An abstract notion of closure

Mathematics often uses families of sets closed under certain operations. Here is an abstract notion capturing some basic common properties.

Let X be a nonempty set, and let $\mathcal{C} \subseteq 2^X$ be a family of subsets of X - called closed sets - satisfying the following two conditions:

(i) $X \in \mathcal{C}$.

(ii) The intersection of any nonempty family of closed sets is closed.

For $A \subseteq X$, define the **closure** of A - written as $\langle A \rangle$ - as the smallest closed set containing A as a subset, that is, a set C such that

(a) $C \in \mathcal{C}$.

(b) $C \supseteq A$.

(c) If D is any closed set containing A, then $D \supseteq C$.

Such a (unique) set exists and is equal to the intersection of all closed sets containing A.

This kind of closed sets are often called *subspaces*. In fact, 'subspace' is more appropriate than 'closed set' (as opposed to 'sets closed under a certain operation'), for the family of closed sets is typically also closed under the union of two of its sets. When the expression 'subspace' is used, the closure $\langle A \rangle$ is called the subspace generated by A and is denoted by span(A). More precisely: A **subspace** of the space $(X, \mathcal{C})$ is a closed set $W \in \mathcal{C}$ together with the family $\{C \cap W : C \in \mathcal{C}\} = \{D \in \mathcal{C} : D \subseteq W\}$ of all closed subsets of W.

Some simple properties of closure

The following properties hold for all $A, B, C, D \subseteq X$:

(1) $A \subseteq \langle A \rangle$ and $\langle A \rangle \in \mathcal{C}$. (by def.)

(2) C is a subspace iff $\langle C \rangle = C$.
Also: C is a subspace iff there is an $A \subseteq P$ such that $C = \langle A \rangle$.

(3) If $D \in \mathcal{C}$ and $D \supseteq A$, then $D \supseteq \langle A \rangle$. (by def.)

(4) Idempotency of closure: $\langle \langle A \rangle \rangle = \langle A \rangle$.

(5) Monotonicity: $A \subseteq B$ implies $\langle A \rangle \subseteq \langle B \rangle$.

(6) Step-by-step closure: $\langle A \cup B \rangle = \langle \langle A \rangle \cup B \rangle$.

Examples

Standard (topological) **closed sets** in $\mathbb{R}^n$ (say) - including $\emptyset$. Here the closure $\langle A \rangle$ is usually denoted by A^c. [A set is closed in $\mathbb{R}^n$ if it contains all its limit points.] They have the additional defining property that the union of two closed sets is closed.

Closed convex sets in $\mathbb{R}^n$ - including $\emptyset$. [A set is convex if it contains all line segments connecting pairs of points of the set.]

Linear subspaces in $\mathbb{R}^n$. Here $\langle A \rangle$ is usually denoted by $\mathrm{span}(A)$. [These are nonempty sets closed under linear combinations. Equivalently: a (linear) subspace is a set of points which contains the origin as well as all lines through pairs of points of the set.]

Affine subspaces in $\mathbb{R}^n$ - including $\emptyset$. [These are sets closed under affine combinations, that is, linear combinations with coefficients summing to 1. The affine subspaces of $\mathbb{R}^n$ are: the empty set, and all translated linear subspaces. Equivalently: an affine subspace is a set of points which contains all lines through pairs of points of the set — this is the abstract definition used in so-called linear and near-linear spaces.]

Subgroups of a group (or subfields of a field).

Definitions

S is a **spanning set** (or generating set) if $\langle S \rangle = X$.
S is a **minimal spanning set** if S is a spanning set, but no proper subset of S is.

I is an **independent set** if $(\forall x \in I) x \notin \langle I - x \rangle$. Otherwise I is dependent.
I is a **maximal independent set** if I is independent, but no set properly containing I is.

> Remark: The $\emptyset$ is always independent. Also, by (5), subsets of independent sets are independent, and supersets of spanning sets are spanning.

B is a **basis** if it's both spanning and independent.

> Remark: Some books define bases as maximal independent sets (not the same!).

A space S is said to be **finite dimensional** if it contains a finite spanning set (otherwise it's infinite dimensional). By (III) below, every finite dimensional space has a finite basis.

The following lemma easily follows from (3).

Lemma 3. *If T is spanning and $\langle A \rangle \supseteq T$, then already A is spanning.*

Some simple facts

(I) Every basis is a minimal spanning set. [Easy.]

(II) Every minimal spanning set is independent – hence a basis. [Follows from Lemma 3.]

(III) Bases are exactly the minimal spanning sets. [Combining (I) and (II).]

(IV) Every basis is a maximal independent set. [Easy.]

Caution! The converse may be false! Example: $\{1, 4, 7\}$ in Figure 1.4.1 on page 10 of Lynn Batten's book is a maximal independent set, but it is not a spanning set, hence not a basis. But maximal independent sets *are* bases in spaces where the following axiom holds:

The Dependence Axiom. *If I is independent but $I + x$ is dependent, then $x \in \langle I \rangle$.*

(V) The Dependence Axiom implies that maximal independent sets are spanning - hence bases. Thus, under the Dependence Axiom, bases, maximal independent sets, and minimal spanning sets are all the same.

Dimension

The Dependence Axiom implies the following important inequality (the proof is not trivial).

Fundamental Inequality. *Assume that the Dependence Axiom holds. Let I be an independent set and T a spanning set. Then, $|I| \leq |T|$. Hence all bases have the same cardinality.*

In this case, this common cardinality minus one is called the **dimension** *of the space.*

(The reason that in linear algebra's dimension definition we don't subtract one from the size of a basis is that there we insist that all subspaces contain one more point: the zero vector.)

