LECTURE 18

Divisibility in $F[x]$

All the results of Section 1.2 on divisibility and greatest common divisors in $\mathbb{Z}$ now carry over, with only minor modifications, to rings of polynomials over a field.

DEFINITION 18.1. *Let F be a field and $f, g \in F[x]$ with f nonzero. We say that f **divides** g (or that f is a **factor** of g), and write*

$$f \mid g \quad ,$$

if

$$g = fh$$

for some $h \in F[x]$.

Basic Observations:

(1) If f divides g, then if c is a nonzero element of F, $cf \mid g$.
(2) Every divisor of g has degree less than or equal to that of g.

DEFINITION 18.2. *A polynomial in $F[x]$ is said to be **monic** if its leading coefficient is 1_F.*

DEFINITION 18.3. *Let F be a field and let $f, g \in F[x]$. g is said to be an **associate** of f if there exists an nonzero c in F, such that*

$$g = cf \quad .$$

PROPOSITION 18.4. *Every non-zero polynomial $f \in F[x]$ has a unique monic associate.*

DEFINITION 18.5. *Let F be a field and $f, g \in F[x]$, not both zero. The **greatest common divisor** (GCD) of f and g is the monic polynomial d of highest degree that divides both f and g. In other words, d is the GCD of f and g if*

(i) *d is monic.*
(ii) *$d \mid f$ and $d \mid g$.*
(iii) *if $c \mid f$ and $c \mid g$, then $\deg(c) \leq deg(d)$.*

Remark: If f and g are nonzero monic polynomials of same degree and such that $f \mid g$, then $f = g$.

Proof. Since $f \mid g$ and $deg(f) = deg(g)$

$$f \quad = \quad qg \quad \Rightarrow \quad deg(g) = def(f) = deg(q) + deg(g)$$

so $deg(q) = 0$. Hence, the factor q must be a constant polynomial; But then $deg(q) = deg(r) = 0$, so the polynomials

$$q = c \quad .$$

Hence

$$f = cg \quad .$$

But the leading coefficients of f and g are both 1. Therefore $c = 1$; hence $f = g$. ∎

THEOREM 18.6. *Let F be a field and $f, g \in F[x]$, not both zero. Then there is a unique greatest common divisor d of f and g. Furthermore, there exist (not necessarily unique) polynomials u and v such that*

$$d = fu + gv \quad .$$

Proof. Let

$$S = \{fm + gn \mid m, n \in F[x]\} \quad .$$

and let

$$R = \{n \in \mathbb{N} \mid d = \deg(s) \text{ for some} s \in S\} \quad .$$

By the Well Ordering Axiom for $\mathbb{N}$, R has a minimal element k. Let d be a monic polynomial of degree k in S. Since $d \in S$, we can express d as

$$d = fu + gv \quad ,$$

with $u, v \in F[x]$. By the Division Algorithm, there exist polynomials q and r such that

(1)
$$f = dq + r$$

with

(2)
$$r = 0_F \quad \text{or} \quad \deg(r) < \deg(d) \quad .$$

Consequently,

$$\begin{aligned} r &= f - dq \\ &= f - (fu + gv)\, q \\ &= f(1-u) + g(-vq) \quad . \end{aligned}$$

Thus, r is a linear combination of f and g, and so r is an element of S. Since d is a monic polynomial of minimal degree in S, we must have

$$\deg(r) \geq \deg(d) \quad .$$

But this contradicts (**??**) unless $r = 0_F$. Therefore, d divides f. Similarly, one shows that d divides g.

Now suppose c is another divisor of f and g; then

$$f = mc \quad , \quad g = nc$$

for some $m, n \in F[x]$. Then

$$\begin{aligned} \deg(d) &= \deg(fu + gv) \\ &= \deg(mcu + ncv) \\ &= \deg(c(mu + nv)) \\ &= \deg(c) + \deg(mu + nv) \end{aligned}$$

So if c another divisor of f and g, then

$$\deg(d) \geq \deg(c) \quad .$$

Thus, d is a GCD of f and g.

Now suppose that d_1 is any *GCD* of f and g. To prove uniqueness, we need to show that $d_1 = d$. Since d_1 is a common divisor, we have

$$f = d_1 a \quad , \quad g = d_1 b$$

for some $a, b \in F[x]$. Therefore,

$$\begin{aligned} d &= fu + gv \\ &= d_1 au + d_1 bv \\ &= d_1 (au + bv) \quad . \end{aligned}$$

By Theorem 4.1,

$$\deg(d) = \deg(d_1) + \deg(au + bv)$$

Since d and d_1 are both GCDs of f and g we must have

$$\deg(d) = \deg(d_1) \quad .$$

This forces $\deg(au + bv) = 0$, so $au + bv$ must be a constant polynomial; i.e., $au + bv = c$, some nonzero element of F. Therefore,

$$d = d_1 c.$$

But, as d and d_1 are both monic polynomials (since they are both GCDs), we must have $c = 1_F$. Therefore $d = d_1$. ∎

COROLLARY 18.7. *Let F be a field and $f, g \in F[x]$, not both zero. A monic polynomial $d \in F[x]$ is the greatest common divisor of f, g if and only if d satisfies these conditions:*

(i) *$d \mid f$ and $d \mid g$;*
(ii) *If $c \mid g$ and $c \mid g$, then $c \mid d$.*

Proof. Property (i) just says that d is a common divisor of f and g. The cruxt of the matter is property (ii). We must show that (in accordance with the definition of a GCD of f and g) that if $c \in F[x]$ satisfies (ii) then $\deg(c) \leq \deg(d)$. But if $c \mid d$, then $d = cs$ for some nonzero polynomial $s \in F[x]$. Hence

$$\deg(d) = \deg(c) + \deg(s) \quad \Rightarrow \quad \deg(d) \geq \deg(c) \quad .$$

So if d satisfies Properties (i) and (ii) above, then d is **a** greatest common divisor of f and g. By Theorem 4.4 above, d is **the** GCD of f and g. ∎

DEFINITION 18.8. *Let F be a field. Two polynomials $f, g \in F[x]$ are said to be* ***relatively prime*** *if their greatest common divisor is 1_F.*

THEOREM 18.9. *Let F be a field and $f, g, h \in F[x]$. If $f \mid gh$ and f and g are relatively prime, then $f \mid h$.*

Proof. Suppose f and g are relatively prime. Then by Theorem 4.4 there exist polynomials u and v such that

$$1_F = fu + gv$$

Multiplying this equation by h yields

$$h = hfu + hgv \quad . \tag{1}$$

But by hypothesis, hg is divisible by f so we may write

$$hg = fq$$

for some nonzero $q \in F[x]$. Then (**??**) can be rewritten as

$$h = hfu + fqv = (hu + qv)f \quad .$$

So $f \mid h$. ∎

Proof: see the following lecture.