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 $\mathbb{R}[X]$.