Homework Assignment 11 Solutions

1. Let R and S be rings and $\varphi : R \to S$ a ring homomorphism.

   (a) Show that $\operatorname{im}\varphi$ is a subring of S.

   Proof. We know from HW 3 Problem 2(b) that $\operatorname{im}\varphi$ is an additive subgroup of S. It remains to show that it is closed under products. Fix $x, y \in \operatorname{im}\varphi$, and write $x = \varphi(a)$ and $y = \varphi(b)$ for $a, b \in R$. Then since φ is a ring homomorphisms, we can directly verify that:

   $$xy = \varphi(a)\varphi(b) = \varphi(ab) \in \operatorname{im}\varphi.$$

   □

   (b) Show that $\ker\varphi$ is a (two-sided) ideal of R.

   Proof. We know from HW 3 Problem 2(a) that $\ker\varphi$ is an additive subgroup of S. It remains to show it is an ideal. We first point out a general fact that we will use from now on without mention: *the condition of being a (left or right) ideal is stronger than being closed under multiplication.* That is, if $I \subseteq R$ is an abelian subgroup and for all $r \in R$ and $i \in I$, $ri \in I$, then checking on $r \in I$ shows I is closed under multiplication (and similarly for right multiplication). In particular, from now on we will only check the ideal condition, since that will also imply that I is closed under multiplication (and therefore a subring).

   We therefore now show $\ker\varphi$ satisfies the ideal condition on both sides. Let $a \in \ker\varphi$ and $r \in R$. Then for any $r \in R$ we have:

   $$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0,$$

   $$\varphi(ar) = \varphi(a)\varphi(r) = 0 \cdot \varphi(r) = 0.$$

   Therefore $ra, ar \in \ker\varphi$ and so φ is a two-sided ideal. □

   (c) Suppose $J \subseteq S$ is an ideal. Show that $\varphi^{-1}(J)$ is an ideal of R.

   Proof. We must have shown at some point that the preimage of a subgroup is a subgroup, but I can't find it in my notes so I will prove it here. Fix $a, b \in \varphi^{-1}(J)$. Then $\varphi(a-b) = \varphi(a) - \varphi(b) \in J$ so that by the subgroup criterion (HW4 1a) J is a subgroup. Also notice that since $\varphi(a) \in J$,

   $$\varphi(ra) = \varphi(r)\varphi(a) \in J,$$

   $$\varphi(ar) = \varphi(a)\varphi(r) \in J.$$

   Therefore $ar, ra \in \varphi^{-1}(J)$ and so it is an ideal. (Observe that this proof shows the preimage of a left (resp. right) ideal is a left (resp. right) ideal). □

   (d) Suppose R and S are unital rings with *nonzero* identities 1_R and 1_S respectively. Prove that if $\varphi(1_R) \neq 1_S$ then $\varphi(1_R)$ is either zero, or a zero divisor in S.

Proof. Notice that

$$1_S \cdot \varphi(1_R) = \varphi(1_R) = \varphi(1_R \cdot 1_R) = \varphi(1_R)\varphi(1_R).$$

If $\varphi(1_R)$ is not a zero divisor or 0, then we can cancel it on the right on both sides, and deduce that $1_S = \varphi(1_R)$. □

(e) Deduce that if S is an integral domain and φ is nonzero then $\varphi(1_R) = 1_S$. (*Remark:* many authors require rings to be unital, and also require ring homomorphisms to take the identity to the identity.)

