MATH 8211 Homework

David DeMark

Fall 2017

Collaborators

Andy Hardt, Galen Dorpalen-Berry, Esther Bannian

Notation and other conventions

We standardize the following notational and mathematical conventions for use throughout this document.

- For L some indexing set, R a commutative ring and any subset $S = \{r_\ell : \ell \in L\} \subset R$, we denote the ideal $I = \sum_{\ell \in L} r_\ell R$ as any of $I = \langle S \rangle$, (in the case $|S| = s < \infty$) $I = \langle r_1, \ldots, r_s \rangle$, or (in a possible slight abuse of notation) $I = \langle r_\ell : \ell \in L \rangle$.
- We let $\mathcal{I}$ denote the (canonical) functor mapping algebraic sets to their associated ideal, and $\mathcal{Z}$ denote the (canonical) functor mapping ideals to their associated algebraic set.

  are these actual functors

- We shall attempt to remind the reader of this each time we introduce one, but unless *explicitly* stated otherwise, all power series may be assumed to be **formal** power series over whichever field or ring the coefficients are said to reside in (which we shall be more precise about).

1.)

Theorem (Eisenbud, problem 1.1)**.** *We let M be an R-module. The following are equivalent:*

(i) *Any submodule of M is finitely generated (i.e. M is Noetherian).*

(ii) *M satisfies the ascending chain condition.*

(iii) *Every set of submodules of M contains maximal elements under inclusion.*

(iv) *Given a sequence $f_1, f_2, \ldots$ of elements in M, there exists some $m > 0$ such that for all $n > m$, there exits an expression $f_n = \sum_{i=1}^{m} a_i f_i$ with $a_i \in R$.*

Proof.

(i) $\Longrightarrow$ *(ii)* We suppose M is Noetherian, and let $0 = M_0 \subset M_1 \subset M_2 \subset \ldots$ be an ascending chain of submodules. Then, $N = \bigcup_{i=1}^{\infty} M_i$ is a submodule of M and hence has a finite generating set, i.e. can be written $N = \langle f_1, f_2 \ldots, f_k \rangle$. We let $m_j = \inf_{i \geq 0}\{i : f_j \in M_i\}$ and let $m = \sup_{1 \leq j \leq}\{m_1, \ldots, m_k\}$. As $[k]$ is a finite set, we have that m is finite, and contains each of $f_1, \ldots, f_k$ and thus $M_n = M_m$ for all $n \geq m$.

(ii) $\Longrightarrow$ *(iii)* We let $\mathcal{A} = \{M_\alpha\}_{\alpha \in A}$ be a set of submodules of M and have that any chain contained within $\mathcal{A}$ is finite and hence contains its own upper bound by the ascending chain condition. Thus, We may apply Zorn's lemma to yield the desired result.

(iii) $\Longrightarrow$ *(iv)* We let $M_i = \langle f_1, \ldots, f_i \rangle$ for any $i \geq 1$. Then, condition *(iii)* implies that $\{M_i\}$ contains some maximal element M_m, and as the M_i form an ascending chain, we have that such a maximal element is unique up to isomorphism. Thus, we have that $\langle f_1, \ldots \rangle = \langle f_1, \ldots f_m \rangle = M_k$, and thus $f_n \in M_k$ for any $n > m$.

(iv) $\implies$ *(i)* We let $N \subset M$ be a submodule and suppose for the sake of contradiction it is not finitely generated. We let $F = \{f_\alpha\}_{\alpha \in A}$ be a generating set and note that for any finite subset S of F, there exists some element $f \in F \setminus S$ such that $f \notin R\{S\}$. Thus, we may choose some $\{f_1, f_2 \ldots, \}$ such that for all $i > 0$, $f_{i+1} \notin \langle f_1, \ldots, f_i \rangle$, contradicting statement *(iv).*

□

2.)

Prompt (Eisenbud, problem 1.13)**.** *Let R be a commutative ring and I an ideal of R. Show that* (i) *if* rad I *is finitely generated, then there exists some N such that* (rad $I)^N \subset I$. *Conclude that* (ii) *if R is Noetherian, then two ideals I, J have the same radical if and only if there is some N for which $I^N \subset J$ and $J^N \subset I$. Use the Nullstellensatz to deduce that* (iii) *for $I, J \subset S = k[x_1, \ldots, x_r]$ ideals with k algebraically closed, then $\mathcal{Z}(I) = \mathcal{Z}(J)$ iff $I^N \subset J$ and $J^N \subset I$ for some N.*

Proof. *(i)* In general, for an ideal $J \subset R$ where R is a commutative ring, J^m is the R-submodule of J consisting of R-linear combinations of elements of the form $a_1 a_2 \ldots a_m$ where $a_i \in J$. We suppose $J = \langle f_1, \ldots, f_r \rangle$. Then, $J^m = \langle f_1^{e_1} f_2^{e_2} \ldots f_r^{e_r} \;:\; \sum_i e_i = m \rangle$. Letting $J = \text{rad } I$, we let $m_i = \min\{m : f_i^m \in I\}$, and let $N = \sum_i m_i$. Then, by a generalization of the pigeonhole principle, we have that any monomial α in $f_1, \ldots, f_r$ of total degree $\geq N$ must in any presentation of the form $\alpha = r f_1^{e_1} \ldots f_r^{e_r}$ have some index ℓ such that $e_\ell \geq m_\ell$. Then, letting $r' = r f_\ell^{e_\ell - m_\ell} \prod_{i \neq \ell} f_i^{e_i}$, we have that $\alpha = r' f_\ell^{m_\ell} \in I$. As (rad $I)^N$ is generated as an R-module by such monomials, we have that (rad $I)^N \subset I$.

