Lecture 42

Handout or Document Camera or Class Exercise

Prove that a polynomial over any field $\mathbb{F}$ of degree $n \geq 1$ has at most n roots.

Instructor's Comments: If you try this by contradiction, you will find yourself using some sort of " dot dot dot" type argument which ideally we'd like to avoid. Try to steer students to the induction solution.

Solution: Let $P(n)$ be the statement that all polynomials over $\mathbb{F}$ of degree n have at most n roots. We prove this by induction on n.

Base Case: If $n = 1$, let $ax + b \in \mathbb{F}[x]$, with $a \neq 0$. Solving for a root gives $x = -a^{-1}b$ which exists since a is a nonzero element in a field and hence has a multiplicative inverse.

Induction Hypothesis: Assume that $P(k)$ is true for some $k \in \mathbb{N}$.

Instructor's Comments: It's always a good idea to emphasize the for some statement above.

Inductive step: Let $p(x) \in \mathbb{F}[x]$ be a degree $k+1$ polynomial. Either $p(x)$ has no root in which case we are done or $p(x)$ has a root, say $c \in \mathbb{F}$. By the Factor Theorem, $x - c$ is a factor of $p(x)$. Write $p(x) = (x-c)q(x)$ for some $q(x) \in \mathbb{F}[x]$ of degree k. By the inductive hypothesis, $q(x)$ has at most k roots. Thus, $p(x)$ has at most $k+1$ roots. Therefore, by the Principle of Mathematical Induction, $P(n)$ is true for all natural numbers n. ■

Instructor's Comments: This could be the 15 minute mark

Definition: Let $\mathbb{F}$ be a field. We say a polynomial of positive degree in $\mathbb{F}[x]$ is reducible in $\mathbb{F}[x]$ if and only if it can be written as the product of two polynomials in $\mathbb{F}[x]$ of positive degree. Otherwise, we say that the polynomial is irreducible in $\mathbb{F}[x]$. For example, x^2+1 is irreducible in $\mathbb{R}[x]$ but reducible in $\mathbb{C}[x]$.
Example: Factor $f(x) = x^4-2x^3+3x^2-4x+2$ into a product of irreducible polynomials over $\mathbb{Z}_7$.

Proof: Note that $f(1) = 0$ and thus, by the Factor Theorem, $x-1$ is a factor. By long division, we have that

$$f(x) = (x-1)(x^3 - x^2 + 2x - 2)$$

Now, the sum of the coefficients of the cubic is still 0 hence $x-1$ is another factor of $f(x)$! By a second application of long division, we see that

$$f(x) = (x-1)^2(x^2+2)$$

Instructor's Comments: Emphasize to students they should do the long division.

Now, the Factor Theorem says that if x^2+2 could be factored, it must have a root since the factors must be linear. Checking the 7 possible roots gives

$$\begin{aligned}
(0)^2 + 2 &\equiv 2 \pmod 7 \\
(1)^2 + 2 &\equiv 3 \pmod 7 \\
(2)^2 + 2 &\equiv 6 \pmod 7 \\
(3)^2 + 2 &\equiv 4 \pmod 7 \\
(4)^2 + 2 &\equiv 4 \pmod 7 \\
(5)^2 + 2 &\equiv 6 \pmod 7 \\
(6)^2 + 2 &\equiv 2 \pmod 7
\end{aligned}$$

Therefore, x^2+2 has no root in $\mathbb{Z}_7$ and the above form was completely factorized. ■

Instructor's Comments: This is the 20 minute mark. You want to emphasize that even though the factor theorem shows that 1 is a root, it doesn't say with what multiplicity. Thus you need to do the long division in order to find any additional factors (or use the gcd of the polynomial and it's derivative but we won't be talking about this)

Definition: The multiplicity of a root $c \in \mathbb{F}$ of $f(x) \in \mathbb{F}[x]$ is the largest $k \in \mathbb{N}$ such that $(x-c)^k$ is a factor of $f(x)$.

Instructor's Comments: Note we can take $\mathbb{N}$ above because we require that c is a root of the polynomial.

Example: The multiplicity of 1 in the last example was 2.

Note: $x^4+2x^2+1 = (x^2+1)^2$ over $\mathbb{R}[x]$ but does not split into linear factors over $\mathbb{R}$.

Theorem: (Fundamental Theorem of Algebra (FTA)) Every non-constant complex polynomial has a complex root.

Instructor's Comments: The proof will not be done in Math 135

Note:

(i) Roots need not be distinct.

(ii) $x^2 + 1$ over $\mathbb{R}$ shows that this does not happen over all fields.

Example: Solve $x^3 - x^2 + x - 1 = 0$ over $\mathbb{C}$.

