Math 110AH Homework 2

Brendan Connelly

Wednesday, October 16, 2024

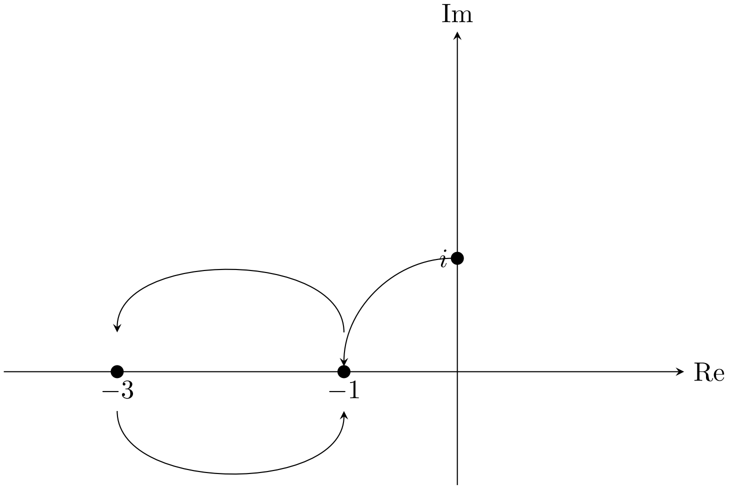
1 Intuition on Fundamental Theorem of Algebra

Let $P(z) = 2 + 3z^2$. Find $\alpha \neq 0$, $\alpha \in \mathbb{C}$ such that

$$|P(i + \alpha t)| \leq |P(i)|$$

for all sufficiently small positive $t \in \mathbb{R}$.

We want to consider the function $P(z) = 2 + 3z^2$. We can draw a picture of $P(z)$ evaluated at $z = i$.



In this situation, we can see that the magnitude of $P(z)$ would be decreasing if it started its initial rotation further down the imaginary axis. Thus, if we decrease the imaginary component of z, we will have $|P(z)| < 1$. We can clearly do this by trying to negate $|i|$. Thus, we can choose an $\alpha = -i$. Then, with sufficiently small t, $|P(i + \alpha t)| \leq |P(i)|$. This works for all $0 < t \leq \sqrt{\frac{2}{3}}$. Graphically, it is easy to see that as t grows from 0 to $\sqrt{\frac{2}{3}}$. It will slowly grow closer and closer down the axis until it reaches 0.

We can see this algebraically too. Let's suppose from the geometric interpretation and solution that ci is a zero of the polynomial where $c \in \mathbb{R}$. Then, we have that

$$\begin{aligned} 0 &= P(ci) \\ &= 2 + 3(ci)^2 \\ &= 2 - 3c^2 \\ &\implies c = \sqrt{\frac{2}{3}} \end{aligned}$$

This verifies that $P(i\sqrt{\frac{2}{3}}) = 0$ which helps demonstrate the Fundamental Theorem of Algebra and the intuition behind it.

---

2 Euclidean Algorithm

a. Find $P_1(x)$ and $P_2(x)$ such that

$$(x-2)^2 P_1(x) + (x-3)^2 P_2(x) = 1$$

where P_1 and P_2 are polynomials.

Applying the Euclidean Algorithm, we have $(x-3)^2$:

$$(x-3)^2 = x^2 - 6x + 9 = x^2 - 4x + 4 + (-2x + 5)$$

Applying it again,

$$x^2 - 4x + 4 = -\frac{x}{2}(-2x+5) - \frac{3x}{2} + 4$$

Now, let's apply the equation for $-2x+5$ and $-\frac{3x}{2}+4$:

$$-2x + 5 = \frac{4}{3}\left(-\frac{3x}{2} + 4\right) - \frac{1}{3}$$

Working backwards, we can reverse engineer to solve for P_1, P_2

$$1 = 4\left(-\frac{3x}{2} + 4\right) - 3(-2x+5)$$

Making our first substitutions:

$$1 = 4\left(x^2 - 4x + 4\right) + \frac{x}{2}(-2x+5) - 3(-2x+5)$$

Recombining:

$$1 = 4\left(x^2 - 4x + 4\right) + (2x-3)(-2x+5)$$

Substituting again:

$$1 = 4(x-2)^2 + (2x-3)\left((x-3)^2 - (x-2)^2\right)$$

Thus:

$$1 = (4 - 2x + 3)(x-2)^2 + (2x-3)(x-3)^2$$

Finally, we get:

$$1 = (-2x+7)(x-2)^2 + (2x-3)(x-3)^2$$

This means our functions are

$$P_1(x) = -2x + 7 \qquad P_2(x) = 2x - 3$$

....

b. How did you know part (a) was possible without actually finding P_1, P_2?