Proof. If $\varphi(1_R) = 0$ then $\varphi(r) = \varphi(r \cdot 1_R) = \varphi(r)\varphi(1_R) = 0$, so φ is the zero map. Therefore $\varphi(1_R)$ is nonzero, and it is not a zero divisor (since S has none). By part (d) it must be 1_S. □

2. In this exercise we prove the third and fourth isomorphism theorems for rings.

(a) We start with the fourth isomorphism theorem. Let R be a ring and $I \subseteq R$ an ideal. In particular (since R is abelian), I is a normal subgroup. Therefore, applying the fourth isomorphism theorem for groups (HW5 Problem 1), there is a bijection:

$$\left\{ \begin{array}{c} \text{Subgroups } A \leq R \\ \text{such that } I \leq A \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{c} \text{Subgroups} \\ \overline{A} \leq R/I \end{array} \right\}$$

Prove the following ring theoretic enhancements hold:

Proof. Before continuing, we review the notation of HW5 Problem 1 (which we don't need to reprove). If $\pi : R \to R/I$ is the projection, then the map in the right direction is $A \mapsto \pi(A) =: \pi(A)$, and the map in the left direction is $\overline{A} \mapsto \pi^{-1}(\overline{A}) =: A$. We already know by HW5 Problem 1 that this gives a bijection on the level of groups. We will also denote $\overline{x} = \pi(x)$ for $x \in R$. We record the following easy lemma.

Lemma 1. *Let $x \in R$ correspond to $\overline{x} \in R/I$. $x \in A$ if and only if $\overline{x} \in \overline{A}$.*

Proof. This is immediate from the definitions: the forward direction holds because $\overline{A} = \pi(A)$. The backward direction holds becasue $A = \pi^{-1}(A)$. □

□

i. A is a subring of R if and only if $\overline{A}$ is a subring of R/I.

Proof. Due to HW5 Problem 1, it only remains to check that A is closed under multiplication if and only if $\overline{A}$ is. Fix $x, y \in A$ corresponding to $\overline{x}, \overline{y} \in \overline{A}$. We must show $xy \in A$ if and only if $\overline{xy} \in \overline{A}$. But since $\overline{xy} = \overline{xy}$, this is just Lemma 1. □

ii. If A is a subring of R, then I is an ideal of A and that $A/I \cong \overline{A}$.

Proof. Restricting π to A gives a surjective ring map $\pi : A \to \overline{A}$ whise kernel is evidently I. The result then follows by the first isomorphism theorem. □

iii. A is a left ideal of R if and only if $\overline{A}$ is a left ideal of R/I.

Proof. Due to HW5 Problem 1, it only remains to show that A is closed under arbitrary multiplication on the left if and only if $\overline{A}$ is. Fix $r \in R$ and $a \in A$ corresponding to $\overline{r}, \overline{a}$ in R/I and $\overline{A}$. Then we must show $ra \in A$ if and only if $\overline{ra} \in \overline{A}$. But this is Lemma 1. □

iv. A is a right ideal of R if and only if $\overline{A}$ is a right ideal of R/I.

Proof. Due to HW5 Problem 1, it only remains to show that A is closed under arbitrary multiplication on the right if and only if $\overline{A}$ is. Fix $r \in R$ and $a \in A$ corresponding to $\overline{r}, \overline{a}$ in R/I and $\overline{A}$. Then we must show $ar \in A$ if and only if $\overline{ar} \in \overline{A}$. But this is Lemma 1. □

v. A is an ideal of R if and only if $\overline{A}$ is an ideal of R/I.

Proof. This follows immediately from iii and iv. □

(b) We now prove the third isomorphism theorem for rings. Let $J \subseteq I \subseteq R$, with J, I ideals of a ring R. By part (a) we know that I/J is an ideal of R/J. Prove that:

$$\frac{R/J}{I/J} \cong \frac{R}{I}.$$

Proof. We define a map $\varphi : R/J \to R/I$ by the rule $\varphi(r + J) = r + I$. By the third isomorphism theorem for groups (or rather, its proof, cf the February 18 Lecture), this is a well defined surjective group homomorphism with kernel I/J. Therefore, if φ commutes with multiplication it is a ring homomorphism we are done by the first isomorphism theorem. But this is easy to check directly:

$$\varphi((r + J)(s + J)) = \varphi(rs + J) = rs + I = (r + I)(s + I) = \varphi(r + J)\varphi(s + J).$$

