Problem 1: Describe all homomorphisms from a given ring R to a given ring S explicitly, i.e. say where every element $r \in R$ goes to in S. Prove that your functions are indeed homomorphisms and that there are no other homomorphisms.

- $R = \mathbb{Z}$, $S = \mathbb{Z} \times \mathbb{Z}$
- $R = \mathbb{Z}_5, S = \mathbb{Q}$
- $R = \mathbb{Z}_2 \times \mathbb{Z}_2, S = \mathbb{Z}_2$

Solution
Preface: A general strategy that I will be using in my solutions is using the fundamental theorem on homomorphisms:

(a) Define $\phi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ as $\phi(z) = (z, 0)$. To prove homomorphism:
$\phi(r + s) = (r + s, 0) = (r, 0) + (s, 0) = \phi(r) + \phi(s)$
$\phi(rs) = (rs, 0) = (r, 0)(s, 0) = \phi(r)\phi(s)$.
$\phi(z) = (0, z)$ works in the same way.

Another homomorphism would be $\phi(z) = \phi(z, z)$. This is a homomorphism: $\phi(r + s) = (r + s, r + s) = (r, r) + (s, s) = \phi(r) + \phi(s)$
$\phi(rs) = (rs, rs) = (r, r)(s, s) = \phi(r)\phi(s)$.

Lastly, $\phi(z) = (0, 0)$ works trivially just as $\psi : \mathbb{Z} \to \mathbb{Z}, \psi(z) = 0$ is a homomorphism.

There are no others, because the additive 0 in R must map to $(0, 0)$ in S. Linearly setting a coordinate to anything other than z or 0 will mean 0 does not transfer in this manner (needs to be linear so addition holds after applying the homomorphism)

(b) The trivial homomorphism of mapping all elements in $\mathbb{Z}_5$ to 0 in $\mathbb{Q}$ will work.

For nontrivial, $0, 1 \in \mathbb{Z}_5$ must map to $0, 1 \in \mathbb{Q}$. For addition to hold, adding 1 to itself 4 times (4 additions so 5 ones) must result in getting 0 in $\mathbb{Z}_5$, which will then be mapped to $0 \in \mathbb{Q}$. However, we must also be able to apply the homomorphism before adding, so we need to map 1 to an element in $\mathbb{Q}$ that, when added to itself 5 times, obtains 0. However, we have already mapped $1_{\mathbb{Z}_5}$ to $1_{\mathbb{Q}}$ (which is required for additive homomorphism to hold), so since $1_{\mathbb{Q}}$ does not behave in this way, there is no valid homomorphism, because we can not obtain the multiplicative identity from repeated addition of the additive identity in $\mathbb{Q}$ like we can in $\mathbb{Z}_5$. We basically can't make the characteristics of the two rings cooperate with each other.

(c) Define $\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$ to be

$$\begin{aligned}
(0, 0) &\to 0 \\
(0, 1) &\to 1 \\
(1, 0) &\to 1 \\
(1, 1) &\to 1
\end{aligned}$$

Which looks a lot like an xor gate. In other words, $\phi((a, b)) = a + b \in \mathbb{Z}_2$.

$\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_2$ are commutative rings (since both are abelian under both operations from 411), so both +

and $\cdot$ are associative and commutative in our ring (axiom)

$$\begin{aligned}
\phi((a,b)+(a',b')) &= \phi((a+a',b+b')) \\
&= (a+a')+(b+b') \\
&= a+(a'+b)+b' \\
&= a+(b+a')+b' \\
&= (a+b)+(a'+b') \\
&= \phi((a,b))+\phi((a',b'))
\end{aligned}$$

$$\begin{aligned}
\phi((a,b)(a',b')) &= \phi((aa',bb')) \\
&= (aa')(bb') \\
&= a(a'b)b' \\
&= a(ba')b' \\
&= (ab)(a'b)' \\
&= \phi((a,b))\phi((a',b))'
\end{aligned}$$

There are no other homomorphisms

Problem 2: For a given subset S of a given ring R, decide whether S is a subring or not (with proof)

- $S = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}, R = \mathbb{R}$
- $S = \{f(x) | f'(3) = 0\}, R = \{f : \mathbb{R} \to \mathbb{R}\}$

Solution

(a) S is closed, because $(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2}$, and $(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (a'b + ab')\sqrt{2}$. The elements of S are an abelian group with $+$ because they are a subgroup of $(\mathbb{R}, +)$, which is an abelian group. (recall subgroup of abelian group is abelian from 411). Elements of S are associative with $\cdot$ because they are in $\mathbb{R}$. The additive identity of reals, which S must inherit, is in S, where $a = b = 0 \in \mathbb{Z}$.

