Subobjects

A quick summary is given here for a standard "construction" that we use several different times. First of all, by "object" we will mean one of the standard types of algebraic structures that are considered in the course: groups, fields, vector spaces, rings, modules, or algebras. (See the section "Some Useful Definitions" for a quick summary of these.) The use of the word construction will appear to most as perhaps not the correct terminology to use, as the method is not constructive, in spite of the fact that it quickly shows, at least mathematically, that the desired object actually exists. In fact, for many proofs, this idea will be the simplest to use. However, in general it gives no idea whatsoever about actually constructing the elements belonging to the object. We'll address that separately, usually immediately afterwards, in each case. It's easy to see the pattern of what we do however:

1. Show that the intersection of an arbitrary number of subobjects of the given type it also a subobject of that same type.
2. Apply the preceding statement to the collection of all subobjects that satisfy some specific condition.
3. Take the intersection of this special collection and show that in fact it is the sought-after subobject.
4. Actually construct a natural list of elements that clearly always satisfy the condition and show that this collection is a subobject. Verify that this is the explicit description of the desired subobject; this usually follows automatically.

The first 3 items show the existence of the sought-after subobject while the last gives an explicit way of obtaining its elements.

This is all fairly vague at this point, so we proceed to the specific cases. We will omit a number of proofs as they are easy, and in most cases the proof for any one type of object is similar to that for a different type (which is given).

Groups

We start with the simplest object, a group, which has only one operation.

Definition 1. A subset H of a group G is a *subgroup* if H is a group with respect to the same operation $\star$ of G.

Lemma 2. *$H \subseteq G$ is a subgroup if and only if*

1. H is not empty.

2. If $h_1, h_2 \in H$ *, then* $h_1 \star h_2 \in H$ *.*

3. If $h \in H$ *, then* $h^{-1} \in H$ *.*

Proof. Note that if H is a subgroup, then the conditions must clearly hold. On the other hand, if $h \in H$ (by condition 1.), $h^{-1} \in H$ (by 3.), and hence $e = h \star h^{-1} \in H$ (by 2.). The only conditions left to check (e.g., associativity) follow immediately as all elements of H are in G. □

Lemma 3. *Let* G *be a group and let* H_i*,* $i \in I$ *be an arbitrary collection of subgroups. Then*

$$H = \bigcap_{i \in I} H_i$$

is a subgroup of G*.* H *is the largest subgroup of* G *which is contained in all of the* H_i*,* $i \in I$ *.*

Proof. Left as an exercise. □

Definition 4. Let G be a group and let S be a subset of G. The subgroup of G *generated by* S is the intersection of all subgroups of G containing S.

This subgroup is usually denoted by $\langle S \rangle$.

Lemma 5. *Let* G *be a group and let* S *be a subset of* G *.*

1. *The subgroup of* G *generated by* S *exists.*
2. $\langle S \rangle = \{ e \}$ *for* $S = \varnothing$*, the empty set.*
3. $\langle S \rangle$ *is the set of all finite products* $t_1 \cdots t_k$ *where either* t_i *or* t_i^{-1} *is in* S *for* S *non-empty.*

Proof. For the first part, the intersection of all subgroups of G which contain S exists by the previous lemma. For S the empty set, then every subgroup of G contains S and the proof is given in the following remark.
Finally, if S is not empty, consider the set X of all finite sequences of the form $t_1 \cdots t_k$ where either t_i or t_i^{-1} lies in S. Since $S \subseteq X$, X is not empty. Clearly the product of two such sequences is just another such sequence, so lies in X, and finally since $(t_i \cdots t_k)^{-1} = t_k^{-1} \cdots t_1^1$ the inverse of such a sequence is the same sort of sequece and hence in X. That is, we've proven that X is a subgroup of G which contains S. Thus $\langle S \rangle \subseteq X$. On the other hand we must have $S \subseteq \langle S \rangle$ since $S \subseteq X$ and all of the products of elements of S and their inverses must lie in $\langle S \rangle$ since $\langle S \rangle$ is a subgroup. □

Remark 6. If C is an arbitrary collection of subgroups of G, then by Lemma 3 $H = \bigcap_{c \in C} c$ is a subgroup of G. We now compute H for the two extreme possibilities for the collection C:

a. If $C = \varnothing$, the empty collection, then $H = G$.

b. If C is the set of all subgroups of G, then $H = \{ e \}$, the trivial subgroup of G.

