AM 106: Applied Algebra **Salil Vadhan**

Lecture Notes 24

December 6, 2018

1 Themes in AM106

- Unification of disparate mathematical structures via abstraction
  - Ex: Modular arithmetic, Permutations, Geometric symmetries all captured by group theory
  - Ex: Integers, polynomials both "Euclidean domains"
  - Common phenomena for all algebraic categories X (e.g. groups, rings, fields, vector spaces): sub-X's, X-homomorphisms, factor X's, $A/\ker(\varphi) \cong \mathrm{im}(\varphi)$.
- Classification Theorems
  - All finite abelian groups are a product of cyclic groups
  - Cayley's Theorem (all finite groups are isomorphic to permutation groups)
  - Finite-dimensional vector spaces over F are all isomorphic to F^n for some n
  - All finite fields are isomorphic to $\mathrm{GF}(p^n)$ for some prime p and positive integer n.
- Algorithms
  - Computations in many algebraic structures can be done efficiently (polynomial time). Notable examples: (Extended) Euclidean Algorithm and its many uses, Fast Modular Exponentiation and its many uses, Gaussian Elimination, Permutation Group Algorithms, Polynomial Factorization.
  - But there are notable exceptions, e.g. integer factorization, discrete logarithms. These hard problems are useful in cryptography!
- Modelling and Applications
  - Solving/optimizing linear equations over $\mathbb{Z}$ (extended euclidean algorithm)
  - Cryptography (cyclic groups, hardness of factoring/Chinese Remainder Thm)
  - Solving puzzles (permutation groups)
  - Crystallography (symmetry groups)
  - Error-correcting codes (polynomial rings, finite fields)

2 Pointers Beyond

- More algebra: Math 122 & 123 (you might be able to skip 122 with some self-study...), and lots of other courses in the math department
- Cryptography: CS 127/227
- Group theory in chemistry and crystallography: Chemistry 154, 255, Engineering Sciences 190
- Error-correcting codes: CS 229r (when topic is "essential coding theory" taught by Madhu Sudan)
- Polynomials and finite fields in theoretical computer science (e.g. interactive proofs, pseudorandomness): CS 221 (computational complexity), CS 225 (pseudorandomness)
- Group theory in physics: Physics 216