3.3 Tensor Products

We will follow Dummit and Foote—they have a good explanation and lots of examples. Here we will just repeat some of the important definitions and results.

Let M_R be a right R module and ${}_RN$ be a left R module. Then $M \otimes N = M \otimes_R N$, the ***tensor product*** of M and N, is an abelian group (that is a $\mathbb{Z}$-module) obtained as follows. First take the free $\mathbb{Z}$-module on the free generating set $M \times N$. In this reguard, we are thinking of (m, n) as a formal symbol; in particular $(m, n) + (m', n') \neq (m + m', n + n')$. Take the subgroup of this free abelian group generated by the elements

$$\begin{aligned}&(m + m', n) - (m, n) - (m', n)\\ &(m, n + n') - (m, n) - (m, n')\\ &(mr, n) - (m, rn)\end{aligned}$$

Then $M \otimes_R N$ is the quotient of this free group modulo this subgroup. Let $m \otimes n$ be the coset of (m, n). This is called a ***simple tensor***. The elements of $M \otimes_R N$ are finite sums of simple tensors and are called tensors. Note tensors satisfy

$$\begin{aligned}(m + m') \otimes n &= m \otimes n + m' \otimes n\\ m \otimes (n + n') &= m \otimes n + m \otimes n'\\ mr \otimes n &= m \otimes rn\end{aligned}$$

If N and M are as above and L is an abelian group. A map $\varphi : M \times N \to L$ is ***middle linear*** with respect to R or R-***balanced*** if it is linear in each of its argments (this is called ***mulitlinear***) and $\varphi(m, rn) = \varphi(mr, n)$. We denote the restriction of the natural map from the free abelian group onto $M \otimes N$ (in the definition of $M \otimes N$) to $M \times N$ by ι. So $\iota(m, n) = m \otimes n$. Note ι is R-balanced. The next theorem shows this is universal for this concept; that is, any balanced map can be factored through this. (Warning: ι is not usually one-to-one.)

Theorem 3.24. *Let M_R and ${}_RN$ be R modules. Let $\iota : M \times N \to M \otimes_R N$ be the map $(m, n) \mapsto m \otimes n$. If $\varphi : M \times N \to L$ is an R-balanced map into an abelian group L, then there is a group homomorphism $\bar{\varphi} : M \otimes_R N \to L$ such that the following diagram commutes:*

$$\begin{tikzcd}M \times N \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & M \otimes_R N \arrow[d, "\bar{\varphi}"] \\ & L\end{tikzcd}$$

It is important to remember that $m \otimes n = m' \otimes n'$ (or even $m \otimes n = m \otimes n'$) does not imply $m = m'$ or $n = n'$. Every element of $M \otimes_R N$ is a sum of elements of the form $m \otimes n$ so these elements generate $M \otimes_R N$, but they are not a basis. This means that not every map from the set of simple tensors into an abelian group L can be extended to a homomorphism. For example, if

$$f : M_R \to M'_R \text{ and } g : {}_RN \to {}_RN' \tag{3.4}$$

are homomorphisms, does the map $m \otimes n \mapsto f(m) \otimes g(n)$ extend to a homomorphism from $M \otimes_R N$ to $M' \otimes_R N'$? The answer in this case is yes, but requires a proof, which we leave for the student. This important homomorphism is denoted $f \otimes g$, so that $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.

If R and S are rings, then M is a (S, R)-***bimodule*** is M is a left S-module and also a right R-module and, in addition

$$(sm)r = s(mr).$$

This is denoted ${}_SM_R$. If M is an (S, R)-bimodule and N is a left R-module, then $M \otimes_R N$ is a left S module in a natural way. Namely, $s(m \otimes n) = sm \otimes n$. We showed in class how Theorem 3.24 can be used to show this works.

