Comprehensive Preparation

Carmen A. Bruni

August 22, 2010

This document was used as a prepatory for the UBC comprehensive examination. Many of these questions were taken from previous comprehensives. A huge thank you to Vince Chan and Faisal al-Faisal for both their help with the problems as well as spotting my typos and mistakes. Please feel free to email comments, suggestions, as well as new problems to cbruni@alumni.uwaterloo.ca.

1 Real Analysis

1.1 Single Variable Calculus

Theorem 1.1. *(Intermediate Value Theorem) Let $f : [a, b] \to \mathbb{R}$ be a continuous function and suppose that $f(a) < x < f(b)$. Then there exists a $c \in [a, b]$ such that $f(c) = x$.*

Theorem 1.2. *(Extreme Value Theorem) Let $f : [a, b] \to \mathbb{R}$ be a continuous function. Then there exists a $c, d \in [a, b]$ such that $f(c) \le f(x) \le f(d)$ for all $x \in [a, b]$.*

Theorem 1.3. *(Mean Value Theorem) Let $f : [a, b] \to \mathbb{R}$ be a continuous function and suppose that f is differentiable on the open interval (a, b). Then there exists a $c \in (a, b)$ such that*

$$\frac{f(b) - f(a)}{b - a} = f'(c)$$

1. Prove that the product of two uniformly continuous real valued functions on $(0, 1)$ is also uniformly continuous on $(0, 1)$.

   Solution: First a lemma

   Lemma 1.4. *If f is a uniformly continuous function on a bounded set $A \subseteq \mathbb{R}$. Show that $f(A)$ is bounded.*

   Proof. Let $\epsilon > 0$. Then there exists a $\delta > 0$ such that for all $x, y \in A$ satisfying $|x - y| < \delta$, then $|f(x) - f(y)| < \epsilon$. Notice that we can cover A with finitely many balls of radius δ and centres $x_1, .., x_n$. The diameter of each of these balls is 2ϵ (maximum variation of two points in the ball) and so in particular, the maximum variation from any two balls is at worst $2n\epsilon$, a finite number. Hence $f(A)$ is bounded. ■

   Let f and g be two uniformly continuous functions and let $\epsilon > 0$. By the lemma, we have that both f and g are bounded say by M and N respectfully. Then there exists a $\delta_f > 0$ such that for all $x, y \in (0, 1)$ with $|x - y| < \delta_f$, then $|f(x) - f(y)| < \frac{\epsilon}{2N}$. Similarly, there exists a δ_g such that for all $x, y \in (0, 1)$ with $|x - y| < \delta_f$, then $|g(x) - g(y)| < \frac{\epsilon}{2M}$. Let $\delta = \min\{\delta_f, \delta_g\}$. Then for all $x, y \in (0, 1)$ with $|x - y| < \delta$, we have

$$\begin{aligned} |f(x)g(x) - f(y)g(y)| &= |f(x)g(x) - f(x)g(y) + f(x)g(y) - f(y)g(y)| \\ &\le |f(x)g(x) - f(x)g(y)| + |f(x)g(y) - f(y)g(y)| \\ &\le |f(x)||g(x) - g(y)| + |g(y)||f(x) - f(y)| \\ &< M\frac{\epsilon}{2M} + N\frac{\epsilon}{2N} = \epsilon \end{aligned}$$

This is precisely the condition that fg is uniformly continuous as required. ■

2. Let $f(x)$ be a continuous and integrable function on $[0, \infty)$. Show that if f is uniformly continuous on $[0, \infty)$ then

$$\lim_{t \to \infty} f(t) = 0$$

3. Let F be a real valued function on $[0, 1]$ having the following property: for any real y, the equation $f(x) - y = 0$ has either no roots, or exactly two roots. Prove that f is not continuous.

Solution: First note f is not a constant function. Assume towards a contradiction that f is continuous. Then the Extreme Value Theorem (1.2) tells us that there exists an a such that $f(a) = \sup_{x \in [0,1]} f(x)$. The conditions on the problem give us a $b \in [0, 1]$ such that $f(b) = f(a)$. Without loss of generality assume $a < b$. Note that by the Intermediate Value Theorem (1.1) there is a point $f(a) - \epsilon$ for some $\epsilon > 0$ such that there are values $c, d \in [0, 1]$ with $a < c < d < b$ and $f(c) = f(a) - \epsilon = f(d)$. Moreover, if $b \neq 1$, then since b is a maximum point, we know that we can find an epsilon small enough so that there is an $e > b$ such that $f(e) = f(c) = f(d)$, a contradiction. So $b = 1$. Similarly in the opposite direction, we can find a $e < a$ with $f(e) = f(c) = f(d)$ for a sufficiently small ϵ provided $a \neq 0$. So indeed $a = 0$. Repeating this argument with $-f(x)$, we see that both the minima must be at 0 and 1. This implies that the minima and the maxima are equal and hence f is constant, a contradiction. Thus, f is not continuous as required. ■

4. Let x_n be a sequence satisfying $x_0 = c$, $x_1 = 1 - c$ and $x_{n+2} = \frac{5}{2}x_{n+1} - \frac{3}{2}x_n$ where $c \in \mathbb{R}$. Fpr what values does x_n converge and what is the value of the limit in these cases.

Solution: We devise a recurrence relation for this polynomial. The associated characteristic polynomial is $x^2 - \frac{5}{2}x + \frac{3}{2} = (x - \frac{3}{2})(x - 1)$. This gives rise to the recurrence relation $x_n = A(\frac{3}{2})^n + B(1)^n$. Solving using the initial conditions gives

$$\begin{aligned} c &= A + B \\ 1 - c &= \frac{3}{2}A + B \end{aligned}$$

yielding $A = 2 - 4c$ and $B = 5c - 2$. Thus, $x_n = (2 - 4c)(\frac{3}{2})^n + (5c - 2)$. Notice that if $2 - 4c \neq 0$ then this limit cannot exist as $1 < \frac{3}{2}$ so the power will not converge. Thus, the seqence only converges when $c = \frac{1}{2}$ in which case $x_n = \frac{1}{2}$ for all $n \in \mathbb{N}$ and hence the limit is $\frac{1}{2}$. ■

5. Let f be a continuous function from $[0, 1]$ to $\mathbb{R}$. Show that there is a $c \in [0, 1]$ such that

$$\int_0^1 f(x)x^2 = \frac{1}{3}f(c)$$

Solution: Since f is a continuous real function from $[0, 1]$, we have by the Extreme Value Theorem (1.2) that

$$\min_{x \in [0,1]} f(x) =: m \leq= M := \max_{x \in [0,1]} f(x)$$

Also by the Extreme Value Theorem (1.2), there exist an $a, b \in [0, 1]$ such that $f(a) = m$ and $f(b) = M$. Hence,

$$\begin{aligned} \frac{f(a)}{3} = \frac{m}{3} \leq \int_0^1 mx^2 \int_0^1 f(x)x^2 \leq \int_0^1 Mx^2 = \frac{M}{3} = \frac{f(b)}{3} \\ \Rightarrow f(a) \leq 3\int_0^1 f(x)f^2 \leq f(b) \end{aligned}$$

Now, since $f(x)$ is continuous, we know that every value from $f(a)$ to $f(b)$ is attained for some value of x by the Intermediate Value Theorem (1.1). Hence, we can invoke the intermediate value theorem to get a value $c \in [0, 1]$ such that

$$f(c) = 3\int_0^1 f(x)x^2$$

giving the desired conclusion. ■

6. (i) Show that a continuous function on $\mathbb{R}$ cannot take every real value exactly twice.
   (ii) Find a continuous function on $\mathbb{R}$ that takes every real value exactly three times.

Solution:

(i) Suppose that such a function exists, say f. Consider the two points $x < y$ where $f(x) = f(y) = 0$. By the Extreme Value Theorem (1.2) there is a point $x < a < y$ where f takes on a non-zero maximum (or a minimum but without loss of generality we'll say maximum). If the function reaches its maximum value twice between x and y, say at b, then there is at least one point in an epsilon ball around a and b that is achieved 4 times, a contradiction. So without loss of generality, the maximum is reached only once. Notice that for all $w < x$ and all $y < z$, the functions is either always positive or always negative. The function cannot be both negative in both directions as then the maximum isn't achieved twice a contradiction. But notice that there is an epsilon and delta ball around x and y where $f(x + \epsilon) = f(y - \delta)$. Hence, if the function goes positive again, we have another contradiction as some point is reached three times. This means that f cannot exist as required. On a side note, it might be best to draw out this picture to see everything clearly (I will omit this from this file...). ■

(ii) One example is a seesaw function. The general shape is as follows. Draw a line from the origin to $(\frac{1}{2}, 1)$ then draw a line from this point to $(1, \frac{1}{2})$. Take this shape and repeat starting at $(1, \frac{1}{2})$. Continue the shape in the negative direction as well. This function visually is very easy to see it satisfies the requirements. ■

7. Let f be a continuous function over $\mathbb{R}$ and suppose that $|f(x) - f(y)| \geq |x - y|$ for all $x, y \in \mathbb{R}$. Show that $\mathrm{Ran}\,(f) = \mathbb{R}$.

Solution: Notice first that this function is clearly one to one for if $f(x) = f(y)$ then $0 = |f(x) - f(y)| \geq |x - y|$ and so $x = y$. This implies that the map f takes open sets to open sets. Now let y_n be a sequence in $\mathrm{Ran}\,(f)$ that converges to a point y. I claim that $y \in \mathrm{Ran}\,(f)$. Let $\epsilon > 0$. Notice that since $y_i \in \mathrm{Ran}\,(f)$, we have that $y_i = f(x_i)$. Moreover, as y_n is convergent, it must be Cauchy and so there exists an N such that for all $n, m > N$, we have

$$|y_n - y_m| < \epsilon$$

Combining this with the given fact yields

$$|x_n - x_m| \leq |f(x_n) - f(x_m)| = |y_n - y_m| < \epsilon$$

and so x_n is Cauchy and hence convergent as $\mathbb{R}$ is complete. Now, let x be the limit of the x_n. Then by continity,

$$y = \lim_{n\to\infty} y_n = \lim_{n\to\infty} f(x_n) = f(\lim_{n\to\infty} x_n) = f(x)$$

and thus $y \in \mathrm{Ran}\,(f)$ showing $\mathrm{Ran}\,(f)$ is closed. Hence $\mathrm{Ran}\,(f)$ is clopen and thus (as it is non-empty) must be all of $\mathbb{R}$ as required. ■

8. Suppose f is a differentiable real valued function such that $f'(x) > f(x)$ for all $x \in \mathbb{R}$ and $f(0) = 0$. Prove that $f(x) > 0$ for all positive x.

   Solution: Notice that $f'(0) > f(0) = 0$ ans so f is increasing in a neighbourhood around the origin. Hence, $f(x) > 0$ for all $x \in (0, \epsilon)$ for some $\epsilon > 0$. Now suppose that there exists a point x_0 such that $f(x_0) \leq 0$. Let $c := \inf\{x | f(x) \leq 0\}$. By the above, we know that $c > 0$ and $f(c) = 0$. By the mean value theorem, we have that

$$\frac{f(c) - f(0)}{c - 0} = f'(d)$$

   for some $d \in (0, c)$. This implies that $f'(d) = 0$. the inequality given in the question gives $f(d) < f'(d) = 0$ contradicting the definition of c. hence $f(x) > 0$ for all $x \in \mathbb{R}^+$. ∎

9. Let $x_0 = 0$ and $x_{n+1} = \frac{1}{2+x_n}$ for all $n \in \mathbb{N}$. Prove that the limit exists and find its value.

   Solution: This is a straightforward odd terms increase and even terms decrease (or vice versa) problem. Use the Monotone Convergence Theorem and you're home free.

1.2 Multivariable Calculus

Definition 1.5. Let $f : \mathbb{R}^n \to \mathbb{R}$ and suppose that $\mathbf{u}$ is a unit vector. Then the directional derivative is

$$\nabla_{\mathbf{u}} f(\mathbf{x}) = \lim_{h \to 0^+} \frac{f(\mathbf{x} + h\mathbf{u}) - f(\mathbf{x})}{h}$$

Definition 1.6. Let $f : \mathbb{R}^n \to \mathbb{R}^m$. Then we say that f is differentiable if there exists a linear map $J : \mathbb{R}^n \to \mathbb{R}^m$ such that the following limit exists

$$\lim_{h \to 0} \frac{f(x + h) - f(x) - J(h)}{||h||} = 0$$

when it is differentiable, the Jacobian is the map used for J (in which case $J(h)$ function like Jh - for whatever reason I always see the Jacobian as a matrix).

1. Find the shortest distance from the line $x + y = 4$ to the elipse

$$\frac{x^2}{4} + y^2 = 1$$

   Solution: 1 I will present two solutions to this problem. One will be shorter but require memory and the second solution will be easier to remember. To solve this problem we wish to minimize the distance function (formula for the distance from a point to a line)

$$f(x, y) := \frac{|x + y - 4|}{\sqrt{1^2 + 1^2}}$$

   subject to the constraint that x and y satisfy

$$g(x, y) := \frac{x^2}{4} + y^2 = 1$$

   So we proceed by Lagrange Multipliers. We solve $\nabla f = \lambda \nabla g$. This gives

$$\pm \frac{1}{\sqrt{2}}(1, 1) = \lambda(\frac{x}{2}, 2y)$$

The $\pm$ comes since our distance function has an absolute value so technically we don't know which sign to use. Solving coordinate wise gives the equations

$$\lambda x = \pm\sqrt{2} \qquad\qquad \lambda y = \pm\frac{1}{2\sqrt{2}}$$

The first says that neither x nor λ are 0. Hence $\lambda = \pm\frac{\sqrt{2}}{x}$. Plugging this into the second equation yields

$$\pm\frac{\sqrt{2}}{x}y = \pm\frac{1}{2\sqrt{2}} \Rightarrow \frac{x}{4} = y$$

Plugging into the equation for the ellipse gives

$$\frac{x^2}{4} + y^2 = 1 \Rightarrow y^2 = \frac{1}{5}$$

So we have that $y = \pm\frac{\sqrt{5}}{5}$ giving $x = \pm\frac{4\sqrt{5}}{5}$. Plugging into the distance function gives

$$d = \frac{|\pm\frac{4\sqrt{5}}{5} + \pm\frac{\sqrt{5}}{5} - 4|}{\sqrt{2}} = \frac{|\pm\sqrt{5} - 4|}{\sqrt{2}}$$

This is minimized when we take the positive and so,

$$d = \frac{4 - \sqrt{5}}{\sqrt{2}}$$

This is the required distance. ■

Solution: 2 For our second solution, we won't need the formula for the distance form a point to a line. We will encode this in the Lagrange Multipliers. As an aside this idea was inspired to me by Vince Chan when he jokingly mentioned that students in his SOS sessions had to compute the minimal distance from a hyperboloid to a paraboloid. It was then that I realized that hyperboloid and epllipse and paraboloid and line were not that far apart.

This time we wish to minimize the distance function

$$F(x, y, z, w) = \sqrt{(x - w)^2 + (y - z)^2}$$

subject to the constraints

$$g(x, y, z, w) := \frac{x^2}{4} + y^2 = 1$$
$$h(x, y, z, w) := w + z = 4$$

For simplicity, we will minimize $f(x, y, z, w) = F(x, y, z, w)^2$ as its gradient will be far easier to compute. So the idea here is to minimize the distance between two points subject to the conditions that the points lie on the ellipse and line respectfully. Our Lagrange Multiplier method gives the equation

$$\nabla f = \lambda\nabla g + \mu\nabla h$$
$$(2(x - w), 2(y - z), -2(y - z), -2(x - w)) = \lambda(\frac{x}{2}, 2y, 0, 0) + \mu(0, 0, 1, 1)$$

Equating coordinates yields

$$2(x - w) = \lambda\frac{x}{2} \qquad\qquad 2(y - z) = 2y\lambda$$
$$-2(y - z) = \mu \qquad\qquad -2(x - w) = \mu$$

Isolating the top row yields

$$(1-\frac{\lambda}{4})x = w \qquad\qquad (1-\lambda)y = z \tag{1}$$

Substituting into the second row yields

$$-2\lambda y = \mu \qquad\qquad -\frac{x}{2}\lambda = \mu$$

Substituting yields $4y = x$ or $\lambda = \mu = 0$. Assuming the second condition is true, we have that $x = w$ and $y = z$ hence $x + y = 4$ and $\frac{x^2}{4} + y^2 = 1$. Substituting yields $5x^2 - 32x + 127 = 0$ which has no real roots. So it must be that $4y = x$ substituting into the equation of the ellipse yields $5y^2 = 1$ or $y = \pm\frac{\sqrt{5}}{5}$. Next, summing the equations in (1) and noting that $z + w = 4$ yields

$$4 = z + w = (5 - 2\lambda)y \quad \Rightarrow \quad \lambda = \frac{5 \mp 4\sqrt{5}}{2}$$

Now we have solved enough variable to finish the problem. Notice that we are trying to minimize f. This function at the point in question becomes

$$\begin{aligned} f(x,y,z,w) &= (x-w)^2 + (y-z)^2 = (\frac{x}{2}\lambda)^2 + (\lambda y)^2 \\ &= \frac{\lambda^2}{4}(\frac{x^2}{4} + y^2 + 3y^2) = \frac{\lambda^2}{4}(1 + 3(\frac{1}{5})) = \frac{\lambda^2}{4}(\frac{8}{5}) = \lambda^2(\frac{2}{5}) \end{aligned}$$

We actually want the square root of this function and thus, our distance becomes

$$d = |\lambda|\sqrt{\frac{2}{5}} = \frac{|\sqrt{5} \mp 4|}{\sqrt{2}} = \frac{4 - \sqrt{5}}{\sqrt{2}}$$

when we take the smaller of the two answers. ■

2. Let $a, b, c, d > 0$ be real numbers. Find conditions on a, b, c, d such that the following limit exists.

$$\lim_{(x,y)\to(0,0)} \frac{|x|^a|y|^b}{|x|^c + |y|^d}$$

Solution: First lets note if the limit exists it must be 0. To see this consider the limit on the line $y = 0$. Then

$$\lim_{(x,0)\to(0,0)} \frac{0}{|x|^c} = 0$$

so if it exists, it better be 0. Now, consider

$$\frac{|x|^a|y|^b}{|x|^c + |y|^d} = \frac{(|x|^c)^{\frac{a}{c}}(|y|^d)^{\frac{b}{d}}}{|x|^c + |y|^d} \le \frac{(|x|^c + |y|^d)^{\frac{a}{c}}(|x|^c + |y|^d)^{\frac{b}{d}}}{|x|^c + |y|^d} = (|x|^c + |y|^d)^{\frac{a}{c} + \frac{b}{d} - 1}$$

and this converges to 0 if and only if the numerator is greater than 0 which occurs whenever $\frac{a}{c} + \frac{b}{d} > 1$. ■

3. Suppose that $f : \mathbb{R}^2 \to \mathbb{R}$ has a directional derivative in all directions at the origin. Prove that f is not necessairly differentiable at the origin.

Solution: Consider the following function

$$f(x,y) := \begin{cases} \frac{y^3}{x^2+y^2} & \text{if } (x,y) \neq (0,0) \\ 0 & \text{if } (x,y) = (0,0) \end{cases}$$

I will actually show a bit more and show that all the partial derivatives exist as well. Let $u = (a, b)$ be a unit vector. By definition, we need to show that the following limit exists

$$\begin{aligned}\nabla_u f(x,y) &= \lim_{h\to 0^+} \frac{f(0+ha, 0+hb) - f(0,0)}{h} = \lim_{h\to 0^+} \frac{\frac{(0+hb)^3}{(0+ah)^2+(0+hb)^2} - 0}{h} \\ &= \lim_{h\to 0^+} \frac{\frac{h^3b^3}{a^2h^2+h^2b^2}}{h} \\ &= \frac{b^3}{a^2+b^2}\end{aligned}$$

and thus the directional derivatives exist in all directions at the origin. Partials clearly exists everywhere not at the origin and at the origin, we have

$$\begin{aligned}\frac{\partial f}{\partial x}(0,0) &= \lim_{h\to 0} \frac{f(0+h,0) - f(0,0)}{h} = 0 \\ \frac{\partial f}{\partial y}(0,0) &= \lim_{h\to 0} \frac{f(0,0+h) - f(0,0)}{h} = \lim_{h\to 0} \frac{h^3}{h^3} = 1\end{aligned}$$

So the partials exist everywhere as well. Also note that this function is continuous. Now, I claim the function itself is not differentiable. I show that the following limit does not exist.

$$\begin{aligned}\lim_{(h,k)\to(0,0)} \frac{f(0+h,k+0) - f(0,0) - (0,1)(h,k)^T}{||(h,k)^T||} &= \lim_{(h,k)\to(0,0)} \frac{\frac{k^3}{h^2+k^2} - 0 - k}{\sqrt{h^2+k^2}} \\ &= \lim_{(h,k)\to(0,0)} \frac{-h^2k}{\sqrt{h^2+k^2}^3}\end{aligned}$$

To show this limit does not exist, we approach it from multiple lines. Suppose $k = mh$. Then, along these lines, our limit is

$$\lim_{h\to 0} \frac{-mh^3}{\sqrt{h^2+h^2m^2}^3} = \lim_{h\to 0} \frac{-m}{\sqrt{1+m^2}}$$

This depends on m and hence we get different values as we approach different lines. Thus, the limit cannot exist and hence this function is not differentiable. ■

4. Let $Q := \{0 < x < 1, 0 < y < 1\}$. For what values of a and b is the following integral bounded on Q

$$x^a y^b \int_0^\infty \frac{1}{(x+t)(y^2+t^2)} dt$$

Solution: We evaluate the integral directly. We proceed by partial fractions.

5. Let $f : [0,1] \times [0,1] \to \mathbb{R}$ be a continuous function. Define $F(t) := \int_0^t f(s,t)ds$. Prove that F is continuous on $[0,1]$

6. Find the critical points of $f(x,y) = x^2 + 2xy + 2y^2 - \frac{1}{2}y^4$ and classify each one as a local minimum, local maximum, or a saddle point.

Solution: We compute the partials, set the first partials to 0, then compute the Hessian and evaluate. Notice that

$$\begin{aligned} f_x &= 2x + 2y & f_y &= 2x + 4y - 2y^3 \\ f_{xx} &= 2 & f_{yy} &= 4 - 6y^2 \\ f_{xy} &= 2 & f_{yx} &= 2 \end{aligned}$$

Setting $f_x = 0$ gives $x = -y$. Into the second yields $y - y^3 = 0$ giving $y = 0, 1, -1$ as solutions. These give points $p_1 := (0,0), p_2 := (1,-1), p_3 := (-1,1)$ as our critical points. Our Hessian is

$$\Delta = \det \begin{bmatrix} f_{xx} & f_{xy} \\ f_{yx} & f_{yy} \end{bmatrix} = \det \begin{bmatrix} 2 & 2 \\ 2 & 4 - 6y^2 \end{bmatrix} = 2(4 - 6y^2) - 4 = 4 - 12y^2$$

Now, for a critical point p, we have the following possibilities,

(i) If $\Delta > 0$ and $f_{xx}(p) < 0$ then f attains a local maximum at p.

(ii) If $\Delta > 0$ and $f_{xx}(p) > 0$ then f attains a local minimum at p.

(iii) If $\Delta < 0$, then f has a saddle point at p

(iv) If $\Delta = 0$, then no conclusion can be drawn.

Since I can never remember these rules, I made a quick little poem to remember this.

When $\Delta > 0$ something can there be
When $\Delta < 0$, nothing can you see
In first when first is < 0
Then the point is big - a hero

Okay so in our case, $\Delta(p_1) = 8 - 4 = 4$ so its positive and $f_{xx} = 2$ so this is a local minimum. The other points yield $\Delta(p_2) = \Delta(p_3) = -8$ in this case the Hessian is negative and so we have two saddle points here. ■

1.3 Stokes Theorem

Theorem 1.7. *(Stokes' Theorem) Let S be an oriented, piecewise smooth surface bounded by a simple closed piecewise smooth curve C with positive orientation. Let F be a vector field whose components have continuous partial derivatives on an open region in $\mathbb{R}^3$ that contain S. Then*

$$\oint_C F \cdot dr = \int\int_S \mathrm{curl} F \cdot dS = \int\int_S \nabla \times F \cdot n dS$$

where n is normal to the surface in question and

$$\nabla = \boldsymbol{i}\frac{\partial}{\partial x} + \boldsymbol{j}\frac{\partial}{\partial y} + \boldsymbol{k}\frac{\partial}{\partial z}$$

and thinking of the formal cross product, where $F = P\boldsymbol{i} + Q\boldsymbol{j} + R\boldsymbol{k}$, we see

$$\begin{aligned} \mathrm{curl} F = \nabla \times F &= \begin{vmatrix} \boldsymbol{i} & \boldsymbol{j} & \boldsymbol{k} \\ \frac{\partial}{\partial x} & \frac{\partial}{\partial y} & \frac{\partial}{\partial z} \\ P & Q & R \end{vmatrix} \\ &= \left(\left(\frac{\partial R}{\partial y} - \frac{\partial Q}{\partial z} \right) \boldsymbol{i} + \left(\frac{\partial P}{\partial z} - \frac{\partial R}{\partial x} \right) \boldsymbol{j} + \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y} \right) \boldsymbol{k} \right) \end{aligned}$$

1. Consider $F(x,y,z) = (yz + x^4)\mathbf{i} + (x(1+z) + e^y)\mathbf{j} + (xy + \sin(z))\mathbf{k}$. Let C be a circle of radius R lying in the plane $2x + y + 3z = 6$. What are the possible values of the line integral $\int_C F \cdot dr$?

2. Consider the vector field

$$F(x,y,z) = \frac{x\mathbf{i} + y\mathbf{j} + z\mathbf{k}}{(x^2 + y^2 + z^2)^{\frac{3}{2}}}$$

(i) Verify that $\nabla \cdot F = 0$ on $\mathbb{R}^3 \backslash \{0\}$

(ii) Let S be a sphere centred at the origin with outward orientation. Show that

$$\int\int_S F \cdot dS = 4\pi$$

(iii) Now, let $E \subseteq \mathbb{R}^3$ be an open region with smooth boundary S with outward orientation. Further, suppose $0 \in E$. Show that the above integral has the same value.

3. Evaluate $\int_C u \cdot dr$ where C is the unit circle centred at the origin and directed in an anticlockwise sense with $u = (\cos(x), 2x + y\sin(y), x)$.

Solution: Let $S = \{(x, y, z)|x^2 + y^2 + z^2 \leq 1, z = 0\}$ and notice that C is the boundary of this surface. Using Stokes' theorem (1.7), we have

$$\begin{aligned}
\int_C u \cdot dr &= \int\int_S \left(\left(\frac{\partial R}{\partial y} - \frac{\partial Q}{\partial z}\right)\mathbf{i} + \left(\frac{\partial P}{\partial z} - \frac{\partial R}{\partial x}\right)\mathbf{j} + \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}\right)\mathbf{k}\right) \cdot ndS \\
&= \int\int_S ((0-0)\,\mathbf{i} + (0-1)\,\mathbf{j} + (2-0)\,\mathbf{k}) \cdot ndS \\
&= \int\int_S (-\mathbf{j} + 2\mathbf{k}) \cdot ndS
\end{aligned}$$

To compute ndS we use the following

$$ndS = \pm(-f_x, -f_y, 1)dxdy$$

where $z = f(x, y) = 0$ which is the curve in question. Using the positive sign gives a positive $\mathbf{k}$ component. This leads to $ndS = (0, 0, 1)$. Combining gives

$$\int\int_S (0, -1, 2) \cdot (0, 0, 1)dxdy = \int\int_R 2dxdy = 2\pi$$

This gives

$$\int_C u \cdot dr = 2\pi$$

as required. ■

4. Compute $\int_C F \cdot dr$ where $F = (z - y)\mathbf{i} - (x + z)\mathbf{j} - (x + y)\mathbf{k}$ and C is the curve $\{(x, y, z)|x^2 + y^2 + z^2 = 4, z = y\}$ oriented counterclockwise when viewed from above.

Solution: We will use Stokes' theorem. First, we need a sufrace S such that $C = \partial S$. We will choose $S := \{(x, y, z)|x^2 + y^2 + z^2 \leq 4, z = y\}$. We compute $\text{curl}(F)$ and $n \cdot dS$. Let $z = f(x, y) = y$.

$$\begin{aligned}
\text{curl}(F) = \det\begin{bmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ \frac{\partial}{\partial x} & \frac{\partial}{\partial y} & \frac{\partial}{\partial z} \\ z - y & -x - z & -x - y \end{bmatrix} &= 2\mathbf{j} \\
ndS = \pm(-f_x, -f_y, 1) &= (0, -1, 1)dxdy \\
\text{curl}(F) \cdot ndS &= -2dxdy
\end{aligned}$$

Notice that our region of integration is $R := \{(x, y)|x^2 + 2y^2 \leq 4\}$ which is an ellipse. This has equation $\left(\frac{x}{2}\right)^2 + \left(\frac{y}{\sqrt{2}}\right)^2 \leq 1$ and hence has area $2\sqrt{2}\pi$. Thus,

$$\int_C F \cdot dr = \int\int_S \text{curl}(F) \cdot ndS = \int\int_R (-2)dxdy = -2(2\sqrt{2}\pi) = -4\sqrt{2}\pi$$

1.4 Green's Theorem

Theorem 1.8. *(Green's Theorem) Let C be a positively oriented, piecewise smooth, simple closed curve in $\mathbb{R}^2$. Let D be the region bounded by C. If L and M are functions of (x, y) defined on an open region containing D and having continuous partial derivatives there, then*

$$\oint_C (Ldx + Mdy) = \int\int_D \left(\frac{\partial M}{\partial x} - \frac{\partial L}{\partial y}\right) dxdy = \int\int_D \left(\frac{\partial M}{\partial x} - \frac{\partial L}{\partial y}\right) dA$$

Proof. This turns out to be a special case of Stokes theorem. Let $F = (L, M, 0)$. Then,

$$\oint_C (Ldx + Mdy) = \oint_C (L, M, 0) \cdot (dx, dy, dz) = \oint_C F \cdot dr$$

Now, applying Stokes Theorem (1.7), we have that

$$\oint_C F \cdot dr = \int\int_S \nabla \times F \cdot \mathbf{n} dS$$

where S is the region in the plane D with unit normals point up in the positive Z direction to match the positive orientation needed for both theorems. Continuing with the simplification,

$$\nabla \times F \cdot \mathbf{n} = \left(\left(\frac{\partial 0}{\partial y} - \frac{\partial M}{\partial z}\right)\mathbf{i} + \left(\frac{\partial L}{\partial z} - \frac{\partial 0}{\partial x}\right)\mathbf{j} + \left(\frac{\partial M}{\partial x} - \frac{\partial L}{\partial y}\right)\mathbf{k}\right) \cdot \mathbf{k} = \left(\frac{\partial M}{\partial x} - \frac{\partial L}{\partial y}\right)$$

This gives us

$$\oint_C (Ldx + Mdy) = \int\int_S \nabla \times F \cdot \mathbf{n} dS = \int\int_D \left(\frac{\partial M}{\partial x} - \frac{\partial L}{\partial y}\right) dA$$

as reqiured. ∎

1. Let C be a simple closed C^1 curve in $\mathbb{R}^2$ with positive orientation enclosing a region D. Assume that D has area 2 and centroid $(3, 4)$. Let $F(x, y) = (y^2, x^2 + 3x)$. Find the line integral $\oint_C F \cdot dS$.