I knew part (a) was possible without actually finding P_1, P_2 because the $\gcd(P_1, P_2)$ is a 1 (or really any constant function). By Euclid and the results of the Euclidean Algorithm, we showed that there must exist such functions because the Euclidean algorithm is always possible, and thus we can always reverse it to find our desired solutions.

---

3 Equivalence Classes and Groups

Suppose G is a finite group and $a \in G$ is an element of order k, i.e., $a^k = e$ but $a^l \neq e$ if $1 \leq l \leq k$.
a. Define a relation on $G : g_1 \sim g_2$ if there exists a non-negative integer m such that $g_1 a^m = g_2$. Prove that $\sim$ is an equivalence relation.

We need to check reflexivity, symmetry, and transitivity.

Reflexivity
We can take $a^0 = e$. Suppose $g \in G$, we know that $ga^0 = ge = g$. Thus, $g \sim g$.

Symmetry
Suppose $g_1, g_2 \in G$ such that $g_1 \sim g_2$. By definition, this means that there exists an $m \in \mathbb{N}$ such that $g_1 a^m = g_2$. We can multiply both sides by $(a^m)^{-1} = a^{-m} = a^{k-m}$. This gives us

$$g_1 a_m (a_m)^{-1} = g_1 = g_2 a^{k-m}$$

Thus, there exists an $m' = k - m \geq 0$ such that $g_2 a^{m'} = g_1$.

Transitivity
Suppose that $x, y, z \in G$ such that $x \sim y$ and $y \sim z$. Then, we have that there exists an $m, m' \geq 0$ such that $xa^m = y$ and $ya^{m'} = z$. By substitution, we have that

$$(xa^m)a^{m'} = z$$

We can use associativity

$$x(a^m a^{m'}) = x(a^{m+m'}) = z$$

If $m + m' \geq k$, we can say that $a^{m+m'} = a^{m+m'-k}$ but this is not necessary for the definition of our given equivalence relation. In either case, we now have an $m'' = m + m'$ such that

$$xa^{m''} = z$$

This implies that $x \sim z$. Thus, our relation is transitive. We are now done and have showed the relation is an equivalence relation. □

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

The equivalences classes of an arbitrary $x \in G$ are defined to be

$$[x] = \{y \mid x \sim y\}$$

But, by how we defined our equivalence relation, this can also be described by

$$[x] = \{y \mid \exists m \in \mathbb{N} \cup \{0\} : xa^m = y\}$$

But, by the given order of a, we have that elements after a^{k-1} repeat, i.e., $a^k = a^0$, $a^{k+1} = a^1$. Thus, for any given x, the elements in its equivalence class are all of xa^i for all $0 \leq i < k$. This is k options. Thus, an arbitrary x has k elements in its equivalence class,

$$[x] = \{x, xa, xa^2, \ldots, xa^{k-1}\}$$

. . . .

c. Deduce that $k \mid \text{ord}(G)$

Equivalence classes are disjoint. Every element in G needs to belong to an equivalence class. Here is a short proof of this. Suppose $a \in [x]$ and $a \in [y]$. Then, we have that $x \sim a$ for some $x \in [x]$ and $a \sim y$ for some $y \in [y]$. Note, we did apply symmetry in our assumption. By transitivity, we have that $x \sim y$. Then, we have that $[x] = [y]$. Thus, equivalence classes are disjoint.

We also know that G is finite. That means there must exist some integer $n \in \mathbb{Z}^+$ equivalence classes. Then, we have that there are kn elements in G. Thus, since $G = kn$, we have that $k \mid \text{ord}(G)$. □

---

4 Polynomial Modular an Irreducible

Let $F = \mathbb{R}[x]/\sim$ where $P(x) \sim Q(x)$ means that $P - Q$ is divisible by $x^2 + 2x + 6$.
a. Show that F is a field.

