HOMEWORK 7, DUE THU MAR 25TH

All solutions should be with proofs, you may quote from the book or from previous home works

(1) Let R, S be rings.

(a) Show that $A = R \times S$ is a ring with co-ordinate wise addition and multiplication. That is, $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b)(c, d) = (ac, bd)$. Show that the map $R \to R \times S$, given by $a \mapsto (a, 0)$ is a ring homomorphism. (Similarly for $S \to R \times S$. The construction can be done more generally, for a collection of rings. If R_i for $i \in I$, an indexing set, is a collection of rings, we can take $\prod R_i$ and give it as above a ring structure.)

Solution. This is an easy checking. □

(b) If R is a commutative ring with identity and $e \in R$ is an idempotent (that means $e^2 = e$), show that $1 - e$ is also an idempotent. Show that, $Re, R(1 - e)$ are subrings of R and $R = Re \times R(1 - e)$ as rings.

Solution. We just calculate, $(1 - e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$.
We check Re is closed under addition and multiplication. If, $ae, be \in Re$, with $a, b \in R$, we get $ae + be = (a + b)e$ and similarly, $(ae)(be) = abe^2 = abe$. Similarly for $R(1 - e)$. Finally, we have a map $f : R \to Re \times R(1 - e)$, $f(a) = (ae, a(1 - e))$. We show that this is a ring isomorphism, which is just easy checking. $f(a + b) = ((a + b)e, (a + b)(1 - e)) = (ae, a(1 - e)) + (b, b(1 - e)) = f(a) + f(b)$, $f(ab) = (abe, ab(1 - e)) = (ae, a(1 - e))(be, b(1 - e)) = f(a)f(b)$.
Finally, we check that this map is one-to-one and onto. If $f(a) = 0$, then $ae = a(1 - e) = 0$ and then, $0 = ae + a(1 - e) = a$. Similarly, if $(xe, y(1 - e)) \in Re \times R(1 - e)$, take $a = xe + y(1 - e) \in R$ and then, $f(a) = (ae, a(1 - e)) = ((xe + y(1 - e))e, (xe + y(1 - e))(1 - e)) = (xe^2, y(1 - e)^2) = (xe, y(1 - e))$. □

(c) Find all non-trivial idempotents (since $0, 1$ are always idempotents, we want to find others if any) in the rings $\mathbb{Z}/25\mathbb{Z}, \mathbb{Z}/15\mathbb{Z}$.
For $\mathbb{Z}/25\mathbb{Z}$, if class $x \in \mathbb{Z}$ is an idempotent, then $x^2 - x = x(x-1)$ must be divisible by 25. So, either 25 divides x, or it divides $x-1$ or 5 divides x and 5 divides $x - 1$. But, the last possibility is impossible, since 5 can not divide both x and $x-1$. If 25 divides x, then class of x is zero and if 25 divides $x-1$, class of x is just 1. So, there are no non-trivial idempotents in $\mathbb{Z}/25\mathbb{Z}$.
For, $\mathbb{Z}/15\mathbb{Z}$, I will leave you to check that the classes of $6, 10 \equiv (1-6)$ are the only non-trivial idempotents.

(2) Let k be a field and V a vector space (possibly infinite dimensional) over k.
(a) Show that $E = \{f : V \to V | f,\ k-\text{linear}\}$ is a ring with addition and multiplication defined as follows. $(f+g)(v) = f(v) + g(v)$ and $fg(v) = f(g(v))$. (If V is finite dimensional, you must recognize this as ring of square matrices, once we choose a basis).

Solution. This is just a straight forward verification. □

(b) Take $V = k[X]$, polynomial ring in one variable. Show that we can identify X as an element of V, multiplication on V by X. Similarly $D = \frac{d}{dX}$, the derivative is an element of E. Show that $DX - XD = 1$, where 1 stands for the identity function.