For distributivity:

$$(a + b\sqrt{2})\left[(a' + b'\sqrt{2}) + (a'' + b''\sqrt{2})\right]$$
$$(a + b\sqrt{2})\left[(a' + a'') + (b' + b''\sqrt{2})\right]$$
$$(aa' + aa'' + 2bb' + 2bb'') + (ab' + ab'' + a'b + a''b)\sqrt{2}$$
$$(aa' + 2bb') + (ab' + a'b)\sqrt{2} + (aa'' + 2bb'') + (ab'' + a''b)\sqrt{2}$$
$$(a + b\sqrt{2})(a' + b'\sqrt{2}) + (a + b\sqrt{2})(a'' + b''\sqrt{2})$$

Right distributivity holds since all elements in S commute in R, therefore they commute in S.

(b) S isn't closed under multiplication. If f and g are two functions with zero 3rd derivatives, the third derivative of $f(x)g(x)$ isn't necessarily zero because of the chain rule:

$$(f(x)g(x))'''$$
$$(f'(x)g(x) + f(x)g'(x))''$$
$$(f''(x)g(x) + 2f'(x)g'(x) + f(x)g''(x))'$$
$$f'''(x)g(x) + 3f''(x)g'(x) + 3f'(x)g''(x) + f(x)g'''(x)$$

The first and last terms are necessarily zero, but the middle two aren't necessarily (say if f and g are degree 2 polynomials with real coefficients), so S isn't closed, and therefore can't be a ring.

Problem 3: Describe all units in a given ring R explicitly

- $R = \mathbb{Z}_4 \times \mathbb{Z}_4$
- $R = Mat_2(\mathbb{Z}_2)$

Solution
(a) the unity of Z_4 is $(1, 1)$, because 1 is the multiplicative identity of $\mathbb{Z}_4$. Therefore, the units of R are the pairs with entries that are invertible in $\mathbb{Z}_4$, more specifically 1 and 3. There does not exist any element x such that $2x = 1 \in \mathbb{Z}_4$, because $\gcd(2, 4) = 2$, so the Diophantine equation equivalent to this congruence cannot equal any positive number strictly less than 2. Therefore, the units in R are $(1, 1), (1, 3), (3, 1)$, and $(3, 3)$.

(b) First note that ring has unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. For a matrix in this ring to be a unit, it must be invertible in the traditional sense of matricies under multiplication. Meaning for a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we have $ad - bc \neq 0$. In this case, the only other option is that $ad - bc = 1$. This equivalent to saying that $ad \neq bc$. All such matricies are units.

Problem 4: Given an example of a ring with unit $1 \neq 0$ that has a subtring with a non-zero unity $e \neq 1$

Solution

Take $R = \mathbb{Z}_2 \times \mathbb{Z}_2$ with subring of $\mathbb{Z}_2 \times 0$. The unit of the first ring is $(1, 1)$, and the unit of the second is $(1, 0)$.

Problem 5: Let U be a collection of all units in a ring $(R, +, \cdot)$ with unity, Prove that $(U, \cdot)$ is a group

Solution

Associative: $(R, +, \cdots)$ being a ring $\implies$ $\cdot$ is associative for all elements in R. Therefore, because all elements in U are also in R, they must all satisfy associativity under multiplication.

Identity: Say R has unity 1. $1 \in U$ because $\forall a \in R : a \cdot 1 = a \implies 1 \cdot 1 = 1$, which is the definition of a unit. Hence, $1 \in U$. Because all other units in U are also in R, the above property of unity (or identity for groups) is satisfied, and $1 \in R$ is the identity element of U.

Inverses: If a is a unit in R, then $\exists a' : aa' = 1$. Likewise, a' will be a unit because $\exists a'' : a'a'' = 1$, where $a'' = a$, so all units in R will "bring their inverses with them" into U.