First, we should note that $G(x) = x^2 + 2x + 6$ is irreducible over $\mathbb{R}$ and thus "prime" from the quadratic formula $b^2 - 4ac = 4 - 24 < 0 \implies$ irreducible.

Next, we should note that we already know that $\mathbb{R}[x]$ is ring. The properties of the ring would be preserved modding the equivalence relation. Thus, to show that F is a field, we just need to show that F has a multiplicative inverse.

So, let's consider an arbitrary $P(x)$. By the (repeated) application of the Euclidean Algorithm for polynomials, we can write

$$[P(x)] = [G(x) \cdot Q(x) + R(x)] = [G(x) \cdot Q(x)] + [R(x)] = [0] + [R(x)] = [R(x)]$$

for some $Q, R \in \mathbb{R}[x]$. However, it is important to note that the Euclidean Algorithm gives us that $R(x)$ has degree less than 2 and thus can be written as $R(x) = ax + b$ for some $a, b \in \mathbb{R}$. This is easy to show. Assuming this is false, $R(x)$ would have some degree 2 term. But, then we could scale $G(x)$ to cancel out the square. The same process could be applied to terms about x^2. This fact is an essential part of the idea behind this field. Thus, we only need to find inverses (below $cx + d$ will be the inverse for $R(x)$ such that

$$[ax + b] \cdot [cx + d] = [1]$$

By the definition of multiplication, we have

$$[acx^2 + x(ad + bc) + bd] = [1]$$

We need to replace acx^2 with $ac(-2x - 6)$ because they are equivalent in our modulo. Then, we have the system

$$\begin{cases} -2ac + ad + bc = 0 \\ -6ac + bd = 1 \end{cases}$$

For a, b not both zero, this system of equations will clearly have a solution. We can see this by looking at the determinant of the matrix representing the system.

$$\begin{pmatrix} -2a + b & a \\ -6a & b \end{pmatrix}$$

The determinant of this matrix is $-2ab + b^2 + 6a^2$. Basic facts of inequalities shows us that $a^2 + b^2 \geq 2ab$. Thus, this determinant will always be greater than zero unless both $a, b = 0$. This means we will always have an inverse unless $R(x) = 0$. Therefore, we have proven that $F = \mathbb{R}[x]/\sim$, which inherited the properties of a ring from $\mathbb{R}[x]$ is also a field by showing the existence of a multiplicative inverse.

b. Show that there exists an $\alpha \in F$ such that $\alpha^2 + 1 = 0$.

Let's suppose that $\alpha = ax + b \in F$ such that $\alpha^2 + 1 = 0$.

$$\begin{aligned} [(ax + b)(ax + b)] &= [(a^2x^2 + 2abx + b^2] \\ &= [a^2(-2x - 6) + 2ab + b^2] && \text{substituting using } G(x) \\ &= [(2ab - 2a^2)x + (b^2 - 6a^2)] \end{aligned}$$

Then, if we add one and equate our equation to zero(i.e., attempt to satisfy our goal), we end up with the system

$$\begin{cases} 2ab - 2a^2 = 0 \\ b^2 - 6a^2 + 1 = 0 \end{cases}$$

Factoring the first equation, we have that $a = 0$ which clearly does not work, or we have that $a = b$. Substituting into our next equation, we have that $5a^2 = 1 \implies a = b = \frac{1}{\sqrt{5}}$. Thus, we can say that

$$\alpha = \frac{1}{\sqrt{5}}(x + 1) \implies \alpha^2 + 1 = 0$$

□

c. Deduce that F is really $\mathbb{C}$ in effect. Part of the problem is deciding what that means.

We know that $\mathbb{C}$ is defined as pairs of reals with specific operations. This is isomorphic to $\mathbb{R}^2$ and to $P_1(\mathbb{R})$. And this is essentially what we have. The main difference between $\mathbb{C}$ and what was just listed–aside from those are vector spaces and not fields–is that there is a solution to $x^2 + 1 = 0$. This is important because we clearly have some form of $P_1(\mathbb{R})$ with some added structure. We have shown that F is a field like $\mathbb{C}$. It is also clear that every element in F can be written as some $d \in \mathbb{R} + \lambda\alpha$. We already established that any element in F can be written as $ax + b$. Now, if we write it in terms of $d + \lambda\alpha$, we can simply let λ scale to the coefficient of whatever element we want in F and then adjust our remaining "real" component–corresponding to a–by d. This is exactly how $\mathbb{C}$ is defined. Thus, F is essentially the same field as $\mathbb{C}$.

