Math 566 - Homework 3

SOLUTIONS

Prof Arturo Magidin

1. Let R and S be rings, and let $f\colon R \to S$ be a ring homomorphism. Prove that if Q is a completely prime ideal of S that does not contain $f(R)$, then $f^{-1}(Q)$ is a completely prime ideal of R that contains $\ker(f)$.

   Proof. Since Q is an ideal of S, $f^{-1}(Q)$ is both an additive subgroup (inverse image of a subgroup is a subgroup), and a multiplicative subsemigroup (inverse image of a subsemigroup is a subsemigroup). To verify it is an ideal, let $x \in f^{-1}(Q)$ and $r \in R$, Then $f(x) \in Q$, and $f(rx) = f(r)f(x) \in Q$, since Q is an ideal; therefore, $rx \in f^{-1}(Q)$. Similarly for $xr \in Q$. So $f^{-1}(Q)$ is an ideal. Since Q does not contain $f(R)$, then $f^{-1}(Q) \neq R$.

   Let $a, b \in R$ be such that $ab \in f^{-1}(Q)$. We want to show that either $a \in f^{-1}(Q)$ or $b \in f^{-1}(Q)$. We have $f(a)f(b) = f(ab) \in Q$; since Q is completely prime in S, this means that $f(a) \in Q$ or $f(b) \in Q$. And in turn this implies that either $a \in f^{-1}(Q)$ or $b \in f^{-1}(Q)$. This proves that $f^{-1}(Q)$ is a completely prime ideal of R.

2. Let R_1, $R_2, \ldots, R_n$ be rings with unity, and let I be an ideal of $R_1 \times \cdots \times R_n$. Prove that there exist ideals $J_i \triangleleft R_i$, $i = 1, \ldots, n$, such that $I = J_1 \times \cdots \times J_n$.

   NOTE: This result is not true for groups and normal subgroups. For example, if $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ is the Klein 4-group, then the subgroup $\{(0,0),(1,1)\}$ is a normal subgroup that is not of the form $M \times N$ with $M, N \triangleleft \mathbb{Z}_2$.

   Proof. Let I be an ideal of $R_1 \times \cdots \times R_n$, and let $J_k = \pi_k(I)$. This is the image of an ideal under a surjective homomorphism, hence J_k is certainly an ideal of R_k for each k.

   Since $\pi_k(I) = J_k$, it follows that $I \subseteq J_1 \times \cdots \times J_n$.

   To prove the reverse inclusion, first note that if $a \in J_k$, then there exists an element $(a_1, \ldots, a_n)$ in I with $a_k = a$. Multiplying by the element that has 1_{r_k} in the kth component and zeros elsewhere, we obtain an element of the form $(0, \ldots, 0, a_k, 0, \ldots) \in I$.

   Next, let $(a_1, \ldots, a_n) \in J_1 \times \cdots \times J_n$. For each k, let $\mathbf{m}_k \in I$ be the element that has a_k in the kth component and 0 elsewhere, constructed as above. Then,

   $$(a_1, \ldots, a_n) = \mathbf{m}_1 + \cdots + \mathbf{m}_n \in I,$$

   which proves that $J_1 \times \cdots \times J_n \subseteq I$, and yields the desired equality. □

3. Let R be a ring, not necessarily commutative, and let $n \geq 1$. Then $M_n(R)$, the group of $n \times n$ matrices with coefficients in R, is a ring with the usual matrix multiplication. (You may take this for granted). Let J be a two-sided ideal of R. Prove that $M_n(J)$ is an ideal of $M_n(R)$.

   Proof. If (a_{ij}), (b_{ij}), and (r_{ij}) are matrices, $r_{ij} \in R$, $a_{ij}, b_{ij} \in J$. Then $(a_{ij}) - (b_{ij}) = (a_{ij} - b_{ij})$ is in $M_n(J)$, so $M_n(J)$ is a subgroup of S.

   The (i,j)th entry of $(a_{ij})(r_{ij})$ is $a_{i1}r_{1j} + \cdots + a_{in}r_{nj}$. Each of $a_{ik}r_{kj}$ lies in J, because J is an ideal; hence their sum lies in J. Thus, every entry of $(a_{ij})(r_{ij})$ is an element of J, so the product lies in $M_n(J)$.