The second case is easy to see since the subgrop $\{ e \}$ is contained in every subgroup in C and further, is one of the subgroups in C, as C contains all subgroups.

The first case may appear trickier at first: Note that one can decide what is in an intersection, by equivalently determining what is not in it. An element x is left out of the intersection of a collection precisely when there exists a member c of C which does not contain it. But there are no members of C since C is the empty collection of subgroups, and hence there are no elements omitted from the collection.

Note: The first case, C is empty, never arises when applying Definition 4. Why?

Vector Spaces

Let V be a vector space over the field F.

Definition 7. A subset W of V is a *subspace* if W is a vector space over F with respect to the operations of addition and scalar multiplication for V.

Lemma 8. *$W \subseteq V$ is a subspace if and only if*

1. *W is not empty.*
2. *If $w_1, w_2 \in W$, then $w_1 + w_2 \in W$.*
3. *If $a \in F$ and $w \in W$, then $aw \in W$.*

Proof. An easy exercise. □

There are other versions of this lemma which perhaps look more efficient, but in fact are not, although they appear in many linear algebra texts.

Lemma 9. *Let V be a vector space over a field F and let W_i, $i \in I$ be an arbitrary collection of subspaces. Then*

$$W = \bigcap_{i \in I} W_i$$

is a subspace of V. Then W is the largest subspace of V which is contained in all of the W_i, $i \in I$.

Proof. We check the required conditions to verify that W is a subpace:

1. $0 \in W$ as $0 \in W_i$ for all $i \in I$. Thus W is non-empty.
2. W is closed under addition: If $u, v \in W$, then $u, v \in W_i$ for all $i \in I$, hence $u + v \in W_i$ for all $i \in I$ (because W_i is a subspace). Hence, $u + v \in W$.

3. W in closed under scalar multiplication: If $a \in F$ and $u \in W$, then $u \in W_i$ for all $i \in I$. Hence $au \in W_i$ for all $i \in I$ (because W_i is a subspace). Hence $au \in W$.

That the subspace W is the largest contained in all W_i is clear. [The only part of the argument that ever seems to cause any worries is the case when I is empty. But by logic (or definition if you like), the intersection of an empty collection of subsets of the set V is V itself.] □

Definition 10. Let V be a vector space over the field F and let S be a subset of V. The subspace of V *spanned by* S is the intersection of all subspaces of V containing S. Sometimes one also says "spanned by S over F" in case one wants to make it clear which field is involved.

We denote this subspace $\mathrm{Span}_F(S)$, or more simply $\mathrm{Span}(S)$ when F is fixed in the entire discussion.

If $\{ v_1, \ldots, v_k \}$ is a finite subset of V and $a_1, \ldots, a_k \in F$, then $\sum_{i=1}^{k} a_i v_i \in V$ is called a *linear combination* of the vectors v_i.

Lemma 11. *Let V be a vector space over the field F and let S be a subset of V.*

1. *The subspace of V* spanned by *S exists.*
2. $\mathrm{Span}_F(S) = \{ 0 \}$ *for $S = \varnothing$, the empty set.*
3. $\mathrm{Span}_F(S)$ *is the set of all linear combinations of finite subsets of S if S is non-empty.*

Proof. Exercise. □

Definition 12. Let V be a vector space over the field F and let $W_1, \ldots, W_k$ be subspaces of V. Then $W_1 + \cdots + W_k$ is the set of all vectors of the form $w_1 + \cdots + w_k$ for $w_i \in W_i$. This is called the *sum of the subspaces* W_i.

See the exercises below to relate the previous definition to span, as well as for a more general definition.

Rings

We next consider the case of associative rings. Recall that we always assume our ring R has an identity element, 1. Again, one should read the section "Some Useful Definitions" to see all of the definitions we consider as well as how they are related to each other.

Definition 13. A subset S of a ring R is a *subring* if S is a ring with respect to the operations of addition and multiplication in R and the identity of S is the identity of R.

Lemma 14. *$S \subseteq R$ is a subring if and only if*

1. *S is a subgroup with respect to addition.*
2. *S is closed under multiplication.*
3. *$1 \in S$.*

Proof. Left as an exercise. □

Lemma 15. *Let R be a ring and let S_i, $i \in I$ be an arbitrary collection of subrings. Then*

$$S = \bigcap_{i \in I} S_i$$

is a subring of R. It is the largest subring of R which is contained in all of the S_i, $i \in I$.

