What I learned: Winter 2024

What follows is a summary of the major concepts touched upon in my coursework this quarter.

1 Real Analysis II: Measure Theory

Let Ω be a set. An algebra of sets on Ω is a subset of the power set $\mathcal{P}(\Omega)$ that is closed under complements and finite intersections (which, by de Morgan's laws, entails closure under finite unions). A **σ-algebra** on Ω is an algebra that is furthermore closed under countable intersections (which, by de Morgan's laws, entails closure under countable unions). In particular, the **Borel sets** are the smallest σ-algebra on $\mathbf{R}$ containing the open sets. Borel sets define Borel-measurable functions: a function f is Borel-measurable if and only if $f^{-1}(U)$ is Borel for all open sets U.

We extend the concept of the length of an interval to other subsets of $\mathbf{R}$ via **Lebesgue outer measure**:

$$\lambda^*(A) = \inf\left\{\sum_n \ell(I_n) : \{I_n\}_n \text{ open covers of } A\right\}.$$

This is defined on all of $\mathcal{P}(\mathbf{R})$. This measure is nonnegative, monotonic, and countably subadditive. To obtain countable additivity, we restrict to sets that satisfy the **Caratheodory criterion**: a set E satisfies this criterion if

$$\lambda^*(W) = \lambda^*(W \cap E) + \lambda^*(W \cap E^c)$$

for all sets $W \in \mathcal{P}(\mathbf{R})$. These sets form a σ-algebra, denoted $\mathcal{M}$, called the **Lebesgue-measurable sets**. The Borel sets form a proper subset of $\mathcal{M}$. Lebesgue outer measure restricted to $\mathcal{M}$ is called Lebesgue measure and is denoted λ.

We now move to integration. We define the integral of a **simple function** (i.e. a function with finite image) as follows:

$$\int_{\mathbf{R}} \sum_{k=1}^{n} a_k \chi_{A_k}(x)\, d\lambda(x) = \sum_{k=1}^{n} a_k \lambda(A_k).$$

The integral of a nonnegative function f, then, is the supremum over all integrals of simple functions dominated by f:

$$\int_{\mathbf{R}} f(x)\, d\lambda(x) = \sup_s \int_{\mathbf{R}} s(x)\, d\lambda(x).$$

This integral satisfies the Monotone Convergence Theorem, which basically says $\lim_n \int f_n = \int \lim_n f_n$ when $\{f_n\}$ is a monotone nondecreasing sequence of nonnegative Lebesgue measurable functions. If the sequence is not necessarily monotone, we have Fatou's lemma, which says $\int \liminf_n f_n \leq \liminf_n \int f_n$. Finally, we define the general **Lebesgue integral** of f to be

$$\int_{\mathbf{R}} f(x)\, d\lambda(x) = \int_{\mathbf{R}} f^+(x)\, d\lambda(x) - \int_{\mathbf{R}} f^-(x)\, d\lambda(x)$$

where f^+ and f^- denote the positive and negative parts of f. We also say f is integrable if

$$\int_{\mathbf{R}} f^+(x)\, d\lambda(x) + \int_{\mathbf{R}} f^-(x)\, d\lambda(x) < \infty.$$

This integral satisfies the Dominated Convergence Theorem, which says that one can swap integral and limit if the sequence of functions is dominated by some other function. If a function is Riemann integrable on $[a, b]$, then it is Lebesgue integrable on $[a, b]$ and the two integrals agree.

Of course, nothing is stopping us from leaving $\mathbf{R}$. An abstract **measure space** is a triple (Ω, Σ, μ) where Ω is a set, Σ is a σ-algebra on Ω, and μ is a measure from Σ to the extended real numbers. A measure space is **complete** if all subsets of Σ-measurable sets of μ-measure zero are also Σ-measurable. In particiular, $\mathcal{M}$ is a completion of the Borel sets.

2 Representation Theory of Finite Groups

Generally, groups can be viewed as abstract entities, but much is gained from thinking of a group as doing something, i.e. acting on a set. One can gain even more if the set acted upon has some structure, i.e. is a vector space over $\mathbf{C}$. A **linear representation** of a finite group G is a homomorphism

$$\rho : G \to \mathrm{GL}_n(V)$$

where V is some complex vector space. If we choose a basis for V, we get a homomorphism

$$\rho : G \to \mathrm{GL}_n(\mathbf{C})$$

called a **matrix representation**. Two representations are **equivalent** if there exists a change of basis map (i.e. an element of $\mathrm{GL}_n(\mathbf{C})$) from one representation to the other.

