Qualifying Exams Study Guide

Personal study guide made to prepare for PhD qualifying exams at the University of British Columbia. Covers basic analysis (real, complex) and abstract algebra (linear, group theory, ring, field/Galois theory), at the 2nd, perhaps 3rd, year undergraduate level.

Notes by Louis Meunier

1 Analysis

1.1 Real

1.1.1 Fundamentals

Definition 1 (Metric Space): A *metric space* is a set X equipped with a *metric* function $d : X \times X \to \mathbb{R}_{\geq 0}$ that satisfies:

(i) $d(x, y) \geq 0$ and equals 0 iff $y = x$
(ii) $d(x, y) = d(y, x)$
(iii) $d(x, z) \leq d(x, y) + d(y, z)$

Definition 2 (Convergence, Subsequences): A *sequence* $\boldsymbol{x} := \{x_n\} \subset X$ in a metric space X is a function $\boldsymbol{x} : \mathbb{N} \to X$ where we write $x_n = \boldsymbol{x}(n)$. We say $\{x_n\}$ *converges* to some point $x \in X$ if

$$\forall\, \varepsilon > 0, \exists\, N \in \mathbb{N} \text{ s.t. } n \geq N \Rightarrow d(x, x_n) < \varepsilon.$$

We write $x_n \to x$ or $\lim_{n\to\infty} x_n = x$. Equivalently, $x_n \to x$ in (X, d) iff $d(x_n, x) \to 0$ in $(\mathbb{R}, |\cdot|)$.

A *subsequence* of $\boldsymbol{x}$ is a new sequence $\tilde{\boldsymbol{x}}$ which can be written as $\tilde{\boldsymbol{x}} = \boldsymbol{x} \circ n$ where $n : \mathbb{N} \to \mathbb{N}$ a strictly increasing function, called the *reindexing* of our sequence. Equivalently we write $\tilde{\boldsymbol{x}} = \left\{x_{n_k}\right\}_k$ where $n_k = n(k)$.

We say a sequence is *bounded* if there exists an $M \in \mathbb{R}$ such that $d(x_n, x_m) \leq M$ for all $n, m \in \mathbb{N}$ (this is equivalent to saying there is some $M' \in \mathbb{R}$ and $x \in X$ such that $d(x_n, x) \leq M'$ for all $n \in \mathbb{N}$).

Definition 3 (Cauchy): A *Cauchy sequence* in a metric space (X, d) is a sequence $\{x_n\}$ such that

$$\forall\, \varepsilon > 0, \exists\, M \in N \text{ s.t. } n, m \geq M \Rightarrow d(x_n, x_m) < \varepsilon.$$

Proposition 1 (Some Properties of Sequences): Fix (X, d) a metric space and $\{x_n\}$ a sequence in X.

- $\{x_n\}$ convergent $\Rightarrow$ $\{x_n\}$ Cauchy. If the converse holds for every sequence in X, we say X is *complete*
- if $\{x_n\}$ Cauchy and has a converging subsequence, then $\{x_n\}$ converges along the whole sequence
- if $\{x_n\}$ Cauchy, $\{x_n\}$ bounded
- if $\{x_n\}$ converges, then every subsequence of $\{x_n\}$ converges, and to the same limit

Definition 4 (Continuity): A function $f : (X, d) \to (Y, \rho)$ is said to be continuous at $x \in X$ if for every $\varepsilon > 0$ there exists $\delta = \delta(x) > 0$ such that

$$d(x, x') < \delta \Rightarrow \rho(f(x), f(x')) < \varepsilon.$$

It is said to be *uniformly continuous* on X if δ as in the definition of continuity can be chosen independently of x.

Proposition 2: $f : (X, d) \to (Y, \rho)$ is continuous at $x \in X$ iff for every $\{x_n\} \subset X$ such that $x_n \to x$ in X, $f(x_n) \to f(x)$ in Y.

Definition 5 (Normed and Inner Product Spaces): Let V be a vector space over $K \in \{\mathbb{R}, \mathbb{C}\}$. Then $\|\cdot\| : V \to \mathbb{R}$ is called a *norm* if:

- $\|v\| \geq 0 \, \forall \, v \in V$, and equal to zero iff $v = 0$
- $\|\alpha v\| = |\alpha| \, \|v\|$ for all $\alpha \in K, v \in V$
- $\|u + v\| \leq \|u\| + \|v\| \, \forall \, u, v \in V$

A function $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{R}$ is called an *inner product* if, for all $u, v, w \in V$ and $\alpha \in K$:

- $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$
- $\langle \alpha u, v \rangle = \alpha \langle u, v \rangle$
- $\langle u, v \rangle = \overline{(\langle v, u \rangle)}$
- $\langle u, u \rangle \geq 0$ and equals zero iff $u = 0$,

Accordingly, $(V, \|\cdot\|)$ is called a *normed vector space* and $(V, \langle \cdot, \cdot \rangle)$ an *inner product space.*

Remark 1: Norms induce natural metrics, $d(u, v) := \|u - v\|$. Inner products induce natural norms, $\|u\| = (\langle u, u \rangle)^{1/2}$. So every inner product space is (naturally) a normed vector space, and every vector space is (naturally) a metric space. We say things like "V is a complete normed vector space" to mean V is complete as a metric space with the natural metric induced by its norm, for convenience.

Definition 6 (Series): Let $(V, \|\cdot\|)$ be a normed vector space. A *series* in V is a sequence of partial sums, i.e. a sequence

$$S_n := \sum_{k=0}^{n} a_k$$

where $\{a_k\}$ a sequence in V. We say the series converges if $\{S_n\}$ converges in V.

Remark 2:

1.1.2 Differentiation

Definition 7: Given $f : \mathbb{R}^n \to \mathbb{R}^m$, the derivative at $x_0 \in \mathbb{R}^n$ is the linear map $\mathrm{D}f(x_0) : \mathbb{R}^n \to \mathbb{R}^m$, if it exists, such that

$$\frac{\|f(x) - f(x_0) - Df(x_0)(x - x_0)\|}{\|x - x_0\|} \to 0 \text{ as } x \to x_0.$$

If we fix bases for $\mathbb{R}^n, \mathbb{R}^m$, then $Df(x_0)$ can be represented by a $m \times n$ matrix $J_f(x_0)$ called the *Jacobian* of f at x_0.

Remark 3: When $m = 1$, one often writes $\mathrm{D}f = (\nabla f)^\top$ where ∇f is viewed as a column vector in $\mathbb{R}^n$.

Proposition 3 (Properties of Derivative): Let $f, g : \mathbb{R}^n \to \mathbb{R}^m$ and $h : \mathbb{R}^k \to \mathbb{R}^n$, and $\alpha, \beta \in \mathbb{R}$.

- $\mathrm{D}f$ is unique when it exists
- $\mathrm{D}(\alpha f + \beta g) = \alpha \, \mathrm{D}f + \beta \, \mathrm{D}g$
- $\mathrm{D}(fg) = (\mathrm{D}f)g + f(\mathrm{D}g)$, when $m = 1$
- $\mathrm{D}(f \circ h) = (\mathrm{D}f)|_h \cdot (\mathrm{D}h)$ (*chain rule*)
- f differentiable at $x_0 \Rightarrow f$ (Lipschitz) continuous at x_0
- If $\mathrm{D}f$ exists at a point x_0, f partially differentiable in all directions, and

$$J_f(x_0) = \left(\frac{\partial f_j}{\partial x_i}(x_0) \right)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$$

- If all of the partial derivatives of f exist and are continuous at x_0, then f differentiable at x_0

Remark 4: One need be careful with the last two properties - existence of partial derivatives needn't imply differentiability in general (we need some extra condition, such as continuity as stated here); consider

$$f : \mathbb{R}^2 \to \mathbb{R}, \quad f(x, y) = \begin{cases} \frac{x^2 y}{x^2 + y^2} & (x, y) \neq 0 \\ 0 & (x, y) = 0 \end{cases}.$$

One can check $\partial_x f, \partial_y f$ both exist (and equal 0) at the origin, but f not differentiable at 0. Intuitively, $\mathrm{D}f$ captures "average change in all directions" while partial derivatives capture "change in a specified direction".

Definition 8 (Other Derivatives): Let $f : \mathbb{R}^n \to \mathbb{R}$ and $F = (F_1, ..., F_n) : \mathbb{R}^n \to \mathbb{R}^n$.

- $\frac{\partial}{\partial x_i} f(x_1, ..., x_n) := \lim_{h\to 0} \frac{f(x_1,...,x_i+h,...,x_n)-f(x_1,...,x_n)}{h}$ is called the *partial derivative* of f in the x_i direction.
- Given a vector $d \in \mathbb{R}^n$ and $x \in \mathbb{R}^n$, define the *directional derivative* of f in the direction d at x by

$$\mathrm{d}f(x; d) := \lim_{h\to 0} \frac{f(x + hd) - f(x)}{h}.$$

- Define the *divergence* of F at x (assuming its first-partial derivatives exist) by

$$\mathrm{div}F(x) := \frac{\partial F_1}{\partial x_1}(x) + \cdots + \frac{\partial F_n}{\partial x_n}(x).$$

- If $n = 3$, define the *curl* of F at x (assuming its first-partial derivatives exist) by

$$\begin{aligned}\mathrm{curl}F(x) &:= \det\left(\begin{pmatrix} e_1 & e_2 & e_3 \\ \partial_x & \partial_y & \partial_z \\ F_1(x) & F_2(x) & F_3(x)\end{pmatrix}\right) \\ &= (\cdots)\end{aligned}$$

Proposition 4: If $f : \mathbb{R}^n \to \mathbb{R}$ differentiable at $x \in \mathbb{R}^n$, then

$$\mathrm{d}f(x; d) = \nabla f(x)^T.$$

If $d = e_i$ and f partially differentiable in x_i at x, then $\mathrm{d}f(x; d) = \frac{\partial f}{\partial x_i}(x)$.