Remarks. The Dependence Axiom holds in vector spaces, as well as in projective spaces. Under the Dependence Axiom, subspaces of finite dimensional spaces are also finite dimensional. Without the Dependence Axiom, bases (as well as maximal independent sets) can have different sizes (e.g., $\{1, 2, 3\}$ and $\{5, 6, 7, 8\}$ in Figure 1.4.1), and it is even possible to construct a finite dimensional space with an infinite dimensional subspace (e.g., a finitely generated group with a subgroup that is not finitely generated.)

Proofs

Proof of (5): If $A \subseteq B$, then $\langle A \rangle \subseteq \langle B \rangle$. Indeed, $\langle B \rangle$ is a subspace containing B, hence it is a subspace containing A. Since $\langle A \rangle$ is the *smallest subspace* containing A, it is contained in *any* other subspace that contains A, e.g., in $\langle B \rangle$. $\square$

Proof of (6): $\langle A \cup B \rangle = \langle \langle A \rangle \cup B \rangle$.
Since $A \cup B \subseteq \langle A \rangle \cup B$, so, by monotonicity: $\langle A \cup B \rangle \subseteq \langle \langle A \rangle \cup B \rangle$.

We still need to show the other direction: $\langle A \cup B \rangle \supseteq \langle \langle A \rangle \cup B \rangle$.
Let $C = \langle \langle A \rangle \cup B \rangle$ and $D = \langle A \cup B \rangle$. Thus, we need to show $C \subseteq D$.

Now, C is the *smallest subspace* containing both $\langle A \rangle$ and B, so if we could show that the subspace D also contains these two sets, then we would have $C \subseteq D$.
Indeed, D clearly contains B, and since D is a subspace and it contains A, by virtue of (3) D also contains $\langle A \rangle$. $\square$

Proof of (I). Let B be a basis. Since B is a spanning set by definition, it remains to show that B is minimal (with respect to spanning), that is, for every $x \in B$, the set $B \setminus \{x\}$ is *not* spanning P. (Why is this equivalent to minimality?)

Assume - indirectly - that *there exists* a point $x_0 \in B$ such that already the smaller set $B' := B \setminus \{x_0\}$ *were* spanning P, that is, $(\forall p \in P) p \in \langle B' \rangle$. Then, in particular, $x_0 \in \langle B' \rangle$, contradicting the independence of B. $\square$

Proof of (II). Let S be a minimal spanning set. We need to show that S is independent.
Let $x \in S$ be arbitrary, and let $S' := S \setminus \{x\}$. We need to show that $x \notin \langle S' \rangle$.

Indeed, if we had $x \in \langle S' \rangle$, then we would have $S \subseteq \langle S' \rangle$, and hence, by Lemma 3, already S' would span P – contradicting the minimality of S. $\square$

Proof of (IV). Let B be a basis. Since B is an independent set by definition, it remains to show that B is maximal (with respect to independence), that is, for every $y \notin B$, the set $B \cup \{y\}$ *cannot be* independent. (Why is this equivalent to maximality?)

Indeed, let $y \notin B$ be arbitrary. Since B is a basis, it is spanning P, that is, $\langle B \rangle = P$, which means $(\forall x \in P) x \in \langle B \rangle$. In particular, $y \in \langle B \rangle$, hence $B \cup \{y\}$ is indeed *de*pendent. $\square$

Finally, we prove that **under the Dependence Axiom,** all maximal independent sets are bases.

Let I be a maximal independent set, and assume that the Dependence Axiom holds. We need to show that I is a basis. Since I is independent, we only need to show that I spans P, that is, $(\forall x \in P) x \in \langle I \rangle$.

Let $x \in P$ be arbitrary. If $x \in I$, then clearly $x \in \langle I \rangle$ (since $I \subseteq \langle I \rangle$).
If $x \notin I$, then, by the maximality of I, the set $I' := I \cup \{x\}$ is dependent. Hence, by the Dependence Axiom, $x \in \langle I \rangle$ as claimed. $\square$

Exchange Properties

The Dependence Axiom follows from the following version of the **Exchange Property**:

$$(\forall A \subseteq X)(\forall x, y \notin \langle A \rangle)\ [x \in \langle A + y \rangle \text{ iff } y \in \langle A + x \rangle],$$

or equivalently,

$$(\forall C \in \mathcal{C})(\forall x, y \notin \mathcal{C})\ [x \in \langle \mathcal{C} + y \rangle \text{ iff } y \in \langle \mathcal{C} + x \rangle].$$

Remark: This Exchange Property holds in vector spaces, as well as in projective spaces (Lemmas 3.9.3-4). Does it hold in all affine spaces? Probably not.

Proof that the Exchange Property implies the Dependence Axiom:
Let I be independent and $I + x$ dependent. Let $y \in I + x$ be such that $y \in \langle I + x - y \rangle$. By the independence of I, we have $y \notin \langle I - y \rangle$. If $x \in \langle I - y \rangle$, we are done (by monotonicity), so assume it is not. Then we can apply the Exchange Property for $A = I - y$.

The Dependence Axiom [through the Fundamental Inequality] implies the following more familiar version:

Matroid Exchange Property (*Hassler Whitney 1936*): *If A and B are independent and $|A| < |B|$, then there is a $y \in B \setminus A$ such that $A + y$ is also independent.*

Question: Does the Matroid Exchange Property imply the other two? While it does imply (in finite dimensional spaces) that all maximal independent sets are of the same size, I don't see how (or if) this fact, without the Dependence Axiom, implies that those are bases.

Literature: Chapter 1 of Lynn Margaret Batten, Combinatorics of finite geometries. Cambridge University Press 1986. QA 167.2 .B38 1986.