Math 167: Game Theory
UCLA

Darsh Verma

Winter 2026

Hello and welcome! As the title suggests, these are my lecture notes on Game Theory. Our professor is **Sylvester Zhang**. The textbook that we are using is **some game theory tb**.

The goal of these lecture notes is to write **understandable** math. Some dude said, "If you can't explain it to a six year old, then you don't understand it yourself". The hope is that anyone coming across these notes (like you!) will be able to at least take away the gist of these concepts. Email me at darsh [at] ucla [dot] edu if you find any errors!

Contents

List of Definitions

List of Theorems

1   Lecture 1: Jan 6

Today was the first lecture of the quarter. We spoke briefly about course logistics and preamble information, as well as a brief overview of the integers. Something cool I learned was a new perspective on the Euclidean Algorithm, which will be described below.

1.1   Course Preamble

This course will cover the basic foundations of Ring Theory. There will be 4 ways in which students are assessed – homeworks, quizzes (of which there are 2), midterm, and final exam.

1.2   Integers

To start off the lecture, we approached a few example problems together as a review of integers.

Example 1.1. Solve the following within the set of integers $\mathbb{Z}$

$$x^2 - y^2 = 31$$
$$(x+y)(x-y) = 31$$

First, notice that 31 is a *prime number.* Thus, our factors $x+y$ and $x-y$ must be $\pm 1, \pm 31$. This leads us to 4 combinations of

$$(x,y) = (16, 15), (-16, -15), (16, -15), (-16, -15)$$

Yay! Good start. From there, we went into some definition refreshers.

Definition (Divides)**.** If $a, b \in \mathbb{Z}$ and $b \neq 0$, then we say **"b divides a"** and denote $b \mid a$ or $a \vdots b$ if there exists some $c \in \mathbb{Z}$ such that $a = bc$

Definition (Greatest common divisor)**.** Let $a, b \in \mathbb{Z}$ with at least one being non-zero. We say $d \in \mathbb{Z}$ is the **greatest common divisor** of a and b and denote $\gcd(a, b) = d$ if

1. $d \mid a$ and $d \mid b$

2. d is the *largest* integer to satisfy (1)

Definition (Prime number)**.** We say $p \in \mathbb{Z}_{>1}$ is **prime** if its only positive divisors are 1 and p.

Theorem 1.1 (Fundamental Theorem of Arithmetic).

If $n \in \mathbb{Z}$ with $n \neq 0, \pm 1$, then there exists a unique *prime decomposition of n*

$$n = \pm p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$

where $p_1 < p_2 < \cdots < p_m$ are primes, and $a_1, ..., a_m \geq \mathbb{Z}_{>0}$.

Proof of existence (sketch). Assume $n \in \mathbb{Z}_{>1}$. Now if n is prime, we are done. Otherwise, there must exist some $a \in \mathbb{Z}$ with $1 < a < n$ such that $a \mid n$. Which leads to some $n/a \in \mathbb{Z}$ with $1 < n/a < n$.

By strong induction, both a and n/a have prime decompositions, and hence so does $n = a \cdot n/a$. $\qquad\square$

Theorem 1.2 (Division with Remainders).

Let $a, b \in \mathbb{Z}, b \neq 0$. Then there exists unique *$q \in \mathbb{Z}$ and $r \in \mathbb{Z}_{>0}$ such that*

   1. $a = bq + r$, and

   2. $0 \leq r < |b|$

Such q is called the quotient, and r is the remainder.

This leads us to a very *powerful* corollary!

Corollary 1.2.1 (Euclidean Algorithm).

This gives us a very fast algorithm to find $\gcd(a,b)$

$$\gcd(a,b) = \gcd(b,r)$$

Example 1.2. Find the greatest common divisor of 524 and 148.

$$
\begin{aligned}
&\gcd(524,148) \\
&= \gcd(148,80) && [524 = 148 \cdot 3 + 80] \\
&= \gcd(80,68) && [148 = 80 \cdot 1 + 68] \\
&= \gcd(68,12) && [80 = 68 \cdot 1 + 12] \\
&\quad\vdots \\
&= \gcd(4,0) = 4
\end{aligned}
$$

Remark. Instead of dividing with remainder, we can also simply **subtract**.

Let's do an example with this remark in mind!

Example 1.3. Simplify $\frac{2n+13}{n+7}$.

$$\gcd(2n+13, n+7) = \gcd(n+7, n+6) = \gcd(n+6, 1) = 1$$

Since both polynomials share a greatest common divisor of 1, the fraction must already be in its simplest form.

We then went over a stronger version of the previous remark.

Corollary 1.2.2.

For $a, b \in \mathbb{Z}$ and $b \neq 0$, if $a = sb + t$ for $s, t \in \mathbb{Z}$, then $\gcd(a, b) = \gcd(b, t)$

Proof. We seek to show that the set of all common divisors of a and b is equal to that of b and t. Consequently, the largest elements in both sets are the same.

Let d be some divisor of a and b. Indeed, if $d \mid a$ and $d \mid b$, then $a = dk$ and $b = dl$ for some $k, l \in \mathbb{Z}$. Then

$$t = a - bs = dk - dls = d(k - ls),$$

and so $d \mid t$, that is $d \mid b$ and $d \mid t$.

Conversely, if $d \mid b$ and $d \mid t$, then $d \mid (bs + t)$ so $d \mid a$. Thus, $d \mid a$ and $d \mid b$. □

Definition (Division Ring). A ring where all non-zero elements are invertible is sometimes called a "non-commutative field". Such a structure is known as a **(non-commutative) division ring**.

