Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1:

Lecture 01: 1/31/24: https://youtu.be/WMFJ9LPNXMo

Introduction: Motivation through Cryptography.

Grading / Administrative

- Move at fast pace: Class Participation: 5%. HW: 15%. Midterm: 40% (if there are two exams only best counts). Final exam: 40%. You may also do a project for 10% of your grade (which reduces all other categories proportionally).
- Pre-reqs: Calc III, basic combinatorics / set theory, linear algebra.

Office hours / feedback

- TBD and when I'm in my office (schedule online)

Being Prepared

Never know when an opportunity presents itself....



S. J. Miller at the Sarnak 61st Dinner

(copyright C. J. Mozzochi, Princeton N.J)

Being Prepared

- Your Job:
  - Be prepared for class: do reading, think about material.
  - Come to me, the TAs and each other with questions.
- My/TAs Job:
  - Provide resources, guiding questions.
  - Be available.

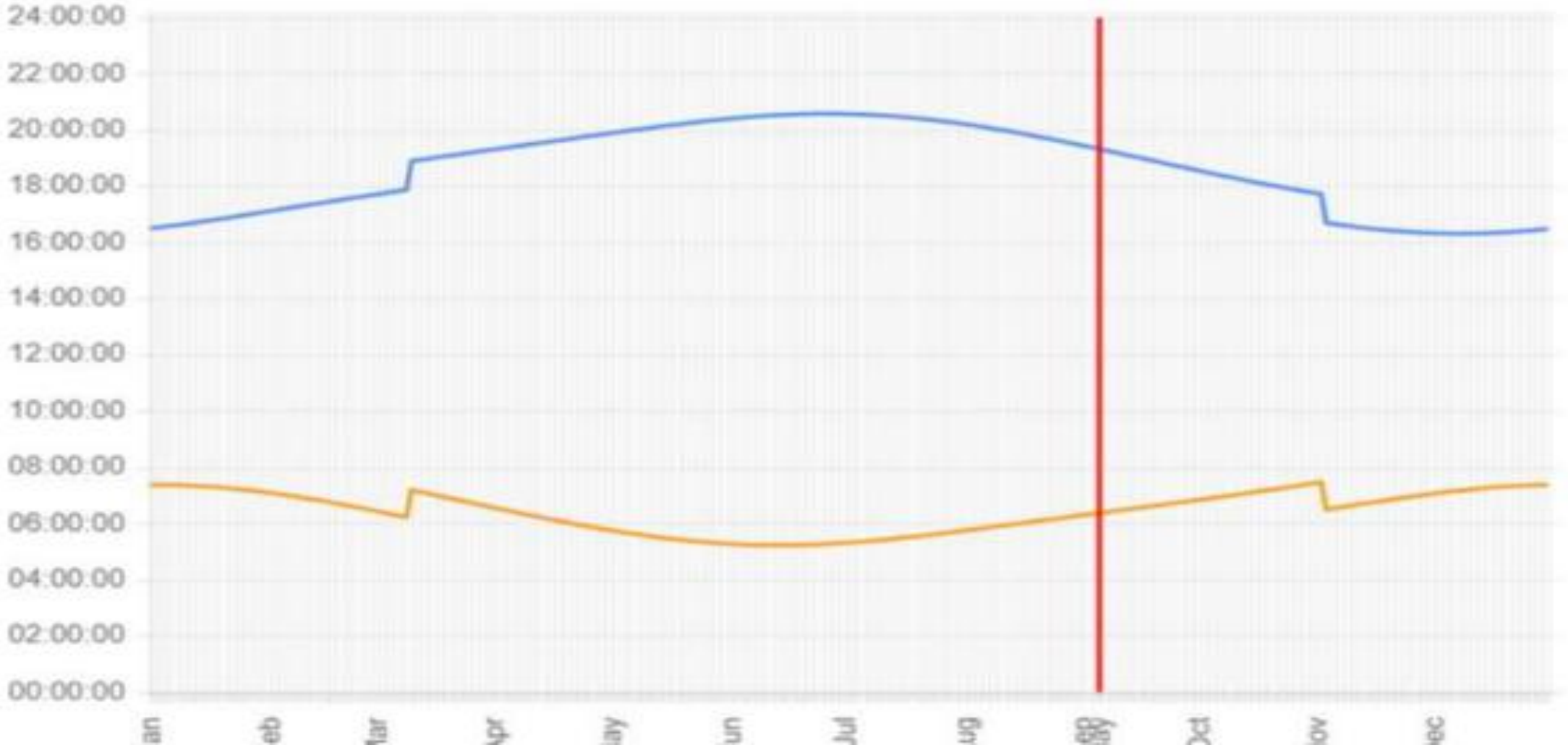
Other: Advice from Jeff Miller

- Party less than the person next to you.
- Take advantage of office hours / mentoring.
- Learn to manage your time: no one else wants to.

Happy to do practice interviews, adjust deadlines....

Year distribution of sunrise and sunset times in North Adams, MA – 2019

https : // sunrise – sunset.org / us / north – adams – ma



Who America is rooting for in the Super Bowl:



Motivation of Abstract Algebra through Cryptography:

- Introduction to Cryptography: Alphabet codes pdf

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: Video from Sec 2:

Lecture 02: 2/6/24: https://youtu.be/8E-zgWvRfT8

Chapter One: Terminology (1-1, onto, equivalence), Proof Techniques (Induction), Binomial Theorem, Predicting Formulas.

Section 1 video here: https://youtu.be/2QpkgY64J4o

Notate: 1-1, onto, equivalence

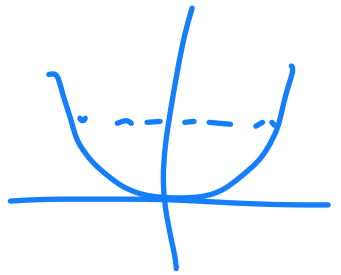
1-1 or injective means if $f(x) = f(y)$ then $x = y$

can do $f(x) = f(y)$ if and only if (iff) $x = y$

onto or surjective if $f: A \to B$, given any $b \in B$ there is an $a \in A$ such that $f(a) = b$. Note: $\exists$ = there exists $\forall$ = for all

bijection if it is injective and surjective;

$f(x) = x^2$ is a bijection from $[0, 2]$ to $[0, 4]$ But not from $[-2, 2]$ to $[0, 4]$.



Reflexive if $x \sim x$, Symmetric if $x \sim y$ then $y \sim x$, transitive if $\begin{matrix} x \sim y \\ y \sim z \end{matrix} \Rightarrow x \sim z$

Satisfy all 3 called equivalence.

Examples for $\sim$: $=$, multiples of vectors, clock arithmetic, $<$ not symm, not reflexive is transitive

Proofs by Induction: Definition, Sum of odds, powers.

Statement $P(n)$

Want to show holds for all n

$P(n)$ is $1+2+\cdots+n = n(n+1)/2$

Direct Proof:

$S = 1 + 2 + \cdots + (n-1) + n$

$S = n + (n-1) + \cdots + 2 + 1$

$2S = (n+1) + (n+1) + \cdots + (n+1) + (n+1) = n(n+1)$

Thus $S = \frac{n(n+1)}{2}$

Induction

One of the most important techniques we have for proving results.

Say we have some statement P(n). Perhaps P(n) is “the sum of the first n integers is n(n+1)/2”.

We can check this for various n; every time we check it is true but that is NOT the same as a proof!

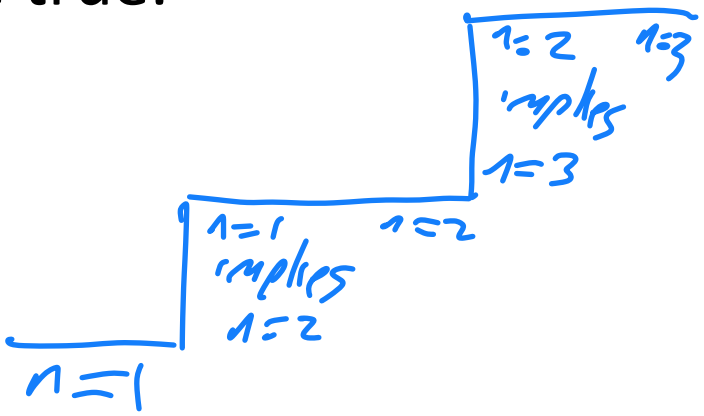
Example: $\frac{16}{64} \neq \frac{1}{4}$, $\frac{19}{95} \neq \frac{1}{5}$, $\frac{49}{98} \neq \frac{1}{2}$ but $\frac{12}{24}$ is not $\frac{1}{4}$.

Induction

Say we have some statement P(n). Perhaps P(n) is “the sum of the first n integers is n(n+1)/2”.

Imagine we can show the following two statements are true.

1. P(1) is true, and
2. Whenever P(n) is true then P(n+1) is true.



If we can do this we now have P(n) is true for all n!

(Note: Sometimes we start at n=0 not n=1)

Induction

Say we have some statement P(n). Perhaps P(n) is “the sum of the first n integers is n(n+1)/2”.

Imagine we can show the following two statements are true.

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Why does this imply that it holds for all n?

Induction (Box, Dirichlet, Pigeonhole Principle)

Imagine we can show the following two statements are true.

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Take n=1: thus the second becomes P(1) true implies P(2) true

P(1) is true

P(1) true implies P(2) true

THEREFORE since P(1) is true we now know P(2) is true.

Induction (Box, Dirichlet, Pigeonhole Principle)

Imagine we can show the following two statements are true.

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

We know P(1) and P(2) are true.
Take n=2: thus the second becomes P(2) true implies P(3) true
P(2) is true
P(2) true implies P(3) true
THEREFORE since P(2) is true we now know P(3) is true.

Induction (Box, Dirichlet, Pigeonhole Principle)

Imagine we can show the following two statements are true.

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

We know P(1), P(2) and P(3) are true.
Take n=3: thus the second becomes P(3) true implies P(4) true
P(3) is true
P(3) true implies P(4) true
THEREFORE since P(3) is true we now know P(4) is true. AND SO ON!

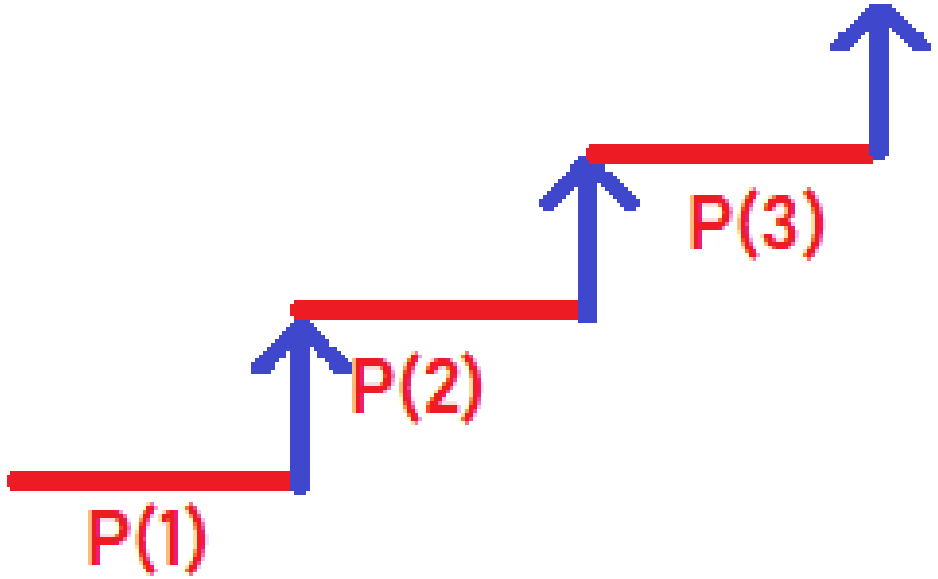
Induction (Box, Dirichlet, Pigeonhole Principle)

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

This is often viewed

as a staircase.



Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

We will prove this by induction. There are two steps.

First we prove P(1) is true, then we show IF P(n) is true THEN P(n+1) is true.

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 1: Base Case: We must show P(1) is true.

Thus we must show that when n=1, we have 1 = 1(1+1)/2.

This however follows immediately!

We are done with the base case.

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

We are done with the base case. We could try to do n=2 or n=3 to build up intuition, but it is not necessary.

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

Extra work: If n=2 let's check: Does 1+2 = 2(2+1)/2? YES!

Extra work: if n=3 let's check: Does 1+2+3 = 3(3+1)/2? YES!

These extra checks are not a substitute for a proof, but the more values of n that work, the more confident we are that it is true.

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

How should we proceed? When we look at P(n+1), do we see anything related to P(n)?

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

How should we proceed? Notice that the sum for n+1 starts off exactly as the sum for n!

What are we assuming we know about 1 + 2 + … + n? We are assuming it equals ….

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

How should we proceed? Notice that the sum for n+1 starts off exactly as the sum for n!

What are we assuming we know about 1 + 2 + … + n? We are assuming it equals n(n+1)/2.

Thus let's substitute for 1 + 2 + … + n in 1 + 2 + … + n + (n+1).

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

Using the inductive assumption, we have

1 + 2 + … + n + (n+1) = (1 + 2 + … + n) + (n+1) = n(n+1)/2 + (n+1).

Now we just need to show the far right equals our claim, (n+1)(n+1+1)/2. How do we add two fractions?

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

We have 1 + 2 + … + n + (n+1) = n(n+1)/2 + (n+1).

But $\frac{n(n+1)}{2} + (n+1) =$

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

We have 1 + 2 + … + n + (n+1) = n(n+1)/2 + (n+1).

But $\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} =$

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

We have 1 + 2 + … + n + (n+1) = n(n+1)/2 + (n+1).

But $\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{n(n+1) + 2(n+1)}{2} =$

Example: P(n): 1 + 2 + … + n = n(n+1)/2

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: We now get to ASSUME that P(n) is true, and we must show that P(n+1) is true.

OK, we now get to assume P(n) is true, we want to prove P(n+1) is true.

What does this mean?

P(n) true means we assume 1 + 2 + … + n = n(n+1)/2.

We want to prove that P(n+1): 1 + 2 + … + n + (n+1) = (n+1)(n+1+1)/2 is true.

We have 1 + 2 + … + n + (n+1) = n(n+1)/2 + (n+1).

But $\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$, which is what we needed to show, completing the proof (as n+2 = n+1+1)!

Example: P(n): $1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

The proof is similar to what we just did!

Step 1: The Base Case: n=1: Is $1^2 = 1(1+1)(2*1 + 1)/6$? YES!

We don't need to, but we can check other values of n.

If n=2 does $1^2 + 2^2 = 2(2+1)(2*2+1)/6$? YES!

If n=3 does $1^2 + 2^2 + 3^2 = 3(3+1)(2*3 + 1)/6$? YES!

Example: P(n): $1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Step 2: Inductive Step: Assume P(n) is true, must show P(n+1) is true.

Since we are assuming P(n) is true, what do we know?

P(n) is true means $1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6$.

We must show P(n+1) is true. What is that?

P(n+1) is $1^2 + 2^2 + \ldots + n^2 + (n+1)^2 = (n+1)(n+1+1)(2(n+1)+1)/6$, note the right hand side is $(n+1)(n+2)(2n+3)/6$.

So is $1^2 + 2^2 + \ldots + n^2 + (n+1)^2 = = n(n+1)(2n+1)/6 + (n+1)^2$.

We have $\frac{n(n+1)(2n+1)}{6} = \frac{6(n+1)2}{6} = \frac{(n+1)(n(2n+1)+\ 6(n+1))}{6} = \frac{(n+1)(2n2+n+6n+6)}{6} \equiv \frac{(n+1)(2n2+7n+6)}{6}$

Doing some algebra, we see $2n2 + 7n + 6$ equals (n+2)(2n+3) by FOIL, completing the proof.

Example: P(n): $1 + 3 + \ldots + (2n-1) = n^2$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

The proof is similar to what we just did!

Step 1: The Base Case: n=1: Is $1 = 1^2$? YES!

We don't need to, but we can check other values of n.

If n=2 does

If n=3 does

Rest of the proof is similar to what we've done before….

Example: P(n): $1 + 3 + \ldots + (2n-1) = n^2$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

The proof is similar to what we just did!

Step 1: The Base Case: n=1: Is $1 = 1^2$? YES!

We don't need to, but we can check other values of n.

If n=2 does $1 + 3 = 2^2$? YES!

If n=3 does $1 + 3 + 5 = 3^2$? YES!

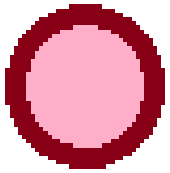
Rest of the proof is similar to what we've done before….

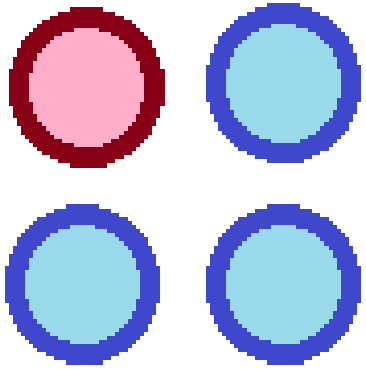
Example: P(n): $1 + 3 + \ldots + (2n-1) = n^2$

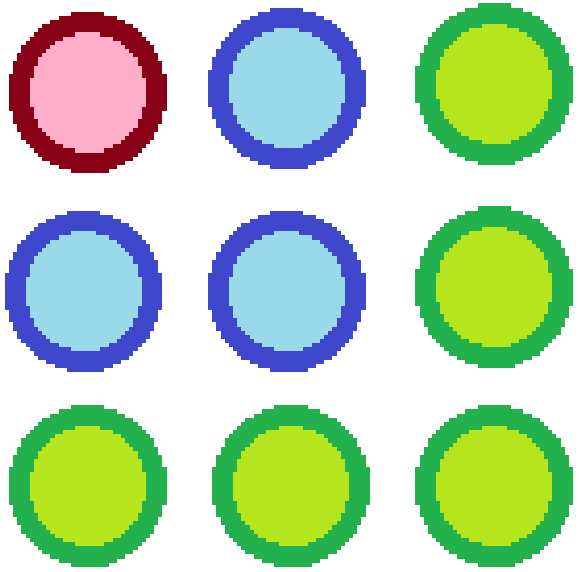
To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Can prove in other ways than Induction….







Example: P(n): 133 divides $11^{n+1} + 12^{2n-1}$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Let's try to show P(1) is true: does 133 divide $11^{1+1} + 12^{2*1-1}$?

Example: P(n): 133 divides $11^{n+1} + 12^{2n-1}$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Let's try to show P(1) is true: does 133 divide $11^{1+1} + 12^{2*1-1}$?

Yes, as $11^{1+1} + 12^{2*1-1} = 11^2 + 12 = 121 + 12 = 133$, which is clearly a multiple of 133.

Example: P(n): 133 divides $11^{n+1} + 12^{2n-1}$

To prove P(n) is true for all n, must show

1. Base case: P(1) is true, and
2. Inductive Step: Whenever P(n) is true then P(n+1) is true.

Now assume P(n) is true, we must show P(n+1) is true.

Can assume 133 divides $11^{n+1} + 12^{2n-1}$, must show 133 divides $11^{n+1} + 12^{2n-1}$.

$$\begin{aligned} 11^{(n+1)+1} + 12^{2(n+1)-1} &= 11^{n+1+1} + 12^{2n-1+2} \\ &= 11 \cdot 11^{n+1} + 12^2 \cdot 12^{2n-1} \\ &= 11 \cdot 11^{n+1} + (133 + 11)12^{2n-1} \\ &= 11\left(11^{n+1} + 12^{2n-1}\right) + 133 \cdot 12^{2n-1}. \quad \text{(A.6)} \end{aligned}$$

By the inductive assumption 133 divides $11^{n+1} + 12^{2n-1}$; therefore, 133 divides $11^{(n+1)+1} + 12^{2(n+1)-1}$, completing the proof.

Getting a feel for the answer….

We showed $1 + 2 + \ldots + n = n(n+1)/2 = n^2/2 + n/2$.

Is this reasonable?

How can we try to get an UPPER BOUND and a LOWER BOUND for the sum?

$0 \le 1 \le n \le 1+2+\cdots+n \le n \cdot n$

But $\left(\text{"}\frac{n}{2}\text{"}+1\right)+\cdots+n \ge \frac{n}{2} \cdot \frac{n}{2} = \frac{n^2}{4}$

"$\frac{n}{2}$"+1 … + n: last half of summands

$\frac{n}{2}$: # of summands

$\frac{n}{2}$: each is at least

Getting a feel for the answer….

We showed $1 + 2 + \ldots + n = n(n+1)/2 = n^2/2 + n/2$.
Is this reasonable?

How can we try to get an UPPER BOUND and a LOWER BOUND for the sum?

Every term in the sum is at most ???
Every term in the sum is at least ???
The number of terms is ???
Thus an upper bound is ???
Thus a lower bound is ???

Getting a feel for the answer….

We showed $1 + 2 + \ldots + n = n(n+1)/2 = n^2/2 + n/2$.

Is this reasonable?

How can we try to get an UPPER BOUND and a LOWER BOUND for the sum?

Every term in the sum is at most n

Every term in the sum is at least 1

The number of terms is n

Thus an upper bound is $n*n = n^2$

Thus a lower bound is $1*n = n$.

Note there is a large difference between the upper and lower bounds, need to do better.

Getting a feel for the answer….

We showed $1 + 2 + \ldots + n = n(n+1)/2 = n^2/2 + n/2$.
Is this reasonable?

How can we try to get an UPPER BOUND and a LOWER BOUND for the sum?

Every term in the sum is at most n
The number of terms is n
Thus an upper bound is $n*n = n^2$

The last half of the terms are each at least n/2 and there are n/2.
Thus a lower bound is $n/2 * n/2 = n^2/4$.

Now $n^2 / 4 \leq 1 + 2 + \ldots + n \leq n^2$, note these bounds are of the same power in n!

Final thoughts on sums of powers….

Hardest part of the induction is knowing what to PROVE.

How can we find the formula?

Looking at the cases we've done it looks like it is always a polynomial of degree one higher than the power, constant term is zero, leading term (if sum of kth powers) is $n^{k+1} / (k+1)$.

Note 2 points determine a line, 3 points a quadratic (parabola), 4 a cubic, and so on; we can evaluate the sum for a few points and then INTERPOLATE and figure out the polynomial!

Homework: Prove $1^3 + 2^3 + \ldots + n^3 = n^2 (n+1)^2 / 4$.

False proofs by Induction

The following is my favorite false proof by induction. Where is the mistake?

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Let's try to prove this by induction. We must show:

1. Base Case: In any group with 1 person, everyone has the same name.
2. Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

False proofs by Induction

The following is my favorite false proof by induction. Where is the mistake?

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Let's try to prove this by induction. We must show:

1. Base Case: In any group with 1 person, everyone has the same name.

PROOF OF BASE CASE: This follows immediately, as….

False proofs by Induction

The following is my favorite false proof by induction. Where is the mistake?

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Let's try to prove this by induction. We must show:

1. Base Case: In any group with 1 person, everyone has the same name.

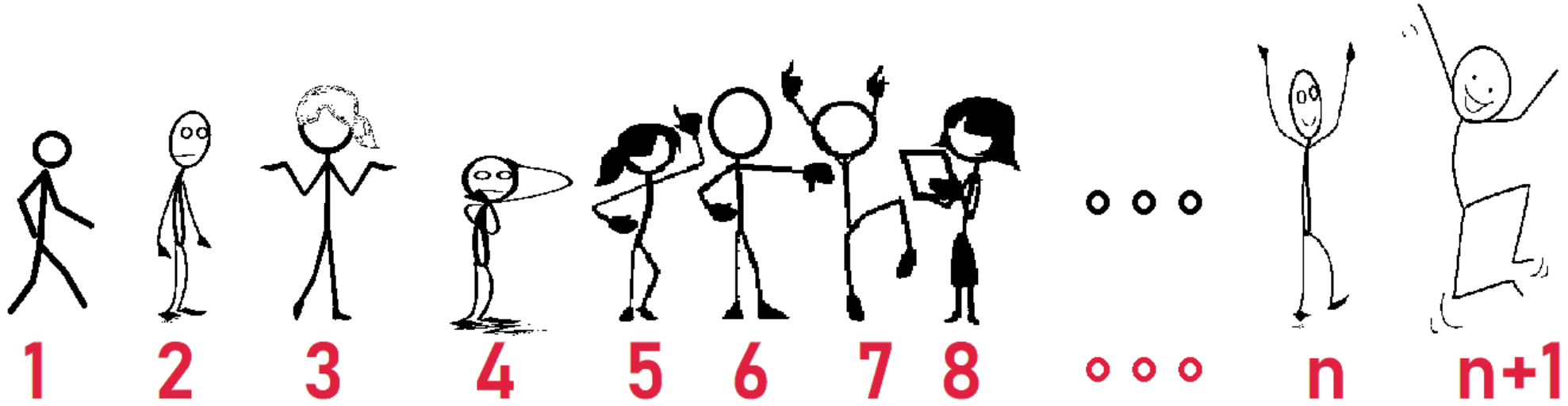
PROOF OF BASE CASE: This follows immediately, as there is only one person in the group, so clearly everyone in the group has the same name!

False proofs by Induction

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

"PROOF" OF INDUCTIVE STEP: We assume everyone in a group of size n has the same name, must show true for a group of size n+1. Consider a group of n+1 people. How can we use the inductive assumption (all groups of size n have all with the same name)? Can you find some groups of size n?

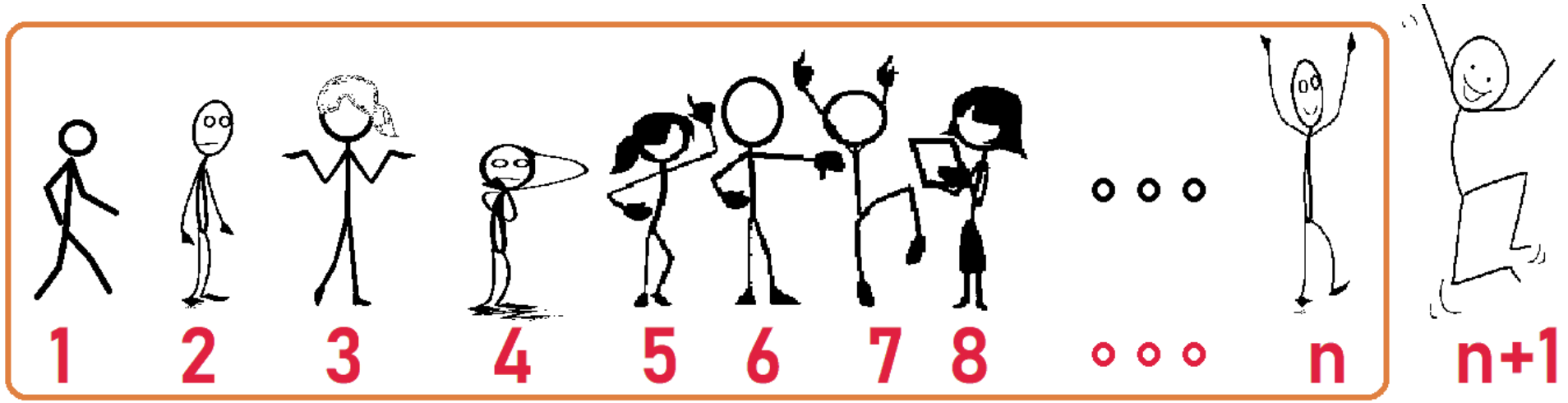


False proofs by Induction

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

"PROOF" OF INDUCTIVE STEP: We assume everyone in a group of size n has the same name, must show true for a group of size n+1. Consider a group of n+1 people. How can we use the inductive assumption (all groups of size n have all with the same name)? Can you find some groups of size n? First n people all have the same name!

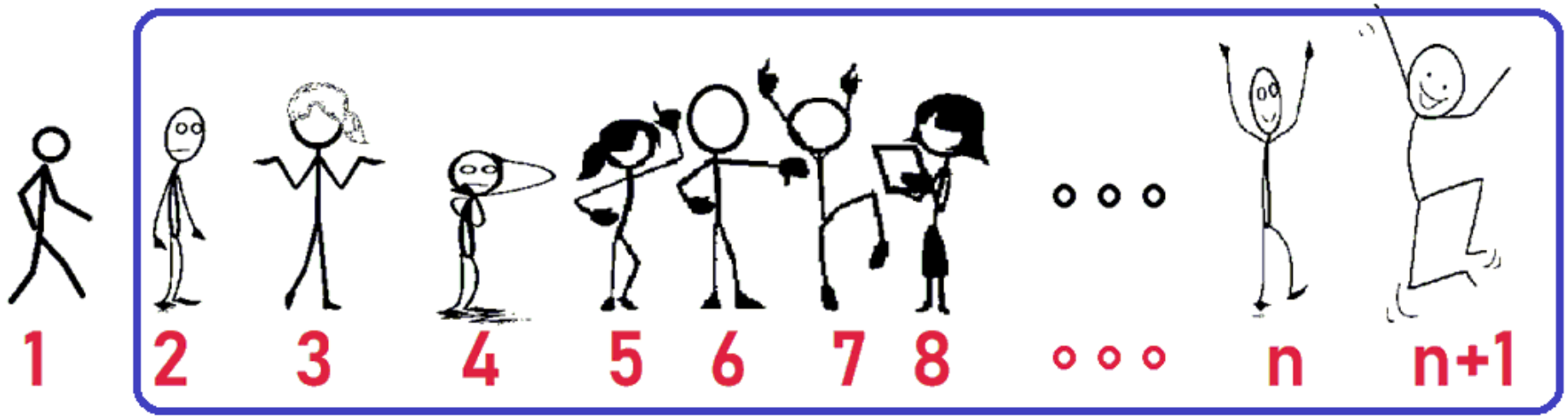


False proofs by Induction

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

"PROOF" OF INDUCTIVE STEP: We assume everyone in a group of size n has the same name, must show true for a group of size n+1. Consider a group of n+1 people. How can we use the inductive assumption (all groups of size n have all with the same name)? Can you find some groups of size n? Last n people all have the same name!

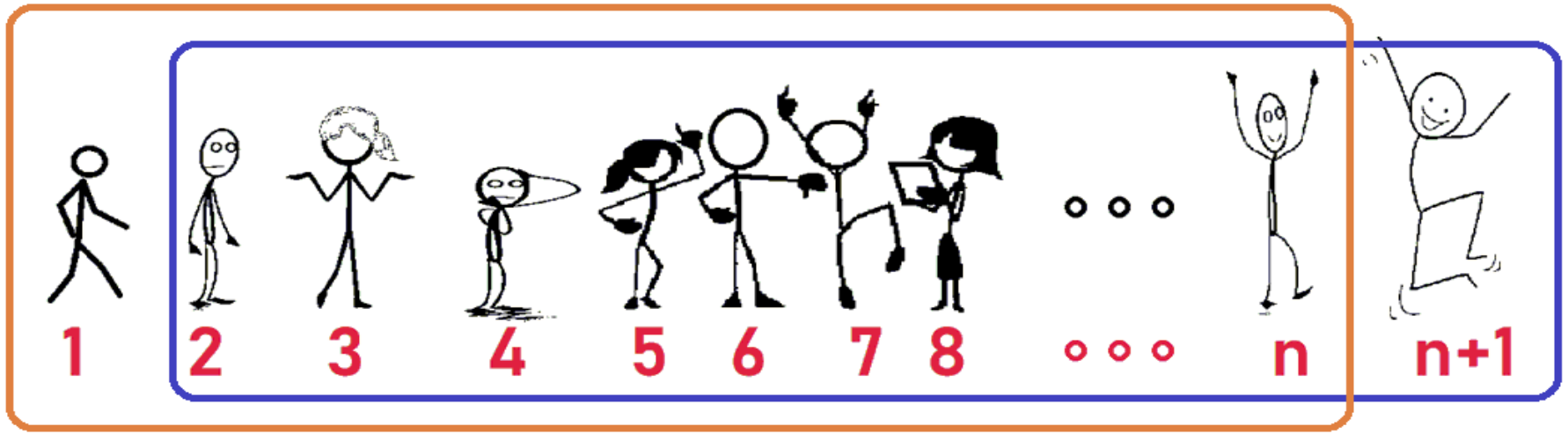


False proofs by Induction

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

"PROOF" OF INDUCTIVE STEP: We assume everyone in a group of size n has the same name, must show true for a group of size n+1. Consider a group of n+1 people. How can we use the inductive assumption (all groups of size n have all with the same name)? Can you find some groups of size n? Note people 2, 3, …, n are in both groups!

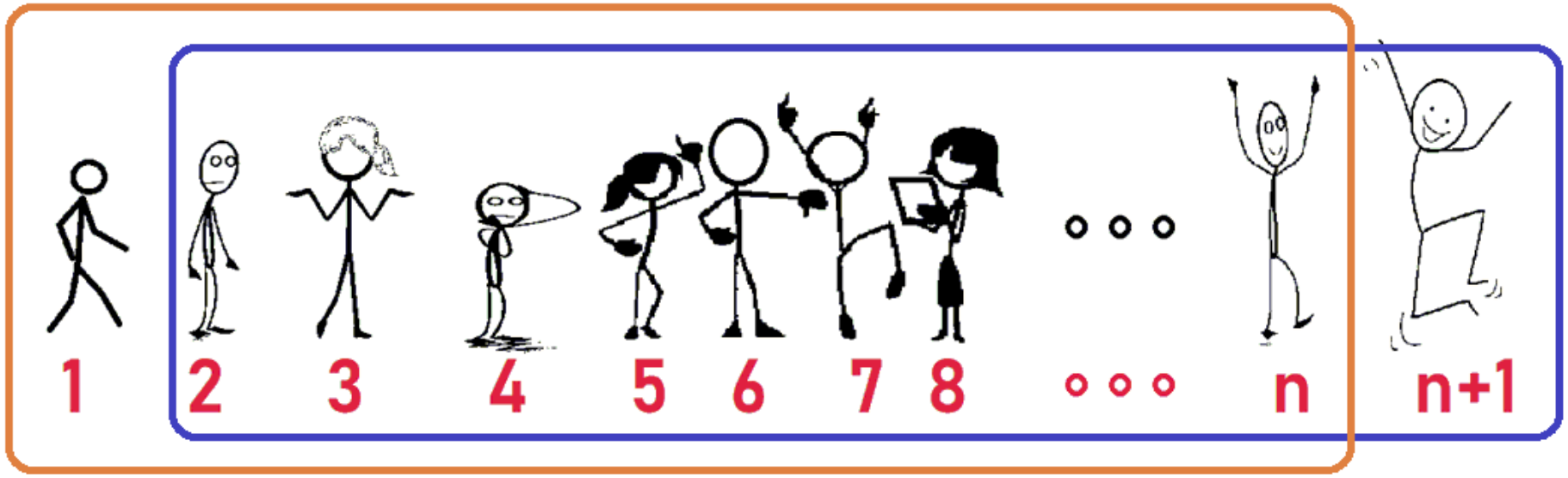


False proofs by Induction

P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

"PROOF" OF INDUCTIVE STEP: We assume everyone in a group of size n has the same name, must show true for a group of size n+1. Consider a group of n+1 people. How can we use the inductive assumption (all groups of size n have all with the same name)? Can you find some groups of size n? Note people 2, 3, …, n are in both groups! Thus everyone in the first n has the same name, everyone in the last n has the same name, and since people 2, 3, …, n are in both that means those two names are the same and our proof is done! If your name is not Steve Miller, you should be skeptical. Mistake?

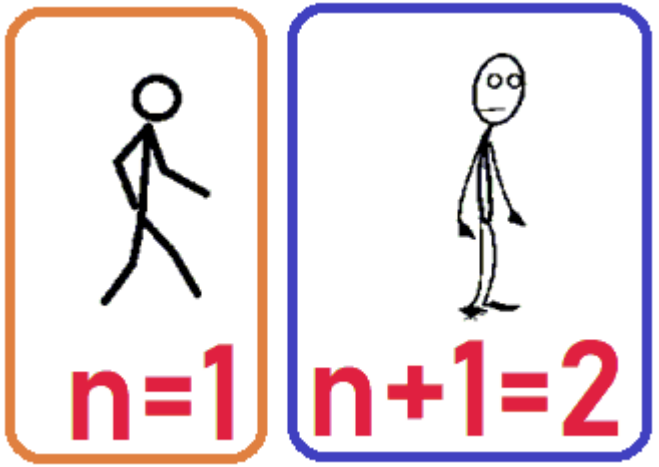


False proofs by Induction

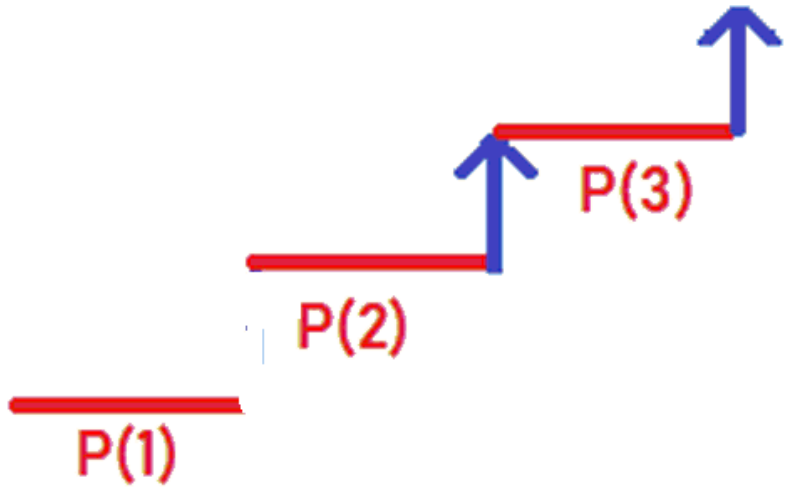
P(n): In any group of n people, everyone has the same name! (Note different groups of n people can have different names).

Inductive Step: If everyone in a group of size n has the same name, then everyone in a group of size n+1 has the same name.

"PROOF" OF INDUCTIVE STEP: The mistake is we drew this for a "large" n. Remember we must show for ANY n that if P(n) is true then P(n+1) is true. If n is 2 or more then there is a person in both groups, but if n=1 there is not!



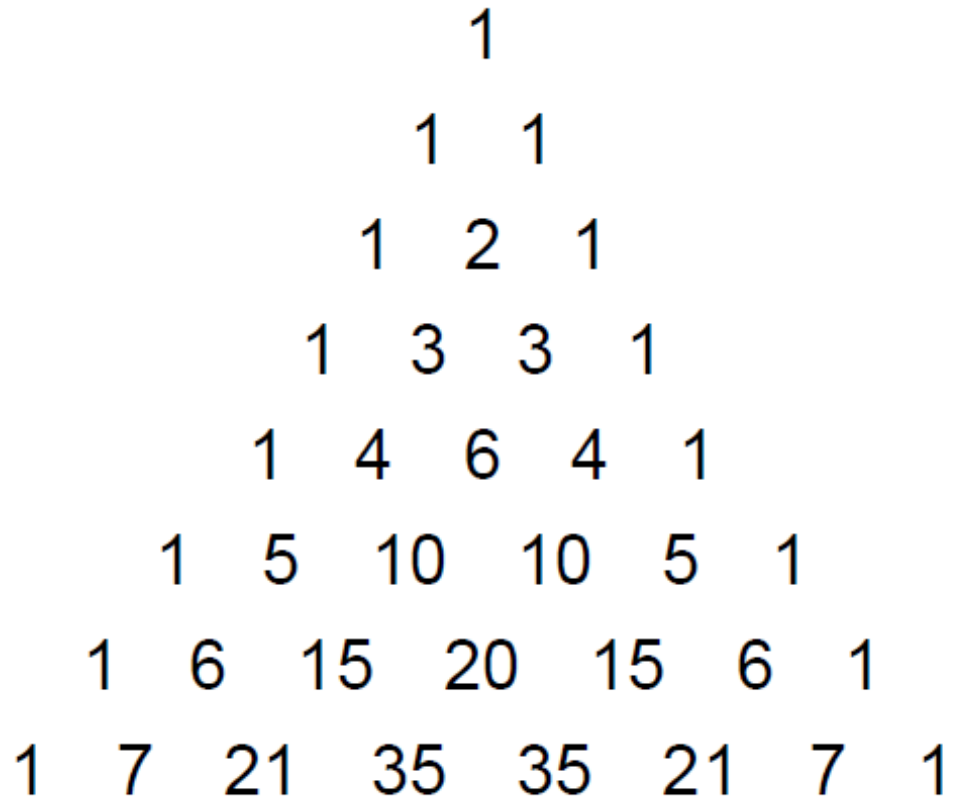
When n=1 we see there is no overlap!



Pascal's Triangle

The numbers in the nth row of Pascal's Triangle are the coefficients we obtain in expanding $(x+y)^n$.

Equivalently, we have two diagonals of 1, and all other elements are the sum of the elements in the row above immediately to the left and immediately to the right.



Expanding $(x + y)^n$

$(x + y)^0 = \mathbf{1}$

$(x + y)^1 = \mathbf{1}\, x + \mathbf{1}\, y$

$(x + y)^2 = \mathbf{1}\, x^2 + \mathbf{2}\, x\, y + \mathbf{1}\, y^2.$

$(x + y)^3 = \mathbf{1}\, x^3 + \mathbf{3}\, x^2\, y + \mathbf{3}\, x\, y^2 + \mathbf{1}\, y^3.$

We can keep going and get more and more rows…..

1

1 1

1 2 1

1 3 3 1

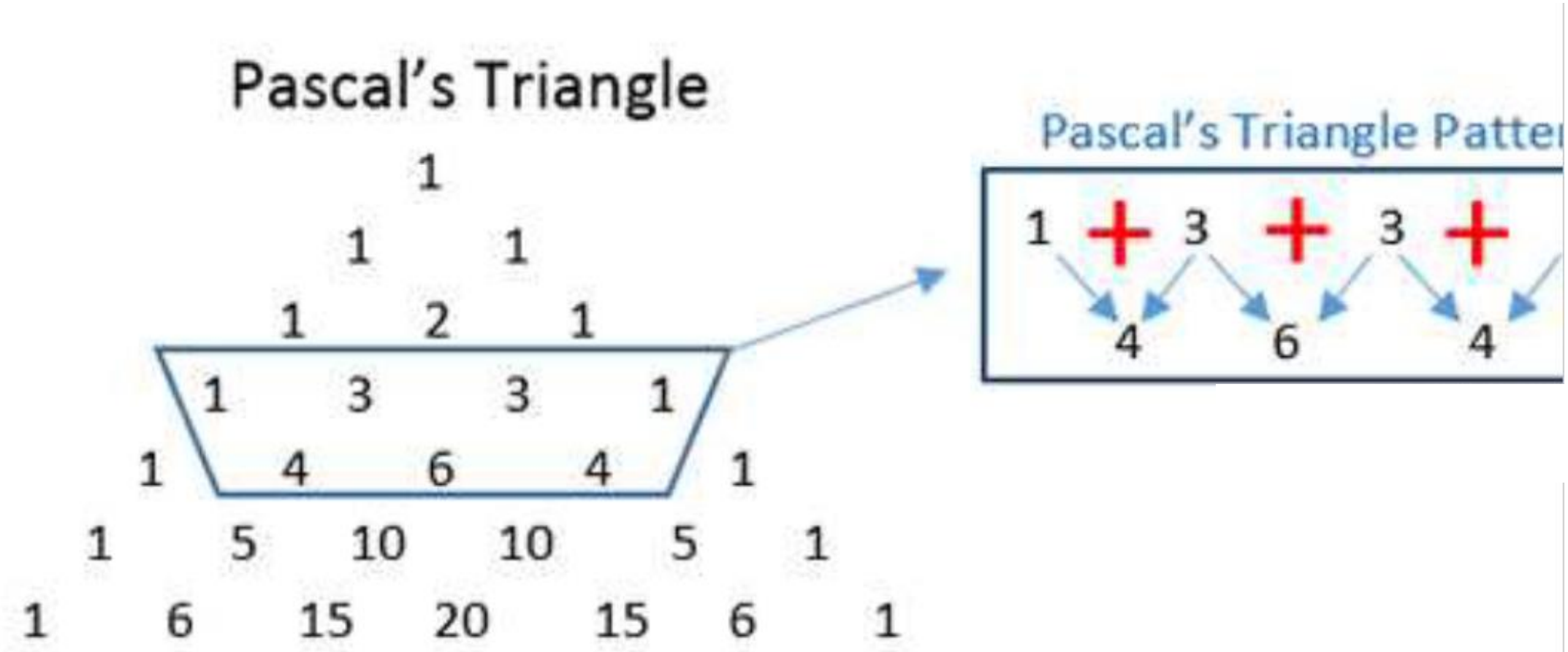
1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

Why is the Pascal Relation true? Each number is the sum of what is immediately above to the right and to the left.



Sketch of the proof:

Assume we know one row, say

$(x+y)^5 = x^5 + 5\,x^4\,y + 10\,x^3\,y^2 + 10\,x^2\,y^3 + 5\,x\,y^4 + y^5$.

Then

$$
\begin{aligned}
(x+y)^6 &= (x+y)\,(x+y)^5 \\
&= x\,(x+y)^5 + y\,(x+y)^5 \\
&= x\,(x^5 + 5\,x^4\,y + 10\,x^3\,y^2 + 10\,x^2\,y^3 + 5\,x\,y^4 + y^5) \\
&\quad + y\,(x^5 + 5\,x^4\,y + 10\,x^3\,y^2 + 10\,x^2\,y^3 + 5\,x\,y^4 + y^5) \\
&= (x^6 + 5\,x^5\,y + 10\,x^4\,y^2 + 10\,x^3\,y^3 + 5\,x^2\,y^4 + x\,y^5) \\
&\quad + (x^5\,y + 5\,x^4\,y^2 + 10\,x^3\,y^3 + 10\,x^2\,y^4 + 5\,x\,y^5 + y^6) \\
&= x^6 + 5\,x^5\,y + 10\,x^4\,y^2 + 10\,x^3\,y^3 + 5\,x^2\,y^4 + x\,y^5 \\
&\quad + x^5\,y + 5\,x^4\,y^2 + 10\,x^3\,y^3 + 10\,x^2\,y^4 + 5\,x\,y^5 + y^6 \\
&= x^6 + (5+1)\,x^5\,y + (10+5)\,x^4\,y^2 + (10+10)\,x^3\,y^3 + (5+10)\,x^2\,y^4 + (1+5)\,x\,y^5 + y^6 \\
&= x^6 + 6\,x^5\,y + 15\,x^4\,y^2 + 20\,x^3\,y^3 + 15\,x^2\,y^4 + 6\,x\,y^5 + y^6
\end{aligned}
$$

Pascal's Triangle

While we can prove many properties of the coefficients of Pascal's triangle, for small n we can just expand directly.

$$(x+y)^n = \sum_{k=0}^{n} a_{n,k} x^k y^{n-k}$$

$$(x+y)^{n+1} = (x+y) \sum_{k=0}^{n} a_{n,k} x^k y^{n-k}$$

$$= \sum_{l=0}^{n+1} a_{n+1,l} x^l y^{n+1-l}$$

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

Binomial Theorem: Proofs by Induction, by Story, ….

Claim: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ $\qquad \binom{n}{k} = \frac{n!}{k!(n-k)!}$

Proof: $(x+y)^n = (x+y)(x+y)\cdots(x+y) = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

Prove $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ Pascal's Identity

Brute Force: $\frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-(k+1))!}$ vs $\frac{(n+1)!}{(k+1)!(n-k)!}$

Claim: $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ By Story

Williams: n students
Amherst: 1 student
} want $k+1$ students

$\binom{1}{1}\binom{n}{k} + \binom{1}{0}\binom{n}{k+1} = \binom{n+1}{k+1}$

One student from Amherst

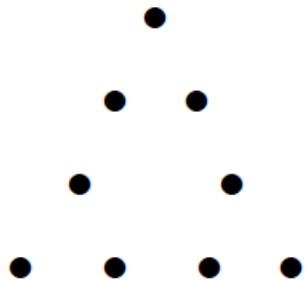
no students from Amherst

Don't write this way as $\binom{1}{1}$ and $\binom{1}{0}$ are 1

Pascal's Triangle

Modify Pascal's triangle: • if odd, blank if even.

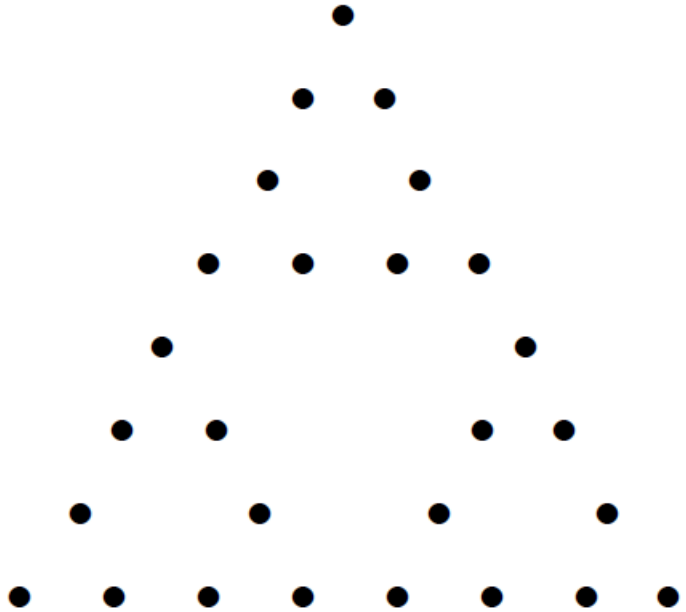
If we have just one row we would see •, if we have four rows we would see



Pascal's Triangle

Modify Pascal's triangle: • if odd, blank if even.

For eight rows we find



Pascal's Triangle

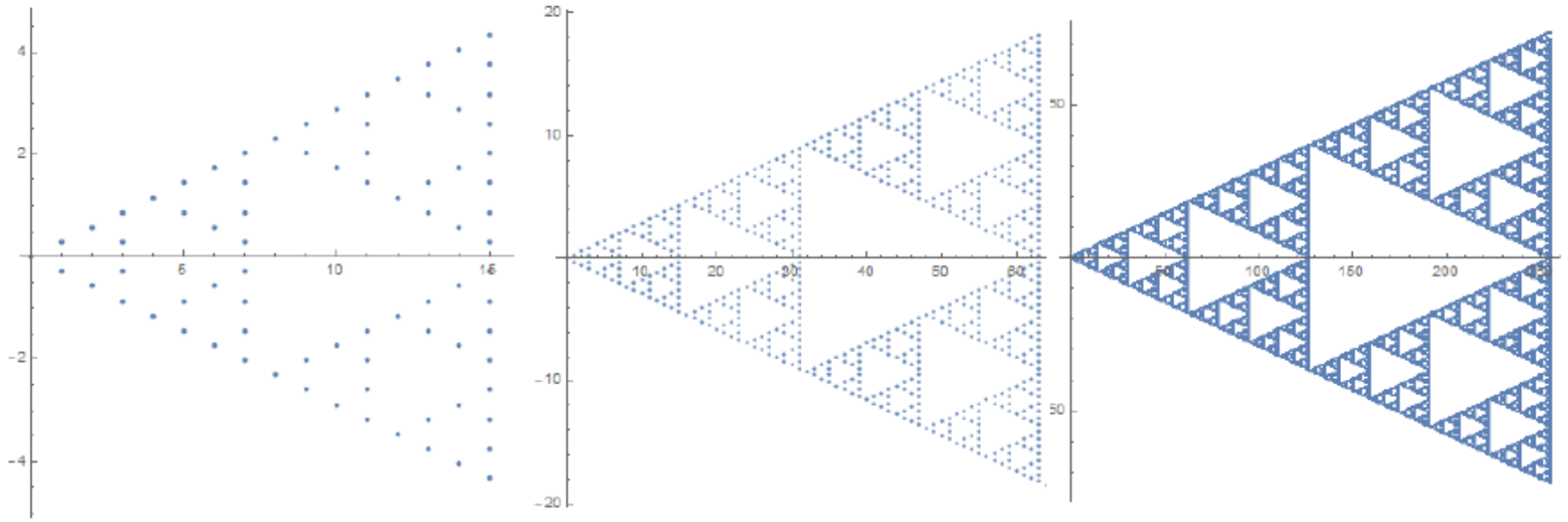


Figure: Plot of Pascal's triangle modulo 2 for 2^4, 2^8 and 2^{10} rows.

https://www.youtube.com/watch?v=tt4_4YajqRM (start 1:35)

Predicting Formulas: Derivative of a Product

$A(x) = x^n$ $\quad B(x) = x^m$ $\quad C(x) = A(x)B(x) = x^{n+m}$

$A'(x) = nx^{n-1}$ $\quad B'(x) = mx^{m-1}$ $\quad C'(x) = (n+m)x^{n+m-1}$

Derivs of $A(x)B(x)$ involve perhaps A, B, A', B'.