   Similarly, the (i,j)th entry of $(r_{ij})(a_{ij})$ is $r_{i1}a_{1j} + r_{i2}a_{2j} + \cdots + r_{in}a_{nj}$, which lies in J because each a_{kj} is in J. Thus, $(r_{ij})(a_{ij}) \in M_n(J)$. We have then shown that $M_n(J)$ is an ideal of S. □

4. Let R be a ring with unity, and let $S = M_n(R)$. Let J be a two-sided ideal of S. We will prove that $J = M_n(I)$ for some two-sided ideal I of R.

(i) Let E_{rs} be the matrix that has 1_R in the (r,s) entry and 0s elsewhere. Show that $E_{rs}A$ is the matrix that has the sth row of A in the rth row, and zeros elsewhere. Give a similar description of AE_{rs} and prove that description holds.

Proof. If the (i,j)th entry of E_{rs} is denoted by e_{ij}, then we have $e_{ij} = 0$ unless $i = r$ and $j = s$, in which case $e_{rs} = 1$. Thus, the (k,ℓ) entry of $E_{rs}A$ is

$$e_{k1}a_{1\ell} + \cdots + e_{kn}a_{n\ell} = \begin{cases} 0 & \text{if } k \neq r, \\ a_{s\ell} & \text{if } k = r. \end{cases}$$

Thus, every row is 0, except perhaps for the rth row; and that row is $(a_{s1}, \ldots, a_{sn})$, which is the sth row of A.

Next, proceeding as above, the (k,ℓ) entry of AE_{rs} is

$$a_{k1}e_{1\ell} + \cdots + a_{kn}e_{n\ell} = \begin{cases} 0 & \text{if } \ell \neq s, \\ a_{kr} & \text{if } \ell = s. \end{cases}.$$

Thus, the ℓth column is 0, except perhaps when $\ell = s$, in which case we get $(a_{1r}, \ldots, a_{nr})^t$, the rth column of A. That is, AE_{rs} has the rth column of A in the sth column, and 0s elsewhere. □

(ii) Let I be the subset of all elements of R that appear as an entry of some element of J. Show that I is an ideal of R.

Proof. The set I is nonempty, since the zero matrix lies in J and so $0 \in I$.

Let $a, b \in I$. Then there exists a matrix $M_a \in J$ that has a in some entry, say the (i,j)th entry. Multiplying on the left by E_{1i} and on the right by E_{j1}, we get the matrix $E_{1i}M_aE_{j1} \in J$. The matrix $E_{1i}M_a$ has the ith row of M_a in the first row and zeros elsewhere, and $(E_{1i}M_a)E_{j1}$ has the jth column of $E_{1i}M_a$ (which has a_{ij} in the top entry and zeros elsewhere) in the first column. that is, $E_{1i}M_aE_{j1}$ is a matrix that as $a_{ij} = a$ in the $(1,1)$ entry, and zeros elsewhere.

Similarly, there is a matrix $M_b \in J$ with b in some entry, say (r,s); then $E_{1r}M_bE_{s1} \in J$ has b in the $(1,1)$ entry, and zeros elsewhere.

Now, $(E_{1i}M_aE_{j1}) - (E_{1r}M_bE_{s1})$ is an element of J, which has $a - b$ in the $(1,1)$ entry; that means that $a - b \in I$. Thus, I is nonempty and closed under differences, so I is a subgroup of R.

If $r \in R$ and $M \in J$, then $(rI)M$ is obtained from M by multiplying every entry by r on the left; and $M(rI)$ is the matrix that is obtained from M by multiplying every entry by r on the right. They both lie in J, since J is an ideal and $M \in J$; hence if $a \in I$, then $ra, ar \in I$. Thus, I is a two-sided ideal, as claimed. □

(iii) Show that $a \in I$ if and only if there exists a matrix M in J such that a is the $(1,1)$ entry of M, and all other entries of M are 0.

Proof. We proved above, *inter alia* ("among other things") that if $a \in I$, and M_a is a matrix in J that has a in the (i,j)th entry, then $E_{1i}M_aE_{j1}$ has a in the $(1,1)$ entry and zeros elsewhere, and lies in J. The converse comes from the definition of I. □

(iv) Prove that $J = M_n(I)$.