We have another way of viewing representations: consider the group algebra $\mathbf{C}G$, which is the free vector space on G with a multiplication inherited from G and extended linearly.[1] A representation is the same thing as a $\mathbf{C}G$-module, i.e. there is an equivalence of categories:

$$\{\mathbf{C}G\text{-modules}\} \qquad \overset{\sim}{\longleftrightarrow} \qquad \{\text{ordered pairs } (V, \rho) \text{ where } \rho : G \to \mathrm{GL}_n(V)\}$$

If V is a $\mathbf{C}G$-module, a subspace W of V is a $\mathbf{C}G$-submodule that is G-stable, i.e. $gw \in W$ for all $g \in G$ and $w \in W$. A $\mathbf{C}G$-module V is **irreducible** if and only if the only submodules of V are 0 and V.

Maschke's theorem says that for any $\mathbf{C}G$ module V, a submodule U of V always has some other submodule W such that $V = U \oplus W$. Since $\mathbf{C}G$-modules are also inner product spaces, this is equivalent to saying that every $\mathbf{C}G$-submodule U has an orthogonal complement $U^{\perp}$ that is also a $\mathbf{C}G$-submodule.

A $\mathbf{C}G$-module V is **completely reducible** if

$$V = \bigoplus_{i=1}^{r} U_i$$

for irreducible $\mathbf{C}G$-submodules U_i of V. By induction on the dimension of V, Maschke's theorem implies that every nonzero $\mathbf{C}G$-module is completey reducible. This is important because it lets us focus only on the irreducible submodules.

Schur's lemma says that for irreducible $\mathbf{C}G$-modules V and W, a homomorphism between V and W is either the zero map or a scalar multiple of the identity map. Conversely, if every $\mathbf{C}G$-homomorphism from V to V is a scalar multiple of the identity map, then V is irreducible.

Schur's lemma also implies that irreducible representations of finite abelian groups always have degree 1. Conversely, if every irreducible representation of a finite group G has degree 1, then G is abelian (this proof uses Maschke's theorem).

One can view the group algebra $\mathbf{C}G$ as a module over itself, which affords the **regular representation**. The module $\mathbf{C}G$ contains a copy of all the irreducible representations of G (potentially with multiplicity). A corollary of this is that every group has a finite number of irreducible representations, and furthermore we have

$$\sum_{i \text{ irred.}} \dim(U_i)^2 = |G|,$$

where the U_i are the irreducible representations of G (without multiplicity).

[1] This is actually a Hopf algebra, since $\mathbf{C}[G \times G] \simeq \mathbf{C}G \otimes \mathbf{C}G$.

The **character** of a $\mathbf{C}G$-module V affording a representation $\rho : G \to \mathrm{GL}_n(\mathbf{C})$ is the function $\chi : G \to \mathbf{C}^\times$ given by $\chi(g) = \mathrm{tr}(\rho(g))$. Character values are always sums of nth roots of unity. The irreducible characters form an orthonormal set with respect to the inner product

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)},$$

which means that for irreducible characters χ and ψ, we have that $\langle \chi, \psi \rangle$ is 1 if $\chi = \psi$ and 0 otherwise. These are called the **orthogonality relations**.

Characters determine the module, i.e. $\chi_V = \chi_W$ implies $V \simeq W$ as $\mathbf{C}G$-modules. We also have that

$$\langle \chi_V, \chi_W \rangle = \dim(\mathrm{Hom}_{\mathbf{C}G}(V, W)).$$

The irreducible characters form a basis for the class functions, the space of which is a subset of $\mathrm{Hom}(G, \mathbf{C})$. The dimension theorem states that the degree of every irreducible character divides $|G|$.

To study the irreducible representations of a group, one constructs a **character table** of irreducible characters. Since the number of irreducible characters of G equals the number of conjugacy classes of G, the character table is always a square.

When G is abelian, the characters form a group under pointwise multiplication (where $\chi_V \chi_W = \chi_{V \otimes W}$) called the **Pontryagin dual** of G, denoted $\widehat{G}$. More generally, Pontryagin duality says that there is a natural isomorphism between G and the Pontryagin dual of $\widehat{G}$.