↳ Look at $A(x)$ or $B(x) = 1$

Note $A'(x)B(x)$ and $A(x)B'(x)$ are (something) x^{n+m-1}

Infact: $A'(x)B(x) + A(x)B'(x) = C'(x)$

$A(x) = \sin x$ $\quad$ $B(x) = \cos x$ $\quad$ $C(x) = \sin x \cos x$

$= \frac{1}{2} \cdot 2 \sin x \cos x$

$= \frac{1}{2} \sin(2x)$

$A'(x) = \cos x$ $\quad$ $B'(x) = -\sin x$ (minus sign)

$C'(x) = \frac{1}{2} \cos(2x) \cdot 2 = \cos(2x)$

Test: $A'(x)B(x) + A(x)B'(x)$

$= \cos x \cos x - \sin x \sin x$

$= \cos(2x)$ which is $C'(x)$

$\cos^2 x = \cos x \cdot \cos x = 1 - \sin^2 x = (1+\sin x)(1-\sin x)$

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1:

Lecture 03: 2/8/24:

Chapter Two: Introduction to groups, abstract groups, examples.

Chapter Two: Section 1: Permutations, Matrix Representations: Notation

S set with n elements: $\{x_1, x_2, \ldots, x_n\}$, have $n!$ permutations

Notation: $\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ a_1 & a_2 & \cdots & a_{n-1} & a_n \end{pmatrix}$ $\quad 1 \to a_1$, $\quad 2 \to a_2$

matrix $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ $\quad i \to j$

j^{th} column 1 in the jth spot and 0 elsewhere

e_i $\qquad$ e_j

Permutation Matrices: each column has one 1, rest are 0
each row has only one 1, rest are 0.

Permutation followed by Permutation is a permutation!

Imagine $P, P^2, P^3, P^4, \ldots$

↳ only $n!$ matrices (Counter: at most 2^{n^2} matrices)

Say $P^a = P^b$ and wlog $a > b$ so $a = (a-b) + b$

(Pigeon-hole-principle: look at $P, P^2, \ldots, P^{n!+1}$ at least two the same)

So $P^a = P^b \Rightarrow P^{a-b} P^b = P^b \Rightarrow P^{a-b} = \text{Identity}$

Chapter Two: Section 2: Definition of Groups:

(0) G is closed under the binary operation:

$g_1, g_2 \in G \Rightarrow g_1 \cdot g_2 \in G$. (Closure)

Definition 2.6. A *group* consists of a set G together with a composition law

$$G \times G \longrightarrow G,$$

$$(g_1, g_2) \longmapsto g_1 \cdot g_2,$$

satisfying the following axioms:

(a) (***Identity Axiom***) There is an element $e \in G$ such that

$$e \cdot g = g \cdot e = g \quad \text{for all } g \in G.$$

The element e is called the *identity element of* G.

(b) (***Inverse Axiom***) For every $g \in G$ there is an element $h \in G$ such that

$$g \cdot h = h \cdot g = e.$$

The element h is denoted g^{-1} and is called the *inverse of* g.

could write $h = h_g$

(c) (***Associative Law***) For all $g_1, g_2, g_3 \in G$, the *associative law* holds; i.e.,

$$g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3.$$

(d) (***Optional Feature: Commutative Law***) If it is further true that

$$g_1 \cdot g_2 = g_2 \cdot g_1 \quad \text{for all } g_1, g_2 \in G,$$

then G is said to be *commutative* or *abelian*.[3,4]

The deriv of a finite sum is the sum of the derivatives.

Induction

Base Case: Show $(f+g)' = f' + g'$

Inductive Step!

$$(f+g+h)' = ((f+g)+h)'$$

$$= (f+g)' + (h)'$$

$$= (f' + g') + (h')$$

$$= f' + g' + h'$$

Proposition 2.9 (Basic Properties of Groups). *Let G be a group.*

(a) *G has exactly one identity element.*

(b) *Each element of G has exactly one inverse.*

(c) *Let $g, h \in G$. Then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.*

(d) *Let $g \in G$. Then $(g^{-1})^{-1} = g$.*

Proof of (c): $(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}(eh) = h^{-1}h = e$

$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = g(eg^{-1}) = gg^{-1} = e$ ∎

(d) is similar

Proof of #1 Assume e_1, e_2 are identity elements: so $\forall g \in G$: $e_1 g = g e_1 = g$, $e_2 g = g e_2 = g$

Take $g = e_2$ in 1st and $g = e_1$ in second:

$e_1 e_2 = e_2 e_1 = e_2$

$e_2 e_1 = e_1 e_2 = e_1$

Thus $e_1 = e_2$ ∎

Definition 2.11. The *order* of a group G, which we denote by $\#G$, is the cardinality of the set of elements of G. In particular, if G is finite, then $\#G$ is simply the number of elements in G. We remark that other common notations for the order of a group are $o(G)$ and $|G|$.

Proposition 2.13. *Let G be a group, let $g \in G$, and let $n \geq 1$ be an integer such that $g^n = e$. Then the order of g divides n.*

order of g is smallest positive integer k such that $g^k = e$ (k can depend on g)

Must show $k \mid n$. Claim $n \geq k$ as k smallest pos integer that works

Write $n = qk + r$ where $r \in \{0, 1, 2, \ldots, k-1\}$

Thus $g^n = g^{qk+r} = g^{qk} g^r = (g^k)^q g^r = e^q g^r = e g^r = g^r$

know k smallest pos integer that works, $r < k$ so $r = 0$

Thus $n = qk$ so $k \mid n$ ∎

Chapter Two: Section 3: Examples of Groups:

Example 2.14 (Groups of Integers and Integers Modulo m).

Example 2.15 (Additive Groups of Real, Rational, and Complex Numbers).

Example 2.16 (Multiplicatives Group of Real, Rational, and Complex Numbers).

Example 2.18 (Cyclic Groups).

Example 2.19 (Permutation Groups).

Example 2.21 (Matrix Groups).

Example 2.22 (Dihedral Groups).

Example 2.23 (Quaternion Group).

Ex: Rational numbers under multiplication: ~~Group~~ issue: 0^{-1} doesn't exist

Study $\mathbb{Q}^+$ positive rationals or $\mathbb{Q}-\{0\} = \mathbb{Q}^\times$ non-zero rationals

Look at Clock group with $n=12$ under clock multiplication, remove 0

↳ still trouble: $X2 = 2x = 1 \bmod 12$ means $\underbrace{2x}_{\text{even}} = \underbrace{M12+1}_{\text{odd}}$

impossible

Try clock with $n = 5$ and non-zero elements

$\{1, 2, 3, 4\}$ closed under multiplication

identity is 1, associative

$1^{-1} = 1$ $\quad 2^{-1} = 3$ $\quad 3^{-1} = 2$ $\quad 4^{-1} = 4$

n	is it a Group
2	yes
3	yes
4	no
5	yes
6	no
7	yes
8	no

n	is it a group
9	no
10	no
11	yes
12	no
13	yes
14	no
15	no
16	no

Clock under multiplication, non-zero elements, is not a group if n composite

Proof: n composite Then $n = ab$ $a, b \geq 2$

Claim a^{-1} does not exist in set:

If div: $xa = ax = 1 \mod ab$

so $ax = mab + 1$

or $ax - mab = 1 \Rightarrow a(x - mb) = 1 \Rightarrow a \mid 1$

Contradiction

Not closed: a, b are non-zero but $ab = 0 \mod n$

What about clock arithmetic under multiplication?

Look at all numbers relatively prime to n on our clock

Ex: $n = 12$: $\{1, 5, 7, 11\}$ identity ✓ assoc ✓ closed ✓

$1^{-1} = 1$ $\quad 5^{-1} = 5$ $\quad 7^{-1} = 7$ $\quad 11^{-1} = 11$

$x^2 = 1 \mod 12$ has 4 solns

Try $n = 2 \cdot 3 \cdot 5 = 30$, look at relatively prime elements

$\{1, 7, 11, 13, 17, 19, 23, 29\}$

identity: ✓
assoc: ✓
closure: ✓

$\{1, 7, 11, 13, 30-13, 30-11, 30-7, 30-1\}$

$1^{-1} = 1, \quad 7^{-1} = 13, \quad 11^{-1} = 11, \quad 13^{-1} = 7$

$17^{-1} = 23 \quad 19^{-1} = 19 \quad 23^{-1} = 17 \quad 29^{-1} = 29$

$(30-11)^{-1}$
$= (-11)^{-1}$
$= (-1)^{-1} 11^{-1}$

$(30-7)^{-1}$
$(-7)^{-1}$
$(-1)^{-1} 7^{-1}$

$(-1)^{-1} = -1$

$23 \cdot 17$
161
23
391
$= 30(13) + 1$

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1:

Lecture 04: 2/13/24: https://youtu.be/Q0EuEXzNAI4 (Sec 2)

Chapter Two: Group Homomorphisms, Subgroups

Definition 2.24. Let G and G' be groups. A *homomorphism from G to G'* is a function $\phi : G \to G'$ satisfying

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2) \quad \text{for all} \quad g_1, g_2 \in G.$$

mult in G mult in G'

If $g_1 = e$ then $\phi(e \cdot g_2) = \phi(e) \cdot \phi(g_2)$ $\forall g_2 \in G$

$$\phi(g_2) = \phi(e)\,\phi(g_2)$$

As G' is a group, multiply on right by $\phi(g_2)^{-1}$ and get $e' = \phi(e)$

as $\underbrace{\phi(g_2)\phi(g_2)^{-1}}_{e'} = \phi(e)\underbrace{\phi(g_2)\phi(g_2)^{-1}}_{e'}$

$$e' = \phi(e)e' = \phi(e)$$

If $g_2 = g_1^{-1} \Rightarrow \varphi(g_1 g_1^{-1}) = \varphi(g_1)\,\varphi(g_1^{-1})$

But $g_1 g_1^{-1} = e$ and $\varphi(e) = e' \Rightarrow e' = \varphi(g_1)\,\varphi(g_1^{-1})$

So $\varphi(g_1)^{-1} = \varphi(g_1^{-1})$: mult on the left by $\varphi(g_1)^{-1}$

Examples: $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$ and $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}$

Clock group with addition

$\varphi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $\varphi(m) = m \bmod n$ (the remainder when $\div$ by n)

Ex: if $n = 12$, $\varphi(27) = 3$ as $27 = 2 \cdot 12 + 3$

Check: $\varphi(m_1 + m_2) \stackrel{?}{=} \varphi(m_1) + \varphi(m_2)$? is $m_1 + m_2 \bmod n \stackrel{?}{=} (m_1 \bmod n) + (m_2 \bmod n) \bmod n$

Proof: $m_k = q_k n + r_k$ so $m_1 + m_2 = (q_1 + q_2)n + (r_1 + r_2)$

Proposition 2.25. *Let $\phi : G \to G'$ be a homomorphism of groups.*

(a) *Let $e \in G$ be the identity element of G. Then $\phi(e)$ is the identity element of G'.*

(b) *Let $g \in G$. Then $\phi(g^{-1})$ is the inverse of $\phi(g)$ in G'.*

What other properties?

$\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ so $\phi(g^2) = (\phi(g))^2$

$\phi(g^3) = \phi(g^2 g) = \phi(g^2)\phi(g) = \phi(g)^2\phi(g) = \phi(g)^3$

By induction $\phi(g^n) = \phi(g)^n$ for all positive integers n

Note $\phi(g^{-2}) = \phi(g^{-1}g^{-1}) = \phi(g^{-1})\phi(g^{-1}) = (\phi(g))^{-1}(\phi(g))^{-1} = (\phi(g))^{-2}$

By induction get negative n

Direct: $\phi(g^0) = \phi(e) = e' = \phi(g)^0$

$\forall n \in \mathbb{Z}$ have $\phi(g^n) = \phi(g)^n$

$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ clock Group $\{0, 1, 2, \ldots, n-1\} = \mathbb{Z}/n\mathbb{Z}$

Ex: $n = 12$, $g = 5$

$g = 5$, $g^2 \Rightarrow 5+5 = 10$, $g^3 \Rightarrow 5+5+5 = 3$

"powers" of g: $5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0, 5$

cycles

Say $\phi: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ is a group homomorphism

all elements have infinite order except 0

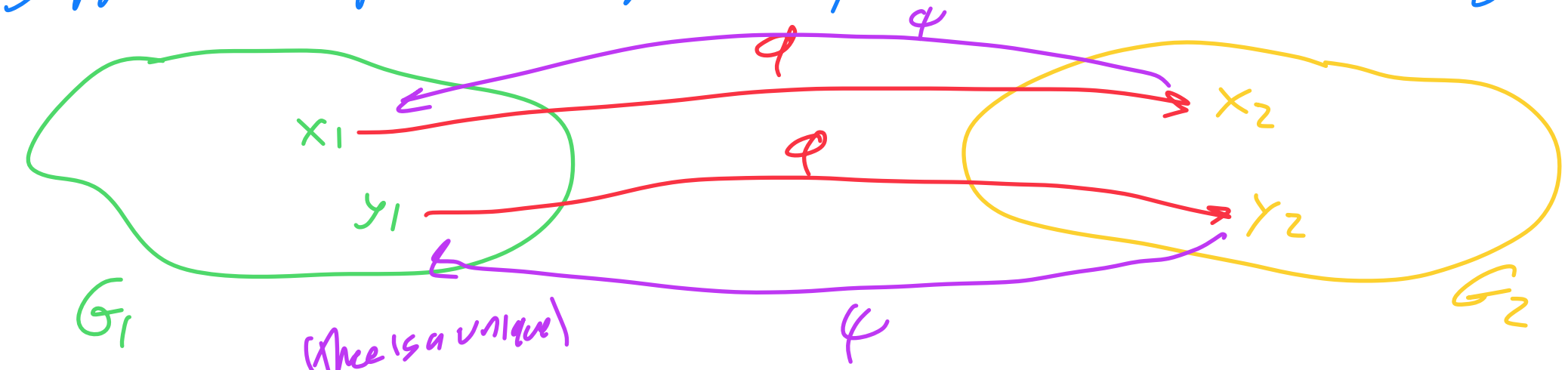
only ϕ works is $\phi(n) = 0$ for all n

Definition 2.30. Two groups G_1 and G_2 are said to be *isomorphic* if there is a bijective homomorphism

$$\phi : G_1 \longrightarrow G_2.$$

The map ϕ is called an *isomorphism* from G_1 to G_2. Isomorphic groups are essentially the same group, but their elements have been given different names.[9]

Is there a group homomorphism $\psi : G_2 \to G_1$ that is bijective?



Given $y_2 \in G_2$ $\exists!$ $y_1 \in G_1$ s.t. $\varphi(y_1) = y_2$ so set $\psi(y_2) = y_1$

Note: $\psi(x_2 y_2) = ?$ $\quad \varphi(x_1 y_1) = \varphi(x_1)\varphi(y_1) = x_2 y_2 \Rightarrow \psi(x_2 y_2) = x_1 y_1 = \psi(x_2)\psi(y_2)$

Remark 2.32. Isomorphic groups have identical structural properties. For example, if G_1 and G_2 are isomorphic, then:

(1) If one of them is finite, then they are both finite, and they satisfy $\#G_1 = \#G_2$.

(2) If one of them is abelian, then they are both abelian.

(3) If G_1 has an element of order n, then G_2 also has an element of order n.

(4) More generally, if G_1 has k different elements of order n, then G_2 also has k different elements of order n.

Exercise 2.23 asks you to prove these four assertions.

Proof of 3: Assume g_1 has order n: $g_1^n = e_1$ and $g_1^k \neq e_1$ if k positive less than n.

Note $\varphi(g_1^n) = \varphi(g_1)^n$. If $g_2 = \varphi(g_1)$ then since $g_1^n = e_1$ and $\varphi(e_1) = e_2$ get $e_2 = g_2^n$. Does a smaller power work?

If $g_2^l = e_2$ and $l < n$ then $e_2 = g_2^l = \varphi(g_1)^l = \varphi(g_1^l)$

So g_1^l sent to identity, since φ is 1-1 and $\varphi(e_1) = e_2 \Rightarrow g_1^l = e_1$ contradiction as $l < n$.

How to Prove that Groups Are Not Isomorphic?

1) if have different # of elements

2) element of order n in one group and no elements of order n in the other.

Negate Remark

3) if one is abelian and the other is not....

3-Step Program to Analyze Mathematical Objects

Step 1 (Deconstruction): Break your object into smaller and simpler pieces.

Step 2 (Analysis): Analyze the smaller, simpler pieces.

Step 3 (Reconstruction): Fit the pieces back together.

Definition 2.34. Let G be a group. A *subgroup of* G is a subset $H \subset G$ that is itself a group using G's group law. Explicitly, H needs to satisfy the following:

(i) For every $h_1, h_2 \in H$, the product $h_1 \cdot h_2$ is in H. Mathematically, we say that H is *closed* for the group law on G.
(ii) The identity element e is in H.
(iii) For every $h \in H$, the inverse h^{-1} is in H.

"inherits associativity

What is the linear algebra equivalent?

Subspaces: $\vec{v}_1, \ldots, \vec{v}_n \in V$ look at $\{a_1\vec{v}_1 + \cdots + a_n\vec{v}_n\}$
$= \text{Span}(\vec{v}_1, \ldots, \vec{v}_n\}$

H is a group with the same group law as G, lives in G

if $h \in H$ so is $h^2, h^3, h^4, \ldots, h^{-1}, h^{-2}, h^{-3}, \ldots$

Two trivial subgroups: $\{e\}$, G

Example 2.38. Let $d \in \mathbb{Z}$, then we can form a subgroup of $\mathbb{Z}$ using the multiples of d,

$$d\mathbb{Z} = \{dn : n \in \mathbb{Z}\} = \{\ldots, -2d, -d, 0, d, 2d, \ldots\}$$

$\mathbb{Z}/n\mathbb{Z}$ view $n\mathbb{Z}$ as multiples of n

Cyclic subgroup of G generated by g, denoted by <g>:

$$\langle g \rangle = \{ g^n : n \in \mathbb{Z} \}$$

Clock Group $\mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, 3, 4, 5, \ldots, 10, 11\}$

$\langle 5 \rangle = \{5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0\}$ 12 elements

$=$ full group!

$\langle 3 \rangle = \{3, 6, 9, 0\}$ 4 elements

Ex. Prove $\langle g \rangle$ is a subgroup.

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: Video from Section 2:

Lecture 05: 2/15/24: https://youtu.be/jiEIycQ3eBo

Chapter Two: Lagrange's Theorem, Product of Groups

Definition 2.41. Let $\phi : G \to G'$ be a group homomorphism. The *kernel of* ϕ is the set of elements of G that are sent to the identity element of G',

$$\ker(\phi) = \{g \in G : \phi(g) = e'\}.$$

Solve $A\vec{x} = \vec{b}$

Nullset $(A) = \{ \vec{v} \text{ st } A\vec{v} = \vec{0} \}$

If $A\vec{x}_0 = \vec{b}$ then $\vec{x} = \vec{x}_0 + \vec{v}$ also goes to $\vec{b}$.

Nullset is a subspace: $\vec{v}, \vec{w} \in N(A)$ so is $\alpha\vec{v} + \beta\vec{w}$

Question: is $\ker(\phi)$ a subgroup G?

Claim: $\ker(\phi) = \{g \in G \text{ s.t. } \phi(g) = e'\}$ is a subgroup of G

Proof: **Closure:** if $g_1, g_2 \in \ker(\phi)$ means $\phi(g_1) = e' = \phi(g_2)$

Show $g_1 g_2 \in \ker(\phi)$

But $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = e' \cdot e' = e'$ ✓

(defn of group homomorphism)

Identity: know $e \in \ker(\phi)$ as proved $\phi(e) = e'$ ✓

Inverse: if $g \in \ker(\phi)$ must show $g^{-1} \in \ker(\phi)$

Since $e = gg^{-1} \Rightarrow \phi(e) = \phi(gg^{-1})$

or $e' = \phi(g)\phi(g^{-1}) = e'\phi(g^{-1}) = \phi(g^{-1})$

(assuming $g \in \ker(\phi)$)

Thus as $\phi(g^{-1}) = e'$, $g^{-1} \in \ker(\phi)$ ∎

Proposition 2.44. *Let $\phi : G \to G'$ be a group homomorphism.*

(a) $\ker(\phi)$ *is a subgroup of* G.

(b) ϕ *is injective if and only if* $\ker(\phi) = \{e\}$.

Proof of (b)

$\Rightarrow$ Assume ϕ is injective, must prove $\ker(\phi) = \{e\}$

If $\ker(\phi) \neq \{e\}$ means $\exists$ at least two distinct $g \in G$ sent to e'

↳ say $\phi(g_1) = \phi(g_2) = e'$

This ϕ is not injective, contradiction, so $\ker(\phi) = \{e\}$

$\Leftarrow$ Assume $\ker(\phi) = \{e\}$, must show ϕ is injective

Assume ϕ is not injective so $\exists$ at least two distinct $g \in G$ sent to same $g \in G'$

↳ $\phi(g_1) = \phi(g_2)$ so $\phi(g_1)^{-1}\phi(g_1) = \phi(g_1)^{-1}\phi(g_2)$

$\Rightarrow e' = \phi(g_1^{-1})\phi(g_2) = \phi(g_1^{-1}g_2)$ as $\ker(\phi) = \{e\}$

$\Rightarrow g_1^{-1}g_2 = e$

$\Rightarrow g_2 = g_1$ ∎

Definition 2.45. Let G be a group, and let $H \subset G$ be a subgroup of G. For each $g \in G$, the (left) *coset of H attached to g* is the set

$$gH := \{gh : h \in H\}.$$

Example: $G = \mathbb{Z}$, $H = 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

$1H = 1 + 3\mathbb{Z} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$ ←

$4H = 4 + 3\mathbb{Z} = \{\ldots, -2, 1, 4, 7, 9, \ldots\}$

$0H = 0 + 3\mathbb{Z} = \{\ldots -6, -3, 0, 3, 6, \ldots\}$ ←

$2H = 2 + 3\mathbb{Z} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$ ←

$3H = 3 + 3\mathbb{Z} = \{\ldots, -3, 0, 3, 6, 9, \ldots\}$

Proposition 2.47. *Let G be a finite group, and let $H \subset G$ be a subgroup of G.*

(a) *Every element of G is in some coset of H.*

(b) *Every coset of H has the same number of elements.*

(c) *Let $g_1, g_2 \in G$. Then the cosets g_1H and g_2H satisfy either*

$$g_1H = g_2H \quad \text{or} \quad g_1H \cap g_2H = \emptyset.$$

Using set-theoretic terminology, this says that cosets of H are either equal or disjoint.

Proof (a): As $e \in H$, given any $g \in G$, have g is in the coset gH as $e \in H$.

Proof (b): Claim $\forall g \in G$: gH and H have same # of elements.

Find bijection from H to gH

$f(h) := gh$ 1-1? If $f(h_1) = f(h_2)$

Then $gh_1 = gh_2 \Rightarrow h_1 = h_2$

onto: if $x \in gH$ then $\exists\, h \in H$ s.t. $x = gh$

and then $f(h) = gh = x$

Proof of (c) Either $g_1H = g_2H$ or $g_1H \cap g_2H \neq \emptyset$ Empty set

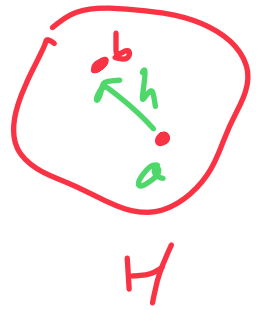
Assume $\exists x \in g_1H \cap g_2H$, prove $g_1H = g_2H$

Since x in both, $\exists h_1, h_2$ st $x = g_1h_1 = g_2h_2$

Claim: $\forall h \in H$, $hH = H$

Given any $b \in H$ find $a \in H$ st $ha = b$

Take $a = h^{-1}b \in H$ as $h, h^{-1}, b \in H$



Since $g_1h_1 = g_2h_2 \Rightarrow g_1 = g_2h_2h_1^{-1} = g_2h$ where $h = h_2h_1^{-1}$

So $g_1H = (g_2h)H = g_2(hH) = g_2H$ so

if not disjoint, identical!

Theorem 2.48 (Lagrange's Theorem). *Let G be a finite group, and let H be a subgroup of G. Then*

$$\#G = \#H \cdot (\#\text{ of distinct cosets of } G \text{ in } H),$$

and hence the order of H divides the order of G.

Proof: $G = \bigcup_{g \in G} gH$ $\quad G \subset \bigcup_{g \in G} gH$ because $e \in H$ so $g \in gH$

$\bigcup_{g \in G} gH \subset G$ as each $gH \subset G$

$G = \bigcup_{k=1}^{m} g_k H$ and each coset distinct from all others

all have same size

Choose cosets one at a time, only take if all new elements. As $\#G$ is finite this terminates

$\Rightarrow \#G$ equals $\#H * m$ (m = # distinct cosets)

∎

Example: $\mathbb{Z}/12\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Subgroups:

$\{0\}$

$\{0, 6\}$

$\{0, 4, 8\}$

$\{0, 3, 6, 9\}$

$\{0, 2, 4, 6, 8, 10\}$

order of H divides 12

$G = (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$

$\#G$ is $12 \cdot 12 = 144$

note: $(0,0) \cup (6,6)$ subgroup of size 2

$(0,0) \cup (0,6)$ " " " "

Definition 2.54. Let G_1 and G_2 be groups. The *product* of G_1 and G_2 is the group whose elements consist of ordered pairs

$$G_1 \times G_2 = \{(a, b) : a \in G_1 \text{ and } b \in G_2\}$$

and whose group operation is performed separately on each component. In other words, the product of two elements of $G_1 \times G_2$ is *defined* by the following formula:

$(a, b) \cdot (a', b')$ is equal to $(a \cdot a', b \cdot b')$

- $\cdot$: the group operation for $G_1 \times G_2$
- $a \cdot a'$: G_1's group operation
- $b \cdot b'$: G_2's group operation

Ex: Prove this is a group.

Example 2.55. For any non-zero integers m and n, there is a homomorphism

Clock Group with mn hours under clock addition $\longrightarrow$

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\varphi} (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),$$
$$a \bmod mn \longmapsto (a \bmod m, a \bmod n).$$

Proof φ is a group homomorphism

$\varphi(ab) = (ab \bmod m,\ ab \bmod n)$

$\varphi(a)\varphi(b) = (a \bmod m,\ a \bmod n) \cdot (b \bmod m,\ b \bmod n)$

$= ((a \bmod n)(b \bmod n) \bmod m,\ \longrightarrow)$

$= (ab \bmod n,\ ab \bmod n)$ ∎

Theorem 2.56 (Structure Theorem for Finite Abelian Groups)**.** *Let G be a finite abelian group. Then there are integers $m_1, \ldots, m_r$ so that*

$$G \cong (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z}).$$

Isomorphic

Further, we may take $m_1, \ldots, m_r$ to be prime powers.

Proof. See Section 11.9.1. □

Example 2.57 (Projections and Inclusions). Products of groups come with two natural *projection homomorphisms*

$$p_1 : G_1 \times G_2 \longrightarrow G_1, \qquad (a, b) \longmapsto a,$$

$$p_2 : G_1 \times G_2 \longrightarrow G_2, \qquad (a, b) \longmapsto b,$$

and two natural *inclusion homomorphisms*

$$\iota_1 : G_1 \longrightarrow G_1 \times G_2, \qquad a \longmapsto (a, e_2),$$

$$\iota_2 : G_2 \longrightarrow G_1 \times G_2, \qquad b \longmapsto (e_1, b).$$

The inclusion maps are injective, but the projections have kernels,

$$\ker(p_1) = \{e_1\} \times G_2 \quad \text{and} \quad \ker(p_2) = G_1 \times \{e_2\}.$$

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: Ring Theory Lecture

Lecture 06: 2/20/24: https://youtu.be/oV8aA_uMoaY

Chapter Three: Rings (Definitions, Examples, Properties)

Chapter 3: Rings — Part 1

Generalizing integers: two operations….

$\mathbb{Z}$ (zahl) $= \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{Q}$ (quotients) $= \{p/q : p, q \in \mathbb{Z} \text{ and } q \neq 0\}$

$\mathbb{N}$ (natural) $= (0 \text{ or } 1), \ldots$

addition + multiplication $\cdot, \times, *$, or nothing!

Definition 3.1. A *ring* R is a set with two operations, generally called *addition* and *multiplication* and written

$$\underbrace{a+b}_{\text{addition}} \quad \text{and} \quad \underbrace{a\cdot b \text{ or } ab}_{\text{multiplication}},$$

satisfying the following axioms:

(1) The set R with its addition law $+$ is an abelian group. The identity element of this group is denoted 0 or 0_R.

(2) The set R with its multiplication law $\cdot$ is almost a group, but its elements are not required to have inverses.[2] Explicitly, the multiplication law of a ring has the following properties:

- There is an element $1_R \in R$ satisfying[3,4]

$$1_R \cdot a = a \cdot 1_R = a \quad \text{for all } a \in R.$$

  As with 0_R versus 0, if there is no ambiguity we often write 1 instead of 1_R.
- The associative law holds,

$$a\cdot(b\cdot c) = (a\cdot b)\cdot c \quad \text{for all } a,b,c \in R.$$

(3) [Distributive Law] For all $a,b,c \in R$ we have

$$a\cdot(b+c) = a\cdot b + a\cdot c \quad \text{and} \quad (b+c)\cdot a = b\cdot a + c\cdot a.$$

(4) [Optional Feature: Commutative Law] If further $a\cdot b = b\cdot a$ for all $a,b \in R$, then the ring is said to be *commutative*.

closure, identity
inverse, assoc
$\forall r \in R$: $r + 0_R = 0_R + r = r$

Closure, identity, assoc
not nec inverses
Ex: non-zero rationals
Ex: non-zero integers

Ex: $R = \{0\}$ under $+$ and $\cdot$

Is R an abelian group under addition?

↳ $0_R = 0$

What about multiplication?

↳ CLOSED ✓

↳ Assoc ✓

↳ Identity: $0 \cdot r = r$ for all $r \in R$! $1_R = 0$

Distributive ✓

Ring where $1_R = 0_R$

0_R is the identity under addition

$-a$ is the notation for the additive inverse of a: $(-a)+a = a+(-a) = 0_R$.

Proposition 3.2. *Let R be a ring.*

(a) $0_R \cdot a = 0_R$ *for all* $a \in R$.

(b) $(-a)\cdot(-b) = a\cdot b$ *for all* $a, b \in R$. *In particular, we have* $(-1_R)\cdot a = -a$.

Proof. (a) We start with $1_R = 1_R + 0_R$, which is true because 0_R is the identity for addition. We multiply both sides by a and compute

Statement	Reason
$a = a \cdot 1_R$	since 1_R is the identity for multiplication,
$= a \cdot (1_R + 0_R)$	since 0_R is the identity for addition,
$= a \cdot 1_R + a \cdot 0_R$	distributive law,
$= a + a \cdot 0_R$	since 1_R is the identity for multiplication.

We now "subtract" a from both sides. But this one time we will spell out every detail so that you can see how the different ring axioms come into play:

$0_R = (-a) + a$	definition of inverse for addition,
$= (-a) + (a + a \cdot 0_R)$	from our earlier calculation,
$= ((-a) + a) + a \cdot 0_R$	associativity of addition,
$= 0_R + a \cdot 0_R$	definition of inverse for addition,
$= a \cdot 0_R$	since 0_R is the identity for addition.

$(-a)+(a+a\cdot 0_R)$

$(-a)+a$

Proposition 3.2. *Let R be a ring.*

(a) $0_R \cdot a = 0_R$ *for all* $a \in R$.

(b) $(-a) \cdot (-b) = a \cdot b$ *for all* $a, b \in R$. *In particular, we have* $(-1_R) \cdot a = -a$.

Claim: $(-a)(-b) = ab \Rightarrow (-1_R) \cdot x = -x$

Take $a = 1_R$ $b = -x$ as $-(-x)$ is x

Yields $(-1_R)(x) = 1_R \cdot (-x) = -x$

Prove $(-a)(-b) = ab$ for all $a, b \in R$

$0_R(-b) = 0_R \Rightarrow (a + -a)(-b) = 0_R$

so $a(-b) + (-a)(-b) = 0_R$ so $(-a)(-b) = -(a(-b))$

Now $a \cdot 0_R = 0_R = a(b + (-b))$ so $ab + a(-b) = 0_R \Rightarrow a(-b) = -(ab)$

Substitute: $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$ ∎

Definition 3.3. Let R and R' be rings. A *ring homomorphism from R to R'* is a function $\phi : R \to R'$ satisfying[5]

$$\begin{aligned} \phi(1_R) &= 1_{R'}, \\ \phi(a+b) &= \phi(a) + \phi(b) \quad \text{for all } a, b \in R, \\ \phi(a \cdot b) &= \phi(a) \cdot \phi(b) \quad \text{for all } a, b \in R. \end{aligned}$$

addition in R'

addition in R

The *kernel of* ϕ is the set of elements that are sent to 0,

$$\ker(\phi) = \{a \in R : \phi(a) = 0_{R'}\}.$$

As with groups, we say that R and R' are *isomorphic* if there is a bijective homomorphism $\phi : R \to R'$, and we call such a map ϕ an *isomorphism*.

Using $\phi(0_R) = 0_{R'}$

First idea gives

$0_{R'} = \phi(a) + \phi(-1_R)\phi(a)$

So $\phi(-1_R) = -1_{R'}$

as $\phi(a)$ and $\phi(-1_R)\phi(a)$ are additive inverses, or $(1_{R'} + \phi(-1_R)) = 0_{R'}$

Does $\phi(0_R) = 0_{R'}$?

$\phi(0) = \phi(a + -a)$

$= \phi(a) + \phi(-a)$

$= \phi(a) + \phi(-1_R \cdot a)$

$= \phi(a) + \phi(-1_R)\phi(a)$

$\phi(a) = \phi(a + 0_R)$

$= \phi(a) + \phi(0_R)$

subtract $\phi(a)$ from both sides

$0_{R'} = \phi(0_R)$

$\phi(0_R)$

$\phi(0_R + 0_R)$

$= \phi(0_R) + \phi(0_R)$

subtract $\phi(0_R)$ both sides

$0_{R'} = \phi(0_R)$

define the ring $\mathbb{Z}/m\mathbb{Z}$ to be the set of congruence classes.

$x+y = x+y \bmod m \qquad x \cdot y = xy \bmod m$

Ex. $m=12$: $12\mathbb{Z} = \{\dots, -24, -12, 0, 12, 24, \dots\} = 0+12\mathbb{Z}$

$1+12\mathbb{Z} = \{\dots, -23, -11, 1, 13, 25, \dots\}$

$\vdots$

$11+12\mathbb{Z} = \{\dots, -13, -1, 11, 23, 35, \dots\}$

$(a+12\mathbb{Z}) + (b+12\mathbb{Z}) = (a+b \bmod 12) + 12\mathbb{Z}$

Ex: $(8+12\mathbb{Z}) + (7+12\mathbb{Z}) = (3+12\mathbb{Z}) = 15+12\mathbb{Z}$

Have 12 elements! $0+12\mathbb{Z}, 1+12\mathbb{Z}, \dots, 11+12\mathbb{Z}$

OR is $0+12\mathbb{Z}$ $\qquad 1_R = 1+12\mathbb{Z}$

are non-zero elements a group under mult? No: no inverse for $2+12\mathbb{Z}$

$(5+12\mathbb{Z}) * (5+12\mathbb{Z}) = 1+12\mathbb{Z}$

Example 3.5 (Gaussian Integers: $\mathbb{Z}[i]$). Here is another interesting subring of $\mathbb{C}$. It is called the *ring of Gaussian integers* and consists of the set

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

$i = \sqrt{-1}$ so $i^2 = -1$

$(a+bi) + (c+di) = (a+c) + (b+d)i$

$(a+bi) \cdot (c+di) = ac + bci + adi + bdi^2$

$= (ac - bd) + (bc + ad)i$

$0_R = 0 + 0i$

$= 0$

$1_R = 1 + 0i$

$= 1$

Example 3.6 (Polynomial Rings: $R[x]$). Polynomials provide a method for creating bigger (and better?) rings from rings that we already know. Thus given any commutative ring R, we can use R to build the *ring of polynomials over* R,

$$R[x] = \left\{ \begin{array}{l} \text{polynomials } a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d \text{ of all} \\ \text{possible degrees with coefficients } a_0, a_1, \ldots, a_d \in R \end{array} \right\}.$$

Commutative: $ab = ba$

What about $R_{2024}[X] = \{$ all poly $a_0 + \cdots + a_{2024} x^{2024} : a_k \in R \}$

identity under addition: $0 + 0x + \cdots + 0x^{2024}$

" " mult : $1 + 0x + \cdots + 0x^{2024}$

NOT CLOSED!

$x^{2024} \cdot x = x^{2025}$ not in $R_{2024}[X]$

$$E_c : R[x] \longrightarrow R, \quad E_c(f) = f(c).$$ here $c \in R$

The evaluation map E_c is a ring homomorphism,[6] as you will verify in Exercise 3.8, and its kernel is exactly the set of polynomials that have a factor of $x - c$.

Ring homomorphism sends $0 \longrightarrow 0$ (not same 0)

So if $f(c) = 0$ saying $f(x) = g(x)(x-c)$

↳ does R need any special properties for this to be true?

Ex: $R = \mathbb{Z}/12\mathbb{Z}$ look at $R[x]$

$c = 4$ $f(x) = 3x$ Then $E_4(f) = f(4) = 12 = 0$

Does $x-4$ "divide" $f(x)$? $3x = 3(x-4+4) = 3(x-4) + 12$

$= 3(x-4)$

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 2: Group Theory and Ring Theory Problems

Lecture 06: 2/20/24: https://youtu.be/kYWnt48j68A

Chapter Two (Groups) and Three (Rings)

Possible Problems:

HW#2: Dues Thursday February 15: (1) Prove by induction that the sum of the first n odd numbers is n^2. (2) Prove (n choose k) = (n choose n-k). (3) What should (3 choose 5) equal? Based on your answer to this, what should the factorial of a negative integer be? (4) Problem 1.12: Let S be the set S = {1, 2, 3, 4, 5, 6, 7, 8} and define an equivalence relation on S, a ~ b if and only if a - b is even. (a) Prove that this is an equivalence relation on S. Write S as a disjoint union of the equivalence classes for the equivalence relation. (5) Problem 1.16: Give an example of a function from the natural numbers to the natural numbers that is (a) injective but not surjective and (b) surjective but not injective.

2.7. Definition 2.6 says that a group is a set G with a composition law satisfying three axioms. In particular, it says that there is an identity element $e \in G$ that works on both sides and that every element $g \in G$ has an inverse that works on both sides. Suppose that we weaken the requirements to specify that the identity and inverse only work on one side. In other words, we suppose that G is a set with a composition law satisfying the following weaker axioms:

(a) (**Right-Identity Axiom**) There is an element $e \in G$ so that $g \cdot e = g$ for all $g \in G$.

(b) (**Right-Inverse Axiom**) For all $g \in G$ there is an element $h \in G$ so that $g \cdot h = e$.

(c) (**Associative Law**) $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ for all $g_1, g_2, g_3 \in G$.

Prove that G is a group. (*Hint*. First show that the right-inverse of g is also a left-inverse of g, and then show that the right identity element e is also a left-identity element.)

2.8. There are other sorts of algebraic structures that are similar to groups in that they are sets S that have a composition law

$$S \times S \longrightarrow S, \quad (s_1, s_2) \longmapsto s_1 \cdot s_2,$$

but they have fewer or different axioms than a group. In this exercise we explore two of these structures.

- The set S with its composition law is a *monoid* if it has an identity element $e \in S$ and satisfies the associative law, but elements are not required to have inverses. (See Exercise 2.19 for another example of a monoid.)
- The set S with its composition law is a *semigroup* if its composition law is associative, but it need not have an identity element or inverses. (Indeed, without an identity element, the definition of inverse doesn't even make sense.)

For each of the following sets S and composition laws $\cdot$, determine if $(S, \cdot)$ is a group, a monoid, or a semigroup.

(a) The set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ with the composition law being addition.
(b) The set of extended natural numbers $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ with the composition law being addition.
(c) The set of integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ with the composition law being addition.
(d) The set of natural numbers $\mathbb{N}$ with the composition law being multiplication.
(e) The set of extended natural numbers $\mathbb{N}_0$ with the composition law being multiplication.
(f) The set of integers $\mathbb{Z}$ with the composition law being multiplication.
(g) The set of integers $\mathbb{Z}$ with composition law $m \cdot n = \max\{m, n\}$.
(h) The set of natural numbers $\mathbb{N}$ with composition law $m \cdot n = \max\{m, n\}$.
(i) The set of natural numbers $\mathbb{N}$ with composition law $m \cdot n = \min\{m, n\}$.
(j) The set of natural numbers $\mathbb{N}$ with composition law $m \cdot n = mn^2$.

2.36. Let G be a group, and let $g \in G$. The *centralizer of* g, denoted $Z_G(g)$, is the set of elements of G that commute with g; i.e.,

$$Z_G(g) = \{g' \in G : gg' = g'g\}.$$

(a) Prove that $Z_G(g)$ is a subgroup of G.

(b) Compute the centralizer $Z_G(g)$ for the following groups and elements:

(i) $G = \mathcal{D}_4$ and g is rotation by $90°$.

(ii) $G = \mathcal{D}_4$ and f is a flip fixing two of the vertices of the square.

(iii) $G = \mathrm{GL}_2(\mathbb{R})$ and $g = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$.

(c) Prove that $Z_G(g) = G$ if and only if $g \in Z(G)$, where the center $Z(G)$ of G is defined in Exercise 2.35.

(d) More generally, if $S \subseteq G$ is any subset of G, then the *centralizer of* S is the set

$$Z_G(S) = \{g \in G : sg = gs \text{ for all } s \in S\}.$$

Prove that $Z_G(S)$ is a subgroup of G.

2.37. This exercise explains when two elements of G determine the same coset of H. Let G be a group, let H be a subgroup of G, and let $g_1, g_2 \in G$. Prove that the following three statements are equivalent:

(1) $g_1H = g_2H$.

(2) There is an element $h \in H$ such that $g_1 = g_2h$.

(3) $g_2^{-1}g_1 \in H$.

2.40. Let p be a prime, and let $a \in \mathbb{Z}$ be an integer satisfying $p \nmid a$. Use Exercise 2.13(b) and Lagrange's Theorem to prove:

Fermat's Little Theorem: $a^{p-1} \equiv 1 \pmod{p}$. Note $a^p \equiv a \bmod p$ for all a.

Proof: Assume $\gcd(a,p) = 1$, wlog $1 \le a < p$

Study $\langle a \rangle = \langle a, a^2, a^3, \ldots, a^k = 1 \rangle \bmod p$

$G = \{1, 2, 3, \ldots, p-1\}$ under clock multiplication

closed: $p \mid xy \rightarrow p \mid x$ or $p \mid y$ assoc: yes

identity: 1 inverse: Assume yes

If assume inverses, as $\#G$ is $p-1$, order of a divides $p-1$,

so $a^{p-1} \equiv 1 \bmod p$

More generally: if $\gcd(a,n) = 1$ Then $a^{\phi(n)} \equiv 1 \bmod n$

Aside: $\gcd(5,6) = 1$, $5^{6-1} = 5^5 \bmod 6 = (-1)^5 \bmod 6 = -1 \bmod 6$

$= 5 \bmod 6$

$\neq 1 \bmod 6$

Thus 6 is composite

Need to show any $x \in \{1, 2, \dots, p-1\}$ has an inverse mod p

If no inverse, then $\forall y \in G$, $xy \neq 1$

So can find y_1, y_2 distinct st $xy_1 = xy_2 = z \in G$ (Pigeon hole principle)

So $x(y_1 - y_2) = 0 \mod p$

Use if $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ (BIG RESULT) ✴

So $p \mid x$ (impossible) or $p \mid (y_1 - y_2) \Rightarrow y_1 = y_2 \mod p$

Note if did $G = \{1, 2, 3, \dots, 11\mathbb{Z}\}$, the non-zero elements mod 12,

Then can have $x(y_1 - y_2) = 0$ and $12 \nmid x$ and $12 \nmid (y_1 - y_2)$

Ex: $x = 3$, $y_1 = 6$, $y_2 = 2$

Warning: $\cos x \cos x = 1 - \sin^2 x = (1 - \sin x)(1 + \cos x)$

$\cos x \mid$ LHS but $\cos x \nmid (1 - \sin x)$ or $(1 + \cos x)$

Consider all integers that are the sum of two squares.... What about the sum of k squares?

$S = \{n \text{ s.t. } n = a^2 + b^2 \text{ for } a, b \in \mathbb{Z}\}$ under multiplication

identity: $1,\ 1 = 1^2 + 0^2 = 0^2 + 1^2$

assoc: $x(yz) = (xy)z$: inherits from real numbers

inverse: $13 = 2^2 + 3^2$ $\quad 25 = 5^2 + 0^2$ $\quad 2 = 1^2 + 1^2$

$1/13 \neq a^2 + b^2$ $\quad 1/25 \neq a^2 + b^2$ $\quad 1/2 \neq a^2 + b^2$

Closure: if $n, m \in S$ is $nm \in S$?

Is $2 \cdot 13 = 26$ a sum of two squares? Yes: $5^2 + 1^2$

$2 \cdot 25 = 50$ " " " " " ? Yes: $7^2 + 1^2$

$4 \cdot 13 = 52$ " " " " " ? Yes: $6^2 + 4^2$

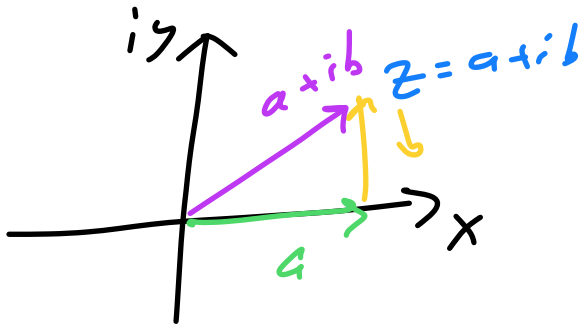
$n = a^2 + b^2$ and $m = c^2 + d^2$ $\quad nm = e^2 + f^2$

how do e, f depend on a, b, c, d?

wlog $a \geq b$ $\quad c \geq d$ $\quad a \geq c$

$n = a^2 + b^2$ $\quad \vec{v} = \begin{pmatrix} a \\ b \end{pmatrix}$ then $|\vec{v}| = \sqrt{a^2+b^2}$

$z = a+ib$ $\quad |z| = \sqrt{a^2+b^2}$ or $|z|^2 = z\bar{z} = (a+ib)(a-ib) = a^2+b^2$



$z = a+ib$ $\quad |z|^2 = a^2+b^2$

$w = c+id$ $\quad |w|^2 = c^2+d^2$

$zw = (ac-bd) + i(bc+ad)$ $\quad |zw|^2 = (ac-bd)^2 + (bc+ad)^2$

if $n = |z|^2$ and $m = |w|^2$ then $nm = |zw|^2$ is the sum of 2 squares!

This is a monoid!

2.7. Definition 2.6 says that a group is a set G with a composition law satisfying three axioms. In particular, it says that there is an identity element $e \in G$ that works on both sides and that every element $g \in G$ has an inverse that works on both sides. Suppose that we weaken the requirements to specify that the identity and inverse only work on one side. In other words, we suppose that G is a set with a composition law satisfying the following weaker axioms:

(a) **(Right-Identity Axiom)** There is an element $e \in G$ so that $g \cdot e = g$ for all $g \in G$.

(b) **(Right-Inverse Axiom)** For all $g \in G$ there is an element $h \in G$ so that $g \cdot h = e$.

(c) **(Associative Law)** $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ for all $g_1, g_2, g_3 \in G$.

Hint: Show the right inverse is also the left inverse

Know $\forall g \in G \ \exists h = h_g$ st $g \cdot h_g = e$ and $\forall \tilde{g} \in G \ \tilde{g} e = \tilde{g}$

Let's try $g = e \Rightarrow \exists h_e$ st $e \cdot h_e = e$

$e \cdot h_e \cdot (h_e^{-1}) = e \cdot h_e^{-1}$ by assoc $e \cdot (h_e \cdot h_e^{-1}) = e \cdot h_e^{-1}$

or $e \cdot e = e \cdot h_e^{-1}$ so $e = e \cdot h_e^{-1}$

$\Rightarrow e \cdot h_e = e \cdot h_e^{-1}$

2.7. Definition 2.6 says that a group is a set G with a composition law satisfying three axioms. In particular, it says that there is an identity element $e \in G$ that works on both sides and that every element $g \in G$ has an inverse that works on both sides. Suppose that we weaken the requirements to specify that the identity and inverse only work on one side. In other words, we suppose that G is a set with a composition law satisfying the following weaker axioms:

(a) **(Right-Identity Axiom)** There is an element $e \in G$ so that $g \cdot e = g$ for all $g \in G$.

(b) **(Right-Inverse Axiom)** For all $g \in G$ there is an element $h \in G$ so that $g \cdot h = e$.

(c) **(Associative Law)** $g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$ for all $g_1, g_2, g_3 \in G$.

Take: $e \cdot he = e \Rightarrow he \cdot e \cdot he = he \cdot e = he$

$he \cdot he = he$

$he \cdot (he \cdot he^{-1}) = he\, he^{-1}$

$he = e$ Shown $e^{-1} = e$

Assume $g \cdot h_g = e$ show $h_g \cdot g = e$

Thus $(h_g \cdot g) h_g = h_g \cdot e$ here h_g is the right inverse of g

$(h_g \cdot g) h_g = h_g$ let h_g^{-1} denote the right inverse of h_g

$(h_g \cdot g)(h_g \cdot h_g^{-1}) = h_g \cdot h_g^{-1}$

$(h_g \cdot g) \cdot e = e$

$h_g \cdot g = e$ so h_g is also the left inverse of g!

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: Problem Lecture

Lecture 07: 2/22/24: https://youtu.be/FTxr3VQYjjw

Chapter Two: Groups (Problems) and Three: Rings (Problems)

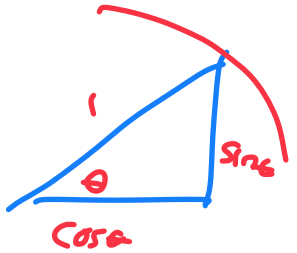
In linear algebra, a **rotation matrix** is a transformation matrix that is used to perform a rotation in Euclidean space. For example, using the convention below, the matrix

$$R = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$ $= R(\theta)$ or R_θ

rotates points in the xy plane counterclockwise through an angle θ about the origin of a two-dimensional Cartesian coordinate system. To perform the rotation on a plane point with standard coordinates $\mathbf{v} = (x, y)$, it should be written as a column vector, and multiplied by the matrix R:

$$R\mathbf{v} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x\cos\theta - y\sin\theta \\ x\sin\theta + y\cos\theta \end{bmatrix}.$$

https://en.wikipedia.org/wiki/Rotation_matrix



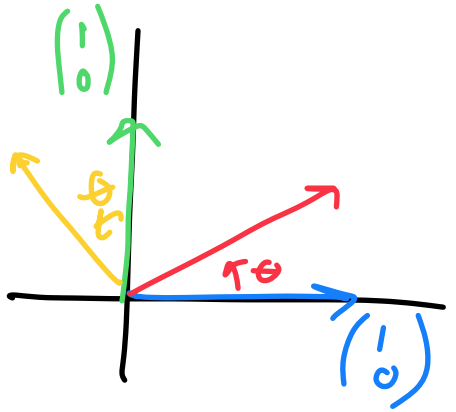
$\cos^2\theta + \sin^2\theta = 1$

$\begin{pmatrix} x \\ y \end{pmatrix} = x\begin{pmatrix} 1 \\ 0 \end{pmatrix} + y\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$R(\theta)\begin{pmatrix} x \\ y \end{pmatrix} = R(\theta)\,x\begin{pmatrix} 1 \\ 0 \end{pmatrix} + R(\theta)\,y\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$= x\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + y\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$= x\begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} + y\begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$



$$R(\theta)R(\phi) = R(\theta+\phi) = R(\phi+\theta) = R(\phi)R(\theta)$$

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} = \begin{pmatrix} \cos\theta\cos\phi - \sin\theta\sin\phi & -(\cos\theta\sin\phi + \sin\theta\cos\phi) \\ \sin\theta\cos\phi + \cos\theta\sin\phi & -\sin\theta\sin\phi + \cos\theta\cos\phi \end{pmatrix}$$

$$= \begin{pmatrix} \cos(\theta+\phi) & -\sin(\theta+\phi) \\ \sin(\theta+\phi) & \cos(\theta+\phi) \end{pmatrix}$$

We just proved angle addition formulas.

$\cos(\theta+\phi) = \cos\theta\cos\phi - \sin\theta\sin\phi$

$\sin(\theta+\phi) =$ ———

$R(\theta)$ $\theta \bmod 2\pi$ vs $e^{i\theta} = \cos\theta + i\sin\theta$ $\theta \bmod 2\pi$

vs $\theta \in [0, 2\pi)$ with clock arithmetic and 2π hours.

ϕ : (2×2 rotation matrices) → exponential of a number mod 2π

$$\phi\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = e^{i\theta}$$

$\phi(R_\theta R_\phi) \stackrel{?}{=} \phi(R_\theta)\phi(R_\phi)$? Yes as $R_\theta R_\phi = R_{\theta+\phi}$

so $\phi(R_\theta R_\phi) = \phi(R_{\theta+\phi}) = e^{i(\theta+\phi)}$

3.2. Let R be a commutative ring.

(a) Suppose that the map

$$f : R \longrightarrow R, \quad f(a) = a^2,$$

is a ring homomorphism. Prove that $1_R + 1_R = 0_R$. In less fancy notation, prove that $2 = 0$ in the ring R.

