Week 5

Characterizing Polynomials

5.1 Prime Factorizations

1/30:

- Midterm next Monday.
  - There's a list of topics on Canvas.
  - Don't worry about quadratic fields (or any of the other examples in Chapter 7 of Dummit and Foote (2004)). These are interesting, but will be saved for the absolute end of the course.
  - After the midterm, Nori will start on modules.
  - We've been talking about fields, which are contained in EDs, which are contained in PIDs. There probably will not be anything on EDs. Use the weakest definition for ED (the ones in class and the book differ). Which is this??
  - PIDs are contained in UFDs, which are contained in integral domains, which are contained in commutative rings.
- PIDs are nice!
  - For instance, $\gcd(a, b)$ can be computed in them without factoring a, b.
  - This is accomplished with the Euclidean Algorithm.
    - Review page 2 of Chapter 8, as referenced in a previous class, for more context.
- In PIDs, you can factor $a = qb + r$, but q, r may not be specific; in EDs (under a nice norm), these q, r are unique.
  - Is this correct??
  - It can be proven that if R is an ED, $a = qb + r$ for $a, b \in R - \{0\}$ and $q, r \in R$ with $N(r) < N(b)$, then r, q are unique iff $N(a + b) \leq \max\{N(a), N(b)\}$.
  - For instance, we have this for $\mathbb{Z}$ under $|n|$ and for $R[X]$ under $2^{\deg(p)}$.
- Theorem: R is a UFD implies $R[X]$ is a UFD.
- Corollary: R is a UFD implies $R[X_1, \ldots, X_n]$ is a UFD.

  Proof. Use induction. □
- Corollary: $R[X]$ is a field implies R is a PID implies $R[X_1, \ldots, X_n]$ is a UFD.
  - Something about $\mathbb{Z}$, $F[[X]]$ where F is a field??
  - These are examples of PIDs.

- Example: What are the irreducibles of $\mathbb{Z}[X]$?
  - Prime numbers.
  - Let $g \in \mathbb{Q}[X]$. Assume g is monic. Then $g(X) = X^d + a_1X^{d-1} + \cdots + a_d$ for all $a_i \in \mathbb{Q}$. There exists $n \in \mathbb{N}$ such that $ng(X) \in \mathbb{Z}[X]$. Let n be the least natural number for which this is true. It follows by our hypothesis that n is the smallest such n that the coefficients of ng are relatively prime. Conclusion: $ng(X)$ is irreducible in $\mathbb{Z}[X]$.
- Takeaway: There are two types of irreducibles (those from $\mathbb{Z}$ and the new ones).
  - This statement has a clear parallel for every UFD.
- Let R be a UFD, and let $\mathcal{P}(R) \subset R - \{0\}$ be such that...
  (i) Every $\pi \in \mathcal{P}(R)$ is irreducible.
  (ii) For all $\alpha \in \mathbb{R} - \{0\}$, α irreducible, there exists a unique $\pi \in \mathcal{P}(R)$ such that $(\alpha) = (\pi)$.
- Statement (*): Every nonzero element $\alpha \in R$ is uniquely expressible as

$$\alpha = u \prod_{\pi \in \mathcal{P}(R)} \pi^{k(\pi)}$$

  where $u \in R^\times$ and for all π, $k(\pi) \in \mathbb{Z}_{\geq 0}$ and $|\{\pi \in \mathcal{P}(R) : k(\pi) > 0\}|$ is finite.

  Proof. R is a UFD implies (*). □
- Conversely, if $\mathcal{P}(R)$ is a subset of an integral domain R such that (*) holds, then R is a UFD.

  Proof. Note that $\pi \in \mathcal{P}(R)$ implies π is irreducible.

  Argument for something?? Let $\pi = ab$. Suppose $a = \pi^{m_0}\pi^{m_1}\cdots\pi_h^{m_h}u$ and $b = \pi^{n_0}\pi_1^{n_1}\cdots\pi_h^{n_h}$. Then $\pi = ab = \pi^{m_0+n_0}\pi^{m_1+n_1}\cdots$. But then because of unique factorization, we cannot have $\pi_1^{x_1}\cdots\pi_h^{x_h}$. □
- **Content** (of $f \in R[X]$): The greatest common divisor of the coefficients of a nonzero $f = a_0 + a_1X + a_2X^2 + \cdots$ in $R[X]$. *Denoted by* $\boldsymbol{c(f)}$. *Given by*

$$c(f) = \gcd(a_0, a_1, a_2, \dots)$$

- Let $c(f) = \prod_{\pi \in \mathcal{P}(R)} \pi^{k(\pi)}$.
- Gauss lemma: $f, g \in R[X]$ both nonzero implies that $c(fg) = c(f)c(g)$.

  Proof. For our purposes, it will suffice to prove the case where $c(f) = c(g) = 1$. This is because our ultimate purpose in proving this lemma is to show that a polynomial in $R[X]$ that is not irreducible is reducible specifically in $R[X]$, i.e., we need not resort to higher container rings such as $\operatorname{Frac} R$ in which we could reduce $p \in R[X]$. Let's begin.

  Let $\pi \in R$ be irreducible (hence prime). Consider the canonical surjection $R \to R/(\pi)$. It gives rise to a ring homomorphism $\varphi : R[X] \to R/(\pi)[X]$ defined by

$$\varphi(a_0 + a_1X + \cdots + a_dX^d) = \bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_dX^d$$

  In words, the ring homomorphism takes any input polynomial and reduces all of its coefficients modulo p. Moving on, $c(f) = 1$ implies that there exists i such that $\bar{a}_i \neq 0$ (if $c(f) = \pi$, for instance, then all $\bar{a}_i = 0$). Therefore, $\varphi(f) \neq 0$. Similarly, $c(g) = 1$ implies that $\varphi(g) \neq 0$. It follows since $R/(\pi)$ is an integral domain and thus contains no zero divisors that $\varphi(fg) = \varphi(f)\varphi(g) \neq 0$. Consequently, $\pi \nmid c(fg)$ (again, if $\pi \mid c(fg)$, then all coefficients would be divisible by π, hence would be equivalent to 0 mod π, hence $\varphi(fg)$ would equal 0). Clearly, this argument holds for any $\pi \in R$ irreducible. Thus, since $c(fg)$ is not divisible by any element of R, we must have that $c(fg) = 1$. □

- This proof can be done by brute force without quotient rings, and elegantly with quotient rings. Dummit and Foote (2004) does both and we should check this out. The above is Nori's cover of just the latter, elegant argument.
- Let K be the fraction field of R. We know that $K[X]$ is a PID (hence a UFD, etc.). The primes are the irreducible monic polynomials. Let $g = a_0 + a_1X + \cdots + a_{d-1}X^{d-1} + X^d \in K[X]$ be monic. Then there exists a nonzero $\alpha \in R$ such that $R[X] \subset K[X]$. It follows that $a_i = \alpha_i/\beta_i$ for some $\alpha_i, \beta_i \in R$ with $\beta_i \neq 0$ since $K = \operatorname{Frac} R$.
- Claim 1: There exists a unique $\beta \in R$, $\beta = \prod_{\pi \in \mathcal{P}(R)} \pi^{k(\pi)}$, such that $\beta g \in R[X]$ and $c(\beta g) = 1$.