Closure: for two units a, b with inverses a', b', the product ab is a unit because $abb'a = a1a' = aa' = 1$.

Problem 6: Let X be the collection of all rings. Prove that isomorphism of rings gives an equivalence relation on X

Solution

Reflexivity: all $R \in X$ are isomorphic to themselves, using the trivial isomorphism $\phi : R \to R$ defined by $\phi(r) = r$ for all $r \in R$.

Symmetry: For two rings R and S with isomorphism $\phi : R \to S$, there exists an inverse function $\phi^{-1} : S \to R$ since ring isomorphism is bijective, which is also a bijective homomorphism (and therefore an isomorphism). For arbitrary $r, r' \in R$, where $\phi(r) = s$ and $\phi(r') = s'$, ϕ is a homomorphism as: $\phi^{-1}(s + s') = \phi^{-1}(\phi(r) + \phi(r')) = \phi^{-1}(\phi(r + r')) = r + r' = \phi^{-1}(s) + \phi^{-1}(s')$
and
$\phi^{-1}(ss') = \phi^{-1}(\phi(r)\phi(r')) = \phi^{-1}(\phi(rr')) = rr' = \phi^{-1}(s)\phi^{-1}(s')$.

Transitivity: Assume that for rings R, S, T, there exist isomorphisms $\phi : R \to S$ and $\psi : S \to T$. Then $\psi \circ \phi : R \to T$ is an isomorphism. It is a bijection because both composing functions are bijective and the codomain of the interior function is the domain of the exterior composing function. $\psi \circ \phi$ is a homomorphism:
$\psi \circ \phi(r + r') = \psi(\phi(r) + \phi(r')) = \psi(s + s') = \psi(s) + \psi(s') = \psi \circ \phi(r) + \psi \circ \phi(r')$
and
$\psi \circ \phi(rr') = \psi(\phi(r)\phi(r')) = \psi(ss') = \psi(s)\psi(s') = \psi \circ \phi(r) \cdot \psi \circ \phi(r')$.

Problem 7: An element x of a ring R is called nilpotent if $x^n = 0$ for some $n > 0$.

(a) Find all nilpotents in $\mathbb{Z}_{2022}$

(b) Give an example of a ring with 2 nilpotents

(c) Let R be a commutative ring with nilpotents x, y. Show that $x + y$ is also nilpotent

Solution
(a) Recall that $n = rs, r, s$ coprime, $\mathbb{Z}_n \cong \mathbb{Z}_r \times \mathbb{Z}_s \implies \mathbb{Z}_{2022} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times Z_{337}$. If we want an element $g^n \in \mathbb{Z}_{2022}$ to be 0, then all of entries in the the corresponding entries must also be 0 when raised to n. Because all of the rings in this example have prime order, and $g^n = 0n > 0 \implies g$ is not a unit, the only possible nilpotent is $(0, 0, 0)$, or $0 \in \mathbb{Z}_{2022}$.

(b) $\mathbb{Z}_4$ has two nilpotents: 0 and 2. 1 and 3 have powers that cycle through 1, and 1 and 3 respectively.

(c) Let $x^n = 0$ and $y^m = 0$. Assume without loss of generality that $n \geq m$. Notice that if $a^b = 0 \in \mathbb{Z}_k$, then any greater power will also be 0, since $\gcd(a^b, k) = k$. Therefore, taking $(x + y)^{m+n}$, and expanding with binomial theorem (*it is important that the ring is commutative to allow the terms to be rearranged so that it's power of x times power of y, or else this doesn't necessarily work*):

$$\sum_{k \geq 0} \binom{n}{k} x^{m+n-k} y^k$$

When $k \leq m$, $m + n - k \geq n \implies x^{m+n-k} = 0$, and $k > m \implies y^k = 0$, s0 all terms in the summation are $0 \in \mathbb{Z}_k$. Therefore the evaluated summation of $(x + y)^{m+n} = 0 \in \mathbb{Z}_k$, and $x + y$ is also nilpotent

Problem 8: Find all solutions of the equation $x^2 + 2x + 2 = 0$ in a given ring R