□

(c) We finish with a ring theoretic analog of *passing to the quotient*. Suppose $\varphi : R \to S$ is a ring map, and suppose that $I \subseteq \ker \varphi$. Prove that there is a unique map $\overline{\varphi} : R/I \to S$ such that the following diagram commutes:

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi"] & S \\ R/I \arrow[ur, dotted, "\overline{\varphi}"'] & \end{tikzcd}$$

That is, $\overline{\varphi}$ is the unique map so that $\overline{\varphi} \circ \pi = \varphi$. (*Hint*: We already know from group theory that there is a unique such map on the level of group homomorphisms. What remains is to confirm that map is a ring homomorphism.)

Proof. From *passing to the quotient for groups* (cf. the February 23 lecture), we know that $\overline{\varphi}(r + I) = \varphi(r)$ is well defined, and is the unique additive group homomorphism making the diagram commute. Therefore it only remains to check that $\overline{\varphi}$ commutes with multiplication. But this is easy to check:

$$\overline{\varphi}((r + I)(s + I)) = \overline{\varphi}(rs + I) = \varphi(rs) = \varphi(r)\varphi(s) = \varphi(r + I)\varphi(s + I).$$

□

3. Let R be a ring.

   (a) Suppose $\{I_j\}$ is a collection of left ideals of R. Show that the intersection $\cap I_j$ is a left ideal of R.

   Proof. We know by HW4 Problem 2(d) that $\cap I_j$ is an additive subgroup. It remains to check the ideal condition. Fix $i \in \cap I_j$ and $r \in R$. For all j, we know $ri \in I_j$ since I_j is a left ideal, so ri is in the intersection. $\square$

   (b) Show that part (a) also holds for right ideals and two-sided ideals.

   Proof. We know by HW4 Problem 2(d) that $\cap I_j$ is an additive subgroup. It remains to check the ideal condition. Fix $i \in \cap I_j$ and $r \in R$. For all j, we know $ir \in I_j$ since I_j is a right ideal, so ir is in the intersection. Since a two-sided ideal is precisely something that is both a left and right ideal, the case for two-sided ideals follows immediately. $\square$

   (c) Let R be a ring with $1 \neq 0$. Show that:

$$RA = \bigcap_{A \subset I \text{ left ideal}} I.$$

   Proof. We first show $RA = \{r_1a_1 + \cdots + r_na_n | r_i \in R, a_i \in A\}$ is an ideal. To see it is an abelian subgroup we use the subgroup criterion (HW4 1a). Fix two elements $x = r_1a_1 + \cdots + a_na_n$ and $y = s_1b_1 + \cdots s_mb_m$ with $a_i, b_i \in A$. Then

$$x - y = r_1a_1 + \cdots + a_na_n + (-s_1)b_1 + \cdots + (-s_m)b_m \in RA.$$

   Now consider $r \in R$, then by the distributive law $rx = rr_1a_1 + \cdots + rr_na_n \in RA$. This proves RA is a left ideal.
   Denote the intersection of all left ideals containing A by $(A]$. Since $A \subseteq RA$, and RA is a left ideal, it is one of the elements in the intersection, so that $(A] \subseteq RA$. Conversely, consider x as in the previous paragraph. For any left ideal I containing A we see $a_i \in I$, so that $r_ia_i \in I$, so taking the sum over all i we see that $x \in I$. Since x was an arbitrary element of RA we have $RA \subseteq I$. Since this is true for all such I then taking intersections we ahve $RA \subseteq (A]$ as desired. $\square$

   (d) State the analog for part (c) for right ideals. (The proof will be identical, so I won't make you repeat yourself.)

