Algebra Notes

April 7, 2011

Contents

Primary Textbook: Jacobson, *Basic Algebra* [4].

Supplementary Textbooks: Hungerford, *Algebra* [3]; Dummitt and Foote. *Abstract Algebra* [1];

Primary Subject: Classical algebra systems: groups, rings, fields, modules (including vector spaces). Also a little universal algebra and lattice theory.

List of Notation

- A^A, the set of maps from a set A into itself.
- $\mathrm{Aut}(\mathbf{A})$, the group of automorphisms of an algebra $\mathbf{A}$.
- $\mathrm{End}(\mathbf{A})$, the set of endomorphisms an algebra $\mathbf{A}$.
- $\mathrm{Hom}(\mathbf{A}, \mathbf{B})$, the set of homomorphism from an algebra $\mathbf{A}$ into an algebra $\mathbf{B}$.
- $\mathrm{Con}(\mathbf{A})$, the set of congruence relations of an algebra $\mathbf{A}$.
- $\mathbf{ConA}$, the lattice of congruence relations of an algebra $\mathbf{A}$.
- $\mathrm{Eq}(A)$, the set of equivalence relations of a set A.
- $\mathbf{EqA}$, the lattice of equivalence relations of a set A.
- $\mathrm{Sub}(\mathbf{A})$, the set of subalgebras of an algebra $\mathbf{A}$.
- $\mathbf{SubA}$, the lattice of subalgebras of an algebra $\mathbf{A}$.
- $\mathrm{Sg}_{\mathbf{A}}(X)$, the subuniverse generated by a set $X \subseteq A$.
- $\mathbb{N} = \{1, 2, \dots\}$, the set of natural numbers.
- $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$, the ring of integers.
- $\mathbb{R} = (-\infty, \infty)$, the real number field.
- $\mathbb{C}$, the complex number field.
- $\mathbb{Q}$, the rational number field.

Part I
Fall 2010: Universal Algebra & Group Theory

1 Universal Algebra

1.1 Basic concepts

A (universal) ***algebra*** is a pair

$$\mathbf{A} = \langle A; F \rangle \tag{1.1}$$

where A is a nonempty set and $F = \{f_i : i \in I\}$ is a set of finitary operations on A; that is, $f_i : A^n \to A$ for some $n \in \mathbb{N}$. A common shorthand notation for (1.1) is $\langle A; f_i \rangle_{i \in I}$. The number n is called the ***arity*** of the operation f_i.

Thus, the arity of an operation is the number of operands upon which it acts, and we say that $f \in F$ is an n-***ary*** operation on A if f maps A^n into A. An operation is called *nullary* (or constant) if its arity is zero. *Unary*, *binary*, and *ternary* operations have arities 1, 2, and 3, respectively.

Example 1.1. If $A = \mathbb{R}$ and $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is the map $f(a, b) = a + b$, then $\langle A; f \rangle$ is an algebra with a single binary operation. Many more examples will be given below.

An algebra $\mathbf{A}$ is called ***unary*** if all of its operations are unary. An algebra $\mathbf{A}$ is ***finite*** if $|A|$ is finite and ***trivial*** if $|A| = 1$. Given two algebras $\mathbf{A}$ and $\mathbf{B}$, we say that $\mathbf{B}$ is a ***reduct*** of $\mathbf{A}$ if both algebras have the same universe and $\mathbf{A}$ (resp. $\mathbf{B}$) can be obtained from $\mathbf{B}$ (resp. $\mathbf{A}$) by adding (resp. removing) operations.

A better approach: An ***operation symbol*** f is an object that has an associated arity, which we'll denote $\text{arity}(f)$. A set of operation symbols F is called a ***similarity type***. An algebra of similarity type F is a pair $\mathbf{A} = \langle A; F^{\mathbf{A}} \rangle$, where $F^{\mathbf{A}} = \{f^{\mathbf{A}} : f \in F\}$ and $f^{\mathbf{A}}$ is an operation on A of arity $\text{arity}(f)$.

Example 1.2. Consider the set of integers $\mathbb{Z}$ with operations $F = \{+, \cdot, -, 0, 1\}$, which have respective arities $\{2, 2, 1, 0, 0\}$. The operation $+$ is the usual binary addition, while $-$ is negation: $a \mapsto -a$. The constants 0 and 1 are nullary operations.

1.2 Subalgebras and Homomorphisms

Suppose $\mathbf{A} = \langle A; F^{\mathbf{A}} \rangle$ is an algebra. We call the nonempty set A the ***universe*** of $\mathbf{A}$. If a nonempty subset $B \subseteq A$ is *closed* under all operations in $F^{\mathbf{A}}$, we call B a ***subuniverse*** of A. By closed under all operations we mean the following: for each $f \in F^{\mathbf{A}}$ (say f is n-ary), we have $f(b_0, \ldots, b_{n-1}) \in B$, for all $b_0, \ldots, b_{n-1} \in B$.

If B is a subuniverse of $\langle A; F^{\mathbf{A}} \rangle$, and if we let[1] $F^{\mathbf{B}} = \{f \restriction B : f \in F^{\mathbf{A}}\}$, then the algebra $\mathbf{B} = \langle B; F^{\mathbf{B}} \rangle$ is called a ***subalgebra*** of $\mathbf{A}$. If $\mathbf{B}$ is a subalgebra of $\mathbf{A}$, we denote this fact by $\mathbf{B} \leqslant \mathbf{A}$. Similarly, we write $B \leqslant A$ if B is a subuniverse of A. We denote the set of all subalgebras of $\mathbf{A}$ by $\text{Sub}(\mathbf{A})$.