Proof. Clearly $J \subseteq M_n(I)$, since every entry of a matrix in J lies in I by definition.

Conversely, let $M = (m_{ij}) \in M_n(I)$. Then for each (i,j), $m_{ij} \in I$, so from (iii) we know that there is a matrix $M_{m_{ij}} \in J$ that has m_{ij} in the $(1,1)$ coordinate. Then $A(i,j) = E_{i1}M_{m_{ij}}E_{1j}$ has m_{ij} in the (i,j)th coordinate, 0s elsewhere. and lies in J. Therefore,

$$M = A(1,1) + A(1,2) + \cdots + A(n,n) \in J,$$

proving that $M_n(I) \subseteq J$ and establishing the desired result. □

5. Show that if R is a division ring, $n \geq 1$, and $S = M_n(R)$, then the zero ideal of S is a prime ideal. Show that if $n > 1$, then the zero ideal is not completely prime.

   Proof. If R is a division ring, then the only ideals of R (two-sided or one-sided) are (0) and R itself: because if I is an ideal an $a \neq 0$, $a \in I$, then $1_R = aa^{-1} = a^{-1}a \in I$.

   From Problem 4 we conclude that the only ideals of S are the zero ideal, and $S = M_n(R)$. Thus, the only possible products of ideals are $(0)(0) = (0)$, $(0)S = (0)$, $S(0) = (0)$, and $SS = S$.

   Hence, if A and B are ideals of S such that $AB \subseteq (0)$, then either $A = (0)$ or $B = (0)$. This proves that (0) is a prime ideal of S. Alternatively, (0) is a maximal ideal of S, and since $S^2 = S$, it follows that (0) is a prime ideal.

   To show the ideal is not completely prime when $n > 1$, consider $E_{12}E_{12}$ (using the same notation as in Problem 4). The product is 0, the (i, j)th entry is $e_{i1}e_{1j} + \cdots + e_{in}e_{nj}$, and at least one of the factors in each summand is 0. Thus, the product is 0 and so lies in the zero ideal, even though E_{12} does not lie in the ideal. Therefore, the zero ideal is not completely prime. □

6. Let $R = 2\mathbb{Z}$, the ring of even integers. Show that $4\mathbb{Z}$ is a maximal ideal of R that is not a prime ideal, and show that $6\mathbb{Z}$ is both maximal and prime in R.

   Proof. Note $4\mathbb{Z}$ is maximal **subgroup** of $2\mathbb{Z}$: it has prime index, $[2\mathbb{Z} : 4\mathbb{Z}] = 2$; thus, it cannot be properly contained in a proper ideal (which would be a subgroup). And since $4\mathbb{Z}$ is an ideal of $\mathbb{Z}$ contained in $2\mathbb{Z}$, it is also an ideal of $2\mathbb{Z}$. Thus, it is a maximal ideal of $2\mathbb{Z}$.

   On the other hand, $(2)(2) \in 4\mathbb{Z}$ but $2 \notin 4\mathbb{Z}$, so this ideal is not completely prime. As the ring is commutative, being prime is equivalent to being completely prime, so this established the result.

   For $6\mathbb{Z}$, it is an ideal of $\mathbb{Z}$ contained in R, so it is also an ideal of R, Since the index $[2\mathbb{Z} : 6\mathbb{Z}] = 3$, it is a maximal **subgroup**, and hence is also a maximal ideal. Finally, it is a prime ideal because if $(2m)(2n) \in 6\mathbb{Z}$, then $3|4mn$, and hence one of m and n is a multiple of 3; thus, at least one of $2m$ and $2n$ lie in $6\mathbb{Z}$. □

   NOTE: If the ideal I is a maximal subgroup of the ring R, then I must be a maximal ideal as well. However, it is possible for an ideal to be maximal and yet for the underlying subgroup to not be maximal. For example, the trivial ideal in $M_2(\mathbb{R})$ is maximal by Problem 4, but the set of all matrices with zero second row is a strictly larger proper additive subgroup.

