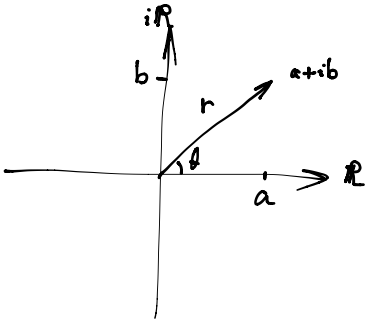
Jan 15th, 2013
Office: BA 6120
Office hour: W 2-4pm or by appt.
email: oyacobi@math.toronto.edu

warm-up: $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R},\ i^2 = -1\}$
(real part, imaginary part)

$= \{r(\cos\theta + i\sin\theta) \mid r \geq 0,\ \theta \in [0, 2\pi]\}$
(absolute value, argument)



$e^{i\theta} = \cos\theta + i\sin\theta$
$e^{i\pi} = 1 + 0i = 1$

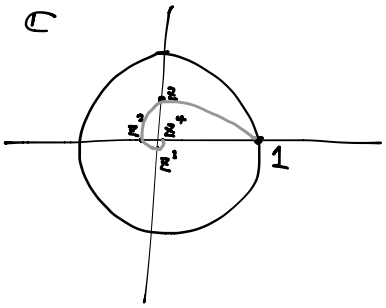
$(a_1 + ib_1)(a_2 + ib_2) = (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1)$
$(a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2)$

$*\ (r(\cos\theta + i\sin\theta))(s(\cos\tau + i\sin\tau))$
$= rs(\cos(\theta + \tau) + i\sin(\theta + \tau))$

Why is this true?
$rs(\cos\theta\cdot\cos\tau - \sin\theta\sin\tau) + i(\sin\theta\cos\tau + \cos\theta\sin\tau))$

$z = \frac{i}{2}$

$1, z, z^2, z^3, \ldots$



Why do we need $\mathbb{C}$?

R_θ = rotation matrix by θ.

$= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$

$Av = \lambda v$ (λ: eigenvalue, v: eigenvector)

To find eigenvalues of R_θ we computer roots of $p(\lambda) = \det(\lambda I - A)$

$= \begin{vmatrix} \lambda - \cos\theta & \sin\theta \\ -\sin\theta & \lambda - \cos\theta \end{vmatrix}$
$= (\lambda - \cos\theta)^2 + \sin^2\theta$
$= \lambda^2 - 2\cos\theta\lambda + 1$
roots: $\frac{2\cos\theta \pm \sqrt{4\cos^2\theta - 4}}{2}$
$= \cos\theta \pm i\sin\theta$

What are the n^{th} roots of unity?

n^{th} roots of unity $= \{z \in \mathbb{C} : z^n = 1\}$

Ex: $n=4$ $\quad z = \pm 1, \pm i$

$z = r(\cos\theta + i\sin\theta)$

$z^n = ?$ $\quad z^n = r^n(\cos n\theta + i \sin n\theta)$

want $r^n(\cos n\theta + i\sin n\theta) = 1$

$\Rightarrow r = 1$ and $n\theta = 2\pi k$

$\Rightarrow r = 1$ and $\theta = \frac{2\pi k}{n}$

$\Rightarrow \{\cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}) \mid k = 0, \dots, n-1\}$ is the nth roots of unity.

Fields:

EXS: Is F a field?

① $\mathbb{N} = \{0, 1, 2, \dots\}$ No. doesn't have additive identity

$a + (b+c) = (a+b) + c$ ✓

② $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ No, doesn't have multiplicative inverse.

③ $\mathbb{Q} = \{\frac{m}{n} \cdot m, n \in \mathbb{Z}\}$ Yes.

If $\frac{m}{n} \neq 0$ then $\frac{n}{m}$ is its mult. inverse.

$x(y+z) = xy + xz$

④ $\mathbb{R}$. Yes.

⑤ $\mathbb{C}$ Yes.

⑥ $\mathbb{R}[x]$ = polynomial with coefficients in $\mathbb{R}$. No.

⑦ $\mathbb{R}(x) = \{\frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{R}[x]\}$ Yes.

⑧ p prime. $\quad \mathbb{F}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$

addition: $\bar{a} + \bar{b} = \bar{c}$ where c is the remainder of $\frac{a+b}{p}$

multiplication: $\bar{a} \cdot \bar{b} = \bar{c}$, where c is the remainder of $\frac{ab}{p}$

$\mathbb{F}_3$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

Why do we need p to be prime? Suppose we try to define $\mathbb{F}_6$ ...

$\mathbb{F}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$						
$\bar{1}$						
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$						
$\bar{4}$						
$\bar{5}$						

→ $\bar{2}$ doesn't have multi. inverse which leads to $\bar{1}$.

Ex: Does $f(x) = x^2 + \bar{2}x - \bar{2}$ have roots in $\mathbb{F}_3$.

$f(\bar{0}) = (\bar{0})^2 + \bar{2}\cdot\bar{0} - \bar{2} = -\bar{2} = \bar{1}$

↑ why? because $\bar{1} + \bar{2} = \bar{0}$ so $\bar{1} = -\bar{2}$

$f(\bar{1}) = (\bar{1})^2 + \bar{2}\cdot\bar{1} - \bar{2} = \bar{1} + \bar{2} - \bar{2} = \bar{1}$

$f(\bar{2}) = (\bar{2})^2 + \bar{2}\cdot\bar{2} - \bar{2} = \bar{1} + \bar{1} - \bar{2} = \bar{0}$

Alternatively, could compute this $2^2 + 2\cdot 2 - 2 = 6 = \bar{0}$

We consider vector spaces over a field F.

* def is exactly the same as for vector spaces over $\mathbb{R}$, except scalars must come from F.

* $F^n = \left\{ \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \mid a_i \in F \right\}$

* $P_n(F)$ = polynomials of deg $\leq n$ with coeffs in F.

Ex: $V = \mathbb{C}^n$.

1. a vector space over $\mathbb{C}$.
   with basis $e_1, \cdots, e_n$
   where $e_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}$ ← i^{th} position

why do they span $\mathbb{C}^n$? Let $v = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix} \in \mathbb{C}^n$.

prove span

$v = z_1 e_1 + \cdots + z_n e_n$

prove linear independence

Sps $z_1e_1 + \cdots + z_ne_n = 0$

$$\Rightarrow \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \Rightarrow z_i = 0 \text{ for } i = 1, \cdots, n$$

Show independence

* Some proof shows F^n has a standard basis $e_1, \cdots, e_n$.

Ex: $V = \mathbb{C}^2$ vector space over $\mathbb{R}$

$$V = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \in \mathbb{C}^2$$

$$V = \begin{bmatrix} a_1 + ib_1 \\ a_2 + ib_2 \end{bmatrix} \qquad v_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \; v_2 = \begin{bmatrix} i \\ 0 \end{bmatrix} \; v_3 = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \; v_4 = \begin{bmatrix} 0 \\ i \end{bmatrix}$$

$V = a_1v_1 + b_1v_2 + a_2v_3 + b_2v_4 \Rightarrow$ spanning

continue $\Rightarrow$ check linear independence.

Note: $\dim_{\mathbb{C}} \mathbb{C}^2 = 2$

$\dim_{\mathbb{R}} \mathbb{C}^2 = 4$