Week 3

???

3.1 Intro to Chapters 8-9

1/18:

- Moving onto Chapter 8 today.
- Friday: Rings of fractions (more than what's in the book; under lesser hypotheses).
  - Def get notes!
- The Chinese Remainder Theorem is at least partially in HW3.
- Today: A leisurely introduction to Chapter 8, as well as Spring Quarter content (which is the most interesting part of the Honors Algebra sequence).
- For the next three weeks or more, all rings will be assumed to be commutative.
  - Excepting matrix rings, which may still appear in exercises.
- At this point, we define $\deg(f) = -\infty$ where f is the zero polynomial.
  - We do this so that $\deg(fg) = \deg(f) + \deg(g)$ still holds.
- Euclidean algorithm for monic polynomials: Let $f \in R[X]$ be a monic polynomial of degree $d \geq 0$, and let $h \in R[X]$. Then there exists a unique pair $q, r \in R[X]$ such that...
  1. $h = qf + r$;
  2. $\deg(r) < \deg(f)$.

  Proof. We tackle uniqueness first, and then existence.

  Uniqueness: Suppose $h = q_1 f + r_1 = q_2 f + r_2$, where $\deg(r_i) < d$ $(i = 1, 2)$. We have that

  $$(q_1 - q_2)f = q_1 f - q_2 f = r_2 - r_1$$

  Now suppose for the sake of contradiction that $q_1 - q_2 \neq 0$. We know that

  $$\deg(r_2 - r_1) = \deg[(q_1 - q_2)f] = \deg(q_1 - q_2) + d \geq d$$

  But since $\deg(r_i) < d$ $(i = 1, 2)$, we have that $\deg(r_2 - r_1) < d$, a contradiction. Thus, $q_1 - q_2 = 0$. It follows easily that $0 = r_2 - r_1$. Therefore, $(q_1, r_1) = (q_2, r_2)$, as desired.

  Existence: If $\deg(h) < d$, then put $q = 0$ and $r = h$. We now induct on $\deg(h)$, starting from d. Our base case is already taken care of via the statement on $\deg(h) < d$. Now suppose using strong induction that we have proven the claim for all nonnegative integers $n < \deg(h)$. Let

  $$h(X) = a_0 + \cdots + a_e X^e$$

where $a_e \neq 0$ and $e \geq d$ by hypothesis. Let

$$f(X) = b_0 + \cdots + b_{d-1}X^{d-1} + X^d$$

Define $g(X)$ by

$$g = h - a_e X^{e-d} f$$

It follows that $\deg(g) < e$, so we may apply the induction hypothesis at this point. We learn from it that there exist q, r such that $g = qf + r$ with $\deg(r) < d$. Therefore, we can deduce that

$$h = (a_e X^{e-d} + q)f + r$$

as desired. $\square$

- Notes on the Euclidean algorithm.
  - Think long polynomial division from high school.
- Example.
  - Let $a \in R$ and $f = X - a$ be a monic polynomial. Let $h \in R[X]$ be arbitrary. Then applying the theorem,
  $$h(X) = q(X)(X - a) + r$$
  - $\deg(r) < 1 = \deg(f)$ implies that r is a constant, and hence $r \in R$.
  - Moreover,
  $$\begin{aligned} h(a) &= q(a)(a - a) + r \\ r &= h(a) \end{aligned}$$
  implying that
  $$h(X) - h(a) = q(X)(X - a)$$
  for arbitrary polynomials h.
- Corollary: Let $a \in R$. $\{h \in R[X] \mid h(a) = 0\}$ is the **principal ideal generated by $\boldsymbol{X - a}$**.
- **Ideal generated by $\boldsymbol{b \in B}$**. *Denoted by* $\boldsymbol{Bb}$, $\boldsymbol{(b)}$.
- Corollary: Let $f \in R[X]$ be monic of degree d. Then
  $$\{g \in R[X] \mid \deg(g) < d\} \hookrightarrow R[X] \twoheadrightarrow R[X]/(f)$$
  and, in particular,
  $$\{g \in R[X] \mid \deg(g) < d\} \cong R[X]/(f)$$
  as groups (in particular, *not* as rings).

Proof. The existence of the first two maps is obvious (they are just instances of the canonical injection and surjection, respectively).

We now verify that the last two sets are in bijective correspondence. Define a map φ between them via the canonical surjection (note that since the domain of φ is not $R[X]$, we will still have to verify surjectivity here). As established previously, φ is well defined.