  Proof. Denote βg by $\tilde{g}$. Then the claim is that $\tilde{g} \in R[X]$ has content 1. Thus,

  $$\frac{\tilde{g}}{\ell(\tilde{g})} = g$$

  □
- Claim 2: $g \mapsto \tilde{g}$ is a monic polynomial in $K[X]$. Then $\tilde{g} \in R[X]$ with content 1 and

  $$\widetilde{gh} = \tilde{g} \cdot \tilde{h}$$

  Proof. Use the Gauss lemma. □
- Statement (*) holds as a result.
- $\mathcal{P}(R[X]) = \mathcal{P}(R) \sqcup \{\tilde{g} : g \in K[X] \text{ is monic and irreducible}\}$.
- Claim 3: (*) holds for $\mathcal{P}(R[X])$.

  Proof. Scratch: Let $f \in R[X]$ be nonzero. Then $f/\ell(f) \in K[X]$ for each g_i monic and irreducible. $\widetilde{\frac{f}{\ell(f)}} = \tilde{g}_1^{k_1} \cdots \tilde{g}_r^{k_r}$. We have $f, \tilde{g}_1^{k_1} \cdots \tilde{g}_r^{k_r} \in R[X]$. $f = \beta(\tilde{g}_1^{k_1} \cdots \tilde{g}_r^{k_r})$. $\beta \in R$. □
- Two remaining lectures on rings: Factoring polynomials in $\mathbb{Z}[X]$ and $\mathbb{R}[X]$.

5.2 Office Hours (Nori)

- Problem 4.1?
  - See picture.
- Lecture 2.2: "We need bijectivity because continuous functions don't necessarily have continuous inverses?"
  - We can use "$f : R_1 \to R_2$ is a ring homomorphism plus bijection" as the definition of isomorphism.
  - An equivalent definition is, "there exists a ring homomorphism $g : R_2 \to R_1$ such that $g \circ f = \mathrm{id}_{R_1}$ and $f \circ g = \mathrm{id}_{R_2}$."
  - Even though the first is simpler, the reason people use the second is because in some contexts, there *is* a difference between the definitions (such as with homeomorphisms, whose inverses need to be continuous [think proper]).
- Lecture 2.2: We have only defined the finite sum of ideals, not an infinite sum, right?
  - We defined an infinite sum, too.
  - In particular, $\sum_{i \in I} M_i = \bigcup_{F \subset IF \text{ is finite}}$.

  - Note that in a more general sense, you can have infinitely generated ideals. For example, infinite polynomials.

- Lecture 2.2: $IJ = I \cap J$ conditions.
  - $IJ \subset I \cap J$ in commutative rings.
  - Counterexample: $R = \mathbb{Z}$ and $I = (d)$ and $J = (d)$. Then $IJ = (d^2) \neq (d) = I \cap J$.
  - Equality is meaningful.

- To what extent are we covering Chapter 9, and to what extent will reading it help my understanding of the course content?
  - Just the result that $F[X]$ is a PID (implies UFD).
  - All we need from Chapter 8 for the midterm is ED implies PID, all we need from Chapter 9 for the midterm is PID implies UFD.
  - Main examples of PIDs are $\mathbb{Z}$, $F[X]$, and $F[[X]]$.

- Have we done anything outside Chapters 7-9, or if I understand them, am I good to go?
  - The Euclidean algorithm for monic polynomials may not be in Chapter 8.

- Lecture 3.1: Everything from creating $\mathbb{C}$ from $\mathbb{R}$, down.
  - We use monic polynomials just so that we can apply the Euclidean algorithm (EA).
  - We want to find ring homomorphisms $\varphi : R[X] \to A$ such that $\varphi(X^2 + 1) = 0$. How do I get hold of a φ and an A? There's exactly one way to do it. We use the universal property of a polynomial ring.
  - We want $X^2 + 1 \in \ker \psi$, so we define $R[X]/(X^2 + 1)$.
  - $R[X]/(X^2+1)$ generalizes the construction of the complex numbers. Creating a new ring in which $X^2 + 1 = 0$ has a solution.
  - Suppose R is a ring such that $f(X) \in R[X]$ doesn't have a solution. Then it does have a solution in $R[X]/(f(X))$.
  - We recover $\mathbb{C}$ as a special case of this more general construction, specifically the case where $f(X) = X^2 + 1$.

- Lecture 3.2: Do I have it right that the only nontrivial ideals of $\mathbb{Q}$ are the dyadic numbers, $\mathbb{Z}_{(2)}$, and (2^n)? Why is this? What about the triadics, for instance?
  - In $\mathbb{Z}_{(2)}$, the only ideals are of the form (2^n) for some n.

- Lecture 3.2: What is the significance of the final theorem?
  - That all rings with the D-to-units property bear a certain similarity to the ring of fractions.

- Section 7.5: Difference between the rational functions and the field of rational functions?

- Lecture 4.1: What all is going on with $F[[X^{1/2^n}]]$?
  - The idea is the irreducible elements of one ring can become reducible in the context of other rings. This is just a specific example; note how X is the only irreducible element in the first ring, but it reduces to $X = (X^{1/2})^2$ in the next ring, and so on.

- Lecture 4.3: Speech for PIDs over UFDs?

- Lecture 4.3: $R - \{0\}$ or R is an integral domain.
  - Takeaway: You don't need to factor a, b to get their gcd; indeed, you can just find a single generator of (a, b).

- Lecture 4.3: Products of commutative diagrams?
- Lecture 5.1: What is the weakest definition for an ED?
  - The *book* teaches the weakest one.
  - *We're* only interested in Euclidean domains with positive norms.
- Lecture 5.1: Uniqueness condition in the Euclidean algorithm.
- Lecture 5.1: The thing about $\mathbb{Z}$ and $F[[X]]$.
  - These are the only rings we've talked about that are PIDs. Gaussian integers are, too, but we haven't proved that yet.
- Lecture 5.1: Argument for something — is this part of the proof of the converse statement?
- Lecture 5.1: Correct notation?
- What is the set $\mathbb{Z}[X, Y, Z, W]_{XW-YZ}$ in Q4.6b?
  - Like R_f.
- What is the purpose of the commutative diagram in Q4.7?
- Where does d come into play in Q4.10?
  - We're gonna prove that the cardinality of the set is less than or equal to d. About the number of roots of a polynomial of a certain degree, like how $X^3 + \cdots$ can't have more then 3 roots. The most relevant property is that $\mathbb{R}$ is an integral domain.

5.3 Factorization Techniques

2/1:
- Notes on HW4 Q4.1.
  - A lot of people have asked questions about this.
  - The point is to get used to universal properties.
  - Universal properties are important because...
    - They will come up time and time again;
    - They will be especially important if/when we get to tensor products;
    - Two objects that satisfy the same universal property are isomorphic.
- We've introduced a lot of theory at this point, but everything is getting used more and more.
- Today: Factoring polynomials. We will look at two methods to do so.
- Assumption for this lecture: Let $f = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ have $c(f) = 1$.
- Factorization prep.
  - Today's ring of interest: $\mathbb{Z}[X]$.
  - We want to test reducibility. Recall from Lecture 5.1 that...
    - If $\deg(f) > 0$, then f is irreducible in $\mathbb{Z}[X]$ iff $c(f) = 1$ and f is irreducible in $\mathbb{Q}[X]$.
    - Why we need the latter condition even though I don't think it was mentioned last lecture (motivation via examples).
      - ➢ Consider $X^2 - 1/4 \in \mathbb{Q}[X]$. This polynomial reduces to $(X - 1/2)(X + 1/2)$. Thus, taking $n = 4$, $4X^2 - 1$ is still reducible in $\mathbb{Z}[X]$ as it equals $(2X - 1)(2X + 1)$.