Theorem 1 (Mean-Value Theorem): Let $f : \mathbb{R}^n \to \mathbb{R}$ be differentiable on an open ball $B \subset \mathbb{R}^n$. Then for any $x, y \in B$, there exists a $z \in B$ such that

$$f(x) - f(y) = \mathrm{D}f(z_0)(x - y).$$

Proof. Define $\varphi(t) := f(y + t(x - y))$ for $t \in [0, 1]$, noting that $\varphi(0) = y$ and $\varphi(1) = x$. One computes, using the chain rule, that $\varphi'(t) = \mathrm{D}f(y + t(x - y)) \cdot (x - y)$. By the one-variable mean-value theorem, there exists some $t_0 \in [0, 1]$ such that $\varphi(1) - \varphi(0) = \varphi'(t_0)$. Letting $z = y + t_0(x - y)$ gives the desired result, noting that z indeed in B by convexity.

For completeness, we also prove the one-variable mean-value theorem. ■

Theorem 2 (Clairaut's Theorem): Suppose $f : \mathbb{R}^n \to \mathbb{R}$ twice differentiable at x_0. Then, $\partial_{x_j} f(x_0) = \partial_{x_i} f(x_0)$ for all $i, j = 1, ..., n$.

Proof. *(Sketch)* For $n = 2$ (the proof extends to general dimensions by fixing all coordinates except the ith, jth) in variables (x, y), consider the function

$$\varphi(s, t) := f(x_0 + s, y_0 + t) - f(x_0 + s, y_0) - f(x_0, y_0 + t) + f(x_0, y_0).$$

The idea is to recognize $\varphi(s, t)$ as a difference of functions in the s, t variables resp., apply mean-value theorem to pick-up $\frac{\partial}{\partial x}, \frac{\partial}{\partial y}$ terms, then use the definition of the second-order partial derivatives to estimate φ in terms of $\frac{\partial^2}{\partial x \partial y}, \frac{\partial^2}{\partial y \partial x}$. One should ultimately find that $\frac{\varphi(t,t)}{t^2} \to \frac{\partial^2 f}{\partial x \partial y}(x_0, y_0)$ and $\frac{\partial^2 f}{\partial y \partial x}$, depending on which variable one chooses to expand in first. ■

Theorem 3 (Inverse Function Theorem): Let $F : \Omega \subset \mathbb{R}^n \to \mathbb{R}^n$ a C^k map such that $\mathrm{D}F(x_0)$ invertible for some $x_0 \in \Omega$. Then there exist neighborhoods $U \subset \Omega$ of x_0 and $V \subset \mathbb{R}^n$ of $F(x_0)$ and a C^k map $G : V \to U$ such that

$$(F \circ G)(y) = y \quad \forall\, y \in V, \qquad (G \circ F)(x) = x \quad \forall\, x \in U.$$

Moreover, $\mathrm{D}F(x)$ invertible for $x \in U$, and

$$\mathrm{D}G(y) = (\mathrm{D}F)^{-1}(x), \quad y = F(x), x \in U.$$

Theorem 4 (Implicit Function Theorem): Let $F : \Omega := \Omega_x \times \Omega_y \subset \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^m$ be a C^k map, and assume $X_0 = (x_0, y_0) \in \Omega$ is such that $F(X_0) = 0$ and $\mathrm{D}_y F(X_0)$ is invertible (*where* D_y *the derivative in just the y-variables, i.e. represented by a* $m \times m$ *matrix*). Then, there exists a neighborhood $U \subset \Omega_x$ of x_0 and a C^k function $h : \Omega_x \to \mathbb{R}^m$ such that

$$F(x, h(x)) = 0, \quad \forall\, x \in \Omega.$$

Proof. *(Sketch)* Define $f : \Omega \to \mathbb{R}^n \times \mathbb{R}^m$ by $f(X) := (X, F(X))$ ("augmenting" F to map to and from spaces of the same dimension). One checks

$$J_f = \begin{pmatrix} I_{n\times n} & 0_{n\times m} \\ \mathrm{D}_x F & \mathrm{D}_y F \end{pmatrix},$$

which has determinant $\det(\mathrm{D}_y F)$ using properties of block matrices. This is non-zero at X_0 by assumption, so we may apply the inverse-function theorem, so locally there exists an inverse g. If we write $g = (\tilde{g}, \tilde{h}) : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^{n+m}$, we see that $f(g(x,y)) = (x,y)$ (by inverse property) and $f(g(x,y)) = \tilde{g}(x,y), F(\tilde{g}(x,y), \tilde{h}(x,y))$ by definition. In particular we see that $\tilde{g}(x,y) \equiv x$, and thus we get the property

$$F(x, \tilde{h}(x,y)) = y.$$

Thus the map $h(x) := \tilde{h}(x, 0)$ gives the desired function. ∎

Theorem 5 (Lagrange Multipliers, one constraint): Let $f, g : \Omega \subset \mathbb{R}^n \to \mathbb{R}$ be C^1 and $\Sigma := \{x \in \Omega : g(x) = 0\}$, and assume $\mathrm{D}g(x)$ nonzero (i.e. the gradient of g) on all of Ω. Then, if f restricted to Σ has a max/min at $x_0 \in \Sigma$, then there exists $\lambda \in \mathbb{R}$ such that

$$\nabla f(x_0) = \lambda g(x_0).$$

Proof. Let x_0 be a max/min of f restricted to Σ. Assume wlog that $\frac{\partial}{\partial x_n} g(x_0) \neq 0$. By implicit function theorem, then locally to x_0, Σ is represented by $\{(x', h(x'))\}$ (where $x' \in \mathbb{R}^{n-1}$) for some C^1 function $h : \mathbb{R}^{n-1} \to \mathbb{R}$. Defining $F : \mathbb{R}^{n-1} \to \mathbb{R}, F(x') := f(x', h(x'))$, this implies $(x_0', h(x_0'))$ a local max/min of F and thus it's gradient must equal zero there. Chain rule gives

$$\nabla F(x') = \left(\frac{\partial}{\partial x_i'} f(x', h(x')) + \frac{\partial}{\partial x_n} f(x', h(x')) \frac{\partial h(x')}{\partial x_i} \right)_{i=1}^{n-1}. \quad (\dagger)$$

Also since $g(x', h(x')) = 0$ locally to x_0, we can take the derivative of this expression and find

$$0 = \left(\frac{\partial g}{\partial x_i}(x_0) + \frac{\partial h}{\partial x_i'}(x_0) \frac{\partial g}{\partial x_n}(x_0) \right)_{i=1}^{n-1}. \quad (\ddagger).$$

Taking $x' = x_0'$ in $(\dagger)$ makes the right-hand side 0. Equating $(\dagger), (\ddagger)$ and simplifying like-terms yields the proof, where λ is found to be $\left(\left[\frac{\partial f}{\partial x_n}\right] / \left[\frac{\partial g}{\partial x_n}\right]\right|_{x_0}$. ∎

Remark 5: When we say "Σ locally looks like V", what we really mean is there exists an open set U such that $\Sigma \cap U = V$.

Remark 6: In particular, then if f, g are C^1 on some open superset of Ω, and $\partial\Omega = \{x \in \Omega : g(x) = 0\}$, then one can compute global maxima of f by
(i) computing *stationary points* i.e. such that $\nabla f = 0$, inside Ω, and
(ii) computing points such that $\nabla f = \lambda \nabla g$, on $\partial\Omega$.

Then, if x_0 a global max of f, then either it lies inside Ω in which case $\nabla f(x_0) = 0$, or it lies on the boundary in which case there exists λ such that $\nabla f(x_0) = \lambda \nabla g(x_0)$. Thus, the global max of f is the point of greatest function value among those from 1., 2.. A similar statement holds for the global min.

Theorem 6 (Lagrange Multiplier, multiple constraints): Let $f, g_1, ..., g_k : \Omega \subset \mathbb{R}^n \to \mathbb{R}$ be C^1. Let $\Sigma = \{x \in \Omega : g_i(x) = 0 \,\forall\, i = 1, ..., k\}$, and assume $\{\nabla g_i(x)\}_{i=1}^k$ a linearly independent set of vectors for all $x \in \Sigma$. Then if f restricted to Σ has a local max/min at $x_0 \in \Sigma$, then there exists $\lambda_1, ..., \lambda_k$ such that

$$\nabla f(x_0) = \lambda_1 \nabla g_1(x_0) + \cdots + \lambda_k \nabla g_k(x_0).$$

Theorem 7 (Taylor's Theorem): Let $f : \Omega \subset \mathbb{R}^n \to \mathbb{R}$ be a $C^{k+1}(\Omega)$ function. For any $x, x^0 \in \Omega$,

$$f(x) = f(x^0) + \sum_{j=1}^{k} \sum_{1 \le i_1, ..., i_j \le n} \frac{\partial^j f}{\partial x_{i_1} \cdots \partial_{x_{i_j}}} \left(x_{i_1} - x^0_{i_1}\right) \cdots \left(x_{i_j} - x^0_{i_j}\right) + R_k(x, x^0),$$

where the *remainder* R_k is such that

$$\left|R_k(x, x^0)\right| \le M_k \left|x - x^0\right|^{k+1} \quad \text{as } x \to x^0,$$

where M_k depends only on the $(k+1)$-st partial derivatives of f.

Remark 7: The easiest way to prove this is to apply 1-dimensional Taylor's theorem to the function $\varphi(t) := f\left(x^0 + t\frac{x-x^0}{\|x-x^0\|}\right), \quad t \in [0, \|x-x^0\|]$, for $t$sufficiently small, and expanding the derivatives of φ by chain rule.

On the other hand, the easiest way to derive the 1-diemnsional Taylor's theorem is by repeated application of the fundamental theorem of calculus,

$$\begin{aligned}\varphi(t) &= \varphi(t_0) + \int_{t_0}^{t} \underbrace{\varphi'(s)}\, \mathrm{d}s \\ &= \varphi(t_0) + \int_{t_0}^{t} \left[\varphi'(t_0) + \int_{t_0}^{s} \varphi''(u)\,\mathrm{d}u\right] \mathrm{d}s \\ &= \varphi(t_0) + \varphi'(t_0)(t-t_0) + \int_{t_0}^{t}\int_{t_0}^{s} \varphi''(u)\,\mathrm{d}u\,\mathrm{d}s,\end{aligned}$$

etc. In particular, one sees that this implies the remainder term can be written as

$$R_k(t) = \int_{t_0}^{t}\int_{t_0}^{s_1}\cdots\int_{t_0}^{s_{k-1}} \varphi^{(k)}(u)\,\mathrm{d}u\cdots\mathrm{d}s_2\,\mathrm{d}s_1,$$

from which obtaining the bound on R_k follows by approximating this integral.

