Inverse Problems and Spectra

March 28, 2016

A major theme of mathematics is the association of invariants to classes of objects as a means of studying the class of objects. This is perhaps best illustrated with the tremendous success of algebraic topology where one can associate to a given topological spaces many invariants like homotopy and homology groups, notions of dimension, measurements of size like diameter, injectivity radius, and volume.

Today, I will talk a bit about different kinds of invariants that arise naturally in the areas of algebra and geometry/topology. Before talking about some specific examples, I will discuss some possible outcomes of such associations.

Let's say that we have some collection $\mathscr{C}$ of objects like groups, fields, manifolds, or varieties. We might insist that $\mathscr{C}$ be nice category with some desirable properties (e.g. existence of certain types of objects like products, fiber products .etc). In this case, we might want some functor F from our category $\mathscr{C}$ to another category $\mathscr{D}$ where we view $F(X) \in \mathscr{D}$ as an invariant of X given by F. We could have a collection of functors F_i indexed by some indexing set $\mathscr{I}$. In many settings, like homotopy or homology groups, we do get such functors. However, I will not make use of any of these formalisms today and so we will remain firmly rooted in the category of bullshit, my speciality. Nevertheless, we might some particular nice features for our assignment of invariants. Indeed, one major point of finding such invariants is to use them to distinguish between pairs of objects in $\mathscr{C}$. To that end, we have the following possible aims:

(A) Given two objects $X, Y \in \mathscr{C}$, we have $X = Y$ if and only if $F(X) = F(Y)$. That is, F is injective.

(B) Given an object $X \in \mathscr{C}$, the set $F^{-1}(F(X))$ is finite.

It should be added that we want the invariant $F(X)$ to be *simpler* than the object X. In the case of (A), we might ask for even more:

(AAA) Given an object X, we can reconstruct X from the invariant $F(X)$.

(AA) Assuming F is injective, we can also determine $F(\mathscr{C}) \subset \mathscr{D}$.

Deciding if F is injective or not will be called the **inverse problem**. Deciding if F satisfies (AAA) or not will be called the **reconstruction problem**.

Remark 1. In some sense, if $F(X)$ is simpler than X, we should not hope to achieve either (AAA) or (A).

Regardless of our aim, it is wise to first investigate what structure of X the invariant $F(X)$ sees.

1 Examples

I will now discuss some simpleminded realizations of the above.

1.1 Finite Groups

Let $\mathscr{FG}$ be the collection of all isomorphism classes of finite groups. The simplest invariant we can associate to $G \in \mathscr{FG}$ is the cardinality or order of the underlying set G. Note that if we were to forget the group structure of G and only view G as a set, then this invariant is quite good. Indeed, we have (AAA) as if I know the order of the set, I can reconstruct the set. However, for finite groups, this invariant is not as good (see this wiki page for a list of groups of small order):

- Groups of order 1: $\{1\} = C_1 = \mathrm{Sym}(1) = \mathrm{Alt}(2)$.
- Groups of order 2: $C_2 = \mathrm{Sym}(2) = \mathrm{Dih}(1)$.
- Groups of order 3: $C_3 = \mathrm{Alt}(3)$.
- Groups of order 4: $C_2 \times C_2 = K_4 = \mathrm{Dih}(2), C_4$.
- Groups of order 5: C_5.

- Groups of order 6: C_6, $\mathrm{Sym}(3) = \mathrm{Dih}(3)$.
- Groups of order 7: C_7.
- Groups of order 8: $C_2 \times C_2 \times C_2$, $C_4 \times C_2$, C_8, $\mathrm{Dih}(8)$, Q_8.