(ii) We assume R to be Noetherian and will use frequently and possibly without explicit mention that for any ideal $L \subset R$, L is finitely generated.
($\implies$) We suppose $I, J \subset R$ are ideals and rad I = rad $J = L$. We then have from statement *(i)* that there exist $m, n \in \mathbb{N}$ such that $L^m \subset I$ and $L^n \subset J$. Noting that for any ideal $Q \subset R$, $Q^k \subset Q^j$ if $k > j$, we let $N = \max\{m, n\}$ and have that (as $I, J \subset L$) $J^N \subset L^N \subset L^m \subset I$ and $I^N \subset L^N \subset L^n \subset J$.
($\impliedby$) We suppose there exists some N such that $I^N \subset J$ and $J^N \subset I$. We let $x \in$ rad I be arbitrary and let $m \in \mathbb{N}$ be such that $x^m \in I$. Then, $x^{mN} = (x^m)^N \in I^N \subset J$, so $x \in$ rad J. As x was arbitrary, we now have that rad $I \subset$ rad J and by symmetry, rad $J \subset$ rad I. Thus, rad J = rad I.

(iii) We suppose $\mathcal{Z}(I) = \mathcal{Z}(J)$. The Nullstellensatz then states that this is equivalent to the statement rad $I = \mathcal{I}(\mathcal{Z}(I)) = \mathcal{I}(\mathcal{Z}(J))) =$ rad J. Then, by part *(ii)*, we have that this is in turn equivalent to the existence of some N such that $I^N \subset J$ and $J^N \subset I$. This completes our proof.

□

3.)

b.)

Proposition (Eisenbud, problem 1.24)**.** *We let $\mathbb{A}^1_k$ be the affine line of $k = \overline{k}$. Then, the only proper open sets of $\mathbb{A}^1_k$ are co-finite.*

Proof. We let $A := k[t]$. We shall prove an (obviously) equivalent statement: all closed sets are finite. We recall that the closed sets of $\mathbb{A}^1_k$ are those of the form $V(E)$ where E is an A-ideal. As $A = k[t]$ is a principal ideal domain, we have that $E = \langle a \rangle$ for some $a \in A$. As A is factorial as well, we have that $a = p_1 p_2 \ldots p_k$ where each p_i is prime in A. Thus, as all prime ideals in A are generated by a single prime element, the only prime ideals to contain a (and hence E) are those generated by the k primes p_i, so $V(E) = \{\langle p_1 \rangle, \langle p_2 \rangle \ldots, \langle p_k \rangle\}$, which is a finite set. □

Proposition. *The Zariski topology on $\mathbb{A}^n_k$ is not the product topology, even when $n = 2$.*

Proof. We note as $k = \overline{k}$, $|k| = \infty$. We note that[1] as a set, $\mathbb{A}^n_k$ may be identified with $(\mathbb{A}^1_k)^n$ and in turn with k^n. By the first proposition of this part, we have that a closed basis for the product topology on $(\mathbb{A}^1_k)^n$ is

[1] throwing out the generic point as far as I can tell. . .

given by finite collections of hyperplanes of dimension $0 \leq d \leq n$. In particular, letting $\pi_i : \mathbb{A}^n_k \to k$ be the ith coordinate projection map, we have that for any closed set V, V is infinite if and only if $\pi_i^{-1}(a)$ is infinite for some $i \in [n]$. We let $I = \langle t_i - t_j \ : \ i < j \rangle$. Then, $V(I) = \{(t_1, \dots, t_n) \ : \ t_i = t_j \ \forall i, j\}$, which is an infinite

still need to finish this oh god oh god oh god oh god

□

4.)

Prompt (Eisenbud, problem 2.4)**.** *For each of the following objects, describe their structures (as modules unless otherwise stated).*

- ***a.)*** (i) $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/m)$ *and* (ii) $\operatorname{Hom}_{k[x]}(k[x]/(x^n), k[x]/(x^m))$
- ***b.)*** (i) $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Z}/m$ *and* (ii) $k[x]/(x^n) \otimes_{k[x]} k[x]/(x^m)$
- ***c.)*** $k[x] \otimes_k k[x]$ *(as an algebra).*

a.)

Response.

(i) We recall that there exists an exact sequence $\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/n \to 0$, with the first map is the multiplication-by-n map $n\cdot$ and the second a quotient map. Then, there is an exact sequence $0 \to \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/m) \to \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/m) \to \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/m)$, where once again the final map is the multiplication-by-n map $(n\cdot)^*$. We recall that $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/m) \cong \mathbb{Z}/m$. Thus, $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/m)$ is isomorphic to the kernel of the map $n\cdot : \mathbb{Z}/m \to \mathbb{Z}/m$, that is $(\frac{\operatorname{lcm}(m,n)}{n})\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/\gcd(m,n)$.

(ii) We denote by $M := \operatorname{Hom}_{k[x]}(k[x]/(x^n), k[x]/(x^m))$. We consider the exact sequence $k[x] \to k[x] \to k[x]/(x^n) \to 0$, and have that it induces an exact sequence

$$0 \to M \to \operatorname{Hom}_{k[x]}(k[x], k[x]/(x^m)) \to \operatorname{Hom}_{k[x]}(k[x], k[x]/(x^m)).$$

We recall $\operatorname{Hom}_{k[x]}(k[x], k[x]/(x^m)) \cong k[x]/(x^m)$. Thus, $M \cong \ker(x^n\cdot : k[x]/(x^m) \to k[x]/(x^m)) \cong x^{\min(m-n,0)}k[x]/(x^m) \cong k[x]/(x^{\min(m,n)})$

□

b.)

Response.

(i) We recall that there exists an exact sequence $\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/n \to 0$, with the first map is the multiplication-by-n map $n\cdot$ and the second a quotient map. Then, there is an exact sequence $\mathbb{Z} \otimes \mathbb{Z}/m \to \mathbb{Z} \otimes \mathbb{Z}/m \to \mathbb{Z}/n \otimes \mathbb{Z}/m \to 0$. We recall $\mathbb{Z} \otimes \mathbb{Z}/m \cong \mathbb{Z}/m$. Thus, $\mathbb{Z}/n \otimes \mathbb{Z}/m \cong \operatorname{coker}(n\cdot : \mathbb{Z}/m \to \mathbb{Z}/m) \cong (\mathbb{Z}/m)/(n\mathbb{Z}/m) \cong \mathbb{Z}/\gcd(m,n)$.

