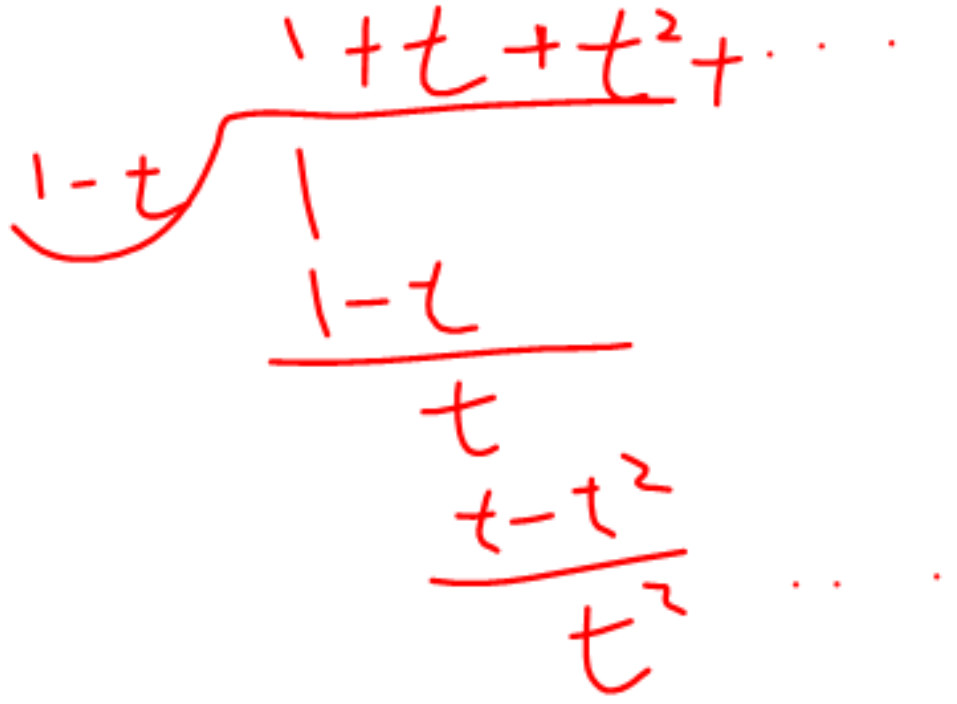
Math 221B, Mon Feb 07

- 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.
- **IN-PERSON CLASSES START MON FEB 14!!!!**
- Reading for today: 11.6–11.8.
- Reading for Wed Feb 09: 12.1–12.2.
- PS02 due Mon Feb 14.
- Problem session Fri Feb 11, 10:00–noon on Zoom.
- Potential new asst prof interviewing today! Algebra talk 3pm today — see email for link.

(2.2) Units in F[[t]]

Ex: (1-t)^-1 = 1+t+t^2+t^3+....



(3.10) Ideals in F[[t]]

I nonzero ideal of F[[t]]

Suppose a(t) in I, a(t) \neq 0.

How much can we simplify a(t) by multiplying it by some p(t) in F[[t]]?

Ex: If 1-t is in I, we can multiply (1-t) by (1+t+t^2+...) to show that 1 is in I.
Any ideal containing 1 must contain all of F[[t]], so I=F[[t]].

A construction of $R[\alpha]$ that is usually good enough

Idea: Take existing ring R, add on alpha with chosen alg properties.

R a ring, $a_i \in R$. Suppose we want to adjoin α to R such that for

$$d(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

we have $d(\alpha) = 0$ (i.e., α satifies that **polynomial identity**). The operations in $R[\alpha] = R[x]/(d(x))$ can be described as follows.

- **Set:** Elements of $R[\alpha]$ are polynomials in α of degree up to $n-1$.
- **Basis:** The set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $R[\alpha]$, i.e., every element of $R[\alpha]$ is a linear combination of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ in exactly one way.
- **Addition:** Ordinary addition of polynomials (i.e., coordinatewise) Remember: Coefficients in R
- **Multiplication:** Multiplication of polynomials, setting $d(\alpha) = 0$.

Proof of $R[\alpha]$ construction

Let $\alpha = x + (f(x))$ in $R[x]/(f(x))$.
WTS that every element of $R[\alpha]$ is an R-linear combination of $\{1, \alpha, \ldots, \alpha^{n-1}\}$ in exactly one way.

$= R[\alpha]$ $I = (d(x))$

(A) $f(x) + (d(x)) \in R[x]/(d(x))$

Div Thm: $f(x) = q(x)d(x) + r(x)$

$\deg r < n$; r unique

$\Rightarrow$ $f(x) + I = r(x) + I = r(\alpha)$

$r(\alpha)$ is R-lin comb of $1, \ldots, \alpha^{n-1}$

Uniqueness of the remainder in Div Thm
<=> r(alpha) is unique elt of R[x]/I equal to f(x) + I.

$$r(x) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

$$\alpha = x + I$$

$$r(\alpha) = b_{n-1}(x+I)^{n-1} + \cdots + b_1(x+I) + b_0$$

By definition of quotient ring:

$$= b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 + I$$

Morally: This works because the operations of R[x]/I are defined to make "reduction mod I" a homomorphism.

