21-238, Math Studies Algebra 2, Department of Mathematical Sciences, Carnegie Mellon University
Spring 2012: Monday, Wednesday, Friday, 10:30 am, Doherty Hall 1211.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

28- Wednesday March 28, 2012.

Remark 28.1: One now considers questions involving polynomials in more than one variable, recalling that for a field F the polynomial ring $F[x_1, x_2]$ is not a PID (principal ideal domain), so that questions of describing ideals in $F[x_1, \ldots, x_n]$ involve understanding more about polynomial rings $R[x]$ for some particular rings R. In particular, it is useful to identify properties of R which are inherited by $R[x]$: it has been mentioned that if R is a UFD (unique factorization domain) then $R[x]$ is a UFD, and *Hilbert basis theorem* (Lemma 28.3) provides another example, involving Noetherian rings.

Lemma 28.2: Let R be a ring, and let J be a left ideal (respectively a right ideal, a two sided ideal) of $R[x]$. For $d = 0, \ldots$, let $L_d(J)$ be the set of *leading terms* of polynomials of degree d from J, together with 0,[1] and $LT(J) = \bigcup_{d\geq 0} L_d(J)$ be the set of leading terms of all polynomials from J, together with 0. Then $L_d(J)$, $d = 0, \ldots$, and $LT(J)$ are left ideals (respectively right ideals, two sided ideals) of R.
Proof: If $a, b \in L_d(J)$ are both non-zero, there exist $f, g \in J$ of degree d such that a is the leading term of f, and b is the leading term of g, and then $a \pm b$ is either 0 or it is non-zero and the leading term of $f \pm g$ which has degree d; similarly, for $r \in R$, $r\,a$ is either 0 or it is non-zero and the leading term of $r\,f$ which has degree d; the cases where a, b, or r are 0 are obvious.

The same property holds for $a\,r$ if J is a right ideal.

One then notices that $a \in L_d(J)$ implies $a \in L_m(J)$ whenever $m \geq d$, since for $a \neq 0$ there exists $f \in J$ of degree d whose leading term is a, and then $x^{m-d} f \in J$ has degree m and leading term a; this shows that $LT(J)$ is a left ideal (respectively a right ideal, a two sided ideal) of R, since it is the union of an increasing sequence of left ideals (respectively right ideals, two sided ideals).

Lemma 28.3: (Hilbert's basis theorem) For R a commutative ring,[2] $R[x]$ is a Noetherian ring if and only if R is a Noetherian ring.
Proof: By definition, a commutative ring is Noetherian if and only if every increasing sequence of ideals becomes constant. If $R[x]$ is Noetherian and I_n is an increasing sequence of ideals of R, then $J_n = (I_n)$ is an increasing sequence of ideals of $R[x]$, which becomes constant, and using the notation of Lemma 28.2 one has $I_n = L_0(J_n)$, which then becomes constant.

A commutative ring is Noetherian if and only if all its ideals are finitely generated. If R is Noetherian and J is an ideal of $R[x]$, one then wants to construct a finite set of generators of J. Since $LT(J)$ is an ideal of R by Lemma 28.2, it has a finite set of (non-zero) generators $\rho_1, \ldots, \rho_m$, and there are polynomials $P_1, \ldots, P_m \in J$ such that the leading term of P_i is ρ_i for $i = 1, \ldots, m$, and one defines $N = \max_{i=1}^m deg(P_i)$. For $d = 0, \ldots, N$, one chooses a finite set of generators of $L_d(J)$ (since $L_d(J)$ is an ideal of R by Lemma 28.2), which one denotes $\sigma_{d,j}$ for $j = 1, \ldots, n_d$, and one chooses corresponding polynomials $Q_{d,j} \in J$ having degree d and leading term $\sigma_{d,j}$ for $j = 1, \ldots, n_d$. One wants to show that $\{P_1, \ldots, P_m\} \bigcup_{d=0}^N \{Q_{d,1}, \ldots, Q_{d,n_d}\}$ is a set of generators of J. If $P \in J$ has degree $\geq N$, then its leading term a belongs to $LT(J)$ and can then be written $a = \sum_{i=1}^m r_i \rho_i$ for some $r_1, \ldots, r_m \in R$, so that $Q = \sum_{i=1}^m r_i x^{deg(P)-deg(P_i)} P_i \in J$, and since Q has the same higher order coefficients $a\,x^{deg(P)}$ than P, one deduces that $P - Q \in J$ with $deg(P-Q) < deg(P)$. One repeats the operation until one obtains a polynomial $S \in J$ of degree $d \leq N$, so that its leading term b can be written as $b = \sum_{j=1}^{n_d} s_j \sigma_{d,j}$ with $s_1, \ldots, s_{n_d} \in R$, hence $T = \sum_{j=1}^{n_d} s_j Q_{d,j} \in J$, and since T has degree d and the same higher order coefficient $b\,x^d$ than S, one deduces that $S - T \in J$ with $deg(S-T) < d$. One then repeats the operation until one obtains the polynomial 0.