(ii) Without loss of generality (by the isomorphism $A \otimes B \to B \otimes A$), we let $n \leq m$. Then, we have that there exists an exact sequence $k[x] \to k[x] \to k[x]/(x^n) \to 0$ inducing an exact sequence $k[x] \otimes k[x]/(x^m) \to k[x] \otimes k[x]/(x^m) \to k[x]/(x^n) \otimes k[x]/(x^m) \to 0$. We recall that $k[x] \otimes k[x]/(x^m) \cong k[x]/(x^m)$. Thus, $k[x]/(x^n) \otimes k[x]/(x^m) \cong \operatorname{coker}(x^n\cdot : k[x]/x^m \to k[x]/x^m) \cong (k[x]/x^m)/(x^n k[x]/x^m) \cong k[x]/x^n$. Thus, in general, $k[x]/(x^n) \otimes k[x]/(x^m) \cong k[x]/x^{\min(m,n)}$.

□

c.)

Response. We claim that $k[x] \otimes_k k[x] \cong k[x,y]$ by the map defined on homogenous generators $x^m \otimes x^n \mapsto x^m y^n$. Indeed, we see immediately that the map is surjective, as for any $f = \sum_{(m,n) \in \mathbb{N}^2} a_{mn} x^m y^n \in k[x,y]$, we have that $\sum_{(m,n)} a_{mn} x^m \otimes x^n \mapsto f$. To see injectivity, we let $\sum_{m,n} a_{mn} x^m \otimes x^n \mapsto 0$ and then have that $\sum_{m,n} a_{mn} x^m y^n = 0$, implying $a_{mn} = 0$ for all (m,n) by freeness of $k[x,y]$. Thus, our map is indeed an isomorphism. □

5.)

For reference, we restate the definition of ring localization by universal property here:

Definition 5.A. We let R be a ring and $U \subset R$ a multiplicative system. The ring $R[U^{-1}]$ is defined by the property that for any ring morphism $\phi : R \to S$ such that $\phi(U) \subset S^{\times}$, there exists a unique morphism $\phi' : R[U^{-1}] \to S$ which commutes with $\iota : R \to R[U^{-1}]$ such that the below diagram commutes:

$$\begin{tikzcd} R \arrow[rr, "\phi"] \arrow[dr, "\iota"'] & & S \\ & R[U^{-1}] \arrow[ur, dashed, "\exists!\ \phi'"'] & \end{tikzcd}$$

Proposition (Eisenbud, problem 2.7). *Ring localizations are unique, that is, for $R \to L$ fulfilling the property of Definition 5.A, there exists a unique isomorphism $R[U^{-1}] \to L$.*

Proof. We let $\iota : R \to R[U^{-1}]$, $\nu : R \to L$ fulfill the property of Definition 5.A. Then, we have that there is a unique map $\nu' : R[U^{-1}] \to L$ commuting with ι. By the same argument, there exists a unique map $\iota' : L \to R[U^{-1}]$ commuting with ν. In other words, we are in the situation of the below commutative diagram:

$$\begin{tikzcd} & R \arrow[dl, "\iota"'] \arrow[d, "\nu"] \arrow[dr, "\iota"] & \\ R[U^{-1}] \arrow[r, dashed, "\exists!\ \nu'"] & L \arrow[r, dashed, "\exists!\ \iota'"] & R[U^{-1}] \end{tikzcd}$$

We then have that the morphism $\iota' \circ \nu' : R[U^{-1}] \to R[U^{-1}]$ commutes with ι. However, Definition 5.A implies that only one such map exists, that is, the identity $\mathrm{id}_{R[U^{-1}]}$. Thus, we have that $\iota' \circ \nu' = \mathrm{id}_{R[U^{-1}]}$, and a symmetric argument shows $\nu' \circ \iota' = \mathrm{id}_L$. Thus, ν' and ι' are mutual inverses, and we have already observed that they uniquely commute with the monomorphisms ι, ν. This completes our proof. $\square$

6.)

Proposition (Eisenbud, problem 2.14). *We let R be a $\mathbb{Z}$-graded ring and $I \subset R$ an R-ideal. Then, I is homogenous iff for all $f \in I$, every homogenous component $f^{(j)} \in R_j$ of f is in I.*

Proof. ($\Longleftarrow$) Trivial: the union of the homogenous components of each element form a generating set.

($\Longrightarrow$) We let $f \in I$ be arbitrary and write $I = \langle g_i \rangle_{i \in I}$ for some indexing set I where all g_i are homogenous. We may then write $f = \sum_{i \in I} h_i g_i$ for $h_i \in R$ and where only finitely many h_i are nonzero. We decompose each h_i into homogenous components $h_i^{(j)}$ and now have $h_i = \sum_{j \in \mathbb{Z}} h_i^{(j)}$ where again for each i only finitely many $h_i^{(j)}$ are nonzero. Now, we may write:

$$\begin{aligned} f = \sum_{i \in I} h_i g_i &= \sum_{i \in I} \left(\sum_{j \in \mathbb{Z}} h_i^{(j)} \right) g_i \\ &= \sum_{(i,j) \in I \times \mathbb{Z}} h_i^{(j)} g_i \end{aligned}$$

We note that each term $h_i^{(j)} g_i$ is homogenous and an element of I. Thus, we may recover each $f^{(k)}$ by summing along terms $h_i^{(j)} g_i$ of degree k and have that $f^{(k)} \in I$. $\square$

7.)

a.)

Proposition (Eisenbud, problem 3.17a). *We let $k := \mathbb{Z}/2$ and $I := \langle x, y \rangle \subset k[x, y]/(x, y)^2$. Then, I is the union of three properly smaller ideals.*

Proof. We note that as $(x,y)^2$ consists of all elements whose homogenous components have degree ≥ 2 and the only nonzero degree-0 element is 1, we have that $\langle x\rangle = \{0,x\}$, $\langle y\rangle = \{0,y\}$ and $\langle x+y\rangle = \{0,x+y\}$. Direct computation once equipped with the above observations shows that $I=(x,y)=\{0,x,y,x+y\}$ and hence $I=\langle x\rangle\cup\langle y\rangle\cup\langle x+y\rangle$. $\square$

b.)

