Math 310
April 22, 2020 Lecture

Steven G. Krantz

March 30, 2020

More on Compactness

Proposition:

A one-to-one, continuous map from a compact space X onto a Hausdorff space Y is bicontinuous.

Proof: Let f be such a map. Let U be an open subset of X. Then $E = X \setminus U$ is closed. Hence it is compact. It follows from that $f(E)$ is compact in Y. So $f(E)$ is closed. But then $f(U) = Y \setminus f(E)$ is open. So f is an open mapping. But that says that f^{-1} is continuous. $\square$

We next turn to one of the more profound and useful results about compactness. It is necessary to begin with a definition.

Definition

Let X be a topological space. Let $\mathcal{F} = \{F_\alpha\}_{\alpha \in A}$ be a family of sets in X. We say that $\mathcal{F}$ has the *finite intersection property* if, whenever $F_{\alpha_1}, F_{\alpha_2}, \ldots, F_{\alpha_m}$ is a finite collection of elements of $\mathcal{F}$, then $\cap_{j=1}^{m} F_{\alpha_j}$ is nonempty.

Theorem:

A topological space $(X, \mathcal{U})$ is compact if and only if any family $\mathcal{F} = \{F_\alpha\}_{\alpha \in A}$ of closed sets in X with the finite intersection property actually satisfies $\cap_{\alpha \in A} F_\alpha \neq \emptyset$.

Proof: First suppose that X is compact. Let $\mathcal{F} = \{F_\alpha\}_{\alpha \in A}$ be a family of closed sets in X and suppose that $\cap_{\alpha \in A} F_\alpha = \emptyset$. Now look at $\{X \setminus F_\alpha\}$. This must (by De Morgan's law) then be an open cover of X. Since X is compact, there is a finite subcover $X \setminus F_{\alpha_1}$, $X \setminus F_{\alpha_2}$, $\ldots$, $X \setminus F_{\alpha_m}$. But this says (again by De Morgan's law) that $F_{\alpha_1} \cap F_{\alpha_2} \cap \cdots \cap F_{\alpha_m} = \emptyset$. So $\mathcal{F}$ does not have the finite intersection property. That proves one direction of the theorem.

Now suppose that, whenever $\mathcal{F} = \{F_\alpha\}_{\alpha \in A}$ is a family of closed sets with the finite intersection property, then $\cap_{\alpha \in A} F_\alpha \neq \emptyset$. Our job then is to show that X is compact. Let $\mathcal{U} = \{U_\alpha\}_{\alpha \in A}$ be an open cover of X. Now consider the family $\mathcal{F} \equiv \{X \setminus U_\alpha : \alpha \in A\}$. Then $\mathcal{F}$ is a family of closed sets and, by De Morgan's law, $\cap_\alpha X \setminus U_\alpha = \emptyset$. So there must be finitely many $X \setminus U_{\alpha_1}, X \setminus U_{\alpha_2}, \ldots, X \setminus U_{\alpha_m}$ with empty intersection. But, again by De Morgan's law, this says that $U_{\alpha_1}, U_{\alpha_2}, \ldots, U_{\alpha_m}$ is a finite subcover of the family $\mathcal{U}$. Thus X is compact. $\square$

An Axiomatic Theory: Group Theory

We close the course with a study of one particular axiomatic system. That is the theory of groups. This set of ideas dates back to the early nineteenth century, and is due to Evariste Galois and Augustin Cauchy. It has grown to a very prominent position in mathematics. Group theory affects all parts of the subject, from number theory to cryptography to complex analysis to mathematical physics. In the present context we will treat only the most basic ideas. But there is a lot to learn here.

Definition:

Let G be a set, and let $P : G \times G \to G$ be a function. We call the ordered pair (G, P) a *group* if the following axioms are satisfied (following custom, we shall usually write $P(g, h)$ as $g \cdot h$):

1. Associativity If $g, h, k \in G$, then $g \cdot (h \cdot k) = (g \cdot h) \cdot k$;
2. Identity Element There is a distinguished identity element $e \in G$ such that, for all $g \in G$, $e \cdot g = g \cdot e = g$.
3. Multiplicative Inverse For each $g \in G$ there is an element $h \in G$ such that $g \cdot h = h \cdot g = e$.

It is common to denote the inverse element specified in Axiom 3 by g^{-1}, and we shall do so in what follows.

Notice that we do *not* assume that a group is commutative; that is, we do not assume that $g \cdot h = h \cdot g$ for all $g, h \in G$. The property of associativity that we postulate in Axiom 1 is a different property: it says that when we are combining three elements we may group them, two by two, in either of the two obvious ways; the same answer results.

Example:

Let G be the positive real numbers, and let the group operation be multiplication: $P(x, y) = x \cdot y$, where $\cdot$ is ordinary multiplication of reals. Then (G, P) is a group.

