Homework 10

1. For every positive integer n let R_n be a ring and suppose for $0 < m < n$ there exist ring homomorphisms $\varphi_{n,m} : R_n \to R_m$ such that if $0 < l < m < n$, we have $\varphi_{n,l} = \varphi_{m,l} \circ \varphi_{n,m}$. This defines an inverse system.

   We have previously shown that the inverse limit $\varinjlim R_n$ of the groups R_n exists. Now we will show that this inverse limit of rings has a ring structure.

   The inverse limit of groups is defined to be the subset $\Gamma \subset \prod_1^\infty R_n$ consisting of elements (x_i) such that for $i < j$, we have $\varphi_{j,i}(x_j) = x_i$. We define the ring operation component-wise. This is well defined since products exist in the category of rings (to be shown), so we just need to show that it takes values in Γ. Let $(a_i), (b_i) \in \Gamma$ and $0 < i < j$. Then

   $$\varphi_{j,i}(a_j b_j) = \varphi_{j,i}(a_j)\varphi_{j,i}(b_j) = a_i b_i$$

   so indeed $(a_i b_i) \in \Gamma$.

2. We will define the product of rings G and H as the cartesian product $G \times H$ equipped with component-wise addition and multiplication. Let p_1 and p_2 be the projections onto G and H respectively.

   Suppose K is another ring with homomorphisms $f : K \to G$ and $g : K \to H$. We must show there is a map u such that the following diagram is commutative:

   $$\begin{tikzcd} & K \arrow[dl, "f"'] \arrow[d, "u"] \arrow[dr, "g"] & \\ G & G \times H \arrow[l, "p_1"'] \arrow[r, "p_2"] & H \end{tikzcd}$$

   If we did have such a map, for $k \in K$ we would have $u(k) = (a, b)$, and $p_1 \circ u(k) = a = f(k)$, and likewise $b = g(k)$. Then $u(k) = (f(k), g(k))$ for all such maps.

   Indeed, the map $u : k \mapsto (f(k), g(k))$ makes the diagram commute, and is the only such map by the above argument. Then $G \times H$ is a direct product of rings.

3. Let $\eta(R)$ be the set of nilpotent elements in a commutative ring R. First we show that $\eta(R)$ is an ideal. Let $a \in R$ and $b \in \eta(R)$ with $b^n = 0$ for some n. Then $(ab)^n = a^n b^n = a^n \cdot 0 = 0$.

   Next we show that $\eta\left(R/\eta(R)\right) = \{0\}$. Let $a + \eta(R) \in R/\eta(R)$ and suppose $(a + \eta(R))^n = 0$ for some n. Then by the definition of the quotient ring, we have $a^n + \eta(R) = 0$ and thus $a^n \in \eta(R)$. Then there is some m such that $(a^n)^m = 0$, and thus $a^{nm} = 0$ and $a \in \eta(R)$. Then $a + \eta(R) = \eta(R) = 0 \in R/\eta(R)$. So the only nilpotent element of $R/\eta(R)$ is 0.

4. We will prove that $\mathrm{End}(\mathbb{Z} \oplus \mathbb{Z})$, the ring of endomorphisms of $\mathbb{Z} \oplus \mathbb{Z}$, is noncommutative.

   Note that $\mathbb{Z} \oplus \mathbb{Z}$ is free, so any map of its generators $(1, 0)$ and $(0, 1)$ into a group G extends to a homomorphism $\mathbb{Z} \oplus \mathbb{Z} \to G$.

   Consider the following homomorphisms $\mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}$, defined by their action on generators:

   $$\varphi : \begin{array}{l} (1, 0) \mapsto (1, 1) \\ (0, 1) \mapsto (1, 1) \end{array}$$

   $$\psi : \begin{array}{l} (1, 0) \mapsto (1, 0) \\ (0, 1) \mapsto (1, 1) \end{array}.$$

   Then $\varphi(\psi(0, 1)) = \varphi(1, 1) = (2, 2)$, but $\psi(\varphi(0, 1)) = \psi(1, 1) = (2, 1)$, and thus $\varphi \circ \psi \neq \psi \circ \varphi$. Then the endomorphism ring of $\mathbb{Z} \oplus \mathbb{Z}$ is noncommutative.

5. Let R be a ring and $I \subset R$ and ideal. (1.) $M_n(I)$ is an ideal: Let $A \in M_n(R)$ and $B \in M_n(I)$. Then the entries of AB are each sums of elements in I multiplied on the left by elements of R. Since I is an ideal and hence a left ideal, each entry of AB is in I, so $AB \in M_n(I)$. Then $M_n(I)$ is a left ideal. A similar proof shows $BA \in M_n(I)$, so that $M_n(I)$ is both a left and right ideal.

   (2.) Let I be an ideal in $M_n(R)$.

   Denote by $I_{i,j}$ the set of all values in the (i, j) coordinate of matrices in I. For any $a \in I_{i,j}$ and any $r \in R$, we can obtain a matrix in I with rar in the (i, j) coordinate and zeros otherwise by multiplying the matrix with only a at position (i, j) on the left and right by the matrices with all entries r. Then $rar \in I_{i,j}$, so $I_{i,j}$ is an ideal for any $0 \leq i, j \leq n$.

