ALGEBRA HOMEWORK SET IV SOLUTIONS

JAMES CUMMINGS

(1) (a) (internal sum) Prove that if M_1 and M_2 are submodules of an R-module M, then the submodule generated by $M_1 \cup M_2$ is

$$M_1 + M_2 = \{m_1 + m_2 : m_i \in M_i\}.$$

Easy! Just check its a submodule, and note that any submodule which contains $M_1 \cup M_2$ is closed under sums so contains it.

(b) (external direct sum) Prove that if M_1 and M_2 are R-modules and we define operations on

$$M_1 \oplus M_2 = \{(m_1, m_2) : m_i \in M_I\}$$

by $r(m_1, m_2) = (rm_1, rm_2)$, $(m_1, m_2) + (n_1, n_2) = (m_1 + n_1, m_2 + n_2)$ then the resulting structure is an R-module.
Routine.

(c) (internal direct sum) Prove that if $M_1, M_2 \leq M$ and $M_1 \cap M_2 = 0$ then $M_1 + M_2 \simeq M_1 \oplus M_2$. What can you say about the structure of $M_1 + M_2$ in general?
Define $\phi : (m_1, m_2) \mapsto m_1 + m_2$. Easily it's a surjective HM (an *epimorphism*). The kernel is the set of pairs with $m_1 + m_2 = 0$, but then $m_1 = -m_2 \in M_1 \cap M_2 = 0$, so the kernel is trivial. In general the same argument shows that $M_1 + M_2$ is isomorphic to the quotient of $M_1 \oplus M_2$ by a submodule isomorphic to $M_1 \cap M_2$.

(2) Let M be an R-module and I an ideal of R. Prove that

(a) If we define IM to be the set of all finite sums $\sum_i r_i m_i$ with $r_i \in I, m_i \in M$ then $IM \leq M$.
Routine!

(b) M/IM has the structure of an R/I module if we define $(r + I)(m + IM) = rm + IM$.
Routine, the main point is that this is well defined (in fact IM is the smallest submodule that makes the quotient have an R/I-module structure).

(3) Consider a sequence of R-modules M_i where the index i runs through some interval of integers, together with R-module HMs $\alpha_i : M_i \to M_{i+1}$. The sequence is said to be *exact at* M_i if $im(\alpha_{i-1}) = ker(\alpha_i)$.

(a) Show that $0 \to M_1 \to M_2$ is exact at M_1 iff α_1 is injective.
α_1 is injective iff the kernel of α_1 is 0 iff the kernel of α_1 is the image of α_0.

(b) Show that $M_1 \to M_2 \to 0$ is exact at M_2 iff α_1 is surjective.
α_1 is surjective iff the image of α_1 is M_2 iff the image of α_1 is the kernel of α_2.

(c) When is the sequence $0 \to M_1 \to M_2 \to 0$ exact at both of M_1, M_2?
By the above, this happens iff $\alpha_1 : M_1 \simeq M_2$.

(d) Suppose that $0 \to M_1 \to M_2 \to M_3 \to 0$ is exact at all of M_1, M_2, M_3. What does this tell you about the relation between the modules M_i?
Let $N \leq M_2$ be the image of α_1. Then N is the kernel of α_2, and is isomorphic to M_1. Also $M_3 \simeq M_2/N$. So this sequence is a slick description of the quotient construction in diagrammatic form.

(4) Recall that when R is an ID we defined the *field of fractions* by considering the set $X = \{(r,s) : r \in R, s \in R \setminus \{0\}\}$ and introducing an equivalence relation $(r_1,s_1) \simeq (r_2,s_2)$ iff $r_1 s_2 \simeq r_2 s_1$.

(a) Show by example that if R is not an ID then the binary relation defined in this way may not be an equivalence relation.
Easy (look at the proof that it is an ER when R is an ID if you are stuck)

(b) Let R be an arbitrary ring. A subset $S \subseteq R$ is called *multiplicatively closed* iff $1 \in S$ and S is closed under multiplication.
Prove that if we define a relation on $R \times S$ by $(r_1,s_1) \simeq^* (r_2,s_2)$ iff there is $s_3 \in S$ such that $s_3(r_1 s_2 - r_2 s_1) = 0$ then $\simeq^*$ is an equivalence relation.
Easy!
What is this in the case when R is an ID and $S = R \setminus \{0\}$?
It reduces to the old ER in this case.

(c) With the same assumptions as the last part, we write r/s for the $\simeq^*$-class of the pair (r,s) and RS^{-1} for the set of such classes. Prove that if we attempt to define

$$r_1/s_1 \times r_2/s_2 = (r_1 r_2)/(s_1 s_2), r_1/s_1 + r_2/s_2 = (r_1 s_2 + r_2 s_1)/(s_1 s_2),$$

then we get well-defined operation which make RS^{-1} into a ring.
Routine and very very dull.

