Week 2 pt 2 #

Issues

1) Greatest common divisors might not be unique
2) Greatest common divisors might not exist

FACT: In a Euclidean domain

- greatest common divisors always exist (can be computed with division algorithm
- they are unique "up to unit"

If d and d' are gcd's for some elements,
then $d = ud'$ for some unit $u \in R$

In $\mathbb{Z}$, units: ± 1

then we can just choose the positive one
$\Rightarrow$ the gcd (a,b)

In $F[x]$ units: $f(x) = c_0$ $c_0 \in F \setminus \{0\}$

→ choose the gcd so the top-deg coeff is 1

$d(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0$ "monic polynomial

Back to ex: 1

$f(x) = x^5 + 3x^3 + 5x^2 + 2x + 5$ $\quad g(x) = 2x^3 + x^2 + 2x + 1$

$f(x) = q_1(x)g(x) + \underbrace{3x^2 + 3}_{r_1(x)}$

$\Rightarrow \gcd(f,g) = \gcd(g, r_1)$

then divide g by r_1

$$
\begin{array}{r|l}
 & 3x + 5 \quad (q_2) \\
\hline
3x^2 + 0x + 3 & 2x^3 + x^2 + 2x + 1 \\
 & 2x^3 + 0 + 2x \\
\hline
 & x^2 + 1 \\
 & x^2 + 1 \\
\hline
 & 0 \quad (r_2)
\end{array}
$$

so $\Rightarrow$ a gcd of f, g is

$r_1(x) = 3x^2 + 3$

$\Rightarrow$ the $\gcd(f,g) = x^2 + 1$

$f(x) = x^5 + 3x^3 + 5x^2 + 2x + 5 = (x^2+1)(x+2)^2(x+3)$

$g(x) = 2x^3 + x^2 + 2x + 1 = (2x+1)(x^2+1)$