(b) Conversely, if $2 = 0$ in the ring R, prove that $f(a) = a^2$ is a homomorphism from R to R.

(c) Suppose that the map

$$f : R \longrightarrow R, \quad f(a) = a^3,$$

is a ring homomorphism. Prove that $6 = 0$ in the ring R.

$f(x+y) = f(x) + f(y)$

$f(xy) = f(x)\,f(y)$

$f(1_R) = 1_R$

3.10. Prove that the map

$$\mathbb{C} \hookrightarrow M_2(\mathbb{R}), \quad x + yi \longmapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix},$$

as discussed in Example 3.8, is an injective ring homomorphism.

f is a ring homomorphism: $f(1_R + 1_R) = f(1_R) + f(1_R) = 1_R + 1_R$

Told: $f(a) = a^2$ is a ring homomorphism

$f(x+y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ as ring homom

What should x and y equal? Use sum or product?

Take $x = y = 1_R$, try sum as know $f(1_R) = 1_R$

$f(1_R + 1_R) = (1_R + 1_R)^2$ and also $= f(1_R) + f(1_R)$ as ring homom

$\Rightarrow 1_R^2 + 1_R 1_R + 1_R 1_R + 1_R^2 = 1_R + 1_R$

$\Rightarrow 1_R + 1_R + 1_R + 1_R = 1_R + 1_R \xRightarrow[1_R \text{ twice}]{\text{subtract}} 1_R + 1_R = 0_R$

Note: $2a = (1_R + 1_R)a = 0_R$

Consider $R = \mathbb{Z}$ and $f(a) = a^2$: is this a ring homomorphism?

know is not as $2 \neq 0$

check: $f(1) = 1$? yes!

check: $f(xy) = f(x)f(y)$? yes: $(xy)^2 = x^2 y^2$

check: $f(x+y) = f(x) + f(y)$? no: $(1+1)^2 \neq 1^2 + 1^2$

$(1+2)^2 \neq 1^2 + 2^2$

$(0+1)^2 = 0^2 + 1^2$ yes!

Consider $R = \mathbb{Z}/2\mathbb{Z}$ and $f(a) = a^2$: is this a ring homom?

Note $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ under clock arithmetic

$f(1) = 1$? Yes ✓

$f(xy) = f(x)f(y)$? As $f(a) = 0$ and $f(1) = 1$, yes: check $(x, y) =$ $(0,0), (0,1), (1,1)$

$f(x+y) = (x+y)^2 = x^2 + 2xy + y^2$ vs $x^2 + y^2 = f(x) + f(y)$

always equal: differ by $2xy$, always even

3.11. For any commutative ring R, let

$$M_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R \right\}$$

be the set of 2-by-2 matrices with entries in R. Define addition by adding the corresponding entries, and define multiplication as described by (2.4) in Example 2.21.

(a) Prove that $M_2(R)$ is a ring.

(b) Prove that $M_2(R)$ is non-commutative.

(c) Find non-zero elements $A, B \in M_2(R)$ such that $AB = 0$. (In the terminology of Section 3.4, the elements A and B are zero divisors, and $M_2(R)$ is not an integral domain.)

(d) Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(R)$. Prove that there is a $B \in M_2(R)$ satisfying $AB = I$ if and only if $ad - bc$ has a multiplicative inverse in R.

(e) Let $A, B \in M_2(R)$. Prove that $AB = I$ if and only if $BA = I$.

(f) More generally, prove that for all $n \geq 2$, the set of matrices $M_n(R)$ is a non-commutative ring using matrix addition and multiplication, and that $A \in M_n(R)$ has a (2-sided) multiplicative inverse in $M_n(R)$ if and only if $\det(A)$ has a multiplicative inverse in R. (*Hint.* For the last statement, recall the definition of the adjoint matrix A^{adj} associated to A, and prove that the identity $AA^{\text{adj}} = (\det A)I$ holds in $M_n(R)$.)

Definition 3.10. A *field* is a commutative ring R with the property that every non-zero element of R has a multiplicative inverse. In other words, for every $a \in R$ with $a \neq 0$ there is a $b \in R$ satisfying $ab = 1$.

Definition 3.13. Let R be a commutative ring. An element $a \in R$ is called a *zero divisor* if $a \neq 0$ and there is some non-zero $b \in R$ such that $ab = 0$. The ring R is an *integral domain* if it has no zero divisors. Equivalently, the ring R is an integral domain if the only way to get $ab = 0$ is to have either $a = 0$ or $b = 0$.

Section 3.4. Some Important Special Types of Rings

3.18. Let m be a positive integer.

(a) Prove that $\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if m is prime.

(b) Prove that $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime.

3.19. Let R be a field. Prove that R is an integral domain; i.e., prove that R does not have any zero divisors.

3.20. Prove that each of the following rings is *not* a field:

(a) $\mathbb{Z}[i]$. (b) $\mathbb{R}[x]$. (c) $\mathbb{H}$. (d) $M_n(\mathbb{R})$ if $n \geq 2$.

Study $\mathbb{Z}/n\mathbb{Z}$ is an integral domain iff n is prime
(if and only if)

Assume $n = ab$ with $a, b > 1$ Ex: $n = 12 = 3 \cdot 4$

Not an integral ring if $\exists\, x, y$ st $xy = 0$ but $x, y \neq 0$

↳ Take $x = a$, $y = b$ Then $xy = 0$ but $x, y \neq 0$

Assume n is prime: can $xy = 0 \bmod n$ and $x, y \neq 0 \bmod n$?

Let $n = p$ a prime: show cannot find $x, y \neq 0 \bmod p$ with $xy = 0 \bmod p$.

If $xy = 0 \bmod p$ means $\exists\, q$ st $xy = qp$

Use if a prime divides a product it divides at least one factor:

So $p \mid xy \rightarrow p \mid x$ or $p \mid y$

Contradiction as $x, y \neq 0 \bmod p$

False for composites: $6 \mid 4 \cdot 9$ but $6 \nmid 4$ and $6 \nmid 9$

$3 \mid xy$ and $3 \nmid x$ and $3 \nmid y$

$x = 3n+1$ or $3n+2$ $\Rightarrow$ $x = 3n+a$ $a \in \{1, 2\}$

$y = 3m+1$ or $3m+2$ $y = 3m+b$ $b \in \{1, 2\}$

$xy = (3n+a)(3m+b) = 9nm + 3nb + 3ma + ab$

$= \underbrace{3(3nm + nb + ma)}_{\text{mult of } 3} + \underbrace{ab}_{\substack{1, 2 \text{ or } 4 \\ \text{not a multiple of } 3}}$

2.40. Let p be a prime, and let $a \in \mathbb{Z}$ be an integer satisfying $p \nmid a$. Use Exercise 2.13(b) and Lagrange's Theorem to prove:

Fermat's Little Theorem: $a^{p-1} \equiv 1 \pmod{p}$.

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 2: Ring Theory (Theory Lecture)

Lecture 07: 2/22/24: https://youtu.be/Dui2qHdNH6c

Chapter Three: Rings: Homomorphisms, Fields

Definition 3.1. A *ring* R is a set with two operations, generally called *addition* and *multiplication* and written

$$\underbrace{a+b}_{\text{addition}} \quad \text{and} \quad \underbrace{a\cdot b \text{ or } ab}_{\text{multiplication}},$$

satisfying the following axioms:

(1) The set R with its addition law $+$ is an abelian group. The identity element of this group is denoted 0 or 0_R.

(2) The set R with its multiplication law $\cdot$ is almost a group, but its elements are not required to have inverses.[2] Explicitly, the multiplication law of a ring has the following properties:

- There is an element $1_R \in R$ satisfying[3,4]

$$1_R \cdot a = a \cdot 1_R = a \quad \text{for all } a \in R.$$

  As with 0_R versus 0, if there is no ambiguity we often write 1 instead of 1_R.
- The associative law holds,

$$a\cdot(b\cdot c) = (a\cdot b)\cdot c \quad \text{for all } a,b,c \in R.$$

(3) [Distributive Law] For all $a,b,c \in R$ we have

$$a\cdot(b+c) = a\cdot b + a\cdot c \quad \text{and} \quad (b+c)\cdot a = b\cdot a + c\cdot a.$$

(4) [Optional Feature: Commutative Law] If further $a\cdot b = b\cdot a$ for all $a,b \in R$, then the ring is said to be *commutative*.

closure, identity
inverse, assoc
$\forall r \in R$: $r + 0_R = 0_R + r = r$

Closure, identity, assoc
not nec inverses
Ex: non-zero rationals
Ex: non-zero integers

Example 3.8 (Matrix Rings). There are also rings whose elements are matrices. Let

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a+\alpha & b+\beta \\ c+\gamma & d+\delta \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix}$$

$$A(B\vec{v}) = (AB)\vec{v}$$

non-invertible: $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, invertible: $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ not invertible

Definition 3.3. Let R and R' be rings. A *ring homomorphism from R to R'* is a function $\phi : R \to R'$ satisfying[5]

also sends $0_R \to 0_{R'}$

$$\begin{aligned} \phi(1_R) &= 1_{R'}, \\ \phi(a+b) &= \phi(a) + \phi(b) \quad \text{for all } a, b \in R, \\ \phi(a \cdot b) &= \phi(a) \cdot \phi(b) \quad \text{for all } a, b \in R. \end{aligned}$$

The *kernel of ϕ* is the set of elements that are sent to 0,

$0_R \in$ $$\ker(\phi) = \{a \in R : \phi(a) = 0_{R'}\}.$$

As with groups, we say that R and R' are *isomorphic* if there is a bijective homomorphism $\phi : R \to R'$, and we call such a map ϕ an *isomorphism*.

$\ker(\phi)$ is a subset of R, is it a sub-ring of R?

Example 3.9 (Homomorphism from $\mathbb{Z}$). For every ring R, there is a unique homomorphism

$$\phi : \mathbb{Z} \longrightarrow R.$$

$\phi(1) = 1_R, \quad \phi(0) = 0_R$ forced on us as ϕ is a ring-homom

Must find $\phi(n)$ for all $n \in \mathbb{Z}$

$\phi(2) = \phi(1+1) = \phi(1) + \phi(1) = 1_R + 1_R = 2 \cdot 1_R$

$\phi(3) = \phi(2+1) = \phi(2) + \phi(1) = 2 \cdot 1_R + 1_R = 3 \cdot 1_R$

Induction: base case done, assume $\phi(n) = n \cdot 1_R$

Then $\phi(n+1) = \phi(n) + \phi(1) = n \cdot 1_R + 1_R = (n+1) 1_R$

$0_R = \phi(0) = \phi(n + (-n)) = \phi(n) + \phi(-n) \Rightarrow \phi(-n) = -\phi(n)$

ϕ is well defined, and have no freedom in choosing it!

Ex! Try to find $\phi: \mathbb{Z}/n\mathbb{Z} \to R$, maybe n prime, maybe not.

Definition 3.10. A *field* is a commutative ring R with the property that every non-zero element of R has a multiplicative inverse. In other words, for every $a \in R$ with $a \neq 0$ there is a $b \in R$ satisfying $ab = 1$.

Example where some non-zero are invertible; some are not

(1) matrices: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ not invertible and not zero element

but $\begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$ is invertible with inverse $\begin{pmatrix} 5 & -2 \\ -2 & 1 \end{pmatrix}$

(2) Clock arithmetic : $\mathbb{Z}/12\mathbb{Z}$: $5^{-1} = 5$, $7^{-1} = 7$, $11^{-1} = 11$

but 2, 3, 4, 6, 8, 9, 10 not invertible

Definition 3.13. Let R be a commutative ring. An element $a \in R$ is called a *zero divisor* if $a \neq 0$ and there is some non-zero $b \in R$ such that $ab = 0$. The ring R is an *integral domain* if it has no zero divisors. Equivalently, the ring R is an integral domain if the only way to get $ab = 0$ is to have either $a = 0$ or $b = 0$.

Consider $M_2(\mathbb{R})$

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ idempotent matrix: $A^2 = A$

$\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$

Find all idempotent 2x2 real matrices

Note: $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ Say A is nilpotent if some power of A is the zero matrix

Consider $\mathbb{Z}/n\mathbb{Z}$ where $n = ab$, with $a, b > 1$

Find $x, y \neq 0$ st $xy = 0 \bmod n$ $\quad x = a \quad y = b$

$n = 12$ $\quad 3 \cdot 4,\ 2 \cdot 6,\ 4 \cdot 3,\ 6 \cdot 2$

If n is prime then no zero divisors

Proposition 3.15 (Cancellation Property for Integral Domains). *A commutative ring R is said to have the* cancellation property *if for every choice of $a, b, c \in R$, the following implication is true:*

$$ab = ac \iff b = c \text{ or } a = 0.$$

A commutative ring has the cancellation property if and only if it is an integral domain.

Example without cancellation property: $\mathbb{Z}/12\mathbb{Z}$: $ab = ac$ but $a \neq 0$, $b \neq c$
↳ Do: $3 \cdot 4 = 3 \cdot 8 \bmod 12$ and $3 \neq 0$ and $4 \neq 8 \bmod 12$

Proof: if $ab = ac \iff ab - ac = 0 \iff a(b-c) = 0$

$\Leftarrow$ If R is an integral domain then no divisors of zero.
Thus $a(b-c) = 0$ either $a = 0$ or $b - c = 0$ or both
$\Rightarrow a = 0$ or $b = c$

$\Rightarrow$ If R has the cancellation property, must show R is an integral domain.
Must show if $xy = 0$ either x or y is zero
Try $a = x$, $b = y$, $c = 0$: then $xy = x \cdot 0 = 0$ so by the cancellation property as $x \neq 0$ have $y = 0$.

Definition 3.16. Let R be a commutative ring.[9] The *group of units of* R is the subset R^* of R defined by

$$R^* = \{a \in R : \text{there is some } b \in R \text{ satisfying } ab = 1\}.$$

The group law on R^* is ring multiplication. The elements of R^* are called *units*.

Proposition 3.17. *The set of units R^* is a group, with group law being ring multiplication.*

Proof: identity: Yes, The multiplicative identity of R.

assoc: Yes, inherited

Inverse: if $a \in R^*$ is $a^{-1} \in R^*$?

Yes: $a \in R^* \Rightarrow \exists b$ st $ab = 1$ so $b = a^{-1}$

but if $ab = 1 \Rightarrow ba = 1$ so $(a^{-1})(a) = 1$

So $\exists$ an element x such that $a^{-1}x = 1$ ($x = a$)

need to show $a^{-1} \in R^*$: since $(a^{-1})^{-1} = a$, and assumed $a \in R$, then all is good.

Closure: $a_1, a_2 \in R^*$ so $\exists b_1, b_2$ st $a_1 b_1 = a_2 b_2 = 1$

Then $(a_1 a_2)(b_2 b_1) = a_1((a_2 b_2) b_1) = a_1 b_1 = 1$

if did $(a_1 a_2)(b_1 b_2)$ need commutivity to get $(a_1 b_1)(a_2 b_2) = 1$

What if commutativity fails? Consider ….

Extra Credit

Do we need commutativity,

or is it just convenience/laziness

Needed results….

Theorem 1.32. *Let $a, b \in \mathbb{Z}$ be integers, not both 0. Then there are integers $u, v \in \mathbb{Z}$ satisfying*

$$au + bv = \gcd(a, b).$$

If a prime divides a product (Steven J. Miller and Cesar Silva), College Mathematics Journal. (**48** (2017), no. 2, 123--128): https://web.williams.edu/Mathematics/sjmiller/public_html/math/papers/PrimeDividesProduct_MillerSilva40.pdf

ABSTRACT. One of the greatest difficulties encountered by all in their first proof intensive class is subtly assuming an unproven fact in a proof. The purpose of this note is to describe a specific instance where this can occur, namely in results related to unique factorization and the concept of the greatest common divisor.

$p|ab$ *implies* $p|a$ *or* $p|b$.

If n is composite and $n|ab$ does $n|a$ or $n|b$? NO

↳ $4 \mid 2 \cdot 6$ but $4 \nmid 2$ and $4 \nmid 6$

↳ $6 \mid 4 \cdot 9$ but $6 \nmid 4$ and $6 \nmid 9$

Proposition 3.20. *Let $m \geq 1$ be an integer. Then*

$$(\mathbb{Z}/m\mathbb{Z})^* = \{a \bmod m : \gcd(a, m) = 1\}.$$

In particular, if p is a prime number, then $\mathbb{Z}/p\mathbb{Z}$ is a field, often denoted $\mathbb{F}_p$.

Assume $m = p$ is prime

If a is relatively prime to p must show a is invertible

$\forall b, \exists u, v$ st $au + bv = \gcd(a, b)$ take $b = p$

Then $au + pv = \gcd(a, p) = 1$

$\Rightarrow au \equiv 1 \bmod p$ so a is invertible!

Assume m is an integer of at least 2

If a is relatively prime to m must show a is invertible

$\forall b, \exists u, v$ st $au + bv = \gcd(a, b)$ take $b = m$

Then $au + mv = \gcd(a, m) = 1$

$\Rightarrow au \equiv 1 \bmod m$ so a is invertible

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: Ring Theory (Theory Lecture)
Lecture 08, 09: 2/26,28/24: Watch video from other section from lectures 06, 07.

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: Ring Theory (Theory Lecture)

Lecture 10: 3/5/24: https://youtu.be/w4WAYa5eBMQ

Chapter Three: Rings: Homomorphisms, Fields. Video from Section 2.

Definition 3.26. Let R be a commutative ring. An *ideal* of R is a non-empty subset $I \subseteq R$ with the following two properties:

- If $a \in I$ and $b \in I$, then $a + b \in I$.
- If $a \in I$ and $r \in R$, then $ra \in I$.

Note $r=0 \Rightarrow 0 \in I$ as long as I is not empty!

Example: $R = \mathbb{Z}$

If $1 \in I$ then $I = R$

If $a \in I$ then $-a \in I$ (take $r=-1$)

let α be smallest positive element in the ideal (if no α then $I = \{0\}$)

know all multiples of α are in I.

Let $\beta \in I$ but $\beta \neq$ a mult. of α: so $\beta = m\alpha + r$ $\quad 0 < r < \alpha$

As $\beta \in I$ and $m\alpha \in I \Rightarrow r = \beta + (-m\alpha) \in I$ but $r < \alpha$, contradiction

Definition 3.27. Let R be a commutative ring, and let $c \in R$. The *principal ideal generated by* c, denoted cR or (c), is the set of all multiples of c,

$$cR = (c) = \{rc : r \in R\}.$$

If $R = \mathbb{Z}$, all ideals are principal!

Study $R = \mathbb{Z}/n\mathbb{Z}$ Study $n = 12$ or $n =$ prime p

Take $n = 12$, consider $I = \{0, 4, 8\}$ mod 12

or $0 + \mathbb{Z}/12\mathbb{Z}$, $4 + \mathbb{Z}/12\mathbb{Z}$, $8 + \mathbb{Z}/12\mathbb{Z}$

Check: I is an ideal

add 2 get a new ideal: $\{0, 2, 4, 6, 8, 10\}$

add 3 get a new ideal: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

or not $2, 3 \in I \Rightarrow 3 - 2 \in I$

Definition 3.31. Let R be a commutative ring, and let I be an ideal of R. Then for each element $a \in R$, the *coset of* a is the set

$$a + I = \{a + c : c \in I\}.$$

Ex: $R = \mathbb{Z}$, $I = 12\mathbb{Z}$

$(7 + 12\mathbb{Z}) + (8 + 12\mathbb{Z})$

$= 15 + 12\mathbb{Z}$

$= 3 + 12\mathbb{Z}$

note $a+I$ and $(a+i)+I$ same coset if $i \in I$

(1) $(a+I) + (b+I) = (a+b) + I$

(2) $(a+I) \cdot (b+I) = ab + I$

Proof of (1) $\Rightarrow$ $X \in (a+I) + (b+I)$ so $X = (a + c_a) + (b + c_b)$

Thus $X = (a+b) + (c_a + c_b)$

but $c_a, c_b \in I \Rightarrow c_a + c_b \in I$, let $c_a + c_b = c_{a+b} \in I$

So $X = (a+b) + c_{a+b} \in (a+b) + I$

$\subseteq$ Assume $X \in (a+b) + I$ so $X = (a+b) + c_{a+b}$ with $c_{a+b} \in I$

Thus $X = (a + 0) + (b + c_{a+b})$ and done

or $X = (a + c) + (b + (c_{a+b} - c))$ for any $c \in I$ ∎

Proposition 3.32. *Let R be a commutative ring, and let I be an ideal of R.*

(a) *Let $a+I$ and $a'+I$ be two cosets. Then $a'+I = a+I$ if and only if $a'-a \in I$.*

(b) *Addition and multiplication of cosets is well-defined, in the sense that it doesn't matter which element of the coset we use in the definition.*

(c) *Addition and multiplication of cosets turns R/I into a commutative ring.*[10]

Proof of (b)

$(a+I)$ and $(\alpha+I)$ same, $(b+I)$ and $(\beta+I)$ same

$\alpha - a \in I$ so $\alpha = a + c_a$ and similarly $\beta = b + c_b$, $c_a, c_b \in I$

$(a+I)(b+I) = ab + I$

$(\alpha+I)(\beta+I) = \alpha\beta + I = (a+c_a)(b+c_b) + I$

$= ab + \underbrace{ac_b + bc_a + c_a c_b}_{\text{must show is in } I} + I$

as anything in R times something in I is in I, and I closed under sums, this is in I, and $i+I = I$

Claim: $i+I = I$

if $x \in I$ then $x = c_x$ for some $c_x \in I$

then $x = i + (c_x - i) \in i+I$

Proposition 3.34. *Let R be a commutative ring.*

(a) *Let I be an ideal of R. Then the map*

$$R \longrightarrow R/I, \quad a \longmapsto a+I,$$

that sends an element to its coset is a ring homomorphism whose kernel is I.

(b) *Let $\phi : R \to R'$ be a ring homomorphism.*

(i) *The kernel of ϕ is an ideal of R, where we recall from Definition 3.3 that*

$$\ker(\phi) = \{a \in R : \phi(a) = 0\}.$$

(ii) *The homomorphism ϕ is injective if and only if $\ker(\phi) = (0)$.*

(iii) *Writing $I_\phi = \ker(\phi)$ for convenience, there is a well-defined injective ring homomorphism*

$$\bar{\phi} : R/I_\phi \longrightarrow R' \quad \text{defined by} \quad \bar{\phi}(a+I_\phi) = \phi(a).$$

Proof of (b)(i) $\forall a, b \in \ker(\phi)$ means: $\phi(a) = \phi(b) = 0$

Must show $a+b \in \ker(\phi)$ and $ar \in \ker(\phi)$ $\forall r \in R$

$\phi(a+b) = \phi(a) + \phi(b) = 0 + 0 = 0 \in \ker(\phi)$ (ring homom)

$\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$ (ring homom and $0 \in \ker(\phi)$)

Ideal Examples:

$\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$

$M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\}$ This is a ring

↳ $I = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$

$I = M_2(\mathbb{Z})$

Is there anything else?

Consider all matrices where a, b, c, d even

But $M_2(\mathbb{Z})$ is not commutative!

3.7. Prime Ideals and Maximal Ideals

Definition 3.37. Let R be a commutative ring. An ideal I of R is a *prime ideal* if $I \neq R$ and if whenever a product of elements $ab \in I$, then either $a \in I$ or $b \in I$.

We observe that if I is a prime ideal, then it also has the following property:

$$a \notin I \text{ and } b \notin I \implies ab \notin I.$$

This statement is the contrapositive of, and hence logically equivalent to, the stated definition of prime ideal.

Definition 3.40. Let R be a commutative ring. An ideal I is called a *maximal ideal* if $I \neq R$ and if there are no ideals properly contained between I and R. In other words, if J is an ideal and $I \subseteq J \subseteq R$, then either $J = I$ or $J = R$.

Consider $R = \mathbb{Z}$ and $I = (6) = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$

look at adding 2 or 3 get (2) or (3) and these are maximal

$I = (12)$ Then $6+I = (6)$ or $4+I = (4)$

Clock Groups?

If $R = \mathbb{Z}$ then $I = (\alpha)$

If $\alpha = ab$ with $a, b > 1$ (so α is composite)

Then I is not maximal: add $a + (\alpha)$ then get (a)

a + multiples of ab = multiple of a

Since it is an ideal, have as many copies of a as we wish

Start with I, build $J \supseteq I$, add a new element a to I,

plus whatever is needed to make it an ideal! closed under sums and multiples of $R = \mathbb{Z}$.

Not maximal: Find J st $I \subsetneq J \subsetneq R$

If α is prime then it is maximal

$R = \mathbb{Z}$, $I = (p)$ take any a not a multiple of p

Thus $a = np + r$

$\gcd(a, p) = 1$

Trying to make an ideal $J \supsetneq I$, so there is some $a \in J$ s.t. $a \notin I$

Euclidean algorithm $\exists\, x, y$ s.t. $ax + py = \gcd(a, p) = 1$

If add a to I and make an ideal, $ax \in J$

Since $p \in I \subset J$ then $py \in J$

so $1 \in J$ and thus $J = R$

proves (p) is maximal.

Theorem 3.43. *Let R be a commutative ring, and let I an ideal with $I \neq R$.*

(a) *I is a prime ideal if and only if the quotient ring R/I is an integral domain.*

(b) *I is a maximal ideal if and only if the quotient ring R/I is a field.*

Corollary 3.44. *Every maximal ideal is a prime ideal.*

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: Lecture 11: 3/7/24:

Part 1: Vector Spaces: https://youtu.be/5rm1FR6GPFc
Part 2: RSA: https://youtu.be/FYs4S4WNidc
Chapter Four: Vector Spaces, RSA Encryption: Slides for RSA here:
https://web.williams.edu/Mathematics/sjmiller/public_html/math/talks/VCTALCryptography/Burlington2019/IntroRSA_VCTAL.pdf

Vector Spaces — Part 1

Chapter 4

Thinking abstractly, we observe that vectors allow two sorts of operations:

- We can multiply a vector by a number. This is called *scalar multiplication*.
- We can add two vectors. This is called *vector addition*.

Definition 4.1. A *field* is a commutative ring F with the property that for every $a \in F$ with $a \neq 0$ there is a $b \in F$ satisfying $ab = 1$.

Definition 4.3. Let F be a field. A *vector space with field of scalars* F, or alternatively an *F-vector space*, is an abelian group V with addition operation $+$ and with a rule for multiplying a vector $\boldsymbol{v} \in V$ by a scalar $c \in F$ to obtain a new vector $c\boldsymbol{v} \in V$. Vector addition and scalar multiplication are required to satisfy the following axioms:

(1) [Identity Law]

$$1\boldsymbol{v} = \boldsymbol{v} \text{ for all } \boldsymbol{v} \in V.$$

(2) [Distributive Law #1]

$$c(\boldsymbol{v}_1 + \boldsymbol{v}_2) = c\boldsymbol{v}_1 + c\boldsymbol{v}_2 \text{ for all } \boldsymbol{v}_1, \boldsymbol{v}_2 \in V \text{ and all } c \in F.$$

(3) [Distributive Law #2]

$$(c_1 + c_2)\boldsymbol{v} = c_1\boldsymbol{v} + c_2\boldsymbol{v} \text{ for all } \boldsymbol{v} \in V \text{ and all } c_1, c_2 \in F.$$

(4) [Associative Law]

$$(c_1c_2)\boldsymbol{v} = c_1(c_2\boldsymbol{v}) \text{ for all } \boldsymbol{v} \in V \text{ and all } c_1, c_2 \in F.$$

The identity element of V is called the *zero vector* and is denoted by $\mathbf{0}$. It should not be confused with $0 \in F$, which is the zero element of the field F.

Is $0\vec{v} = \vec{0}$?

Proof: $\vec{v} + (-\vec{v}) = \vec{0}$ Know $\exists \vec{w}$, s.t. $\vec{v} + \vec{w} = \vec{0}$

$(0+0)\vec{v} = 0\vec{v}$

distributive law: $0\vec{v} + 0\vec{v} = 0\vec{v}$

now add $-(0\vec{v})$ to both sides, the additive inverse

yield $0\vec{v} = \vec{0}$

Using this: $(1+(-1))\vec{v} = 0\vec{v} = \vec{0}$

so $\vec{v} + (-1)\vec{v} = \vec{0}$ so $(-1)\vec{v}$ is the additive inverse

Definition 4.5. Let F be a field, and let V and W be F-vector spaces. A *linear transformation* from V to W is a function

$$L : V \longrightarrow W$$

satisfying:

$$L(c_1\boldsymbol{v}_1 + c_2\boldsymbol{v}_2) = c_1L(\boldsymbol{v}_1) + c_2L(\boldsymbol{v}_2) \quad \text{for all } \boldsymbol{v}_1, \boldsymbol{v}_2 \in V \text{ and all } c_1, c_2 \in F.$$

If we want to specify the scalar field, we will say that L is an F-linear transformation.

$V = \mathbb{R}^2$ L be a matrix!

$A(c_1\vec{v}_1 + c_2\vec{v}_2) = A(c_1\vec{v}_1) + A(c_2\vec{v}_2) = c_1 A\vec{v}_1 + c_2 A\vec{v}_2$

If $L(\vec{v}) = \vec{v} + \vec{w}$ then

$L(\vec{v}_1 + \vec{v}_2) = \vec{v}_1 + \vec{v}_2 + \vec{w}$

$L(\vec{v}_1) + L(\vec{v}_2) = \vec{v}_1 + \vec{w} + \vec{v}_2 + \vec{w}$

Definition 4.11. Let V be an F-vector space. A *finite*[5] *basis for* V is a finite set of vectors $\mathcal{B} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\} \subset V$ with the following property:

> Every vector $\boldsymbol{v} \in V$ can be written in the form
>
> $$\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n$$
>
> for exactly one choice of scalars $a_1, \ldots, a_n \in F$.

An expression of the form $a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n$ is called a *linear combination of* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$.

Theorem 4.18 (Invariance of Dimension)**.** *Let V be a vector space that has a finite basis. Then every basis for V has exactly the same number of elements.*

Slides for RSA here:
https://web.williams.edu/Mathematics/sjmiller/public_html/math/talks/VCTALCryptography/Burlington2019/IntroRSA_VCTAL.pdf

More slides / talks on cryptography and error detecting/correcting codes here:
https://web.williams.edu/Mathematics/sjmiller/public_html/math/talks/VCTALCryptography/Burlington2019/index.htm

My book (with Midge Cozzens):
The Mathematics of Encryption: An Elementary Introduction
https://bookstore.ams.org/mawrld-29

https://www.amazon.com/Mathematics-Encryption-Elementary-Introduction-Mathematical/dp/0821883216/ref=sr_1_1?crid=2E3QTSJZEGU8V&dib=eyJ2IjoiMSJ9.tl9AM9D1Cfpo6RlrvbmeZhbhMXW8_AEx18LXdURURerGjHj071QN20LucGBJIEps._F6Y6Z0AJIK5knbjd4R1z21ShF8cEotb7mrcDb1NekY&dib_tag=se&keywords=The+Mathematics+of+Encryption%3A+An+Elementary+Introduction&qid=1709658023&sprefix=the+mathematics+of+encryption+an+elementary+introduction%2Caps%2C152&sr=8-1

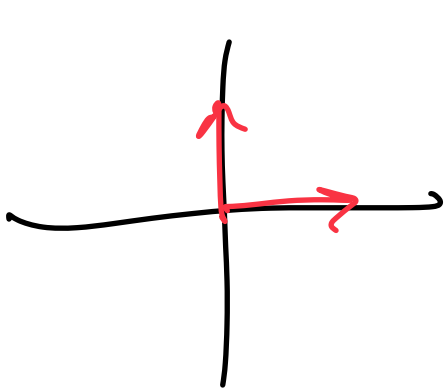
Definition 4.11. Let V be an F-vector space. A *finite*[5] *basis for* V is a finite set of vectors $\mathcal{B} = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\} \subset V$ with the following property:

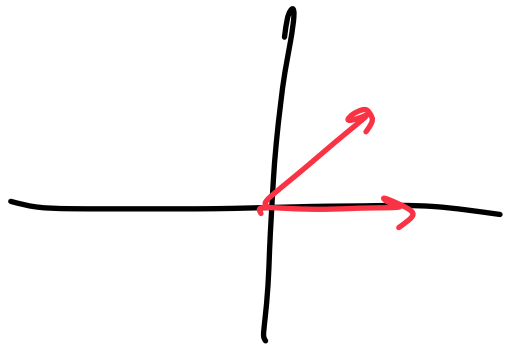
> Every vector $\boldsymbol{v} \in V$ can be written in the form
>
> $$\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2 + \cdots + a_n\boldsymbol{v}_n$$
>
> for exactly one choice of scalars $a_1, \ldots, a_n \in F$.

An expression of the form $a_1\boldsymbol{v}_1 + \cdots + a_n\boldsymbol{v}_n$ is called a *linear combination of* $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$.

Theorem 4.18 (Invariance of Dimension)**.** *Let V be a vector space that has a finite basis. Then every basis for V has exactly the same number of elements.*

$\mathbb{R}^2$





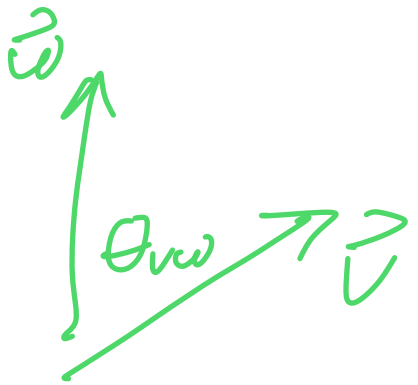
Example: $P_n(F)$ = all polys with coeffs in F of deg at most n

$P_2(\mathbb{R})$ = quadratics with real coeffs

$P_3(\mathbb{C})$ = cubics with complex coeff

Basis: $1, x, x^2$ or $1, x, x^2, x^3$

$$1, \quad 1+x, \quad 1+x+\frac{x^2}{2!}$$



$$\vec{v}\cdot\vec{w} = |\vec{v}|\,|\vec{w}|\cos\theta_{vw}$$

$$\sum_{k=1}^{n} v_k w_k \qquad \sqrt{v_1^2+\cdots+v_n^2}$$

$y = 17 \quad x = 11$

$17 = \boxed{1}\,11 + \boxed{6}$

$11 = \boxed{1}\,6 + \boxed{5}$

$6 = \boxed{1}\,5 + \boxed{1}$ ← gcd

$5 = \boxed{5}\,1 + \boxed{0}$

↑ gcd

$1 = 6 - 1 \cdot 5$

$= 6 - 1\left(11 - 1 \cdot 6\right)$

$= 6 - 1 \cdot 11 + 1 \cdot 6$

$= 2 \cdot 6 - 1 \cdot 11$

$= (-1) \cdot 11 + 2 \cdot 6$

$= (-1)(11) + 2\,(17 - 1 \cdot 11)$

$= -1 \cdot 11 + 2 \cdot 17 - 2 \cdot 11$

$= \underbrace{2 \cdot 17}_{34} - \underbrace{3 \cdot 11}_{33}$

$r_n = q_n r_{n+1} + r_{n+2} \qquad 0 \leq r_{n+2} < r_{n+1}$

Prove: $r_{n+2} \leq \frac{1}{2} r_n$

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: Theory; Section 2: Examples/Coding

Lecture 12: 3/12/24: https://youtu.be/piMrVKstQyE

Chapter Five: Fields

Definition 5.1. A *field* is a commutative ring F with the property that for every $a \in F$ with $a \neq 0$ there is a $b \in F$ satisfying $ab = 1$.

Definition 5.3. Let R be a commutative ring. The *unit group of* R is the group

$$R^* = \{a \in R : \text{there is a } b \in R \text{ such that } ab = 1\},$$

Normally write a^{-1} for b, and $ba = ab = 1$ as commutative

Examples: $\mathbb{Z}^* = \{-1, 1\}$

$\mathbb{Q}^* = \{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } a, b \neq 0\} = \mathbb{Q} \setminus \{0\}$

$(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \{1, 2, \ldots, n-1\} \text{ s.t. } \gcd(a, n) = 1\}$

Proof. Euclidean Alg: $\exists\, x, y$ s.t. $ax + ny = \gcd(a, n)$

if $\gcd(a, n) = 1$ then $ax + ny = 1$

so $ax \equiv 1 \bmod n$ so a is invertible! ∎

If n is prime this is a field

Proposition 5.4. *Let F and K be fields, and let $\phi : F \to K$ be a ring homomorphism.*

(a) *The map ϕ is injective.*

(b) *Let $a \in F^*$. Then $\phi(a^{-1}) = \phi(a)^{-1}$.*

Proof of (b): $\forall x,y \in F \quad \phi(xy) = \phi(x)\phi(y)$ as ϕ is a ring-homom

Take $x = a$, $y = a^{-1}$ Then $\phi(aa^{-1}) = \phi(a)\phi(a^{-1})$

but as $aa^{-1} = 1_F$ and $\phi(1_F) = 1_K$ Then $\phi(a)\phi(a^{-1}) = 1_K$

Thus the mult inverse of $\phi(a)$ is $\phi(a^{-1})$ so $\phi(a)^{-1} = \phi(a^{-1})$

Can also show $(\phi(a^{-1}))^{-1} = \phi(a)$

Proof of (a)

See next page

Proof that ring homom $\varphi: F \to K$ is injective

Assume $\varphi(x) = \varphi(y)$, must show $x = y$

Implies $\varphi(x) - \varphi(y) = 0_K$ or $\varphi(x-y) = 0_K$ as φ is a ring-homom

Means $x - y \in \ker(\varphi)$

Know $0_F \in \ker(\varphi)$, must show nothing else.

Assume $x - y \neq 0_F$ This has an inverse as F is a field (using field)

So $(x-y)^{-1}$ exists and $\varphi\left((x-y)(x-y)^{-1}\right) = \varphi(1_F) = 1_K$

As φ is a ring-homom $\Rightarrow$ $\varphi(x-y)\,\varphi((x-y)^{-1}) = 1_K$

$0_K \cdot \varphi((x-y)^{-1}) = 1_K$ so $0_K = 1_K$

Contradiction

Thus $x - y = 0_F$ or $x = y$ so injective ∎

$\{a+b\sqrt{2}+c\sqrt{3} : a,b,c \in \mathbb{Q}\}$ $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d \in \mathbb{Q}\}$

Is $\sqrt{6} = a+b\sqrt{2}+c\sqrt{3}$ for some a,b,c?

If $a=0$: Square: $6 = (b\sqrt{2}+c\sqrt{3})^2 = 2b^2+3c^2+2bc\sqrt{6}$

so $2bc\sqrt{6} = 2b^2+3c^2-6$

or $\sqrt{6} = \dfrac{2b^2+3c^2-6}{2bc} \in \mathbb{Q}$ Contradiction

Note: if $\sqrt{6} \in \mathbb{Q}$ then $\sqrt{6} = p/q$ so w.l.o.g. assume $gcd(p,q)=1$

Square: $6 = p^2/q^2$ or $6q^2 = p^2$

know $6 \mid p^2 = p\cdot p \Rightarrow 2 \mid p$ and $3 \mid p$ as a prime dividing a product divides at least one factor

so $p = 6u$ so $6q^2 = p^2 \Rightarrow 6q^2 = (6u)^2 = 6^2u^2$

Thus $q^2 = 6u^2$ and a similar argument shows $q = 6v$

Thus $6 \mid p$ and $6 \mid q$, violates relatively prime, contradiction

The Finite Field $\mathbb{F}_p$

$\mathbb{F}_p$: $(\mathbb{Z}/p\mathbb{Z})^*$ invertible elements: everything but 0

$\mathbb{Z}/p\mathbb{Z}$ ring: $(\mathbb{Z}/p\mathbb{Z})^* \cup \{0\}$

Euclidean algorithm: if $\gcd(a,p)=1$ Then $\exists x,y$ st $ax+bp=1$

so $ax = 1 \bmod p$ so a is invertible.

Consider $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$ with $\binom{p}{k} = \frac{p!}{k!(p-k)!}$

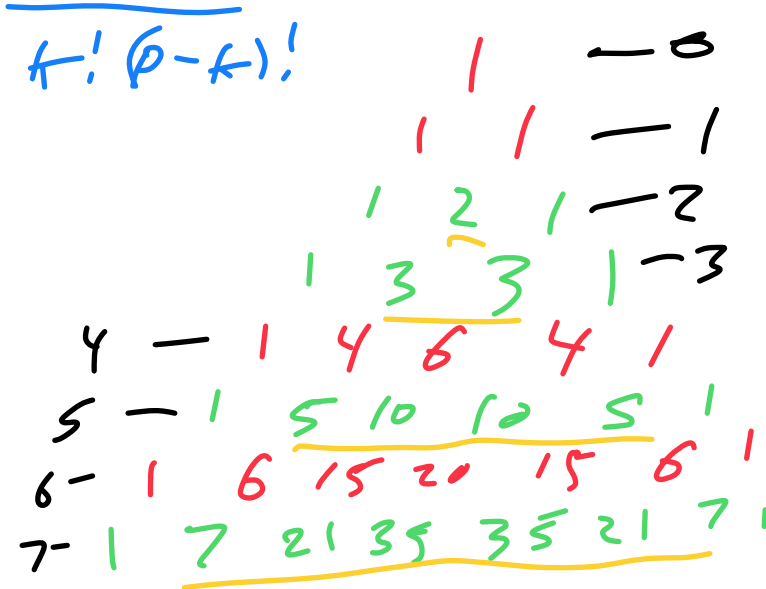
$= x^p + \left[\sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}\right] + y^p$

multiple of p when p prime

$\binom{p}{k} = \frac{p!}{k!(p-k)!}$ is an integer and p divides numerator but not denom if $1 \le k \le p-1$

If p is prime Then

$(x+y)^p = x^p + y^p$



Showed $(x+y)^p = x^p + y^p \bmod p$ if p prime

if $x=y=1 \Rightarrow (1+1)^p = 1^p + p^p \bmod p$

so $2^p = 2 \bmod p$ or $2^{p-1} = 1 \bmod p$ if $p \neq 2$

if $x=2, y=1 \Rightarrow (2+1)^p = 2^p + 1^p \bmod p$

$3^p = 2+1 \bmod p$

$3^p = 3 \bmod p$ so $3^{p-1} = 1 \bmod p$ if $p \neq 2,3$

Fermat's little Theorem!

Try $(1+1+1)^p$ instead of $(2+1)^p$

$((x+y)+z)^p = (x+y)^p + z^p \bmod p = x^p + y^p + z^p \bmod p$

Calc Recall: $(f(x)+g(x))' = f'(x) + g'(x)$

$$(f_1(x)+f_2(x)+f_3(x))' = \big((f_1(x)+f_2(x))+f_3(x)\big)'$$
$$= (f_1(x)+f_2(x))' + f_3'(x)$$
$$= (f_1'(x)+f_2'(x)) + f_3'(x)$$
$$= f_1'(x) + f_2'(x) + f_3'(x)$$

Challenge: find function $f(x)$ s.t. $f(x) = \sum_{n=0}^{\infty} f_n(x)$,
each $f_n(x)$ is differentiable but
$f'(x)$ is not $\sum_{n=0}^{\infty} f_n'(x)$

Definition 5.11. Let K be a field.[4] A *subfield of* K is a subset F of K that is itself a field using the addition and multiplication operations from K.

Definition 5.12. Let F be a field. An *extension field of* F is a field K such that F is a subfield of K. We write K/F to indicate that K is an extension field of F.[5]

$\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{R} \subsetneq \mathbb{C}$

field field field

Ex: let n be square-free, consider $\mathbb{Q}(\sqrt{n}) = \{a+b\sqrt{n} : a,b \in \mathbb{Q}\}$

$a+b\sqrt{n} \neq 0$ (since n is square-free, if a,b not both 0 then $a+b\sqrt{n}$ is non-zero)

Find inverse in $\mathbb{Q}(\sqrt{n})$: $(a+b\sqrt{n})^{-1} = \frac{1}{a+b\sqrt{n}} \frac{a-b\sqrt{n}}{a-b\sqrt{n}} = \frac{a-b\sqrt{n}}{a^2-b^2n}$

So inverse is $\frac{a}{a^2-b^2n} + \frac{-b}{a^2-b^2n}\sqrt{n}$, $a^2-b^2n \neq 0$. This is in $\mathbb{Q}(\sqrt{n})$

Section 2: Examples/Coding: https://youtu.be/v5Kg8F4WaFg

https://web.williams.edu/Mathematics/sjmiller/public_html/math/handouts/latex.htm

MATHEMATICA:

•Notebook: sample notebook for version 6: MathematicaIntroVer6.nb
•Video: Introductory lecture to using Mathematica (YouTube) Introductory lecture to using Mathematica (file)
•Mathematica starting tutorial: http://url.wolfram.com/6D6YZu/
•Importing data tutorial: http://www.wolfram.com/broadcast/screencasts/integrateddata/
•Interactive graphics: http://www.wolfram.com/broadcast/screencasts/makingmodels/
•Utilizing models: http://www.wolfram.com/broadcast/screencasts/utilizingmodels/
•Pascal triangle
example: PascalTriangleMod2_Streamlined_StevenJMiller.nb pascaltrianglemod2to2000ver2.dat pascaltrianglemod2to4000ver2.dat video here
•Marriage problem: cardgamemarriage.nb
•Catalan program: code (Mathematica notebook) printed pdf file
•Practice coding lectures: From Math/Stat 341: Probability From Math 12: Mathematics of Lego Bricks
•Practice coding problems and solutions: BasicCoding.nb BasicCoding.pdf

Much of math is about solving equations.

Example: polynomials:

- $ax + b = 0$, root $x = -b/a$.
- $ax^2 + bx + c = 0$, roots $(-b \pm \sqrt{b^2 - 4ac})/2a$.
- Cubic, quartic: formulas exist in terms of coefficients; not for quintic and higher.

$ax^2 + c = 0 \Rightarrow x^2 = -c/a$ thus $x = \pm\sqrt{-c/a}$

$ax^2 + bx + c = 0 \Rightarrow \alpha u^2 + \gamma = 0$ with $u = u(x)$

$a\left(x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} - \frac{b^2}{4a^2}\right) + c = 0$

$a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2}\right) + c = 0$

$a\left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a} + c = 0$

$a\left(x + \frac{b}{2a}\right)^2 + \frac{-(b^2 - 4ac)}{4a}$

$So\ \left(x + \frac{b}{2a}\right) = \pm\sqrt{\frac{b^2 - 4ac}{4a^2}} = \frac{\pm\sqrt{b^2 - 4ac}}{2a}$

$x = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a}$

Solve $x^2 + c = 0$

$ax^2 + c = 0$

vertex form $\rightarrow a(x+h)^2 + c = 0$

$ax^2 + bx + c = 0$

Cubic: For fun, here's the solution to $ax^3 + bx^2 + cx + d = 0$

w/log: a=1, b=6

```
Solve[a x^3 + b x^2 + c x + d == 0, x]
```

$$\left\{\left\{x \to -\frac{b}{3a} - \frac{2^{1/3}\left(-b^2 + 3ac\right)}{3a\left(-2b^3 + 9abc - 27a^2d + \sqrt{4\left(-b^2 + 3ac\right)^3 + \left(-2b^3 + 9abc - 27a^2d\right)^2}\right)^{1/3}} + \frac{\left(-2b^3 + 9abc - 27a^2d + \sqrt{4\left(-b^2 + 3ac\right)^3 + \left(-2b^3 + 9abc - 27a^2d\right)^2}\right)^{1/3}}{3 \times 2^{1/3} a}\right\},\right.$$

$$\left\{x \to -\frac{b}{3a} + \frac{\left(1 + i\sqrt{3}\right)\left(-b^2 + 3ac\right)}{3 \times 2^{2/3} a\left(-2b^3 + 9abc - 27a^2d + \sqrt{4\left(-b^2 + 3ac\right)^3 + \left(-2b^3 + 9abc - 27a^2d\right)^2}\right)^{1/3}} - \frac{\left(1 - i\sqrt{3}\right)\left(-2b^3 + 9abc - 27a^2d + \sqrt{4\left(-b^2 + 3ac\right)^3 + \left(-2b^3 + 9abc - 27a^2d\right)^2}\right)^{1/3}}{6 \times 2^{1/3} a}\right\},$$

$$\left.\left\{x \to -\frac{b}{3a} + \frac{\left(1 - i\sqrt{3}\right)\left(-b^2 + 3ac\right)}{3 \times 2^{2/3} a\left(-2b^3 + 9abc - 27a^2d + \sqrt{4\left(-b^2 + 3ac\right)^3 + \left(-2b^3 + 9abc - 27a^2d\right)^2}\right)^{1/3}} - \frac{\left(1 + i\sqrt{3}\right)\left(-2b^3 + 9abc - 27a^2d + \sqrt{4\left(-b^2 + 3ac\right)^3 + \left(-2b^3 + 9abc - 27a^2d\right)^2}\right)^{1/3}}{6 \times 2^{1/3} a}\right\}\right\}$$

One of three solutions to quartic $ax^4 + bx^3 + cx^2 + dx + e = 0$

wlog: $a=1$, $b=0$

```
Solve[a x^4 + b x^3 + c x^2 + d x + e == 0, x]
```

$$\left\{\left\{x \to -\frac{b}{4a} - \frac{1}{2}\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{\left(2^{1/3}\left(c^2 - 3bd + 12ae\right)\right)}{\left(3a\left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace + \sqrt{-4\left(c^2 - 3bd + 12ae\right)^3 + \left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace\right)^2}\right)^{1/3}\right)} + \frac{1}{3 \times 2^{1/3} a}\left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace + \sqrt{-4\left(c^2 - 3bd + 12ae\right)^3 + \left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace\right)^2}\right)^{1/3}} - \frac{1}{2}\sqrt{\frac{b^2}{2a^2} - \frac{4c}{3a} - \frac{\left(2^{1/3}\left(c^2 - 3bd + 12ae\right)\right)}{\left(3a\left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace + \sqrt{-4\left(c^2 - 3bd + 12ae\right)^3 + \left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace\right)^2}\right)^{1/3}\right)} - \frac{1}{3 \times 2^{1/3} a}\left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace + \sqrt{-4\left(c^2 - 3bd + 12ae\right)^3 + \left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace\right)^2}\right)^{1/3} - \left(-\frac{b^3}{a^3} + \frac{4bc}{a^2} - \frac{8d}{a}\right) \Big/ \left(4\sqrt{\frac{b^2}{4a^2} - \frac{2c}{3a} + \frac{\left(2^{1/3}\left(c^2 - 3bd + 12ae\right)\right)}{\left(3a\left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace + \sqrt{-4\left(c^2 - 3bd + 12ae\right)^3 + \left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace\right)^2}\right)^{1/3}\right)} + \frac{1}{3 \times 2^{1/3} a}\left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace + \sqrt{-4\left(c^2 - 3bd + 12ae\right)^3 + \left(2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace\right)^2}\right)^{1/3}}}\right)\right\}\right\},$$

Motivation: Generating Functions: Riemann Zeta Function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad Re(s) > 1$$

(p-series with $p > 1$ converges from calculus)

Study $\sum_{n=1}^{\infty} \frac{1}{n^p}$ p is a positive real

Integral test:

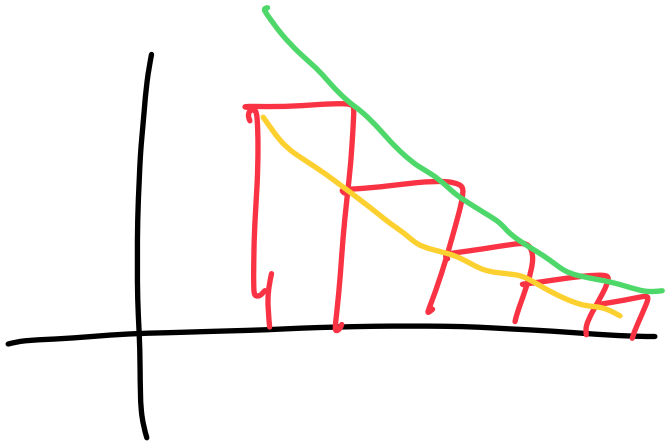
$$\sum_{n=1}^{N} \frac{1}{n^p} \approx \int_1^N \frac{1}{x^p}\,dx$$

$f(x)$ st $f(n) = 1/n^p$

Try $f(x) = 1/x^p$

If sum is monotonically ↑ or ↓

Then sum ≈ integral



$$= \int_1^N x^{-p}\,dx = \begin{cases} \frac{x^{1-p}}{1-p}\Big|_1^N & p \neq 1 \\ \log x \Big|_1^N & p = 1 \end{cases}$$

Converges if $p > 1$, diverges if $p < 1$

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\substack{p \\ \text{primes}}} \left(1 - 1/p^s\right)^{-1} \quad \mathrm{Re}(s) > 1$$

Fund Thm of Arithm (unique factorization)

$2024 \to 2025 \to 2026 \to \cdots$

$\mathrm{Inf}(n) = n$

If $s = 1$ $\lim_{s \to 1^+} \zeta(s) = \lim_{s \to 1^+} \sum_{n=1}^{\infty} \frac{1}{n^s}$ converging to $\sum_{n=1}^{\infty} \frac{1}{n}$

harmonic series: diverges

$\Rightarrow \infty$ many primes

If $s = 2$: $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \underbrace{\frac{\pi^2}{6}}_{\text{irrational}} = \underbrace{\prod_{p \text{ prime}} \left(1 - 1/p^2\right)^{-1}}_{\text{clearly finitely many primes}}$

This is rational!