   Solution: We know that the formula for the centroid is

   $$\overline{x} = \frac{1}{A}\int\int_D xdA \qquad \text{and} \qquad \overline{y} = \frac{1}{A}\int\int_D ydA$$

   Now by Green's Theorem (1.8), we have

   $$\begin{aligned}\oint_C F \cdot dS = \int\int_D \left(\frac{\partial(x^2+3x)}{\partial x} - \frac{\partial y^2}{\partial y}\right) dA &= \int\int_D (2x + 3 - 2y)\, dA \\ &= 2\int\int_D (x)\, dA + 3\int\int_D dA - 2\int\int_D (y)\, dA \\ &= 2\overline{x}A + 3A - 2\overline{y}A \\ &= 2(3)(2) + 3(2) - 2(4)(2) = 12 + 6 - 16 = 2\end{aligned}$$

   as required. ∎

1.5 Divergence Theorem (Gauss' Theorem)

Theorem 1.9. *(Divergence Theorem) Suppose that V is a subset of $\mathbb{R}^n$ which is compact and has a piecewise smooth boundary S. If F is a continuously differentiable vector field defined on a neighbourhood of V, then we have*

$$\int\int\int_V (\nabla \cdot F) dV = \int\int_S F \cdot \boldsymbol{n} dS$$

where $\boldsymbol{n}$ is the outward pointing unit normal field of the boundary ∂V.

1. Let S be the unit sphere and let F be the vector field $F = 2x\mathbf{i} + y^2\mathbf{j} + z^2\mathbf{k}$. Compute $\int\int_S F \cdot \mathbf{n} dS$ where $\mathbf{n}$ is the outward pointing unit normal field.

   Solution: This is a straightforward application of the Divergence Theorem (1.9).

$$\int\int_S F \cdot \mathbf{n} ds = \int\int\int_W (\nabla \cdot F) dV = 2\int\int\int_W (1 + y + z) dV$$

   Now since the functions y and z are odd, we have

$$\int\int\int_W y dV = \int\int\int_W z dV = 0$$

   Hence,

$$\int\int_S F \cdot \mathbf{n} ds = 2\int\int\int_W dV = \frac{8\pi}{3}$$

   Where we use the fact that the volume of a sphere is $\frac{4\pi}{3}$. ■

2. Let S be the hemisphere $\{x^2 + y^2 + z^2 = 1 | z \geq 0\}$ and let F be the vector field $F = (x + \cos(z^2))\mathbf{i} + (y + \ln(x^2 + z^5))\mathbf{j} + \sqrt{x^2 + y^2}\mathbf{k}$. Compute $\int\int_S F \cdot \mathbf{n} dS$ where $\mathbf{n}$ is the outward pointing unit normal field.

   Solution: This is a straightforward application of the Divergence Theorem (1.9).

$$\int\int_S F \cdot \mathbf{n} ds = \int\int\int_W (\nabla \cdot F) dV = \int\int\int_W (1 + 1 + 0) dV$$

   Hence,

$$\int\int_S F \cdot \mathbf{n} ds = 2\int\int\int_W dV = \frac{4\pi}{3}$$

   Where we use the fact that the volume of a hemisphere is $\frac{2\pi}{3}$. ■

3. Let S be the cylinder bounded by $x^2 + y^2 = 1, z = 0, z = 2$ and let $u = (xz^2, \sin(x), y)$. Compute $\int\int_S u \cdot \mathbf{n} dS$ where $\mathbf{n}$ is the outward pointing unit normal field.

   Solution: We use the Divergence Theorem (1.9).

$$\int\int_S u \cdot \mathbf{n} ds = \int\int\int_W (\nabla \cdot F) dV = \int\int\int_W (z^2 + 0 + 0) dV$$

   Setting C to be the unit circle centred at the origin. Hence,

$$\int\int\int_W (z^2 + 0 + 0) dV = \int\int_C \int_0^2 z^2 = \int\int_C \frac{2^3}{3} = \frac{8\pi}{3}$$

   Where we use the fact that the area of a circle is $\pi(1)^2$. ■

1.6 Stone-Weierstrass Approximation Theorem

Theorem 1.10. *(Stone-Weierstrass Approximation Theorem)*

1. Let $g_1, g_2, ...$ be non-negative continuous functions on $[0, 1]$ such that the limie

$$\lim_{n\to\infty} \int_0^1 x^k g_n(x) dx$$

exists for every $k \in \mathbb{N}$ (including $k = 0$). Show that the limit

$$\lim_{n\to\infty} \int_0^1 f(x) g_n(x) dx$$

exists for every continuous function f on $[0, 1]$.

Solution: First, we plug in $k = 0$ to see that

$$\lim_{n\to\infty} \int_0^1 g_n(x) dx$$

exists for all n and hence that $|\int_0^1 g_n(x)dx| \leq M$ for all n. Now, by the Stone Weierstrass Theorem (1.10), we have that there is a sequence of polynomials converging to f in sup norm say $\{p_n\}$. Now, given an $\epsilon > 0$ there exists some integer k_ϵ such that $||f - p_{k_\epsilon}||_\infty \leq \frac{\epsilon}{3M}$. Also, as $\int_0^1 p_{k_\epsilon}(x) g_n(x)dx$ converges, it is Cauchy and hence, there is an integer n_ϵ such that

$$|\int_0^1 p_{k_\epsilon}(x) g_n(x) dx \int_0^1 p_{k_\epsilon}(x) g_m(x) dx| < \frac{\epsilon}{3}$$

for all $m, n \geq n_\epsilon$. Thus, for all $n, m \geq n_\epsilon$, we have

$$\begin{aligned}
\left|\int_0^1 f(x) g_n(x) dx - \int_0^1 f(x) g_m(x) dx\right| &\leq \left|\int_0^1 f(x) g_n(x) dx - \int_0^1 p_{k_\epsilon}(x) g_n(x) dx\right| \\
&+ \left|\int_0^1 p_{k_\epsilon}(x) g_n(x) dx - \int_0^1 p_{k_\epsilon}(x) g_m(x) dx\right| \\
&+ \left|\int_0^1 p_{k_\epsilon}(x) g_m(x) dx - \int_0^1 f(x) g_m(x) dx\right| \\
&< \int_0^1 |(f(x) - p_{k_\epsilon}(x)) g_n(x)| dx + \frac{\epsilon}{3} \\
&+ \int_0^1 |(f(x) - p_{k_\epsilon}(x)) g_m(x)| dx \\
&\leq ||(f(x) - p_{k_\epsilon}(x))||_\infty \int_0^1 g_n(x) dx + \frac{\epsilon}{3} \\
&+ ||(f(x) - p_{k_\epsilon}(x))||_\infty \int_0^1 g_m(x) dx \\
&\leq \epsilon
\end{aligned}$$

Thus the sequence $\int_0^1 f(x) g_n(x)dx$ is Cauchy and hence convergent in our complete metric space.

1.7 Uniform Convergence and Arzela-Ascoli

Definition 1.11. Let f_n be a sequence of functions on a closed and bounded interval $I = [a, b]$. We say that f_n is uniformly bounded if there exists an M such that $|f_n(x)| \leq M$ for all $x \in I$ and all f_n in teh sequence.

Definition 1.12. Let f_n be a sequence of functions on a closed and bounded interval $I = [a, b]$. We say that f_n is equicontinuous if for every $\epsilon > 0$ there exists a $\delta > 0$ such that if $|x - y| < \delta$ then $|f_n(x) - f_n(y)| < \epsilon$ for every f_n.

Theorem 1.13. *(Arzela-Ascoli Theorem) Let f_n be a sequence of functions on a closed and bounded interval $I = [a, b] \subseteq \mathbb{R}$. If this sequence is uniformly bounded and equicontinuous, then there exists a subsequence f_{n_k} such that it converges uniformly to some limit function f.*

Theorem 1.14. *(Dini's Theorem) Suppose $K \subseteq \mathbb{R}$ is a compact set and $f_n)_{n\geq 1}$ is a sequence of functions satisfying*

(i) Each f_n is continuous

(ii) f_n converges pointwise to a continuous function f in K

(iii) $f_n(x) \geq f_{n+1}(x)$ for all $x \in K$ and $n = 1, 2, ...$

Then $f_n \to f$ uniformly on K.

Proof. Let $\epsilon > 0$ and fix $x \in K$. Pointwise convergence tells us that there exists an $N_{x,\epsilon}$ such that $|f_n(x) - f(x)| < \frac{\epsilon}{3}$ for all $N \geq N_{x,\epsilon}$. Now, there exists a $\delta_{N,\epsilon}$ such that for all $|x - y| < \delta_{N,\epsilon}$ we have that both $|f_N(y) - f_N(x)| < \frac{\epsilon}{3}$ and $|f(x) - f(y)| < \frac{\epsilon}{3}$ (use the delta that is the minimum in both definitions of continuity). Hence, for all $y \in B_{\delta_{N,\epsilon}}(x)$, we have that

$$|f_N(y) - f(y)| \leq |f_N(y) - f_N(x)| + |f_N(x) - f(x)| + |f(x) - f(y)| < \epsilon$$

Notice that we can write $K = \bigcup_{\substack{x\in K \\ n\geq N_{x,\epsilon}}}^{\infty} B_{\delta_{n,\epsilon}}(x)$. By compactness, we need only finitely many of these sets say $K = \bigcup_{i=1}^{k} B_{\delta_{n_i,\epsilon}}(x_i)$. Let $N = \max_{1\leq i\leq k}\{n_i\}$. Thus, for any $z \in K$, we have that $z \in B_{\delta_{n_i,\epsilon}}(x_i)$ for some i. This implies that $|f_{n_i}(z) - f(z)| < \epsilon$. Since $n_i \geq N$, we have for all $n \geq N$ that

$$|f_n(z) - f(z)| \leq |f_{n_i}(z) - f(z)| < \epsilon$$

where the first inequality holds since $-f_n(x) \leq -f_{n+1}(x) \Rightarrow |f(x) - f_n(x)| \leq |f(x) - f_{n+1}(x)|$ (note this holds similarly if the functions were non-decreasing). This is the precise statement of uniform convergence (we found an N so that for all $n \geq N$ we have pointwise limits holding for every x). ■

■

1. Suppose that $f_n : [0, 1] \to \mathbb{R}$ are C^1 functions such that for all $x \in [0, 1]$ we have

$$|f_n(x)| + |f_n'(x)| \leq 1$$

Prove that $(f_n)_{n\geq 1}$ has a uniformly convergent subsequence.

Solution: Notice that $|f_n(x)| \leq |f_n(x)| + |f_n'(x)| \leq 1$ and $|f_n'(x)| \leq 1$. The first condition says that f_n is uniformly bounded. I claim that this sequence is equicontinuous. Let $\epsilon > 0$ and let $\delta = \epsilon$. Suppose $|x - y| < \delta$. Then, using the Mean Value Theorem (1.3), we have that for some $c \in [0, 1]$

$$|f_n(x) - f_n(y)| = |x - y||f_n'(c)| < \epsilon(1) = \epsilon$$

Hence f_n is equicontinuous. By the Arzela-Ascoli Theorem (1.13) we have that $(f_n)_{n\geq 1}$ must have a uniformly convergent subsequence as required. ■

2. Let $\{f_n\}$ be an equicontinuous sequence of functions on a compact set K, which converges pointwise to a function f. Prove that f is continuous. Further, show that $\{f_n\}$ converges uniformly to f.

Solution: Let $\epsilon > 0$ and fix an arbitrary $a \in K$. We need to find a δ so that for all $|x - a| < \delta$ we have that $|f(x) - f(a)| < \epsilon$. By equicontinuity, we know that there exists a δ such that $|f_n(x) - f_n(a)| < \frac{\epsilon}{3}$ whenever $|x - a| < \delta$. Choose this delta and suppose $|x - a| < \delta$. Note by pointwise convergence there is a n_1 such that for all $n \geq n_1$ we have that $|f_n(x) - f(x)| < \frac{\epsilon}{3}$.

Similarly, by pointwise convergence there is a n_2 such that for all $n \geq n_2$ we have that $|f_n(a) - f(a)| < \frac{\epsilon}{3}$. Let $n_0 = \max\{n_1, n_2\}$. For all $n \geq n_0$ and all $|x - a| < \delta$, we have that

$$|f(x) - f(a)| < |f(x) - f_n(x)| + |f_n(x) - f_n(a)| + |f_n(a) - f(a)| < \frac{\epsilon}{3} + \frac{\epsilon}{3} + \frac{\epsilon}{3} = \epsilon$$

proving that f is continuous. Using the fact that f_n are equicontinuous, choose a $\delta > 0$ such that $|f_n(x) - f_n(y)| < \frac{\epsilon}{3}$ and $|f(x) - f(y)| < \frac{\epsilon}{3}$ for all $x, y \in K$ such that $|x - y| < \delta$. Notice that $\bigcup_{x \in K} B_\delta(x) = K$ and so by compactness, there must exist a finite subcover say $K = \bigcup_{i=1}^{k} B_\delta(x_i)$. Pointwise convergence for each i gives us an N_i such that $|f_n(x_i) - f(x_i)| < \frac{\epsilon}{3}$ for all $n \geq N_i$. Let $N = \max_{1 \leq l \leq k}\{N_i\}$. Now, for any $x \in K$, there is an x_i such that $x \in B_\delta(x_i)$. This tells us that for all $n \geq N$ we have

$$|f_n(x) - f(x)| \leq |f_n(x) - f_n(x_i)| + |f_n(x_i) - f(x_i)| + |f(x_i) - f(x)| < \epsilon$$

showing that f_n is uniformly convergent. ■

3. Let $(f_n)_{n \geq 1}$ be a set of continuous functions on $[0, 1]$. Suppose that for all $x, y \in [0, 1]$ and all $n \in \mathbb{N}$, we have that

$$|f_n(x) - f_n(y)| \leq L|x - y|$$

where L is a fixed constant. Suppose further that f_n converges pointwise to a function f. Show that f_n converges uniformly to f and that f satisfies (for all $x, y \in [0, 1]$)

$$|f(x) - f(y)| \leq L|x - y|$$

Solution: Let $\epsilon > 0$ and set $\delta = \frac{\epsilon}{L}$. Then

$$|f_n(x) - f_n(y)| \leq L|x - y| < L\frac{\epsilon}{L} = \epsilon$$

and so the set of functions is equicontinuous. The previous question tells us that f is continuous and moreover that f_n converges uniformly to f. All that's left is showing f satisfies the same Lipschitz property with the constant L. This follows since for all $x, y \in [0, 1]$, and large enough n,

$$\begin{aligned}|f(x) - f(y)| &\leq |f(x) - f_n(x)| + |f_n(x) - f_n(y)| + |f_n(y) - f(y)| \\ &\leq \epsilon + L|x - y| + \epsilon\end{aligned}$$

and since ϵ is arbitrary, we get our desired result. ■

4. Let $\phi : [0, 1] \times \mathbb{R} \to \mathbb{R}$ be a bounded and continuous function. For each $n \in \mathbb{N}$, let $F_n : [0, 1] \to \mathbb{R}$ satisfy (for $t \in [0, 1]$),

$$F_n(0) = \frac{1}{n} \qquad\qquad F_n'(t) = \phi(t, F_n(t))$$

Here $F_n'(0)$ denotes the right derivative and $F_n'(1)$ denotes the left derivative.

(i) Prove that there is a subsequence of $(F_n)_{n \geq 1}$ such that it converges uniformly to a limit function F.

(ii) Prove that F solves (for $t \in [0, 1]$),

$$F(0) = 0 \qquad\qquad F'(t) = \phi(t, F(t))$$

Solution:

(i) Notice that $F_n(x) = \int_0^x F_n'(t)dt + F_n(0)$ by the Fundamental Theorem of Calculus. Since ϕ is bounded, we have that F_n' is bounded on $[0,1]$ say by C. Now, for all $x \in [0,1]$ and using the Mean Value Theorem (1.3) to get a $c \in [0,x]$,

$$|F_n(x)| \leq |F_n(x) - F_n(0)| + |F_n(0)| = |x||F_n'(c)| + \frac{1}{n} \leq (1)(C) + 1 = C + 1$$

So $(F_n(x))_{n\geq 1}$ is uniformly bounded. Since ϕ is bounded, there exists a C such that $|\phi(t, F_n(t))| \leq C$. Now, suppose that $\epsilon > 0$. Then let $\delta = \frac{\epsilon}{C}$. If $|x - y| < \delta$, then again by using the Mean Value Theorem (1.3) to get a $d \in [0,1]$, we have

$$|F_n(x) - F_n(y)| \leq |x - y||F_n'(c)| < \frac{\epsilon}{C}C = \epsilon$$

Hence $(F_n)_{n\geq 1}$ are equicontinuous. Thus, by the Arzela-Ascoli theorem (1.13), we have that there is a uniformly continuous subsequence of this sequence that convergse to a limit function F as required. ■

(ii) Notice that $F(0) = \lim_{n\to\infty} F_n(0) = \lim_{n\to\infty} \frac{1}{n} = 0$. For the other part, NEEDS TO BE COMPLETED. ■

5. For $n = 1, 2, ..$ and $x \in \mathbb{R}$, let

$$f_n(x) = \frac{\sin(x)}{1 + n^2x^2}$$

Show that $(f_n)_{n\geq 1}$ converges uniformly on $[-\pi, \pi]$.

Solution: We will use Dini's Theorem (1.14) which we can use since our interval is compact. We need three properties.

(i) Firstly, since both the numerator and denominator are continuous functions and the denominator is never 0, we have that each f_n are continuous.

(ii) I claim that $f_n(x) \to 0$ as $n \to \infty$ and this is easy to see when $x \neq 0$. If $x = 0$ then notice that the function $f_n(0) = 0$ and so this too converges to the zero function. Moreover, since the zero function is continuous, this property is satisfied.

(iii) Since $n^2 \leq (n+1)^2$ for all $n \in \mathbb{N}$, we have that $f_{n+1}(x) \leq f_n(x)$.

Hence our theorem is satisfied and thus $f_n \to f$ uniformly as required. ■

6. Consider

$$f(x) = \sum_{n=1}^{\infty} \frac{1}{1 + n^2x}$$

(i) For which x does this series converge absolutely?

(ii) On which intervals does it converge uniformly?

(iii) Is f continuous wherever the series converges?

(iv) Is f bounded?

Solution:

(i) Notice that this function is not convergent at $x = 0$ and isn't even defined at $\frac{-1}{n^2}$. Let $S = \mathbb{R}\backslash\{0, (\frac{-1}{n^2})_{n=1}^{\infty}\}$. I claim that the series is absolutely convergent if and only if $x \in S$. It is clear if $f(x)$ is absolutely convergent at x, then $x \in S$. Suppose $x \in S$. Choose $N > \frac{1}{\sqrt{x}}$. Then for all $n \geq N$, we have

$$\sum_{n \geq N} |f_n(x)| \leq \frac{1}{n^2|x| - 1}$$

Clearly, the right hand side is convergent, we have by the comparison theorem that $f(x)$ is absolutely convergent at x. ■

(ii) Suppose $c > 0$. Define $S_c = \{x \in S \mid |x| \geq c\}$. I claim that $f(x)$ is uniformly convergent on S_c. Let

$$s_n(x) := \sum_{i=1}^{n} \frac{1}{1 + i^2 x}$$

Now, let $\epsilon > 0$ and $N_1 > \frac{1}{\sqrt{c}}$. Then for $m > n \geq N_1$,

$$|s_m(x) - s_n(x)| = \left| \sum_{k=n+1}^{m} f_k(x) \right| \leq \sum_{k=n+1}^{m} |f_k(x)| \leq \sum_{k=n+1}^{m} \frac{1}{k^2 c - 1}$$

Again since the right hand side converges, there is an $N_2 > N_1$ such that if $m > n \geq N_2$, then

$$\sum_{k=n+1}^{m} \frac{1}{k^2 c - 1} \leq \frac{\epsilon}{2} < \epsilon$$

Thus for all $m > n \geq N_2$ and for all $x \in S_c$,

$$|s_m(x) - s_n(x)| < \epsilon$$

Hence $f(x)$ is uniformly convergent on the intervals $I_n = \left(\frac{-1}{n^2}, \frac{-1}{(n+1)^2}\right)$ (when they intersect S_c), $(-\infty, -1)$ and $[c, \infty)$. The only points excluded are those in $(0, c)$. Assume towards a contradiction that f is uniformly convergent on $(0, c)$. Then there exists an n such that for $n > m > N$ and $0 < x < c$ we have

$$|s_n(x) - s_m(x)| < \frac{1}{2}$$

Therefore for $n > N$ and $0 < x < c$

$$|s_{n+1}(x) - s_n(x)| = |f_{n+1}(x)| < \frac{1}{2}$$

However, $f_n(x)$ tends to 1 at 0, a contradiction. Thus, the set of points where f is uniformly convergent is S_c. ■

(iii) From the first part, it follows that f converges exactly on the set S. The above also tells us that f is uniformly convergent on S_c and hence continuous on S_c. Note that if $x \in S$, then $x \in S_c$ for any $c < |x|$. Therefore, f is continuous at x. ■

(iv) Assume that $|f(x)| \leq M$ for all $x \in S$. For $x > 0$ we have that $M \geq f(x) \geq s_n(x)$. Therefore, $M \geq \sup_{x>0} s_n(x) = n$ (recalling at 0 we have $s_n(0) = n$). This holds for each n giving a contradiction. ■

1.8 Fourier Series

Theorem 1.15. *(Fourier formula) Let $f(x)$ be a function with period $2L$. Then, the Fourier series of f is*

$$\frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n \cos(\frac{nx\pi}{L}) + b_n \sin(\frac{nx\pi}{L})$$

where

$$a_n = \frac{1}{L}\int_{-L}^{L} f(x)\cos(\frac{nx\pi}{L})dx$$
$$b_n = \frac{1}{L}\int_{-L}^{L} f(x)\sin(\frac{nx\pi}{L})dx$$

1. Define a periodic function $f(x)$ by $f(x) = e^x$ on $[-\pi, \pi]$ and $f(x + 2\pi) = f(x)$. Find the Fourier series representation of $f(x)$ and check if its derivative is itself.

   Solution: We note

$$\begin{aligned} a_n &= \frac{1}{L}\int_{-L}^{L} f(x)\cos(\frac{nx\pi}{L})dx \\ &= \frac{1}{\pi}\int_{-\pi}^{\pi} e^x \cos(nx)dx \end{aligned}$$

   Note that

$$\begin{aligned} \int e^x \cos(nx)dx &= \frac{1}{n}e^x \sin(nx) - \frac{1}{n}\int e^x \sin(nx) \\ &= \frac{1}{n}e^x \sin(nx) - \frac{1}{n}(\frac{1}{n}e^x \cos(nx) + \frac{1}{n}\int e^x \cos(nx)) \\ \Rightarrow (1 + \frac{1}{n^2})\int e^x \cos(nx) &= \frac{1}{n}e^x \sin(nx) - \frac{1}{n^2}e^x \cos(nx) \\ \Rightarrow \int e^x \cos(nx) &= \frac{n}{n+1}e^x \sin(nx) - \frac{n}{n+1}e^x \cos(nx) \end{aligned}$$

   Hence,

$$\begin{aligned} a_n &= \frac{1}{\pi}\,\frac{n}{n+1}e^x \sin(nx) - \frac{n}{n+1}e^x \cos(nx)\Big|_{-\pi}^{\pi} \\ &= \frac{1}{\pi}(-\frac{n}{n+1}e^{\pi}\cos(n\pi) - \frac{n}{n+1}e^{-\pi}\cos(-n\pi)) \end{aligned}$$

   Similarly... Man this is painful I'm going to sleep. ■

1.9 Random Real Analysis Questions

1. Let (X, d) be a complete metric space (all Cauchy sequences converge). Let $L : X \to X$ be a function such that for some $k < 1$, we have for all $x, y \in X$,

$$d(L(x), L(y)) < kd(x, y)$$

   Prove that there exists a point $z \in X$ such that $L(z) = z$ and that this z is unique.

Solution: I believe in the literature this is called the Banach Contractive Mapping Theorem (or the Banach Fixed Point Theorem). Let $x_0 = x$ for some fixed $x \in X$ and $x_n = L^n(x)$. Now for a large enough $n \in \mathbb{N}$ we have

$$d(x_{n+1}, x_n) = d(L^{n+1}(x), L^n(x)) < kd(L^n(x), L^{n-1}(x)) < ... < k^n d(L(x), x)$$

Let $\epsilon > 0$. Now, choose an $N \in \mathbb{N}$ such that $q^N < \frac{\epsilon(1-k)}{d(L(x),x)}$. This gives us for all $n > m \geq N$

$$\begin{aligned} d(x_n, x_m) &\leq d(x_n, x_{n-1}) + ... + d(x_{m+1}, x_m) \\ &< k^{n-1} d(L(x), x) + k^{n-2} d(L(x), x) + ... + k^m d(L(x), x) \\ &= d(L(x), x) \frac{q^m}{1-q} \\ &\leq d(L(x), x) \frac{q^N}{1-q} \\ &< \epsilon \end{aligned}$$

Hence this sequence is Cauchy and thus converges by completeness. Let $z = \lim_{n\to\infty} x_n$. I claim $L(z) = z$. Let N be large enough so that $d(x_n, z) < \frac{\epsilon}{2}$ for all $n \geq N$. Hence,

$$d(L(z), z) \leq d(L(z), x_{N+1}) + d(x_{N+1}, z) < kd(z, x_N) + \frac{\epsilon}{2} < d(z, x_N) + \frac{\epsilon}{2} < \epsilon$$

Thus the distance is as arbitrarily small as we want and hence $L(z) = z$. For uniqueness, suppose that there is another fixed point say $L(w) = w$ with $w \neq z$. Then

$$d(z, w) = d(L(z), L(w)) < kd(z, w) \quad \Rightarrow \quad 1 < k$$

which is a contradiction since $k < 1$. ■

2 Complex Analysis

2.1 Conformal Mapping Theorem

Theorem 2.1. *(Möbius Transformation Theorem) The following maps take straight lines and circles to straight lines or circles from $\mathbb{C} \cup \{\infty\}$ to itself (bijectively).*

$$\begin{aligned} z &\mapsto z + b \\ z &\mapsto \frac{1}{z} \\ z &\mapsto kz \\ z &\mapsto \frac{az+b}{cz+d} \end{aligned}$$

where $k \neq 0$ and $ad - bc \neq 0$. A fun note: These functions form a group under composition. Moreover, these maps are conformal (on the extended complex plane).

Theorem 2.2. *Let $U \subseteq \mathbb{C}$ be an open set. A function $f : U \to \mathbb{C}$ is conformal if and only if it is complex analytic (holomorphic) and its derivative everywhere on U is non-zero.*

1. Let D be the unit disc. Then there is a conformal map from the unit disc to $\mathbb{H} := \{z | \Im(z) > 0\}$.

Solution: Define $f(z) := \frac{z-i}{z+i}$. Notice that its inverse is $f^{-1}(w) = i\frac{1+w}{1-w}$. Moreover, $f(0) = -1$, $f(1) = -i$, and $f(-1) = i$ and such by (2.1), this map is conformal and takes the real line to the unit circle. Since $f(i) = 0$ we also have that this map takes $\mathbb{H}$ to D. Hence f^{-1} takes D to $\mathbb{H}$ as required. ■

2. Let D be the unit disc. Find a conformal map from the half plane $\mathbb{H}$ rotated counter clockwise by α to D. Note this map will take the closed upper half plane to the closed unit disc.

   Solution: Notice that $S(z) := e^{-i\alpha}z$ rotates the rotated half plane to $\mathbb{H}$. So, using the fact that $f(z) := \frac{z-i}{z+i}$ maps $\mathbb{H}$ to D by the previous exercise, we have that $f(S(z)) = \frac{e^{-i\alpha}z-i}{e^{-i\alpha}z+i}$ maps the rotated half plane to the unit disc as required. ■

3. Let D be the unit disc. Find a conformal map from D to D that sends the point a to 0.

   Solution: $f(z) := \frac{a-z}{1-\bar{a}z}$ does the trick. This map is also an automorphism and an involution (it is its own inverse). (Note Marsden also has an $e^{i\theta}$ factor but i'm not sure why). ■

4. Find a conformal map from the open upper semicircle $U = \{z|0 < \arg(z) < \pi, 0 < |z| < 1\}$ to the open first quadrant $V = \{z|0 < \arg(z) < \frac{\pi}{2}\}$.

   Solution: Consider the map from the open unit disc to the upper half plane $f(z) = i\frac{1+z}{1-z}$. Notice that this takes the open upper semi circle to the open second quadrant. Hence, rotating this by $\frac{3\pi}{2}$ (ie multiplying by $e^{i\frac{3\pi}{2}} = -i$) will map the open upper semi circle to the open first quadrant. This map is simply $g(z) := -if(z) = \frac{1+z}{1-z}$. ■

5. Find a conformal map from $U = \{z|0 < \arg(z) < \frac{\pi}{2}, 0 < |z| < 1\}$ to the open unit disc D.

   Solution: Note that the map $z \mapsto z^4$ is not correct as it misses the positive axis. The set U is just the quarter circle in the first quadrant without the x and y axes. What we shall do is perform the following transformations:

   (i) Open quarter circle to open half circle via $f_1(z) = z^2$
   (ii) Open half circle to open first quadrant via $f_2(z) = \frac{-iz-i}{-iz+i} = \frac{1+z}{1-z}$
   (iii) Open first quadrant to (open) upper half plane via $f_3(z) = z^2$
   (iv) (Open) Upper half plane to D via $f_4(z) = \frac{z-i}{z+i}$

   Taking the composition of all these functions in order yields

$$f(z) = \frac{(1+z^2)^2 - i(1-z^2)^2}{(1+z^2)^2 + i(1-z^2)^2}$$

   as required. ■

2.2 Laurent Series

Theorem 2.3. *A Laurent series is unique whenever it exists. if $f(z) = \sum_{n=-\infty} \infty a_n(x-c)^n$, then*

$$a_n = \frac{1}{2\pi i}\oint_\gamma \frac{f(z)}{(z-c)^{n+1}}$$

1. Find the Laurent Expansion of $f(z) = \frac{1}{(z-1)(z-2i)}$ in the region

   (i) $|z| < 1$
   (ii) $1 < |z| < 2$
   (iii) $2 < |z|$

Solution: We begin by first by a partial fraction decomposition.

$$\begin{aligned}\frac{1}{(z-1)(z-2i)} &= \frac{A}{z-1} + \frac{B}{z-2i}\\ \Rightarrow 1 &= A(z-2i) + B(z-1)\\ \Rightarrow A &= \frac{1}{1-2i} = \frac{1+2i}{5}\\ B &= \frac{1}{2i-1} = -A\end{aligned}$$

(i) In this case,

$$\frac{A}{z-1} = \frac{-A}{1-z} = -A(1+z+z^2+...) = -A\sum_{n=0}^{\infty} z^n$$

$$\frac{B}{z-2i} = \frac{-B}{2i-z} = \frac{-B}{2i}\frac{1}{1-\frac{z}{2i}} = \frac{-B}{2i}\sum_{n=0}^{\infty}(\frac{z}{2i})^n = A\sum_{n=0}^{\infty}\frac{z^n}{(2i)^{n+1}}$$

$$\Rightarrow \frac{1}{(z-1)(z-2i)} = \frac{A}{z-1} + \frac{B}{z-2i} = -A\sum_{n=0}^{\infty} z^n + A\sum_{n=0}^{\infty}\frac{z^n}{(2i)^{n+1}} = A\sum_{n=0}^{\infty}(\frac{z^n}{(2i)^{n+1}} - z^n)$$

$$\Rightarrow \frac{1}{(z-1)(z-2i)} = \frac{1+2i}{5}\sum_{n=0}^{\infty}(\frac{1}{(2i)^{n+1}} - 1)z^n$$

■

(ii) In this case, we still have that

$$\frac{B}{z-2i} = A\sum_{n=0}^{\infty}\frac{z^n}{(2i)^{n+1}}$$

However the Laurent series changes for $\frac{A}{z-1}$. This becomes,

$$\frac{A}{z-1} = \frac{-A}{1-z} = \frac{A}{z}\frac{1}{1-\frac{1}{z}} = \frac{A}{z}(1+\frac{1}{z}+(\frac{1}{z})^2+...) = A\sum_{n=0}^{\infty}\frac{1}{z^{n+1}} = A\sum_{n=1}^{\infty}\frac{1}{z^n}$$

Combining yields

$$\frac{1}{(z-1)(z-2i)} = A\sum_{n=1}^{\infty}\frac{1}{z^n} + A\sum_{n=0}^{\infty}\frac{z^n}{(2i)^{n+1}} = \frac{1+2i}{5}(\sum_{n=1}^{\infty}\frac{1}{z^n} + \sum_{n=0}^{\infty}\frac{1}{(2i)^{n+1}}z^n)$$

■

(iii) In this case, we still have that

$$\frac{A}{z-1} = A\sum_{n=1}^{\infty}\frac{1}{z^n}$$

However the Laurent series changes for $\frac{A}{z-1}$. This becomes,

$$\frac{B}{z-2i} = \frac{-B}{2i-z} = \frac{B}{z}\frac{1}{1-\frac{2i}{z}} = \frac{B}{z}\sum_{n=0}^{\infty}(\frac{2i}{z})^n = -A\sum_{n=1}^{\infty}\frac{(2i)^{n-1}}{z^n}$$

Combining yields

$$\frac{1}{(z-1)(z-2i)} = A\sum_{n=1}^{\infty}\frac{1}{z^n} - A\sum_{n=1}^{\infty}\frac{(2i)^{n-1}}{z^n} = \frac{1+2i}{5}\sum_{n=1}^{\infty}\frac{1-(2i)^{n-1}}{z^n}$$

■

2.3 Singularities

Definition 2.4. Removable Singularity: The Laurent series has no negative terms (the principle value is zero). One can think of this as a pole of order 0 (see below).

