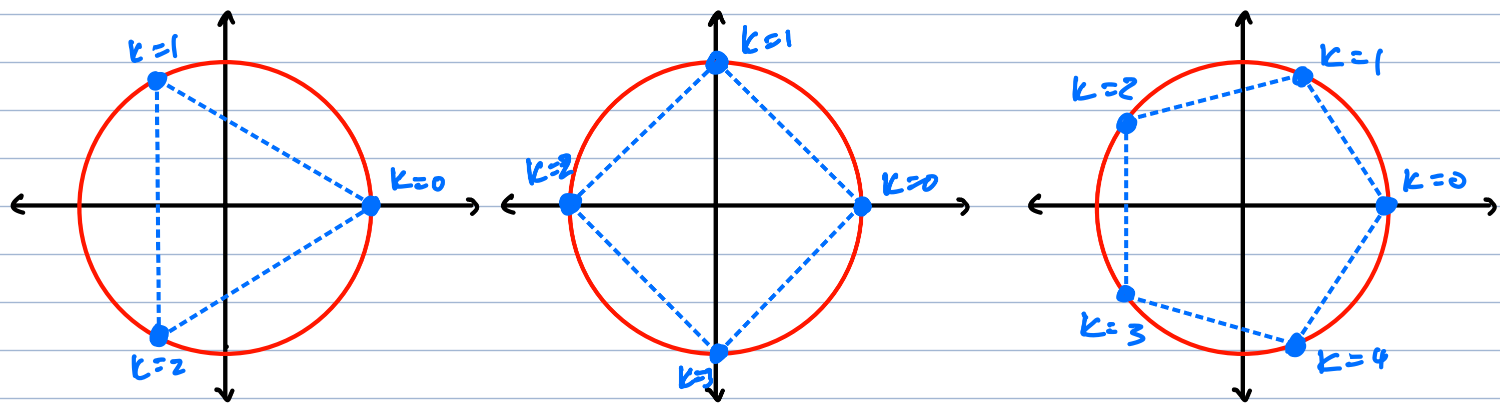
Corollary: Let F be a field. A nonzero polynomial $p(x) \in F[x]$ of degree n has at most n roots, including multiplicities.

Example: Consider $x^n - 1 \in \mathbb{C}[x]$. Recall that $e^{i\theta} = \cos(\theta) + i\sin(\theta)$, then by De Moivre's Theorem, we have that $(e^{i\theta})^n = e^{in\theta}$. Then if we let $0 \leq k \leq n-1$ be such that $\theta = \frac{2\pi k}{n}$, we have

$(e^{i\frac{2\pi k}{n}})^n = e^{2\pi k i} = \cos(2\pi k) + i\sin(2\pi k) = 1$ and therefore, our n roots of unity are $1, e^{\frac{2\pi}{n}i}, e^{\frac{4\pi}{n}i}, \ldots, e^{\frac{(n-1)\pi}{n}i}$. When $n = 3, 4, 5$



Remark: If p is prime, then $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$ is called the cyclotomic polynomial, where it has no roots on $\mathbb{R}$ and $(p-1)$ roots on $\mathbb{C}$.

Fundamental Theorem of Algebra: A polynomial of degree n in $\mathbb{C}[x]$ has exactly n roots in $\mathbb{C}$.

Proposition: Let F be an infinite field, and let $f(x) \in F[x]$. If $f(a) = 0$ for infinitely many elements $a \in F$, then $f(x) = 0$.

Proof: Assume that $f(x) \neq 0$. Then $\deg(f(x)) = n \in \mathbb{N}$ and so by the above Corollary, $f(x)$ has at most n distinct roots in F, so $f(x)$ does not have infinitely many roots.

Corollary: Let $g(x), h(x) \in F[x]$ for some field F such that the degree of $g(x)$ is the same as the degree of $h(x)$. If $g(a) = h(a)$ for $n+1$ distinct elements $a \in F$, then $g(x) = h(x)$.

