Rational Canonical Form

Glenna Toomey

April 2014

This work is liscensed under creative commons Attribution-NoDerivs ©2014

1 Introduction

In mathematics, complete classification of structures, such as groups and rings, is often a primary goal. Linear transformations are no exception to this. Certain canonical forms exist to classify linear transformations, therefore creating a unique representative of linear transformations in the same similarity class. Diagonal representation is of course one of the simplest examples of a canonical form. However, not every matrix is diagonalizable. Jordan Canonical Form is yet another common matrix representation, but as we will soon see, this representation may not be achieved for every matrix.

Consider the matrix over $\mathbb{R}$,

$$A = \begin{pmatrix} 5 & 6 & 3 & 4 \\ -1 & 9 & 2 & 7 \\ 4 & -2 & -8 & 10 \\ 21 & -14 & 6 & 3 \end{pmatrix}$$

The characteristic polynomial for this matrix is $x^4 + 9x^3 - 97x^2 + 567x - 9226$, which can not be factored into linear factors over $\mathbb{R}$ and thus the eigenvalues for this matrix can not be found. Therefore, it is impossible to put this matrix in Jordan Canonical Form. Thus, Jordan Canonical Form can only be achieved for matrices in an algebraically closed field, which leads us to a second canonical form: that is, **Rational Canonical Form**.

2 Modules

Most proofs of the existence of Rational Canonical Form rely on the module associated with a linear operator, that is, the $F[x]$-module. Before examining this specific type, let us briefly explore some properties of general modules.

2.1 The Basics

The notion of a module extends easily from the concept of a vector space. To make this extension, we need only alter our idea the scalars associated with a vector space. Let us present this idea a bit more formally.

Definition. Let R be a commutative ring. An R-**module** is an additive abelian group M equipped with scalr multiplication $RxM \to M$, denoted by

$$(r, m) \to rm$$

such that the following axioms hold for all $m, m' \in M$ and all $r, r' \in R$.

(i) $r(m + m') = rm + rm'$
(ii) $(r + r')m = rm + r'm$
(iii) $(rr')m = r(r'm)$
(iv) $1m = m$.

As we can see from this definition, the only real difference between a vector space and a module is that a module admits scalar multiplication from elements in a ring instead of a field. Because these structures are so similar, it is not surprising that they share similar properties. Just as we can have morphisms between vector spaces, we can also have morphisms between modules.

Definition. Let M and N be R-modules. Then a map $f : M \to N$ is an R-map if for $m, m' \in M$ and $r \in R$ and

1.$f(m + m') = f(m) + f(m')$
2.$f(rm) = rf(m)$

Since a module is of course an abelian group, we can also relate properties of groups to modules through the isomorphism theorems. The three isomorphism theorems that exist for groups correspond nearly identically to isomorphism theorems of modules. Instead of exploring all three of the theorems, we will only state and prove the first since it will later be applicable to our exploration of cyclic submodules.

Theorem 1. *If $f : M \to N$ is an R-map of modules, then there is an R-isomorphism*

$$\phi : M/ker(f) \to im(f)$$

given by

$$\phi : m + ker(f) \to f(m).$$

Proof. Let us consider M and N as abelian groups. The First Isomorphism Theorem of Groups tells us that $\phi : M/\text{ker}(f) \to \text{im}(f)$ is an isomorphism of groups. However, we have the added operation of scalar multiplication, so we must show that $\phi(r(m + \text{ker}(f)) = r\phi(m + (\text{ker}(f))$.

$$\begin{aligned}\phi(r(m + \text{ker}(f))) =& \phi(rm + \text{ker}(f))\\ =& f(rm)\\ =& rf(m) \text{ since f is an } R - map\\ =& r\phi(m + \text{ker}(f))\end{aligned}$$

Thus, ϕ is an R-isomorphism. ∎

Now, let us define two more important properties of modules which will be used later in our study of cyclic modules and $F[x]$-modules.

Definition. Given an R-module, M, and $m \in M$, the **annihilator** of $m \in M$ is:

$$\text{ann}(m) = \{r \in R : rm = 0\}.$$

Furthermore, the annihilator of M is:

$$\text{ann}(M) = \{r \in R : rm = 0 \text{ for all } m \in M\}.$$

Definition. Given an R-module, M, an element $m \in M$ is a **torsion element** if $\text{ann}(m) \neq 0$. Furthermore, an R-module is a **torsion module** if for all elements $m \in M$, m is a torsion element.