Nevertheless, this invariant does satisfy (B). Now, one thing we can do is try to find another invariant to pair with the order to form a new, better, more powerful invariant (this makes me think of the 6 million dollar man). We could take for instance the orders of all of the quotient groups of G and we could also record the **multiplicity** or number of times a particular order occurs. We will call this the **spectrum of finite quotients**. For instance, for C_4, we have

$$F(C_4) = \{(1,1),(2,1),(4,1)\}$$

while for $C_2 \times C_2$, we have

$$F(C_2 \times C_2) = \{(1,1),(2,2),(4,1)\}.$$

Here, the first number is the order of the quotient and the second number is the number of times that order occurs. We see that this invariant is better. We could even package this data via a function like

$$z_G(s) = \sum_{H \lhd G} \frac{1}{|G/H|^s}.$$

We could package the data via a counting function

$$C_G(n) = |\{H \lhd G \ : \ |G/H| \leq n\}|.$$

Another very natural invariant for a finite group is the number $r_G(n)$ of irreducible representations of G into $\mathrm{GL}(n,\mathbf{C})$ (or equivalently $\mathrm{U}(n)$) up to conjugation. We can again package this data in various ways as we did before. We have the spectrum $\{(n, r_G(n)\}$. By the class equation for groups, we know that

$$|G| = \sum_{n=1}^{\infty} (r_G(n))^2.$$

This identity is derived from the left multiplication action of G on itself. The conjugate action of G on itself gives the other side of the class equation for G

$$|G| = \sum_{[g] \subset G} [G : C_G(g)]$$

where $[g]$ denotes the conjugacy class associated to $g \in G$ and $C_G(g)$ is the centralizer of g in G (i.e., the subgroup of elements of G that commute with g). In particular,

$$\sum_{n=1}^{\infty} (r_G(n))^2 = \sum_{[g] \subset G} [G : C_G(g)].$$

This identity is analogous to more famous identities that we will come to momentarily; see Jacobi's identity and the Selberg trace formula below.

1.2 Infinite Groups

If G is an infinite group, the invariant $|G|$ is not very good. In particular, this invariant does not satisfy (B). We can take a similar approach as done above and enrich this invariant by taking all of the orders of the finite quotients of G (with or without multiplicity). Note that there exist infinitely many infinite simple groups and for those groups, this invariant is especially bad as it cannot see these objects as different. In fact, if G is a group, we can take

$$K_G = \bigcap_{H \lhd G,\ [G:H] < \infty} H,$$

then G and G/K_G will have the same spectrum of finite quotients. Consequently, we will assume that G has $K_G = 1$ which is the same as saying that G is **residually finite**. The counting function

$$C_G(n) = |\{H < G \ : \ [G : H] < \infty\}|$$

is good at determining center properties of the group G. Specifically, if $C_G(n) \leq n^D$ for some $D \in \mathbf{R}$, then G must be virtually solvable (note that both virtually and solvable have separate links to related wiki pages). The growth type of $C_G(n)$ is referred to as the subgroup growth rate of G; we are assuming that G is finitely generated.

We can form a function as well with the data of the orders of the finite quotients of G. Specifically, let I_G denote the distinct orders (without multiplicity) of the finite quotients of G, and set

$$z_G(s) = \sum_{i \in I_G} i^{-s}.$$

The abscissa of convergence of z_G, namely

$$s_G = \inf\{s \in \mathbf{R} \ : \ z_G(s) < \infty\}$$

is related to the representation theory of G by a remarkable result of Michael Larsen. To that end, we define d_G by

$$d_G = \min\left\{\dim(\overline{\rho(G)}) \ : \ \rho : G \to \mathrm{GL}(n,C),\ n \in \mathbf{N}\right\}$$

where $\dim(\overline{\rho(G)})$ is the dimension of the Zariski closure of $\rho(G)$ in $\mathrm{GL}(n,\mathbf{C})$. Larsen proved that $d_G = s_G^{-1}$. One direction requires that classification of finite simple groups. Of course, the best invariant for recording the data of all of the finite quotients of G is the profinite completion $\widehat{G}$ of G. Similarly, for recording the data of the finite dimensional representation theory of G, one has the associated Tannaka duality groups (see also here and here).