Theorem 1.3. *If $\mathbf{A}_i \leqslant \mathbf{A}$, $i \in I$, then $\bigcap A_i$ is a subuniverse if it is not empty.*

If S is a nonempty subset of A, the ***subuniverse generated by*** S, denoted $\text{Sg}_{\mathbf{A}}(S)$ or $\langle S \rangle$ is the smallest subuniverse of $\mathbf{A}$ containing the set S. When $\langle S \rangle = A$, we say that S generates A.

[1] Here $f \restriction B$ denotes restriction of the function f to the set B (see Appendix Sec. A.2).

Theorem 1.4. *If $S \subseteq A$, then* $\mathrm{Sg}_{\mathbf{A}}(S) = \langle S \rangle = \bigcap\{B \leqslant A : S \subseteq B\}$.

Define $\{S_i\}$ recursively as follows:

$$S_0 = S;$$
$$S_{i+1} = \{f(a_1, \ldots, a_k) : f \text{ is a } k\text{-ary basic operation of } A \text{ and } a_i \in S_i\}.$$

Let $\mathbf{A} = \langle A; F^{\mathbf{A}} \rangle$ and $\mathbf{B} = \langle B; F^{\mathbf{B}} \rangle$ be algebras of the same type F, and let F_n denote the set of n-ary operation symbols in F. Consider a mapping $\varphi : A \to B$ and operation symbol $f \in F_n$, and suppose that for all $a_0, \ldots a_{n-1} \in A$ the following equation holds:

$$\varphi(f^{\mathbf{A}}(a_0, \ldots, a_{n-1})) = f^{\mathbf{B}}(\varphi(a_0), \ldots, \varphi(a_{n-1})).$$

Then φ is said to *respect the interpretation of* f. If φ respects the interpretation of every $f \in F$, then we call φ a ***homomorphism*** from $\mathbf{A}$ into $\mathbf{B}$, and we write $\varphi \in \mathrm{Hom}(\mathbf{A}, \mathbf{B})$, or simply, $\varphi : \mathbf{A} \to \mathbf{B}$.

1.3 Direct Products

The ***direct product*** of two sets A_0 and A_1, denoted $A_0 \times A_1$, is the set of all ordered pairs[2] $\langle a_0, a_1 \rangle$ such that $a_0 \in A_0$ and $a_1 \in A_1$. That is, we define

$$A_0 \times A_1 := \{\langle a_0, a_1 \rangle : a_0 \in A_0, a_1 \in A_1\}.$$

More generally, $A_0 \times \cdots \times A_{n-1}$ is the set of all sequences of length n with i^{th} element in A_i. That is,

$$A_0 \times \cdots \times A_{n-1} := \{\langle a_0, \ldots, a_{n-1} \rangle : a_0 \in A_0, \ldots, a_{n-1} \in A_{n-1}\}.$$

Equivalently, $A_0 \times \cdots \times A_{n-1}$ it is the set of all functions with domain $\{0, 1, \ldots, n-1\}$ and range $\bigcup_{i=1}^{n-1} A_i$. More generally still, let $\{A_i : i \in I\}$ be an indexed family of sets. Then the ***direct product*** of the A_i is

$$\prod_{i \in I} A_i := \{f \mid f : I \to \bigcup_{i \in I} A_i \text{ with } f(i) \in A_i\}.$$

When $A_0 = A_1 = \cdots = A$, we often use the shorthand notation $A^2 := A \times A$ and $A^n := A \times \cdots \times A$ (n terms).

Question: How do you know $\prod_{i \in I} A_i \neq \emptyset$, even supposing $I \neq \emptyset$ and $A_i \neq \emptyset$ for all $i \in I$.[3]

[2] For the definition of *ordered pair*, consult the appendix.

[3] *Answer:* Each f "chooses" an element from each A_i, but when the A_i are all different and I is infinite, we may not be able to do this. The Axiom of Choice (AC) says you can.

Gödel proved that the AC is consistent with the other axioms of set theory. Cohen proved that the negation of the AC is also consistent.

1.4 Relations

A ***k*-ary relation** R on a set A is a subset of the cartesian product A^k.

Example 1.5.

(a) $A = \mathbb{R}$ (the line) and $R = \{a \in \mathbb{R}^2 : a \text{ is rational}\}$.

(b) $A = \mathbb{R}^2$ (the plane) and $R = \{(a, b, c) \in \mathbb{R}^2 \times \mathbb{R}^2 \times \mathbb{R}^2 : a, b, c \text{ lie on a line}\}$; i.e. tripples of points which are *colinear*.

(c) $A = \mathbb{R}^2$ and $R = \{(a, b) \in \mathbb{R}^2 \times \mathbb{R}^2 : a = (a_1, a_2),\ b = (b_1, b_2),\ a_1^2 + a_2^2 = b_1^2 + b_2^2\}$. This is an equivalence relation. The equivalence classes are circles centered at $(0, 0)$.

(d) $A = \mathbb{R}^2$ and $R =$ "$\leqslant$ on each component" $= \{(a, b) \in \mathbb{R}^2 \times \mathbb{R}^2 : a_1 \leqslant b_1,\ a_2 \leqslant b_2\}$.