Definition 2.5. Essential Singularity: The Laurent series has infinitely many non-zero negative terms (that is, the principle value is infinite).

Definition 2.6. Pole: The Laurent series has only finitely many negative terms with at least one non-zero (the principle value is finite and non-zero).

Theorem 2.7. *(Riemann's Theorem) Let $D \subseteq \mathbb{C}$ be open, $a \in D$ and f a holomorphic function on $D\backslash\{a\}$. Then TFAE*

(i) f is holomorphically extendable over a

(ii) f is continuously extendable over a

(iii) There exists a neighbourhood of a of which f is bounded

(iv) $\lim_{z\to a}(z-a)f(z) = 0$

When any of these hold, we say that the singularity is removable. As a corollary, let f be an analytic function on $\mathbb{C}$ except on a set of singularities. If all singularities of a function are removable, then the function can be extended to an entire function.

2.3.1 Liouville's Theorem

Theorem 2.8. *(Cauchy's Inequality) Let f be an analytic function on a region A and let γ be a circle with radius R and centre z_0 that lies in A. Suppose that $|f(z)| \leq M$ for all z on γ. Then for each $k \in \mathbb{N}$ (including $k = 0$), we have*

$$|f^k(z_0)| \leq \frac{k!}{R^k}M$$

Theorem 2.9. *(Liouville's Theorem) If f is an entire (analytic on all of $\mathbb{C}$) and bounded ($|f(z)| \leq M$ for some finite M) function, then f is constant.*

Proof. By Cauchy's Inequality (2.8) on $k = 1$, we have that

$$|f^{'}(z_0)| \leq \frac{M}{R}$$

This holds for any circle $|z - z_0| = R$. Thus, taking the limit as $R \to \infty$ gives us $|f'(z_0)| = 0$ and hence $f'(z_0) = 0$. As $z_0 \in \mathbb{C}$ was also arbitrary, $f'(z) = 0$ for all $z \in \mathbb{C}$. Hence f is constant as required. ■

1. Find all entire functions f such that $|f(z)| \leq e^{\Re(z)}$.

   Solution: Notice that the following function is entire and

   $$|\frac{f(z)}{e^z}| = \frac{|f(z)|}{e^{\Re(z)}} \leq 1$$

   and so the function is bounded. By Liouville's Theorem (2.9) we have that $\frac{f(z)}{e^z} = c$ for some $c \in \mathbb{C}$. Now, $f(z) = ce^z$ and since $|c|e^{\Re(z)} = |f(z)| \leq e^{\Re(z)}$ we have that $|c| \leq 1$. This constitutes all the functions as required. ■

2. Let f be an entire function such that $\Re(f(z)) \geq -2$ for all $z \in \mathbb{C}$. Show that f is constant.

   Solution: Consider $g(z) := e^{-f(z)}$. This function is entire and $|g(z)| = e^{-\Re(z)} \leq e^{-2}$. Hence g is a bounded entire function so by Liouville's Theorem (2.9) this function is constant. Notice that this constant is nonzero, call it $c \in \mathbb{C}$. Now this gives us that $f(z) = \log|c| + \arg(c) + 2\pi k$ for $k \in \mathbb{Z}$. But since f is continuous, this has to be a specific value for k. Hence f is also constant. (I have spelt this out very bluntly hopefully to make it as clear as possible where the continuity of f matters here - in the past I haven't truly understood where the continuity mattered here). ■

3. Let f and g be two entire functions such that $\Re(f(z)) \geq k\Re(g(z))$ for all $z \in \mathbb{C}$ and some $k \in \mathbb{C}$ (independent of z). Show that there exist constant a and b such that $f(z) = ag(z) + b$.

   Solution: Consider $h(z) := f(z) + kg(z)$. This function is entire and

$$|e^{h(z)}| = e^{\Re(f(z)) - k\Re(g(z))} \leq e^0 = 1$$

   Hence $e^{h(z)}$ is a bounded entire function so by Liouville's Theorem (2.9) this function is constant. As in the previous question, we must have by the continuity of h that $h(z) = b$ for some $b \in \mathbb{C}$. The result follows. ■

4. Show that if $|f(z)| \leq M|z|^n$ then f is a polynomial function of degree at most n.

   Solution: Note this is true even if $|f(z)| \leq M|z|^n$ holds only for $|z| \geq R$. By Cauchy's Inequality (2.8) on n, we have that (for any $z_0 \in \mathbb{C}$),

$$|f^{(n)}(z_0)| \leq \frac{n!M_0}{R^n}$$

   where for γ a circle of radius R and centre z_0,

$$M_0 = \max_{z\in\gamma} |f(z)| \leq \max_{z\in\gamma} M|z|^n = MR^n$$

   and hence

$$|f^{(n)}(z_0)| \leq \frac{n!M_0}{R^n} \leq n!M$$

   (this holds not just for n but for all $n_0 > n$ as well). Since z_0 was arbitrary, we have that $f^{(n)}(z)$ is bounded for all $z \in \mathbb{C}$. By Liouville's Theorem (2.9) we have that $f^{(n)}(z) = c_n$ for some $c_n \in \mathbb{C}$. Thus, antidifferentiating n times tells us that

$$f^{(n-1)}(z) = c_n z + c_{n-1} \vdots f^{(1)}(z) = c_n z^{n-1} + c_{n-1} z^{n-2} + ... + c_1 f(z) = c_n z^n + c_{n-1} z^{n-1} + ... + c_0$$

   where $c_i \in \mathbb{C}$. Thus f is a polynomial of degree at most n. ■

5. Let f and g be entire functions and suppose that $|f(z)| \leq |g(z)|$ for all $z \in \mathbb{C}$. Prove that $f(z) = ag(z)$ for some $a \in \mathbb{C}$

   Solution: If $g(z) = 0$ then this is trivial. Otherwise, $|\frac{f(z)}{g(z)}| \leq 1$ for all $z \in \mathbb{C}$. Hence all singularities are removable by Riemann's Theorem (2.7) and thus our function can be extended to an entire function (also by Riemann's Theorem). Since this function is bounded, then Liouville's Theorem (2.9) tells us that $\frac{f(z)}{g(z)} = a$ for some $a \in \mathbb{C}$. ■

6. Let f be an entire nonconstant function. Then the image of f is dense in $\mathbb{C}$.

   Solution: If the image is not dense, then there exists a complex number w and a neighbourhood (in particular, an open disc of radius r) of w such that the image does not intersect it. This means that $|f(z) - w| > r$. Define $g(z) := \frac{1}{f(z)-w}$. This function is entire. Moreover g is bounded since $|g(z)| = \frac{1}{|f(z)-w|} < \frac{1}{r}$ which holds for all $z \in \mathbb{C}$. This means that g is constant.

2.3.2 Classifying Singularities and Theorems of Complex Analysis

Theorem 2.10. *(Casorati-Weierstrass Theorem) Let $U \subseteq \mathbb{C}$ be open and let $z \in U$. Suppose that f is a holomorphic function on $U \backslash \{z\}$ and that f has an essential singularity at z. Then if V is any neighbourhood of z contained in U, then $f(V \backslash \{z\})$ is dense in $\mathbb{C}$.*

Theorem 2.11. *(Open Mapping Theorem) Let $U \subseteq \mathbb{C}$ be a connected open subset. Suppose that f is a non-constant holomorphic function from U to $\mathbb{C}$. Then f is an open map (that is, it takes open sets to open sets).*

Theorem 2.12. *(Weierstrass Factorization Theorem) An entire function can be represented by a product involving their zeroes. In particular, every entire function can be represented by a power series (that is a Laurent expansion with no negative terms).*

Theorem 2.13. *(Little Picard) Let $f(z)$ be an entire non-constant complex function. Then the set of values that $f(z)$ assumes is either the whole complex plane or the plane minus a single point*

Theorem 2.14. *(Big Picard) Let $f(z)$ be an analytic and suppose f has an essential singularity at a point w. Then on any open set containing w, the function $f(z)$ takes on all possible complex values, with at most a single exception, infinitely often.*

1. Prove that all entire functions that are injective are linear.

   Solution: Let $f(z)$ be an entire injective function. Let $g(z) := f(\frac{1}{z})$ defined from $\mathbb{C}^*$ to $\mathbb{C}$. Essentially we wish to classify the singularity of f at ∞. To do this we classify the singularity of 0 on g.

   If the singularity at 0 is removable, then Riemann's Theorem (2.7) tells us that g is bounded on a closed disc centred at the origin. This means that $f(z) = g(\frac{1}{z})$ is bounded outside a closed circle centred at the origin. Now, since f is continuous and the closed circle centred at the origin is compact, we have that f must also be bounded on the closed circle. Hence f is bounded. Thus, by Liouville's Theorem (2.9), since f is entire, we have that f is constant. This contradicts the injectivity of f.

   If the singularity at 0 is essential, Then by Casorati-Weierstrass (2.10), setting D to be a punctured closed disc of radius r at the origin, we have that $g(D)$ is dense in $\mathbb{C}$. This means that $f(\{|z| > r\})$ is dense in $\mathbb{C}$. Now, by the open mapping theorem (2.11), $f(\{|z| < r\})$ is a non-empty open set. Hence $f(\{|z| < r\}) \cap f(\{|z| > r\}) \neq \emptyset$. This contradicts the injectivity of f as now two points map to the same point.

   Hence, by the classification, 0 must be a pole of g. By the uniqueness of Laurent Expansions, we must have that the Laurent expansion of g has only finitely many terms of negative degree (the principle part). Hence f has only finitely many positive degree terms. Since f can be written as a power series by Weierstrass Factorization Theorem (2.12), we have that f is a polynomial. Since f is injective, this function can have at most one root. Since f is injective, it must be non-constant. Hence $f(z) = az + b$ with $a \neq 0$ and $a, b \in \mathbb{C}$ as reqiured. ■

2. Prove that the unit disc D and $\mathbb{C}$ are homeomorphic but that there is no holomorphic function f from $\mathbb{C}$ onto D.

Solution: The function $g(z) := \frac{z}{1-|z|^2}$ is a real analytic and bijective function with analytic inverse. This shows that they are homeomorphic.

Let $f : \mathbb{C} \to D$ be a holomorphic onto function. By the Little Picard theorem (2.13), we have that since f is entire, $f(\mathbb{C})$ misses at most one point in the complex plane. But f was supposed to be onto the unit disc, a contradiction. Hence no function can exist. ■

3. Show that there cannot be an analytic bijective function f from $\mathbb{C}$ to the unit disc D or vice versa.

Solution: In the first case, the function is entire and $|f| < 1$ so by Liouville's Theorem (2.9) f is a constant function. In the opposite direction, We have that f^{-1} will be a bounded entire function.

2.4 Maximum Modulus Principle

Theorem 2.15. *(Maximum Modulus Principle) Suppose that $A \subseteq \mathbb{C}$ is an open, connected and bounded set. Let $f : \mathrm{cl}(A) \to \mathbb{R}$ be an analytic function on A and continuous on $\mathrm{cl}(A)$. Then $|f|$ has a finite maximum attained at some $z \in \mathrm{cl}(A)$. Further, if this max is contained at some point in $A\backslash\mathrm{cl}(A)$, then f is constant on $\mathrm{cl}(A)$ (which contains A).*

Theorem 2.16. *(Maximum Modulus Principle Harmonic) Suppose that $A \subseteq \mathbb{C}$ is an open, connected and bounded set. Let $u : \mathrm{cl}(A) \to \mathbb{C}$ be a continuous and harmonic function on A and continuous on $\mathrm{cl}(A)$. Then u has a finite maximum attained at some $(x, y) \in \mathrm{cl}(A)$. Further, if this max is contained at some point in $A\backslash\mathrm{cl}(A)$, then u is constant on $\mathrm{cl}(A)$ (which contains A).*

1. Suppose that $f(z)$ is analytic on the plane, $f(0) = 3 + 4i$, and that $|f(z)| \leq 5$ whenever $|z| < 1$. Find $f'(0)$.

Solution: By the Maximum Modulus Principle (2.15), note that f attains its maximum in the interior of the open unit disc ($|f(0)| = 5$ and $|f(z)| \leq 5$ on the open unit disc). Thus, f is the constant function $f(z) = 3 + 4i$ and so $f'(0) = 0$. ■

2. Let f be an analytic function on the open unit disc D. Moreover, suppose that f is continuous on the closure of D and that f is real valued on the boundary. Show that f is constant.

Solution: Note that on the boundary, f is a real valued function. So the imaginary part of f is 0 on the boundary. Write $f(x+iy) = u(x, y)+iv(x, y)$. Note since f is analytic, f satisfies the Cauchy Riemann Equations and hence both u and v are harmonic (the sums of the double partial derivatives with respect to x and y equal 0). Since $v(x, y)$ is 0 on the boundary, we have by the Maximum Modulus Principle Harmonic version (2.16) that $v(x, y) = 0$ for all $(x, y) \in D$. Thus, f is a function form $\mathbb{C}$ to $\mathbb{R}$. Again, using the Cauchy Riemann Equations gives us that $u_x = u_y = 0$ and so $u(x, y) = c \in \mathbb{R}$ for some c. This shows us that f is constant as required. ■

3. Suppose that $p(z)$ and $q(z)$ are polynomial functions of the same degree with all their zeros inside the unit disc D. Suppose further that $|p(z)| = |q(z)|$ on $|z = 1|$. Show that $q(z) = ap(z)$ with $|a| = 1$.

Solution: Since p and q are of the same degree, the ration $\frac{p}{q}$ has a non-zero finite limit at ∞. Consider the function $f(z) := \frac{p(\frac{1}{z})}{q(\frac{1}{z})}$. This function has a removable singularity at 0. Moreover,

$\frac{1}{f}$ also has this property. Since p and q have no zeros in $|z| \geq 1$, we also have that f and $\frac{1}{f}$ are analytic in a neighbourhood of $|z| \leq 1$. By assumption, f and $\frac{1}{f}$ have unit modulus on $|z| = 1$. By the Maximum Modulus Principle (2.15) we have that $|f(z)| \leq 1$ and $|\frac{1}{f(z)}| \leq 1$ on the closure of the unit disc. Therefore, $|f(z)| = 1$ on D. Thus, f attains its maximum on the interior of D. So the Maximum Modulus Principle applies again telling us that f is constant on D say $f(z) = a$. Note that $1 = |f(z)| = |a|$. Moreover, this means that $p(\frac{1}{z}) = aq(\frac{1}{z})$ and since p and q are of the same degree, we get that $p(z) = aq(z)$ as required. ■

4. Suppose that f is analytic on the open unit disc, continuous on its closure, and satisfies $|f(z)| = 1$ on $|z| = 1$. Show that f is a rational function.

   Solution:

5. Let f be an entire function and suppose $\frac{f(z)}{z} \to 0$ as $|z| \to \infty$. Show that $f(z)$ is constant.

   Solution: Let $g(z) := f(z) - f(0)$. Note that $g(0) = 0$ and that $\frac{g(z)}{z}$ tends to 0 as $|z| \to \infty$. Moreover, we can extend $\frac{g(z)}{z}$ to an entire function as 0 is a removable singularity (then use Riemann's Theorem (2.7)). Call this function $h(z)$. The first part above says that for any $\epsilon > 0$ there is an $R > 0$ such that $|h(z)| < \epsilon$ for all $|z| \geq R$. Now, on the disc $|z| < R$, we can invoke the Maximum Modulus Principle (2.15) (since h is entire) to get that $|h(z)| \leq M$. Note that if $|h(z)| > \epsilon$ inside the disc, then $h(z)$ must be a constant function since it obtains its maximum in the interior of the disc. This will contradict that $|h(z)| < \epsilon$ outside the disc. Hence $M < \epsilon$. Thus $|h(z)| < \epsilon$ everywhere. But ϵ was arbitrary so $h(z) = 0$. Now $\frac{g(z)}{z} = 0$ and thus $g(z) = 0$ for all z. This gives $f(z) = f(0)$ for all z, that is, f is a constant function. ■

6. Suppose that f is analytic on the open connected bounded region A, continuous on its closure, and satisfies $|f(z)| = c$ on its boundary for some real number c. Show that f has a zero or f is constant.

   Solution: Suppose that f has no zeros in A. It suffices to show that f is constant. Notice that $g(z) := \frac{c}{f(z)}$ is analytic on all of A and continuous on its boundary. Moreover on the boundary, $|g(z)| = 1$. Hence by the Maximum Modulus Principle (2.15) we have that $|f(z)| \leq c$ and $|\frac{c}{f(z)}| \leq 1$. This implies that $c \leq |f(z)| \leq c$ on all of A. So $|f(z)| = c$ on A. Thus, a second application of the Maximum Modulus Principle (it attains its max on the interior of A) tells us that f is constant on A as required.

2.5 Schwarz Lemma

Theorem 2.17. *(Schwarz Lemma) Let D be the open unit disc and f a holomorphic map from D to D fixing the origin ($f(0) = 0$). Then*

$$|f(z)| \leq |z| \; \forall z \in D \text{ and}$$
$$|f'(0)| \leq 1$$

Moreover, if $|f(z)| = |z|$ for some nonzero z or if $|f'(0)| = 1$ then f is a rotation, that is $f(z) = az$ for some $a \in \mathbb{C}$ with $|a| = 1$.

1. Suppose that $f(z)$ is analytic inside the unit disc D and continuous on its boundary. Suppose further that $|z| \leq |f(z)| \leq 1$ for all $z \in D$. Find all possible function f.

   Solution: Notice that on the boundary, $1 = |z| \leq |f(z)| \leq 1$ and so $|f(z)| = 1$ on the boundary, that is, it is constant. By a problem in the Maximum Modulus Principle section

(6.), we have that either $f(z) = 1$ or that f has a zero inside the unit disc. By assumption $|z| \leq |f(z)|$ so the only place a zero is possible is at $z = 0$. Thus, f fixes 0 and so we can apply Schwarz Lemma (2.17) to get that $|f(z)| \leq |z|$. Thus, $|z| \leq |f(z)| \leq |z|$ so $|f(z)| = |z|$ for every $z \in D$. By Schwarz Lemma again we have that $f(z) = az$ with $a \in \mathbb{C}$ and $|a| = 1$.

2. Let $\mathbb{H} := \{z|\Im(z) > 0\}$ and suppose that $f : \mathbb{H} \to \mathbb{C}$ is an analytic function such that $|f(z)| < 1$ for all $z \in \mathbb{H}$ and $f(i) = 0$. Show that $|f(2i)| \leq \frac{1}{3}$. Prove that there is a unique function satisfying $f(2i) = \frac{i}{3}$ and find its formula.

   Solution: Let $g(z) := i\frac{1+z}{1-z}$. By the exercises on conformal mappings, we know this map takes D to $\mathbb{H}$. Now note that the map in question takes $\mathbb{H}$ to D so define $h := f \circ g : D \to D$. Notice that $h(0) = f(g(0)) = f(i) = 0$ and hence by Schwarz lemma (2.17) we have for every point on D, $|h(z)| \leq |z|$. Now consider $\frac{1}{3} \geq |h(\frac{1}{3})| = |f(g(\frac{1}{3}))| = |f(2i)|$ as required. If $f(2i) = \frac{i}{3}$ then note that $|h(\frac{1}{3})| = |\frac{1}{3}|$ and hence h is a rotation. So $h(z) = az$. Plugging in $\frac{1}{3}$ yields $\frac{i}{3} = a\frac{1}{3}$ so $a = i$ and hence $h(z) = iz$. Solving using inverses of functions yields $f(z) = \frac{1+zi}{z+i}$. ■

3. Let $H := \{z|\Re(z) > 0\}$ and suppose that $f : H \to \mathbb{C}$ is an analytic function such that $|f(z)| < 1$ for all $z \in \mathbb{H}$ and $f(1) = 0$. What is the largest possible value of $|f'(1)|$?

   Solution: Let $g(z) := \frac{e^{-3\frac{\pi}{2}}z-i}{e^{-3\frac{\pi}{2}}z+i} = \frac{iz-i}{iz+i} = \frac{z-1}{z+1}$ so that $g^{-1}(z) = -\frac{z+1}{z-1}$. By the exercises on conformal mappings, we know this inverse map takes D to H. Now note that the map in question takes H to D so define $h := f \circ g^{-1} : D \to D$. Notice that $h(0) = f(g^{-1}(0)) = f(1) = 0$ and hence by Schwarz lemma (2.17) we have for every point on D, $|h(z)| \leq |z|$ and $|h'(0)| \leq 1$. Notice that $h'(z) = f'(g^{-1}(z))(g^{-1})'(z) = f'(g^{-1}(z))\frac{2}{(z-1)^2}$ giving that $h'(0) = 2f'(1)$ hence $|f'(1)| \leq \frac{1}{2}$ which is achievable. ■

4. Let $f : D \to D$ be a holomorphic map (where D is the unit disc) and suppose that $f(z)$ is not the identity map $f(z) = z$. Prove that f can have at most one fixed point.

   Solution: Suppose that $f(z_1) = z_1$ and $f(z_2) = z_2$ for distinct z_1 and z_2. Take the conformal map from D to D mapping z_1 to 0 automorphically, namely $g(z) := \frac{z-z_1}{1-\overline{z_1}z}$. Note that $h := g \circ f \circ g^{-1}$ is a map from D to D fixing the origin. Hence Schwarz lemma applies and we see that $|h(z)| \leq |z|$ for all $z \in D$. Note that $h(g(z_2)) = g(z_2)$ and $g(z_2) \neq 0$. Schwarz theorem then tells us that h is a rotation (since there is a second point satisfying $|h(z)| = |z|$). Thus, $h(z) = az$. Next, $ag(z_2) = h(g(z_2)) = g(z_2)$ and hence $a = 1$. So $h(z) = z \Rightarrow f(g^{-1}(z)) = g^{-1}(z)$. Since g is an automorphism, we have that f maps D to D identically, that is $f(z) = z$ a contradiction. Hence f has only at most one fixed point as claimed. ■

5. Let $f(z)$ be an analytic function and $|f(z)| \leq 1$ in the unit disc $D \subseteq \mathbb{C}$. Given $z_0 \in D$, find a Möbius transformation (i.e., a transformation of the form $z \mapsto \frac{az+b}{cz+d}$) which maps D to D and sends z_0 to 0. Then show that

$$|\frac{f(z) - f(z_0)}{z - z_0}| \leq \frac{2}{1 - |z_0||z|}$$

   for any $z \in D$.

   Solution: The map as in the section on conformal maps is $g(z) := \frac{z_0-z}{1-\overline{z_0}z}$. Recall that this map is an involution. Let $h(z) := \frac{f(z_0)-z}{1-\overline{f(z_0)}z}$. Notice that this sends the unit disc to itself and $f(z_0)$ to 0. Hence $h \circ f \circ g$ is a map sending 0 to 0. We can now apply Schwarz Lemma (2.17) to get that $|(h \circ f \circ g)(w)| \leq |w|$ for any $w \in D$. Set $z = g^{-1}(w) = g(w)$. Expanding gives

$$|\frac{f(z_0) - f(z)}{1 - \overline{f(z_0)}f(z)}| = |\frac{f(z_0) - f(g(w))}{1 - \overline{f(z_0)}f(g(w))}| = |(h \circ f \circ g)(w)| \leq |w| = |g(z)| = |\frac{z_0 - z}{1 - \overline{z_0}z}|$$
$$\Rightarrow |\frac{f(z_0) - f(z)}{1 - \overline{f(z_0)}f(z)}| \leq |\frac{z_0 - z}{1 - \overline{z_0}z}|$$
$$\Rightarrow |\frac{f(z_0) - f(z)}{z_0 - z}| \leq |\frac{1 - \overline{f(z_0)}f(z)}{1 - \overline{z_0}z}| \leq \frac{1 + |\overline{f(z_0)}||f(z)|}{|1 - \overline{z_0}z|} \leq \frac{2}{1 - |\overline{z_0}z|}$$

which holds since $|f(z)| \leq 1$ for all $z \in D$ and since $|1| \leq |1 - \overline{z_0}z| + |\overline{z_0}z|$ and hence $\frac{1}{|1-\overline{z_0}z|} \leq \frac{1}{1-|\overline{z_0}z|}$. ■

2.6 Rouché's Theorem

Theorem 2.18. *(Rouché's Theorem) Let C be a simply connected region. Then two holomorphic (analytic) functions f and g have the same number of roots if*

$$|f(z) - g(z)| < |f(z)| + |g(z)|$$

holds for all $z \in \partial C$. Equivalently, if f and g satisfies

$$|f(z) + g(z)| < |f(z)|$$

holds for all $z \in \partial C$, then f and g have the same number of roots.

1. (i) Show that all the zeros of the polynomial $f(z) = z^8 - 3z + 1$ lie inside the disc $|z| < \frac{5}{4}$.

   Solution: Let $f(z) := z^8 - 3z + 1$ and $g(z) := -z^8$. Then on the boundary of the disc,

   $$|f(z) + g(z)| = |-3z + 1| \leq 3(\frac{5}{4}) + 1 = \frac{19}{4} < 5 < (\frac{5}{4})^8 = |-z^8| = |g(z)|$$

   So f and g have the same number of roots inside the unit disc by (2.18). Sinze g has eight roots at the origin, we know that f must also have eight roots inside the disc $|z| < \frac{5}{4}$. ■

   (ii) How many zeros lie inside the unit circle?

   Solution: Let $f(z) := z^8 - 3z + 1$ and $g(z) := 3z - 1$. Then on the boundary of the unit disc,

   $$|f(z) + g(z)| = |z^8| = 1 < 2 = |3z| - |1| \leq |3z - 1| = |g(z)|$$

   So f and g have the same number of roots inside the unit disc by (2.18). Sinze g has one root at $\frac{1}{3}$, we know that f must also have one root inside the unit disc. ■

2. (i) Show that all the zeros of the polynomial $f(z) = z^4 - 7z - 1$ lie inside the disc $|z| < 2$.

   Solution: Let $f(z) := z^4 - 7z - 1$ and $g(z) := -z^4$. Then on the boundary of the disc,

   $$|f(z) + g(z)| = |-7z - 1| \leq 7(2) + 1 = 15 < 16 <= |-z^4| = |g(z)|$$

   So f and g have the same number of roots inside the unit disc by (2.18). Sinze g has four roots at the origin, we know that f must also have four roots inside the disc $|z| < 2$. ■

(ii) How many zeros lie inside the unit circle?

Solution: Let $f(z) := z^4 - 7z - 1$ and $g(z) := 7z + 1$. Then on the boundary of the unit disc,

$$|f(z) + g(z)| = |z^4| = 1 < 6 = |7z| - |1| \leq |7z + 1| = |g(z)|$$

So f and g have the same number of roots inside the unit disc by (2.18). Sinze g has one root at $\frac{-1}{7}$, we know that f must also have one root inside the unit disc. ■

3. Let $a > 1$ be a real number. Prove that $ze^{a-z} - 1 = 0$ has one solution inside the unit disc. Show that this solution is real.

Solution: Let $f(z) := ze^{a-z} - 1$ and let $g(z) := -ze^{a-z}$. Then on $|z| = 1$,

$$|f(z) + g(z)| = |-1| = 1 = e^0 < |e^{a-\Re(z)}| = |e^{a-\Re(z)}||e^{-\Im(z)}| = |-z||e^{a-z}| = |g(z)|$$

So f and g have the same number of roots inside the unit disc by (2.18). Sinze g has one root at 0, we know that f must also have one root inside the unit disc. This solution is real by the intermediate value theorem noting that $f(0) = -1 < 0 < e^{a-1} = f(1)$. ■

4. How many zeros of $f(z) = e^z - 2z - 1$ lie inside the unit circle?

Solution: Let $g(z) := 2z$. Then on the boundary of the unit disc,

$$\begin{aligned}|f(z) + g(z)| = |e^z - 1| = |z + \frac{z^2}{2!} + \frac{z^3}{3!} + ...| &\leq |z| + \frac{|z|^2}{2!} + \frac{|z|^3}{3!} + ... \\ &= 1 + \frac{1}{2!} + \frac{1}{3!} + ... = e - 1 < 2 = |g(z)|\end{aligned}$$

So f and g have the same number of roots inside the unit disc by (2.18). Sinze g has one root at 0, we know that f must also have one root inside the unit disc. ■

5. How many zeros of $f(z) = 4z^{100} - e^z$ lie inside the unit circle? How many distinct zeros are there?

Solution: Let $g(z) := 4z^{100}$. Then on the boundary of the unit disc,

$$|f(z) + g(z)| = |-e^z| = |e^{\Re(z)}| < e < 4 = |4z^{100}| = |g(z)|$$

So f and g have the same number of roots inside the unit disc by (2.18). Sinze g has one hundred roots at 0, we know that f must also have one hundred roots inside the unit disc. If the roots are distinct then f' and f do not share any roots. Let x be a root of f inside the unit circle. Then

$$f'(x) = 400x^{99} - e^x = 400x^{99} - 4x^{100} = 4x^{99}(100 - x) \neq 0$$

holding since $x = 0$ nor $x = 100$ are solutions inside the unit disc ($z = 0$ doesn't satisfy the equation and the latter is too big). Thus f has 100 distinct roots inside the unit circle. ■

6. How many zeros of $f(z) = z^6 - 4z^5 + z^2 - 1$ lie inside the unit circle?

Solution: Let $g(z) := 4z^5$. Then on the boundary of the unit disc,

$$|f(z) + g(z)| = |z^6 + z^2 - 1| \leq 3 < 4 = |-4z^5| = |g(z)|$$

So f and g have the same number of roots inside the unit disc by (2.18). Sinze g has five roots at 0, we know that f must also have five roots inside the unit disc. ■

7. How many zeros of $f(z) = z^4 - 5z + 1$ lie inside the annulus $1 < |z| < 2$?

Solution: We break this into two parts, one inside the unit circle and one inside the circle of radius two centres at the origin. Let $g(z) := 5z - 1$. Then on the boundary of the unit disc,

$$|f(z) + g(z)| = |z^4| = 1 < 4 = |5z| - |1| \le |5z - 1| = |g(z)|$$

So f and g have the same number of roots inside the unit disc by (2.18). Sinze g has one root at $\frac{1}{5}$, we know that f must also have one root inside the unit disc.

