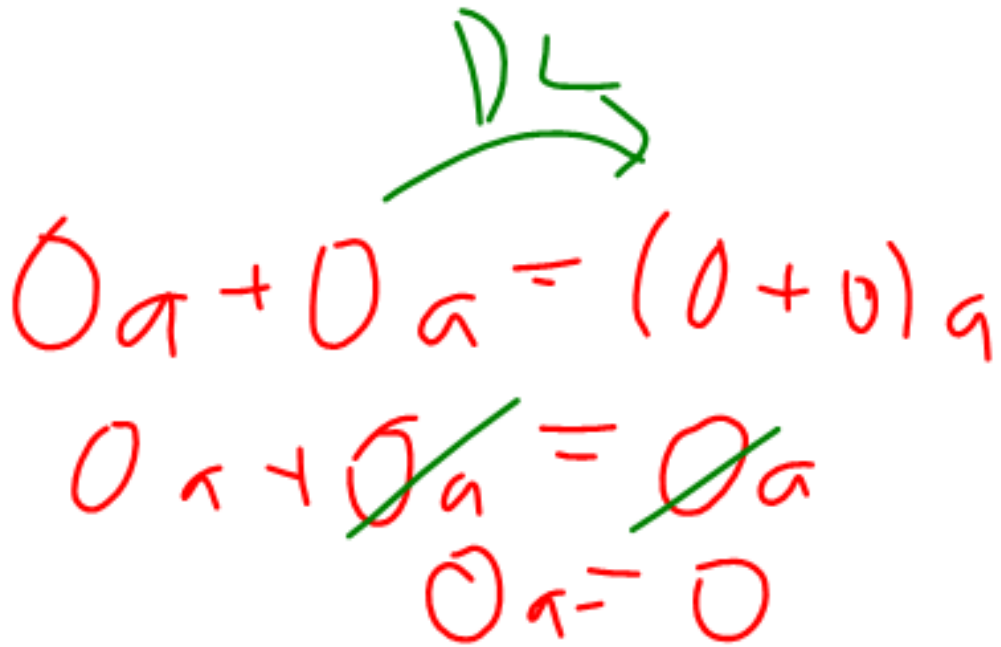
Welcome to Math 221B

- 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: 11.3.
- Reading for Wed Feb 02: 11.4.
- COVID Safety HW ~~and PS00~~ due today.
- PS01 due Mon Feb 07.
- First problem session Fri Feb 04, 10:00–noon on Zoom.

Last time

- Definition of ring (remember that in this course, all rings are commutative with unity 1)
- Examples of rings
- $R[x]$



How abstract algebra always works:

To study the abstract algebra object called a FOO:

* Give axiomatic definition of FOOs

* Look at natural examples of FOOs

* Examine subFOOs (subFOO = subset of a FOO that is itself a FOO using the operations from the larger FOO)

* Look at FOO homomorphisms: maps between FOOs that preserve the structure of a FOO

* (In any kind of additive or multiplicative FOO) Look at the kernel of a FOO homomorphism (everything sent to identity)