The relation in the last example above is a ***partial order***; that is, $\leqslant$ satisfies, for all a, b, c,

1. $a \leqslant a$ *(reflexive)*
2. $a \leqslant b,\ b \leqslant a \quad \Rightarrow \quad a = b$ *(anti-symmetric)*
3. $a \leqslant b,\ b \leqslant c \quad \Rightarrow \quad a \leqslant c$ *(transitive)*

A relation R on a set A is an ***equivalence relation*** if it satisfies, for all a, b, c,

1. $a\, R\, a$ *(reflexive)*
2. $a\, R\, b \quad \Rightarrow \quad b\, R\, a$ *(symmetric)*
3. $a\, R\, b,\ b\, R\, c \quad \Rightarrow \quad a\, R\, c$ *(transitive)*

We denote the set of all equivalence relations on a set A by $\mathrm{Eq}(A)$.

A ***partition*** of a set A is a collection $\Pi = \{A_i : i \in I\}$ of non-empty subsets of A such that

$$\bigcup_{i \in I} A_i = A \quad \text{and} \quad A_i \cap A_j = \emptyset \text{ for all pairs } i \neq j \text{ in } I.$$

Facts and notation:

1. The A_i are called "blocks."
2. Each partition Π determines an equivalence relation – namely, the relation θ defined by $a\, \theta\, b$ if and only if a and b are in the same block of Π.
3. Conversely, if θ is an equivalence relation on A ($\theta \in \mathrm{Eq}(A)$), we denote the equivalence class of θ containing a by $a/\theta := \{b \in A : a\, \theta\, b\}$ and the set $A/\theta := \{a/\theta : a \in A\}$ of all θ classes is a partition of A.
4. "an SDR" (add something here)

1.5 Congruence Relations

Let A and B be sets and let $\varphi : A \to B$ be any mapping. We say that a pair $\langle a_0, a_1\rangle \in A^2$ belongs to the ***kernel*** of φ, and we write $\langle a_0, a_1\rangle \in \ker\varphi$, just in case $\varphi(a_0) = \varphi(a_1)$. Thus, to every map φ there corresponds a relation $\sim_\varphi = \ker\varphi$, defined by

$$a \sim_\varphi a' \qquad \Leftrightarrow \qquad \varphi(a) = \varphi(a').$$

We leave it as an exercise to prove

Proposition 1.6. $\ker\varphi$ *is an equivalence relation.*

If $\sim$ is an equivalence relation on a set A, then $a/\!\sim$ denotes the equivalence class containing a; that is, $a/\!\sim := \{a' \in A : a' \sim a\}$. The set of all equivalence classes of $\sim$ in A is denoted $A/\!\sim$. That is, $A/\!\sim = \{a/\!\sim : a \in A\}$.

Let $\mathbf{A} = \langle A; F^{\mathbf{A}}\rangle$ and $\mathbf{B} = \langle B; F^{\mathbf{B}}\rangle$ be algebras of the same type and let $\varphi : A \to B$ be any mapping. As above, φ determines the equivalence relation $\sim_\varphi = \ker\varphi$ on A. A ***congruence relation*** on $\mathbf{A}$ is an equivalence relation $\sim_\varphi$ arising from a *homomorphism* $\varphi : \mathbf{A} \to \mathbf{B}$, for some $\mathbf{B}$. We denote the set of all congruence relations on $\mathbf{A}$ by $\mathrm{Con}\mathbf{A}$.

To reiterate, $\theta \in \mathrm{Con}\mathbf{A}$ iff $\theta = \ker\varphi$ for some homomorphism φ of $\mathbf{A}$. It is easy to check that this is equivalent to: $\theta \in \mathrm{Con}\mathbf{A}$ iff $\theta \in \mathrm{Eq}(A)$ and

$$\langle a_i, a_i'\rangle \in \theta \quad (0 \leqslant i < n) \qquad \Rightarrow \qquad \langle f(a_0, \dots, a_{n-1}), f(a_0', \dots, a_{n-1}')\rangle \in \theta, \tag{1.2}$$

for all $f \in F_n$ and all $a_0, \dots, a_{n-1}, a_0', \dots, a_{n-1}' \in A$. Equivalently,[4]

$$\mathrm{Con}\mathbf{A} = \mathrm{Eq}(A) \cap \mathrm{Sub}(\mathbf{A} \times \mathbf{A}).$$

We record this fact as

Theorem 1.7. *Suppose $\mathbf{A} = \langle A; F\rangle$ is an algebra and θ is an equivalence relation on the set A. Then θ is congruence relation on the algebra $\mathbf{A}$ if and only if for every n-ary basic operation $f \in F$ and for all $a_0, \dots, a_{n-1}, a_0', \dots, a_{n-1}' \in A$,*

$$a_i\,\theta\,a_i' \quad (0 \leqslant i < n) \qquad \Rightarrow \qquad f(a_0, \dots, a_{n-1})\,\theta\,f(a_0', \dots, a_{n-1}').$$

In fact, we can replace the final implication in the theorem with: for each $0 \leqslant i < n$,

$$a_i\,\theta\,a_i' \qquad \Rightarrow \qquad f(a_0, \dots, a_i, \dots a_{n-1})\,\theta\,f(a_0, \dots, a_i', \dots, a_{n-1}).$$

Proof sketch: Recall that a/θ denotes the equivalence class of θ which contains a, and A/θ denotes the full set of θ classes: $A/\theta = \{a/\theta : a \in A\}$. For every operation $f^{\mathbf{A}}$ on A (say it is n-ary), we *define*

$$f^{\mathbf{A}/\theta}(a_1/\theta, \dots, a_n/\theta) := f^{\mathbf{A}}(a_1, \dots, a_n)/\theta.$$

One easily checks that this is well-defined and that the map $a \mapsto a/\theta$ is a homomorphism of $\mathbf{A}$ onto the algebra $\mathbf{A}/\theta := \langle A/\theta, F^{\mathbf{A}/\theta}\rangle$, where $F^{\mathbf{A}/\theta} := \{f^{\mathbf{A}/\theta} : f^{\mathbf{A}} \in F\}$. Finally, note that the kernel of this homomorphism is θ.