Proposition (Eisenbud, problem 3.17b)**.** *We let k be any field and $R := k[x,y]/\langle xy, y^2\rangle$. We define the R-ideals $I_1 := \langle x\rangle$, $I_2 := \langle y\rangle$, and $J := \langle x^2, y\rangle$. Then, the homogenous elements of J are contained in $I_1\cup I_2$ but $J\not\subset I_1$ and $J\not\subset I_2$.*

Proof. We compute the homogenous components of J explicitly by degree. In degree 1, we have one degree-1 generator and hence $J_1 = \{ry \ : \ r\in k\}\subset I_2$. In degree 2, we have one degree-2 generator x^2 and as $xy = y^2 = 0 \in R$, we have that there are no degree-2 elements of the type $g(x,y)y$. Thus, $J_2 = \{rx^2 \ : \ r\in k\}\subset I_1$. The same argument shows that all degree ≥ 2 elements with a factor of y in R are 0, and thus, $J_d = \{rx^d \ : \ r\in k\}\subset I_1$ for all $d\geq 2$. However, $y\notin I_1$ and $x^2\notin I_2$, so we have that $J\not\subset I_1$ and $J\not\subset I_2$. $\square$

8.)

Prompt (Eisenbud, problem 3.1)**.** *Identify the associated primes of any finitely generated $\mathbb{Z}$-module G in terms of the structure theorem for finitely generated Abelian groups.*

Response. By the aforementioned structure theorem,

$$G\cong \mathbb{Z}^{e_0}\oplus\left(\bigoplus_{i=1}^{n}\mathbb{Z}/p_i^{e_i}\right)$$

where each $e_i > 0$ for $i > 0$, $e_0\geq 0$, and the p_i are not necessarily distinct. Then, for any prime p, we have $\langle p\rangle\in \mathrm{Ass}_{\mathbb{Z}}(G)$ if and only if there exists some $g\in G$ such that $rp^kg = 0$ for some $k>0$, $r\in\mathbb{Z}$, but $mg\neq 0$ for any $m<rp^k$. Thus, g has order rp^k, which is possible if and only if p divides the order of the torsion group of G, which here is $\bigoplus_{i=1}^{n}\mathbb{Z}/p_i^{e_i}$. Thus, the full list of associated primes of G are (deleting any redundancies) $\{\langle p_1\rangle, \langle p_2\rangle,\ldots,\langle p_n\rangle\}$. $\square$

12.)

14.)

15.)

17.)

18.)

Proposition (Eisenbud, problem 1.21a)**.** *We let $F(n)$ be a function defined for significantly large integers n and*[2] *taking on values in $\mathbb{Q}$, and let $G(n) := F(n+1)-F(n)$. Then, $F(n)\in\mathbb{Q}[n]$ if and only if $G(n)\in\mathbb{Q}[n]$. Furthermore,* $\deg G = \deg F - 1$.

Proof. ($\Longrightarrow$) Trivial: we assume that $F\in\mathbb{Q}[n]$. Then, $F(n+1)$ is in $\mathbb{Q}[n]$ as well, with the same going for their difference $F(n+1)-F(n)$.

($\Longleftarrow$) We let N be some integer for which $F(n)$ is defined for all $n\geq N$. Then, for $n>N$, we have that

$$F(N)+\sum_{m=N}^{n-1}G(m) = F(N)+(F(N+1)-F(N))+(F(N+2)-F(N+1))+\ldots+(F(n)-F(n-1)) = F(n).$$

Thus, showing our desired result is equivalent to showing the following proposition:

[2] As Galen pointed out to me, this assumption seems to be necessary and is missing, as one can easily find silly counter-examples (e.g. $F(n) = 1+\pi$) without it.

Proposition 18.A. *For a polynomial $p(n) \in Q[n]$, we let $P(n) := \sum_{m=1}^{n-1} p(m)$. Then, $P(n) \in \mathbb{Q}[n]$, with* $\deg P = \deg p + 1$

In order to prove this, we shall start with the following lemma:

Lemma 18.B. *For a map $a : \mathbb{Z} \to \mathbb{Q}$, we let*

$$A(x) := \sum_{n \geq 0} a(n)x^n \in \mathbb{Q}[[x]].$$

Then, $a(n) \in \mathbb{Q}[n]$ and $\deg a = k$ if and only if $A(x)$ has a rational expression of the form

$$\frac{p(x)}{(1-x)^{k+1}}$$

where $p(x) \in \mathbb{Q}[x]$, $\deg p \leq k+1$, and $\gcd(p(x),(1-x)) = 1$.

Proof of Lemma 18.B. ($\Longrightarrow$) We shall first show our statement for $a(n) = n^k$ for $k \geq 0$. We recall the (xD) operator on $\mathbb{Q}[[x]]$ of [Wil06], which maps $R(x) \mapsto x(\frac{\mathrm{d}}{\mathrm{d}x}R(x))$. For $R(x) = \sum_{n \geq 0} a_n x^n$, we now have $(xD)(R(x)) = \sum_{n \geq 0} n a_n x^n$. Thus, letting $P_k(x) := \sum_{n \geq 0} n^k x^n$ we have that $P_k(x) = (xD)^n \left(\frac{1}{1-x}\right)$. We claim that $K(x)$ can be written $\frac{p_k(x)}{(1-x)^{k+1}}$ for some $p_k(x)$ with $\gcd(p_k(x),(1-x)) = 1$ and $\deg p_k \leq k$. We show this by induction. The case $k = 0$ is trivial, with $p_0(x) = 1$. For the inductive step, we suppose $P_{k-1}(x) = \frac{p_{k-1}(x)}{(1-x)^k}$ with $\deg p_{k-1} < k$ and $\gcd(p_{k-1},(1-x)) = 1$. Then,

$$\begin{aligned} P_k(x) &= (xD)(P_{k-1}(x)) \\ &= \frac{kxp_{k-1}(x)}{(1-x)^{k+1}} + \frac{xp'_{k-1}(x)}{(1-x)^k} \\ &= \frac{kxp_{k-1}(x) + x(1-x)p'_{k-1}(x)}{(1-x)^{k+1}} \end{aligned}$$

Direct inspection coupled with the reminders that (1) $p_{k-1}(x)$ and $(1-x)$ are assumed to be nonzero and coprime and (2) $\deg p_{k-1} < k$ and $\deg p'_{k-1} < k-1$ yields the claim in the case $a(n) = n^k$. To prove this direction in full, we let $a(n) = b_k n^k + b_{k-1}n^{k-1} + \ldots + b_0$. Then,

$$\begin{aligned} A(x) &= b_k P_k(x) + b_{k-1}P_{k-1}(x) + \ldots + b_0 \\ &= b_k \frac{p_k(x)}{(1-x)^{k+1}} + b_{k-1}\frac{p_{k-1}(x)}{(1-x)^k} + \ldots + b_0 \\ &= \frac{b_k p_k(x) + (1-x)b_{k-1}p_{k-1}(x) + \ldots + b_0(1-x)^{k+1}}{(1-x)^{k+1}} \end{aligned}$$

We note that the numerator is congruent to $b_k p_k(x) \neq 0$ modulo $(1-x)$, and it is clear from what we have established regarding the degrees of p_j that the degree of the numerator is at most $k+1$. This completes this direction of the proof.

