Week 3

Intro to Ring Types

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. □

- 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. □

- $R[X]$ is also a vector space with $1, X, X^2, \ldots$ as the basis.
- We have that

$$\{g \in R[X] \mid \deg(g) < d\} = \{a_0 + \cdots + a_{d-1}X^{d-1} \mid a_0, \ldots, a_{d-1} \in R\}$$

  - 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, $h \in (f)$. ☐

- 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.

3.2 Rings of Fractions

1/20:

- This lecture will cover material from Sections 7.5 and 15.4 of Dummit and Foote (2004).
- Defining $\mathbb{Q}$.
  - Rigorously, we define $\mathbb{Q}$ as a subset of $(\mathbb{Z} \times \mathbb{Z}) \setminus \{(a, 0) \mid a \in \mathbb{Z}\}$. In particular, we let $\mathbb{Q}$ be the set of equivalence classes in $\mathbb{Z} \times \mathbb{Z}$ under the equivalence relation
    $$\frac{a}{b} = \frac{c}{d} \quad \Longleftrightarrow \quad ad - bc = 0$$
    where a/b denotes $(a, b) \in \mathbb{Z} \times \mathbb{Z}$.
  - Addition on $\mathbb{Q}$:
    $$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}$$
    - This makes $(\mathbb{Q}, +)$ an abelian group with identity $0 = 0/c$ for any $c \neq 0$.
  - Multiplication on $\mathbb{Q}$:
    $$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$
    - This makes $(\mathbb{Q}, +, \cdot)$ a ring with identity $1 = 1/1 = d/d$ for any $d \neq 0$.
- Notice the similarities between the above approach and the definition of $\mathbb{C}$ from $\mathbb{R}$ in Lecture 2.1.
- It follows from the definition that $\mathbb{Q}$ is also a field: For any $a/b \in \mathbb{Q}$, $a/b \cdot b/a = 1$.
- We can generalize this construction to any commutative ring R.
  - As in $\mathbb{Q}$, we may only be able to take the "quotient" of certain elements of R by certain other elements of R. For example, $a/0$ does not make sense in $\mathbb{Q}$. Thus, we first define a subset of R called D: D contains elements which can act as <u>d</u>enominators. The properties of D are motivated by the properties of denominators in $\mathbb{Q}$. In particular...
  - Let $D \subset R$ be such that $1_R \in D$, $0_R \notin D$, D has no zero divisors, and D is closed under multiplication (that is, $b, d \in D$ implies $bd \in D$).
    - We need $1_R \in D$ so that all of the elements $a \in R$ appear in the related ring of fractions as $a/1_R$.
    - We can't have $0_R \in D$ because you cannot divide by zero.
    - We can't have any zero divisors in D because then during addition or multiplication, as defined above, the sum or product could have zero in the denominator.
    - We need closure under multiplication so that the sums and products defined above are well-defined.
  - With these constraints on D, we can define the **ring of fractions**.
- $\sim$: The equivalence relation on a product ring $(A \times B, +, \cdot)$ defined as follows. *Given by*
  $$(a_1, b_1) \sim (a_2, b_2) \quad \Longleftrightarrow \quad a_1 \cdot b_2 - a_2 \cdot b_1 = 0$$
- Exercise: Confirm that $\sim$ is an equivalence relation.

- Just as taking the quotient of a group by a normal subgroup or a ring by an ideal yields a partition of the original object where all elements in any set in the partition are related by the substructure, taking the quotient of a set by an equivalence relation yields a partition of that set into classes called *equivalence* classes.
  - Thus, when we write $(A \times B)/\sim$, we refer to the set of equivalence classes of $A \times B$ under $\sim$.
- **Ring of fractions** (of D with respect to R): The set defined as follows, under the operations defined as follows. *Denoted by* $\boldsymbol{D^{-1}R}$. *Given by*

$$D^{-1}R = \{(x,t) \mid x \in R,\ t \in D\}/\sim$$

  1. Addition:
$$\frac{x_1}{t_1} + \frac{x_2}{t_2} = \frac{x_1t_2 + x_2t_1}{t_1t_2}$$
     - Let $0_{D^{-1}R} = 0/1$.
       - Note that because of the way $0/1$ is defined (i.e., as an equivalence class), we no longer need to say $0/1 = 0/d$ for all $d \in D$ since all $0/d$ are included in $0/1$. In fact, at this point, $0/d$ is just an alternate name for the set $0/1$.
     - It follows from the above definition that $-(x/t) = -x/t$.
  2. Multiplication:
$$\frac{x_1}{t_1} \cdot \frac{x_2}{t_2} = \frac{x_1x_2}{t_1t_2}$$
     - Let $1_{D^{-1}R} = 1/1$.
- Notes on the ring of fractions.
  - Notice how the notation is a nice alternative to the (already taken) R/D.
  - Notation: Write x/t for the equivalence class $[(x,t)]$.
- Proposition: $D^{-1}R$ is a ring as defined above.

