We are all in this together

And we will get through this together.

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 10.1–10.3. Reading for Wed: 11.1–11.2.
- PS10 due today; PS11 outline due Thu; PS11 due on last day of class. BUT ALL DEADLINES ARE FLEXIBLE
- Problem session Fri 10:30–noon.
- Today's DJ: Jin.

HW accepted thru end of finals (May 19)

The Discrete Fourier Transform (DFT)

Definition

Fix $N \in \mathbf{N}$, let $\omega = e^{2\pi i/N}$ be the natural primitive Nth root of unity in $\mathbf{C}$, and let $f : \mathbf{Z}/(N) \to \mathbf{C}$ be a signal. We define the DFT of f to be $\hat{f} : \mathbf{Z}/(N) \to \mathbf{C}$ given by

fn on freq space

$$\hat{f}(k) = \frac{1}{N} \sum_{n=0}^{N-1} f(n)\omega^{-nk}.$$

Think of $\hat{f}(k)$ as the **spectrum** of f, because (roughly) $\hat{f}(k)$ measures the strength of the part of f that has "frequency k".

the "ω^{kx} part"

The inverse DFT

Definition

Let $\hat{f} : \mathbf{Z}/(N) \to \mathbf{C}$ be a spectrum function. The **inverse DFT** of $\hat{f}$ is defined to be

$$\sum_{k=0}^{N-1} \hat{f}(k)\omega^{kn}.$$

(DFT with a sign change.) & different constant.

Point of the inverse DFT is:

Theorem (Inversion Theorem)

Fix $N \in \mathbf{N}$, $\omega = \omega_N$, $f : \mathbf{Z}/(N) \to \mathbf{C}$ be a signal. If $\hat{f}$ is the DFT of f, then

$$f(n) = \sum_{k=0}^{N-1} \hat{f}(k)\omega^{kn}.$$

$f \xrightarrow{DFT} \hat{f} \xrightarrow{IDFT} f$

I.e., inverse DFT inverts the DFT.

(And inverse DFT computed in almost the same way.)

Proof of Inversion Theorem

Uses (see PS10):

Lemma (Orthogonality Lemma)

Fix $N \in \mathbf{N}$ and let $\omega = \omega_N$. For $t \in \mathbf{Z}/(N)$, we have:

t fixed

$$\sum_{k=0}^{N-1} \omega^{kt} = \begin{cases} N & \text{if } t = 0 \pmod N, \\ 0 & \text{otherwise.} \end{cases}$$

t=0

$\sum \omega^{kt}$

$= 1 + \cdots + 1$

Proof of Inversion:

x is constant; WTS this is equal to f(x)

$$\sum_{k=0}^{N-1} \hat{f}(k)\omega^{kx} = \frac{1}{N} \sum_{k=0}^{N-1} \left(\sum_{n=0}^{N-1} f(n)\omega^{-nk} \right) \omega^{kx}$$

switch $\Sigma\Sigma$

laws of exps

$kx - kn$

$$= \frac{1}{N} \sum_{h=0}^{N-1} \sum_{k=0}^{N-1} f(h)\omega^{kx-kn}$$

const w.r.t. k

$$= \frac{1}{N} \sum_{n=0}^{N-1} f(n) \left(\sum_{k=0}^{N-1} \omega^{k(x-n)} \right)$$

$t = x - n$

This is N when $0 = x - n$, 0 otherwise.

So $\sum_{n=0}^{N-1}$ reduces to one term, the $n = x$ term

$$= \frac{1}{N} f(x) \left(\text{sum when } n = x \right)$$

$$= \frac{1}{N} f(x)(N) = f(x)$$

Takeaway: Orthog means that double sums will often simplify in this manner.

The killer app: Fast DFT gives fast multiplication

Recall that multiplication of two polynomials of degree N takes time $O(N^2)$.

Thanks to convolution (see Sec. 9.4), we have the following fact:

> **FACT:** *If we can compute the DFT of a period N signal in (for example) time $O(N \log N)$, we can multiply two polynomials in time $O(N \log N)$.* (at least in principle)

2019: There exists an O(N log N) algorithm for multiplying N-digit numbers

Can actually adapt algorithm to N-digit numbers, i.e., a fast DFT let us perform ordinary multiplication (of zillion-digit numbers) way way faster. So we ask:

Motivating question: How do we compute the DFT in $O(N \log N)$ time?

Answer: Groups!

Current open problem: If you can understand groups just a little bit better, you can find algorithm for multiplying NxN matrices in O(N^{2+a little bit}).

Groups

Why is $\mathbb{F}_q^\times$ ab gp?

Definition

A **group** is a set G along with a binary operation $\cdot$, usually written as multiplication, such that the following axioms are satisfied.

