

More Stuff

June 6, 2005

1 Useful Module Facts

1.1 You Can Make a Quotient Module From Any Submodule

In groups, in order to form a quotient, you need a subgroup that is normal. For modules, you don't need any special property to form a quotient. Given any submodule N , $\frac{M}{N}$ is a module (over the same ring).

1.2 The First Isomorphism Theorem is Useful

If you need an isomorphism involving quotients, find a natural homomorphism, find the kernel and the image, and invoke this theorem, just as you would in groups and rings.

1.3 When Possible, Reduce a Complex Form to a Simple Form

Given an ideal I , and a module M , the product IM is defined to be $\{\sum_{j=0}^n x_j m_j | x_j \in I, m_j \in M\}$. If $M = (m_1, \dots, m_k)$ (ie M is finitely generated), then it is not immediate from the definition of IM that $IM = \{\sum_{j=0}^k x_j m_j | x_j \in I, m_j \text{ is the } j\text{th generator}\}$. Yet, this is the case (the distributive property is the key). There is an analogous situation in the land of ideals. If $I = (a)$ and $J = (b)$, then $IJ = (ab)$ even though this is not immediate from the definition (again, it relies on the distributive property...ie a well-chosen factorization). One need not memorize these facts: Usually in a problem you know whether you want a simple form or not, and if you do, it is easy to check whether such a simple form exists.

2 Sums and Direct Sums

If every element of m can be written as a sum of elements from the submodules N_1, \dots, N_k , then we say $M = N_1 + N_2 + \dots + N_k$. One has to be careful here. A common trap to fall into is to use uniqueness of the representation of the sum. In other words, if you have $n_1 + n_2 + \dots + n_k = n'_1 + n'_2 + \dots + n'_k$, you'd like to conclude $n_1 = n'_1, n_2 = n'_2$, etc. In order to do this sort of thing, you'd really need your sum to be direct. A sum is direct if you also have the condition that $N_i \cap (N_1 + N_2 + \dots + N_{i-1} + N_{i+1} + \dots + N_k) = 0$. Some problems are really easy if you have this uniqueness, but the uniqueness may not be there (so watch out!).

2.1 One Nice Thing About Rings Viewed as Modules

We often say R is an R -module acting on itself by left multiplication. Suppose we have $R \cong M$ as R -modules. Then the submodules of M correspond to the ideals of R . In Aug95(b) this is implicitly used in the solution. Even if you don't mention this explicitly in your solution, it is often part of the discovery process in problems like that.

3 Tensor Products

D+F Section 10.4 is long - skipping it may seem like a wise thing to do. However, there are two antidifficult things to master in the realm of the tensor product that will at least give you a chance with a tensor problems.

3.1 Tensors are Bilinear

$rm \otimes n = r(m \otimes n)$. Compare this with the direct product. Certainly it is not the case that $(rm, n) = r(m, n)$ - you'd need (rm, rn) to get $r(m, n)$. This is the main difference between bilinearity and linearity. We also have $(m + n) \otimes p = m \otimes p + n \otimes p$. These properties hold in the other coordinate as well. Bilinearity is sometimes described as "linear in each coordinate". One trick you can do with tensors that you can't in direct products is to bring a scalar from one side to another: $rm \otimes n = r(m \otimes n) = m \otimes rn$.

3.2 The Universal Property of Tensor Products

Let M and N be R -modules. Consider the good old direct product $M \times N$. There is a map $\iota : M \times N \rightarrow M \otimes N$ given by $\iota(m, n) = m \otimes n$. Suppose $\phi : M \times N \rightarrow L$ is a bilinear map of R -modules. That is, $\phi(rx + sy, z) = r\phi(x, z) + s\phi(y, z)$ (similarly for the second coordinate). Then, there is a unique homomorphism $\Phi : M \otimes_R N \rightarrow L$ such that $\Phi \circ \iota = \phi$. How does one use such a property??? You get to control T and ϕ . ϕ tells you where certain elements get sent to in the homomorphism Φ . So, knowledge about ϕ translates into knowledge about Φ , and if you know a lot about T , you can get information about elements in $M \otimes_R N$ via the homomorphism Φ . If this sounds vague (it does, I admit), go through my solution to D+F p356 #2 and example (3) p349 and what I said might make sense.