Theorem 8 (Taylor's Theorem, Weaker Assumptions): Let $f \in C^{k-1}(\Omega)$ and such that $\mathrm{D}^{k-1}f$ is differentiable at $x^0 \in \Omega$. Then for $x \in \Omega$, the same conclusion as above holds, but with remainder

$$\lim_{x\to x^0} \frac{R_k(x)}{|x-x^0|^k} = 0,$$

i.e. we can't in general say anything about how *quickly* this quantity goes to zero.

Remark 8: In "asymptotic" notation, the first theorem says $R_k(x) = \mathcal{O}\left(|x-x^0|^{k+1}\right)$ and the second says $R_k(x) = o\left(|x-x^0|^k\right)$.

1.1.3 Integration

Definition 9 (Partition): Given a rectangle $R \subset \mathbb{R}^n$, a *box partition* of R is a **finite** collection $\mathcal{P} = \{B_k\}_{k=1}^N$ of *boxes* (rectangles) B_k such that $R = \bigcup_{k=1}^N B_k$.

Definition 10 (Upper/Lower Riemann Sum): Let $f : R \subset \mathbb{R}^n \to \mathbb{R}$ a bounded function. Given a partition $\mathcal{P}$ of R, define the *upper, lower Riemann sums*

$$U(f,\mathcal{P}) := \sum_{B\in\mathcal{P}} \sup_{x\in B} f(x)\cdot \mathrm{vol}(B), \quad L(f,\mathcal{P}) := \sum_{B\in\mathcal{P}} \inf_{x\in B} f(x)\cdot \mathrm{vol}(B),$$

where, if $B = [a_1,b_1]\times\cdots\times[a_n,b_n]$, $\mathrm{vol}(B) := (b_1-a_1)\cdots(b_n-a_n)$. Define the *upper, lower Riemann integrals* of f by

$$\overline{\int_R} f\,\mathrm{d}x := \inf_{\mathcal{P}\text{: partition of } R} U(f,\mathcal{P}), \qquad \underline{\int_R} f\,\mathrm{d}x := \sup_{\mathcal{P}\text{: partition of } R} L(f,\mathcal{P}).$$

In particular, we trivially have the inequalities

$$\inf_R f\cdot\mathrm{vol}(R) \le L(f,\mathcal{P}) \le \underline{\int_R} f\,\mathrm{d}x \le \overline{\int_R} f\,\mathrm{d}x \le U(f,\mathcal{P}) \le \sup_R f\cdot\mathrm{vol}(R).$$

If the lower, upper Riemann sums agree, we write their shared value by $\int_R f\,\mathrm{d}x$, called the Riemann integral of f over R.

Remark 9: We can extend this definition to general f over bounded domains Ω by taking R a rectangle such that $R \supset \Omega$ and extending f by zero outside of R.

Definition 11 (Content Zero): A set $\Omega \subset \mathbb{R}^n$ is said to be of *content zero* if for every $\varepsilon > 0$, there exists a finite number of boxes $B_1, \ldots, B_N$ which cover Ω and such that $\sum_{n=1}^N \mathrm{vol}(B_n) \le \varepsilon$.

Theorem 9: If f bounded on R and has set of discontinuities with content 0, it is Riemann integrable on R.

Proposition 5: Riemann integrals are linear.

Theorem 10 (Fubini):

Definition 12 (Regular Partition): Let $\Omega \subset \mathbb{R}^n$ a domain with $\text{content}(\partial\Omega) = 0$. A *regular partition* $\mathcal{P} = \{D_k\}_{k=1}^N$ is a finite collection of sets D_k satisfying

- $\Omega = \bigcup_{k=1}^N D_k$ and $\text{content}(\partial D_k) = 0$ for all $k = 1, ..., N$, and
- $\text{content}\left(\overline{D_k} \cap D_j\right) = 0$ for all $k \neq j$.

Proposition 6: Let $f : \Omega \to \mathbb{R}$. Then f is Riemann integrable over Ω iff for all $\varepsilon > 0$ there exists a *regular* partition $\mathcal{P}$ such that $U(f, \mathcal{P}) - L(f, \mathcal{P}) < \varepsilon$

Theorem 11 (Change of Variables): Let $\Omega, \Omega' \subset \mathbb{R}^n$ be bounded domains and $T : \Omega' \to \Omega$ a C^1 bijection. Then, for any $f : \Omega \to \mathbb{R}$ which is Riemann integrable over Ω, then

$$\int_\Omega f \, \mathrm{d}V = \int_{\Omega'} (f \circ T) \, |\det \mathrm{D}T| \, \mathrm{d}V.$$

Proof. ∎

Theorem 12 (Differentiation under the Integral):

Theorem 13 (Improper Integrals):

1.1.4 Vector Calculus

Definition 13 (Curve): A *(parametrized) C^k curve* in $\mathbb{R}^n$ is a connected set $\mathcal{C} \subset \mathbb{R}^n$ such that there exists a C^k function $\gamma : I \to \mathbb{R}^n$ with $\gamma(I) = \mathcal{C}$, where $I \subset \mathbb{R}$ an interval. We say $\mathcal{C}$ *regular* if γ' never vanishes on I.

A *piecewise C^k curve* is a set $\mathcal{C} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_m$ where each $\mathcal{C}_i$ a C^k curve and each has "shared endpoints" (in practice, think of something like a triangle).

Remark 10: More generally, a curve is generally defined as a connected subset of $\mathbb{R}^n$ that is "locally a parametrized curve".

Definition 14 (Surface): A *C^k surface* in $\mathbb{R}^n$ is a connected set $S \subset \mathbb{R}^n$ such that for every point $p \in S$, there exists an open subset $U \subset \mathbb{R}^2$ and $V \subset \mathbb{R}^n$ such that $p \in V$, and a C^k homeomorphism $\varphi : U \to V \cap S$ such that $\varphi(U) = V \cap S$.

We call S regular if every such φ has $\mathrm{d}\varphi_q : \mathbb{R}^2 \to \mathbb{R}^n$ is one-to-one for all $q \in U$, i.e. the Jacobian $J_\varphi(q)$ has rank 2.

Definition 15 (Tangent Plane): Let $S \subset \mathbb{R}^3$ a regular C^1 surface. The *tangent plane* at a point $p \in S$ is

$$T_p S = \mathrm{d}_q\varphi(\mathbb{R}^2),$$

where $\varphi(q) = p$. Since $\mathrm{d}_q\varphi$ one-to-one, this is a 2-dimensional subspace of $\mathbb{R}^3$.

Remark 11: This is well-defined, regardless of choice of parametrization, by an inverse function theorem argument.

Definition 16 (Normal): A normal to a regular C^1 surface $S \subset \mathbb{R}^3$ at a point p is a vector $n \in \mathbb{R}^3$ such that n is orthogonal to $T_p S$. If we restrict n to be of unit length, then since $T_p S$ two dimensional, there are precisely two such n's, given by $\pm(v_1 \times v_2)$ where $\{v_1, v_2\}$ a basis for $T_p S$.

Definition 17 (Integration over a Surface in $\mathbb{R}^3$): Let $S \subset \mathbb{R}^3$ a regular parametrized surface with parametrization $\varphi : D \to \mathbb{R}^3$ and $f : \mathbb{R}^3 \to \mathbb{R}$ Riemann integrable. Define the *surface integral*

$$\iint_S f \, \mathrm{d}\sigma := \iint_D (f \circ \varphi) \, |\varphi_u \times \varphi_v| \, \mathrm{d}u \, \mathrm{d}v.$$

Suppose $F : \mathbb{R}^3 \to \mathbb{R}^3$ a vector field, and S an oriented surface with unit normal n. Define the *flux integral*

$$\iint_S F \cdot \mathrm{d}\sigma := \iint_S (F \cdot n) \, \mathrm{d}\sigma = \iint_D (F \circ \varphi) \cdot (n \circ \varphi) \, |\varphi_u \times \varphi_v| \, \mathrm{d}u \, \mathrm{d}v.$$

Remark 12: Since we are in dimension 3, $n = \pm\frac{\varphi_u \times \varphi_v}{|\varphi_u \times \varphi_v|}$ so the flux integral can be evaluated as $\pm \iint_D (F \circ \varphi) \cdot (\varphi_u \times \varphi_v)\, du\, dv$ (one needs to be careful of using the right sign).

1.1.5 Analysis on Functions

Remark 13: A lot of what is stated in this section could be generalized without too much hassle to functions on/to general metric spaces, but is cumbersome and unnecessary for my interests.

Definition 18 (Convergence of sequences of functions): Let $\{f_n\}$ be a sequence of real-valued functions defined on some set S. We say $f_n \to f$ *pointwise on* S if $f_n(x) \to f(x)$ (as sequences of real-numbers) for every $x \in S$.

We say that the convergence is *uniform* if $\sup_{x\in S}|f_n(x) - f(x)| \to 0$ as $n \to \infty$, or equivalently if $f_n \to f$ under the *uniform norm* $\|f\|_\infty := \sup_S |f|$ (where we may omit the set if clear from context).

Remark 14: Equivalently, $f_n \to f$ uniformly if for every $\varepsilon > 0$, there exists an $N \in \mathbb{N}$ such that for all $n \geq N$, $|f_n(x) - f(x)| \leq \varepsilon$ for all $x \in S$.

Remark 15: It's clear that uniform $\Rightarrow$ pointwise convergence. A good counterexample for the other direction is the functions $f_n(x) = x^n$ defined on $[0, 1]$. We see that f_n converges pointwise to the function that is 0 everywhere except 1, at which point it is equal to 1. However, this convergence is not uniform.

Theorem 14: Let $C(K)$ be the set of continuous functions on a compact set $K \subset \mathbb{R}^n$. This is a complete metric space when equipped with the uniform norm.

Remark 16: In particular, this means that the uniform limit of continuous functions is continuous.

Theorem 15 (Interchange of Limit and Integral): Let $\{f_n\}$ be a sequence of Riemann integrable functions on some box domain B which converge uniformly to some Riemann integrable function f on B. Then, $\int_B f_n\, dx \to \int_B f\, dx$.

