Math 221B, Wed Feb 03

- 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: 11.4–11.5.
- Reading for ~~Wed Feb 02~~: 11.6–11.8 (through Prop. 11.8.4(a)).
- PS01 due Mon Feb 07.
- First problem session Fri Feb 04, 10:00–noon on Zoom.

Mon Feb 07

The story (of any kind of abstract algebra) so far

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)
- Define quotient FOOs
- (In additive/multiplicative situation) Understand homomorphisms in terms of kernels

Today: $R[\alpha]$

More about $F[x]$

From last time:

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

Every ideal of F[x] is principal
F[x] is a Principal Ideal Domain (PID)

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:

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

gcd

all F[x]-linear combs of f and g

Bezout identity

(f,g) = ideal generated by f and g
= { p(x)f(x) + q(x)g(x) | p(x), q(x) in F[x] } = all F[x]-linear combs of f,g
(d) = principal ideal gen by d = { p(x)d(x) | p(x) in F[x] }

1. f is in (d), so f is a multiple of d; same for g.
2. d is in (f,g), so by defn of (f,g), d = pf+qg for some p,q in F[x].
3. If e divides both f and g, then e divides pf+qg, since f,g are in the ideal (d), and therefore, so is pf+qg.

Characteristic of a ring R

In $\mathbb{F}_3[x]$: $3(x^3+2x+2)$ char 3

$3=0$

$=3x^3+6x+6=0$

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**.

Examples:
Z_n has characteristic n because you add 1 to itself n times to get 0.
Notation: If p is prime, instead of Z_p, we often write F_p because integers mod p form a field.
Example: F_p[x] is a ring with infinitely many elements, and F_p[x] has characteristic p. (So for any f(x) in F_p[x], f(x)+f(x)+... (p times) = 0.)

Quotient rings

Given an ideal I of a ring R, we can define the quotient ring R/I as follows.

- **Set:** We define R/I to be the set of (additive) cosets of I in R, i.e.,
$$R/I = \{r + I \mid r \in R\}.$$
- **Operations:** For $r, s \in R$, we define
$$(r + I) + (s + I) = (r + s) + I$$
$$(r + I)(s + I) = (rs) + I.$$

Abelian quot gp R/I

Quot ring

We might worry that these operations are not well-defined, but:

Theorem

The above is well-defined, and R/I is a ring.

Note that the additive and multiplicative identities of R/I are $0 + I$ and $1 + I$, respectively.

Proof that quotient rings are well-defined

As with groups, the hard part is to prove that the operations are well-defined. (product doesn't depend on choice of reps r, s)