[4]The direct product algebra $\mathbf{A} \times \mathbf{A}$ is defined below in section 1.7.

1.6 Quotient Algebras

Let $\mathbf{A} = \langle A; F\rangle$ be an algebra. Recall, F denotes the set of operation symbols, and to each operation symbol $f \in F$ there corresponds an arity, and the set of arities determines the similarity type of the algebra. (We might do better to denote the algebra by $\langle A; F^{\mathbf{A}}\rangle$, since the algebra is not defined until we have associated to each operation symbol $f \in F$ an actual operation $f^{\mathbf{A}}$ on A, but this is a technical point, and we will often denote two algebras of the same similarity type as $\langle A; F\rangle$ and $\langle B; F\rangle$ with the understanding that the meaning of F depends on the context.)

Let $\theta \in \mathrm{Con}\mathbf{A}$ be a congruence relation. The ***quotient algebra*** $\mathbf{A}/\theta$ is an algebra with the same similarity type as $\mathbf{A}$, with universe $A/\theta = \{a/\theta : a \in A\}$, and operation symbols F, where for each (k-ary) symbol $f \in F$ the operation $f^{\mathbf{A}/\theta}$ is defined as follows: for $(a_1/\theta, \dots, a_k/\theta) \in (A/\theta)^k$,

$$f^{\mathbf{A}/\theta}(a_1/\theta, \dots, a_k/\theta) = f^{\mathbf{A}}(a_1, \dots, a_k)/\theta.$$

(As mentioned above, F denotes the set of operation symbols of the similarity type of the algebra, and it is "overloaded" in the sense that we write $\mathbf{A} = \langle A; F\rangle$ and $\mathbf{A}/\theta = \langle A/\theta, F\rangle$, and for each $f \in F$ the corresponding operation in these algebras is interpreted appropriately – i.e., as $f^{\mathbf{A}}$ or $f^{\mathbf{A}/\theta}$.)

1.7 Direct Products of Algebras

Above we defined direct products of sets. We now define direct products of algebras. Let $\mathbf{A} = \langle A; F\rangle$ and $\mathbf{B} = \langle B; F\rangle$ be two algebras of the same similarity type. The ***direct product*** $\mathbf{A} \times \mathbf{B}$ is an algebra of the same type as $\mathbf{A}$ and $\mathbf{B}$, with universe $A \times B = \{(a, b) : a \in A, b \in B\}$, and operation symbols F. To each (k-ary) symbol $f \in F$ corresponds an operation $f^{\mathbf{A}\times\mathbf{B}}$ defined as follows: for $((a_1, b_1), \dots, (a_k, b_k)) \in (A \times B)^k$,

$$f^{\mathbf{A}\times\mathbf{B}}((a_1, b_1), \dots, (a_k, b_k)) = (f^{\mathbf{A}}(a_1, \dots, a_k), f^{\mathbf{B}}(b_1, \dots, b_k)). \tag{1.3}$$

This definition can be easily extended to the direct product $\prod \mathbf{A}_i$ of any collection of algebras $\{\mathbf{A}_i : i \in I\}$, and we leave it to the reader to write down the defining property of the operations, which is completely analogous to (1.3).

When all the algebras are the same – that is, when $\mathbf{A}_i \cong \mathbf{A}$, for some $\mathbf{A}$ – we call $\prod \mathbf{A}_i$ the ***direct power*** of $\mathbf{A}$. When the set I is finite, say, $I = 1, 2, \dots, n$, we have alternative notations for the direct power, namely,

$$\prod \mathbf{A}_i = \mathbf{A}_1 \times \mathbf{A}_2 \times \cdots \times \mathbf{A}_n = \mathbf{A}^n.$$

The constructions of this subsection section and the preceeding one are often combined to give direct products of quotient algebras. For instance, if θ_1 and θ_2 are two congruences of $\mathbf{A}$, the algebra $\mathbf{A}/\theta_1 \times \mathbf{A}/\theta_2$ has the same similarity type as $\mathbf{A}$, and its universe is

$$A/\theta_1 \times A/\theta_2 = \{(a/\theta_1, b/\theta_2) : a, b \in A\}.$$

The operation symbols are again F, and to each (k-ary) symbol $f \in F$ corresponds an operation $f^{\mathbf{A}/\theta_1\times\mathbf{A}/\theta_2}$ defined as follows: for $((a_1/\theta_1, b_1/\theta_2), \dots, (a_k/\theta_1, b_k/\theta_2)) \in (A/\theta_1 \times A/\theta_2)^k$,

$$\begin{aligned} f^{\mathbf{A}/\theta_1\times\mathbf{A}/\theta_2}((a_1/\theta_1, b_1/\theta_2), \dots, (a_k/\theta_1, b_k/\theta_2)) &= (f^{\mathbf{A}/\theta_1}(a_1/\theta_1, \dots, a_k/\theta_1), f^{\mathbf{A}/\theta_2}(b_1/\theta_2, \dots, b_k/\theta_2)) \\ &= (f^{\mathbf{A}}(a_1, \dots, a_k)/\theta_1, f^{\mathbf{A}}(b_1, \dots, b_k)/\theta_2). \end{aligned}$$

1.8 Lattices

A ***relational structure*** is a set A and a collection of (finitary) relations on A. A ***partially ordered set***, or ***poset***, is a set A together with a partial order (Sec. 1.4) $\leqslant$ on it, denoted $\langle A, \leqslant \rangle$.