7. Let R be a ring, not necessarily commutative, not necessarily with unity. Let $f, g\colon \mathbb{Q} \to R$ be ring homomorphisms. Prove that if $f(n) = g(n)$ for all $n \in \mathbb{Z}$, then $f = g$.

   Proof. Let $\frac{x}{y} \in \mathbb{Q}$, with $x, y \in \mathbb{Z}$, $y \neq 0$. We have:

$$\begin{aligned}
f\left(\frac{x}{y}\right) &= f\left(\frac{1}{y}x\right) \\
&= f\left(\frac{1}{y}\right) f(x) \\
&= f\left(\frac{1}{y}\right) g(x) \\
&= f\left(\frac{1}{y}\right) g\left(\frac{xy}{y}\right) \\
&= f\left(\frac{1}{y}\right) g\left(xy\frac{1}{y}\right) \\
&= f\left(\frac{1}{y}\right) g(xy) g\left(\frac{1}{y}\right) \\
&= f\left(\frac{1}{y}\right) f(xy) g\left(\frac{1}{y}\right)
\end{aligned}$$

$$
\begin{aligned}
&= f\left(\frac{xy}{y}\right) g\left(\frac{1}{y}\right) \\
&= f(x) g\left(\frac{1}{y}\right) \\
&= g(x) g\left(\frac{1}{y}\right) \\
&= g\left(\frac{x}{y}\right).
\end{aligned}
$$

Therefore, $f = g$, as claimed. □

REMARK: Note that we did not even use all the properties of homomorphisms, we only used the fact that f and g are multiplicative homomorphisms; so this claim is also true for the semigroup morphism $\mathbb{Z} \hookrightarrow \mathbb{Q}$ and any semigroup homomorphisms $f, g\colon (\mathbb{Q}, \cdot) \to S$ that agree on $\mathbb{Z}$.

This establishes that the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is right-cancellable when workign with rings and ring homomorphisms; that is, it is an *epimorphism* even though it is not surjective. Which is one reason why I don't like to use "epimorphism" as a synonym for "surjective".

NOTE: The argument above is called a "Zigzag argument".

8. Let R be a ring, not necessarily commutative, not necessarily with unity. Prove that the following are equivalent:

   (a) Every left ideal of R is finitely generated: if I is a left ideal of R, then there exist $a_1, \ldots, a_n \in I$ such that $I = (a_1, \ldots, a_n)$.

   (b) R satisfies ACC (the *Ascending Chain Condition*) on left ideals: that is, if we have $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ an ascending chain of left ideals of R, then there exists n such that $I_n = I_{n+j}$ for all $j \geq 0$.

   (c) Every nonempty collection $\mathcal{S}$ of left ideals of R has maximal elements: if $\mathcal{S}$ is a nonempty collection of left ideals of R, then there exists a left ideal $M \in \mathcal{S}$ such that for all left ideals $I \in \mathcal{S}$, if $M \subseteq I$ then $M = I$.

Proof. One can prove this in the traditional "cyclic" fashion (say, prove that (a) implies (b), (b) implies (c), and (c) implies (a)). However, some of the implications require the Axiom of Choice, and I want to highlight which ones do, so I'm going to directly prove each of the six implications.

(a) $\Longrightarrow$ (b) (Does not require the Axiom of Choice) Let $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ be a chain of left ideals, and let $I = \cup_{n=1}^{\infty} I_n$. We proved in class that I is a left ideal (when we proved that maximal ideals exist, we showed that the union of a chain of left/right/2-sided ideals is a left/right/2-sided ideal), and so by (i) there exist $a_1, \ldots, a_k \in I$ such that $I = (a_1, \ldots, a_k)_\ell$. For each j, there exists n_j such that $a_j \in I_{n_j}$, since I is the union of the I_n and $a_j \in I$. Let $n = \max\{n_1, \ldots, n_k\}$; then $I_{n_j} \subseteq I_n$ for all j, so $a_j \in I_n$ for $j = 1, \ldots k$. Therefore,

$$I = (a_1, \ldots, a_k)_\ell \subseteq I_n \subseteq \cup_{j=1}^{\infty} I_j = I.$$

So for every $j \geq 0$, $I = I_n \subseteq I_{n+j} \subseteq I$; and hence $I_n = I_{n+j}$. □

(b) $\Longrightarrow$ (a) (Uses the Axiom of Choice) We prove this implication by contrapositive. Assume that I is not finitely generated. Then for every finite subset $X \subseteq I$, the left ideal $(X)_\ell$ does not equal I, and hence the set $I - (X)_\ell$ is nonempty. Using the Axiom of Choice, there is a function f whose domain is the family of finite subsets of I, with the property that for every finite subset X of I, $f(X) \in I - (X)_\ell$.

