M3P8 LECTURE NOTES 9: POLYNOMIAL RINGS IN SEVERAL VARIABLES

1. The Hilbert Basis Theorem

In this section, we will use the ideas of the previous section to establish the following key result about polynomial rings, known as the *Hilbert Basis Theorem*:

Theorem 1.1. *Let R be a Noetherian ring. Then $R[X]$ is Noetherian.*

Proof. The following proof is due to Emmy Noether, and is a vast simplification of Hilbert's original proof. Let I be an ideal of $R[X]$; we want to show that I is finitely generated.

Let $P(X) = b_0 + b_1X + \cdots + b_nX^n$, with $b_n \in R$ nonzero. We say that b_n is the *leading coefficient* of $P(X)$. Let $J \subseteq R$ be the set of leading coefficients of polynomials in I; that is, the set of $a \in R$ such that there exists a polynomial $P(X)$ in I with leading coefficient b. We will show that J is an ideal of R.

Certainly if a is the leading coefficient of $P(X)$, then for any $r \in R$, ra is the leading coefficient of $rP(X)$, so J is closed under multiplication. On the other hand, if a, b are the leading coefficients of $P(X)$ and $Q(X)$ in I then let d, d' be the degrees of $P(X)$ and $Q(X)$ respectively. Without loss of generality we may assume $d \geq d'$. Then $a + b$ is the leading coefficient of $P(X) + X^{d-d'}Q(X)$, and the latter polynomial is in I. Thus J is closed under addition, and is therefore an ideal.

Now since R is Noetherian, J is finitely generated, say by $a_1, \ldots, a_n$. There are thus polynomials $P_1, \ldots, P_n$ in I, of degrees $d_1, \ldots, d_n$, such that P_i has leading coefficient a_i for all i. Let d be the largest of the d_i.

Let $I_{\leq d}$ be the subset of I consisting of all polynomials of degree at most d. Then $I_{\leq d}$ is an R-submodule of the R-module $R[X]_{\leq d}$ of all polynomials of degree at most d. The latter is generated by $1, X, X^2, \ldots, X^d$ as an R-module, so it is finitely generated, hence Noetherian. In particular $I_{\leq d}$ is also a finitely generated R-module. Let $Q_1, \ldots, Q_s$ generate $I_{\leq d}$ as an R-module.

We will show that $P_1, \ldots, P_r, Q_1, \ldots, Q_s$ generate I as an $R[X]$-module. More precisely, for any polynomial P of degree e in I we will show that P is an $R[X]$-linear combination of the P_i and Q_j. The proof is by induction on e and the base case is clear: if P has degree $\leq d$, then P is an R-linear combination of the Q_j.

Suppose the claim is true for polynomials of degree less than or equal to $e - 1$, with $e > d$. Let a be the leading coefficient of $P(X)$, so that $P(X) - aX^e$ has degree at most $e - 1$. Since a lies in J we can write

$a = r_1 a_1 + \cdots + r_n a_n$. Then the leading term of the polynomial

$$r_1 X^{e-d_1} P_1 + r_2 X^{e-d_2} P_2 + \cdots + r_n X^{e-d_n} P_n$$

is aX^e, so the difference:

$$r_1 X^{e-d_1} P_1 + r_2 X^{e-d_2} P_2 + \cdots + r_n X^{e-d_n} P_n - P(X)$$

has degree at most $e-1$ and lies in I. By the inductive hypothesis this difference is an $R[X]$-linear combination of the $P_i(X)$ and $Q_j(X)$, and so $P(X)$ is as well. □

As a corollary, we deduce:

Corollary 1.2. *Let R be any field or PID (or indeed any Noetherian ring!). Then for any n, the ring $R[X_1, \ldots, X_n]$ is Noetherian.*

Indeed, since any quotient of a Noetherian ring is Noetherian, we can say more:

Definition 1.3. Let R be a ring. An *R-algebra* is a ring S together with a homomorphism $R \to S$. If S is an R-algebra, we say that S is *finitely generated* over R if there exists a finite set of elements $s_1, \ldots, s_n \in S$ such that the homomorphism $R[X_1, \ldots, X_n] \to S$ sending X_i to s_i is surjective.