Lets consider the disc $|z| < 2$. Let $g(z) := -z^4$. Then on the boundary of the unit disc,

$$|f(z) + g(z)| = |5z - 1| \le |5z| + |1| = 11 < 16 = |-z^4| = |g(z)|$$

So f and g have the same number of roots inside the unit disc by (2.18). Sinze g has four roots at 0, we know that f must also have four roots inside the disc $|z| < 2$. Taking the difference yields that there are 3 zeros inside the annulus in question. ■

8. Show that there is exactly one point z in the right half plane $\{z|\Re(z) > 0\}$ for which $z+e^{-z} = 2$.

Solution: Let $f(z) := z + e^{-z} - 2$ and $g(z) := -z + 2$. Consider γ_R to be the semi circle from $-Ri$ to Ri passing entirely in the positive real plane. Now, on $\partial\gamma_R$,

$$|f(z) + g(z)| = |e^{-z}| = e^{-\Re(Z)} \le e^0 = 1$$

I claim $1 < |g(z)|$ whenever $R \ge 4$. For suppose not, then on $\partial\gamma_R \cap \{x = i\}$, we have

$$|g(z)| = |-iy + 2| = \sqrt{y^2 + 4} \ge 2 > 1$$

and on the arc alone,

$$\begin{aligned} 1 \ge |g(z)| = |z - 2| = \sqrt{(\Re(z) - 2)^2 + \Im(z)^2} = \sqrt{R^2 - 4\Re(z) + 4} \\ \Rightarrow R^2 + 3 \le 4\Re(z) \le 4R\# \end{aligned}$$

(the last inequality holds since z is on the boundary of the semicircle and thus cannot have real part bigger than the radius) a contradiction when $R \ge 4$. Thus $1 < |g(z)|$. So f and g have the same number of roots inside the semicircle γ_R by (2.18). Sinze g has one root at 2, we know that f must also have one root inside the semicircle γ_R. Since we can vary R as large as we want, there must only be one root with positive real part. ■

9. Show that there is exactly one point z in the right half plane $\{z|\Re(z) > 0\}$ for which $z+e^{-z} = 2$.

Solution: Let $f(z) := 2e^{-z} - z + 3$ and $g(z) := z - 3$. Consider γ_R to be the semi circle from $-Ri$ to Ri passing entirely in the positive real plane. Now, on $\partial\gamma_R$,

$$|f(z) + g(z)| = |2e^{-z}| = 2e^{-\Re(Z)} \le 2e^0 = 2$$

I claim $2 < |g(z)|$ whenever $R \ge 5$. For suppose not, then on $\partial\gamma_R \cap \{x = i\}$, we have

$$|g(z)| = |-iy + 2| = \sqrt{y^2 + 9} \ge 3 > 2$$

and on the arc alone,

$$\begin{aligned} 1 \ge |g(z)| = |z - 3| = \sqrt{(\Re(z) - 3)^2 + \Im(z)^2} = \sqrt{R^2 - 6\Re(z) + 9} \\ \Rightarrow R^2 + 8 \le 6\Re(z) \le 6R\# \end{aligned}$$

(the last inequality holds since z is on the boundary of the semicircle and thus cannot have real part bigger than the radius) a contradiction when $R \geq 5$. Thus $1 < |g(z)|$. So f and g have the same number of roots inside the semicircle γ_R by (2.18). Sinze g has one root at 3, we know that f must also have one root inside the semicircle γ_R. Since we can vary R as large as we want, there must only be one root with positive real part. ■

10. Prove the fundamental theorem of algebra.

Solution: Let $p(z) := a_n z^n + ... + a_0$ and let $g(z) := -a_n z^n$. Then on the boundary of the circle centred at the origin of radius R,

$$|p(z) + g(z)| = |a_{n-1}z^{n-1} + ... + a_0| \leq |a_{n-1}|R^{n-1} + ... + |a_0| \leq MR^{n-1}$$

where $M = \max_{i=1..n-1} |a_i|$. So if R was such that $\frac{M}{|a_n|} < R$ then

$$|p(z) + g(z)| \leq MR^{n-1} < |a_n|R^n = |g(z)|$$

So p and g have the same number of roots inside $|z| < R$ by (2.18). Sinze g has n roots at 0, we know that p must also have$n$ roots inside $|z| < R$. ■

11. Let f be analytic in an open set containing the closed unit disc. Suppose that $|f(z)| > 2$ for $|z| = 1$ and that $|f(0)| < 2$. Prove that f has at least one zero in the open disc $|z| < 1$.

Solution: Let $g(z) := f(0) - f(z)$. Then on $|z| = 1$,

$$|f(z) + g(z)| = |f(0)| < 2 < |f(z)|$$

So f and g have the same number of roots inside the unit disc by (2.18). Sinze g has at least one root at $z = 0$, we know that f must also have at least one root inside the unit disc. ■

2.7 Residue Theorem

Theorem 2.19. *Let $f(z)$ be a complex meromorphic (analytic except at a finite number of isolated poles) function with a pole of order n at c. Then the residue of f at c is equal to*

$$\text{Res}(f, c) = \frac{1}{(n-1)!} \lim_{z \to c} \frac{d^{n-1}}{dz^{n-1}}((z-c)^n f(z))$$

Theorem 2.20. *(The Residue Theorem) Suppose U is a simply connected open subset of the complex plane. Further, suppose $a_1, ..., a_n \in U$ and f is a complex function which is defined and holomorphic on $U \backslash \{a_1, ..., a_n\}$. If C is a rectifiable curve (ie finite arclength) in U which bound the a_k, but does not meet any a_k and whose start and end points are equal, then*

$$\oint_C f(z)dz = 2\pi i \sum_{i=1}^{n} \text{I}(C, a_i)\text{Res}(f, a_i)$$

where $I(C, x)$ denotes the winding number.

1. Evaluate the following integrals

   (i) $\oint_C \frac{\sin(3z)}{(z-1)^4} dz$, where C is the circle $|z| = 2$ oriented counterclockwise.

   Solution: Here we use the residue theorem. Let $f(z) := \frac{\sin(3z)}{(z-1)^4}$. Notice that $z = 1$ is a removable pole of f. By (2.19), we have

$$\begin{aligned}\operatorname{Res}(f,1) &= \frac{1}{(4-1)!}\lim_{z\to 1}\frac{d^{4-1}}{dz^{4-1}}((z-1)^4 f(z)) \\ &= \frac{1}{6}\lim_{z\to 1}\frac{d^3}{dz^3}(\sin(3z)) \\ &= \frac{1}{6}\lim_{z\to 1} -27\cos(3z) \\ &= \frac{-9}{2}\cos(3)\end{aligned}$$

Hence by the residue theorem (2.20), we have

$$\oint_C f(z)dz = 2\pi i \operatorname{Res}(f,1) = -9\pi i\cos(3)$$

■

2.8 Contour Integration

Theorem 2.21. *Let f be a complex valued continuous function on a contour C. Suppose that $|f(z)| \le M$ for some $M \in \mathbb{R}$ for all $z \in C$. Then*

$$\left|\int_C f(z)dz\right| \le M l(C)$$

where $l(C)$ denotes the arc length of C. Note one may choose $M := \max_{z\in C}|f(z)|$.

Theorem 2.22. *Let $n \in \mathbb{N}$. Then*

$$\lim_{x\to 0}\frac{x\log(x)^n}{1+x^2} = 0$$

Proof. Suppose n is odd. Note that for $x \in (0,1)$,

$$x\log(x)^n \le \frac{x\log(x)^n}{1+x^2} \le 0$$

Next by L'Hopitals Rule, we have

$$\lim_{x\to 0} x\log(x)^n = \lim_{x\to 0}\frac{\log(x)^n}{\frac{1}{x}} = \lim_{x\to 0}\frac{\frac{n\log(x)^{n-1}}{x}}{\frac{-1}{x^2}} = \lim_{x\to 0}\frac{n\log(x)^{n-1}}{\frac{-1}{x}} = \dots = \lim_{x\to 0}(n!)x = 0$$

An application of the squeeze theorem completes the proof for odd n. Now for even n, note that

$$0 \le \frac{x\log(x)^n}{1+x^2} \le x\log(x)^n$$

and the same argument above finishes this proof.

1. Evaluate $\int_0^\infty \frac{x^2}{1+x^6}dx$.

   Solution: Let γ_R be the semicircle in the upper half plane with radius R. Let C_R represent the arc of the semi circle and L_R the straight line of the semicircle (coinsiding with the real axis). First, note that

$$\int_{\gamma_R}\frac{z^2}{1+z^6}dz = \int_{C_R}\frac{z^2}{1+z^6}dz + \int_{L_R}\frac{z^2}{1+z^6}dz$$

Next, consider the first integrand. We know that by the Estimation Lemma (2.21)

$$|\int_{C_R} \frac{z^2}{1+z^6}dz| \leq \frac{R^2}{1+R^6}R\pi \overset{R\to\infty}{\longrightarrow} 0$$

Now we set up the Residue Theorem (2.20). For x^6+1 we see that the zeroes that lie in γ_R are precisely $i, i\zeta_6$ and $i\zeta_6^5$ where ζ_6 is a primitive sixth root of unity. We need to evaluate the residues at these points. Notice that these are simple poles and thus,

$$\begin{aligned}
\int_{\gamma_R} \frac{z^2}{1+z^6}dz &= 2\pi i \left(\frac{(i)^2}{\prod\limits_{k=1}^{5}(i - i\zeta_6^k)} + \frac{(i\zeta_6)^2}{\prod\limits_{\substack{k=0\\k\neq 1}}^{5}(i\zeta_6 - i\zeta_6^k)} + \frac{(i\zeta_6^5)^2}{\prod\limits_{\substack{k=0\\k\neq 5}}^{5}(i\zeta_6^5 - i\zeta_6^k)} \right) \\
&= 2\pi i \left(\frac{-1}{i\prod\limits_{k=1}^{5}(1 - 1\zeta_6^k)} + \frac{-\zeta_6^2}{i\zeta_6^5\prod\limits_{k=1}^{5}(1 - \zeta_6^k)} + \frac{-\zeta_6^4}{i\zeta_6^{25}\prod\limits_{k=1}^{5}(1 - \zeta_6^k)} \right) \\
&= 2\pi(\frac{-1}{6} + \frac{-\zeta_6^3}{6} + \frac{-\zeta_6^3}{6}) \\
&= 2\pi(\frac{-1}{6} + \frac{1}{6} + \frac{1}{6}) \\
&= \frac{\pi}{3}
\end{aligned}$$

Combining gives us

$$\begin{aligned}
\frac{\pi}{3} = \lim_{R\to\infty}\frac{\pi}{3} = \lim_{R\to\infty}\int_{\gamma_R}\frac{z^2}{1+z^6}dz &= \lim_{R\to\infty}\int_{C_R}\frac{z^2}{1+z^6}dz + \lim_{R\to\infty}\int_{L_R}\frac{z^2}{1+z^6}dz \\
&= \lim_{R\to\infty}\int_{-R}^{R}\frac{z^2}{1+z^6}dz \\
&= 2\lim_{R\to\infty}\int_{0}^{R}\frac{z^2}{1+z^6}dz \\
&= 2\int_{0}^{\infty}\frac{z^2}{1+z^6}dz \\
\Rightarrow \frac{\pi}{6} &= \int_{0}^{\infty}\frac{z^2}{1+z^6}dz
\end{aligned}$$

as required. ■

2. Evaluate $\int_0^\infty \frac{x^2}{x^4+5x^2+6}dx$.

Solution: Let γ_R be the semicircle in the upper half plane with radius R. Let C_R represent the arc of the semi circle and L_R the straight line of the semicircle (coinsiding with the real axis). First, note that

$$\int_{\gamma_R}\frac{z^2}{z^4+5z^2+6}dz = \int_{C_R}\frac{z^2}{z^4+5z^2+6}dz + \int_{L_R}\frac{z^2}{z^4+5z^2+6}dz$$

Next, consider the first integrand. We know that by the Estimation Lemma (2.21)

$$|\int_{C_R} \frac{z^2}{z^4+5z^2+6}dz| \leq \frac{R^2}{R^4+5R^2+6}R\pi \overset{R\to\infty}{\longrightarrow} 0$$

Now we set up the Residue Theorem (2.20). For x^4+5x^2+6 we see that the zeroes that lie in γ_R are precisely $i\sqrt{2}$ and $i\sqrt{3}$. We need to evaluate the residues at these points. Notice that these are simple poles and thus,

$$\begin{aligned}
\int_{\gamma_R} \frac{z^2}{z^4+5z^2+6}dz &= 2\pi i\left(\frac{(i\sqrt{2})^2}{(i\sqrt{2}+i\sqrt{2})(i\sqrt{2}-i\sqrt{3})(i\sqrt{2}+i\sqrt{3})}\right)\\
&+2\pi i\left(\frac{(i\sqrt{3})^2}{(i\sqrt{3}+i\sqrt{2})(i\sqrt{3}-i\sqrt{2})(i\sqrt{3}+i\sqrt{3})}\right)\\
&=2\pi i(\frac{-2}{-i(2\sqrt{2})(\sqrt{2}-\sqrt{3})(\sqrt{2}+\sqrt{3})}+\frac{-3}{-i(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{2})(2\sqrt{3})})\\
&=2\pi i(\frac{-2}{-i(2\sqrt{2})(-1)}+\frac{-3}{-i(1)(2\sqrt{3})})\\
&=2\pi(\frac{-1}{\sqrt{2}}+\frac{3}{2\sqrt{3}})\\
&=2\pi(\frac{-3\sqrt{2}}{6}+\frac{3\sqrt{3}}{6})\\
&=\pi(\sqrt{3}-\sqrt{2})
\end{aligned}$$

Combining gives us

$$\begin{aligned}
\pi(\sqrt{3}-\sqrt{2}) = \lim_{R\to\infty}\pi(\sqrt{3}-\sqrt{2}) &= \lim_{R\to\infty}\int_{\gamma_R}\frac{z^2}{z^4+5z^2+6}dz\\
&=\lim_{R\to\infty}\int_{C_R}\frac{z^2}{z^4+5z^2+6}dz+\lim_{R\to\infty}\int_{L_R}\frac{z^2}{z^4+5z^2+6}dz\\
&=\lim_{R\to\infty}\int_{-R}^{R}\frac{z^2}{z^4+5z^2+6}dz\\
&=2\lim_{R\to\infty}\int_{0}^{R}\frac{z^2}{z^4+5z^2+6}dz\\
&=2\int_0^\infty\frac{z^2}{z^4+5z^2+6}dz\\
\Rightarrow \frac{\pi}{2}(\sqrt{3}-\sqrt{2}) &= \int_0^\infty\frac{z^2}{z^4+5z^2+6}dz
\end{aligned}$$

3. Evaluate $\int_0^\infty \frac{1}{1+x^4}dx$.

Solution: Let γ_R be the semicircle in the upper half plane with radius R. Let C_R represent the arc of the semi circle and L_R the straight line of the semicircle (coinsiding with the real axis). First, note that

$$\int_{\gamma_R}\frac{1}{z^4+1}dz = \int_{C_R}\frac{1}{z^4+1}dz+\int_{L_R}\frac{1}{z^4+1}dz$$

Next, consider the first integrand. We know that by the Estimation Lemma (2.21)

$$|\int_{C_R} \frac{1}{z^4+1} dz| \le \frac{1}{R^4+1} R\pi \overset{R\to\infty}{\longrightarrow} 0$$

Now we set up the Residue Theorem (2.20). For x^4+1 we see that the zeroes that lie in γ_R are precisely $\pm\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i = \frac{(\pm 1+i)\sqrt{2}}{2}$. We need to evaluate the residues at these points. Notice that these are simple poles and thus,

$$\begin{aligned}
\int_{\gamma_R} \frac{1}{z^4+1} dz &= 2\pi i \left(\frac{1}{(\frac{(1+i)\sqrt{2}}{2} - \frac{(1-i)\sqrt{2}}{2})(\frac{(1+i)\sqrt{2}}{2} - \frac{(-1+i)\sqrt{2}}{2})(\frac{(1+i)\sqrt{2}}{2} - \frac{(-1-i)\sqrt{2}}{2})} \right) \\
&+ 2\pi i \left(\frac{1}{(\frac{(-1+i)\sqrt{2}}{2} - \frac{(1+i)\sqrt{2}}{2})(\frac{(-1+i)\sqrt{2}}{2} - \frac{(1-i)\sqrt{2}}{2})(\frac{(-1+i)\sqrt{2}}{2} - \frac{(-1-i)\sqrt{2}}{2})} \right) \\
&= 2\pi i \left(\frac{4}{\sqrt{2}(2i)(2)(2+2i)} + \frac{4}{\sqrt{2}(-2)(-2+2i)(2i)} \right) \\
&= 2\pi i \left(\frac{1}{2\sqrt{2}(-1+i)} + \frac{1}{2\sqrt{2}(1+i)} \right) \\
&= 2\pi i \left(\frac{(-1-i)}{4\sqrt{2}} + \frac{(1-i)}{4\sqrt{2}} \right) \\
&= 2\pi i \left(\frac{(-1-i)}{4\sqrt{2}} + \frac{(1-i)}{4\sqrt{2}} \right) \\
&= \pi \frac{\sqrt{2}}{2}
\end{aligned}$$

Combining gives us

$$\begin{aligned}
\pi \frac{\sqrt{2}}{2} = \lim_{R\to\infty} \pi \frac{\sqrt{2}}{2} &= \lim_{R\to\infty} \int_{\gamma_R} \frac{1}{z^4+1} dz \\
&= \lim_{R\to\infty} \int_{C_R} \frac{1}{z^4+1} dz + \lim_{R\to\infty} \int_{L_R} \frac{1}{z^4+1} dz \\
&= \lim_{R\to\infty} \int_{-R}^{R} \frac{1}{z^4+1} dz \\
&= 2 \lim_{R\to\infty} \int_{0}^{R} \frac{1}{z^4+1} dz \\
&= 2 \int_{0}^{\infty} \frac{1}{z^4+1} dz \\
\Rightarrow \pi \frac{\sqrt{2}}{4} &= \int_{0}^{\infty} \frac{1}{z^4+1} dz
\end{aligned}$$

as required. ∎

4. Evaluate $\int_{-\infty}^{\infty} \frac{1}{(4+x^2)^3} dx$.

Solution: Let γ_R be the semicircle in the upper half plane with radius R. Let C_R represent the arc of the semi circle and L_R the straight line of the semicircle (coinsiding with the real axis). First, note that

$$\int_{\gamma_R} \frac{1}{(4+z^2)^3}dz = \int_{C_R} \frac{1}{(4+z^2)^3}dz + \int_{L_R} \frac{1}{(4+z^2)^3}dz$$

Next, consider the first integrand. We know that by the Estimation Lemma (2.21)

$$|\int_{C_R} \frac{1}{(4+z^2)^3}dz| \leq \frac{1}{(4+R^2)^3}dzR\pi \overset{R\to\infty}{\longrightarrow} 0$$

Now we set up the Residue Theorem (2.20). For $(4+x^2)^3$ we see that the zeroes that lie in γ_R are precisely $2i$ repeated 3 times. We need to evaluate the residues at this point. Using the residue formula above (2.19),

$$\begin{aligned}
\int_{\gamma_R} \frac{1}{(4+z^2)^3}dz &= 2\pi i\left(\frac{1}{(3-1)!}\lim_{z\to 2i}\frac{d^{3-1}}{dz^{3-1}}\frac{1}{(z+2i)^3}\right)\\
&= 2\pi i\left(\frac{12}{2(2i+2i)^5}\right)\\
&= 2\pi i\left(\frac{3}{512i}\right)\\
&= \pi\frac{3}{256}
\end{aligned}$$

Combining gives us

$$\begin{aligned}
\pi\frac{3}{256} = \lim_{R\to\infty}\pi\frac{3}{256} &= \lim_{R\to\infty}\int_{\gamma_R}\frac{1}{z^4+1}dz\\
&= \lim_{R\to\infty}\int_{C_R}\frac{1}{z^4+1}dz + \lim_{R\to\infty}\int_{L_R}\frac{1}{z^4+1}dz\\
&= \lim_{R\to\infty}\int_{-R}^{R}\frac{1}{z^4+1}dz\\
&= \int_{-\infty}^{\infty}\frac{1}{z^4+1}dz\\
\Rightarrow \pi\frac{3}{256} &= \int_{-\infty}^{\infty}\frac{1}{z^4+1}dz
\end{aligned}$$

as required. ■

5. Evaluate $\int_0^\infty \frac{1}{\sqrt{x}(1+x^2)}dx$.

Solution: We have a lot of things to consider here. Firstly, note that $\sqrt{x}$ requires that we specify a branch for evaluation. We will choose the positive x-axis for reason that will be made manifest later. To solve this integral, we will use a *key hole* contour. Draw a large circle starting at (but not touching) the x-axis. Call this circle Γ and suppose it has radius R. Next, create a small circle of radius ϵ around the point 0 starting at the x-axis (but not touching it). Call this circle γ. So you picture right now should look like two *pacman* like figures almost but not quite touching the x-axis. Lastly, connect the remaining ends of the small circle horizontally with straight lines to the big circle. Your picture should look like a keyhole facing the right side of your page. Call the keyhold K. This gives us the following:

$$\int_K \frac{1}{\sqrt{z}(1+z^2)}dz = \int_\gamma \frac{1}{\sqrt{z}(1+z^2)}dz + \int_\Gamma \frac{1}{\sqrt{z}(1+z^2)}dz$$
$$+ \int_\epsilon^R \frac{1}{\sqrt{z}(1+z^2)}dz + \int_R^\epsilon \frac{1}{\sqrt{z}(1+z^2)}dz$$

Consider the first two integrals as both $\epsilon \to 0$ and $R \to \infty$. We have that by the Estimation Lemma (2.21)

$$|\int_\gamma \frac{1}{\sqrt{z}(1+z^2)}dz| \leq \frac{1}{\sqrt{\epsilon}(1+\epsilon^2)}(2\epsilon\pi) \overset{\epsilon\to 0}{\to} 0$$
$$|\int_\Gamma \frac{1}{\sqrt{z}(1+z^2)}dz| \leq \frac{1}{\sqrt{R}(1+R^2)}(2R\pi) \overset{R\to\infty}{\to} 0$$

This leaves only the two inside integrals to evaluate. Consider the two pieces we haven't looked at. Notice that they are NOT the negative of each other. This is due to our branch choice. We pick up an extra value of 2π as we traverse the outer circle (for example) in the argument of z.

$$\begin{aligned}
\int_R^\epsilon \frac{1}{\sqrt{z}(1+z^2)}dz &= \int_R^\epsilon \frac{e^{-\frac{1}{2}\log|z| - \frac{1}{2}i\arg(z)}}{(1+z^2)}dz \\
&= \int_R^\epsilon \frac{e^{-\frac{1}{2}\log|z| - \frac{1}{2}i(2\pi)}}{(1+z^2)}dz \\
&= \int_R^\epsilon \frac{-e^{-\frac{1}{2}\log|z|}}{(1+z^2)}dz \\
&= \int_\epsilon^R \frac{e^{-\frac{1}{2}\log|z|}}{(1+z^2)}dz \\
&= \int_\epsilon^R \frac{1}{\sqrt{z}(1+z^2)}dz
\end{aligned}$$

Notice for the last equality, the argument of z is 0 so these two integrals are equal. Thus, taking the limits as $\epsilon \to 0$ and $R \to \infty$ gives us

$$\int_K \frac{1}{\sqrt{z}(1+z^2)}dz = 2\int_\epsilon^R \frac{1}{\sqrt{z}(1+z^2)}dz$$

All that's left is an application of the residue theorem. Notice that when we take the square root of a complex number we wish to consider the principle value of it. Roughly speaking, if we want the square root of $a \in \mathbb{C}$, draw it on the plane then take the value corresponding to half the angle from the positive real axis. Other things to note about complex number square roots include that $\sqrt{ab} \neq \sqrt{a}\sqrt{b}$ for complex a, b, necessairly due to the nature of the branch cut. We might introduce extra values of 2π amongst other problems. Basically, when dealing with roots of complex numbers in these computations, the best bet is to evaluate it immediately and deal with math in a 'normal' setting. With this caveat in place, we note that $\sqrt{i} = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$ and $\sqrt{-i} = -\frac{1}{\sqrt{2}} + \frac{1}{2}i$. Both roots i and $-i$ are in our keyhole region. So, by the Residue Theorem (2.20),

$$
\begin{aligned}
\int_K \frac{1}{\sqrt{z}(1+z^2)}dz &= 2\pi i \left(\frac{1}{\sqrt{i}(i+i)} + \frac{1}{\sqrt{-i}(-i-i)} \right) \\
&= 2\pi i \left(\frac{\sqrt{2}}{(1+i)(2i)} + \frac{\sqrt{2}}{(-1+i)(-2i)} \right) \\
&= 2\pi i \left(\frac{\sqrt{2}}{(-2+2i)} + \frac{\sqrt{2}}{(2+2i)} \right) \\
&= 2\pi i \left(\frac{\sqrt{2}(-2-2i)}{8} + \frac{\sqrt{2}(2-2i)}{8} \right) \\
&= 2\pi i \left(\frac{-4\sqrt{2}i}{8} \right) \\
&= \sqrt{2}\pi
\end{aligned}
$$

Substituting into the above (after taking limits) yields

$$
\int_0^\infty \frac{1}{\sqrt{z}(1+z^2)}dz = \frac{\sqrt{2}}{2}\pi
$$

as required. ■

6. Evaluate $\int_0^\infty \frac{x^{\frac{1}{3}}}{1+x^2}dx$.

Solution: We start off by defining the key hole region

(i) Curve γ_1 is $z = x$ where x goes from ϵ to R.
(ii) Curve γ_2 is $z = Re^{it}$ where t goes from 0 to 2π.
(iii) Curve γ_3 is $z = 2\pi ix$ where x goes from R to ϵ (remember we introduce a 2π).
(iv) Curve γ_4 is $z = \epsilon e^{it}$ where t goes from 2π to 0.

Calling the combined region K, we have

$$
\begin{aligned}
\int_K \frac{z^{\frac{1}{3}}}{1+z^2}dz = \int_{\gamma_2} \frac{z^{\frac{1}{3}}}{1+z^2}dz + \int_{\gamma_4} \frac{z^{\frac{1}{3}}}{1+z^2}dz \\
+ \int_\epsilon^R \frac{z^{\frac{1}{3}}}{1+z^2}dz + \int_R^\epsilon \frac{z^{\frac{1}{3}}}{1+z^2}dz
\end{aligned}
$$

Consider the first two integrals as both $\epsilon \to 0$ and $R \to \infty$. We have that by the Estimation Lemma (2.21)

$$
\begin{aligned}
|\int_{\gamma_2} \frac{z^{\frac{1}{3}}}{1+z^2}dz| \leq \frac{(\epsilon)^{\frac{1}{3}}}{1+(\epsilon^2}dz(2\epsilon\pi) \overset{\epsilon\to 0}{\to} 0 \\
|\int_{\gamma_4} \frac{z^{\frac{1}{3}}}{1+z^2}dz| \leq \frac{R^{\frac{1}{3}}}{1+R^2}dz(2R\pi) \overset{R\to\infty}{\to} 0
\end{aligned}
$$

This leaves only the two inside integrals to evaluate. Consider the two pieces we haven't looked at. Notice that they are *NOT* the negative of each other. This is due to our branch choice. We pick up an extra value of 2π as we traverse the outer circle (for example) in the argument of z.

$$\begin{aligned}
\int_R^\epsilon \frac{z^{\frac{1}{3}}}{1+z^2}dz &= \int_R^\epsilon \frac{e^{\frac{1}{3}\log|z|+\frac{1}{3}i\arg(z)}}{1+z^2}dz \\
&= \int_R^\epsilon \frac{e^{\frac{1}{3}\log|z|+\frac{1}{3}i(2\pi)}}{1+z^2}dz \\
&= e^{\frac{2}{3}\pi i}\int_R^\epsilon \frac{e^{\frac{1}{3}\log|z|}}{1+z^2}dz \\
&= -e^{\frac{2}{3}\pi i}\int_\epsilon^R \frac{e^{\frac{1}{3}\log|z|}}{1+z^2}dz \\
&= -e^{\frac{2}{3}\pi i}\int_\epsilon^R \frac{z^{\frac{1}{3}}}{1+z^2}dz
\end{aligned}$$

Notice for the last equality, the argument of z is 0 so these two integrals are equal. Thus, taking the limits as $\epsilon \to 0$ and $R \to \infty$ gives us

$$\int_K \frac{z^{\frac{1}{3}}}{1+z^2}dz = (1-e^{\frac{2}{3}\pi i})\int_\epsilon^R \frac{z^{\frac{1}{3}}}{1+z^2}dz$$

All that's left is an application of the residue theorem. We note that $\sqrt[3]{i} = -i\zeta_3$ and $\sqrt[3]{-i} = i$ where ζ_3 denotes a primitive third root of unity. Both roots i and $-i$ are in our keyhole region. So, by the Residue Theorem (2.20),

$$\begin{aligned}
\int_K \frac{z^{\frac{1}{3}}}{1+z^2}dz &= 2\pi i\left(\frac{\sqrt[3]{i}}{i+i}+\frac{\sqrt[3]{-i}}{-i-i}\right) = 2\pi i\left(\frac{-i\zeta_3-i}{2i}\right) = 2\pi i\left(\frac{-\zeta_3-1}{2}\right) \\
&= \zeta_3^2\pi i = e^{\frac{4}{3}\pi i}\pi i
\end{aligned}$$

Substituting into the above (after taking limits) yields

$$\begin{aligned}
\int_0^\infty \frac{z^{\frac{1}{3}}}{1+z^2}dz &= \frac{e^{\frac{4}{3}\pi i}\pi i}{1-e^{\frac{2}{3}\pi i}} = \frac{e^{\frac{4}{3}\pi i}\pi i(1-e^{\frac{4}{3}\pi i})}{3} = \frac{\pi i(e^{\frac{4}{3}\pi i}-e^{\frac{2}{3}\pi i})}{3} \\
&= \frac{\pi i(2e^{\frac{4}{3}\pi i}-1)}{3} = \frac{\pi i(2(\cos(\frac{4}{3}\pi)+\sin(\frac{4}{3}\pi)i)-1)}{3} \\
&= \frac{\pi i(2(\frac{1}{2}-\frac{\sqrt{3}}{2}i)-1)}{3} = \frac{\pi\sqrt{3}}{3}
\end{aligned}$$

as required. ■

7. Evaluate $\int_0^\infty \frac{x^p}{1+x^2}dx$ where $0 < p < 1$.

Solution: It turns out that the above construction generalizes nicely. This will also work for negative values of p with $0 < |p| < 1$. The key changes in the above argument come with the residue computation and the simplification of the two straight lines in the key hole contour. I'm only including this problem because I saw it on a comp and it might help to double check answers in the end.

$$\begin{aligned}\int_R^\epsilon \frac{z^p}{1+z^2}dz &= \int_R^\epsilon \frac{e^{p\log|z|+pi\arg(z)}}{1+z^2}dz \\ &= \int_R^\epsilon \frac{e^{p\log|z|+pi(2\pi)}}{1+z^2}dz \\ &= e^{2p\pi i}\int_R^\epsilon \frac{e^{p\log|z|}}{1+z^2}dz \\ &= -e^{2p\pi i}\int_\epsilon^R \frac{e^{p\log|z|}}{1+z^2}dz \\ &= -e^{2p\pi i}\int_\epsilon^R \frac{z^p}{1+z^2}dz\end{aligned}$$

and the residue computation yields (see 2.20), using the fact that $i = e^{\frac{\pi i}{2}}$, $-i = e^{\frac{3\pi i}{2}}$, and $\sin(x) = \frac{e^{ix}-e^{-ix}}{2i}$,

$$\int_K \frac{z^p}{1+z^2}dz = 2\pi i\left(\frac{e^{\frac{p\pi i}{2}}}{i+i} + \frac{e^{\frac{-3p\pi i}{2}}}{-i-i}\right) = -2\pi i e^{p\pi i}\left(\frac{e^{\frac{p\pi i}{2}} - e^{\frac{-p\pi i}{2}}}{2i}\right) = -2\pi i e^{p\pi i}\sin(\frac{p\pi}{2})$$

This with the argument from the previous problem gives

$$(1-e^{2p\pi i})\int_0^\infty \frac{z^p}{1+z^2}dz = -2\pi i e^{p\pi i}\sin(\frac{p\pi}{2})$$

Note that

$$(1-e^{2p\pi i}) = e^{p\pi i}(e^{-p\pi i}-e^{p\pi i}) = -2ie^{p\pi i}\sin(p\pi) = -2ie^{p\pi i}(2\sin(\frac{p\pi}{2})\cos(\frac{p\pi}{2}))$$