1. *(Associativity)* For any $a, b, c \in G$, $(ab)c = a(bc)$. Mult in field is associative.
2. *(Identity)* There exists an element $1 \in G$ such that $1a = a = a1$ for all $a \in G$. Every field has an identity element.
3. *(Inverses)* For every $a \in G$, there exists some $a^{-1} \in G$ such that $aa^{-1} = 1 = a^{-1}a$. Every nonzero element of a field has a multiplicative inverse.

Multiplication in a field is commutative.

Definition

Let G be a group. To say that G is **abelian** means that for all $a, b \in G$, we have that $ab = ba$. abelian = commutative multiplication

Example: If $\mathbf{F}_q$ is a finite field, its multiplicative group $\mathbf{F}_q^\times$ is a finite abelian group.

non-0 elts

Subgroups

In abstract algebra, after we define a FOO, we often next define a subFOO.

Definition

Let G be a group. A **subgroup** of G is a sub*set* of G that is itself a group, using the same operation as G.

Notation: $H \leq G$ means H is a subgroup of a group G. The point of using $\leq$ is to distinguish between H being a sub*group* of G and H being merely a sub*set* of G ($H \subseteq G$).

Example: If G is a group, $a \in G$, then

$$\langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}$$

set of all powers of a, positive, negative, and zero

is a subgroup of G, called the **cyclic subgroup generated by** a. How do we know this is a subgroup?

Exmp $G = \mathbb{F}_{17}^{\times}$ $\left(\mathbb{F}_{17} \cong \mathbb{Z}/(17)\right)$

$\langle 4 \rangle = \{1, 4, 16, 13\} \pmod{17}$

$16 = -1$

$= \{1, 4, 13, 16\} \leq \mathbb{F}_{17}^{\times}$

Subgroup Theorem

Theorem (Subgroup Theorem)

Let G be a group, and let S be a subset of G. Then S is actually a subgroup of G if and only if all three of the following conditions hold.

1. *(Identity) $1 \in S$ (i.e., S contains the multiplicative identity of G).*
2. *(Multiplicative closure) S is closed under the operation of G, i.e., if $a, b \in S$, then $ab \in S$.*
3. *(Inverse closure) S is closed under taking inverses, i.e., if $a \in S$, then $a^{-1} \in S$.*

Proof that $\langle a \rangle$ is a subgroup of G

Suppose G a group, $a \in G$, and

$$S = \langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}.$$

Identity

1. $1 = a^0$, so $1 = a^0 \in S$ by defn of S.

2. [A] $x, y \in S$

So $x = a^n$, $y = a^k$ $(n, k \in \mathbb{Z})$

Closed multiplication

Then $xy = a^{n+k}$

which is in S by defn

[C] $xy \in S$

3. (A) $x \in S$

Closed under inverses

$x = a^n$ for some $n \in \mathbb{Z}$

So $x^{-1} = (a^n)^{-1} = a^{-n}$, $-n \in \mathbb{Z}$

(C) $x^{-1} \in S$ (by defn of S)

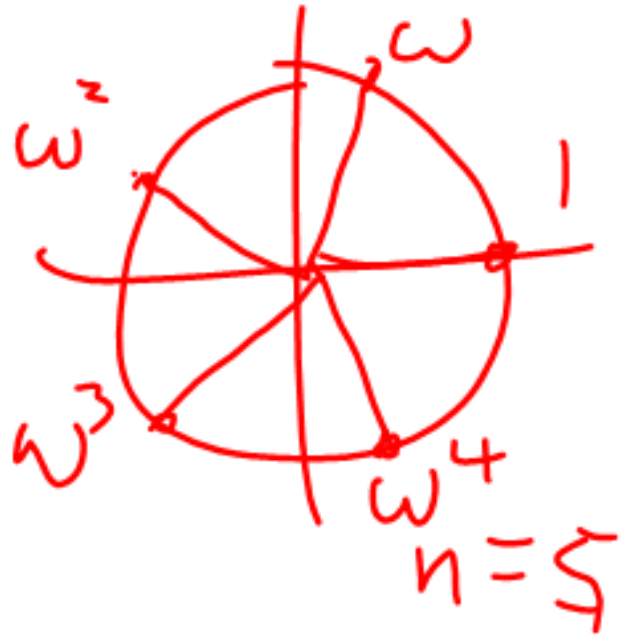
Subgroups of $\mathbf{C}^\times$

multiplicative group of nonzero complex numbers

Definition

We define C_n to be the set of all nth roots of unity in $\mathbf{C}$. In other words:

