Zhengdong Zhang
Email: zhengz@uoregon.edu
Course: MATH 648 - Abstract Algebra
Instructor: Professor Arkady Berenstein

Homework - Week 3
ID: 952091294
Term: Winter 2025
Due Date: 29^{th} January, 2025

Problem 15.1.5
Calculate the invariant factors of the following matrices, working over the ring $\mathbb{Z}[i]$ of Gaussian integers:

(a) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1+i & 0 \\ 0 & 0 & 2+i \end{pmatrix}$;

(b) $\begin{pmatrix} 2i & i & 2+i \\ i-1 & 1+i & 0 \\ 0 & 0 & 2+i \\ 1+i & -1 & 2+i \end{pmatrix}$

Solution:

(a) Note that we have

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & -2-i & 1+i \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1+i & 0 \\ 0 & 0 & 2+i \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2-i \\ 0 & 1 & -1-i \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1+3i \end{pmatrix}$$

where both

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & -2-i & 1+i \end{vmatrix} = 1 \text{ and } \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & -2-i \\ 0 & 1 & -1-i \end{vmatrix} = 1$$

So the invariant factors of this matrix is $(1, 1, 1+3i)$.

(b) Note that we have

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & -i & -2+i & 1-i \\ 0 & -2-i & 6i & -1-3i \\ 1 & -1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 2i & i & 2+i \\ i-1 & 1+i & 0 \\ 0 & 0 & 2+i \\ 1+i & -1 & 2+i \end{pmatrix} \begin{pmatrix} 0 & 1 & -2-i \\ -1 & 3+2i & -6-8i \\ 0 & 1 & -3-i \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 5-5i \\ 0 & 0 & 0 \end{pmatrix}$$

where $\begin{vmatrix} 0 & 0 & 0 & 1 \\ 0 & -i & -2+i & 1-i \\ 0 & -2-i & 6i & -1-3i \\ 1 & -1 & 0 & -1 \end{vmatrix} = -1$ and $\begin{vmatrix} 0 & 1 & -2-i \\ -1 & 3+2i & -6-8i \\ 0 & 1 & -3-i \end{vmatrix} = -1$ are invertible in $\mathbb{Z}[i]$. So the invariant factors are $(1, 1, 5-5i)$.

Problem 15.1.6
Let $R = \mathbb{C}[[x]]$, the ring of formal power series over $\mathbb{C}$. Consider the submodule W of the free module $V = Rv_1 \oplus Rv_2$ generated by

$$(1-x)^{-1}v_1 + (1-x^2)^{-1}v_2 \quad \text{and} \quad (1+x)^{-1}v_1 + (1+x^2){-1}v_2$$

Find a basis $\{v_1', v_2'\}$ of V and elements $\delta_1 \mid \delta_2 \in R$ such that W is generated by $\delta_1 v_1'$ and $\delta_2 v_2'$. Describe V/W.

Solution: Assume W is the row spaces spanned by the following matrix

$$A\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} \frac{1}{1-x} & \frac{1}{1-x^2} \\ \frac{1}{1+x} & \frac{1}{1+x^2} \end{pmatrix}\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

Note that

$$\frac{\frac{1}{1+x}}{\frac{1}{1-x}} = \frac{1-x}{1+x} = 1 - \frac{2x}{1+x} \in \mathbb{C}[[x]]$$

since

$$\frac{2x}{1+x} = 2x - 2x^2 + 2x^3 - 2x^4 + \cdots \in \mathbb{C}[[x]].$$

So we have

$$\begin{pmatrix} 1 & 0 \\ \frac{x-1}{x+1} & 1 \end{pmatrix} A = \begin{pmatrix} \frac{1}{1-x} & \frac{1}{1-x^2} \\ 0 & \frac{1}{1+x^2} - \frac{1}{(1+x)^2} \end{pmatrix}$$

Define

$$\begin{aligned} v_1' &= v_1 + \frac{1}{1+x}v_2 \\ v_2' &= v_2 \end{aligned}$$

Let $\delta_1 = \frac{1}{1-x}$ and $\delta_2 = \frac{1}{1+x^2} - \frac{1}{(1+x)^2}$. Note that W is generated by $\delta_1 v_1'$ and $\delta_2 v_2'$. Moreover, we have $\delta_1 \mid \delta_2$ since

$$\frac{\frac{1}{1+x^2} - \frac{1}{(1+x)^2}}{\frac{1}{1-x}} = \frac{1-x}{1+x^2} - \frac{1-x}{(1+x)^2} \in \mathbb{C}[[x]].$$

