Week 5

???

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! $\gcd(a, b)$ can be computed without factoring a, b. Review page 2 of Chapter 8, as referenced in a previous class.
- In PIDs, you can factor $a = qb + r$, but q, r may not be specific; in EDs, these q, r are unique.
  - Is this correct??
- 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??
- 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 $\mathcal{P}(R) \subset R \setminus \{0\}$ be such that...

  (i) Every $\pi \in \mathcal{P}(R)$ is irreducible.

  (ii) For all $\alpha \in \mathbb{R} \setminus \{0\}$, 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 $|\{\pi \in \mathcal{P}(R) \mid k(\pi) > 0\}|$ 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. It suffices to prove the case where $c(f) = c(g) = 1$.

  Let π 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

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

  Notationally, if $a_i \in R$, then $\bar{a}_i$ is the image of a_i in $R/(\pi)$ under the canonical surjection.

  $c(f) = 1$ implies that there exists i such that $a_i \neq 0$. Therefore, $\varphi(f) \neq 0$. Similarly, $c(g) = 1$ implies that $\varphi(g) \neq 0$. It follows that $\varphi(fg) = \varphi(f)\varphi(g)$. Since $R/(\pi)$ is an integral domain and thus contains no zero divisors, we know that $\varphi(fg) = \varphi(f)\varphi(g) \neq 0$. It follows that $\pi \nmid c(fg)$. This is true for all irreducible $\pi \in R$. Indeed, it follows 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.
- $\mathcal{P}(R[X]) = \mathcal{P}(R) \sqcup \{\tilde{g} \mid g \in K[X] \text{ is monic and irreducible}\}$.
- 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 diadic 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: $R \setminus \{0\}$ 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 $\mathbb{Z}[X]$.
    - 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

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

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

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

    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??
    - We also assume that $\gcd(a, b) = 1$.
  - Because of the above constraint, we know that

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

    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

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

  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 $e_0, \dots, e_d \in F$ arbitrary, there exists a unique $g \in P_d$ such that $g(c_i) = e_i$ ($i = 0, \dots, d$).
  - 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 $g(c_0), \dots, g(c_d)$. But $g(c_i) \mid f(c_i)$ for all $i = 0, \dots, d$. 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 $f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{C}[X]$ have $a_0 \neq 0$. Define the number

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

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

$$\begin{aligned} 0 &= 1z^n + a_1z^{n-1} + \cdots + a_n \\ -z^n &= a_1z^{n-1} + \cdots + a_n \\ -1 &= a_1\frac{1}{z} + a_2\frac{1}{z^2} + \cdots + a_n\frac{1}{z^n} \\ &= \left(\frac{a_1}{C}\right)\left(\frac{C}{z}\right) + \left(\frac{a_2}{C^2}\right)\left(\frac{C}{z}\right)^2 + \cdots + \left(\frac{a_n}{C^n}\right)\left(\frac{C}{z}\right)^n \end{aligned}$$

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.

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

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

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

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.

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

□

- 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 $X^2 - h^2 \equiv m \pmod 5$.