($\Longleftarrow$) We recall that a standard stars-and-bars argument shows that

$$\frac{1}{(1-x)^{k+1}} = \sum_{n \geq 0} \binom{n+k}{k} x^n = \sum_{n \geq 0} \frac{(n+k)(n+k-1)(n+k-2)\ldots(n+1)}{k!}x^n$$

which indeed has coefficients given by $s_k(n) = \binom{n+k}{k} \in \mathbb{Q}[n]$. Moreover, this implies that for $0 \leq j \leq k$, $\frac{x^j}{(1-x)^{k+1}}$ has coefficients given by $s_k(n-j)$, which is still[3] an element of $\mathbb{Q}[n]$. We shall use this fact to prove

[3]There is one subtlety here which I'm shoving under the rug: for $j > k$, we have that the x^0 coefficient of $\frac{x^j}{(1-x)^{k+1}}$ is 0, which is *not* the value of $s_k(-j)$. Fortunately, as we shall see, our assumptions on the degree of $p(x)$ in the statement of Lemma 18.B as well as a trick we shall introduce shortly will take care of this and we shan't worry about it any further. We reserve the right to talk around this subtlety without explicitly mentioning it throughout the rest of this proof; the grader can check for theirself that it is successfully dodged.

this direction of our proposition as follows: we let $\gcd(p(x),(1-x))=1$ with $p(x)\in\mathbb{Q}[x]$ and $\deg p(x)\leq k+1$ and let $A(x)=\frac{p(x)}{(1-x)^{k+1}}$. We use the euclidean property of $\mathbb{Q}[x]$ to write $p(x)=a_0(1-x)^{k+1}+q(x)$ where $\deg q(x)\leq k$. Then, $A(x)=a_0+B(x)$, where $B(x)=\frac{q(x)}{(1-x)^{k+1}}$. We let $q(x)=b_kx^k+\ldots+b_0$. By our assumptions on $p(x)$, we have that at least some $b_j\neq 0$ and $\gcd(q(x),(1-x))=1$. Then, the coefficients of $B(x)$ are given by $\hat{a}(n)=\sum_{j=0}^k b_js_k(n-j)\in\mathbb{Q}[n]$ with $\deg\hat{a}\leq k$. To show that $\deg\hat{a}=k$, we note that when expanded, each term $s_k(n-j)$ has the same leading coefficient $n^k/k!$. Thus, we have that the n^k-coefficient of $\hat{a}(n)$ is $\left(\sum_{j=0}^k b_j\right)\frac{n^k}{k!}n^k=q(1)\frac{n^k}{k!}$. As $\gcd(q(x),(1-x))=1$ by assumption, we have that $q(1)\neq 0$. Thus, $\deg\hat{a}=k$. Letting $a(n)=\hat{a}(n)+a_0$, we now have that $a(n)\in\mathbb{Q}[n]$ with $\deg a=k$ and $A(x)=\sum_{n\geq 0}a(n)x^n$. This completes our proof. ■

Proof of Proposition 18.A. We state one more lemma, the proof of which is immediate and well-known:

Lemma 18.C. *We let $\{a_n\}$ be a sequence and let $s_n=\sum_{m=0}^{n-1}a_m$. Then,*

$$\sum_{n\geq 0}s_nx^n=\left(\frac{x}{1-x}\right)\left(\sum_{n\geq 0}a_nx^n\right)$$

We let $k:=\deg p$, $A(x)=\sum_{n\geq 0}p(n)x^n$ and $B(x)=\sum_{n\geq 0}P(n)x^n$. By the result of the forward direction of Lemma 18.B, we have that $A(x)=\frac{q(x)}{(1-x)^{k+1}}$ for some $q(x)\in\mathbb{Q}[x]$ with $\deg q\leq k+1$ and $\gcd(q,(1-x))=1$. Then, Lemma 18.C implies that

$$B(x)=\left(\frac{x}{1-x}\right)A(x)=\frac{xq(x)}{(1-x)^{k+1}}.$$

An application of the result of the converse direction of Lemma 18.B then implies that $P(n)\in\mathbb{Q}[n]$ with $\deg P=k+1$. ■

As we have already shown Proposition 18.A to imply the reverse direction of our original statement, this completes our proof. □

24.)

Proposition. *We let R be a ring, $x\in R$, M an R-module, and $\{M_i,\phi_{i,j}\}$ the direct system indexed by $\mathbb{N}$ and given by (1). Then, $\varinjlim M_i\cong M_x$ uniquely with the map $\psi_i: M_i\to M_x$ mapping $a\mapsto\frac{a}{x^i}$.*

$$M_0=M\xrightarrow{\cdot x}M_1=M\xrightarrow{\cdot x}M_2=M\xrightarrow{\cdot x}\cdots\tag{1}$$

Proof. We recall the following universal definition of the module $M[U^{-1}]$:

Definition 24.A (Eisenbud, problem 2.8[4])**.** We let $U\subset R$ be a multiplicative system. Then, $M[U^{-1}]$ is defined as follows: for any map $M\to N$ such that for all $u\in U$, $uN=N$, there exists a unique extension $M[U^{-1}]\to N$ of the map $M\to N$.

