MATH 830 FALL 2025: HOMEWORK 1

For this assignment, you may use your notes, the Daily Summary, and any daily homework you have done. You may also work with classmates on these problems, but please indicate who you worked with, and write up the solutions completely on your own. You may not consult outside sources, including, any algebra textbook, the internet, graduate students not in this class, or any professor except your Math 830 instructor. You may not cite any facts not covered in class or the homework. To receive full credit, all proofs must be complete and contain the appropriate amount of detail. Your solutions are due at the start of class on Monday, September 15.

Throughout R will denote a commutative ring.

1. Suppose M is an R-module and $I \subseteq R$ is an ideal. Define IM to be the set of all finite linear combinations of the form $i_1x_1 + \cdots + i_nx_n$, with each $i_j \in I$ and $x_j \in M$.

(i) Prove that IM is a submodule of M.
(ii) Show that if $X \subseteq M$ and $\langle X \rangle = M$, then IM is the set of all finite linear combinations of the form $i_1x_1 + \cdots + i_nx_n$, with each $i_j \in I$ and $x_j \in X$.
(iii) Prove that M/IM has the structure of an R/I-module.
(iv) Conclude that if $IM = 0$, then M is also an R/I module and $N \subseteq M$ is an R-submodule of M if and only if N is an R/I submodule of M.

Solution. Part (i) is straightforward, since sums and scalar multiples of expressions of the form $i_1x_1 + \cdots + i_nx_n$, with each $i_j \in I$ and $x_j \in M$, clearly have this form. For (ii), a typical element in I has the form $\sum_j i_j z_j$ with each $i_j \in I$ and z_j in M. Each z_j has the form $\sum_k a_{jk}x_k$, for $a_{jk} \in R$ and $x_k \in X$. Thus, a typical element in I can be written as $\sum_j i_j(\sum_k a_{jk}x_k) = \sum_k(\sum_j i_j a_{jk})x_k$, which gives what we want.

For (iii), M/IM is an abelian group. To make M/IM into an R/I-module, define scalar multiplications as follows: $(r+I)\cdot(m+IM) := rm+IM$. Suppose $r+I = r'+I$ and $m+IM = m'+IM$. Then $r-r' \in I$ and $m-m' \in IM$. Thus, $(r-r')m \in IM$ and $r'(m-m') \in IM$. Adding, we obtain $rm - r'm' \in IM$, so $rm+IM = r'm'+IM$, and therefore scalar multiplication is well defined. The required scalar multiplication axioms are automatically inherited from the existing R-module structure on M, e.g.

$$(r+I)\{(s+I)(m+IM)\} = (r+I)(sm+IM) = r(sm)+IM = (rs)m+IM = \{(r+I)(s+I)\}(m+IM).$$

For (iv), if $IM = 0$, then $M/IM = M$, so the first statement follows from part (iii) and $(r+I)m = rm$, for all $r \in R$ and $m \in M$. Now, suppose $N \subseteq M$ is an R-submodule of M. Then N is an abelian subgroup of M and moreover, for all $r \in R$ and $n \in N$: $(r+I)n = rn$, since $IN = 0$. Thus, any R-submodule of M is also an R/I-submodule of M and conversely.

2. Let $\{H_i\}_{i\in I}$ be a collection of R modules and $S := \bigoplus_{i\in I} H_i$ be the (external) direct sum of the H_i. For each $i \in I$, we have a canonical injective R-module homomorphism $j_i : H_i \to S$, given by $j_i(h) = t$, where $t \in S$ is the I-tuple whose ith component is h and all other components are 0.

(i) Suppose T is an R-module and for each $i \in I$, we have an R-module homomorphism $f_i : H_i \to T$. Show that there exists a unique R-module homomorphism $F : S \to T$ such that $Fj_i = f_i$, for all $i \in I$.
(ii) Let P be an R-module with the following property: For each $i \in I$, there exists an injective R-module homomorphisms $k_i : H_i \to P$ such that given R-module homomorphisms $g_i : H_i \to T$, there exists a unique R-module homomorphism $G : P \to T$ satisfying $Gk_i = g_i$. Prove that P is isomorphic to S.

Solution. Maintaining the notation in the statement of the problem, let us write (h_i) for a typical element in S. For (i) we define $F : S \to T$ by $F((h_i)) := \sum_{i\in I} f_i(h_i)$. Note that the sum makes sense in T, since by definition, all but finitely many h_i are zero, so the sum involves only finitely many non-zero terms. Adding finite sums of the form $\sum_i t_i$ in the obvious way, we have

$$F((h_i)+(h_i')) = F((h_i+h_i')) = \sum_i f_i(h_i+h_i') = \sum_i f_i(h_i)+f_i(h_i') = \sum_i f_i(h_i)+\sum_i f_i(h_i') = F((h_i))+F((h_i')),$$

so that F is additive. Similarly, for all $r \in R$,

$$rF((h_i)) = r\sum_i f_i(h_i) = \sum_i rf_i(h_i) = \sum_i f_i(rh_i) = F((rh_i)) = F(r(h_i)),$$

showing that F is an R-module homomorphism. Moreover, for each $i \in I$ and $h_i \in H_i$, we have $Fj_i(h_i) = f_i(h_i)$, since all of the coordinates of $j_i(h_i)$ are zero, except the ith coordinate, which is h_i.