Example: $\overline{R} = \mathbf{F}_2[x]/(x^2 + x + 1)$

$\alpha^2 = -\alpha - 1$

$\alpha^2 = \alpha + 1$

Think: $\mathbf{F}_2 = \{0, 1\}$, $\overline{R} = \mathbf{F}_2[\alpha]$, $\alpha^2 + \alpha + 1 = 0$.

Go to: `http://go.limnu.com/gaura-meaningful`

1. How many elements are there in $\overline{R}$? List them.
2. What does the multiplication table of $\overline{R}$ look like?

table:

	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

$\alpha \cdot 1 + \alpha = 1$

$i^2 + \alpha = 1$

$(1+\alpha)^2 =$

$1 + 2\alpha + \alpha^2 = \alpha$

Some other general constructions of rings

Rest of Ch. 11 gives some other ways to construct new examples of rings.

- 11.6: The product ring $R \times R'$ and how to prove that a ring is a product
- 11.7: Integral domains and fields of fractions
- 11.8: Maximal ideals and fields

The product ring $R \times R'$

As usual in abstract algebra, a ring isomorphism is a bijective ring homomorphism.

Let R, R' be rings. Define $R \times R'$ to be:

- **Set:** Cartesian product $R \times R' = \{(x, x') \mid x \in R,\ x' \in R'\}$
- **Addition:** $(x, x') + (y, y') = (x + y, x' + y')$
- **Multiplication:** $(x, x')(y, y') = (xy, x'y')$

This works (i.e., it's a ring). Question: When is a ring $S \approx R \times R'$ for some rings R, R'?

$0 = (0,0)$, $1 = (1,1)$

Idempotents and detecting product rings

S a ring.

Defn: An idempotent in S is some $e \in S$ such that $e^2 = e$.

Ex: In R x R', (1,0) and (0,1) are idempotents.

Theorem

Let $e \in S$ be an idempotent, and let $e' = 1 - e$. Then:

- $e'^2 = e'$, $e + e' = 1$, $ee' = 0$.
- *The multiplicative identity of eS is e, and $\varphi : S \to eS$ given by $\varphi(x) = ex$ is a ring homomorphism.*
- $\Phi : S \to (eS \times e'S)$ *given by* $\Phi(x) = (ex, e'x)$ *is an isomorphism.*

This is really the Chinese Remainder Theorem

Example: $S = \mathbf{Z}/(30)$.

Take e = 6; e^2 = 36 = 6; e' =

6S = {0,6,12,18,24} = Z/(5) by reducing mod 5 to {0,1,2,3,4}
(-5)S = {0,-5,-10,-15,-20,-25} = Z/(6) by reducing mod 6 to {0,1,2,3,4,5}

$\Phi(x) = (6x, -5x) \pmod 5, \pmod 6$

$\mathbb{Z}/(30) \to \mathbb{Z}/(5) \times \mathbb{Z}/(6)$

Integral domains

(Or domains for short)

Definition

To say that a ring R is an **integral domain** means that it has the **zero factor property:** If $a, b \in R$ and $ab = 0$, then either $a = 0$ or $b = 0$.

Non-example of an integral domain:

Thm: Zero Factor Property is equivalent to:
Cancellation Property: If $ab = ac$, $a \neq 0$, then $b = c$.

The field of fractions of an integral domain

Let D be a domain. Define the **field of fractions** F of D to be:

- **Set:** Symbols $\frac{a}{b}$, where $a, b \in D$, $D \neq 0$, and $\frac{a}{b}$ is equivalent to $\frac{a'}{b'}$ exactly when $ab' = a'b$.
- **Addition:**
- **Multiplication:**

This gives well-defined operations of addition and multiplication that make F a field. (Hard/annoying part: Show well-defined.)
See: Jim Tanton, *Fractions are Hard!*
`https://www.jamestanton.com/?p=1461`

Maximal ideals and fields

Defn: I an ideal of a ring R. To say that I is **maximal** in R means that $I \neq R$ and if A is an ideal of R such that $I \subset A \subset R$, then either $I = A$ or $A = R$.

Theorem

An ideal I of a ring R is maximal iff $\overline{R} = R/I$ is a field.

The examples to keep in mind: $\mathbf{Z}$, $F[x]$

- Maximal ideals of $\mathbf{Z}$ are the principal ideals (p), where p is prime
- Maximal ideals of $F[x]$ are the principal ideals $(f(x))$, where $f(x)$ is irreducible.