2014 Algebra SEP $\sim$ Rings and Modules Day 1 Solutions, by E. Dummit

1. (Aug-13.3) Let I and J be ideals in a commutative ring R.

   (a) Show that if $I + J = R$, then $I \cap J = IJ$.

   (b) Suppose that I and J are ideals in $\mathbb{C}[x]$, and suppose that $I + J = (x)$. Show that $(I \cap J)/IJ$ is 1-dimensional as a complex vector space, and moreover that it is isomorphic to $\mathbb{C}[x]/(x)$ as a $\mathbb{C}[x]$-module.

   (c) On the other hand, for general commutative rings R, once $R/(I+J)$ is not trivial, the difference between $I \cap J$ and IJ can be large even if $R/(I \cap J)$ is small. Demonstrate this by showing that, if $R = \mathbb{C}[x, y]$, there exist ideals I and J in R such that $I + J = (x, y)$ and the dimension of $(I \cap J)/IJ$ as a $\mathbb{C}$-vector space is at least 100.

Solution: We will also assume that R has a 1, because otherwise the result of (a) is false: if $I = J = R = 2\mathbb{Z}$, then clearly $I + J = R$, $I \cap J = 2\mathbb{Z}$, and $IJ = 4\mathbb{Z}$.

a) Clearly $IJ \subseteq I \cap J$, even without the comaximality condition. For the other direction, suppose $x \in I \cap J$ and note that there exist $r_i \in I$ and $r_j \in J$ such that $r_i + r_j = 1$: then $x = x(r_i + r_j) = r_i x + x r_j$, and each term is in IJ.

b) Since $\mathbb{C}[x]$ is a PID, let $I = (xp)$ and $J = (xq)$. Since $I+J = (x)$, there exist polynomials r and s such that $rxp + sxq = x$ hence $rp + sq = 1$, so p and q are relatively prime. It is then immediate that $I \cap J = (xpq)$ and $IJ = (x^2pq)$. The cosets of $(I \cap J)/IJ$ are just the $\mathbb{C}$-multiples of $\overline{xpq}$, and multiplication by x kills everything, so the $\mathbb{C}[x]$-module structure is the same as that of $\mathbb{C}[x]/(x)$. The statement about the dimension follows immediately.

c) Take $I = (x^n, x^{n-1}y, \cdots, y^n)$ and $J = (x, y)$: then $I \cap J = I$ while $IJ = (x^{n+1}, x^n y, \cdots, y^{n+1})$. Then each coset of $(I \cap J)/IJ$ has a unique representative that is a homogeneous polynomial of degree n, so the quotient is an $(n + 1)$-dimensional $\mathbb{C}$-vector space. Now just pick any $n \geq 99$.

---

2. (Jan-04.2) Let K be a field and R be the subring of $K[x]$ of all polynomials with zero x-coefficient.

   (a) Show that x^2 and x^3 are irreducible but not prime in R.

   (b) Show that R is Noetherian.

   (c) Show that the ideal of all polynomials of R with zero constant term is not principal.

Solution:

a) If $p(x) \cdot q(x)$ were a nontrivial factorization of x^2 or x^3, then one of p, q would necessarily have degree 1, but there are no polynomials in R of degree 1. They are not prime since x^2 divides $x^6 = x^3 \cdot x^3$ but does not divide x^3, and x^3 divides $x^6 = x^4 \cdot x^2$ but does not divide x^4 or x^2.

b) Observe that R is generated (as a ring) by $1, x^2, x^3$, since these elements generate all the monomials in R. Hence we see that R is a quotient of the ring $K[y, z]$ under the map φ sending $y \mapsto x^2$ and $z \mapsto x^3$. Then since $K[y, z]$ is Noetherian and quotients of Noetherian rings are Noetherian, we see R is Noetherian.

Remark It is not necessary for the argument above, but one can show that the kernel of φ is the principal ideal $(y^3 - z^2)$.

c) If this ideal were principal and generated by $q(x)$, then x^2 and x^3 would necessarily be polynomials in $q(x)$, but then $\deg(q)$ must divide 2 and 3, hence must divide 1, which is impossible.