➢ Consider $X^2 - 1/3 \in \mathbb{Q}[X]$. This polynomial reduces to $(X - 1/\sqrt{3})(1 + 1/\sqrt{3})$ in $\mathbb{R}[X]$, but is irreducible in $\mathbb{Q}[X]$. Thus, taking $n = 3$, $3X^2 - 1$ is still irreducible in $\mathbb{Z}[X]$.

➢ This is the logic underlying Proposition 9.5.

■ If $\deg(f) = 0$, then f is irreducible in $\mathbb{Z}[X]$ iff f is a prime integer.

– Recall that $\ell(f)$ denotes the leading coefficient.

– If f is irreducible in $\mathbb{Q}[X]$, then so is $f/\ell(f)$, but now $f/\ell(f)$ is monic.

– Consider $f \mapsto f/\ell(f)$. It sends

$$\{f \in \mathbb{Z}[X] : f \text{ is irreducible and } \deg(f) > 0\} \to \{\text{monic irreducible polynomials in } \mathbb{Q}[X]\}$$

– The above is not a bijection as is, but if we treat $\pm f$ as the same, then it is. In other words,

$$\pm\backslash\{f \in \mathbb{Z}[X] : f \text{ is irreducible and } \deg(f) > 0\} \cong \{\text{monic irreducible polynomials in } \mathbb{Q}[X]\}$$

where the isomorphism is defined as above.

- Factorization by monomials.

– How many $g(X) = aX + b$ are there in $\mathbb{Z}[X]$ that divide f?

– If $aX + b \mid f$, then $a \mid a_0$ and $b \mid a_n$.

– We know that $a_0 > 0$ by the definition of the X^n term as the leading term. It may be either way with a_n.

■ For the sake of continuing, we will assume that $a_n \neq 0$. Why?? Perhaps because then we would have $b = 0$ in one monomial and 0 doesn't divide anything?

■ We also assume that $\gcd(a, b) = 1$.

– Because of the above constraint, we know that

$$\{g \in \mathbb{Z}[X] : \deg g = 1,\ g \mid f\} \subset \text{known finite set}$$

where the latter set consists of all monomials g with $a \mid a_0$ and $b \mid a_n$.

– $aX + b \mid f$ in $\mathbb{Z}[X]$ iff $aX + b \mid f$ in $\mathbb{Q}[X]$ iff $f(-b/a) = 0$.

– Note: If $\deg(f) \leq 3$ and f is reducible, then there exists $g \in \mathbb{Z}[X]$ such that $\deg(g) = 1$ and $g \mid f$.

■ Let $f = gh$. We know that $3 \geq \deg(f) = \deg(g) + \deg(h)$. Since $c(f) = 1$ by hypothesis, $\deg(g) \neq 0 \neq \deg(h)$. Thus, $1 \leq \deg(g) \leq 3 - \deg(h) \leq 2$ and a similar statement holds for $\deg(h)$. If $\deg(g) = 1$, then we are done. If $\deg(g) = 2$, then $\deg(h) = 1$, and we are done.

■ When we get to $\deg(f) = 4$, the above argument obviously won't work (it would be perfectly acceptable to have $\deg(g) = \deg(h) = 2$ here, for instance).

- We now move on to actual factorization techniques.

- Method 1: **Kronecker's method**.

– This method should be covered in the book somewhere.

- Let f have the same n-degree form as above.

- Let $1 \leq d \leq n$. Does there exist $g \in \mathbb{Z}[X]$ with $c(g) = 1$ and $\deg(g) = d$ such that $g \mid f$?

- Select $d + 1$ distinct integers $c_0, \ldots, c_d$.

- Easy lemma: Let $c_0, \ldots, c_d \in F$ be distinct, and let

$$P_d = \{g \in F[X] : \deg(g) \leq d\}$$

be a a $(d + 1)$-dimensional vector space. Then $T : P_d \to F^{d+1}$ given by

$$T(g) = (g(c_0), \ldots, g(c_d))$$

is an isomorphism of F-vector spaces.

Proof. P_d and F^{d+1} both have the same dimension. Thus, to prove bijectivity of this linear transformation, it will suffice to prove injectivity. To do so, we will show that $\ker(T) = \{0\}$. Let $g \in \ker(T)$ be arbitrary. Then

$$T(g) = 0$$
$$(g(c_0), \ldots, g(c_d)) = (0, \ldots, 0)$$

Thus, g has $d+1$ distinct roots $c_0, \ldots, c_d$. It follows that $g \in ((X - c_0) \ldots (X - c_d))$, meaning that $g = 0$ or $\deg(g) \geq d+1$. However, $g \in P_d$ by hypothesis as well, meaning $\deg(g) \leq d$. Therefore, $g = 0$, as desired. □

- There is an alternative proof of this result that doesn't deal with any existence business but just gives you a formula for computing T.
- Corollary: Given $e_0, \ldots, e_d \in F$ arbitrary, there exists a unique $g \in P_d$ such that $g(c_i) = e_i$ $(i = 0, \ldots, d)$.
  - Note that this is less a corollary and more a restatement of the lemma: A "unique" element of the domain speaks to bijectivity.
- If such a g exists, then $f = gh$ for some $h \in \mathbb{Z}[X]$. It follows that it is uniquely determined by its the values $g(c_0), \ldots, g(c_d)$. But $g(c_i) \mid f(c_i)$ for all $i = 0, \ldots, d$. Note that if $f(c_i) = 0$, then $X - c_i \mid f$ in $\mathbb{Z}[X]$.
- Now consider $S_i = \{u_i \in \mathbb{Z} : u_i \mid f(c_i)\}$. Then $S_0 \times \cdots \times S_d \subset \mathbb{Q}^{d+1}$.
- Take $F = \mathbb{Q}$. Then $T : P_d \to \mathbb{Q}^{d+1} \supset S_0 \times \cdots \times S_d$ where T is an isomorphism.
- It follows that $g \in T^{-1}(S_0 \times \cdots \times S_d) \cap \mathbb{Z}[X] \cap \{g : c(g) = 1\}$. Thus, g is an element of a finite set that is somewhat "known."
- Check whether or not $g \mid f$ (use the Euclidean Algorithm for monic polynomials).
- Then $f(X) = (X - c_0) \cdots (X - c_n) + b$
- Method 2.
  - Basic philosophy: Given a monic polynomial over $\mathbb{C}$ and for which you know all of the coefficients, said coefficients yield an upper bound on the value of every root.
- Lemma: Let $f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{C}[X]$ have $a_0 \neq 0$. Define the number

$$C = \max\left\{\left|\frac{a_1}{a_0}\right|, \left|\frac{a_2}{a_0}\right|^{1/2}, \ldots, \left|\frac{a_n}{a_0}\right|^{1/n}\right\}$$

The elements in the max set are the coefficients of $1/\ell(f)$. If $z \in \mathbb{C}$ and $f(z) = 0$, then $|z| \leq 2C$. Moreover,

$$\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} = 1$$

Proof. If $C = 0$, you're done. Thus, we assume that $C \neq 0$.