So

$$V/W \cong R/(\frac{1}{1-x}) \oplus R/(\frac{1}{1+x^2} - \frac{1}{(1+x)^2})$$

Note that $\frac{1}{1-x}$ is invertible in $\mathbb{C}[[x]]$ and

$$\frac{1}{1+x^2} - \frac{1}{(1+x)^2} = x \cdot \frac{x}{(1+x^2)(1+x)^2}$$

where $\frac{x}{(1+x^2)(1+x)^2}$ is also invertible in R. So $V/W \cong (0) \oplus R/(x) \cong \mathbb{C}$.

Problem 15.1.8
If R is a PID, then
$$\hom_R(R/(a), R/(b)) \cong R/(\gcd(a,b)).$$

Solution: Suppose $a = p_1^{n_1} \cdots p_k^{n_k}$ is a prime factorization in R where $p_1, p_2, \ldots, p_k$ are distinct irreducible elements in R, by Lemma 15.1.7, we have

$$R/(a) \cong R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_k^{n_k}).$$

We can write

$$\hom(R/(a), R/(b)) \cong \hom(R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_k^{n_k}), R/(b)) \cong \oplus_{i=1}^k \hom(R/(p_i)^{n_i}, R/(b)).$$

Now Suppose $R/(b) \cong \oplus_{j=1}^l R/(q_i^{m_l})$ where $q_1, \ldots, q_l$ are distinct primes in R.
Claim: Let $\phi : R/(p^n) \to R/(q^m)$ be a R-module homomorphism. If $p \neq q$ are distinct primes in R, then $\phi = 0$.
Proof: Suppose $\phi(1 + (p^n)) = k + (q^m) \in R/(q^m)$. Since $p \neq q$ are different primes in R, p^n and q^m are coprime to each other. There exists $s, t \in \mathbb{Z}$ such that $sp^n + tq^m = 1$. Now we have

$$k + (q^m) = \phi(1 + (p^n)) = \phi(tq^m + sp^n + (p^n)) = \phi(tq^m + (p^n)) = q^m\phi(t + (p^n)) = (q^m).$$

This implies $\phi = 0$. ∎

Now assume n, m be positive integers. We need to determine $\hom(R/(p^n), R/(p^m))$. Let $\phi \in \hom(R/(p^n), R/(p^m))$ and assume $\phi(1 + (p^n)) = k + (p^m)$. Note that ϕ is completely determined by $k + (p^m)$. If $n \geq m$, consider the map

$$\begin{aligned} T : \hom(R/(p^n), R/(p^m)) &\to R/(p^m), \\ k + (p^m) &\mapsto k + (p^m). \end{aligned}$$

It is easy to see that this map is both injective and surjective. On the other hand, if $n \leq m$, note that
$$p^n\phi(1 + (p^n)) = \phi((p^n)) = (p^m) = p^n k + (p^m).$$
So there exists $r \in R$ such that $k = rp^{m-n}$. Consider the map

$$\begin{aligned} T : \hom(R/(p^n), R/(p^m)) &\to R/(p^n), \\ k + (p^m) &\mapsto r + (p^n). \end{aligned}$$

This map is a well-defined R-module homomorphism. Suppose k_1, k_2 are two different representatives for the ideal $k_1 + (p^m)$, then $k_1 - k_2 \in (p^m)$, this implies there exists $r_3 \in R$ such that $r_1p^{m-n} - r_2p^{m-n} = r_3p^m$, namely $r_1 - r_2 = r_3p^n \in (p^n)$. Moreover, suppose $k + (p^m) \in \ker T$, then $r \in (p^n)$, so $k = rp^{m-n} \in (p^m)$. This implies $k + (p^m) = (p^m)$. So T is injective. For any $r + (p^n)$, consider the $k = rp^{m-n}$, the map $1 + (p^n) \mapsto k + (p^m)$ defines an element in $\hom(R/(p^n).R/(p^m))$. So T is also surjective. Thus,

$$\hom(R/(p^n), R/(p^m)) \cong R/(p^{\min(n,m)})$$

we can conclude that
$$\hom(R/(a), R/(b)) \cong R/(\text{gcd(a,b)}).$$

Problem 15.1.12
True or false? If R is a PID and V is a finitely generated R-module with invariant factors $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_k$, then V cannot be generated by fewer than k elements.