Theorem 3.25. *Suppose f and g are homomorphism as in* (3.4)*. Then there is a homomorphism $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ such that $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$. If ${}_SM_R$ and ${}_SM'_R$ are bimodules and f is a bimodule homomorphism, then $f \otimes g$ is an S module homomorphism.*

Proof. Use Theorem 3.24. □

Another use of Theorem 3.24 is to show that tensor products are associative see Theorem 14 of Dummit and Foote. Also tensor products distribute over direct sums. One consequence of this is that if R is a subring of S, then, viewing ${}_SS_R$ as a bimodule,

$$S \otimes_R R^n \cong S^n$$

(This uses that $S \otimes_R R \cong S$ under the map $s \otimes r \mapsto sr$, which is another application of Theorem 3.24.

When R is commutative every left module is a right module, and vice versa. In this case if M_i are R-modules then

$$M_1 \otimes_R \cdots \otimes_R M_k$$

makes sense and is an R-module.

The fact that the tensor product distributes over direct sums implies that if V and U are vector spaces over a field F, of dimensions m and n respecitvely, then $V \otimes_F U$ is a vector space over F of dimension nm. In summary, $F^m \otimes_F F^n \cong F^{mn}$.

3.3.1 Algebraic Integers

A complex number is an ***algebraic number*** if it is a root of a polynomial with coefficients in $\mathbb{Q}$ (or equivalently $\mathbb{Z}$). It is an ***algebraic integer*** if it is root of a monic polynomial over $\mathbb{Z}$.

Theorem 3.26. *α is an algebraic integer if and only if it is eigenvalue of a matrix $A \in \mathrm{M}_n(\mathbb{Z})$.*

Theorem 3.27. *The set of all algebraic integers form a ring.*

Proof. Suppose α and β are algebraic integers. Then there are matrices $A \in \mathrm{M}_n(\mathbb{Z})$ and $B \in \mathrm{M}_m(\mathbb{Z})$ and vectors $v \in \mathbb{C}^n$ and $u \in \mathbb{C}^m$ and such that

$$Av = \alpha v \qquad Bu = \beta u$$

Now $A \otimes B$ is a homomorphism (linear transformation) of $\mathbb{C}^n \otimes \mathbb{C}^m$ to itself. If $e_1, \ldots, e_n$ is the standard basis of $\mathbb{C}^n$ and $e'_1, \ldots, e'_m$ are the standard bases of $\mathbb{C}^n$ and $\mathbb{C}^m$, respectively, then $e_i \otimes e'_j$ is a basis of $\mathbb{C}^n \otimes \mathbb{C}^m$. Under this basis, ordered lexicographically, the matrix corresponding to $A \otimes B$ is the ***Kronecker product*** of A and B, which is also denoted $A \otimes B$. This consists of n^2 blocks, each of size $m \times m$, of the form $a_{ij}B$. This is a straightforward calculation given in Proposition 16 of Section 11.2 of Dummit and Foote. In particular $A \otimes B$ has integer entries and so its eigenvalues are algebraic integers by Theorem 3.26.

Now we calculate

$$(A \otimes B)(v \otimes u) = Av \otimes Bu = \alpha v \otimes \beta v = \alpha\beta(v \otimes u)$$

showing that $v \otimes u$ is an eigenvector of $A \otimes B$ with eigenvalue $\alpha\beta$. Thus algebraic integers are closed under multiplication. To see that they are closed under addition, we calculate

$$(I_n \otimes B + A \otimes I_m)(v \otimes u) = v \otimes \beta u + \alpha v \otimes u = (\alpha + \beta)(v \otimes u)$$

Thus $\alpha + \beta$ is an eigenvalue of the integer matrix $I_n \otimes B + A \otimes I_m$ and so an algebraic integer. □

Exercises 3.28.