An infinite product of rationals can be irrational

$$e = 2 * \frac{e * 1000}{2 * 1000}$$

$$= 2 * \frac{\lfloor e * 1000 \rfloor}{2000} *$$

An infinite product of rationals can be rational

$$\frac{1 \cdot 3}{2 \cdot 2} \cdot \frac{2 \cdot 4}{3 \cdot 3} \cdot \frac{3 \cdot 5}{4 \cdot 4} \cdot \frac{4 \cdot 6}{5 \cdot 5} \cdot \frac{5 \cdot 7}{6 \cdot 6} \cdots = \frac{1}{2}$$

$$\frac{1}{2} * \frac{7}{6}$$

In[43]:=
```
Det[M.W] - Det[M] × Det[W]
```

Out[43]=
```
0
```

In[47]:=
```
q1 = {{a, b}, {c, d}};
q2 = {{w, x}, {y, z}};
Simplify[Det[q1.q2] - Det[q1] × Det[q2]]
```

Out[49]=
```
0
```

In[50]:=
```
p1 = {{1, 0, 0, 0}, {0, 0, 1, 0}, {0, 0, 0, 1}, {0, 1, 0, 0}}
MatrixForm[p1]
```

Out[50]=
```
{{1, 0, 0, 0}, {0, 0, 1, 0}, {0, 0, 0, 1}, {0, 1, 0, 0}}
```

Out[51]//MatrixForm=

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

In[57]:=
```
For[n = 1, n ≤ 10, n++, Print["n = ", n, " and p1^", n, " = ",
  MatrixForm[MatrixPower[p1, n]]]]
```

$$n = 1 \text{ and } p1^1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$n = 2 \text{ and } p1^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$n = 3 \text{ and } p1^3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$n = 4 \text{ and } p1^4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Consider the group Z/2027Z. Look at the invertible elements mod 2027, so (Z/2027Z)*. Is this cyclic?

In[91]:=
```
findingcyclicgenerator[p_, justone_] := Module[{},
  For[g = 2, g ≤ p - 1, g++,
    { (* begins the for loop, this is a comment *)
     (* if justone = 1 stop once we find a generator, otherwise find all *)
     ggenerator = 1; (* use 1 for generator, 0 for not generator *)
     For[power = 1, power ≤ p - 2, power++, If[ Mod[g^power, p] == 1,
       {
        ggenerator = 0;
        power = p + 1;
       }]];
     If[ggenerator == 1, Print["Found a generator -- it is ", g]];
     If[ggenerator == 1 && justone == 1, g = p + 1];
    }]; (* this ends the for loop *)
 ]
```

In[92]:=
```
Timing[findingcyclicgenerator[NextPrime[200090], 1]]
```

```
Found a generator -- it is 3
```

Out[92]=
```
{18.25, Null}
```

In[82]:=
```
generatortest[a_, p_] := For[n = 1, n ≤ p - 1, n++, Print[Mod[a^n, p]]]
```

In[83]:=
```
generatortest[20, 23]
```

In[94]:=
```
efficientlyfindingcyclicgenerator[p_, justone_] := Module[{},
 For[g = 2, g ≤ p - 1, g++,
   { (* begins the for loop, this is a comment *)
    (* if justone = 1 stop once we find a generator, otherwise find all *)
    ggenerator = 1; (* use 1 for generator, 0 for not generator *)
    current = 1;
    For[power = 2, power ≤ p - 2, power++,
     {
      current = Mod[current * g, p]; (* g^power mod p *)×
       If[current == 1,
        {
         ggenerator = 0;
         power = p + 1;
        }]
     }];
    If[ggenerator == 1, Print["Found a generator -- it is ", g]];
    If[ggenerator == 1 && justone == 1, g = p + 1];
   }]; (* this ends the for loop *)
 ]
```

In[99]:=
```
Timing[efficientlyfindingcyclicgenerator[NextPrime[2007990], 1]]
```

```
Found a generator -- it is 7
```

Out[99]=
```
{2.5625, Null}
```

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: Examples/Coding; Section 2: Theory

Lecture 13: 3/14/24: https://youtu.be/prwj2_sApjc

Section 2: Chapter Five: Fields: Part II: https://youtu.be/U7nzejZt6gQ

$\{a+b\sqrt{2}+c\sqrt{3} : a,b,c \in \mathbb{Q}\}$ $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d \in \mathbb{Q}\}$

$\sqrt{6} = -a + b\sqrt{2} + c\sqrt{3}$ $a,b,c \in \mathbb{Q}$: can we do this?

$\sqrt{6} + a = b\sqrt{2} + c\sqrt{3}$

$6 + a^2 + 2a\sqrt{6} = 2b^2 + 3c^2 + 2bc\sqrt{6}$

Need $bc = a$

Need $6 + a^2 = 2b^2 + 3c^2$

Case 1: $a = 0$ then either b or c or both are 0, can show no soln.

Case 2: $a \neq 0$ so $b, c \neq 0$

$\hookrightarrow a = bc \Rightarrow \underbrace{6}_{\deg 0} + \underbrace{b^2c^2}_{\deg 4} = \underbrace{2b^2 + 3c^2}_{\deg 2}$

$b=1, c=2$ $b^2c^2 = 4$

$2b^2 + 3c^2 = 2 + 12 = 14$

Solve $10 + b^2c^2 = 2b^2 + 3c^2$

Cannot take $b=2, c=1$

Might be better to study say

$r\sqrt{6} = -a + b\sqrt{2} + c\sqrt{3}$

Then clear denoms so everything is an integer

Will show no integers work

RHS $\leq 5 \max(b,c)^2$

LHS $> \min(b,c)^2 \cdot \max(b,c)^2$

Cannot be a soln once $\min(b,c)^2 \geq 5$

So no soln unless $\min(b,c) \leq 2$ (wlog, $b, c \geq 0$)

Studying $6 + b^2c^2 = 2b^2 + 3c^2$ with $0 \le \min(b,c) \le 2$ integers

Subcase 0: $\min(b,c) = 0$: already done

Subcase 1 : $\min(b,c) = 1$

Subsubcase 1 : $b = 1$

Solve $6 + c^2 = 2 + 3c^2$

$4 = 2c^2$

$c^2 = 2$ no soln

Subsubcase 2: $c = 1$

$6 + b^2 = 2b^2 + 3$

$3 = b^2$ no soln

Subcase 2: $\min(b,c) = 2$

Subsubcase 1 : $b = 2$

$6 + 4c^2 = 8 + 3c^2$

$c^2 = 2$ no soln

Subsubcase : $c = 2$

$6 + 4b^2 = 2b^2 + 12$

$2b^2 = 6$

$b^2 = 3$ no soln

only does integers!

Consider a number of the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ with $a, b, c, d \in \mathbb{Q}$

Claim: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{$all numbers of this form$\}$: field!

If I give you a specific element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$,

i.e., say $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, it has an inverse

$\alpha + \beta\sqrt{2} + \gamma\sqrt{3} + \delta\sqrt{6}$ so long as it is not 0.

Ex: $(3 + 5\sqrt{2})^{-1} = \frac{1}{3+5\sqrt{2}} * \frac{3-5\sqrt{2}}{3-5\sqrt{2}} = \frac{3-5\sqrt{2}}{9-50} = -\frac{3}{41} + \frac{5}{41}\sqrt{2}$

$(1 - \sqrt{2} + \sqrt{3} + 8\sqrt{6})^{-1} = \frac{1}{1-\sqrt{2}+\sqrt{3}+8\sqrt{6}} * \frac{?}{?}$

Assume $r = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$

Imagine $f(x)=0$ has $x = r$ a root, $f(x) = \sum_{k=0}^{n} \alpha_k x^k$ smallest deg with $f(r)=0$

$\sum_{k=0}^{n} \alpha_k r^k = 0$, wlog assume $f(x)$ does not factor as the product of two polynomial. If it did,

say $f(x) = f_1(x) f_2(x)$, since we are in a field (rationals) $f(r)=0 \Rightarrow f_1(r)=0$ or $f_2(r)=0$,

so could study a smaller degree polynomial)

Constant term $\alpha_0 \neq 0$, if $\alpha_0 = 0$ then $f(x) = x g(x)$.

$\alpha_n r^n + \cdots + \alpha_1 r + \alpha_0 = 0$ with $\alpha_0 \neq 0$

$\alpha_n r^n + \cdots + \alpha_1 r = -\alpha_0$ with $\alpha_0 \neq 0$

$r(\alpha_n r^{n-1} + \cdots + \alpha_1) = -\alpha_0 \Rightarrow r\left(\underbrace{-\frac{\alpha_n}{\alpha_0} r^{n-1} - \cdots - \frac{\alpha_1}{\alpha_0}}_{\text{inverse to } r!}\right) = 1$

$r = 3 + 5\sqrt{2}$

$r^2 = 9 + 50 + 30\sqrt{2} = 59 + 30\sqrt{2}$

$r^2 - 6r = (59 + 30\sqrt{2}) - (18 + 30\sqrt{2}) = 41$

$r^2 - 6r - 41 = 0$ so here is a poly with $r = 3 + 5\sqrt{2}$ a root

$r(r-6) = 41$ $\quad r\left(\frac{1}{41}r - \frac{6}{41}\right) = 1$

Approach: $r = 3 + 5\sqrt{2}$

$(r-3) = 5\sqrt{2}$

$\left(\frac{r-3}{5}\right) = \sqrt{2}$ $\quad$ so $\left(\frac{r-3}{5}\right)^2 = 2$

so $(r-3)^2 - 50 = 0$

so $r^2 - 6r - 41 = 0$

Consider $r = a + b\sqrt{m} + c\sqrt{n} + d\sqrt{mn}$ m, n square-free distinct integers

looks like a vector with 4 components

$$r^2 = (a^2 + mb^2 + nc^2 + mnd^2) + (2ab\sqrt{m} + 2ncd\sqrt{m}) + (2ac\sqrt{n} + 2mbd\sqrt{n}) + (2bc\sqrt{mn} + 2ad\sqrt{m})$$

$$r \longleftrightarrow \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \quad \begin{matrix} \text{const} \\ \sqrt{m} \\ \sqrt{n} \\ \sqrt{mn} \end{matrix} \qquad r^2 \longleftrightarrow \begin{pmatrix} a^2 + mb^2 + nc^2 + mnd^2 \\ 2ab + 2ncd \\ 2ac + 2mbd \\ 2bc + 2ad \end{pmatrix}$$

$r^3 = \begin{pmatrix} \\ \\ \\ \end{pmatrix}$ $r^4 = \begin{pmatrix} \\ \\ \\ \end{pmatrix}$ $1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$

These live in $\mathbb{Q}^4$

$1, r, r^2, r^3, r^4$: linearly dependent

So $\alpha_0 1 + \alpha_1 r + \alpha_2 r^2 + \alpha_3 r^3 + \alpha_4 r^4 = 0$

Case 1: if $\alpha_0 = 0$ get $r(\alpha_1 + \alpha_2 r + \alpha_3 r^2 + \alpha_4 r^3) = 0$

Since $r \neq 0$ Then $\alpha_1 + \alpha_2 r + \alpha_3 r^2 + \alpha_4 r^3 = 0$

Keep doing and eventually get a poly with r as its root

Case 2: if $\alpha_0 \neq 0$ get $\alpha_1 r + \alpha_2 r^2 + \alpha_3 r^3 + \alpha_4 r^4 = -\alpha_0$

$r\left(-\frac{\alpha_1}{\alpha_0} - \frac{\alpha_2}{\alpha_0} r - \frac{\alpha_3}{\alpha_0} r^2 - \frac{\alpha_4}{\alpha_0} r^3\right) = 1$

Found the inverse!

Linear Algebra Review

Given vectors $\vec{v}_1, \ldots, \vec{v}_{n+1}$ in $\mathbb{Q}^n$ or $\mathbb{R}^n$: how do we find the linear combination that vanishes with at least one coefficient non-zero?

Solve $\alpha_1 \vec{v}_1 + \cdots + \alpha_n \vec{v}_n + \alpha_{n+1} \vec{v}_{n+1} = \vec{0}$

Assume soln exists with $\alpha_{n+1} \neq 0$

w.l.o.g. rescale so that $\alpha_{n+1} = 1$

Solve $\alpha_1 \vec{v}_1 + \cdots + \alpha_n \vec{v}_n = \vec{v}_{n+1}$

$$\underbrace{\begin{pmatrix} \uparrow & & \uparrow \\ \vec{v}_1 & \cdots & \vec{v}_n \\ \downarrow & & \downarrow \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}}_{\vec{x}} = \underbrace{\vec{v}_{n+1}}_{\vec{b}} \iff A\vec{x} = \vec{b}$$

If A invertible then $\vec{x} = A^{-1}\vec{b}$

$r = 1 - \sqrt{2} + \sqrt{3} - \sqrt{6}$ $\quad r \leftrightarrow (1, -1, 1, -1)^T$

$r * (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})$

$(1 - \sqrt{2} + \sqrt{3} - \sqrt{6})(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})$

$= (a - 2b + 3c - 6d)$

$+ (-a + b + 3d - 3c)\sqrt{2}$

$+ (c + a - 2d - 2b)\sqrt{3}$

$+ (d - a + b - c)\sqrt{6}$

$$\begin{pmatrix} 1 & -2 & 3 & -6 \\ -1 & 1 & -3 & 3 \\ 1 & -2 & 1 & -2 \\ -1 & 1 & -1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

A_r

$r \leftrightarrow \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$

```
A = {{1, -2, 3, -6}, {-1, 1, -3, 3}, {1, -2, 1, -2}, {-1, 1, -1, 1}};
MatrixForm[A]
r = Transpose[{1, -1, 1, -1}];
A.r
Print["Made it here"];
Expand[(1 - Sqrt[2] + Sqrt[3] - Sqrt[6])^2];
v1 = r
v2 = A.r
v3 = A.v2
v4 = A.v3
Print["Now here"];
B = {v1, v2, v3, v4}
MatrixForm[B]
M = Transpose[B];
Det[M]
Inverse[M]
Inverse[M].{1, 0, 0, 0}
```

$$\begin{pmatrix} 1 & -2 & 3 & -6 \\ -1 & 1 & -3 & 3 \\ 1 & -2 & 1 & -2 \\ -1 & 1 & -1 & 1 \end{pmatrix}$$

This matrix send a number of the form (a, b, c, d), *which is how we are representing* $a + b\ sqrt(2) + c\ sqrt(3) + d\ sqrt(6)$ *and multiplies by our* $r = 1 - sqrt(2) + sqrt(3) - sqrt(6)$. We call this matrix A, and our four vectors are r, A r = r^2, A^2 r = r^3, A^3 r = r^4.

```
{1, -1, 1, -1}

{12, -8, 6, -4}

{70, -50, 42, -30}

{476, -336, 272, -192}
```

$$\begin{pmatrix} 1 & 12 & 70 & 476 \\ -1 & -8 & -50 & -336 \\ 1 & 6 & 42 & 272 \\ -1 & -4 & -30 & -192 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 2 & \frac{5}{2} & -5 & -\frac{13}{2} \\ 4 & \frac{13}{2} & -\frac{5}{2} & -5 \\ 1 & \frac{9}{4} & \frac{1}{2} & -\frac{3}{4} \\ -\frac{1}{4} & -\frac{1}{2} & 0 & \frac{1}{4} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \\ 1 \\ -\frac{1}{4} \end{pmatrix}$$

```
Clear[r]

r = 1 - Sqrt[2] + Sqrt[3] - Sqrt[6]
Expand[2 r + 4 r^2 + r^3 - (1 / 4) r^4 - 1]
```

$1 - \sqrt{2} + \sqrt{3} - \sqrt{6}$

```
0
```

We have found our polynomial which has
r = 1 – sqrt(2) + sqrt(3) – sqrt(6)
as a root! Remember we were solving Ax = (1,0,0,0)^T so had to subtract 1 from the linear combinations, but we found a polynomial with integer coefficients and the desired root.

Section 2: 3/14/24: Lecture 13: https://youtu.be/U7nzejZt6gQ

Proposition 5.15. *Let L/F be an extension of fields, and let $\alpha_1, \ldots, \alpha_n \in L$. Then there is a unique field K with the following properties:*

(i) $F \subseteq K \subseteq L$.
(ii) $\alpha_1, \ldots, \alpha_n \in K$.
(iii) *If K' is a field satisfying $F \subseteq K' \subseteq L$ and $\alpha_1, \ldots, \alpha_n \in K'$, then $K \subseteq K'$.*

The field K is denoted $F(\alpha_1, \ldots, \alpha_n)$ and is called the extension field of F generated by $\alpha_1, \ldots, \alpha_n$. *The definition says that $F(\alpha_1, \ldots, \alpha_n)$ is the smallest subfield of L that contains both F and $\alpha_1, \ldots, \alpha_n$.*

$\mathbb{R}$, $i = \sqrt{-1}$

$x^2 + 1 = 0$

$\mathbb{C} = \mathbb{R}(i)$

$(2+\pi i)x^3 + \sqrt{3}x - 11 + 8i = 0$

Proof: Look at all subfields of L containing $F, \alpha_1, \ldots, \alpha_n$

↳ non-empty as L works.

Try $K = \bigcap$ (all subfields of L containing $F, \alpha_1, \ldots, \alpha_n$)

Clearly $F \subseteq K, \alpha_1, \ldots, \alpha_n \in K$.

Must show K is a field

Must check all field conditions: most are inherited!

Given $x, y \in K$ is $x+y$ and $xy \in K$?

As $x, y \in K$ They are in every subfield of L containing $F, \alpha_1, \ldots, \alpha_n$

$x+y$ is in every subfield of L containing $F, \alpha_1, \ldots, \alpha_n$

Say S is a subfield of L containing $F, \alpha_1, \ldots, \alpha_n$

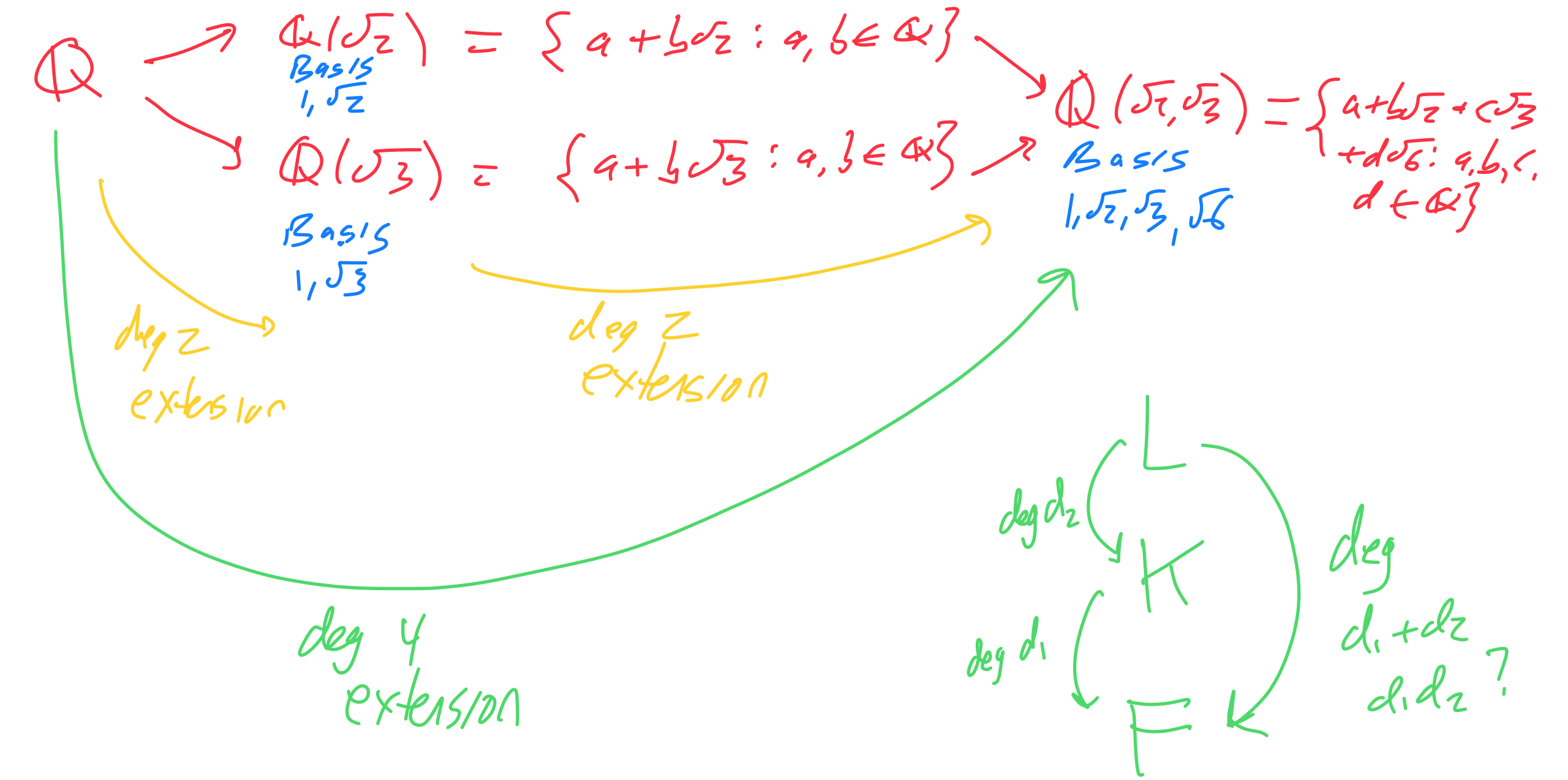
Since $x, y \in K \Rightarrow x, y \in S$ and $x^{-1} \in S$ if $x \neq 0$

But S is a field so $x+y, xy \in S$

As S is arbitrary, $x+y$ and xy in all our subfields

Thus $x, y \in K \Rightarrow x+y$ and $xy \in K$.

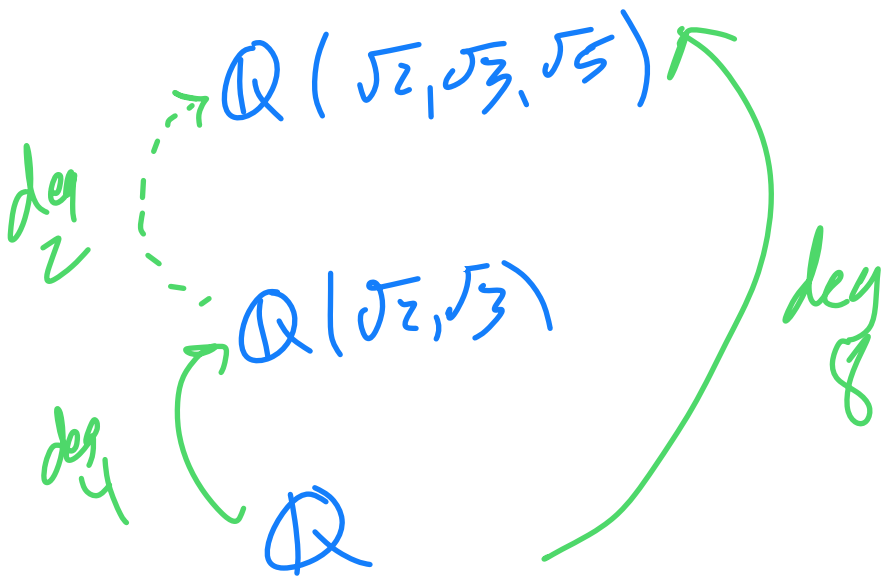
and also $x^{-1} \in K$


$\mathbb{Q}$
$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$
Basis
$1, \sqrt{2}$
$\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$
Basis
$1, \sqrt{3}$
$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$
Basis
$1, \sqrt{2}, \sqrt{3}, \sqrt{6}$
deg 2 extension
deg 2 extension
deg 4 extension
L
K
F
deg d_2
deg d_1
deg $d_1 + d_2$
$d_1 d_2$?

$1, \sqrt{2}, \sqrt{3}, \sqrt{5}$

$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{5} + e\sqrt{6} + f\sqrt{10} + g\sqrt{15} + h\sqrt{30}$

8 dimensional space



Suggests multiply degrees

Definition 5.16. Let K/F be an extension of fields. The *degree of* K *over* F, denoted $[K : F]$, is the dimension of K when viewed as an F-vector space,

$$[K : F] = \dim_F(K).$$

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 8$

Basis

$1, \sqrt{2}$

$1, \sqrt{2}, \sqrt{3}, \sqrt{6}$

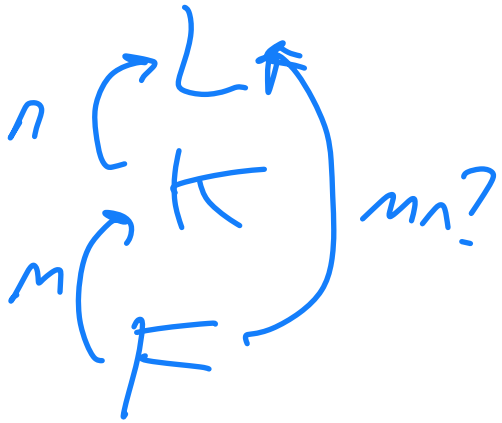
$1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}$

Theorem 5.18 (Multiplicativity of Degree in Towers of Fields). *Let $L/K/F$ be extensions of fields; i.e., L is an extension field of K, and K is an extension field of F, so we may also view L as an extension field of F.*

(a) *If both of the degrees $[L : K]$ and $[K : F]$ are finite, then $[L : F]$ is also finite, and the degrees satisfy the relation*

$$[L : F] = [L : K] \cdot [K : F]. \tag{5.1}$$

(b) *If either of the degrees $[L : K]$ and $[K : F]$ is infinite, then $[L : F]$ is also infinite.*



Proof of (a): deg K over F is m: any $k \in K$ of form $\alpha_1 k_1 + \cdots + \alpha_m k_m$ (α's in F)
deg L over K is n: any $l \in L$ of form $\beta_1 l_1 + \cdots + \beta_n l_n$ (β's in K)
here $k_1, \ldots, k_m$ is a basis for K over F, $l_1, \ldots, l_n$ basis for L over K
Thoughts for basis elements of L over F? Try: $k_1 l_1, k_1 l_2, \ldots, k_m l_n$

Given $x \in L$, write $x = x_1 l_1 + \cdots + x_n l_n$, $x_i \in K$
But have a basis for K over F: each $x_i = x_{i1} k_1 + \cdots + x_{im} k_m$, $x_{ij} \in F$
$x = (x_{11} k_1 + \cdots + x_{1m} k_m) l_1 + \cdots = x_{11} k_1 l_1 + \cdots$
($x_{11} \in F$)
shows $k_1 l_1, \ldots, k_m l_n$ spans

Must show $k_1 l_1, \dots, k_m l_n$ are lin independent

Assume $\sum_{j=0}^{n} \sum_{i=0}^{m} c_{ij} k_i l_j = 0$ Must show all c's vanish

$$= \left(\sum_{i=0}^{m} c_{i1} k_i \right) l_1 + \left(\sum_{i=0}^{m} c_{i2} k_i \right) l_2 + \cdots + \left(\sum_{i=0}^{m} c_{in} k_i \right) l_n$$

as $l_1, l_2, \dots, l_n$ are Lin Indep, only way a lin combination can be zero is if each coeff is zero!

$$\Rightarrow \sum_{i=0}^{m} c_{i1} k_i = 0, \quad \dots, \quad \sum_{i=0}^{m} c_{in} k_i = 0$$

$c_{11} k_1 + c_{21} k_2 + \cdots + c_{m1} k_m = 0$ as k's Lin Indep $\Rightarrow$ c's $= 0$



5.5. Polynomial Rings

Definition 5.19. Let F be a field, and let $f(x) \in F[x]$ be a non-zero polynomial. We write the polynomial $f(x)$ as

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d \quad \text{with } a_d \neq 0.$$

each $a_k \in F$

Then the *degree of* f is

$$\deg(f) = d.$$

By convention, we set $\deg(0) = -\infty$, a quantity that is smaller than every real number. Further, if $a_d = 1$, then we say that f is a *monic polynomial*.

Hope: $\deg(fg) = \deg(f) + \deg(g)$

$\deg(x^4 x^5) = \deg(x^4) + \deg(x^5)$

$9 \qquad\qquad 4 \qquad\quad 5$

$\deg(0 \cdot f) = \deg(0) + \deg f$

$\deg(0) = \deg(0) + \deg(f)$

need $\deg(0) = -\infty$ for this to work

What if F is not a field

Consider $\mathbb{Z}/12\mathbb{Z}$

$f(x) = 3x^5 + 1$

$g(x) = 4x$

$f(x)g(x) = 12x^6 + 4x = 4x$

so $\deg(fg) \neq \deg(f) + \deg(g)$

problem: divisors of zero

Ex: $f(x) = a_n x^n + \dots \quad g(x) = b_n x^n + \dots$

$f(x)g(x) = a_n b_n x^{n+n} + \dots$ and $a_n b_n \neq 0$

Avoid

$\infty - \infty$

$0 \cdot \infty$

∞ / ∞

$0/0$

OK

$r - \infty$

$r + \infty$

$r \cdot \infty$

r / ∞

Proposition 5.20 (Division-with-Remainder for Polynomials). *Let F be a field, and let $f(x), g(x) \in F[x]$ be a polynomials with $g(x) \neq 0$. Then there are unique polynomials $q(x), r(x) \in F[x]$ satisfying*

$$f(x) = g(x)q(x) + r(x) \quad \text{with} \quad \deg(r) < \deg(g). \tag{5.4}$$

Proof by Induction $f(x) = a_n x^n + \cdots$ $g(x) = b_m x^m + \cdots$ assume $n \geq m$

$f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = c_{n-1} x^{n-1}$ done by induction

$a_n x^n$ $b_m x^m$ note $b_m \neq 0$ as $\deg(g) = m$

If F isn't a field, may not have $b_m^{-1} = 1/b_m$

$a_n b_m^{-1}$

Show uniqueness

Theorem 5.21. *Let F be a field, and let $I \subseteq F[x]$ be an ideal in the ring $F[x]$. Then I is a principal ideal.*

Proof Principal

Let g be a poly of smallest (finite) deg in I

Wlog, assume $I \neq \{0\}$, that's principal and just (a)

If $f \in I$ then $f(x) = q(x)g(x) + r(x)$, $\deg r < \deg g$

but $r(x) = \underbrace{\underbrace{f(x)}_{\in I} - \underbrace{q(x)g(x)}_{\in I}}_{\in I} \in I$

Must have $r(x) = 0$ so f is a multiple of g
so it is principal ∎

5.6. Building Extension Fields

Reducible and irreducible polynomials:

$x^2 - 1 = (x-1)(x+1)$

$x^2 + 1 = (x+i)(x-i)$ in complex numbers

not factorizable over reals

Consider $R = \mathbb{Z}/2\mathbb{Z}$ so $2 = 0$

$x^2 + 1 = x^2 + 2x + 1 = (x+1)(x+1)$

Theorem 5.26. *Let F be a field, and let $f(x) \in F[x]$ be a non-zero polynomial. The following are equivalent:*

(a) *The polynomial $f(x)$ is irreducible.*

(b) *The principal ideal $f(x)F[x]$ generated by $f(x)$ is a maximal ideal.*

(c) *The quotient ring $F[x]/f(x)F[x]$ is a field.*

Theorem 5.27. *Let F be a field, let $f(x) \in F[x]$ be an irreducible polynomial, let $I_f = f(x)F[x]$ be the principal ideal generated by $f(x)$, and let $K_f = F[x]/I_f$ be the indicated quotient ring.*

(a) *The ring K_f is a field.*

(b) *We may identify the field F with a subfield of K_f via the map $F \to K_f$ defined by $c \mapsto c + I_f$.*

(c) *The polynomial $f(x)$ has a root in the field K_f.*

(d) *The field K_f is a finite extension of the field of F. Its degree is given by*

$$[K_f : F] = \deg(f).$$

5.7. Finite Fields

Proposition 5.28. *Let F be a finite field.*

(a) *The characteristic of F is prime.*

(b) *Let $p = \mathrm{char}(F)$. Then the finite field $\mathbb{F}_p$ is a subfield of F, in the sense that there is a unique injective homomorphism*

$$\mathbb{F}_p \hookrightarrow F.$$

(c) *The number of elements of F is given by the formula*

$$\#F = p^{[F:\mathbb{F}_p]}.$$

In particular, the number of elements in a finite field is always a power of a prime.

$\mathbb{Z}/p\mathbb{Z}$

$a_i \in \mathbb{F}_p$

$F = a_1 f_1 + \cdots + a_k f_k$

choices is p^k

Proof of a $\varphi: \mathbb{Z} \to F$ $\varphi(0) = 0$ $\varphi(1) = 1$

Assume $\varphi(n) = 0$ with $n = ab$, $a, b > 1$, smallest n

$0 = \varphi(ab) = \varphi(a)\varphi(b)$ in F, F is a field, no divisors of zero

$0 = \varphi(p) = \varphi(p \cdot 1) = \varphi(p)\varphi(1) = \varphi(p)$

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: Groups II: https://youtu.be/-Fh-2GC5CE0

Lecture 14: 4/2/24:

Chapter Six: Groups: Part II: Normal Subgroups

Definition 6.1. Let G be a group, and let H be a subgroup of G. We denote the set of (left) cosets of G by

$$G/H = \{\text{(left) cosets of } H\}.$$

$G = \mathbb{Z}$ $H = n\mathbb{Z}$ clock group $\mathbb{Z}/n\mathbb{Z}$

Same as $\{0, 1, 2, \ldots, n-1\}$ under clock addition

closure $(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b \bmod n) + n\mathbb{Z}$

or $(a + b) + n\mathbb{Z}$

inverse $(a + n\mathbb{Z}) + ((n - a) + \mathbb{Z}) = 0 + n\mathbb{Z}$ (identity)

Assoc

Definition 6.2 (Proposed Coset Multiplication Algorithm)**.** Let G be a group, and let H be a subgroup of G.

Input:	Cosets C_1 and C_2 of H.
Computation:	Choose an element $g_1 \in C_1$ and an element $g_2 \in C_2$.
Output:	The coset $g_1 g_2 H$ containing the product $g_1 g_2$.

Concern: $C_1 C_2 = g_1 g_2 H$ where $g_1 \in C_1$ and $g_2 \in C_2$

What if took $g_1' \in C_1$ and $g_2' \in C_2$: is $g_1 g_2 H = g_1' g_2' H$?

Namely: $g_1 H \; g_2 H$ "=" $(g_1 g_2) H$ ⟵ same?

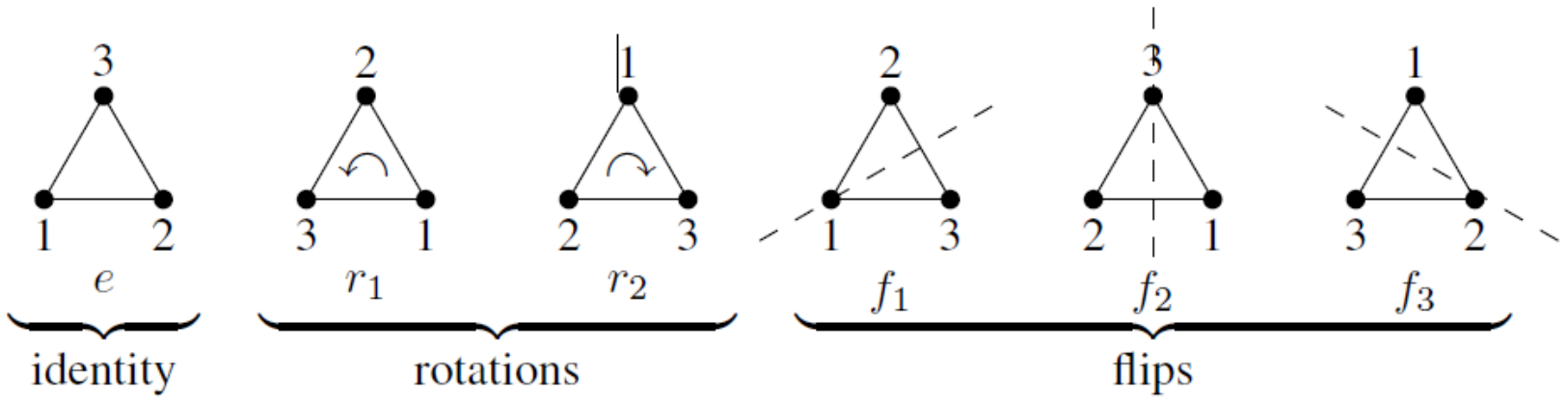
$g_1' H \; g_2' H$ "=" $(g_1' g_2') H$ ⟵

OK if G is Commutative

Example 2.46. We consider the dihedral group

$$\mathcal{D}_3 = \{e, r_1, r_2, f_1, f_2, f_3\}$$

associated to an equilateral triangle; cf. Example 2.22. As illustrated in Figure 8, it contains two rotations r_1 and r_2 and three flips (reflections) f_1, f_2, f_3.



$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

Read Example in Book

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$f_1 r_1 = f_3$$

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

$$r_1 f_1 = f_2$$

Not comm.

For all cosets C_1 and C_2 of H, for all pairs of elements $g_1, g_1' \in C_1$, and for all pairs of elements $g_2, g_2' \in C_2$, we want it to be true that

$$g_1 g_2 H = g_1' g_2' H.$$

$C_1 = g_1 H = g_1' H$ $\quad$ $C_2 = g_2 H = g_2' H$

$\exists h_1 \in H \Rightarrow g_1 = g_1' h_1$ $\quad$ $\exists h_2 \in H \Rightarrow g_2 = g_2' h_2$

Want $g_1 g_2 H = g_1' g_2' H = g_1' h_1 g_2' h_2 H$

same

Want $g_1' g_2' = g_1' h_1 g_2' h_2 h$ for some $h \in H$ (def of comm) (ok if H is cyclic)

Want $g_1' g_2' = g_1' g_2' (g_2')^{-1} h_1 g_2' h_2 h$

$= g_1' g_2' \underbrace{\left[(g_2')^{-1} h_1 g_2' \right]}_{\text{if in } H \text{ we win!}} \underbrace{h_2 h}_{\text{in } H}$

Want: $\forall g \in G, \forall h \in H$

$g^{-1} h g \in H$

Definition 6.5. Let G be a group, let $H \subset G$ be a subgroup, and let $g \in G$. The *g-conjugate of H* is the subgroup

$$g^{-1}Hg = \{g^{-1}hg : h \in H\}.$$

We say that H is a *normal subgroup of G* if it satisfies

$$g^{-1}Hg = H \quad \text{for every } g \in G.$$

$gH = Hg$

Example 6.6. If G is an abelian group, then every subgroup $H \subseteq G$ is normal, since $g^{-1}hg = h$.

$G = \{e, g, g^2, \dots, g^{p-1}\}$ p prime, has p elements

by Lagrange, no non-trivial subgroups

$G = \{e, g, g^2, \dots, g^{11}\}$ Then $\{e, g^2, g^4, g^6, g^8, g^{10}\}$

$\{e, g^3, g^6, g^9\}$

$\{e, g^4, g^8\}$

$\{e, g^6\}$

Proposition 6.9. *Let $\phi : G \to G'$ be a homomorphism of groups. Then $\ker(\phi)$ is a normal subgroup of G.*

$\phi(e) = e'$ and $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$

Proof:

Shows $\ker(\phi)$ is a subgroup

Closure: $\phi(g_1) = \phi(g_2) = e'$ Then $\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = e'e' = e'$ ✓

Assoc: $g_1, g_2, g_3 \in \ker(\phi)$ Then $(g_1 g_2)g_3 = g_1(g_2 g_3)$ inherited ✓ ✓

Identity: as $\phi(e) = e'$ get $e \in \ker(\phi)$

Inverses: if $g \in \ker(\phi)$ Then $\phi(gg^{-1}) = \phi(g)\phi(g^{-1})$ or $\phi(e) = \phi(g)\phi(g^{-1})$

but $\phi(e) = e' \Rightarrow e' = \phi(g)\phi(g^{-1})$ so $\phi(g)^{-1} = \phi(g^{-1})$ ✓

as $g \in \ker(\phi) \Rightarrow e' = e'\phi(g^{-1})$ so $\phi(g^{-1}) = e'$

$\ker(\phi)$ is normal

Show $\forall g \in G$: $g\ker(\phi)g^{-1} = \ker(\phi)$

let $h \in \ker(\phi)$ Then $\phi(g^{-1}hg) = \phi(g^{-1})\underbrace{\phi(h)}_{e'}\phi(g) = \phi(g^{-1})\phi(g)$

$= \phi(g^{-1}g) = \phi(e) = e'$

$\Rightarrow$ so $g\ker(\phi)g^{-1} \subset \ker(\phi)$ $\Leftarrow$ replace g with g^{-1} !

Should $g^{-1}\ker(\phi)g \subset \ker(\phi)$ $\forall g \in G$

Need $g^{-1}\ker(\phi)g \supset \ker(\phi)$

Same as $\ker(\phi) \supset g\ker(\phi)g^{-1}$

Use this with g^{-1} for g

Yields $(g^{-1})^{-1}\ker(\phi)g^{-1} \subset \ker(\phi)$

or $g\ker(\phi)g^{-1} \subset \ker(\phi)$

Proposition 6.10. *Let G be a group, and let $H \subset G$ be a subgroup.*

(a) *If $g^{-1}Hg \subseteq H$ for all $g \in G$, then H is a normal subgroup of G; i.e., it is enough to check one inclusion.*

(b) *For all $g \in G$, the conjugate set $g^{-1}Hg$ is a subgroup of G.*

(c) *For all $g \in G$, the map $H \to g^{-1}Hg$ defined by $h \mapsto g^{-1}hg$ is a group isomorphism. In particular, if H is finite, then H and its conjugates have the same number of elements.*

(b) $g^{-1}Hg = \{g^{-1}hg : h \in H\}$

closure: $(g^{-1}h_1g)(g^{-1}h_2g) = g^{-1}h_1h_2g \in g^{-1}Hg$

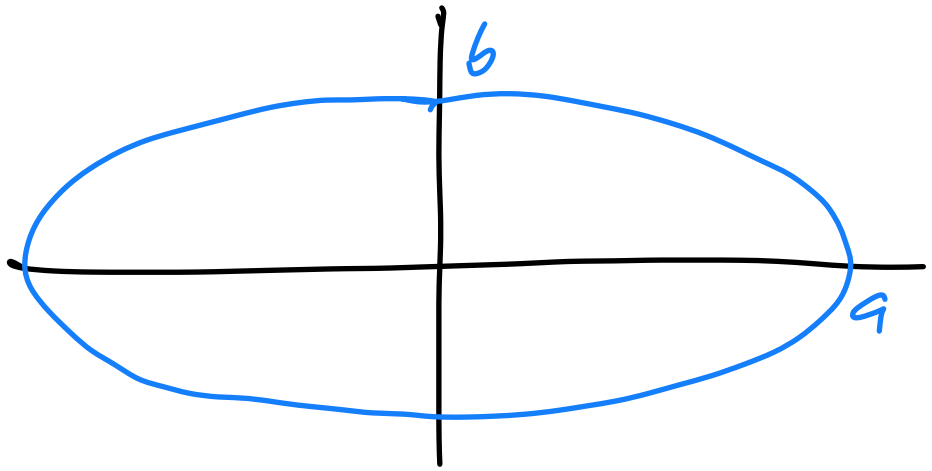
rest similar: identity is e, assoc inherit, $\bar{g}\bar{h}^{-1}g$ is inverse of $\bar{g}hg$

Linear Alg: Spectral Thm: if A is real sym, $\exists$ orthog Q st $A = Q^T \Lambda Q$

where $\Lambda = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ matrix of eigenvalues.

$$A^n = Q^T \Lambda Q \, Q^T \Lambda Q \cdots Q^T \Lambda Q = Q^T \Lambda^n Q$$

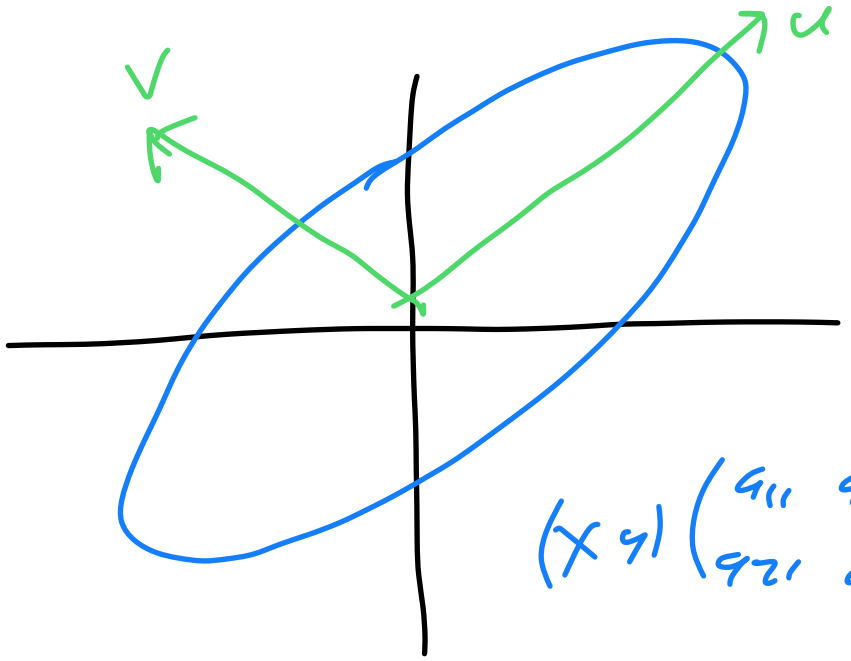
$Q^T = Q^{-1}$ this is conjugation



$$\left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 = 1$$

$$(x\ y)\begin{pmatrix} 1/a^2 & 0 \\ 0 & 1/b^2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 1$$

$$\begin{pmatrix} u \\ v \end{pmatrix} = Q\begin{pmatrix} x \\ y \end{pmatrix} \qquad Q = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$



$$(x\ y)\begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 1$$

$$\left(\frac{u}{a}\right)^2 + \left(\frac{v}{b}\right)^2 = 1$$

Lemma 6.11. *Let G be a group, and let H be a normal subgroup of G. Suppose taht $g_1, g_1', g_2, g_2' \in G$ satisfy*

$$g_1'H = g_1H \quad \text{and} \quad g_2'H = g_2H.$$

Then

$$g_1'g_2'H = g_1g_2H.$$

If H is normal, mult of cosets is well defined!

Read the Book

Theorem 6.12. *Let G be a group, and let H be a normal subgroup of G.*

(a) *The collection of cosets G/H is a group via the well-defined group operation*

$$g_1H \cdot g_2H = g_1g_2H. \tag{6.7}$$

(b) *The map*

$$\phi : G \longrightarrow G/H, \quad \phi(g) = gH,$$

is a homomorphism whose kernel is $\ker(\phi) = H$.

(c) *Let*

$$\psi : G \longrightarrow G'$$

be a homomorphism with the property that $H \subseteq \ker(\psi)$. Then there is a unique homomorphism

$$\lambda : G/H \longrightarrow G' \quad \textit{satisfying} \quad \lambda(gH) = \psi(g).$$

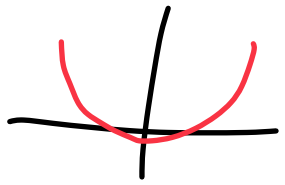
(d) *If we take $H = \ker(\psi)$ in* (c)*, then the homomorphism*

$$\lambda : G/\ker(\psi) \longrightarrow G'$$

is injective. In particular, we get an isomorphism

$$\lambda : G/\ker(\psi) \xrightarrow{\text{isomorphism}} \text{Image}(\lambda) \subseteq G'.$$

$f(x) = x^2$



$f : \mathbb{R} \to \mathbb{R}$ a bijection?

$f : [0,\infty) \to [0,\infty)$

bijection

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: Groups II: https://youtu.be/BS4TEOSoNY4
(video from section 2)

Lecture 15: 4/4/24:

Chapter Six: Groups: Part II: Orbits, Stabilizers, Sylow Theorem

6.2. Groups Acting on Sets

Definition 6.13. Let G be a group, and let X be a set. An *action of G on X* is a rule that assigns to each element $g \in G$ and each element $x \in X$ another element $g \cdot x \in X$, so that the following two axioms hold:

$f_g(x)$

Identity Axiom : $e \cdot x = x$ for all $x \in X$.

Associative Axiom : $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

$f_{g_1}(f_{g_2}(x)) = f_{g_1 g_2}(x)$

$G = GL_2(\mathbb{R}) = \{2\times 2 \text{ invertible matrices with real entries}\}$

$z = x + iy \in \mathbb{C}$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \dfrac{az+b}{cz+d}$ $\quad Iz = \dfrac{1z+0}{0z+1} = z$; Exercise : Show Assoc

If $\mathrm{Re}(z) > 0$, $\mathrm{Re}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} z\right) > 0$

What are the elements of X to which x is sent by the action of G? This set is called the *orbit of* x and is denoted by

$$Gx = \{g \cdot x : g \in G\}.$$

outputs

What are the elements of G that leave x unchanged? This set is called the *stabilizer of* x and is denoted by

$$G_x = \{g \in G : g \cdot x = x\}.$$

The stabilizer G_x is a subgroup of G; see Proposition 6.19(a).

$G = GL_2(\mathbb{R})$ $X = \{z \in \mathbb{C} : Re(z) > 0\}$

Solve $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = z$ or $\frac{az+b}{cz+d} = z \Rightarrow az+b = cz^2+dz$

If $b=c=0$ have $\frac{az}{d} = z$ get $a=d$

$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} z = \frac{az+0}{0z+a} = z$ Does G_z contain a non-diag matrix?

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ Case 1: $a = 0$ $\begin{pmatrix} 0 & b \\ c & d \end{pmatrix}$

Case 2: $a \neq 0$

$$\frac{az+b}{cz+d} = \frac{a(z+b/a)}{a(\frac{c}{a}z+d/a)} = \frac{z+b/a}{\frac{c}{a}z+\frac{d}{a}} = \begin{pmatrix} 1 & \frac{b}{a} \\ \frac{c}{a} & \frac{d}{1} \end{pmatrix} z$$

Can you reduce Ncle to $\frac{b}{a}=0$ or $\frac{b}{a}=1$?

Proposition 6.19. *Let G be a group that acts on a set X.*

(a) *Let $x \in X$. The stabilizer G_x is a subgroup of G.*

(b) *Define a relation $\sim$ on X by the following rule:*

$$x \sim y \quad \text{if} \quad y = gx \quad \text{for some} \quad g \in G.$$

Then $\sim$ is an equivalence relation, and

$$(\text{the equivalence class of } x) = (\text{the orbit } Gx \text{ of } x).$$

reflexive
symmetric
transitive

Proof: reflexive: $x \sim x$: take $g = e$

symmetric: if $x \sim y$ then $y = gx$ so $x = g^{-1}y$ so $y \sim x$

transitive is similar

to show $x \sim y$, $y \sim z \Rightarrow x \sim z$

Prove G_x is a subgroup of G

identity: $e \in G_x$ as $ex = x$ so e is in the stabilizer of x

assoc: inherits

inverse: if $g \in G_x$ then $g \cdot x = x \Rightarrow x = g^{-1}x$ so $g^{-1} \in G_x$

closure: assume $g_1, g_2 \in G_x$, show $g_1 g_2 \in G_x$

$$(g_1 g_2)x = g_1(g_2 x) = g_1 x = x$$

(g_2 in stabilizer; g_1 in stabilizer)

so $g_1 g_2 \in G_x$

∎

Proposition 6.19. *Let G be a group that acts on a set X.*

(c) *Let $x \in X$. There is a well-defined bijection*

orbit

$$\alpha : G/G_x \longrightarrow Gx$$

Stabilizer

defined by the following algorithm:

Input:	A coset $\mathcal{C}$ of the subgroup G_x.
Computation:	Choose an element $g \in \mathcal{C}$.
Output:	$\alpha(\mathcal{C})$ is the element $g \cdot x$ in the orbit Gx.

In particular, if G is finite, then

$$\#Gx = \frac{\#G}{\#G_x}.$$

Is this well-defined?

$g, \tilde{g} \in C = hG_x$ for some h

$g = hg_1$

$\tilde{g} = hg_2$

$g_1, g_2 \in G_x$

$gx = hg_1x = hx$ } same

$\tilde{g}x = hg_2x = hx$

Could $h_ix = h_jx$?