Now, suppose $G : S \to T$ is an R-module homomorphism having the property that $Gj_i = f_i$, for all $i \in I$. Let $s \in S$, and suppose that the only non-zero components of s are $h_{i_1}, \ldots, h_{i_k}$. For $1 \leq c \leq k$, let (h_{i_c}) dente the I-tuple that is h_{i_c} in the i_c coordinate, and zero elsewhere, so that $s = (h_{i_1}) + \cdots + (h_{i_k})$. Then,

$$\begin{aligned} G(s) &= G((h_{i_1}) + \cdots + (h_{i_k})) \\ &= G((h_{i_1})) + \cdots + G((h_{i_k})) \\ &= Gj_{i_1}(h_{i_1}) + \cdots + Gj_{i_k}(h_{i_k}) \\ &= f_{i_1}(h_{i_1}) + \cdots + f_{i_k}(h_{i_k}) \\ &= F(s), \end{aligned}$$

so F is unique.

3. Let

$$\mathcal{C} : \quad 0 \to C_n \xrightarrow{f_n} C_{n-1} \xrightarrow{f_{n-1}} \cdots \xrightarrow{f_2} C_1 \xrightarrow{f_1} C_0 \to 0$$

be a sequence of finite length R-modules and R-module homomorphisms satisfying $f_i \circ f_{i+1} = 0$, for all i, in other words, $\mathcal{C}$ is a *complex* of finite length R-modules. For each i, set $\mathrm{H}_i(\mathcal{C}) := \ker(f_i)/\mathrm{im}((f_{i+1})$, the i^{th} *homology module of* $\mathcal{C}$. Prove that the homology modules $\mathrm{H}_i(\mathcal{C})$ have finite length and

$$\sum_{i \geq 0} (-1)^i \lambda(C_i) = \sum_{i \geq 0} (-1)^i \lambda(\mathrm{H}_i(\mathcal{C})).$$

Solution. For each $0 \leq i \leq n$, let K_i denote the kernel of f_i and A_i denote the image of f_{i+1}, so that $\mathrm{H}_i(\mathcal{C}) = K_i/A_i$. Note, here we are taking f_0 to be the zero map. Since submodules and quotient modules of finite length modules have finite length, each homology module in the complex $\mathcal{C}$ has finite length. For the second statement, induct on n. If $n = 0$, then $C_0 = K_0$ and $A_0 = (0)$, so that $C_0 = \mathrm{H}_0(\mathcal{C})$, and the result is clear. Suppose $n > 0$. Let $\mathcal{C}$' denote the complex

$$\mathcal{C}' : \quad 0 \to C_n \xrightarrow{f_n} C_{n-1} \xrightarrow{f_{n-1}} \cdots \longrightarrow C_2 \xrightarrow{f_2} C_1 \to 0.$$

By induction,

$$\sum_{i \geq 1} (-1)^i \lambda(C_i) = \sum_{i \geq 2} (-1)^i \lambda(\mathrm{H}_i(\mathcal{C})) - \lambda(C_1/A_1)$$

Adding $\lambda(C_0)$ to both sides of this equation gives

$$\begin{aligned} \sum_{i \geq 0} (-1)^i \lambda(C_i) &= \sum_{i \geq 2} (-1)^i \lambda(\mathrm{H}_i(\mathcal{C})) - \lambda(C_1/A_1) + \lambda(C_0) \\ &= \sum_{i \geq 2} (-1)^i \lambda(\mathrm{H}_i(\mathcal{C})) - \lambda(C_1) + \lambda(A_1) + \lambda(C_0/A_0) + \lambda(A_0) \\ &= \sum_{i \geq 2} (-1)^i \lambda(\mathrm{H}_i(\mathcal{C})) - \lambda(C_1) + \lambda(A_1) + \lambda(C_0/A_0) + \lambda(C_1/K_1) \\ &= \sum_{i \geq 2} (-1)^i \lambda(\mathrm{H}_i(\mathcal{C})) - \lambda(C_1) + \lambda(A_1) + \lambda(C_0/A_0) + \lambda(C_1) - \lambda(K_1) \\ &= \sum_{i \geq 2} (-1)^i \lambda(\mathrm{H}_i(\mathcal{C})) - \lambda(\mathrm{H}_1(\mathcal{C})) + \lambda(\mathrm{H}_0(\mathcal{C})) \\ &= \sum_{i \geq 0} (-1)^i \lambda(\mathrm{H}_i(\mathcal{C})), \end{aligned}$$

as required. □

4. Suppose $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is a short exact sequence of R-modules. Prove that if C is a free R-module, then there exists an R-module homomorphism $j : C \to B$ satisfying:

(i) $g \circ j = 1_C$.
(ii) $B = f(A) \bigoplus j(C)$.

Conclude that B is isomorphic to $A \bigoplus C$.

Solution. Let $X = \{x_i\}_{i \in I}$ be a basis for C. Since g is surjective, for each i we have $b_i \in B$ such that $g(b_i) = x_i$. Set $j_0(x_i) := b_i$, for all i. This gives a set map $j_0 : X \to B$ satisfying $h \circ j_0 = 1_C$. Since C is free with basis X, j_0 extends to an R-module homomorphism $j : C \to B$, and the linearity of j together with $g \circ j_0 = 1_C$ gives $g \circ j = 1_C$.