WLOG, take $a_0 = 1$ so that f is monic (if $a_0 \neq 1$, divide through by a_0). It follows that

$$\begin{aligned} 0 &= 1z^n + a_1 z^{n-1} + \cdots + a_n \\ -z^n &= a_1 z^{n-1} + \cdots + a_n \\ -1 &= a_1 \frac{1}{z} + a_2 \frac{1}{z^2} + \cdots + a_n \frac{1}{z^n} \\ &= \left(\frac{a_1}{C}\right)\left(\frac{C}{z}\right) + \left(\frac{a_2}{C^2}\right)\left(\frac{C}{z}\right)^2 + \cdots + \left(\frac{a_n}{C^n}\right)\left(\frac{C}{z}\right)^n \end{aligned}$$

By the definition of C, we have that

$$|a_r|^{1/r} \leq C$$

Thus, $|a_r| \leq C^r$ and hence $|a_r/C^r| \leq 1$. We now can relate back to the above.

If $|C/z| \leq 1/2$, this contradicts the triangle inequality (why??), so we must have $|C/z| > 1/2$ or $|z/C| < 2$ so $|z| < 2C$.

We now want $g \in \mathbb{Z}[X]$ with $c(g) = 1$, $\deg(g) = d$, and $g \mid f$ in $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{C}[X]$. We have $g = b_0X^d + b_1X^{d-1} + \cdots + b_d$ ($b_i \in \mathbb{Z}$). Thus, $g/b_0 = (X - z_1)\cdots(X - z_d)$ with $f(z_1) = \cdots = f(z_d) = 0$. Then we have the following by expanding.

$$= X^d - \left(\sum_{i=1}^{d} z_i\right) X^{d-1} + \left(\sum_{1 \leq i \leq j \leq d} z_i z_j\right) X^{d-2} + \cdots$$

The second term is equal to b_1/b_0; the third is b_2/b_0; etc. We thus have an upper bound

$$|b_r/b_0| \leq (2C)^r \binom{d}{r}$$

Note that $\ell(g) \mid \ell(f)$. The search for the coefficients is now limited to a finite space, and we are done. $a_0b_r/b_0 \in \mathbb{Z}$ and we have an upper bound on its absolute value, specifically the following which, at this point, we can turn over the problem to someone with a computer to solve.

$$|a_0b_r/b_0| \leq (2C)^r \binom{d}{r}(a_0)$$

□

- A great technique for reducing polynomials modulo a prime number.
  - Consider $0^2, 1^2, 2^2, 3^2, 4^2 \pmod 5$. This is $\{0, \pm 1\}$. It follows that $m \equiv \pm 2 \pmod 5$. $X^2 - m \in \mathbb{Z}[X]$ is irreducible, but $(X^2 - m) = (X - h)(X + h)$ implies that $X^2 - h^2 \equiv m \pmod 5$.

5.4 Office Hours (Callum)

- Lecture 3.2: Is the final theorem the "Universal Property of the Ring of Fractions?"
- I^e means extending I. If $f : A \to B$ where $I \subset A$, then $I^e = (f(I)) \subset B$ ($f(I)$ is not an ideal in B unless f is surjective). Similarly, the contraction J^c of some $J \subset B$ is $J^c = f^{-1}(J)$ (this is already an ideal).
- I asked misc. questions about the HW4 problems as I went through them.

5.5 Prime Ideals of Complex Polynomials

2/3:

- Last lecture on rings for a while.
- Monday begins modules.
- Today: Applications of the Gauss lemma.
- Questions to answer today.
  1. Prime ideals of $\mathbb{C}[X, Y]$.
  2. Branched coverage.
  3. Relation between topology and algebra.

- Prerequisites for today: The following lemma.
- Lemma: Let R be a UFD and $K = \operatorname{Frac} R$. Then there exists a bijection

$$R^\times \backslash \{f \in R[Y] : \deg_Y(f) > 0,\ c(f) = 1\} \cong K^\times \backslash \{f \in K[Y] : \deg_Y(f) > 0\}$$

  defined by $f \mapsto f$.

  - This bijection sends irreducibles to irreducibles.
  - We should have proven this on Monday.
- Example: $R = \mathbb{C}[X]$ and $K = \mathbb{C}(X)$.
- What are the prime ideals P in $\mathbb{C}[X, Y]$?
  - $\{0\}$.
  - (f) where f is irreducible.
  - Are there any others?
- We presently build up to answering this question.
  - Let $P \in \mathbb{C}[X, Y]$ be a nonzero prime ideal. Pick a nonzero $f \in P$. Let $f = f_1 \cdots f_r$, where each f_i is irreducible.
  - Since P is a prime, it follows that one of the f_i must be an element of P.
  - Additionally, $(f_i) \subset P$. Then assuming that $(f_i) \neq P$, there exists $g_i \in P$ such that $g_i \notin (f_i)$. Repeat the same argument for each f_j.
  - Then we get $(f_j, g_j) \subset P$. f_j, g_j are irreducible and $g \notin (f)$.
  - Case 0: If $f \in R = \mathbb{C}[X]$ and f is irreducible, then $(f) = (X - a)$. Recall that $\mathbb{C}[X, Y]/(X - a) \cong \mathbb{C}[Y]$ (the isomorphism is given by $f(X, Y) = f(a, Y)$). More generally, we have that $\mathbb{C}[X, Y]/P \cong \mathbb{C}[Y]/\phi(P)$ since $P \supsetneq (X - a)$ and hence $\phi(P) \neq 0$.
  - It follows that there exists a $b \in \mathbb{C}$ such that $\phi(P) = (Y - b)$. Thus, $P = (X - a, Y - b)$.
- **Nonzero** (ideal): An ideal I for which there exists a nonzero $f \in I$.
- We now state the theorem.
- Theorem: Every prime ideal of $\mathbb{C}[X, Y]$ is either...

  (i) $\{0\}$.

  (ii) (f) where f is irreducible.

  (iii) $(X - a, Y - b)$ for all $(a, b) \in \mathbb{C}^2$.

  The ideals (iii) are the maximal ideals. We define $\phi : \mathbb{C}[X, Y] \to \mathbb{C}$ by $\phi(f) = f(a, b)$; then $\ker \phi = (X - a, Y - b)$.

