Week 9

Extension Topics

9.1 Intro to the Langlands Program

2/27:

- Sometime before 2:30 PM today, Nori will post an exam syllabus that will also put an upper bound on the types of questions he will ask.
  - "There's only so much you can cover in a 2-hour exam on an 8-week course."
- We now begin on some — in Nori's opinion — very interesting mathematics.
- Let $f \in \mathbb{Z}[X]$ be irreducible, monic, and of degree d.
- **Split** (prime for f): A prime number p for which

$$\bar{f} = \prod_{i=1}^{d} (X - a_i) \in \mathbb{F}_p[X]$$

- **Langlands program**: The name for the overall problem, "which primes are split for a given f?"
  - Gauss answers this for degree 2 polynomials using quadratic reciprocity.
  - There has been a lot of progress since then: See Artin's reciprocity law.
  - This is a major unsolved problem.
- Example: $X^2 + 1$.
  - Informally: If we go modulo a prime, does this factor or not?
  - Formally: For which primes p does there exist $m \in \mathbb{Z}$ such that $m^2 \equiv -1 \bmod p$.
  - Answer: m exists if and only if $p \equiv 1 \bmod 4$.
  - Proving this: Let p be an odd prime. Let $x \in \mathbb{F}_p - \{0\}$. Let $S(x) = \{x, -x, 1/x, -1/x\}$ be the stabilizer. We either have $\{x, -x\} \cap \{1/x, -1/x\} = \emptyset$ or both elements. Thus, we either have $x = \pm 1$ or $x^2 = -1$. It follows that $|S(x)| = 4$ except when $\{1, -1\}$ or $\{\alpha, -\alpha\}$ with $\alpha \in \mathbb{F}_p$ satisfies $\alpha^2 = -1$.
  - $p - 1 \equiv 2 \bmod 4$.
  - Thus, we're partitioning the set into elements of multiplicity 4.
- We'll skip considering the Gaussian integers.
- Consider the d square-free integers for $d \neq 1$. Let $R_d = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d} \cong \mathbb{Z}[X]/(X^2 - d)$.
  - If $d \equiv 2, 3 \bmod 4$, no bueno.

- If $d \equiv 1 \mod 4$, then $R_d = \mathbb{Z} \oplus \mathbb{Z}\theta$, where

$$\theta = \frac{1 + \sqrt{d}}{2}$$

- All of these rings have an automorphic ring homomorphism $\sigma : R_d \to R_d$ defined by

$$a + b\sqrt{d} \mapsto a - b\sqrt{d}$$

- Recall the norm $N(a + b\sqrt{d}) = |(a + b\sqrt{d})(a - b\sqrt{d})| = |a^2 - b^2 d|$.
- Let $I \subset R_d$ be a nonzero ideal. If $\alpha \in I$ nonzero, then $|\alpha\sigma\alpha| = N(\alpha) \in I$.
- Suppose $m \in \mathbb{N}$. Then $R_d/mR_d = \mathbb{Z}/(m) \oplus \sqrt{d}\mathbb{Z}/(m)$ has m^2 elements.
- In particular, R_d/I is finite as the quotient of a finite ring $R_d/R_d N(\alpha)$ (as implied by the fact that I is nonzero).
- Let $P \subset R_d$ be a nonzero prime ideal. We have just shown that $P \cap \mathbb{Z} \neq 0$. It follows that if $m \in \mathbb{N}$ and $m \in P$, then $p_1 \cdots p_r$ implies some $p_i \in P$.
- There exists a unique prime number p such that $p \in P$.
- Fix p. Search for all P prime ideals of R_d such that $p \in P$, i.e., $(p) \subset P \subset R_d$, i.e., $P/(p)$ is a prime ideal of $R_d/(p)$.
- Recall that

$$R_d/(p) = \mathbb{F}_p \oplus \mathbb{F}_p\sqrt{d} \cong \mathbb{F}_p[X]/(X^2 - d)$$

- Case 1: $p \nmid d$ and $p \neq 2$.
  - Case 1(a): There exists an integer $m \in \mathbb{Z}$ such that $m^2 \equiv d \bmod p$.
  - Case 1(b): No integer $m \in \mathbb{Z}$ exists such that $m^2 \equiv d \bmod p$.
- Case 2: $p \mid d$.

