Welcome to Math 221B

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, you may turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: 11.1–11.2.
- Reading for Mon Jan 31: 11.3.
- COVID Safety HW and PS00 due Mon Jan 31.
- PS01 due Mon Feb 07.
- First problem session Fri Feb 04, 10:00–noon on Zoom.

Tour of the course website

The course website is:

`http://www.timhsu.net/courses/221b/`

Important: WE ARE COMING BACK

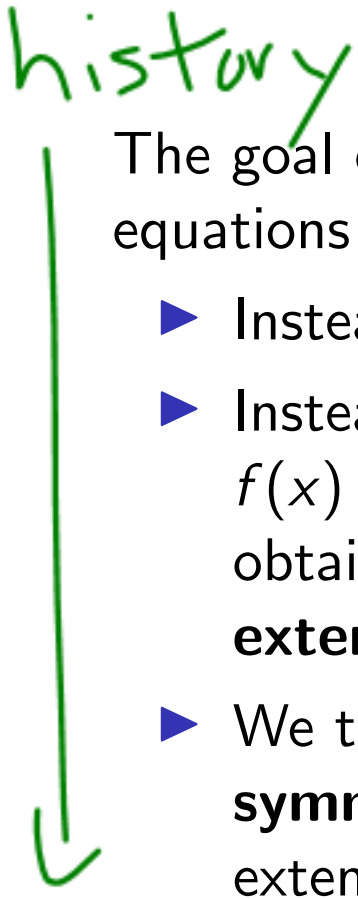
(see today's COVID stats for the Bay Area)

So the important thing to know is:

WE WILL BE BACK HOLDING CLASS IN PERSON ON MON FEB 14

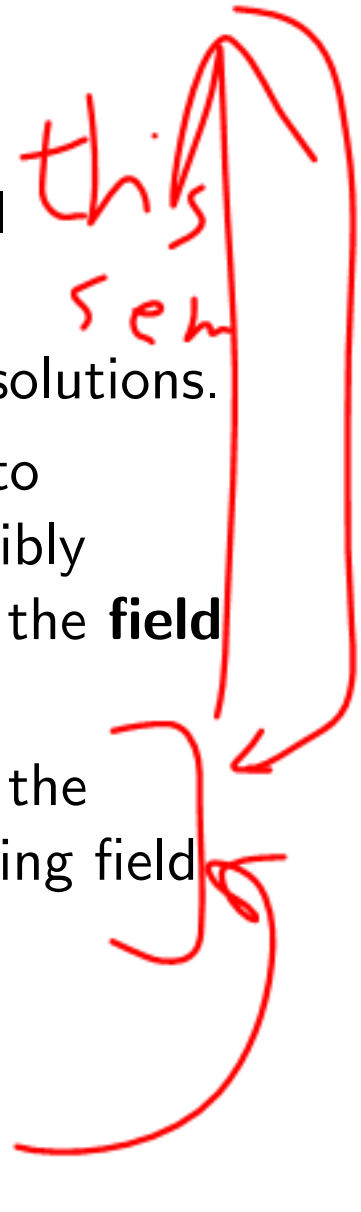
I would bet $50 on it!

The goal of this course



The goal of this course is to learn how to solve polynomial equations $f(x) = 0$. (High school math!) Except:

- Instead of just looking at one solution, we look at all solutions.
- Instead of just looking at the finitely many solutions to $f(x) = 0$, we look at all numbers that you could possibly obtain from combinations of those solutions. (This is the **field extension** corresponding to those solutions.)
- We then characterize solutions qualitatively based on the **symmetries** of the solution set (i.e., their corresponding field extension).