2.2 Submodules

Definition. If M is an R-module, then a **submodule** N of M, denoted $N \subseteq M$ is an additive subgroup N of M closed under scalar multiplication. That is, $rn \in N$ for $n \in N$ and $r \in R$.

Now, let us present an important type of submodule. Though the significance of this specific submodule may not be clear now, we will come back to this concept shortly.

Definition. Given an R-module, M, and an element $m \in M$, the **cyclic submodule** generated by m is

$$\langle m \rangle = \{rm : r \in R\}$$

Proposition 2. *An R-module, M, is cyclic if and only if $M \cong R/I$ where I is an ideal of R.*

Proof. We will prove this theorem using the First Isomorphism Theorem of Modules. Suppose M is a cyclic module. Then we know that $\langle m \rangle = M$ for some $m \in M$. Let us define a map $f : R \to M$ by $f(r) = rm$. This map is surjective since given any element $x \in M$, $x = rm$ since M is cyclic. Furthermore, the $\ker(f) = \{r \in R : rm = 0\} = \text{ann}(m)$. Therefore, the $\ker(f)$ is an ideal of R and $M \cong R/I$. □

2.3 F[x]-Modules

We now have the tools to examine a specific type of module which will later be applied to the Rational Canonical Form of a matrix, that is, the $F[x]$-module. Because scalars of a module do not need to come from a field, nothing prevents us from defining a module over a ring of polynomials. Let us formalize this idea.

Definition. Let V be a vector space over a field F and let $T : V \to V$ be a linear transformation. Then we can extend this vector space to a module over $F[x]$ with scalar multiplication defined as follows: Given $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in F[x]$ and $v \in V$,

$$f(x)v = \sum_{i=1}^{n} a_i x^i v = \sum_{i=1}^{n} a_i T^i(v) = f(T)(v).$$

. This is called an $F[x]$**-module** which we will denote V^T.

Now, let us relate the idea of a torsion module to these $F[x]$-modules.

Proposition 3. *Given a vector space V over a field F and a linear transformation $T : V \to V$, the $F[x]$-module, V^T, is a torsion module.*

Proof. Let V be an n-dimensional vector space. Then for any $v \in V$, the set $\{v, T(v), T^2(v), ..., T^n(v)\}$ is linearly dependent since it contains $n+1$ vectors. Therefore, there exist scalars $a_0, a_1, ..., a_n$ not all equal to zero such that $\sum_{i=0}^{n} a_i T^i = 0$. Therefore, the nonzero polynomial $g(x) = \sum_{i=1}^{n} a_i x^i$ $\in \text{ann}(v)$ and v is a torsion element. $\square$

Now, let us consider submodules of an $F[x]$-module. We know that a submodule must be closed under scalar multiplication. However, in the case of an $F[x]$-module, scalar multiplication depends on a linear transformation, T. Thus, we can conclude that a submodule of an $F[x]$-module must be T-invariant.

Proposition 4. *Given a vector space V over a field F and a linear transformation, $T : V \to V$, a submodule W of the $F[x]$-module V^T is a T-invariant subspace. More specifically, $T(W) \subseteq W$.*

3 Minimal Polynomials

Before examining matrix representations of $F[x]$-modules, we must present one more concept: the minimal polynomial. As we will later see, minimal polynomials play an important roll in finding the Rational Canonical Form of a matrix.

Definition. The **minimal polynomial** of a matrix A, denoted $m_A(x)$, is the unique monic polynomial of least degree such that $m_A(A) = 0$.

Let us examine this notion in the context of an $F[x]$-module. Let V be a vector space over a field F and let $T : V \to V$ be a linear transformation. We know that the minimum polynomial for T is the polynomial $m_T(x)$ such that $m_T(T) = 0$. However,

$$\begin{aligned}\text{ann}(V^T) =& \{f(x) \in F[x] | f(x)v = 0 \text{ for all } v \in V\} \\ =& \{f(x) \in F[x] | f(T)v = 0 \text{ for all } v \in V\} \\ =& \{f(x) \in F[x] | f(T) = 0\}\end{aligned}$$

But since F is a field, $m_T(x)$ divides any polynomial with T as a zero so $\{f(x) \in F[x] : f(T) = 0\} = \langle m_t(x) \rangle$. Therefore, given a vector space V over a field F and a linear transformation $T : V \to V$, we can equivalently define the minimal polynomial of T to be the generator for $\text{ann}(V^T)$. We will return to this result in our analysis of the Decomposition Theorems of modules over Principal Ideal Domains.