---

3. (Jan-13.3) A ring R is "von Neumann regular" if for every $a \in R$ there exists an $x \in R$ with $a = axa$. (The element x is called a weak inverse of a.) In particular, observe that every division ring is von Neumann regular: take $x = 0$ for $a = 0$ and $x = a^{-1}$ otherwise.

(a) Give an example of a commutative von Neumann regular ring which is not a field.

(b) Let $R = M_2(\mathbb{C})$ and $a = e_{12}$, the nilpotent matrix which sends $(e_1, e_2) \mapsto (0, e_1)$. Find a weak inverse for a.

(c) Show that if V is a vector space over a field k, the ring of endomorphisms $\mathrm{End}_k V$ is von Neumann regular.

Solution:

a) A general class of examples is the collection of (finite or infinite) direct products of fields $R = \prod F_i$, where there is more than one term in the product. The weak inverse of an element is taken componentwise: either 0 (for a component of 0) or the inverse (for nonzero components).

Remark This class includes all rings $\mathbb{Z}/n\mathbb{Z}$ where n is squarefree. In fact, $\mathbb{Z}/n\mathbb{Z}$ is von Neumann regular iff n is squarefree: we require for every $a \in R$ that there exists x such that n divides $a(1-ax)$; if n is divisible by p^2 where p is prime, then taking $a = p$ yields a contradiction. Otherwise, if $\gcd(a,n) = d$, then we require $\frac{n}{d}$ to divide $1 - ax$, and such an x exists because a and $\frac{n}{d}$ are relatively prime (since n is squarefree).

b) One can check with direct calculation that for $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $x = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$, we have $axa = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} r & s \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix}$, so we can take $x = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

c) Choose a basis $\{e_i\}_{i \in I}$ for $\mathrm{im}(a)$ and a basis $\{f_j\}_{j \in J}$ for ker(a). By the first isomorphism theorem, if we choose arbitrary $v_i \in V$ with $a(v_i) = e_i$ for $i \in I$, then $\{v_i\}_{i \in I} \cup \{f_j\}_{j \in J}$ is a basis of V. Now define the transformation x by setting $x(e_i) = v_i$ and $x(f_j) = 0$: we have $axa(v_i) = ax(e_i) = a(v_i)$, and $axa(f_i) = ax(0) = 0 = a(f_i)$, so x is a weak inverse of a.

c-alt) In the event that V is finite-dimensional we can give a more explicit linear-algebra argument: write $V = W \oplus W'$ where W is the generalized 0-eigenspace of a. On W', a acts as an invertible matrix so there we can take the weak inverse to be $a^{-1}|_{W'}$. On W, the Jordan form of $a|_W$ has entries of only 0 and 1, hence by changing K-basis we can assume that $a|_W$ is a direct sum of Jordan blocks. Again by considering each block separately, it is enough to find a weak inverse of a $d \times d$ Jordan block with eigenvalue 0. Following the example from part (b), we see that if we take $a : e_1 \mapsto 0$ and $e_{i+1} \mapsto e_i$, then it has a weak inverse given by $x : e_d \mapsto 0$, $e_i \mapsto e_{i+1}$. We conclude that every element of $\mathrm{End}_k V$ has a weak inverse.

---

4. (Aug-05.2) Let R be a ring with 1, V a Noetherian right R-module, and $\theta : V \to V$ a homomorphism.

(a) Show that $\ker(\theta^{n+1}) = \ker(\theta^n)$ for some $n \geq 1$.

(b) If θ is onto, prove that it is one-to-one.

(c) If V has a unique maximal submodule M, and it is true that if $X \subseteq Y$ are any submodules with $Y/X \cong V/M$ then $Y = V$, prove that θ is either 0 or an isomorphism.