Note that any finitely generated R-algebra is isomorphic to a quotient $R[X_1, \ldots, X_n]/I$ for some ideal I. Thus we can rephrase the Hilbert Basis theorem as saying that if R is Noetherian, then any finitely generated R-algebra is Noetherian.

2. Polynomial Rings Over UFDs are UFDs

Our next goal is to study factorization in rings of the form $R[X]$. Certainly if R is not a UFD then we can't expect to have unique factorization in $R[X]$- we don't even have it in R! Assume R is a UFD. Then the ring $R[X]$ might be quite complicated, but $R[X]$ is contained in a much simpler ring where we do understand factorization- the ring $K[X]$, where K is the field of fractions of R. Our goal will thus be to compare factorizations in $K[X]$ and $R[X]$.

Factorizations in these two rings differ in several important ways. The first, of course, is that if a polynomial $P(X)$ in $R[X]$ factors as a product of two polynomials in $K[X]$, it is not immediately clear that we can also factor $P(X)$ in $R[X]$. The second, slightly more subtle problem is that some irreducible elements of $R[X]$ become units in $K[X]$; for instance, a polynomial like $2X + 4$ is irreducible in $\mathbb{Q}[X]$ (since 2 is a unit in $\mathbb{Q}$), but in $\mathbb{Z}[X]$ this polynomial factors as the product of the two irreducible polynomials $X + 2$ and 2.

To help us deal with the second issue, we introduce the following terminology: we say that a polynomial $P(X)$ in $R[X]$ is *primitive* if the greatest common divisor of its coefficients is 1. We then have:

Lemma 2.1. *Let $P(X)$ be any polynomial in $F[X]$. Then there exists an element $c \in F^\times$ such that $cP(X)$ is a primitive polynomial in $R[X]$. Moreover, c is unique up to multiplication by an element of $R^\times$; in particular if $P(X)$ lies in $R[X]$ then c^{-1} lies in R and is the greatest common divisor of the coefficients of $P(X)$.*

Proof. Choose d divisible by all the deminominators of coefficients of $P[X]$. Then $dP(X)$ lies in $R[X]$. Let d' be the greatest common divisor of all the cofficients of $dP(X)$. Then $\frac{d}{d'}P(X)$ is still an element of $R[X]$, and the greatest common divisor of its coefficients is 1, so we may take $c = \frac{d}{d'}$.

For uniqueness, let $P(X)$ be a primitive polynomial in $R[X]$, and let $u = \frac{a}{b} \in K[X]$ be such that $uP(X)$ is also a primitive polynomial in $R[X]$. We must show that u is a unit. But if the GCD of the coefficients of $P(X)$ is 1, then the GCD of the coefficients of $aP(X)$ is a. Since $buP(X) = aP(X)$, and $uP(X)$ lies in $R[X]$, b must divide every coefficient of $aP(X)$, so b divides a. On the other hand, since $uP(X)$ is primitive, the GCD of the coefficients of $buP(X)$ is b; since $P(X)$ is primitive this means a divides b. So u is a unit. □

The key to understanding factorization in $R[X]$, for R a UFD, is the following result, often called Gauss's Lemma:

Lemma 2.2 (Gauss's Lemma)**.** *Let R be a UFD, and let $P(X)$ and $Q(X)$ be primitive polynomials in $R[X]$. Then the product $P(X)Q(X)$ is also primitive.*