Now take $b \in B$, then $g(b - jg(b)) = g(b) = gjg(b) = g(b) - g(b) = 0$, so that $b - jg(b)$ is in the kernel of g, which equals the image of f. Thus, $b - jg(b) = f(a)$, for some $a \in A$, and therefore $b = f(a) + j(g(b))$, showing $B = f(A) + j(C)$. Suppose $f(a_1) = j(c)$, is in $f(A) \cap j(C)$, for some $a_1 \in A$ and $c \in C$. Then $0 = gf(a_1) = gj(c) = c$, so $c = 0$ and hence $j(c) = 0$, showing that $f(A) \cap j(C) = 0$. Thus, $B = f(A) \bigoplus j(C)$.

For the final statement, f is 1-1, so $A \cong f(A)$. Suppose $j(c) = 0$, some $c \in C$, then $c = gj(c) = 0$, showing j is 1-1. Thus, $C \cong j(C)$. It follows immediately that $B \cong A \bigoplus C$.

5. Let M be an Artinian R-module and $\phi : M \to M$ an injective R-module homomorphism. Prove that ϕ is an isomorphism.

Solution. We have a descending sequence of submodules $\mathrm{im}(\phi) \supseteq \mathrm{im}(\phi^2) \supseteq \cdots$, so by the Artinian property, the image of ϕ^n equals the image of ϕ^{n+1}, for some n. Take $a \in A$. Then $\phi^n(a) = \phi^{n+1}(a')$, for some $a' \in A$. Thus, $\phi^n(a - \phi(a')) = 0$. Since ϕ is injective, an easy induction argument shows that ϕ^n is injective. Thus, $a - \phi(a') = 0$, so $a = \phi(a')$, showing ϕ is surjective, and hence an isomorphism.

6. Let $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ be an exact sequence or R-modules. Prove that B is Artinian if and only A and C are Artinian.

Solution. Suppose B is Artinian, then $f(A)$ is Artinian, since a descending sequence of submodules in $f(A)$ is also a descending sequence of submodules in B. Since $A \cong f(A)$, we have that A is Artinian. Now suppose $C_1 \supseteq C_2 \cdots$ is a descending sequence of submodules of C. then $g^{-1}(C_1) \supseteq g^{-1}(C_2) \supseteq \cdots$ is a descending sequence of submodules of B containing the kernel of g. Suppose $g^{-1}(C_n) = g^{-1}(C_{n+1}) = \cdots$. Since g is surjective $gg^{-1}(C_j)) = C_j$ for all j, so the descending chain in C stabilizes, showing that C is Artinian.

Suppose A and C are Artinian. Then $f(A) \cong A$ is Artinian and $B/f(A) \cong C$ is Artinian. So it suffices to show that if M is an R-module and $N \subseteq M$ is a submodule, then M is Artinian, if both N and M/N are Artinian. Consider a descending chain of submodules in M: $M_1 \supseteq M_2 \supseteq \cdots$. Then we have two descending chains: the chain $M_1 \cap N \supseteq M_2 \cap N \supseteq \cdots$ in N and the chain $(M_1 + N)/N \supseteq (M_2 + N)/N \supseteq \cdots$ in M/N. Suppose both chains are stable for $n \geq n_0$. Take $x \in M_n$. Then the coset $x + N$ belongs to $(M_n + N)/N = (M_{n+1} + N)/N$, so that $x - y \in N$, for some $y \in M_{n+1}$. Since $x - y \in M_n$, we have $x - y \in M_n \cap N = M_{n+1} \cap N$. If $x - y = z$, for $z \in M_{n+1} \cap N$, we have $x = y + z \in M_{n+1}$, showing $M_n = M_{n+1}$, for all $n \geq n_0$, so M is Artinian.

7. Assume that R has a *unique* maximal ideal P and let A be an Artinian R-module. For $p \in P$ and $x \in A$, prove there exists $n \geq 1$ such that $p^n x = 0$. Conclude that if P is finitely generated (e.g., R is Noetherian), then for each $x \in A$, there exists $r \geq 1$ (depending on x) such that $P^r x = 0$.

Solution. For $x \in A$ and $p \in P$, we have a descending sequence of submodules $\langle px \rangle \supseteq \langle p^2 x \rangle \supseteq \cdots$, and hence there is $n \geq 1$ such that $\langle p^n x \rangle = \langle p^{n+1} x \rangle$. It follows that $p^n x = rp^{n+1} x$, for some $r \in R$. Thus, $(1 - rp)p^n x = 0$. However, since P is the only maximal ideal of R, and $1 - rp \notin P$, we have that $1 - rp$ is a unit. Thus, cancelling this unit, we have $p^n x = 0$, for some n.

Now suppose $P = \langle p_1, \ldots, p_c \rangle$ is finitely generated. Fix $x \in A$. Then for each i we have $p_i^{n_i} x = 0$, for some $n_1, \ldots, n_c \geq 1$. If we set $N = \max\{n_1, \ldots, n_c\}$, we have $\langle p_1^N, \ldots, p_c^N \rangle x = 0$. By the pigeonhole principle, for $r >> 0$, $P^r \subseteq \langle p_1^N, \ldots, p_c^N \rangle$, giving $P^r x = 0$.

8. Let R be an Artinian ring.

(i) Prove that R has finitely many maximal ideals.
(ii) Let J denote the Jacobson radical. Prove that $J^n = 0$, for some $n \geq 1$.
(iii) Suppose R has one maximal ideal P satisfying $P^n = 0$, for some $n \geq 1$. Show that R is Noetherian.