$x = h_i^{-1}h_jx \Rightarrow h_i^{-1}h_j \in G_x$

$h_j \in h_iG_x$: in same coset

$G = \cup h_kG_x$

all $g \in h_kG_x$ has same effect on x

Orbit of x is $Gx = \{h_1x, h_2x, h_3x, \dots\}$

By Lagrange: $\#G = \#(G/G_x)\,\#G_x \Rightarrow \#Gx = \frac{\#G}{\#G_x}$

Lagrange: $\#G = \#(G/H)\,\#H$

$H = G_x$ Stabilizer, Gx = orbit

Showed $\#G/G_x = \#Gx$

$\Rightarrow \#G = \#(Gx)\,\#G_x$

or $\#(Gx) = \dfrac{\#G}{\#G_x}$

Gx: orbit; G: group; G_x: stabilizer

6.3. The Orbit-Stabilizer Counting Theorem

Take $X = G$

$g \cdot x = gx$

$g \cdot x = g^{-1} x g$ or $g x g^{-1}$ conjugation

Let G be a finite group that acts on a finite set X. We start by proving a powerful theorem relating the sizes of X, G, and the various orbits and stabilizers. This counting theorem has many applications. It will be a crucial tool in our proof of Sylow's theorem in Section 6.4.

Theorem 6.21 (Orbit-Stabilizer Counting Theorem). *Let G be a finite group that acts on a finite set X. Choose $x_1, \ldots, x_k \in X$ so that $Gx_1, \ldots, Gx_k$ are the distinct orbits of elements of X. Then*[4]

$$\#X = \sum_{i=1}^{k} \#Gx_i = \sum_{i=1}^{k} \frac{\#G}{\#G_{x_i}}.$$

Previous page: $\#Gx_i = \#G / \#G_{x_i}$

Split X up into its orbits: $X = Gx_1 \cup Gx_2 \cup \cdots \cup Gx_k$

Prove Center is a subgroup

$Z = \{ z \in G \text{ s.t. } gz = zg \ \forall g \in G \}$

identity : ✓

assoc : inherited

inverse : if $gz = zg \ \forall g$ then $z^{-1} g z z^{-1} = z^{-1} z g z^{-1} \ \forall g \in G$

$z^{-1} g = g z^{-1} \ \forall g \in G$ s.t. z^{-1} in center

closure : exercise

Definition 6.23. Let G be a group. The *center of* G, denoted $Z(G)$, is the set of elements of G that commute with every element of G,

$$Z(G) = \{g \in G : gg' = g'g \text{ for every } g' \in G\}.$$

Remark 6.24. We leave it for you to prove that the center of G is a subgroup of G, and indeed, it is a normal subgroup; see Exercise 6.18.

Theorem 6.25. *Let p be a prime, and let G be a finite group with p^n elements for some $n \geq 1$. Then $Z(G) \neq \{e\}$; i.e., G contains a non-identity element that commutes with every element of G.*

Proof: $X = G$, define $g \cdot x$ by $g^{-1}xg$ conjugation

$$\#X = \sum \#G_{x_k} = \sum \#G / \#G_{x_k}$$

$\#X$: orbit; $\#G_{x_k}$: stabilizer

$$p^n = 1 + \text{stuff} = \sum_{k=1}^{m} p^n / p^{r_k}$$

p^n: multiple of p; 1: orbit of e

as by Lagrange $\#G_{x_k} = p^{r_k}$

$$1 + \left(\begin{array}{l}\#\text{ of } k \text{ such} \\ \text{that } r_k = n \\ (\text{Stabilizer} = G)\end{array}\right) + \sum_{\text{rest where } r_k < n} p^n / p^{r_k}$$

$1 + (\#\text{ of } k \text{ such that } r_k = n \text{ (Stabilizer} = G))$: multiple of p

$\sum_{\text{rest where } r_k < n} p^n / p^{r_k}$: multiple of p

Must be at least $p-1$ other elements whose stabilizer is G

$\forall g: g^{-1}xg = x$ or $\forall g: xg = gx$ so x commutes with all G, $x \in$ Center

Corollary 6.26. *Let p be prime, and let G be a group with p^2 elements. Then G is an abelian group.*

See book for proof

subgroups of order $1, p, p^2$

if $\exists x \in G$ with $\text{ord}(x) = p^2$ then $G = \langle x \rangle$

$G = \{0, x, 2x, 3x, \dots, (p^2-1)x\}$

What if no elements of size p^2?

Consider $\{(x,y) : 0 \le x, y < p\}$ clock version

Lemma 6.30. *Let p be prime, let $n \geq 0$, and let $m \geq 1$ with $p \nmid m$. Then the binomial coefficient $\binom{p^n m}{p^n}$ is not divisible by p.*

$$\binom{p^n m}{p^n} = \frac{p^n m \cdot (p^n m - 1) \cdot (p^n m - 2) \cdots (p^n m - p^n + 1)}{p^n \cdot (p^n - 1) \cdot (p^n - 2) \cdots 3 \cdot 2 \cdot 1} = \prod_{r=0}^{p^n - 1} \frac{p^n m - r}{p^n - r}.$$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

$$= \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1}$$

$$\frac{p^n m - p^l}{p^n - p^l} = \frac{p^l(p^{n-l} m - 1)}{p^l(p^{n-l} - 1)}$$

6.4. Sylow's Theorem (Slides from Section 2)

Theorem 6.29 (The First Part of Sylow's Theorem). *Let G be a finite group, let p be a prime, and let p^n be the largest power of p that divides $\#G$. Then G has a subgroup of order p^n.*

X = all subsets of G of size p^n, $\#X = ?$

Proceed by Induction: Assume $\#G = p^n m$

Base Case: $n = 1$: Win: G is the desired subgroup

Inductive Step: Assume true $\forall n' < n$, do for n

$$\#G = p^n m$$

$$\#X = \binom{p^n m}{p^n}$$ not divisible by p!

$$X = \bigcup G x_k$$

$$\#X = \sum \#G x_k = \sum \frac{\#G}{\#G_{x_k}}$$

orbit — Stabilizer

$\#G = p^n m$

$\#G_{x_k} = p^l \hat{n}$ and $\hat{n} \mid m$

not a multiple of p

Stabilizer's $l = n$

cannot be empty or LHS is a multiple of p and RHS is not.

So at least one orbit has a stabilizer with $l = n$

$\#G_x = p^l \hat{n}$: if $\hat{n} < m$ done by induction as this is a smaller group than G.

Stabilizer's $l < n$

$\frac{\#G}{\#G_x}$ is a multiple of p

multiple of p when summed all of these

What happens if $\tilde{n} = n$ so $\#G_x = \#G$

Have some set A with $p^\wedge$ elements and $\forall g \in G$, $gA = A$ $(A \in X)$

Remember $n \geq 2$ so $A \subsetneq G$

Claim: if $gA = A$ Then g live in

Define $g \cdot x$ to be gx

$\forall g \in G$: $gA = A$

Assume $\tilde{g}A = A$ $\forall \tilde{g} \in G$

Then $ga^{-1}A = A$ as $ga^{-1} \in G$ (set $\tilde{g} = ga^{-1}$)

so $ga^{-1}.a \in A$ but $ga^{-1}a = g$ so $g \in A$ $\forall g \in G$

$\#A$ is $p^\wedge$, $\#G = p^\wedge n > p^\wedge$ as $n \geq 2$, contradiction

QED

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: https://youtu.be/ZvRomUL37Gw

Lecture 16: 4/9/24:

Chapter Eight: Algebraic and Transcendental Numbers, Benford's Laws, Lessons from Eclipse/Totality (96% vs 100%, main term masking lower order terms, adapt on the fly)

Chapter 8: Fields — Part 2

8.1. Algebraic Numbers and Transcendental Numbers

Definition 8.1. Let L/F be an extension of fields, and let $\alpha \in L$. We say that α is *algebraic over* F if α is the root of a non-zero polynomial in $F[x]$. Otherwise we say that α is *transcendental over* F.

Who cares about such small differences?

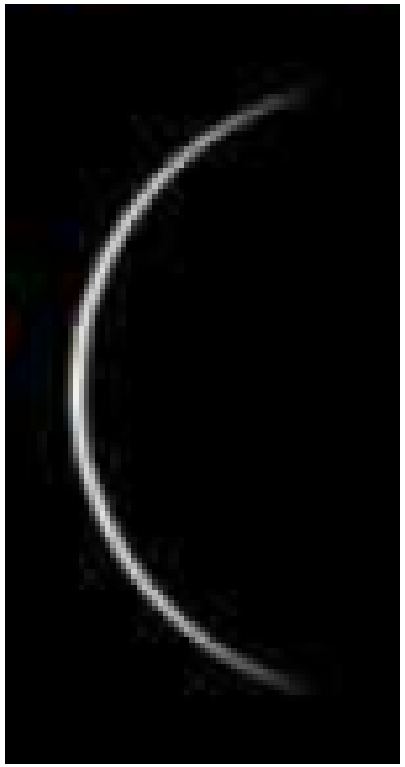
First 125 digits of some famous numbers….

```
3.14159265358979323846264338327950288419716939937510582097494459230781640628620899
 86280348253421170679821480865132823066470938446095505 82
```

```
0.21000100000000000000010000000000000000000000000000000000000000000000000000000000
 00000000000000000000000000000000000010000000000000
```

```
1.73205080756887729352744634150587236780342043159474350440560235337023472538513619
 72874074839619140675495145842432975769042969
```

So I can see 96% of the eclipse here, I don't think it's worth driving 90 minutes for just 4%.





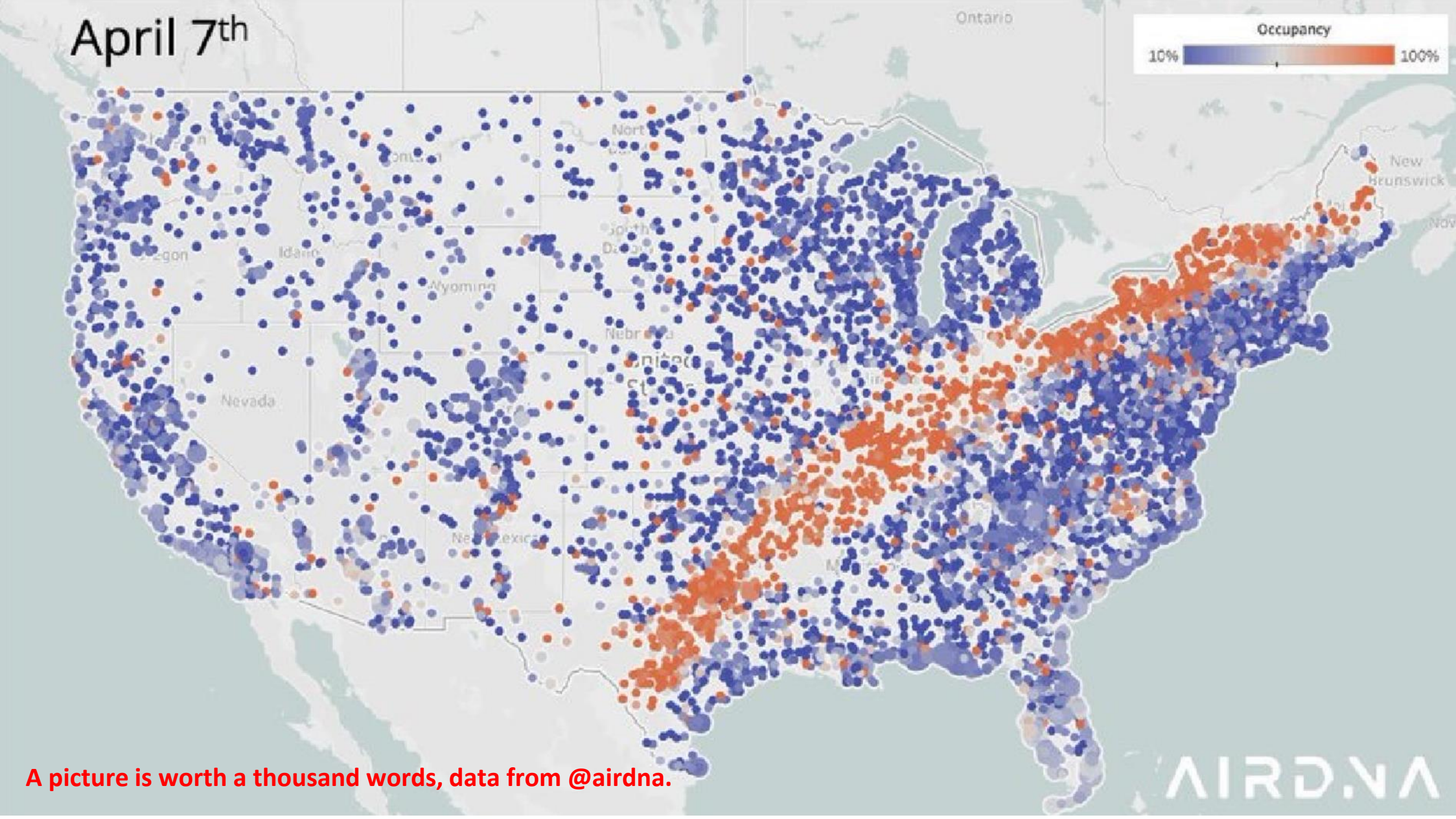

First from https://i.ytimg.com/vi/0TLAG0IeQBE/hqdefault.jpg, second from https://www.nbcnews.com/news/us-news/total-solar-eclipse-photos-2024-rcna146832 (Forth Worth), last two by me (Middlebury, VT): April 8, 2024.

Main term can dwarf lower order terms….





First from me (April 8, 2024 at Middlebury, VT); second from https://www.wgauradio.com/news/national/missing-totality/OJDGRCOH5DJLHO3FXJK2UMW3QQ/



A picture is worth a thousand words, data from @airdna.

Adjust to changing times….

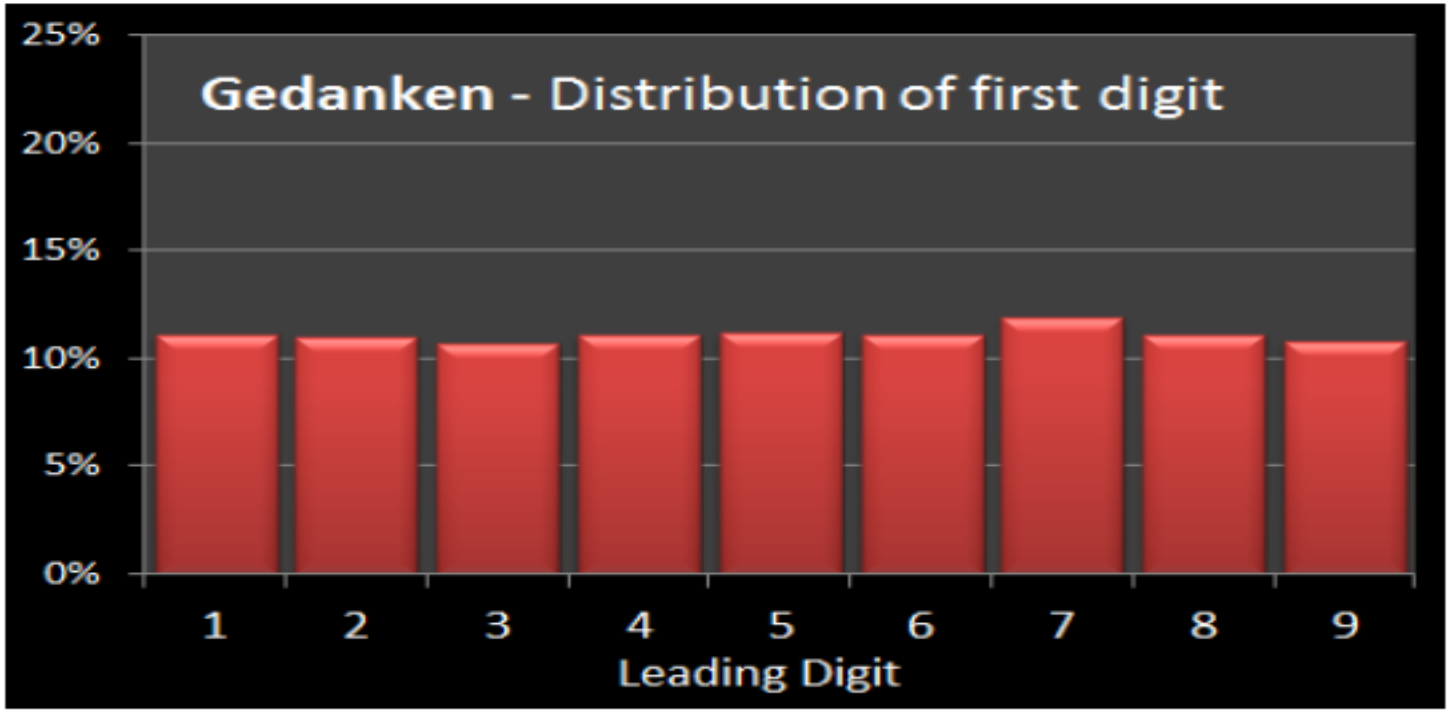




Left is inn we stayed at, took almost an hour to check in b/c only one person could handle the computer for arrivals.
Right is a froyo place, normally closed on Mondays, called and said open as today is the eclipse, huge crowds, went twice!

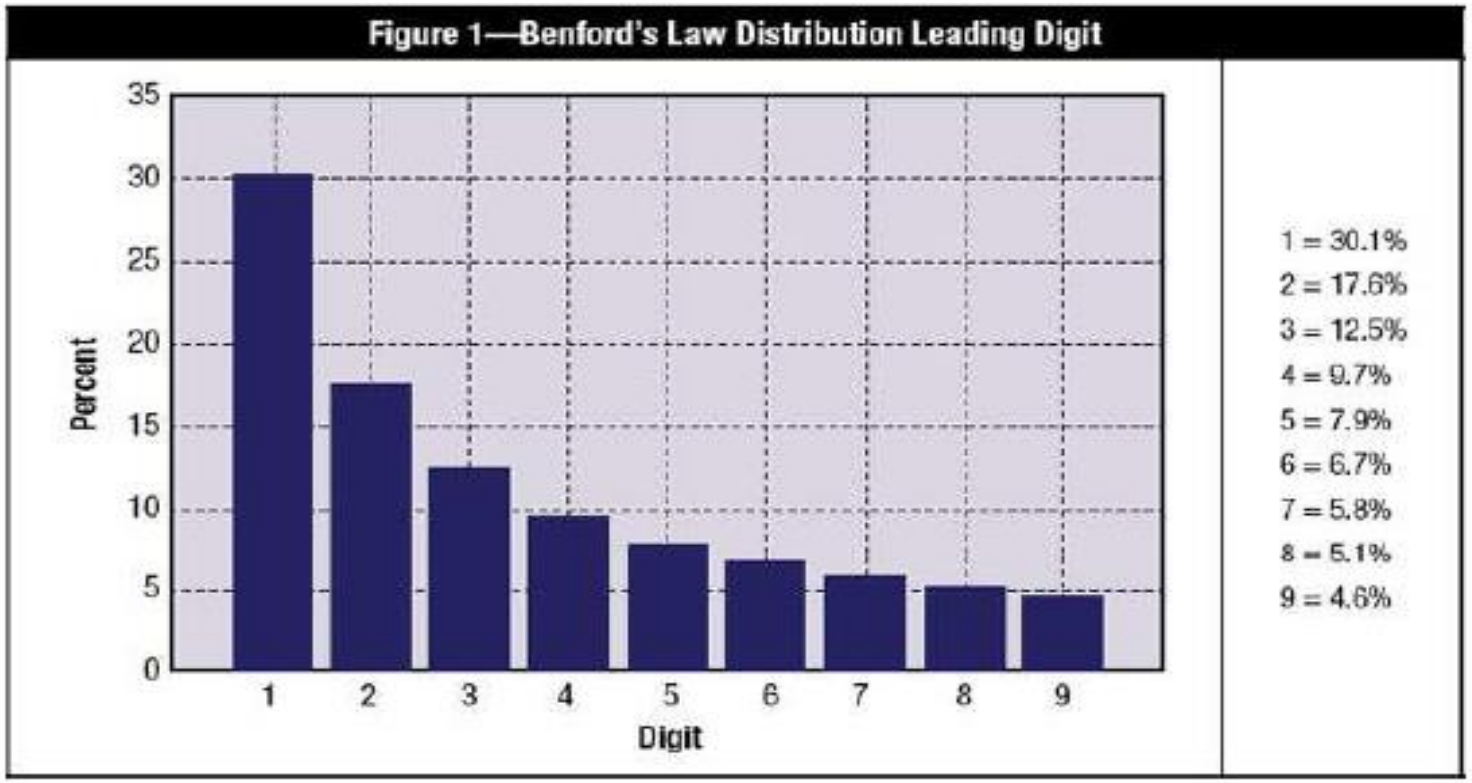
Benford's Law: Why the IRS and others care about Number Theory (and you should too!), PIMS Distinguished Lecture, UNBC, November 4, 2020 (https://youtu.be/NSuXJRIFcXc). pdf Vassar College pdf (https://youtu.be/fm3s-xjcnAE).

Motivating Question: For a nice data set, such as the Fibonacci numbers, stock prices, street addresses of college employees and students, ..., what percent of the leading digits are 1?



Natural guess: 10% (but immediately correct to 11%!).

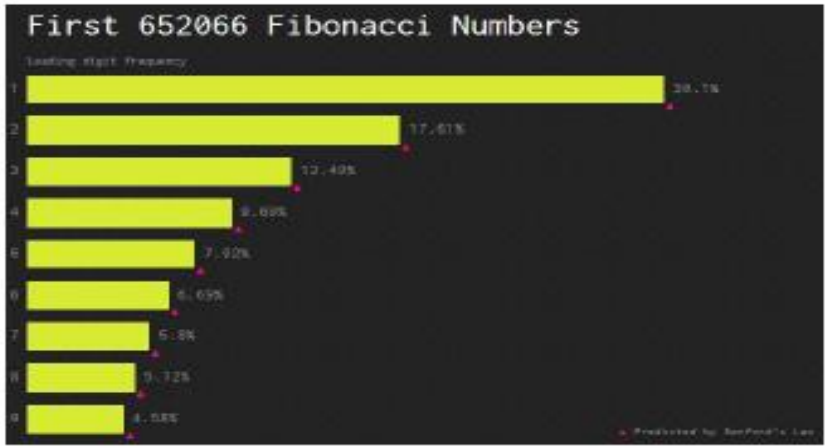
Motivating Question: For a nice data set, such as the Fibonacci numbers, stock prices, street addresses of college employees and students, ..., what percent of the leading digits are 1?



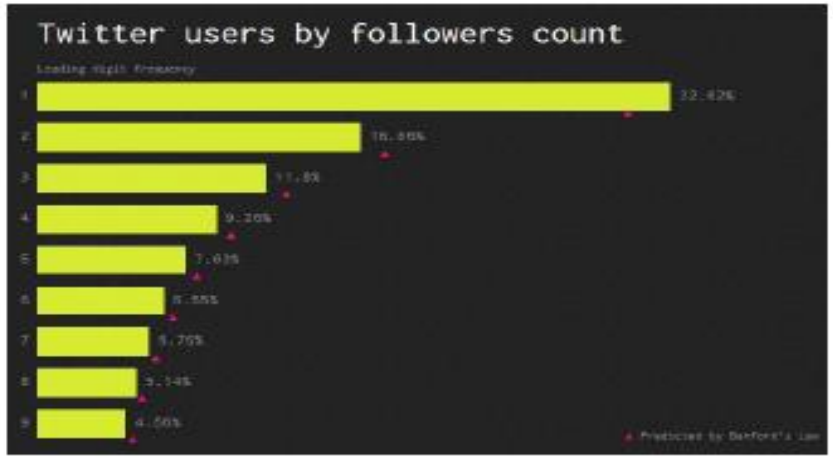
Answer: Benford's law!

Examples with First Digit Bias

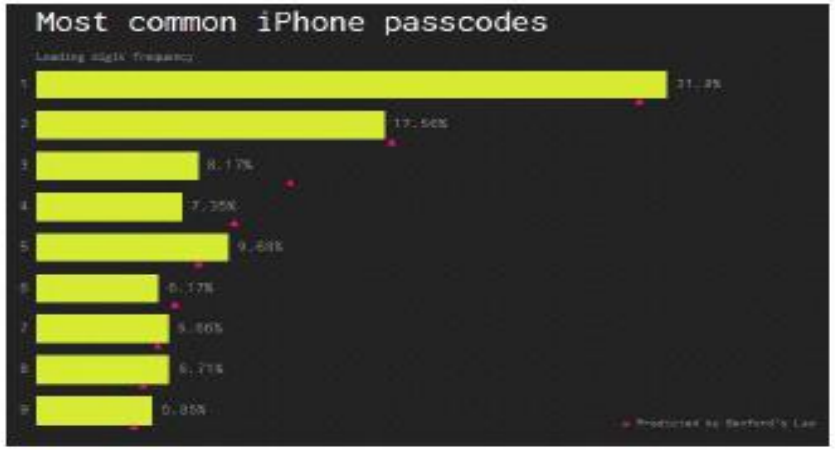
Fibonacci numbers



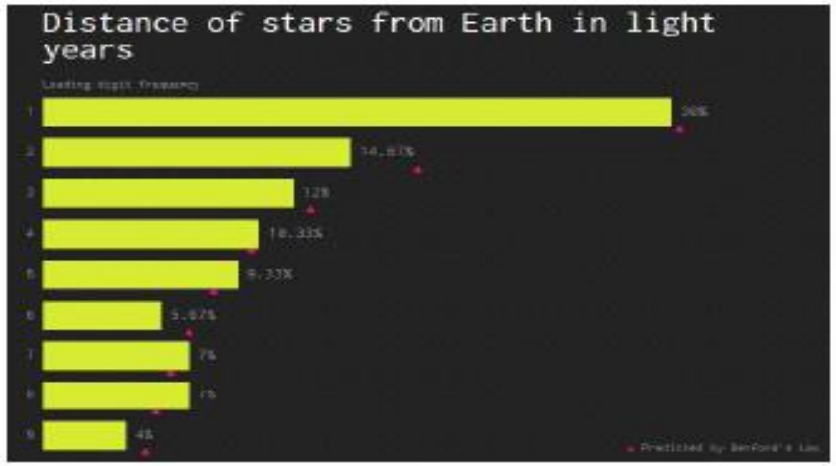
Twitter users by # followers



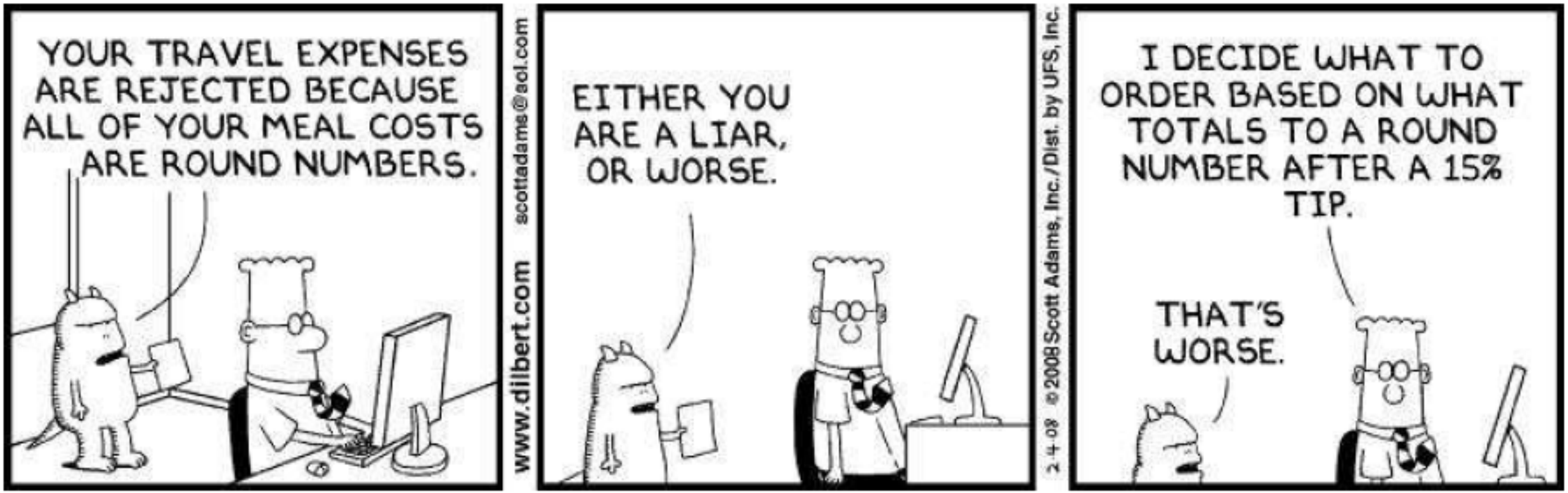
Most common iPhone passcodes



Distance of stars from Earth



- A math test indicating fraud is *not* proof of fraud: unlikely events, alternate reasons.



Applications

- Analyzing round-off errors.
- Determining the optimal way to store numbers.
- Detecting tax and image fraud, and data integrity.

Background Material

- Modulo: $a = b \mod c$ if $a - b$ is an integer times c; thus $17 = 5 \mod 12$, and $4.5 = .5 \mod 1$.
- Significand: $x = S_{10}(x) \cdot 10^k$, k integer, $1 \leq S_{10}(x) < 10$. Thus $2020.1701 = 2.0201701 \cdot 10^3$.
- $S_{10}(a) = S_{10}(b)$ if and only if a and b have the same leading digits. Note $\log_{10} a = \log_{10} S_{10}(b) + k$.
- Key observation: $\log_{10}(x) = \log_{10}(\widetilde{x}) \mod 1$ if and only if x and $\widetilde{x}$ have the same leading digits.

Thus often study $y = \log_{10} x \mod 1$.
Advanced: $e^{2\pi i u} = e^{2\pi i (u \mod 1)}$.

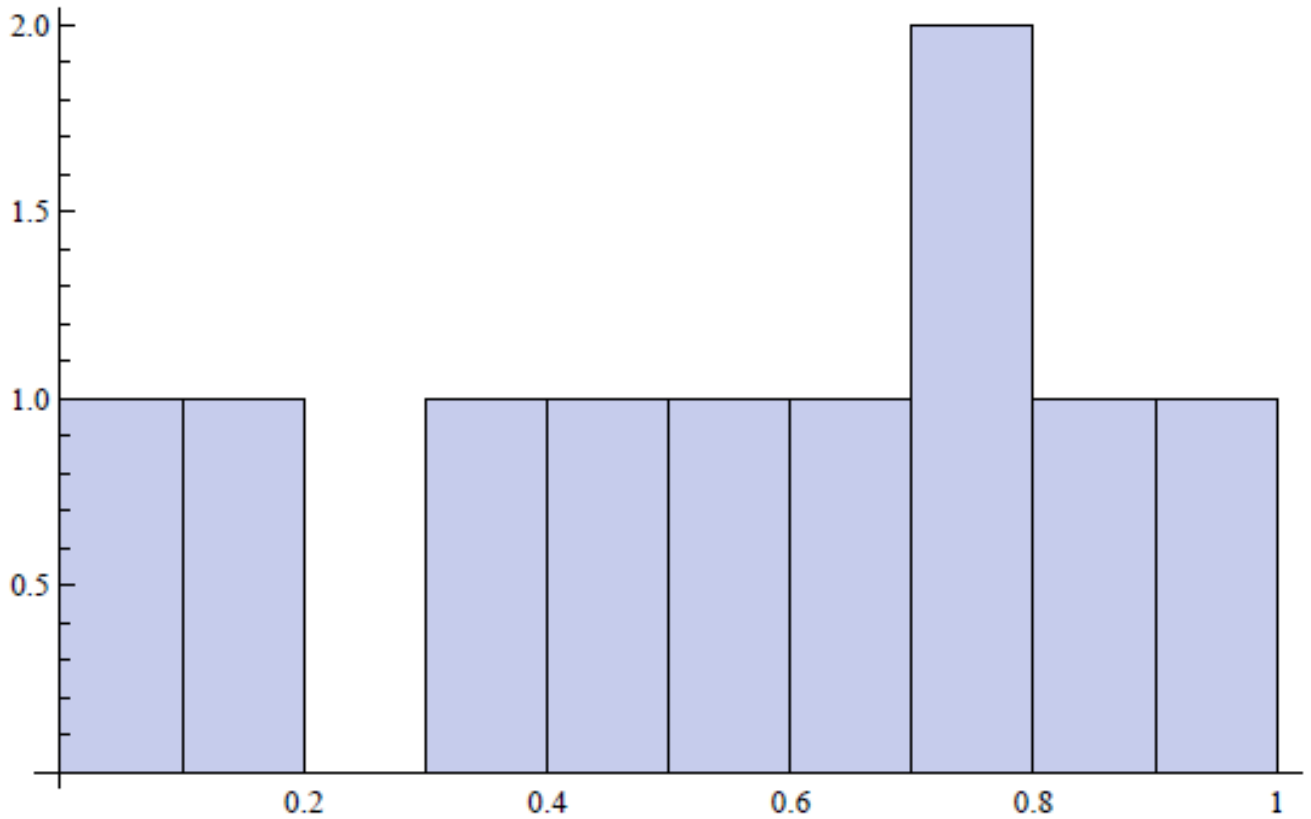
Equidistribution

$\{y_n\}_{n=1}^{\infty}$ is equidistributed modulo 1 if probability $y_n \bmod 1 \in [a, b]$ tends to $b - a$:

$$\frac{\#\{n \leq N : y_n \bmod 1 \in [a, b]\}}{N} \rightarrow b - a.$$

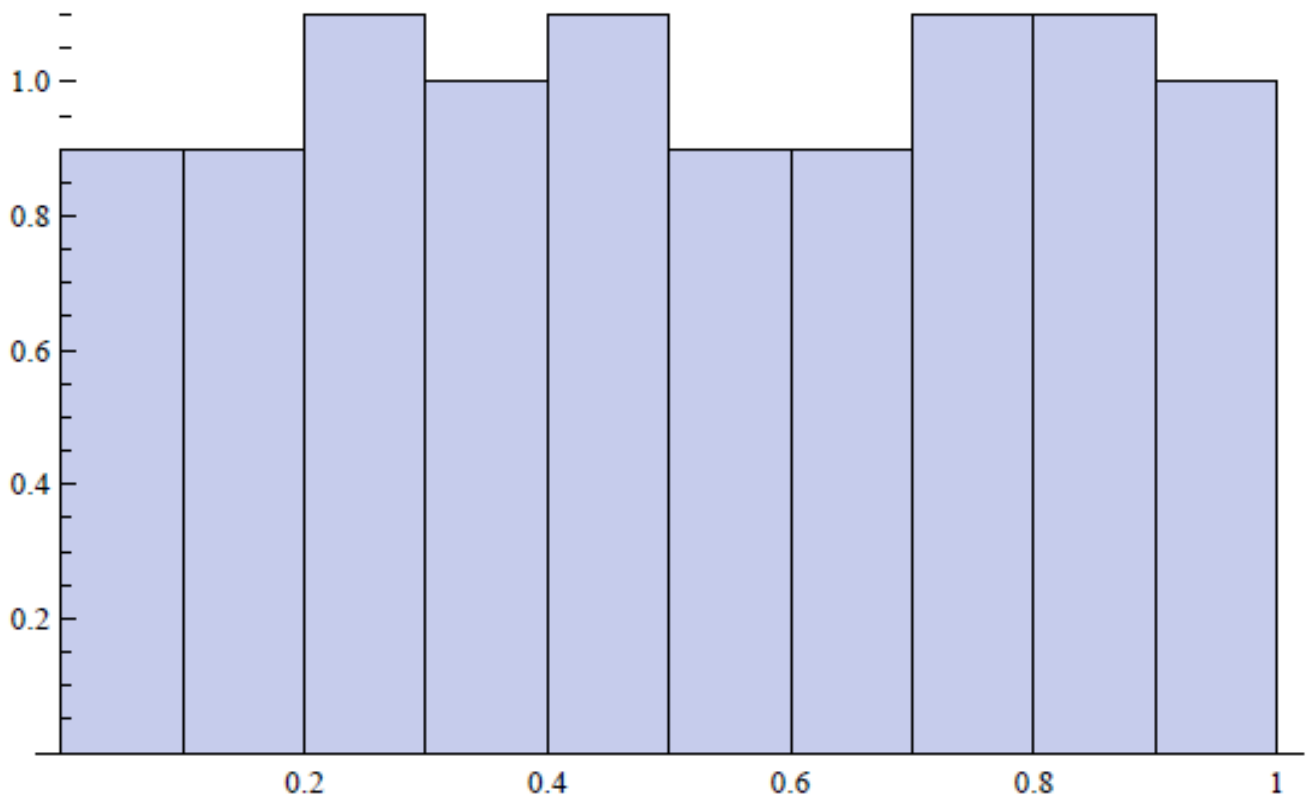
- Thm: $\beta \notin \mathbb{Q}$, $n\beta$ is equidistributed mod 1.
- Examples: $\log_{10} 2, \log_{10}\left(\frac{1+\sqrt{5}}{2}\right) \notin \mathbb{Q}$.

Example of Equidistribution: $n\sqrt{\pi}$ mod 1



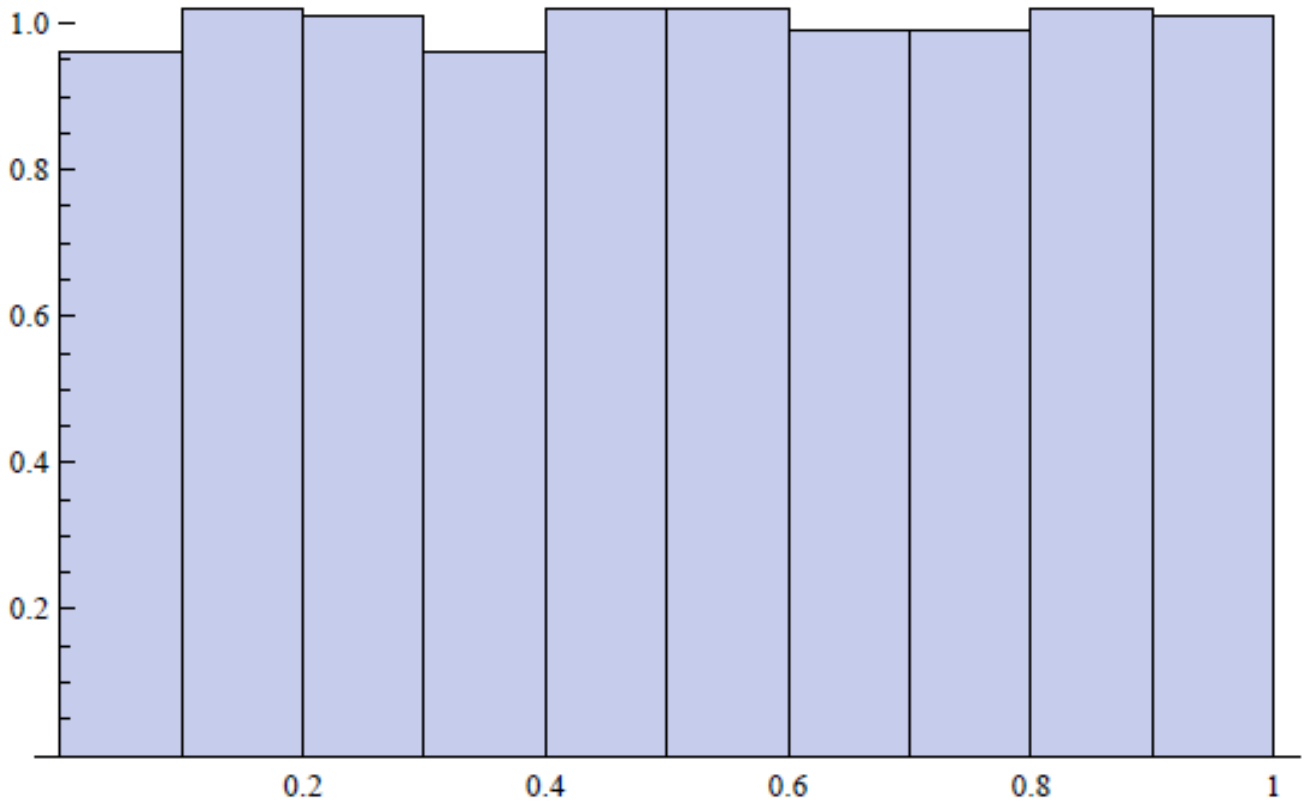
$n\sqrt{\pi}$ mod 1 for $n \leq 10$

Example of Equidistribution: $n\sqrt{\pi}$ mod 1



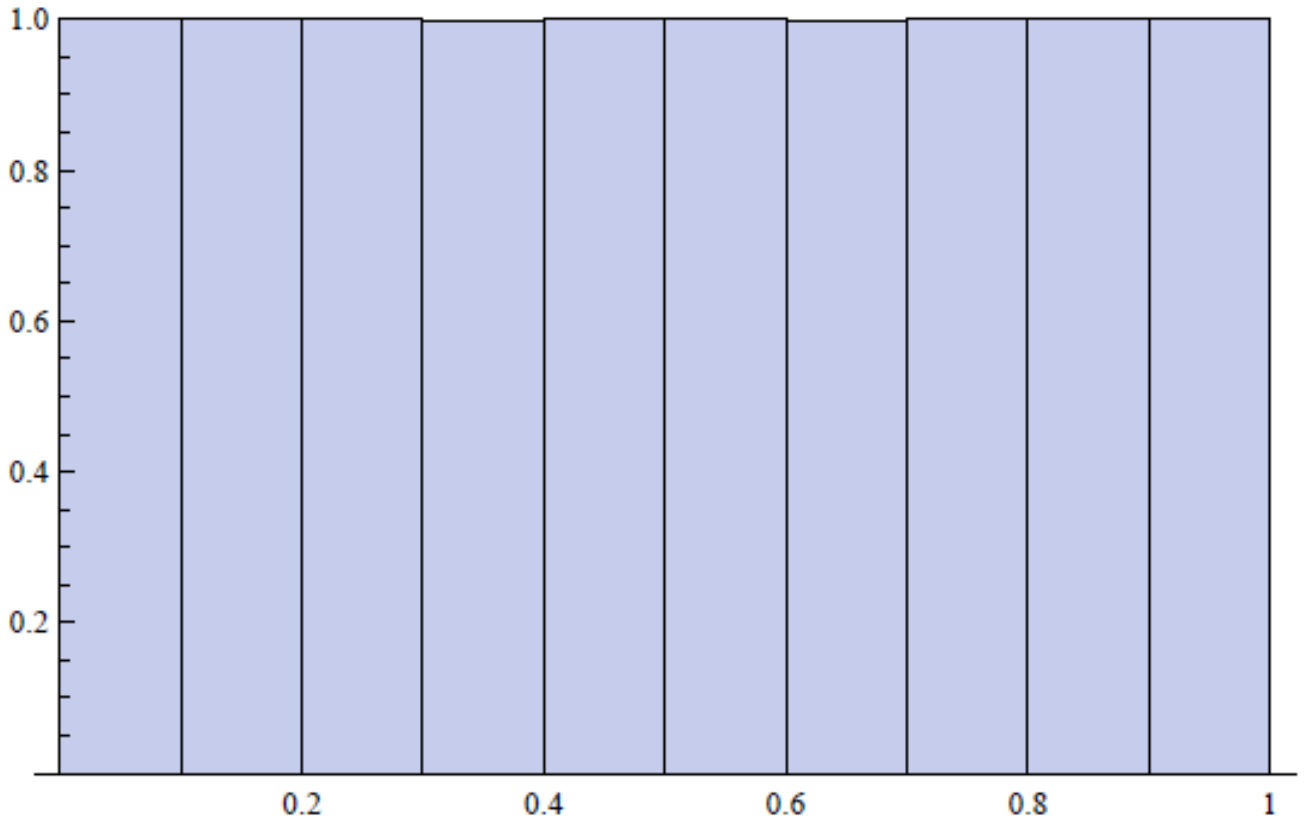
$n\sqrt{\pi}$ mod 1 for $n \leq 100$

Example of Equidistribution: $n\sqrt{\pi} \bmod 1$



$n\sqrt{\pi} \bmod 1$ for $n \leq 1000$

Example of Equidistribution: $n\sqrt{\pi} \bmod 1$



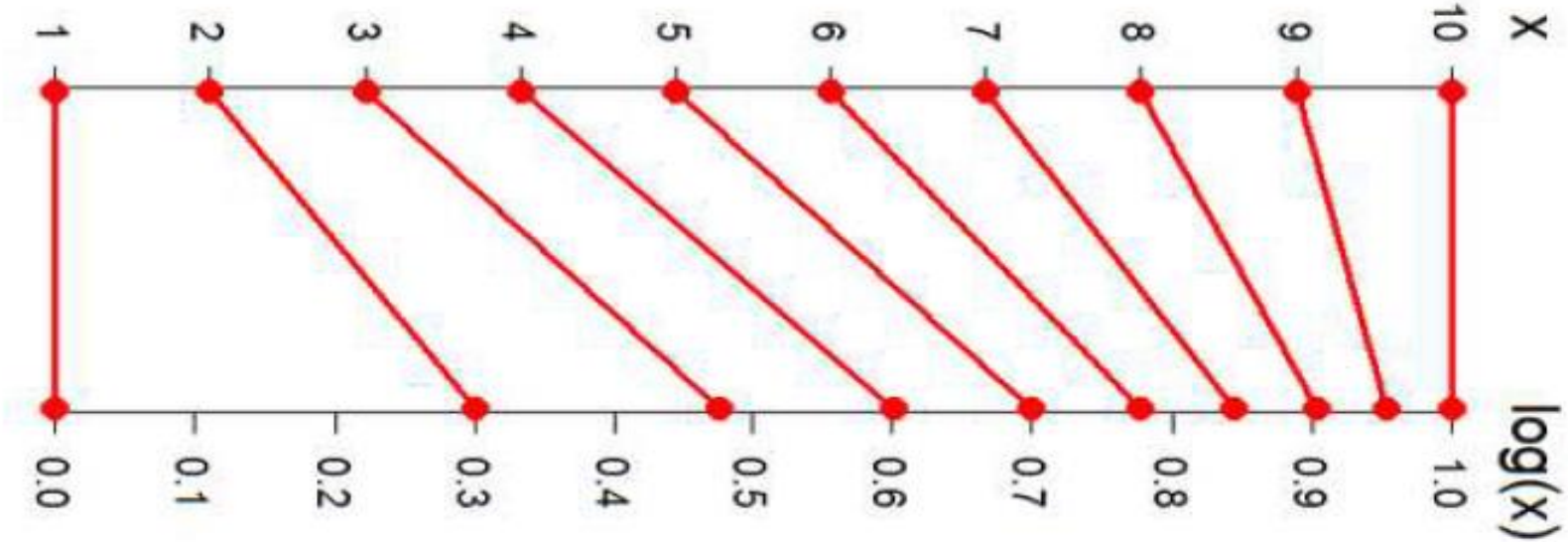
$n\sqrt{\pi} \bmod 1$ for $n \leq 10,000$

Fundamental Equivalence

Data set $\{x_i\}$ is Benford base B if $\{y_i\}$ is equidistributed mod 1, where $y_i = \log_B x_i$.

$$x = S_{10}(x) \cdot 10^k \text{ then}$$

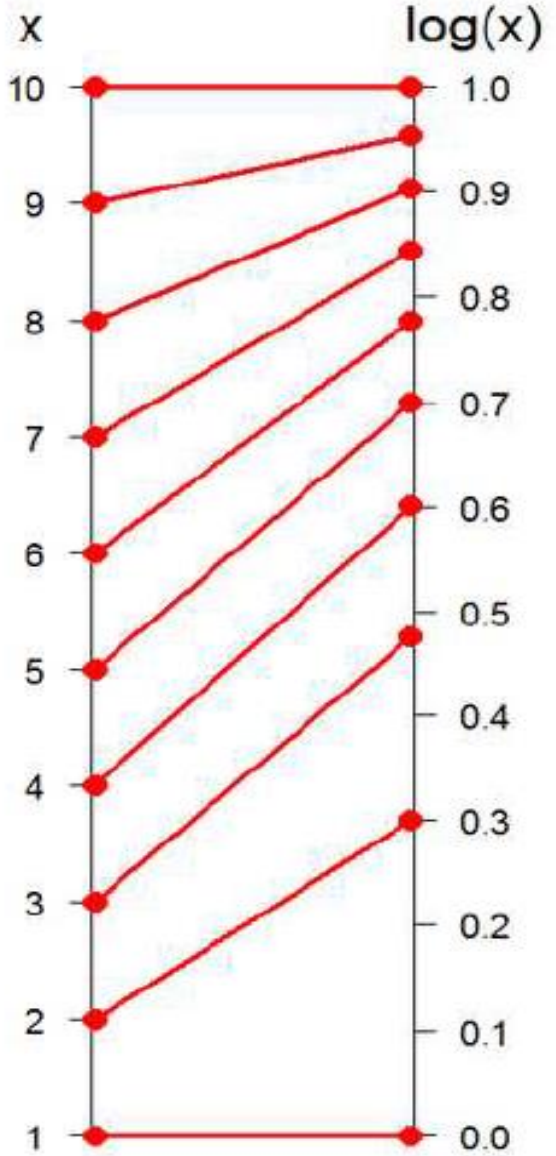
$$\log_{10} x = \log_{10} S_{10}(x) + k = \log_{10} S_{10}x \bmod 1.$$



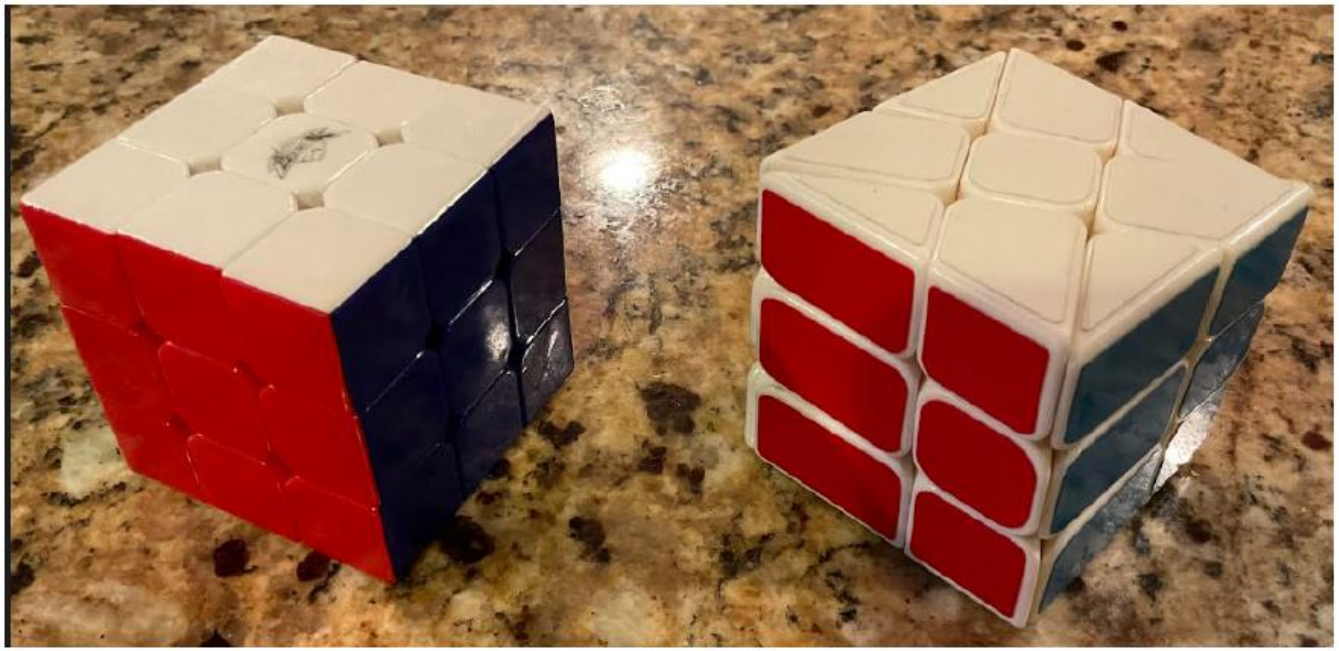
Logarithms and Benford's Law

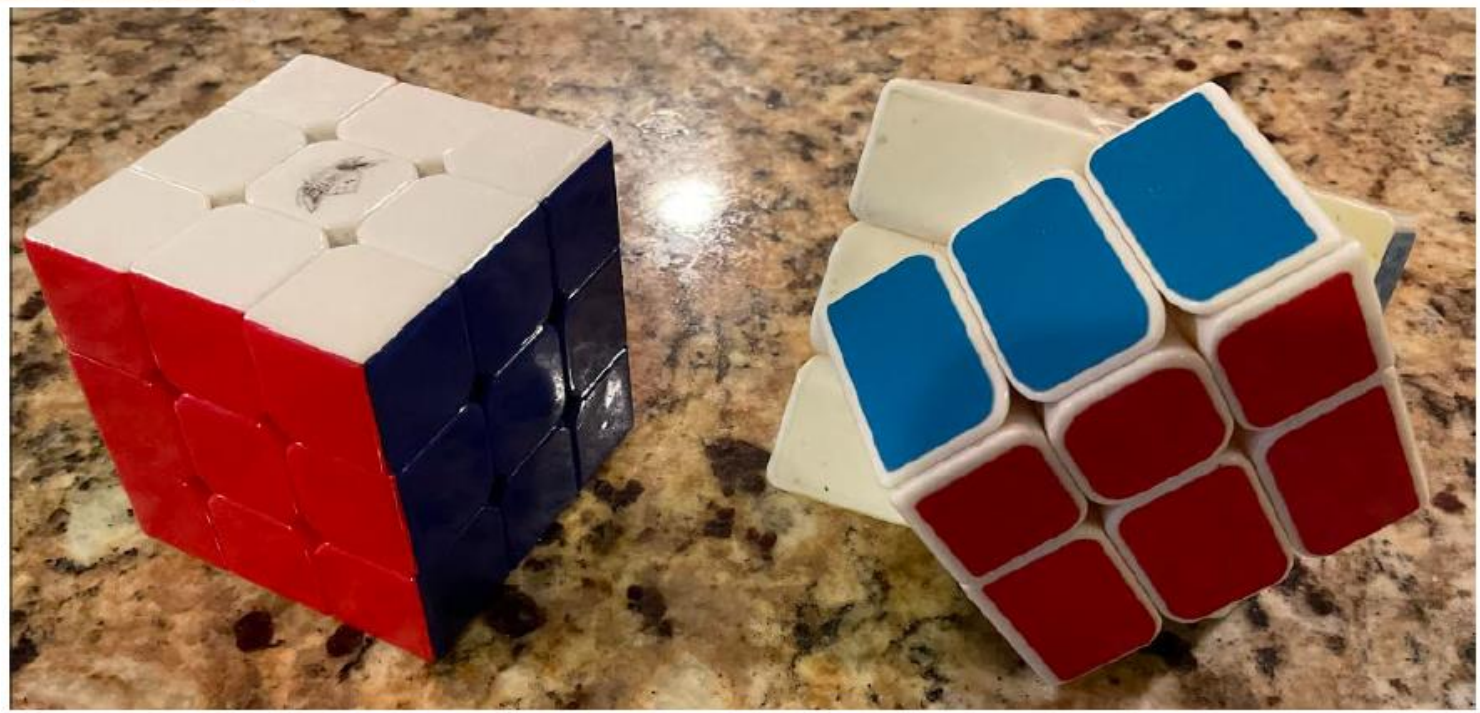
$$\begin{aligned}&\text{Prob}(\text{leading digit } d)\\ &= \log_{10}(d+1) - \log_{10}(d)\\ &= \log_{10}\left(\tfrac{d+1}{d}\right)\\ &= \log_{10}\left(1+\tfrac{1}{d}\right).\end{aligned}$$

Have Benford's law $\leftrightarrow$ mantissa of logarithms of data are uniformly distributed



The Power of the Right Perspective





- 2^n is Benford base 10 as $\log_{10} 2 \notin \mathbb{Q}$.
- Fibonacci numbers are Benford base 10.