Proof. Let d be an element of R that divides every coefficient of $P(X)Q(X)$. We must show that d is a unit. Suppose not. Then choose irreducible divisor d' of d. Since d' divides every coefficient of $P(X)Q(X)$, we have $P(X)Q(X) = 0$ in the polynomial ring $R/\langle d'\rangle[X]$. But since in a UFD irreducible elements generate prime ideals, $R/\langle d'\rangle$ is an integral domain, and hence so is $R/\langle d'\rangle[X]$. Thus either $P(X) = 0$ or $Q(X) = 0$ in $R/\langle d'\rangle$, so d' divides all of the coefficients of either $P(X)$ or $Q(X)$. Since both of these polynomials were primitive, this is a contradiction. □

Corollary 2.3. *Let $P(X) \in R[X]$, and let $A(X)$ be a polynomial in $K[X]$ that divides $P(X)$ (in $K[X]$). Then there is an element $\alpha \in K^\times$ such that $\alpha A[X]$ lies in $R[X]$, and divides $P(X)$ in $R[X]$. (In particular, if $P(X)$ is reducible in $K[X]$, then $P(X)$ is also reducible in $R[X]$.)*

Proof. Write $P(X) = A(X)B(X)$ in $K[X]$, and choose nonzero elements $\alpha, \beta \in F^\times$ such that $\alpha A(X)$ and $\beta B(X)$ are primitive polynomials in $R[X]$. Letting $d = \alpha\beta$, we have $dP(X) = A'(X)B'(X)$ with $A'(X) = \alpha A(X)$ and $B'(X) = \beta B(X)$. Moreover, $dP(X)$ is a primitive polynomial in $R[X]$.

Let d' be the greatest common divisor of the coefficients of $P(X)$. Then $(d')^{-1}P(X)$ is a primitive polynomial in $R[X]$. Thus $(d')^{-1} = ud$ for some $u \in R^\times$. So we have:

$$P(X) = ud'(dP(X)) = ud'A'(X)B'(X)$$

which is a factorization of $P(X)$ over $R[X]$. □

Note that the converse to the last claim of the Corollary is not true: if $P(X)$ is reducible in $R[X]$, it might be irreducible in $K[X]$. For example, the polynomial $7x$ factors into irreducibles as $7 \cdot x$ in $\mathbb{Z}[X]$, but since 7 is a unit in $\mathbb{Q}[X]$, $7x$ is irreducible in $\mathbb{Q}[X]$. The following lemma shows that this kind of thing is all that can happen, however:

Lemma 2.4. *Let $P(X)$ in $R[X]$ be a polynomial and suppose that the greatest common divisor of all of its coefficents is 1. Then if $P(X)$ is irreducible in $K[X]$, it is also irreducible in $R[X]$.*

Proof. Suppose $P(X)$ is reducible in $R[X]$, and write $P(X) = A(X)B(X)$, with A and B nonunits. If $A(X)$ or $B(X)$ were constant then it would divide every coefficient of $P(X)$ and thus divide the GCD of those coefficients, making it a unit. Thus $A(X)$ and $B(X)$ are nonconstant and the factorization $P(X) = A(X)B(X)$ is also a nontrivial factorization in $K[X]$. □

We are now in a position to prove:

Theorem 2.5. *If R is a UFD, then $R[X]$ is a UFD.*

Proof. Let $P(X)$ be an element of $R[X]$. We must show that $P(X)$ factors into irreducibles. Let d be the greatest common divisor of the coefficients of $P(X)$, and write $P(X) = dQ(X)$ where $Q(X)$ is primitive. Since d factors into irreducibles in R, and these remain irreducible in $R[X]$, it suffices to show that $Q(X)$ factors into irreducibles. We do this by induction on the degree of $Q(X)$.

If the degree of $Q(X)$ is zero and $Q(X)$ is primitive then $Q(X)$ is a unit and we are done.

Suppose $Q(X)$ has positive degree d, and that we have proven the claim for all polynomials of degree less than d. Since the GCD of the coefficients of $Q(X)$ is one, the same will be true of any divisor of $Q(X)$. Let $R_1(X)$ be an irreducible factor of $Q(X)$, and write $Q(X) = R_1(X)Q_1(X)$. If $R_1(X)$ had degree zero it would be a unit since the GCD of its coefficents is 1. Thus $R_1(X)$ has positive degree, and the greatest common divisor of the coefficients of $Q_1(X)$ is one, so our inductive hypothesis shows that $Q_1(X)$ factors into irreducible factors and we are done.