Solution. Suppose there are infinitely many distinct maximal ideals of R, say $P_1, P_2, \ldots$. Then we have a descending chain of ideals $P_1 \supseteq P_1 \cap P_2 \supseteq \cdots$. Thus, for some $n \geq 1$, $P_1 \cap \cdots \cap P_n = P_1 \cap \cdots \cap P_n \cap P_{n+1}$. It follows that $P_1 \cap \cdots \cap P_n \subseteq P_{n+1}$. Since P_{n+1} is a prime ideal, we have $P_i \subseteq P_{n+1}$, for some $1 \leq i \leq n$. Since P_{n+1} is a maximal ideal, we have the contradiction $P_i = P_{n+1}$. Thus, R has finitely many maximal ideals.

For (ii), on the one hand, since R is Artinian, there exists $n_0 \geq 1$ such that $J^n = J^{n+1}$, for all $n \geq n_0$, since $J \supseteq J^2 \supseteq \cdots$. On the other hand, suppose $J^n \neq 0$. Then there exists $x_1 \in J^n$ such that $x_1 J^n \neq 0$, since if $x_1 J^n = 0$ for all $x_1 \in J^n$, $J^n J^n = J^{2n} = J^n = 0$, a contradiction. Now choose $x_2 \in J^n$ such that $x_1 x_2 J^n \neq 0$. We can do this, otherwise, $x_1 x_2 J^n = 0$ for all $x_2 \in J^n$, and thus $0 = x_1 J^n J^n = x_1 J^n = 0$, contradicting the choice of x_1.

Thus, inductively, we can find $x_1, x_2, \ldots, \in J^n$,, such that for all $c \geq 1$, $x_1 \cdots x_c J^n \neq 0$. Now, the descending chain $\langle x_1 \rangle \supseteq \langle x_1 x_2 \rangle \supseteq \cdots$ must stabilize. Thus, for some $e \geq 1$, we can write $x_1 \cdots x_e = r x_1 \cdots x_e x_{e+1}$, for some $r \in R$. Thus, $(1 - r x_{e+1}) x_1 \cdots x_e = 0$. Since $x_{e+1} \in J$, $1 - r x_{e+1}$ is a unit. Thus, $x_1 \cdots x_e = 0$, a contradiction. Therefore, we must have $J^n = 0$, as required.

For (iii), we use the fact that if V is a vector space over the field F, then V is finite dimensional if and only if V is an Artinian F-module if and only if V is a Noetherian F-module. We now proceed by induction on r, to show that R/P^r is Noetherian for all $r \geq 1$. Since $P^n = 0$, it follows that R is a Noetherian ring. To proceed, if $r = 1$, then $F := R/P$ is a field and thus Noetherian. Now suppose R/P^r is a Noetherian ring. Then R/P^r is also a Noetherian R-module. Consider the natural exact sequence of R-modules:

$$0 \to P^r/P^{r+1} \to R/P^{r+1} \to R/P^n \to 0.$$

Since $P \cdot (P^r/P^{r+1}) = 0$, P^r/P^{r+1} is a vector space over F and its subspace structure as a vector space over F is the same as its submodule structure as an R-module, by Problem 1 (iv). Now, R is Artinian, and hence R/P^{r+1} is an Artinian R-module, and hence its submodule P^r/P^{r+1} is an Artinian R-module, and therefore an Artinian R/P-module, i.e., a finite dimensional vector space over F. Thus, P^r/P^{r+1} is a Noetherian R/P-module, and hence a Noetherian R-module. The induction hypothesis, together with the exact sequence above (and a theorem from class) give R/P^{r+1} is a Noetherian R-modules, and hence a Noetherian ring. Thus, R/P^r is Noetherian for all r, which is what we want. □.

9. Prove that an Artinian ring is Noetherian.[1].

Solution. Suppose R is an Artnian ring. Let $J \subseteq R$ be the Jacobson and $P_1, \ldots, P_k$ be the maximal ideals of R, which are finite in number, by Problem 8. For all $r \geq 1$, $P_1^r, \ldots, P_k^r$ are pairwise co-maximal, so that

$$J^r = P_1^r \cdots P_k^r = P_1^r \cap \cdots \cap P_k^r,$$

for all $r \geq 1$ (see the comments below). By Problem 8 (ii), we have $J^n = 0$, for some $n \geq 1$. Thus, as R-modules, we have

$$R \cong R/J^n \cong R/(P_1^r \cap \cdots \cap p_k^r) \cong R/P_1^r \oplus \cdots \oplus R/P_k^r,$$

where the third isomorphism follows by the Chinese remainder theorem. It now follows from Problem 6 and induction on k that each R/P_i^r is an Artinian R-module, and hence an Artinian ring. Suppose $Q \subseteq R/P_i^r$ is a maximal ideal. Then $Q = P/P_i^r$, for a maximal ideal $P \subseteq R$ containing P_i^r, by the correspondence theorem. Since P is prime, $P_i \subseteq P$, and since P_i is maximal, $P = P_i$. Thus, P_i/P_i^r is the only maximal ideal of R/P_i^r and $(P_i/P_i^r)^r = 0$. Thus, by Problem 8 (iii), R/P_i^r is a Noetherian ring, and hence a Noetherian R-module, for each $1 \leq i \leq k$. It follows that $R \cong R/P_1^r \oplus \cdots \oplus R/P_k^r$ is a Noetherian R-module, and hence a Noetherian ring. □

10. Follow the steps below to prove Hilbert's Basis Theorem: If R is a Noetherian ring, then the polynomial ring $R[x]$ is a Noetherian ring. To begin, let $J \subseteq R[x]$ be an ideal and $I := \{a \in R \mid a \text{ is the leading coefficient of some element of } J\}$.

(i) Show that I is an ideal of R.