To prove that φ is injective, it will suffice to show that $\ker \varphi = 0$. Let h be an arbitrary polynomial in $R[X]$ with $\deg(h) < d$. Suppose $\varphi(h) = 0 = 0 + (f) = (f)$. Then $h \in (f)$. It follows that either $h = 0$ or $\deg(h) \geq \deg(f) = d$. But as an element of the domain $\deg(h) < d$ by hypothesis. Therefore, $h = 0$, as desired.

To prove that φ is surjective, it will suffice to show that for every $h + (f) \in R[X]/(f)$, there exists $r \in R[X]$ with $\deg(r) < d$ such that $\varphi(r) = h + (f)$. Let $h + (f) \in R[X]/(f)$ be arbitrary. By the Euclidean algorithm, $h = qf + r$ for some $q, r \in R[X]$ where $\deg(r) < \deg(f) = d$. Moreover, since $r = h + (-q)f$, $r \in h + (f)$ and hence $h + (f) = r + (f)$. Therefore, since r is in the domain of φ (as it has degree less than d), $\varphi(r) = r + (f) = h + (f)$, as desired. $\square$

- $R[X]$ is also a vector space with $1, X, X^2, \dots$ as the basis.
- We have that
$$\{g \in R[X] \mid \deg(g) < d\} = \{a_0 + \cdots + a_{d-1}X^{d-1} \mid a_0, \dots, a_{d-1} \in R\}$$
  - As an abelian group (ignoring multiplication), this set is group isomorphic to $(R^d, +)$.
- Revisiting the creation of $\mathbb{C}$ from $\mathbb{R}$.
  - We can use quotient rings to solve $X^2 + 1 = 0$.
  - In particular, the equation $X^2 + 1 = 0$ does not have a solution in $\mathbb{R}[X]$. However, it does have a solution in $\mathbb{R}[X]/(X^2 + 1)$, as we will see presently.
  - Consider the function described in the above corollary, sending $\mathbb{R} \hookrightarrow \mathbb{R}[X] \twoheadrightarrow \mathbb{R}[X]/(X^2+1)$. Let $\bar{X} := X + (X^2 + 1) \in \mathbb{R}[X]/(X^2 + 1)$ denote the image of X in $\mathbb{R}[X]/(X^2 + 1)$ under the second map. It follows that in this new ring,
$$\begin{aligned}
\bar{X}^2 + 1 &= [X + (X^2 + 1)] \cdot [X + (X^2 + 1)] + [1 + (X^2 + 1)]\\
&= [X^2 + 1] + (X^2 + 1)\\
&= 0 + (X^2 + 1)\\
&= 0
\end{aligned}$$
    as desired.
  - Additionally, the elements of this ring are of the form $a_0 + a_1\bar{X}$ ($a_0, a_1 \in \mathbb{R}$) by the above corollary. As per the rules of addition and multiplication in quotient rings, our addition and multiplication in this ring are
$$\begin{aligned}
(a_0 + a_1\bar{X}) + (b_0 + b_1\bar{X}) &= (a_0 + b_0) + (a_1 + b_1)\bar{X}\\
(a_0 + a_1\bar{X}) \cdot (b_0 + b_1\bar{X}) &= (a_0b_0 - a_1b_1) + (a_0b_1 + a_1b_0)\bar{X}
\end{aligned}$$
    - For addition, we expect componentwise.
    - For multiplication, we apply the distributive law, and then reduce our final element mod $X^2 + 1$ using the fact that $\bar{X}^2 = -1$ so $a_1b_1\bar{X}^2 = -a_1b_1$.
  - Thus, since they have isomorphic sets of elements and identical operations,
$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$$
  - Note that $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{R}[i]$, where $i = \sqrt{-1}$. In other words, we can look at the elements of $\mathbb{R}[X]/(X^2 + 1)$ as complex numbers, or as polynomials in i. The two concepts are equivalent since any polynomial in i reduces to a complex number via the i-cycle as follows.
$$\begin{aligned}
\sum_{j=0}^{\infty} a_j i^j &= a_0 + a_1 i + a_2 i^2 + a_3 i^3 + a_4 i^4 + a_5 i^5 + \cdots\\
&= a_0 + a_1 i - a_2 - a_3 i + a_4 + a_5 i - \cdots\\
&= (a_0 - a_2 + a_4 - \cdots) + (a_1 - a_3 + a_5 - \cdots)i\\
&= \left(\sum_{j=0}^{\infty} a_{2j}\right) + \left(\sum_{j=0}^{\infty} a_{2j+1}\right) i
\end{aligned}$$
- However, this construction renders $\mathbb{C}$ as just one particular special case of interest in a far more general construction.
  - Specifically, $\mathbb{C}$ is the special case that takes $f = X^2 + 1$ as the divisor.

