AM 106/206: Applied Algebra **Madhu Sudan**[1]

Lecture Notes 17

November 6, 2017

1 Factorization of Polynomials

- Reading: Gallian Ch. 16
- Throughout F is a field, and we consider polynomials in $F[x]$.
- **Def:** For $f(x), g(x) \in F[x]$, not both zero, the *greatest common divisor* of $f(x)$ and $g(x)$ is the monic polynomial $h(x)$ of largest degree such that $h(x)$ divides both $f(x)$ and $g(x)$.
- **Euclidean Algorithm for Polynomials:** Given two polynomials $f(x)$ and $g(x)$ of degree at most n, not both zero, their greatest common divisor $h(x)$, can be computed using at most $n+1$ divisions of polynomials of degree at most n. Moreover, using $O(n)$ operations on polynomials of degree at most n, we can also find polynomials $s(x)$ and $t(x)$ such that $h(x) = s(x)f(x) + t(x)g(x)$.

  Proof: analogous to integers, using repeated division.

  Euclid(f, g):

  1. Assume WLOG $\deg(f) \geq \deg(g) > 0$.
  2. Set $i = 1$, $f_1 = f$, $f_2 = g$.
  3. Repeat until $f_{i+1} = 0$:
     (a) Compute $f_{i+2} = f_i \bmod f_{i+1}$ (i.e. f_{i+2} is the remainder when f_i is divided by f_{i+1}).
     (b) Increment i.
  4. Output f_i divided by its leading coefficient (to make it monic).

  Here the complexity analysis is simpler than for integers: note that the degree of f_{i+2} is strictly smaller than that of f_i, so f_{n+2} is of degree zero, and $f_{n+3} = 0$. Thus we do at most n divisions.

  The Extended Euclidean Algorithm (finding the polynomials $s(x)$ and $t(x)$) is obtained analogously to the case of the integers.

- **Def:** Let R be a commutative ring with unity. An element $a \in R$ is *irreducible* if a is not a zero or a unit, and if $a = bc$ then either b or c is a unit.
- **Examples:**

[1] These notes are copied mostly verbatim from the lecture notes from the Fall 2010 offering, authored by Prof. Salil Vadhan. I will attempt to update them, but apologies if some references to old dates and contents remain.

  - Units in $\mathbb{Z}$:
  - Irreducible elements of $\mathbb{Z}$:
  - Units in $F[x]$ for a field F:
  - Irreducible polynomials in $F[x]$ of degree 1:
  - Irreducible polynomials in $F[x]$ of degree 2:
  - Irreducible polynomials in $F[x]$ of degree 3:
  - Irreducible polynomials in $F[x]$ of degree 4+:
  - No simple characterization in general for high degree polynomials. (The conditions in Gallian are necessary or sufficient, but not both.) But there are efficient algorithms for testing irreducibility (see discussion of factorization below).

- **Euclid's Lemma for Polynomials:** If $p(x)$ is irreducible and $p(x)|(f(x)g(x))$, then $p(x)|d(x)$ or $p(x)|g(x)$.

- **Proof:** Similar to proof for integers. If $p(x)$ does not divide $f(x)$, then $\gcd(p(x), g(x)) = 1$ because the only factors of $p(x)$ are 1 and $p(x)$ (up to multiplication by units). So $1 = s(x)p(x) + t(x)f(x)$ for some polynomials $s(x)$ and $t(x)$. Then $g(x) = s(x)p(x)g(x) + t(x)f(x)g(x)$ is divisible by $p(x)$ because both terms on the right-hand side are divisible by $p(x)$.

- **Thm (Unique Factorization of Polynomials):** Every $f(x) \in F[x]$ can be written as a product of irreducible polynomials $f(x) = g_1(x)g_2(x)\cdots g_k(x)$, and this factorization is unique up to the order of the g_i's and multiplying them by units (elements of F).

  - Compare with unique factorization over $\mathbb{Z}$, unique up to multiplication by ± 1.

  Proof: Similar to integers. Existence of factorization by induction on the degree. Uniqueness by Euclid's Lemma.

- Unlike $\mathbb{Z}$, there *are* efficient algorithms known for factoring polynomials over fields. The best known deterministic algorithms use $\text{poly}(n, p, \log q)$ operations over F, where p is the characteristic of F and $q \geq p$ is the size of F. The best known randomized algorithms use $\text{poly}(n, \log q)$ operations. Take CS 226r to learn about these!

