Poly Divisibility
Factoring Polys

$f(x) = q(x)g(x) + r(x)$
$\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$

Definition: $g(x) \mid f(x)$ if there is $q(x)$ such that $f(x) = q(x)g(x)$

$\mathbb{C}[x]$

$(x+1) \mid (x^2-1) \qquad x^2-1 = (x+1)(x-1)$

$3(x+1) \mid (x^2-1) \qquad x^2-1 = (3x+3)(\frac{1}{3}x - \frac{1}{3})$

Definition: $\gcd(f(x), g(x))$ is the polynomial $d(x)$ such that $d(x) \mid f(x)$, $d(x) \mid g(x)$, $d(x)$ has the largest degree, where coeff of x with highest degree is 1.

$\gcd(x^2-1, x^2+2x+1) = x+1$

Proposition: If $f(x) = g(x)q(x) + r(x)$, then $\gcd(f(x), g(x)) = \gcd(g(x), r(x))$.

Proposition: There exists $p(x), q(x)$ such that
$f(x)p(x) + g(x)q(x) = \gcd(f(x), g(x))$

$(x^2-1)\boxed{} + (x^2+2x+1)\boxed{} = x+1$

$$\begin{array}{r|l} & 1 \\ x^2+2x+1 & x^2 \quad -1 \\ & x^2+2x+1 \\ \hline & -2x-2 \end{array} \qquad \begin{array}{r|l} & -1/2x \\ -2x-2 & x^2+2x+1 \\ & x^2+x \\ \hline & x+1 \end{array}$$

$x^2+1 = 1\cdot(x^2+2x+1) + (-2x-2)$ *calculations on last page*

$x^2+2x+1 = -\frac{1}{2}x(-2x-2) + \underbrace{(x+1)}_{\text{gcd}}$

$x+1 = (x^2+2x+1) + \frac{1}{2}x\left[(x^2-1) - (x^2+2x+1)\right]$

$x+1 = \frac{1}{2}x(x^2-1) + (1-\frac{1}{2}x)(x^2+2x+1)$

Exercise: Find $\gcd(x^3+x^2+x+1,\ x^3-x^2+x+1)$

Factoring Polys

Let $f(x) \in \mathbb{F}[x]$. When does $x-c$ divide $f(x)$?

By div. Alg, $f(x) = q(x)(x-c) + r(x)$, where $r(x)$ is a constant, r. So $f(c) = r$.

Proposition (Remainder Theorem): The remainder of $f(x)$ divided by $x-c$ is $f(c)$.

Proposition (Factor Theorem): $x-c$ is a factor of $f(x)$ if and only if $f(c)=0$, i.e. c is a root of $f(x)$.

Example: $\mathbb{C}[x]$ $f(x) = x^3+x^2+x+1$

$x-1$? $f(1)=4$, rem. of $f(x)$ divided by $x-1$ is 4,

so $(x-1) \nmid f(x)$.

$x+1$: $f(-1)=0$. So $x+1$ is a factor.

$x+i$: $f(-i)=(-i)^3+(-i)^2+(-i)+1=0$ $x+i$ is another factor.

$x-i$ is another factor.

Fun. T. of Al.: Any poly in $\mathbb{C}[x]$ of deg ≥ 1 has a root in $\mathbb{C}$.

Let $f(x) \in \mathbb{C}[x]$, $\deg(f(x))=n$ By F.T. of Al., $f(x)$ has a root $r_1 \in \mathbb{C}$. By factor Theorem, $x-r_1$ is a factor of $f(x)$.

So $f(x)=(x-r_1)g(x)$ where $\deg(g(x))=n-1$.

(Assume n large). $g(x)$ has a root r_2, $(x-r_2) \mid g(x)$.

So $f(x)=(x-r_1)(x-r_2)h(x)$. $\deg(h(x))=n-2$.

Theorem: If $f(x) \in \mathbb{C}[x]$ has deg. n, then:

$$f(x)=a(x-r_1)(x-r_2)\dots(x-r_n)$$

where $a, r_1, \dots, r_n \in \mathbb{C}$.

Proof: by induction.