Chapter 14

Linear Algebra over $\mathbb{Z}_p$

For each integer n, let $V = \mathbb{Z}_p^n$ be set of n-tuple of elements of $\mathbb{Z}_p = \{0, 1, \ldots p-1\}$ (we'll drop the overlines from now on). Of particular interest for applications, is the case of $p = 2$. One might think of the elements of $\mathbb{Z}_2^n$ as representing strings of bits on a computer. $\mathbb{Z}_p^n$ is an abelian group with

$$(a_1, a_2, \ldots a_n) + (b_1, b_2, \ldots b_n) = (a_1 + b_1, \ldots a_n + b_n)$$

as one might expect. The order of this group is p^n.

Let $S \subseteq V$ be a subgroup. By Lagrange's theorem $|S|$ must also be a power of p. We will explain this in a different way by borrowing the notion of a basis from linear algebra. Given $N \in \mathbb{Z}_p$ define

$$N(a_1, a_2, \ldots a_n) = (Na_1, Na_2, \ldots Na_n)$$

This is consistent with our earlier notation

$$N(a_1, a_2, \ldots a_n) = (a_1, \ldots a_n) + (a_1, \ldots a_n) + \ldots (a_1, \ldots a_n) \; (N \text{ times})$$

A collection of elements $v_1, v_2 \ldots v_k \in V$ is called *linearly independent* if the only solution to

$$a_1 v_1 + a_2 v_2 + \ldots a_k v_k = 0, \; a_i \in \mathbb{Z}_p$$

is

$$a_1 = a_2 = \ldots a_k = 0$$

Recall that $v_1, v_2 \ldots v_k \in S$ generates S if every element $s \in S$ can be written as a sum

$$s = a_1 v_1 + a_2 v_2 + \ldots a_k v_k$$

In this context the word "spans" is also used. A collection of elements $v_1, v_2 \ldots v_k \in S$ is called a *basis* if it is linearly independent and generates S.

Lemma 14.1. *If $v_1, v_2 \ldots v_k \in S$ generate S, then $|S| \leq p^k$. Equality holds if and only if this is a basis.*

Proof. Let $v_1, v_2 \dots v_k \in S$ generate S. Define a function $c : \mathbb{Z}_p^k \to S$ which assigns $a_1 v_1 + \dots a_k v_k \in \mathbb{Z}_p^n$ to the vector $(a_1, \dots a_k) \in \mathbb{Z}_p^k$. The function c is onto, therefore $|S| \leq |\mathbb{Z}_p^k| = p^k$.

Suppose that $v_1, v_2 \dots v_k$ is a basis, and suppose that $c(a_1, \dots a_k) = c(a_1', \dots a_n')$. Then

$$(a_1 - a_1')v_1 + \dots (a_n - a_n')v_n = a_1 v_1 + \dots a_k v_k - (a_1' v_1 + \dots a_k' v_k) = 0$$

By linear independence, this is only possible if $a_i = a_i'$. This proves that c is a one to one correspondence in this case. Therefore $|S| = p^k$.

Suppose that $|S| = p^k$...

□

An application of these ideas is in the construction of (linear) error correcting codes. Suppose a message, which we think of as a string of bits, is to be sent over a noisy medium. The noise causes some of the bits to be flipped to incorrect values. In order to detect those errors and possibly recover the orginal message, we can encode the message so as to add redundent "check" bits. The original message can be viewed as a vector in $\mathbb{Z}_2^k$. The encoded message is vector in a subspace $S \subset \mathbb{Z}_2^N$, and the function c constructed in the above proof can be used to encode the original message. We define the distance $d(u, v)$ between two vectors $u, v \in \mathbb{Z}_2^N$ to be the number of entries of u and v which differ. If u is the original encoded message and v the recieved messages, $d(u, v)$ is the number of errors in transmission. The further the distances between distinct code vectors, the better our chances of detecting/correcting errors.