4 Matrix Representations of Cyclic Submodules

Now we are ready to further explore cyclic submodules of an $F[x]$-module, V^T. We will begin this section with a simple, seemingly unmotivated definition. The motivation for this definition will become clear later in this section.

Definition. Given a polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, its **companion matrix**, denoted $C(p(x))$ is the $n \times n$ matrix:

$$\begin{pmatrix} 0 & 0 & ... & 0 & -a_0 \\ 1 & 0 & ... & 0 & -a_1 \\ 0 & 1 & ... & 0 & -a_2 \\ 0 & 0 & ... & 0 & -a_3 \\ . & . & ... & . & . \\ . & . & ... & . & . \\ 0 & 0 & ... & 1 & -a_{n-1} \end{pmatrix}$$

Now, let us return to the concept of a cyclic submodule of a $F[x]$-module, V^T. Suppose $W = \langle w \rangle$ is a cyclic submodule of V^T. We have already proven that W is T-invariant, so it makes sense to examine the linear transformation $T|_W$. Let $m_{T|_W}(x)$ be the minimal polynomial of $T|_W$ with degree n and consider $w_1 \in \langle w \rangle$.

$$\begin{aligned} w_1 =& f(x)w \text{ for some } f(x) \in F[x] \\ =& (m(x)q(x) + r(x))w \text{ for some } q(x), r(x) \in F[x] \text{ where } \deg(r(x)) < n \\ =& (m(x)q(x))w + r(x)w \\ =& 0 + r(x)w \end{aligned}$$

Let us interpret this result. We have just shown that any vector $w_1 \in \langle w \rangle$ can be written as the product of a polynomial of degree less than $n = \deg(m_{T|W}(x))$ and w. Thus, for any vector $w_1 \in \langle w \rangle$,

$$\begin{aligned} w_1 =& r(x)w \\ =& r(T)w \\ =& a_{n-1}T^{n-1}(w) + a_{n-2}T^{n-2}(w) + ... + a_0(v). \end{aligned}$$

But this is simply a linear combination of the set of n vectors, $\{T^{n-1}(v), T^{n-2}(v), ..., T(v), v\}$. Thus, this set spans $\langle w \rangle$. This motivates our next theorem.

Theorem 5. *Let $W = \langle w \rangle$ be a cyclic submodule of the $F[x]$-module V^T and deg$(m_T|W(x)) = n$. Then the set $\{T^{n-1}(w), T^{n-2}(w), ..., T(w), w\}$ is a basis for W.*

Proof. We have already shown that this set spans V, so we only must show that this set is linearly independent. Let Let $a_0 v + a_1 T(w) + ... + a_{n-1}T^{n-1}(w) = 0$ be a relation of linear dependence. We know that

$$a_0v + a_1T(w) + ... + a_{n-1}T^{n-1}(w) = p(T)w = p(x)w$$

where $p(x) \in F[x]$. However, since

$$\deg(p(x)) = n - 1 < n = \deg(m_{T|W(x)})$$

$p(x)$ must be the zero polynomial and $a_0, a_1, ..., a_n$ must all equal zero, making the relation of linear dependence trivial. Therefore, this set is a basis for for W. □

Now, let us consider the matrix representation of $T|_W$ relative to this basis. Since $T(w) = 0v + 1T(w) + 0T^2(w) + ... + 0T^{n-1}(w)$, the first column of our matrix is:

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ . \\ . \\ . \\ 0 \end{pmatrix}$$

Likewise, since $T(T(v)) = T^2(v) = 0v + 0T(v) + 1T^2(v) + 0T^3(v) + ... + 0T^{n-1}(v)$, the second column of our matrix is

$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ . \\ . \\ . \\ 0 \end{pmatrix}$$

