

# MATH 503: HOMEWORK #3A

DUE MONDAY, MARCH 17, 5 P.M. YING ZONG'S MAILBOX

## 1. ALGORITHMS FOR CARRYING OUT THE FUNDAMENTAL THEOREM

In class we talked about algorithms for taking a given free finitely generated module  $M$  for a P.I.D.  $R$  together with a set of generators for a submodule  $N$  of  $M$  and producing a basis  $\{y_i\}_{i=1}^m$  for  $M$  over  $R$  such that  $N$  has basis  $\{a_i y_i\}_{i=1}^n$  for some  $1 \leq n \leq m$  and some non-zero elements  $a_1, \dots, a_n \in R$  such that  $a_1 | a_2 | \dots | a_n$ . This exercise has to do with carrying out this algorithm

- 1.1 Suppose  $R = \mathbb{Z}$  and that  $M = Re_1 \oplus Re_2 \oplus Re_3$  for the basis  $\{e_1, e_2, e_3\}$  of  $M$ . Suppose that  $N$  is generated by  $q_1, \dots, q_4$  where  $q_i = \sum_{j=1}^3 q_{i,j} e_j$  and  $q_{i,j} = i^j$ . In other words,  $A = (q_{i,j})$  is the  $4 \times 3$  matrix

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 4 & 8 \\ 3 & 9 & 27 \\ 4 & 16 & 64 \end{pmatrix}.$$

Write down a basis  $\{y_i\}_{i=1}^3$  and a set of invariant factors  $\{a_i\}_{i=1}^3$  for  $N$  as above. You should express each  $y_i$  as an explicit integral combination of the basis elements  $\{e_1, e_2, e_3\}$ .

- 1.2 In class we talked about how if  $R$  is Euclidean we can use the Euclidean algorithm for  $R$  to carry about computations of the above kind. Suppose now only that  $R$  is a P.I.D.. Suppose  $\alpha, \beta \in R$  are not both 0. Suppose we have an oracle which tells us how to find elements  $\lambda, \gamma \in R$  such that

$$(1.1) \quad \lambda\alpha + \gamma\beta = d$$

where  $d$  is a g.c.d. for  $\alpha$  and  $\beta$  in  $R$ . Prove that  $\tau = \alpha/d$  and  $z = \beta/d$  are in  $R$ , and that

$$(1.2) \quad \begin{pmatrix} \lambda & \gamma \\ -z & \tau \end{pmatrix}$$

is an invertible matrix with inverse

$$(1.3) \quad \begin{pmatrix} \tau & -\gamma \\ z & \lambda \end{pmatrix}$$

Show that

$$\begin{pmatrix} \lambda & \gamma \\ -z & \tau \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$$

and

$$(1.4) \quad \begin{pmatrix} \alpha & \beta \end{pmatrix} \cdot \begin{pmatrix} \lambda & -\gamma \\ \gamma & \tau \end{pmatrix} = \begin{pmatrix} d & 0 \end{pmatrix}$$

- 1.3 Suppose  $q = (q_{i,j})_{i,j}$  is a matrix with elements in  $R$ , and call  $r_i = (q_{i,j})_j$  the  $i^{\text{th}}$  row. Show that if  $i \neq j$ , we can make a new kind of row operation on matrices such as  $q$  by replacing  $r_i$  by  $\lambda r_i + \gamma r_j$  and  $r_j$  by  $-z r_i + \tau r_j$  and by leaving the other rows alone. Prove that this operation is invertible by another operation of the same kind using that (1.2) is an invertible matrix. Explain how you would make similar new column operations using (1.4).

- 1.4 Suppose now that we are given a finitely generated free  $R$ -module  $M = \bigoplus_{i=1}^m R e_i$  together with an explicit finite set of generators  $q_i = \sum_{j=1}^m q_{i,j} e_j$  for a submodule  $N$  of  $M$ . Explain how you would be able to use an oracle of the above kind along with the new row and column operations in the last two problems to produce  $\{y_i\}_i$  and  $\{a_i\}_i$  of the kind described at the beginning of this section.

## 2. THE RATIONAL CANONICAL FORM

This section has to do with carrying out the algorithm for how to conjugate a matrix into rational canonical form which was described in class. We'll use this on the matrix

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

over the field  $F = \mathbb{Z}/2$  which we talked about in class. Define

$$M = xI_{3,3} - A = \begin{pmatrix} x-1 & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x-1 \end{pmatrix}.$$

- 2.1 Let  $V$  the  $F[x]$  module which is the three dimensional  $F$ -vector space

$$V = Fb_1 \oplus Fb_2 \oplus Fb_3$$

on which  $x$  acts as multiplication by the matrix  $A$  when we identify

$$a_1 b_1 + a_2 b_2 + a_3 b_3 \quad \text{for } a_1, a_2, a_3 \in F$$

with the column vector

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}.$$

Let

$$F[x]^3 = F[x]c_1 \oplus F[x]c_2 \oplus F[x]c_3$$

be the free rank 3  $F[x]$ -module with basis  $\{c_1, c_2, c_3\}$ . Check that there is an  $F[x]$ -module isomorphism

$$V \rightarrow \frac{F[x]^3}{MF[x]^3}$$

defined by

$$a_1 b_1 + a_2 b_2 + a_3 b_3 \rightarrow [a_1 c_1 + a_2 c_2 + a_3 c_3]$$

where  $[v]$  is the image of  $v \in F[x]^3$  in  $\frac{F[x]^3}{MF[x]^3}$ . This is the inverse of the  $F[x]$ -module isomorphism we discussed in class.