Suppose $I := \langle a_1, \ldots, a_r \rangle$ and let $f_1(x), \ldots, f_r(x) \in J$ be such that the leading coefficient of $f_i(x)$ is a_i. Set $N := \max\{\text{degree}(f_i(x))\}$. Let F denote the free R-module generated by $1, x, \ldots, x^{N-1}$ and set $M := J \cap F$.

(ii) Show that M is an R-submodule of F and conclude that M is a finitely generated R-module.

(iii) Let $g_1(x), \ldots, g_t(x)$ generate M as an R-module. Prove that J is generated by $f_1(x), \ldots, f_r(x), g_1(x), \ldots, g_t(x)$. Hint: Show that if $h(x) \in J$ and $h(x)$ has degree greater than or equal to N, the there exist $d_1(x), \ldots, d_r(x)$ in $R[x]$ such that $h(x) - \{d_1(x)f_1(x) + \cdots + d_r(x)f_r(x)\}$ belongs to J and has degree strictly less than the degree of $h(x)$.

Solution. For(i), suppose $a, b \in I$. Then there exist $f(x) := ax^n + \cdots$ and $g := bx^m + \cdots$ in J. Suppose $n \geq m$. Then $f(x) + x^{n-m} g(x) = (a+b)x^n + \cdots$ belongs to J, and thus, $a + b \in I$. Moreover, if $r \in R$, $rf(x) = rax^n + \cdots$ belongs to J, and thus $ra \in I$. Therefore I is an ideal.

For (ii), suppose $f(x), g(x) \in M$. Then $f(x), g(x)$ belong to J and have degree less than N. Thus, the sum $f(x) + g(x) \in J$ and has degree less than N. In other words, $f(x) + g(x) \in M$. In addition, for any $r \in R$, $rf(x) \in J$ and has degree less than N, showing that M is a submodule of F. Since F is Noetherian (it's finitely generated over the Noetherian ring R), M is Noetherian, and hence finitely generated as an R-module.

For (iii), write L for the ideal of $R[x]$ generated by $f_1(x), \ldots, f_r(x), g_1(x), \ldots, g_c(x)$. Clearly, $L \subseteq J$. Take $h(x) \in J$. If $h(x)$ has degree less than N, then $h(x) \in M$, so that $h(x)$ is a finite R-linear combination of $g_1(x), \ldots, g_c(x)$, and hence $h(x) \in L$. Suppose $e := \deg(h(x)) \geq N$. We prove by induction on e that $h(x) \in L$. The argument for the

[1]This theorem is also true for non-commutative rings. Hopkins' Theorem states that a left (or right) Artinian ring is left (or right) Noetherian

base case $e = N$ is the same as for the inductive step, so assume $e > N$. Write $h(x) = bx^e + \cdots$. Then $b \in I$, so we can write $b = u_1a_1 + \cdots + u_ra_r$, for $u_j \in R$. For $1 \leq i \leq r$, set $n_i := \deg(f_i(x))$. Then the polynomial

$$h(x) - \{u_1x^{e-n_1}f_1(x) + \cdots + u_rx^{e-n_r}f_r(x)\}$$

belongs to J and has degree strictly less than e. Thus, by induction on e, $h(x) - \{u_1x^{e-n_1}f_1(x) + \cdots + u_rx^{e-n_r}f_r(x)\}$ is in L. It follows readily that $h(x) \in L$, giving $L \subseteq J$. Thus, $L = J$ and J is finitely generated. Therefore, $R[x]$ is Noetherian. □

Comments on the Chinese Remainder theorem. Throughout these comments $I, J \subseteq R$ are ideals.

(i) $I, J \subseteq R$ are said to be be co-maximal if there is no maximal ideal of R containing both I and J. Since every ideal of R is contained in a maximal ideal, this is equivalent to the condition $I + J = R$, which in turn is equivalent to $i + j = 1$, for some $i \in I$ and $j \in J$.

(ii). Suppose I and J are co-maximal, and $x \in I \cap J$. Write $1 = i + j$, for $i \in I$ and $j \in J$. Then $x = xi + xj \in IJ$. Thus, $I \cap J \subseteq IJ$. Since $IJ \subseteq I \cap J$ always holds, we have that if I and J are co-maximal, then $I \cap J = IJ$.

(iii) Suppose that I and J are co-maximal. Define $\phi : R \to (R/I) \oplus (R/J)$, by $\phi(r) = (r + I, r + J)$. It is easy to check that ϕ is a ring homomorphism. Clearly, $I \cap J$ is the kernel of ϕ. Now suppose $(a + I, b + J) \in (R/I) \oplus (R/J)$. Take $i \in I$ and $j \in J$ such that $i + j = 1$. Then $ai + aj = a$, so that $a + I = aj + I$. Similarly, $bi + bj = b$, so that $b + J = bi + J$. It follows that $\phi(aj + bi) = (aj + bi + I, aj + bi + J) = (aj + I, bi + J) = (a + I, b + J)$, so that ϕ is surjective. Thus, we have $R/(I \cap J) \cong (R/I) \oplus (R/J)$. This also yields $R/IJ \cong (R/I) \oplus (R/J)$.