Solution: This is true. Assume V can be generated by l elements $v_1, \ldots, v_l$ such that $l < k$. Then V can be written as $V = Rv_1 + \cdots + Rv_l$. There exists a surjective R-module homomorphism $\theta : R^{\oplus l} = F \twoheadrightarrow V$ where $F = R^{\oplus l} = Rv_1 \oplus \cdots \oplus Rv_l$.If $\ker\theta = 0$, then V is free and by theorem 14.3.7, the basis for V has the same cardinality, so $l = k$. Suppose $\ker\theta \neq 0$. We know $V \cong F/\ker\theta$. By Corollary 15.1.4, there exists a basis $\{e_1, \ldots, e_l\}$ of F and non-zero elements $d_1 \mid d_2 \mid \cdots \mid d_p$ of R such that
$$\ker\theta = Rd_1e_1 \oplus \cdots \oplus Rd_pe_p$$
for some $p \leq l$. Therefore, we have
$$V \cong F/\ker\theta = R/(d_1) \oplus \cdots \oplus R/(d_p).$$
By Theorem 15.1.10 and Lemma 15.1.9, $l = k$. So V cannot be generated by fewer than k elements.

Problem 15.1.19
Find the isomorphism classes of abelian groups of order 108 having exactly 4 subgroups of order 6.

Solution: Note that $108 = 2^2 \cdot 3^3$. Suppose G is an abelian group of order 108 and H is a subgroup of order 6. H must be a product of cyclic groups so $H \cong C_2 \times C_3$. By Theorem 15.1.17, we know G must be product of abelian groups whose order is a prime power. We know $C_2 \times C_2$ has three distinct subgroup of order 2, generated by $(1,0), (0,1), (1,1)$. So G cannot contain a subgroup isomorphic to $C_2 \times C_2$. This means G must contain a subgroup isomorphic to C_4, which has exactly 1 subgroup isomorphic to C_2 generated by 2. This means G/C_4 must contain exactly 4 distinct subgroup of order 3. We know C_{27} has exactly one subgroups of order 3 generated by 9. And $C_3 \times C_3 \times C_3$ has at least five distinct subgroup of order 3, generated relatively by $(1,0,0), (0,1,0), (0,0,1), (1,1,1), (1,1,0)$. Finally, $C_3 \times C_9$ has exactly 4 distinct subgroups of order 3, generated relatively by $(1,0), (0,3), (1,3), (2,3)$. So G has to be isomorphic to $C_4 \times C_3 \times C_9$.

Problem 15.2.1
Let $\delta_1, \ldots, \delta_k$ be the invariant factors of a linear transformation ϕ on a finite dimensional vector space V. Then δ_k is the minimal polynomial of ϕ.

Solution: By Theorem 15.1.10, V can be decomposed into $V_\phi = V_1 \oplus \cdots \oplus V_k$ where each V_i is isomorphic to $\mathbb{F}[x]/(\delta_i)$ for $1 \leq i \leq k$. This means that for any $v \in V$, v can be written as

$v = f_1 v_1 + \cdots + f_k v_k$ for some $f_i \in \mathbb{F}[x]$ and $v_i \in V_i$, $1 \leq i \leq k$. For each i, The annihilator $\operatorname{Ann}(Vi) \subset \mathbb{F}[x]$ is the ideal (δ_i). And since $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_k$, we have $\delta_k \in (\delta_i)$ for all $1 \leq i \leq k$. This is just saying $\delta_k \cdot v_i = \delta_k(\phi)(v_i) = 0$ for any $1 \leq i \leq k$. Thus, $\delta_k \in \operatorname{Ann}(V)$. Suppose $\operatorname{Ann}(V)$ is generated by $p \in \mathbb{F}[x]$ with $\deg p < \deg \delta_k$, then p annihilating all $v \in V$ means that $p \in (\delta_i)$ for all $1 \leq i \leq k$, so $R/(\delta_1) \oplus \cdots \oplus R/(\delta_{k-1}) \oplus R/(p)$ is another decomposition of V and by Lemma 15.1.9, p and δ_k only differ by a unit in $\mathbb{F}[x]$. We know $\mathbb{F}[x]^\times = \mathbb{F}^\times$, so $\deg \delta_k = \deg p$. A contradiction. This shows that δ_k is the minimal polynomial of ϕ.