There remains the problem of finding bases. Here we use the technique of Gauss Jordan elimination. Given a set of vectors

$$v_1 = (a_{11}, a_{12}, \dots a_{1n})$$

$$v_2 = (a_{21}, a_{22}, \dots a_{2n})$$

we arrange them in the rows of a matrix

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & & & \end{pmatrix}$$

We then apply a sequence of the following operations called elementary row operations:

- Interchange rows.
- Multiply all elements of a row a by nonzero element of $\mathbb{Z}_p$.
- Add a multiple of one row to another.

The goal is to get the matrix to reduced echelon form which means:

- The leftmost nonzero entry of any row is 1 (called a leading 1).
- The leading 1 occurs to the right of any leading 1 above it.
- A row consisting of 0's occurs at the bottom of the matrix.
- All entries above a leading 1 are 0. it.

The standard results from linear algebra, in our context, tells us:

Theorem 14.2. *Any matrix A over a field can be taken to a reduced echelon matrix B by a finite sequence of elementary row operations. The nonzero rows of B forms a basis of the sybgroup generated by the nonzero rows of A.*

Corollary 14.3. *Any subgroup of $\mathbb{Z}_p^n$ has a basis.*

Here's an example in $\mathbb{Z}_7$:

$$\begin{pmatrix} 2 & 3 & 0 \\ 4 & 5 & 1 \end{pmatrix} \overset{4Row1}{\longrightarrow} \begin{pmatrix} 1 & 5 & 0 \\ 4 & 5 & 1 \end{pmatrix} \overset{Row2-4Row1}{\longrightarrow} \begin{pmatrix} 1 & 5 & 0 \\ 0 & 6 & 1 \end{pmatrix}$$
$$\overset{6Row1}{\longrightarrow} \begin{pmatrix} 1 & 5 & 0 \\ 0 & 1 & 6 \end{pmatrix} \overset{Row1-5Row2}{\longrightarrow} \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 6 \end{pmatrix}$$

In Maple, this computation can done by

```
> matrix([[2,3,0], [4,5,1]]);
```

$$\begin{bmatrix} 2 & 3 & 0 \\ 4 & 5 & 1 \end{bmatrix}$$

```
> Gaussjord(%) mod 7;
```

$$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 6 \end{bmatrix}$$

14.4 Exercises

1. The weight of a vector $w(v)$ in $v \in \mathbb{Z}_2^N$ is the distance $d(v, 0)$. Show that $d(u, v) = w(u - v)$.
2. Let $S \subset \mathbb{Z}_2^N$ be a subspace. Prove that the minimum distance between distinct vectors of S is the minimum of weights of nonzero vectors $v \in S$.
3. Let $S \subset \mathbb{Z}_2^6$ be the subspace generated by rows of

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

List all the elements of S. Calculate the minimum distance between distinct vectors of S.

4. Find a basis for the subgroup of $\mathbb{Z}_5^4$ generated by $(1, 2, 3, 4)$ $(2, 3, 0, 1)$, $(0, 0, 1, 0)$ and $(3, 0, 2, 0)$.

Chapter 15

Nonabelian groups

Let's start with definition.

Definition 15.1. *A group consists of a set A with an associative operation $*$ and an element $e \in A$ satisfying*

$$a * e = e * a = a,$$

and such that for every element $a \in A$, there exists an element $a' \in A$ satisfying

$$a * a' = a' * a = e$$

A better title for this chapter would have been *not necessarily abelian groups*, since abelian groups are in fact groups.

Lemma 15.2. *An abelian group is a group.*

Proof. The extra conditions $e * a = a * e$ and $a' * a = a * a'$ follow from the commutative law. □

Before giving more examples, let's generalize some facts about abelian groups.