  Proof. There are three steps needed: (1) check that $+, \times$ are well defined; (2) check that $(D^{-1}R, +)$ is an abelian group; and (3) check that $\times$ is an associative, commutative, and distributive operation with an identity. □

- **Field of fractions** (of R): The set $D^{-1}R$ where R is an integral domain and $D = R \setminus \{0\}$. *Also known as* **quotient field**. *Denoted by* $\textbf{Frac}\,\boldsymbol{R}$.
  - Inverses are given by
$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$$
    for all nonzero elements $a/b \in \operatorname{Frac} R$ (i.e., all elements for which $a, b \neq 0$).
- Example: Let R be an integral domain, and let $f \in R$ not be nilpotent. Take $D = \{1, f, f^2, \dots\}$. Then $R_f = D^{-1}R$.
  - Example: If $R = \mathbb{Z}$ and $f = 2$, then $R_2 = \{a/b \in \mathbb{Q} \mid b = 2^n\}$. Recall that these are the diadic rationals.
- Example: Let $R = \mathbb{Z}$ and $D = \{a \in \mathbb{Z} : 2 \nmid a\}$. Then $D^{-1}R = \{a/b \in \mathbb{Q} : 2 \nmid b\}$.
- Besides the last two examples, the only nontrivial ideal of $\mathbb{Q}$ left is (2^n).
  - Do I have this statement right??
- If R is an integral domain, then $\operatorname{Frac}(R[X])$ is the set of all rational functions with coefficients in R.

- We have a canonical injection $\iota : R \to D^{-1}R$ defined by $x \mapsto x/1$.
- Theorem (universal property of the ring of fractions):

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, hook, "\iota"'] & S \\
D^{-1}R \arrow[ur, "\tilde{\varphi}"'] &
\end{tikzcd}$$

Figure 3.1: Decomposition of a ring homomorphism using $D^{-1}R$.

(1) $\iota : R \to D^{-1}R$ is an injective ring homomorphism.

(2) If $\varphi : R \to S$ is a ring homomorphism such that $\varphi(r)$ is a unit in S for all $r \in D$, then there exists a unique ring homomorphism $\tilde{\varphi} : D^{-1}R \to S$ such that $\tilde{\varphi} \circ \iota = \varphi$ (see Figure 3.1).

(3) If φ is injective, then so is $\tilde{\varphi}$.

Proof. (1) is easy.

We address (2) in two parts.

<u>Existence</u>: Define $\tilde{\varphi}(x/t) = \varphi(x)\varphi(t)^{-1}$.

<u>Uniqueness</u>: Suppose that there exists $\rho : D^{-1}R \to S$ such that $\rho \circ \iota = \varphi$. Then $\varphi(x) = (\rho \circ \iota)(x) = \rho(x/1)$. This result combined with the fact that ρ is a ring homomorphism implies that

$$1 = \rho(\tfrac{1}{1}) = \rho(\tfrac{t}{1})\rho(\tfrac{1}{t}) = \varphi(t)\rho(\tfrac{1}{t})$$

It follows since $\varphi(D) \subset S^{\times}$ by hypothesis that if $t \in D$, then $\rho(1/t) = \varphi(t)^{-1}$. Therefore,

$$\rho(\tfrac{x}{t}) = \rho(\tfrac{x}{1})\rho(\tfrac{1}{t}) = \varphi(x)\varphi(t)^{-1} = \tilde{\varphi}(\tfrac{x}{t})$$

We now address (3).

Suppose that φ is injective. To prove that $\tilde{\varphi}$ is injective, it will suffice to show that $\ker\tilde{\varphi} = 0$. Let $x/t \in \ker\tilde{\varphi}$ be arbitrary. Then $\tilde{\varphi}(\frac{x}{t}) = 0$. It follows by the definition of $\tilde{\varphi}$ that $\varphi(x)\varphi(t)^{-1} = 0$. Since $\varphi(t)$ is a unit by hypothesis and hence nonzero, it must be that $\varphi(x) = 0$. Additionally, as a ring homomorphism, $\varphi(0) = 0$. Combining the last two results, we have by transitivity that $\varphi(x) = \varphi(0)$. Thus, since φ is injective, $x = 0$. It follows that $x/t = 0/t$, so $\ker\tilde{\varphi} = 0$, as desired. $\square$

3.3 Chapter 7: Introduction to Rings

From Dummit and Foote (2004).