Definition of a ring

Think: A ring is an abstract version of a "system of numbers".
ring (Artin) = commutative ring w/ unity (elsewhere)

Definition: A ring is a set R with two binary operations $+$ (addition) and $\cdot$ (multiplication) such that:

- $(R, +)$ is an abelian group, with identity 0;
- Multiplication is commutative and associative, with identity 1; and
- **Distributive law:** For all $a, b, c \in R$, we have

$$a(b + c) = ab + ac.$$

in Artin

Two features that may differ from the definition of ring as you have seen it before: In this course, a ring must be **commutative** and have a **multiplicative identity**.

ring w/ unity

Examples and near-examples

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

- **Z**, **Q**, **C**, **R** integers, rationals, complexes, reals

rings

- $R[x]$ in one sec
- Ideals on Monday: Groups are to normal subgroups as rings are to ideals.
- Real-valued functions on a set X

$(f+g)(x) = f(x)+g(x)$

$(fg)(x) = f(x)\,g(x)$

- $\mathbf{Z}[i]$ = {a+bi | a, b in Z}

non comm rings

- **H** = {a+bi+cj+dk | a, b in R}, where ij = k, ji = -k, etc. (Google quaternions)
- $\mathbf{Z}_n$ = {0,1,2,...,n-1} with +, * (mod n)
- $M(n, \mathbf{R})$ n x n matrices w/ real entries
- Operator algebras. . . .

Algebraic vs. transcendental; units

Two important definitions:

- $\alpha \in \mathbf{C}$ is **algebraic** if it is a solution to some polynomial with integer coefficients, and **transcendental** otherwise.
  We are usually more interested in algebraic numbers.
- Let R be a ring. A **unit** of R is some $u \in R$ that has a multiplicative inverse, i.e., there exists some $v \in R$ such that $uv = 1$.

Units of Z are {+1,-1}; units of R (reals) are all real numbers except 0. (A _field_ is a ring where every nonzero element is a unit.) NB: 2 is a unit in R but not in Z.

subring: A subring of a ring R is a subset S of R that is itself a ring under the same operations and contains 1. (i.e., S must be closed under *, +, - and contain 1)

The ring of polynomials $R[x]$

Let R be a ring. We define the ring $R[x]$, the **ring of polynomials with coefficients in** R, as follows.
Set: All expressions of the form

$$\sum_{i=1}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

where each a_i is an element of the ring R. and "x" is an indeterminate.
Addition and multiplication: in $R[x]$ are each defined to work like addition and multiplication of polynomials with real coefficients, except that all coefficient arithmetic is performed in the ring R.
Long story short: This construction produces a ring $R[x]$.

Terminology

For $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$: $= f(x)$

- degree

  if $a_n \neq 0$, $\deg f = n$

- constant polynomial poly deg 0

NB: deg of zero poly is undef

- leading coefficient

  if $a_n \neq 0$, a_n (or $-\infty$)