Proof. $|\int_B f\, dx - \int_B f_n\, dx| \leq \int_B |f - f_n|\, dx \leq \text{vol}(B) \sup_B |f - f_n|$; the right-hand side above goes to zero by uniform convergence. ■

Theorem 16 (Interchange of Limit and Derivative): Suppose $f : U \subset \mathbb{R}^n \to \mathbb{R}$ where U open, where f_m differentiable, converge pointwise at some point $x_0 \in U$, and their derivatives converge uniformly, then $\{f_m\}$ converges uniformly to some differentiable function f and $\partial_x f_m(x) \to \partial_x f(x)$ as $m \to \infty$ on U.

Proof. Assume $n = 1$ for simplicity. Let $g_n = f_n'$ and let g be the uniform limit of g_n. Take as candidate $f(x) := f(x_0) + \int_{x_0}^x g(y)\, dy$. It's clear f is differentiable, and by the fundamental theorem of calculus,

$$\begin{aligned}
|f_n(x) - f(x)| &= |f_n(x_0) - f(x_0) + \int_{x_0}^x f_n'(y) - g(y)\, dy\,| \\
&\leq |f_n(x_0) - f(x_0)| + \int_{x_0}^x |f_n'(y) - g(y)|\, dy \\
&\leq |f_n(x_0) - f(x_0)| + |x - x_0| \sup_y |f_n'(y) - g(y)|,
\end{aligned}$$

and the right-hand side converges by the point-wise convergence at x_0 and the uniform convergence of the derivatives. Finally, for $x \in U$, $|f_n'(x) - f'(x)| = |g(x) - g_n(x)|$ by definition, so the convergence is immediate. ■

Theorem 17 (Bounded Convergence for Integrals): Assume $f_n \to f$ pointwise, $\{f_n\}, f$ Riemann integrable, and $|f_n(x)| \leq B$ for all $x \in I, n \geq 1$. Then $\int_I f_n(x)\, dx \to \int_I f(x)\, dx$.

Proof.

■

Theorem 18 (Dini's Theorem): Let $\{f_n\}, f$ continuous functions on I and $f_n \to f$ pointwise. Suppose $f_n(x) \leq f_{n+1}(x)$ for all x and $n \geq 1$. Then $f_n \to f$ uniformly.

Theorem 19 (Interchange of Integral and Summation): Suppose $f_n : K \to \mathbb{R}$ are Riemann integrable and $\sum_n f_n \to f$ uniformly, and f Riemann integrable. Then,

$$\sum_n \int_K f_n\, dx = \int_K \sum_n f_n\, dx.$$

Proof. Letting $S_N(x) = \sum_{n \le N} f_n(x)$, this theorem says $\lim_N \int_K S_N \, \mathrm{d}x = \int_K \lim_N S_N \, \mathrm{d}x$. This follows from an earlier proposition on uniform convergence of sequences of functions and integrals. ■

Theorem 20 (Power Series): A *power series* (centered at x_0) is a function of the form

$$f(x) = \sum_{n \ge 0} a_n (x - x_0)^n.$$

Define $\frac{1}{R} := \limsup_{n \to \infty} |a_n|^{1/n}$. Then,

- if $|x - x_0| < R$, the series converges absolutely
- if $|x - x_0| > R$, the series diverges

1.2 Complex

1.2.1 Analytic Functions

Throughout this section, we'll usually assume $\Omega \subset \mathbb{C}$ a connected open set.

Definition 19 (Analytic/Holomorphic): A function $f : \mathbb{C} \to \mathbb{C}$ is said to be *analytic* on Ω if f is given by a converging power series everywhere in Ω. It is said to be holomorphic if f' exists.

For $z = x + iy \in \mathbb{C}$ and $f : \mathbb{C} \to \mathbb{C}$, write $f(z) = u(x, y) + v(x, y)i$ for real-valued functions u, v. Then, the *Cauchy-Riemann (CR) equations* are the equations

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

Theorem 21 (Cauchy-Riemann Equations): f is holomorphic if and only if u, v satisfy the CR equations.

Proof. ($\Rightarrow$) follows by taking different limit directions in the definition of the derivative. ($\Leftarrow$) follows by writing, for some small $h = h_1 + h_2 i$,

$$u(x + h_1, y + h_2) = u(x, y) + h_1 \partial_x u(x, y) + h_2 \partial_y u(x, y) + |h|\ \psi_1(h), \quad \psi_1(h) \underset{h \to 0}{\to} 0,$$

similar for v. This implies, simplifying things with CR,

$$f(z + h) = f(x, y) + (\partial_x v - i\partial_y u)(h) + \psi(h)h|, \quad \psi(y) = o(|h|),$$

which gives the proof upon dividing both sides by h and sending $h \to 0$. ∎

Definition 20 (Contour Integration): Given a piecewise C^1 contour $C = C_1 \cup \cdots \cup C_k$ with C_i parametrized by C^1 functions $\gamma_i : [t_i, t_{i+1}] \to C_i$, define

$$\int_{C^\pm} f(z)\, \mathrm{d}z := \pm \sum_{i=1}^{k} \int_{t_i}^{t_{i+1}} (f \circ \gamma_i)(s) \cdot \gamma_i'(s)\, \mathrm{d}s,$$

where the $\pm$ indicates the *orientation* of C.

A domain Ω is said to be *simply connected* if for any two curves $\gamma_0, \gamma_1 : [0, 1] \to \mathbb{C}$ with common endpoints α, β in Ω, there exists a function $\gamma_t : I \to \mathbb{C}$ for $t \in [0, 1]$ such that $(t, s) \mapsto \gamma_t(s)$ is a continuous map, $\gamma_0 = \gamma_0$ and $\gamma_1 = \gamma_1$, and $\gamma_t(0) = \alpha, \gamma_t(1) = \beta$ for all $t \in [0, 1]$.

A curve C is said to be *simple* if it does not intersect itself, i.e. it has an injective parametrization, and *closed* if its parametrization $\gamma : I \to \mathbb{C}$ is equal on the endpoints of I.

Theorem 22 (Cauchy): Let f be a holomorphic function defined on Ω being simply connected with C a simple closed curve contained in Ω. Then

$$\int_C f(x)\, \mathrm{d}z = 0.$$

Partial converse:

Theorem 23 (Morera): Let f be continuous on Ω and such that

$$\int_\gamma f\, \mathrm{d}z = 0$$

for every closed, piecewise C^1 curve γ contained in Ω. Then f is holomorphic in Ω.

Theorem 24 (Cauchy's Integral Formula): Let f holomorphic on Ω, which contains a circle C and its interior. Then

$$f(z) = \int_{C^+} \frac{f(w)}{w-z}\,\mathrm{d}w, \quad \forall\, z \in \Omega.$$

In particular, this implies f is analytic on all of Ω, with

$$f^{(n)}(z) = \frac{n!}{2\pi i}\int_{C^+} \frac{f(w)}{(w-z)^{n+1}}\,\mathrm{d}w,$$

and thus

$$f(z) = \sum_{n=0}^{\infty} \frac{f^{(n)}(z_0)}{n!}(z-z_0)^n,$$

for any $z_0 \in \Omega$ and z such that $z - z_0 \in \Omega$.

Proof. Make a small indent in the contour around the singularity of the denominator and use holomorphicity to approximate. ■

Corollary 1 (Cauchy's Inequalities): Let $f : \Omega \to \mathbb{C}$ holomorphic. Then

$$|f^{(n)}(z)| \leq \frac{n!\|f\|_{C_R(z),\infty}}{R^n},$$

where $R > 0$ any real number such that $D_R(z) \subset \mathbb{C}$, where $D_R(z)$ the R-radius disc centered at z, and

$$\|f\|_{C_R(z),\infty} := \sup_{w \in C_r(z)} |f(w)|.$$

Corollary 2 (Liouville's Theorem): Let $f : \mathbb{C} \to \mathbb{C}$ be *entire*, i.e. holomorphic everywhere, and bounded. Then f is constant.

Proof. For every $R > 0$ and z fixed, Cauchy's inequalities given that $|f'(z)| \leq \frac{C}{R}$ for some C uniform in z. Letting $R \to \infty$ gives that $f'(z) = 0$ everywhere, and thus $f \equiv$ constant. ■

Theorem 25 (Analytic Continuation): Let f holomorphic on Ω, and assume either

- $f \equiv 0$ on a open set $D \subset \Omega$ or
- $f = 0$ on a sequence $\{z_n\} \subset \Omega$ and its limit point z_∞.

Then $f \equiv 0$ on Ω.

Remark 17: As a result, if two holomorphic functions agree on an open subset of Ω or on a converging sequence, then they agree everywhere in Ω. This is the *principle of analytic continuation*, demonstrating how rigid analytic functions are.

Proof. The first criteria follows from the first by a connectedness argument. The second follows by contradiction and looking at a local power series centered at z_∞. ■

Theorem 26 (Convergence of Holomorphic Functions): Let $\{f_n\}$ a sequence of holomorphic functions converging uniformly on compact subsets of Ω to some function f. Then f is holomorphic, and moreover, f_n' converges uniformly to f' on compact subsets.

Proof. This follows directly from Morera's theorem; the uniform convergence implies that $0 = \int_C f_n\,\mathrm{d}z \to \int_C f\,\mathrm{d}z = 0$. ■

Remark 18: The analgous statement is *not* true in real variables! That is, uniform convergence of differentiable real-valued functions are not necessarily differentiable.

1.2.2 Meromorphic Functions

Definition 21 (Singularities): A holomorphic function $f : \Omega \setminus \{z_0\} \to \mathbb{C}$ is said to have a *singularity* at z_0. z_0 is called a

- *removable singularity* of f if there exists a holomorphic function $\tilde{f} : \Omega \to \mathbb{C}$ that agrees with f on $\Omega \setminus \{z_0\}$;
- *pole singularity* of f if $\frac{1}{f}$ has a removable singularity at z_0 (we define $\frac{1}{f}$ to be zero at z_0); or
- *essential singularity* of f otherwise.

We will say a singularity is *isolated* if there exists a neighborhood around it in which it is the only singularity of f.