This process continues until we get to the coordinatization of our last basis vector, $T^{n-1}(w)$. $T(T^{n-1}(w)) = T^n(w)$, but since $0 = m_T(T)w = T^n(w) + \sum_{i=1}^{n-1} a_iT^i(w)$, $T^n(w) = -\sum_{i=1}^{n-1} a_iT^i(w)$ where each a_i is a coefficient of $m_T(x)$. Therefore, the final column vector of our matrix representation is

$$\begin{pmatrix} -a_0 \\ -a_1 \\ . \\ . \\ . \\ -a_{n-1} \end{pmatrix}$$

Therefore, every cyclic submodule W of V^T has a matrix representation that is the companion matrix of $m_{T|W}(x)$.

5 Modules over Principal Ideal Domains

We will now explore the properties of modules over Principal Ideal Domains. More specifically, we will show that since $F[x]$ is a principal ideal domain, an $F[x]$-module can be written as a direct sum of cyclic submodulesthrough a series of decomposition theorems. We can then employ the matrix representations of cyclic submodules to construct the rational canonical form of a matrix. First, let us begin with a definition.

Definition. Given an R-module M with submodules S and T, M is the **direct sum** of S and T, denoted $M = S \oplus T$ if:
(i) $S \cap T = 0$
(ii) For each $m \in M$, m can be represented uniquely as $m = s + t$ where $s \in S$ and $t \in T$

We will now state a theorem which we will need later in our invariant factor decomposition of a module.[1]

Theorem 6. *M be an R-module and*
(i) Let $u_1, ..., u_n$ be nonzero elements in M with annihilators, $a_1, a_2, ..., a_n$, that are relatively prime. Then

$$\langle u_1 + u_2 + ... + u_n \rangle = \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus ... \oplus \langle u_n \rangle$$

(ii) If $v \in M$ has annihilator $\langle a_1 a_2 ... a_n \rangle$, then v can be written in the form $v = a_1 + a_2 + ... + a_n$. Furthermore,

$$\langle v \rangle = \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus ... \oplus \langle u_n \rangle$$

Thus, the direct sum of cyclic modules with relatively prime generators of annihilators is another cyclic module. We will need this result later in our Invariant Factor Decomposition.

5.1 The Decomposition Theorems

Theorem 7. *Let M be a finitely generated torsion module over a principal ideal domain, D, and let $ann(M) = \langle u \rangle = p_1^{e_1} p_2^{e_2} ... p_n^{e_n}$ where each p_i is prime in D. Then*

$$M = M_{p_1} \oplus M_{p_2} \oplus ... \oplus M_{p_n}$$

where $M_{p_i} = \{v \in V : p_i^e v = 0\}$.

Proof. For notational convenience, let $u_i = u/p_i^{e_i}$ and define $u_i M = \{u_i v : v \in M\}$. We wish to show that $u_i M = M_{p_i}$. Let $x \in u_i M$.

$$\begin{aligned} p_i^{e_i} x &= p_i^{e_i} u_i v \text{ where } v \in M \\ &= uv \end{aligned}$$

[1] For the proof of this theorem, see Roman,126

But $uv = 0$ since u annihilates all elements of M. Thus, $x \in M_{p_i}$ and $u_iM \subseteq M_{p_i}$. To show the opposite inclusion, suppose $y \in M_{p_i}$. Since u_i and $p_i^{e_i}$ are relatively prime, there exist $a, b \in D$ such that $au_i + bp_i^{e_i} = 1$. So,

$$\begin{aligned} y = 1y =&(au_i + bp_i^{e_i})y \\ =&au_iy + bp_i^{e_i}y \\ =&au_iy + b0 \\ =&au_iy \in u_iM \end{aligned}$$

Therefore, $M_{p_i} = u_iM$. Now, we will show that for any $x \in M$, $x = \sum_{i=1}^{n} u_iM$. We know that $u_1, u_2, ..., u_n$ are relatively prime and thus there exist elements of D, $a_1, a_2, ..., a_n$ such that $1 = a_1u_1 + a_2u_2 + ... + a_nu_n$. Therefore,

$$x = 1x = (a_1u_1 + a_2u_2 + ... + a_nu_n) = \sum_{i=1}^{n}(a_iu_i)x = \sum_{i=1}^{n} u_i(a_ix).$$