Let $\langle A, \leqslant \rangle$ be a poset and let B be a subset of the set A. An element a in A is an upper bound for B if $b \leqslant a$ for every b in B. An element a in A is the ***least upper bound*** of B, denoted $\bigvee B$, or ***supremum*** of B ($\sup B$), if a is an upper bound of B, and $b \leqslant c$ for every b in B implies $a \leqslant c$ (i.e., a is the smallest among the upper bounds of B). Similarly, a is a lower bound of B provided $a \leqslant b$ for all b in B, and a is the ***greatest lower bound*** of B ($\bigwedge B$), or ***infimum*** of B ($\inf B$) if a is a lower bound and is above every other lower bound of B.

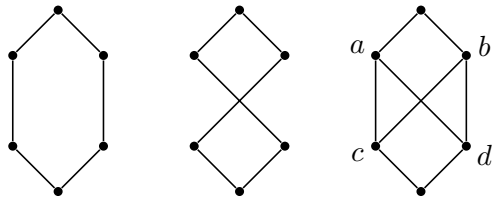
Let a, c be two elements in the poset A. We say c ***covers*** a, or a is covered by c provided $a \leqslant c$ and whenever $a \leqslant b \leqslant c$ it follows that $a = b$ or $b = c$. We use the notation $a \prec c$ to denote that c covers a.

A ***lattice*** is a partially ordered set $\langle L; \leqslant \rangle$ such that for each pair $a, b \in L$ there is a least upper bound, denoted $a \vee b := \text{lub}\{a, b\}$, and a greatest lower bound, denoted $a \wedge b := \text{glb}\{a, b\}$, contained in L. A lattice can also be viewd as an algebra $\langle L; \vee, \wedge \rangle$ where $\vee$, called "join," and $\wedge$, "meet," are binary operations satisfying

1. $x \vee x = x$ and $x \wedge x = x$ *(idempotent)*
2. $x \vee y = y \vee x$ and $x \wedge y = y \wedge x$ *(commutative)*
3. $x \vee (y \vee z) = (x \vee y) \vee z$ *(associative)*
4. $x \vee (y \wedge x) = x$ and $x \wedge (y \vee x) = x$ *(absorbtive)*

Posets in general, and lattices in particular, can be visualized using a so-called ***Hasse diagram***. The Hasse diagram of a poset $\langle A, \leqslant \rangle$ is a graph in which each element of the set A is denoted by a vertex, or "node" of the graph. If $a \prec b$ then we draw the node for b above the node for a, and join them with a line segment. The resulting diagram gives a visual description of the relation $\leqslant$, since $a \leqslant b$ holds iff for some finite sequence of elements $c_1, \ldots, c_n$ in A we have $a = c_1 \prec c_2 \prec \cdots \prec c_n = b$. Some examples appear in the figures below.

Figure 1: Hasse diagrams



Note that the first two examples in Figure 1 depict the same poset, which illustrates that Hasse diagrams are not uniquely determined. Also, note that the poset represented in the first two diagrams is a lattice. In contrast, the poset depicted in the third diagram is not a lattice since

Figure 2: Hasse diagrams of some small lattices.

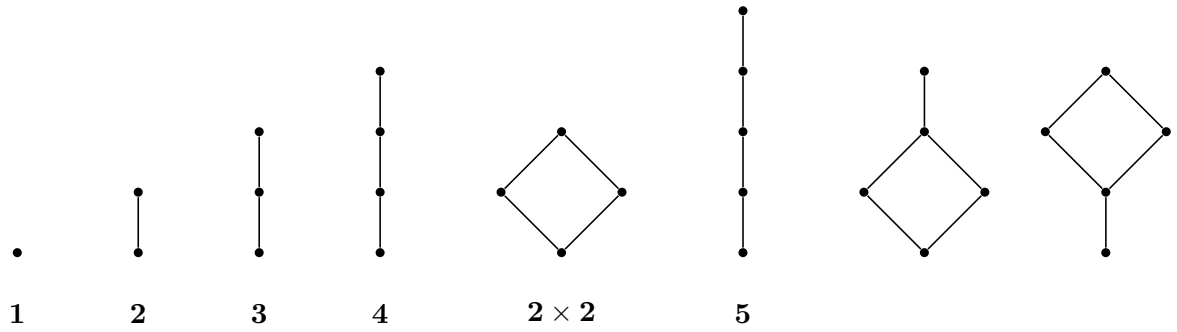
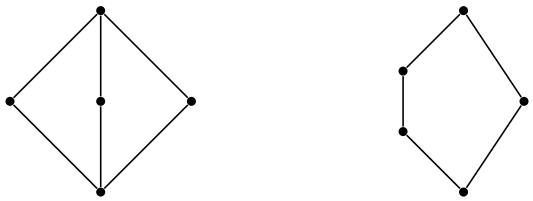


Figure 3: Hasse diagrams of two important lattices.



M_3 N_5

neither $a \wedge b$ nor $c \vee d$ is defined – the sets $\{a, b\}$ and $\{c, d\}$ have upper and lower bounds, but $\{a, b\}$ has no *greatest* lower bound, and $\{c, d\}$ has no *least* upper bound.

Part II
Rings, Modules and Linear Algebra

2 Rings

2.1 Factorization in Rings

In this sections R denotes a commutative ring with 1. For a, $b \in R$, we say a ***divides*** b if there exists $x \in R$ such that $ax = b$. This is denotes $a \mid b$. We say a and b are ***associates*** if $a \mid b$ and $b \mid a$. An element u is a ***unit*** if there exists a $v \in R$ with $uv = vu = 1$.