  Proof. Rest of the proof: Let $f, g \in P$ be such that $f, g \notin \mathbb{C}[X]$. It follows from the Gauss lemma that f, g are irreducible in $\mathbb{C}(X)[Y]$ and the gcd in $\mathbb{C}(X)[Y]$ is $(f, g) = 1$. It follows that there exist $A, B \in \mathbb{C}(X)[Y]$ such that $1 = Af + By$. Form of A, B: We have

$$A = \alpha_d Y^d + \cdots + \alpha_0$$

  where each $\alpha_i = u_i(X)/v_i(X)$ for $u_i, v_i \in \mathbb{C}[X]$. Similarly, $B = \beta_e Y^e + \cdots + \beta_0$ with a similar condition on the β_i. Let $h = \prod_i v_i \cdot \prod_j \omega_j$. Then h is nonzero and an element of $\mathbb{C}[X]$. It follows that $hA = A'$ and $hB = B'$ are elements of $\mathbb{C}[X, Y]$. It follows that $A'f + B'g = h$ where $A', B' \in \mathbb{C}[X, Y]$. Thus, $h \in (f, g) \subset P$. Thus, $h = \prod_{i=1}^{e}(X - a_i)$ and $X - a \in P$ for some $a \in \mathbb{C}$. And thus we have reduced to case 0. □

- Hilbert null statement The only maximum ideals of $\mathbb{C}[X_1, \ldots, X_n]$ are $(X_1 - a_1, \ldots, X_n - a_n)$ where $(a_1, \ldots, a_n) \in \mathbb{C}^n$.
  - This is outside this course.
- Exercise: Continue the proof to show that the collection $\{(a, b) \in \mathbb{C}^2 : f(a, b) = g(a, b) = 0\}$ is finite if both f, g are distinct and irreducible in the usual sense, i.e., $(f) \neq (g)$.
- The set

$$\{(a, b) \in \mathbb{C}^2 : (f \cdot g)(a, b) = 0\} = \{(a, b) \in \mathbb{C}^2 : f(a, b) = 0\} \cup \{(a, b) \in \mathbb{C}^2 : g(a, b) = 0\}$$

  minus a finite set is disconnected. *picture; draw diagram of Cartesian plane with missing origin!!*
- Example: Let $f = X$ and $g = Y$. Then $\{(a, b) \in \mathbb{C}^2 : ab = 0\}$ is the X, Y axes and it is disconnected if we remove a finite set of points (e.g., 0). Same in more general, curvy spaces.
- Consider one irreducible polynomial $f(X, Y) = a_0(X)Y^d + \cdots + a_d(X)$. where the $a_i \in \mathbb{C}[X]$ and $a_0(X) \neq 0$.
  - Freeze $X = c$.
  - Denote $f(c, Y)$ by $f_c(Y)$.
  - Take the intersection of $X = c$ and the polynomial in Y.
  - There is a finite set of distinct points. How do we know that there are at most d?
  - Now assume f is irreducible and in $\mathbb{C}[X][Y]$. Then f is irreducible in $\mathbb{C}(X)[Y]$.
  - Comparing f_c and $\partial f_c/\partial y = (\partial f/\partial y)_c$. The Y-degree of $\partial f/\partial y$ is $d - 1$. Since f is irreducible,

$$\gcd_{\mathbb{C}(X)[Y]}(f, \partial f/\partial y) = 1$$

  - Same game gives $A', B' \in \mathbb{C}[X, Y]$ and a nonzero $h \in \mathbb{C}[X]$ such that

$$A'(X, Y)f(X, Y) + B'(X, Y)\frac{\partial f}{\partial Y} = h(X)$$

- Now consider $\{c \in \mathbb{C} : a_0(c) \neq 0 \text{ and } h(c) \neq 0\}$.
- What we have shown is that if you omit a finite set of vertical lines, you understand the zeroes pretty well. This is called a **branched covering**.
- Complex analysis takes it from here.
- Theorem: If $f \in \mathbb{C}[X, Y]$ is square-free and not a constant, then $\{(a, b) \in \mathbb{C}^2 : f(a, b) = 0\}$ minus any finite set is connected iff f is irreducible.

5.6 Office Hours (Ray)

- For Q4.5a, do specify nonoverlapping ideals $(n)^e$.
- Q3.10?
  - The actually most important thing is working with the characteristic. We don't need a ton of detail on p, p^2. 1-2 sentences will suffice, just to show that we understand it follows from the additive group structure and Lagrange's theorem. p^2 case: $\mathbb{Z}/p^2 \cong R$. Multiplication is defined modulo p^2.

- The rest is the other case. As an additive group, we have it as a decomposition into the direct sum of two vector spaces $\mathbb{F}_p \langle 1 \rangle \oplus \mathbb{F}_p \langle \theta \rangle$. Now we just need to pin down $\theta^2 = \alpha\theta + \beta$. If $p \neq 2$, then division exists, so $\theta' = \theta - \alpha/2$. Then $\theta'^2 = \gamma \in \mathbb{F}_p$. If you bash it out, then the linear $\alpha/2$ term cancels. We want to say that there's only three different γs. We can change γ by scalars. γ matters up to $(\mathbb{F}_p^\times)^2$. Case 1: $\gamma = 0$. Second case: γ is a square (so pick $\gamma = 1$). Third case: γ is nonzero and not a square. Because any square is the same, there's only one case there. Three cases correspond to $\mathbb{F}_p[X]/X^2$, $(\mathbb{F}_p^\times)^2$, and $\mathbb{F}_{p^2}$. $X^2 - c$ is irreducible in this last case. So take $\mathbb{F}_p[X]/(X^2 - c)$. Irreducible in a PID implies prime implies maximal implies $\mathbb{F}_p[X]/(X^2 - c)$ is a field.
- A small number of people did it a cleaner way: We know we have a map from $\mathbb{F}_p[X] \to R$ by the universal property that sends $X \mapsto \theta$ and $\theta \notin i(\mathbb{F}_p)$. By the FIT, $\mathbb{F}_p[X]/(\ker \phi) \cong R$. For size reasons, $\ker \phi$ must be a quadratic. There are three cases then for a quadratic $X^2 + aX + b$: Irreducible, reducible to a product of two distinct factors, reducible to a square. These are analogous to the other cases in the other method. This is a nicer way of doing it since there's often a feeling in algebra like it's just definition upon definition, but this allows us to use some of the "algebra" we remember from high school!
- Let R be a ring with cardinality p^2 (we know that at least one exists: $\mathbb{Z}/p^2\mathbb{Z}$ under addition and multiplication mod p^2). Let $j : \mathbb{Z} \to R$ be a ring homomorphism. Then $j(0) = 0_R$ and $j(1) = 1_R$. It follows that $j(n) = n_R$. By the pidgeonhole principle, $j(p^2) = j(a)$ for some $a \in [0, p^2 - 1]$. Thus, the only values of $\mathbb{Z}$ we really need to worry about are where $[0, p^2 - 1]$ get sent since everything else is determined by these values. One option would be to send them all to distinct elements.
- As proven last quarter, there are only two abelian groups of cardinality p^2: $\mathbb{Z}/p^2\mathbb{Z}$ and $(\mathbb{Z}/p\mathbb{Z})^2$.

5.7 Chapter 9: Polynomial Rings

From Dummit and Foote (2004).

Section 9.1: Definitions and Basic Properties

2/5:

- Review of the definitions of **polynomial rings**, **formal sums**, **degrees**, **leading terms**, **leading coefficients**, **monic** polynomials, and polynomial **addition** and **multiplication**.
- Restatement of Proposition 7.4.

  Proposition 9.1. Let R be an integral domain and let $p(X), q(X)$ be nonzero elements of $R[X]$. Then

  1. $\deg p(X)q(X) = \deg p(X) + \deg q(X)$;
  2. The units of $R[X]$ are just the units of R;
  3. $R[X]$ is an integral domain.