- Indeed, we may create a ring in which the root of any polynomial $f \in R[X]$ exists.
  - For the sake of simplicity, let f be monic of degree d. Let $A = R[X]/(f)$. Then as per the corollary, $R \hookrightarrow R[X] \twoheadrightarrow A$.
  - Once again, we let $\bar{X}$ be the image of X under the second map. $f(X) \mapsto f(\bar{X}) = 0$, as desired.
  - In analogy to the last line above,
$$R[X]/(f) \cong R[\bar{X}]$$
for any $\bar{X}$ satisfying $f(\bar{X}) = 0$.
- Additional examples.
  1. Take $R = \mathbb{Z}$, $f(X) = 2$. Then $\mathbb{Z} \hookrightarrow \mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[X]/(2)$.
     - (2) is the set of all polynomials with even integer coefficients. Thus, any polynomial with even integer coefficients in $\mathbb{Z}[X]$ will be projected down to zero, and any polynomial containing any odd coefficients will correspond to a coset in which all polynomials with odd terms in the same places are lumped together.
     - Essentially, reducing occurs termwise and is modulo 2 based on the coefficients. For example,
$$5 + 2X + 4X^2 + 7X^4 + (2) = 1 + 1X^4 + (2)$$
since $4 + 2X + 4X^2 + 6X^4 \in (2)$ and
$$5 + 2X + 4X^2 + 7X^4 = 1 + 1X^4 + 4 + 2X + 4X^2 + 6X^4$$
     - Thus, $\mathbb{Z}[X]/(2) \cong \mathbb{Z}/2\mathbb{Z}[X]$.
     - What is $\bar{X}$ in this set?? It must be some integer??
  2. Take $R = \mathbb{Z}$ and $f(X) = 2X + 3$. Then we have $\mathbb{Z}[X]/(2X + 3)$.
     - $X \mapsto \bar{X}$ and $2\bar{X} + 3 = 0$, so $\bar{X} = -3/2$.
     - Just like $i \notin \mathbb{R}$, $-3/2 \notin \mathbb{Z}$.
     - We still have $\mathbb{Z}[X]/(2X + 3) \cong \mathbb{Z}[-3/2]$.
       - In other words, $\mathbb{Z}[X]/(2X + 3)$ is the set of all "polynomials" in $-3/2$ with integer coefficients, which is just equal to
$$\{a/2^n \mid a \in 3\mathbb{Z}\}$$
which is the diadic rationals with numerator equal to a multiple of 3.
     - This construction will be integral to Spring Quarter.
- Question/exercise: Let $\alpha \in R$. Then $R[X]/R[X]\alpha \cong (R/R\alpha)[X]$.
- Is it that dividing by a polynomial of degree 0 puts a constraint on the coefficients whereas dividing by a polynomial of degree greater than zero puts a constraint on the variable??
- **Principal ideal domain**: A commutative ring R that is an integral domain and for which every ideal is principal. *Also known as* **PID**.
- There is a useful explanation of something on Chapter 8, page 2 of Dummit and Foote (2004).
- Theorem: Let F be a field. Then $F[X]$ is a PID.

  Proof. We have proven previously that F an integral domain implies $F[X]$ is an integral domain.

  Let $I \subset F[X]$ be a nonzero ideal. Let
$$d = \min\{\deg(g) \mid g \in I,\ g \neq 0\}$$
  Pick $g \in I$ such that $\deg(g) = d$. We have that $g = a_0 + \cdots + a_d X^d$, $a_d \neq 0$, $a_d^{-1} \in F$. Let $f = a_d^{-1} g \in I$ (as guaranteed by the presence of $g \in I$). Let $h \in I$. Then the EA produces q, r such that $h = qf + r$ with $\deg(r) < d$. We know that $h, f \in I$. Thus, $h - qf = I$. It follows by the definition of d that $r = 0$. Therefore, $h \in (f)$. $\square$

- Callum will lecture on Friday.
- Feedback on the HW.
  - Most people seem to think that the HW is at a reasonable level of difficulty.
  - The third one should be more challenging.