Solution. We calculate $DX - XD$ on a polynomial $P(X) \in V$.

$$\begin{aligned}(DX - XD)(P(X)) &= D(XP(X)) - X(D(P(X))) \\ &= XP'(X) + P(X) - XP'(X) \\ &= P(X)\end{aligned}$$

□

(3) Let R be any *commutative* ring with identity. A map $D : R \to R$ is called a *derivation* if $D(a+b) = D(a) + D(b)$ and $D(ab) = aD(b) + bD(a)$. (This is called the Leibniz' rule or product rule in Calculus, if you remember).
(a) Show that $D(1) = 0$.

Solution. $D(1) = D(1 \cdot 1) = 1D(1) + 1D(1) = D(1) + D(1)$ and then $D(1) = 0$. ☐

(b) Let $A = \{a \in R | D(a) = 0\}$ (often called the kernel of D). Show that A is a subring of R.

Solution. If $a, b \in A$, then $D(a+b) = D(a) + D(b) = 0$ and similarly, $D(ab) = aD(b) + bD(a) = a \cdot 0 + b \cdot 0 = 0$. Thus, both $a + b, ab \in A$. ☐

(c) Assume that $\mathbb{Q}$, the field of rational numbers, is a subring of R. Then, show that $D(q) = 0$ for all $q \in \mathbb{Q}$.

Solution. It is immediate that $D(0) = 0$ and if n is a positive integer, write $n = 1 + \cdots + 1$ and then, $D(n) = D(1) + \cdots + D(1) = 0$. Notice that the same argument says $D(na) = nD(a)$ for any $a \in R$. If $n < 0$, $D(n) = -D(-n) = 0$. Finally, if $r = p/q \in \mathbb{Q}$, with p, q integers and $q > 0$, then we have, $0 = D(p) = D(q \cdot p/q) = qD(r)$ and then, $D(r) = \frac{1}{q}0 = 0$. ☐

(d) Assume further, that for any element $a \in R$ there is an n, positive integer such that $D^n(a) = 0$ (D^n as usual is the short form for composition of D with itself n times) and that there is an $x \in R$ with $D(x) = 1$. Show that $R = A[x]$. That is, any element in R is just a polynomial in x with coefficients from A.

Solution. Let me start with an easy remark. For any non-negative integer n and $b \in A$, one easily checks that $D^n(bx^n) = bD^n(x^n) = bn!$.
If $D(a) = 0$, then $a \in A$ by definition of A. So assume that we have shown by induction that if $D^n(a) = 0$ for some fixed n, then $a \in A[x]$. Since we know this for $n = 1$, we have the initial case for induction. Now, let $a \in R$ be such that $D^{n+1}(a) = 0$. If $D^n(a) = 0$, we will be done by induction, so assume $D^n(a) = b \neq 0$. Notice that $D(b) = D^{n+1}(a) = 0$ and thus $b \in A$. Then, consider $a' = a - \frac{bx^n}{n!}$. An easy calculation shows $D^n(a') = 0$ and thus $a' \in A[x]$, but then $a = a' + \frac{bx^n}{n!} \in A[x]$. ☐

(4) Consider $R = M_2(\mathbb{R})$, the $n \times n$ matrices. We have seen that it is a (non-commutative) ring with the usual matrix addition and multiplication. So, we can multiply a matrix $A \in R$ with a vector $\mathbf{v} \in \mathbb{R}^2 = V$ as usual. (The results below are true for any $M_n(K)$, where K is any field and n is any positive integer, but the ideas can already be seen in the case $n = 2$.)

(a) Let $\mathbf{0} \neq \mathbf{v} \in V$ and let $I = \{A \in R | A\mathbf{v} = \mathbf{0}\}$. Show that I is a left ideal of R.

Solution. This is obvious, since if $A \in I$ and $M \in R$, $(MA)\mathbf{v} = M(A\mathbf{v}) = M\mathbf{0} = \mathbf{0}$. □

(b) Show that I is maximal. That is if $I \subset J \subset R$, where J is another left ideal, then $I = J$ or $J = R$.