Section 7.5: Rings of Fractions

1/30:

- Let R be a *commutative* ring throughout this section.
- Review of how zero divisors are similar to units in some ways and dissimilar in other ways.
- "The aim of this section is to prove that a commutative ring R is always a subring of a larger ring Q in which every nonzero element of R that is not a zero divisor is a unit in Q" (Dummit & Foote, 2004, p. 260).
  - If R is an integral domain, Q will be its **field of fractions** or **quotient field**.
- Review of the construction and properties of $\mathbb{Q}$.

- Why we can't include zeroes or zero divisors in the denominators.
  - Suppose b is a zero or zero divisor such that $bd = 0$.
  - If we allow b as a denominator, then
    $$d = \frac{d}{1} = \frac{bd}{d} = \frac{0}{b} = 0$$
  - Thus, there is a certain "collapsing," and we cannot expect that R appears as a natural subring of this "ring of fractions."
- Why we must have closure under multiplication for the denominators.
  - Review from class.
- "The main result of this section shows that these two restrictions are sufficient to construct a ring of fractions for R. Note that this theorem includes the construction of $\mathbb{Q}$ from $\mathbb{Z}$ as a special case" (Dummit & Foote, 2004, p. 261).

  Theorem 15. Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors, and is closed under multiplication (i.e., $ab \in D$ for all $a, b \in D$). Then there is a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q. The ring Q has the following additional properties.

  1. Every element of $\mathbb{Q}$ is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R \setminus \{0\}$, then Q is a field.
  2. (Uniqueness of Q) The ring Q is the "smallest" ring containing R in which all elements of D become units in the following sense. Let S be any commutative ring with identity and let $\varphi : R \to S$ be any injective ring homomorphism such that $\varphi(d)$ is a unit in S for every $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi|_R = \varphi$. In other words, any ring containing an isomorphic copy of R in which all the elements of D become units must also contain an isomorphic copy of Q.

  Proof. Given.

  Same as in class: A general construction of Q, confirmation of its properties, and then the steps of the analogous theorem. Very well written, though, should I need additional insight in the future! ☐

- Theorem 36 in Section 15.4 generalizes Theorem 15 by allowing D to contain zero and/or zero divisors.
- Definition of the **ring of fractions** and **field of fractions**.
- **Subfield generated by A**: The subfield of F equal to the intersection of all subfields of F containing A, where A is some subset of a field F.
- The subfield generated by A is the smallest subfield of F containing A.
- The smallest field containing an integral domain R is its field of fractions.

  Corollary 16. Let R be an integral domain and let Q be the field of fractions of R. If a field F contains a subring R' isomorphic to R, then the subfield of F generated by R' is isomorphic to Q.

  Proof. Given. ☐

- Examples.
  1. $\operatorname{Frac} F \cong F$ for any field F.
  2. $\operatorname{Frac} \mathbb{Z} = \mathbb{Q}$.

    - Quadratic integer rings from Section 7.1 are brought up again.

3. $\text{Frac}(2\mathbb{Z}) = \mathbb{Q}$.
    - Notice how an identity "appears" in the field of fractions.
4. The **rational functions**.
    - $\text{Frac}(R[X])$ contains $\text{Frac}(R)$.
    - $\text{Frac}(R[X]) = \text{Frac}(R)(X)$.
        - Example: We have that

$$\text{Frac}(\mathbb{Z}[X]) = \text{Frac}(\mathbb{Q}[X]) = \mathbb{Q}(X) = \text{Frac}(\mathbb{Z})(X)$$

        - We can easily see this since if $p(X)/q(X) \in \text{Frac}(\mathbb{Q}[X])$, then there exists $N \in \mathbb{Z}$ such that $Np(X), Nq(X)$ both have integer coefficients (pick, for example, N to be the common denominator of all the coefficients in $p(X), q(X)$). Then $p(X)/q(X) = Np(X)/Nq(X) \in \text{Frac}(\mathbb{Z}[X])$, as desired.
5. $R_d = R[1/d] = D^{-1}R$, where $D = \{1, d, d^2, d^3, \dots\}$.

- **Rational functions** (in X over R): The field of fractions of the polynomial ring $R[X]$, where R is an integral domain and hence $R[X]$ is an integral domain. *Denoted by* $\textbf{Frac}(\boldsymbol{R[X]})$.
- **Field of rational functions**: The rational functions in X over a field F. *Denoted by* $\boldsymbol{F(x)}$.