  $F_{n+1} = F_n + F_{n-1}$.

  Guess $F_n = r^n$: $r^{n+1} = r^n + r^{n-1}$ or $r^2 = r + 1$.

  Roots $r = (1 \pm \sqrt{5})/2$.

  General solution: $F_n = c_1 r_1^n + c_2 r_2^n$.

  Binet: $F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$.

  $F_{n+1} \leq 2F_n$

  $\leq 0 \; F_n \leq 2^n$

  $F_{n+1} \geq \frac{1}{2} F_n$

  $F_n \approx \frac{1}{\sqrt{5}} \varphi^n$

  $\log_{10} F_n \approx n \log_{10} \varphi - \frac{1}{2} \log_{10} 5$
- Most linear recurrence relations Benford:
  - $a_{n+1} = 2a_n - a_{n-1}$
  - take $a_0 = a_1 = 1$ or $a_0 = 0$, $a_1 = 1$.

First 60 values of 2^n (only displaying 30)

			digit	#	Obs Prob	Benf Prob
1	1024	1048576	1	18	.300	.301
2	2048	2097152	2	12	.200	.176
4	4096	4194304	3	6	.100	.125
8	8192	8388608	4	6	.100	.097
16	16384	16777216	5	6	.100	.079
32	32768	33554432	6	4	.067	.067
64	65536	67108864	7	2	.033	.058
128	131072	134217728	8	5	.083	.051
256	262144	268435456	9	1	.017	.046
512	524288	536870912				

First 60 values of 2^n (only displaying 30)

			digit	#	Obs Prob	Benf Prob
1	1024	1048576	1	18	.300	.301
2	2048	2097152	2	12	.200	.176
4	4096	4194304	3	6	.100	.125
8	8192	8388608	4	6	.100	.097
16	16384	16777216	5	6	.100	.079
32	32768	33554432	6	4	.067	.067
64	65536	67108864	7	2	.033	.058
128	131072	134217728	8	5	.083	.051
256	262144	268435456	9	1	.017	.046
512	524288	536870912				

First 60 values of 2^n (only displaying 30): $2^{10} = 1024 \approx 10^3$.

			digit	#	Obs Prob	Benf Prob
1	1024	1048576	1	18	.300	.301
2	2048	2097152	2	12	.200	.176
4	4096	4194304	3	6	.100	.125
8	8192	8388608	4	6	.100	.097
16	16384	16777216	5	6	.100	.079
32	32768	33554432	6	4	.067	.067
64	65536	67108864	7	2	.033	.058
128	131072	134217728	8	5	.083	.051
256	262144	268435456	9	1	.017	.046
512	524288	536870912				

First 1000 values of 2^n (only displaying 30): $2^{10} = 1024 \approx 10^3$.

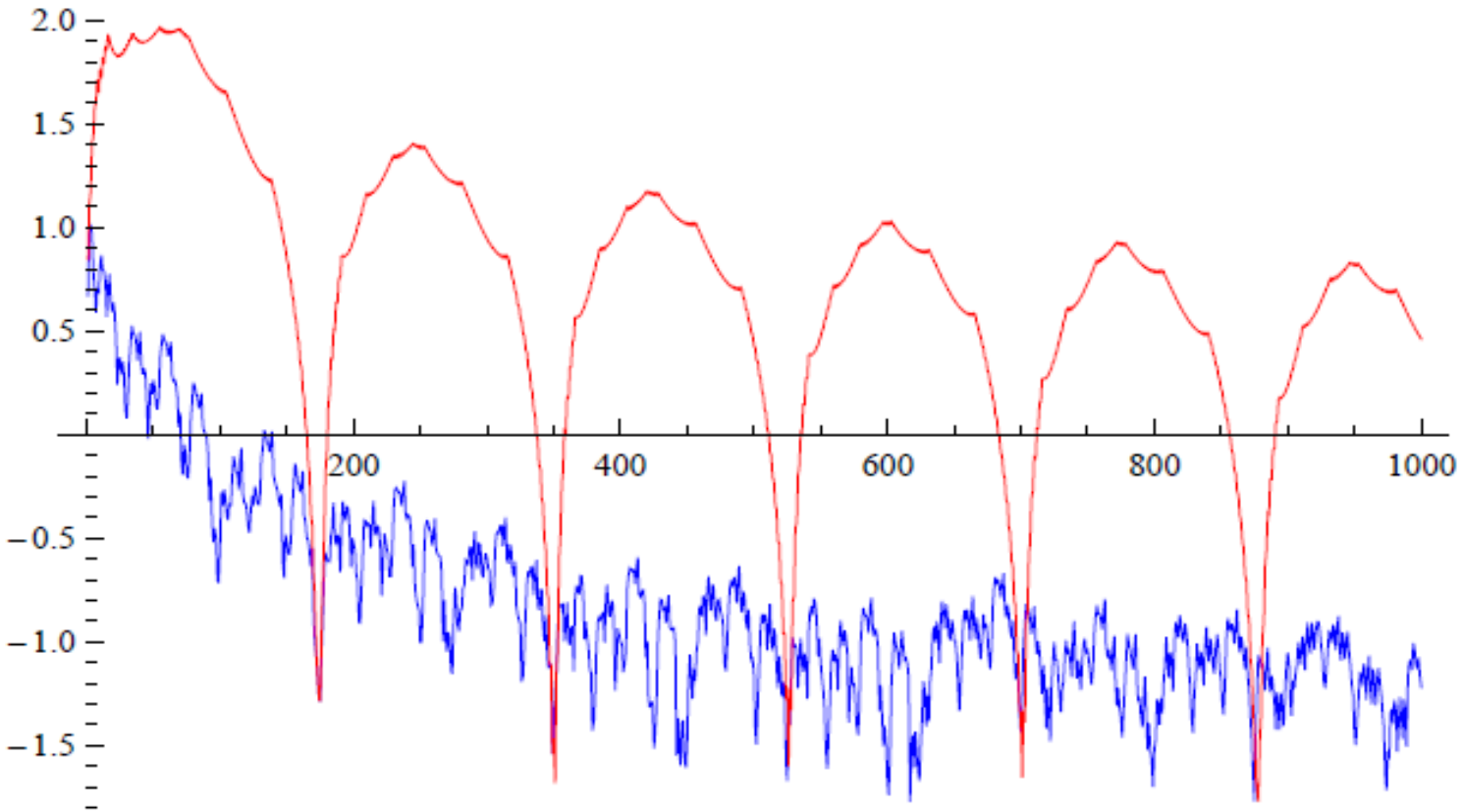
			digit	#	Obs Prob	Benf Prob
1	1024	1048576	1	301	0.301	.301
2	2048	2097152	2	176	0.176	.176
4	4096	4194304	3	125	0.125	.125
8	8192	8388608	4	97	0.097	.097
16	16384	16777216	5	79	0.079	.079
32	32768	33554432	6	69	0.069	.067
64	65536	67108864	7	56	0.056	.058
128	131072	134217728	8	52	0.052	.051
256	262144	268435456	9	45	0.045	.046
512	524288	536870912				

χ^2 values for α^n, $1 \leq n \leq N$ (5% 15.5).

N	$\chi^2(\gamma)$	$\chi^2(e)$	$\chi^2(\pi)$
100	0.72	0.30	46.65
200	0.24	0.30	8.58
400	0.14	0.10	10.55
500	0.08	0.07	2.69
700	0.19	0.04	0.05
800	0.04	0.03	6.19
900	0.09	0.09	1.71
1000	0.02	0.06	2.90

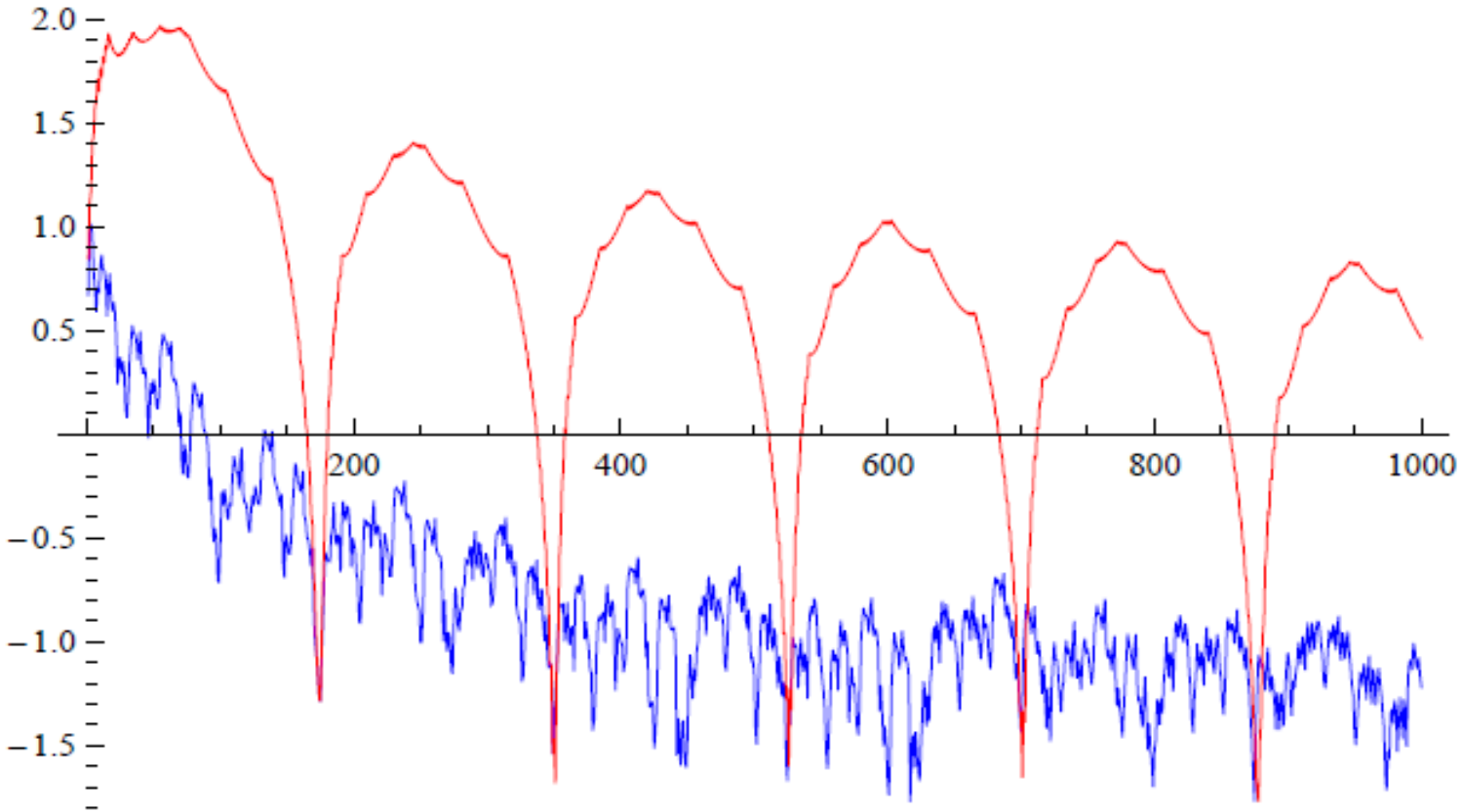
Logarithms and Benford's Law: Base 10 (5%: $\log(\chi^2) \approx 2.74$)

$\log(\chi^2)$ vs N for π^n (red) and e^n (blue), $n \in \{1, \ldots, N\}$.



Logarithms and Benford's Law: Base 10 (5%: $\log(\chi^2) \approx 2.74$)

$\log(\chi^2)$ vs N for π^n (red) and e^n (blue), $n \in \{1, \ldots, N\}$. Note $\pi^{175} \approx 1.0028 \cdot 10^{87}$.



The Hilbert Hotel: Every room is booked but we can always take more….

Rooms numbered 1, 2, 3, 4, ….

Guest arrives, wants a room, but all inuse!

Hotel: $1 \to 2$ room is free!

$2 \to 3$

$3 \to 4$

⋮

What if ∞ many guest arrive?

$1 \to 2$ $\quad 3 \to 6$ $\quad n \to 2n$

$2 \to 4$ $\quad 4 \to 8$ frees up $1, 3, 5, 7, \ldots$

A set is COUNTABLE if can be put in a 1-1 correspondence with the integers (or the non-negative integers)

$\{a_1, a_2, a_3, \ldots\}$ or $\{a_0, a_1, a_2, \ldots\}$

Integers: $\ldots, -2, -1, 0, 1, 2, \ldots$

Input $\mathbb{N}$		output $\mathbb{Z}$
0	$\longrightarrow$	0
1	$\longrightarrow$	-1
2	$\longrightarrow$	1
3	$\longrightarrow$	-2
$\vdots$	$\longrightarrow$	$\vdots$
n	$\longrightarrow$	$\frac{n}{2}$

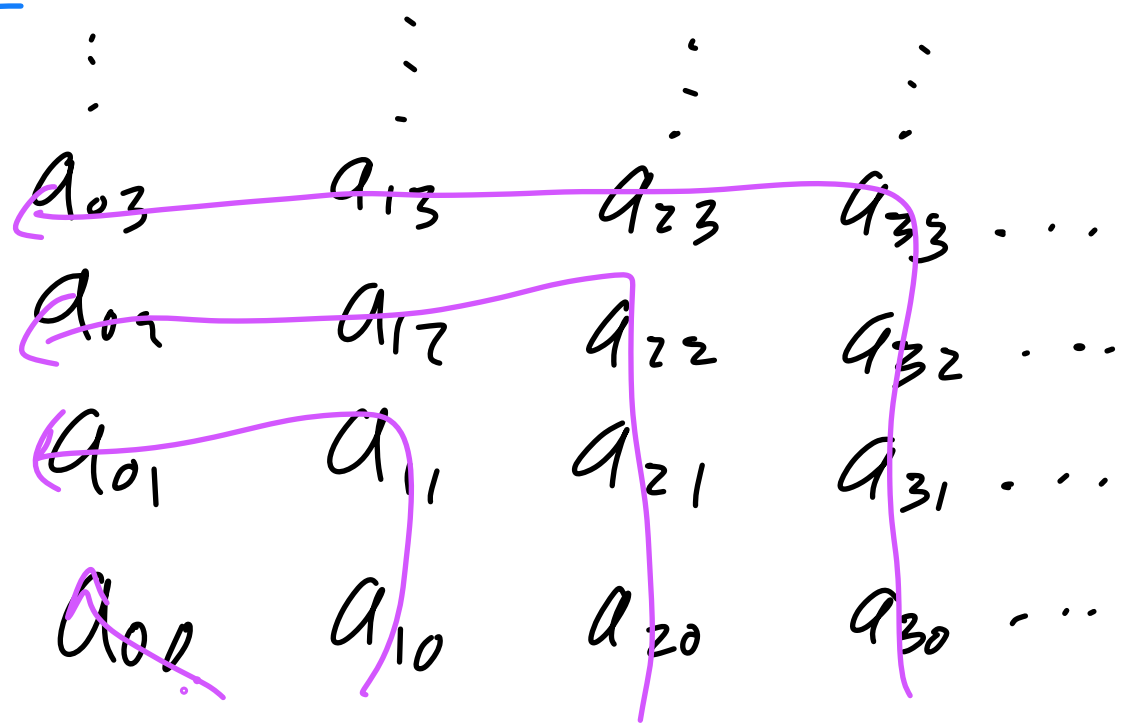
$f(2n) = n$

$f(2n-1) = -n$

The RATIONALS are countable (a countable union of countable sets is countable).

Countable union: $\bigcup_{n=0}^{\infty} A_n = A_1 \cup A_2 \cup \cdots$

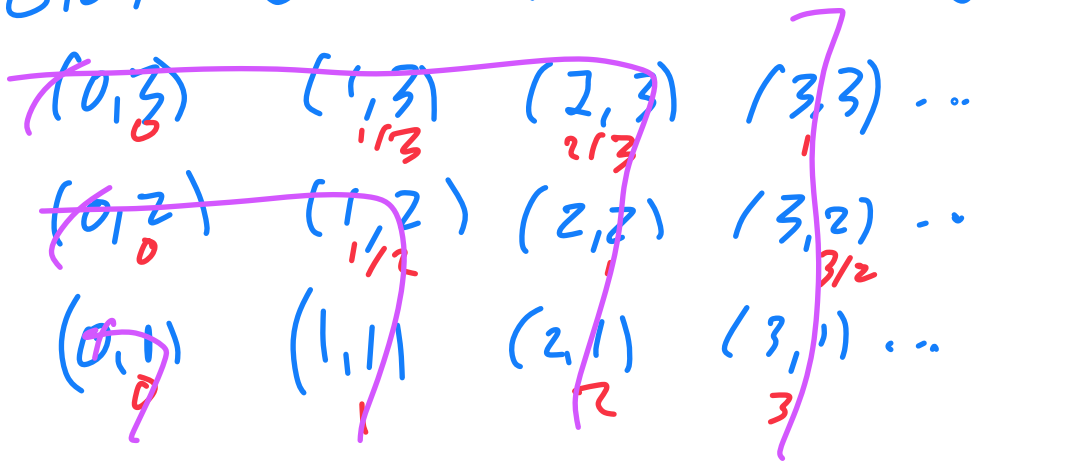
Proof



Rationals are Countable

Enough to do pos rationals:

Given $a/b \longleftrightarrow (a,b)$, and $b > 0$



just take number if new

$0, 1, 1/2, 2, 2/3, 1/3, 3, 3/2, \ldots$

The REALS are uncountable

Cantor's Diagonalization Argument

If countable: $\mathbb{R} = \{q_1, q_2, q_3, \ldots\}$

WLOG enough to show $\mathbb{R} \cap [0,1]$ is uncountable

Take decimal expansions (if two options take finite)

Ex: $.019999\,9\ldots = .02$

If countable:

$x_1 = .x_{11}\, x_{12}\, x_{13}\, x_{14}$

$x_2 = .x_{21}\, x_{22}\, x_{23}\, x_{24}$

$x_3 = .x_{31}\, x_{32}\, x_{33}\, x_{34}$

Construct x not on the list: choose k^{th} digit to be $9 - x_{kk}$

not on the list <u>but</u> maybe an equivalent representation is...

Almost every real number is transcendental....

Theorem: The set of algebraic numbers is countable.

α is algebraic if α is a root of $f(x)=0$ with f a deg n poly with integer coeff.

$A_n = \{\alpha \in \mathbb{R}$ st α is a root of a poly of deg n with integer coeff$\}$

poly deg n has $n+1$ coeff: $(a_0, a_1, \ldots, a_n) \in$ countable

countably many poly of deg n, each has n roots, so

each A_n is countable

Countable union of countable sets is countable ∎

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: https://youtu.be/ZEkSF2cMiug

Lecture 17: 4/11/24:

Chapter Eight: Approximating Irrationals by Rationals

Finding a good metric:

Truncate decimal expansion: $\frac{3}{1}, \frac{31}{10}, \frac{314}{100}, \frac{3141}{1000}, \ldots$

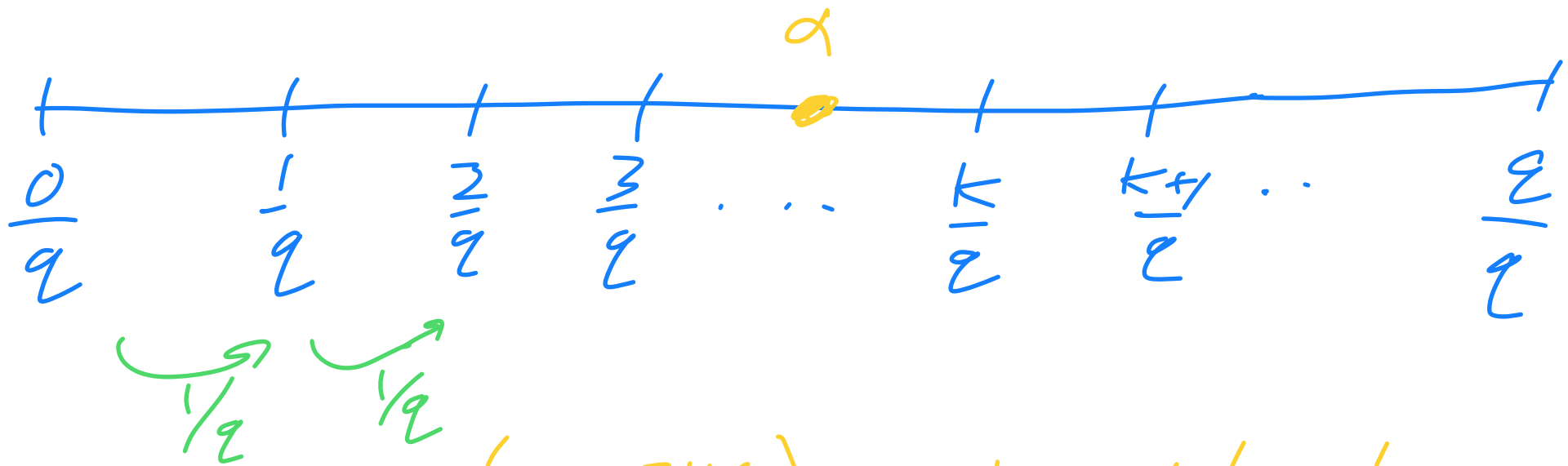
$|\pi - \text{approx}| \sim \frac{1}{\text{denom}}$

Better: $|\pi - p/q| \leq 1/q^{1.5}$ or $1/q^2$ or $1/q^3 \ldots$

Infinitely often $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q}$ if α irrational.

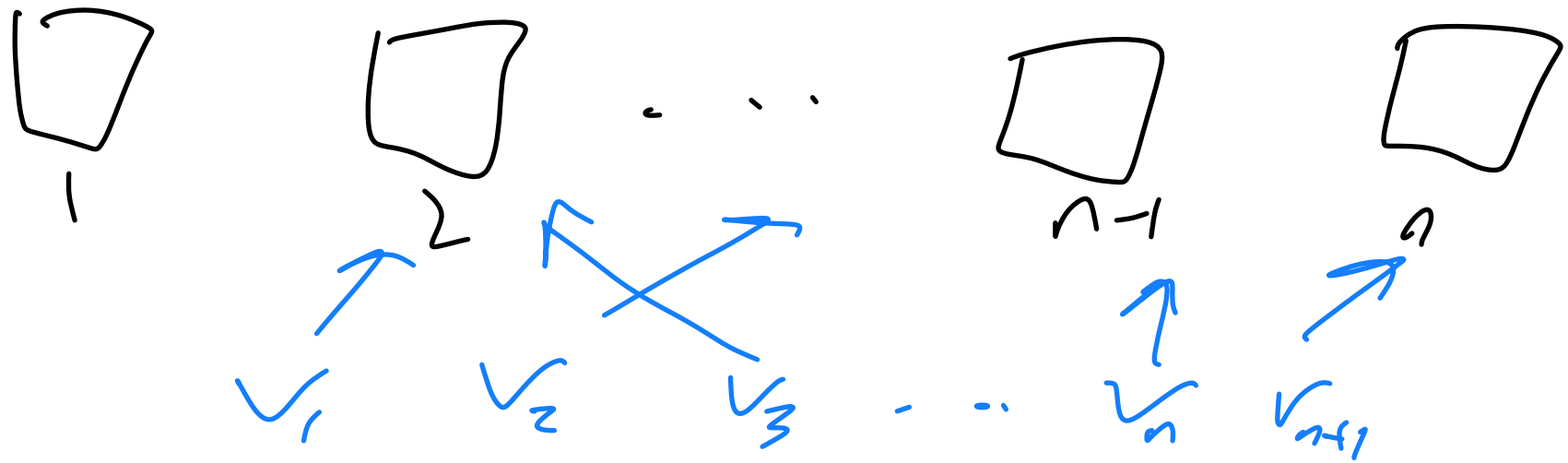
w/ log $\alpha \in [0,1]$

Proof



So α is in some subinterval $(p/q, p+1/q)$ so $|\alpha - p/q| < \frac{1}{q}$

Dirichlet Box/Pigeonhole Principle:
n+1 pigeons, n boxes: one box has at least two pigeons.



Proof: if not, each box has ≤ 1 pigeon, total # accounted for is at most $n \cdot 1 < n+1$

ave # pigeons / box is $\frac{n+1}{n} > 1$

Dirichlet Box/Pigeonhole Principle:

See Math 409: https://www.youtube.com/watch?v=g0pf8eqD2NE

Problem: Given $a_1, a_2, \ldots, a_n$ prove a subset has a sum divisible by n; what if only n-1 summands?

If $n-1$ summands: Consider $\underbrace{1, 1, 1, \ldots, 1}_{n-1 \text{ times}}$: sum is in $\{1, 2, 3, \ldots, n-1\}$

subsets of of n elements: $2 * 2 * \cdots * 2 = 2^n$, so $2^n - 1$ non-empty subsets

Consider $S_1 = a_1$

$S_2 = a_1 + a_2$

$S_3 = a_1 + a_2 + a_3 \ldots$ up to $S_n = a_1 + \cdots + a_n = S_{n-1} + a_n$

Assume no S_k is a multiple of n, Then all n remainders in $\{1, 3, \ldots, n-1\}$

Say S_k, S_j have same remainder, $k > j$

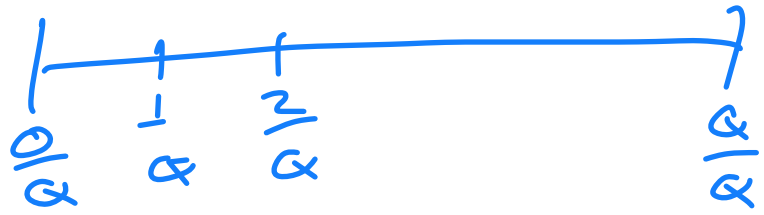
Then $a_{j+1} + \cdots + a_k$ has remainder zero as it is $S_k - S_j$

Infinitely often $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q2}$ if α irrational.

2

if $\alpha - p/q = \pm 1/q^2 \Rightarrow \alpha = p/q \pm 1/q^2 \in \mathbb{Q}$

Fix Q, look at $\alpha, 2\alpha, 3\alpha, \ldots, (Q+1)\alpha \mod 1$



By Pigeonhole, two in same subinterval of size $\frac{1}{Q}$

$$|(a_1\alpha - n_1) - (a_2\alpha - n_2)| < 1/Q \qquad 1 \leq a_1, a_2 \leq Q+1$$

$$|(a_1 - a_2)\alpha - (n_1 - n_2)| < 1/Q$$

$$\left|\alpha - \frac{n_1 - n_2}{a_1 - a_2}\right| < \frac{1}{(a_1 - a_2)Q}$$

try $p = n_1 - n_2$ $q = a_1 - a_2 \leq Q$ non-zero

$$|\alpha - p/q| < \frac{1}{qQ} \leq \frac{1}{q^2}$$

$\Rightarrow 1/Q \leq 1/2$

take a seq of $Q \to \infty$, nec constr same fractions if Q grows fast enough

An Invitation to Modern Number Theory: Steven J. Miller and Ramin Takloo-Bighash, Princeton University Press:

Theorem 7.9.5 (Hurwitz). *Let $x \in [0,1]$ be an irrational number. Then there are infinitely many relatively prime integers p, q such that*

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{q^2\sqrt{5}}. \tag{7.117}$$

Exercise 7.9.7. *Show that $\frac{1}{\sqrt{5}q^2}$ is the best one can have for all irrationals by studying the golden mean, $\frac{1+\sqrt{5}}{2} = [1,1,1,\ldots]$.*

Exercise 7.9.8. *Let x be any irrational other than the golden mean. How well can x be approximated? See for example [HW].*

G. H. Hardy and E. Wright, An Introduction to the Theory of Numbers, 5th edition, Oxford Science Publications, Clarendon Press, Oxford, 1995.

Theorem 5.7.1 (Roth's Theorem)**.** *Let α be a real algebraic number (a root of a polynomial equation with integer coefficients). Given any $\epsilon > 0$ there are only finitely many relatively prime pairs of integers (p, q) such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}. \tag{5.70}$$

Remark 5.7.2. We have seen for $\alpha \notin \mathbb{Q}$ that there are infinitely many pairs of relatively prime integers (p, q) such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{5.71}$$

Therefore any non-rational algebraic number has approximation exponent exactly 2.

Theorem 5.5.9. *Let C, ϵ be positive constants. Let S be the set of all points $x \in [0,1]$ such that there are infinitely many relatively prime integers p, q with*

$$\left| x - \frac{p}{q} \right| \leq \frac{C}{q^{2+\epsilon}}. \tag{5.42}$$

Then the length (or measure) of S, denoted $|S|$, equals 0.

Proof. Let $N > 0$. Let S_N be the set of all points $x \in [0,1]$ such that there are $p, q \in \mathbb{Z}$, $q > N$ for which

$$\left| x - \frac{p}{q} \right| \leq \frac{C}{q^{2+\epsilon}}. \tag{5.43}$$

If $x \in S$ then $x \in S_N$ for every N. Thus if we can show that the measure of the sets S_N becomes arbitrarily small as $N \to \infty$, then the measure of S must be zero. How large can S_N be? For a given q there are at most q choices for p. Given a pair (p,q), we investigate how many x's are within $\frac{C}{q^{2+\epsilon}}$ of $\frac{p}{q}$. Clearly the set of such points is the interval

$$I_{p,q} = \left(\frac{p}{q} - \frac{C}{q^{2+\epsilon}}, \ \frac{p}{q} + \frac{C}{q^{2+\epsilon}} \right). \tag{5.44}$$

Note that the length of $I_{p,q}$ is $\frac{2C}{q^{2+\epsilon}}$. Let I_q be the set of all x in $[0,1]$ that are within $\frac{C}{q^{2+\epsilon}}$ of a rational number with denominator q. Then

$$I_q \subset \bigcup_{p=0}^{q} I_{p,q} \tag{5.45}$$

and therefore

$$|I_q| \leq \sum_{p=0}^{q} |I_{p,q}| = (q+1) \cdot \frac{2C}{q^{2+\epsilon}} = \frac{q+1}{q} \frac{2C}{q^{1+\epsilon}} < \frac{4C}{q^{1+\epsilon}}. \tag{5.46}$$

Hence

$$|S_N| \leq \sum_{q>N} |I_q| = \sum_{q>N} \frac{4C}{q^{1+\epsilon}} < \frac{4C}{1+\epsilon} N^{-\epsilon}. \tag{5.47}$$

Thus, as N goes to infinity, $|S_N|$ goes to zero. As $S \subset S_N$, $|S| = 0$. □

Remark 5.5.10. It follows from Roth's Theorem (Theorem 5.7.1) that the set S consists entirely of transcendental numbers; however, in terms of length, it is a small set of transcendentals.

Example 5.7.5. *There are only finitely many integer solutions* $(x, y) \in \mathbb{Z}^2$ *to*

$$x^3 - 2y^3 = a. \tag{5.75}$$

In order to see this, we proceed as follows. Let $\rho = e^{2\pi i/3} = (-1)^{1/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. *Then*

$$x^3 - 2y^3 = (x - 2^{1/3}y)(x - \rho 2^{1/3}y)(x - \rho^2 2^{1/3}y), \tag{5.76}$$

and therefore

$$\begin{aligned} \left|\frac{a}{y^3}\right| &= \left|\frac{x}{y} - 2^{1/3}\right| \left|\frac{x}{y} - \rho 2^{1/3}\right| \left|\frac{x}{y} - \rho^2 2^{1/3}\right| \\ &\geq \left|\frac{x}{y} - 2^{1/3}\right| \left|\Im(\rho 2^{1/3})\right| \left|\Im(\rho^2 2^{1/3})\right| \\ &= \frac{3}{2^{4/3}} \left|\frac{x}{y} - 2^{1/3}\right|. \end{aligned} \tag{5.77}$$

Hence every integer solution (x, y) *to* $x^3 - 2y^3 = a$ *is a solution to*

$$\left|2^{1/3} - \frac{x}{y}\right| \leq \frac{3 \cdot 2^{-4/3}}{|y|^3}. \tag{5.78}$$

By Roth's Theorem there are only finitely many such solutions.

Note Liouville's Theorem is not *strong enough to allow us to conclude there are only finitely many integer solutions. As* $2^{1/3}$ *is an algebraic number of degree* 3, *Liouville's Theorem says* $2^{1/3}$ *can be approximated by rationals to order at most* 3. *Thus the possibility that* $2^{1/3}$ can *be approximated by rationals to order* 3 *is* not *ruled out by Liouville's Theorem.*

Theorem 5.6.1 (Liouville's Theorem). *Let α be a real algebraic number of degree d. Then α is approximated by rationals to order at most d.*

What d should we try first?

If $d=1$: α is a real alg number of deg 1: $f(x)=ax+b$, $a\neq 0$, $f(\alpha)=0$

$\longrightarrow \alpha$ solves $f(x)=0$ so $a\alpha+b=0 \Rightarrow \alpha=-b/a \in \mathbb{Q}$

$$|\alpha - p/q| = \left|-\frac{b}{a}-\frac{p}{q}\right| = \left|\frac{-bq-ap}{aq}\right|$$

p,q relatively prime, $p/q \neq -b/a$ so $|\text{numerator}| \geq 1$

$$|\alpha - p/q| \geq \frac{1}{aq} = \frac{1}{a}\cdot\frac{1}{q}$$

8.3.2. Separability, or How To Tell If $f(x)$ Has Repeated Roots.

Definition 8.21. Let F be a field, and let $f(x) \in F[x]$ be a non-zero polynomial. Theorem 8.17 tells us that there is an extension field in which $f(x)$ factors as

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_d). \tag{8.13}$$

Then f is said to be *separable* if the roots $\alpha_1, \ldots, \alpha_d$ are distinct. This terminology comes from the idea that in a separable polynomial, the roots are separated from one another. Conversely, if f has one or more repeated roots, then it is *inseparable*.

Proposition 8.24. *Let F be a field, and let $f(x) \in F[x]$ be a non-constant polynomial. Then*[3]

$$f \text{ is separable} \iff \gcd\bigl(f(x), f'(x)\bigr) = 1.$$

$(x^n)' = nx^{n-1}$

A.2.1 Intermediate Value Theorem

Theorem A.2.1 (Intermediate Value Theorem (IVT)). *Let f be a continuous function on $[a, b]$. For all C between $f(a)$ and $f(b)$ there exists a $c \in [a, b]$ such that $f(c) = C$. In other words, all intermediate values of a continuous function are obtained.*

Sketch of the proof. We proceed by **Divide and Conquer**. Without loss of generality, assume $f(a) < C < f(b)$. Let x_1 be the midpoint of $[a, b]$. If $f(x_1) = C$ we are done. If $f(x_1) < C$, we look at the interval $[x_1, b]$. If $f(x_1) > C$ we look at the interval $[a, x_1]$.

In either case, we have a new interval, call it $[a_1, b_1]$, such that $f(a_1) < C < f(b_1)$ and the interval has half the size of $[a, b]$. We continue in this manner, repeatedly taking the midpoint and looking at the appropriate half-interval.

If any of the midpoints satisfy $f(x_n) = C$, we are done. If no midpoint works, we divide infinitely often and obtain a sequence of points x_n in intervals $[a_n, b_n]$. This is where rigorous mathematical analysis is required (see §A.3 for a brief review, and [Rud] for complete details) to show x_n converges to an $x \in (a, b)$.

For each n we have $f(a_n) < C < f(b_n)$, and $\lim_{n\to\infty} |b_n - a_n| = 0$. As f is continuous, this implies $\lim_{n\to\infty} f(a_n) = \lim_{n\to\infty} f(b_n) = f(x) = C$. □

A.2.2 Mean Value Theorem

Theorem A.2.2 (Mean Value Theorem (MVT)). *Let $f(x)$ be differentiable on $[a, b]$. Then there exists a $c \in (a, b)$ such that*

$$f(b) - f(a) = f'(c) \cdot (b - a). \tag{A.14}$$

We give an interpretation of the Mean Value Theorem. Let $f(x)$ represent the distance from the starting point at time x. The average speed from a to b is the distance traveled, $f(b) - f(a)$, divided by the elapsed time, $b - a$. As $f'(x)$ represents the speed at time x, the Mean Value Theorem says that there is some intermediate time at which we are traveling at the average speed.

To prove the Mean Value Theorem, it suffices to consider the special case when $f(a) = f(b) = 0$; this case is known as Rolle's Theorem:

Theorem A.2.3 (Rolle's Theorem). *Let f be differentiable on $[a, b]$, and assume $f(a) = f(b) = 0$. Then there exists a $c \in (a, b)$ such that $f'(c) = 0$.*

Proof of Mean Value Theorem:

If always are speed: all times work

If not, at some time less than are
at some time greater than are

USE IVT

$$\frac{f(x)-f(a)}{x-a} = f'(c) \Rightarrow f(x) = f(a) + f'(c)(x-a)$$

Tangent Line $y = f(a) + f'(a)(x-a)$

Theorem 5.6.1 (Liouville's Theorem). *Let α be a real algebraic number of degree d. Then α is approximated by rationals to order at most d.*

$f(x) = a_d x^d + \cdots + a_1 x + a_0$, $f(\alpha) = 0$, assume α is a root of multiplicity one, so $f'(\alpha) \neq 0$ (double root: $f(x) = c(x-\alpha)^2 g(x)$, then $f'(\alpha) = 0$)

Assume $f(\alpha) = 0$, let p/q be an approximation to α

$$|f(\alpha) - f(p/q)| = |f(p/q)| = \left| a_d \left(\frac{p}{q}\right)^d + a_{d-1}\left(\frac{p}{q}\right)^{d-1} + \cdots + a_1 \frac{p}{q} + a_0 \right|$$

$$= \left| \frac{a_d p^d + a_{d-1} p^{d-1} q + \cdots + a_1 p q^{d-1} + a_0 q^d}{q^d} \right| \quad \frac{\text{integer}}{\text{integer}}$$

If numerator is 0 then $f(p/q) = 0$ so $qx - p$ divides polynomial after clearing denominators get smaller deg f working for α.

So $|f(\alpha) - f(p/q)| \geq 1/q^d$.

$$\frac{1}{q^d} \le |f(\alpha) - f(p/q)| = |f'(c)|\,|\alpha - p/q| \quad \text{by MVT}$$

since $f'(\alpha) \neq 0$, have $f'(x) \neq 0$ for x close to α

say $C_1 \le |f'(c)| \le C_2$

so $$|\alpha - p/q| \ge \frac{1}{C_2}\,\frac{1}{q^d}$$

if had ∞ many p/q s.t. $|\alpha - p/q| \le 1/q^{d+\varepsilon} = \frac{1}{q^\varepsilon}\frac{1}{q^d}$



Theorem 5.6.4 (Liouville). *The number*

$$\alpha = \sum_{m=1}^{\infty} \frac{1}{10^{m!}} \tag{5.56}$$

is transcendental.

If not transcendental it is algebraic, say of deg d.

$p_n/q_n = \sum_{m=1}^{n} 1/10^{m!}$ so $\left|\alpha - \frac{p_n}{q_n}\right| = \sum_{m=n+1}^{\infty} \frac{1}{10^{m!}}$

Sum $\sum_{m=n+1}^{\infty} \frac{1}{10^{m!}} \sim \frac{2}{10^{(n+1)!}}$ rest is $\sum_{m=n+2}^{\infty} \frac{1}{10^{m!}} \le \sum_{l=(n+2)!}^{\infty} \frac{1}{10^l}$ use geom series

$q_n \le 10^{n!}$

$\left|\alpha - p_n/q_n\right| \le \frac{2}{10^{(n+1)!}} = 2\left(\frac{1}{10^{n!}}\right)^n = 2\frac{1}{q_n^n}$ true once $n > d$

$\Rightarrow$ transcendental ☒

Exercise 5.6.5. *Consider the binary expansion for $x \in [0,1)$, namely*

$$x = \sum_{n=1}^{\infty} \frac{b_n(x)}{2^n}, \quad b_n(x) \in \{0,1\}. \tag{5.59}$$

For irrational x this expansion is unique. Consider the function

$$M(x) = \sum_{n=1}^{\infty} 10^{-(b_n(x)+1)n!}. \tag{5.60}$$

Prove for irrational x that $M(x)$ is transcendental. Thus the above is an explicit construction for uncountably many transcendentals! Investigate the properties of this function. Is it continuous or differentiable (everywhere or at some points)? What is the measure of these numbers? These are "special" transcendental numbers (compare these numbers to Theorem 5.5.9). See also Remark 8.3.3.

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: https://youtu.be/xyLP6ViJyPM

Lecture 18: 4/16/24:

Chapter Eight: Fields and Roots

Definition 8.1. Let L/F be an extension of fields, and let $\alpha \in L$. We say that α is *algebraic over* F if α is the root of a non-zero polynomial in $F[x]$. Otherwise we say that α is *transcendental over* F.

$$\{ p(x) : p(x) = a_n x^n + \cdots + a_0 : a_k \in F \}$$

$$\sqrt{\sqrt{2}+1} + \sqrt[3]{5} \approx 3.26374992070673\ldots$$

is a root of the polynomial

$$x^{12} - 6x^{10} - 20x^9 + 9x^8 + 154x^6 - 360x^5 + 441x^4 - 180x^3 - 456x^2 - 1680x + 274.$$

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \}$$

$$\mathbb{Q}(\sqrt{2}) \subset (\mathbb{Q}(\sqrt{2}))(\sqrt[3]{5}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5})$$

$$\subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{5}, \sqrt{\sqrt{2}+1})$$

Definition 8.4. Let L/F be an extension of fields, and let $\alpha \in L$. We define $F[\alpha]$ to be the subring of L given by

$$F[\alpha] = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n : n \geq 0 \text{ and } a_0, \ldots, a_n \in F\}.$$

Ex: $F = \mathbb{Q}$ $\quad \alpha \notin \mathbb{Q}$ but $\alpha^2 \in \mathbb{Q}$: take $\alpha = i = \sqrt{-1}$

$$a_0 + a_1 i + a_2(-1) + a_3(-i) + a_4 + a_5 i + \cdots$$

$$= (a_0 - a_2 + a_4 - a_6 + \cdots) + i(a_1 - a_3 + a_5 - a_7 + \cdots)$$

$$= \underbrace{\qquad\qquad}_{b_0 + b_1 i}$$

$2 + 3i = 2 + 3i$ or $2 + 3(i)^5$

Intuition: From Proposition 5.15 and Definition 8.4, we have the following:

$$F(\alpha) = \text{smallest subfield of } L \text{ containing both } F \text{ and } \alpha.$$
$$F[\alpha] = \text{smallest subring of } L \text{ containing both } F \text{ and } \alpha.$$

In general, one expects that $F[\alpha]$ might be smaller than $F(\alpha)$, since the latter contains multiplicative inverses. For example, $F(\alpha)$ contains α^{-1}, but there's no reason to expect $F[\alpha]$ to contain α^{-1}. The next result tells us exactly when $F[\alpha]$ and $F(\alpha)$ are equal.

Theorem 8.5. *Let L/F be an extension of fields, and let $\alpha \in L$. Then*

$$F[\alpha] = F(\alpha) \iff \alpha \text{ is algebraic over } F.$$

$f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$, f "minimal poly"

$\alpha(a_n\alpha^{n-1} + \cdots + a_1) = -a_0$ so $\alpha\left(\underbrace{-\frac{a_1}{a_0}\alpha^{n-1} - \cdots - \frac{a_1}{a_0}}_{\alpha^{-1}}\right) = 1$ as $a_0 \neq 0$

Theorem 8.8. *Let R be a commutative ring, and let $f(x) \in R[x]$ be a non-zero polynomial.*

(a) *Suppose that $\alpha \in R$ is a root of $f(x)$; i.e., suppose that $f(\alpha) = 0$. Then there is a polynomial $g(x) \in R[x]$ such that $f(x)$ factors as*

$$f(x) = (x - \alpha)g(x).$$

(b) *Suppose that R is an integral domain. If $\alpha_1, \ldots, \alpha_n \in R$ are distinct roots of $f(x)$, then there is a polynomial $g(x) \in R[x]$ such that $f(x)$ factors as*

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)g(x). \tag{8.6}$$

(c) *Continuing with the assumption that R is an integral domain, a non-zero polynomial $f(x) \in R[x]$ of degree d has as most d distinct roots in R.*

(a) $f(x) = a_n x^n + \cdots + a_0 \quad f(\alpha) = a_n \alpha^n + \cdots + a_0 = 0$

$f(x) - f(\alpha) = f(x) = a_n(x^n - \alpha^n) + \cdots + a_1(x - \alpha) = (x-\alpha)(\text{poly in } x, \alpha \text{ of deg } n-1)$

$(x-\alpha)(x^{n-1} + x^{n-2}\alpha + \cdots + x\alpha^{n-2} + \alpha^{n-1})$

Warning: in $(\mathbb{Z}/12\mathbb{Z})^*$ have $x^2 - 1$ has 4 roots: 1, 5, 7, 11

Definition 8.13. Let F be a field, let L/F be an extension field, and let $f(x) \in F[x]$ be a non-zero polynomial. We say that f *splits completely in* L if $f(x)$ factors as

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_d) \tag{8.12}$$

for some $c \in F^*$ and $\alpha_1, \ldots, \alpha_d \in L$. Note that $\alpha_1, \ldots, \alpha_d$ need not be distinct. We say that L is a *splitting field for* $f(x)$ *over* F if f splits completely in L but does not split completely in any proper subfield of L that contains F.

$f(x) = x^2 - 2$ splits in $\mathbb{Q}(\sqrt{2})$ and in $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ and in $\mathbb{R}$, ...

poly with integer coeff must roots be integers? $2x-3=0 \to x = 3/2 \notin \mathbb{Z}$

" " $\mathbb{Q}$ " " " " " $\mathbb{Q}$? $x^2-2=0 \to x = \pm\sqrt{2} \notin \mathbb{Q}$

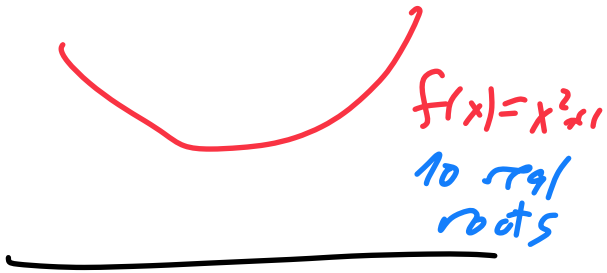
" " $\mathbb{R}$ " " " " " $\mathbb{R}$? $x^2+1=0 \to x = \pm i \notin \mathbb{R}$

" " $\mathbb{C}$ " " " " " $\mathbb{C}$? Yes!

$a_n x^n + \cdots + a_0$, all $x_i \in \mathbb{C}$, has n roots in $\mathbb{C}$

Fundamental Theorems of Mathematics (from https://math.chapman.edu/~jipsen/mathposters/fundamentals.pdf)

Fundamental Theorem of Arithmetic: Every positive integer has a prime factorisation, unique up to the order of the factors



Fundamental Theorem of Algebra: Every nonconstant polynomial over the field of complex numbers has at least one root

Fundamental Theorem of Calculus: For every continuous function f on an interval $[a, b]$ the function $g(x) = \int_a^x f(t)\,dt$ is an antiderivative of f on (a, b)

Area under the curve

Fundamental Theorem of Linear Algebra: The row space of a matrix is orthogonal to the nullspace of the matrix, and the dimensions add up to the number of columns of the matrix

https://kconrad.math.uconn.edu/blurbs/fundthmalg/fundthmalgcalculus.pdf
https://en.wikipedia.org/wiki/List_of_theorems_called_fundamental

Theorem 8.17. *Let F be a field, and let $f(x) \in F[x]$ be a non-zero polynomial.*

(a) *There exists an extension field L/F that is a splitting field for $f(x)$ over F.*

(b) *If L/F is a splitting field for $f(x)$ over F, then the degree of L/F is bounded by*

$$[L : F] \leq (\deg f)!\,.$$

(b) $f(x) = (x-\alpha_1)\,g_1(x)$ — degree n; degree $n-1$

$F[\alpha_1] : F$ should be 5

$g_1(x) = (x-\alpha_2)\,g_2(x)$ — degree $n-2$

$F \xrightarrow{n} F[\alpha_1] \xrightarrow{n-1} F[\alpha_1, \alpha_2]$

$= \frac{\square}{\square\square} + \frac{\square}{\square\square} + \frac{\square}{\square\square}$ ← $1, 2, \ldots, 9$

Definition 8.18. Let F be a field, let $f(x) \in F[x]$ be a polynomial, and write $f(x)$ as

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{d-1} x^{d-1} + a_d x^d.$$

The (*formal*) *derivative* of $f(x)$ is the polynomial

$$f'(x) = a_1 + 2a_2 x + \cdots + (d-1) a_{d-1} x^{d-2} + d a_d x^{d-1}.$$

Sum: $(f(x) \pm g(x))' = f'(x) \pm g'(x)$

diff

product: $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

Chain: $(f(g(x)))' = f'(g(x)) \cdot g'(x)$

Prove $(ax^n + bx^m)' = anx^{n-1} + bmx^{m-1}$

$(x^n x^m)' = (n+m)x^{n+m-1}$

Definition 8.21. Let F be a field, and let $f(x) \in F[x]$ be a non-zero polynomial. Theorem 8.17 tells us that there is an extension field in which $f(x)$ factors as

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d). \tag{8.13}$$

Then f is said to be *separable* if the roots $\alpha_1, \ldots, \alpha_d$ are distinct. This terminology comes from the idea that in a separable polynomial, the roots are separated from one another. Conversely, if f has one or more repeated roots, then it is *inseparable*.