- Recall that the quotient field of $R[X]$ is the field of rational functions in X with coefficients in R.
- Relating the ideals of R and $R[X]$.

  Proposition 9.2. Let I be an ideal of the ring R, and let $(I) = I[X]$ denote the ideal of $R[X]$ generated by I (the set of polynomials with coefficients in I). Then

  $$R[X]/(I) \cong (R/I)[X]$$

  In particular, if I is a prime ideal of R, then (I) is a prime ideal of $R[X]$.

  Proof. Given. □

- $I \subset R$ maximal $\not\Rightarrow$ $(I) \subset R[X]$ maximal.

- However, $I \subset R$ maximal $\Rightarrow (I, X) \subset R[X]$ maximal.
- Example.
  1. $R = \mathbb{Z}$ and $I = n\mathbb{Z}$.
     - The "reduction homomorphism" is given by reducing the coefficients of polynomials in $\mathbb{Z}[X]$ modulo n.
     - If n is composite, then $\mathbb{Z}[X]/(n\mathbb{Z}) = \mathbb{Z}[X]/n\mathbb{Z}[X]$ is not an integral domain.
     - If p is prime, then $\mathbb{Z}[X]/(p\mathbb{Z})$ is an integral domain — and in fact an ED as well.
     - Additionally, $p\mathbb{Z}[X] \subset \mathbb{Z}[X]$ is a prime ideal.
- We now introduce polynomial rings in several variables.
- **Polynomial ring** (in the variables $X_1, \ldots, X_n$ with coefficients in R): The ring defined inductively as follows. *Denoted by* $\boldsymbol{R[X_1, \ldots, X_n]}$. *Given by*

$$R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$$

  - Interpretation: Polynomials in n variables with coefficients in R are just "polynomials in *one* variable but now with coefficients that are themselves *polynomials in* $n-1$ *variables*" (Dummit & Foote, 2004, pp. 296–97).
  - Such a polynomial is a finite sum of nonzero **monomial terms**.
- **Monomial term**: A term of the following form, where $a \in R$ is the **coefficient** of the term and the $d_i \in \mathbb{Z}_{\geq 0}$. *Also known as* **term**. *Given by*

$$aX_1^{d_1} \cdots X_n^{d_n}$$

- **Monomial**: A monic term of the above form. *Given by*

$$X_1^{d_1} \cdots X_n^{d_n}$$

- **Monomial part** (of a term): The part $X_1^{d_1} \cdots X_n^{d_n}$ of a term $aX_1^{d_1} \cdots X_n^{d_n}$.
- **Degree** (in X_i of a term): The exponent d_i.
- **Degree** (of a term): The quantity defined as follows. *Denoted by* $\boldsymbol{d}$. *Given by*

$$d = d_1 + \cdots + d_n$$

- **Multidegree** (of a term): The ordered n-tuple of the following form, where the term corresponds to a nonzero polynomial in n variables. *Given by*

$$(d_1, \ldots, d_n)$$

- **Degree** (of a nonzero polynomial): The largest degree of any of its terms.
- **Homogeneous** (polynomial): A polynomial in which all terms have the same degree. *Also known as* **form**.
- **Homogeneous component** (of f of degree k): The sum of all the monomial terms in f of degree k, where f is a nonzero polynomial in n variables. *Denoted by* $\boldsymbol{f_k}$.
- To define a polynomial ring in an arbitrary number of variables with coefficients in R, we can take the union of all the polynomial rings in a finite number of variables.
  - Dummit and Foote (2004) also discusses another way to define such a ring using homogeneous components.
- Dummit and Foote (2004) gives an example in which all of the terms above are used.
- Each statement in Proposition 9.1 is true for polynomial rings with an arbitrary number of variables.
  - To see this, just induct.

Section 9.2: Polynomial Rings Over Fields I

- Herein, we focus on polynomial rings of the form $F[X]$, where F denotes a field.
- Dummit and Foote (2004) choose a different norm on $F[X]$ than Nori; they choose $N(p) = \deg(p)$ and $N(0) = 0$.
- Polynomial division.

  Theorem 9.3. Let F be a field. The polynomial ring $F[X]$ is a Euclidean Domain. Specifically, if $a(X)$ and $b(X)$ are two polynomials in $F[X]$ with $b(X)$ nonzero, then there are *unique* $q(X), R(X) \in F[X]$ such that
  $$a(X) = q(X)b(X) + r(X)$$
  with $r(X) = 0$ or $\deg r < \deg b$.

  Proof. Given (see Lecture 3.1).

  Differences between the two version: The in-class one does not assume that the coefficients lie in a field, and thus divisors are taken to be monic therein. Otherwise, the arguments are identical. □

- Further relating $F[X]$ to the terms from Chapter 8.

  Corollary 9.4. If F is a field, then $F[X]$ is a PID and a UFD.

  Proof. Follows from Theorem 9.3, Proposition 8.1, and Theorem 8.14. □

- Examples.
  1. $\mathbb{Z}[X]$ is not a PID.
     - Recall $(2, X)$.
  2. $\mathbb{Q}[X]$ is a PID.
     - Here, $(2, X) = (1) = \mathbb{Q}[X]$.
  3. $\mathbb{Z}/p\mathbb{Z}[X]$ is a PID.
     - Takeaway: The quotient of a ring that is *not* a PID *may* be a PID, itself.
     - Example: $(2, X)$ becomes (X) when $p = 2$, and (1) when $p \neq 2$.
  4. $\mathbb{Q}[X, Y]$ is not a PID.
     - $\mathbb{Q}[X, Y] = \mathbb{Q}[X][Y]$, and $\mathbb{Q}[X]$ is not a field.
     - (X, Y) is not principal.
- The quotient and remainder of Theorem 9.3 are independent of field extensions.
  - Suppose $F \subset E$ are both fields. Divide a by q in both $F[X]$ and $E[X]$. Applying the uniqueness condition in $E[X]$, we get that there is only one factorization in $E[X]$, which must be the same as the one in $F[X] \subset E[X]$.
  - It follows that $\gcd(a, b)$ is the same in both $F[X], E[X]$, since the gcd is obtained from the Euclidean Algorithm.

Section 9.3: Polynomial Rings That Are Unique Factorization Domains

- Allowing fractional coefficients makes calculations in $R[X]$ much nicer.
  - We know that $R \subset \operatorname{Frac} R = F$ for any integral domain R.
  - It follows by Theorem 9.3 that $F[X]$ is an ED, hence a PID and a UFD.
  - Thus, it is very nice to perform calculations on $R[X]$ in its containing ring $F[X]$.
  - We spend this section specifying how computations (e.g., factorizations of polynomials) in $F[X]$ can give information about $R[X]$.
- R a UFD is a *necessary* condition for $R[X]$ to be a UFD.
  - Suppose that $R[X]$ is a UFD.
  - Then any $r \in R \subset R[X]$ has a unique factorization in terms of the irreducibles of $R[X]$, specifically those of degree 0 (i.e., in R) since $\deg(r) = 0$. Thus, r has a unique factorization, and R must be a UFD.
- We now build up to proving that R being a UFD is also a *sufficient* condition for $R[X]$ to be a UFD.
  - Sketch: To do so, we'll factor in $F[X]$ and then "clear denominators."
- We begin by comparing the factorization of a polynomial in $F[X]$ to a factorization in $R[X]$.