(a) $R = \mathbb{Z}_5$

(b) $R = \mathbb{Z}_7$

(c) $R = \mathbb{Z}_8$

Solution
(a) $x = 1 \implies 1 + 2 + 2 = 5 = 0 \in \mathbb{Z}_5$, and $x = 2 \implies 4 + 4 + 2 = 10 = 0 \in \mathbb{Z}_5$. (there cannot be more by Lagrange's Theorem for polynomials, or you can brute force check it)

(b) No solutions. I couldn't think of a convincing argument that is less work than just checking all of them manually:
$0^2 + 2(0) + 2 = 2$
$1^2 + 2(1) + 2 = 5$
$2^2 + 2(2) + 2 = 3$
$3^2 + 2(3) + 2 = 3$
$4^2 + 2(4) + 2 = 5$
$5^2 + 2(5) + 2 = 2$
$6^2 + 2(6) + 2 = 1$

(c) No solutions. If $x = 2n$ even, $4n^2 + 4n \equiv 6 \pmod 8$ can be reduced to $2n^2 + 2n \equiv 3 \pmod 4$. The equivalent Diophantine equation cannot be solved, because the left side will always be a multiple of 2, and therefore cannot be 3.

If $x = 2n + 1$ odd, $4n^2 + 8n + 5 \equiv 4n^2 + 5 \equiv 0 \pmod 8 \implies 4n^2 \equiv 3 \pmod 8$, which again is unsolvable since 3 is not a multiple of 2.

Problem 9: Show that the characteristic of an integral domain is either 0 or a prime number p

Solution

If $1 = 0$ in the integral domain, the characteristic is 0. Else, assume that an integral domain R has characteristic $n = ab$, where $a, b \neq 1$. Then $1 + 1 + \cdots + 1 = 0$ additions can be broken up into a different disjoint sets of b additions. This is equivalent to $a(1 + 1 + \cdots + 1) = 0$, with b additions. This produces producing a zero division of two elements of R (if they aren't elements of R we have closure problems), contradicting R being an integral domain. Therefore, n must not be factorable (and must be a prime p)

Problem 10: For each of the following rings R decide (with proof) whether R is a field and whether R is an integral domain:

(a) $R = \mathbb{Z}_{2021}$

(b) $R = \{\text{even integers}\}$

(c) $R = \{\text{polynomials with } x \text{ with coeffiecients in } \mathbb{R}\}$ ($\mathbb{R}[X]$)

(d) $R = \mathbb{C}$

Solution

Note that we are told all four examples are rings, so I'll just skip verifying that they are rings in each proof.

(a) Neither. 43 does not have a multiplicative inverse since $\gcd(43, 2021) > 1$ (and therefore we can't solve their linear Diophantine equation for 1), so $\mathbb{Z}_{2021}$ cannot be a field. $43 \cdot 47 = 0 \in \mathbb{Z}_{2021}$, so $\mathbb{Z}_{2021}$ has zero division, and therefore cannot be an integral domain.

(b) Not a field since there are no multiplicative inverses in $2\mathbb{Z}$. However, for $x \in 2\mathbb{Z}^{\neq 0}$, there does not exist a $y \in 2\mathbb{Z}^{\neq 0}$ such that $xy = 0$ by the definition of non-zero integer multiplication, therefore $2\mathbb{Z}$ is an integral domain.

(c) R is not a field because taking a polynomial with degree $n > 1$ and zero constant coefficient, and attempt to invert the polynomial at $x = 0$ will result in $0 = 1$, therefore not all non-zero polynomials with real coefficints are units, and R cannot be a field. R is an integral domain because evaluating an element of R at some x such that the result is not 0 will give a unit real number (since $\mathbb{R}$ is a field), meaning the product of two non-zero unit polynomials results in a non-zero real.

(d) $\mathbb{C}$ is a field. Multiplication of complex numbers is commutative because multiplication of reals (modulus dilation) and addition of reals (argument addition) are commutative. For a complex number $z = re^{i\theta}$ with $r > 0$, z can be inverted by multiplying by $z^{-1} = r^{-1}e^{-i\theta}$ to get $zz^{-1} = rr^{-1}e^{i(\theta-\theta)} = 1$. The constaint on r is necessary since 0 is not invertible in the reals. Because $\mathbb{C}$ is a field, it is also an integral domain