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 handout "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 that, at least mathematically, 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:

- Show that the intersection of an arbitrary number of subobjects of the given type it also a subobject of that same type.

- Apply the preceding statement to the collection of all subobjects that satisfy some specific condition.

- Take the intersection of this special collection and observe that in fact it is the sought-after subobject.

- 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. [HK, group p. 82] 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 $S = \emptyset$, 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. Exercise. □

Vector Spaces

Let V be a vector space over the field F.

Definition 6. [HK, p. 34] A subset W of V is a *subspace* if W is a vector space over F with respect to the same operations of addition and scalar multiplication.

Lemma 7. *$W \subseteq V$ 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. Exercise. □

A not particularly pleasing version of this Lemma appears in your text and in many other linear algebra books.

Lemma 8. *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. It is the largest subspace of V which is contained in all of the W_i, $i \in I$.

Proof. We check the required conditions for 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 $u, v \in W$, the $u, v \in W_i$ 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 is the largest 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 9. 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.

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

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

Lemma 10. *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 $S = \emptyset$, 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 11. Let V be a vector space over the field F and let $W_1, \ldots, W_k$ be subspaces of V. $W_1 + \cdots + W_k$ 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 general definition.

Rings

We next consider the case of associative rings. Recall that we always assume our ring R has an identity element, 1.

Definition 12. [HK, ring p. 140 ff] A subset S of a ring R is a *subring* if S is a ring with respect to the same operations of addition and multiplication and the identity of S is the identity of R.

Lemma 13. *$S \subseteq R$ is a subring if and only if*

(1) S is a subgroup group with respect to addition.

(2) S is closed under multiplication.

(3) $1 \in S$.

Proof. Left as an exercise. □

Lemma 14. *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 that's the case for all S_i. The rest is left as an exercise. □

Definition 15. 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 is denoted by $[S]$.

The idea of the smallest subring generated by a subset is used frequently. See the section on R-algebras below.

Lemma 16. *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 17. [HK, p. 2] A subset K of a field F is a *subfield* if K is a field with respect to the same operations of addition and multiplication.

Lemma 18. $K \subseteq F$ *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 13, 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 F. □

Lemma 19. *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. □

Definition 20. 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 21. *Let* F *be a field and let* S *be a subset of* F.

1. *The subfield of F generated by S exists.*

2. *See 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 handout on "Fields").

R-Modules

This is getting a bit repetitive by now. Write your own version of this section.

R-Algebras

A complete section on R-algebras for R a commutative ring (with 1), would be quite repetitive as well. That will be left as an exercise. However, here we'll give 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 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!).

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 $S = \{i\}$.

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.

Exercises

SubObj 1. Verify Lemma 7.

SubObj 2. Verify that the sum of subpaces which appears in Definition 11 is in fact a subspace of V.

SubObj 3. Verify Lemma 10.

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

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

Verify that for I finite this yields the same as Definition 11.

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. $\mathrm{Span}_F\big(\bigcup_{i \in I} S_i\big) = \sum_{i \in I} \mathrm{Span}_F(S_i)$.
4. $\mathrm{Span}_F\big(\bigcap_{i \in I} S_i\big) \subseteq \bigcap_{i \in I} \mathrm{Span}_F(S_i)$. 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 16).

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.