(iv) Ideals $I_1, \ldots, I_k$ are pairwise co-maximal, if for each $1 \leq i \neq j \leq k$, I_i and I_j are co-maximal. Given (iii) above, one can show via induction on k, that if $I_1, \ldots, I_k$ are co-maximal, then $R/(I_1 \cap \cdots \cap I_k) \cong (R/I_1) \oplus \cdots \oplus (R/I_k)$. Indeed, since I_1 and $I_2 \cap \cdots \cap I_k$ are comaximal, we have

$$R/(I_1 \cap \cdots \cap I_k) = R/(I_1 \cap (I_2 \cap \cdots \cap I_k)) \cong (R/I_1) \oplus (R/(I_2 \cap \cdots \cap I_k)) \cong (R/I_1) \oplus (R/I_2) \oplus \cdots \oplus (R/I_k).$$

(v) The modern version of the classical version of the Chinese remainder theorem take the following form. Suppose $n_1, \ldots, n_k$ are pairwise relatively prime positive integers. Set $n := n_1 \cdots n_k$. Then $\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

(vi) The classical form of the Chinese remainder theorem states the following: Suppose $n_1, \ldots, n_k$ are pairwise relatively prime positive integers. Then, given $a_1, \ldots, a_k \in \mathbb{Z}$, the system of congruences

$$x \equiv a_1 \pmod{n_1\mathbb{Z}}, \ldots, x \equiv a_k \pmod{n_k\mathbb{Z}}$$

has a solution in $\mathbb{Z}$, and any two solutions are congruent modulo $n := n_1 \cdots n_k$. Indeed, since the map from $\mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ taking $r \in \mathbb{Z}$ to $(r + n_1\mathbb{Z}, \ldots, r + n_k\mathbb{Z})$ is surjective, a solution to the system of congruences is any element $t \in \mathbb{Z}$ that maps to $(a_1 + n_1\mathbb{Z}, \ldots, a_k + n_k\mathbb{Z})$, while uniqueness of solutions up to congruence modulo n follows because the map is injective.

7. Assume that R has a *unique* maximal ideal P and let A be an Artinian R-module. For $p \in P$ and $x \in A$, prove there exists $n \geq 1$ such that $p^nx = 0$. Conclude that if P is finitely generated (e.g., R is Noetherian), then for each $x \in A$, there exists $r \geq 1$ (depending on x) such that $P^rx = 0$.

Solution. For $x \in A$ and $p \in P$, we have a descending sequence of submodules $\langle px\rangle \supseteq \langle p^2x\rangle \supseteq \cdots$, and hence there is $n \geq 1$ such that $\langle p^nx\rangle = \langle p^{n+1}x\rangle$. It follows that $p^nx = rp^{n+1}x$, for some $r \in R$. Thus, $(1 - rp)p^nx = 0$. However, since P is the only maximal ideal of R, and $1 - rp \notin P$, we have that $1 - rp$ is a unit. Thus, cancelling this unit, we have $p^nx = 0$, for some n.

Now suppose $P = \langle p_1, \ldots, p_c\rangle$ is finitely generated. Fix $x \in A$. Then for each i we have $p_i^{n_i}x = 0$, for some $n_1, \ldots, n_c \geq 1$. If we set $N = \max\{n_1, \ldots, n_c\}$, we have $\langle p_1^N, \ldots, p_c^N\rangle x = 0$. By the pigeonhole principle, for $r >> 0$, $P^r \subseteq \langle p_1^N, \ldots, p_c^N\rangle$, giving $P^rx = 0$.

8. Let R be an Artinian ring.

(i) Prove that R has finitely many maximal ideals.
(ii) Let J denote the Jacobson radical. Prove that $J^n = 0$, for some $n \geq 1$.
(iii) Suppose R has one maximal ideal P satisfying $P^n = 0$, for some $n \geq 1$. Show that R is Noetherian.

Solution. Suppose there are infinitely many distinct maximal ideals of R, say $P_1, P_2, \ldots$. Then we have a descending chain of ideals $P_1 \supseteq P_1 \cap P_2 \supseteq \cdots$. Thus, for some $n \geq 1$, $P_1 \cap \cdots \cap P_n = P_1 \cap \cdots \cap P_n \cap P_{n+1}$. It follows that $P_1 \cap \cdots \cap P_n \subseteq P_{n+1}$. Since P_{n+1} is a prime ideal, we have $P_i \subseteq P_{n+1}$, for some $1 \leq i \leq n$. Since P_{n+1} is a maximal ideal, we have the contradiction $P_i = P_{n+1}$. Thus, R has finitely many maximal ideals.

For (ii), on the one hand, since R is Artinian, there exists $n_0 \geq 1$ such that $J^n = J^{n+1}$, for all $n \geq n_0$, since $J \supseteq J^2 \supseteq \cdots$. On the other hand, suppose $J^n \neq 0$. Then there exists $x_1 \in J^n$ such that $x_1J^n \neq 0$, since if $x_1J^n = 0$ for all $x_1 \in J^n$, $J^nJ^n = J^{2n} = J^n = 0$, a contradiction. Now choose $x_2 \in J^n$ such that $x_1x_2J^n \neq 0$. We can do

this, otherwise, $x_1x_2J^n = 0$ for all $x_2 \in J^n$, and thus $0 = x_1J^nJ^n = x_1J^n = 0$, contradicting the choice of x_1. Thus, inductively, we can find $x_1, x_2, \ldots, \in J^n$,, such that for all $c \geq 1$, $x_1 \cdots x_cJ^n \neq 0$. Now, the descending chain $\langle x_1 \rangle \supseteq \langle x_1x_2 \rangle \supseteq \cdots$ must stabilize. Thus, for some $e \geq 1$, we can write $x_1 \cdots x_e = rx_1 \cdots x_ex_{e+1}$, for some $r \in R$. Thus, $(1 - rx_{e+1})x_1 \cdots x_e = 0$. Since $x_{e+1} \in J$, $1 - rx_{e+1}$ is a unit. Thus, $x_1 \cdots x_e = 0$, a contradiction. Therefore, we must have $J^n = 0$, as required.