3 Modular Forms I

This winter we focused on modular forms over the entirity of $\mathrm{SL}_2(\mathbf{Z})$, with the intention of studying them over congruence subgroups in the spring. The group $\mathrm{SL}_2(\mathbf{Z})$ is called the **modular group**, and consists of all 2×2 matrices with integer entries and determinant 1. The set $\mathbf{H}$ is called the **upper half-plane**. The group $\mathrm{SL}_2(\mathbf{Z})$ acts on $\mathbf{H}$ via fractional linear tranformations:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \frac{az + b}{cz + d} \in \mathbf{H}.$$

A **modular form** of integer **weight** k for $\mathrm{SL}_2(\mathbf{Z})$ is a function $f : \mathbf{H} \to \mathbf{C}$ such that f is holomorphic on $\mathbf{H}$, bounded at ∞, and satisfies the weight k modularity condition

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau)$$

for all $\tau \in \mathbf{H}$, $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbf{Z})$. The modular group is generated by the matrices corresponding to the translation $T : \tau \mapsto 1 + \tau$ and the inversion $S : \tau \mapsto -\frac{1}{\tau}$.

The modular forms of weight k form a complex vector space $\mathcal{M}_k$. Note that there are no nontrivial modular forms of odd weight.

There exists a subset $\mathcal{F}$ of $\mathbf{H}$, called the **fundamental domain**, such that any point in $\mathbf{H}$ is $\mathrm{SL}_2(\mathbf{Z})$-equivalent to a point in $\mathcal{F}$, and no two points in $\mathcal{F}$ are $\mathrm{SL}_2(\mathbf{Z})$-equivalent.

Modular forms also have Fourier series: the ***q*-expansion** of a modular form is a series

$$f(\tau) = \sum_{n \geq 0} a_n q^n, \qquad q = e^{2\pi i \tau}.$$

If f has $a_0 = 0$, then f is called a **cusp form**. The space of cusp forms is denoted $\mathcal{S}_k$. The cusp forms make the following sequence exact:

$$0 \to \mathcal{S}_k \to \mathcal{M}_k \to \mathbf{C} \to 0.$$

For an example of a nontrivial modular form, consider the **Eisenstein series** of weight $k > 2$:

$$G_k(\tau) = \sum_{m,n}{}' \frac{1}{(m\tau + n)^k}$$

where the primed sum is over $(m, n) \in \mathbf{Z}^2 \setminus \{(0, 0)\}$. We often work with the nomalized Eisenstein series,

$$E_k(\tau) = \frac{G_k(\tau)}{2\zeta(k)} = 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n) q^n$$

In particular, we have that

$$E_4(\tau) = 1 + 240 \sum_{n \geq 1} \sigma_3(n) q^n \quad \text{and} \quad E_6(\tau) = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n$$

generate the graded algebra of modular forms, i.e. $\mathcal{M}(\mathrm{SL}_2(\mathbf{Z})) = \mathbf{C}[E_4, E_6]$. For an example of a nontrivial cusp form, consider the modular discriminant function

$$\Delta(\tau) = \frac{E_4^3(\tau) - E_6^2(\tau)}{1728} = q - 24q^2 + 252q^3 + O(q^4)$$

The modular discriminant can also be expressed as an infinite product,

$$\Delta(\tau) = q \prod_{n \geq 1} (1 - q^n)^{24}$$

We have that Δ is nonvanishing on $\mathbf{H}$ and has a simple zero at $q = 0$, i.e. $\Delta(i\infty) = 0$.

Spaces of weight k modular forms are finite-dimensional. In particular, we have

$$\dim(\mathcal{M}_k) = \begin{cases} \lfloor \frac{k}{12} \rfloor + 1 & \text{if } k \neq 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor & \text{if } k = 2 \pmod{12} \end{cases}.$$

A **modular function** is like a modular form of weight 0, except we relax holomorphicity to meromorphicity. An example of a modular function (indeed, the example that generates the rest of them) is the j-invariant:

$$j(z) = \frac{E_4^3(z)}{\Delta(z)} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + O(q^3)$$

It is holomorphic on $\mathbf{H}$ with a simple pole at $i\infty$, and is a bijection from $\widehat{\mathcal{F}}$ to $\widehat{\mathbf{C}}$. Every modular function is a rational function of j, i.e. the field of modular functions can be written $\mathbf{C}(j)$.

Since modular forms are holomorphic, we may speak of their derivatives. The **Serre derivative** of a weight k modular form is

$$\theta_k[f](z) = \frac{1}{2\pi i} f'(z) - \frac{k}{12} E_2(z) f(z).$$

It sends weight k modular forms to weight $k + 2$ modular forms, and cusp forms to cusp forms.

