Solution of Algebra III End-sem 2009

October 26, 2016

Q0: For ideals I, J in a ring R, suppose that the natural ring homomorphism from R to $R/I \times R/J$ is an isomorphism. Show that $I + J = R$ and that the intersection of I, J is zero.

The natural map described above is also a R-module homomorphism. Suppose that there exists a bijection between R and $R/I \times R/J$, which is both a ring homomorphism as well as a R-module homomorphism. Why do the conclusions in above still remain valid?

<u>Solution</u>: Let z in R be mapped to $(1 + I, J)$, that is $z - 1$ belongs to I and z in J, that gives us that 1 is in $I + J$, whence $I + J = R$. Since $R \to R/I \times R/J$ is isomorphism we have that $I \cap J$, which is the kernel is 0.

Suppose that we have a bijection $f : R \to R/I \times R/J$, which is a ring homomorphism and a R-module homomorphism. Then we have two idempotents e_1, e_2 in R such that $R = Re_1 + Re_2$, from which it follows that $I + J = R$ (more explained in the solution of QA).

Q1: Let R be a non-zero ring and I an ideal of R.

a) If I is a free R-module, show that $I = zR$, where z is non-zero divisor in R.

b) If R/I is a free R-module, then $I = 0$.

c) If R/I is free R module for every ideal I then what can be said about R?

<u>Solution</u>: Since I is a free submodule of R, we have that I is of rank one and hence generated by z, since $r \mapsto rz$ is an isomorphism we have that z a non-zero divisor.

R/I is a free R-module. We prove that it is of rank one. Suppose it is of rank two. That is there exists a, b, in R such that $a+I, b+I$ generate R/I as a free module. But we have that $ab-ba = 0$. So $a+I, b+I$ are linearly dependent. So $R/I \cong R$, hence $I = 0$.

If R/I is a free R-module for every ideal I, then $I = 0$, hence R is a field.

Q2: Let A be the 3×3 matrix with rows $(6, 2, 15), (0, 4, 10), (0, 0, 8)$. Consider the abelian group G presented by A. Write G as a direct sum of k non-zero abelian groups.

For which integers n, G can be made a module over $\mathbb{Z}/n\mathbb{Z}$.

<u>Solution</u> Consider the matrix transformation $x \mapsto Ax$, where A is the matrix given above. Then the image of A is spanned by $(6, 0, 0), (2, 4, 0), (15, 10, 8)$. So a basis for the image of A would be $(120, 0, 0), (0, 60, 0), (0, 0, 48)$, which means G is $\mathbb{Z}/120\mathbb{Z} \oplus \mathbb{Z}/60\mathbb{Z} \oplus \mathbb{Z}/48\mathbb{Z}$. IT can be made a $\mathbb{Z}_n$ module for $n = 120, 60, 48$.

Q3: How many similarity classes of complex matrices are there whose characteristic polynomial is $(x-2)^6$. Show that there is no polynomial $p(x)$ such that there is 13 similarity classes of complex matrices whose characteristic polynomial is $p(x)$.

Solution: By the Smith normal form we know that the matrix $xI - A$ is a diagonal matrix having 1's in the diagonals and then having $a_1(x), \cdots, a_m(x)$ such that $a_1|a_2|\cdots|a_m$. So we can have the number of partitions of 6 equal to the number of required similarity classes. That is

$6 = 6, 5+1, 4+2, 3+3, 3+2+1, 4+1+1, 3+1+1+1, 2+2+1+1, 2+1+1+1+1, 1+1+1+1+1+1$

10 classes.

We prove that a polynomial with complex coefficients cannot have 13 similarity classes. First assume that $p(x)$ is of degree two, then it is of the form $(x-\alpha)^2$ or $(x-\alpha)(x-\beta)$, in both cases we have two choices for the Smith normal form. Now suppose that it is of degree 3, then we have $p(x)$ equal to $(x-\alpha)^3, (x-\alpha)^2(x-\beta), (x-\alpha)(x-\beta)(x-\gamma)$. In the first case we have 3 choices for the Smith form. In the second case we have, 3 possibilities, so it is the number of partitions of 3. Similarly for 4, the number of partitions will be 5 possibilities. Continuing this process we can see that there is no natural number which has 13 as its partition number.

Q4: Show that a square matrix with entries in a field F is diagonalizable iff its minimal polynomial factors into distinct linear factors.

Solution: The matrix is diagonalizable means that there exists P such that PAP^{-1} is a diagonal matrix. So we have the characteristic polynomial of A equal to $\prod_i (x-\lambda_i)^{n_i}$, hence the minimal polynomial is $\prod_i (x-\lambda_i)$.