1.3 Fields and Rings

Let K be a finite extension of the rational field $\mathbf{Q}$; such fields are called **number fields**. The ring of K–integers $\mathscr{O}_K$ of K is a finite extension of $\mathbf{Z}$. For each prime $p \in \mathbf{Z}$, the principal ideal generated by p in $\mathscr{O}_K$ has a primary decomposition (this rings are **Dedekind domains**)

$$(p)_{\mathscr{O}_K} = \prod_{i=1}^{r_p} \mathfrak{p}_i^{e_i}.$$

Each quotient ring $\mathscr{O}_K/\mathfrak{p}_i$ is finite and the order is denoted by p^{f_i}. One fundamental observation is that

$$\sum_{i=1}^{r_p} e_i f_i = [K : \mathbf{Q}].$$

We can record the pairs $\left\{\left\{(e_i,f_i)_{i=1}^{r_p}\right\}\right\}_p$ over all the primes $p \in \mathbf{Z}$ and get an invariant of K. This is referred to as the splitting type. We can also record this data in terms of the **Dedekind zeta function**

$$\zeta_K(s) = \sum_{\mathfrak{a} \lhd \mathscr{O}_K} \frac{1}{|\mathscr{O}_K/\mathfrak{a}|^s}$$

where the sum is taken over all non-zero ideals $\mathfrak{a} \lhd \mathscr{O}_K$. The term $|\mathscr{O}_K/\mathfrak{a}|$ is referred to as the **absolute norm** of $\mathfrak{a}$.

The function $\zeta_K(s)$ determines some basic invariants of K like the degree and the discriminant; to a geometer, these are the analogs of the dimension and volume. The following is a consequence of class field theory:

Theorem 1.1. *The assignment $K \mapsto \zeta_K(s)$ is finite-to-one. If K is Galois and $L/\mathbf{Q}$ is a number field with $\zeta_K(s) = \zeta_L(s)$, then $K = L$.*

For any positive integer r, one can construct number fields $K_1, \ldots, K_r$ that are pairwise non-isomorphic and $\zeta_{K_i}(s) = \zeta_{K_j}(s)$ for all $1 \leq i < j \leq r$. Such fields are referred to as **arithmetically equivalent** fields. This construction can be done using elementary number theory and a theorem of Shafarevich. Given two subgroups $H_1, H_2 < G$ of a finite group G, we say that H_1, H_2 are almost conjugate if for each conjugacy class $[g] \subset G$, we have

$$|[g] \cap H_1| = |[g] \cap H_2|.$$

This condition is equivalent to the condition that for each representation $\rho : G \to \mathrm{GL}(n, \mathbf{C})$, we have

$$\dim_{\mathbf{C}}(\mathrm{Fix}_{\rho(H_1)}) = \dim_{\mathbf{C}}(\mathrm{Fix}_{\rho(H_2)})$$

where

$$\mathrm{Fix}_{\rho(H)} = \{v \in \mathbf{C}^n \ : \ \rho(h)v = v \text{ for all } h \in H\}.$$

The triple (H_1, H_2, G) are sometimes called Gassmann triples or Sunada triples. There are many sources for such pairs. One method utilizes automorphisms called almost inner automorphisms. An automorphism $\psi : G \to G$ is called almost inner if for each $g \in G$, the elements $g, \psi(g)$ are conjugate in G. Inner automorphisms (i.e., automorphisms induced by conjugation) are almost inner. Not all groups admit almost inner, non-inner automorphisms; finitely generated free groups do not have such automorphisms and this was used by Grossman to prove $\mathrm{Out}(F_r)$ is residually finite. Given a prime p and an integer $\ell > 1$, the group

$$\mathrm{Heis}(3, \mathbf{F}_{p^\ell}) = \left\{ \begin{pmatrix} 1 & x & t \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \ : \ x, y, t \in \mathbf{F}_{p^\ell} \right\}$$

has at least $p^{\ell^2 - \ell}$ distinct almost inner, non-inner automorphisms. Here, $\mathbf{F}_{p^\ell}$ is the unique finite field of cardinality p^ℓ. The group $\mathrm{Heis}(3, \mathbf{F}_{p^\ell})$ is nilpotent for all choices of p, ℓ and so by Shafarevich can be realized as a Galois group for a Galois extension $K/\mathbf{Q}$. You can apply these automorphisms to the subgroup

$$H_0 = \left\{ \begin{pmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \ : \ x \in \mathbf{F}_{p^\ell} \right\} \cong \underbrace{C_p \times C_p \times \cdots \times C_p}_{\ell \text{ times}}$$

to obtain $p^{\ell^2 - \ell}$ non-conjugate, almost conjugate subgroups of $\mathrm{Heis}(3, \mathbf{F}_{p^\ell})$. Via the Galois correspondence, these subgroups correspond to subfields of K. By construction, these fields are non-isomorphic and arithmetically equivalent. Take $p = 11$ and $\ell = 4$, for instance, and this yields $3,138,428,376,721$ distinct pairs. The common degree of these fields is $214,358,881$.