4 A Few Words About Linear Algebra

Of course, its good to know what a basis is, what dimension is, and how linear transformations can be converted into matrices. Also of importance are eigenvectors, eigenvalues, and eigenspaces. v is an eigenvector of a linear transformation T if $T(v) = \lambda v$ for some λ . λ is the eigenvalue associated with v . The eigenspace of λ consists of all vectors such that $T(v) = \lambda v$. These definitions are not arbitrary. Notice that if you have a diagonal matrix, that each element of the basis is an eigenvector (check this - the intuition for all of this becomes easier if you perform the calculations). The converse is also true - if you have a basis of eigenvectors of a linear transformation T , then T has a diagonal

matrix with respect to that basis. So, we care about eigenvectors because we care about diagonal matrices (a very simple form for a matrix to have). There is a polynomial - the characteristic polynomial - whose zeroes are the eigenvalues of a linear transformation.

The rational canonical form and the Jordan canonical form are not as nice as diagonal matrices, but they are still nicer than most matrices. They are obtained via $F[x]$ -modules over a vector space V given by a fixed linear transformation. Using the fundamental theorem of finitely generated modules over a PID, we convert that module into a nice form and out pops the rational canonical form (using the invariant factor decomposition), and the Jordan canonical form (using the elementary divisor decomposition). See D+F for more detail. An important theorem of that section is the Cayley-Hamilton theorem - the minimal polynomial divides the characteristic polynomial and its zeroes are also all the eigenvalues.

5 Brief Solution Descriptions

Aug03 #3 - Parts a and b are similar to Spr82 #3, and can also be found in the proof for the Chinese Remainder Theorem. For part c, note that $4Z \cdot 25Z = 100Z$ and $4Z + 25Z = Z$. Thus, by the Chinese Remainder theorem we have $\frac{Z}{100Z} \cong \frac{Z}{4Z} \times \frac{Z}{25Z}$. Now, it is not hard to prove (or to intuitively guess) that if we have $R \cong R_1 \times R_2$ then $R^\times \cong R_1^\times \times R_2^\times$. One might also prove it more directly.

Aug00 #3 - Part a: $\overline{(ab)^k} = \overline{a^k b^k} = \overline{a^k b b^{k-1}} = \bar{0}$, so \overline{ab} is nilpotent.

Part b: Suppose $\bar{a} \in \frac{Z}{nZ}$ is nilpotent. Let $p|n$. $\overline{a^k} = \bar{0}$, so $n|a^k$. Thus $p|a^k$. Since p is prime, $p|a$. Now suppose every prime divisor of n divides a . Write out the unique factorization of both n and a , and then raise a to a high enough power so that $n|a^k$.

Part c: $(1+x)(\sum_{k=0}^n (-1)^k x^k) = 1 + (-1)^{n+1} x^{n+1}$. The x^{n+1} term is 0 for some n because x is nilpotent.

Sum97 #7 - This is similar to D+F p273, but choosing p and q to be the nearest integers to r and s doesn't work this time because the bounds aren't good enough. However, finding the nearest half-integer to s and choosing p and q accordingly does work.

Aug96 #3 - To show R is a ring you can use the fact that R is a subset of $Q(\sqrt{-15})$, which is a field. Then show R is closed under addition and multiplication (this is quicker than checking all axioms). The automorphism sends elements to their complex conjugate, so you just need to verify that if you conjugate an element of R , you are back in R . To find units and whatnot, use the usual tricks involving $N(ab) = N(a)N(b)$ (see my previous sheet).

Jan96 #5 - There is no brief solution to this. The problem involves many straightforward manipulations, but is quite long.

Aug 93 #4 - The $\ker \phi^n$'s form an ascending chain of ideals. Use the ascending chain condition in combination with the fact that each ϕ^n is onto to obtain $\ker \phi = 0$. Hence

ϕ is 1-1, and automorphismality follows.