Proposition 7 (Order of zeros, poles): Let $f : \Omega \to \mathbb{C}$ holomorphic have an isolated zero at $z_0 \in \Omega$. Then there exists a neighborhood of z_0, a unique positive integer $n := \operatorname{ord}_f(z_0)$, and a nonvanishing holomorphic function g such that $f(z) = (z - z_0)^n g(z)$ on that neighborhood.

The same statement holds if z_0 an isolated pole of f, with n a negative integer. When $n = -1$ we call the pole *simple;* more generally, $-n$ is called the *order/mulitiplicity* of z_0.

Proof. Follows from writing f in a local power series centered at z_0; there exists a minimally indexed nonzero coefficient. Factoring out this term gives the desired representation. Uniqueness follows easily. ∎

Corollary 3: If f has a pole of order n at z_0, then

$$f(z) = \frac{a_{-n}}{(z - z_0)^n} + \frac{a_{-n+1}}{(z - z_0)^{n-1}} + \cdots + \frac{a_{-1}}{z - z_0} + G(z) =: P(z) + G(z),$$

for some holomorphic (locally to z_0) function G.

The function P is called the *principal part* of f at z_0, and a_{-1} is called the *residue*, denoted $\operatorname{res}_{z_0} f = a_{-1}$.

Proof. Follows from the previous proposition by expanding terms. ∎

Proposition 8 (Computation of Residues): If $n = \operatorname{ord}_f(z_0)$,

$$\operatorname{res}_{z_0} f = \lim_{z \to z_0} \frac{1}{(n-1)!} \left(\frac{\mathrm{d}}{\mathrm{d}z} \right)^{n-1} (z - z_0)^n f(z).$$

Proof. This follows from the previous corollary by taking computing the appropriate derivatives term-by-term. ∎

Theorem 27 (Residue Theorem): Let f be holomorphic in an open set containing a disc with boundary C, except for finitely many poles $z_1, \ldots, z_N$ in the disc. Then,

$$\int_C f(z)\,\mathrm{d}z = 2\pi i \sum_{k=1}^{N} \operatorname{res}_{z_k} f.$$

Proof. The idea is to use a "keyhole contour" that indents the original circle in N places to miss the poles. By holomorphicity, the integral over this contour is zero and one finds that (since the "walls" of the keyhole neighborhoods tend to zero) our integral in question is equal to the sum over the poles of the integral of f over small circles centered at each pole. Appealing to the representation in the corollary from earlier and computing quickly yields the result, using crucially the fact that

$$\int_C \frac{1}{(z - z_0)^n}\,\mathrm{d}z = \begin{cases} 0 & n > 1 \\ 2\pi i & n = 1 \end{cases}.$$

∎

Theorem 28 (Classification of Isolated Singularities): Suppose $f : \Omega \setminus \{z_0\} \to \mathbb{C}$ holomorphic. Then:

- if f bounded on $\Omega \setminus \{z_0\}$, z_0 a removable singularity
- z_0 a pole iff $|f(z)| \to \infty$ as $z \to z_0$.

Proof. The second follows from the first. For the first, one contends that, inspired by the Cauchy's integral formula, the representation $\frac{1}{2\pi i}\int_C \frac{f(w)}{w-z}dw$ remains a holomorphic function that agrees with f everywhere away from z_0. ∎

Essential singularities are a lot harder to deal with. An example of a function with an essential singularity is $f(z) := e^{\frac{1}{z}}$ at 0.

Theorem 29 (Casorati-Weierstrass): Let f holomorphic on a punctured disc $D \setminus \{z_0\}$ with an essentially singularity at z_0. Then $f(D \setminus \{z_0\})$ is dense in $\mathbb{C}$.

Proof. Argue by contradiction. ∎

Definition 22 (Meromorphic Function, Singularities at Infinity): Let $f : \Omega \to \mathbb{C}$. We say f is *meromorphic* if there exists a sequence $\{z_n : n \geq 0\}$ of points in Ω such that

- $\{z_n\}$ has no limit points in Ω;
- f holomorphic on $\Omega \setminus \cup_n \{z_n\}$; and
- f has poles at each $\{z_n\}$.

Define $F(z) := f\left(\frac{1}{z}\right)$. We say f has a *pole/removable/essential singularity at infinity*/is *holomorphic at infinity* if F has a pole/removable/essential singularity/is holomorphic at 0. If f is a meromorphic function that is either holomorphic or has a pole at infinity is said to be *meromorphic in the extended complex plane*.

Proposition 9: The only meromorphic functions in the extended comlex plane are the rational functions.

Theorem 30 (Argument Principle): Let f be a meromorphic function on the interior of a simple closed curve $C \subset \mathbb{C}$, such that f has no roots nor poles on C. Then,

$$\frac{1}{2\pi i}\int_C \frac{f'(z)}{f(z)}\,\mathrm{d}z = \#\{\text{zeroes of } f \text{ inside } C\} - \#\{\text{poles of } f \text{ inside } C\},$$

the right-hand side counted with multiplicity.

Proof. If z_0 a zero of multiplicity n of f, then it will be a pole of $\frac{f'}{f}$ with residue n, and if z_0 a pole of order n of f, then it will be a pole of $\frac{f'}{f}$ with residue $-n$. The result then follows by the residue theorem. ∎

Remark 19: Sometimes the quantity $\frac{f'}{f}$ is called the *logarithmic derivative* of f, agreeing with the idea that "$\frac{\mathrm{d}}{\mathrm{d}z}\log(f) = \frac{f'}{f}$".

Theorem 31 (Rouché's): Let f, g be holomorphic functions on Ω with a curve $C \subset \Omega$ such that

- $|f| > |g|$ on C,
- both f, g never vanish on C.

Then, f and $f + g$ have the same number of zeros in the interior of C.

Proof. Define $f_t = f + tg$ for $t \in [0, 1]$. The conditions on f, g show that this function has no zeroes on C for any t, so we can apply the argument principle. Defining $N(t) = \frac{1}{2\pi i}\int_C \frac{f_t'(z)}{f_t(z)}\,\mathrm{d}z$, one sees that this is a continuous (in t) function that is integer valued, and is therefore constant. In particular, this implies $N(0) = N(1)$, where the form is the number of zeros of f and the latter of $f + g$, inside C. ∎

Theorem 32 (Maximum Modulus Principle): Let $f : \Omega \to \mathbb{C}$ a nonconstant holomorphic function. Then $|f|$ cannot attain its maximum inside Ω. In particular, if Ω bounded, then

$$\max_{\overline{\Omega}}|f| = \max_{\partial\Omega}|f|,$$

and if $|f|$ attains an "interior" maximum, then f is constant.

Theorem 33 (Logarithms): Let Ω a simply connected domain containing 1 and not containing 0. Then there exists a function $F(z) = \log_\Omega(z)$, called a *branch* of the logarithm, such that

- F holomorphic on Ω,
- $e^{F(z)} = z$ on Ω, and
- $F(r) = \log(r) := \int_1^r \frac{1}{x}\,\mathrm{d}x$ whenever r is a real number near 1 in Ω.

Proof. The idea is to define F by

$$F(z) = \int_{\gamma_z} \frac{1}{w}\,\mathrm{d}w,$$

where γ_z any curve connecting 1 to z. By simple connectedness, this integral is independent of choice of curve, and one checks the necessary properties rather easily by verifying $F'(z) = \frac{1}{z}$. In particular, the last follows form the fact that if $r \approx 1$, one can take γ_z to lie entirely on the real line. ■

Theorem 34 (Function Logarithms): Let f a non-vanishing holomorphic function on a simply connected domain Ω. Then there exists a holomorphic function g on Ω such that $f = e^g$.

1.2.3 Harmonic Functions

Theorem 35: Let f holomorphic on a disc $D_R(z_0)$ with series expansion $f(z) = \sum_{n\geq 0} a_n(z-z_0)^n$. Then, for any $0 < r < R$ and $n \geq 0$,

$$a_n = \frac{1}{2\pi r^n}\int_0^{2\pi} f\big(z_0 + re^{i\theta}\big)e^{-in\theta}\,\mathrm{d}\theta.$$

In particular, the case $n = 0$ yields the *mean value property* for holomorphic functions.

Proof. This follows directly by parametrizing the circle in the Cauchy integral formula for the derivatives of f. ■

Proposition 10 (Mean Value Property for Harmonic Functions): Let $u : \Omega \to \mathbb{R}$ be a harmonic function on a simply connected domain Ω. Then there exists a holomorphic function $f : \Omega \to \mathbb{R}$ such that $u = \mathrm{Re}(f)$, and so in particular,

$$u(z_0) = \left(\frac{1}{2\pi r}\right)\int_0^{2\pi} u\big(z_0 + re^{i\theta}\big)\,\mathrm{d}\theta,$$

for any $z_0 \in \Omega$ and $r > 0$ such that $D_r \subset \Omega$.

Proof. We need to find v such that $f = u + iv$ is a holomorphic function. Such a v is called a *harmonic conjugate* of u. We can define f to be the antiderivative of $2\frac{\partial u}{\partial z}$, which, since $\mathbb{D}$ simply connected, exists. This would imply $f'(z) = u_x + iu_y$, which should hold. Moreover, $\Re(f) = u$ up to a constant (check!). The mean value property for harmonic functions then holds as a consequence of the previous theorem (with $n = 0$) and taking real parts of both sides of the identity. ■

Proposition 11 (Other Properties of Harmonic Functions): Let u be harmonic on Ω. Then:

- u cannot achieve an interior min/max, unless it is constant, and if Ω bounded, u obtains its absolute min/max on $\partial\Omega$
- if $\Omega = \mathbb{R}^2$ and u bounded, then u is constant
- u is real-analytic, and in particular C^∞

1.2.4 Conformal Mappings

Definition 23 (Conformal Map): A function $f : U \to V$, where $U, V \subset \mathbb{C}$ open, is said to be a *conformal mapping* if it is bijective and holomorphic. If U, V are given and there exists a conformal map $f : U \to V$, we say U, V are *conformal*.

Proposition 12: Let $f : U \to V$ be holomorphic and injective. Then:

- $f'(z) \neq 0$ for every $z \in U$
- f is invertible when restricted to its image, and its inverse is holomorphic

In particular, if f conformal, then it's inverse $f^{-1} : V \to U$ is automatically holomorphic, and its derivative never vanishes.

