Lecture 40

Handout or Document Camera or Class Exercise

What is the value of $\left|\left(\overline{-\sqrt{3}+i}\right)^5\right|$?

A) $16i$

B) 27

C) 32

D) -45

E) 64

Solution:

Instructor's Comments: Emphasize there are lots of ways to get the solution.

$$\begin{aligned}
\left|\left(\overline{-\sqrt{3}+i}\right)^5\right| &= \left|\left(-\sqrt{3}-i\right)^5\right| \\
&= \left|\left(-\sqrt{3}-i\right)\right|^5 \qquad \text{PM} \\
&= \sqrt{(-\sqrt{3})^2+(-1)^2}^{\,5} \\
&= \sqrt{4}^{\,5} \\
&= 32
\end{aligned}$$

Instructor's Comments: This is the 7-10 minute mark depending on how many ways you find the above answer

Polynomials For us, a field will mean to include $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ where p is a prime number. A ring will include the aforementioned fields as well as $\mathbb{Z}$ and $\mathbb{Z}_m$ for any $m \in \mathbb{N}$.

Definition: A polynomial in x over a ring R is an expression of the form

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

where $a_0, a_1, ...a_n \in R$ and $n \geq 0$ is an integer. Denote the set (actually a ring) of all polynomials over R by $R[x]$.

Instructor's Comments: We will predominately use fields in the above definition. Some of the theorems we do will only work in the case of fields. For simplicity I will state all the theorems with fields to match the textbook though in many cases, a ring is all you need.

Example:

(i) $(2\pi + i)z^3 - \sqrt{7}z + \frac{55}{4}i \in \mathbb{C}[z]$.

(ii) $[5]x^2 + [3]x + [1] \in \mathbb{Z}_7[x]$. We usually write this as $5x^2 + 3x + 1 \in \mathbb{Z}_7[x]$.

(iii) $x^2 + \frac{1}{x}$ is *not* a polynomial.

(iv) $x + \sqrt{x}$ is *not* a polynomial.

(v) $1 + x + x^2 + ...$ is *not* a polynomial.

Definition:

(i) The coefficient of $a_n x^n$ is a_n

(ii) A term of a polynomial is any $a_i x^i$

(iii) The degree of a polynomial is n provided $a_n x^n$ is the term with the largest exponent on x and nonzero coefficient.

(iv) 0 is the zero polynomial (all coefficients are 0). The degree of the zero polynomial is undefined (some books say it is negative infinity for reasons we will see later)

(v) A root of a polynomial $p(x) \in R[x]$ is a value $a \in R$ such that $p(a) = 0$.

(vi) If the degree of a polynomial is

- 1, then the polynomial is linear.
- 2, then the polynomial is quadratic.
- 3, then the polynomial is cubic.

(vii) $\mathbb{C}[x]$ are the complex polynomials, $\mathbb{R}[x]$ are the real polynomials, $\mathbb{Q}[x]$ are the rational polynomials, $\mathbb{Z}[x]$ are the integral polynomials.

(viii) Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \qquad \text{and} \qquad g(x) = b_n x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0$$

be polynomials over $R[x]$. Then $f(x) = g(x)$ if and only if $a_i = b_i$ for all $i \in \{0, 1, ..., n\}$.

(ix) x is an indeterminate (or a variable). It has no meaning on it's own but can be replaced by a value whenever it makes sense to do so.

(x) Operations on polynomials: Addition, Subtraction, Multiplication (See next page)

Instructor's Comments: This is probably the 25-30 minute mark. The lecture is a bit dry but we need to be on the same page.

Handout or Document Camera or Class Exercise

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

Solution:

$$\begin{aligned}
(x^5 + x^2 + 1)(x + 1) + (x^3 + x + 1) &= x^6 + x^5 + x^3 + x^2 + x + 1 + x^3 + x + 1 \\
&= x^6 + x^5 + 2x^3 + x^2 + 2x + 2 \\
&= x^6 + x^5 + x^2
\end{aligned}$$

Example: Prove that $(ax+b)(x^2+x+1)$ over $\mathbb{R}$ is the zero polynomial if and only if $a = b = 0$.

Proof: Expanding gives

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

This is the zero polynomial if and only if $a = 0$, $a + b = 0$ and $b = 0$ which holds if and only if $a = b = 0$. ■

Instructor's Comments: This is the 40 minute mark

Theorem: (Division Algorithm for Polynomials (DAP)) Let $\mathbb{F}$ be a field. If $f(x), g(x) \in \mathbb{F}[x]$ and $g(x) \neq 0$ then there exists unique polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that

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

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

Proof: Exercise (or extra reading). ■

Note:

(i) $q(x)$ is the quotient.

(ii) $r(x)$ is the remainder.

(iii) If $r(x) = 0$, then $g(x)$ divides $f(x)$ and we write $g(x) \mid f(x)$. Otherwise, $g(x) \nmid f(x)$. In this case, we say that $g(x)$ is a factor of $f(x)$. If a polynomial has no nonconstant polynomial factor of smaller degree, we say that the polynomial is irreducible.

Instructor's Comments: Note here that we're generalizing the definition of $\mid$. This reduces to the definition we had for integers.

Example: Show over $\mathbb{R}$ that

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

Proof: By DAP, there exists $q(x)$ and $r(x)$ polynomials over $\mathbb{R}$ such that

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

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

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

giving $2 = r(1)$. Therefore, $r(x) \neq 0$ hence $(x-1) \nmid x^2 + 1$. ■

Instructor's Comments: My guess is that you will need to push this to the next lecture which is fine.

Long Division

Let's divide

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

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

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

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

$$r(z) = 2i$$