**Hints:** Start with the surjective  $F[x]$  module homomorphism  $\psi : F[x]^3 \rightarrow V$  for which  $c_i \rightarrow b_i$  for  $i = 1, 2, 3$ . Show that

$$MF[x]^3 = \{Mv : v \in F[x]^3\}$$

is in the kernel of  $\psi$ , and deduce that it is enough to prove that

$$\dim_F \left( \frac{F[x]^3}{MF[x]^3} \right) \leq 3.$$

Then show that modulo  $MF[x]^3$ , every element of  $F[x]^3$  is congruent to an element of the form  $a_1b_1 + a_2b_2 + a_3b_3$  with  $a_i \in F$ . For this, write each element of  $F[x]^3$  as

$$(2.5) \quad \begin{aligned} f_1(x)c_1 + f_2(x)c_2 + f_3(x)c_3 &= \begin{pmatrix} f_1(x) \\ f_2(x) \\ f_3(x) \end{pmatrix} \\ &= f_1(x) \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + f_2(x) \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + f_3(x) \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}. \end{aligned}$$

for some  $f_i(x) \in F[x]$ . Using that  $M = xI_{3,3} - A$  show that

$$(2.6) \quad \begin{pmatrix} f_1(x) \\ f_2(x) \\ f_3(x) \end{pmatrix} \equiv f_1(A) \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + f_2(A) \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + f_3(A) \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \pmod{MF[x]^3}.$$

where the right side is a vector with entries in  $F$ .

2.2 In class we talked about finding matrices  $C$  and  $D$  in  $\text{Mat}_3(F[x])$  such that  $CMD = M'$  is diagonal with the invariant factor polynomials  $a_1(x), \dots, a_n(x)$  appearing down the diagonal. Find  $C$  and  $D$  which correspond to the following sequence of operations:

- i. Replace column 3 by the sum of column 2 and column 3.
- ii. Replace row 3 by row 3 minus row 2.
- iii. Replace row 2 by row 2 plus  $x$  times row 3.
- iv. Replace column 2 by column 2 minus  $x$  times column 3.
- v. Replace column 2 and column 3 by  $-1$  times themselves.

Show that this leads to

$$CMD = M' = \begin{pmatrix} x-1 & 0 & 0 \\ 0 & x^2-x & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

2.3 Show that if  $F[x]^3 = F[x]c_1 \oplus F[x]c_2 \oplus F[x]c_3$  as above, then

$$\frac{F[x]^3}{M'F[x]^3} = \frac{F[x]}{F[x](x-1)} \oplus \frac{F[x]}{F[x](x^2-x)} \oplus \frac{F[x]}{F[x](-1)}$$

where the last summand is trivial. View elements of  $F[x]^3$  as column vectors, and let  $[v]'$  be the image of  $v \in F[x]^3$  in  $\frac{F[x]^3}{M'F[x]^3}$ . Define

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad v_3 = \begin{pmatrix} 0 \\ x \\ 0 \end{pmatrix}$$

Show that  $\{[v_1]', [v_2]', [v_3]'\}$  is an  $F$ -basis for  $\frac{F[x]^3}{M'F[x]^3}$  and that the matrix of multiplication by  $x$  on  $\frac{F[x]^3}{M'F[x]^3}$  relative to this basis is the rational canonical form matrix associated to the invariant factors  $a_1(x) = x-1$  and  $a_2(x) = x(x-1)$ .

2.3 In class we discussed the fact that left multiplication by  $C^{-1}$  gives an  $F[x]$ -module isomorphism

$$\frac{F[x]^3}{M'F[x]^3} \rightarrow \frac{F[x]^3}{MF[x]^3}$$

defined by

$$[v]' \mapsto [C^{-1}v]$$

where  $[y]$  is the image of  $y \in F[x]^3$  in  $\frac{F[x]^3}{MF[x]^3}$ . Find  $C^{-1} \in \text{Mat}_3(F[x])$  by using the factorization of  $C$  into a product of elementary matrices. Compute the vectors

$$y_1 = C^{-1}v_1 \quad y_2 = C^{-1}v_2 \quad y_3 = C^{-1}v_3$$

as column vectors with entries in  $F[x]$ .

- 2.4 Using (2.6) and the expressions you found for  $y_1$ ,  $y_2$  and  $y_3$  in part 3 of this problem, find column vectors  $d_1, d_2, d_3$  with entries in  $F$  such that

$$[d_1] = [y_1], \quad [d_2] = [y_2], \quad [d_3] = [y_3]$$

in  $\frac{F[x]^3}{MF[x]^3}$ .

- 2.5 Part 1 of this problem gives an  $F[x]$ -module isomorphism  $V \rightarrow \frac{F[x]^3}{MF[x]^3}$  sending  $d_i$  to  $[d_i]$  when  $d_1, d_2, d_3$  are as in part 4 of this problem. Show that if we use the basis  $E = \{d_1, d_2, d_3\}$  of  $V = F^3$  then the matrix  $\text{Mat}_E^E(x)$  of multiplication by  $x$  on  $V$  relative to this basis is the rational canonical form  $C(x)$  of  $x$ . Conclude that  $\text{Mat}_E^E(x)$  is the rational canonical form of the matrix  $A$  we started with, and

$$\text{Mat}_E^E(x) = C(x) = \text{Mat}_B^E(I) \cdot A \cdot \text{Mat}_B^E(I)^{-1}$$

where here  $I$  stands for the identity map. Use the description of  $d_1, d_2, d_3$  as column vectors to write down the  $\text{Mat}_B^E(I)$  and verify that conjugation by this matrix carries  $A$  to a matrix in rational canonical form.

### 3. JORDAN CANONICAL FORMS

- 3.1 Do problem 23 on page 501 of Dummit and Foote.  
 3.2 Do problem 39 on page 502 of Dummit and Foote.

### 4. GAUSS JORDAN ELIMINATION

- 4.2 Do problem 27 on page 427 of Dummit and Foote.