$$C_n = \{z \in \mathbf{C} \mid z^n = 1\}.$$



Fact: If $\omega = e^{2\pi i/n}$, then

$$C_n = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}.$$

$= \langle \omega \rangle$

Theorem

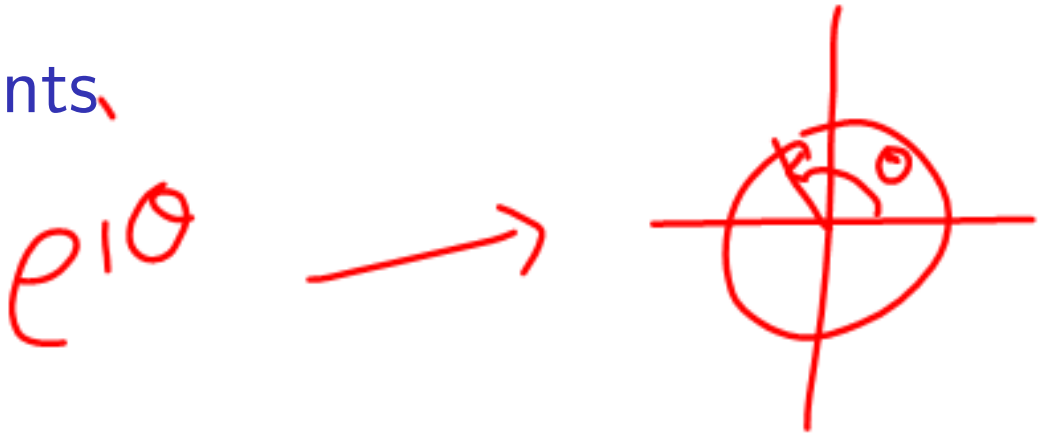
For $n, k \in \mathbf{N}$, we have that:

1. *C_n is a subgroup of $\mathbf{C}^\times$, the multiplicative group of the complex numbers; and*
2. *If k divides n, then C_k is a subgroup of C_n.*

Proof: PS11.

Fast Fourier Transform: from structure of groups C_n.

Orders of elements



Definition

Let G be a group and let a be an element of G. If $a^n = 1$ for some positive integer n, we define the **order** of a to be the *smallest* possible n such that $a^n = 1$. Otherwise, if $a^n \neq 1$ for all positive integers n, we say that a has **infinite order**.

Example: Let $\omega = e^{2\pi i/N}$.

We see:

$w^1, w^2, \ldots, w^{N-1} \neq 1$

But $w^N = \left(e^{\frac{2\pi i}{N}}\right)^N = e^{2\pi i} = 1$.

so $\text{order}(w) = N$.

$N = 6$

The powers of an element of order n

Ex. If α prim in $\mathbb{F}_{512}$, order$(\alpha)=511$
so α^k only uses $k \pmod{511}$

Theorem

Let G be a group and let a be an element of G of finite order n. Then the expression a^k depends precisely on the congruence class of k mod n. In other words, $k = \ell$ in $\mathbf{Z}/(n)$ if and only if $a^k = a^\ell$.

Proof: (A) $k=\ell \pmod n$ so $k=\ell+qn$ $(q\in\mathbb{Z})$

So $a^k = a^{\ell+qn} = a^\ell a^{qn} = a^\ell (a^n)^\ell = a^\ell 1^\ell = a^\ell$.

(C)

(A) $a^k = a^\ell \Rightarrow a^{k-\ell} = 1$

By Division Theorem: $k-\ell = qn + r \quad 0 \le r < n$

So $r = k-\ell-qn$, $a^r = a^{k-\ell-qn} = a^{k-\ell}a^{-qn} = 1\cdot 1 = 1$

So $a^r = 1$, $0 \leq r < n$

But n is the smallest positive integer power of a that is equal 1.
That means that r can't be positive, so r=0.

So $k - l = qn$, i.e. $k = l + qn$

$k \equiv l \pmod{n}$

The different meanings of order

Corollary

Let G be a group and let a be an element of G of finite order n. Then the cyclic subgroup $\langle a \rangle$ contains n elements (i.e., has order n).

Proof: Elts of $\langle a \rangle \iff$ possible a^{thing}
$\iff$ possible $k \pmod n$
$\iff \{a^0 = 1, a^1, a^2, \ldots, a^{n-1}\}$
(n things)

Theorem

Let G be a group and let a be an element of G of finite order n. Then the order of a^k is $\dfrac{n}{\gcd(k,n)}$.

Proof: PS11.

Cosets

Definition

Let G be a group, and let H be a subgroup of G. For $a \in G$, we define the **left multiplicative coset** aH to be

$$aH = \{ah \mid h \in H\}. \tag{1}$$

If the context is clear, instead of saying "left multiplicative coset", we just say **coset**. (In particular, since we mainly care about abelian groups, we won't worry too much about left cosets vs. right cosets.)

Example: $\langle 4 \rangle$ in $G = \mathbf{F}_{17}^{\times}$

$H = \langle 4 \rangle =$

Cosets of H in G?