IITM-CS6842 : Algorithmic Algebra **Given on : Sep 5, 2015**

Problem Set #1 ($7 \times 5 = 35$ **points)** **Due on : Sep 17, 2015**

1. (7 points) We showed in class that every ideal of $\mathbb{F}[x]$ is principal (generated by one element). We will show two observations about it.

   (a) This is special to the case of polynomials in one variable. Consider the ideal $\langle x, y\rangle \subset \mathbb{F}[x, y]$. Prove that I is not a principal ideal. (Hint : If $x = fg$ where $f, g \in \mathbb{F}[x, y]$ prove that f or g is a constant.)

   (b) This is special to the case of fields. Let I be a subset of $\mathbb{Z}[x]$ consisting of all polynomials with an even constant term, i.e. for $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in \mathbb{Z}[x]$, $p \in I$ if and only if a_0 is even. Show that I is an ideal of $\mathbb{Z}[x]$ but not a principal ideal.

2. (7 points) Let R and R' be two commutative rings with identities. A map $\phi : R \to R'$ is called a *ring homomorphism* if $\phi(1) = 1$ and,

$$(\forall a, b)\,[\phi(a + b) = \phi(a) + \phi(b) \text{ and } \phi(ab) = \phi(a)\phi(b)]$$

   That is, ϕ respects (multiplicative and additive) identity, addition, and multiplication. The set of elements of R which gets mapped to the additive identity of R' by the homomorphism ϕ is called *kernel* of the homomorphism.

   (a) Show that the kernel of ϕ is always a subring of R. Is it also an ideal?. Give arguments.

   (b) For every ideal $I \subseteq R$, there is a ring homomorphism ($\phi : R \to R'$) such that I is the kernel of ϕ.

   (c) Show that image of the ϕ is a subring of R'. Is it also an ideal? Give arguments.

3. (7 points) Let $f \in \mathbb{F}[x_1, x_2, \ldots x_n]$ and $x_1 > x_2 > \ldots > x_n$ be the variable order.

   (a) Work out the proof of the statement *every term ordering is also a well-ordering* (Theorem 1.4.6, Page 21 of the textbook - half-page proof). Is the converse also true? Argue the following. Let $<$ be a total order on the set of terms. Assume that $<$ is a well-order and satisfies the second condition of the definition of term ordering. Prove that for the term $x^\alpha \neq 1$ satisfies $1 < x^\alpha$.

   (b) We call f to be homogeneous if the total degree of every term is the same. Let the term ordering be degrevlex. Prove that x_n divides f if and only if x_n divides $lt(f)$. Generalize your argument to show $f \in \langle x_i, \ldots x_n\rangle$ if and only if $lt(f) \in \langle x_i, \ldots x_n\rangle$.

4. (7 points) Let $I \subseteq \mathbb{F}[x_1, x_2, \ldots x_n]$ be an ideal generated by a (possibly infinite) set of power products (such ideals are called *monomial ideals*).

   (a) Prove the following stricter version of Hilbert basis theorem for monomial ideals : there exists $\alpha_1, \alpha_2, \ldots \alpha_m \in \mathbb{N}^n$ such that $I = \langle x_1^\alpha, x_2^\alpha, \ldots, x_m^\alpha\rangle$.
   (Hint for one possible solution : Equivalently, you can show the following fact about natural numbers : for any $A \subseteq \mathbb{N}^n$, there exists $\alpha_1, \alpha_2, \ldots \alpha_m \in A$ such that $A \subseteq \bigcup_{i=1}^m(\alpha_i + \mathbb{N}^n)$. Show the equivalence if you are using the hint.)

   (b) Prove that every monomial ideal contain a unique minimal generating set. That is, prove that there is a subset $G \subseteq I$ generating I such that for all subsets $F \subseteq I$ generating I, we have that $G \subseteq F$.

5. (7 points) Let I be an ideal and G be a Grobner basis of I. For any $f \in \mathbb{F}[x_1, x_2, \ldots x_n]$, let $\overline{f}^G$ denote the unique r such that $f \to_+^G r$.

(a) Show that $\overline{f}^G = \overline{g}^G$ if and only if $f - g \in I$.

(b) Use this to deduce that : $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$.