  Proposition 9.5 (Gauss' Lemma)**.** Let R be a UFD with $\operatorname{Frac} R = F$, and let $p \in R[X]$. If p is reducible in $F[X]$, then p is reducible in $R[X]$. More precisely, if $p = AB$ for some nonconstant polynomials $A, B \in F[X]$, then there are nonzero elements $r, s \in F$ such that $rA = a$ and $sB = b$ both lie in $R[X]$ and $p = ab$ is a factorization in $R[X]$.

  Proof. The coefficients of A, B lie in F. Let d be a common denominator[1] of these coefficients. Then

  $$dp = a'b'$$

  where $a', b' \in R[X]$. If $d \in R^\times$, then the proposition is true with $a = d^{-1}a'$ and $b = b'$. If $d \notin R^\times$, then we continue.

  Since $d \notin R^\times$, we may write $d = p_1 \cdots p_n$ as a product of irreducibles in R. By Proposition 8.12, p_1 irreducible implies p_1 prime. Thus, by Proposition 9.2, $p_1 R[X]$ is prime in $R[X]$. Consequently, by Proposition 7.13, $(R/p_1R)[X] \cong R[X]/p_1R[X]$ is an integral domain. Reducing the equation modulo p_1 yields

  $$0 = \overline{a'} \cdot \overline{b'}$$

  Moreover, since $(R/p_1R)[X]$ is an integral domain, at least one of $\overline{a'}, \overline{b'}$ is zero. Suppose that $\overline{a'} = 0$. Then the coefficients of a' are congruent to 0 modulo p_1, i.e., are divisible by p_1 so that $\frac{1}{p_1}a'$ has coefficients in R. Since $p_1 \mid d$ by definition as well, we can divide p_1 from both sides of $dp = a'b'$ to obtain an equation in which every term still has coefficients in R. Iterating the process allows us to cancel out all of the factors of d, leaving an equation $p = ab$ with $a, b \in R[X]$ and a, b being F-multiples of A, B, respectively, as desired. □

- Relation to the Gauss Lemma, as presented in Lecture 5.1.
  - If the gcd of the coefficients of fg is 1, then $fg \in R[X]$. Nori's Gauss Lemma proves that the coefficients of fg being in $R[X]$ imply that the coefficients of both f, g are only divisible by 1, i.e., are in $R[X]$ as well.
  - Essentially, Nori's Gauss lemma skips the whole business with fraction fields and just goes straight from polynomials in $R[X]$ to reducibility in $R[X]$.

[1] We may choose the *greatest* common denominator, but we don't need to in this case.

  - Nori's version probably is better and more powerful.
  - Perhaps it's a bit like Proposition 9.5 rolls Nori's version, Claim 1, and Claim 2 from class all into one statement.

- Example:
  - Let $R = \mathbb{Q}$, $F = \mathbb{Q}$.
  - Consider $p(X) = 2X^2 + 7X + 3 \in \mathbb{Z}[X]$.
  - We know that p is reducible in $\mathbb{Q}[X]$. In particular, we have that
$$p(X) = (X + \tfrac{1}{2})(2X + 6)$$
  - Choose 2 as a common denominator. Then we have
$$2p(X) = (2X + 1)(2X + 6)$$
which is a factorization of $2p$ in $\mathbb{Z}[X]$.
  - The prime factorization of d is just 2. Reducing the coefficients above modulo 2, we get
$$0 = (0X + 1)(0X + 0) = 1 \cdot 0$$
  - Evidently, $2X + 6$ has coefficients which are divisible by 2, so we may take $\frac{1}{2}(2X + 6)$ to get
$$p(X) = (2X + 1)(X + 3)$$

- The only difference between the irreducible elements in $R[X]$ and $F[X]$: That all elements of R become units in the UFD $F[X]$, so (for example) $7X = 7 \cdot X$ in $\mathbb{Z}[X]$, but $7X$ is irreducible in $\mathbb{Q}[X]$.

  Corollary 9.6. Let R be a UFD, left $F = \operatorname{Frac} R$, and let $p \in R[X]$. Suppose that the gcd of the coefficients of p is 1. Then p is irreducible in $R[X]$ iff it is irreducible in $F[X]$. In particular, if p is a monic polynomial that is irreducible in $R[X]$, then p is irreducible in $F[X]$.

  Proof. We prove this claim via double contrapositives.

  Suppose first that p is reducible in $F[X]$. Then by Gauss' Lemma, p is reducible in $R[X]$.

  Now suppose that p is reducible in $R[X]$. Then $p = ab$ for some $a, b \in R[X]$. Moreover, neither a nor b is constant as if (say a) were, then the assumption that the gcd of its coefficients is 1 would imply that $a = 1$, itself, i.e., a is a unit, contradicting the statement that ab is a factorization of p. This same factorization proves that p is reducible in F. □

- We can now prove the result we've been building up toward.

  Theorem 9.7. R is a UFD iff $R[X]$ is a UFD.

  Proof. Given. □

- Extending Theorem 9.7 to multivariable polynomials.

  Corollary 9.8. If R is a UFD, then a polynomial ring in an arbitrary number of variables with coefficients in R is also a UFD.

  Proof. Given. □

- Examples.
  1. $\mathbb{Z}[X]$ and $\mathbb{Z}[X, Y]$ are UFDs.

  - As mentioned earlier, $\mathbb{Z}[X]$ is a UFD that is not a PID.
2. $\mathbb{Q}[X]$, $\mathbb{Q}[X, Y]$, etc. are UFDs.

- "A nonconstant monic polynomial... is irreducible if and only if it cannot be factored as a product of two monic polynomials of smaller degree" (Dummit & Foote, 2004, p. 306).
- Polynomials that are irreducible in $R[X]$ for R an arbitrary *integral domain* are not necessarily irreducible in $(\operatorname{Frac} R)[X]$.
  - Dummit and Foote (2004) justifies this using an example with quadratic integer rings.

Section 9.4: Irreducibility Criteria

- **Irreducibility criterion**: An easy mechanism for determining when some types of polynomials are irreducible.
  - Simplify the typically laborious process of checking for factors.
- **Linear** (factor): A factor of degree 1.
- **Root** (in F of $p \in F[X]$): An $\alpha \in F$ with $p(\alpha) = 0$.
- When is there a linear factor?

  Proposition 9.9. Let F be a field and let $p \in F[X]$. Then p has a factor of degree one iff p has a root in F.

  Proof. Given (related to the example following the in-class proof of the Euclidean algorithm for monic polynomials in Lecture 3.1). □

- Reducibility in polynomials of small degree.

  Proposition 9.10. A polynomial of degree two or three over a field F is reducible iff it has a root in F.

  Proof. Given (see the argument under "Factorization by monomials" in Lecture 5.2). □

- Possible roots of polynomials with integer coefficients.

  Proposition 9.11. Let $p(X) = a_n X^n + \cdots + a_0$ be a polynomial of degree n with integer coefficients. If $r/s \in \mathbb{Q}$ is in lowest terms (i.e., $(r, s) = 1$ or r, s are relatively prime) and r/s is a root of $p(X)$, then r divides the constant term and s divides the leading coefficient of p:

  $$r \mid a_0 \qquad\qquad s \mid a_n$$

  In particular, if p is a monic polynomial with integer coefficients and $p(d) \neq 0$ for all integers d dividing the constant term of p, then p has no roots in $\mathbb{Q}$.