We denote the q-coefficients of Δ by $\tau(n)$ – this is called the **Ramanujan tau function**. We have that τ is multiplicative, and satisfies the following identity for prime powers:

$$\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1}).$$

In addition to these two observations, Ramanujan also noticed that $|\tau(p)| \leq 2p^{11/2}$, but this wasn't proven until Deligne in 1974 as a consequence of his proof of the Weil conjectures.

The nth **Hecke operator** is

$$T_n[f](z) = n^{k-1} \sum_A d^{-k} f(Az) = \frac{1}{n} \sum_A a^k f(Az).$$

where A runs through orbit representatives of 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with determinant n. If $f(z) = \sum a_m q^m$ then

$$T_n[f](z) = \sum_{n \geq 0} \left(\sum_{d|(m,n)} d^{k-1} a_{\frac{mn}{d^2}} \right) q^m.$$

The linear q-coefficient of $T_n[f]$ is a_n.

We call a nonzero modular form an **eigenform** if for all $n \geq 1$, $T_n f = \lambda(n) f$ for some complex Hecke eigenvalue λ. A normalized eigenform has $a_1 = 1$ and hence $a_n = \lambda(n)$. Normalized eigenforms have multiplicative q-coefficients, i.e. $a_n a_m = a_{mn}$ for coprime m and n. In fact, if $(m, n) = 1$ then $T_m T_n = T_{mn}$. By linear algebra, any nonzero space of cusp forms has at least one eigenform for all the Hecke operators.

To any normalized eigenform in S_k we may associate an ***L*-function**

$$L(f, s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}},$$

which in turn has a completion

$$\Lambda(f, s) = (2\pi)^{-s} \Gamma(s) L(f, s)$$

which satisfies

$$\Lambda(f, s) = (-1)^{k/2} \Lambda(f, k - s).$$

The completed L-function is also the Mellin tranform of $F(t) = f(it)$.

4 Algebraic Number Theory II

Algebraic number theory is both the algebraic side of the study of number theory and the theory of algebraic numbers. A complex number α is an **algebraic number** if it is the root of a nonzero polynomial with integer coefficients. The field of algebraic numbers is denoted $\overline{\mathbf{Q}}$; it is an infinite extension of $\mathbf{Q}$ (and hence not a number field). It is also the algebraic closure of $\mathbf{Q}$.

If the polynomial satisfying the condition above is also monic, then α is an **algebraic integer**. The set of all algebraic integers forms an integral domain denoted $\overline{\mathbf{Z}}$. We have $\overline{\mathbf{Q}} = \text{Frac}(\overline{\mathbf{Z}})$.

The ring $\overline{\mathbf{Z}}$ is too overwhelming to work with all at once, so we intersect it with **number fields** (finite extensions of $\mathbf{Q}$) to get rings of algebraic integers. If K is a number field, its ring of integers is $\mathcal{O}_K = K \cap \overline{\mathbf{Z}}$. We have $K = \text{Frac}(\mathcal{O}_K)$.

Since $\mathbf{Q}$ has characteristic zero, all finite extensions of $\mathbf{Q}$ are separable. Thus, a degree n number field K has exactly n monomorphisms $\sigma_i : K \hookrightarrow \mathbf{C}$ that fix $\mathbf{Q}$. The monomorphisms map α to its conjugates

$$\sigma_1(\alpha) \overset{\text{WLOG}}{=} \alpha, \quad \sigma_2(\alpha), \quad \ldots \quad \sigma_n(\alpha).$$

The **norm** of an algebraic integer α is the product of the conjugates of α; the **trace** of α is the sum of the conjugates. The norm is multiplicative while the trace is linear.

The ring of integers $\mathcal{O}_K$ of a number field K is a special kind of ring called a **Dedekind domain**, defined to be a Noetherian integral domain in which every localization at a nonzero prime ideal $\mathfrak{p}$ is a discrete valuation ring (a PID with a unique maximal ideal). Equivalently, a Noetherian integral domain is Dedekind if it is

integrally closed and all nonzero prime ideals are maximal.

In a Dedekind domain, we have unique factorization into ideals. Since $\mathcal{O}_K$ is a Dedekind domain for any number field K, we have that rings of integers of number fields have unique ideal factorization.

In the homework, we made progress towards proving the following result. Let R a Dedekind domain with field of fractions K, and let L be a finite separable extension of K. Let R' be the integral closure of R in L and let $\mathfrak{p}$ be a nonzero prime ideal of R. If

$$\mathfrak{p}R' = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},$$

then

$$[L : K] = \sum_{i=1}^{g} e_i f_i,$$

where $f_i = f(\mathfrak{P}_i/R)$. In particular, if L is Galois, then the e_i and f_i are the same for all i, and so we get

$$efg = [L : K].$$

Of course, what's going on here is that $R = \mathcal{O}_K$ and $R' = \mathcal{O}_L$.