Equating and simplifying yields

$$\int_0^\infty \frac{z^p}{1+z^2}dz = \frac{-2\pi i e^{p\pi i}\sin(\frac{p\pi}{2})}{-2ie^{p\pi i}(2\sin(\frac{p\pi}{2})\cos(\frac{p\pi}{2}))} = \frac{\pi\sec(\frac{p\pi}{2})}{2}$$

8. Evaluate $\int_{-\pi}^{\pi} \frac{1}{5+3\cos(x)}dx$.

Solution: To solve problems that are polynomial in only trigonometric problems, we need to use one of the identities

$$\cos(x) = \frac{e^{ix}+e^{-ix}}{2} \qquad\qquad \sin(x) = \frac{e^{ix}-e^{-ix}}{2}$$

derivable from $e^{ix} = \cos(x) + i\sin(x)$. Using this substitution and setting $z = e^{ix}$, we get

$$\int_\gamma \frac{1}{5+3\cos(x)}dx = \int_\gamma \frac{1}{5+3\frac{z+\frac{1}{z}}{2}}\frac{dz}{iz} = \int_\gamma \frac{-2i}{3z^2+10z+3}dz = \int_\gamma \frac{-2i}{3(z+\frac{1}{3})(z+3)}dz$$

where γ represents the unit circle. The only residue we need to consider is at $z = -\frac{1}{3}$ and so by the Residue Theorem (2.20),

$$\int_\gamma \frac{-2i}{3(z+\frac{1}{3})(z+3)}dz = 2\pi\frac{-2i}{3(\frac{-1}{3}+3)} = 4\pi(\frac{1}{8}) = \frac{\pi}{2}$$

Hence

$$\int_{-\pi}^{\pi} \frac{1}{5+3\cos(x)}dx = \frac{\pi}{2}$$

as required. ■

9. Let $0 < b < a$ be real numbers. Evaluate $\int_0^{2\pi} \frac{1}{(a+b\cos(x))^2} dx$.

Solution: Let $z = e^{ix}$. Then $\cos(x) = \frac{z+z^{-1}}{2}$ and $dx = \frac{dz}{iz}$. Substituting gives the integral

$$\int_0^{2\pi} \frac{1}{(a+b\cos(x))^2} dx = \int_{|z|=1} \frac{1}{(a+b(\frac{z+z^{-1}}{2}))^2} \frac{dz}{iz} = \frac{4}{ib^2} \int_{|z|=1} \frac{zdz}{(z^2+\frac{2a}{b}z+1)^2}$$

Now we apply the Residue Theorem (2.20). First we examine which poles lies within the unit circle. The roots of the denominator are

$$\lambda_\pm = \frac{-a \pm \sqrt{a^2-b^2}}{b}$$

Examining the absolute value, we see that

$$|\lambda_-| = \frac{a+\sqrt{a^2-b^2}}{b} > \frac{b+\sqrt{a^2-b^2}}{b} > \frac{b}{b} = 1$$

So this root is outside the unit circle. As for the other,

$$|\lambda_+| = \left| \frac{-a+\sqrt{a^2-b^2}}{b} \right| < \frac{a-\sqrt{(a-b)^2}}{b} = 1$$

and thus we have one pole inside the unit circle. Hence, the residue at λ_+ is

$$\begin{aligned}
\operatorname{Res}(f, \lambda_+) &= \frac{1}{(2-1)!} \lim_{z\to\lambda_+} \frac{d^{2-1}}{dz^{2-1}}((z-\lambda_+)^2 f(z)) \\
&= \lim_{z\to\lambda_+} \frac{d}{dz}(\frac{z}{(z-\lambda_-)^2}) \\
&= \lim_{z\to\lambda_+} \frac{(z-\lambda_-)^2 - 2z(z-\lambda_-)}{(z-\lambda_-)^4} \\
&= \lim_{z\to\lambda_+} \frac{-z-\lambda_-}{(z-\lambda_-)^3} \\
&= \frac{\frac{2a}{b}}{\frac{8\sqrt{a^2-b^2}}{b^3}} \\
&= \frac{ab^2}{4\sqrt{a^2-b^2}^3}
\end{aligned}$$

and the Residue theorem gives us

$$\int_0^{2\pi} \frac{1}{(a+b\cos(x))^2} dx = \frac{4}{ib^2}(2\pi i)\frac{ab^2}{4\sqrt{a^2-b^2}^3} = \frac{2a\pi}{\sqrt{a^2-b^2}^3}$$

as reqiured. ■

10. Evaluate $\int_{-\infty}^{\infty} \frac{\cos(\alpha x)}{1+x^2} dx$ for some positive real α.

Solution: Let γ_R be the upper half semi-circle. Notice that

$$\int_{\gamma_R} \frac{\cos(\alpha z)}{1+z^2} dz = \int_{\gamma_R} \frac{\Re(e^{\alpha iz})}{1+z^2} dz = \Re\left(\int_{\gamma_R} \frac{e^{\alpha iz}}{1+z^2} dz\right)$$

So we evaluate the last integral. First note that if C represents the arc of the upper half circle,

$$\int_{\gamma_R} \frac{e^{\alpha iz}}{1+z^2}dz = \int_C \frac{e^{\alpha iz}}{1+z^2}dz + \int_{-R}^{R} \frac{e^{\alpha iz}}{1+z^2}dz$$

Now, by the Estimation Lemma (2.21), since $|e^{\alpha iz}| \leq 1$ on the upper half plane, we have

$$|\int_C \frac{e^{\alpha iz}}{1+z^2}dz| \leq \frac{1}{1+R^2}R\pi \overset{R\to\infty}{\longrightarrow} 0$$

Now we apply the residue theorem (2.20). Notice that the only root in the upper half circle is i and so

$$\int_{\gamma_R} \frac{e^{\alpha iz}}{1+z^2}dz = 2\pi i \frac{e^{\alpha i(i)}}{i+i} = \pi e^{-\alpha}$$

Taking the real part and limiting as $R \to \infty$ yields

$$\int_{-\infty}^{\infty} \frac{\cos(\alpha z)}{1+z^2}dz = \pi e^{-\alpha}$$

as required (note if $\alpha < 0$, just use the lower half circle and get the same answer, making the general answer $\pi e^{-|\alpha|}$). ■

11. Evaluate $\int_0^\infty \frac{\cos(x)}{9+x^2}dx$.

Solution: First note that since the function in question is an even function,

$$\int_0^\infty \frac{\cos(x)}{9+x^2}dx = \frac{1}{2}\int_{-\infty}^{\infty} \frac{\cos(x)}{9+x^2}dx$$

So it suffices to evaluate the second integral. Let γ_R be the upper half semi-circle. Notice that

$$\int_{\gamma_R} \frac{\cos(z)}{9+z^2}dz = \int_{\gamma_R} \frac{\Re(e^{iz})}{9+z^2}dz = \Re\left(\int_{\gamma_R} \frac{e^{iz}}{9+z^2}dz\right)$$

So we evaluate the last integral. First note that if C represents the arc of the upper half circle,

$$\int_{\gamma_R} \frac{e^{iz}}{9+z^2}dz = \int_C \frac{e^{iz}}{9+z^2}dz + \int_{-R}^{R} \frac{e^{iz}}{9+z^2}dz$$

Now, by the Estimation Lemma (2.21), since $|e^{iz}| \leq 1$ on the upper half plane, we have

$$|\int_C \frac{e^{iz}}{9+z^2}dz| \leq \frac{1}{9+R^2}R\pi \overset{R\to\infty}{\longrightarrow} 0$$

Now we apply the residue theorem (2.20). Notice that the only root in the upper half circle is $3i$ and so

$$\int_{\gamma_R} \frac{e^{iz}}{9+z^2}dz = 2\pi i \frac{e^{i(3i)}}{3i+3i} = \frac{\pi}{3}e^{-3}$$

Taking the real part and limiting as $R \to \infty$ and cutting in half yields

$$\int_0^\infty \frac{\cos(\alpha z)}{9+z^2}dz = \frac{\pi}{6e^3}$$

as required. ■

12. Evaluate $\int_{-\infty}^{\infty} \frac{\sin(\pi x)}{1+x+x^2} dx$.

Solution: Let γ_R be the upper half semi-circle. Notice that

$$\int_{\gamma_R} \frac{\sin(\pi z)}{1+z+z^2} dz = \int_{\gamma_R} \frac{\Im(e^{\pi i z})}{1+z+z^2} dz = \Im\left(\int_{\gamma_R} \frac{e^{\pi i z}}{1+z+z^2} dz\right)$$

So we evaluate the last integral. First note that if C represents the arc of the upper half circle,

$$\int_{\gamma_R} \frac{e^{\pi i z}}{1+z+z^2} dz = \int_C \frac{e^{\pi i z}}{1+z+z^2} dz + \int_{-R}^{R} \frac{e^{\pi i z}}{1+z+z^2} dz$$

Now, by the Estimation Lemma (2.21) since $|e^{i\pi z}| \leq 1$ on the upper half plane,

$$|\int_C \frac{e^{\pi i z}}{1+z+z^2} dz| \leq \frac{1}{1+R+R^2} R\pi \overset{R\to\infty}{\longrightarrow} 0$$

Now we apply the residue theorem. Notice that the only root in the upper half circle is $\frac{-1+\sqrt{3}i}{2}$ and so

$$\int_{\gamma_R} \frac{e^{\pi i z}}{1+z+z^2} dz = 2\pi i \frac{e^{\pi i\left(\frac{-1+\sqrt{3}i}{2}\right)}}{\left(\frac{-1+\sqrt{3}i}{2} - \frac{-1-\sqrt{3}i}{2}\right)} = 2\pi i \left(\frac{(-i)e^{\frac{-\pi\sqrt{3}}{2}}}{\sqrt{3}i}\right) = -\frac{2\sqrt{3}}{3}\pi i e^{\frac{-\pi\sqrt{3}}{2}}$$

Taking the imaginary part and limiting as $R \to \infty$ yields

$$\int_{-\infty}^{\infty} \frac{\sin(\pi x)}{1+x+x^2} dz = -\frac{2\sqrt{3}}{3}\pi e^{\frac{-\pi\sqrt{3}}{2}}$$

as required. ■

13. Evaluate $\int_{-\infty}^{\infty} \frac{\sin(3x)}{x^2+2x+3} dx$.

Solution: Let γ_R be the upper half semi-circle. Notice that

$$\int_{\gamma_R} \frac{\sin(3z)}{z^2+2z+3} dz = \int_{\gamma_R} \frac{\Im(e^{3iz})}{z^2+2z+3} dz = \Im\left(\int_{\gamma_R} \frac{e^{3iz}}{z^2+2z+3} dz\right)$$

So we evaluate the last integral. First note that if C represents the arc of the upper half circle,

$$\int_{\gamma_R} \frac{e^{3iz}}{z^2+2z+3} dz = \int_C \frac{e^{3iz}}{z^2+2z+3} dz + \int_{-R}^{R} \frac{e^{3iz}}{z^2+2z+3} dz$$

Now, by the Estimation Lemma (2.21), since $|e^{3iz}| \leq 1$ on the upper half plane, we have

$$|\int_C \frac{e^{3iz}}{z^2+2z+3} dz| \leq \frac{1}{R^2+2R+3} R\pi \overset{R\to\infty}{\longrightarrow} 0$$

Now we apply the residue theorem. Notice that the only root in the upper half circle is $-1+\sqrt{2}i$ and so

$$\int_{\gamma_R} \frac{e^{3iz}}{1+z+z^2} dz = 2\pi i \frac{e^{3i(-1+\sqrt{2}i)}}{(-1+\sqrt{2}i-(-1-\sqrt{2}i))} = \frac{\pi\sqrt{2}}{2} e^{-3\sqrt{2}} e^{3i}$$
$$= \frac{\pi\sqrt{2}}{2} e^{-3\sqrt{2}} (\cos(-3) + i\sin(-3))$$

Taking the imaginary part and limiting as $R \to \infty$ yields

$$\int_{-\infty}^{\infty} \frac{\sin(3x)}{x^2+2x+3} dz = \frac{\pi\sqrt{2}}{2} e^{-3\sqrt{2}} \sin(-3)$$

as required. ■

Solution: Similar to the contour integration question with fractional roots, we have an issue with branch cuts. Here we wish to use the branch that corresponds to the negative x-axis (so $-\pi < \arg(z) < \pi$).

$$\int_0^{\infty} \frac{\log(pz)}{q^2+x^2} dx = \frac{\pi}{2q} \log(pq)$$

as required. ■

14. Evaluate $\int_0^{\infty} \frac{\log(x)}{(1+x^2)^2} dx$.

Solution: To solve logarithm question, we actually want to consider the integral

$$\int_K \frac{\log(z)^2}{(1+z^2)^2} dz$$

where K is the key hole region defined below around the negative x-axis (our choice of branch).

(i) Curve γ_1 is $z = -\pi x$ where x goes from ϵ to R.
(ii) Curve γ_2 is $z = Re^{it}$ where t goes from 0 to 2π.
(iii) Curve γ_3 is $z = \pi i x$ where x goes from R to ϵ (remember we introduce a 2π).
(iv) Curve γ_4 is $z = \epsilon e^{it}$ where t goes from 2π to 0.

Calling the combined region K, we have

$$\begin{aligned}\int_K \frac{\log(z)^2}{(1+z^2)^2} dz = \int_{\gamma_2} \frac{\log(z)^2}{(1+z^2)^2} dz + \int_{\gamma_4} \frac{\log(z)^2}{(1+z^2)^2} dz \\ - \int_{\epsilon}^{R} \frac{\log(z)^2}{(1+z^2)^2} dz - \int_{R}^{\epsilon} \frac{\log(z)^2}{(1+z^2)^2} dz\end{aligned}$$

(Note that the negative signs come in as we substitute the line integral in and so $dz = -dx$ on those lines). Consider the first two integrals as both $\epsilon \to 0$ and $R \to \infty$. We have that by the Estimation Lemma (2.21) and the Log Lemma (2.22),

$$|\int_{\gamma_2} \frac{\log(z)^2}{(1+z^2)^2} dz| \leq \frac{\log(\epsilon)^2}{(1+(\epsilon)^2)^2} dz(2\epsilon\pi) \overset{\epsilon \to 0}{\to} 0$$

$$|\int_{\gamma_4} \frac{\log(z)^2}{(1+z^2)^2} dz| \leq \frac{\log(R)^2}{(1+R^2)^2} dz(2R\pi) \overset{R \to \infty}{\to} 0$$

This leaves only the two inside integrals to evaluate. Consider the two pieces we haven't looked at. Notice that they are *NOT* the negative of each other. This is due to our branch choice. We pick up an extra value of 2π as we traverse the outer circle (for example) in the argument of z.

$$
\begin{aligned}
-\int_R^{\epsilon} \frac{\log(z)^2}{(1+z^2)^2}dz - \int_{\epsilon}^{R} \frac{\log(z)^2}{(1+z^2)^2}dz &= \int_{\epsilon}^{R} \frac{(\log|z|+i\pi)^2}{(1+z^2)^2}dz - \int_{\epsilon}^{R} \frac{(\log|z|-i\pi)^2}{(1+z^2)^2}dz \\
&= \int_{\epsilon}^{R} \frac{4\pi i \log(z)}{(1+z^2)^2}dz
\end{aligned}
$$

Thus, taking the limits as $\epsilon \to 0$ and $R \to \infty$ gives us

$$
\int_K \frac{\log(z)^2}{(1+z^2)^2}dz = 4\pi i \int_0^{\infty} \frac{\log(z)}{(1+z^2)^2}dz
$$

All that's left is an application of the residue theorem. Both roots i and $-i$ are in our keyhole region. So, by the Residue Theorem (2.20),

$$
\begin{aligned}
\int_K \frac{\log(z)^2}{(1+z^2)^2}dz &= 2\pi i \left(\frac{1}{(2-1)!} \lim_{x\to i} \frac{d^{2-1}}{dz^{2-1}} \frac{\log(z)^2}{(z+i)^2} + \frac{1}{(2-1)!} \lim_{x\to -i} \frac{d^{2-1}}{dz^{2-1}} \frac{\log(z)^2}{(z-i)^2} \right) \\
&= 2\pi i \left(\frac{\frac{2\log(i)(i+i)^2}{i} - 2(i+i)\log(i)^2}{(i+i)^4} + \frac{\frac{2\log(-i)(-i-i)^2}{-i} - 2(-i-i)\log(-i)^2}{(-i-i)^4} \right) \\
&= 2\pi i \left(\frac{-\pi}{4} + \frac{\pi^2 i}{16} + \frac{-\pi}{4} - \frac{\pi^2 i}{16} \right) \\
&= -i\pi^2
\end{aligned}
$$

Substituting into the above (after taking limits) yields

$$
\int_0^{\infty} \frac{\log(x)}{(1+x^2)^2}dx = \frac{-\pi}{4}
$$

as required. ■

15. Evaluate $\int_0^{\infty} \frac{\log(x)^2}{9+x^2}dx$.

Solution: To solve logarithm question, we actually want to consider the integral

$$
\int_K \frac{\log(z)^3}{9+z^2}dz
$$

where K is the key hole region defined below around the negative x-axis (our choice of branch).

(i) Curve γ_1 is $z = -\pi x$ where x goes from ϵ to R.
(ii) Curve γ_2 is $z = Re^{it}$ where t goes from 0 to 2π.
(iii) Curve γ_3 is $z = \pi i x$ where x goes from R to ϵ (remember we introduce a 2π).
(iv) Curve γ_4 is $z = \epsilon e^{it}$ where t goes from 2π to 0.

Calling the combined region K, we have

$$
\begin{aligned}
\int_K \frac{\log(z)^3}{9+z^2}dz = \int_{\gamma_2} \frac{\log(z)^3}{9+z^2}dz + \int_{\gamma_4} \frac{\log(z)^3}{9+z^2}dz \\
- \int_{\epsilon}^{R} \frac{\log(z)^3}{9+z^2}dz - \int_{R}^{\epsilon} \frac{\log(z)^3}{9+z^2}dz
\end{aligned}
$$

(Note that the negative signs come in as we substitute the line integral in and so $dz = -dx$ on those lines). Consider the first two integrals as both $\epsilon \to 0$ and $R \to \infty$. We have that by the Estimation Lemma (2.21) and the Log Lemma (2.22),

$$|\int_{\gamma_2} \frac{\log(z)^3}{9+z^2}dz| \leq \frac{\log(\epsilon)^3}{9+(\epsilon)^2}dz(2\epsilon\pi) \overset{\epsilon\to 0}{\to} 0$$
$$|\int_{\gamma_4} \frac{\log(z)^3}{9+z^2}dz| \leq \frac{\log(R)^3}{9+R^2}dz(2R\pi) \overset{R\to\infty}{\to} 0$$

This leaves only the two inside integrals to evaluate. Consider the two pieces we haven't looked at. Notice that they are *NOT* the negative of each other. This is due to our branch choice. We pick up an extra value of 2π as we traverse the outer circle (for example) in the argument of z.

$$\begin{aligned} -\int_R^\epsilon \frac{\log(z)^3}{9+z^2}dz - \int_\epsilon^R \frac{\log(z)^3}{9+z^2}dz &= \int_\epsilon^R \frac{(\log|z|+i\pi)^3}{9+z^2}dz - \int_\epsilon^R \frac{(\log|z|-i\pi)^3}{9+z^2}dz \\ &= \int_\epsilon^R \frac{6\pi i \log(z)^2 - 2\pi^3 i}{9+z^2}dz \end{aligned}$$

Thus, taking the limits as $\epsilon \to 0$ and $R \to \infty$ gives us

$$\int_K \frac{\log(z)^3}{9+z^2}dz = 6\pi i \int_0^\infty \frac{\log(z)^2}{9+z^2}dz - 2\pi^3 i \int_0^\infty \frac{1}{9+z^2}dz$$

To evaluate the last integral, we can use standard methods of integration to get:

$$\begin{aligned} \lim_{R\to\infty} \int_0^R \frac{1}{9+z^2}dz &= \lim_{R\to\infty} \frac{1}{9} \int_0^R \frac{1}{1+(\frac{z}{3})^2}dz \\ &= \lim_{R\to\infty} \frac{1}{3} \arctan(\frac{z}{3})\Big|_0^R \\ &= \frac{1}{3}(\frac{\pi}{2} - 0) = \frac{\pi}{6} \end{aligned}$$

To evaluate the first integral, all we need is an application of the residue theorem. Both roots $3i$ and $-3i$ are in our keyhole region. So, by the Residue Theorem (2.20),

$$\begin{aligned} \int_K \frac{\log(z)^3}{9+z^2}dz &= 2\pi i \left(\frac{\log(3i)^3}{3i+3i} + \frac{\log(-3i)^3}{-3i-3i} \right) \\ &= 2\pi i \left(\frac{(\log(3) + \frac{i\pi}{2})^3}{6i} + \frac{(\log(3) + \frac{-i\pi}{2})^3}{-6i} \right) \\ &= \log(3)^2\pi^2 i - \frac{\pi^4 i}{12} \end{aligned}$$

Substituting into the above (after taking limits) yields

$$\int_0^\infty \frac{\log(x)^2}{9+x^2}dx = \frac{1}{6\pi i}\left(\log(3)^2\pi^2 i - \frac{\pi^4 i}{12} + 2\pi^3 i\frac{\pi}{6}\right) = \frac{\pi^3}{24} + \frac{\log(3)^2\pi}{6}$$

as required. ■

3 Linear Algebra

Before I begin, I would like to give a huge thank you to Faisal al-Faisal for this section. Many of the creative solutions are due either directly or indirectly to his invaluable input.

Theorem 3.1. *A real symmetric matrix $A \in M_n(\mathbb{R})$ has only real eigenvalues and eigenvectors.*

Proof. Let v be an eigenvector of A over $\mathbb{C}$ and let λ be its corresponding eigenvalue. then the following is true,

$$\begin{aligned} Av = \lambda v &\Rightarrow (Av)^T = \lambda v^T \\ &\Rightarrow (v)^T A = \lambda v^T && (A \text{ is symmetric}) \\ &\Rightarrow (\overline{v})^T A = \overline{\lambda}(\overline{v})^T \end{aligned}$$

and therefore

$$\lambda(\overline{v})^T v = (\overline{v})^T (Av) = ((\overline{v})^T A)v = \overline{\lambda}(\overline{v})^T v$$

Now, recalling that $||v||^2 =< v, v >= \overline{v}^T v$ and since v is non zero, the above gives us that $\lambda\,||v||^2 = \overline{\lambda}\,||v||^2$ and so $\lambda = \overline{\lambda}$ and hence is real. To get that v must be real note that $(A - \lambda I)$ is noninvertible and hence there is a real vector satisfying $(A - \lambda I)v = 0$. This is our eigenvector.

Theorem 3.2. *A matrix is diagonalizable if all of its eigenvalues are distinct.*

Theorem 3.3. *A matrix is diagonalizable if is real and symmetric. Further, there is an orthogonal matrix making it diagonal.*

Proof. (Sketch) Use induction. Get an eigenvalue and unital eigenvector v (exists by real symmetry). Use GS to get an o.n.b. with the eigenvector then construct the matrix M consisting of these vectors. Notice that $Me_1 = v$. Moreover, e_1 is an eigenvector of $M^{-1}AM$ we can write this as a block diagonal matrix with the eigenvalue in the top left corner (as any matrix times e_1 gives you the first column of the matrix) and the bottom right corner is a symmetric matrix (since $M^{-1}AM$ is symmetric) of strictly smaller size. Induction takes us home.

Definition 3.4. A *Hermitian* matrix is a square self-adjoint matrix, that is, one whose conjugate transpose equals itself.

3.1 Trace and Determinant

1. Show $AB - BA = I$ has no solution over $M_n(\mathbb{R})$.

   Solution: Suppose there were matricies A, B satisfying $AB - BA = I$. Then

   $$n = \mathrm{tr}(I) = \mathrm{tr}(AB - BA) = \mathrm{tr}(AB) - \mathrm{tr}(BA) = \mathrm{tr}(AB) - \mathrm{tr}(AB) = 0$$

   which is a contradiction. For a counter example with infinite dimensional vector spaces, see the eigenvalues section. ■

3.2 Decomposition Theorems

Theorem 3.5. *(Jordan Decomposition Theorem) Every matrix $M \in M_n(\mathbb{C})$ is similar to a block diagonal matrix. In otherwords, there exist a matrix P such that $J = P^{-1}MP$ where J is of the form*

$$J = \begin{bmatrix} J_1 & & \\ & \ddots & \\ & & J_p \end{bmatrix}$$

where

$$J_i = \begin{bmatrix} \lambda_i & 1 & & \\ & \lambda_i & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_i \end{bmatrix}$$

subject to the conditions that

(i) Each λ_i is an eigenvalue of M

(ii) Given an eigenvalue λ_i its geometric multiplicity is the dimension of $\ker(M - \lambda_i I)$*, and it is the number of Jordan blocks corresponding to λ_i*

(iii) The sum of the sizes of all Jordan blocks corresponding to an eigenvalue λ_i is its algebraic multiplicity

Theorem 3.6. *(Primary Decomposition Theorem) Every matrix is similar to the companion matrix of its minimal polynomial (roughly speaking)*

1. Show that no n by n real matrix A can be of the form

$$A^2 = \begin{bmatrix} -a_1 & & \\ & \ddots & \\ & & -a_n \end{bmatrix}$$

where each a_i is positive, real and distinct.

Solution: Suppose that such an A exists. If n is odd, then note

$$0 < \det(A)^2 = \det(A^2) = \prod_{i=1}^{n}(-a_i) = -\prod_{i=0}^{n}(a_i)$$

a contradiction. So suppose n is even. Note that A satisfies $p(A^2) = 0$ where $p(x) = \prod_{i=0}^{n}(-a_i - x) = \prod_{i=0}^{n}(x + a_i)$. In particular, we know that A is a zero of $p(x^2)$. Let $m_A(x)$ be the minimal polynomial of A. We know that $m_A \mid p(x^2)$ and since all the factors are monic and irreducible, we have that $m_A = \prod_{i=0}^{n/2}(x^2 + b_i)$ where the b_i form a subset of the a_i. Applying the primary decomposition theorem (3.6), we see that A is similar to the following block matrix

$$\begin{bmatrix} 0 & -b_1 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & \vdots \\ 0 & & \ddots & & \\ \vdots & & & 0 & -b_{\frac{n}{2}} \\ 0 & \dots & 0 & 1 & 0 \end{bmatrix}$$

and thus A^2 is similar to

$$\begin{bmatrix} b_1 & & & & \\ & b_1 & & & \\ & & \ddots & & \\ & & & b_{\frac{n}{2}} & \\ & & & & b_{\frac{n}{2}} \end{bmatrix}$$

but similar matricies share the same eigenvalues (the proof is similar to the problem where $AB = BA$ with B invertible - show they share the same eigenvalues). The matrix above only has $\frac{n}{2}$ distinct eigenvalues while A^2 has n distinct eigenvalues, a contradiction. Hence A cannot exist. ■

2. For what values of r and n is there an $n \times n$ matrix of rank r with real entries such that $A^2 = 0$?

Solution: Without loss of generality, we may suppose that A is in Jordan canonical form (for A must be similar to a matrix in Jordan canonical form and we can do all the math with the similar matrix and everything will carry over as similarity is rank and eigenvalue invariant). Now, since A is nilpotent, its only eigenvalue is 0. Since $A^2 = 0$ we know that the Jordan blocks must consist only of matricies of the form

$$\begin{bmatrix} 0 \end{bmatrix} \qquad \text{or} \qquad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

So we may construct a matrix consisting of these two blocks. Everytime we use the second block, we add 1 to the rank. At most, we can use $\lfloor \frac{n}{2} \rfloor$ of the second blocks. Also, we can decide to use non of the second blocks giving $r = 0$ as our value. Hence for any value of n, we have that $0 \le r \le \lfloor \frac{n}{2} \rfloor$ as requried. ■

3. Show that $GL(3, \mathbb{Z})$ cannot have an element of order 7.

Solution: By Gauss' Lemma it suffices to show that $GL(3, \mathbb{Q})$ cannot have an element of order 7. Suppose there was an $A \in GL(3, \mathbb{Q})$ such that $A^7 = I$. Then letting $p(x)$ be the minimal polynomial for A, we see that $p(x) | x^7 - 1$. since $p(x) \neq x - 1$, we must have that $p(x) = x^6 + x^5 + ... + 1$ as it is irreducible over $\mathbb{Q}$ (I will show this in the ring section but for a quicky proof, use Eisenstein on $\frac{(y+1)^7 - 1}{(y+1) - 1} = p(y + 1)$ to show this is irreducible and note that irreducibility is invariant under shifts). By the Primary Decomposition Theorem (3.6) we have that A is similar to the characteristic polynomial of $p(x)$ which is a 6 by 6 matrix. This is absurd. Hence A cannot have order 7.

As an aside, we can show that the only orders a matrix can have are $1, 2, 3, 4, 6$ using a very similar method. Moreover, this method extends to $GL(n, \mathbb{Z})$. ■

4. Let $A \in M_n(\mathbb{C})$. Show that the nullity of the commutator of A is at least of dimension n.

Solution: The commutator is the set of all matricies such that $AB - BA = 0$. We wish to find a set of dimension n such that every element of this set commutes with A. Note that it suffices to do this for an A in Jordan Canonical Form. By the Jordan Decomposition Theorem (3.5), we have that $A = P^{-1}JP$ for some invertible matrix P and J in normal form. If we find B such that $JB = BJ$, then note $P^{-1}JPP^{-1}BP = P^{-1}BPP^{-1}JP \Rightarrow AP^{-1}BP = P^{-1}BPA$ and invertible matricies do not change the linear independence or matricies. Now, analyzing the matrix block by block, it sufices to consider a Jordan block and extend the results block by block. So suppose we have a Jordan block J_1 of size $k \le n$. Now, notice that J_1 commutes with powers of itself. So it suffices to show that k of these powers are linearly independent. Consider the minimal polynomial of J_1. Since it is a Jordan block, we know that the degree of the minimal polynomial is k. Hence the matricies $I, J_1, ..., J_1^{k-1}$ must be linearly independent for otherwise we could find a polynomial with rational coefficients of a smaller degree, a contradiction. Hence, we have found k linearly independent matricies that commute with J_1. Now, what we can do is do this construction block by block and thus we get at least n linearly independent matricies that commute with our matrix A as required.

5. Compute the Jordan Canonical form of

$$A := \begin{bmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 4 \end{bmatrix}$$

Solution: It turns out that you don't need much effort to compute this one. Notice that the characteristic polynomial is $(1-\lambda)(4-\lambda)^2$ corresponding the eigenvalues $\lambda = 1, 4$. All we need to do is determine the nullity of the eigenvalue associated to 4. Plugging in we note that

$$A - 4I = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 0 & 5 \\ 0 & 0 & 0 \end{bmatrix}$$

which has nullity 1. Hence the geometric multiplicity (ie dimension of the nullspace ie the dimension of the eigenspace associated to 0) is 1. Thus, the two eigenvalues of 4 correspond to one Jordan block and hence the Jordan canonical form is

$$A := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 4 \end{bmatrix}$$

3.3 Eigenvalues and Eigenvectors

1. Prove that the following matrix has two positive and two negative eigenvalues (counting multiplicities)

$$\begin{bmatrix} 0 & 5 & 1 & 0 \\ 5 & 0 & 5 & 0 \\ 1 & 5 & 0 & 5 \\ 0 & 0 & 5 & 0 \end{bmatrix}$$

Solution: This is a plug and chug. Turns out the characteristic polynomial is $f(\lambda) := \lambda^4 - 76\lambda^2 - 50\lambda + 625$. Then simply note that

$$f(-8) > 0 > f(-7) < 0 < f(-3) > 0 > f(3) < 0 < f(9)$$

So applying the Intermediate Value Theorem (1.1) four times gives us the desired conclusion. ■

2. Let A and B be two $n \times n$ commuting matricies over $\mathbb{C}$. Show that they share a common eigenvector.

Solution: . Let λ be an eigenvalue of A (which exists since A has entries in an algebraically closed field). Consider $V_\lambda := \{v \in \mathbb{C}^n \mid Av = \lambda v\}$, the eigenspace of λ. Note that this Eigenspace is B-invariant. For if $v \in V_\lambda$, then $Bv \in V_\lambda$ since $ABv = BAv = B(\lambda v) = \lambda Bv$. So we may view B as an operator acting on the eigenspace. Since it is complex valued it too must have an eigenvector $v_0 \in V_\lambda$. By definition, this eigenvector is an eigenvector for A as well proving the claim.