1.4 Norms of Vectors and Tori

The n–torus T^n can be defined many ways. It is the product of n circles S^1. It is the quotient space $\mathbf{R}^n/\mathbf{Z}^n$. It can be built by identifying opposite faces of the n–cube. The 1–torus is the circle and the 2–torus looks like the boundary/surface of a popular breakfast food that I am a personal fan of. It turns out tori are important for a lot of things; so is the n–sphere which has an identical origin when one takes $n = 1$. Viewed as $\mathbf{R}^n/\mathbf{Z}^n$, we can really think of the n–torus as given by taking *any* n–dimensional parallelogram or parallelepiped. Topologically, it makes no difference but if we are interested in the geometry of these spaces, it matters quite a lot! Each choice gives rise to a flat geometry on the n–torus. It turns out that the choice of such a parallelogram is equivalent to choosing a norm for the vectors in $\mathbf{Z}^n$. Indeed, given an n–dimensional parallelogram P, we can assume that one of the vertices is at the origin in $\mathbf{R}^n$, and then identify the edges emanating from the origin with a basis for $\mathbf{R}^n$ (as a vector space). The norm is completely determined by this basis and is given by the standard Euclidean dot product but written in this basis instead of the standard orthonormal basis.

If $L = \mathbf{Z}[v_1, \ldots, v_n]$ where $v_1, \ldots, v_n$ is the basis associated to the parallelogram, then for each vector $v \in L$, we have an associated norm $||v||$. We can form a spectrum $\mathscr{L}(L) = (\ell, m_\ell)$ where ℓ is a non-negative real number and m_ℓ is the number of vectors in L with norm equal to ℓ. This spectrum is called the (geodesic) length spectrum of the torus $\mathbf{R}^n/L$ associated to L.

This spectrum is also related to another invariant that arises from a more analytic view point. The functions $f\colon \mathbf{R}^n/L \to \mathbf{R}$ on $\mathbf{R}^n/L$ can be identified with the functions $\widetilde{f}\colon \mathbf{R}^n \to \mathbf{R}$ such that $\widetilde{f}(x+v) = \widetilde{f}(x)$ for all $v \in L$. If $n = 1$, then $L = \mathbf{Z}[v]$ for some non-zero vector $v \in \mathbf{R}$. In this case, the functions $\widetilde{f}$ are period with period $|v|$. For $n > 1$, these functions satisfy higher dimensional analogs of periodicity. For instance, if $L = \mathbf{Z}^n$, then

$$\widetilde{f}(x_1, \ldots, x_{j-1}, x_j + 1, x_{j+1}, \ldots, x_n) = \widetilde{f}(x_1, \ldots, x_{j-1}, x_j, x_{j+1}, \ldots, x_n)$$

for all $j = 1, \ldots, n$. Recall that the Laplacian on $\mathbf{R}^n$ is given by

$$\Delta_n = \sum_{j=1}^{n} \frac{\partial^2}{\partial^2 x_j}.$$

A function of $\mathbf{R}^n$ is called an **eigenfunction** for Δ_n if there exists $\lambda \in \mathbf{C}$ such that $\Delta f = \lambda f$. The eigenvalue spectrum for L is defined to be $\mathscr{E}(L) = (\lambda, m_\lambda)$ where $\lambda \in \mathbf{C}$ and m_λ is the dimension of the subspace of λ–eigenfunctions $\widetilde{f}$ that satisfy the periodicity condition imposed by L.