A number field K also has **fractional ideals**, which are finitely generated nonzero submodules of K (or, equivalently, rank one vector bundles over the affine scheme $\mathrm{Spec}(\mathcal{O}_K)$). Yet another equivalent condition for an integral domain to be Dedekind is if every nonzero fractional ideal is invertible.

When this happens, the fractional ideals form an abelian group under ideal multiplication. The nonzero principal ideals form a subgroup of this group. The quotient of the nonzero fractional ideals by the nonzero principal ideals is called the **ideal class group**.

The size of the ideal class group of a number field K is denoted h_K and is called the **class number** of K. If $h_K = 1$, then $\mathcal{O}_K$ is a PID and hence a UFD. So, in a sense, h_K measures how far $\mathcal{O}_K$ is from having unique factorization of elements. A theorem of Carlitz (1960) states that if $h_K \leq 2$, then every factorization has the same number of irreducible factors.

A **lattice** is a discrete subgroup of $\mathbf{R}^n$. Minkowski's theorem states that if L is a full rank lattice with fundamental domain T and X is a bounded symmetric convex subset of $\mathbf{R}^n$ such that the volume of X strictly exceeds 2^n times the volume of T, then X contains a nonzero point of L. A corollary of this theorem is that $h_K < \infty$ for all number fields K.

5 Independent reading

Let $(X, \leq_X)$ and $(Y, \leq_Y)$ be partially ordered sets. A map $f : X \to Y$ is **antitone** if

$$x_1 \leq_X x_2 \quad \Longrightarrow \quad f(x_2) \leq_Y f(x_1).$$

An antitone **Galois connection** between X and Y is a pair of antitone maps

$$\Phi : X \to Y \quad \text{and} \quad \Psi : Y \to X$$

such that

$$x \leq_X \Psi(y) \quad \Longleftrightarrow \quad y \leq_Y \Phi(x).$$

Each Galois connection induces a bijective **Galois correspondence** between $\Psi(\Phi(X))$ and $\Phi(\Psi(Y))$.

Here's the prototypical example. Let L/K be a field extension, $(A, \subseteq)$ the partially ordered set of subfields of L that contain K, and $(B, \subseteq)$ the partially ordered set of subgroups of $\mathrm{Gal}(L/K)$. Furthermore, let L^H be the field consisting of all the elements of L fixed by all elements of a subgroup H. Then the maps

$$\Phi : A \to B \quad \text{via} \quad E \mapsto \mathrm{Gal}(L/E) \qquad \text{and} \qquad \Psi : B \to A \quad \text{via} \quad H \mapsto L^H$$

form an antitone Galois connection.

Though that last example was fundamental, this one is perhaps more exciting.

Fix a natural number n and an algebraically closed field k. Let $A = \mathcal{P}(k[x_1, \ldots, x_n])$ and $B = \mathcal{P}(k^n)$ be power sets, partially ordered by inclusion. Then $V : A \to B$ given by

$$S \mapsto \{x \in k^n : f(x) = 0 \quad \forall f \in S\}$$

and $I : B \to A$ given by

$$U \mapsto \{f \in k[x_1, \ldots, x_n] : f(x) = 0 \quad \forall x \in U\}$$

form an antitone Galois connection. We have $I(V(J)) = \sqrt{J}$ where $\sqrt{J}$ is the **radical** of the ideal J. The closed sets of $V(I(B))$, known as **affine algebraic sets**, form the **Zariski topology**. This is arguably where algebraic geometry begins.

Now, we don't need to work over an algebraically closed field. In fact, we don't need a field at all. All we need is a commutative ring with identity R. We denote by $\mathrm{Spec}(R)$ the **spectrum** of R, which is the set of prime ideals. We can endow $X = \mathrm{Spec}(R)$ with the Zariski topology, and further define the **structure sheaf** $\mathcal{O}_X$. The result is an **affine scheme**.

A **scheme** is basically a bunch of affine schemes fused together, an algebraic manifold. Add a few more conditions and one gets the definition of an **affine variety**. A **curve** is a variety of dimension one.[2]

The point of algebraic geometry is to *think about things geometrically, but prove them algebraically.*

The theory of schemes is a mix of algebraic geometry, algebraic number theory, and commutative algebra.

[2]This is remarkably similar to being a Dedekind domain, if you think about it.