   Proof. This would state that:

$$AR = \bigcap_{A \subset I \text{ right ideal}} I.$$

   $\square$

4. Let I and J be ideals of a ring R.

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

Proof. Let K be an ideal containing both I and J. Then any $i + j \in I + J$ is contained in K (since K is closed under addition), so that $I + J \subseteq K$, and therefore is smaller. Since K was arbitrary, $I + J$ must be the smallest. □

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

Proof. We first record that $I \cap J$ is an ideal by 3(b). We next show that IJ is an ideal. We first show it is a subgroup using the subgroup criterion. Consider arbitrary elements $x = i_1 j_i + \cdots + i_n j_n$ and $y = i'_1 j'_1 + \cdots + i'_m j'_n$ in IJ (where $i_k, i'_k \in I$ and $j_k j'_k \in J$). Then:

$$x - y = i_1 j_i + \cdots + i_n j_n + (-i'_1) j'_1 + \cdots + (-i'_m) j'_n \in IJ.$$

Next fix $r \in R$.

$$rx = r i_1 j_1 + \cdots + r i_n j_n,$$

$$xr = i_1 j_1 r + \cdots + i_n j_n x.$$

Since I is an ideal, $r i_k \in I$ for all k, so that $rx \in IJ$. Similarly, $j_k r \in J$ for all k so that $xr \in IJ$, and so IJ is indeed an ideal. Next we hope to show that $IJ \subseteq I \cap J$. Since $x \in IJ$ was arbitrary, we may show $x \in I \cap J$. But $i_k \in I$ and $j_k \in J$ implies that $i_k j_k \in I \cap J$. Since $I \cap J$ is closed under sums, we win. □

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

Proof. Let $R = \mathbb{Z}$ and $I = J = 2\mathbb{Z}$. Then $IJ = 4\mathbb{Z}$ but $I \cap J = 2\mathbb{Z}$. □

(d) Suppose R is commutative and unital, and that $I + J = R$. Show $IJ = I \cap J$.

Proof. We must show that $I \cap J \subseteq IJ$. Fix $x \in I \cap J$. Since $I + J = R$, there is some $i \in I$ and $j \in J$ such that $i + j = 1$. Then $x(i + j) = ix + xj \in IJ$ completing the proof. □

5. Let R be a commutative ring with $1 \neq 0$.

(a) Fix $a \in R$. Show that $(a) = R$ if and only if $a \in R^\times$.

Proof. We showed in class that $(a) = \{ra : r \in R\}$. Suppose $(a) = R$. Then there is some $r \in R$ such that $ra = 1$. Since R is commutative this implies that $a \in R^\times$. Conversely, if $a \in R^\times$ then there is some $r \in R$ so that $ra = 1$. Thus $1 \in (a)$. Fix $f \in R$, then $f = f \cdot 1 \in (a)$. This shows $R \subseteq A$. □

(b) Fix $a, b \in R$, and suppose that a is not a zero divisor. Show that $(a) = (b)$ if and only if $a = ub$ for some unit $u \in R^\times$.

Proof. If $a = ub$ for some unit then $a \in (b)$ so that $(a) \subseteq (b)$. But also $b = u^{-1} a \in (a)$ so that $(b) \subseteq (a)$. Conversely, if $(a) = (b)$ then $a = xb$ and $b = ya$. We must show x is a unit. Substituting, $a = xya$. Since a is not a zero divisor we ma cancel so that $xy = 1$, and therefore x and y are units, completing the proof. □

(c) Let I be any ideal. Show that $I = R$ if and only if I contains a unit $u \in R^\times$.

Proof. If $I = R$ then $1 \in I$ so that I contains a unit. Conversely, suppose I contains a unit u. Then I contains $uu^{-1} = 1$, and so it contains $f = f \cdot 1$ for any $f \in R$. Thus $R \subseteq I$ as desired. □

(d) Prove that R is a field if and only if the only ideals in R are (0) and R itself.