(d) Prove that the map $r \mapsto r/1$ is a HM from R to RS^{-1}, and that every element of S is mapped to a unit in RS^{-1}. When is the map injective? When is it surjective?
The defn of the ring structure ensures that it's a HM. We have explicitly added an inverse $1/s$ for each element $s/1$ in the image of S.
Now we analyse the kernel. r is in the kernel iff $r/1 = 0/1$ iff there is $s \in S$ such that $sr = 0$. So the map is injective iff S does not contain zero divisors.
As for surjectivity, that amounts to the assertion that for all $r \in R$ and $s \in S$ there is $r_1 \in R$ such that $r_1/1 = r/s$, that is to say that for some $s_1 \in S$ we have $s_1(r - s r_1) = 0$.

(5) Let R be a ring and let $Spec(R)$ be the set of prime ideals of R. For each ring element a, let $O_a = \{P \in Spec(R) : a \notin P\}$. Say that a set X of prime ideals is *open* if for every $P \in X$ there exists a such that $P \in O_a \subseteq X$.

(a) Prove that $O_a \cap O_b = O_{ab}$, $O_0 = \emptyset$, $O_1 = Spec(R)$.
For a prime ideal P, $ab \in P$ iff $a \in P$ or $b \in P$. So $ab \notin P$ iff $a \notin P$ and $b \notin P$. Every prime ideal contains 0 and no prime ideal contains 1.

(b) Prove that the collection of open sets form a topology for $Spec(R)$, and describe it when $R = \mathbb{Z}$.
The properties of the O_a listed above make this easy, in fact they form a basis for this *Zariski topology*. Now the prime ideals of $\mathbb{Z}$ are (0) and

(p) for p prime. When n is nonzero and composite we see that O_n is the cofinite set of ideals (p) for p not dividing n together with the ideal (0). So the open sets are $\emptyset$ and all cofinite sets of prime ideals which contain (0).

(c) (Trickier) Prove that this topology is compact.
We need to show that any open cover has a finite subcover. Enough to show that any cover by sets of form O_a has a finite subcover. So let O_a for $a \in X$ be a cover. This means that every prime ideal is in O_a for some $a \in X$, that is no prime ideal contains X, that is no prime ideal contains the ideal generated by X. But any proper ideal extends to a maximal (hence prime) ideal so X generates R. Hence a finite subset of X generates R, and from this we read off an open subcover.

(6) Let p be prime. Let $R_n = \mathbb{Z}/p^n\mathbb{Z}$, and let $\pi_n : R_{n+1} \mapsto R_n$ be the surjective HM which maps $a + p^{n+1}\mathbb{Z}$ to $a + p^n\mathbb{Z}$. Define a ring $\mathbb{Z}_p$ as follows: the elements are infinite sequences $(r_0, r_1, \ldots)$ such that $r_i \in R_i$ and $\pi_i(r_{i+1}) = r_i$ for all i. Addition are multiplication are defined coordinatewise
Prove that

(a) $\mathbb{Z}_p$ is uncountable.
Diagonalise a la Cantor.

(b) $\mathbb{Z}_p$ is an ID which contains an isomorphic copy of $\mathbb{Z}$.
Routine.

(c) The sequence $(2, 2, 2, \ldots)$ has a square root in $\mathbb{Z}_7$.

Build a square root by induction, starting either with $r_0 = 3$ or $r_0 = 4$. At stage n suppose we have $r_n^2 = 2 \mod p^n$. Then we must choose $r_{n+1} = r_n + xp^n$ so that $r_{n+1}^2 = 2 \mod p^{n+1}$. This is an easy problem in mod p arithmetic.

Cultural note: this is the ring of *p-adic integers* and we just did an easy example of *Hensel's Lemma*.

(7) The R-module M is said to be *Artinian* iff there is no infinite strictly decreasing sequence of submodules. R is *Artinian* iff it is Artinian as an R-module, that is there is no infinite strictly decreasing sequence of ideals.

(a) Give an example of an infinite Artinian ring.
Any field.

(b) Prove that if R is a field, the classes of Artinian and Noetherian modules coincide.
Using basic facts about dimension, both classes coincide with the class of finite dimensional R-modules.

(c) Give an example of a Noetherian module which is not Artinian.
$\mathbb{Z}$ is Noetherian but not Artinian.

(d) Give an example of a Artinian module which is not Noetherian.
We work with $\mathbb{Z}$-modules, that is abelian groups. Consider the subgroup of $\mathbb{Q}/\mathbb{Z}$ consisting of elements of form $a/2^n$ for integers a, n where $n \geq 0$. Easily the subgroups generated by $1/2^n$ form an infinite strict increasing chain.
Let H be any subgroup, let $h \in H$ and write $h = a/2^n$ for a odd. So $gcd(a, 2^n) = 1$, and by elementary number theory there are integers C, D with $Ca + D2^n = 1$, that is $Ca/2^n + D = 1/2^n$. So easily H contains the subgroup generated by $1/2^n$. Therefore either H is

generated by $1/2^n$ for some n or it's the whole group. It follows easily that the group is Artinian as a $\mathbb{Z}$-module.

Note: all Artinian rings are Noetherian, but it is not completely easy to see this.