L40P1

Restatement of CNRT

If $a = re^{i\theta}$, then solutions to $z^n = a$ are given by

$$z = \sqrt[n]{r}\, e^{i\left(\frac{\theta + 2\pi k}{n}\right)}$$

for $k \in \{0, 1, \ldots n-1\}$

Solve $z^6 + 2z^3 - 3 = 0$

Sol'n: $(z^3 - 1)(z^3 + 3) = 0$

$\Rightarrow z^3 = 1$ OR $z^3 = -3$

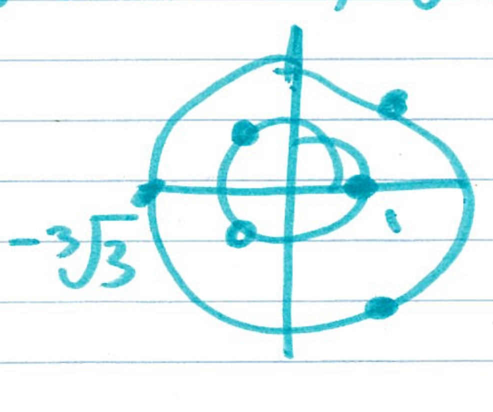
Note $1 = e^{i \cdot 0}$ & $-3 = 3e^{i\pi}$

By CNRT, sol'ns to $z^3 = 1$ are given by

$$z \in \{e^{i \cdot 0}, e^{i 2\pi/3}, e^{i 4\pi/3}\}.$$

and solutions to $z^3 = -3$ are given by

$$z \in \{\sqrt[3]{3}\, e^{i\pi/3}, \sqrt[3]{3}\, e^{i\pi}, \sqrt[3]{3}\, e^{i 5\pi/3}\}$$



Polynomials

For us fields include

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}_p$ for p a prime

Def'n: A polynomial in x over a field $\mathbb{F}$ is an expression of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where $a_0, a_1, \ldots a_n \in \mathbb{F}$ and $n \geq 0$ is an integer. Denote the set/ring of all polynomials over $\mathbb{F}$ by $\mathbb{F}[x]$.

Ex:
- $(2\pi + i)z^3 - \sqrt{7}z + \frac{55i}{4} \in \mathbb{C}[z]$
- $[5]x^2 + [3]x + [1] \in \mathbb{Z}_7[x]$

  $5x^2 + 3x + 1 \in \mathbb{Z}_7[x]$
- $x^2 + \frac{1}{x}$ is <u>NOT</u> a polynomial.
- $x + \sqrt{x}$ is <u>NOT</u> a polynomial.

Definitions:

- The coefficient of x^n is a_n.
- The degree of a polynomial is n provided $a_n x^n$ is the largest non-zero term.
- A term of a polynomial is any $a_i x^i$.
- 0 is the zero polynomial
- A root of a polynomial $p(x) \in \mathbb{F}[x]$ is a value $a \in \mathbb{F}$ s.t. $p(a) = 0$.
- If the degree of a polynomial is
  - ↳ 1, the polynomial is linear
  - ↳ 2, the polynomial is quadratic
  - ↳ 3, the polynomial is cubic.

$\mathbb{C}[x]$ complex polynomials, $\mathbb{R}[x]$ real, $\mathbb{Q}[x]$ rational, $\mathbb{Z}[x]$ integral

- Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$

  $g(x) = b_n x^n + \cdots + b_1 x + b_0$

be polynomials over $\mathbb{F}[x]$. Then $f(x) = g(x)$ iff $a_i = b_i$ forall $i \in \{0, 1, \ldots n\}$

- Operations:

  Addition, subtraction, multiplication

- x is an indeterminate (or a variable). It has no meaning on its own (but can be replaced with a value when this makes sense.

L40P5

Simplify $(x^5 + x^2 + 1)(x + 1) + (x^3 + x + 1)$ over $\mathbb{Z}_2[x]$

$= x^6 + x^5 + x^3 + x^2 + x + 1 + x^3 + x + 1$

$= x^6 + x^5 + 2x^3 + x^2 + 2x + 2$

$= x^6 + x^5 + x^2$

Prove $(ax+b)(x^2+x+1)$ over $\mathbb{R}$ is the zero polynomial iff $a=b=0$.

Pf: Expanding gives

$$(ax+b)(x^2+x+1)$$
$$= ax^3+(a+b)x^2+(a+b)x+b$$

This is 0 iff

$$a=0 \ \& \ (a+b)=0 \ \& \ b=0$$

which holds iff $a=0=b$. ☒

(DAP) Division Algorithm for Polynomials

If $f(x), g(x) \in \mathbb{F}[x]$ & $g(x) \neq 0$ then $\exists!$ polynomials $q(x)$ & $r(x) \in \mathbb{F}[x]$ s.t.

$$f(x) = q(x)g(x) + r(x)$$

with $r(x)=0$ OR $\deg(r(x)) < \deg(g(x))$

Pf: Exercise.

Notes:

- $q(x)$ is the quotient
- $r(x)$ is the remainder
- If $r(x)=0$ then $g(x)$ divides $f(x)$ and we write $g(x) \mid f(x)$. Otherwise, $g(x) \nmid f(x)$.

Ex: Show over $\mathbb{R}[x]$ that

$$(x-1) \nmid x^2+1$$

Pf: By DAP, $\exists\ q(x), r(x) \in \mathbb{R}[x]$ s.t.

$$x^2+1 = (x-1)q(x) + r(x)$$

To show $r(x) \neq 0$ it suffices to show $r(a) \neq 0$ for some $a \in \mathbb{F}$. Take $x=1$.

Then $$(1)^2+1 = (1-1)q(1) + r(1)$$

$$2 = r(1)$$

$\therefore r(x) \neq 0$ hence $(x-1) \nmid x^2+1$ ∎

Long Division

Let's Divide

$$f(z) = iz^3 + (i+3)z^2 + (5i+3)z + (2i-2)$$

by $g(z) = z + (i+1)$

$$\begin{array}{r|l}
 & iz^2 + 4z + (i-1) \\ \hline
z+(i+1) & iz^3 + (i+3)z^2 + (5i+3)z + (2i-2) \\
 & \underline{-(iz^3 + (i-1)z^2)} \\
 & \qquad 4z^2 + (5i+3)z \\
 & \qquad \underline{-(4z^2 + (4i+4)z)} \\
 & \qquad\qquad (i-1)z + (2i-2) \\
 & \qquad\qquad \underline{-((i-1)z \quad -2)} \\
 & \qquad\qquad\qquad\qquad 2i
\end{array}$$

$\therefore q(z) = iz^2 + 4z + (i-1)$

$r(z) = 2i$