Solution. Assume we had such a $J \neq I$. Then we will show that $J = R$. So, we have an $A \in J$ such that $A\mathbf{v} = \mathbf{v}' \neq \mathbf{0}$. Since there is always a linear transformation $M \in R$ such that $M\mathbf{v}' = \mathbf{v}$ (any non-zero vector can be mapped to any other non-zero vector), and since $MA \in J$, we have $(MA)\mathbf{v} = \mathbf{v}$. So, we may rename MA by A. Now, let $\mathbf{w}$ be another vector so that $\mathbf{v}.\mathbf{w}$ form a basis of V. We have $A\mathbf{v} = \mathbf{v}$. Consider $A\mathbf{w} = a\mathbf{v} + b\mathbf{w}$ for some $a, b \in \mathbb{R}$. If $b \neq 0$, then, the matrix corresponding of A with respect to the basis $\mathbf{v}, \mathbf{w}$ is of the form $\begin{bmatrix} 1 & a \\ 0 & b \end{bmatrix}$ and thus invertible. Then, $Id = A^{-1}A \in J$ and then $M \cdot Id = M \in J$ for any M and thus $J = R$.
Finally assume that $b = 0$ in the above expression. We have a matrix B such that $B\mathbf{v} = 0, B\mathbf{w} = \mathbf{w}$. Then $B \in I \subset J$. Now replace A with $A + B \in J$. Then, $(A + B)\mathbf{v} = \mathbf{v}$ and $(A + B)\mathbf{w} = a\mathbf{v} + \mathbf{w}$ and then by the previous argument, again we are done. □

(c) Show that R has no non-trivial two sided ideals.

Solution. Let $I \subset R$ be a non-zero (two-sided) ideal. We will show that $I = R$. Since $0 \neq I$, pick $0 \neq A \in I$. Then, there is a (non-zero) vector $\mathbf{v} \in V$ such that $A\mathbf{v} = \mathbf{v}' \neq 0$. We can find an $A' \in R$ such that $A'\mathbf{v}' = v$ and then $B = A'A \in I$ with $B\mathbf{v} = \mathbf{v}$. Similarly, extending $\mathbf{v}$ to a basis $\mathbf{v}, \mathbf{w}$, we look at $B\mathbf{w} = a\mathbf{v} + b\mathbf{w}$. If $b \neq 0$, as before, we see that B is invertible and then $I = R$. So, we may

assume $b = 0$. Replacing $\mathbf{w}$ with $\mathbf{w} - a\mathbf{v}$, then we can further assume $B\mathbf{w} = 0$.
Thus, we have a basis $\mathbf{v}, \mathbf{w}$ of V and a $B \in I$ with $B\mathbf{v} = \mathbf{v}, B\mathbf{w} = 0$. So, the matrix of B looks like, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.
Now, consider

$$C = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} B \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

One easily computes $C = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ and thus $Id = B + C \in I$ and then $I = R$.

□

(5) These are a few problems on homomorphisms.
  (a) Let $A \in M_n(K) = R$, K any field and consider the map $\phi : K[X] \to R$, given by, $\phi(P(X)) = P(A)$ (this means, if $P(X) = a_0 + a_1X + \cdots + a_rX^r$, $P(A) = a_0I + a_1A + \cdots + a_rA^r$). Show that this is a ring homomorphism. What is its kernel? (I am just asking for a word you might have learned in linear algebra).

  Solution. Checking this is a homomorphism of rings is just routine. The kernel is of the form $M(X)K[X]$, where $M(X) \in K[X]$, with $M(A) = 0$ and M is a monic polynomial of the least degree satisfying the equation $M(A) = 0$. $M(X)$ is called the *minimal polynomial* of A. □

  (b) We define new binary operations on R as above. The addition is the same, but a new multiplication is given by $A \star B = BA$. Show that $(R, +, \star)$ is a ring which we call R^{op}. Show that the map $R \to R^{op}$ given by $A \mapsto A^T$ is a ring homomorphism.

  Solution. This too is routine and if you have difficulties, talk to me. □