3. Let A and B be real symmetric matricies with positive eigenvalues. Show that $A+B$ has the same property.

Solution: That $A + B$ is real and symmetric is clear. We show that all eigenvalues of $A + B$ are positive. Let x be an eigenvector of $A + B$ with associated eigenvalue λ. Then $Ax + Bx = (A + B)x = \lambda x$. Taking the inner product of both sides with x gives $< Ax, x >$ $+ < Bx, x >= \lambda < x, x >$. Since $x \neq \mathbf{0}$, we know that $< x, x >> 0$. So it suffices to show that for any real symmetric matrix with positive eigenvalues say M that $< Mx, x >> 0$. Since M is positive real symmetric, we can write $M = P^T DP$ where D is a diagonal matrix whose entries are precisely the eigenvalues of M (think Jordan Canonical Decomposition) and where P is an orthogonal matrix (by 3.3). Consider $Q = P^T D^{\frac{1}{2}} P$ where $D^{\frac{1}{2}}$ is the diagonal matrix with the entries square rooted (possible since D has only positive elements). Notice that $Q^2 = M$ and that $Q^T = Q$ and hence is symmetric. Thus, by the properties of the inner product,

$$< Mx, x >=< Q^2x, x >=< Q^TQx, x >=< Qx, Qx >> 0$$

The last inequality holds since $Qx \neq \mathbf{0}$ as it is invertible (with inverse $P^TD^{-1}P$) and $x \neq \mathbf{0}$. ■

4. Let A and B be real matricies with B invertible. Show that AB and BA share common eigenvalues.

   Solution: Let x be an eigenvector for AB, that is $ABx = \lambda x$. Set $v := Bx$. Then

   $$BAv = BABx = B(\lambda x) = \lambda Bx = \lambda v$$

   So λ is an eigenvalue for BA. Conversely, suppose y is an eigenvector for BA with eigenvalue μ. Set $u := B^{-1}y$. Then

   $$ABu = B^{-1}BABB^{-1}y = B^{-1}BAy = B^{-1}\mu y = \mu B^{-1}y = \mu u$$

   So μ is an eigenvalue for AB. This completes the proof. ■

5. Let $a, b, c, d \in \mathbb{R}$ not all zero. Find eigenvalues of the following matrix and describe the eigenspace decomposition of $\mathbb{R}^4$.

   $$\begin{bmatrix} aa & ab & ac & ad \\ ba & bb & bc & bd \\ ca & cb & cc & cd \\ da & db & dc & dd \end{bmatrix}$$

   Solution: Without loss of generality, suppose $a \neq 0$. Notice that the matrix will row reduce via the operations

   $$\frac{-b}{a}R_1 + R_2 \to R_2 \quad \frac{-c}{a}R_1 + R_3 \to R_3 \quad \frac{-d}{a}R_1 + R_4 \to R_4$$

   to the matrix

   $$\begin{bmatrix} aa & ab & ac & ad \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

   Hence the kernel has dimension 3 and thus 0 is an eigenvalue of this matrix with multiplicity three. A quick check reveals that this eigenspace is spanned by the eigenvectors

   $$\begin{pmatrix} b \\ -a \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} c \\ 0 \\ -a \\ 0 \end{pmatrix} \quad \begin{pmatrix} d \\ 0 \\ 0 \\ -a \end{pmatrix}$$

   All that is left is the last eigenvalue and its corresponding eigenvector. To compute this we explicitly compute the characteristic polynomial.

   $$\det\left(\begin{bmatrix} aa-\lambda & ab & ac & ad \\ ba & bb-\lambda & bc & bd \\ ca & cb & cc-\lambda & cd \\ da & db & dc & dd-\lambda \end{bmatrix}\right) = \det\left(\begin{bmatrix} aa-\lambda & ab & ac & ad \\ \frac{b\lambda}{a} & -\lambda & 0 & 0 \\ \frac{c\lambda}{a} & 0 & -\lambda & 0 \\ \frac{d\lambda}{a} & 0 & 0 & -\lambda \end{bmatrix}\right)$$
   $$\begin{aligned} &= (aa-\lambda)(-\lambda^3) - (\frac{b\lambda}{a})(\lambda^2 ba) \\ &\quad + (\frac{c\lambda}{a})(-\lambda^2 ca) - (\frac{d\lambda}{a})(\lambda^2 da) \\ &= \lambda^4 - (a^2+b^2+c^2+d^2)\lambda \end{aligned}$$

where the first equality holds by invariance of scalar row multiplication. So the last eigenvalue is $a^2+b^2+c^2+d^2$. A quick check reveals that the associated eigenvector is $(a,b,c,d)^T$. ■

6. Let M be an n by n real matrix with a 7 in each of the first p rows and a 4 in each of the last $n-p$ rows. Find the eigenvalues and eigenvectors of this matrix.

   Solution: First we start off with the easy eigenvalues and eigenvectors. Note that each of $(1,-1,0,..0)^T, (1,0,-1,0,..,0)^T, ..., (1,..,0,-1)^T$ are eigenvectors associated to the eigenvalue 0 (this is very clear from inspection). This is a set of $n-1$ vectors. So all that is left is discovering the final eigenvector.

   Suppose that $Mx = \lambda x$ where $x = (x_1, ..., x_n)^T \neq 0$. Let $S := \sum_{i=1}^n x_i$. Expanding yields

$$7S = \lambda x_1, 7S = \lambda x_2, ..., 7S = \lambda x_p, 4S = \lambda x_{p+1}, ..., 4S = \lambda x_n$$

   Summing all the equations yields

$$7pS + 4(n-p)S = \lambda S \Rightarrow (4n+3p-\lambda)S = 0$$

   So either $S=0$ (which we solved by inspection - in theory there COULD be another eigenvector in this category but this is not the case as we will see) or $\lambda = 4n+3p$. Now, we compute the eigenvectors. We know that $S = \frac{\lambda x_1}{7}$. Hence $x_1 = x_2 = ... = x_p$ and $x_{p+1} = ... = x_n = \frac{4x_1}{7}$. Setting $x_1 = 1$ yields the eigenvector $(1,..,1,\frac{4}{7},...,\frac{4}{7})^T$ and thus completing the list. ■

7. Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $a,b,c,d > 0$. Show that A has an eigenvector $\begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2$ with $x,y>0$.

   Solution: Let $v = (x,y)^T$ be an eigenvector. Notice that it satisfies

$$ax + by = \lambda x \qquad\qquad cx + dy = \lambda y$$

   where λ is the associated eigenvalue. In particular, if $x=0$ the the above says that $by = 0$ and since $b>0$, we have that $y=0$ contradicting the fact that eigenvectors are nonzero. Similarly, $y=0$ leads to $x=0$ a contradiction. So it suffices to show that x and y have the same sign (if both are negative then $-v$ has strictly positive entries and is also an eigenvalue). The characteristic polynomial for this matrix is $\lambda^2 - (a+d)\lambda + ad - bc$ leading to the eigenvalues

$$\lambda_{\pm} = \frac{a+d \pm \sqrt{(a-d)^2+4bc}}{2}$$

   Consider λ_+. I claim that $\lambda_+ - a > 0$. This holds since

$$\begin{aligned} \lambda_+ - a = \frac{d-a+\sqrt{(a-d)^2+4bc}}{2} &> \frac{d-a+\sqrt{(a-d)^2}}{2} \\ &= \frac{d-a+|d-a|}{2} = \max\{0, d-a\} \geq 0 \end{aligned}$$

   Using this eigenvalue, the first equation becomes

$$by = (\lambda_+ - a)x$$

   Now both b and $\lambda_+ - a$ are strictly greater than 0 so it must be that x and y have the same sign as required. ■

8. Let V be the vector space of all polynomials $p(x)$ with real coefficients. Let A and B denote the linear transformation on V of multiplication by x and differentiation respectfully.

(i) Show that A has no eigenvalues and that 0 is the only eigenvalue of B

(ii) Compute the transform $BA - AB$

(iii) Show that no two linear transformation A and B ona finite dimensional real vector space can satisfy $BA - AB = I$.

Solution:

(i) Let $p(x) \in \mathbb{R}[x]$ be an eigenvector for A, that is $A(p(x)) = \lambda p(x)$. Then $xp(x) = \lambda p(x)$. A degree argument shows a contradiction unless $p(x) = 0$ in which case we don't have an eigenvector. Let $q(x) \in \mathbb{R}[x]$ be an eigenvector for B, that is $B(q(x)) = \mu q(x)$. Hence $q'(x) = \mu q(x)$. Since $q(x) \neq 0$, then this holds if and only if $q'(x) = 0$ and $\mu = 0$. This completes the proof. ■

(ii) Let $p(x) \in \mathbb{R}[x]$. Note that

$$\begin{aligned} BA(p(x)) &= B(xp(x)) = (p(x) + x'p(x)) \\ AB(p(x)) &= A(p'(x)) = xp'(x) \end{aligned}$$

Subtracting shows that $(BA - AB)(p(x)) = p(x)$ and since $p(x)$ was an arbitrary polynomial, we get that $BA - AB = I$.

(iii) This was solved before - just take the traces and note that we get $n = 0$ a contradiction. ■

3.4 Nilpotent Matricies

1. Let A be a nilpotent n by n matrix. Prove or disprove the following.

(i) $A^n = 0$

(ii) $\det(A + I) = 1$

(iii) $\det(A + D) = \det(D)$

Solution:

(i) Since A is nilpotent, its minimal polynomial is $p(t) = t^k$ where $k \leq n$. Hence $A^n = A^{n-k}A^k = A^{n-k}0 = 0$. ■

(ii) By the Jordan Decomposition Theorem, A is similar to an upper triangular matrix with all 0 entries on both the diagonal and the lower triangle. Call this matrix M and say $PAP^{-1} = M$. Notice that $\det(M + I) = 1$ and hence

$$\begin{aligned} 1 = \det(M + I) &= \det(PAP^{-1} + I) = \det(P(A + I)P^{-1}) = \det(P)\det(A + I)\det(P^{-1}) \\ &= \det(A + I) \end{aligned}$$

as claimed. ■

(iii) We construct a counter example. Notice that for a 2 by 2 matrix A, the characteristic polynomial is $p(t) = t^2 - \text{tr}(A)t + \det(A)$. Consider

$$\begin{bmatrix} 6 & -9 \\ 4 & -6 \end{bmatrix}$$

This matrix has $\text{tr}(A) = \det(A) = 0$. By the above, we know that $A^2 = 0$ and so A is nilpotent. Set

$$\begin{bmatrix} -6 & 0 \\ 0 & 6 \end{bmatrix}$$

and note that

$$-36 = \det(D) \neq \det(D + A) = \det(\begin{bmatrix} 0 & -9 \\ 4 & 0 \end{bmatrix}) = 36$$

disproving the claim . ■

2. Let M, N be 6 by 6 complex nilpotent matricies. Suppose further that N and M have the same minimal polynomial and nullity. Show that N and M are similar. Moreover, show this is not the case for 7 by 7 matricies.

   Solution: Since every matrix has a unique Jordan decomposition, and both the minimal polynomial and nullity are similarity invariant, it suffices to examine the Jordan decomposition of matricies with the stated properties. Notice that for every Jordan block in the decomposition, we add 1 to the nullity (there will be a zero row in the decomposition). So it suffices to examine the nullity cases. Moreover note that flipping Jordan blocks does not change the similarity (just use permutation matricies to flip the order of the blocks).

   (i) Nullity is 0. This cannot happen as we have at least one Jordan block and hence the nullity is at least 1

   (ii) Nullity is 1. There is only one way this can happen and that is if the minimal polynomial is t^6. Hence M and N have the same Jordan decomposition.

   (iii) Nullity is 2. We have two Jordan blocks. If the minimal polynomial is t^k with $k \leq 2$ then we have at least three Jordan blocks contradicting the nullity. If the minimal polynomial is t^3 then it must be the matrix with two Jordan blocks corresponding to t^3. If the minimal polynomial is t^4 then we have again exactly two blocks one corresponding to t^4 and one corresponding to t^2. If the minimal polynomial is t^5 then again there is only one matrix namely the one with the t^5 block and the t block. In all these cases, there is a unique Jordan matrix per nullity and minimal polynomial.

   (iv) Nullity is 3. We have three Jordan blocks. If the minimal polynomial is t^2 then we have three equal Jordan blocks. If the minimal polynomial is t^3, then we have a t^3, a t^2, and a t block. If the minimal polynomial is t^4 then we need two t blocks to meet the nullity quota. Again in all cases we have a unique matrix.

   (v) Nullity is 4. If the minimal polynomial is t^2 then we have another t^2 block and two t blocks. If the minimal polynomial is t^3, then we have all t blocks.

   (vi) Nullity is 5. The minimal polynomial is t^2 and we have four t blocks.

   (vii) Nullity is 6. The minimal polynomial is t. We have the zero matrix. End of story.

   In all cases we have a unique matrix and hence M and N are similar as required. Lastly, for 7 by 7 matricies, we do not have uniqueness. Consider the matrices where the Jordan blocks are t^3, t^3 and t and the other matrix has blocks t^3, t^2, t^2. These matrices have the same nullity and the same minimal polynomial but are not similar. ■

3.5 Gram-Schmidt Orthogonalization

Theorem 3.7. *Let V be a finite dimensional inner product space. Define the projection operator by*

$$\text{proj}_u(v) = \frac{< v, u >}{< u, u >} u$$

The Gram-Schmidt process takes a basis $\{v_i\}$ to an orthonormal basis. To do this use the vectors

$$\begin{aligned} u_1 &= v_1 \\ u_2 &= v_2 - \mathrm{proj}_{u_1}(v_2) \\ u_3 &= v_3 - \mathrm{proj}_{u_1}(v_3) - \mathrm{proj}_{u_2}(v_3) \\ &\vdots \\ u_k &= v_k - \sum_{j=1}^{k-1} \mathrm{proj}_{u_j}(v_k) \end{aligned}$$

then normalize to $e_i = \frac{u_i}{||u_i||}$. This works for an infinite dimensional vector space as well - at each iteration we get a set of orthonormal vectors where the first k vectors share the same span.

1. (i) Prove that an orthogonal set of vectors $\{u_1, .., u_n\}$ in an n-dimensional Euclidean space is linearly independent.

   (ii) Let V be the subspace of $\mathbb{R}^4$ spanned by $v_1 = (0,1,1,0)^T$, $v_2 = (1,0,1,1)^T$, $v_3 = (1,1,0,2)^T$. Using Gram-Schmidt, construct an orthgonal basis for V.

   (i) Suppose that $v := a_1 u_1 + ... + a_n u_n = 0$. Notice that $0 =< v, u_i >= a_i$ as u_i form an orthonormal basis. Hence the set is linearly independent. ∎

   (ii) Plug and chug...

$$u_1 = v_1 = (0,1,1,0)^T$$

$$u_2 = v_2 - \mathrm{proj}_{u_1}(v_2) = (1,0,1,1)^T - \frac{< (1,0,1,1)^T, (0,1,1,0)^T >}{< (0,1,1,0)^T, (0,1,1,0)^T >}(0,1,1,0)^T = \begin{pmatrix} 1 \\ \frac{-1}{2} \\ \frac{1}{2} \\ 1 \end{pmatrix}$$

$$\begin{aligned} u_3 &= v_3 - \mathrm{proj}_{u_1}(v_3) - \mathrm{proj}_{u_2}(v_3) \\ &= (1,1,0,2)^T - \frac{< (1,1,0,2)^T, (0,1,1,0)^T >}{< (0,1,1,0)^T, (0,1,1,0)^T >}\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} - \frac{< (1,1,0,2)^T, (1, \frac{-1}{2}, \frac{1}{2}, 1)^T >}{< (1, \frac{-1}{2}, \frac{1}{2}, 1)^T, (1, \frac{-1}{2}, \frac{1}{2}, 1)^T >}\begin{pmatrix} 1 \\ \frac{-1}{2} \\ \frac{1}{2} \\ 1 \end{pmatrix} \\ &= (0,1,-1,1)^T \end{aligned}$$

3.6 Random Linear Algebra Questions

1. Let x be a unit vector in $\mathbb{R}^n$. Let $A := I - \beta x x^T$.

   (i) Show A is symmetric.

   (ii) Find all β such that A is orthogonal.

   (iii) Find all β such that A is invertible.

   Solution:

   (i) Notice that $(xx^T)^T = (x^T)^T x^T = xx^T$ and thus is symmetric. Multiplying this by a scalar doesn't change the "symmetricness". Lastly, adding by I (that is, only adding elements to the diagonal) also doesnt change the symmetricness and hence A is symmetric.

(ii) We wish to find values of β so that $AA^T = I$. Since A is symmetric, it suffices to find values such that $A^2 = I$. Evaluating directly yields,

$$\begin{aligned} I = A^2 = (I - \beta xx^T)^2 &= I - 2\beta xx^T + \beta^2 (xx^T)(xx^T) \\ &= I - 2\beta xx^T + \beta^2 x(x^T x)x^T = I - 2\beta xx^T + \beta^2 xx^T \end{aligned}$$

where the last equality holds since x is a unit vector. This implies that $(\beta^2 - 2\beta)xx^T = 0$. Since x is a unit vector, xx^T has a non-zero entry and thus we must have that $(\beta^2 - 2\beta) = 0$. This is true if and only if $\beta = 0$ or $\beta = 2$.

(iii) Since xx^T is real symmetric, it is diagonalizable. Let Q be a real matrix such that $Q(xx^T)Q^{-1} = D$ for some diagonal matrix D. Notice that the entries of the diagonal are the eigenvalues of xx^T.

$$\begin{aligned} A = I - \beta xx^T &\Leftrightarrow QAQ^{-1} = I - \beta Qxx^T Q^{-1} = I - \beta D \\ &\Rightarrow \det(A) = \det(QAQ^{-1}) = \det(I - \beta D) = (1 - \beta\lambda_1)...(1 - \beta\lambda_n) \end{aligned}$$

Where each of the λ_i represents the eigenvalue in position (i, i) of D. Notice that since x is a unit vector, we have as before that $(xx^T)(xx^T) = x(x^T x)x^T = xx^T$ and so xx^T as a matrix satisfies $t^2 - t = 0$. Since all eigenvalues satisfy the minimal polynomial, the eigenvalues of xx^T must be either 0 or 1 and at least one is non-zero since otherwise xx^T is nilpotent and using the above we see that $0 = (xx^T)^n = xx^T$ (for some $n \in \mathbb{N}$), a contradiction for a unit vector x. Thus for A to be invertible, we need a non-zero determinant, and so we need $(1 - \beta\lambda_1)...(1 - \beta\lambda_n) \neq 0$. As these $\lambda_i = 0$ or 1 and not all are 0, we reduce this to $(1 - \beta) \neq 0$ or simply $\beta \neq 1$. So if $\beta \neq 1$ then A is invertible. ■

2. Let U, W be subspaces if a finite-dimensional vector space V. Prove that $\dim(U) + \dim(W) = \dim(U \cap W) + \dim(U + W)$.

Solution: Let $i = \dim(U), j = \dim(W), k = \dim(U \cap W)$ and $e_1, .., e_k$ a basis for $U \cap W$. Next, extend this basis to a basis of U via $e_1, .., e_k, f_1, .., f_{i-k}$ and extend this basis to a basis of W via $e_1, .., e_k, g_1, .., g_{j-k}$. I claim that $B := \{e_1, .., e_k, f_1, .., f_{i-k}, g_1, .., g_{j-k}\}$ is a basis of $U + W$. First, let $v = u + w \in U + W$ with $u \in U$ and $w \in W$. Note that

$$\begin{aligned} u &= \sum_{a=1}^{k} \lambda_a e_a + \sum_{b=1}^{i-k} \mu_a f_b \\ w &= \sum_{a=1}^{k} \omega_a e_a + \sum_{b=1}^{j-k} \nu_b g_b \\ \Rightarrow v = u + w &= \sum_{a=1}^{k} (\lambda_a + \omega_a) e_a + \sum_{b=1}^{i-k} \mu_b f_b + \sum_{c=1}^{j-k} \nu_c g_c \end{aligned}$$

so B spans $U + W$. Next, suppose

$$v = u + w = \sum_{a=1}^{k} \lambda_a e_a + \sum_{b=1}^{i-k} \mu_b f_b + \sum_{c=1}^{j-k} \nu_c g_c = 0$$

I claim each of the scalars must be 0. Observe that

$$\sum_{a=1}^{k} \lambda_a e_a + \sum_{b=1}^{i-k} \mu_a f_b = \sum_{c=1}^{j-k} -\nu_c g_c$$

The right hand side is in W and the left hand side is in U so both sides lie in the intersection $U \cap W$. By choice of g_c, we know that g_c were chosen in W and not in $U \cap W$ so we have that both sides equal 0. Since the g_c is a part of a basis for W, we know that $\nu_c = 0$. Since $e_1, .., e_k, f_1, .., f_{i-k}$ is a basis for U, we know that each of the λ_a and μ_b are also 0. Hence all scalars are 0 and thus B is linearly independent. Hence B is a basis for $U + W$. Thus,

$$\dim(U + W) = k + i - k + j - k = i + j - k = \dim(U) + \dim(W) - \dim(U \cap W)$$

giving the desired result. ■

3. Let $A = [a_{ij}]$ be an n by n matrix of complex numbers satisfying for each $1 \leq i \leq n$,

$$|a_{ii}| > \sum_{j \neq i} |a_{ij}|$$

Suppose that $Ax = 0$ where $x = (x_1, .., x_n)^T \in \mathbb{C}^n$.

(i) Show that $a_{ii}x_i = -\sum_{j \neq i} a_{ij}x_j$

(ii) Let $M = \max_{1 \leq k \leq n} |x_k|$. Show that $M = 0$.

(iii) Show that the matrix A is invertible

Solution:

(i) Direct multiplication gives for each $1 \leq i \leq n$,

$$\sum_{j=0}^{n} a_{ij}x_j$$

Isolating gives the result. ■

(ii) Let k be the index such that $M = |x_k|$. Then

$$M \sum_{j \neq k} |a_{kj}| = |x_k| \sum_{j \neq k} |a_{kj}| \leq |x_k||a_{kk}| = |a_{kk}x_k| = |\sum_{j \neq k} a_{kj}x_j| \leq \sum_{j \neq k} |a_{kj}x_j| \leq M \sum_{j \neq k} |a_{kj}|$$

Hence if $M \neq 0$ we have that

$$\sum_{j \neq k} |a_{kj}| = |a_{kk}|$$

contradicting the above. Hence $M = 0$ as required. ■

(iii) Since Ax has only the trivial solution by the above, we have that A is invertible. ■

4. Consider $L : M_n(\mathbb{R}) \to M_n(\mathbb{R})$ defined by $L(A) = A + A^T$.

(i) For $n = 2$ find bases for $\ker(L)$ and $\mathrm{Ran}\,(L)$.

(ii) For all $n \geq 2$, find $\dim(\ker(L))$ and $\dim(\mathrm{Ran}\,(L))$.

5. Let A be an n by n real symmetric matrix and define the matrix e^A by the convergent series

$$e^A := \sum_{j=0}^{\infty} \frac{1}{j!} A^j$$

where $A^0 = I$ by convention. Show that e^A is non-singular.

Solution: Notice that since A was an arbitrary real symmetric matrix, we have that the following sum must also converge,

$$e^{-A} := \sum_{j=0}^{\infty} \frac{1}{j!} (-A)^j$$

I claim that this is the inverse of e^A. Notice that

$$e^A e^{-A} = \sum_{j=0}^{\infty} \frac{1}{j!} A^j \sum_{j=0}^{\infty} \frac{1}{j!} (-A)^j = \sum_{k=0}^{\infty} \sum_{j=0}^{k} \frac{(-1)^k}{(k-j)!j!} A^k$$

Now for all $k \geq 1$, we have

$$0 = (1-1)^k = \sum_{i=1} k \binom{k}{i} (-1)^k = \sum_{i=1} k \frac{k!}{(k-i)!i!} (-1)^k$$

dividing by $k!$ tells us that $\sum_{i=1} k \frac{(-1)^k}{(k-i)!i!} = 0$. Hence

$$e^A e^{-A} = \sum_{k=0}^{\infty} \sum_{j=0}^{k} \frac{(-1)^k}{(k-j)!j!} A^k = A^0 + 0 = I$$

Thus, e^A is invertible as required. ■

6. For a vector $v = (v_1, ..., v_n)^T \in \mathbb{R}^n$, define $||v||_1 := \sum_{j=1}^{n} |v_j|$ and for an n by n complex matrix, define

$$||A||_1 := \sup_{\substack{v \in \mathbb{R}^n \\ v \neq 0}} \frac{||Av||_1}{||v||_1}$$

Show if $A = [a_{ij}]$, then

$$||A||_1 := \max_{1 \leq j \leq n} \sum_{i=1}^{n} |a_{ij}|$$

Solution: Let $M := \max_{1 \leq j \leq n} \sum_{i=1}^{n} |a_{ij}|$. First notice that M is obtained using one of the vectors $(0, .., 0, 1, 0, ..0)^T$ (namely the one corresponding to the max) so $||A||_1 \leq M$. Next, we have

$$\begin{aligned}
M \leq ||A||_1 &= \sup_{\substack{v \in \mathbb{R}^n \\ v \neq 0}} \frac{||Av||_1}{||v||_1} = \sup_{\substack{v \in \mathbb{R}^n \\ v \neq 0}} \frac{\sum_{i=1}^{n} \left| \sum_{j=1}^{n} a_{ij} v_j \right|}{\sum_{j=1}^{n} |v_j|} \\
&\leq \sup_{\substack{v \in \mathbb{R}^n \\ v \neq 0}} \frac{\sum_{i=1}^{n} \sum_{j=1}^{n} |a_{ij} v_j|}{\sum_{j=1}^{n} |v_j|} = \sup_{\substack{v \in \mathbb{R}^n \\ v \neq 0}} \frac{\sum_{j=1}^{n} |v_j| \sum_{i=1}^{n} |a_{ij}|}{\sum_{j=1}^{n} |v_j|} \\
&\leq \sup_{\substack{v \in \mathbb{R}^n \\ v \neq 0}} \frac{M \sum_{j=1}^{n} |v_j|}{\sum_{j=1}^{n} |v_j|} = M
\end{aligned}$$

This shows that $||A||_1 = M$ as required. ■

7. Let A be an n by n matrix with diagonal entries s and all off-diagonal entries t. For which complex values is this matrix not invertible? For each of these describe the null space of A including its dimension.

   Solution: Recall that a matrix is not invertible if and only if it has an eigenvalue of zero. So we solve $Ax = 0$ where $x = (x_1, .., x_n)^T \neq 0$. this becomes

   $$tx_1 + ... + tx_{i-1} + sx_i + tx_{i+1} + ... + tx_n = 0$$

   or equivalently,

   $$(s - t)x_i + tR = 0$$

   for every $1 \leq i \leq n$. Summing all these together and setting $R = x_1 + ... + x_n$ gives

   $$(s + (n - 1)t)R = 0$$

   This gives us either $R = 0$ or $s = (1 - n)t$. In the first case, the above tells us that either each $x_i = 0$, which can't happen as x is non-zero or it tells us that $s = t$. In this case we have two possible nullspaces for A. If $s = t = 0$, then $A = 0$ and the null space has full dimension. If $s = t \neq 0$, then A has dimension $n - 1$ and consists of vectors $(1, -1, 0, .., 0)^T, (1, 0, -1, 0, .., 0)^T, ..., (1, 0, .., 0, -1)^T$. In the second case, $s = (1 - n)t$ and so $A = tB$ where B is the matrix of all ones except on the diagonal where it has $1 - n$. Clearly, $(1, .., 1)^T$ is an eigenvector and hence lies in the nullspace. To see the dimension of the nullspace is indeed 1, negate the first row. Then take the first row and add it to all subsequent rows one at a time (so sort of like a Gaussian Elimination). Then multiply all non first rows by $\frac{-1}{n}$ and add all rows to the first row to get a zero row on the top and all other rows are non-zero (and are not multiples of the other rows). ■

4 Group Theory

Theorem 4.1. *(Lagrange's Theorem) Let G be a finite group and $H \leq G$. Then $|H| \mid |G|$.*

Theorem 4.2. *(First Isomorphism Theorem) Let G and H be groups and $\phi : G \to H$ a group homomorphism. Then $G/\ker(\phi) \cong \text{im}(\phi)$ in particular, if ϕ is one to one, then $G/\ker(\phi) \cong H$.*

Theorem 4.3. *(Third Isomorphism Theorem) Let G be a group and H and K normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong (G/K)$*

Theorem 4.4. *(The Class Equation) Let G be a finite group and let R be a set of representatives from each conjugacy class (not in the centre). Then*

$$|G| = |Z(G)| + \sum_{a \in R} [G : C_G(a)]$$

where $Z(G)$ is the centre of the group (all commutative elements) and $C_G(a) = \{g \in G \mid ag = ga\}$ a subgroup of G called the centralizer.

Theorem 4.5. *(Sylow's First Theorem) Let G be a finite group with $|G| = p^n m$ with p a prime and $\gcd(p, m) = 1$. Then, there exist p-subgroups (group of prime power order) of order p^k for $k = 0..n$. In particular, there exists a Sylow p-subgroup (ie a subgroup of order p^n).*

Theorem 4.6. *(Sylow's Second Theorem) Let G be a finite group with $|G| = p^n m$ with p a prime and $\gcd(p, m) = 1$. If P is a Sylow p-subgroup and Q is and p-subgroup, then there is an element $g \in G$ so that $Q \leq gPg^{-1}$. This means Q is contained in a conjugate of P. In particular, all Sylow p-subgroups are conjugate to each other.*

Theorem 4.7. *(Sylow's Third Theorem) Let G be a finite group with $|G| = p^n m$ with p a prime and $\gcd(p, m) = 1$. Let n_p be the number of Sylow p-subgroups. Then $n_p \equiv 1 \pmod p$. Moreover, $n_p \mid m$ as n_p is the index of the normalizer $[G : N_G(P)]$ for any Sylow p-subgroup P (where $N_G(P) = \{g \in G \mid gPg^{-1} \in P\}$).*

Theorem 4.8. *(Cauchy's Theorem) Let G be a finite group and p a prime dividing the order of G. Then there is an element of order p.*

Theorem 4.9. *(Fundamental Theorem of Finitely Generated Abelian Groups) Let G be a finitely generated abelian group. Then G is isomorphic to copies of $\mathbb{Z}$ along with copies of $\mathbb{Z}_{p_i^{\alpha_i}}$ for primes p_i. That is,*

$$G \cong \mathbb{Z}^{\alpha} \times \mathbb{Z}_{p_1^{\alpha_1}} \times ... \times \mathbb{Z}_{p_k^{\alpha_k}}$$

for primes p_i and non-negative integers α, α_i.

Definition 4.10. A group G is called *solvable* if there is a subnormal series

$$\{1\} = G_0 \leq G_1 \leq ... \leq G_n = G$$

where $G_{i-1} \trianglelefteq G_i$ and G_i/G_{i-1} is abelian for all $i = 1, ..n$.