$f(x) = x^4 - 2x^2 + 1 = (x^2 - 1)^2 = (x-1)^2(x+1)^2$

Proposition 8.24. *Let F be a field, and let $f(x) \in F[x]$ be a non-constant polynomial. Then*[3]

$$f \text{ is separable} \iff \gcd\big(f(x), f'(x)\big) = 1.$$

PolynomialGCD[x^2 - 1, x^4 - 1]

$-1+x^2$

$f(x) = q_1(x)g(x) + r_1(x)$ where $\deg r_1 < \deg g$

$\deg f \geq \deg g$

$$g_k x^k + \cdots + g_0 \;\overline{)\; f_d x^d + f_{d-1} x^{d-1} + \cdots + f_0}$$

$$\frac{f_d}{g_k} x^{d-k}$$

Euclidean Division Algorithm

↳ as field, $g_k \neq 0$

note $q_1(x)$ well defined

$\deg r_1 < \deg g$

Theorem 8.26. *Let F be a field, and let $f(x) \in F[x]$ be an irreducible polynomial.*

(a) *If the derivative $f'(x)$ is not identically 0, then $f(x)$ is separable.*

(b) *If F has characteristic 0, then $f(x)$ separable.*

Ex: $f(x) = x^{p-1}$

$f'(x) = p x^{p-1}$

if $\mathrm{char}(F) = p$, else 0

Proposition 8.24. *Let F be a field, and let $f(x) \in F[x]$ be a non-constant polynomial. Then*[3]

$$f \text{ is separable} \iff \gcd\big(f(x), f'(x)\big) = 1.$$

Proof:

Sketch

$f(x) = (x-\alpha)^2 g(x)$ so f is not separable

$f'(x) = 2(x-\alpha)\, g(x) + (x-\alpha)^2 g'(x) = (x-\alpha)\,(\text{crap}(x))$

$\gcd(f(x), f'(x)) \neq 1$ as has $x-\alpha$

8.5. Gauss's Lemma and Eisenstein's Irreducibility Criterion

Definition 8.29. Let

$$f(x) = c_0 + c_1 x + \cdots + c_d x^d \in \mathbb{Z}[x]$$

be a non-zero polynomial with integer coefficients. The *content of* f is the greatest common divisor of its coefficients,

$$\text{Content}(f) = \gcd(c_0, c_1, \ldots, c_d).$$

$f(x) = 3 - 7x^2 + 81x + 19x^5$ content$(f) = 1$

$f(x) = 3 - 9x^2 + 81x + 18x^5$ content$(f) = 3$

Compute content of the product of f, g

Observe: Content(fg) = content(f) content(g)

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1: https://youtu.be/xyLP6ViJyPM

Lecture 19: 4/18/24:

Chapter Eight: Fields and Roots, Geometric Constructions

Lemma 8.30. *Let $f(x), g(x) \in \mathbb{Z}[x]$ be non-zero polynomials. Then*

$$\text{Content}(fg) = \text{Content}(f)\,\text{Content}(g).$$

wlog: assume Content(f), Content(g) = 1

Must show Content(fg) = 1

↳ Assume not, so wlog ∃ prime p dividing all coeff of f(x)g(x)

$$f(x) = \underbrace{a_0}_{\text{mult of } p} + a_1 x + a_2 x^2 + \cdots + \underline{\underline{a_k x^k}} + \cdots$$

first coeff not a mult of p

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + \underline{\underline{b_\ell x^\ell}} + \cdots$$

first term not a mult of p

$$f(x)g(x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \ldots$$

wlog: assume $p \mid a_0$

$$f(x) = \underbrace{a_0 + a_1 x + \cdots + a_{k-1} x^k}_{\text{mult of } p} + \underbrace{a_k x^k}_{\text{not a mult of } p} + \cdots$$

$$g(x) = \underbrace{b_0 + \cdots + b_{l-1} x^{l-1}}_{\text{mult of } p} + \underbrace{b_l x^l}_{\text{not a mult of } p} + \cdots$$

Look at the x^{k+l} term in $f(x)g(x)$

$$\underbrace{a_0 b_{k+l} + a_1 b_{k+l-1} + \cdots + a_{k-1} b_{l+1}}_{\text{mult of } p} + \underbrace{a_k b_l}_{\text{not a mult of } p} + \underbrace{a_{k+1} b_{l-1} + \cdots + a_{k+l} b_0}_{\text{mult of } p}$$

Contradiction, so $\text{Content}(fg) = 1$

Theorem 8.31 (Gauss's Lemma). *Let $f(x) \in \mathbb{Z}[x]$, and suppose that $f(x)$ factors in $\mathbb{Q}[x]$, say*

$$f(x) = g(x)h(x) \quad \text{with} \quad g(x), h(x) \in \mathbb{Q}[x].$$

Then there is an analogous factorization of $f(x)$ using polynomials with integer coefficients, by which we mean that there are polynomials $G(x), H(x) \in \mathbb{Z}[x]$ and rational numbers $\alpha, \beta \in \mathbb{Q}^*$ satisfying

$$f(x) = G(x)H(x), \quad \text{where } G(x) = \alpha g(x) \text{ and } H(x) = \beta h(x).$$

In particular, a polynomial in $\mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$.

Proof: find $\alpha, \beta \in \mathbb{Q}^*$ st $\alpha g(x)$, $\beta h(x)$ have integer coeff and content 1

$\alpha\beta f(x) = G(x)H(x) = \alpha\beta\, g(x)h(x)$ $\quad \alpha\beta = A/B \in \mathbb{Q}^*$, A, B rel prime

$A f(x) = B\, G(x)H(x)$ wlog, content of $f = 1$

content A $=$ content B Since $A = B \Rightarrow \alpha\beta = 1 \Rightarrow f(x) = G(x)H(x)$

Corollary 8.32 (Irreducibiity via Reduction mod p). *Let*

$$f(x) = c_0 + c_1 x + \cdots + c_d x^d \in \mathbb{Z}[x]$$

be a polynomial of degree $d \geq 1$, let p be a prime, and let

$$\overline{f}_p(x) = \overline{c}_0 + \overline{c}_1 x + \cdots + \overline{c}_d x^d \in \mathbb{F}_p[x]$$

be the polynomial obtained by reducing the coefficients of $f(x)$ modulo p. Then

$$p \nmid c_d \text{ and } \overline{f}_p(x) \text{ irreducible in } \mathbb{F}_p[x] \implies f(x) \text{ is irreducible in } \mathbb{Q}[x].$$

Assume $\overline{f}_p(x) = \overline{g}_p(x)\,\overline{h}_p(x)$ factors

if $f(x) = g(x)h(x)$, highest terms in g, h are not 0 mod p, so when reduce mod p still not zero.

If f is reducible in $\mathbb{Z}[x]$ then it is reducible in $\mathbb{F}_p[x]$

So, if not reducible in $\mathbb{F}_p[x]$ cannot be reducible in $\mathbb{Z}[x]$

$p^2x^2 - 2px + 1$

$(px-1)^2$

Reduce mod p:

$$\frac{1}{x^2 - px - 1}$$

$(a_1x + a_0)(b_1x + b_0)$

$(x + a_0)(x + b_0)$

$(x-1)(x+1)$

mod p

$x^2 - 1 = (x-1)(x+1)$

To be useful, just need

ONE

prime where $\bar{F}_p$ is irreducible.

Remark 8.34. We stress that Corollary 8.32 is a one-way implication. If $\overline{f}_p(x)$ is reducible, that does not tell us that $f(x)$ is necessarily reducible. For example, the polynomial

$$f(x) = x^5 + 3x - 1$$

is irreducible in $\mathbb{Q}[x]$, but it often factors modulo p,

$$\begin{aligned}
\overline{f}_3 &= (x+2)(x^4+x^3+x^2+x+1) \in \mathbb{F}_3[x],\\
\overline{f}_5 &= (x+1)(x^4+4x^3+x^2+4x+4) \in \mathbb{F}_5[x],\\
\overline{f}_7 &\text{ is irreducible in } \mathbb{F}_7[x],\\
\overline{f}_{11} &= (x+3)(x^2+x+8)(x^2+7x+5) \in \mathbb{F}_{11}[x].
\end{aligned}$$

Corollary 8.35 (Eisenstein Irreducibility Criterion). *Let $p \in \mathbb{Z}$ be a prime, and let*

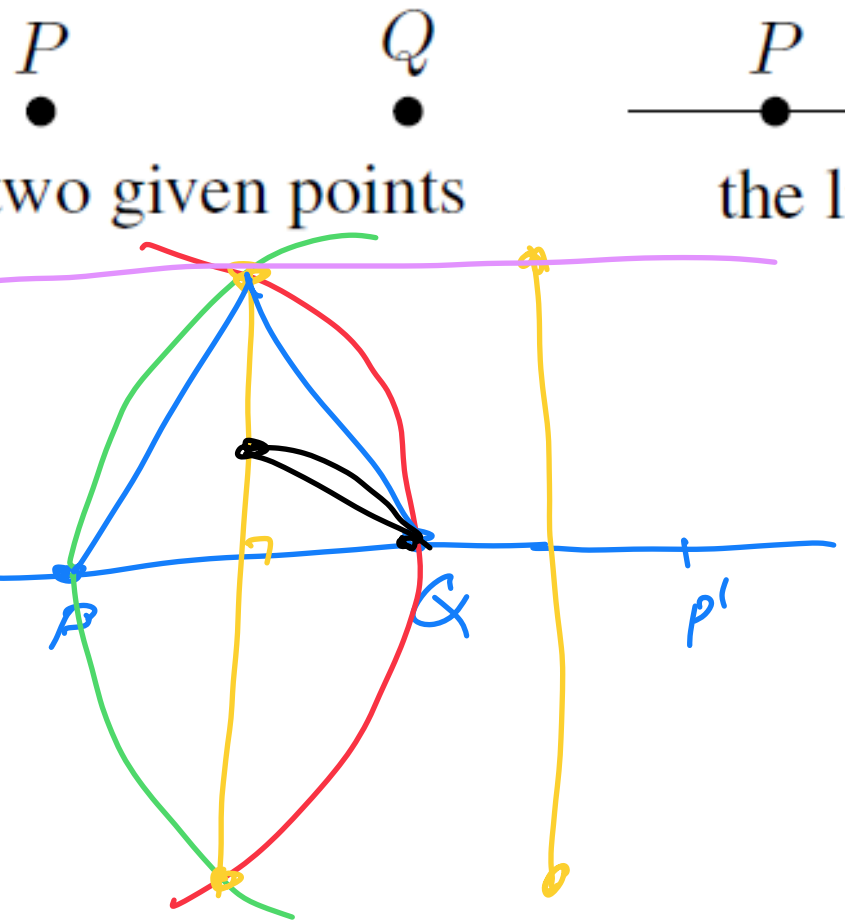
$$f(x) = c_0 + c_1 x + \cdots + c_d x^d \in \mathbb{Z}[x]$$

be a polynomial whose coefficients satisfy

$$p \nmid c_d, \quad p \mid c_i \quad \text{for all} \quad 0 \le i < d, \quad \text{and} \quad p^2 \nmid c_0.$$

Then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

8.6. Ruler and Compass Constructions



P Q

two given points

P Q

the line $L(P, Q)$

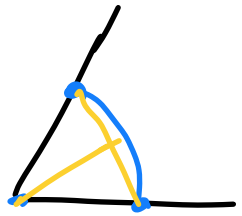
P Q

the circle $C(P, Q)$

Here are three famous problems that defied solution for centuries.

The Angle Trisection Problem: Divide a given angle into three equal angles. In other words, given an angle $\angle(P, Q, R)$, construct points S and T so that

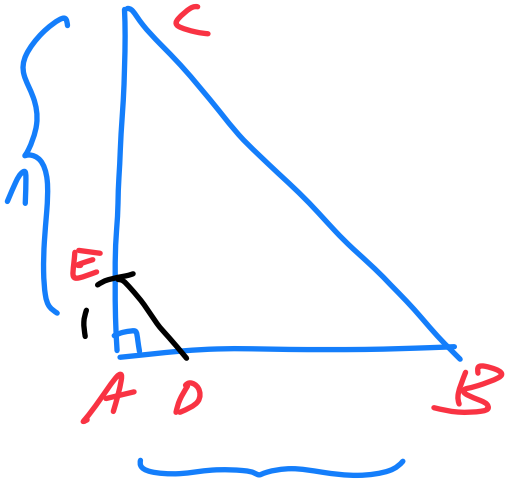
$$\angle(P, Q, S) = \angle(S, Q, T) = \angle(T, Q, R) = \frac{1}{3}\angle(P, Q, R).$$



The Doubling the Cube Problem: Given a cube whose volume is 1, construct a cube whose volume is 2. More precisely, given a line segment of length 1, construct a line segment of length $\sqrt[3]{2}$, since the edges of a cube of volume 2 have length $\sqrt[3]{2}$.

The Squaring the Circle Problem: Construct a square whose area is equal to the area of a circle of radius 1. (To do this, it suffices to construct a line segment of length π.)

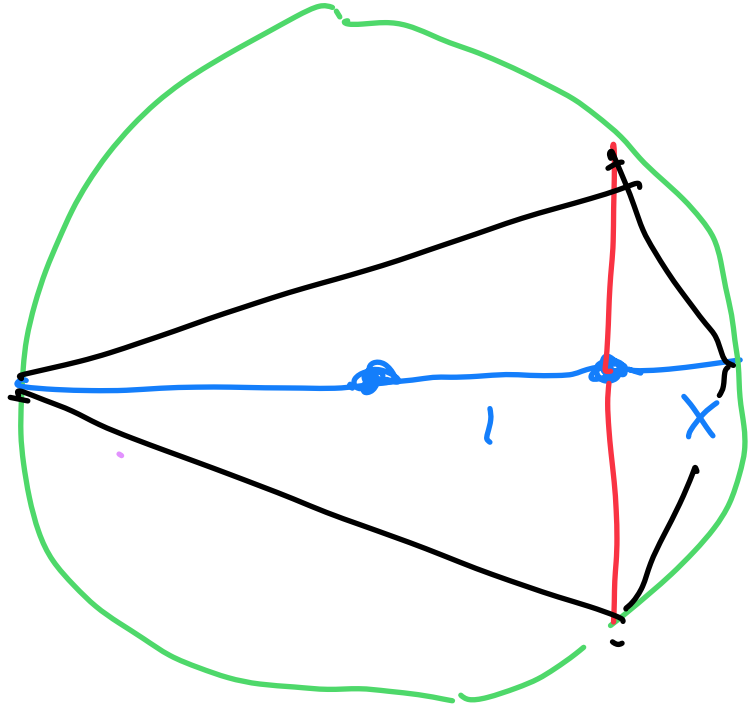
- Given two points P and Q, construct the midpoint of the line segment $\overline{PQ}$. (1/n)
- Given two points P and Q, construct an equilateral triangle having $L(P, Q)$ as one side.
- Given a line L and a point P on L, construct a line L' containing P that is perpendicular to L.
- Given a line L and a point P not on L, construct a line L' containing P that is parallel to L.
- Given three points P, Q, and R, construct a bisector for the angle $\angle(P, Q, R)$. In other words, construct a point S so that the angles $\angle(P, Q, S)$ and $\angle(S, Q, R)$ are equal. Figure 22 on page 209 gives a step-by-step ruler and compass procedure for bisecting an angle.

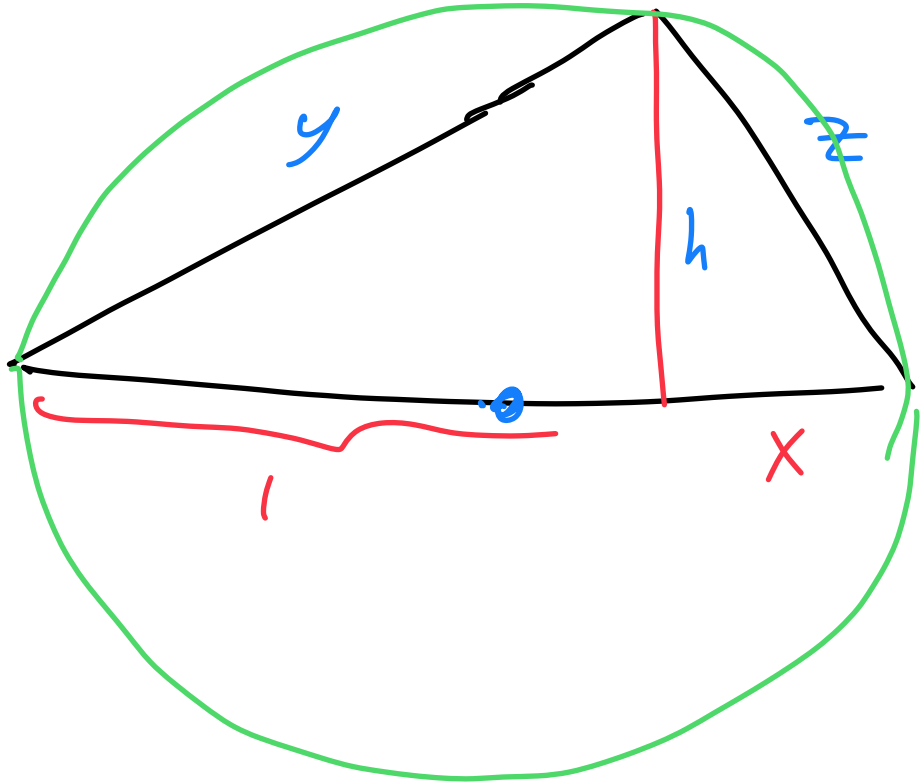


CPCTC

$\triangle ABC \sim \triangle ADE$

$\frac{AD}{AB} = \frac{AE}{AC} = \frac{1}{n}$





$$y^2 + z^2 = (1+x)^2 = x^2 + 2x + 1$$

$$z^2 = x^2 + h^2$$

$$y^2 = 1^2 + h^2$$

$$0 = 2x - 2h^2$$

$$\text{So } h^2 = x$$

$$\text{So } h = \sqrt{x}$$

Definition 8.40. The set of *constructible points* is the smallest set of points in the plane $\mathbb{R}^2$ having the following two properties:

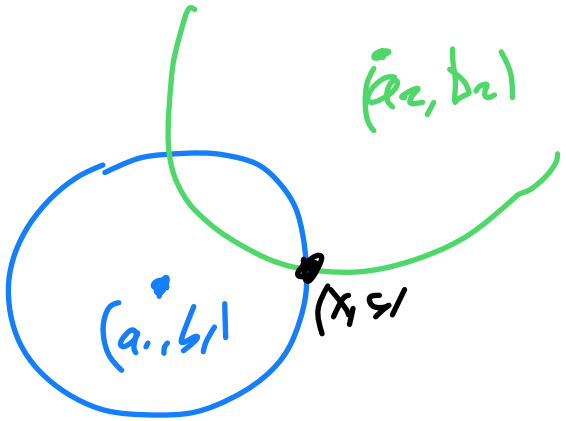
(I) $(0,0)$ and $(1,0)$ are constructible.

(II) If P, Q, R, S are constructible, then all of the points in the following intersections are constructable:

$$L(P,Q) \cap L(R,S), \quad C(P,Q) \cap L(R,S), \quad C(P,Q) \cap C(R,S).$$

The set of *constructible numbers* is the subset of $\mathbb{R}$ consisting of the X and Y coordinates of all of the constructible points in $\mathbb{R}^2$.

Theorem 8.41. *Let α be a constructible number. Then α is algebraic over $\mathbb{Q}$, and $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2.*



$$(x-a_1)^2 + (y-b_1)^2 = r_1^2$$

$$(x-a_2)^2 + (y-b_2)^2 = r_2^2$$

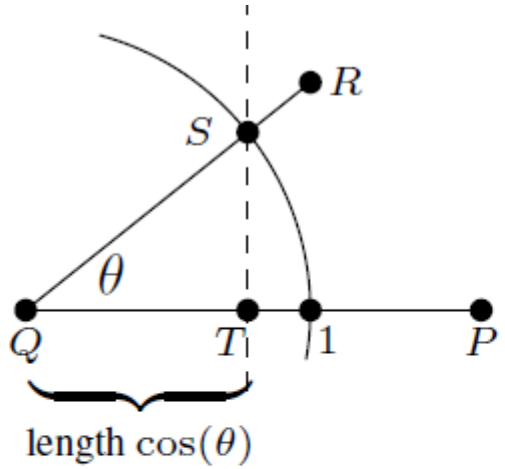


Figure 25. Given the angle θ, construct a segment of length $\cos(\theta)$.

We have thus shown the following:

If the angle θ is constructible, then the number $\cos(\theta)$ is constructible.

If $\cos\theta$ is not constructible then θ is not constructible.

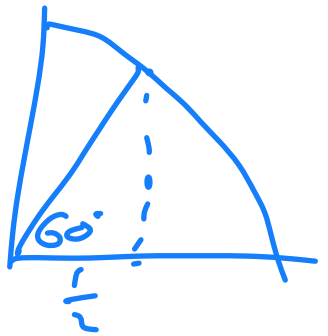
Want to show $\cos(20^\circ)$ not constructible $\Rightarrow$ Can't trisect 60°

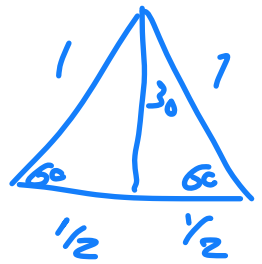
In particular, if we could trisect a $60°$ angle, then the number

$$\cos(20°) \text{ would be constructible.}$$

We can find a polynomial that has $\cos(20°)$ as a root by using the following triple angle formula:[18]

$$\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta).$$





$\cos(A+B) = \cos A \cos B - \sin A \sin B$

$\sin(A+B) = \sin A \cos B + \cos A \sin B$

$\cos^2 x + \sin^2 x = 1$

If $\cos 20°$ is constructible: $\cos(60°) = 1/2$ Let $x = \cos\theta$

$\Rightarrow 4x^3 - 3x = 1/2$ has root $x = \cos 20°$

or $8x^3 - 6x - 1 = 0$

$8x^3 - 6x - 1 = 0 = g(x)\,h(x)$

deg 1 deg 2

$= (a_1 x + a_0)(b_2 x^2 + b_1 x + b_0)$

So $-a_0/a_1$ is a root

$p = a_0$ $q = a_1$ Need $p \mid 1$ $q \mid 8$

So $p = \pm 1$ $q = \pm 1, \pm 2, \pm 4, \pm 8$

Way $p=1$, have 8 things to check

$8\left(\frac{\pm 1}{q}\right)^3 - 6\left(\frac{\pm 1}{q}\right) - 1 = 0$ Minus sign won't work

$8\left(\frac{1}{8}\right)^3 - 6\frac{1}{8} - 1$, $8\left(\frac{1}{4}\right)^3 - 6\frac{1}{4} - 1$, $8\left(\frac{1}{2}\right)^2 - 6\frac{1}{2} - 1$, $8 \cdot 1 - 6 \cdot 1 - 1$

$\neq 0$ $\neq 0$ $\neq 0$ $\neq 0$

Corollary 8.44. *The number $\sqrt[3]{2}$ is not constructible and hence it is not possible to "double the cube" using ruler and compass.*

$x^3 - 2 = 0$: Is this irreducible?

Eisenstein: $p = 2$

$x^3 - 0x^2 - 0x - 2 = 0$

all mult of p

not mult of p^2

Remark 8.45 (Squaring the Circle)**.** As noted in Example 8.3, Lindemann proved in 1882 that π is transcendental over $\mathbb{Q}$. Thus the field $\mathbb{Q}(\pi)$ is not even an algebraic extension of $\mathbb{Q}$, much less an extension of 2-power degree. It follows from Theorem 8.41 that π is not a constructible number, and hence that it is impossible to "square the circle" using ruler and compass.

Rational root theorem

From Wikipedia, the free encyclopedia

In algebra, the **rational root theorem** (or **rational root test**, **rational zero theorem**, **rational zero test** or **p/q theorem**) states a constraint on rational solutions of a polynomial equation

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

with integer coefficients $a_i \in \mathbb{Z}$ and $a_0, a_n \neq 0$. Solutions of the equation are also called roots or zeros of the polynomial on the left side.

The theorem states that each rational solution $x = {}^{p}/_{q}$, written in lowest terms so that p and q are relatively prime, satisfies:

- p is an integer factor of the constant term a_0, and
- q is an integer factor of the leading coefficient a_n.

The rational root theorem is a special case (for a single linear factor) of Gauss's lemma on the factorization of polynomials. The **integral root theorem** is the special case of the rational root theorem when the leading coefficient is $a_n = 1$.

https://en.wikipedia.org/wiki/Descartes%27_rule_of_signs

Descartes' rule of signs [edit]

Positive roots [edit]

The rule states that if the nonzero terms of a single-variable polynomial with real coefficients are ordered by descending variable exponent, then the number of positive roots of the polynomial is either equal to the number of sign changes between consecutive (nonzero) coefficients, or is less than it by an even number. A root of multiplicity k is counted as k roots.

In particular, if the number of sign changes is zero or one, the number of positive roots equals the number of sign changes.

Negative roots [edit]

As a corollary of the rule, the number of negative roots is the number of sign changes after multiplying the coefficients of odd-power terms by −1, or fewer than it by an even number. This procedure is equivalent to substituting the negation of the variable for the variable itself. For example, the negative roots of $ax^3 + bx^2 + cx + d$ are the positive roots of

$$a(-x)^3 + b(-x)^2 + c(-x) + d = -ax^3 + bx^2 - cx + d.$$

Thus, applying Descartes' rule of signs to this polynomial gives the maximum number of negative roots of the original polynomial.

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1:

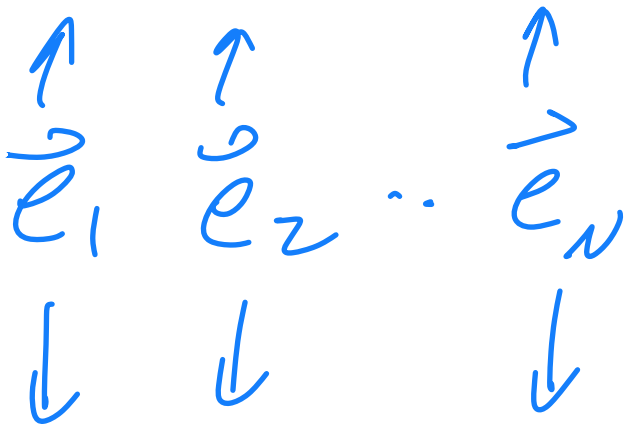
Lecture 20: 4/23/24: No lecture, museum trip

Lecture 21: 4/25/24: https://youtu.be/JqeseAM0lfQ

Chapter Twelve: Preliminaries: Groups in Number Theory

Given any large number N, are there infinitely many vectors in R^N such that any subset of N of them are linearly independent, but any subset of N+1 of them are linearly dependent?

If yes, can you give a constructive proof, in other words can you give a formula that would work and explicitly enumerate them?



$\vec{v}_{N+1}$

Choose any vector not in unions of $\binom{N}{N-1}$ hyperplanes spanned by $\vec{e}_1, \ldots \vec{e}_N$

$\vec{v}_{N+2}$

Choose any vector not in $\binom{N+1}{N-1}$ unions of hyperplanes

$\vec{v}_{N+3}$ ....

Choose any of in $\binom{N+2}{N-1}$

⋮

Vandermonde Matrices

$$\begin{pmatrix} 1 & x_0 & x_0^2 & x_0^3 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & x_1^3 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & x_2^3 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & x_n^3 & \cdots & x_n^{n-1} \end{pmatrix}$$

det is zero if two rows are equal

so if $x_i = x_j$ then det is zero, so

poly is divisible by $(x_i - x_j)$

$$\text{Det} = g(x) \cdot \prod_{0 \le j < i \le n-1} (x_i - x_j)$$

determinant is a polynomial in $x_0, x_1, \ldots, x_n$

terms will be of deg $0, 1, 2, \ldots, n-1$

$n-1$ in each summand

maybe $1 \cdot x_3 \cdot x_0^2 \cdot x_5^3 \cdots$

poly has degree $0 + 1 + \cdots + n-1$

$= (n-1)n/2$

$S = 0 + 1 + \cdots + n-1$

$S = (n-1) + (n-2) + \cdots + 0$

$2S = (n-1)n \Rightarrow S = \frac{(n-1)n}{2}$

$$Det = g(X) \cdot \prod_{0 \le j < i \le n-1} (x_i - x_j)$$ poly of deg $\frac{(n-1)n}{2}$ ⟷ same

ways to choose two distinct indices in $\{0, 1, 2, \ldots, n-1\}$ is $\binom{n}{2} = \frac{n(n-1)}{2}$

Thus $g(x) =$ Constant, if can find det for one choice, done

$$\begin{pmatrix} 1 & x_0 & x_0^2 & x_0^3 & \cdots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & x_1^3 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & x_2^3 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & x_n^3 & \cdots & x_n^{n-1} \end{pmatrix}$$

$$\begin{pmatrix} 1 & 10^{1000} & (10^{1000})^2 & & \\ 1 & (10!)^{1000!} & ((10!)^{1000!})^2 & & \\ 1 & (10^{10!})^{1000!} & (\quad)^2 & & \end{pmatrix}$$

$x_n \ggg x_{n-1} \ggg \cdots \ggg x_2 \ggg x_1$

$\det \approx x_n^{n-1} x_{n-1}^{n-2} \cdots x_2^2 \cdot x_1^1 \cdot 1$

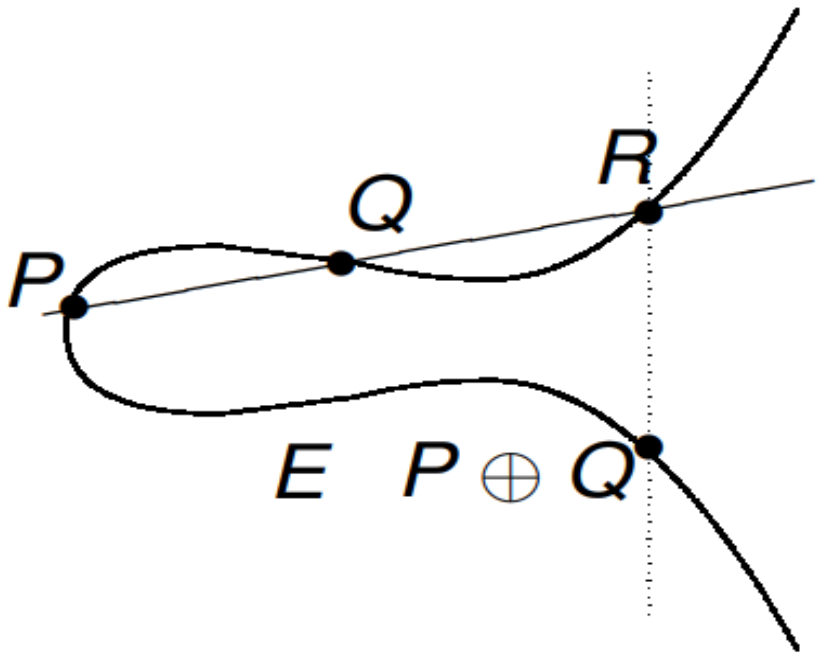
$\det = \text{Const} \prod_{0 \le j < i \le n-1} (x_i - x_j)$

Constant not zero

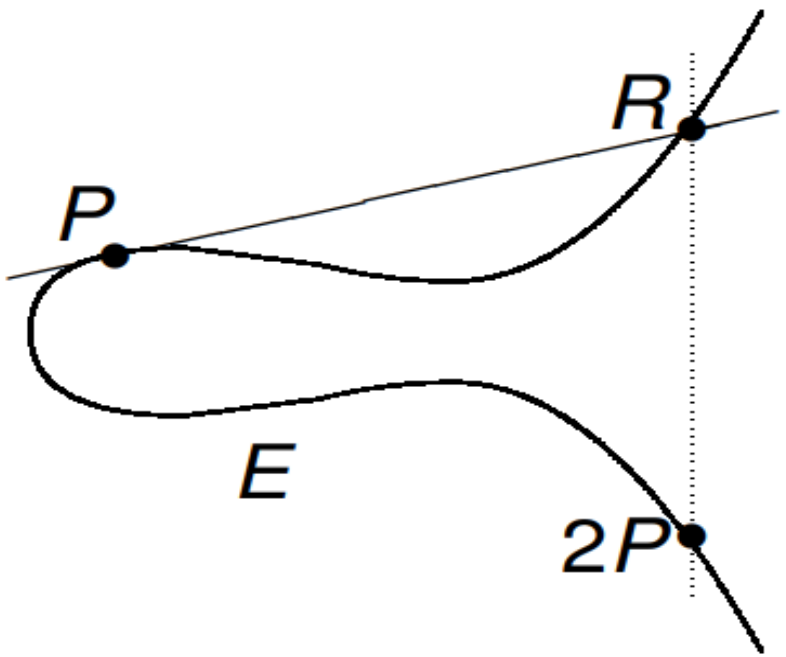
EC: Find the constant
For Tuesday)

Elliptic Curves: Mordell-Weil Group

Elliptic curve $y^2 = x^3 + ax + b$ with rational solutions $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ and connecting line $y = mx + b$.



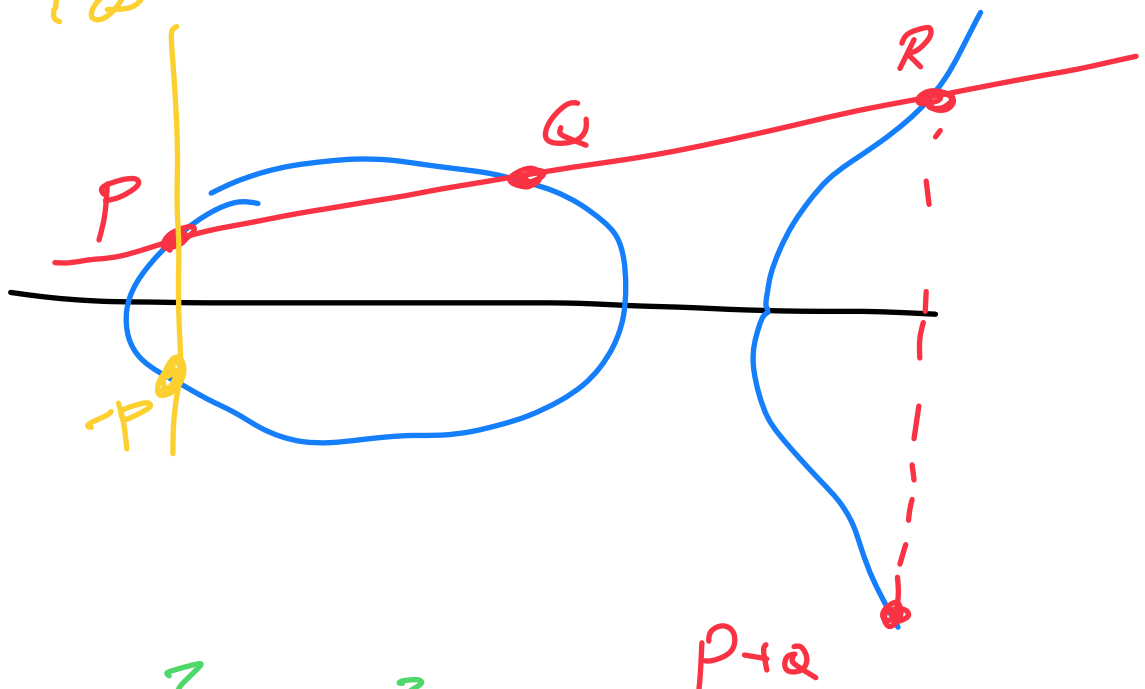
Addition of distinct points P and Q



Adding a point P to itself

$$E(\mathbb{Q}) \approx E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

$y^2 = x^3 + ax + b$, $a, b \in \mathbb{Q}$ $(x_1, y_1), (x_2, y_2) \in \mathbb{Q}^2$ solving the equation.



$y = mx + \beta$

$y_1 = mx_1 + \beta$

$y_2 = mx_2 + \beta$

$y_1 - y_2 = m(x_1 - x_2)$

$m = \frac{y_1 - y_2}{x_1 - x_2} \in \mathbb{Q}$

$\beta = y_1 - mx_1 \in \mathbb{Q}$

$y^2 = x^3 + ax + b$ know (x_1, y_1) and (x_2, y_2) solve this and on line $y = mx + \beta$

$(mx+\beta)^2 = x^3 + ax + b$ or $x^3 - m^2x^2 + (a - 2m\beta)x + b$

$x^3 - m^2x^2 + (a-2m\beta)x + b = (x - x_1)(x - x_2)(x - x_3)$ Ex: prove $x_3 \in \mathbb{Q}$

$= x^3 - (\underbrace{x_1 + x_2 + x_3}_{\mathbb{Q}})x^2 + (\underbrace{\quad}_{\mathbb{Q}})x - \underbrace{x_1x_2x_3}_{\mathbb{Q}}$

Group!

Closure: ✓

Identity! "2"

Assoc: had but true

Inverse: -P

Riemann Zeta Function

Geometric Series!

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

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \mathrm{Re}(s) > 1.$$

Unique Factorization: $n = p_1^{r_1} \cdots p_m^{r_m}$.

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \left[1 + \frac{1}{2^s} + \left(\frac{1}{2^s}\right)^2 + \cdots\right]\left[1 + \frac{1}{3^s} + \left(\frac{1}{3^s}\right)^2 + \cdots\right]\cdots$$

$$= \sum_n \frac{1}{n^s}.$$

Riemann Zeta Function (cont)

$$\zeta(s) = \sum_n \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \mathrm{Re}(s) > 1$$

$$\pi(x) = \#\{p : p \text{ is prime}, p \leq x\}$$

Properties of $\zeta(s)$ and Primes:

- $\lim_{s \to 1^+} \zeta(s) = \infty$, $\pi(x) \to \infty$.
- $\zeta(2) = \frac{\pi^2}{6}$, $\pi(x) \to \infty$.

Dirichlet Characters (m prime)

$(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic of order $m-1$ with generator g. Let $\zeta_{m-1} = e^{2\pi i/(m-1)}$. The principal character χ_0 is given by

$$\chi_0(k) = \begin{cases} 1 & (k,m) = 1 \\ 0 & (k,m) > 1. \end{cases}$$

The $m-2$ primitive characters are determined (by multiplicativity) by action on g.

As each $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$, for each χ there exists an l such that $\chi(g) = \zeta_{m-1}^l$. Hence for each $l, 1 \leq l \leq m-2$ we have

$$\chi_l(k) = \begin{cases} \zeta_{m-1}^{la} & k \equiv g^a(m) \\ 0 & (k,m) > 0 \end{cases}$$

$(\mathbb{Z}/n\mathbb{Z})^*$ has $n-1$ elements

Generator $\zeta_n = e^{2\pi i/n-1}$

Group is $\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-2}\}$ as $\zeta_n^{n-1} = 1$

Given any $n \in (\mathbb{Z}/n\mathbb{Z})^*$ it is equivalent to ζ_n^a for some a

Map $\chi_\ell(n) = \chi_\ell(\zeta_n^a) = (\zeta_n^a)^\ell$

Dirichlet L-Functions

Let χ be a primitive character mod m. Let

$$c(m,\chi) = \sum_{k=0}^{m-1} \chi(k) e^{2\pi i k/m}.$$

$c(m,\chi)$ is a Gauss sum of modulus $\sqrt{m}$.

$$\begin{aligned} L(s,\chi) &= \prod_p (1-\chi(p)p^{-s})^{-1} \\ \Lambda(s,\chi) &= \pi^{-\frac{1}{2}(s+\epsilon)} \Gamma\left(\frac{s+\epsilon}{2}\right) m^{\frac{1}{2}(s+\epsilon)} L(s,\chi), \end{aligned}$$

where

$$\epsilon = \begin{cases} 0 & \text{if } \chi(-1) = 1 \\ 1 & \text{if } \chi(-1) = -1 \end{cases}$$

Character Sums

$$\sum_{\chi} \chi(k) = \begin{cases} m-1 & k \equiv 1(m) \\ 0 & \text{otherwise.} \end{cases}$$

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:

https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

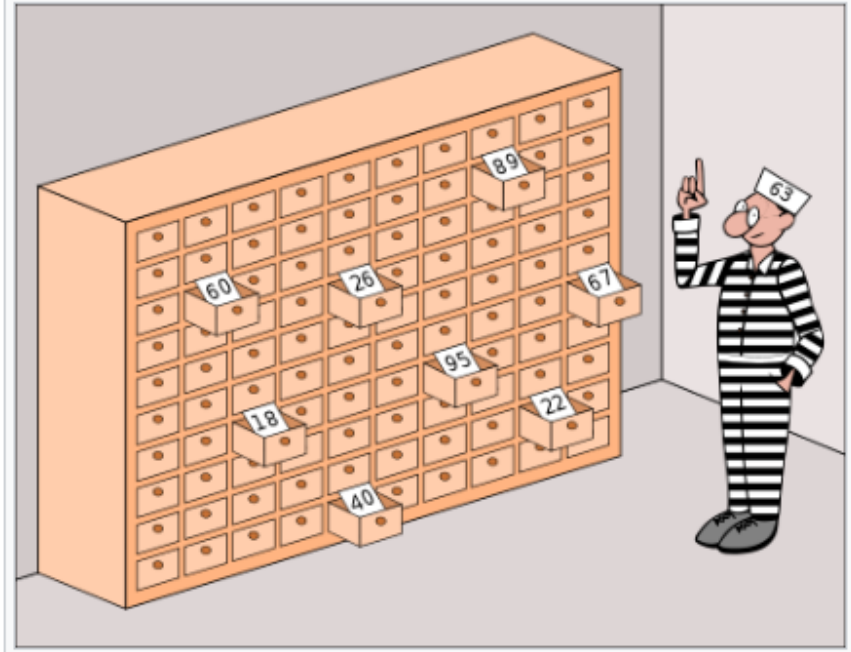
Section 1:

Lecture 22: 4/30/24: https://youtu.be/KTHY13pT7Uw

Chapter Twelve: Groups: Groups Part III: Permutation Groups, Cycles, Solvable

The **100 prisoners problem** is a mathematical problem in probability theory and combinatorics. In this problem, 100 numbered prisoners must find their own numbers in one of 100 drawers in order to survive. The rules state that each prisoner may open only 50 drawers and cannot communicate with other prisoners. At first glance, the situation appears hopeless, but a clever strategy offers the prisoners a realistic chance of survival.

Anna Gál and Peter Bro Miltersen first proposed the problem in 2003.



Each prisoner has to find their own number in one of 100 drawers, but may open only 50 of the drawers.

Problem [edit]

The 100 prisoners problem has different renditions in the literature. The following version is by Philippe Flajolet and Robert Sedgewick:[1]

> *The director of a prison offers 100 death row prisoners, who are numbered from 1 to 100, a last chance. A room contains a cupboard with 100 drawers. The director randomly puts one prisoner's number in each closed drawer. The prisoners enter the room, one after another. Each prisoner may open and look into 50 drawers in any order. The drawers are closed again afterwards. If, during this search, every prisoner finds their number in one of the drawers, all prisoners are pardoned. If even one prisoner does not find their number, all prisoners die. Before the first prisoner enters the room, the prisoners may discuss strategy — but may not communicate once the first prisoner enters to look in the drawers. What is the prisoners' best strategy?*

If every prisoner selects 50 drawers independently and randomly, the probability that a single prisoner finds their number is 50%. The probability that all prisoners find their numbers is the product of the single probabilities, which is $(\frac{1}{2})^{100} \approx 0.000\,000\,000\,000\,000\,000\,000\,000\,000\,0008$, a vanishingly small number. The situation appears hopeless.

https://en.wikipedia.org/wiki/100_prisoners_problem

12.1. Permutation Groups

We recall that a permutation of a set X is a bijective function $\pi : X \to X$ and that the set of permutations $\mathcal{S}_X$ forms a group whose group law is composition of functions. In the case that X is finite, it is often convenient to identify X with the set of integers $\{1, \ldots, n\}$.

Definition 12.1. The group of permutations of $\{1, 2, \ldots, n\}$ is denoted $\mathcal{S}_n$ and is called the *symmetric group*.

$\#S_n = n! \Rightarrow \log \#S_n = \log(n!) = \log 1 + \log 2 + \cdots + \log n$

$\approx \int_1^n \log t \, dt$

$= [t \log t - t]_1^n = (n \log n - n) - (1 \log 1 - 1)$

$\approx n \log n - n$

$n! \approx e^{n \log n - n} = n^n e^{-n}$

Proposition 12.3. (a) *The group S_n has order $n!$.*
(b) *For all $n \geq 3$, the group S_n is non-abelian.*

$n=1$: S_1 is just the identity permutation

$n=2$: S_2 is just $\begin{pmatrix}1&2\\1&2\end{pmatrix}=e$ and $\begin{pmatrix}1&2\\2&1\end{pmatrix}$

$n\geq 3$: $\begin{pmatrix}1&2&3&4&5&\cdots&n\\2&1&3&4&5&\cdots&n\end{pmatrix}$ $\begin{pmatrix}1&2&3&4&5&\cdots&n\\3&2&1&4&5&\cdots&n\end{pmatrix}$

either $2\to 3$ or $2\to 1$

τ_{12} switches 1 and 2 τ_{13} switches 1 and 3

$$\tau_{13}\tau_{12} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&\\2&\end{pmatrix}$$

$$\tau_{12}\tau_{13} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&\\3&\end{pmatrix}$$

Go later to alter

not abelian

Definition 12.4. Let $\pi \in S_n$, and suppose that the π-orbit of a contains k elements. Then we write the orbit as

$$(a, \pi(a), \pi^2(a), \ldots, \pi^{k-1}(a)),$$

and we call this k-tuple the *π-cycle of a*.

$\gamma_{12}(1) = 2$ $\quad \gamma_{12}(\gamma_{12}(1)) = \gamma_{12}(2) = 1$

$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

$\pi(1) = 2, \quad \pi^2(1) = 3, \quad \pi^3(1) = 1$

$\pi(4) = 5, \quad \pi^2(4) = 4$

Same as disjoint

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 4 & 5 \\ 5 & 4 \end{pmatrix} \text{ or } \begin{pmatrix} 4 & 5 \\ 5 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Theorem 12.11. *Let $\pi \in S_n$. There are pairwise disjoint cycles $\sigma_1, \ldots, \sigma_k \in S_n$ such that*

$$\pi = \sigma_1 \sigma_2 \cdots \sigma_k, \tag{12.3}$$

and the list of cycles $\sigma_1, \ldots, \sigma_k$ is uniquely determeind by π, up to listing them in a different order.

Idea: Break group into orbits when it acts on itself by π

$1 \to 3 \to 7 \to 11 \to 6 \to 1$

X $2 \to 8 \to 16 \to 31 \to 17 \to 2024 \to 6 \to 2$ illegal

$2 \to 8 \to 16 \to 31 \to 17 \to 2024 \to 2$

know $3 \to 7 \to 11 \to 6 \to 1 \to 3$

$$\begin{pmatrix} 1 & 3 & 7 & 6 \\ 3 & 7 & 11 & 1 \end{pmatrix} \begin{pmatrix} 2 & 8 & 16 & 31 & 17 & 2024 \\ 8 & 16 & 31 & 17 & 2024 & 2 \end{pmatrix} \cdots$$

each orbit is a cycle, orbits are disjoint

Example 12.12. Let $\pi \in \mathcal{S}_{10}$ be the permutation

1	2	3	4	5	6	7	8	9	10
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
3	1	7	2	10	9	4	5	6	8

$$\begin{pmatrix} 1 & 3 & 7 & 4 & 2 \\ 3 & 7 & 4 & 2 & 1 \end{pmatrix}\begin{pmatrix} 5 & 10 & 8 \\ 10 & 8 & 5 \end{pmatrix}\begin{pmatrix} 6 & 9 \\ 9 & 6 \end{pmatrix}$$

Shortest non-trivial cycle

Definition 12.13. An element $\pi \in \mathcal{S}_n$ is called a *transposition* if there are distinct $a, b \in \{1, 2, \ldots, n\}$ such that

$$\pi(a) = b, \quad \pi(b) = a, \quad \pi(i) = i \text{ for all } i \neq a, b.$$

τ_{ab} or τ_{ba}

$\tau_{ab}^2 = e$

Proposition 12.14. *Let $\pi \in S_n$. There exist transpositions $\tau_1, \ldots, \tau_k \in S_n$ so that π is equal to the product*

$$\pi = \tau_1 \tau_2 \cdots \tau_k.$$

Proof: Wlog assume π is the cycle $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots & 1 \end{pmatrix}$

Divine Inspiration $\tau_{1n} \cdots \tau_{14} \tau_{13} \tau_{12}$

$1 \to 2$
$2 \to 1$

$1 \to 2$
$2 \to 3$
$3 \to 1$

$1 \to 2$
$2 \to 3$
$3 \to 4$
$4 \to 1$

Could do

$\tau_{21} \tau_{2n} \cdots \tau_{24} \tau_{23}$

Theorem 12.16. *Let $\pi \in \mathcal{S}_n$, and suppose that we write π as a product of transpositions in two ways, say*

$$\pi = \tau_1 \tau_2 \cdots \tau_k = \sigma_1 \sigma_2 \cdots \sigma_\ell,$$

where $\tau_1, \ldots, \tau_k$ and $\sigma_1, \ldots, \sigma_\ell$ are transpositions. Then

$$k \equiv \ell \pmod 2.$$

$e = \tau_{12}\tau_{21}$

$e = \tau_{12}\tau_{34}\tau_{12}\tau_{34}$

Proof of Theorem 12.16

$$D(X_1, \ldots, X_n) = \prod_{1 \le j < i \le n} (X_i - X_j).$$

Vandermonde Matrices

#terms $\binom{n}{2} = \frac{n(n-1)}{2}$

$\pi D(X_1, \ldots, X_n) = D(X_{\pi(1)}, \ldots, X_{\pi(n)})$

Ex. $n=3$: $D(X_1, X_2, X_3) = (X_3 - X_1)(X_3 - X_2)(X_2 - X_1)$

$\tau_{13} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau_{13}$

$\tau D(X_1, X_2, X_3) = D(X_3, X_2, X_3) = (X_1 - X_3)(X_1 - X_2)(X_2 - X_3)$

$= -D(X_1, X_2, X_3)$

A calculation (Exercise 12.7) shows that the square of the polynomial D is equal to the discriminant polynomial

$$D(X_1, \ldots, X_n)^2 = (-1)^{(n^2-n)/2} \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (X_i - X_j).$$

$(X_i - X_j)(X_i - X_j)$

$= -(X_i - X_j)(X_j - X_i)$

$\binom{n}{2} = \frac{n(n-1)}{2} = \frac{n^2-n}{2}$

$\pi D^2(X_1, \ldots, X_n) = D^2(X_{\pi(1)}, \ldots, X_{\pi(n)}) = D^2(X_1, \ldots, X_n)$

Ex: before π change as $(-1)^2$

In particular, we see that D^2 is invariant for the action of $\mathcal{S}_n$; i.e., it is a symmetric polynomial as defined in Section 7.6. Thus for every $\pi \in \mathcal{S}_n$ we have

$$D^2 = \pi(D^2) = \pi(D)^2, \quad \text{and hence} \quad \pi(D) = \pm D.$$

$\tau_{13}(D) = -D$

$\tau_{13}^2(D) = \tau_{13}(\tau_{13} D) = D$

$\downarrow$

Id

$\tau_{13}(-D) = -\tau_{13}(D)$

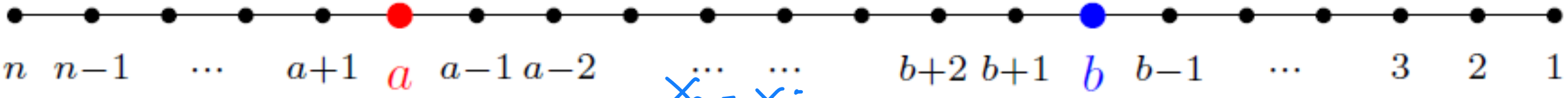
$= (-1)^2 D$

$$\pi(D) = \prod_{1 \le j < i \le n} \pi(X_i - X_j) = \prod_{1 \le j < i \le n} (X_{\pi(i)} - X_{\pi(j)}),$$

so the sign changes in (12.6) come from the $i > j$ pairs satisfying $\pi(i) < \pi(j)$.

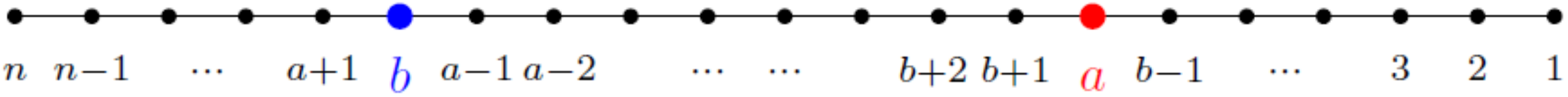
$(X_1 - X_3)$ → $(X_3 - X_1)$ or $(X_1 - X_3)$

The indices between a and b have no effect before we swap a and b.



Indices from n to 1 before applying $\tau = (a, b)$

Swapping a and b causes sign flips in D for the indices between a and b.



Indices from n to 1 after applying $\tau = (a, b)$

$X_j - X_a$

$X_b - X_j$

$X_a - X_j$

$\sum_{ab}$

i, j or both in $\{a, b\}$ to have $\sum_{ab}$ have an impact on $X_i - X_j$

Factor of D	Apply $\tau = (a, b)$	Flip?	# of factors
$X_i - X_a$ with $i > a > b$	$X_i - X_b$	No	
$X_a - X_i$ with $a > i > b$	$X_b - X_i$	Yes	$a - b - 1$
$X_a - X_i$ with $a > b > i$	$X_b - X_i$	No	
$X_i - X_b$ with $i > a > b$	$X_i - X_a$	No	
$X_i - X_b$ with $a > i > b$	$X_i - X_a$	Yes	$a - b - 1$
$X_b - X_i$ with $a > b > i$	$X_a - X_i$	No	
$X_a - X_b$	$X_b - X_a$	Yes	1
$X_i - X_j$ with $\{i, j\} \cap \{a, b\} = \emptyset$	$X_i - X_j$	No	

same

odd

Hence we can write the product defining $\tau(D)$ as

$$\tau(D) = \begin{pmatrix} X_i - X_j \text{ factors} \\ \text{that don't have} \\ \text{a sign flip} \end{pmatrix} \cdot \tau\Bigg(\underbrace{(X_a - X_b) \cdot \prod_{a>i>b} (X_a - X_i) \cdot \prod_{a>i>b} (X_i - X_b)}_{\text{These are the } X_i - X_j \text{ factors that flip when } \tau = (a,b) \text{ is applied.}} \Bigg)$$

$$= (-1)^{1+(a-b-1)+(a-b-1)} D$$

$$= -D.$$

This completes the proof that $\tau(D) = -D$ for all transpositions $\tau \in \mathcal{S}_n$.