Axiom 1: Of course multiplication of real numbers is associative.
Axiom 2: The number 1 is the identity element for multiplication: $1 \cdot x = x \cdot 1 = x$ for any real number x.
Axiom 3: The multiplicative inverse of a group element is its ordinary reciprocal. That is, if $x \in \mathbb{R}$ satisfies $x > 0$, then $1/x$ is its multiplicative inverse.

Example:

Let G be the integers, and let $P(x, y) = x + y$ (ordinary addition). Then (G, P) is a group.

Axiom 1: Certainly addition of integers is associative.
Axiom 2: The number 0 is the additive identity.
Axiom 3: The additive inverse of a group element is its negative: if $m \in \mathbb{Z}$, then $-m$ is its group inverse.

Example:

Let G be the $k \times k$ matrices with real entries and nonzero determinant. This is sometimes called the *general linear group on k letters* and is denoted by $GL(k, \mathbb{R})$.

Let P be ordinary matrix multiplication. Then (G, P) is a group.

Axiom 1: Matrix multiplication is associative.

Axiom 2: The group identity is the matrix

$$I_k \equiv \underbrace{\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ & & \dots & & \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}}_{k} \Bigg\} k$$

Thus, if $m \in G$, then $I_k \cdot m = m \cdot I_k = m$.

Axiom 3: The multiplicative inverse of a group element is its matrix inverse. Thus, if $m \in G$, then the inverse matrix m^{-1} is the group inverse.

Notice in this example that it is important to restrict attention to square matrices, so that multiplication of any two elements in any order will make sense. We also require that each matrix have nonzero determinant, so that each matrix will have an inverse. To see that G is closed under the group operation of matrix multiplication, we must note that if $M, N \in G$, then $\det(M \cdot N) = (\det M)(\det N) \neq 0$.

Unlike the previous two examples, this last one is a noncommutative group. Commutative groups are usually referred to as *abelian*, in honor of N. H. Abel (1802–1829), who first studied them in detail. The book [HAL] gives a solid introduction to classical group theory.

The advantage of the axiomatic method, in the present context, is that when we prove a proposition or theorem about "a group G," it applies simultaneously to all groups. Thus the axiomatic method gives us both a way of being concise and a way of cutting to the heart of the matter.

Proposition:

The multiplicative identity for a group is unique.

Proof: Let G be a group. Let e and e' both be elements of G that satisfy Axiom 2. Then

$$e = e \cdot e' = e'.$$

Thus e and e' must be the same group element. $\square$

Proposition:

Let G be a group and $g \in G$. Then there is only one multiplicative inverse for g.

Proof: Suppose that h and k both satisfy the properties of the multiplicative inverse (Axiom 3) relative to g. Then

$$h = h \cdot e = h \cdot (g \cdot k) = (h \cdot g) \cdot k = e \cdot k = k.$$

Thus h and k must be the same group element, establishing that the multiplicative inverse is unique. $\square$

Proposition:

Let g be an element of the group G. Then

$$\left(g^{-1}\right)^{-1} = g.$$

Proof: Observe that

$$g \cdot g^{-1} = e$$

and

$$g^{-1} \cdot g = e.$$

Thus g satisfies the properties of the inverse element (Axiom 3) relative to g^{-1}. Since the last proposition establishes that the inverse element for g is unique, it follows that g must be the multiplicative inverse for g^{-1}. In other words, $\left(g^{-1}\right)^{-1} = g$. $\square$

Proposition:

Let g, h be elements of a group G. Then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.

Proof: We calculate that

$$\begin{aligned}
\left[h^{-1} \cdot g^{-1}\right] \cdot [g \cdot h] &= h^{-1} \cdot \left[g^{-1} \cdot [g \cdot h]\right] \\
&= h^{-1} \cdot \left[(g^{-1} \cdot g) \cdot h\right] \\
&= h^{-1} \cdot \left[e \cdot h\right] \\
&= h^{-1} \cdot h \\
&= e.
\end{aligned}$$

A similar calculation shows that

$$[g \cdot h] \cdot \left[h^{-1} \cdot g^{-1}\right] = e.$$

The assertion follows. $\square$

Definition:

Let G be a group and $H \subset G$. We call H a *subgroup* of G if the following three properties hold:

(1) **Closure** The group operation P associated with G satisfies $P : H \times H \to H$. In other words, H is closed under the group operation of G (see Section 6.3 for the concept of "closed");

(2) **Identity Element** The group identity e is an element of H;

(3) **Multiplicative Inverse** If $h \in H$, then its group inverse element h^{-1} lies in H.

Notice that the point of the last definition is that H is itself a group, using operations (and the group identity) inherited from the larger group G.