Remark. Technically, more rigorously, in general, "division rings" refer to rings where all elements are invertible, and doesn't imply non-commutativity.

To start, we considered the 4-dimensional vector space $\mathbb{H}$ with basis $1, i, j, k$. So elements are of the form $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$.

Addition is simple- we add like-terms!

$$v = a + bi + cj + dk$$
$$w = a' + b'i + c'j + d'k$$
$$(v + w) = (a + a') + (b + b')i + (c + C')j + (d + d')k$$

Now we need to define multiplication. We define these products as follows:

- 1 is the identity, and $rq = qr$ for any quaternion $q \in \mathbb{H}$ and $r \in \mathbb{R}$.

- For other basis vectors

$$i^2 = j^2 = k^2 = -1$$
$$ij = k \quad jk = -k$$
$$jk = i \quad kj = -i$$
$$ki = j \quad ik = -j$$

> **Intuition.** *Here, imagine i, j, and k lie on a circle in that order when traversed clockwise. Now, multiplication is simply traversing along that circle from the first element to the second, where CW implies positive and CCW implies negative.*

The product is then extended to all elements of $\mathbb{H}$ by using the distributive law.

Example 1.4. Compute $(a + bi + cj + dk)(a' + b'i + c'j + d'k)$

$$(a + bi + cj + dk)(a' + b'i + c'j + d'k) = aa' + ab'i + ac'j + ad'k+$$
$$ba'i + bb'(-1) + bc'k + bd'(-j)+$$
$$ca'j + cb'(-k) + cc'(-1) + cd'i+$$
$$da'k + db'j + dc'(-i) + dd'(-1)$$

$$(a + bi + cj + dk)(a' + b'i + c'j + d'k) = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i$$
$$+ (ac' - bd' + ca' + db')j + (ad' + bc' - cb' + da')k$$

Here comes the fun- let's now prove that $\mathbb{H}$ is a ring. We need to check that $+$ and $\times$ satisfy the desired properties.

Remember that $\mathbb{H}$ is just some vector space $\mathbb{R}^4$, so properties of $+$ simply follow. $\times$ and distributivity will be proved in HW3, and the identity is simple as well: $1 = 1 + 0i + 0j + 0k$.

How do we check that $\mathbb{H}$ has a multiplicative inverse? Well, recall from $\mathbb{C}$ that $\frac{1}{a+bi} = \frac{1}{a^2+b^2}(a - bi)$, and so by analogy, the inverse

$$v = a + bi + cj + dk \neq 0$$
$$\frac{1}{v} = \frac{1}{a + bi + cj + dk} = \frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk)$$

(a more rigorous proof will be given on the hw)

Note also that $\mathbb{R}$ and $\mathbb{C}$ are commutative *subrings* of $\mathbb{H}$.

Finally, as a summary, the ring $\mathbb{H}$ of quaternions is a non-commutative **division ring** (ring with 1 and each element has an inverse).

1.3   Basic properties of rings (cont'd)

Assume R is a ring. We already saw that the zero element, the identity, and for each element, its additive inverse, are all *unique*! This means that we can now define subtraction.

That is, we define $a - b := a + (-b)$.

Canncellation property: In a ring R, $a + b = a + c$ if and only if $b = c$.

Note that unless R is a division ring, we cannot apply the same logic to multiplication (elements don't have an inverse, and there may not even be a multiplicative identity!)

That doesn't necessarily mean the multiplication cancellation won't hold if R is not a division ring though!! In fact, we now discuss the cancellation property in integral domains.

Proposition 1.3.
If R is an integral domain, then $ab = ac, a \neq 0$ does imply $b = c$.

Proof. Begin by subtracting both sides by ac. We get

$$ab - ac = a(b - c) = 0$$

Since R is an integral domain and $a \neq 0$, we must have by definition of integral domains that $b - c = 0$. $\qquad \square$

Here is another useful fact

Proposition 1.4.

Any field F is an integral domain.

Proof. We need to show that for $a, b \in F$, if $ab = 0$ and wlog $a \neq 0$, then $b = 0$. Simply multiply both sides by a^{-1}, we get

$$a^{-1}(ab) = (a^{-1}a)b = b = 0 = 0 \cdot a^{-1}$$

$\square$

In general, not all integral domains can be fields. One example of this is $\mathbb{Z}$.

But is there some property to say that *some* integral domains are fields? Yes. There is.

Theorem 1.5.

If R is a finite *integral domain (i.e., $|R| < \infty$), then R is a field.*

>   **Intuition.** *The intuition here is that if R is finite, then it will have modular arithmetic-esque behavior. Meaning if you multiply every pair of elements then it has to like "circle back" at some point and go back to 1, and that's where we find the inverse.*

Proof. We need to show that every element in R has a multiplicative inverse. Since R is finite, let's first list out all of its elements

$$R = \{0, a_1, a_2, ..., a_n\}$$

(here we suppose R has n non-zero elements)

Pick any a_i. We'll show that there exist some a_i^{-1}. We do this by writing out the "row" of the multiplication table of R, aka $\{a_i a_1, a_i a_2, ..., a_i a_n\}$

Notice two things about this row: (1) none of these elements can be 0, since R is an integral domain. (2) there cannot be any duplicate elements, since by the cancellation property, we have $a_i a_j = a_i a_k$ implies that $a_j = a_k$ which means $j = k$.

Since no elements of the row are 0, and no elements repeat, we thus know that the row must contain every non-zero element in R. This is huge(!), as it implies that there exists some j where

$$a_i a_j = 1$$

where 1 is the identity, meaning $a_j = a_i^{-1}$. $\square$

We now have a complete picture of the types of rings!