Proof. Suppose R is a field. If I is a nonzero ideal then I contains a unit (as any nonzero element of a field is a unit), so that $I = R$ by part (c). Conversely, suppose the only ideals of R are (0) and R, and consider any nonzero $a \in R$. (a) is nonzero so it must be all of R. Thus $a \in R^\times$ by part (a). Therefore every nonzero element of R is a unit, but that's what it means to be a field. □

(e) Now suppose S is a (not necessarily commutative) ring with $1 \neq 0$. Show that S is a division ring if and only if the only all left, right, and 2-sided ideals are one of S or (0). (*Hint*: Start by proving a version of part (c) for noncommutative rings.)

Proof. We first establish (c) for noncommutative rings: if I is a left (resp. right) ideal of S then $I = S$ if and only if I contains a unit. Indeed, if $I = S$ then $1 \in I$. Conversely, let $u \in I$ be a unit. Then $1 = u^{-1}u \in I$ (resp. $1 = uu^{-1} \in I$). Thus for any $f \in S$, $f = f \cdot 1 \in I$ (res. $f = 1 \cdot f \in I$), and so $R \subseteq I$.

Now suppose S is a division ring. Then if I is a nonzero left (or right) ideal, it contains a unit so $I = S$. Conversely, consider $a \in R$ nonzero. Then $Ra = R$ so that Ra contains a 1. In particular, there is some $r \in R$ such that $ra = 1$. Similarly, $aR = R$ so that aR contains 1, and so there is a $s \in R$ such that $as = 1$. We conclude by showing $r = s = a^{-1}$. Indeed:

$$r = r(1) = r(as) = ras = (ra)s = (1)s = s.$$

□

6. Let R be any ring. We define the *n by n matrix ring* of R: $M_n(R)$, to be the set of n by n matrices whose entries are elements of R. We often denote an element of M as a n^2-tuple of entries indexed by i and j between 1 and n:

$$M = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = (a_{ij}).$$

We make $M_n(R)$ into a ring under usual matrix multiplication and addition. That is, given $M = (a_{ij})$ and $N = (b_{ij})$ then $M + N = (a_{ij} + b_{ij})$, and the ijth entry of MN is $\sum_{k=1}^n a_{ik}b_{kj}$.

(a) Prove that $M_n(R)$ is a ring.

Proof. We first show that $M_n(R)$ is an abelian group under addition. Indeed, the abelian group structure is just n^2 coordinates of the abelian group structure of R, indexed by ij for pairs i and j between 1 and n. We next show the distributive law. Let

$M = (m_{ij})_{ij}, N = (n_{ij})_{ij}, L = (l_{ij})_{ij}$. Then we show $M(N+L) = MN + ML$ by considering the ijth entry:

$$\begin{aligned}
((m_{ij}))((n_{ij}) + (l_{ij})) &= (m_{ij})(n_{ij} + l_{ij}) \\
&= \left(\sum_{k=1}^{n} m_{ik}(n_{kj} + l_{kj})\right) \\
&= \left(\sum_{k=1}^{n} m_{ik}n_{kj} + m_{ik}l_{kj}\right) \\
&= \left(\sum_{k=1}^{n} m_{ik}n_{kj}\right) + \left(\sum_{k=1}^{n} + m_{ik}l_{kj}\right) \\
&= (m_{ij})(n_{ij}) + (m_{ij})(l_{ij}).
\end{aligned}$$

The distributive law on the right is completely symmetric. Finally we show associativity of multiplication....yikes. Again we consider the ijth entry:

$$\begin{aligned}
((m_{ij})(n_{ij}))(l_{ij}) &= \left(\sum_{k=1}^{n} m_{ik}n_{kj}\right)(l_{ij}) \\
&= \left(\sum_{r=1}^{n}\left(\sum_{k=1}^{n} m_{ik}n_{kr}\right) l_{rj}\right) \\
&= \left(\sum_{r=1}^{n}\sum_{k=1}^{n} m_{ik}n_{kr}l_{rj}\right) \\
&= \left(\sum_{k=1}^{n}\sum_{r=1}^{n} m_{ik}n_{kr}l_{rj}\right) \\
&= \left(\sum_{k=1}^{n} m_{ik}\left(\sum_{r=1}^{n} n_{kr}l_{rj}\right)\right) \\
&= (m_{ij})\left(\sum_{r=1}^{n} n_{ir}l_{rj}\right) \\
&= (m_{ij})((n_{ij})(l_{ij}))
\end{aligned}$$

□

(b) Suppose R is a ring with $1 \neq 0$, and that $n \geq 2$. Show that $M_n(R)$ always has a left ideal that is not a right ideal, and vice versa.

