Math 128B, Mon Feb 15

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please 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 Mon: Ch. 16. Exam 1 ends w/ Ch 15
- PS03 outline due tonight, full version due Mon Feb 22.
- Next problem session Fri Feb 19, 10:00–noon on Zoom.
- **Exam 1 now on Wed Feb 24**, in 1 week.

Hand out review and sample. . . .

* Exam Zoom proctored
* Exam handed out on chat and turned in as HW on Gradescope
* LEAVE MIC ON
  (If background noise annoying, mute your own speaker)

* Camera on, first on face, then on hands

* 65 min work time, 10 min upload
* Problems written on paper, 1 page per problem
* Must stay until upload time starts -- bring analog reading

Ring homomorphisms

Definition

Let R and S be rings. To say that $\varphi : R \to S$ is a **homomorphism** (of rings) means that for all $a, b \in \cancel{\mathbf{R}}$ R

$$\varphi(a+b) = \varphi(a) + \varphi(b), \qquad \varphi(ab) = \varphi(a)\varphi(b).$$

If φ is also bijective, we say that φ is an **isomorphism** (of rings).

I.e., ring homomorphisms preserve **both** ring operations, $+$ and $\cdot$.

Homomorphism preserve ring-theoretic properties

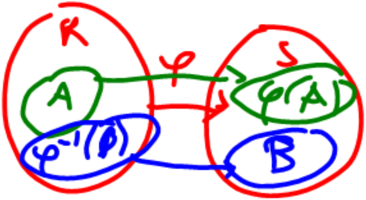
Ring s

Just like Ch. 10 and groups!

Suppose $\varphi : R \to S$ is a ring homomorphism, A an ideal of R, and B an ideal of S.

Defn: $\varphi^{-1}(B) = \{r \in R \mid \varphi(r) \in B\}$, and $\ker \varphi = \varphi^{-1}(\{0\})$.

Thm:



- $\varphi(nx) = n\varphi(x)$ and $\varphi(x^n) = \varphi(x)^n$.
- $\varphi(A)$ is an ideal of: S
- $\varphi^{-1}(B)$ is an ideal of: R
- If $1 \in R$, $S \neq \{0\}$, and φ is onto, then $\varphi(1)$ is the multiplicative identity of S.
- φ is injective if and only if $\ker \varphi = \{0\}$.

If φ onto

(φ is $\ker\varphi$-to-1)

Proof of ~~one~~ two of those

Special case of third fact: ker(phi) is an ideal.
HW: Prove that w/o using the third fact.

* $1 \in R$, $S \neq \{0\}$, φ onto

A $s \in S$

$\boxed{\text{B/c } \varphi \text{ onto}, \exists r \in R \text{ s.t. } \varphi(r) = s.}$

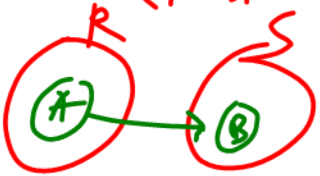
So $\varphi(1)s = \varphi(1)\varphi(r)$ $\leftarrow$ φ hom.

$= \varphi(1 \cdot r)$

$= \varphi(r) = s.$

C $\varphi(1)s = s = s\varphi(1)$

(4) A ideal of R, φ onto $\varphi(A) = \{\varphi(a) \mid a \in A\}$



0

$0 \in A$

so

$\varphi(0) = 0$

$\in \varphi(A)$

So

$\varphi(A) \neq \emptyset$

1

(A) $b_1, b_2 \in \varphi(A)$

so $b_1 = \varphi(a_1)$

$b_2 = \varphi(a_2)$ $(a_i \in A)$

$$\left.\begin{aligned} b_1 - b_2 &= \varphi(a_1) - \varphi(a_2) \\ &= \varphi(a_1 - a_2) \end{aligned}\right] \varphi \text{ hom}$$

B/c A ideal, $a_1 - a_2 \in A$.