Therefore, $x = y_1 + y_2 + ... + y_n$ where $y_i \in u_iM$. Furthermore, since the order of u_iM divides $p_i^{e_i}$ and the $p_i^{e_i}$'s are relatively prime, the intersection of the u_iM's is trivial and thus

$$M = u_1M \oplus u_2M \oplus ... \oplus u_nM = M_{p_1} \oplus M_{p_2} \oplus ... \oplus M_{p_n}$$

□

Another decomposition which we will state, but not prove, allows us to even further decompose M into cyclic submodules.[2]

Theorem 8. *Let M be a primary, finitely generated torsion module over a principle ideal domain, R with ann$(M) = \langle p^e \rangle$, then M is the direct sum,*

$$M = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus ... \oplus \langle v_n \rangle$$

where ann$(\langle v_i \rangle) = p^{e_i}$ and the terms in each cyclic decomposition can be arranged such that

$$ann(v_1) \supseteq ann(v_2) \supseteq ... \supseteq ann(v_n).$$

From these results, we can now deduce that given a vector space V, a field F, and a linear transformation $T : V \to V$, the $F[x]$-module V^T can be represented as

$$V^T = M_{p_1} \oplus M_{p_2} \oplus ... \ M_{p_n} = (\langle v_{1,1} \rangle \oplus \langle v_{1,2} \rangle \oplus ... \oplus \langle v_{1,k_1} \rangle) \oplus ... \oplus (\langle v_{n,1} \rangle \oplus ... \oplus \langle v_{n,k_n} \rangle)$$

Where $\text{ann}(\langle v_{i,j} \rangle) = \langle p_i^{e_{i,j}} \rangle$ and the terms of each cyclic decomposition of M_{p_i} can be ordered such that

$$\text{ann}(\langle v_{i,1} \rangle) \supseteq \text{ann}(\langle v_{i,2} \rangle) \supseteq ... \supseteq \text{ann}(\langle v_{i,k_i} \rangle)$$

Equivelently, we can say that $p_i^{e_{i,1}} \geq p_i^{e_{i,2}} \geq ... \geq p_i^{e_{i,k_i}}$ or $e_i = e_{i,1} \geq e_{i,2} \geq ... \geq e_{i,k_i}$.

[2] For the proof of this theorem, see Roman, 131

5.2 The Invariant Factor Decomposition

We know from **Theorem 6** that the direct sum of cyclic modules with relatively prime annihilaters is another cyclic module. Thus we will reorder the above decomposition into the following groups:

$$\begin{aligned} W_1 &= \langle v_{1,1}\rangle \oplus \langle v_{2,1}\rangle \oplus ... \oplus \langle v_{n,1}\rangle \\ W_2 &= \langle v_{1,2}\rangle \oplus \langle v_{2,2}\rangle \oplus ... \oplus \langle v_{n,2}\rangle \\ &\vdots \end{aligned}$$

Since each p_i is relatively prime, by **Theorem 6**, we know that each W_i is a cyclic submodule with order $d_i = p^{e_{1,i}}p^{e_{2,i}}...p^{e_{j,i}}$. Therefore,

$$V^T = W_1 \oplus W_2 \oplus ... \oplus W_n$$

Where each $W_i = F[x]/\langle d_i\rangle$. Each d_i is called an **invariant factor** of V^T. Notice that $d_n|d_{n-1}|...|d_1$ since as i increases, d_i is built on subsequently lower powers of the primes $p_1, p_2, ..., p_n$.

Example 1. Suppose that W is cyclic submodule with ann $= p_1^{e_1}p_2^{e_2}p_3^{e_3}$ and that $W = M_{p_1} \oplus M_{p_2} \oplus M_{p_3}$. Each of these primary components can further be decomposed into cyclic module. Let us suppose that

$$M_{p_1} \oplus M_{p_2} \oplus M_{p_3} = (\langle v_{1,1}\rangle \oplus \langle v_{1,2}\rangle \oplus \langle v_{1,3}\rangle) \oplus (\langle v_{2,1}\rangle \oplus \langle v_{2,2}\rangle) \oplus (\langle v_{3,1}\rangle)$$

Then the $\langle p^{e_1}\rangle = ann(v_{1,1}) \supseteq ann(v_{1,2}) \supseteq ann(v_{1,3}), \langle p^{e_2}\rangle = ann(v_{2,1}) \supseteq ann(v_{2,2}), p^{e_3} = ann(v_{3,1})$.