Proof. Let

$$L = \left\{ \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & 0 & \cdots & 0 \end{pmatrix} \text{ such that } a_i \in R \right\}$$

Then L is evidently an additive subgroup of $M_n(R)$ (it is n factors of the n^2 direct product of R). Suppose I multiply on the left by (b_ij). The ij entry will be $\sum b_{ik}a_{kj}$.

In particular, if $j \neq 1$ then $a_{kj} = 0$ so the sum will be 0. Thus the resulting matrix is concentrated in the first column and so $(b_ij)(a_ij) \in L$. On the other hand, we compute that:

$$\begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & a_{11} \\ 0 & 0 & \cdots & a_{21} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n1} \end{pmatrix}.$$

In particular, if any of the a_{i1} are nonzero, this will not lie in L. Next consider

$$R = \left\{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \text{ such that } a_i \in R \right\}$$

Arguing symmetrically, we see that R is an additive subgroup, and if we multiply on the right by b_{ij} we have an ijth entry $\sum a_{ik} b_{kj}$ which will be 0 unless $i = 1$ so that R is a right ideal. But it is not a left ideal since

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{11} & a_{12} & \cdots & a_{1n} \end{pmatrix}.$$

□

(c) Let I be a left (respectively right) ideal of R. Show that $M_n(I)$ is a left (respectively right) ideal of $M_n(R)$.

Proof. That $M_n(I)$ is an additive subgroup can be checked coordinatewise. Then $M_n(I)$ is closed under subtraction in each coordinate since I is closed under subtraction in R. To see the ideal structure, fix $M = (m_{ij}) \in M_n(I)$ and an arbitary matrix $A = (a_{ij})$. The ijth entry of AM is $\sum a_{ik} m_{kj}$, so if I is a left ideal, each element of the sum is in I so the sum is and $AM \in M_n(I)$ and we win. Symmetrically, the ijth entry of MA is $\sum m_{ik} a_{kj}$ so that if I is a right ideal each element of the sum is in I so their sum is and $MA \in M_n(I)$ and we win. □

(d) Suppose R is unital. Show that the 2-sided ideals of $M_n(R)$ are precisely $M_n(J)$ for two sided ideals $J \subseteq R$. (*Hint*: Think about mutliplication by the matrices E_{ij} which have a 1 in the ij entry and are are 0 everywhere else).

Proof. If J is a two-sided ideal of R then we know that $M_n(J)$ is a two-sided ideal of $M_n(R)$ by part (c). Conversely, we must study an general two-sided ideal $\mathcal{J} \subseteq M_n(R)$. We record the following fact, which is proved by a direct computation of matrix multiplication.

Lemma 2. *Let $M = (m_{ij})$, and E_{ij} the matrix with 0's in every entry except the ij'th entry. Then:*

$$E_{ij}M = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ m_{j1} & m_{j2} & \cdots & m_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

where the nontrivial row is the ith row.

$$ME_{ij} = \begin{pmatrix} 0 & \cdots & m_{i1} & \cdots & 0 \\ 0 & \cdots & m_{i2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & m_{in} & \cdots & 0 \end{pmatrix}$$

where the nontrivial column is the jth one. In particular, $E_{ij}ME_{kr}$ is the matrix with zero's everwhere except m_{jk} in the irth entry.