Jan92 #4 - Part a: To show the ideal is closed under $+$, suppose $x^n = 0$ and $y^m = 0$. Use the binomial expansion on $(x + y)^{n+m}$ to show $x + y$ is nilpotent.

Part b: Suppose P is a prime ideal. If $x^n = 0$ and $x \notin P$ then $x^{n-1} \in P$ since P is prime (and $x^n \in P$). But now $x \notin P$ implies $x^{n-2} \in P$. Induct on this idea to get $x \in P$.

Part c: Let $\bar{a} \in \frac{A}{N}$. Suppose $\bar{a}^k = \bar{0}$ for some k . Then $a^k \in N$, so $(a^k)^n = 0$ for some n . Thus $a \in N$, so $\bar{a} = \bar{0}$.

Aug90 #5 - Part a: The homomorphism that sends polynomials to their constant term is onto and has kernel (x, y) . Thus $\frac{Z[x,y]}{(x,y)} \cong Z$. Z is an integral domain and not a field, so (x, y) is prime, but not maximal.

Part b: All ideals containing (x, y) are of the form (n, x, y) where $n \in Z$. $\frac{Z[x,y]}{(n,x,y)} \cong Z_n$ and is thus only a field if n is prime. Hence (p, x, y) , with p prime are the maximals.

Part c: $Z[x, y]$ is a UFD. In a UFD, irreducible elements are prime. Thus, if you show $y^2 - x^3$ is irreducible then $(y^2 - x^3)$ is prime. Check this fact: A monic polynomial of degree 2 is reducible if and only if it has a zero. Thus, it suffices to show that $y^2 - x^3$ has no zeroes in the polynomial ring $(Z[x])[y]$ because it is degree 2 in that ring. The coefficients are polynomials in the variable x , so note that if you plug in any such polynomial into y^2 , you get a leading term with an even power. This won't cancel with x^3 , so there are no zeroes of $y^2 - x^3$. So, $(y^2 - x^3)$ is prime. It is not maximal (note that $(y^2 - x^3)$ contains no constant polynomials, so in the quotient rings the constants act like they usually do, which means they'll have no multiplicative inverse in the quotient).

Aug88 #4 - Part a: Any power series with 0 constant term isn't a unit. To show that any power series with a nonzero constant term is a unit, expand the equation $\sum_{n=0}^{\infty} a_n x^n \sum_{m=0}^{\infty} b_m x^m = 1$ and compare coefficients. You'll need induction for a rigorous proof.

Part b: If $I = R$ then $I = x^0 R$, so it works there. If $I \neq 0, I \neq R$ then I contains $p(x)$ with zero constant term (by part a). There is a smallest $k \geq 1$ such that for any $p(x) \in I$, $p(x) = x^k q(x)$ for some $q(x) \in R$. Thus, $I \subseteq x^k R$. There is a $p(x)$ s.t. the associated $q(x)$ has nonzero constant term. By part a, $q(x)$ is a unit, so we can get $x^k \in I$ so that $x^k R \subseteq I$.

Part c: $\frac{F[[x]]}{(x)} \cong F$, and F is a field, so (x) is a prime ideal. Show that it is the only prime ideal, and that $(f(x)) = (x)$ only if the smallest nonzero term of $f(x)$ is the x -term (ie $f(x)$ is associate to x by part a).

Jan86 #4 - The strategy - Suppose $R \neq 0$, and that $|R| = p$, p prime, implies $\exists a, b \in R$ $a \cdot b = 0$ (In other words, suppose the negation of (i) and the negation of (ii) hold). Prove that (iii) must be true. Now, $\forall x, Rx$ is an ideal. $Rx = 0$ or $Rx = R$ by hypothesis. Suppose that $\forall x Rx = 0$. Then $\forall a, b$ $a \cdot b = 0$. Thus, we can't have $|R| = p$ for any p prime, by $(\neg ii)$. Now, for $|R| = n$ with n not prime (and possibly infinite), construct an ideal I such that $I \neq 0$ and $I \neq R$. This is a contradiction, so we must have $\exists x Rx = R$. Then $\exists r rx = x$. Furthermore, $\forall y \exists s y = sx$. Thus $ry = rsx = srx = sx = y$. Thus r is an identity element for R . This implies that if $y \neq 0$ then $y \in yR$ and $yR = R$. Thus,

$\exists z \ yz = 1$, so every nonzero element is a unit. Thus R is a field.