today

* Define quotient FOOs

* (In additive/multiplicative situation) First homomorphism theorem

Wed

Remainder and factor theorems

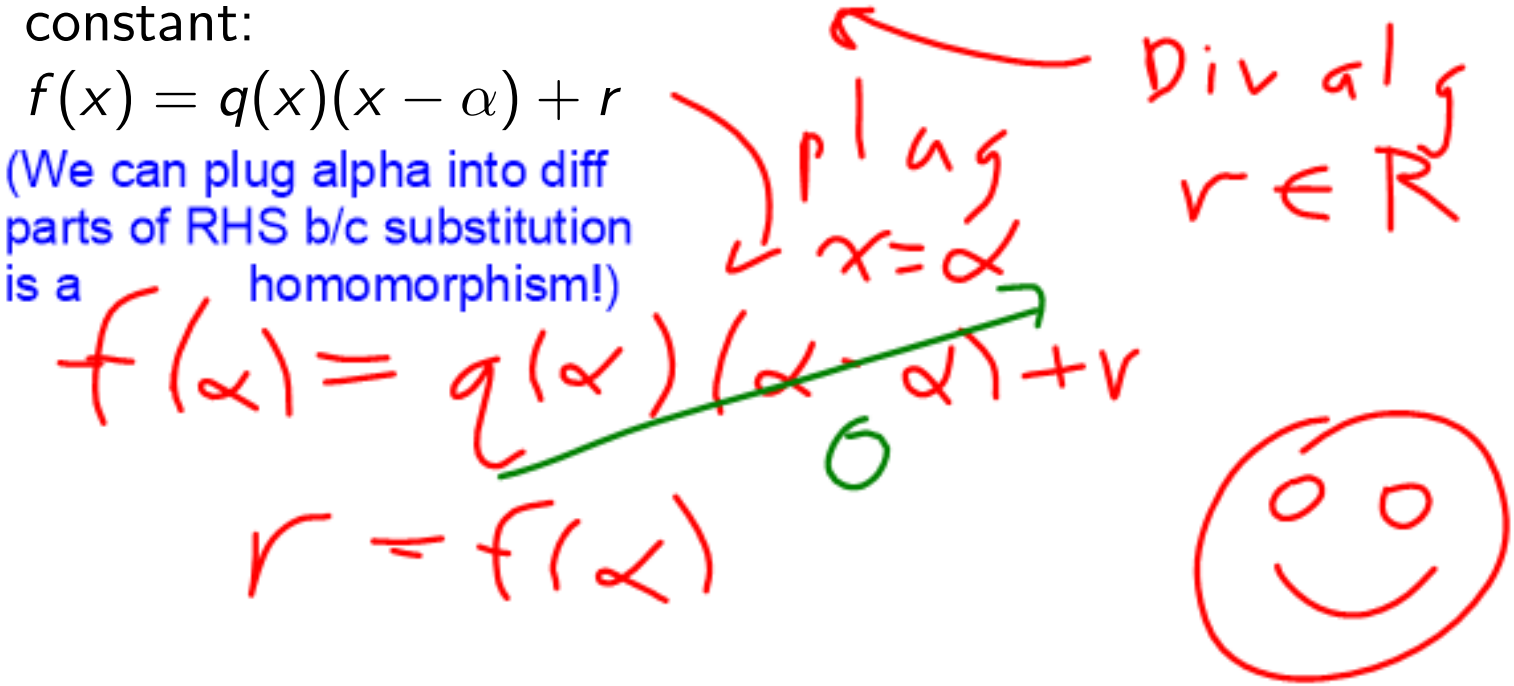
R a ring.

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: $f(x) = q(x)(x - \alpha) + r(x)$, where $\deg r(x) < 1$, so $r(x)$ is constant:

$f(x) = q(x)(x - \alpha) + r$

(We can plug alpha into diff parts of RHS b/c substitution is a homomorphism!)



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: Take the case $r = 0$ above.

Ring homomorphisms

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

- $\varphi(a + b) = \varphi(a) + \varphi(b)$; phi preserves addition
- $\varphi(ab) = \varphi(a)\varphi(b)$; and phi preserves multiplication
- $\varphi(1) = 1$. phi preserves multiplicative identity

The most important example: Plugging in on both sides for proof of remainder theorem, i.e., substitution.

More precisely, this generalizes to a sort of substitution-reduction homomorphism.

The Substitution Principle

expand/reduce coefficients

Thm. Let $\varphi : R \to R'$ be a ring homomorphism and fix $a \in R'$. There exists a unique homomorphism $\Phi : R[x] \to R'$ such that

- For any constant polynomial $c \in R \subseteq R[x]$, $\Phi(c) = \varphi(c)$; and
- $\Phi(x) = a$. (plug in a for x)

Why: Because the operations in $R[x]$ are defined using rules that have to apply in any ring.

Special cases: * Substituting an element a of R in for x (see proof of Remainder Thm)

- For $a \in \mathbf{Z}_n$, $\varphi : \mathbf{Z} \to \mathbf{Z}_n$ induces $\Phi : \mathbf{Z}[x] \to \mathbf{Z}_n$, sending $f(x)$ to $\overline{f}(a)$. So for $f(x) \in \mathbf{Z}[x]$, we **reduce** coefficients mod n, giving $\overline{f}(x) \in \mathbf{Z}_n[x]$, and then plug in a for x.
- For $a \in \mathbf{C}$, the **inclusion** map $\varphi : \mathbf{R} \to \mathbf{C}$ induces $\Phi : \mathbf{R}[x] \to \mathbf{C}$ (treat real coefficients as complex numbers and plug in a for x).

Ideals

Normal subgroups:Groups as Ideals:Rings
Ideals are way more important in ring theory than normal subgps are to group theory.