Proposition 13 (Conformal map from $\mathbb{D}$ to $\mathbb{H}$): Let $\mathbb{D}$ be the open unit disc in $\mathbb{C}$ and $\mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ be the open upper half-plane. Then $\mathbb{D}$ and $\mathbb{H}$ are conformal, under the mapping

$$F : \mathbb{H} \to \mathbb{D}, \quad F(z) := \frac{i - z}{i + z},$$

with inverse

$$G : \mathbb{D} \to \mathbb{H}, \quad G(w) := i\frac{1 - w}{1 + w}.$$

Lemma 1 (Schwarz's Lemma): Let $f : \mathbb{D} \to \mathbb{D}$ be a holomorphic function with $f(0) = 0$. Then the following hold:

- $|f(z)| \leq |z|$, and if there exists a $z_0 \neq 0$ such that $|f(z_0)| = |z_0|$, then $f(z) = cz$ where $|c| = 1$ (i.e. f a rotation)
- $|f'(0)| \leq 1$, and if equality holds, then $f(z) = cz$ where $|c| = 1$.

Proof. Let $g(z) := \frac{f(z)}{z}$. Since $f(0) = 0$, g has a removable singularity at the origin and therefore is holomoprhic. Let $z \in \mathbb{D}$, assuming $|z| = r < 1$. Since f maps to $\mathbb{D}$ and thus $|f| \leq 1$, we have that $|g(z)| \leq \frac{1}{r}$. By the maximum modulus principle, this bound must hold for all $z \in \mathbb{D}_r$ i.e. for any $|z| < r$. Letting $r \to 1$ gives that $|g| \leq 1$ which gives the proof. Again by the maximum modulus principle, we see that if $|g(z_0)| = 1$ for z_0 in $\mathbb{D}$ (i.e. an "interior max"), it must be that $|g|$ constant equal to 1, which gives the result. For the second point, note that $g(z) \to f'(0)$ as $z \to 0$, but also converges to $g(0)$ by holomorphicity. We know $|g| \leq 1$, so it follows that $|f'(0)| \leq 1$. Finally if $|f'(0)| = |g(0)| = 1$, from the same line of reasoning as above we have that f a rotation. ■

Theorem 36 (Automorphisms of the Unit Disc): For $\Omega \subset \mathbb{C}$, define $\mathrm{Aut}(\Omega) := \{f : \Omega \to \Omega \mid f \text{ a conformal map}\}$. This is naturally a group under composition.

If $f \in \mathrm{Aut}(\mathbb{D})$, then there exists a $\theta \in \mathbb{R}$ and $\alpha \in \mathbb{D}$ such that

$$f(z) = e^{i\theta}\psi_\alpha(z),$$

where $\psi_\alpha(z) := \frac{\alpha - z}{1 - \overline{\alpha}z}$ is a *Blaschke factor*.

Proof. Let $\alpha \in \mathbb{D}$ be such that $f(\alpha) = 0$, which exists and is unique. Let $g = f \circ \psi_\alpha$. One checks that $g(0) = 0$, so by Schwarz, $|g(z)| \leq |z|$. g is also invertible, and $g^{-1}(0) = 0$ so we also have $|g^{-1}(w)| \leq |w|$. This implies, taking $w = g(z)$, that $|z| \leq |g(z)| \leq |z|$ i.e. $|g(z)| = |z|$. This implies $g(z) = e^{i\theta} \cdot z$ for some $\theta \in \mathbb{R}$, which gives the proof upon composing both sides by ψ_α (which is its own inverse). ■

Corollary 4 (Automorphisms of the Upper Half Plane): Every automorphism in $\mathrm{Aut}(\mathbb{H})$ is a *linear fractional transformation* of the form

$$f_M(z) = \frac{az + b}{cz + d},$$

for some $M \in \mathrm{SL}_2(\mathbb{R}) = \{M \in \mathbb{R}^{2\times 2} : \det(M) = 1\}$. In fact,

$$\mathrm{Aut}(\mathbb{H}) \cong \mathrm{PSL}_2(\mathbb{R}) := \mathrm{SL}_2(\mathbb{R})/\{I, -I\}$$

Proof. Recall the conformal function $F : \mathbb{H} \to \mathbb{D}$. One checks that $\Gamma : \mathrm{Aut}(\mathbb{D}) \to \mathrm{Aut}(\mathbb{H})$ given by $\Gamma(\varphi) := F^{-1} \circ \varphi \circ F$ is a group isomorphism. Thus to characterize automorphisms of $\mathbb{H}$ it suffices to compute the conjugation by F of automorphisms of $\mathbb{D}$, which yields the result. ■

Theorem 37 (Riemann-Mapping Theorem): Let $\Omega \subset \mathbb{C}$ be a simply connected open domain that is not all of $\mathbb{C}$. Given $z_0 \in \Omega$, then there exists a unique conformal map $F : \Omega \to \mathbb{D}$ such that

$$F(z_0) = 0, \quad F'(z_0) > 0.$$

In particular, every such domain is conformal to the open unit disc.

Proof. The proof is long. The idea is as follows:

(i) Show Ω conformal to an open subset of $\mathbb{D}$ containing the origin. One does this by basically 'shrinking' Ω via a logarithmic-type transformation.

(ii) Assuming from 1. that $0 \in \Omega \subset \mathbb{D}$, one considers the family of functions

$$\mathcal{F} := \{f : \Omega \to \mathbb{D}, f \text{ holomorphic, injective, and } f(0) = 0\}.$$

One sees that $\mathcal{F}$ is a nonempty, uniformly bounded family of holomorphic functions. By the Cauchy inequalities, $s := \sup_{f\in\mathcal{F}} |f'(0)|$ exists (and is finite). Let $\{f_n\} \subset \mathcal{F}$ such that $|f_n'(0)| \to s$. By combining Cauchy's integral representation theorem, one obtains equicontinuity of $\mathcal{F}$, which allows us to use an Arzela-Ascoli-type argument to argue that $\{f_n\}$ actually converges uniformly (on compact sets) to some holomorphic function f. We see that f is injective (by an "argument principle"-type argument, using properties of f).

(iii) We claim f in step 2. is conformal. We showed holomorphicity and injectivity, so we need to show surjectivitiy. Supposing otherwise, the idea is to construct another function that lives in $\mathcal{F}$ but with strictly greater derivative norm at 0, contradiciting the maximality. Then by precomposing f with a rotation, one automatically gets the $f'(0) > 0$.

■

Corollary 5: Any two simply connected proper open subsets of $\mathbb{C}$ are conformal.

Remark 20: Remark that there is no hope that there exists a conformal map $f : \mathbb{C} \to \mathbb{D}$ for such a map would necessarily be entire and bounded and thus constant by Liouville's, and in particular not injective.

1.2.5 Some Fourier Transform

Definition 24 (Fourier Transform): The *Fourier transform* of a function $f : \mathbb{C} \to \mathbb{C}$ is defined by, where the integrals make sense and converge,

$$\hat{f}(\xi) := \int_{-\infty}^{\infty} f(x) e^{-2\pi i x\xi} \, \mathrm{d}x, \quad \xi \in \mathbb{R}.$$

For $a > 0$, define the class of functions

$$\mathcal{F}_a := \left\{ f : \begin{array}{c} f \text{ holomorphic on } S_a := \{z \in \mathbb{C} \mid |\mathrm{Im}(z)| \le a\} \\ \exists\, A > 0 \text{ such that } |f(z)| \le \frac{A}{1+\Re(z)^2} \text{ for all } z \in S_a \end{array} \right\}.$$

Define finally $\mathcal{F} := \bigcup_{a>0} \mathcal{F}_a$.

Proposition 14: Let $f \in \mathcal{F}_a$ for some $a > 0$. Then $|\hat{f}(\xi)| \le Be^{-2\pi b\,|\xi|}$ for all $\xi \in \mathbb{R}$ and $0 \le b < a$; when such a bound on a function exists, we say it is of *exponential type*.

Proof. The idea is to "shift" the contour to the line from $-\infty - ib$ to $\infty - ib$. ■

Theorem 38 (Fourier Inversion): For $f \in \mathcal{F}$, then the *Fourier inversion formula* holds, that is, for all $x \in \mathbb{R}$,

$$f(x) = \int_{-\infty}^{\infty} \hat{f}(\xi) e^{2\pi i x\xi} \, \mathrm{d}\xi.$$

Theorem 39 (Poisson Summation Formula): If $f \in \mathcal{F}$,

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n).$$

2 Algebra

2.1 Linear

2.1.1 Elementary

2.1.2 Vector Spaces

2.1.3 Diagonalization and Related

2.2 Groups

2.2.1 Fundamentals

Definition 25 (Groups, Action): A group G is a set equipped with a binary operation $\cdot$ satisfying the axioms:

- $f \cdot (g \cdot h) = (f \cdot g) \cdot h,\ \forall\, f, g, h \in G$
- $\exists\, 1 \in G$ s.t. $g \cdot 1 = 1 \cdot g = g\, \forall\, g \in G$
- $\forall\, g \in G, \exists\, g^{-1} \in G$ s.t. $g \cdot g^{-1} = g^{-1} \cdot g = 1$

G is said to be abelian/commutative if $gh = hg$ for every $g, h \in G$.

A group action on a set X is a function $\varphi : G \times X \to X$ satisfying:

- $\varphi(h, \varphi(g, x)) = \varphi(h \cdot g, x), \forall\, g, h \in G, x \in X$
- $\varphi(1, x) = x\, \forall\, x \in X$

When clear from context, we write $g \cdot x = \varphi(g, x)$. When $\varphi(G, X) := \{\varphi(g, x) : g \in G, x \in X\}$ is equal to X, we say the action of G is *transitive*. A set X equipped with a group action of G is sometimes called a *G-set*.

Definition 26 (Orbit, Stabilizer): Let G act on a set X. Define, for $x \in X$,

$$\mathcal{O}_x = \mathrm{Orb}_G(x) := \text{orbit of } x \text{ under } G = \{g \cdot x : g \in G\} \subset X,$$
$$G_x = \mathrm{Stab}_G(x) := \text{stabilizer of } x \text{ under } G = \{g \in G : g \cdot x = x\} \subset G.$$

Remark 21: The orbit is "everywhere x can go" (under G), and the stablizer is what "fixes" x (under G).