D+F p356 #2 - Using the bilinearity of tensors, note that, in $Z \otimes_Z Z_2$, $2 \otimes 1 = 2(1 \otimes 1) = 1 \otimes 2 = 1 \otimes 0 = 0(1 \otimes 0) = 0$. Now, notice that $1 \notin 2Z$ so the first equation is not possible in $2Z \otimes_Z Z_2$. To rigorously prove $2 \otimes 1 \neq 0$ in $2Z \otimes_Z Z_2$, construct a bilinear map $\phi : 2Z \times Z_2 \rightarrow Z_4$ such that $\phi(2, 1) \neq 0$. Then apply the universal property of tensor products to obtain a homomorphism $\Phi : 2Z \otimes_Z Z_2 \rightarrow Z_4$ that sends $2 \otimes 1$ to a nonzero element of Z_4 and conclude $2 \otimes 1 \neq 0$. For inspiration on what bilinear map to use, see D+F p349 example (3).

D+F p383-4 #2 - There are many small steps you have to put together in the right way. Mostly, you use exactness (which gives equations of the form

$\text{Im } f = \ker g$), and the commutativity of the diagram (which gives equations of the form $f' \circ \alpha = \beta \circ f$). But, you also need to combine those facts with these:

- 1) If δ is 1-1 then $\ker \delta \circ h = \ker h$.
- 2) If α is onto then $\text{Im } f = \text{Im } f \circ \alpha$.
- 3) $x \in \ker \gamma \Rightarrow x \in \ker h \circ \gamma$.

Jan04 #5 - The fact that e is in the center is necessary for the fact that eM is a submodule (they don't ask you to prove this though). To show $M = M_1 + M_2$, let $y \in M$ and note that $y = ey + (1 - e)y$. To show it is a direct sum, use the fact that $e(1 - e) = e - e^2 = 0$ since $e = e^2$. To prove $\text{End}_R(M) \cong \text{End}_R(M_1) \oplus \text{End}_R(M_2)$ you send $f : M \rightarrow M$ to $f|_{M_1} + f|_{M_2}$ (the restriction of f to M_1 and M_2). In general, $f|_N$ (where N is a submodule of M), need not map into N , so you need to use facts about e to show that $f|_{M_1}$ is an endomorphism. The generalization uses the same ideas. Part 3 is hard (one might argue that it is way off the syllabus), and I am unsure of my solution, so I will say nothing of it.

Aug00 #4 - Part a: Suppose $m_1, m_2 \in \text{Tor}(M)$. Then $\exists r, s \ rm_1 = 0, \ sm_2 = 0$. Of course $rs(m_1 + m_2) = 0$, but also we need $rs \neq 0$, so use the integral domainness of R .

Part b: Z_6 is such that $\text{Tor}(Z_6)$ is not a submodule.

Part c: Let $m \neq 0$ be in an R -module M . Suppose $r, s \neq 0$ and $rs = 0$. If $sm = 0$ then m is a non-zero torsion element. Otherwise $r(sm) = (rs)m = 0$, so sm is a non-zero torsion element.

Sum97 #4 - If we suppose there's a basis for V such that the matrix rep for f is diagonal, we can form a polynomial $m(x) = \prod_{i=0}^k (x - \lambda_i)$ where each λ_i is distinct and from the diagonal of the matrix. Check that $m(f) = 0$ (the 0 transformation).