Theorem 2.1 (Theorem 4 in class)**.** *R commutative with 1, a, b, $u \in R$, then*

1. *$a \mid b$ iff $(b) \subseteq (a)$.*
2. *a and b are associates iff $(a) = (b)$.*
3. *u is a unit iff $u \mid r$ for all $r \in R$.*
4. *u is a unit iff $(u) = R$.*
5. *The relation "a is an associate of b" is an equivalence relation.*
6. *If $a = bu$, where u is a unit, then a and b are associates. If R is an integral domain the converse is true.*

Proof. Exercise. □

An ideal P is ***prime*** in R if $P \neq R$ and if A and B are ideals then

$$AB \subseteq P \implies A \subseteq P \text{ or } B \subseteq P$$

Theorem 2.2 (Theorem 5 in class)**.** *R commutative with 1. An ideal P of R is primve iff*

$$\forall a, b \in R,\ ab \in P \implies a \in P \text{ or } b \in P$$

Proof. Coming. □

Definition 2.3. R is a ***principal ideal domain***, or ***PID***, if it is an integral domain and all ideals are principal.

Definition 2.4. $c \in R$ is ***irrediducible*** if

1. c is a nonunit and not 0, and
2. $c = ab$ implies a or b is a unit.

$p \in R$ is ***prime*** if

1. p is a nonunit and not 0, and
2. $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Theorem 2.5 (Theorem 6 in class)**.** *Let R be an integral domain, and let $p \in R$.*

1. *p is a prime iff (p) is a nonzero prime ideal.*

2. *c is irreducible iff (c) is a maximal in the set of all proper, principal ideal fo R.*
3. *Every prime is irreducible.*
4. *If R is a PID then p is prime iff it is irreducible.*
5. *Associates of prime [irreducible] elements are prime [irreducible].*
6. *The only divisors of an irreducible element are associates and units.*

Proof. Coming. □

Definition 2.6. An integral domain is a ***unique factorization domain***, or ***UFD*** if

1. If $a \in R$, $a \neq 0$, and a is not a unit then $a = c_1 c_2 \cdots c_n$, where the c_i's are irreducible.
2. If $a = c_1 c_2 \cdots c_n$ and $a = d_1 d_2 \cdots d_m$, c_i, d_j irredicible, then $n = m$ and there is a $\sigma \in S_n$ such that c_i and $d_{\sigma(i)}$ are associates.

Lemma 2.7. *If R is a PID then R satisfies the ACC; that is if I_i an ideal and*

$$I_1 \subseteq I_2 \subseteq \cdots$$

then, for some n and all $k \geq 0$, $I_{n+k} = I_n$.

Proof. Laters. □

Theorem 2.8 (Theorem 7 in class)**.** *If R is a PID then it is a UFD.*

We proved that in a PID, an element is prime iff it is irreducible. Now we extend this to UFD's.

Theorem 2.9. *In a UFD R, a nonzero element is prime iff it is irreducible.*

Proof. By Theorem 2.5(3), if an element is prime in R it is irreducible. So suppose $p \in R$ is irredicible and suppose $p \mid ab$. So $pc = ab$ for some $c \in R$. If we write a, b and c as a product of irreducibles and use the uniqueness of the factorization and that p is irreducible, we see that p must be an associate of one of the irreducibles in a or one in b. WLOG we may assume the former so $a = (up)c_2 \cdots c_n$ so $p \mid a$. □

2.2 Rings of Frations

Coming.

2.3 Euclidean Domain and the Eucidean Algorithm

Coming.

2.4 Polynomial Rings, Gauss' Lemma

A ***greatest common divisor*** or ***gcd*** of elements a and b is an element c such that $c \mid a$ and $c \mid b$ and if d is any element such that $d \mid a$ and $d \mid b$ then $d \mid c$. The gcd will not in general be unique but any two are associates. In a UFD we can find $\gcd(a, b)$ by letting $p_1, \ldots, p_n$ be the distinct primes that occur in either a or b. Then, $a = u\prod_{i=0}^{n} p_i^{r_i}$ and $b = v\prod_{i=0}^{n} p_i^{s_i}$, u and v units, r_i, $s_i \geq 0$. Then if $t_i = \min(r_i, s_i)$, $\prod p_i^{t_i}$ is a gcd of a and b. If $\gcd(a, b) = 1$ then we say a and b are ***relatively prime***. $\gcd(a_0, \ldots, a_n)$ is defined in an obvious way.

Let R be a UFD and let $f = \sum_{i=0}^{n} a_i x^i \in R[x]$. The ***content***, denoted $\mathrm{C}(f)$, of f is $\gcd(a_0, \ldots, a_n)$. Again this is unique only up to associates. If $\mathrm{C}(f)$ is a unit (which is the same as saying $\mathrm{C}(f) = 1$) then f is called ***primitive***.

Exercise 2.10. Show that if R is a UFD and $a \in R$ then $\mathrm{C}(af) = a\,\mathrm{C}(f)$.