Lemma 28.4: If F is a field and $n \geq 1$, then every ideal of $F[x_1, \ldots, x_n]$ is finitely generated.

[1] By definition, if P has degree d it means that $P = a_0 + \ldots + a_d x^d$ with $a_d \neq 0$, and the subset $\{a_d \mid P \in J\}$ could not be an additive subgroup of R without adding 0.
[2] The hypothesis of commutativity can be dropped if one uses the notions of left Noetherian ring or right Noetherian ring, but in the sequel the ring R will be $F[x_1, \ldots, x_n]$ for a field F.

Proof: Since $F[x_1]$ is a PID,[3] it is a Noetherian ring, and then for $n \geq 2$ one can use Lemma 28.3 for proving by induction on n that $F[x_1, \ldots, x_n]$ is a Noetherian ring, by taking $R = F[x_1, \ldots, x_{n-1}]$ and noticing that $F[x_1, \ldots, x_n]$ is isomorphic to $R[x_n]$.

Remark 28.5: By a simple abuse of notation, one writes $F[x_1, x_2] = R[x_2] = S[x_1]$ with $R = F[x_1]$ and $S = F[x_2]$, instead of saying that theses rings are isomorphic (with obvious isomorphisms), but since the proof of Lemma 28.3 for finding a set of generators of an ideal first uses leading coefficients in powers of x_2 in one case, and leading coefficients in powers of x_1 in the other case, one discovers in a natural way the following notion of monomial ordering.

Definition 28.6: A *monomial ordering* on the polynomial ring $F[x_1, \ldots, x_n]$ is a *well ordering* $\geq$ on the set of monic monomials,[4] satisfying $m\,m_1 \geq m\,m_2$ whenever $m_1 \geq m_2$ for monic monomials m, m_1, m_2. Equivalently, when working with polynomials in variables $x_1, \ldots, x_n$, a monomial ordering is equivalent to giving a well ordering $\geq$ on multi-indices $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ (for the monic monomials $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$), which satisfies $\alpha + \gamma \geq \beta + \gamma$ whenever $\alpha \geq \beta$.

Lemma 28.7: For any monomial ordering, one has $m \geq 1$ for all monic monomials.

Any total ordering of monic monomials satisfying $m \geq 1$ for all monic monomials and $m\,m_1 \geq m\,m_2$ whenever $m_1 \geq m_2$ for monic monomials m, m_1, m_2 is a monomial ordering.

Proof: If one had $1 > m$ for a monic monomial $m \neq 1$, then one would deduce $m > m^2$, and by induction $m^k > m^{k+1}$ for all $k \geq 0$, so that the sequence of monic monomials m^n would be strictly decreasing, contradicting the well ordering.

Let I be a non-empty subset of monic monomials, of which one wants to show that it has a minimum for the ordering. Let $J = (I)$ be the ideal generated by I in $R[x]$, with $R = F[x_1, \ldots, x_n]$, which is finitely generated by Hilbert's basis theorem (Lemma 28.3); since each generator is itself a finite combination of terms of the form $r\,m\,i$ for some $r \in R$, some monic monomial m, and some $i \in I$, J is generated by a finite set $K \subset I$. In particular, since $I \subset J$, every $i \in I$ has the form $i = \sum_{k \in K} P_{i,k} k$ with $P_{i,k} \in R$, so that there exists $k \in K$ and a monic monomial m such that $i = m\,k$, and since $m \geq 1$ implies $m\,k \geq k$, one finds that $i \geq \min_{k \in K} k$ for all $i \in I$, hence the minimum for I is the minimum for the finite subset K.

[3] It is useful to observe that for $F[x]$ one only needs one generator for each ideal, and one may start the induction in the proof at $n = 1$ since a field F is obviously a Noetherian ring, because its only non-trivial ideal is F, generated by 1.

[4] A well ordering is a total ordering for which any non-empty subset has a minimum.