Conversely suppose that the minimal polynomial of A factors into distinct linear factors. Then we have $\lambda_1, \lambda_2, \cdots, \lambda_k$ are distinct eigenvalues of the matrix with multiplicities n_i. So A has a Jordan canonical form and the largest block associated to the Eigenvalue λ equals the largest power of $t-\lambda$ dividing the minimal polynomial. The matrix is diagonalizable if and only if all the Jordan blocks have size 1. Since minimal polynomial splits into distinct linear factors, this is the case. Hence A is diagonalizable.

Q5: Either show that the following are irreducible or factor it into irreducibles.

a) 30 in the ring of Gaussian integers.

b) $x^{50} - x^{49} - 9x^2 + 15x - 6$ in $\mathbb{Z}[x]$

c) $1234567x^4 - 5123476x^3 - 1543276x^2 + 7654321x - 1524367$ in $\mathbb{Q}[x]$.

d) $64x^6 + 32x^5 + 16x^4 + 8x^3 + 4x^2 + 2x + 1$ in $\mathbb{Z}[x]$.

Solution: a)$30 = 5.6 = (2+i)(2-i)3(1+i)(1-i)$

b) $(x-1)(x^{49} - 9x + 6)$, where $x^{49} - 9x + 6$ is irreducible by Eisenstein criterion.

c) Try to apply Eisenstein crieterion.

d) The polynomial is irreducible by the Eisenstein criterion.

Q6: For each ring R determine the number of maximal and prime ideals when it is finite and determine them in terms of relevant polynomials.

a) $F[x]/(p(x))$, F a field, p a polynomial.

b) $\mathbb{C}[x,y]/(f)$

c) $\mathbb{C}[x,y]/(f,g)$

Solution: The number of maximal ideals of $F[x]/(p(x))$ is the same as number of maximal ideals of $F[x]$ which contains $p(x)$, which is the number of irreducible factors of $p(x)$. Same for prime ideals.

b) In this case since f describes a curve on $\mathbb{C}^2$ we have infinite number of maximal hence prime ideals of the given ring.

c) In this case the number is finite if f, g does not have a common factor. The number of maximal ideals can be calculated by using Bezout's theorem. That is first homogenize f, g and look at the intersection in $\mathbb{P}^2$, and subtract all the points in the line at infinity.

QA: In problem 0 suppose that we are given only that there is a ring isomorphism between R and $R/I \times R/J$. Do the conclusions remain valid? What if we have a R-module isomorphism?

Solution: In this case consider f to be an isomorphism between R and $R/I \times R/J$. Now $(1+I, J), (I, 1+J)$ are idempotents in $R/I \times R/J$. Therefore they corresponds to idempotents e_1, e_2 in R, such that $e_1 + e_2 = 1$. Now $e_1 = 1 + a$ for $a \in I$ and $e_2 = 1 + b$ for $b \in J$. Hence we have $I + J = R$. Since the idempotents are coming from the ring structure, the result may not be true if we have a R-module isomorphism.

QB: Find the necessary and sufficient conditions on integers a, b, m, n for there to be an isomorphism between $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Do it for three integers also.

Solution: Since we have $(1,1)$ in $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ which is of order $lcm(m,n)$, we have its image under the isomorphism is a multiple of $(1,1)$, which is of order $lcm(m,n)$, also it is of order $lcm(a,b)$. So we have that $lcm(a,b)$ divides $lcm(m,n)$, similarly $lcm(m,n)$ divides $lcm(a,b)$. So we have that $lcm(a,b) = lcm(m,n)$ and $mn = ab$ and hence $gcd(a,b) = gcd(m,n)$. This is the condition. By the fundamental theorem on finitely generated abelian group, this is also the necessary condition. Similar argument works for product of three groups.

QC: If there is an abelian group isomorphism between the product of some $\mathbb{Z}/n_i\mathbb{Z}$ and a product of $\mathbb{Z}/m_j\mathbb{Z}$, then there is a ring isomorphism between individual factors.

Solution: Take $\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/80\mathbb{Z}$ and $\mathbb{Z}/45\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, they are isomorphic but $\mathbb{Z}/72\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/45\mathbb{Z}$.

QD: Using Jordan form, we know that any linear operator A on a finite dimensional complex vector space can be written as $D + N$, where D is diagonalizable and N is nilpotent and $DN = ND$. Recall that uniqueness of D, N was an easy consequence of

a) D, N can be expressed as polynomials in A.

b) Two commuting diagonalizable operators on a finite dimensional vector space can be simultaneously diagonalizable.

Solution: Please read the section on rational canonical forms and Jordan canonical forms in the book by Dummit and Foote on abstract algebra, page 471-495.

FOr part b) see,

http://www.math.uconn.edu/ kconrad/blurbs/linmultialg/minpolyandappns.pdf on page 8.