Problem 15.2.2
Let $f \in \mathbb{F}[x]$ be a monic polynomial of degree $d > 0$. $I_d \in M_d(\mathbb{F})$ be the identity matrix, and consider $xI_d - \operatorname{Com}(f)$ as a matrix over $\mathbb{F}[x]$. Then the invariant factors of $xI_d - \operatorname{Com}(f)$ are $1, \ldots, 1, f(x)$ with 1 appearing $d-1$ times.

Solution: Suppose the monic polynomial

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

and write $A = xI_d - \operatorname{Com}(f)$. By defintion, we have

$$A = \begin{pmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & x & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & x & a_{d-2} \\ 0 & 0 & \cdots & -1 & x + a_{d-1} \end{pmatrix}$$

Let $p \in \mathbb{F}[x]$ and $L_{i,j}(p) = I_d + pe_{ij}$ where e_{ij} is a matrix with all zero entries except its (i,j)-entry is 1. Note that $\det L_{i,j}(p) = 1$, so it is always invertible. Left multiply $L_{i,j}(p)$ is equivalent to the elemenary transformation that multiply jth row with p then add it to ith row. Right multiply $L_{i,j}(p)$ is equivalent to the elementary transformation that multiply the ith column with p then add it to the jth column. Consider EA where

$$E := L_{1,2}(x) \cdots L_{d-2,d-1}(x) L_{d-1,d}(x)$$

We get a matrix

$$EA = \begin{pmatrix} 0 & 0 & \cdots & 0 & f(x) \\ -1 & 0 & \cdots & 0 & x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1 \\ 0 & -1 & \cdots & 0 & x^{d-2} + a_{d-2}x^{d-3} + \cdots + a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & x^2 + a_{d-1}x + a_{d-2} \\ 0 & 0 & \cdots & -1 & x + a_{d-1} \end{pmatrix}$$

Write

$$f_i(x) := x^{d-i} + a_{d-1}x^{d-i-1} + \cdots + a_i$$

for $0 \le i \le d-1$. Note that $f_0(x) = f(x)$ and EA can be rewrite as

$$EA = \begin{pmatrix} 0 & 0 & \cdots & 0 & f_0(x) \\ -1 & 0 & \cdots & 0 & f_1(x) \\ 0 & -1 & \cdots & 0 & f_2(x) \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & f_{d-2}(x) \\ 0 & 0 & \cdots & -1 & f_{d-1}(x) \end{pmatrix}$$

Next consider EAF where

$$F := L_{1,d}(f_1(x))L_{2,d}(f_2(x)) \cdots L_{d-1,d}(f_{d-1}(x)).$$

We have

$$EAF = \begin{pmatrix} 0 & 0 & \cdots & 0 & f(x) \\ -1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & -1 & 0 \end{pmatrix}$$

Note that -1 and 1 differ by a unit in $\mathbb{F}[x]$, and by switching rows and columns, EAF is a diagonal matrix, so the invariant factors of $A = xI_d - \mathrm{Com}(f)$ are $1, 1, \ldots, 1, f(x)$ with 1 appearing $d-1$ times.

Problem 15.2.8
The number of similarity classes of $n \times n$ nilpotent matrices over a field $\mathbb{F}$ is equal to the number of partition of n.

Solution: By Exercise 15.2.7, given two matrices $A, B \in M_n(\mathbb{F})$, A is similar to B if and only if $xI_n - A$ and $xI_n - B$ have the same invariant factors viewed as $\mathbb{F}[x]$-modules. By Exercise 15.2.2, we know that the invariant factors of $xI - A$ are just 1 together with invariant factors of A. So to determine the similarity classes of nilpotent matrices, we only need to determine the invariant factors of a nilpotent matrix A. Since A is nilpotent, the characteristic polynomial of A is x^n. By Exercise 15.2.1, suppose A has invariant factors $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_k = x^k$ where x^k is the minimal polynomial. For $1 \le i \le k-1$, $\delta_i = x^{d_i}$ where $1 \le d_i \le k$ and $d_1 \le d_2 \le \cdots \le d_{k-1}$. By Exercise 15.2.9, x^n is the product of invariant factors, so $d_1 + d_2 + \cdots + d_{k-1} = n$. This gives a partition of n. Now we can see that a partition of n gives a similar class of nilpotent matrices, and any similar class can be obtained in this way.

Problem 15.2.11
Give a list of 2×2 matrices over $\mathbb{F}_2$ such that every 2×2 matrix over $\mathbb{F}_2$ is similar to exactly one on your list.