4.1 Random Group Theory Questions

1. Let G be a group of even order. Show that G contains an element of order 2.

   Solution: Note that if a is an element of order n then so is a^{-1} for if not, then $(a^{-1})^k = 1 \Rightarrow a^k = 1$ and thus must have the same order. Pair off elements with their inverses. Note that the identty is its own inverse. We go through the list and eventually we must reach an element who's partner is itself. This element has order 2 as claimed. ■

2. Show that the kernel of a group homomorphism is a normal subgroup. Moreover, show that the image is a subgroup.

   Solution: Let $\phi : G \to H$ be a group homomorphism for groups G and H. Let $K := \ker(\phi)$ and $I := \mathrm{im}(\phi)$. If $a \in K$ then $\phi(a) = e$. Moreover, as $e \in K$, we have

   $$e = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = \phi(a^{-1})$$

   so $a^{-1} \in K$. Next, if $a, b \in K$, then $\phi(ab) = \phi(a)\phi(b) = (e)(e) = e$. So K is a subgroup. If $g \in G$ then $gag^{-1} \in K$ since

   $$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = e$$

   So K is normal in G. Similarly, the image is a subgroup of G. ■

3. Let $H, K \leq G$ with $G = HK$, $H \cap K = \{e\}$ and elements of H commute with elements of K. Then $G \cong H \times K$.

   Solution: We define a homomorphism $\phi : H \times K \to G$ via $\phi(h, k) = hk$. This is a homomorphism since

   $$\phi((h, k) * (j, l)) = \phi(hj, kl) = hjkl = hkjl = \phi((h, k))\phi((j, l))$$

   where the second to last equality holds by the commuting property. This map is injective as

$$\phi((h,k)) = \phi((j,l)) \Rightarrow hk = jl \Rightarrow j^{-1}h = lk^{-1}$$

Note that the right hand side is in H and the left hand side is in K hence both sides lie in $H \cap K = \{e\}$. This gives us that $h = j$ and $k = l$ and hence ϕ is injective. Since $G = HK$ we have that every element of G can be written as hk and hence is surjective as $\phi(h,k) = hk$. Thus ϕ is an isomorphism and so $H \times K \cong G$. ■

4. Let $G = NK$ with $N \trianglelefteq G$ and $K \trianglelefteq G$ and $N \cap K = \{e\}$. Show that $ab = ba$ for all $a \in N$ and $b \in K$.

   Solution: Consider $aba^{-1}b^{-1}$. Notice that $aba^{-1} \in K$ by normality of K and $b^{-1} \in K$ so $aba^{-1}b^{-1} \in K$. Similarly, $a \in N$ and $ba^{-1}b^{-1} \in N$ so $aba^{-1}b^{-1} \in N$. Thus, $aba^{-1}b^{-1} \in N \cap K = \{e\}$ and hence $aba^{-1}b^{-1} = e$, that is $ab = ba$ as claimed. ■

5. Let $G = NK$ with $N \trianglelefteq G$ and $K \trianglelefteq G$ and $N \cap K = \{e\}$. If $< a >= N$ and $< b >= K$ (ie N and K are cyclic), show that G is abelian.

   Solution: The above shows $ab = ba$. Notice that any element of G is just a^ib^j. So let $a^ib^j, a^kb^l \in G$. Then,

$$a^ib^ja^kb^l = a^{i+k}b^{j+l} = a^{k+i}b^{l+j} = a^ka^ib^lb^j = a^kb^la^ib^j$$

   showing that G is abelian. ■

6. Find all group automorphisms of $(\mathbb{Q}, +)$. Moreover, find all automorphisms of finite order.

   Solution: Let $\phi : \mathbb{Q} \to \mathbb{Q}$ be an automorphism. Note that group automorphisms preserve the additive identity and so $\phi(0) = 0$. Let $\phi(1) = c$. Note that

$$\phi(n) = \phi(\underbrace{1 + 1 + ... + 1}_{n\ times}) = \underbrace{\phi(1) + \phi(1) + ... + \phi(1)}_{n\ times}) = n\phi(1) = nc$$

   Also, note $0 = \phi(0) = \phi(1-1) = \phi(1) + \phi(-1) = 1 + \phi(-1) \to -c = \phi(-1)$ and so as before, $\phi(-n) = -nc$. Hence $\phi(n) = nc$ for all $n \in \mathbb{Z}$. As well, if $n \neq 0$,

$$c = \phi(1) = \phi(\frac{n}{n}) = \phi(\underbrace{\frac{1}{n} + \frac{1}{n} + ... + \frac{1}{n}}_{n\ times}) = \underbrace{\phi(\frac{1}{n}) + \phi(\frac{1}{n}) + ... + \phi(\frac{1}{n})}_{n\ times}) = n\phi(\frac{1}{n})$$

   and so $\phi(\frac{1}{n}) = \frac{c}{n}$ giving for all $n, m \in \mathbb{Z}$ with $n \neq 0$, $\phi(\frac{m}{n}) = m\phi(\frac{1}{n}) = \frac{m}{n}c$ and so $\phi(q) = qc$ for all $q \in \mathbb{Q}$. It is clear that this is an automorphism so long as $c \neq 0$. Injectivity follows from

$$\phi(p) = \phi(q) \Leftrightarrow pc = qc \Leftrightarrow p = q$$

   For surjectivity, note that for any $q \in \mathbb{Q}$ we have that $\phi(\frac{q}{c}) = q$. Now, the automorphisms of finite order have the property that $\phi^n(q) = q$ for some $n \in \mathbb{N}$. In this case, $qc^n = q$ and consequently, c is a root of unity. The only rational roots of unity are 1 and -1 corresponding to $n = 1$ and $n = 2$. Hence there are only two automorphisms of finite order.

7. Let G be a group and $H \leq G$ with $[G : H] = n$. Suppose $g \in G$.

(i) Show that $g^k \in H$ for some $0 < k \leq n$

(ii) Show by example that g^n may not lie in H

Solution:

(i) Consider $H, gH, ..., g^nH$. Since $[G : H] = n$ we must have that (at least) two of these cosets are the same. Suppose that $g^jH = g^lH$ and without loss of generality, $n \geq j > l$. Notice that $g^{j-l}H = H$ and hence $g^{j-l} \in H$. Since $n \geq j > l, n \geq j - l > 0$ as required. ■

(ii) Consider $G = S_n$ and H a subgroup of G consisting of all permutations of the elements $1, .., n-1$. Notice that $H \cong S_{n-1}$. Hence $[G : H] = \frac{n!}{(n-1)!} = n$. Let $g = (2 \dots n)$. Notice that $g \notin H$. Moreover, note $g^{n-1} = 1 \in H$ so $g^n = g \notin H$ as required. ■

8. Let G be a finite group with $|G| = ab$ and $\gcd(a, b) = 1$. Suppose that H is a normal subgroup of G with order a. Show that H contains every subgroup of G whose order divides a. Find a counter example when H is not normal.

Solution: For a counter example, consider $G = S_3$ and $H =< (1, 2) >$ (note that the subgroup of S_3 of size 3 is normal since its index is 2). Now consider $K =< (2, 3) >$. Notice that K is not contained in H but both K and H have order equal to 2. Now, with the original question, consider the map

$$\pi : G \to G/H$$

Let K be a subgroup of G whose order divides a. Then we know that $\pi(K)$ is a subgroup of G/H. Notice that the size of G/H is b and that the group $\pi(K)$ has order dividing a. This can only occur if $\pi(K) = \{1\}$ which occurs only if $K \subseteq H$ as required. ■

9. Let G be an abelian group on generators x, y, z subject to

$$32x + 33y + 26z = 0 \tag{2}$$
$$29x + 31y + 27z = 0 \tag{3}$$
$$27x + 28y + 26z = 0 \tag{4}$$

How many elements does G have? Is G cyclic?

Solution: Subtracting (2) and (4) yields

$$5x + 5y = 0 \tag{5}$$

Subtracting (3) and (4) yields

$$2x + 3y + z = 0 \tag{6}$$

Summing the previous two equations (after isolating for z) yields

$$z = 3x + 2y \tag{7}$$

Subbing (6) into (2) yields (after simplifying using (5))

$$25y = 0 \tag{8}$$

Taking (5) and multiplying by 5 along with (8) yields

$$25x = 0 \tag{9}$$

Similarly, 25 times (6) yields

$$25z = 0 \tag{10}$$

Using (3) and (5) yields

$$2z = x - y \tag{11}$$

Examining the original set of equations, we see they are equivalent to

$$z = 3x + 2y \tag{12}$$
$$5x + 5y = 0 \tag{13}$$

This tells us that our group is generated by two elements x, y (as z is redundant). We know that x and y have order 25. So our group has at most 625 elements. But $5x = 20y$ so 125 of the elements are redundant leaving us with a 500 element group. ■

4.2 Classification of Small Ordered Groups

1. Classify all groups of order 4.

   Solution: Let G be a group or order 4. Let $a \in G \backslash \{e\}$. If $|a| = 4$ we are done. Otherwise, $|a| = 2$ (by Lagrange's Theorem). Pick a $b \in G \backslash < a >$. Again $|b| = 2$ and note that $ab! = a$ or b or e (otherwise $b = e, a = e$ or $a = b^{-1}$, all contradictions). So $G = \{e, a, b, ab\} =< a >< b >$. Note that ba must equal (by similar reasoning to above) ab. Hence, elements of $< a >$ commute with elements of $< b >$ and $< a > \cap < b >= \{e\}$. Thus, by the above exercise (3.), $G \cong < a > \times < b > \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. ■

2. Classify all groups of order 6.

   Solution: By Cauchy's theorem (4.8) there exists an element of order 2 and one of order 3 say a and b respectfully. Notice that $< a >$, $< a > b$ and $< a > b^2$ generate G. So $G = \{e, a, b, ab, b^2, ab^2\}$. Now, we look at ba. A quick check shows that it must be equal to ab or ab^2. If $ab = ba$, then the elements of $< a >$ commute with the elements of $< b >$, $< a > \cap < b >= \{e\}$, and $G =< a >< b >$ and so by the above exercise (3.), $G \cong < a > \times < b > \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. If $ab^2 = ba$ then $ab = b^2 a$. This group is non-abelian. In fact, it can be shown that this group is isomorphic to S_3 by sending $a \mapsto (12)$ and $b \mapsto (123)$. Hence there are two groups of order 6, namely Z_6 and S_3. ■

3. Classify all groups of order 8.

   Solution: We know there should be 5. Three are abelian and then we have D_4 and Q. Let's show this directly. If G has an element of order 8, then $G \cong \mathbb{Z}_8$. Suppose that every element of G has order 2 and let $x, y, z \in G$ be distinct nonidentity elements with $z \neq xy$. Notice here that $xy = yx$ (as $yx = x, yx = y$ lead to contradictions) and in particular that G is abelian (since $xz = zx$ and $yz = zy$ by similar reasoning). Then note that $H := \{e, x, y, xy\}$ is a subgroup and by the classification above, is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Setting $K :=< z >$ and noting that $G = HK$, $H \cap K \cong \{e\}$, and the elements of H and K commute, we see that from the above exercise (3.) that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

   Lastly, assume that G has an element of order 4, say x. let $y \in G \backslash < x >$. Notice that $< x >$ and $< x > y$ generate G, that is $G = \{e, x, x^2, x^3, y, y, xy, x^2y, x^3y\}$. Looking at yx and noting that it cannot be e, x, x^2, x^3, y nor x^2y as the last one forces

$$yx = x^2y \Rightarrow x = y^{-1}x^2y \Rightarrow x^2 = y^{-1}x^2yy^{-1}x^2y = e$$

a contradiction. So $yx = xy$ or $yx = x^3y$. If $yx = xy$, then G is abelian. If $y^2 = e$, then sending $x \mapsto (1, 0)$ and $y \mapsto (0, 1)$ gies an isomorphism with $\mathbb{Z}_4 \times \mathbb{Z}_2$. If $y^2 = x^2$ then sending $x \mapsto (1, 0)$ and $xy^{-1} \mapsto (0, 1)$ gies an isomorphism with $\mathbb{Z}_4 \times \mathbb{Z}_2$(or invoking the structure theorem for abelian groups (4.9) gives us that it must be isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_2$ immediately). If instead $yx = x^3y$, then if $y^2 = e$ we can quickly see an isomorphism with D_4. If $y^2 = x^2$, then sending $x \mapsto i$ and $y \mapsto j$ gies an isomorphism with Q. This completes the classification. ■

4. Classify all groups of order 12.

   Solution: Once again there are 5. Two abelian, A_4, D_6 and a semi-direct product of $\mathbb{Z}_3$ and $\mathbb{Z}_4$.

5. Show that a group of order 15 must be cyclic.

   Solution: Let G be a group of order $15 = 3 \times 5$. We use the Sylow Theorems. Note that $n_3 \mid 5$ and $n_3 \equiv 1$ so $n_3 = 1$. Hence if P is a Sylow-3 subgroup, then it is normal. Next, note $n_5 \mid 5$ and $n_5 \equiv 1$ so $n_5 = 1$ and thus if Q is a Sylow-5 subgroup, then it is normal (recalling that n_i is the index or the normalizer of P_i in G by (4.7)). A quick count shows that there are 15 distinct elements in PQ, since $P \cap Q = \{e\}$, and so $G = PQ$. The above shows that G must be abelian. Now, notice that the ordre of ab is 15 and hence G is cyclic as required. ■

6. Classify all groups of order 21.

7. Classify all groups of order 30.

8. Classify all groups of order 45.

4.3 Group Actions

Definition 4.11. A group action on a set X is a map ϕ from $G \times X \to X$ satisfying

(i) $\phi(gh, x) = \phi(g, \phi(h, x))$

(ii) $\phi(e, x) = x$

Lemma 4.12. *Let G act on a set X. Then the map $\phi : G \to S_X$ defined by $\phi(g) = \tau_g$ where $\tau_g(x) = gx$ is a well defined group homomorphism*

Proof. First, we show that for all $g \in G$ the map τ_g is a permutation of X. It suffices to show that τ_g is an isomorphism. If $\tau_g(x) = \tau_g(y) \Leftrightarrow gx = gy \Leftrightarrow x = y$ showing injectivity. Next, if $x \in X$ then so is $g^{-1}x$ and $\tau_g(g^{-1}x) = g(g^{-1}x) = (gg^{-1})x = x$. Hence, $\tau_g \in S_X$. Next, it is a group homomorphism as for all $x \in X$,

$$\phi(gh)(x) = \tau_{gh}(x) = (gh)x = g(hx) = \tau_g(\tau_h(x))$$

This completes the proof. ■

Theorem 4.13. *(Cayley's Theorem) Every group is isomorphic to a subgroup of S_n for some sufficiently large n.*

Proof. Let G be a group and let it act on the underlying set $X = G$ via left multiplication. TO BE COMPLETED!!! ■

Let G be a group, H a proper subgroup of G and $X = \{xH \mid x \in G$, the set of left cosets. Define $\phi : G \to S_X$ via $\phi(g) = \tau_g$ where $\tau_g(xH) = gxH$.

(i) Show that this is a well defined map, that is that τ_g actually is a permutation.

(ii) Show if $|G| \nmid [G : H]!$ then G has a nontrivial proper normal subgroup, that is, G is not simple.

Solution:

(i) (See above)

(ii) Consider $K := \ker(\phi)$. I claim that K is not the identity and is not the whole of G. Thus, K is a proper nontrivial normal subgroup. If $K = \{e\}$, then ϕ is one to one. The first isomorphism theorem (4.2) gives us that $G \cong \text{im}(\phi) \leq S_X$. Note that $|S_X| = [G : H]!$ and so by Lagrange's Theorem (4.1), we have that $|G| = |\text{im}(\phi)| \mid |S_X| = [G : H]!$ a contradiction. Next, suppose $K = G$. Then every τ_g is the identity permutation so $gxH = xH$ for all $g \in G$ and $xH \in X$. In particular, $H = gg^{-1}H = g^{-1}H$ so $g^{-1} \in H$ and hence $g \in H$ for any arbitrary $g \in G$. this implies $G = H$, a contradiction since H was chosen to be proper in G. Hence G is not simple.

1. Let G be a group and suppose that H is a subgroup whose index is p, the smallest prime dividing G. Show that H is normal.

   Solution: This solution is ver similar to the solution of the problem where $|G| \nmid [G : H]!$. Let $X = \{xH \mid x \in G$, the set of left cosets. Define $\phi : G \to S_X$ via $\phi(g) = \tau_g$ where $\tau_g(xH) = gxH$. Consider $K := \ker(\phi)$. Let $[H : K] = k$ and note $[G : K] = [G : H][H : K] = pk$ The first isomorphism theorem (4.2) gives us that $G/K \cong \text{im}(\phi) \leq S_X$. Note that $|S_X| = [G : H]! = p!$ and so by Lagrange's Theorem (4.1), we have that $pk = |G/K| = |\text{im}(\phi)| \mid |S_X| = [G : H]! = p!$. This gives $k|(p-1)!$. However, k has only prime divisors larger than or equal to p by definition of p. this gives us that $k = 1$ and hence $[H : K] = 1$ giving $H = K$. Since K is normal, H must be as well as required. ■

4.4 Application of Class Equation

1. Let G be a group with $|G| = p^n$. Show that the centre is nontrivial.

   Solution: Recall the class equation (4.4).

$$|G| = |Z(G)| + \sum_{a \in R} [G : C_G(a)]$$

   Notice that $|Z(G)| \geq 1$ as it contains the identity element. Moreover, each $[G : C_G(a)]$ divides the order of the group and is not 1 for any a not in the centre and so $p \mid [G : C_G(a)]$ for each a. In particular, since $p \mid |G|$ we must have that $p \mid |Z(G)|$ and so must be nontrivial.

2. Show that any group of order p^2 is abelian.

   Solution: Using the class equation (or by the previous problem) we see that the centre of the group must have order p or p^2. If it has order p^2 then we are done (as the centre is the entire group) so suppose the order is p. Then choose $x \in G \backslash Z(G)$. Notice that $Z(G) \subseteq C_G(x) \subsetneq G$ (the last one holds since x cannot commute with everything as $x \notin Z(G)$). Lagrange's Theorem tells us that the order of $C_g(x)$ divides the order of G and so must be p or p^2. This forces $C_G(x) = Z(G)$ and since $x \in C_G(x)$, this is a contradiction. Hence $G = Z(G)$ and the group is abelian.

3. Prove that every group of order p^m with p a prime number can be generated by m elements.

   Solution: We proceed by induction. The $m = 1$ case is trivial. Assume true for all $k < m$. Now, let G be a group of order p^m. The class equation tells us that the centre is nontrivial. In particular $Z(G)$ has order p^k with $k \le m$. If $k = m$ we are finished. Otherwise $Z(G)$ can be generated by k elements. Consider the onto projection map

$$\pi : G \to G/Z(G)$$

   $G/Z(G)$ is a group of size p^l with $l < m$ (since $k \neq m$) and $l + k = m$. This can be generated by l elements say $h_1, ..h_l$. Considering these elements as elements of g, I claim that these elements along with the generators of $Z(G)$ generate G. Let $g \in G$. Then $g \in aZ(G)$ for some $a \in G$ as elements must lie in a coset. Hence $g = az$ for some z in $Z(G)$. Now $\pi(g) = a$ and so a can be generated by elements of $G/Z(G)$. Taking the collection of the elements that generate a and z gives us that g is generated by these elements. Since g was arbitary, we have that G is generated by $l + k = m$ elements completing the induciton and the proof. ■

4. Let p be a prime number and G a group of order p^3. Show that for any $g, h \in G$, we have that $g^p h = hg^p$.

   Solution: One way to solve this is to classify all groups of order p^3. Not a bad solution but a bit tedious. Let's instead examine the orders of g and h. Firstly, if g has order 1 then $g = e$ and we win. If g has order p then $g^p = e$ and we win. If g has order p^3, then the group is cyclic and we win. So we may assume that g has order p^2. Similarly, h has to have either order p or p^2. Consider $< g > \cap < h >$. If $< g > \cap < h >= \{e\}$ then since $< g >$ and $< h >$ combine for at least $p^2 + p - 1$ distinct elements. Thus we know that one of g^k or h^l are in $Z(G)$. This implies that either $g^p \in Z(G)$ or $h \in Z(G)$. If $< g > \cap < h > \neq \{e\}$, then since the intersection is a subgroup (and proper since $h \notin < g >$), we must have that $g^p \in < g > \cap < h >$ (the subgroup has order p and only g^p and its powers satisfy the fact that the elements must have prime order). This means $g^p \in < h >$ and hence g^p and h commute as requires. ■

4.5 Application of Sylow's Theorems

1. Let G be a group of order pq with p and q prime, $p < q$ and $p \nmid q - 1$. Show G is abelian. Moreover, prove it is cyclic.

   Solution: By Sylow's Third Theorem (4.7), note that $n_p \equiv 1 \pmod{P}$ and $n_p \mid q$. So $n_p = 1$ or q. If $n_p = q$ then $q \equiv 1 \pmod{p}$ and so $p \mid q-1$ a contradiction. So $n_p = 1$. Since $p < q$ and $n_q \mid p$ we have that $n_q = 1$. So let P be the Sylow p-subgroup and Q be the Sylow q-subgroup. By the above, we know each is normal in G. Moreover, an element count shows $G = PQ$ and $P \cap Q = \{e\}$. If we show G is abelian, by a previous exercise, we know $G \cong P \times Q$ and hence is cyclic as P and Q are two cyclic groups of coprime order. By (5.) we see that G is abelian as claimed.

2. Let p and q be primes with $p < q$ and $p \mid q - 1$. Show that there is a non-abelian group of order pq.

3. Let G be a group of order p^2q with p and q prime. Classify all such groups.

4. Show that a subgroup of index 2 is a normal subgroup.

   Solution: If G is a group and H is a subgroup such that $[G : H] = 2$ then there are only two distinct left cosets say H and aH (holding for any $a \in G \backslash H$). Moreover there are only two distinct right cosets H and Ha. So here we must have that $aH = Ha$ showing $aHa^{-1} = H$.

Since a was arbitrary in $G\backslash H$, we get that H is normal as required (noting of course that $aHa^{-1} = H$ holds for all $a \in H$). ■

5. Show that a group of order 36 is not simple.

   Solution: Note that $36 = 2^2 \times 3^2$ So we consider n_3. If $n_3 = 1$ we are done so suppose $n_3 \neq 1$. Then since $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 4$ we have that $n_3 = 4$. So let P and Q be two Sylow 3-subgroups (note that the order of each is 9). Consider their intersection. We know $|P \cap Q| = 3$ for if not then their intersection is trivial and this results in too many elements (as PQ has size 81 and is contained in G, a contradiction). Take a $g \in P \cup Q$ and any $a \in P \cap Q$. Notice that since the order of P and Q is 9, both are abelian (by (2.)) and hence $gag^{-1} = a$ so $g \in N_G(P \cap Q)$. This means $|N_G(P \cap Q)| \geq 3 + 6 + 6 = 15$. Since it is a subgroup of G it divides the order of G and hence must be either 18 or 36. If it is order 18, then its index is 2 in G and hence is normal by (4.). If it is 36, then the index is 1 and thus $P \cap Q$ is normal in $G = N_G(P \cap Q)$ as a group is always normal in its normalizer. This shows that a group of order 36 has a normal subgroup as claimed. ■

6. Show that a group of order 56 has a normal subgroup.

   Solution: Note $56 = 2^3 \times 7$ so we exploit Sylow's Third Theorem (4.7). If $n_7 = 1$ we are done so supose not. Then $n_7 \equiv 1 (\mathrm{mod}\ 7)$ and $n_7 \mid 8$ so $n_7 = 8$. Now, the total number of non identity elements is $6 \times 8 = 48$ this leaves 8 elements (with the identity element) left for Sylow 2-subgroups. Since a Sylow 2-subgroup has order 8, there can only be one and hence it is normal in this group. Thus a group of order 56 always has a normal subgroup. ■

7. Show that a group of order 105 is not simple.

   Solution: By Sylow's Third Theorem (4.7),

$$\begin{aligned} n_3 &\equiv 1 \pmod 3 \text{ and } n_3 \mid 35 \\ n_5 &\equiv 1 \pmod 5 \text{ and } n_5 \mid 21 \\ n_7 &\equiv 1 \pmod 7 \text{ and } n_7 \mid 15 \end{aligned}$$

   So if G is simple, none of the above numbers can be 1. Thus, $n_3 = 7, n_5 = 21, n_7 = 15$. Counting the number of elements gives $7\times2+21\times4+15\times6+1 = 14+84+90+1 = 189 > 105$ a contradiction. Hence one of n_3, n_5 or n_7 is 1 and thus is normal. So G has a normal subgroup and thus is non-simple. ■

8. Show that a group of order 3393 is not simple.

   Solution: We see that $3393 = 3^2 \times 13 \times 29$. By (4.11), we know that the minimal index of a proper subgroup is 29 as $|G| \nmid 28!$. Next, by Sylow's third theorem, $n_3 \equiv 1 (\mathrm{mod}\ 3)$ and $n_3 \mid 377 = 13 \times 29$. So if $n_3 \neq 1$ then $n_3 = 13$. But this is the index of the normalizer of a Sylow 3-subgroup contradicting the fact that the minimal index is at least 29. Hence this group is not simple. ■

9. Show if G is a group of order 105 and $n_3 = 1$, then G is abelian (and hence is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$).

10. Show that a group of order pqr for distinct primes p, q, r is not simple.

Solution: Assume without loss of generality that $p < q < r$. Sylow's Third Theorem (4.7) tells us that

$$\begin{aligned} n_r &\equiv 1 \pmod r & n_r &\mid pq \\ n_q &\equiv 1 \pmod q & n_r &\mid pr \\ n_p &\equiv 1 \pmod p & n_r &\mid qr \end{aligned}$$

and so in particular, if none of n_p, n_q, n_r equal 1, then

$$n_r = pq \quad n_q \geq r \quad n_p \geq q$$

By an element counting argument, we have

$$pqr \geq pq(r-1) + r(q-1) + q(p-1) = pqr + rq - r - q > pqr$$

as $rq > r + q$. This is a contradiction. Hence one of n_p, n_q, n_r must be 1 as required and thus our group is not simple as required. ■

11. Let F be a field. Show that every finite subgroup of the multiplicative group F^* is cyclic.

Solution: We prove this by induction on the size of the finite subgroup $H \leq F^*$. If $|H| = 1$ then this is trivial. Assume the claim is true for all $|H| \leq n$. For $|H| = n$ consider a Sylow p-subgroup P where $p|n$ and $|P| = p^k$. Since F is a field, H is abelian and hence P is a normal subgroup. If $H = P$ then notice that all subgroups of P are cyclic which can only happen if $P \cong \mathbb{Z}_{p^{k-1}} \times \mathbb{Z}_p$ or $P \cong \mathbb{Z}_{p^k}$ using the abelianness and the Fundamental Structure Theorem for Abelian Groups (4.9) (and using the induction fact that all proper subgroups are cyclic). If the first case is true, then $P \cong < a > \times < b >$. Notice that $< a^p >< b >$ is a proper subgroup (as both subgroups are abelian and hence normal) but this group is not cyclic contradicting the induction assumption. Hence $H \cong \mathbb{Z}_{p^k}$. If $H \neq P$ then H is the product of its Sylow p-subgroups all of which are cyclic and normal. Hence H is the product of $\mathbb{Z}_{p_i^{a_i}}$ and thus H is cyclic completing the induction. Note this proof actually only requires an integral domain. ■

5 Ring Theory

Theorem 5.1. *(Eisenstein's Criterion) Suppose that $f(x) = a_n x^n + ... + a_1 x + a_0$ is such that there exists a prime number p satisfying*

(i) $p|a_i$ for all $i \neq n$

(ii) p doesn't divide a_n

(iii) p^2 doesn't divide a_0

the $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem 5.2. *(Gauss' Lemma)*

1. Show that the sum of an invertible element and a nilpotent element of a commutative ring R is invertible.

Solution: Let $a \in R$ be invertible with $ab = 1$, $b \in R$ and suppose $r \in R$ is nilpotent so that $r^n = 0$. Then consider

$$(a + r) = a(1 + br)$$

and note:

$$\frac{1}{1+br} = \frac{1}{1-(-br)} = (1 - br + b^2r^2 - b^3r^3 + ... \pm b^{n-1}r^{n-1})$$

as $r^n = 0$ so we do not use terms beyond r^n. Hence setting $c = b(1 - br + b^2r^2 - b^3r^3 + ... \pm b^{n-1}r^{n-1})$, we see that

$$\begin{aligned}(a+r)c = a(1+br)c &= a(1+br)b(1 - br + b^2r^2 - b^3r^3 + ... \pm b^{n-1}r^{n-1}) \\ &= ab(1+br)(1 - br + b^2r^2 - b^3r^3 + ... \pm b^{n-1}r^{n-1}) = 1\end{aligned}$$

■

2. Show that the sum of finitely many nilpotent elements of a commutative ring R is nilpotent.

   Solution: We prove this by induction on the nummber of summands. The result is trivial for $n = 1$. If we have two nilpotent elements a_1, a_2 with $a_1^{i_1} = 0$ and $a_2^{i_2} = 0$ (with i_j minimal and WLOG $i_1 < i_2$), then note that

$$(a_1 + a_2)^{i_1+i_2} = \sum_{j=0}^{i_1+i_2} \binom{i_1+i_2}{j} a_1^j a_2^{i_1+i_2-j}$$

   Notice that for $0 \leq j \leq i_1$ then $a_2^{i_1+i_2-j} = a_2^{i_2} a_2^{i_1-j} = 0$ and for $i_1 \leq j \leq i_2$ then $a_1^j = a_1^{i_1} a_2^{j-i_1} = 0$. Hence the above is equal to 0 and thus the sum is nilpotent. Induction takes us home. ■

3. Denote $N(R)$ to be the collection of all nilpotent elements in a commutative ring R. Show this is an ideal.

   Solution: The sum property is shown above. Zero is in this ideal clearly and moreover, if $r \in N(R)$ with $r^n = 0$ then for any $a \in R$, then $(ar)^n = a^n r^n = 0$ so $ar \in N(R)$ (where in the previous step, we used commutativity).

4. Let R be a commutative ring. Show that $N(R)$ is the intersection of all prime ideals.

   Solution: We proceed by double inclusion. Assume $N(R)$ is non empty (or else this inclusion is done) and let $r \in N(R)$ and let P be a prime ideal of the ring R. We note that $r^n = r^{n-1}r = 0 \in P$ and so by definition of prime either $r \in P$ and we're done or $r^{n-1} \in P$ and we repeat inductively to get that $r \in P$. Since P was arbitrary, every element of $N(R)$ lies in every prime ideal and hence in their intersection.

   Next, suppose that x is not a nilpotent element (so $x \in R \backslash N$). I show that x is not in the intersection of all prime ideals finishing the proof. Consider

$$S := \{I \text{ is an ideal of } R \mid x^k \notin I \text{ for all } k \geq 1\}$$

   a set of ideals. Notice that S is nonempty as it contains the zero ideal. Moreover, it is a poset with respect to inclusion and every chain has an upper bound (namely the union of all elements of S) so by Zorn's Lemma, it must contain a maximal element say P. I claim that P is prime. Suppose for two elements $a, b \in R$ that $ab \in P$ with neither a nor b in P and seek a contradiction. Then note that P is a proper subset of both $P + aR$ and $P + bR$. Hence by definition of S, we must have that $x^k \in P + aR$ and $x^l \in P + bR$ for some positive integers k and l. This implies that $x^{k+l} \in P + abR$ that is, $P + abR \notin S$. However, $P = P + abR$ since $ab \in P$ so $P \notin S$ a contradiction. Hence P is prime. Since $x \notin P$ we have that x is not in the intersection of all prime ideals. thus, $N(R)$ is the intersection of all prime ideals. ■

5. Let R be a commutative integral domain and suppose $f(x) = a_0 + a_1x + ... + a_nx^n \in R[x]$. Show that f is invertible if and only if a_0 is invertible and each a_i is zero for $1 \leq i \leq n$.

   Solution: The reverse direction is clear. Suppose f is invertible. Then notice that there is a $g = b_0 + b_1x + ... + b_mx^m \in R[x]$ with $b_m \neq 0$ and $fg = 1$. If n and m are both greater than 1, then we have that $a_nb_m = 0$. Thus both n and m must be 1. Here, we have that $1 = fg = a_0b_0$. and so a_0 is invertible. ■

6. Let R be a commutative ring and suppose $f(x) = a_0 + a_1x + ... + a_nx^n \in R[x]$. Show that f is invertible if and only if a_0 is invertible and each a_i is nilpotent for $1 \leq i \leq n$.