For the opposite direction, let $m(x) = \prod_{i=0}^k (x - \lambda_i)$ be the minimal polynomial with distinct linear factors. Note that the λ_i 's are eigenvalues. Apply induction on $\dim(V)$. For $n = 1$ the result is clear. For $n > 1$, show that $V = R(T - \lambda_k I) \oplus N(T - \lambda_k I)$. $N(T - \lambda_k I)$ is the eigenspace of λ_k so its basis consists of eigenvectors. The induction hypothesis gets used to show $R(T - \lambda_k I)$ has a basis consisting of eigenvectors. The direct sum is then used to obtain a basis for V consisting of eigenvectors. Notation: $N(T)$ is the "nullspace of T " (the kernel of T), while $R(T)$ is the range of T .

Aug95 #4 - Part a: Let $M = (x)$. Let $\phi : R \rightarrow (x)$ be given by $\phi(r) = rx$. Use the 1st isomorphism theorem.

Part b: $\phi^{-1}(N) = J$, where J is an ideal of R . R is a PID, so $J = (s)$. Now show that $\phi(J) = (sx)$.

Jan91 #7 - Parts a and b are a matter of routine checks. For part c note that $\frac{R}{S}$ is a field. Let $n = \dim_F \frac{R}{S}$, $m = \dim_{\frac{R}{S}} \frac{V}{W}$. Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis for $\frac{R}{S}$ over F , let $\{\beta_1, \dots, \beta_m\}$ be a basis for $\frac{V}{W}$ over $\frac{R}{S}$. Show that all combinations $\alpha_i \beta_j$ form a basis for $\frac{V}{W}$ over F .

Aug90 #6 - Part a: It is enough to show that every finite subset of E is linearly independent. Let $\{v_i\}_{i=0}^n$ be such a set. We must use induction. Clearly, $\{v_0\}$ is linearly independent. For the inductive step suppose $\sum_{i=0}^k \alpha_i v_i = 0$ (where $k \leq n$). Apply $\phi - \lambda_k I$ to both sides of this equation (the λ_i are the distinct eigenvalues). The v_k term cancels and we get $\sum_{i=0}^{k-1} \alpha_i (\lambda_i - \lambda_k) v_i = 0$. But, these $k-1$ elements are linearly independent (induction hypothesis), so $\alpha_i (\lambda_i - \lambda_k) = 0$. The distinctness of the λ_i 's allows us to conclude $\alpha_i = 0$ for $i \leq k-1$ which also allows us to conclude $\alpha_k = 0$, giving the result.

Part b: Use the fact that any n linearly independent vectors forms a basis. ϕ has n distinct eigenvalues, so choose n distinct eigenvectors. By part a, these vectors will form a basis. Now check that the associated matrix is diagonal.

Jan90 #4 - Unlike Jan04 #5, this asks you to show eM and $(1-e)M$ are submodules. Its a straightforward check, and it relies on R 's commutativity (they could have just had e in R 's center like in Jan04). Part b is a repeat of Jan04.

Jan87 #3 - Part a is a routine check as is part b. For part c, suppose $A \subseteq B$ and let $N = \{xm | x \in B\}$. $N = 0$ or $N = M$. If $N = 0$ then $B = A$. If $N = M$, then given $r \in R$, $\exists x \in B$ $rx = xm$ so $(r-x)m = 0$ implying $(r-x) \in A$. This implies $r \in B$ since $A \subseteq B$. Thus $R = B$.

Fal80 #2 - R must have an identity for this argument to work. Every proper ideal is contained in a maximal ideal. Thus, if $r \notin P$ then $(r) = R$, so r is a unit. Now, let $M = (m_1, \dots, m_n)$, where n is the minimum number of elements M can be generated by. Suppose $n \geq 2$. Then $m_1 = \sum_{i=2}^n p_i m_i$ where $p_i \in P$ (since $PM = M$). Thus $(1-p_1)m_1 = \sum_{i=2}^n p_i m_i$. But, $(1-p_1) \notin P$ so $(1-p_1)$ is a unit. Multiply both sides by its inverse to obtain m_1 written as a linear combination of the other m_i 's. But this allows us to generate M without m_1 , contradicting minimality, so $n = 1$. Suppose $M = (x)$. Then, for any $r \in R$ we have $rx = px$ for some $p \in P$. Thus, $(r-p)x = 0$. Again $r-p \notin P$, so its a unit and we get $m = 0$.