1. **a.** Show that if α is a nonzero algebraic number, then $1/\alpha$ is also an algebraic number. Hint: suppose $f(\alpha) = 0$ where $f(x) \in \mathbb{Q}[x]$. Start by dividing the equation $f(\alpha) = 0$ by α^k, where k is the degree of f.

   b. Show the if α is an algebra number then $\alpha = \beta/n$ is also an algebraic number for all $n \neq 0$ in $\mathbb{Z}$.

   c. Show the α is an algebra number iff $\alpha = \beta/n$ for some algebraic integer and $n \in \mathbb{Z}$.

   d. Show that the algebraic numbers form a field.

3.4 Projective, Injective and Flat Modules; Exact Sequences

This topic is covered well by Dummit and Foote. You should read their Section 10.5. Hungerford also does a good job. Here we just present some highlights and exercises.

A sequence of homomorphisms

$$\cdots \to X_{n-1} \xrightarrow{\alpha} X_n \xrightarrow{\beta} X_{n+1} \to \cdots$$

is said to be ***exact*** if the image of α equals the kernel of β at each X_n which has something to its left and its right. An exact sequence of the form

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0 \tag{3.5}$$

is called a ***short exact sequence***. Note this is equivalent to saying α is injective and β is surjective and that $\alpha(A) = \ker \beta$. We use $A \rightarrowtail B$ to indicate a monomorphism and $B \twoheadrightarrow C$ to indicate an epimorphism.

Let $\mathcal{V}$ be a variety of algebras in the general sense. An algebra $\mathbf{P}$ is said to be ***projective*** if for each $\mathbf{A}$ and $\mathbf{B} \in \mathcal{V}$, epimorphism $f : \mathbf{A} \twoheadrightarrow \mathbf{B}$ and homomorphism $h : \mathbf{P} \to \mathbf{B}$, there is a homomorphism $g : \mathbf{P} \to \mathbf{A}$ with $h = fg$. Pictorially

$$\begin{tikzcd}
& \mathbf{P} \arrow[ld, dashed, "g"'] \arrow[d, "h"] \\
\mathbf{A} \arrow[r, two heads, "f"] & \mathbf{B}
\end{tikzcd}$$

A homomorphism ρ from an algebra $\mathbf{A}$ to itself is called a ***retraction*** on $\mathbf{A}$ if $\rho^2 = \rho$. We say that $\mathbf{B}$ is a ***retract*** of $\mathbf{A}$ if $B = \rho(A)$ for some retraction ρ on $\mathbf{A}$.

Exercises 3.29.

1. If ρ is a retraction of $\mathbf{A}$ onto $\mathbf{B}$, then $\rho|_B$ (ρ restricted to B) is the identity on $\mathbf{B}$.

2. Prove the following are equivalent for an algebra $\mathbf{P}$ in a variety $\mathcal{V}$:

(a) $\mathbf{P}$ is projective.

(b) If $f : \mathbf{A} \twoheadrightarrow \mathbf{P}$ is a epimorphism then there is a homomorphism $g : \mathbf{P} \to \mathbf{A}$ so that $fg(x) = x$. Note this forces g to be a monomorphism.

(c) $\mathbf{P}$ is isomorphic to a retract of a free algebra in $\mathcal{V}$.

3. Let R be a ring and assume now that $\mathcal{V}$ is the variety of all R-modules.

a. Show that if A and B are R-modules and if $\rho : A \to B$ is a retraction, then A has a submodule C such that $A = B \oplus C$ and $\rho(b, c) = b$.

b. Use this to show that an R-module is projective iff it is a direct summand of a free R-module.

4. Let R be a PID. Use Theorem 3.5 to show that an R module is projective iff it is free. (We only proved Theorem 3.5 in the finitely generated case, but you can use it anyway.)

5. Let F be the two-element field and let $R = F \times F$ be the direct product. Let $P = \{(x, 0) : x \in F\}$. Show that P is projective but not free.