  Proof. Given (also related to the "Factorization by monomials" discussion from Lecture 5.2). □

- Note that Proposition 9.11 generalizes to $R[X]$ for any UFD R.
- Examples.
  1. $X^3 - 3X - 1$ is irreducible in $\mathbb{Z}[X]$.
     - Gauss' Lemma: To prove that it is irreducible in $\mathbb{Z}[X]$, it will suffice to show that it is irreducible in $\mathbb{Q}[X]$.

  - Proposition 9.10: To show that it is irreducible in $\mathbb{Q}[X]$, it will suffice to show that it has no roots in $\mathbb{Q}$.
  - Proposition 9.11: The only possible roots are the integers which divide the constant term 1, i.e., ± 1.
  - Since

$$(1)^3 - 3(1) - 1 = -3 \neq 0 \qquad (-1)^3 - 3(-1) - 1 = 1 \neq 0$$

    we have the desired result.

2. $X^2 - p$ and $X^3 - p$ are irreducible in $\mathbb{Q}[X]$ for any prime p.
   - Use the same strategy as above.
   - This is very related to my $X^2 - 1/4$ and $X^2 - 1/3$ example from Lecture 5.2, since 3 is prime and this implies irreducibility in $\mathbb{Q}[X]$.
3. $X^2 + 1$ is reducible in $\mathbb{Z}/2\mathbb{Z}[X]$.
4. $X^2 + X + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[X]$.
5. $X^3 + X + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[X]$.

- Treating higher degree polynomials.

  Proposition 9.12. Let I be a proper ideal in the integral domain R and let p be a nonconstant monic polynomial in $R[X]$. If the image of p in $(R/I)[X]$ cannot be factored in $(R/I)[X]$ into two polynomials of smaller degree, then p is irreducible in $R[X]$.

  Proof. Given. □

- This technique is not a be-all/end-all: "There are examples of polynomials even in $\mathbb{Z}[X]$ which are irreducible but whose reductions modulo every ideal are reducible (so their irreducibility is not detectable by this technique)" (Dummit & Foote, 2004, p. 309).

- Examples.

  0. $X^4 + 1$ is irreducible in $\mathbb{Z}[X]$ but reducible modulo every prime (see Chapter 14 for a proof of this). $X^4 - 72X^2 + 4$ is irreducible in $\mathbb{Z}[X]$ but is reducible modulo every integer.
  1. Using Proposition 9.12 to treat $X^2 + X + 1$ and $X^3 + X + 1$ again.
  2. The converse to Proposition 9.12 does not hold: $X^2 + 1$ is irreducible in $\mathbb{Z}[X]$ since is is irreducible in $\mathbb{Z}/2\mathbb{Z}[X]$ but it reducible mod 2.
  3. We can reduce modulo ideals in multivariable cases *to an extent*.
     - Some nonunit polynomials can reduce to units modulo certain ideals, creating challenges.

- A special case of reducing modulo an ideal to test for irreducibility.

  Proposition 9.13 (Eisenstein's Criterion)**.** Let P be a prime ideal of the integral domain R, and let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be a polynomial in $R[X]$ (here, $n \geq 1$). Suppose $a_{n-1}, \ldots, a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then f is irreducible in $R[X]$.

  Proof. Given. □

- This method is in frequent use.
  - Note that it was originally proven by Schönemann, so it is more properly known as the **Eisenstein-Schönemann Criterion**.

- Eisenstein's criterion is most frequently applied to $\mathbb{Z}[X]$, so we state that special case separately.

Corollary 9.14 (Eisenstein's Criterion for $\mathbb{Z}[X]$)**.** Let p be a prime in $\mathbb{Z}$ and let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$, $n \geq 1$. Suppose p divides a_i for all $i \in \{0, 1, \ldots, n-1\}$ but that p^2 does not divide a_0. Then f is irreducible in both $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$.

Proof. Follows from Proposition 9.13 and Corollary 9.6. □

- Example applications of Eisenstein's Criterion.
- There are now efficient algorithms for factoring polynomials over certain fields.
  - Moreover, many of these are now available as computer packages.
- **Berlekamp Algorithm**: An efficient algorithm for factoring polynomials over $\mathbb{F}_p$.
  - Described in detail in the exercises at the end of Section 14.3.

Section 9.5: Polynomial Rings Over Fields II

- Additional results for the one-variable polynomial ring $F[X]$.

Proposition 9.15. The maximal ideals in $F[X]$ are the ideals (f) generated by irreducible polynomials f. In particular, $F[X]/(f)$ is a field iff f is irreducible.

Proof. Apply Propositions 8.10 and 8.7 to the PID $F[X]$. □

Proposition 9.16. Let g be a nonconstant element of $F[X]$, and let $g(X) = f_1(X)^{n_1} \cdots f_k(X)^{n_k}$ be its factorization into irreducibles, where the f_i are distinct. Then we have the following isomorphism of rings.

$$F[X]/(g) \cong F[X]/(f_1^{n_1}) \times \cdots \times F[X]/(f_k^{n_k})$$

Proof. Follows from the Chinese Remainder Theorem. □

Proposition 9.17. If the polynomial f has roots $\alpha_1, \ldots, \alpha_k$ in F (not necessarily distinct), then f has $(x - \alpha_1) \cdots (x - \alpha_k)$ as a factor. In particular, a polynomial of degree n in one variable over a field F has at most n roots in F, even counted with multiplicity.

Proof. First statement: Induct. Second statement: $F[X]$ is a UFD (Corollary 9.4). □

Proposition 9.18. A finite subgroup of the multiplicative group of a field is cyclic. In particular, if F is a finite field, then the multiplicative group $F^\times$ of nonzero elements of F is a cyclic group.

Proof. Given; relies on more group theory than I covered in Honors Algebra I. □

Corollary 9.19. Let p be a prime. The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ of nonzero residue classes mod p is cyclic.

Proof. This is the multiplicative group of the finite field $\mathbb{Z}/p\mathbb{Z}$, so apply Proposition 9.18. □

Corollary 9.20. Let $n \geq 2$ be an integer with factorization $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ in $\mathbb{Z}$, where $p_1, \ldots, p_r$ are distinct primes. We have the following isomorphisms of multiplicative groups.

1. $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^\times$.
2. $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ is the direct product of a cyclic group of order 2 and a cyclic group of order $2^{\alpha-2}$ for all $\alpha \geq 2$.
3. $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ is a cyclic group of order $p^{\alpha-1}(p-1)$ for all odd primes p.

Proof. Given. □

- Note that Corollary 9.20 gives the group-theoretic structure of the automorphism group of the cyclic group of order n since $\mathrm{Aut}(Z_n) = \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Section 9.6: Polynomials in Several Variables Over a Field and Gröbner Bases

- A potentially useful result.

  Corollary 9.22. Every ideal in the polynomial ring $F[X_1, \ldots, X_n]$ with coefficients from a field F is finitely generated.

- Everything else is unquestionably beyond the scope of this class.