We define an infinite strictly increasing chain of ideals as follows: let $a_1 = f(\varnothing)$. Then let $a_2 = f(\{a_1\})$. Assuming we have defined $a_1, \ldots, a_k$, let $a_{k+1} = f(\{a_1, \ldots, a_k\})$.

Now let $I_m = (a_1, \ldots, a_m)_\ell$. By construction $a_{m+1} \notin (a_1, \ldots, a_m)_\ell$, so $I_m \subsetneq I_{m+1}$. Thus, we have an infinite strictly increasing chain of left ideals

$$I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_m \subsetneq \cdots$$

which is what we needed to show. □

REMARK. In fact, this only requires a weak form of the Axiom of Choice, known as the Axiom of Dependent Choice:

> Let X be a nonempty set, and let R be a binary relation on X with the property that for all $a \in X$ there exists a $b \in X$ with aRb. Then there is a sequence $\{x_n\}_{n=1}^{\infty}$ of elements of X such that $x_n R x_{n+1}$ for all $n \in \mathbb{N}$.

(c) $\Longrightarrow$ (a) (Does not require the Axiom of Choice) Let I be a left ideal, and let S be the collection of all finitely generated left ideals that are contained in I. Since $(0) \in S$, the collection is not empty. Thus, S has a maximal element M; this is a finitely generated left ideal that is contained in M. In particular, there exist $a_1, \ldots, a_n \in M$ such that $M = (a_1, \ldots, a_n)_\ell$.

For every $x \in I$, the ideal $(a_1, \ldots, a_n, x)_\ell$ is a finitely generated ideal contained in I, so $(a_1, \ldots, a_n, x)_\ell \in S$. Since $M \subseteq (a_1, \ldots, a_n, x)$, the maximality of M implies that $(a_1, \ldots, a_n, x)_\ell = M$. Thus, $x \in M$.

Therefore, $I \subseteq M \subseteq I$, hence $I = M$, and so I is finitely generated, as claimed. □

(a) $\Longrightarrow$ (c) (Uses the Axiom of Choice) Let $\mathcal{C}$ be a chain in S. Then $\cup\mathcal{C}$ is a left ideal, as we proved in class, and so is finitely generated: $\cup\mathcal{C} = (a_1, \ldots, a_n)_\ell$. Arguing as we did in the proof that (i) implies (ii), it follows that there exists $I \in \mathcal{C}$ such that $(a_1, \ldots, a_n)_\ell = I$, so $(a_1, \ldots, a_n)_\ell$ is in $\mathcal{C} \subseteq S$. That means that the chain $\mathcal{C}$ has an upper bound (namely $(a_1, \ldots, a_n)_\ell$) which is in S.

By Zorn's Lemma, it follows that S has maximal elements, as claimed. □

(b) $\Longrightarrow$ (c) (Uses the Axiom of (Dependent) Choice) Assume that there is a nonempty collection S of left ideals that does not have maximal elements. Let $I_1 \in S$. Then I_1 is not maximal in S, so there exists $I_2 \in S$ such that $I_1 \subsetneq I_2$. Assuming we have constructed $I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_n$, since I_n is not maximal in S there exists $I_{n+1} \in S$ such that $I_n \subsetneq I_{n+1}$. Inductively, we construct an infinite ascending chain of left ideals, so R does not satisfy the ACC. □

(c) $\Longrightarrow$ (b) (Does not require the Axiom of Choice). Let $I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$ be an ascending chain of left ideals. Let $S = \{I_k \mid k \geq 1\}$. This is a nonempty collection of left ideals, hence it has a maximal element I_N. If $j \geq 0$, then $I_N \subseteq I_{N+j}$, so by maximality of I_N we have $I_N = I_{N+j}$, as desired. □