Solution:

a) Clearly $\ker(\theta^{j+1}) \supseteq \ker(\theta^j)$, so the successive kernels of $\theta, \theta^2, \cdots$ form an ascending chain of submodules. Since V is Noetherian, it must stabilize at some finite stage $j = n$.

b) Suppose $\theta(v) = 0$. By a trivial induction, θ^n is onto, so there exists v' with $\theta^n(v') = v$. Then $\theta^{n+1}(v') = 0$, meaning that $v' \in \ker(\theta^{n+1})$. But $\ker(\theta^{n+1}) = \ker(\theta^n)$, so in fact $v' \in \ker(\theta^n)$ whence $v = \theta^n(v') = 0$.

c) Suppose θ is nontrivial: then the kernel of θ is a proper submodule hence contained in M. The first isomorphism theorem then says $\theta(V) \cong V/\ker(\theta)$ and $\theta(M) \cong M/\ker(\theta)$, so by the third isomorphism theorem we see $V/M \cong \theta(V)/\theta(M)$. The given criterion then says $\theta(V) = V$ so θ is onto; then by part (b) it is one-to-one, hence an isomorphism.

---

5. (Aug-03.2) Let R be a commutative integral domain (with 1).

   (a) If K is the field of fractions of R and $t \in R$ is such that $K = R[1/t]$, show that t is contained in every nonzero prime ideal of R.

   (b) Let $R = F[x_1, \cdots, x_n]$ for a field F. If $f(x_1, \cdots, x_n)$ is contained in every nonzero prime ideal of R, show that $f(a_1, \cdots, a_n) = 0$ for all $a_1, \cdots, a_n \in F$.

   (c) Suppose $f(x_1, \cdots, x_n)$ is a polynomial with coefficients in F, where F is an infinite field. If $f(a_1, \cdots, a_n) = 0$ for all $a_1, \cdots, a_n \in F$, show that f is the zero polynomial.

Solution:

a) Let P be a prime ideal and $r \in P\backslash\{0\}$. By hypothesis, $1/r$ is a polynomial in $1/t$, so $1/r = a_0 + a_1 t^{-1} + \cdots + a_n t^{-n}$, so $t^n = r(a_0 t^n + \cdots + a_n)$. We conclude that $t^n \in P$ so since P is prime, $t \in P$.

b) The evaluation map $g \mapsto g(a_1, \cdots, a_n)$ is a surjective homomorphism from R to F, whose kernel is therefore a maximal hence prime ideal of R. Then f is contained in the kernel of this homomorphism, so $f(a_1, \cdots, a_n) = 0$ for any $a_1, \cdots, a_n \in F$.

c) We prove the contrapositive (a nonzero function takes a nonzero value) by induction on the number of variables. If f is a one-variable function, it has only finitely many zeroes over F, since F is a field, so it is nonzero somewhere since F is infinite. Now suppose the result holds for any polynomial in at most k variables and let $f \in F[x_1, \cdots, x_k, y]$ where f has positive y-degree. Consider f as a function of y with coefficients in $F[x_1, \cdots, x_k]$: explicitly, as $f(\bar{x}, y) = p_0 + p_1 y + \cdots + p_n y^n$, where p_n is not the zero polynomial. Now by hypothesis, there exists a choice $(a_1, \cdots, a_k)$ for which $p_n(a_1, \cdots, a_k) \neq 0$: then $f(\bar{a}, y) = c_0 + \cdots + c_n y^n$ where $c_n \neq 0$. Since this polynomial in the single variable y is not the zero polynomial, we conclude that it is nonzero somewhere. Hence we are done.

Remark Part (c) is a version of the weak Nullstellensatz.

---

6. (Jan-09.2) Let S be the subring of $\mathbb{C}[x]$ consisting of all polynomials with real constant term.

   (a) Show that the ideal of S consisting of all polynomials with 0 constant term is not principal.

   (b) Let I be a nonzero ideal of S and choose $f \in I\backslash\{0\}$ to have minimal possible degree n. If $g \in I$, show that there exists $s \in S$ with $g - sf$ either equal to 0 or to a polynomial of degree n.

   (c) Conclude that any ideal I of S is either principal or generated by two elements of the same degree.

