HW 2 - 110AH

Asher Christian 006-150-286

10.10.24

1

Let $P(z) = 2 + 3z^2$. Find $\alpha \neq 0, \alpha \in \mathbb{C}$ such that $|P(i + \alpha t)| < |P(i)|$ for all sufficiently small positive $t \in \mathbb{R}$

$$\begin{aligned} P(i+\alpha t) &= 2 + 3(i+\alpha t)^2 \\ &= 2 - 3 + 6i\alpha t + 3(\alpha t)^2 \\ &= -1 + 6i\alpha t + 3(\alpha t)^2 \\ P(i) &= 2 + 3(i)^2 \\ &= 2 - 3 \\ &= -1 \end{aligned}$$

find α s.t $|P(i + \alpha t)| < 1$

$$1 < 6i\alpha t + 3(\alpha t)^2 < 2.$$

take $\alpha = -i \to P(i+\alpha t) = -1+6t-3t^2$ taking $0 < t < \frac{1}{4}$ we have $P|(i+\alpha t)| < 1$

2

1. (a) Find $P_1(x)$ and $P_2(x)$ such that $(x-2)^2 P_1(x) + (x-3)^2 P_2(x) = 1$
2. $$(x-2)^2 = x^2 - 4x + 4, (x-3)^2 = x^2 - 6x + 9.$$

$$\begin{aligned} x^2 - 6x + 9 &= (x^2 - 4x + 4)(1) + (-2x + 5) \\ (x^2 - 4x + 4) &= (-2x + 5)(-\frac{1}{2}x + \frac{3}{4}) + \frac{1}{4} \\ \frac{1}{4} &= (x-2)^2 - (-2x+5)(-\frac{1}{2}x + \frac{3}{4}) \\ &= (x-2)^2 - ((x-3)^2 - (x-2)^2)(-\frac{1}{2}x + \frac{3}{4}) \\ &= (\frac{1}{2}x - \frac{3}{4})(x-3)^2 - (\frac{1}{2}x - \frac{7}{4})(x-2)^2 \\ 1 &= (2x-3)(x-3)^2 - (2x-7)(x-2)^2 \end{aligned}$$

$P_1(x) = (2x-7), P_2(x) = (2x-3)$

3. (b) How did you know part (a) was possible without actually finding p_1, p_2?

4. $(x-2)^2$ and $(x-3)^2$ are mutually prime. Therefore their gcd is a constant and there exists a modular inverse of the smallest with respect to the larger.

3

Suppose G is a finite group and $a \in G$ is an element of order k (i.e. $a^k = e$ for $a^l \neq e$ if $1 \leq l < k$)

1. (a) Define a relation on G:
   $g_1 \sim g_2$ if $\exists m \in \mathbb{Z}, m \geq 0$ such that $g_1 a^m = g_2$.
   Prove $\sim$ is an equivalence relation

2. reflexivity take $m = k$ $g_1 a^k = g_1 e = g_1$.
   symmetry if $g_1 a^m = g_2$ then right multiply by a^{k-m} and get $g_2 a^{k-m} = g_1$
   transitivity if $g_1 a^{m_1} = g_2$ and $g_2 a^{m_2} = g_3$ then $g_1 a^{m_1 m_2} = g_3$

3. (b) Show that the equivalence classes of $\sim$ all have exactly k elements.

4. It is obvious that there are no more than k elements in an equivalence class for every element is of the form $g_i a^m$ and if $m > k$ then $a^m = a^{m-k} a^k = a^{m-k} e = a^{m-k}$ so there are at most k elements.
   Assume there are less than k elements then for some $m < k$, $g_1 a^m = g_1$ a contradiction because $a^m \neq e$ Therefore there are exactly k elements in each equivalence class

5. Deduce that $k|$ ord G

6. each element g_i has an equivalence class with k elements. Consider the set of all equivalence classes. every element of G is necessarily contained within only one equivalence class. So the total amount of elements is a multiple of k and $k|ord(G)$

4

Let $F = \mathbb{R}[x]/\sim$ where $p(x) \sim Q(x)$ means $x^2 + 2x + 6 | P - Q$.

1. (a) Show that F is a field.
   call $x^2 + 2x + 6$ $G(x)$
   Because $R[x]$ is a ring it suffices to show that every element of F that is not zero has an inverse in F
   $[P(x)] \neq [0] = \{0 + f(x)G(x)\}$ so by division algorithm

$$p(x) = f(x)G(x) + r(x).$$

with $deg(r(x)) < deg(G(x))$ and because $G(X)$ has no prime factors besides itself, all deg(1) polynomials are coprime. Thus $\exists q(x), s(x) \rightarrow G(x)s(x) + q(x)r(x) = 1$ and so $[q(x)r(x)] = [1]$ and since $[r] = [q]$, $[u(x)q(x)] = [1]$

2. (b) Show that $\exists \alpha \in F$ such that $\alpha^2 + 1 = 0$.
   The roots of $G(x)$ are
   $$x = -1 \pm \sqrt{5}i.$$
   with $i = \sqrt{-1}$. Rearranging
   $$i = \frac{x+1}{\sqrt{5}}.$$
   let $\alpha = i$ so $\alpha = \frac{x}{\sqrt{5}} + \frac{1}{\sqrt{5}}$ It suffices to show that $\alpha \sim -1$
   $$\alpha^2 = \frac{x^2}{5} + \frac{2x}{5} + \frac{1}{5}$$
   $$\alpha^2 = \frac{1}{5}G(x) - 1$$
   $$\alpha^2 - (-1) = p(x)G(x)$$
   So α^2 is congruent to -1.