5 Vector Spaces

Suppose F is a field and E is another field with $F \subset E$ and F has the same operations as E, just restricted to F.
a. Explain how E becomes a vector space over F

We can treat elements in F as scalars. We can define addition as it is defined in the larger field E with any elements in E. We can define scalar multiplication as individual multiplications in E. Any element in F times an element in E will remain in E since E is a field. Any elements in E are closed under addition. All the vector space axioms from this logic. Distributivity, associativity, and commutativity all field axioms and thus our vector space satisfies these as well. The only thing left to check is the existence of identities and additive inverses. We know that $1 \in E$ satisfies the multiplicative identity. Because fields have additive inverses, the vector space would as well. Thus, E can become a vector space over F.

b. Suppose that the dimension of E over F is finite. Deduce that for each $\alpha \in E$, there exists a polynomial $P(x)$ with coefficients in F such that $P(\alpha) = 0$ and degree of P can be chosen to be less than or equal to the dimension of E over F.

Assuming that the dimension of E over F is finite, we can suppose that the dimension is n.

In order to construct our polynomial, let's consider $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$. All of the elements in this set must be in E. But also, because the dimension is n, there must exist a non-trivial dependence relation for a power of α by some collection of the other terms. This is a consequence of the Replacement Theorem. In symbols, we have that there exists $b_o, b_1, \ldots, b_n \in F$ such that

$$b_0 + b_1\alpha + b_2\alpha^2 + \ldots + b_n\alpha^n = 0$$

Because this set has $n + 1$ elements, we know that they are linearly dependent and $b_i \neq 0$ for some i. Thus, we have that there exists a nontrivial polynomial $P(x)$ with coefficients in F–which correspond to the scalars in our dependence relation such that

$$P(x) = b_0 + b_1x + b_2x^2 + \ldots + b_nx^n$$

Our work has thus shown that

$$P(\alpha) = 0$$

□

6 Dimensions of Vector Spaces

Prove that if F_1, F_2, F_3 are fields with $F_1 \subset F_2 \subset F_3$ and F_3 is finite dimensional over F_1, then

$$\dim(F_3 \text{ over } F_1) = \dim(F_3 \text{ over } F_2) \cdot \dim(F_2 \text{ over } F_1)$$

Suppose that $\dim(F_3 \text{ over } F_2) = n$ and that $\dim(F_2 \text{ over } F_1) = m$. We can choose bases β, γ for the two vector spaces respectively

$$\beta = \{v_1, v_2, \ldots, v_n\} \qquad \text{and} \qquad \gamma = \{w_1, w_2, \ldots, w_m\}$$

Suppose that $x \in F_3$. We then have that

$$x = \sum_{i=1}^{n} a_i v_i$$

for scalars $a_i \in F_2$. But, we can use our knowledge of the middle field as a vector space over the smallest field to rewrite each of these scalars. For each a_i, we have that

$$a_i = \sum_{j=1}^{m} b_j w_j$$

for elements $b_j \in F_1$. Substituting, we have

$$x = \sum_{i=1}^{n} (\sum_{j=1}^{m} b_{ij} w_j) v_i$$

Thus, let's claim that $\delta = \{v_i w_j \mid 1 \leq i \leq n \text{ and } 1 \leq j \leq m\}$ is a basis for our vector space F_3 over F_1. From above, we clearly have that δ generates F_3 because we found a linear combination that corresponds with every vector. We only need to show linear independence. If we consider this same expression and set it equal to the zero vector, we have

$$\sum_{i=1}^{n} (\sum_{j=1}^{m} b_{ij} w_j) v_i = \vec{0}$$

By the linear independence of β, we know that each of the $a_i = \vec{0}$, which means that we have that for each of $\sum_{j=1}^{m} b_{ij} w_j$, we have that

$$\sum_{j=1}^{m} b_{ij} w_j = \vec{0}$$

But, we already know that γ is linearly independent. Thus, each b_{ij} must be zero for all $i \leq n$ and $1 \leq j \leq m$. This implies that δ is linearly independent. We have shown that δ spans F_3 by construction, and now we have shown it is linearly independent. Thus, the dimension of F_3 over F_1 is clearly n times m, the number of basis vectors in δ. Thus, we have shown that for arbitrary fields such that $F_1 \subset F_2 \subset F_3$ and F_3 is finite dimensional over F_1, then

$$\dim(F_3 \text{ over } F_1) = \dim(F_3 \text{ over } F_2) \cdot \dim(F_2 \text{ over } F_1)$$