Solution:

a) Suppose this ideal were principal and generated by $p(x)$; note clearly that p has degree ≥ 1. Then there would necessarily exist elements q_1 and q_2 in S such that $p(x) \cdot q_1(x) = x$ and $p(x) \cdot q_2(x) = ix$. Since the degree of p is ≥ 1 we see that it must equal 1, which forces q_1 and q_2 to have degree 0 hence be (nonzero) constants. Since they are in S they must be real numbers, but this is a contradiction since dividing the two relations yields $i = \dfrac{q_2}{q_1}$.

b) By minimality of $f = b_n x^n + \cdots$, we know that g has degree at least n. If the degree of g is exactly n then we are done since we may take $s = 0$. If the degree of g is larger than n, say $g = a_{n+k} x^{n+k} + \cdots$ with $k \geq 1$, then we may perform the first step of polynomial division to replace g with $g - \dfrac{a_{n+k}}{b_n} x^k f$ to reduce the degree of g by (at least) 1; note that $\dfrac{a_{n+k}}{b_n} x^k \in S$ since it has positive degree. Then by an obvious downward induction, the result holds.

c) If $I = 0$ we are done. Otherwise, apply part (b) with $f \in I$ of minimal degree n, say $f = (c+di)x^n + o(x^{n-1})$. Either it is the case that every other $g \in I$ is a multiple of f (in which case I is principal) or some $g \in I$ can be written as $g = sf + g'$ where the degree of g' is also n, say $g' = (a+bi)x^n + o(x^{n-1})$. By minimality, we know that $a + bi$ and $c + di$ must be $\mathbb{R}$-linearly independent, otherwise we would have an $\mathbb{R}$-linear combination $f - rg'$ of degree less than n, contradicting the minimality of f. Hence we may take appropriate linear combinations to see that I contains two elements $f' = x^n + o(x^{n-1})$ and $g'' = ix^n + o(x^{n-1})$. Applying the result of part (b) to this f' shows that every $h \in I$ can be written in the form $h = sf + \left[ax^n + bix^n + o(x^{n-1})\right] = (s-a)f' + bg'' + o(x^{n-1})$, and by minimality the $o(x^{n-1})$ term must be zero since $h - (s-a)f' - bg''$ lies in I and has degree less than n. Hence I is generated by f' and g'', so it is generated by 2 elements.

---

7. (Aug-01.2) Let R be a commutative ring with 1 and M a maximal ideal of R.

(a) Show that R/M^2 has no idempotents other than 0 and 1.

(b) If R is Noetherian, show that M/M^2 is a finitely-generated R/M-module.

(c) If $R = K[x_1, \cdots, x_t]$ where K is a field, show that $\dim_K(R/M^2) < \infty$.

Solution:

a) The ring R/M^2 has a maximal ideal M/M^2, since $(R/M^2)/(M/M^2) \cong R/M$ is a field. If e is an idempotent in R/M^2 then $\bar{e}(1-\bar{e})$ in R/M, but this forces $\bar{e}$ or $1-\bar{e}$ to be zero since R/M is a field. We conclude that e or $1-e$ is in M/M^2, but since the square of any element in M/M^2 is zero, we see either $e^2 = e$ or $(1-e)^2 = 1-e$ is zero, so that e is 0 or 1.

b) Since R is Noetherian, M is finitely-generated as an R-module, say by $x_1, \cdots, x_k$: then for any $m \in M$ we can write $m = \sum r_i x_i$ for some $r_i \in R$. Passing to M/M^2 gives $\bar{m} = \sum \bar{r}_i \bar{x}_i$, so we see that $\bar{x}_1, \cdots, \bar{x}_k$ generate M/M^2. (Note that $\bar{r}_i \in R/M = F$ so this does make sense!)

c) Since polynomial rings are Noetherian by Hilbert's Basis Theorem, part (b) implies that M/M^2 is a finitely-generated R/M-module. Since $(R/M^2)/(M/M^2) \cong R/M$, the desired statement then follows from the fact that R/M is itself a finite-dimensional K-vector space, which is in turn implied by the Nullstellensatz. Explicitly: if $M = (p_1, \cdots, p_t)$, then if $(\alpha_1, \cdots, \alpha_t)$ is a common root of the polynomials p_i (in some algebraic closure $\bar{F}$) whose existence is guaranteed by the Nullstellensatz, then the evaluation map sending $p \mapsto p(\alpha_1, \cdots, \alpha_t)$ yields an isomorphism of R/M with $K(\alpha_1, \cdots, \alpha_t)$, and the latter is a finite-degree extension of K (since all of the α_i are roots of polynomials of finite degree over K).