Note $\mathrm{Hom}_R(A, B)$ is an abelian group is an obvious way. Let D be another R-module. If $\alpha : A \to B$ is a homomorphism, let $\alpha' : \mathrm{Hom}_R(D, A) \to \mathrm{Hom}_R(D, B)$ be given by $f \mapsto f' = \alpha \circ f$, for $f \in \mathrm{Hom}_R(D, A)$. This is a homomorphism of abelian groups. Now suppose that (3.5) is a short exact sequence. Then the following sequence is exact:

$$0 \to \mathrm{Hom}_R(D, A) \xrightarrow{\alpha'} \mathrm{Hom}_R(D, B) \xrightarrow{\beta'} \mathrm{Hom}_R(D, C)$$

Note the last $\to 0$ part is missing since β' need not be onto. But if D is projective it is easy to see that it is. The converse is also true so this is another characterization of projective modules.

What does "tensoring with D" do to short exact sequences, where now D is a right R-module. Again assume that (3.5) is a short exact sequence. Then

$$D \otimes_R A \xrightarrow{1\otimes\alpha} D \otimes_R B \xrightarrow{1\otimes\beta} D \otimes_R C \to 0$$

is exact. But this time we have a problem at the left end: $1 \otimes \alpha$ is not necessarily injective. If it is injective for all injective maps $\alpha : A \to B$ for all A and B, then D is said to be a ***flat module***.

Warning: the element notation $a \otimes b$ can be misleading since it does not indicate the ring R. For example, $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$, but $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$, as we showed. So $1 \otimes 1 = 0$ in $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$ but $1 \otimes 1 \neq 0$ in $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}$.

Exercises 3.30.

1. In this problem you will show $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$ as $\mathbb{Z}$-modules.

a. Show that $\varphi : \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathbb{Q}$ given by $\varphi(r \otimes s) = rs$ for r and $s \in \mathbb{Q}$ is a homomorphism. To do this you need to find the appropriate middle linear map.

b. Show that if r and $s \in \mathbb{Q}$ then $r \otimes s = 1 \otimes rs$. This is a little harder that it looks: if we were working over $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ then we could just bring the r to the other side. But in $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ we can only move integers over. Nevertheless a trick similar to the one I used in class showing $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ works.

c. Show that $r \mapsto 1 \otimes r$ is a homomorphism and is the inverse of φ.

(By the way, this same argument shows that if K is the field of fractions of an integral domain R, the $K \otimes_R K \cong K$. On the other hand $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \ncong \mathbb{C}$. You do not need to prove either of these.)

2. Suppose R is commutative and I and J are ideals of R. Show that

$$R/I \otimes_R R/J \cong R/(I \vee J).$$

($I \vee J$ is the ideal generated by I and J. It is often written $I + J$.) For the map $R/I \otimes_R R/J \to R/(I \vee J)$ you need to use the usual trick of making a middle linear map $R/I \times_R R/J \to R/(I \vee J)$. For the other direction map $R \to R/I \otimes_R R/J$ by $r \mapsto r(\bar{1} \otimes \bar{\bar{1}})$, where $\bar{1} = 1 + I \in R/I$ and $\bar{\bar{1}} = 1 + J \in R/J$, and show that $I \vee J$ is contained in the kernel.

3. Using the previous problem (and the fundamental theorem of abelian groups and that tensor products distribute over direct sum; Theorem 14 of Dummit and Foote) describe $A \otimes_{\mathbb{Z}} B$, where A and B are finite abelian groups. This may be a little vague so, if you prefer, you can find $A \otimes_{\mathbb{Z}} B$, where $A = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ and $B = \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/27\mathbb{Z}$.