We are free to rearange the direct sum of these cyclic subspaces, so for the invariant factor decomposition, we reorder this direct sum in the following way:

$$W = (\langle v_{1,1}\rangle \oplus \langle v_{2,1}\rangle \oplus \langle v_{3,1}\rangle) \oplus (\langle v_{1,2}\rangle \oplus \langle v_{2,2}\rangle) \oplus (\langle v_{1,3}\rangle)$$

Our new cyclic subspaces are:
$D_1 = \langle v_{1,1}\rangle \oplus \langle v_{2,1}\rangle \oplus \langle v_{3,1}\rangle$
$D_2 = \langle v_{1,2}\rangle \oplus \langle v_{2,2}\rangle$
$D_3 = \langle v_{1,3}\rangle$
and our invaraint factors are: $d_1 = p^{e_{1,1}}p^{e_{2,1}}p^{e_{3,1}} = p^{e_1}p^{e_2}p^{e_3}$, $d_2 = p^{e_{1,2}}p^{e_{2,2}}$, and $d_3 = p^{e_{1,3}}$.

6 Rational Canonical Form

We are finally ready to state our main result. We have determined that given any vector space, V and any linear transformation $T : V \to V$, the $F[x]$-module V^T can be decomposed into cyclic subspaces such that

$$V^T = W_1 \oplus W_2 \oplus ... \oplus W_n.$$

Where each $W_i = F[x]/\langle d_i \rangle$. From our results in **Matrix Representations of Cyclic Submodules**, we know that we can create a matrix representation of $T|_{W_i}$ that is $C(d_i)$. Thus, given any $m \times n$ matrix, M, we can consider M as a linear transformation, T, that is the linear operator associated with the $F[x]$-module, V^T. We can thus create matrix representations of T restricted to the cyclic submodules $W_1, W_2, ..., W_n$. Thus, we can create a matrix representation of T relative to a basis that looks like:

$$\begin{pmatrix} C[d_n] & & & \\ & C[d_{n-1}] & & \\ & & \ddots & \\ & & & C[d_1] \end{pmatrix}$$

Example 2. Consider the matrix[1],

$$\begin{pmatrix} -2 & 0 & 0 \\ -1 & -4 & -1 \\ 2 & 4 & 0 \end{pmatrix}$$

We can easily calculate that the characteristic polynomial of this matrix is $x^3 + 6x^2 + 12x + 8 = (x+2)^3$. $(A+2I) \neq 0$, but $(A+2I)^2 = 0$. Thus, the minimal polynomial for the matrix is $(x+2)^2$. We know that the largest invariant factor is simply the minimal polynomial. Furthermore, we know that the size of our canonical form matrix must be 3×3, and that our invariant factors must divide $(x+2)^3$. Thus, there are two invariant factors: $(x+2)^2 = x^2 + 4x + 4$ and $x + 2$. Therefore, the rational canonical form of the matrix is:

$$\begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & -4 \\ 0 & 1 & -4 \end{pmatrix}$$

7 Conclusion

To summarize our results, given any mxn matrix A, we can consider the $F[x]$ module for the vector space V of dimension n defined on A and thus achieve a rational canonical form for A. This form can be realised through finding the minimal polynomial for A, examining the invariant factors that divide this polynomial, and then constructing the companion matrices for these factors. Unlike diagonalization or Jordan Canonical Form, a Rational Canonical Form can be constructed for any matrix. Therefore, we have found a canonical representation for all matrices within the same equivalence class and achieved our goal of the classification of all linear transformations.

[1] Coley,Ian, http://www.math.ucla.edu/ iacoley/

Sources:

Coley,Ian. http://www.math.ucla.edu/ iacoley/.
Judson, Thomas. Abstract Algebra.
Pearl, Martin. Matrix Theory and Finite Mathematics. McGraw-Hill, Inc.(1973).
Rotman, Joseph. Advanced Modern Algebra. Pearson Education(2002).
Roman, Steven. Advanced Linear Algebra. Springer(2000).