We let $\{\alpha_i: M_i\to\varinjlim M_i\}$ be the co-cone defining $\varinjlim M_i$. We shall show that the universal property definitions of each of M_x and $\varinjlim M_i$ establish a canonical isomorphism between the two.

We first check that equipping M_x with $\{\psi_i\}$ indeed establishes M_x as a co-cone for $\{M_i,\phi_{i,j}\}$. Indeed, it is immediately clear that each ψ_i is well-defined and R-linear, as it may be defined on generators then extended to the rest of M by linearity. We check that

$$\begin{aligned}(\psi_j\circ\phi_{i,j})(a)&=\psi_j(x^{j-i}a)\\&=\frac{x^{j-i}a}{x^j}\\&=\frac{a}{x^i}=\psi_i(a),\end{aligned}$$

[4] To the grader: I spoke with Christine and confirmed that it is indeed kosher to assume the result of this problem for the purposes of this problem set.

showing that the ψ_i do indeed commute with the maps $\phi_{i,j}$. Thus, there exists a unique map $\varinjlim M_i \to M_x$ by the universal property of the direct limit, as we illustrate in (2).

$$\begin{tikzcd}
M_i \arrow[rr, "\phi_{i,j}"] \arrow[dr, "\alpha_i"] \arrow[ddr, "\psi_i"'] & & M_j \arrow[dl, "\alpha_j"'] \arrow[ddl, "\psi_j"] \\
& \varinjlim M_i \arrow[d, dashed, "\exists!"] & \\
& M_x &
\end{tikzcd} \tag{2}$$

We now wish to show that $x\varinjlim M_i = \varinjlim M_i$. We recall that the map $\bigoplus_i \alpha_i : \bigoplus_i M_i \to \varinjlim M_i$ is surjective, and in particular $\varinjlim M_i$ is generated by elements of the form $\alpha_i(a)$. We consider the set $S = \{\alpha_i(a) \,:\, a \in M, i \in \mathbb{N}_0\}$; as $\varinjlim M = \langle S\rangle$, it follows that if $xS \supset S$, then as $x\varinjlim M_i \subseteq \varinjlim M = \langle S\rangle$, we must have $xM = M$. Indeed, we consider $\alpha_i(a) \in S$, and note that $x\alpha_{i+1}(a) = \alpha_{i+1}(xa) = \alpha_{i+1}(\phi_{i,i+1}(a))$. Thus, as $\varinjlim M_i$ is a co-cone, we have that $\alpha_{i+1}(\phi_{i,i+1}(a)) = \alpha_i(a)$. Thus, $S \subset xS$, and it follows that $\varinjlim M_i = x\varinjlim M_i$. Then, by definition 24.A, we have that there exists a unique map $M_x \to \varinjlim M_i$ extending each α_j; as M_x is a co-cone, it follows that $M_x \to \varinjlim M_i$ commutes with the $\phi_{i,j}$. We illustrate this in (3).

$$\begin{tikzcd}
M_i \arrow[rr, "\phi_{i,j}"] \arrow[dr, "\alpha_i"] \arrow[ddr, bend right, "\psi_i"'] & & M_j \arrow[dl, "\alpha_j"'] \arrow[ddl, bend left, "\psi_j"] \\
& \varinjlim M_i \arrow[d, dashed, bend left, "\exists!"] & \\
& M_x \arrow[u, dashed, bend left, "\exists!"] &
\end{tikzcd} \tag{3}$$

By the universality of the constructions of $\varinjlim M_i$ and M_x, the maps $\varinjlim M_i \to M_x$ and $M_x \to \varinjlim M_i$ are mutual isomorphisms commuting uniquely with the co-cone structure of each, as desired. $\square$

29.)

Proposition (Eisenbud, problem A3.13: "Schanuel's Lemma")**.** *We let $0 \to N_F \to F \to M \to 0$ and $0 \to N_G \to G \to M \to 0$ be exact sequences of R-modules with F and G projective. Then, $N_F \oplus G \cong \ker(F \oplus G \to M) \cong N_G \oplus F$.*

Proof. By symmetry, it is enough to show $N_F \oplus G \cong \ker(F \oplus G \to M)$. We let $K := \ker(F \oplus G \to M)$. We note that $F \hookrightarrow F \oplus G$ and as $N_F = \ker(F \to M)$ by exactness, we have that $N_F \hookrightarrow K$. We then have that the following diagram commutes with exact rows and columns wherever those rows/columns are populated with maps:

$$\begin{tikzcd}
& 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & N_F \arrow[r, hook] \arrow[d, hook] & F \arrow[r, two heads] \arrow[d, hook] & M \arrow[r] \arrow[d, "\parallel"] & 0 \\
0 \arrow[r] & K \arrow[r, hook] \arrow[d, two heads] & F \oplus G \arrow[r, two heads] \arrow[d, two heads] & M \arrow[r] \arrow[d] & 0 \\
& K/N_F \arrow[d] & G \arrow[d] & 0 & \\
& 0 & 0 & &
\end{tikzcd}$$

The snake lemma then states that there exists an exact sequence $0 \to K/N_F \to G \to 0$, so we have that $K/N_f \cong G$. We have that there exists a surjective map $q : K \twoheadrightarrow K/N_F$, so as we now have that K/N_F is projective, we have that there exists a map $r : K/N_F \to K$ such that $q \circ r = \mathrm{id}_{K/N_F}$. Thus, we now have that $K \cong (K/N_F) \oplus N_F \cong G \oplus N_F$ as desired. □

30.)

Proposition (Eisenbud, problem A3.14)**.** *For a projective resolution $P_\bullet$, we let $\ell(P_\bullet) := \min_{d\geq 1}\{d : \mathrm{im}(P_d \to P_{d-1})$ projective$\}$. Then, for $F_\bullet$, $G_\bullet$ two projective resolutions of M, $\ell(F_\bullet) = \ell(G_\bullet) = \operatorname{pd} M$.*

Proof. A quick sketch of the structure of our proof: we shall show that $\mathrm{im}(F_1 \to F_0)$ is projective if and only if $\mathrm{im}(G_1 \to G_0)$ is projective. Then, in the case that neither is projective, we will show there exist projective resolutions of a different module $F'_\bullet, G'_\bullet$ such that $\ell(F'_\bullet) = \ell(F_\bullet) - 1$ and $\ell(G'_\bullet) = \ell(G_\bullet) - 1$. Applying the two steps recursively then eventually reduces our situation to the case of the first claim.