Proof. The only real change in the pattern here is to verify that 1 is in the intersection, and that it is the same 1 as in R, but of course it is, as the corresponding statement for each i holds for S_i. The rest is left as an exercise. □

Definition 16. Let R be a ring and let S be a subset of R. The subring of R *generated by* S is the intersection of all subrings of R containing S, and will denoted here by $[S]$.

The idea of the smallest subring generated by a subset is used frequently. However, the notation used here, $[S]$, is not commonly used. Also see the section on R-algebras below.

Lemma 17. *Let R be a ring and let S be a subset of R.*

1. *The subring of R generated by S exists.*
2. *$[S] = \langle T \rangle$ where T is the subset consisting of all finite products of elements from $\{ 1 \} \cup S$, where $\langle T \rangle$ is the additive subgroup generated by T.*

Proof. Exercise. □

Note that in particular $[S] = \langle 1 \rangle$, the additive subgroup generated by 1, in case S is empty. The result may be slightly different from what you expected due to the requirement that rings have an identity element.

Fields

We next consider the case of fields.

Definition 18. A subset K of a field F is a *subfield* if K is a field with respect to the operations of addition and multiplication of F.

For K a field, we denote by K^* the subset $K \setminus \{0\}$, i.e., K with 0 removed.

Lemma 19. *$K \subseteq F$ is a subfield if and only if*

1. *K is a subgroup of F with respect to addition, and*
2. *K^* is a subgroup of F^* with respect to multiplication.*

Proof. The conditions listed are certainly necessary. The identity of any subfield is the same as the identity of the containing field: $1' \cdot 1' = 1' \cdot 1$ and since $1' \neq 0$ and a field is a domain (no product of two elements is 0 unless at least one of the factors is 0) it follows that $1' = 1$. Applying Lemma 14, we see that additionally we only need check that every non-zero element of K has a multiplicative inverse. This is asserted by the last condition. That the distributive law holds for elements of K follows from the fact that it holds in the larger field F. □

Lemma 20. *Let F be a field and let K_i, $i \in I$ be an arbitrary collection of subfields. Then*

$$K = \bigcap_{i \in I} K_i$$

is a subfield of F. It is the largest subfield of F which is contained in all of the K_i, $i \in I$.

Proof. The proof follows exactly the same pattern as earlier ones and is left as an exercise. It can be shortened a bit by applying the result for rings first. □

Definition 21. Let F be a field and let S be a subset of F. The subfield of F *generated by* S is the intersection of all subfields of F containing S.

The subfield generated by S is the smallest subfield containing S. This idea is used frequently. See the section on R-algebras below.

Lemma 22. *Let F be a field and let S be a subset of F.*

1. *The subfield of F generated by S exists.*
2. *Insert correct description of the elements. [Exercise 6.]*

Proof. The last statement differs slightly from the case of rings since inverses must exist in a field. Other than that, the proof is similar to previous cases and left as an exercise. □

Note that in particular that the smallest subfield is $\langle 1 \rangle \cdot \langle 1 \rangle^{-1}$ in case S is empty, where $\langle 1 \rangle^{-1}$ denotes the set of inverses of the non-zero elements in $\langle 1 \rangle$. This smallest subfield of F is called the *prime subfield* (mentioned earlier in the paragraph after Remark 8 in the section on "Fields").

R-Modules

This is getting a bit repetitive by now, perhaps boring, but we hope, very easy. Write your own version of this section, with details!

R-Algebras

A complete section on R-algebras for R a commutative ring (with 1), would include many repetitions as well. That will be left as an exercise. However, instead we'll give here some typical applications which are the main ones used (in fact, they were used earlier!) in this course.

Note that there is a natural R-algebra homomorphism $i: R \longrightarrow A$ given by $i(r) = r \cdot 1$, where 1 denotes the identity of A. Recall that this just means that i preserves all algebraic structure:

$$\begin{aligned} i(r+s) &= i(r) + i(s) \\ i(rs) &= i(r)i(s) \\ i(r \cdot s) &= r \cdot i(s) \end{aligned}$$

This holds for all $r, s \in R$. The $\cdot$ on the left side of the last equation is just ordinary multiplication in R, but the one on the right is from the module structure of A.