Lemma 2.11 (Gauss' Lemma)**.** *If R is a UFD and f, $g \in R[x]$ then $\mathrm{C}(fg) = \mathrm{C}(f)\,\mathrm{C}(g)$. In particular the product of primitive polynomials is primitve.*

Proof. Let $a = \mathrm{C}(f)$ and $b = \mathrm{C}(g)$. Then $f = af_1$ and $g = bg_1$, for some f_1 and $g_1 \in R[x]$ which are primitive. Note $fg = abf_1g_1$. By the exercise it is enough to show f_1g_1 is primitive. Let $f_1 = \sum_{i=0}^{n} a_i x^i$ and $g_1 = \sum_{i=0}^{m} b_i x^i$, then $f_1g_1 = \sum_{i=0}^{m+n} c_i x^i$, where $c_k = \sum_{i+j=k} a_i b_j$. Suppose f_1g_1 is not primitive, then there is an irreducible element p such that $p \mid c_i$ for all i. Since f_1 is primitive, there is a smallest s such that $p \nmid a_s$ and a smallest t such that $p \nmid b_t$. Now $p \mid c_{s+t} = a_0b_{s+t} + \cdots + a_sb_t + \cdots + a_{s+t}b_0$. This implies $p \mid a_sb_t$ (since it divides all other terms on both sides). But since p is irreducible and hence prime, this implies $p \mid a_s$ or $p \mid b_t$, a contradiction. □

Lemma 2.12. *Let R be a UFD with quotient field F and let f and g be primitive polynomials in $R[x]$. Then f and g are associates in $R[x]$ iff they are associates in $F[x]$.*

Proof. Let f and g be associates in $F[x]$. Since $F[x]$ is an integral domain, Theorem 2.1(6) there is a unit $u \in F[x]$ such that $f = ug$. Units in $F[x]$ are just the nonzero elements of F. Hence $u = b/c$ for some b, $c \in R$, $c \neq 0$. So $cf = bg$. Since $C(f)$ and $C(g)$ are units in R,

$$c \approx cC(f) \approx C(cf) \approx C(bg) \approx bC(g) \approx b$$

where $a \approx b$ means a and b are associates. Hence $b = vc$ for some unit $v \in R$ and so $cf = bg = vcg$. Since $c \neq 0$, $f = vg$, showing f and g are associates in $R[x]$.

The converse is easy. □

Theorem 2.13 (This is also called Gauss' Lemma)**.** *Let R be a UFD with quotient field F and let f be a primitive polynomial of positive degree in $R[x]$. Them f is irreduible in $R[x]$ iff it is irreducible in $F[x]$.*

Proof. Suppose f is irreducible in $R[x]$ but $f = gh$ in $F[x]$ with the degrees of g and h positive. Then

$$g = \sum_{i=0}^{n} (a_i/b_i)x^i \text{ and } h = \sum_{i=0}^{m} (c_i/d_i)x^i$$

with $a_i, b_i, c_j, d_j \in R$ and $b_i \neq 0 \neq d_j$. Let $b = b_0 b_1 \cdots b_n$ and for each i let $b_i^* = b/b_i$. Of course b_i^* is in R. Let $g_1 = \sum_{i=0}^{n} a_i b_i^* x^i \in R[x]$. Then $g_1 = a g_2$ with $a = C(g_1)$ and g_2 is primitive in $R[x]$. Now

$$g = (1/b)g_1 = (a/b)g_2$$

and $\deg g = \deg g_2$. Similarly $h = (c/d)h_2$ with c, $d \in R$, h_2 primitive in $R[x]$ and $\deg h = \deg h_2$. Hence $f = gh = (a/b)(c/d)g_2h_2$, so $bdf = acg_2h_2$. Since f is primitive and g_2h_2 is primitive by Gauss' Lemma,

$$bd \approx bdC(f) \approx C(bdf) \approx C(acg_2h_2) \approx acC(g_2h_2) \approx ac.$$

So bd and ac are associates in $R[x]$ which implies f and g_2h_2 are associates in $R[x]$. So f is reducible in $R[x]$, a contradiction. So f is irreducible in $F[x]$.

Conversely suppose f is irreduible in $F[x]$ but $f = gh$ in $R[x]$. This is still a factorization in $F[x]$ so either g or h is a unit in $F[x]$. The units of $F[x]$ are just the nonzero constant elements of F so one, say g, is constant (and in R). Now $C(f) = gC(h)$. Since f is primitive, g must be a unit in R and so in $R[x]$. Therefore f is irreducible in $R[x]$. □

Theorem 2.14. *R is a UFD iff $R[x]$ is.*

Proof. Assume R is a UFD. We will first show that every $f \in R[x]$ can be factored into irreduibles and then prove the uniqueness. As usual let $f = cf_1$, $c = C(f)$, f_1 primitive. Since R is a UFD, c can be uniquely factored uniquely into irreducibles, so we only need to factor f_1. So switching notation we assume the f is a primitive. We may also assume $\deg f > 0$.

Now $F[x]$ is a UFD (since it is a Euclidean domain) and so f can be factored into irreducibles in $F[x]$. Using the proof of the second version of Gauss's Lemma, f can be factored in $R[x]$ and the factors are multiples by elements in F of the factors in $F[x]$. Since the content of f is 1, the content of each of these factors must be 1. So by the last theorem each is irreducible in $R[x]$.

For the uniquess suppose $f = g_1 \cdots g_r = h_1 \cdots h_s$ are two factorizations of f into irreducibles. Since the content of f is 1, the content of each g_i and h_j is 1. So they are irreducible in $F[x]$ by Gauss. Since $F[x]$ is a UFD, $r = s$ and, after renumbering, g_i and h_i are associates in $F[x]$, so $g_i = (a/b)h_i$, for some nonzero a and $b \in R$. So $bg_i = ah_i$. The content of the left side is b and of the right side is a. Hence $a = ub$, for a unit $u \in R$. Thus $g_i = uh_i$ so g_i and h_i are associates in $R[x]$, completing the proof. □

Corollary 2.15. *If F is a field then $F[x_1, \ldots, x_n]$ is a UFD.*

Corollary 2.16. *If F is a field then $F[x_1, x_2, \ldots]$ is a UFD.*

2.5 Irreducibility Tests

Theorem 2.17 (Eisentein criterion)**.** *Let R be a UFD with quotient field F. Let*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

be in $R[x]$. If there exists a prime p of R such that p divides all the coeffients except the highest, and $p^2 \nmid a_0$, that is,

$$p \mid a_i \ , i = 0, \ldots, a_{n-1}, \qquad p \nmid a_n, \qquad p^2 \nmid a_0,$$

then f is irreducible in $F[x]$. If f is primitive it is also irreducible in $R[x]$.