---

8. (Aug-00.5) Let R be a ring with 1 and Z be its center. A derivation $D : R \to R$ is an additive map such that $D(ab) = aD(b) + D(a)b$.

(a) If $r \in R$, show that the map $A_r : R \to R$ given by $A_r(A) = ar - ra$ for all $a \in R$, is a derivation.

(b) If D is a derivation, show that $D(Z) \subseteq Z$.

(c) If D is a derivation of R and $e \in Z$ is an idempotent, show that $D(e) = 0$.

Solution:

a) A_r is obviously additive, and $A_r(ab) = abr - rab = a\,[br - rb] + [ar - ra]\,b$.

b) If $z \in Z$ and $r \in R$, then $0 = D(rz) - D(zr) = rD(z) + [D(r)z - zD(r)] - D(z)r = rD(z) - D(z)r$, so $D(z)$ commutes with r hence is in Z.

c) We have $D(e) = D(e^2) = 2eD(e)$ so $(1-2e)D(e) = 0$. Multiplying by $1-2e$ gives $0 = (1-2e)^2 D(e) = (1 - 4e + 4e^2) = D(e)$.

---

9. (Aug-12.2) Let F be a field, $R = F[x, y]$, and $I = (x)$.

(a) Prove that I/I^2 is infinite-dimensional as an F-vector space.

(b) Let $S \subset R$ be the subring $S = F + I$, so that I is also an ideal of S. Show that I is not finitely-generated as an ideal of S.

(c) Let M be a maximal ideal of R and $\theta : R \to R/M$ be the projection map. Then $\theta(S)$ is a ring with $\theta(F) \subseteq \theta(S) \subseteq \theta(R)$. Discuss the nature of the extension $\theta(F) \subseteq \theta(R)$, prove that $\theta(S)$ is a field, and conclude that $M \cap S$ is a maximal ideal of S.

Solution:

a) The elements of I are of the form $x \cdot p(x, y)$ for a polynomial $p(x, y)$. We can write any such element in the form $x \cdot q(y) + x^2 r(x, y)$, the image of which in I^2 is $x \cdot q(y)$. Thus we see that I/I^2 is generated as a vector space by x, xy, $xy^2, \cdots$, and is infinite-dimensional.

b) If I were finitely-generated as an ideal of S, then I/I^2 would be a finitely-generated ideal of S/I^2. But the elements of S/I^2 are of the form $\overline{c + xp(y)}$ where $c \in F$ and $p(y) \in F[y]$, and the only ones in I/I^2 are those with $c = 0$. But then the product of any two terms $\overline{xp(y)}$ and $\overline{xq(y)}$ is zero, so I/I^2 has trivial ring structure. The non-finite-generation then follows from part (a), since then finite generation of I/I^2 as a ring is equivalent to finite generation as an F-vector space. (Or, explicitly: if there are only finitely many generators, then it is not possible to obtain the term $x \cdot y^n$ where n is any integer larger than any of the y-degrees of the generators' images in I/I^2.)

c) $\theta(R) \cong R/M$ is a field extension of $\theta(F)$; since R is Noetherian, this field extension is of finite degree. If $x \in M$ then $\theta(S) = \theta(F)$ is a field; otherwise, assume $x \notin M$, so that x is invertible in R/M. We also see that $S + M = F + I + M$, and $I + M$ is an ideal of R containing M, hence since M is maximal it is either equal to M or to R: thus $S + M$ is either $F + M$ or $F + R$, so we see $\theta(S)$ is either $\theta(F)$ or $\theta(R)$, hence is a field. By the first isomorphism theorem for rings, we conclude that $S/(M \cap S) \cong \theta(S)$ is a field, so $M \cap S$ is a maximal ideal of S.