With this tool, we prove the desired result. Let $\mathcal{J} \subseteq M_n(R)$ be a two-sided ideal. Define a subset $J \subseteq R$ to be the set of elements of R that appear as *any* entry in *any* matrix in $\mathcal{J}$. In particular, if $M = (m_{ij}) \in \mathcal{J}$, then $m_{ij} \in J$ for each i, j. Notice that essentially by definition, $\mathcal{J} \subseteq M_n(J)$. We now show the reverse inclusion. Fix $X = (x_{ij})$ in $M_n(J)$. Let X_{ij} be the matrix which is 0 everywhere and x_{ij} in the ijth position. If each $X_{ij} \in \mathcal{J}$, then because $\mathcal{J}$ is closed under addition, their sum is so that $X \in \mathcal{J}$. Therefore to prove the reverse inclusion, it suffices to show that $X_{ij} \in \mathcal{J}$. Since $x_{ij} \in J$, there is some $M \in \mathcal{J}$ with some entry equal to x_{ij}, say it's the pqth entry of M. Then by the lemma, $E_{ip}ME_{qj} = X_{ij}$, and so we win!

It remains to show that J is an ideal of R (at this point it is only a random subset). To do this we identify that the entire ring structure of R is contained in matrices of the form:

$$[r] = \begin{pmatrix} r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

(Here we are introducing the notation that $[r]$ denotes the matrix with r in the 11 entry and 0 everywhere else). Indeed, one can easily check that $[r]+[s] = [r+s]$ and $[r][s] = [rs]$. We first show J is an abelian subgroup of R. Fix $x, y \in J$. Then $[x], [y] \in M_n(J) = \mathcal{J}$, so that $[x] - [y] = [x - y] \in \mathcal{J}$. Since $x - y$ is an element in an entry of a matrix in $\mathcal{J}$, we may conclude that $x - y \in J$. Similarly, let $r \in R$ be any matrix. Then $[r][x] = [rx] \in \mathcal{J}$ (since $\mathcal{J}$ is an ideal), so that arguing as in the previous sentence, $rx \in J$. Therefore J is an ideal of R, completing the proof. $\square$

(e) The determinant $\det : M_n(R) \to R$ is a function. Is it always a ring homomorphism? If yes, prove it. If no, give a counterexample.

Proof. The determinant is not a ring homomorphism. It is multiplicative, but not additive. For example, letting $R = \mathbb{R}$. Then

$$\det\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \begin{pmatrix}-1 & 0\\ 0 & 0\end{pmatrix}\right) = \det\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} = 0,$$

but

$$\det\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \det\begin{pmatrix}-1 & 0\\ 0 & 0\end{pmatrix} = 1 + 0 = 1.$$

□

7. Recall that a group was called *simple* if it had no normal subgroups, or equivalently, if it has no nontrivial quotients. There is a similar notion for rings. A ring R is called *simple* if the only quotients of R are R itself and the the zero ring.

   (a) Give an equivalent formulation of simplicity in terms of ideals.

   Proof. A ring R is simple if and only if the only two sided ideals of R are the 0 ideal and R itself. This is because two-sided ideals of R are in one-to-one correspondance with quotients of R (the correspondance is $I \leftrightarrow R/I$). □

   (b) Show that a commutative unital ring is simple if and only if it is a field.

   Proof. By part (a), R is simple if and only if the only ideals of R are (0) and R, which by 5(d) is true if and only if R is a field. □

   (c) Give an example to show that a noncommutative ring may be simple even but not a division ring.

   Proof. Let F be a field and consider the matrix ring $M_n(F)$ for any $n \geq 2$. Since it has a nontrivial left ideal (by 6(c)), it is not a division ring (by 5(e)). On the other hand, if $\mathcal{J} \subseteq M_n(F)$ is a two-sided ideal, 6(d) tells us that $\mathcal{J} = M_n(J)$ for a two-sided ideal of F. But since F is a field, $J = 0$ or F, so that $\mathcal{J} = M_n(0) = 0$ or $\mathcal{J} = M_n(F)$. Therefore $M_n(F)$ has non nontrivial two-sided ideals and thus by part (a) it is simple. □

8. Let R be a ring. The *nilradical* of R is $\mathfrak{N}(R) = \{r \in R : r \text{ is nilpotent}\}$. By HW10 Problem 3 we know that $\mathfrak{N}(R)$ is an ideal of R.