Claim 30.A. $\mathrm{im}(F_1 \to F_0)$ *is projective if and only if* $\mathrm{im}(G_1 \to G_0)$ *is projective.*

Proof of Claim 30.A. We shall show only the forward implication; the converse is then given by symmetry. We suppose $\mathrm{im}(F_1 \to F_0)$ is projective. We denote $N_F := \mathrm{im}(F_1 \to F_0)$, and $N_G := \mathrm{im}(G_1 \to G_0)$ and note that $N_F \cong \ker(F_0 \to M)$. We now have exact sequences $0 \to N_F \to F_0 \to M \to 0$ and $0 \to N_G \to G_0 \to M \to 0$ so by the result of Shanuel's lemma, we have that $N_F \oplus G_0 \cong N_G \oplus F_0 := K$. As N_F and G_0 are projective, we have that K is projective, and as N_G is a direct summand of K, we have that N_G is projective ■

Claim 30.B. *If* $\mathrm{im}(F_1 \to F_0)$ *is not projective, there exist projective resolutions $F'_\bullet$ and $G'_\bullet$ of K (as defined above) such that $\ell(F'_\bullet) = \ell(F_\bullet) - 1$ and $\ell(G'_\bullet) = \ell(G_\bullet) - 1$.*

Proof of claim 30.B. We state the following basic fact without proof:

Fact 30.C. *If Q and S are R-modules with (respectively) projective resolutions $A_\bullet$ and $B_\bullet$, then $(A \oplus B)_\bullet$ is a projective resolution for $Q \oplus S$ where $(A \oplus B)_n = A_n \oplus B_n$.*

We note that $0 \to G_0$ is a projective resolution of G_0 and $0 \to F_0$ a projective resolution of F_0. We claim $\tilde{F}_\bullet$ is a projective resolution of N_F where $\tilde{F}_n = F_{n+1}$. Indeed, as $\mathrm{im}(F_1 \to F_0) = N_F$, our claim is immediate. An identical claim holds for $\tilde{G}_\bullet$ defined analogously with respect to N_G. We let $F'_\bullet$ be defined by

$$F'_n = \begin{cases} F_1 \oplus G_0 & i = 0 \\ F_{n+1} & i > 0 \end{cases}$$

and $G'_\bullet$ defined by

$$G'_n = \begin{cases} G_1 \oplus F_0 & i = 0 \\ G_{n+1} & i > 0 \end{cases}$$

Then, by Fact 30.C and Schanuel's lemma, we have that $F'_\bullet$ is a projective resolution for $N_F \oplus F_0 \cong K$ and $G'_\bullet$ is a projective resolution for $N_G \oplus G_0 \cong K$. Further, we have that $\mathrm{im}(F'_d \to F'_{d-1}) = \mathrm{im}(F_{d+1} \to F_d)$ for all $d > 1$ with a similar statement holding for G. This shows indeed that $\ell(F') = \ell(F) - 1$ with a similar statement again holding for G.

■

As stated above, these two claims come together to prove the proposition. □

31.)

Proposition (Eisenbud, problem A3.16). *For R a ring, and x a nonzerodivisor,* $\mathrm{Tor}_1(R/x, M) = 0 :_M x = \{m \in M \ : \ xm = 0\}$.

Proof. As Tor is symmetric, we consider $\mathrm{Tor}_1(M, R/x) = H_1(F_\bullet)$ where $F_\bullet = M \otimes P_\bullet$ for $P_\bullet$ a projective resolution of R/x. We have that $P_2 = 0 \to P_1 = R \to P_0 = R$ is a projective resolution of R/x where $P_1 \to P_0$ is $x\cdot$, the multiplication-by-x map. Thus, the complex in question is $F : F_2 = 0 \to F_1 = M \otimes R \cong M \to F_0 \cong M$, where $F_1 \to F_0$ is the map $\mathrm{id}_M \otimes (x\cdot)$, which corresponds to $(x\cdot)$ under the isomorphism $R \otimes M \cong M$. Thus,

$$\mathrm{Tor}_1(M, R/x) = \frac{\ker(x\cdot : M \to M)}{\mathrm{im}(0 \to M)} = \ker(x\cdot : M \to M) = 0 :_M x$$

□

32.)

Proposition (Eisenbud, problem A3.18). *We let $(R, \mathfrak{m})$ be a local ring, and let $(F_\bullet, \phi_\bullet)$ be a minimal free resolution of M in the sense that* $\mathrm{im}\phi_i \subset \mathfrak{m}F_{i-1}$. *We suppose* $\mathrm{rank}\ F_i = b_i$. *Then,* $\mathrm{Tor}(R/\mathfrak{m}, M) = (R/\mathfrak{m})^{b_i}$.

Proof. We note that if $\mathrm{rank}\ F_i = b_i$, then $F_i \cong R^{b_i}$. Thus, without loss of generality, we assume $F_i = R^{b_i}$ for all i. Then,

$$\begin{aligned}\mathrm{Tor}_i(R/\mathfrak{m}, M) &= H_i(R/\mathfrak{m} \otimes F) \\ &= \frac{\ker\left(\mathrm{id}_{R/\mathfrak{m}} \otimes \phi_i : R/\mathfrak{m} \otimes R^{b_i} \to R/\mathfrak{m} \otimes R^{b_{i-1}}\right)}{\mathrm{im}\left(\mathrm{id}_{R/\mathfrak{m}} \otimes \phi_{i+1} : R/\mathfrak{m} \otimes R^{b_{i+1}} \to R/\mathfrak{m} \otimes R^{b_i}\right)}\end{aligned} \tag{4}$$

We denote by ∂_i the function $\mathrm{id}_{R/\mathfrak{m}} \otimes \phi_i$.