The Poisson Summation Formula yields a remarkable identity between these two spectra; this

identity is sometimes referred to as Jacobi's identity for Dirichlet series:

$$\sum_{\lambda} e^{-\lambda t} = \frac{\mathrm{Vol}(\mathbf{R}^n/L)}{(4\pi t)^{n/2}} \sum_{\ell} e^{-\ell^2/4t}.$$

M. Kneser proved the following theorem:

Theorem 1.2 (Kneser)**.** *The assignment $L \mapsto \mathscr{E}(L)$ or $\mathscr{L}(L)$ both satisfy (B).*

Milnor was the first to show that one cannot improve on this result. He constructed to lattices L_1, L_2 in $\mathbf{R}^{16}$ that are non-isometric but have the same invariants. However, we can use the same methods employed above to construct number fields with the same zeta functions in this setting. This construction is due to Sunada and produces examples of isospectral manifolds.

Remark 2. For $n = 1,2,3$, Kneser's theorem can be upgraded. Specifically, if $n = 1,2,3$ the assignment $L \mapsto \mathscr{E}(L)$ or $\mathscr{L}(L)$ is 1-1.

Question 1.3. *Given a symmetric, positive definite bilinear form $B\colon \mathbf{Z}^3 \times \mathbf{Z}^3 \to \mathbf{Q}$, can you determine B, up to $\mathbf{Q}$–isomorphism, from the set $\left\{ \sqrt{B(v,v)} \ : \ v \in \mathbf{Z}^3 \right\}$?*

1.5 Riemann Surfaces

Riemann surfaces can be constructed, as with tori, in many different ways. First, they can be built in the same way as tori are via polygons. These types of cut-and-paste constructions date back to Dehn and one can view a genus g surface as arising from gluing pairs of edges of a polygon; you can read more about the genus two surface here and more about the genus three surface here. As with tori, this is a topological construction and not a geometric construction. In order to make the construction geometric, we need to take our polygons in the hyperbolic plane $\mathbf{H}^2$ and not the Euclidean plane $\mathbf{R}^2$. In this way, our genus g surfaces arises as a quotient space $\mathbf{H}^2/\Gamma$ where Γ plays the role that L played in the case of the torus. The object Γ is a group and conjugacy classes in Γ replace the roles that vectors in L played in the case of the torus. Each conjugacy class $[\gamma]$ has an associated translation distance ℓ_γ and we can again form a spectrum from this data given by $\mathscr{L}(\Gamma) = \{(\ell, m_\ell)\}$ called the (geodesic) length spectrum. We also have a Laplace operator $\Delta_{\mathbf{H}^2}$. Each function $f\colon \mathbf{H}^2/\Gamma \to \mathbf{R}$ can be lifted to $\widetilde{f}\colon \mathbf{H}^2 \to \mathbf{R}$ such that $\widetilde{f}(\gamma x) = \widetilde{f}(x)$ for all $\gamma \in \Gamma$. We can again consider the eigenfunctions of $\Delta_{\mathbf{H}^2}$ that satisfy the periodicity condition, obtaining a spectrum $\mathscr{E}(\Gamma) = \{(\lambda, m_\lambda)\}$. These two invariants can again be related via Selberg's Trace Formula which has the same "shape" as the class equation for groups and Jacobi's identity.

Selberg introduced a zeta function using the invariant $\mathscr{L}(\Gamma)$ and established the analog of the Riemann hypothesis in this setting. In particular, one can again package the data from these invariants functionally and this can be used with great success.

Remark 3. Though we have not mentioned it yet, these spectra are all quite well behaved. The lengths or eigenvalues form a discrete set of the non-negative real numbers with finite multiplicities. Such spectra are called discrete. Neither is clear though for the eigenvalue spectrum it follows from the fact that Δ is self-adjoint and has a compact resolvent. In particular, discreteness is a consequence of the spectral theorem for compact operators.

Wolpert proved the following:

Theorem 1.4. *The assignment $\Gamma \mapsto \mathscr{E}(\Gamma)$ or $\mathscr{L}(\Gamma)$ is finite-to-one. Moreover, for a generic Γ (in the Baire Category sense on the moduli space of genus g curves), the assignment is one-to-one.*

Using the same method for zeta functions and tori (i.e., Sunada's method), we can again show that the above theorem is the best possible. Brooks showed that the map is at worst e^{72g^2}–to–one and Brooks–Gornet–Gustafson proved that it can be exponentially large as a function of genus. There are no known examples where the genus is either two or three.