Solution: We first determine the characteristic polynomial of the matrices. We list all degree 2 polynomials over $\mathbb{F}_2$. There are four: x^2, $x^2+1=(x+1)^2$, x^2+x and x^2+x+1. Note that the characteristic polynomial is a product of invariant factors, and by Theorem 15.2.3, we can give a matrix in the first canonical form as $\mathrm{diag}(\mathrm{Com}(\delta_1),\dots,\mathrm{Com}(\delta_k))$. All the classes of similar matrices are listed below.

	characteristic polynomial	invariant factor	matrix
1	x^2	$x \mid x$	$\begin{pmatrix}0&0\\0&0\end{pmatrix}$
2	x^2	x^2	$\begin{pmatrix}0&0\\1&0\end{pmatrix}$
3	x^2+1	$x+1 \mid x+1$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$
4	x^2+1	x^2+1	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$
5	x^2+x	x^2+x	$\begin{pmatrix}0&0\\1&1\end{pmatrix}$
6	x^2+x+1	x^2+x+1	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$

Problem 15.2.12

Let V be a 7-dimensional vector space over $\mathbb{Q}$.

(1) How many similarity classes of linear transformations on V have characteristic polynomial $(x-1)^4(x-2)^3$?

(2) Of the similarity classes in (a), how many have minimal polynomial $(x-1)^2(x-2)^2$?

(3) Let ϕ be a linear transformation of V having characteristic polynomial $(x-1)^4(x-2)^3$ and minimal polynomial $(x-1)^2(x-2)^2$. Find $\dim\ker(\phi-2id)$.

Solution:

(a) Write $p=x-1$ and $q=x-2$. p and q are coprime in $\mathbb{F}[x]$. The characteristic polynomial p^4q^3 is a product of invariant factors $\delta_1 \mid \delta_2 \mid \cdots \mid \delta_k$ where $\delta_1,\delta_2,\dots,\delta_k$ are powers of p, q or their product. We list the partition of 4 and 3 as follows:(1's are omitted in the final invariant factors, they are just there to easily determine the corresponding chain of invariant factors)

partition of 4	partition of 3
$p\ p\ p\ p$	$1\ q\ q\ q$
$1\ p\ p\ p^2$	$1\ 1\ q\ q^2$
$1\ 1\ p^2\ p^2$	$1\ 1\ 1\ q^3$
$1\ 1\ p\ p^3$	
$1\ 1\ 1\ p^4$	

Any choice of one partition of 4 and one partition of 3 from the table gives us a chain of invariant factors just by multiplying them accordingly and omit 1's in the result. For example, $(1, p, p, p^2)$ and $1, q, q, q$ will gives us the unqiue invariant factors $pq \mid pq \mid p^2q$. So there are in total 15 similarity classes.

(b) By Exercise 15.2.1, we need to final term multiplied together to get p^2q^2. There are two of them, namely $p \mid pq \mid p^2q^2$ and $p^2q \mid p^2q^2$.

(c) By Exercise 15.2.10, we need to find the dimension of 2-eigenspace of the linear transformation ϕ. ϕ must have invariant factors $p \mid pq \mid p^2q^2$ or $p^2q \mid p^2q^2$.

<u>Claim:</u> Suppose λ is an eigenvalue of ϕ. Then the dimension of λ-eigenspace is equal to the number of Jordan blocks $J(x-\lambda, a)$ appears in the Jordan normal form.

<u>Proof:</u> We need to show that each Jordan block $J(x-\lambda, a)$ defines a one-dimensional subspace of λ-eigenspace. By definition,

$$J(x-\lambda, a)\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} = \begin{pmatrix} \lambda v_1 \\ \lambda v_2 \\ \vdots \\ \lambda v_m \end{pmatrix} = \begin{pmatrix} \lambda v_1 + v_2 \\ \lambda v_2 + v_3 \\ \vdots \\ \lambda v_m \end{pmatrix}$$

This implies $v_2 = v_3 = \cdots = v_m = 0$. So this $J(x-\lambda, a)$ gives a one dimensional eigenspace generated by v_1. And since Jordan Normal Form is diagonal in each block, they do not intersect. So to count the dimension of λ-eigenspace, we only need to count the time $J(x-\lambda, a)$ appears. ∎

In $p \mid pq \mid p^2q^2$ or $p^2q \mid p^2q^2$, q or q^2 appear exactly twice. So $\dim\ker(\phi - 2id) = 2$.