For (iii), we use the fact that if V is a vector space over the field F, then V is finite dimensional if and only if V is an Artinian F-module if and only if V is a Noetherian F-module. We now proceed by induction on r, to show that R/P^r is Noetherian for all $r \geq 1$. Since $P^n = 0$, it follows that R is a Noetherian ring. To proceed, if $r = 1$, then $F := R/P$ is a field and thus Noetherian. Now suppose R/P^r is a Noetherian ring. Then R/P^r is also a Noetherian R-module. Consider the natural exact sequence of R-modules:

$$0 \to P^r/P^{r+1} \to R/P^{r+1} \to R/P^n \to 0.$$

Since $P \cdot (P^r/P^{r+1}) = 0$, P^r/P^{r+1} is a vector space over F and its subspace structure as a vector space over F is the same as its submodule structure as an R-module, by Problem 1 (iv). Now, R is Artinian, and hence R/P^{r+1} is an Artinian R-module, and hence its submodule P^r/P^{r+1} is an Artinian R-module, and therefore an Artinian R/P-module, i.e., a finite dimensional vector space over F. Thus, P^r/P^{r+1} is a Noetherian R/P-module, and hence a Noetherian R-module. The induction hypothesis, together with the exact sequence above (and a theorem from class) give R/P^{r+1} is a Noetherian R-modules, and hence a Noetherian ring. Thus, R/P^r is Noetherian for all r, which is what we want. □.

9. Prove that an Artinian ring is Noetherian.[2].

Solution. Suppose R is an Artnian ring. Let $J \subseteq R$ be the Jacobson and $P_1, \ldots, P_k$ be the maximal ideals of R, which are finite in number, by Problem 8. For all $r \geq 1$, $P_1^r, \ldots, P_k^r$ are pairwise co-maximal, so that

$$J^r = P_1^r \cdots P_k^r = P_1^r \cap \cdots \cap P_k^r,$$

for all $r \geq 1$ (see the comments below). By Problem 8 (ii), we have $J^n = 0$, for some $n \geq 1$. Thus, as R-modules, we have

$$R \cong R/J^n \cong R/(P_1^r \cap \cdots \cap p_k^r) \cong R/P_1^r \oplus \cdots \oplus R/P_k^r,$$

where the third isomorphism follows by the Chinese remainder theorem. It now follows from Problem 6 and induction on k that each R/P_i^r is an Artinian R-module, and hence an Artinian ring. Suppose $Q \subseteq R/P_i^r$ is a maximal ideal. Then $Q = P/P_i^r$, for a maximal ideal $P \subseteq R$ containing P_i^r, by the correspondence theorem. Since P is prime, $P_i \subseteq P$, and since P_i is maximal, $P = P_i$. Thus, P_i/P_i^r is the only maximal ideal of R/P_i^r and $(P_i/P_i^r)^r = 0$. Thus, by Problem 8 (iii), R/P_i^r is a Noetherian ring, and hence a Noetherian R-module, for each $1 \leq i \leq k$. It follows that $R \cong R/P_1^r \oplus \cdots \oplus R/P_k^r$ is a Noetherian R-module, and hence a Noetherian ring. □

10. Follow the steps below to prove Hilbert's Basis Theorem: If R is a Noetherian ring, then the polynomial ring $R[x]$ is a Noetherian ring. To begin, let $J \subseteq R[x]$ be an ideal and $I := \{a \in R \mid a \text{ is the leading coefficient of some element of } J\}$.

(i) Show that I is an ideal of R.

Suppose $I := \langle a_1, \ldots, a_r \rangle$ and let $f_1(x), \ldots, f_r(x) \in J$ be such that the leading coefficient of $f_i(x)$ is a_i. Set $N := \max\{\text{degree}(f_i(x))\}$. Let F denote the free R-module generated by $1, x, \ldots, x^{N-1}$ and set $M := J \cap F$.

(ii) Show that M is an R-submodule of F and conclude that M is a finitely generated R-module.

(iii) Let $g_1(x), \ldots, g_t(x)$ generate M as an R-module. Prove that J is generated by $f_1(x), \ldots, f_r(x), g_1(x), \ldots, g_t(x)$. Hint: Show that if $h(x) \in J$ and $h(x)$ has degree greater than or equal to N, the there exist $d_1(x), \ldots, d_r(x)$ in $R[x]$ such that $h(x) - \{d_1(x)f_1(x) + \cdots + d_r(x)f_r(x)\}$ belongs to J and has degree strictly less than the degree of $h(x)$.

Solution. For(i), suppose $a, b \in I$. Then there exist $f(x) := ax^n + \cdots$ and $g := bx^m + \cdots$ in J. Suppose $n \geq m$. Then $f(x) + x^{n-m}g(x) = (a + b)x^n + \cdots$ belongs to J, and thus, $a + b \in I$. Moreover, if $r \in R$, $rf(x) = rax^n + \cdots$ belongs to J, and thus $ra \in I$. Therefore I is an ideal.