- We now treat each case above individually.
- Case 2.
  - Let P be unique and $P = (p, \sqrt{d}) = \sigma P$.
  - We have $P\sigma P = (p, \sqrt{d})(p, \sqrt{d}) = (p^2, d, p\sqrt{d}) \subset (p)$.
  - Even in $\mathbb{Z}$, $\gcd_{\mathbb{Z}}(p^2, d) = p$ (because $p \mid d$ and $p^2 \nmid d$; the latter claim follows because d is square-free).
  - This implies that $p \in P\sigma P$, which implies that $(p) = P\sigma P$.
- Case 1b.
  - $X^2 - d$ is irreducible in $\mathbb{F}_p[X]$.
  - Thus, $P = (p)$.
  - It follows that $P = \sigma P$ and hence $P\sigma P = (p^2)$.
- Case 1a.
  - There exists an $m \in \mathbb{Z}$ such that $m^2 \equiv d \bmod p$.
  - Let $P = (p, m - \sqrt{d})$, $\sigma P = (p, m + \sqrt{d})$.
  - There exists exactly two prime ideals P.
  - Thus, $P\sigma P = (p^2, m^2 - d, p(m - \sqrt{d}), p(m + \sqrt{d})) \subset (p)$.
  - Adding the last two generators together, we obtain $(p^2, 2mp) \in P\sigma P$. But since $p \nmid m$ and p ??, we know that

$$\gcd_{\mathbb{Z}}(p^2, 2mp) = p$$

- It follows that $P\sigma P = (p) \sim (p^2)$ in all cases.
- We now consider the $p = 2$ case.
  - Let $R = \mathbb{Z} \oplus \mathbb{Z}\sqrt{d}$. Let $\varepsilon = 0, 1$ and $\varepsilon = \varepsilon^2$.
  - Case 1(a): Does not exist; $\mathbb{F}_2[X]/(X^2 - \varepsilon)$ and $\mathbb{F}_2[X]/((X-\varepsilon)^2)$.
  - Case 2: $2 \mid d$ and $4 \nmid d$. It follows that P is unique and equal to $(2, \sqrt{d})$. We have $p^2 = (2)$.
  - Case 1(b): $p = 2$ and $2 \nmid d$. Let $\mathbb{F}_2[X]/(X^2 - 1)$. We have a unique P and $P = (2, 1 - \sqrt{d}) = \sigma P = (2, 1 + \sqrt{d})$.
  - Let $P^2 = P\sigma P = (4, 1 - d, 2(1 - \sqrt{d})) = (2)$ if $d \equiv 3 \bmod 4$. Note that $P\sigma P$ is *not* principal if $d \equiv 1 \bmod 4$.
  - Consider (example): $F[X^2, X^3] \subset F[X]$.
  - If $R_d = \mathbb{Z} + \mathbb{Z}\theta$ and $d \equiv 1 \bmod 8$, then there exists $P \neq \sigma P$ with $P\sigma P = (2)$.
  - If $d \equiv 5 \bmod 8$, then $P = (2)$.
- Next lecture: Dedekind domains.
  - Every nonzero ideal can be written as a product of nonzero not necessarily unique prime ideals.
  - Next best thing to a PID.
- Theorem: $\mathbb{Z}[\sqrt{-1}]$ is a Euclidean domain.

  Proof. Given g, f, we want $g = qf + r$ in $\mathbb{Z}[\sqrt{-1}]$ with $N(r) < N(f)$.

  Technique: Go outside the integers into $\mathbb{Q}(\sqrt{-1})$. This is a field. Consider $g/f \in \mathbb{Q}(\sqrt{-1})$. Choose the closest lattice point in $\mathbb{Z}[\sqrt{-1}]$ to $g/f \in \mathbb{Q}(\sqrt{-1})$, visualized as a complex plane and complex lattice subset. This makes $g/f = q + c$ where $q \in \mathbb{Z}[\sqrt{-1}]$. Let $c = \alpha + \beta\sqrt{-1}$. Then $|\alpha| \leq 1/2$, $|\beta| \leq 1/2$, and $N(\alpha + i\beta) = \alpha^2 + \beta^2 \leq 1/4 + 1/4 = 1/2$.

  It follows that $g \in \mathbb{Z}[\sqrt{-1}]$ equals $qf + (fc)$, where $qf \in \mathbb{Z}[\sqrt{-1}]$ and $fc = r \in \mathbb{Z}[\sqrt{-1}]$. Moreover, $N(r) = N(f)N(c) \leq 1/2N(f)$. ☐

- The same proof applies to $\mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[(1 + \sqrt{-3})/2]$, $\mathbb{Z}[(1 + \sqrt{p})/2]$, and in fact all Euclidean domains.

9.2 Factorization of Ideals

3/1:

- Nori proves that any ideal, perhaps under certain conditions, can be factored into prime ideals.

9.3 Office Hours (Nori)

3/7:

- Computing the JCF and RCF is going to be on the midterm.
- Gauss's lemma may well be on the final. There is a difference between Gauss's lemma in class and in the textbook; the textbook version is a corollary of the real one (which Nori presented).
  - To clarify on the final, specify which version of Gauss's lemma you are using.
- One question like the universal properties of polynomial rings stuff from the first midterm.
- $R' = R/(f)$ looks a lot like a final question.
- We'll never have to decide which (JCF or RCF) to use; we'll only be asked, "what is the JCF/RCF of this?"
- RCF: We'll be able to stop after writing down the invariant factors.