3. (c) Deduce that F is really $\mathbb{C}$ in effect. (part of the problem is deciding what this means!)
   Every element of F is a polynomial in $\mathbb{R}[x]$ of degree at most 1. Taking x as a linear combination of i and a real number. We have shown that i can be written as a linear combination of x and thus both Fields contain the same elements and have the same singular extra element up to combination. Both fields can represent all of the same elements and respect the same operations. Therefore they are isomorphisms and in some sense the same.

5

Suppose F is a field and E is another field with $F \subset E$ (and F has the same operators as E, just restricted to F).

1. (a) explain how E becomes a vector space over F

2. Starting with the identity on F, 1_f and consider all $F' = \{a1_f, a \in F\}$ this includes all elemments of F.
   Proceeding inductively take any $e_i \in E, e_i \notin F'$ and all $ae_i, a \in F$ necessarily $ae_i \in F \cup \{e_i\}$
   repeat the process with the next e_{i+1} adding all previous elements to F'
   In this way repeat until all elements of E are in F'
   now E is a vector space spanned by $\{1_f, e_1, e_2, ...\}$ basis elements.

3. (b) Show that dimension of E over F is $< +\infty$. Deduce that for each $\alpha \in E, \exists P(x)$ poly with coefficients in F such that $P(\alpha) = 0$ and degree of P can be chose $\leq$ deg of E over F.

4. The dimensions of E over F are not necessarily finite. Consider $\mathbb{R}$ over $\mathbb{Q}$ There is no finite basis that spans the entire field. Consider the set $S = \{\alpha, \alpha^2, \alpha^3, ..., \alpha^k\}$, k = deg($E$ over F). S cannot be linearly independent over F because it has $k+1$ elements. Therefore there exists a polynomaial P(x) in $F[x]$ with deg($P(x)$) $\leq$ deg(E over F) such that $P(\alpha) = 0$ not all coefficients = 0

6

Prove If F_1, F_2, F_3 are fields with $F_1 \subset F_2 \subset F_3$ and F_3 finite dimensional over F_1, then dim(F_3 over F_1) = dim(F_3 over F_2) * dim(F_2 over F_1)
Consider a basis of F_3 over F_2, $B = \{b_1, b_2, ..., b_n\}$ with dimension n all $b_i \in F_3$. Additionally consider a basis of F_2 over F_1, $G = \{g_1, g_2, ..., g_k\}$ with dimension k all $g_i \in F_2$ The set spanned by any $b \in B$ is all $f_2 * b, f_2 \in F_2$ since F_2 is spanned by F_1 under G the span of b is also spanned by $\{bg_1, bg_2, ..., bg_k\}$ with k elements. This is true for all $b_i \in B, 1 \leq i \leq n$ and call each set D_i so the set that spans all of B is the concatenation of all D_i. Each D_i is also mutually independent because the b_i are all mutually independent under F_2 and since $F_1 \subset F_2$ it implies they are independent under F_1 as well. Clearly there are nk elements of the basis D and D is F_3 over F_1 thus we have proved the equality.

7

Use this idea to show $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$
Start by picking a basis for $Q(\sqrt{2})$ over $\mathbb{Q}$, $\{1, \sqrt{2}\}$. This works because $\sqrt{2}^2 = 2 \in \mathbb{Q}$ also pick a basis for $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$, $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$. Because the basis for $\mathbb{Q}(\sqrt[3]{2})$ has a higher degree, it cannot be a subset of $\mathbb{Q}(\sqrt{2})$ and so $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$

8

Show $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$ directly (Suggestion: if $(a + b\sqrt{2})^3 = 2$ then what is $(a - b\sqrt{2})^3$?

Assume $\exists a, b \in \mathbb{Q}$ s.t. $(a + b\sqrt{2})^3 = 2$,

$$\begin{aligned}
(a - b\sqrt{2})^3 &= a^3 - 3a^2b\sqrt{2} + 6ab^2 - 2b^3\sqrt{2} \\
(a + b\sqrt{2})^3 &= a^3 + 3a^2b\sqrt{2} + 6ab^2 + 2b^3\sqrt{2} \\
(a - b\sqrt{2})^3 &= 2 - 6a^2b\sqrt{2} - 4b^3\sqrt{2} \\
&= 2 - \sqrt{2}(6a^2b - 4b^3) \\
(a - b\sqrt{2})^3(a + b\sqrt{2})^3 &= 2(2 - \sqrt{2}(6a^2b - 4b^3)) \\
(a^2 - 2b^2)^3 &= 4 - \sqrt{2}(12a^2b - 4b^3) \\
\sqrt{2} &= \frac{4 - (a^2 - 2b^2)^3}{12a^2b - 4b^3}
\end{aligned}$$

This is a violation of the fact that $\sqrt{2}$ is irrational and therefore our assumption that $a + b\sqrt{2} = \sqrt[3]{2}$ is invalid.