For (ii), suppose $f(x), g(x) \in M$. Then $f(x), g(x)$ belong to J and have degree less than N. Thus, the sum $f(x) + g(x) \in J$ and has degree less than N. In other words, $f(x) + g(x) \in M$. In addition, for any $r \in R$, $rf(x) \in J$ and has degree less than N, showing that M is a submodule of F. Since F is Noetherian (it's finitely generated over the Noetherian ring R), M is Noetherian, and hence finitely generated as an R-module.

For (iii), write L for the ideal of $R[x]$ generated by $f_1(x), \ldots, f_r(x), g_1(x), \ldots, g_c(x)$. Clearly, $L \subseteq J$. Take $h(x) \in J$. If $h(x)$ has degree less than N, then $h(x) \in M$, so that $h(x)$ is a finite R-linear combination of $g_1(x), \ldots, g_c(x)$, and

[2]This theorem is also true for non-commutative rings. Hopkins' Theorem states that a left (or right) Artinian ring is left (or right) Noetherian

hence $h(x) \in L$. Suppose $e := \deg(h(x)) \geq N$. We prove by induction on e that $h(x) \in L$. The argument for the base case $e = N$ is the same as for the inductive step, so assume $e > N$. Write $h(x) = bx^e + \cdots$. Then $b \in I$, so we can write $b = u_1a_1 + \cdots + u_ra_r$, for $u_j \in R$. For $1 \leq i \leq r$, set $n_i := \deg(f_i(x))$. Then the polynomial

$$h(x) - \{u_1x^{e-n_1}f_1(x) + \cdots + u_rx^{e-n_r}f_r(x)\}$$

belongs to J and has degree strictly less than e. Thus, by induction on e, $h(x) - \{u_1x^{e-n_1}f_1(x) + \cdots + u_rx^{e-n_r}f_r(x)\}$ is in L. It follows readily that $h(x) \in L$, giving $L \subseteq J$. Thus, $L = J$ and J is finitely generated. Therefore, $R[x]$ is Noetherian. □

Comments on the Chinese Remainder theorem. Throughout these comments $I, J \subseteq R$ are ideals.

(i) $I, J \subseteq R$ are said to be be co-maximal if there is no maximal ideal of R containing both I and J. Since every ideal of R is contained in a maximal ideal, this is equivalent to the condition $I + J = R$, which in turn is equivalent to $i + j = 1$, for some $i \in I$ and $j \in J$.

(ii). Suppose I and J are co-maximal, and $x \in I \cap J$. Write $1 = i + j$, for $i \in I$ and $j \in J$. Then $x = xi + xj \in IJ$. Thus, $I \cap J \subseteq IJ$. Since $IJ \subseteq I \cap J$ always holds, we have that if I and J are co-maximal, then $I \cap J = IJ$.

(iii) Suppose that I and J are co-maximal. Define $\phi : R \to (R/I) \oplus (R/J)$, by $\phi(r) = (r + I, r + J)$. It is easy to check that ϕ is a ring homomorphism. Clearly, $I \cap J$ is the kernel of ϕ. Now suppose $(a + I, b + J) \in (R/I) \oplus (R/J)$. Take $i \in I$ and $j \in J$ such that $i + j = 1$. Then $ai + aj = a$, so that $a + I = aj + I$. Similarly, $bi + bj = b$, so that $b + J = bi + J$. It follows that $\phi(aj + bi) = (aj + bi + I, aj + bi + J) = (aj + I, bi + J) = (a + I, b + J)$, so that ϕ is surjective. Thus, we have $R/(I \cap J) \cong (R/I) \oplus (R/J)$. This also yields $R/IJ \cong (R/I) \oplus (R/J)$.

(iv) Ideals $I_1, \ldots, I_k$ are pairwise co-maximal, if for each $1 \leq i \neq j \leq k$, I_i and I_j are co-maximal. Given (iii) above, one can show via induction on k, that if $I_1, \ldots, I_k$ are co-maximal, then $R/(I_1 \cap \cdots \cap I_k) \cong (R/I_1) \oplus \cdots \oplus (R/I_k)$. Indeed, since I_1 and $I_2 \cap \cdots \cap I_k$ are comaximal, we have

$$R/(I_1 \cap \cdots \cap I_k) = R/(I_1 \cap (I_2 \cap \cdots \cap I_k)) \cong (R/I_1) \oplus (R/(I_2 \cap \cdots \cap I_k)) \cong (R/I_1) \oplus (R/I_2) \oplus \cdots \oplus (R/I_k).$$

(v) The modern version of the classical version of the Chinese remainder theorem take the following form. Suppose $n_1, \ldots, n_k$ are pairwise relatively prime positive integers. Set $n := n_1 \cdots n_k$. Then $\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

(vi) The classical form of the Chinese remainder theorem states the following: Suppose $n_1, \ldots, n_k$ are pairwise relatively prime positive integers. Then, given $a_1, \ldots, a_k \in \mathbb{Z}$, the system of congruences

$$x \equiv a_1 \pmod{n_1\mathbb{Z}}, \ldots, x \equiv a_k \pmod{n_k\mathbb{Z}}$$

has a solution in $\mathbb{Z}$, and any two solutions are congruent modulo $n := n_1 \cdots n_k$. Indeed, since the map from $\mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ taking $r \in \mathbb{Z}$ to $(r + n_1\mathbb{Z}, \ldots, r + n_k\mathbb{Z})$ is surjective, a solution to the system of congruences is any element $t \in \mathbb{Z}$ that maps to $(a_1 + n_1\mathbb{Z}, \ldots, a_k + n_k\mathbb{Z})$, while uniqueness of solutions up to congruence modulo n follows because the map is injective.