- monic polynomial

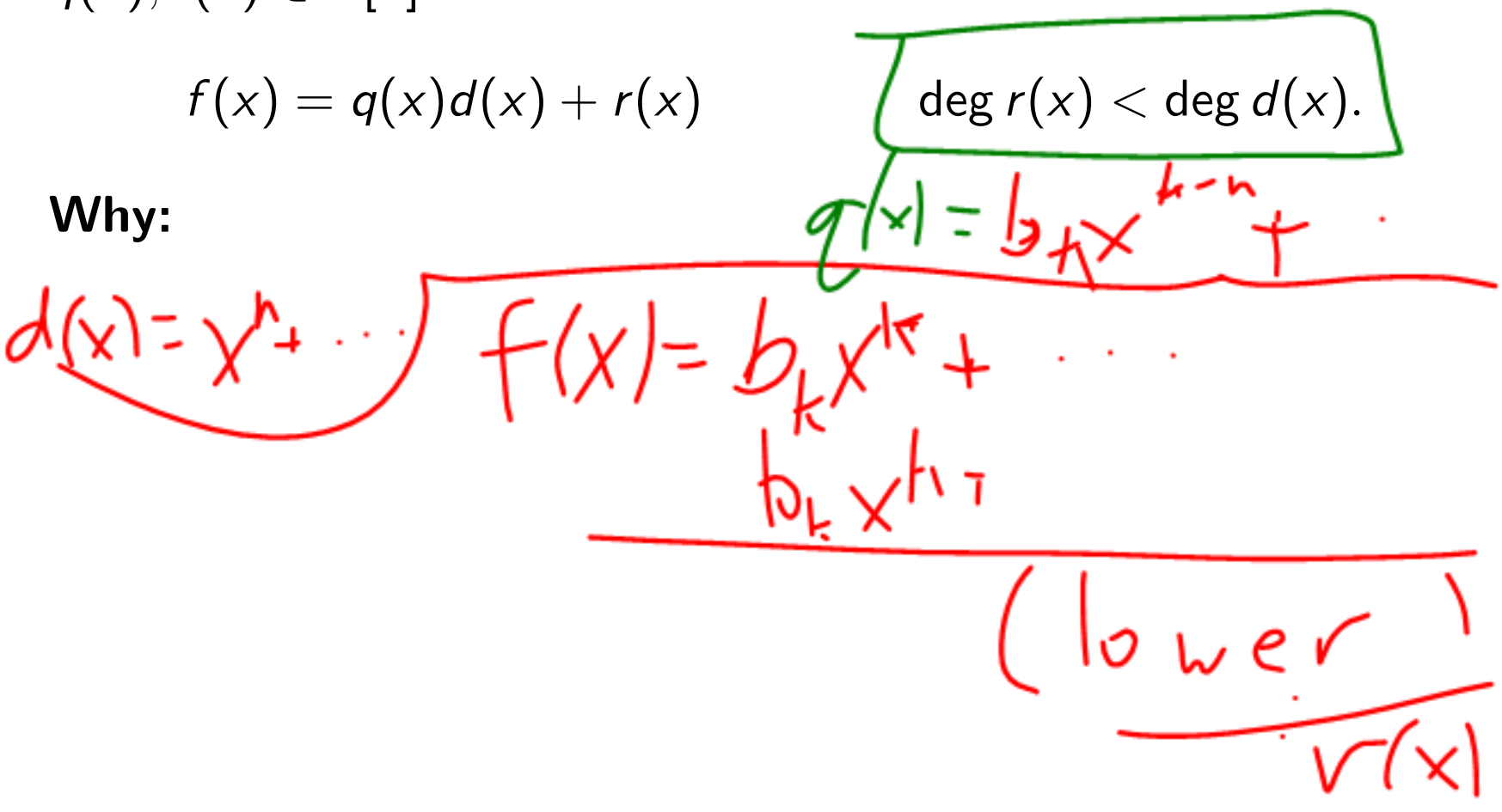
  $a_n = 1$

Polynomial division

Thm: R a ring, $f(x), d(x) \in R[x]$.
Suppose $d(x)$ is a **monic** polynomial (or more generally, a polynomial whose leading coefficient is a unit). There exist unique $q(x), r(x) \in R[x]$ such that

$$f(x) = q(x)d(x) + r(x) \qquad \deg r(x) < \deg d(x).$$

Why:



Remainder and factor theorems

R a ring.

Remainder theorem: Let $f(x) \in R[x]$ and $\alpha \in R$. The remainder upon dividing $f(x)$ by $(x - \alpha)$ is $f(\alpha)$.

Proof:

$f(x) = q(x)(x-\alpha) + r(x)$, $\deg < 1$

Plug α: $f(\alpha) = 0 + r$

Factor theorem: Let $f(x) \in R[x]$ and $\alpha \in R$. Then $(x - \alpha)$ divides $f(x)$ if and only if $f(\alpha) = 0$.

Proof:

Challenge for next time: What is the flaw in the proof of the remainder theorem? I.e., what is the important but unstated algebraic fact we just used?

Ring homomorphisms

Definition: R, R' rings. A ring **homomorphism** from R to R' is a map $\varphi : R \to R'$ such that for all $a, b \in R$:

- $\varphi(a + b) = \varphi(a) + \varphi(b)$;
- $\varphi(ab) = \varphi(a)\varphi(b)$; and
- $\varphi(1) = 1$.

Examples:

- Plugging in on both sides for proof of remainder theorem (In Artin: The **Substitution Principle**)
- More next time