Math 521A

4.2 – Divisibility in $F[x]$

- Throughout this section F denotes a field.
- $f(x)$ divides $g(x)$ (notation $f(x) \mid g(x)$) if $\exists\, h(x) \in F[x]$ such that $g(x) = f(x) \cdot h(x)$.
- An integer has finitely many divisors. This may not be the case for polynomials:

$$f(x) \mid g(x) \Rightarrow cf(x) \mid g(x) \quad \forall\, c \neq 0 \text{ in } F.$$

- Suppose $f(x) \mid g(x)$. Then $g(x) = f(x) \cdot h(x)$ and $\deg g = \deg f + \deg h$. Thus, $0 \leq \deg f \leq \deg g$.

Definition (Greatest Common Divisor)

Let $f(x), g(x) \in F[x]$, not both zero. Then $d(x)$ is the gcd of $f(x)$ and $g(x)$ (notation: $d(x) = \gcd(f(x), g(x))$) if:

1. $d(x)$ is *monic* (that is, its leading coefficient equals 1_F);
2. $d(x) \mid f(x), \quad d(x) \mid g(x)$;
3. $c(x) \mid f(x), \quad c(x) \mid g(x) \Rightarrow \deg c(x) \leq \deg d(x)$.

The existence and uniqueness of the gcd is guaranteed by

Theorem

Let F be a field, and $f(x), g(x) \in F[x]$, not both zero. Then the gcd of $f(x)$ and $g(x)$, namely, $d(x)$, exists and is unique. Moreover, there exist polynomials $u(x), v(x) \in F[x]$ such that

$$d(x) = f(x) \cdot u(x) + g(x) \cdot v(x).$$

Proof sketch (see details on the board):

1. Let $S = \{f(x) \cdot m(x) + g(x) \cdot n(x) \mid m(x), n(x) \in F[x]\}$;
2. Let $t(x)$ be the monic polynomial of smallest degree in S;
3. Prove that $t(x) = \gcd(f(x), g(x))$ and that $t(x)$ is unique. $\square$

Corollary

$d(x) = \gcd(f(x), g(x))$ *if and only if:*

1. $d(x)$ *is monic;*
2. $d(x) \mid f(x), \quad d(x) \mid g(x);$
3. $c(x) \mid f(x), \quad c(x) \mid g(x) \Rightarrow c(x) \mid d(x).$

Example

Calculate $\gcd(f(x), g(x))$ when:

- $f(x) = x^3 + 2x^2 + 2x + 1, \ g(x) = x^3 + 3x^2 + 3x + 2 \in \mathbb{Q}[x];$
- $f(x) = x^5 + x^2 + x + 1, \ g(x) = x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x].$

Definition

$f(x)$ and $g(x)$ in $F[x]$ are said to be relatively prime if

$$\gcd(f(x), g(x)) = 1_F.$$

Theorem

Let $f(x), g(x), h(x) \in F[x]$. If $f \mid gh$ and $(f, g) = 1$ then $f \mid h$.