Defn: Let R be a ring. An **ideal** of R is a nonempty subset I of R such that:

- I is closed under $+$, and
- If $a \in I$ and $r \in R$, then $ra \in I$. So: I closed under (external) R-mult

So to prove $I \subseteq R$ is an ideal of R:

0. Prove $I \neq \emptyset$.

1 (A) $a, b \in I$

(C) $a+b \in I$

2. (A) $a \in I$ $r \in R$

(C) $ra \in I$ I absorbs outside stuff under mult

Kernels are ideals

Let $\varphi : R \to R'$ be a ring homomorphism. We define

$$\ker \varphi = \{r \in R \mid \varphi(R) = 0\}.$$

Thm: $\ker \varphi$ is an ideal of R.

Proof:

0. $\varphi(0) = 0$, so $0 \in \ker \varphi$.

1. (A) $a, b \in \ker \varphi$
$\varphi(a) = 0$, $\varphi(b) = 0$
$\varphi(a) + \varphi(b) = \varphi(a+b)$
$\varphi(a+b) = 0+0 = 0$
(C) $a+b \in \ker \varphi$

2. (A) $a \in \ker \varphi$, $r \in R$
So $\varphi(a) = 0$
So $\varphi(ra) = \varphi(r)\varphi(a)$
$= \varphi(r) \cdot 0 = 0$
So $\varphi(ra) = 0$.
(C) $ra \in \ker \varphi$

General constructions and examples

R a ring, $a, b, \cdots \in R$. $\{0\}$ = zero ideal

- $(a) = \{ra \in R \mid r \in R\}$ is the **principal ideal generated by** a. I.e., the set of all R-multiples of a fixed element $a \in R$ is an ideal of R.
- $(a, b) = \{ra + sb \in R \mid r, s \in R\}$ is the **ideal generated by** a **and** b. I.e., the set of all R-linear combinations of the fixed elements $a, b \in R$ is an ideal of R.
- We'll see momentarily that the ideals of $\mathbf{Z}$ each have the form $(n) = n\mathbf{Z}$ for some $n \in \mathbf{Z}$. $2\mathbb{Z}, 3\mathbb{Z}, 0\mathbb{Z} = \{0\}$
- Similarly, for a field F, every ideal of $F[x]$ has the form (f) for some $f \in F[x]$. Later: Z, F[x] are principal ideal domains (PIDs).
- However, in $\mathbf{Z}[x]$, the ideal $(2, x)$ is not principal (as we'll see later). (2,x) = (All polynomial mults of 2) + (All poly mults of x)
  = (Polys w/even coefficients) + (Polys with 0 constant term)
  = Polys w/even constant term

Fields and ideals

Recall that a **field** is a ring in which every nonzero element is a unit.

Thm: Let R be a ring in which $0 \neq 1$. Then TFAE:

1. R is a field.
2. R has exactly two ideals, $\{0\}$ and R itself.

Sketch (1) $\Rightarrow$ (2) non-0

Prove: I ideal of $R \Rightarrow 1 \in I$

$\Rightarrow I = R$

(2) $\Rightarrow$ (1) For $a \neq 0$, show (a) contains 1.

Every ideal in $F[x]$ is principal

Let F be a field, and suppose I is an ideal of $F[x]$. Then $I = (f)$ for some $f \in F[x]$.

Proof: If I is nonzero, let $f(x)$ be a nonzero element of I of smallest possible degree.

For any f(x) in I, we have (Div Alg):

f(x) = q(x)d(x) + r(x), where deg r < deg d.

But r(x) = f(x) - q(x)d(x), and f and d are in I, so r is in I.

However, d has smallest possible degree of any NONZERO element of I, so r must be 0, i.e., f is a multiple of d.

So I = (d).

Bezout's identity in $F[x]$

Cor: Let F be a field and $f, g \in F[x]$. Suppose the ideal (f, g) is equal to (d) for some $d \in F[x]$. Then:

- d divides f and g.
- If e divides f and g, then e divides d.
- There exist $p, q \in F[x]$ such that $d = pf + qg$.

Characteristic of a ring R

Since $1 \in R$, there exists a unique homomorphism $\varphi : \mathbf{Z} \to R$ such that $\varphi(1) = 1$. (So in R, we can talk about $2 = 1 + 1$, $3 = 1 + 1 + 1$, and so on.)

Defn: Since $\ker \varphi$ is an ideal of $\mathbf{Z}$, $\ker \varphi = (n)$ for some $n \in \mathbf{Z}$, $n \geq 0$. We then say that the **characteristic** of R is n.
In particular, if $\ker \varphi = \{0\}$, then $\ker \varphi = (0)$, and so R has **characteristic 0**.