Definition 27: A *subgroup* H of a group G is a subset of G which is still a group when endowed with the operation from G (so in particular it is closed under the operation). One sometimes write $H < G$, or $H \leq G$ if H possibly equal to G.

A *(left) coset* of H in G is a set of the form

$$aH = \{ah : h \in H\},$$

where a some element of G. One denotes $G/H = \{\text{set of cosets of } H\}$ Equivalently, there is a natural action of H acting on G as a set (by right-multiplication), given by $h \star g := g \cdot h$; thus cosets of H are just orbits under this action.

Definition 28 (Homomorphism): A *group homorphism* $\varphi : G_1 \to G_2$ is a function such that

$$\varphi(gh) = \varphi(g)\varphi(h)$$

for all $g, h \in G_1$. When φ a bijection we call it a group isomorphism.

Theorem 40 (Lagrange): Let $H \subset G$ a finite subgroup of a finite group. Then all cosets of H have the same cardinality, and in particular are disjoint. In particular, we have

$$|G| = |G/H| \cdot |H|,$$

and so $|H|$ divides $|G|$.

Proof. The disjointness follows from the "orbit of an action" characterization (namely, orbits are either disjoint or equal). For the equality of cardinality, fix $a \notin H$ and define the map $f : H \to aH, h \mapsto ah$. This is an injection, since $f(h_1) = f(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2$ by multiplying both sides by a^{-1}. This is also a surjection since given $ah \in aH$, one simply maps h by f. This shows $|aH| = |H|$ and since a was arbitrary, completes the proof. The "in particular" follows from the partitioning result. ∎

Proposition 15: Let X a transitive G-set. Then there exists a subgroup H of G such that X is isomorphic (as a G-set) to $X \cong G/H$, equipped with the left-action

$$(g, aH) \in G \times G/H \mapsto g \cdot aH := (ga)H \in G/H.$$

Thus, $|X|$ divides $|G|$ and the *orbit-stabilizer formula* holds:

$$|G| = |X| \cdot |G_x|, \quad \forall\, x \in X.$$

Remark 22: When we say "X_1, X_2 isomorphic as G-sets", we mean a bijection which respects the respect group actions, i.e. $f : X_1 \to X_2$, $f(g \cdot_1 x) = g \cdot_2 f(x)$.

Remark 23: If X not transitive, we can reword this proof by taking any orbit $\mathcal{O}_x$ in X, in which case the formula reads $|G| = |\mathcal{O}_x| \cdot |G_x|$.

Proof. Fix $x \in X$ and let $H := G_x$, and let $f : G/H \to X$ be given by $f(aH) := a \cdot x$. ■

Definition 29 (Normal subgroup, quotients): Given a group G, a subgroup $H \subset G$ is said to be *normal* if it is closed under conjugation by G, that is,

$$ghg^{-1} \in H, \quad \forall\, g \in G, h \in H.$$

Sometimes people write $H \triangleleft G$ for "H is a normal subgroup of G" (*sometimes with a bar underneath if H possible equal to G*).

The *quotient group* is the group G/H of cosets of G with respect to H equipped with left-multiplication (*one checks that this is indeed a well-defined group when H normal in G).*

G is said to be *solvable* if there exists a sequence of subgroups

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{n-1} \subset G_n \subset G$$

such that G_{i-1} a normal subgroup of G_i and G_i/G_{i-1} abelian, for $i = 1, ..., n$.

Proposition 16: Let $\varphi : G \to H$ a group homomorphism. Then $N := \ker(\varphi)$ a normal subgroup of G.

Moreover, φ induces an injective homomorphism $\tilde{\varphi} : G/N \to H$ defined by $\tilde{\varphi}(aN) := \varphi(a)$. In particular, $\mathrm{im}(\varphi)$ is isomorphic to G/N.

Proof. If $h \in N, g \in G$, then $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g) \cdot \varphi(g)^{-1} = 1$ so $ghg^{-1} \in N$.

We need to show $\tilde{\varphi}$ well-defined. If $aN = a'N$, then there exists $h \in N$ such that $a = a'h$. So

$$\tilde{\varphi}(aN) = \varphi(a) = \varphi(a'h) = \varphi(a')\varphi(h) = \tilde{\varphi}(a'N) \cdot 1 = \tilde{\varphi}(a'N),$$

so the function is well-defined. It is injective since

$$\tilde{\varphi}(aN) = 1 \Leftrightarrow \varphi(a) = 1 \Leftrightarrow a \in N \Leftrightarrow aN = N,$$

but $N = 1_{G/N}$, so φ injective. ■

2.2.2 Sylow

Theorem 41 (Sylow's Theorem): Suppose $\#G = m \cdot p^t$, where $p \nmid m$ and p prime.

(i) (*Sylow 1*) G has a subgroup of cardinality p^t (called a *Sylow-p subgroup* of G).
(ii) (*Sylow 2*) Suppose H_1, H_2 are Sylow-p subgroups of G, then there exists a $g \in G$ such that $gH_1g^{-1} = H_2$.
(iii) (*Sylow 3*) If N_p the number of distinct Sylow-p subgroups of G, then:
  (i) $N_p \mid m$
  (ii) $N_p \underset{p}{\equiv} 1$

Proof. ■

2.2.3 Some Particular Groups

Definition 30 (Generator of a group): We say a group G is *generated* by elements $g_1, ..., g_n$ if

$$G = \langle g_1, ..., g_n \rangle := \{\text{all possible products of powers of } g_1, ..., g_n\}.$$

Definition 31 (Cyclic Groups, Unit Groups): For $n \geq 1$ an integer, the *cyclic group of order* n is defined as $\mathbb{Z}/n\mathbb{Z} = \{0, 1, ..., n-1\}$ equipped with addition and with entries read mod n.

For $n \geq 1$ an integer, the *unit group of order* n is defined as $(\mathbb{Z}/n\mathbb{Z})^\times$ equipped with multiplication, where we restrict $\mathbb{Z}/n\mathbb{Z}$ to the invertible elements (mod n).

Proposition 17: Let p prime and G a group of order p. Then $G = \mathbb{Z}/p\mathbb{Z}$. In addition, $\#(\mathbb{Z}/p\mathbb{Z})^\times = p - 1$.

Proof. Let $a \in G$ not equal to the identity. Then the subgroup H generated by a (i.e. $\{a, a+a, a+a+a, ...\}$) is a subgroup of G isomorphic to $\mathbb{Z}/n\mathbb{Z}$ where $n = \#H$. Being a subgroup, $n|\#G$, and since $n > 1$ and $\#G$ prime, $n = p$ and thus $H = G \cong \mathbb{Z}/p\mathbb{Z}$.

Let $a \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$. Then $a \nmid p$ so $\gcd(a, p) = 1$. Thus there exists a $b, c \in \mathbb{Z}$ such that $ab + cp = 1$ i.e. $ab \underset{p}{\equiv} 1$. Rewriting b mod p so that $b \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ completes the proof of the second part, since then we've shown ($(\mathbb{Z}/p\mathbb{Z})^\times$ equals (as a set) $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$). ■

Definition 32 (Permutation, Symmetric, Alternatic Groups): Let X a finite set of n elements. The *symmetric group* of X is the set of bijections of X, i.e.

$$S_X := \{f : X \to X \mid f \text{ a bijection}\}.$$

When $X = \{1, ..., n\}$, we often write $S_n \equiv S_X$. We call $f \in S_X$ a *permutation* of X.

The *sign*, or sgn, of a permutation $f \in S_n$ is defined to be

$$\text{sgn}(f) := (-1)^{N(f)}, \quad N(f) := \#\{(x, y) \in X \times X \mid x < y \text{ and } f(x) > f(y)\},$$

i.e. the number of "inversions" that f contains. We sometimes say f is even/odd if $\text{sgn}(f) = +1/-1$.

The *alternating group* on n elements is the subgroup

$$A_n := \{f \in S_n \mid \text{sgn}(f) = 1\}.$$

Proposition 18:

- $\#S_n = n!$, $\#A_n = \frac{n!}{2}$
- a *transposition* of $\{1, ..., n\}$ is a permutation that only interchanges two elements and fixes the rest. Any permutation can be written as a composition of transpositions. Moreover, the sign of a permutation is equal to the parity of (any) number of transpositions needed to write the permutation

Proof. A permutation, being a bijection of $\{1, ..., n\}$ has n choices of where to send 1, $n-1$ choices of where to send 2, etc, for $n \cdot (n-1) \cdots 1 = n!$ total choices. So, $\#S_n = n!$. The size of $\#A_n$ follows pretty clearly from the definition of sgn. Alternatively, one notes that $\text{sgn} : S_n \to \{-1, 1\}$ a surjective group homomorphism (with the right-hand side equipped with multiplication). Then $A_n = \ker(\text{sgn})$, and thus $(\#S_n)/(\#A_n) = 2$. ■

Definition 33 (Dihedral Groups): For $n \geq 1$, the *order* $2n$ *dihedral group* (on n vertices) is defined as the gorup generated by

$$D_{2n} := \langle \sigma, \tau \rangle, \quad \text{ord}(\sigma) = 2, \text{ord}(\tau) = n, \sigma\tau\sigma^{-1} = \tau^{-1}.$$

Proposition 19: $\#D_{2n} = 2n$.

Proposition 20 (Finitely Generated Abelian Groups): An abelian group G is said to be *finitely generated* if it has a finite generating set. Any finitely generated abelian group G is isomorphic to

$$\mathbb{Z}^m \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_m\mathbb{Z}.$$

2.3 Rings

Definition 34 (Rings, Ideals): A *ring* is a set R equipped with two binary operators $+$ and $\times$ such that

- $(R, +)$ an abelian group
- $(R, \times)$ a monoid (has identity and is associative)
- $a \times (b + c) = a \times b + a \times c$
- $(b + c) \times a = b \times a + c \times a$

A commutative ring is a ring where $\times$ is commutative.

An *ideal* I of a ring R is a subset $I \subset R$ such that I is an additive subgroup of R and is closed under multiplication by R. We sometimes write $I \triangleleft R$.