2 Ideals in Polynomial Rings

- **Reading:** Gallian Ch. 16

- **Q:** Let F be a field, $p(x), q(x) \in F[x]$. Can we find a single polynomial $r(x)$ such that $\langle r(x) \rangle = \langle p(x), q(x) \rangle$?

- **Def:** An ideal I in a ring R is *principal* if there is a single element $a \in R$ that generates I (i.e. $I = \langle a \rangle$). R is a *principal ideal domain* if every ideal in R is principal.

  - **Examples and Non-examples:**

- **Thms 16.3–16.4:** For F a field, $F[x]$ is a principal ideal domain. Moreover, for every nonzero ideal $I \subseteq F[x]$, if $g(x)$ is a nonzero polynomial of minimal degree in I, then $I = \langle g(x) \rangle$.
- **Proof:** Omitted (in book).

3 Factors of Polynomial Rings

- Reading: Gallian Ch. 17.
- Now our goal is to understand the factor rings $F[x]/\langle p(x) \rangle$. We'll write $f(x) \bmod p(x)$ to denote the remainder when $f(x)$ is divided by $p(x)$.
- **Thm (characterizing $F[x]/\langle p(x) \rangle$):** Let F be a field and let $p(x) \in F[x]$ be a nonzero polynomial. Then:
  - $f(x) + \langle p(x) \rangle = g(x) + \langle p(x) \rangle$ if and only if $f(x) \bmod p(x) = g(x) \bmod p(x)$.
  - $F[x]/\langle p(x) \rangle$ is isomorphic to the ring consisting of all polynomials of degree smaller than $\deg(p)$ with arithmetic modulo $p(x)$.

  cf. $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$.
- **Proof:**

- **Examples:**
  - $\mathbb{Z}_p[x]/\langle x^2 - k \rangle$.
  - $\mathbb{Q}[x]/\langle x^5 - x^3 - 1 \rangle$.
- **Remark:** above thm holds more generally for $R[x]$ if leading coefficient of p is a unit in R (otherwise division/modding by p is not possible).
- **Q:** When is $F[x]/\langle p(x) \rangle$ a field?

- **Thm 17.5:** For a field F and a nonzero polynomial $p(x) \in F[x]$, the factor ring $F[x]/\langle p(x) \rangle$ is a field if and only if $p(x)$ is irreducible.

  Proof:

- This is a way of building larger fields from smaller fields!
- **Examples:**
  - $\mathbb{R}[x]/\langle x^2 + 1 \rangle$.
  - $\mathbb{Z}_p[x]/\langle x^2 - k \rangle$.
  - $\mathbb{Z}_2[x]/\langle x^3 + x^2 + 1 \rangle$.
- **Q:** How to compute inverses in $F[x]/\langle p(x) \rangle$?

4 Analogy between $\mathbb{Z}$ and $F[x]$

- We have seen that $\mathbb{Z}$ and $F[x]$ share many properties. For example, both are:
  - *Euclidean Domains:* There exists division with remainder, and hence also gcds.
  - *Principal Ideal Domains:* Every ideal is principal.
  - *Unique Factorization Domains:* Every non-unit factors uniquely into irreducible elements (up to order and multiplication by units).
- In general every Euclidean domain is a Principal Ideal Domain, and every Principal Ideal Domain is a Unique Factorization Domain.
- However, the converse does not hold. For $R[x]$ to be a Unique Factorization Domain turns out to only require that R is a Unique Factorization Domain. For example $\mathbb{Z}[x]$ and $F[x_1, \ldots, x_n]$ are Unique Factorization Domains but not Principal Ideal Domains.
- The lack of being a Euclidean Domain or PID makes computations in $F[x_1, \ldots, x_n]$ and its ideals and quotients more difficult. A *Grobner Basis* is a special kind of generating set for an ideal in $F[x_1, \ldots, x_n]$ that enables for a weaker form of division with remainder. These are very important in practice for solving systems of simultaneous polynomial equations (which has applications, e.g. in robot motion).
- A full treatment of these issues can be found in Gallian Ch. 18 (which we will not cover).