Solution: Note that $x - 1$ is a factor (sum of coefficients is 0). Thus, either do long division or note that

$$x^3 - x^2 + x - 1 = x^2(x - 1) + (x - 1) = (x - 1)(x^2 + 1) = (x - 1)(x - i)(x + i).$$

Instructor's Comments: This is the 30 minute mark

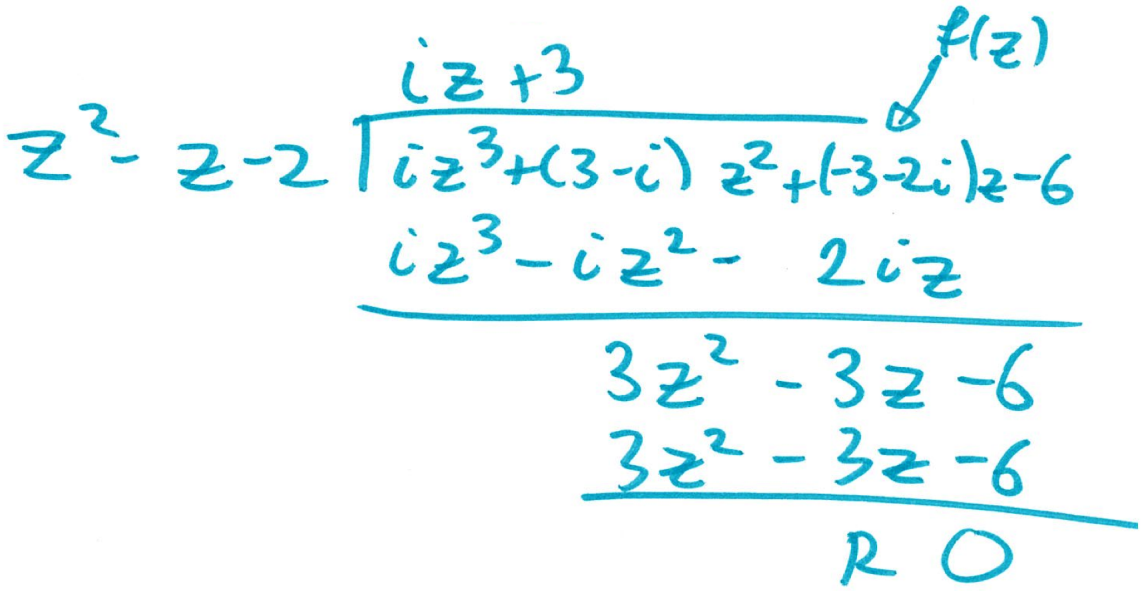
Handout or Document Camera or Class Exercise

Factor $iz^3 + (3-i)z^2 + (-3-2i)z - 6$ as a product of linear factors. Hint: There is an easy to find integer root!

Solution: By testing roots, notice that $z = -1$ and $z = 2$ are roots!

Instructor's Comments: Note that you could look at the real part of this polynomial when you plug in a real root r and get $3r^2 - 3r - 6$ which has the two roots -1 and 2.

Hence $(z+1)(z-2) = z^2 - z - 2$ is a factor. Performing the long division yields



and therefore, $f(x) = (z+1)(z-2)(iz+3)$.

Instructor's Comments: Alternatively, you could note that since the constant term of the polynomial is -6, the last linear factor must have $+3$ as its constant term and since the leading coefficient is iz^3, the leading coefficient must be i.

Instructor's Comments: This is the 40 minute mark.

Theorem: (Complex Polynomials of Degree n Have n Roots (CPN)) A complex polynomial $f(z)$ of degree $n \geq 1$ can be written as

$$f(z) = c(z - c_1)(z - c_2)...(z - c_n)$$

for some $c \in \mathbb{C}$ where $c_1, c_2, ..., c_n \in \mathbb{C}$ are the (not necessarily distinct) roots of $f(z)$.

Example: The polynomial $2z^7 + z^5 + iz + 7$ can be written as

$$2(z - z_1)(z - z_2)...(z - z_7)$$

for some roots $z_1, z_2, ..., z_7 \in \mathbb{C}$.

Note: The factorization depends on the field! For example, factoring $z^5 - z^4 - z^3 + z^2 - 2z + 2$...

(i) ... over $\mathbb{C}$, $(z - i)(z + i)(z - \sqrt{2})(z + \sqrt{2})(z - 1)$

(ii) ... over $\mathbb{R}$, $(z^2 + 1)(z - \sqrt{2})(z + \sqrt{2})(z - 1)$

(iii) ... over $\mathbb{Q}$, $(z^2 + 1)(z^2 - 2)(z - 1)$

Instructor's Comments: If you're getting close, it might be best to stop here and continue this on the next lecture.

Proof: (of CPN) We prove the given statement by induction on n.

Base Case: When $n = 1$, take $az + b \in \mathbb{C}[z]$ where $a \neq 0$ and rewrite this as $a(z - \frac{-b}{a})$.

Inductive Hypothesis: Assume all polynomials over $\mathbb{C}$ of degree k can be written in the given form for some $k \in \mathbb{N}$.

Inductive Step: Take $f(z) \in \mathbb{C}[z]$ of degree $k + 1$. By the Fundamental Theorem of Algebra and the Factor Theorem there is a factor $z - c_{k+1}$ of $f(z)$ for some $c_{k+1} \in \mathbb{C}$. Write

$$f(z) = (z - c_{k+1})g(z)$$

where $g(z)$ has degree k. By the inductive hypothesis, write

$$g(z) = c(z - c_1)...(z - c_k)$$

for $c_1, c_2, ...c_k \in \mathbb{C}$. Combine to get

$$f(z) = c\prod_{i=1}^{k+1}(z - c_i).$$

Therefore, by the Principle of Mathematical Induction, the given statement is true for all $n \in \mathbb{N}$. ■

Instructor's Comments: This is the 50 minute mark