Remark 24: Some conventions do not require rings to have multiplicative identities, and call those with such elements "rings with identity".

Definition 35 (Types of Ideals): Let $I \triangleleft R$. We say I is:

- *maximal* if for all ideals $J \triangleleft R$, if $I \subsetneq J$ then $J = R$
- *prime* if $a \cdot b \in I \Rightarrow a$ or $b \in I$
- *principal* if I of the form $aR = (a) = \{ar : r \in R\}$ for some $a \in R$

Definition 36 (Types of Rings): Let R be a nonzero ring. A *left (right) zero divisor* of R is an element $a \in R$ such that there exists a nonzero $b \in R$ such that $ab = 0$ ($ba = 0$). We say R is:

- an *integral domain* if it is commutative and has no nonzero zero divisors
- a *principal ideal ring* if every ideal in R is principal
- a *Euclidean domain* if it is an integral domain upon which there exists a function $f : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ such that for all $a \in R, b \in R \setminus \{0\}$ there exists q and r in R such that $a = bq + r$ and either $r = 0$ or $f(r) < f(b)$
- a *principal ideal domain (PID)* if it is an integral domain and a principal ideal ring

Remark 25: The f function, called a *Euclidean function*, is essentially a generalization of "size", which is not necessarily an ordering but reflects some of its properties.

Proposition 21: Euclidean domain $\Rightarrow$ PID. The integers are a Euclidean domain. If $\mathbb{F}$ a field, then $\mathbb{F}[x] = \{p(x) : p \text{ a polynomial with coefficients in } \mathbb{F}\}$ is a Euclidean domain.

Proof. Let R a Euclidean domain and $I \subset R$ an ideal. Then, $S := \{f(r) \mid r \in I\}$ is a subset of the natural numbers and thus must have a least element by the Well-Ordering Principle. Let $m \in I$ be such that $f(m) = \min S$. We claim $I = (m)$. The direction $(m) \subset I$ is clear since $m \in I$. Now let $a \in I$ be any other element. By the Euclidean property, $a = mq + r$ for some $q, r \in R$. If $r = 0$ we're done, so assume $r \neq 0$ so then $f(r) < f(m)$. This implies r cannot be in I, else we'd contradict the minimality of m. But $a - mq \in I$ (since $a, m \in I$, and $q \in R$ implies $mq \in I$), but this equals r, so we have a contradiction. Thus $r = 0$, and so $a = mq \in (m)$, hence $I = (a)$.

The integers are Euclidean by taking $f(r) = r$ and by employing the Euclidean algorithm, and $\mathbb{F}[x]$ is by taking $f(p) = \deg(p)$ and employing the Euclidean algorithm (for polynomials). ■

Definition 37 (Homomorphism): A ring homomorphism $\varphi : R \to S$ is a map that is a group homomorphism on $(R, +)$, is multiplicative (i.e. $\varphi(ab) = \varphi(a)\varphi(b)$), and $\varphi(1) = 1$.

Proposition 22: Given a ring homomorphism $\varphi : R \to S$, $\ker(\varphi)$ an ideal of R. Conversely, if $I \subset R$ is an ideal, then there exists a ring S and a surjective homomorphism $\varphi : R \to S$ such that $I = \ker(\varphi)$.

If $\varphi : R \to S$ is a surjective ring homomorphism, then $R/\ker(\varphi)$ is isomorphic to S.

Proof. For the first, we know from the group homomorphism property that $\ker(\varphi)$ closed under addition, and if $r \in \ker(\varphi)$ and $a \in R$, then $\varphi(ar) = \varphi(a)\varphi(r) = \varphi(a) \cdot 0 = 0$ so $ar \in \ker(\varphi)$. For the second, we can define the *quotient ring* $S := R/I = \{a + I : a \in R\}$, with addition defined as in a quotient group and multiplication defined "component wise" (one checks this is well-defined and defines a ring). Then define $\varphi : R \to S$ by $\varphi(r) = r + I$.

The last point is the *first isomorphism theorem* (for rings) and the proof is identical as the analog for groups. ■

Proposition 23: Let R a ring.

- I is a prime ideal iff R/I has no nonzero zero divisors
- I is a maximal ideal iff R/I is a field

Proof. Assume I prime and that $(a+I)(b+I) = 0+I$. This implies $ab \in I$, so either a or b in I by primality. Thus either $a+I$ or $b+I = I$, and in either case neither can be a nonzero zero divisor. The converse direction is identical.

Assume I maximal. We need to show R/I has inverses. Let $a+I \in R/I$ nonzero (i.e. $a \notin I$). Consider the ideal $J \coloneqq Ra+I = \{ra+b : r \in R, b \in I\}$. This is an ideal which contains I as a subset. By maximality, $J = I$ or $J = R$, but the first is not possible since this would imply $a \in I$. So $J = R$, and thus given $1 \in R$, there exists $r \in R$ and $b \in I$ such that $ar + b = 1$. Thus,

$$(a+I)(r+I) = ar + I = ar + b + I = 1 + I,$$

i.e. $r + I = (a+I)^{-1}$. Conversely, assume $J \supsetneq I$. Let $a \in J \setminus I$, so $a + I \neq 0 \in R/I$ is invertible, i.e. there is a $b \in R$ such that $(a+I)(b+I) = 1+I$. This implies there is an $r \in I$ such that $ab + r = 1$. Since also $r \in J$, this implies $1 \in J$, and thus $J = R$ and so I maximal. ■

2.4 Fields & Galois Theory

Definition 38 (Fields, Field Extensions): A *field* is a commutative ring F with identity in which every nonzero element has a multiplicative inverse.

A *field extension* E of a field F is a field which contains F as a subfield; we write E/F. We can canonically view E as an F vector space (by forgetting the multiplicative structure of elements); we write $[E : F] := \dim_F(E)$ for the *degree* of E over F. We say E/F a *finite extension* if this number is finite.

Proposition 24 (Multiplicativity of Degrees): Let K/E and E/F be finite extensions. Then K/F also a finite extension, and

$$[K : F] = [K : E] \cdot [E : F].$$

Proof. If $\{e_1, ..., e_n\}$ a basis for E/F and $\{k_1, ..., k_m\}$ a basis for K/E, one checks that $\{e_i \cdot k_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ a basis for K/F. ■

Definition 39 (Algebraic, Transcendental): Let E/F. We say $\alpha \in E$ is *algebraic* if it is the root of some polynomial $f(x) \in F[x]$. We say α is *transcendental* otherwise.

Proposition 25: If E/F finite, every $\alpha \in E$ is algebraic. Moreover, there exists a polynomial of degree at most $[E : F]$ that α satisfies.

Proof. Let $\alpha \in E$ and put $n := [E : F]$. Then $\{1, \alpha, \alpha^2, ..., \alpha^n\}$ must be a linearly independent set, and thus there exist $f_0, ..., f_n \in F$ such that

$$f_0 + f_1\alpha + \cdots + f_n\alpha^n = 0.$$

In particular, we see that this implies $f(x) := f_n x^n + \cdots + f_1 x + f_0$ is a polynomial in $F[x]$ with α as a root. ■

Definition 40 (Splitting Fields): We say E/F a *splitting field* of a polynomial $f(x) \in F[x]$ if

(i) $f(x)$ factors into linear factors in $E[x]$, i.e. there exists $r_1, ..., r_n \in E$ such that

$$f(x) = (x - r_1)\cdots(x - r_n),$$

and

(ii) E is *generated* by $r_1, ..., r_n$.

Remark 26: We say a field extension E/F is *generated by a set* S if it is the smallest field containing F as a subfield and the elements in S.

Definition 41 (Automorphisms of a Field Extension): Let E/F, and define the group

$$\mathrm{Aut}(E/F) := \{\sigma : E \to E \mid \sigma \text{ is } F - \text{linear, multiplicative, and } \sigma|_F \equiv \mathrm{id}\}.$$

Remark 27: $\sigma \in \mathrm{Aut}\ (E/F)$ preserves the field structure on E and leaves F invariant.

Proposition 26 (Properties of $\mathrm{Aut}(E/F)$): Let E/F be a finite extension. Then the following hold:

- $\mathrm{Aut}(E/F)$ acts on E with finite orbits (that is, $\#\mathrm{Orb}_{\mathrm{Aut}(E/F)}(\alpha) < \infty$ for every $\alpha \in E$)
- $\#\mathrm{Aut}(E/F) < \infty$; in fact,
- $\#\mathrm{Aut}(E/F) \leq [E : F]$.

If $\#\mathrm{Aut}(E/F) = [E : F]$, we say that E/F a *Galois extension*, and write $\mathrm{Gal}(E/F) = \mathrm{Aut}(E/F)$.

Proof. Let $\alpha \in E/F$ satisfy $f(x) = a_n x^n + \cdots + a_0$ (exists by finiteness). Let $\sigma \in \mathrm{Aut}(E/F)$. Then notice, using linearity and multiplicativity of σ,

$$\begin{aligned} f(\sigma(\alpha)) &= a_n\sigma^n(\alpha) + \cdots + a_1\sigma(\alpha) + a_0 \\ &= a_n\sigma(\alpha^n) + \cdots + a_1\sigma(\alpha) + a_0 \\ &= \sigma(a_n\alpha^n + \cdots + a_1\alpha + a_0) \\ &= \sigma(f(\alpha)) = \sigma(0) = 0. \end{aligned}$$

Thus, $\sigma(\alpha) \in \{\text{roots of } f\}$ hence $\mathrm{Orb}\ (\alpha) \subset \{\text{roots of } f\}$, proving the finiteness since f has only finitely many roots. By a previous proposition, this moreover shows $\#\mathrm{Orb}(\alpha) \leq [E : F]$.

Let $e_1, ..., e_n$ a basis for E/F and $\sigma \in \mathrm{Aut}(E/F)$. By linearity, σ uniquely determined by the n-tuple $S_\sigma := (\sigma(e_1), ..., \sigma(e_n))$. We see that $S_\sigma \in \mathrm{Orb}(e_1) \times \cdots \times \mathrm{Orb}(e_n)$. The set on the right-hand side is finite (with size at most n^n by the previous proof) so $\#\mathrm{Aut}(E/F) < \infty$.

■

2.4.1 Characterization of Finite Fields