(C) $b_1 - b_2 \in \varphi(A)$

(C) $\varphi(A$ ideal of S

2] (A) $b \in \varphi(A),\ s \in S$

B/c $b \in \varphi(A)$, $b = \varphi(a)$ for $a \in A$

B/c φ onto, $s = \varphi(r)$ for $r \in R$

$$\left.\begin{aligned} bs &= \varphi(a)\varphi(r) \\ bs &= \varphi(ar) \end{aligned}\right\} \varphi \text{ hom}$$

$ar \in A$ b/c A ideal of R

defn of $\varphi(A)$ $\downarrow$ (sb similar)

(C) $bs \in \varphi(A),\ sb \in \varphi(A)$

Important facts about group homomorphisms

Suppose $\varphi : G \to H$ is a group homomorphism. Recall that:

- **Kernels are normal subgroups:** $\ker \varphi \lhd G$.
- **Normal subgroups are kernels:** If $N \lhd G$, define $\gamma : G \to G/N$ by $\gamma(a) = aN$. Then $\ker \gamma = N$.
- **First isomorphism theorem:**

Gallian Ch. 10

$\varphi : G \to \overline{G}$ $\quad \ker \varphi = T$

$G/T \cong \varphi(G)$

I.e: $\varphi(G) \approx G/\ker \varphi$

"By their kernels shall ye know them"

Important facts about ring homomorphisms

Suppose $\varphi : R \to S$ is a ~~right~~ ring homomorphism. Then:

- **Kernels are ideals:** $\ker \varphi$ is an ideal of R. PSOJ
- **Ideals are kernels:** If A is an ideal of R, define $\gamma : R \to R/A$ by $\gamma(r) = r + A$. Then $\ker \gamma = A$. $\ker \gamma = \{r \in R \mid \gamma(r) = 0\}$
- **First isomorphism theorem:**

$$\varphi : R \to S$$

$$\varphi(R) \approx R/\ker \varphi$$

"By their kernels shall ye know them"

1IT holds generally:

V.S. $T: V \to W$

$\text{nullsp}(T) = \ker T$ subsp of V

$$\underbrace{T(V) \simeq V/\ker T}_{\text{rank-nullity}}$$

$\text{rank}(T) = \dim V - \text{null}(T)$

The image of $\mathbf{Z}$ in a ring with unity

R a ring with 1.

Theorem

The map $\varphi : \mathbf{Z} \to R$ given by $\varphi(n) = n \cdot 1$ is a ring homomorphism.

key: $(a \cdot 1)(b \cdot 1) = ab \cdot 1$

Corollary

If characteristic of R is $n > 0$, there exists a subring of R isomorphic to $\mathbf{Z}_n$. ($\ker \varphi = n\mathbb{Z}$)
If characteristic of R is 0, there exists a subring of R isomorphic to $\mathbf{Z}$.

($\ker \varphi = \{0\}$)

Let F be a field.

Point: Every field is "based on" either Z_p or Q.

Corollary

If characteristic of F is $p > 0$, there exists a subfield of F isomorphic to $\mathbf{Z}_p$.
If characteristic of ~~R~~ F is 0, there exists a subfield of ~~R~~ F isomorphic to $\mathbf{Q}$. (take copy of Z in F and include inverses of those elements)

Field of quotients (field of fractions)

Let D be an integral domain. Define

$$S = \{(a, b) \mid a, b \in D, b \neq 0\}$$

Write $\dfrac{a}{b}$ instead of (a, b).
Define an equivalence relation $\sim$ on S by saying that $\dfrac{a}{b} \sim \dfrac{c}{d}$ exactly when $ad = bc$. Let F be the set of equivalence classes of S. Define

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Can check that F is well-defined, and:

Theorem
F is a field that contains a subring isomorphic to D. $= \left\{ \frac{a}{1} \,\middle|\, a \in D \right\}$

Examples and notation

$\mathbb{Z} \to \mathbb{Q}$

$F \to F$

Example: For $D = F[x]$, the field of quotients of D is

$$F(x) = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f, g \in F[x],\ g(x) \neq 0 \right\}.$$

$F(x)$ is called the field of rational functions over F.

Example: $\mathbf{Z}_p(x)$ is an infinite field of characteristic p. prime

F[x] is ring of polynomials with coefficients in the field F.

END MATERIAL COVERED IN EXAM 1

Polynomials with coefficients in a ring R

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

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

where each a_i is an element of the ring R.
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.

Example

Take $R =$