   (a) Show that $R/\mathfrak{N}(R)$ is reduced. This is often called the *reduction of R*, and is denoted R_{red}.

   Proof. Let $r+\mathfrak{N}(R)$ be a nilpotent element of $R/\mathfrak{N}(R)$. Then $(r+\mathfrak{N}(R))^n = r^n+\mathfrak{N}(R) = 0$, or equivalently $r^n \in \mathfrak{N}(R)$. This means r^n is nilpotent in R, so that $0 = (r^n)^m = r^{nm}$. But this says that r was nilpotent to begin with, i.e., that $r \in \mathfrak{N}(R)$. In particular $r + \mathfrak{N}(R) = 0$ in $R/\mathfrak{N}(R)$ and so the only nilpotent element of the quotient is the zero element, but that's what it means to be reduced. □

   (b) Let $\varphi : R \to S$ be any ring homomorphism. Show that $\varphi(\mathfrak{N}(R)) \subseteq \mathfrak{N}(S)$. Deduce that if S is reduced then $\mathfrak{N}(R)$ is contained in the kernel of φ.

Proof. Let $r \in \mathfrak{N}(R)$, so that $r^n = 0$. Then $\varphi(r)^n = \varphi(r^n) = \varphi(0) = 0$, so that $\varphi(r)$ is nilpotent as well. This proves the first part. For the second, we notice that if S is reduced then $\mathfrak{N}(S) = \{0\}$. Therefore $\varphi(\mathfrak{N}(R)) = \{0\}$, which means that $\mathfrak{N}(R)$ is contained in the kernel of φ. $\square$

(c) Let S be a reduced ring. Show that there is a bijection:

$$\{\text{Ring homomorphisms } \varphi : R \to S\} \Longleftrightarrow \{\text{ Ring homomorphisms } \tilde{\varphi} : R_{red} \to S\}.$$

Hint: Use passing to the quotient! *Remark:* This should feel reminicient of the *abelianization* from HW6 Problem 4. In fact, both are examples of something more general, called a *universal property.* Keep your eyes open for things like this, they appear all over mathematics!

Proof. We denote the projection map $R \to R_{red}$ by π. We first describe a map $\varphi \mapsto \tilde{\varphi}$ in the right-hand direction. Given a homomorhpism $\varphi : R \to S$, we observe that by part (b), $\mathfrak{N}(R) \subseteq \ker \varphi$. Therefore by 2(c) there is a unique map $\tilde{\varphi} : R/\mathfrak{N}(R) \to S$ such that $\tilde{\varphi} \circ \pi = \varphi$. Since $R/\mathfrak{N}(R) = R_{red}$, $\tilde{\varphi}$ is an object on the right. In the other direction, fix some $\tilde{\varphi} : R_{red} \to S$. Then we define φ to be the composition

$$\begin{tikzcd} R \arrow[r, "\pi"] \arrow[rr, bend left, "\varphi"] & R_{red} \arrow[r, "\tilde{\varphi}"] & S. \end{tikzcd}$$

These constructions are evidently inverses to eachother. Indeed, starting on the left we have $\varphi \mapsto \tilde{\varphi} \mapsto \tilde{\varphi} \circ \pi$ but the latter is φ so these compose to the identity. Conversely, we consider $\tilde{\varphi} \mapsto \tilde{\varphi} \circ \pi \mapsto \widetilde{\tilde{\varphi} \circ \pi}$. The latter must be $\tilde{\varphi}$ since when we precompose either map with π we recover φ, and there only one map with this property (by 2(c)). $\square$