4. Let B_1 and B_2 be submodules of the left R-module A. Let D be a flat right R-module. Show

$$D \otimes_R (B_1 \vee B_2) = (D \otimes_R B_1) \vee (D \otimes_R B_2)$$
$$D \otimes_R (B_1 \cap B_2) = (D \otimes_R B_1) \cap (D \otimes_R B_2)$$

proving the map $B \mapsto D \otimes_R B$ is a lattice homomorphism of $\mathbf{Sub}(A) \to \mathbf{Sub}(D \otimes_R A)$. Hint: the hardest part is proving the inclusion $(D \otimes_R B_1) \cap (D \otimes_R B_2) \subseteq D \otimes_R (B_1 \cap B_2)$. To see this first note $B_1/(B_1 \cap B_2) \cong (B_1 \vee B_2)/B_2$. Hence we have the short exact sequence

$$0 \to B_1 \cap B_2 \to B_1 \xrightarrow{\varphi} (B_1 \vee B_2)/B_2 \to 0$$

and hence

$$0 \to D \otimes_R (B_1 \cap B_2) \to D \otimes_R B_1 \xrightarrow{1 \otimes \varphi} D \otimes (B_1 \vee B_2)/B_2 \to 0$$

is exact so $\ker 1 \otimes \varphi = D \otimes_R (B_1 \cap B_2)$. Use this to show $(D \otimes_R B_1) \cap (D \otimes_R B_2) \subseteq D \otimes_R (B_1 \cap B_2)$.

Theorem 3.31. *Let ${}_RA$ be a left R-module and let D_R be a flat right R-module. Then the map* $\mathbf{Sub}({}_RA) \to \mathbf{Sub}(D \otimes_R A)$ *given by $B \mapsto D \otimes_R B$ is a lattice homomorphism.*

Proof. First note that if $B_1 \leq B_2$ are submodules of A, then

$$0 \to B_1 \to B_2 \to B_2/B_1 \to 0$$

is a short exact sequence. Since D is flat this implies that $D \otimes B_1$ is embedded into $D \otimes B_2$. It follows that for arbitrary B_1, $B_2 \leq A$

$$(D \otimes_R B_1) \vee (D \otimes_R B_2) \leq D \otimes_R (B_1 \vee B_2).$$

If $b \in B_1 \vee B_2$ the $b = b_1 + b_2$ for some $b_i \in B_i$. But then, if $d \in D$, $d \otimes b = d \otimes b_1 + d \otimes b_2$, proving the other inclusion.

As above

$$D \otimes_R (B_1 \cap B_2) \leq (D \otimes_R B_1) \cap (D \otimes_R B_2).$$

To see that $(D \otimes_R B_1) \cap (D \otimes_R B_2) \subseteq D \otimes_R (B_1 \cap B_2)$ note $B_1/(B_1 \cap B_2) \cong (B_1 \vee B_2)/B_2$, by the Second Isomorphism Theorem. Hence we have the short exact sequence

$$0 \to B_1 \cap B_2 \to B_1 \xrightarrow{\varphi} (B_1 \vee B_2)/B_2 \to 0$$

and hence

$$0 \to D \otimes_R (B_1 \cap B_2) \to D \otimes_R B_1 \xrightarrow{1 \otimes \varphi} D \otimes (B_1 \vee B_2)/B_2 \to 0$$

is exact so $\ker 1 \otimes \varphi = D \otimes_R (B_1 \cap B_2)$.

Let ψ be the natural map from $B_1 \vee B_2$ onto $(B_1 \vee B_2)/B_2$ and note φ is the restriction of ψ to B_1. Now let $\sum d_i \otimes c_i$ with $c_i \in B_2$ be an element of $D \otimes_R B_2$. If this element is also in $D \otimes_R B_1$ then, since $\psi(c_i) = 0$, we can calculate

$$(1 \otimes \varphi)(\sum d_i \otimes c_i) = (1 \otimes \psi)(\sum d_i \otimes c_i) = \sum d_i \otimes \psi(c_i) = 0.$$

This shows $(D \otimes_R B_1) \cap (D \otimes_R B_2) \subseteq \ker 1 \otimes \varphi = D \otimes_R (B_1 \cap B_2)$, completing the proof. □

Part III
Fields

4 Basics

Since we view 1 as a fundamental (nullary) operation of a ring, every ring has a unique smallest subring, the subring generated by 1. This subring is called the ***prime subring***. Note the prime subring is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, for some $n > 0$, or to $\mathbb{Z}$. In the former case we say the ring R has ***characteristic*** n; in the latter case R is said to have characteristic 0. We denote this as $\operatorname{char}(R)$. Also, since $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain unless n is a prime, the characteristic of a field is either a prime or 0.