$$(r + I) + (s + I) = (r + s) + I$$
$$(r + I)(s + I) = (rs) + I$$

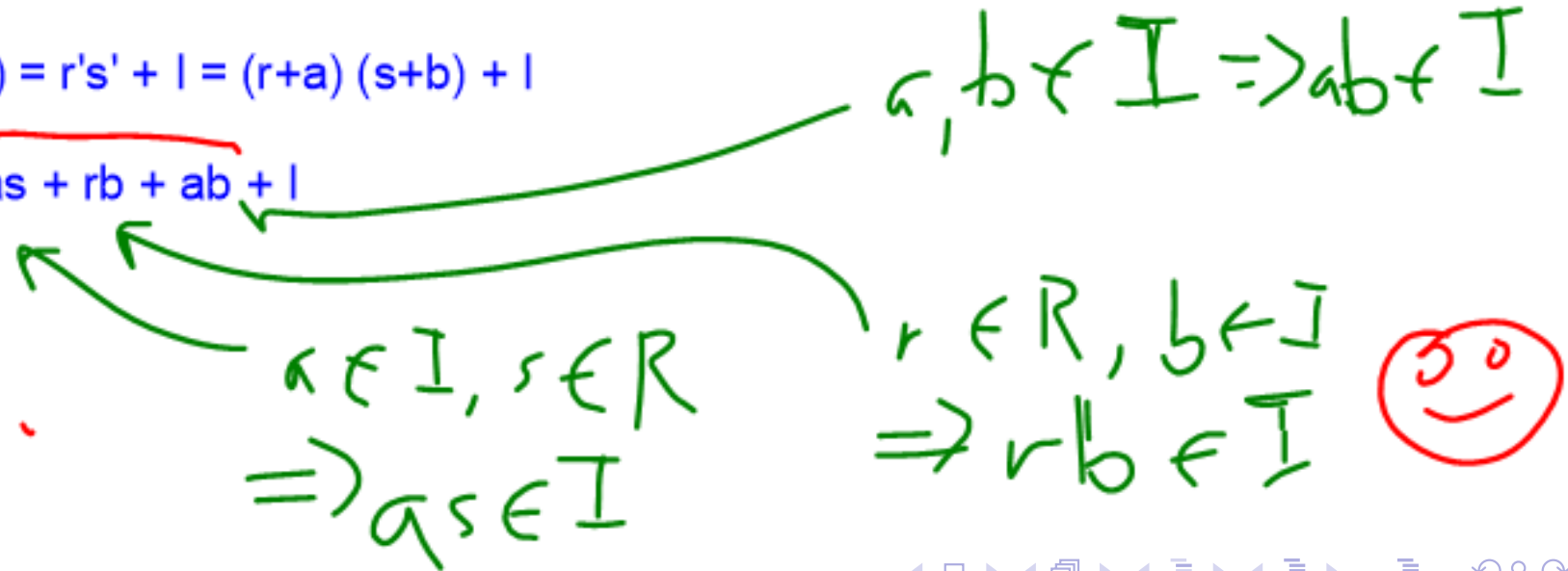
Suppose r+I = r'+I, s+I = s'+I.
Then by a first course in algebra, we have that r' = r+a, s' = s+b for some a,b in the ideal I.

So:

(r'+I)(s'+I) = r's' + I = (r+a) (s+b) + I

= rs + as + rb + ab + I

= rs + I .



An example that turns out to be familiar

Example: $R = \mathbf{R}[x]$, $I = (x^2 + 1)$. $R/I = \mathbf{R}[x]/(x^2 + 1)$ has:

- **Elements:**
- **Addition:**
- **Multiplication:**

Complex numbers are polynomials in i, except that i^2 = -1

In general: For $a \in R$, $R/(a)$ is "R after setting $a = 0$".

11.4 and 11.5: The big picture

Our main technique for constructing new rings is to start with a known ring R and then **adjoin** an element α with certain desired properties (basically, satisfying a given polynomial equation). The result is a ring $[\alpha]$. $R[\alpha]$.

But there are possible catches to this idea:

- How do we know there is such a thing as $R[\alpha]$ at all?
- How do we know that $R[\alpha]$ doesn't have unintended properties (i.e., unexpected identities satisfied by α)? For example, is it possible that R is not a subring of $R[\alpha]$? Maybe adjoining α makes R collapse to 0?
- What is the strucure of ideals in $R[\alpha]$?