Lemma 15.3. *If $a * b = a * c$ then $b = c$. If $b * a = c * a$ then $b = c$.*

Corollary 15.4. *Given a, there is a unique element a', called the inverse such that $a * a' = a' * a = e$.*

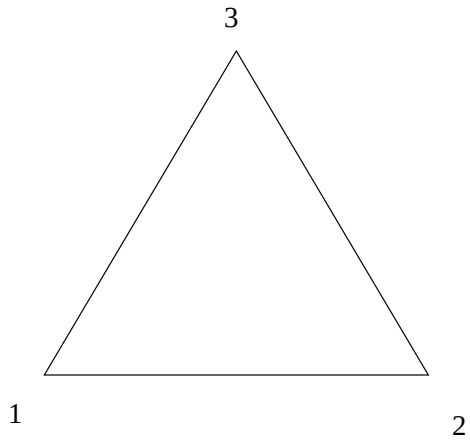
We want give some examples of genuinely nonabelian groups. The next example should already be familiar from linear algebra class (where F is usually taken to be $\mathbb{R}$ or maybe $\mathbb{C}$).

Example 15.5. *The set of $n \times n$ invertible (also known as nonsingular) matrices over a field F forms a group denoted by $GL_n(F)$. The operation is matrix multiplication, and the identity element is the identity matrix*

$$I = \begin{pmatrix} 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \dots & & & \end{pmatrix}$$

When $n = 1$, this is just F^* which is abelian. However, this group is not abelian when $n > 1$.

We want to consider a more elementary example next. Consider the equilateral triangle.



We want to consider various motions which takes the triangle to itself (changing vertices). We can do nothing I. We can rotate once counterclockwise.

$$R_+ : 1 \to 2 \to 3 \to 1.$$

We can rotate once clockwise

$$R_- : 1 \to 3 \to 2 \to 1.$$

We can also flip it in various ways

$$F_{12} : 1 \to 2, 2 \to 1, 3 \text{ fixed}$$

$$F_{13} : 1 \to 3, 3 \to 1, 2 \text{ fixed}$$

$$F_{23} : 2 \to 3, 3 \to 2, 1 \text{ fixed}$$

To multiply means to follow one motion by another. For example doing two R rotations takes 1 to 2 and then to 3 etc. So

$$R_+ R_+ = R_+^2 = R_-$$

Let's do two flips, F_{12} followed by F_{13} takes $1 \to 2 \to 2$, $2 \to 1 \to 3$, $3 \to 3 \to 1$, so

$$F_{12} F_{13} = R_+$$

Doing this the other way gives

$$F_{13} F_{12} = R_-$$

Therefore this multiplication is not commutative. The following will be proved in the next section.

Lemma 15.6. *$\{I, R_+, R_-, F_{12}, F_{13}, F_{23}\}$ is a group with I as the identity. It is called the triangle group.*

The full multiplication table can be worked out.

.	I	F_{12}	F_{13}	F_{23}	R_+	R_-
I	I	F_{12}	F_{13}	F_{23}	R_+	R_-
F_{12}	F_{12}	I	R_+	R_-	F_{13}	F_{23}
F_{13}	F_{13}	R_-	I	R_+	F_{23}	F_{12}
F_{23}	F_{23}	R_+	R_-	I	F_{12}	F_{13}
R_+	R_+	F_{23}	F_{12}	F_{13}	R_-	I
R_-	R_-	F_{13}	F_{23}	F_{12}	I	R_+

where each entry represents the product in the following order

.	a	b	$\ldots$
a	$a \cdot a$	$a \cdot b$	$\ldots$

This is latin square (chapter 3), but it isn't symmetric because the commutative law fails.

15.7 Exercises

1. 1. Determine the inverse for every element of the triangle group.
2. Prove lemma 15.3.
3. Let $(G, *, e)$ be a group. Prove that the inverse of the product $(x * y)' = y' * x'$.
4. The commutator of x and y is the expression $x * y * x' * y'$. Prove that $x * y = y * x$ if and only if the commutator $x * y * x' * y' = e$.
5. Prove that the multiplication table for a group is always a latin square (see the proof of lemma 3.10 for hints).