If F is a subfield of a field K, then K is a vector space over F. The dimension is denoted $[K : F] = \dim_F(K)$.

If $f(x) \in F[x]$, f may not have any roots in F; for example, $x^2 - 2 \in \mathbb{Q}[x]$. But $x^2 - 2$ does have a root in $\mathbb{R}$. This will be one of the primary foci of our study of fields.

APPENDIX

A Prerequisites

This section briefly lists some prerequisites from set theory needed in order to read the main text. It consists primarily of paraphrased excerpts from the excellent introductory textbook by Enderton, "Elements of Set Theory" [2].

A.1 Relations

Probably the reader already has an idea of what is meant by an "ordered pair," $\langle x, y\rangle$. It consists of two elements (or sets) x and y, given in a particular order. How to make this notion mathematically precise is not quite so obvious. According to [2], in 1921 Kazimierz Kuratowski gave us the definition in general use today: given two sets x and y, the ***ordered pair*** $\langle x, y\rangle$ is defined to be the set $\{\{x\}, \{x, y\}\}$. It is not too hard to prove that this definition captures our intuitive idea of ordered pair – namely, $\langle x, y\rangle$ uniquely determines both what x and y are, and the order in which they appear. Indeed, it is a theorem (Theorem 3A of [2]) that $\langle u, v\rangle = \langle x, y\rangle$ iff $u = x$ and $v = y$.

A ***relation*** is a set of ordered pairs. Thus, if X is a set, a relation R on X is simply a subset of the Cartesian product; that is,

$$R \subseteq X \times X := \{\langle x_1, x_2\rangle : x_1, x_2 \in X\}.$$

For a relation R, we sometimes write $x\, R\, y$ in place of $\langle x, y\rangle \in R$. For example, in the case of the ordering relation $<$ on the set $\mathbb{R}$ of real numbers, $<$ is defined to be the set $\{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} : x \text{ is less than } y\}$, and the notation "$x < y$" is preferred to "$\langle x, y\rangle \in <$." See Enderton [2] for more details.

For a relation R, we define the ***domain*** of R ($\operatorname{dom} R$), the ***range*** of R ($\operatorname{ran} R$), and the ***field*** of R ($\operatorname{fld} R$) by

$$\begin{aligned} x \in \operatorname{dom} R \;&\Leftrightarrow\; \exists y\ \langle x, y\rangle \in R,\\ x \in \operatorname{ran} R \;&\Leftrightarrow\; \exists t\ \langle t, x\rangle \in R,\\ \operatorname{fld} R &= \operatorname{dom} R \cup \operatorname{ran} R. \end{aligned}$$

A relation R on a set A is called ***reflexive*** iff $x\, R\, x$ for all $x \in A$; ***symmetric*** iff whenever $x\, R\, y$ then also $y\, R\, x$; ***transitive*** iff whenever $x\, R\, y$ and $y\, R\, z$, then also $x\, R\, z$. A relation is an ***equivalence relation*** iff it is a binary relation that is reflexive, symmetric, and transitive. Given a set A, we denote the set of all equivalence relations on A by $\operatorname{Eq}(A)$.

A.2 Functions

A ***function*** (or mapping) is a relation F such that for each x in $\operatorname{dom} F$ there is only one y such that $x\, F\, y$.

The following operations are most commonly applied to functions, are sometimes applied to relations, but can actually be defined for arbitrary sets A, F, and G.