□

7 Showing an Element is not in $\mathbb{Q}(\sqrt{2})$

Use these ideas to show that $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$

Consider the field extension, $\mathbb{Q}(\sqrt[3]{2})$. If $\sqrt[3]{2} \in \mathbb{Q}(\sqrt{2})$, then we must have that $\mathbb{Q}(\sqrt[3]{2}) \in \mathbb{Q}(\sqrt{2})$. However, from our discussion above, we can leverage the fact that the dimension of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is three and the dimension of $\mathbb{Q}(\sqrt{2})$ is two. We just need to show that $\mathbb{Q}(\sqrt[3]{2})$ is a field. Like above, this inherits a ring structure from its definition. We need to show that division is well-defined, i.e., that all elements have multiplicative inverses. We should know this is true because this is simply $\mathbb{Q}[x]/(x^3 - 2)$. We also know that $x^3 - 2$ is irreducible over $\mathbb{Q}$ and thus this will produce a field. However, we should show that the polynomial structure of $\mathbb{Q}[x]$–which gives it a commutative ring structure–does indeed endow it with multiplicative inverses. We thus want to show for arbitrary $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ where $a, b, c \in \mathbb{Q}$, we have that

$$\frac{1}{a + b\sqrt[3]{2} + c\sqrt[3]{4}} = A + B\sqrt[3]{2} + C\sqrt[3]{4}$$

This is equal to

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4}) \cdot (A + B\sqrt[3]{2} + C\sqrt[3]{4}) \equiv 1 \mod (x^3 - 2)$$

Because $x^3 - 2$ is irreducible over $\mathbb{Q}$, we have by the Euclidean Algorithm that such an $A + B\sqrt[3]{2} + C\sqrt[3]{4}$ exists since the $\gcd(a + bx + cx^2, x^3 - 2)$. Thus, the multiplicative inverse exists.

Now, we can apply our previous ideas. If $\sqrt[3]{2}$ was in $\mathbb{Q}(\sqrt{2})$, then we would have that $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt{2})$. But because the dimension of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is three and the dimension of $\mathbb{Q}(\sqrt{2})$ is two, we have a contradiction. More precisely, $\mathbb{Q}(\sqrt{2})$ would have to equal $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}))$ which would then have dimension six which is yet again a contradiction. Thus, we have shown that $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$. □

8 Direct Proof that an Element is not in $\mathbb{Q}(\sqrt{2})$

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

If we suppose that $\sqrt[3]{2} \in \mathbb{Q}(\sqrt{2})$, we have that $(a + b\sqrt{2})^3 = 2$ for some $a, b \in \mathbb{Q}$. Now, lets expand.

$$2 = (a + b\sqrt{2})^3 = a^3 + 3a^2b\sqrt{2} + 6ab^2 + 2b^3\sqrt{2}$$

Because $a, b \in \mathbb{Q}$, we have that

$$a^3 + 6ab^2 = 2 \qquad 3a^2b + 2b^3 = 0$$

If we consider that second equation, we have that $b(3a^2 + 2b^2) = 0$. One solution is clearly that $b = 0$. If $b = 0$, we have that $a^3 = 2$ for some rational number a. We know that this does not have a rational solution. Thus, $b = 0$ is impossible. We can also consider $3a^2 + 2b^2 = 0$, we have that $\frac{a^2}{b^2} = \frac{-2}{3}$. However, this is also a contradiction because the left hand side must be positive and the right hand side is negative. Therefore, we cannot have $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2})$. $(a + b\sqrt{2})^3 = 2 = (a - b\sqrt{2})^3$ which does not work and is thus a contradiction. Briefly, it is worth noting we can see this even more clearly when we add these expanded equations together and have that $a^3 + 6ab^2 = 2$. When $b = 0$, this clearly will not have a solution for $a \in \mathbb{Q}$. In either case, we are done.

□