9.4 Final Review Sheet

- See midterm review sheet for everything rings-related.
- **Gauss's lemma**: Reducible polynomials in $R[X]$ are reducible in $R[X]$.
- Dividing the first and last coefficients of the polynomial by monomials.
- **Left *A*-module**: An abelian group $(M,+)$ equipped with a binary operation $\cdot : A\times M \to M$ satisfying the following constraints.
    1. $a(v_1+v_2) = av_1 + av_2$.
    2. $(a+b)v = av + bv$.
    3. $a(bv) = (ab)v$.
    4. $1_A v = v$.
- Alternatively: $\rho : A \to \text{End}(M)$ satisfies:
    1. $\rho(a)$ is a group homomorphism from $M \to M$.
    2. $\rho(a+b) = \rho(a) + \rho(b)$.
    3. $\rho(a)\rho(b) = \rho(ab)$.
    4. $\rho(1_A) = 1_{\text{End}(M)}$.
- **Module homomorphism**: A group homomorphism that commutes with scalar multiplication, i.e., $T(av) = aT(v)$.
- $T : A^n \to M$ is defined by the action of T on the e_i's.
- **Module isomorphism**: A bijective module homomorphism.
- Quotient module exist in a natural way.
- FIT for modules.
- Let R be a PID; then every R-submodule of R^n is isomorphic to R^m for some $0 \leq m \leq n$.
- If $M/M' \cong A^n$, then $M' \oplus A^n \cong M$.
- ***R*-algebra**: A pair (A, f), where A is a ring, $f : R \to A$ is a ring homomorphism, and R is a commutative ring, such that $f(R) \subset Z(A)$.
    - A is an R-module under $r \cdot a = f(r) \cdot a$.
- ***R*-algebra homomorphism**: A ring homomorphism $\varphi : A \to B$ such that $\varphi(r \cdot a) = r \cdot \varphi(a)$.
- $\text{Hom}_R(M, M)$ is a ring under componentwise addition and composition; it is an R-algebra when R is commutative.
- **Poset**.
- **Maximal** ($f \in P$): An element $f \in P$ a poset such that for all $q \in P$, the statement $q > f$ is false.
- **Chain**: A totally ordered subset of a poset.
- **Zorn's lemma**: If P is a poset such that $P \neq 0$ and every chain $C \subset P$ has an upper bound, then P has a maximal element.
- Corollary: Every nonzero finitely generated A-module M has a maximal submodule.
- Corollary: Every nonzero commutative ring R has a maximal ideal.

- **Torsion module**: An R-module such that for all $m \in M$, there exists a nonzero $a \in R$ such that $am = 0$.
- **Torsion-free module**: An R-module M such that for all nonzero $m \in M$ and for all nonzero $a \in R$, $am \neq 0$.
- **Torsion element**: An element $m \in M$ for which there exists a nonzero $a \in R$ such that $am = 0$.
- **Tor(M)**: The set of all torsion elements in M.
- ***p*-primary** (module): An R-module M such that for all $m \in M$, there exists $k \geq 0$ for which $p^k m = 0$, where $p \in R$ is prime.
- ***p*-primary** (component): The submodule of a module M consisting of all $m \in M$ such that $p^k m = 0$ for some $k \in \mathbb{Z}_{\geq 0}$ and $p \in R$ prime.
- All finitely generated torsion-free R-modules are isomorphic to R^n.
- $\operatorname{Tor}(M)$ is an R-submodule of M.
- $M/\operatorname{Tor}(M)$ is torsion-free.
  - To prove that something is torsion-free, it suffices to prove that every torsion element is zero.
- Every finitely generated R-module has a free submodule.
- Finitely generated torsion-free modules M over a PID R are isomorphic to R^h.
- If M is a finitely generated R-module over a PID, then $M \cong \operatorname{Tor}(M) \oplus R^h$, where $\operatorname{Tor}(M)$ is finitely generated.
- Finitely generated R-module are isomorphic iff they have the same rank and their torsion components are isomorphic.
- The direct sum of the p-primary components is equal to $\operatorname{Tor}(M)$.
- Every finitely generated p-primary module is the direct sum of the cyclic submodule Re_i.
- **RCF**: Let R be a PID. Then every finitely generated R-torsion module is isomorphic to $R/(a_1) \oplus \cdots \oplus R/(a_\ell)$ where $a_\ell \mid a_{\ell-1} \mid \cdots \mid a_1$.
- Every finitely generated R-module, where R is a PID, is isomorphic to $R/I_1 \oplus R/I_2 \oplus \cdots$ for a unique increasing sequence of ideals $I_1 \subset I_2 \subset \cdots$ which have the property that $I_n = R$ for some n.
- Vector spaces (V, T) as $F[X]$-modules under $\rho : F[X] \to \operatorname{End}_F(V)$ defined by $X \mapsto T$.
- **Minimal polynomial**: The polynomial that generates $\ker(\rho)$, an ideal of the PID $F[X]$.
- Cyclic vectors and linear dependence, defining the minimal polynomial by $g(X) = X^k - (a_{k-1}X^{k-1} + \cdots + a_0)$.