It remains to show that if $Q(X)$ is irreducible in $R[X]$ and divides $A(X)B(X)$ in $R[X]$ then $Q(X)$ divides either $A(X)$ or $B(X)$ in $R[X]$. The irreducible elements of $R[X]$ are either irreducible elements of R or primitive polynomials in $R[X]$ that are irreducible in $K[X]$.

Suppose first that $Q(X)$ is an irreducible element d of R that divides $A(X)B(X)$. Let a and b be the greatest common divisors of the coefficients of $A(X)$ and $B(X)$, so that we have $A(X) = aA'(X)$ and $B(X) = bB'(X)$ with $A'(X)$ and $B'(X)$ primitive. Then $Q(X) = abA'(X)B'(X)$, and $A'(X)B'(X)$ is primitive, so d divides ab. But since R is a UFD and d

is irreducible, we must have $d|a$ or $d|b$, in which case d also divides $A(X)$ or $B(X)$, respectively.

Now suppose that $Q(X)$ is a primitive polynomial in $R[X]$ that is irreducible in $K[X]$. Then $Q(X)$ divides either $A(X)$ or $B(X)$ in $K[X]$. Suppose $Q(X)$ divides $A(X)$ in $K[X]$. Then there is an element $\alpha \in K^\times$ such that $\alpha Q(X)$ lies in $R[X]$ and divides $A(X)$ in $R[X]$. On the other hand, since $Q(X)$ is irreducible in $R[X]$ it is primitive, so the only way $\alpha Q(X)$ lies in $R[X]$ is if α lies in R. Thus $Q(X)$ also divides $A(X)$. □

Corollary 2.6. *If R is a UFD, then $R[X_1, \ldots, X_n]$ is a UFD for any n.*

3. Irreducible Polynomials

We will now use the results of the previous section to obtain criteria for proving polynomials are irreducible. We begin with some trivial observations:

Proposition 3.1. *Let K be a field, and $P(X) \in K[X]$ of degree at most three. Then $P(X)$ is irreducible if, and only if, $P(X)$ has no root in K.*

Proof. Any nontrivial factor of $P(X)$ would have to have degree one or two; either way, if $P(X)$ is reducible it must have a linear factor. □

Slightly less trivially, if K is finite there is a necessary and sufficient criterion for irreducibility:

Proposition 3.2. *Let K be a field with $q = p^r$ elements and let $P(X)$ in $K[X]$ have degree d. Then $P(X)$ is irreducible if, and only if, the greatest common divisor of $P(X)$ and $X^{q^a} - X$ is one for all $a < d$.*

Proof. The polynomial $P(X)$ is reducible if, and only if, it has an irreducible factor of degree less than d. It thus suffices to show that every irreducible polynomial $Q(X)$ in $K[X]$ of degree a divides $X^{q^a} - X$. Let $K' = K(\alpha)$, where α is a root of $Q(X)$; then K' has q^a elements, so every element of K' is a root of $X^{q^a} - X$. In particular α is such a root. Since $Q(X)$ is the minimal polynomial of α over K we must have $Q(X)|X^{q^a} - X$ in $K[X]$. □

Having obtained a satisfactory criterion for finite fields, the next simplest case to look at this that of $\mathbb{Q}[X]$. This is already much more complicated! We will take advantage of the fact that $\mathbb{Z}[X]$ lives inside $\mathbb{Q}[X]$. In fact, all of our tricks will work in the following more general situation: R is a UFD with field of fractions K, and we consider polynomials over $K[X]$. As we have seen, irreducibility over K is closely related to irreducibility in $R[X]$!