For most of our applications, we'll assume that i is a one-to-one function. That is, we can use i to identify R with a subring of A. Now let A be an R-algebra and let S be a subset of A. The R-algebra generated by S will be denoted by $R[S]$ – it is just the smallest subset of A which is a ring (so contains 1), an R-module (so contains R), and contains S. It can be described as $\mathrm{Span}_R(T)$ where T is the set of all finite products of elements of S (note the missing definition of span over rings! What is it?).

Earlier in the course examples of fields of the form $\mathbb{Q}[\sqrt{2}]$ or $\mathbb{Q}[i]$ were given. These are just applications for $R = \mathbb{Q}$, $A = \mathbb{C}$ and $S = \{\sqrt{2}\}$ or $S = \{i\}$. Similarly for $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ as well as $\mathbb{Q}[\sqrt[3]{3}]$.

There is another standard notion that is commonly in use which should be mentioned here. As in the preceding examples, we assume that we have fields $F \subseteq K$, where the F is a subfield of K. Then K is an F-algebra. For $S \subseteq K$ an arbitrary subset, $F[S]$ denotes the F-subalgebra of K generated by S. Since K is a field, there also exists a smallest subfield of K which contains both F and S (it's the smallest subfield containing S which is also an F-algebra). This is denoted by $F(S)$. Now $F[S] \subseteq F(S)$, but the two are not always equal. As an exercise, you'll later prove that they are equal in case $F[S]$ has finite dimension over F.

Remark 23. One important case where i defined above is not one-to-one, is the case of $i: \mathbb{Z} \longrightarrow F$, for F a field. See the discussion on the characteristic of a field F in the section "Fields". The kernel of i ($\ker i = \{k \in \mathbb{Z} \mid i(k) = 0\}$) is used to define $\mathrm{char}\, F$: it is the smallest positive integer in $\ker i$ if $\ker i \neq \{0\}$ and it is 0 when $\ker i = \{0\}$.

Exercises

SubObj 1. Verify Lemma 8.

SubObj 2. Verify that the sum of subpaces which appears in Definition 12 is in fact a subspace of V.

SubObj 3. Verify Lemma 11.

SubObj 4. Let W_i, $i \in I$ be a collection of subspaces of the vector space V over the field F. Define

$$\sum_{i\in I} W_i = \mathrm{Span}_F(\bigcup_{i\in I} W_i) \ .$$

Verify that for I finite this yields the same as Definition 12.

SubObj 5. Let V be a vector space over the field F. Assume W is a subspace of V and S, S_i, $i \in I$ are arbitrary subsets. Verify the following:

1. $\mathrm{Span}_F(W) = W$.
2. $\mathrm{Span}_F(\mathrm{Span}_F(S)) = \mathrm{Span}_F(S)$.
3. $\mathrm{Span}_F(\bigcup_{i\in I} S_i) = \sum_{i\in I} \mathrm{Span}_F(S_i)$.
4. $\mathrm{Span}_F(\bigcap_{i\in I} S_i) \subseteq \bigcap_{i\in I} \mathrm{Span}_F(S_i)$. Equality may not hold; give an explicit example of this.

SubObj 6. Give a careful description of the set of elements in the smallest subfield of a field F which is generated by a set of elements S (analagous to, but a bit different from, that given in Lemma 17).

SubObj 7. Let K be a field and S a subset. Let F be the prime subfield of K. Show that the field of fractions of $F[S]$ is naturally isomorphic to $F(S)$.

SubObj 8. Write a complete version of the section for R-modules following the patterns you've seen above.

SubObj 9. Write a complete version of the section for R-algebras.

The Notes for the course *Math 4330, Honors Linear Algebra* at Cornell University have been developed over the last ten years or so mainly by the following (in chronological order):

Gerhard O. Michler

R. Keith Dennis

Martin Kassabov

W. Frank Moore

and

Yuri Berest.

Most sections have been revised so many times the original author may no longer recognize it. The intent is to provide a modern treatement of linear algebra using consistent terminology and notation. Some sections are written simply to provide a central source of information such as those on "Useful Definitions", "Subobjects", and "Universal Mapping Properties" rather than as a chapter as one might find in a traditional textbook. Additionally there are sections whose intent is to provide proofs of some results which are not given in the lectures, but rather provide them as part of a more thorough development of a tangential topic (e.g., Zorn's Lemma to develop cardinal numbers and the existence of bases and dimension in the general case).

A large number of challenging exercises from many different sources have been included. Although most should be readily solvable by students who have mastered the material, a few even more challenging ones still remain.

Much still remains to be done. Corrections and suggestions for additional exercises, topics and supplements are always welcome.