(a) The ***inverse*** of F is the set
$$F^{-1} = \{\langle u, v\rangle \mid v\,F\,u\} = \{\langle u, v\rangle \mid \langle v, u\rangle \in F\}.$$

(b) The ***composition*** of F and G is the set
$$F \circ G = \{\langle u, v\rangle \mid \exists t\,(u\,G\,t \;\&\; t\,F\,v)\} = \{\langle u, v\rangle \mid \exists t\;(\langle u, t\rangle \in G \;\&\; \langle t, v\rangle \in F)\}.$$

(c) The ***restriction*** of F to A is the set
$$F \restriction A = \{\langle u, v\rangle \mid u\,F\,v \;\&\; u \in A\} = \{\langle u, v\rangle \mid \langle u, v\rangle \in F \;\&\; u \in A\}.$$

(d) The ***image*** of A under F is the set
$$F[\![A]\!] = \operatorname{ran}(F \restriction A) = \{v \mid (\exists u \in A)\ \langle u, v\rangle \in F\}.$$

$F[\![A]\!]$ can be characterized more simply when F is a function and $A \subseteq \operatorname{dom} F$; in this case
$$F[\![A]\!] = \{F(u) \mid u \in A\}.$$

In each case we can easily apply a subset axiom to establish the existence of the desired set. Specifically,
$$F^{-1} \subseteq \operatorname{ran} F \times \operatorname{dom} F, \quad F \circ G \subseteq \operatorname{dom} G \times \operatorname{ran} F, \quad F \restriction A \subseteq F, \quad F[\![A]\!] \subseteq \operatorname{ran} F.$$

(A more detailed justification of the definition of F^{-1} would go as follows: By a subset axiom there is a set B such that for any x,
$$x \in B \quad\Leftrightarrow\quad x \in \operatorname{ran} F \times \operatorname{dom} F \;\&\; \exists u\,\exists v\;(x = \langle u, v\rangle \;\&\; \langle v, u\rangle \in F).$$
It then follows that
$$x \in B \quad\Leftrightarrow\quad \exists u\,\exists v\;(x = \langle u, v\rangle \;\&\; \langle v, u\rangle \in F).$$
This unique set B we denote by F^{-1}.)

Example A.1. Let
$$F = \{\langle \emptyset, a\rangle, \langle \{\emptyset\}, b\rangle\}.$$
Observe that F is a function. We have $F^{-1} = \{\langle a, \emptyset\rangle, \langle b, \{\emptyset\}\rangle\}$. Thus, F^{-1} is a function iff $a \neq b$. The restriction of F to $\emptyset$ is $\emptyset$, but $F \restriction \{\emptyset\} = \{\langle 0, a\rangle\}$. Consequently, $F[\![\{\emptyset\}]\!] = \{a\}$, in contrast to the fact that $F(\{\emptyset\}) = b$.

Theorem A.2. *Assume that $F : A \to B$, and that A is nonempty.*

(a) There exists a function $G : B \to A$ (a "left inverse") such that $G \circ F$ is the identity function id_A on A iff F is one-to-one.

(b) There exists a function $H : B \to A$ (a "right inverse") such that $F \circ H$ is the identity function id_B on B iff F maps A onto *B.*

Axiom of Choice 1. For any relation R there is a function $H \subseteq R$ with $\operatorname{dom} H = \operatorname{dom} R$.

With this axiom we can prove the sufficiency direction of part (b) of the Theorem above: take H to be a function with $H \subseteq F^{-1}$ and $\operatorname{dom} H = \operatorname{dom} F^{-1} = B$. Then H does what we want: Given any $y \in B$, we have $\langle y, H(y)\rangle \in F^{-1}$ hence $\langle H(y), y\rangle \in F$, and so $F(H(y)) = y$. □

References

[1] David S. Dummit and Richard M. Foote. *Abstract algebra.* John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[2] Herbert Enderton. *Elements of set theory.* Academic Press, 1977.

[3] Thomas W. Hungerford. *Algebra.* S-V, New York, 1974.

[4] Nathan Jacobson. *Basic Algebra I.* W. H. Freeman and Co., New York, 1985.