N$, then $A \cap B$ and $A + B$ are subsets of N, too; and so is $-A$

since $-A = A$ in this ring. So $\mathcal{P}(N)$ is a subring. The mult' identity M is NOT in $\mathcal{P}(N)$, if N is a strict subset of M.

However, N is the (new) multiplicative identity in $\mathcal{P}(N)$.

Hwk 27:

Why can a similar substitution of the *additive* identity not happen?

Solution: Let S be a subring of R. Let 0_S be its additive neutral, i.e., $0_S + a = a$ for all $a \in S$. This equation is an equation in the big ring R, too, and we can add $-a$ to the equation in this ring. So we get $0_S + a + (-a) = a + (-a)$ in R. But this means $0_S = 0_R$.

Hwk 28:

Divisibility by 11: To find the remainder of a number when divided by 11, for an integer given in decimal notation, the following rule can be used with the digits: Add the digits from right to left, with *alternating sign*. Add/subtract multiples of 11 as needed or desired. The result (between 0 and 10) is the remainder of the given integer upon division by 11.

Example: $a = 357123946803$; We calculate $c = 3-0+8-6+4-9+3-2+1-7+5-3 = -3$ Add 11 to get 8 (between 0 and 10): The remainder of a when divided by 11 is therefore 8.

Prove this rule by writing up a calculation in the ring $\mathbb{Z}_{11}$

Solution: The number $x = d_n d_{n-1} \dots d_1 d_0$ (to be read as a sequence of digits d_i in decimal representation, not as a product of variables) is actually $x = \sum_{i=0}^n d_i 10^i$. Now $10 \equiv -1 \bmod 11$. So in the ring $\mathbb{Z}_{11}$, we have $\bar{x} = \sum_{i=0}^n \bar{d}_i \overline{(-1)}^i$.

Hwk 29:

Given an integer a, let $Q(a)$ be the sum of its digits. E.g., $Q(37491) = 3+7+4+9+1 = 24$. What is

$$Q(Q(Q(4444^{4444})))\ ?$$

To answer the problem, give a rough estimate how large the number could be at most, and use a calculation in $\mathbb{Z}_9$ as a second piece of information.

Solution: We use two pieces of information: the first is modular arithmetic, which tells us that $x \equiv Q(x) \bmod 9$.

$$\begin{aligned} Q(Q(Q(4444^{4444}))) &\equiv 4444^{4444} \equiv Q(4444)^{4444} = 16^{4444} \equiv (-2)^{4444} = (-2)^{3\cdot 1481+1} = \\ &= (-8)^{1481}(-2) \equiv 1^{1481} 7 = 7 \qquad\qquad \bmod 9 \end{aligned}$$

This leaves still many possibilities for $Q(Q(Q(4444^{4444})))$: It could be 7 or 16 or 25 or 34 or ....

The next piece of info is a size estimate: $4444^{4444} < 10000^{4444} = 10^{4\cdot 4444}$. This means 4444^{4444} has at most $4 \cdot 4444 < 20000$ digits. (Sharper info could be obtained, but will not be needed.) Therefore $Q(4444^{4444}) < 20000 \cdot 9 = 180000$. In particular $Q(4444^{4444})$ has at most 6 digits, and unless it is actually at most five digits, the first digit is 1 and the second at most 7. This means $Q(Q(4444^{4444})) \leq 45$. Among numbers up to 45, it is 39 that has the lergest Q, namely 12.

We have therefore concluded that $Q(Q(Q(4444^{4444}))) \leq 12$, and at the same time $Q(Q(Q(4444^{4444}))) \equiv 7 \bmod 9$. Both together leave only one choice for the result, namely 7.

Hwk 30:

> Show that 13 (which is a prime in $\mathbb{Z}$ of course) is *not* irreducible in the ring $\mathbb{Z}[i]$. In other words, find integers a, b, c, d such that $(a+bi)(c+di) = 13$, but neither of the numbers $a+bi$, $c+di$ should be 1, -1, i or $-i$.

Solution: $13 = 2^2 + 3^2 = (2+3i)(2-3i)$.

Remember that the punchline is that neither factor is a unit, i.e., a divisor of 1 in the ring at hand. The wording of the problem anticipates that the only units are ± 1 *and* $\pm i$.

We may wish to prove this claim, or else we just prove that neither of $2 \pm 3i$ *is a unit in* $\mathbb{Z}[i]$. *If* $2-3i$ *were a unit, we'd need* $(2-3i)(a+bi) = 1$ *for some* $a+bi \in \mathbb{Z}[i]$. *We can solve this equation in the larger ring* $\mathbb{C}$ *(of which* $\mathbb{Z}[i]$ *is a subring), and then we see that* $a+bi = (2+3i)/13 \notin \mathbb{Z}[i]$.

Alternatively, if we want to prove that ± 1 *and* $\pm i$ *are the only units, we notice that if* $(a+bi)(c+di) = 1$, *then by taking the absolute value squared of the equation we get* $(a^2+b^2)(c^2+d^2) = 1$, *So* a^2+b^2 *must be 1, and this leaves only the four said possibilities for a unit* $a+bi$.