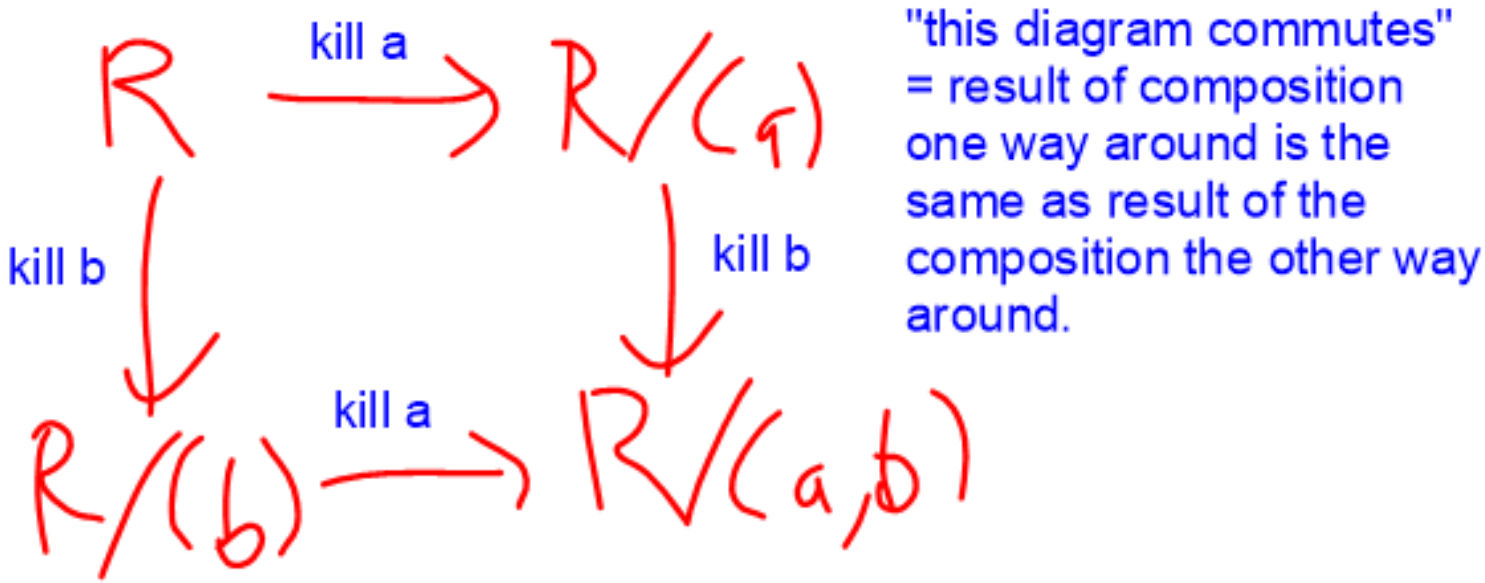
Tools: The Correspondence Theorem and a commuting diagram

- **The Correspondence Thm:** Suppose $\varphi : R \to \mathcal{R}$ is **surjective** and $K = \ker \varphi$. Then we have a bijection:

$$\{\text{ideals of } R \text{ containing } K\} \leftrightarrow \{\text{ideals of } \mathcal{R}\}$$

(Similar ideas give the First Isomorphism Theorem for Rings.)

- For $a, b \in R$, consider the quotient ring $R/(a, b)$. We have the following **commuting diagram**:



Example: What is $\mathbf{Z}[i]/(3+2i)$?

$\cong R$

$i = x + (x^2+1)$

$\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1)$

So $R = \mathbb{Z}[x]/(x^2+1, 3+2x)$

I

What is in I?

→ all $\mathbb{Z}[x]$-lin combs of $x^2+1, 2x+3$

→ $2(x^2+1) - x(2x+3) = 2x^2+2-2x^2-3x$

$= 2-3x \in I$

$\rightarrow \left.\begin{matrix} 3(2x+3) \\ +2(-3x+2) \end{matrix}\right\} \in I$

$6x+9-6x+4=13 \in I$

So $R = \mathbb{Z}(x)/(x^2+1, 3+2x, 13)$

kill first

$= \mathbb{F}_{13}[x]/(x^2+1, 2x+3)$

$7(2x+3) = x+8$. So $x = -8$ in R

$= \mathbb{F}_{13}/((-8)^2+1) = F_{13}/65 = \mathbb{F}_{13}$

A construction of $R[\alpha]$ that works

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

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

we have $f(\alpha) = 0$ (i.e., we have that α satifies the above **polynomial identity**). The operations in $R[\alpha] = R[x]/(f(x))$ 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)
- **Multiplication:** Multiplication of polynomials mod $f(\alpha)$.

Proof: Let $\alpha = x + (f(x))$ in $R[x]/(f(x))$.

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

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

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