Example: In $\mathbb{Z}_3$, if $f(x) = x^{k_1}(x-1)^{k_2}(x-3)^{k_3}$, then $f(x)$ is a nonzero polynomial in $\mathbb{Z}_3[x]$ that contains every element of $\mathbb{Z}_3$ as a root.

Exercise: Prove that for every positive integer n, a field F can have at most a finite number of elements of multiplicative order at most n.

Irreducible Polynomials

Definition: Let F be a field and let $p(x) \in F[x]$ with $\deg(p(x)) = n \in \mathbb{N}$.

- $p(x)$ is said to be irreducible over F, if $p(x)$ cannot be expressed as a product of polynomials in $F[x]$ with degree at least 1.
- $p(x)$ is reducible over F if $f(x) = g(x)h(x)$ for some polynomial that have degree at least 1.

Example: Consider $f(x) = 2x^2 + 2$ over $\mathbb{R}$. Then note that $f(x) = 2(x^2+1)$, but it is irreducible over $\mathbb{R}$, because if $g(x) = 2$ and $h(x) = x^2+1$, then $\deg(g(x)) = 0 \not\geq 1$, so $f(x)$ cannot be reducible.

Example: Consider $f(x) = 2x^2 + 2$ over $\mathbb{C}$. Then because we are in $\mathbb{C}$, we can now write $f(x) = (\sqrt{2}x - \sqrt{2}i)(\sqrt{2}x + \sqrt{2}i)$ where if $g(x) = \sqrt{2}x - \sqrt{2}i$ and $h(x) = \sqrt{2}x + \sqrt{2}i$, then $\deg(g(x)) = \deg(h(x)) = 1 \geq 1$, so it is reducible.

Example: By the Fundamental Theorem of Algebra, the irreducible polynomials in $\mathbb{C}[x]$ have degree 1.

Example: In $\mathbb{Z}_3$, $f(x) = x^2+1$ is not irreducible.

$f(0) = 0^2 + 1 = 1 \qquad f(1) = 2 \qquad f(2) = 2.$

Because $f(x) \neq 0$ for all $x \in \mathbb{Z}_3$, then $f(x)$ has no roots and therefore cannot be reducible over $\mathbb{Z}_3$. Since $f(x)$ has degree 2, if $f(x) = g(x)h(x)$ then either one of $g(x)$ and $h(x)$ has degree 2, or each of $g(x)$ and $h(x)$ has degree 1.

If $f(x)$ was reducible over $\mathbb{Z}_3$, then it would have 2 roots, but $f(0) \neq 0$, $f(1) \neq 0$, $f(2) \neq 0$, so $f(x)$ has no roots. Therefore, $f(x)$ is irreducible over $\mathbb{Z}_3$.

Example: In $\mathbb{Z}_5$, $f(x) = x^2+1$ is irreducible. Note that $f(3) = 3^2+1 = 0$ in $\mathbb{Z}_5$, so $f(x) = (x+2)(x+3)$.

Proposition: Let F be a field and let $f(x) \in F[x]$ with $\deg(f(x)) = 2$ or $\deg(f(x)) = 3$. Then $f(x)$ is reducible over F if and only if $f(x)$ has a root in F.

Proof: Exercise.

Theorem: If F is a field,

(1) Every ideal $I \triangleleft F[x]$ is a principal ideal

$\langle f(x) \rangle = \{ r(x) f(x) : r(x) \in F[x] \}$

(2) $F[x]/\langle f(x) \rangle$ is a quotient ring.

(3) $\langle f(x) \rangle$ is a maximal ideal if and only if $F[x]/\langle f(x) \rangle$ is a field.

Theorem: Let F be a field and let $f(x) \in F[x]$. Then $\langle f(x) \rangle$ is a maximal ideal of $F[x]$ if and only if it is an irreducible polynomial.