   Note that for any $A \in I$, by multiplying A on the right by the matrix with all zeros except 1 in the (j, j) coordinate we can reduce every column of A to zero except the jth one. by multiplying A on the left by a matrix with all zeros except a 1 in the (i, i) coordinate, we obtain a matrix with only the ith row of A. This allows us to obtain a new matrix with only the (i, j)th position equal to that of A, and all other entries zero. Note also that this new matrix is in I, since I is a left and right ideal within $M_n(R)$.

   Also note that for any matrix A in $M_n(R)$, we can obtain a new matrix equal to A with any two of its rows or columns swapped by multiplying by a certain matrix on the left or right. I is closed under this operation since it is an ideal. Then for any $0 \leq h, i, j, k \leq n$, we can produce a matrix with any of the values of $I_{h,i}$ appearing in the (j, k)th coordinate. Hence, $I_{h,i} \subset I_{j,k}$, and likewise $I_{j,k} \subset I_{h,i}$. Then it follows that the $I_{i,j}$'s are equal for any choice of $0 \leq i, j \leq n$. Call this set I'.

   This proves that $I \subset M_n(I')$. We showed that I contains all the matrices with only one coordinate nonzero and with this entry equal to any element of I'. Then we can add these to obtain any element of $M_n(I')$. I is closed under addition, and hence $M_n(I') \subset I$ and we are done.

6. We prove R is a division ring if and only if it has no proper left ideals.

   First suppose R is a division ring. Then every element of R is a unit. Thus any nonzero ideal must contain a unit and is thus equal to R itself.

   Conversely suppose R has no proper ideals. Then for any nonzero $a \in R$, the left ideal $\langle a \rangle$ must equal R. Then $\langle a \rangle$ contains 1, so there is some $b \in R$ such that $ba = 1$. This proves every nonzero element of R has a left inverse.

   This in fact proves that every nonzero element has a right inverse as well. Again let $a, b \in R$ such that $ba = 1$. Take some $c \in R$ such that $cb = 1$. Then

$$ab = cbab = cb = 1,$$

   and we see b is the right inverse of a as well. Then R is a division ring.

7. Let m be a positive integer and consider the ring $\mathbb{Z}_m$ of integers modulo m. Note that this is a commutative ring.

   Proposition: $\mathbb{Z}_m$ is an integral domain if and only if m is prime. In particular, $\mathbb{Z}_p$ is a field for p prime.

   Proof: If m is not prime, say $m = nl$, then we have $nl = 0 \mod m$ and thus n and l are zero divisors.

   If m is prime, suppose there are $a, b \in \mathbb{Z}_m$ such that $ab = 0 \mod m$. Then $ab|m$ and m must divide either a or b, hence one of them must be 0 in $\mathbb{Z}_m$.

   If p is prime, then by Fermat's Little Theorem, for any nonzero $a \in \mathbb{Z}_p$ we have

$$a^{p-1} = 1 \mod p$$

   and we see that a^{p-2} is the multiplicative inverse of a in $\mathbb{Z}_p$.

Proposition: If R is a commutative ring and $M \subset R$ is an ideal, then M is maximal if and only if R/M is a field.

Proof: The direction R/M is a field if M is maximal was proved in class.

Conversely suppose R/M is a field. Suppose $N \subset R$ is another ideal, not necessarily proper, and $M \subsetneq N$. Take $a \in N \setminus M$ so that $\overline{a} \in R/M$ is not equal to zero. Then $\overline{a}$ is a unit since R/M is a field, so there is some $\overline{b} = b + M$, $b \in R$, such that $\overline{a}\overline{b} = 1$. Then $ab + m = 1$ for some $m \in M$. But $M \subset N$, so $1 \in N$ and hence $N = R$. Then M is maximal.

It was proven in class that R/I is an integral domain if and only if I is a prime ideal.

Finally, we know every ideal in $\mathbb{Z}_m$ is principal.

If m is prime, $\mathbb{Z}_m$ has no proper ideals.

Otherwise, the maximal ideals and prime ideals coincide except for the ideal $\langle 0 \rangle$ which is prime. Every nonzero maximal or prime ideal is generated by a prime number, and every prime number generates an ideal which is both prime and maximal.

To see this, suppose $\langle a \rangle$ is prime or maximal. Then $\mathbb{Z}_m/\langle a \rangle$ is a field, and all quotients of $\mathbb{Z}_m$ are isomorphic to $\mathbb{Z}_n$ for some n. Then we must have $\mathbb{Z}_m/\langle a \rangle \simeq \mathbb{Z}_p$ for some p, and thus $a = p$.

Moreover for any prime $p < m$, we have $\mathbb{Z}_m/\langle p \rangle = \mathbb{Z}_p$ which is a field. Then $\langle p \rangle$ is prime and maximal.

8. Let S be a subset of a ring R. We will show the intersection of all ideals containing S is the set

$$N = \left\{ \sum_1^n r_i s_i t_i : r_1, t_1, \ldots, r_n, t_n \in R, s_1, \ldots, s_n \in S, n \in \mathbb{N} \right\}.$$

First suppose

$$x \in \bigcap \{I : I \text{ an ideal with } S \subset I\}.$$

Note that N is an ideal since multiplication satisfies the distributive property and because N is closed under addition, and that S is contained in N. Then $x \in N$.

Conversely, suppose $x \in N$ with

$$x = \sum_1^n r_i s_i t_i,$$

for r_i, t_i elements of R and s_i elements of S. Then for any ideal I containing S, I contains every s_i and thus contains x. Then x is contained in the intersection of all ideals containing S.