Let $P(X)$ be a polynomial in $K[X]$; we can multiply $P(X)$ by scalars without substantially changing its factorization, so we can assume that $P(X)$ is monic. In general there might be denominators in the coefficients of $P(X)$, but note that for any $r \in R$, if

$$P(X) = c_0 + c_1 X + c_2 X^2 + \cdots + X^n,$$

then define a polynomial $Q_r(X)$ by

$$Q_r(X) = r^n P(\frac{X}{r}) = c_0 r^n + c_1 r^{n-1} X + c_2 r^{n-2} X^2 + \cdots + X^n.$$

It is easy to see that $Q_r(X)$ is irreducible in $K(X)$ if, and only if, $P(X)$ is. Moreover, we can choose r so that $Q_r(X)$ has coefficients in R. We are thus reduced to the problem of deciding whether a monic polynomial with coefficients in R is irreducible in $K[X]$. Moreover, we have shown that such a polynomial is irreducible in $K[X]$ if, and only if, it is irreducible in $R[X]$!

We therefore get the following nice criterion for irreducibility:

Proposition 3.3. *Let $P(X)$ be a monic polynomial in $R[X]$, and let $\mathfrak{p}$ be a prime ideal of R. Suppose that the mod $\mathfrak{p}$ reduction $\overline{P}(X)$ is irreducible in $R/\mathfrak{p}[X]$. Then $P(X)$ is irreducible in $R[X]$.*

Proof. Suppose $P(X)$ were reducible in $R[X]$. Since $P(X)$ is monic, $P(X)$ must factor as $S(X)T(X)$ where both $S(X)$ and $T(X)$ are monic of positive degree. Then $\overline{P}(X)$ factors in $R/\mathfrak{p}[X]$ as $\overline{S}(X)\overline{T}(X)$, where both are monic of positive degree, so $\overline{P}(X)$ is also reducible. □

This means, for instance, that we can show that a monic polynomial in $\mathbb{Z}[X]$ is irreducible if we can find even one prime p for which it is irreducible mod p. Unfortunately, even when the polynomial is irreducible we won't always be able to do this. For instance, the polynomial $X^4 + 1$ is irreducible in $\mathbb{Z}[X]$, but reducible mod p for every p. (You can prove this with some elementary number theory, but it would take us a bit far afield to do that here.)

There is another sufficient criterion for irreducibility by "reducing mod $\mathfrak{p}$", known as "Eisenstein's Criterion":

Proposition 3.4. *Let $P(X) = c_0 + c_1 X + \cdots + X^n$ be a monic polnyomial in $R[X]$, and let $\mathfrak{p}$ be a prime ideal of R. Suppose that for $0 \leq i \leq n-1$, c_i lies in $\mathfrak{p}$, and c_0 does* not *lie in $\mathfrak{p}^2$. Then $P(X)$ is irreducible in $R(X)$.*

Proof. Suppose $P(X)$ is reducible; then we can write $P(X) = S(X)T(X)$ in $R[X]$, with $S(X)$ and $T(X)$ monic of positive degree. Reducing mod $\mathfrak{p}$ we find that $\overline{P}(X) = X^n = \overline{S}(X)\overline{T}(X)$. Write $\overline{S}(X) = X^s \overline{S'}(X)$ and $T(X) = X^t \overline{T'}(X)$ where $\overline{S'}(X)$ and $\overline{T'}(X)$ have nonzero constant term. Then $\overline{P(X)} = X^{s+t}\overline{S'}(X)\overline{T'}(X)$, so $s + t = n$ and $\overline{S'}(X)$ and $\overline{T'}(X)$ must both be 1 (compare the degree $s+t$ terms on both sides, and use that $R/\mathfrak{p}$ is an integral domain.) But then the constant terms of $S(X)$ and $T(X)$ both lie in $\mathfrak{p}$, so the constant term of $S(X)T(X)$ must lie in $\mathfrak{p}^2$, contradicting our assumptions. □