Claim 32.A. $\mathrm{im}\partial_i = 0$ *for all i.*

Proof of claim 32.A. Indeed, we have that $\mathrm{im}\phi_i \subset \mathfrak{m}F_{i-1}$. Thus, for any $r \otimes p \in F_i = R^{b_i}$, we have that $\phi_i(r \otimes p) = r \otimes m$ where $m \in \mathfrak{m}F_{i-1} = (\mathfrak{m}R)^{b_{i-1}}$. As tensors respect products, we may represent this as $(r \otimes m_1, \dots r \otimes m_{b_{i-1}}) = (rm_1 \otimes 1, \dots, rm_{b_{i-1}} \otimes 1) \in \bigoplus_{i=1}^{b_{i-1}} R/\mathfrak{m} \otimes R$ where each $m_j \in \mathfrak{m}R = \mathfrak{m}$. As $r \in R/\mathfrak{m}$, and $\mathrm{Ann}_R(R/\mathfrak{m}) = \mathfrak{m}$, we have that $rm_j = 0$ for all j. Thus, $r \otimes m = 0$, and as $r \otimes m$ was an arbitrary element of $\mathrm{im}\phi_i$, we have shown our claim. ■

With that taken care of, we how have from equation (4) that $\mathrm{Tor}_i(R/\mathfrak{m}, M) = \ker \partial_i$. However, as claim 32.A demonstrates that each ∂_i is the zero map, we have that $ker(\partial_i) = F_i = R/\mathfrak{m} \otimes R^{b_i}$. As tensors respect products and $R/\mathfrak{m} \otimes R \cong R/\mathfrak{m}$, we have now shown $\mathrm{Tor}_i(R/\mathfrak{m}, M) = (R/\mathfrak{m})^{b_i}$. □

33.)

Proposition (Eisenbud, problem A3.23). *If x is a nonzerodivisor in ring R, and M is an R-module, then* $\mathrm{Ext}^0_R(R/x, M) \cong 0 :_M x$ *and* $\mathrm{Ext}^1_R \cong M/xM$. *In particular,* $\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/n, /ZZ/m) \cong \mathbb{Z}/\gcd(n, m) = \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/m)$

Proof. We again let that $P_2 = 0 \to P_1 = R \to P_0 = R$ be a projective resolution of R/x where $P_1 \to P_0$ is $x\cdot$, the multiplication-by-x map. Then, $\mathrm{Ext}^i_R(R/x, M) = H_{-i}(F_\bullet)$ where $F_\bullet \colon 0 \to F_0 = \mathrm{Hom}(P_0, M) \to F_1 = \mathrm{Hom}(P_1, M) \to \mathrm{Hom}(P_2, M) \to \dots$. As $P_2 = 0$ and $P_0 = P_1 = R$, we have that this is isomorphic to $F'_\bullet \colon 0 \to M \to M \to 0$ where $M \to M$ is the map $x\cdot$. Then,

$$\begin{aligned}\mathrm{Ext}^0_R(R/x, M) &\cong \frac{\ker(x\cdot : M \to M)}{\mathrm{im}(0 \to M)} \\ &= \ker(x\cdot : M \to M) \\ &= 0 :_M x\end{aligned}$$

and

$$\begin{aligned}\operatorname{Ext}^1_R(R/x, M) &\cong \frac{\ker(M \to 0)}{\operatorname{im}(x\cdot : M \to M)} \\ &= M/xM\end{aligned}$$

In particular, letting $R = \mathbb{Z}$, $x = n$, and $M = \mathbb{Z}/m$, we have that

$$\begin{aligned}\operatorname{Ext}^0_R(\mathbb{Z}/n, \mathbb{Z}/m) &\cong 0 :_{\mathbb{Z}/m} n \\ &= \left(\frac{\operatorname{lcm}(m,n)}{n}\mathbb{Z}/m\right) / \left(\mathbb{Z}/m\right) \\ &= \left(\frac{m}{\gcd(m,n)}\mathbb{Z}/m\right) / \left(\mathbb{Z}/m\right) \\ &\cong \mathbb{Z}/\gcd(n,m),\end{aligned}$$

and

$$\begin{aligned}\operatorname{Ext}^1_R(\mathbb{Z}/n, \mathbb{Z}/m) &\cong (\mathbb{Z}/m)/\left(n\mathbb{Z}/m\right) \\ &\cong \mathbb{Z}/\gcd(m,n)\end{aligned}$$

□

34.)

Proposition (Eisenbud, problem A3.24)**.** *We let A be a finitely generated Abelian group. A is free if and only if* $\operatorname{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) = 0$.

Proof. We recall that an Abelian group G is injective if and only if it is *divisible,* i.e. for any $g \in G$, $m \in \mathbb{N}$, there exists some $h \in G$ such that $mh = g$. We note that $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are divisble and hence injective and thus there exists an injective resolution for $\mathbb{Z}$

$$I \colon I_0 = \mathbb{Q} \xrightarrow{\partial_0} I_1 = \mathbb{Q}/\mathbb{Z} \xrightarrow{\partial_1} I_2 = 0$$

Then,

$$\operatorname{Ext}^1_{\mathbb{Z}}(A, \mathbb{Z}) = \frac{\ker\left(\partial_{1*} : \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z}) \to \operatorname{Hom}(A, 0)\right)}{\operatorname{im}\left(\partial_{0*} : \operatorname{Hom}(A, \mathbb{Q}) \to \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z})\right)} = \frac{\operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z})}{\operatorname{im}\left(\partial_{0*} : \operatorname{Hom}(A, \mathbb{Q}) \to \operatorname{Hom}(A, \mathbb{Q}/\mathbb{Z})\right)}$$

We recall by the structure theorem for Abelian groups that A is the direct product of finitely many $\mathbb{Z}$-modules of rank 1. We use this to write $A = A^F \oplus A^T$ where A^F is free and A^T is a torsion group (and hence finite by assumption in our case). We note that for any $m \in \mathbb{N}$, there exists a subgroup of $\mathbb{Q}/\mathbb{Z}$ cyclic of □

References

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004, pp. xii+932.

[Eis95] David Eisenbud. *Commutative algebra*. Vol. 150. Graduate Texts in Mathematics. With a view toward algebraic geometry. Springer-Verlag, New York, 1995, pp. xvi+785.

[Wil06] Herbert S. Wilf. *generatingfunctionology*. Third. A K Peters, Ltd., Wellesley, MA, 2006, pp. x+245.