$\pi = \tau_1 \cdots \tau_k$ and $\tau_1' \cdots \tau_\ell'$

$\pi(D) = (-1)^k D$ $\qquad$ $\pi(D) = (-1)^\ell D$

$\Longrightarrow k \equiv \ell \mod 2$

Theorem 12.23 (Cayley's Theorem). (a) *Every group is isomorphic to a subgroup of some symmetric group.*

(b) *If G is a finite group of order n, then G is isomorphic to a subgroup of $S_{n!}$.*

trivial subgroups

Definition 12.25. A group G is a *simple group* if its only normal subgroups are G and $\{e\}$.

Theorem 12.29. *For all $n \geq 5$, the alternating group A_n is a simple group.*

permutations with an even # of transpositions

H is normal in G, $H \trianglelefteq G$, if $\forall g \in G: gHg^{-1} = H$

or $gH = Hg$

Ex: $G = \{e, a, a^2, a^3, a^4, a^5, a^6\} = \langle a \rangle$ and $a^7 = e$

Lagrange: order of a subgroup divides $\#G \Rightarrow$

Definition 12.31. Let G be a (finite) group. A *composition series for* G is a nested list of subgroups

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_{n-1} \supsetneq G_n = \{e\}, \tag{12.11}$$

starting at G and ending at the identity $\{e\}$, that has the following properties:

(1) For every $0 \leq i < n$, the group G_{i+1} is a normal subgroup of G_i.

(2) For every $0 \leq i < n$, the quotient group G_i/G_{i+1} is a simple group.

The quotient groups

$$G_0/G_1,\ G_1/G_2,\ \ldots,\ G_{n-1}/G_n$$

are called the *composition quotients* of the composition series (12.11), and the integer n is called the *length* of the series.

Definition 12.36. A finite group G is said to be *solvable* if the composition quotients in its composition series are abelian;[8] cf. Definition 9.75.

Theorem 12.38 (Classification of Finite Simple Groups)**.** *Let G be a finite simple group. Then G is isomorphic to one of the following*:

- *A cyclic group of prime order.*
- *An alternating group $\mathcal{A}_n$ with $n \geq 5$.*
- *A group of* Lie type. *These consist of several explicit families of groups of matrices with coefficients in finite fields.*
- *An explicit list of* 26 *additional* sporadic finite simple groups. *The largest sporadic group* M *is called the* monster group. *It has order*

$$\#\mathsf{M} = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71,$$

so it has roughly 10^{54} elements.

Proof. The proof is far beyond the scope of this textbook. □

Theorem 12.52 (Structure Theorem for Finite Abelian Groups)**.** *Let G be a finite abelian group. Then G is isomorphic to a product of cyclic groups. More precisely, we have the following two characterizations of G, where $\mathcal{C}_n$ denotes a cyclic group of order n:*

(a) *There are positive integers $b_1, \ldots, b_s \geq 2$, uniquely determined by G, such that*

$$b_1 \mid b_2 \mid \cdots \mid b_s \quad \text{and} \quad G \cong \mathcal{C}_{b_1} \times \mathcal{C}_{b_2} \times \cdots \times \mathcal{C}_{b_s}.$$

(b) *There are prime powers $q_1, \ldots, q_t \in \mathbb{Z}$, uniquely determined by G, such that*

$$G \cong \mathcal{C}_{q_1} \times \mathcal{C}_{q_2} \times \cdots \times \mathcal{C}_{q_t}.$$

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

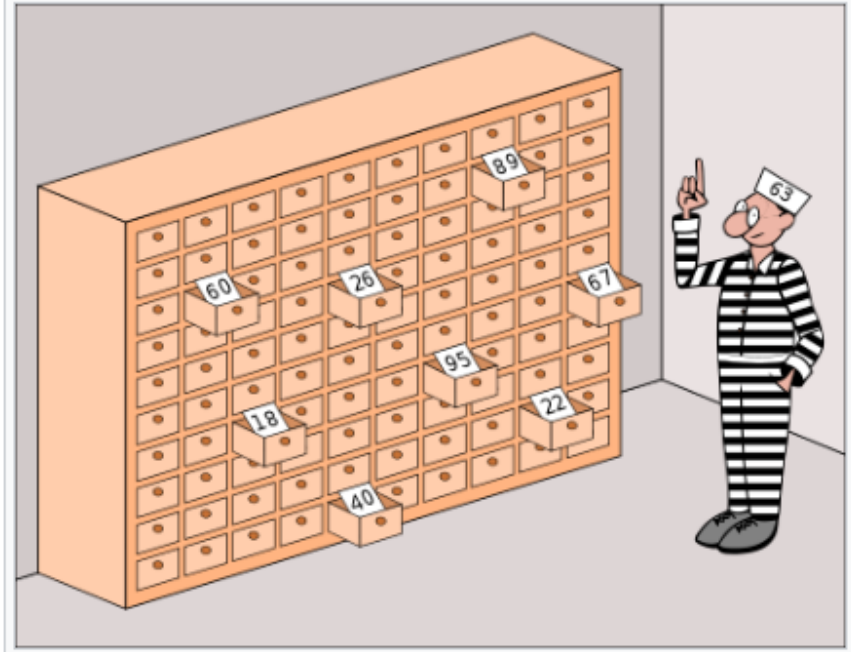
Section 1:

Lecture 23: 5/2/24: https://youtu.be/_-FCs_nDlF0

Chapter Twelve: Groups: Groups Part III: Problems, Finite Abelian

The **100 prisoners problem** is a mathematical problem in probability theory and combinatorics. In this problem, 100 numbered prisoners must find their own numbers in one of 100 drawers in order to survive. The rules state that each prisoner may open only 50 drawers and cannot communicate with other prisoners. At first glance, the situation appears hopeless, but a clever strategy offers the prisoners a realistic chance of survival.

Anna Gál and Peter Bro Miltersen first proposed the problem in 2003.



Each prisoner has to find their own number in one of 100 drawers, but may open only 50 of the drawers.

Problem [edit]

The 100 prisoners problem has different renditions in the literature. The following version is by Philippe Flajolet and Robert Sedgewick:[1]

> *The director of a prison offers 100 death row prisoners, who are numbered from 1 to 100, a last chance. A room contains a cupboard with 100 drawers. The director randomly puts one prisoner's number in each closed drawer. The prisoners enter the room, one after another. Each prisoner may open and look into 50 drawers in any order. The drawers are closed again afterwards. If, during this search, every prisoner finds their number in one of the drawers, all prisoners are pardoned. If even one prisoner does not find their number, all prisoners die. Before the first prisoner enters the room, the prisoners may discuss strategy — but may not communicate once the first prisoner enters to look in the drawers. What is the prisoners' best strategy?*

If every prisoner selects 50 drawers independently and randomly, the probability that a single prisoner finds their number is 50%. The probability that all prisoners find their numbers is the product of the single probabilities, which is $(\frac{1}{2})^{100} \approx 0.000\,000\,000\,000\,000\,000\,000\,000\,000\,0008$, a vanishingly small number. The situation appears hopeless.

https://en.wikipedia.org/wiki/100_prisoners_problem

$1 \to 7 \to 88 \to 13 \to 1$ found it!

$2 \to 3 \to 4 \to 5 \to 6 \to 88 \to 89 \to 90 \to \dots$

eventually returns to 2

ok if cycle length is ≤ 50

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix} = \begin{pmatrix} i_1 & i_2 & \cdots & i_k \\ a_{i_1} & a_{i_2} & \cdots & a_{i_k} \end{pmatrix} \begin{pmatrix} i_{k+1} & \cdots & i_{k+l} \\ a_{i_{k+1}} & \cdots & a_{i_{k+l}} \end{pmatrix} \cdots$$

as long as $\pi = \sigma_1 \sigma_2 \cdots \sigma_r$ has each σ of length ≤ 50, ok.

at most one cycle of length > 50 (or $> \frac{n}{2}$)

What is the prob have no cycles of length > 50 or $\frac{n}{2}$?

Find the prob have a cycle of length $> n/2$: so $\frac{n}{2} < l \le n$

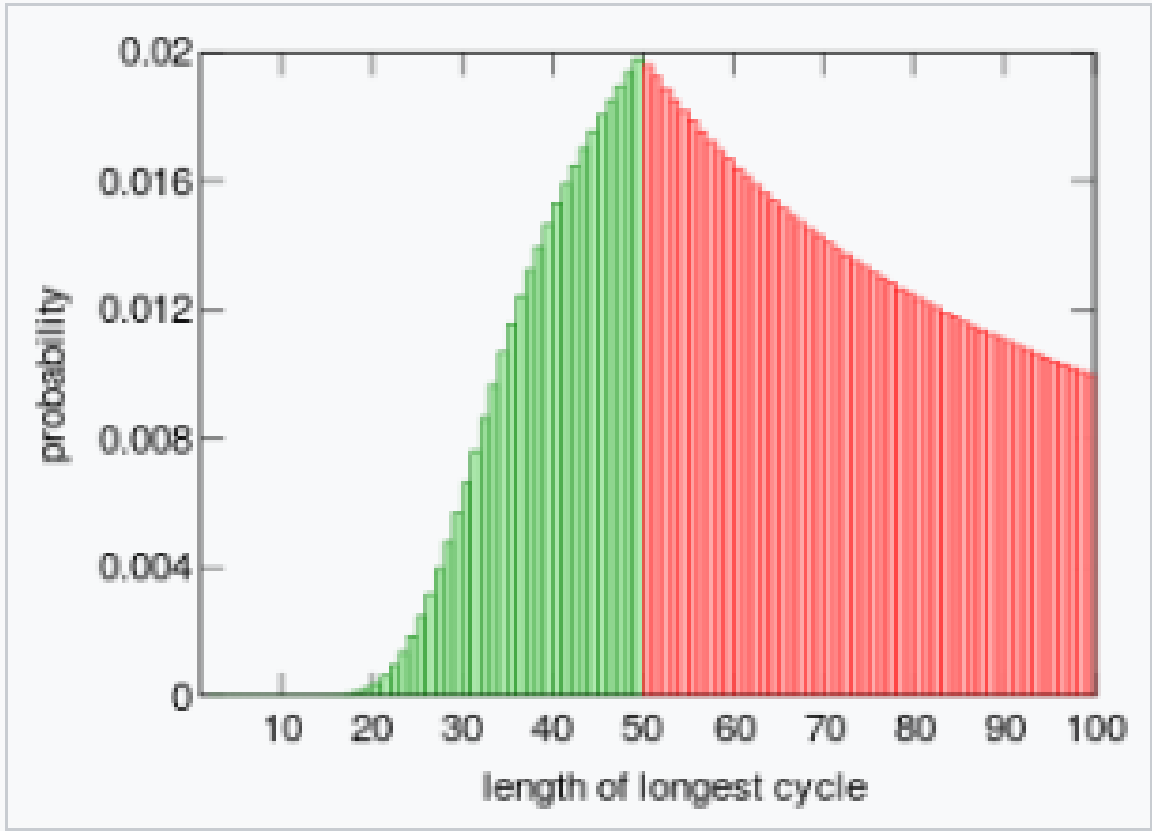
$\frac{1}{n!}$ # of perm of n objects $\begin{cases} \binom{n}{l} & \text{\# ways to choose } l \text{ numbers for our cycle} \\ (l-1)! & \text{lose one in ordering as can always make one number first} \end{cases}$

$(n-l)!$ # ways to order the remaining $n-l$ numbers $= \frac{1}{n!} \frac{n!}{l!(n-l)!} (l-1)!(n-l)! = \frac{1}{l}$

So Prob have a cycle of length $> n/2$ is $\sum_{l=\frac{n}{2}+1}^{n} \frac{1}{l} = H_n - H_{\frac{n}{2}}$

Harmonic Numbers: $H_k = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k}$

$$\sum_{l=\frac{n}{2}+1}^{n} \frac{1}{l} = \sum_{l=1}^{n} \frac{1}{l} - \sum_{l=1}^{\frac{n}{2}} \frac{1}{l} = H_n - H_{\frac{n}{2}} \approx \log n - \log \frac{n}{2} = \log 2$$



Probability distribution of the length of the longest cycle of a random permutation of the numbers 1 to 100. The green area corresponds to the survival probability of the prisoners.

https://en.wikipedia.org/wiki/Euler%27s_constant

Euler's constant (sometimes called the **Euler–Mascheroni constant**) is a mathematical constant, usually denoted by the lowercase Greek letter gamma (γ), defined as the limiting difference between the harmonic series and the natural logarithm, denoted here by log:

$$\gamma = \lim_{n\to\infty}\left(-\log n + \sum_{k=1}^{n}\frac{1}{k}\right)$$
$$= \int_1^\infty \left(-\frac{1}{x} + \frac{1}{\lfloor x\rfloor}\right) dx.$$

$\sum_{k=1}^{n} \frac{1}{k} = \log n + \gamma + \text{lower order}$

Here, $\lfloor\cdot\rfloor$ represents the floor function.

The numerical value of Euler's constant, to 50 decimal places, is:[1]

0.57721 56649 01532 86060 65120 90082 40243 10421 59335 93992 ...

$H_n - H_{n/2} = (\log n + \gamma + \text{lower}) - (\log \frac{n}{2} + \gamma + \text{lower})$

$= \log 2 + \text{lower}$

https://en.wikipedia.org/wiki/Abelian_group#Finite_abelian_groups

The **fundamental theorem of finite abelian groups** states that every finite abelian group G can be expressed as the direct sum of cyclic subgroups of prime-power order; it is also known as the **basis theorem for finite abelian groups**. Moreover, automorphism groups of cyclic groups are examples of abelian groups.[13] This is generalized by the fundamental theorem of finitely generated abelian groups, with finite groups being the special case when G has zero rank; this in turn admits numerous further generalizations.

The classification was proven by Leopold Kronecker in 1870, though it was not stated in modern group-theoretic terms until later, and was preceded by a similar classification of quadratic forms by Carl Friedrich Gauss in 1801; see history for details.

The cyclic group $\mathbb{Z}_{mn}$ of order mn is isomorphic to the direct sum of $\mathbb{Z}_m$ and $\mathbb{Z}_n$ if and only if m and n are coprime. It follows that any finite abelian group G is isomorphic to a direct sum of the form

$$\bigoplus_{i=1}^{u} \mathbb{Z}_{k_i}$$

in either of the following canonical ways:

- the numbers $k_1, k_2, \ldots, k_u$ are powers of (not necessarily distinct) primes,
- or k_1 divides k_2, which divides k_3, and so on up to k_u.

For example, $\mathbb{Z}_{15}$ can be expressed as the direct sum of two cyclic subgroups of order 3 and 5: $\mathbb{Z}_{15} \cong \{0, 5, 10\} \oplus \{0, 3, 6, 9, 12\}$. The same can be said for any abelian group of order 15, leading to the remarkable conclusion that all abelian groups of order 15 are isomorphic.

For another example, every abelian group of order 8 is isomorphic to either $\mathbb{Z}_8$ (the integers 0 to 7 under addition modulo 8), $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ (the odd integers 1 to 15 under multiplication modulo 16), or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

https://www.gcsu.edu/sites/files/page-assets/node-808/attachments/piro.pdf

The **direct sum** is an operation between structures in abstract algebra, a branch of mathematics. It is defined differently, but analogously, for different kinds of structures. As an example, the direct sum of two abelian groups A and B is another abelian group $A \oplus B$ consisting of the ordered pairs (a, b) where $a \in A$ and $b \in B$. To add ordered pairs, we define the sum $(a, b) + (c, d)$ to be $(a + c, b + d)$; in other words addition is defined coordinate-wise. For example, the direct sum $\mathbb{R} \oplus \mathbb{R}$, where $\mathbb{R}$ is real coordinate space, is the Cartesian plane, $\mathbb{R}^2$. A similar process can be used to form the direct sum of two vector spaces or two modules.

https://en.wikipedia.org/wiki/Direct_sum

$\langle a \rangle$ with $a^7 = 1$ $\quad \langle b \rangle = b^5 = 1$

$\{1, a, a^2, \ldots, a^6\}$ $\quad \{1, b, \ldots, b^4\}$

look at $\{a^n b^n : 0 \le n \le 6,\ 0 \le n \le 4\}$

$a^{n_1} b^{n_1} = a^{n_2} b^{n_2} \Rightarrow a^{n_1 - n_2} = b^{n_2 - n_1}$

$\text{ord}(a^k) = 7$ unless $k = 0$, $\quad \text{ord}(b^k) = 5$ unless $k = 0$

If $c^4 = 1$ then $\text{ord}(c) = 4$, $\text{ord}(c^2) = 2$, $\text{ord}(c^3) = 3$

As a, b have prime orders, so too do their powers, and $n_1 = n_2$, $n_1 = n_2$

Views $\{(ia, jb) : 0 \le i < 6$ here $7a = 0$ drop the a
$0 \le j \le 4\}$ $\quad 5b = 0$ $\quad (i, j)$

Rotman's *Introduction to the Theory of Groups* (theorem 6.9 on page 130) contains such a proof, attributed to Schenkman, but this proof is not exactly as I have outlined in the question.

Theorem 6.9 (Basis Theorem). *Every finite abelian group G is a direct sum of cyclic groups.*

***Proof* (E. Schenkman).** Choose n smallest such that G can be generated by a set with n elements. Among all generating sets $\{x_1, \ldots, x_n\}$ of size n, choose one containing an element x_1 of smallest order k; that is, no generating set of size n contains an element of order less than k. If $H = \langle x_2, \ldots, x_n \rangle$, then H is a proper subgroup of G (by the minimal choice of n), so that an induction on $|G|$ gives H a direct sum of cyclic groups. We claim that $G = \langle x_1 \rangle \oplus H$. It suffices to show that $\langle x_1 \rangle \cap H = 0$, for $\langle x_1 \rangle + H = \langle x_1, \ldots, x_n \rangle = G$. If $z \in \langle x_1 \rangle \cap H$ and $z \neq 0$, then $z = a_1 x_1 = \sum_{i=2}^{n} a_i x_i$, for $a_1, \ldots, a_n \in \mathbb{Z}$ and $0 < a_1 < k$. If d is the gcd of $a_1, \ldots, a_n$, define $g = -(a_1/d)x_1 + \sum_{i=2}^{n} (a_i/d)x_i$. Now the order of g is smaller than k, for $dg = 0$ and $d \leq a_1 < k$. But $a_1/d, \ldots, a_n/d$ are relatively prime, so that the lemma gives a generating set of G of size n one of whose elements is g; this contradicts the minimality of k. ∎

The book *The Theory of Finite Groups: An Introduction*, by Kurzweil and Stellmacher, does what I had in mind in Chapter 2.

***Proof* (E. Schenkman).** Choose n smallest such that G can be generated by a set with n elements. Among all generating sets $\{x_1, \ldots, x_n\}$ of size n, choose one containing an element x_1 of smallest order k; that is, no generating set of size n contains an element of order less than k. If $H = \langle x_2, \ldots, x_n \rangle$, then H is

G is finite, has $\sum_{l=1}^{\#G} \binom{\#G}{l}$ sum of the # of non-empty subsets of size l

G has $2^{\#G} - 1$ non-empty subsets, finite

Know G satisfies everything in G generated from this, so as we have at least one, can take one with fewest elements.

Only finitely many sets to check, can find one with smallest order

size n contains an element of order less than k. If $H = \langle x_2, \ldots, x_n \rangle$, then H is a proper subgroup of G (by the minimal choice of n), so that an induction on $|G|$ gives H a direct sum of cyclic groups. We claim that $G = \langle x_1 \rangle \oplus H$. It

Is H proper? Can x_1 be obtained from $x_2, \ldots, x_n$?

↳ If not, then $\{x_2, \ldots, x_n\}$ generate G and only $n-1$ objects.

Show H is a group.

As H is proper, by Induction it is a sum of cyclic groups.

$|G|$ gives H a direct sum of cyclic groups. We claim that $G = \langle x_1 \rangle \oplus H$. It suffices to show that $\langle x_1 \rangle \cap H = 0$, for $\langle x_1 \rangle + H = \langle x_1, \ldots, x_n \rangle = G$. If $z \in$

Clear $\langle x_1 \rangle \oplus H$ gives all of G as have $x_1, x_2, \ldots, x_n$

Want to show only element in common is 0.

$\langle x_1 \rangle \cap H$ and $z \neq 0$, then $z = a_1 x_1 = \sum_{i=2}^{n} a_i x_i$, for $a_1, \ldots, a_n \in \mathbb{Z}$ and $0 < a_1 < k$. If d is the gcd of $a_1, \ldots, a_n$, define $g = -(a_1/d)x_1 + \sum_{i=2}^{n} (a_i/d)x_i$. Now the order of g is smaller than k, for $dg = 0$ and $d \leq a_1 < k$. But $a_1/d, \ldots, a_n/d$ are relatively prime, so that the lemma gives a generating set of G of size n one of whose elements is a: this contradicts the minimality of k. ∎

$z \in \langle x_1 \rangle \cap H \Rightarrow z = a_1 x_1$ for $0 < a_1 < k$ and $z = \sum_{i=2}^{n} a_i x_i$

$d = \gcd(a_1, \ldots, a_n)$ $\quad z - z = 0 = -a_1 x_1 + \sum_{i=2}^{n} a_i x_i$ (*)

$0 = -(a_1/d) x_1 + \sum_{i=2}^{n} (a_i/d) x_i = g$

now coeffs are rel prime

Is $g = 0$? Know $dg = 0$ so g has order d.

If $d > 1$ then clearly $g \neq 0$. WHY? Make FALSE!

By the lemma, $g, x_2, \ldots, x_n$ generate G as $x_1, \ldots, x_n$ generate G and $o(g) = d < k$ so contradicts minimality of the order of x_1.

https://math.stackexchange.com/questions/3251882/how-to-complete-a-primitive-vector-to-a-unimodular-matrix

2 x 2 Matrices:

$\begin{pmatrix} 3 & 1 \\ 4 & 1 \end{pmatrix}$ det -1 $\quad$ $\begin{pmatrix} 3 & -2 \\ 4 & 3 \end{pmatrix}$ det 1

$\begin{pmatrix} x & -b \\ y & a \end{pmatrix}$ det 1 $\quad$ $\gcd(x,y)=1 \Rightarrow \exists\, a,b$ s.t. $ax+by=1$

all these matrices have inverses with integer entries

How we go from integer-span of x_1, x_2 same as that of g, x_2

$(a\ b\ c)\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ ~~$\begin{matrix} g \\ t \end{matrix}$~~

$\gcd(x,y,z)=1 \Rightarrow \exists\, a,b,c$ s.t.

$ax+by+cz=1$

Extended Euclidean Algorithm (Groups)

Let $x = x_1$ be the given integer vector. We look for $2n-1$ integer vectors $x_2, \ldots, x_n, y_1, \ldots, y_n$ such that

$$Y^T X = \begin{pmatrix} y_1^T \\ y_2^T \\ \vdots \\ y_n^T \end{pmatrix} \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} = \begin{pmatrix} 1 & * & \cdots & * \\ & 1 & \ddots & \vdots \\ & & \ddots & * \\ \bigcirc & & & 1 \end{pmatrix}.$$

Since both X and Y have integer determinants and $\det(Y)\det(X) = \det(Y^T X) = 1$, if X and Y do exist, we must have $\det(X) = \pm 1$.

$X\vec{u} = \vec{v} \iff X^{-1}\vec{v} = \vec{u}$

For us $X_1 = g$, and know how to find y_1 (Euclidean Alg)

We can construct the columns of X and Y by mathematical induction. In the base case, we pick an y_1 such that $y_1^T x_1 = 1$. This is possible because the GCD of the entries of $x_1 = x$ are coprime.

In the inductive step, suppose $1 \leq k < n$ and $x_1, \ldots, x_k, y_1, \ldots, y_k$ are such that $y_i^T x_i = 1$ for each $i \leq k$ and $y_i^T x_j = 0$ whenever $j < i \leq k$. Since the rank of $A = \begin{pmatrix} x_1 & \cdots & x_k \end{pmatrix}$ is smaller than n, the equation $y_{k+1}^T A = 0$ has a nontrivial solution $y_{k+1} \in \mathbb{Q}^n$. By rationalising the denominators in its entries, y_{k+1} can be chosen as an integer vector. Then by pulling out common factors in its entries, y_{k+1} can be chosen to be primitive. Thus there exists an integer vector x_{k+1} such that $y_{k+1}^T x_{k+1} = 1$ and our proof is complete.

$y_k^T A = 0$

Clear denominators

pull at common factors

https://en.wikipedia.org/wiki/Classical_group

Name	Group	Field	Form	Maximal compact subgroup	Lie algebra	Root system
Special linear	$\mathrm{SL}(n, \mathbf{R})$	$\mathbf{R}$	—	$\mathrm{SO}(n)$		
Complex special linear	$\mathrm{SL}(n, \mathbf{C})$	$\mathbf{C}$	—	$\mathbf{SU}(\boldsymbol{n})$	Complex	A_m, $n = m + 1$
Quaternionic special linear	$\mathrm{SL}(n, \mathbf{H}) = \mathrm{SU}^*(2n)$	$\mathbf{H}$	—	$\mathrm{Sp}(n)$		
(Indefinite) special orthogonal	$\mathrm{SO}(p, q)$	$\mathbf{R}$	Symmetric	$\mathrm{S}(\mathrm{O}(p) \times \mathrm{O}(q))$		
Complex special orthogonal	$\mathrm{SO}(n, \mathbf{C})$	$\mathbf{C}$	Symmetric	$\mathbf{SO}(\boldsymbol{n})$	Complex	$\begin{cases} B_m, & n = 2m + 1 \\ D_m, & n = 2m \end{cases}$
Symplectic	$\mathrm{Sp}(n, \mathbf{R})$	$\mathbf{R}$	Skew-symmetric	$\mathrm{U}(n)$		
Complex symplectic	$\mathrm{Sp}(n, \mathbf{C})$	$\mathbf{C}$	Skew-symmetric	$\mathbf{Sp}(\boldsymbol{n})$	Complex	C_m, $n = 2m$
(Indefinite) special unitary	$\mathrm{SU}(p, q)$	$\mathbf{C}$	Hermitian	$\mathrm{S}(\mathrm{U}(p) \times \mathrm{U}(q))$		
(Indefinite) quaternionic unitary	$\mathrm{Sp}(p, q)$	$\mathbf{H}$	Hermitian	$\mathrm{Sp}(p) \times \mathrm{Sp}(q)$		
Quaternionic orthogonal	$\mathrm{SO}^*(2n)$	$\mathbf{H}$	Skew-Hermitian	$\mathrm{SO}(2n)$		

https://en.wikipedia.org/wiki/Classical_group

Name	Group	Field	Form	Maximal compact subgroup	Lie algebra	Root system
Special linear	$\mathrm{SL}(n, \mathbf{R})$	$\mathbf{R}$	—	$\mathrm{SO}(n)$		
Complex special linear	$\mathrm{SL}(n, \mathbf{C})$	$\mathbf{C}$	—	$\mathbf{SU}(\boldsymbol{n})$	Complex	A_m, $n = m + 1$
Quaternionic special linear	$\mathrm{SL}(n, \mathbf{H}) = \mathrm{SU}^*(2n)$	$\mathbf{H}$	—	$\mathrm{Sp}(n)$		
(Indefinite) special orthogonal	$\mathrm{SO}(p, q)$	$\mathbf{R}$	Symmetric	$\mathrm{S}(\mathrm{O}(p) \times \mathrm{O}(q))$		
Complex special orthogonal	$\mathrm{SO}(n, \mathbf{C})$	$\mathbf{C}$	Symmetric	$\mathbf{SO}(\boldsymbol{n})$	Complex	$\begin{cases} B_m, & n = 2m + 1 \\ D_m, & n = 2m \end{cases}$
Symplectic	$\mathrm{Sp}(n, \mathbf{R})$	$\mathbf{R}$	Skew-symmetric	$\mathrm{U}(n)$		
Complex symplectic	$\mathrm{Sp}(n, \mathbf{C})$	$\mathbf{C}$	Skew-symmetric	$\mathbf{Sp}(\boldsymbol{n})$	Complex	C_m, $n = 2m$
(Indefinite) special unitary	$\mathrm{SU}(p, q)$	$\mathbf{C}$	Hermitian	$\mathrm{S}(\mathrm{U}(p) \times \mathrm{U}(q))$		
(Indefinite) quaternionic unitary	$\mathrm{Sp}(p, q)$	$\mathbf{H}$	Hermitian	$\mathrm{Sp}(p) \times \mathrm{Sp}(q)$		
Quaternionic orthogonal	$\mathrm{SO}^*(2n)$	$\mathbf{H}$	Skew-Hermitian	$\mathrm{SO}(2n)$		

Math 355: Abstract Algebra: Spring '24 (Williams)

Professor Steven J Miller: sjm1@williams.edu

Homepage:
https://web.williams.edu/Mathematics/sjmiller/public_html/355Sp24/

Section 1:

Lecture 24: 5/7/24: https://youtu.be/3HlcmFZEpE4

Special Topics: Group Theory and Linear Algebra

https://en.wikipedia.org/wiki/Baker%E2%80%93Campbell%E2%80%93Hausdorff_formula

Baker–Campbell–Hausdorff formula

8 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

In mathematics, the **Baker–Campbell–Hausdorff formula** gives the value of Z that solves the equation

$$e^X e^Y = e^Z$$

for possibly noncommutative X and Y in the Lie algebra of a Lie group. There are various ways of writing the formula, but all ultimately yield an expression for Z in Lie algebraic terms, that is, as a formal series (not necessarily convergent) in X and Y and iterated commutators thereof. The first few terms of this series are:

If real #s, Then $Z = X + Y$

If Matrices, maybe $Z = X + Y$ if X, Y "nice to each other" commute?

1) What does e^X mean if X is a matrix?

2) Define commutator: $[X, Y] = XY - YX$: "measures" how far from commuting

Why do we care? Discrete Logarithm Problem

$(\mathbb{Z}/p\mathbb{Z})^*$

$x^7 \cdot x^8 = x^{15}$: imagine just given x and $y = x^n$:
Can you find the exponent n? $n = \frac{\log y}{\log x}$

Consider some group generated by g, so $g^v = 1$

Know g and g^n find n

Ex. Maybe g generates $(\mathbb{Z}/p\mathbb{Z})^*$ (cyclic group) for some prime $p \approx 10^{400}$

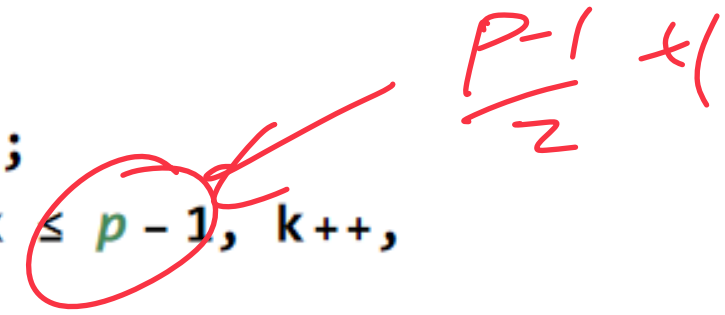
$y = g^n \bmod p$: cannot use real logarithm

Alice	Bob	Charlie/Eve
g	g	g
Secret a	Secret b	
Shouts g^a	Shouts g^b	g^a, g^b
Heard g^b	Heard g^a	
Computes $(g^b)^a$	Computes $(g^a)^b$	
$= g^{ab}$	$= g^{ab}$	

use fast exponentiation

write ab in binary

```
generatorzmodpzstar[p_] := Module[{},
  isgenerator = {};
  For[n = 2, n ≤ p - 1, n++,
   {
    list = {};
    current = 1;
    For[k = 1, k ≤ p - 1, k++,
     {{
       current = Mod[current * n, p];
       If[MemberQ[list, current] == True, k = p + 1, list = AppendTo[list, current];
        (* exit loop if true as not generator *)
       ]; (* end of if statement *)
     }}]; (* end of k loop \*)
    If[Length[list] == p - 1, isgenerator = AppendTo[isgenerator, n]];
   }]; (* end of n loop *)
  Print[isgenerator];
 ]
```



```
Timing[generatorzmodpzstar[NextPrime[2024]]]
```

```
{2, 5, 6, 7, 8, 11, 15, 18, 20, 21, 23, 24, 26, 28, 29, 32, 33, 34, 37, 38, 43, 44, 45, 47, 50, 54, 59, 60, 62, 63, 65, 67, 69, 70, 72, 73, 78, 79, 80, 82, 84, 85, 87, 91,
 92, 95, 96, 97, 98, 99, 101, 102, 104, 106, 107, 109, 110, 111, 112, 114, 116, 119, 122, 125, 127, 128, 129, 131, 132, 133, 135, 136, 139, 141, 142, 143, 148,
 149, 150, 151, 152, 154, 155, 162, 163, 166, 172, 175, 176, 177, 178, 180, 186, 187, 188, 189, 191, 195, 197, 200, 201, 205, 206, 207, 209, 210, 216, 217,
 219, 226, 229, 230, 233, 234, 236, 237, 240, 241, 242, 245, 246, 248, 252, 255, 260, 261, 263, 265, 268, 273, 274, 275, 276, 280, 281, 285, 287, 288, 290,
 291, 292, 294, 297, 299, 303, 305, 306, 312, 313, 314, 316, 317, 318, 320, 321, 322, 327, 328, 330, 333, 334, 336, 337, 338, 340, 341, 342, 343, 346, 347,
 348, 355, 357, 358, 362, 364, 366, 368, 370, 371, 373, 375, 377, 379, 380, 381, 383, 384, 385, 386, 387, 388, 389, 391, 392, 393, 396, 398, 399, 404, 405,
 406, 408, 415, 416, 417, 419, 422, 423, 424, 426, 427, 428, 429, 430, 433, 436, 437, 439, 440, 442, 444, 445, 446, 447, 448, 449, 450, 451, 453, 454, 456,
 457, 461, 462, 464, 465, 467, 470, 476, 478, 481, 486, 488, 489, 493, 494, 497, 498, 499, 500, 502, 506, 508, 512, 514, 515, 516, 518, 523, 524, 525, 528,
 531, 532, 534, 538, 539, 540, 542, 544, 551, 554, 556, 557, 558, 559, 561, 564, 565, 566, 567, 568, 572, 573, 575, 577, 578, 581, 583, 585, 586, 587, 590,
 591, 592, 596, 600, 601, 602, 603, 604, 605, 608, 611, 614, 615, 616, 618, 619, 620, 621, 622, 623, 627, 629, 630, 631, 638, 646, 647, 648, 650, 651, 652,
 653, 657, 658, 662, 664, 670, 671, 678, 685, 687, 688, 690, 698, 699, 700, 702, 703, 704, 706, 708, 711, 712, 713, 718, 720, 721, 722, 723, 725, 726, 727,
 730, 731, 733, 734, 735, 738, 744, 748, 751, 752, 756, 764, 765, 767, 769, 773, 780, 781, 783, 785, 787, 788, 789, 790, 791, 794, 795, 797, 799, 800, 802,
 804, 805, 806, 811, 814, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 835, 836, 840, 842, 843, 845, 847, 850, 853, 855, 857, 861, 862, 864,
 865, 868, 870, 871, 873, 876, 877, 881, 882, 883, 886, 891, 893, 895, 897, 899, 904, 905, 909, 910, 911, 913, 915, 916, 918, 919, 920, 925, 926, 932, 936,
 938, 939, 942, 943, 944, 946, 947, 948, 949, 950, 951, 954, 958, 959, 960, 963, 964, 965, 966, 968, 970, 971, 974, 977, 979, 980, 981, 982, 984, 990, 991,
 992, 995, 997, 999, 1002, 1003, 1006, 1008, 1010, 1011, 1014, 1015, 1018, 1020, 1022, 1023, 1026, 1027, 1029, 1031, 1033, 1034, 1038, 1039, 1040, 1041,
 1042, 1044, 1049, 1051, 1052, 1054, 1055, 1058, 1060, 1065, 1066, 1070, 1071, 1072, 1074, 1075, 1082, 1086, 1087, 1090, 1092, 1093, 1094, 1096, 1097, 1098,
 1099, 1100, 1103, 1104, 1105, 1106, 1110, 1113, 1115, 1119, 1120, 1121, 1124, 1125, 1126, 1127, 1129, 1131, 1133, 1135, 1137, 1138, 1139, 1140, 1142, 1143,
 1147, 1148, 1149, 1152, 1153, 1155, 1158, 1160, 1161, 1164, 1167, 1168, 1169, 1171, 1173, 1175, 1176, 1178, 1179, 1181, 1183, 1186, 1188, 1189, 1190, 1193,
 1194, 1195, 1196, 1197, 1198, 1211, 1212, 1214, 1215, 1217, 1218, 1219, 1220, 1224, 1226, 1229, 1231, 1234, 1235, 1241, 1243, 1245, 1248, 1249, 1250, 1251,
 1252, 1253, 1255, 1256, 1257, 1259, 1261, 1264, 1265, 1266, 1267, 1268, 1269, 1270, 1272, 1273, 1274, 1277, 1278, 1280, 1281, 1282, 1284, 1285, 1286, 1287,
 1288, 1290, 1291, 1295, 1298, 1299, 1303, 1308, 1310, 1311, 1312, 1313, 1317, 1318, 1320, 1322, 1326, 1330, 1331, 1332, 1333, 1334, 1335, 1336, 1338, 1341,
 1343, 1344, 1345, 1346, 1347, 1348, 1350, 1351, 1352, 1353, 1354, 1355, 1358, 1359, 1360, 1361, 1362, 1364, 1366, 1367, 1368, 1371, 1372, 1373, 1378,
 1382, 1383, 1384, 1385, 1386, 1387, 1388, 1390, 1391, 1392, 1393, 1394, 1395, 1399, 1401, 1402, 1403, 1410, 1414, 1415, 1417, 1418, 1420, 1421, 1428,
 1429, 1430, 1432, 1433, 1434, 1438, 1439, 1443, 1445, 1447, 1448, 1451, 1453, 1456, 1457, 1458, 1464, 1465, 1467, 1472, 1474, 1475, 1477, 1478, 1479,
 1480, 1481, 1482, 1484, 1486, 1490, 1491, 1492, 1494, 1497, 1498, 1500, 1501, 1505, 1506, 1507, 1508, 1510, 1514, 1516, 1517, 1518, 1520, 1522, 1523,
 1524, 1526, 1531, 1532, 1535, 1536, 1537, 1540, 1542, 1543, 1544, 1545, 1547, 1548, 1550, 1552, 1553, 1554, 1555, 1556, 1558, 1559, 1561, 1564, 1567,
 1568, 1569, 1572, 1575, 1584, 1586, 1589, 1592, 1593, 1595, 1596, 1602, 1606, 1607, 1609, 1613, 1614, 1615, 1616, 1617, 1618, 1620, 1624, 1625, 1626,
 1627, 1630, 1632, 1633, 1637, 1645, 1649, 1651, 1653, 1655, 1658, 1660, 1662, 1664, 1666, 1667, 1668, 1671, 1673, 1674, 1675, 1676, 1677, 1678, 1682,
 1683, 1688, 1692, 1695, 1696, 1698, 1701, 1702, 1703, 1704, 1708, 1712, 1716, 1717, 1718, 1719, 1720, 1723, 1725, 1726, 1727, 1729, 1731, 1732, 1734,
 1738, 1741, 1743, 1744, 1745, 1748, 1749, 1750, 1755, 1756, 1757, 1758, 1760, 1761, 1763, 1765, 1768, 1769, 1770, 1771, 1773, 1774, 1776, 1777, 1778,
 1780, 1783, 1784, 1788, 1789, 1792, 1795, 1796, 1799, 1800, 1802, 1803, 1804, 1805, 1806, 1807, 1809, 1812, 1813, 1814, 1815, 1816, 1819, 1823, 1824,
 1825, 1828, 1829, 1831, 1833, 1834, 1835, 1837, 1842, 1843, 1844, 1845, 1846, 1848, 1853, 1854, 1856, 1857, 1858, 1859, 1860, 1862, 1863, 1866, 1867,
 1868, 1869, 1870, 1871, 1874, 1880, 1881, 1882, 1883, 1887, 1889, 1890, 1893, 1897, 1901, 1903, 1904, 1906, 1907, 1909, 1910, 1912, 1914, 1919, 1922,
 1924, 1927, 1933, 1934, 1937, 1938, 1939, 1941, 1944, 1946, 1950, 1951, 1952, 1953, 1956, 1959, 1961, 1963, 1966, 1969, 1970, 1971, 1972, 1974, 1975,
 1976, 1978, 1979, 1981, 1985, 1986, 1987, 1988, 1991, 1992, 1996, 1997, 2000, 2002, 2005, 2008, 2010, 2011, 2013, 2014, 2015, 2017, 2018, 2023, 2024}

{34.7969, Null}
```

```
generatorzmodpzstar[7]
```

```
{3, 5}
```

```
powers[p_, n_] := Module[{},
   list = {}; current = 1;
   For[k = 1, k ≤ p - 1, k++,
    {
     current = Mod[current * n, p];
     list = AppendTo[list, current];
    }];
   Print[list];
  ];
```

```
powers[7, 3]
```

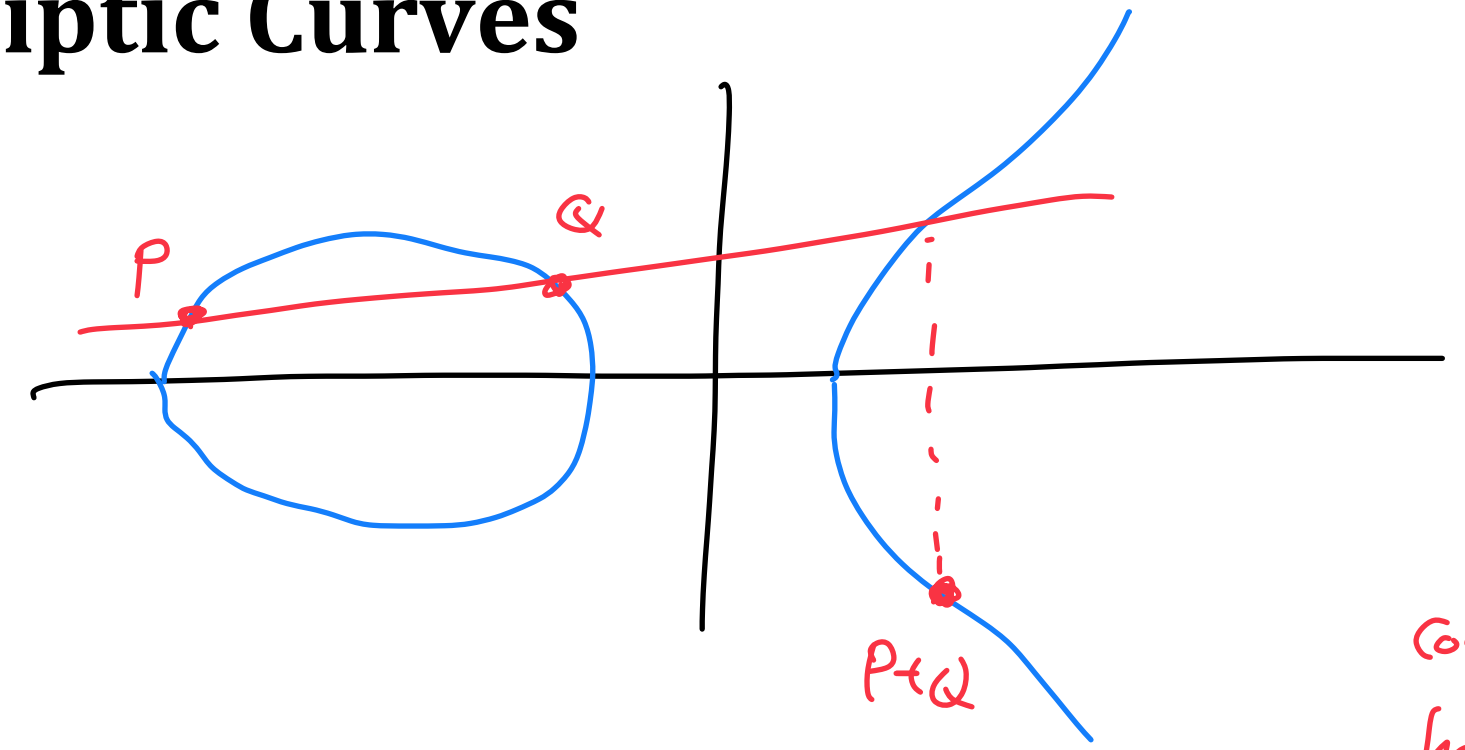
```
{3, 2, 6, 4, 5, 1}
```

```
powers[7, 4]
```

```
{4, 2, 1, 4, 2, 1}
```

Why do we care? Discrete Logarithm Problem

Elliptic Curves



Alice	Bob	Charlie / Eve
a	b	
P	P	P
compute P^a	P^b	P^a, P^b
hear P^b	P^a	
compute $(P^b)^a$	compute $(P^a)^b$	

Exponentials and Matrix Exponentials

$$e^x = 1 + x + x^2/2! + x^3/3! + \cdots = \sum_{n=0}^{\infty} x^n/n! = \exp(x)$$

$$e^x e^y = \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{m=0}^{\infty} \frac{y^m}{m!}$$

collect all terms $x^n y^m$ s.t. $n+m=k$ so if $n=l$ then $m=k-l$

$$= \sum_{k=0}^{\infty} \sum_{l=0}^{k} \frac{x^l y^{k-l}}{l!\,(k-l)!} \frac{k!}{k!}$$

$$= \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{l=0}^{k} \binom{k}{l} x^l y^{k-l} \longrightarrow (x+y)^k \quad \text{Binomial thm}$$

$$= \sum_{k=0}^{\infty} \frac{(x+y)^k}{k!} = e^{x+y}$$

∎

$e^X e^Y$ matrices...?

$$e^X = I + X + \frac{1}{2!}X^2 + \frac{1}{3!}X^3 + \dots$$

If X is a square matrix, can do!

converges for all X.

A is real symmetric $\exists$ orthog Q ($QQ^T = Q^TQ = I$) diag Λ s.t. $A = Q\Lambda Q^T$

$$e^A = e^{Q\Lambda Q^T} = I + \underbrace{QQ^T}_{I} + Q\Lambda Q^T + \frac{1}{2}\underbrace{Q\Lambda Q^T Q}_{Q\Lambda^2 Q^T}\Lambda Q^T + \dots$$

$$e^A = e^{Q\Lambda Q^T} = Q e^{\Lambda} Q^T = Q \begin{pmatrix} e^{\lambda_1} & & \\ & \ddots & \\ & & e^{\lambda_n} \end{pmatrix} Q^T$$

A, B commute:

$$e^A e^B = \sum \frac{A^n}{n!} \sum \frac{B^m}{m!}$$

$$= \sum \sum \frac{A^n B^m}{n!\, m!}$$

$$= \sum_k \frac{1}{k!} \underbrace{\sum_{l=0}^{k} \binom{k}{l} A^l B^{k-l}}_{(A+B)^k \text{ as } A, B \text{ commute}} = e^{A+B}$$

https://en.wikipedia.org/wiki/Baker%E2%80%93Campbell%E2%80%93Hausdorff_formula

Baker–Campbell–Hausdorff formula

8 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

In mathematics, the **Baker–Campbell–Hausdorff formula** gives the value of Z that solves the equation

$$e^X e^Y = e^Z$$

for possibly noncommutative X and Y in the Lie algebra of a Lie group. There are various ways of writing the formula, but all ultimately yield an expression for Z in Lie algebraic terms, that is, as a formal series (not necessarily convergent) in X and Y and iterated commutators thereof. The first few terms of this series are:

$$Z = X + Y + \frac{1}{2}[X,Y] + \frac{1}{12}[X,[X,Y]] - \frac{1}{12}[Y,[X,Y]] + \cdots,$$

where "$\cdots$" indicates terms involving higher commutators of X and Y. If X and Y are sufficiently small elements of the Lie algebra $\mathfrak{g}$ of a Lie group G, the series is convergent. Meanwhile, every element g sufficiently close to the identity in G can be expressed as $g = e^X$ for a small X in $\mathfrak{g}$. Thus, we can say that *near the identity* the group multiplication in G—written as $e^X e^Y = e^Z$—can be expressed in purely Lie algebraic terms. The Baker–Campbell–Hausdorff formula can be used to give comparatively simple proofs of deep results in the Lie group–Lie algebra correspondence.

If X and Y are sufficiently small $n \times n$ matrices, then Z can be computed as the logarithm of $e^X e^Y$, where the exponentials and the logarithm can be computed as power series. The point of the Baker–Campbell–Hausdorff formula is then the highly nonobvious claim that $Z := \log\left(e^X e^Y\right)$ can be expressed as a series in repeated commutators of X and Y.

https://en.wikipedia.org/wiki/Lie_algebra

https://en.wikipedia.org/wiki/Lie_group

https://en.wikipedia.org/wiki/Discrete_logarithm

Lie

say Lee

Real Simple Lie Algebras

https://en.wikipedia.org/wiki/Classical_group

Name	Group	Field	Form	Maximal compact subgroup	Lie algebra	Root system
Special linear	$\mathrm{SL}(n, \mathbf{R})$	$\mathbf{R}$	—	$\mathrm{SO}(n)$		
Complex special linear	$\mathrm{SL}(n, \mathbf{C})$	$\mathbf{C}$	—	$\mathbf{SU}(\boldsymbol{n})$	Complex	A_m, $n = m + 1$
Quaternionic special linear	$\mathrm{SL}(n, \mathbf{H}) = \mathrm{SU}^*(2n)$	$\mathbf{H}$	—	$\mathrm{Sp}(n)$		
(Indefinite) special orthogonal	$\mathrm{SO}(p, q)$	$\mathbf{R}$	Symmetric	$\mathrm{S}(\mathrm{O}(p) \times \mathrm{O}(q))$		
Complex special orthogonal	$\mathrm{SO}(n, \mathbf{C})$	$\mathbf{C}$	Symmetric	$\mathbf{SO}(\boldsymbol{n})$	Complex	$\begin{cases} B_m, & n = 2m + 1 \\ D_m, & n = 2m \end{cases}$
Symplectic	$\mathrm{Sp}(n, \mathbf{R})$	$\mathbf{R}$	Skew-symmetric	$\mathrm{U}(n)$		
Complex symplectic	$\mathrm{Sp}(n, \mathbf{C})$	$\mathbf{C}$	Skew-symmetric	$\mathbf{Sp}(\boldsymbol{n})$	Complex	C_m, $n = 2m$
(Indefinite) special unitary	$\mathrm{SU}(p, q)$	$\mathbf{C}$	Hermitian	$\mathrm{S}(\mathrm{U}(p) \times \mathrm{U}(q))$		
(Indefinite) quaternionic unitary	$\mathrm{Sp}(p, q)$	$\mathbf{H}$	Hermitian	$\mathrm{Sp}(p) \times \mathrm{Sp}(q)$		
Quaternionic orthogonal	$\mathrm{SO}^*(2n)$	$\mathbf{H}$	Skew-Hermitian	$\mathrm{SO}(2n)$		

Real Sym: $A = A^T$ entries real $\longrightarrow$ $\lambda \in \mathbb{R}$

Orthog: $Q^T Q = Q Q^T = I$, entries real $\longrightarrow$ $|\lambda| = 1$

Unitary: $U^H U = U U^H = I$ $\longrightarrow$ $|\lambda| = 1$

H = complex conjugate transpose

$$A = \begin{pmatrix} 2+3i & 4-i \\ 6+2i & 7 \end{pmatrix} \quad A^H = \begin{pmatrix} 2-3i & 6-2i \\ 4+i & 7 \end{pmatrix}$$

Complex Hermitian: $A = A^H$ $\longrightarrow$ $\lambda \in \mathbb{R}$

$\vec{v}$ is an eigenvector with eigenvalue λ of A if $\vec{v} \neq \vec{0}$ and $A\vec{v} = \lambda \vec{v}$.

Thm: U unitary then if $U\vec{v} = \lambda\vec{v}$ have $|\lambda| = 1$

Proof $\vec{v}^H\vec{v} = 1$ normalizing my eigenvector to have length 1.

$$(1\ \ i)\begin{pmatrix}1\\ i\end{pmatrix} = 1^2 + i^2 = 0 \qquad (1\ \ -i)\begin{pmatrix}1\\ i\end{pmatrix} = 1^2 - i^2 = 2$$

As U unitary, $U^HU = I$ so $\vec{v}^H\vec{v} = 1$

Same as $\vec{v}^H U^H U\vec{v} = 1$

$$= (U\vec{v})^H(U\vec{v}) = (\lambda\vec{v})^H(\lambda\vec{v})$$

$$= \bar{\lambda}\vec{v}^H\lambda\vec{v} = \lambda\bar{\lambda}\,\vec{v}^H\vec{v} = |\lambda|^2$$

Orthogonal Rotation:

$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ rotates by 90°

$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} -i \\ 1 \end{pmatrix} = -i\begin{pmatrix} 1 \\ i \end{pmatrix}$ So $-i$ eigenvalue with $\begin{pmatrix} 1 \\ i \end{pmatrix}$ eigenvector