   Solution: Assume f is invertible. Notice that there is a $g = b_0 + b_1x + ... + b_mx^m \in R[x]$ with $b_m \neq 0$ and $fg = 1$. This gives us that $a_0b_0 = 1$ and so a_0 is invertible. Next, consider a prime ideal of R say P and examine f reduced modulo P. Notice that R/P is an integral domain and hence the previous proposition implies that a_i is zero in R/Pm that is each a_i lies in P. But P was arbitrary so this means a_i lies in each prime ideal. A previous exercise shows that this means a_i is in the nilradical and hence is nilpotent.

   For the other direction, note that a_0 is invertible and $a_1x, ..., a_nx^n$ are nilpotent thus the above propositions show us that $a_1x + ... + a_nx^n$ is nilpotent and also that $a_0 + a_1x + ... + a_nx^n$ is invertible. ■

7. Let R be a commutative ring and suppose $f(x) = a_0 + a_1x + ... + a_nx^n \in R[x]$. Show that if f is a zero divisor then there is a nonzero element $b \in R$ so that $bf = 0$.

   Solution: Let $0 \neq g = b_0 + b_1x + ... + b_mx^m \in R[x]$ so that $fg = 0$ with g of minimal degree. Expanding this gives $a_nb_m = 0$. Now $a_ng = 0$ for otherwise, we note that $\deg(a_ng) < \deg(g)$ and hence since $a_nfg = 0 \Rightarrow f(a_ng) = 0$, that is, g was not minimal, a contradiction. Thus, consider

$$\begin{aligned} fg &= (a_0 + a_1x + ... + a_{n-1}x^{n-1} + a_nx^n)g \\ &= (a_0 + a_1x + ... + a_{n-1}x^{n-1})g + (a_nx^n)g \\ &= (a_0 + a_1x + ... + a_{n-1}x^{n-1})g \end{aligned}$$

   and thus, $a_{n-1}b_m = 0$. Procceding as before, we see $a_{n-1}g = 0$ and moreover, inductively, we continue this argument to show $a_{n-r}g = 0$ for all $0 \leq r \leq n$. Thus, $a_kg = 0$ for all $0 \leq k \leq n$. It is clear then that taking $b = b_m$ gives

$$b_mf = b_m(a_0 + a_1x + ... + a_nx^n) = a_0b_m + a_1b_mx + ... + a_nb_mx^n = 0$$

   as required ■

8. Factor 143 into prime elements in $\mathbb{Z}[i]$

   Solution: Notice that $143 = 11 \times 13$. We make two claims:

   Claim: If $p \equiv 3 \pmod 4$, then p is prime in $\mathbb{Z}[i]$.

   Solution: Suppose otherwise. Consider the quadratic norm $N(a + bi) = a^2 - d * b^2 = a^2 + b^2$ (To show it is a norm only the multiplicative property needs to be checked which is routine). Suppose $p = (a+bi)(c+di)$. Notice that $p^2 = N(p+0i) = N(a+bi)N(c+di) = (a^2+b^2)(c^2+d^2)$. We make another claim,

   Claim: Let d be a square free nonzero integer. In $\mathbb{Z}[\sqrt{d}]$ unital elements correspond to elements of norm 1. Also, the unital elements when $d < 0$ are ±1 or $\pm1, \pm i$ when $d = -1$.

Solution: If $N(a+b\sqrt{d})=1$ then $a^2-db^2=1$. If $d\leq -2$ then clearly $b=0$ and $a=\pm 1$. If $d=-1$ then either $a=\pm 1$ and $b=0$ or $a=0$ and $b=\pm 1$. This corresponds to $1,-1,i,-i$, each of which are units. In general, if $N(a+b\sqrt{d})=1$ then $a^2-db^2=1$ so consider the following:

$$(a+b\sqrt{d})(a-b\sqrt{d})=a^2-db^2=1$$

hence $(a+b\sqrt{d})$ is a unit. ■

So we note that if p factors nontrivially, then we must have that $N(a+bi)=N(c+di)=p$, that is, p can be written as the sum of two squares, say $p=a^2+b^2$. However, consider this (mod 4). We get $3\equiv a^2+b^2 \pmod 4$, which is a contradiction since $a^2,b^2\in\{0,1\} \pmod 4$. So p is (a Gaussian) prime if $p\equiv 3 \pmod 4$. ■

Claim: If $p\equiv 1 \pmod 4$, then p factors in $\mathbb{Z}[i]$.

Solution: By Fermat's two squares theorem, we can write p as a sum of two squares say $p=a^2+b^2=(a+bi)(a-bi)$. Notice here that each element has prime norm and hence if $a+bi=(c+di)(e+fi)$ taking the norm yields that one of $(c+di)$ or $(e+fi)$ is unital (since it must have norm one adn the other element has norm p as p is prime). Hence p factors into two exactly two prime elements. ■

As a side note, $2=(1+i)(1-i)$ both elements on the right are prime. So we have:

$$143=11\times 13=11\times(9+4)=11(3+2i)(3-2i)$$

giving the prime factorization. ■

9. Show that 2 is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$.

Solution: Suppose that $2=(a+b\sqrt{-5})(c+d\sqrt{-5})$. I claim one of these elements is a unit. Look at the quadratic norm $N(a+b\sqrt{-5})=a^2+5b^2$. Notice that

$$4=N(2)=N((a+b\sqrt{-5})(c+d\sqrt{-5}))=N(a+b\sqrt{-5})N(c+d\sqrt{-5})=(a^2+5b^2)(c^2+5d^2)$$

thus since elements of norm 1 are units, we must have that $a^2+5b^2=2$, a contradiction. So one of$a+b\sqrt{-5}$ or $c+d\sqrt{-5}$ is a unit as claimed. Hence 2 is irreducible. Next, note that $2\cdot 3=6=(1+\sqrt{-5})(1-\sqrt{-5})$ and so if 2 is prime, then $2\mid(1+\sqrt{-5})$ or $2\mid(1-\sqrt{-5})$. In the first case, we get that $2\in(1+\sqrt{-5})$ and so there is an element such that $2=(a+b\sqrt{-5})(1+\sqrt{-5})=a-5b+(a+b)\sqrt{-5}$ and so $a=-b$ and $2=a-5b=6a$ ao $a=\frac{1}{3}$, a contradiction. Similarly, the second case yields $2\in(1-\sqrt{-5})$ and so there is an element such that $2=(a+b\sqrt{-5})(1-\sqrt{-5})=a+5b+(a-b)\sqrt{-5}$ and so $a=b$ and $2=a+5b=6a$ ao $a=\frac{1}{3}$, a contradiction. Hence 2 is not prime. ■

10. Show that $(2,1+\sqrt{-5})$ is not principal in $\mathbb{Z}[\sqrt{-5}]$.

Solution: Assume that it is principal so $(a)=(2,1+\sqrt{-5})$ for some $a\in\mathbb{Z}[\sqrt{-5}]$. This implies that $a\mid 2$ and $a\mid(1+\sqrt{-5})$ so $N(a)\mid N(2)=4$ and $N(a)\mid N(1+\sqrt{-5})=6$. This means that $N(a)=1$ or 2. Previously, we showed that $N(a)=2$ leads to a contradiction (recalling that $x^2+5y^2=2$ has no integer solutions) so we must have that a is a unit. By a previous exercise, $a=\pm 1$ and these ideals are the same so we show that $a=1$ is impossible. Otherwise, there are elements such that

$$1 = 2(w + x\sqrt{-5}) + (1 + \sqrt{-5})(y + z\sqrt{-5}) = 2w + y - 5z + (2w + y + z)\sqrt{-5}$$

So $2w + y + z = 0$ and thus $2 \mid (y + z)$ so y and z have the same parity. The above also says that $1 = 2w + y - 5z$. Since $2 \mid 2w$ and y and z have the same parity so $2 \mid (y - 5z)$ which implies $2 \mid 1$ a contradiction. Hence this ideal is not principal. ■

11. Show that the only ring automorphism of $\mathbb{R}$ is the identity automorphism.

Solution: Let $\phi : \mathbb{R} \to \mathbb{R}$ be a ring automorphism. First note $\phi(0) = 0$ and $\phi(1) = 1$ as ring automorphisms preserve the additive and multiplicative elements. Next, note for all $n \in \mathbb{N}$,

$$\phi(n) = \phi(\underbrace{1 + 1 + ... + 1}_{n\ times}) = \underbrace{\phi(1) + \phi(1) + ... + \phi(1)}_{n\ times}) = n\phi(1) = n$$

Also, note $0 = \phi(0) = \phi(1 - 1) = \phi(1) + \phi(-1) = 1 + \phi(-1) \to -1 = \phi(-1)$ and so arguing as before (or we can use $\phi(-n) = \phi(-1)\phi(n) = -n$), we have that $\phi(-n) = -n$. Hence $\phi(n) = n$ for all $n \in \mathbb{Z}$. As well, if $n \neq 0$,

$$1 = \phi(1) = \phi(\frac{n}{n}) = \phi(\underbrace{\frac{1}{n} + \frac{1}{n} + ... + \frac{1}{n}}_{n\ times}) = \underbrace{\phi(\frac{1}{n}) + \phi(\frac{1}{n}) + ... + \phi(\frac{1}{n})}_{n\ times}) = n\phi(\frac{1}{n})$$

and so $\phi(\frac{1}{n}) = \frac{1}{n}$ giving for all $n, m \in \mathbb{Z}$ with $n \neq 0$, $\phi(\frac{m}{n}) = \phi(m)\phi(\frac{1}{n}) = \frac{m}{n}$ and so $\phi(q) = q$ for all $q \in \mathbb{Q}$. Next, we make a claim.

Claim: If $a < b$ then $\phi(a) < \phi(b)$.

Solution: By considering $0 < b - a$ and showing $0 < \phi(b - a)$ it suffices to show $0 < a \Rightarrow 0 < \phi(a)$. Since $0 < a$, by the properties of the real numbers, there is a $b \in \mathbb{R}$ such that $b^2 = a$. Hence $\phi(a) = \phi(b^2) = \phi(b)^2 > 0$ as claimed. ■

Now, suppose there is an $x \in \mathbb{R}$ such that $\phi(x) \neq x$. Without loss of generality, we may assume x is positive (otherwise use $-x$). Without loss of generality, suppose $x < \phi(x)$. The density of the rational implies that there is a rational say q between x and $\phi(x)$. Thus, $x < q = \phi(q) < \phi(x)$ contradicting the claim. Hence, all real numbers map to themselves and thus ϕ is the identity automorphism as required. ■

12. Let $a, b \in \mathbb{C}$ and consider $I = \{f \in \mathbb{C}[x, y] \mid f(a, b) = 0\}$. Show that I is a maximal ideal in $\mathbb{C}[x, y]$ and find a minimal set of generators.

Solution: First, it is clear that I is an ideal for if $f, g \in I$ then $f(a, b)+g(a, b) = 0$ so $f+g \in I$ and for all $h \in \mathbb{C}[x, y]$, $h(a, b)f(a, b) = 0$ so $hf \in I$. Now I claim that $I =< x-a, y-b >$. It is clear that $< x-a, y-b >\subseteq I$. Now, since $\mathbb{C}[x, y]\setminus < x-a, y-b >\cong \mathbb{C}$, the ideal $< x-a, y-b >$ is maximal. Since $I \neq \mathbb{C}[x, y]$ (for example $1 \notin I$), we have that $I =< x-a, y-b >$ as required. Next, notice that this is a minimal set of generators. For if only one element generated I, we know that both $x - a$ and $y - b$ must divide it. Neither $x - a$ nor $y - b$ generate I on their own and this leads to a contradiction. ■

13. Let $C = C^0([0, 1], \mathbb{R})$. For $a \in [0, 1]$, define $I_a = \{f \in C | f(a) = 0\}$.

   (i) Show that I_a is a maximal ideal of C.

   (ii) Show that every maximal ideal of C is of the form I_a for some $a \in [0, 1]$.

(iii) Show that the previous part fails if $[0, 1]$ is replaced by $(0, 1)$.

Solution:

(i) Let $I_a \subseteq I \subseteq C$ where I is an ideal of C. If $I \neq I_a$, then there is an $f \in I$ such that $f(a) \neq 0$. Consider the function $-(f(x) - f(a))$. This function lies in I_a. Hence $f(x) - (f(x) - f(a)) = f(a) \in I$. Thus, I contains a constant function so multiplying by the inverse shows that the constant function $1 \in I$ and hence $I = C$ showing that I_a is maximal. ■

(ii) Seriously this question is way too large for a comp problem. Please refer to

http://www.math.washington.edu/ greenber/MATH403-MaxIdeals.pdf

(iii) Let $I = \{f | f$ vanishes on a compact set $\}$. Notice that this is not contained in any I_a. Using Zorn's lemma, we can get a maximal ideal that contains I. This cannot be any of the I_a as I cannot be contained in any of these ideals. ■

14. Let $R = \mathbb{Z}[\sqrt{-3}]$.

(i) Show that $2R \subseteq R$ is not a prime ideal

(ii) Show that 2 is an irreducible element of R.

(iii) Is R a PID?

Solution:

(i) Notice that $(1 - \sqrt{-3})(1 + \sqrt{-3}) \in 2R$ but clearly neither element is in $2R$ otherwise $\frac{1}{2} \pm \frac{\sqrt{-3}}{2} \in R$, which is absurd.

(ii) Suppose $2 = uv$ with $u, v \in R$. Let N be the usual quadratic norm, that is $N(a+b\sqrt{-3}) = a^2 + 3b^2$. Then we have that $4 = N(u)N(v)$. if one of the norms is 1 then we are done. Otherwise both elements have norm 2. That is, there is an element such that $a^2+3b^2 = 2$ a contradiction. Hence one of u, v has norm 1 and thus one of u, v is ± 1 showing 2 is irreducible as claimed.

(iii) R is not a PID for all PIDs are UFDs and since 2 is irreducible we have that $2 = (1 - \sqrt{-3})(1 + \sqrt{-3}) = (2)(1)$, that is, we have two different factorizations into irreducible elements (the left hand elements are reducible as they have norm 4 so the same argument that showed 2 is irreducible works for the other elements) ocntradicting the UFD property.

15. Let R be a PID and $I \subseteq R$ a non-zero ideal. Show that only finitely many ideals J in R contain I.

Solution: Let $I = (a)$. Then since every PID is a UFD, $a = ua_1...a_n$ and this is unique up to multiplication by a unit u. Hence, if J contains I, then since $J = (b)$, we have that there is an r such that $a = br$. But $a = a_1...a_n$ uniquely and so b has only 2^n many choices as required. ■

6 Galois Theory

1. Let E be the splitting field of $(x^2 - 3)(x^2 - 5)$ over $\mathbb{Q}$.

(i) Find $[E : \mathbb{Q}]$

(ii) Find an α such that $E = \mathbb{Q}(\alpha)$

(iii) Find $\mathrm{Gal}(E/\mathbb{Q})$

Solution:

(i) First I claim that $E = \mathbb{Q}(\sqrt{3}, \sqrt{5})$. The roots of our polynomial are $\pm\sqrt{3}$ and $\pm\sqrt{5}$ Note that $\sqrt{3} \notin \mathbb{Q}$ and so $\mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}$ and it has degree 2 over $\mathbb{Q}$ since $x^2 - 3$ is a monic polynomial with $\sqrt{3}$ as a root. Next, I claim that $\sqrt{5} \notin \mathbb{Q}(\sqrt{3})$. If not then

$$\sqrt{5} = a + b\sqrt{3} \Rightarrow 5 = a^2 + 3b^2 + 2ab\sqrt{3} \Rightarrow 5 = a^2 + 3b^2$$

which is a contradiction. As an aside, note that $\sqrt{3} \notin \mathbb{Q}(\sqrt{5})$ since

$$\sqrt{3} = a + b\sqrt{5} \Rightarrow 3 = a^2 + 5b^2 + 2ab\sqrt{5} \Rightarrow 3 = a^2 + 5b^2$$

also a contradiction. Hence, our lattice looks like the following

$$\begin{array}{ccc} & \mathbb{Q}(\sqrt{3}, \sqrt{5}) & \\ \swarrow & & \searrow \\ \mathbb{Q}(\sqrt{3}) & & \mathbb{Q}(\sqrt{5}) \\ & \searrow \quad \swarrow & \\ & \mathbb{Q} & \end{array}$$

Since the polynomial splits in $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ and it is the smallest field our polynomial splits in, we have that this is our field E. Note that $[E : \mathbb{Q}(\sqrt{3})] = 2$ as $x^2 - 5$ is a minimum polynomial (and it is not degree 1) and that $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ also by the above. Hence, by the KLM theorem, $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$ as required. ■

(ii) I claim that $\alpha = \sqrt{3} + \sqrt{5}$ suffices. It is clear that $\mathbb{Q}(\alpha) \supseteq E$. For the other direction, it suffices to show that $\sqrt{3} \in \mathbb{Q}(\alpha)$. Consider the following:

$$\begin{aligned} &(\sqrt{3} + \sqrt{5})^2 \in \mathbb{Q}(\alpha) \\ \Rightarrow &(3 + 5 + 2\sqrt{15}) \in \mathbb{Q}(\alpha) \\ \Rightarrow &\sqrt{15} \in \mathbb{Q}(\alpha) \\ \Rightarrow &\sqrt{15}(\sqrt{3} + \sqrt{5}) \in \mathbb{Q}(\alpha) \\ \Rightarrow &3\sqrt{5} + 5\sqrt{3} \in \mathbb{Q}(\alpha) \\ \Rightarrow &2\sqrt{3} \in \mathbb{Q}(\alpha) \\ \Rightarrow &\sqrt{3} \in \mathbb{Q}(\alpha) \end{aligned}$$

This completes the proof. ■

(iii) By the lattice diagram above and the Fundamental theorem of Galois Theory, we have that $\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ as required (it is a size 4 group so there are only 2 possibilities and $\mathbb{Z}_2$ only has one subgroup of size 2). ■

2. Find a cubic polynomial with integer coefficients such that $p(2\cos(40°)) = 0$. Then compute the Galois group of $p(x)$.

Solution: Notice that

$$2\cos(40°) = 2\cos(\frac{360°}{9}) = \text{cis}(\frac{360°}{9}) + \text{cis}(\frac{-360°}{9}) = \zeta_9 + \zeta_9^{-1}$$

Next note that $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$ the latter is the cyclotomic polynomial corresponding to ζ_9 so $\zeta_9^6 + \zeta_9^3 + 1 = 0 \Rightarrow \zeta_9^{-3} + \zeta_9^3 = -1$. Next note that $(\zeta_9 + \zeta_9^{-1})^3 = \zeta_9^3 + 3\zeta_9 + 3\zeta_9^{-1} + \zeta_9^{-3} = 3\zeta_9 + 3\zeta_9^{-1} - 1$. Thus, if $p(x) := x^3 - 3x + 1$ we must have

$$\begin{aligned} p(2\cos(40^\circ)) = p(\zeta_9 + \zeta_9^{-1}) &= (\zeta_9 + \zeta_9^{-1})^3 - 3(\zeta_9 + \zeta_9^{-1}) + 1 \\ &= 3\zeta_9 + 3\zeta_9^{-1} - 1 - 3(\zeta_9 + \zeta_9^{-1}) + 1 = 0 \end{aligned}$$

Notice that the conjugates of $\zeta_9 + \zeta_9^{-1}$ are $\zeta_9^2 + \zeta_9^{-2}$ and $\zeta_9^4 + \zeta_9^{-4}$ as can be seen by plugging them in and checking. Notice that $(\zeta_9 + \zeta_9^{-1})^2 - 2 = \zeta_9^2 + \zeta_9^{-2}$ and so $\zeta_9^2 + \zeta_9^{-2} \in \mathbb{Q}(\zeta_9 + \zeta_9^{-1}) = \mathbb{Q}(2\cos(40^\circ))$. As a result, this field contains two of the conjugates and hence contains the third. Thus $\mathbb{Q}(2\cos(40^\circ))$ is a normal extension and hence a splitting field for $p(x)$. Therefore, the Galois group has size 3. Since 3 is prime, we know that the Galois group must be isomorphic to $\mathbb{Z}_3$.

3. Suppose E is an algebraic extension of F and suppose that R is a subring of E containing F. Show that R is a field.

   Solution: Let $0 \neq \alpha \in R$. We show that α has an inverse and explicitly compute it. Let $p(x) := \sum_{i=0}^{n} f_i x^i$ be the minimal polynomial of α (which exists since E is an algebraic extension of F) where $f_i \in F$ and $f_0 \neq 0$ otherwise we can divide $p(\alpha)$ by at least one power of α contradicting the minimality of p. Next, since $p(\alpha) = 0$ we can multiply by α^{-1} and f_0^{-1} to see that

$$\alpha^{-1} = \frac{1}{f_0} \sum_{i=i}^{n} f_i \alpha^{i-1} \in R$$

   and hence R is a field as required. ■

4. Show that $\alpha = \cos(72^\circ)$ is algebraic and find the minimal polynomial.

   Solution: Notice that $\cos(72^\circ) = \cos(\frac{\pi}{5}) = \frac{1}{2}(\zeta_5 + \zeta_5^{-1})$. We know that $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = \phi(5) = 4$. Now I claim that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. First I show $\alpha \notin \mathbb{Q}$. Suppose it were. Then consider $p(x) := x^2 - 2\alpha x + 1$. This polynomial has the property that $p(\zeta_5) = 0$ contradicting $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$. So $\alpha \notin \mathbb{Q}$. Next, consider $q(x) := x^2 + x - 1$. Evaluating yields $q(\zeta_5) = 0$. This is exactly what we required (note: To compute q notice that $1 + \zeta_5 + ... + \zeta_5^4$ so the $x^2 + x$ term kills more of α off) . ■

5. Show that $\sin(\pi r)$ is algebraic for all $r \in \mathbb{Q}$.

   Solution: This is in a sense a generalization of the previous problem. Let $r = \frac{p}{q}$. Notice that if $z = \cos(\frac{\pi p}{q}) + i\sin(\frac{\pi p}{q}) = e^{\frac{pi\pi}{q}}$ then it is clear that $z^{2q} = 1$ and so z is algebraic. Now, notice that

$$\cos(\frac{\pi p}{q}) = \frac{z + z^{-1}}{2} \text{ and } \sin(\frac{\pi p}{q}) = \frac{z - z^{-1}}{2i}$$

   Since the set of algebraic numbers is a field, we have that both $\cos(\frac{\pi p}{q})$ and $\sin(\frac{\pi p}{q})$ are algebraic as required. ■

6. Let F be a finite field, $f(x) \in F[x]$ an irreducible polynomial of degree n and suppose that E is an extension of F. Show that if E contains one root of $f(x)$, then it contains every root of $f(x)$.

Solution: Let α be a root of $f(x)$. It suffices to show that $f(x)$ splits in $F(\alpha)$. Let $F = \mathbb{F}_q = \mathbb{F}_{p^e}$ where p is a prime and $e \in \mathbb{N}$. Consider the Frobenius homomorphism $\phi : x^{p^e}$. Since the kernel is trivial, this map must be an injective. Since F is a finite field, this is an isomorphism (as any finite field automorphism that is an injection is automatically surjective). Now, since the non-zero elements of F form a group under multiplication of order $q-1$ we have that $a^{q-1} = 1$ by Lagrange's Theorem (4.1). Thus, every element of F satisfies $a^q = a$. This means that F is fixed by ϕ. In particular, $\phi(f(x)) = f(\phi(x))$. Thus, we have $f(\phi(\alpha)) = \phi(f(\alpha)) = \phi(0) = 0$. Continuing this iterative procedure shows that α^{q^l} are all roots of f for all $l \in \mathbb{N}$. Now, we know that there are only finitely many of these elements are distinct. In fact, since $F(\alpha)$ is a finite extension of a finite field, $F(\alpha) \cong \mathbb{F}_{q^n}$ and thus $\alpha^{q^n} = \alpha$ by the above argument. I claim the list $\alpha, \alpha^q, .., \alpha q^{n-1}$ is a distinct list of roots of f. Suppose that $\alpha^{q^a} = \alpha^{q^b}$ where $a \geq b$ and $0 \leq a, b \leq n-1$. Applying ϕ a total of $n-a$ times yields $\alpha = \alpha^{q^n} = \alpha^{q^{n-a+b}}$ with $0 < n - a + bleqn$. This argument tells us that $\alpha \in \mathbb{F}_{q^{n-a+b}}$ and thus $n - a + b = n$ or $a = b$ giving that our list is unique. Hence

$$f(x) = \prod_{i=0}^{n-1} (x - \alpha^{p^i}) \in F(\alpha)[x]$$

as required. ■

7. Let $\alpha \in \mathbb{C}$ be an algebraic number and p a prime. Show that there exist field extensions of finite degree $\mathbb{Q} \subseteq F \subseteq K$ such that $\alpha \in K$, the degree $[K : F]$ is a power of p, and $[F : \mathbb{Q}]$ is prime to p.

   Solution: Let $p(x)$ be the min poly of α and n its degree. If $\gcd(n, p) = 1$, then take $F = \mathbb{Q}(\alpha)$ and $K = \mathbb{Q}(\alpha, \sqrt[p]{2})$ and this will work as $[K : F] = p$ and $[F : \mathbb{Q}] = n$. Otherwise, let $K = \mathbb{Q}(\alpha)$ and let L be the splitting field of $p(x)$. By the Fundamental Theorem of Galois Theory, we have that $\mathrm{Gal}(L/K)$ is a group of order $n = p^l m$ where $\gcd(p, m) = 1$. By Sylow's First Theorem (4.5), there is a Sylow p subgroup H of $\mathrm{Gal}(L/K)$. Again invoking the Fundamental Theorem of Galois Theory, we have that this subroup H corresponds to a subfield of K. Setting this to be F we know that $[F : \mathbb{Q}] = |H| = p^l$ and further by the KLM Theorem that $[K : F] = \frac{[K:\mathbb{Q}]}{[[F:\mathbb{Q}]} = \frac{p^l m}{p^l} = m$ and this meets the criteria as required. I have summarized the proof in the following lattice where $G = \mathrm{Gal}(L/\mathbb{Q})$, $I = \mathrm{Gal}(L/F)$ and $H = \mathrm{Gal}(L/K)$ (notice how the diagram flips).

$$\begin{array}{ccc} L & \qquad\qquad\qquad & G \\ | & & | \\ K & & I \\ | & & | \\ F & & H \\ | & & | \\ \mathbb{Q} & & \{e\} \end{array}$$

   Done! ■

8. Factor $p(x) = x^3 - 3x + 3$ and find the Galois group of its splitting field if the ground field is

   (i) $\mathbb{R}$

   (ii) $\mathbb{Q}$

   Solution:

(i) Notice that $p(-3) < 0 < p(-2)$ so the Intermediate Value Theorem (1.1) says that there is a real root α between -2 and -3. notice that $p'(x) = 3x^2 - 3$. This tells us that the function is increasing up to -1, decreasing to 1 and increasing there out. Since $f(-1) = 5 > f(1) = 1 > 0$, we know that there is only one real root. This function hence has one real root and two complex roots that are conjugates. Thus, we know that the splitting field of this polynomial over $\mathbb{R}$ is a degree two splitting field and hence its Galois group isomorphic to $\mathbb{Z}_2$. ■

(ii) By Eisenstein's Criteria (5.1) using 3, this polynomial is irreducible over the rationals. By the above, it has one real root and two complex roots. Let β be one of the complex roots. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$. this means that the splitting field $E = \mathbb{Q}(\alpha, \beta)$ has degree 6. Since the Galois group is a subgroup of S_3 (remember elements of the Galois group are simply root permutations), it must be that it is equal to S_3 as required. ■

9. Let F be a field and let $f(x) := \prod_{i=1}^{n}(x - \alpha_i) \in F[x]$ be a polynomial. Define the discriminant of f by

$$D(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$$

(i) Suppose $f(x) = x^3 + ax + b$. Show that $D(f) = -4a^3 - 27b^2$.

(ii) Show that the polynomial $f(x) = x^3 - 48x + 64$ is irreducible over $\mathbb{Q}$.

(iii) Compute the Galois group over $\mathbb{Q}$ of $x^3 - 48x + 64$.

Solution:

(i) Notice that

$$f'(x) = (x - \alpha_1)(x - \alpha_2) + (x - \alpha_1)(x - \alpha_3) + (x - \alpha_2)(x - \alpha_3)$$

In particular,

$$\begin{aligned} f'(\alpha_1) &= (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) \\ f'(\alpha_2) &= (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3) \\ f'(\alpha_3) &= (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) \\ D(f) &= -f'(\alpha_1)f'(\alpha_2)f'(\alpha_3) \end{aligned}$$

In this light, notice that $f'(x) = 3x^2 + a$ and hence

$$\begin{aligned} -f'(\alpha_1)f'(\alpha_2)f'(\alpha_3) &= -(3(\alpha_1)^2 + a)(3(\alpha_2)^2 + a)(3(\alpha_3)^2 + a) \\ &= -27\alpha_1^2\alpha_2^2\alpha_3^2 - 9a(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) - 3a^2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) - a^3 \end{aligned}$$

By expanding $f(x) := \prod_{i=1}^{n}(x - \alpha_i)$ and comparing coefficients, we see that

$$\begin{aligned} -\alpha_1\alpha_2\alpha_3 &= b \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= a \\ \alpha_1 + \alpha_2 + \alpha_3 &= 0 \end{aligned}$$

Squaring all three equations yields (after simplification)

$$\begin{aligned} \alpha_1^2\alpha_2^2\alpha_3^2 &= b^2 \\ \alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2 &= a^2 \\ \alpha_1^2 + \alpha_2^2 + \alpha_3^2 &= -2a \end{aligned}$$

Substituting for $D(f)$ finally gives

$$\begin{aligned} D(f) &= -27\alpha_1^2\alpha_2^2\alpha_3^2 - 9a(\alpha_1^2\alpha_2^2 + \alpha_1^2\alpha_3^2 + \alpha_2^2\alpha_3^2) - 3a^2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) - a^3 \\ &= -27b^2 - 9a(a^2) - 3a^2(-2a) + a^3 = -4a^3 - 27b^2 \end{aligned}$$

as required. ■

(ii) Consider this equation in $\mathbb{Z}_5$. It becomes $p(x) \equiv x^3 - 3x + 4 (\text{mod } 5)$. Now, if the polynomial is reducible, then it has a linear factor and by the factor theorem, evaluating the polynomial at this root must give you zero. In particular, when reduced modulo 5, then we must get that one of the numbers from $0, ..4$ must be such that $p(i) \equiv 0$. Notice

$$p(0) \equiv 4 \quad p(1) \equiv 2 \quad p(2) \equiv 1 \quad p(3) \equiv 2 \quad p(4) \equiv 1$$

Notice that none of these are zero and hence $f(x)$ cannot have a linear factor. Hence $f(x)$ is ireducible over $\mathbb{Q}$ (I've probably implicitly used Gauss' Lemma here as well). ■

(iii) Notice that the discriminant is equal to

$$\begin{aligned} D(f) &= -4a^3 - 27b^2 = -4(-48)^3 - 27(64)^2 = 2^2(2^4 3)^3 - 3^3(2^6)^2 = 2^{14}3^3 - 3^3 2^{12} \\ &= 2^{12}3^3(4-1) = 2^{12}3^4 \end{aligned}$$

This is a perfect square. Thus, $\sqrt{D(f)} \in \mathbb{Q}$. Notice that since $f(x)$ is irreducible, this means that the Galois group has order either 3 or 6 and since it is isomorphic to a subgroup of S_3, we have that it equals either A_3 or S_3. Notice that the permutation σ that fixes $\mathbb{Q}$ (and hence $\sqrt{D(f)}$ as it is rational) and that changes only two roots (say α_1 and α_2) gives

$$\begin{aligned} D(f) = \sigma(\sqrt{D(f)}) = \sigma((\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)) \\ &= (\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3) \\ &= -\sqrt{D(f)} \end{aligned}$$

Which is a contradiction. Hence there can only be 3 elements in the Galois group and thus the Galois group is isomorphic to A_3. ■