AM 106/206: Applied Algebra	**Prof. Salil Vadhan**

Lecture Notes 17

November 23, 2009

1 Ideals in Polynomial Rings

- **Reading:** Gallian Ch. 16
- 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.
  - **Example:**
- **Thms 16.3–16.4:** For F a field, $F[x]$ is a principal ideal domain. Moreover, for every ideal $I \subseteq F[x]$, if $g(x)$ is a polynomial of minimal degree in I, then $I = \langle g(x) \rangle$.
- **Proof:**

2 Factors of Polynomial Rings

- Reading: Gallian Ch. 17, 14.
- 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 $F[x]/\langle p(x) \rangle$):**
  - $f(x) + \langle p(x) \rangle = g(x) + \langle p(x) \rangle$ 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?

- **Def:** An ideal $I \subseteq R$ is *maximal* if $I \subsetneq R$ and there does not exist an ideal J such that $I \subsetneq J \subsetneq R$.

- **Thm 14.4:** R/I is a field if and only if I is maximal.

- **Proof:**

- **Remark:** there is also a characterization of when R/I is an integral domain, but we won't cover it (Thm 14.3).

- **Thm 17.5:** Characterization of maximal ideals $\langle p(x)\rangle$ in $F[x]$.

- **Examples:**
  - $\mathbb{Z}_p[x]/\langle x^2 - k\rangle$.
  - $\mathbb{Z}_2[x]/\langle x^4 + x^3 + 1\rangle$.
  - $\mathbb{Q}[x]/\langle x^2 + x + 1\rangle$.
  - $\mathbb{R}[x]/\langle x^2 + 1\rangle$.

- **Q:** How to compute inverses in $F[x]/\langle p(x)\rangle$?

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

- We have seen that $\mathbb{Z}$ and $\mathbb{F}[x]$ 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.

- A full treatment of these issues can be found in Gallian Ch. 18 (which we will not cover).