Proof. $f = C(f)f_1$ for some primitive polynomial f_1. So f and f_1 are associates in $F[x]$ since $C(f)$ is a unit of F. This implies f is irreducible in $F[x]$ iff f_1 is. So by the second version of Gauss' Lemma, it suffices to show f_1 is irreducible in $R[x]$. Suppose $f_1 = gh$, g, $h \in R[x]$, where

$$g = b_r x^r + \cdots + b_0, \ \deg g = r \geq 1$$
$$h = c_s x^s + \cdots + c_0, \ \deg h = s \geq 1.$$

Since $p \nmid a_n$, $p \nmid C(f)$, so if we write $f_1 = \sum_{i=0}^{n} a_i^* x^i$, then the a_i^* have the same divibility properties with respect to p as the a_i's. Since $p \mid a_0^* = b_0 c_0$, it divides one of them; say b_0. Since $p^2 \nmid a_0^*$, $p \nmid c_0$. p cannot divide every b_i since otherwise p would divide g and hence $f_1 = gh$. Let k be the least integer not divisible by p. So $p \mid b_i$, $i < k$ and $p \nmid b_k$. Since $r < n$, $k < n$. Now

$$a_k^* = b_0 c_k + b_1 c_{k-1} + \cdots b_{k-1} c_1 + b_k c_0.$$

This implies $p \mid b_k c_0$, a contradiction. □

Exercises 2.18.

1. Show that $2x^5 - 6x^3 + 9x^2 - 15$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

2. Let $f = y^3 + x^2 y^2 + x^3 y + x \in R[x, y]$, where R is a UFD. Show that f is irreducible in $R[x, y]$. (Hint: view $R[x, y]$ as $(R[x])[y]$ and note that x is irreducible (and hence prime) in $R[x]$.)

3. Let p be a prime in $\mathbb{Z}$ and $f = \frac{x^p - 1}{x - 1} = \sum_{k=0}^{p} \binom{p}{k} x^k$. Show that f is irreducible in $\mathbb{Z}[x]$. (Hint: show that $g(x) = f(x + 1)$ is irreducible and use this to show f is irreducible.)

3 Modules

3.1 Basics

Let R be a ring. An R-***module*** is an algebra M with operations $+$, $-$, 0, such that $\langle A; +, -, 0\rangle$ is an abelian group and for each $r \in R$ there is a unary operation $a \mapsto ra$ such that for all r, $s \in R$ and a, $b \in M$,

$$\begin{aligned} r(a+b)a &= ra + rb \\ (r+s)a &= ra + sa \\ (rs)a &= r(sa) \end{aligned}$$

If $1 \in R$ and $1a = a$ then M is a ***unitary*** R-module. The student can show that $0a = 0$ (note here the first 0 is the zero of R and the second is the zero of M. Also $r(-a) = -ra$. The notation ${}_RM$ means M is a left R module. Right R-modules are defined in the obvious way and denote M_R.

Unless otherwise stated, we will assume R has a 1 and modules are unitary.

Example 3.1.

(a) Each abelian group is a $\mathbb{Z}$ module (in an obvious way).

(b) A vector space V over a field F is an F-module.

(c) Column vectors of length n with entries in R are a module over $M_n(R)$, the ring of $n \times n$ matricies.

(d) R itself is both a left and a right R-module, ${}_RR$ and R_R. $I \subseteq R$ is a left idea if and only if it is a submodule of ${}_RR$.

(e) Let F be a field, V a vector space over F and $T : V \to V$ a linear transformation on V. Then V is a $F[x]$-modules under the action $f(x)v = f(T)v$.

Just as for abelian groups, the congruence associated with a module homomorphism $\varphi : A \to C$ is determined by $f^{-1}(0)$, which is a submodule (as you can easily check). Conversely if B is a sumbmodule of A, we can form the quotient module A/B in the usual way. The usual isomorphism theorems hold; see Dummit and Foote [1], section 10.2.

Free modules can be defined in the usual way: If M is an R module and $X \subseteq M$, then M is ***freely generated*** by X (or M is ***free over*** X) if M is generated by X and if $\varphi : X \to N$ (N another R-module) then φ can be extended to a homomorphism of $\bar{\varphi} : M \to N$.

As in groups, we call a module M ***cyclic*** if it is one-generated; that is, there is an element $a \in M$ such that the smallest submodule containing a, which is

$$Ra := \{ra : r \in R\}$$

is M. One easily verifies that the map $r \mapsto ra$ is an R-module homomorphism of ${}_RR$ onto $Ra = M$. The kernel of this map is called the ***annihilator*** of a and is denoted $\operatorname{ann} a$; thus $\operatorname{ann} a := \{r \in R : ra = 0\}$ and so

$$Ra \cong R/\operatorname{ann} a$$

The above homomorphism also shows that ${}_RR$ is the free R-module on the single generator 1. In fact free R-modules are particularly simple to describe: they are the direct sums of copies of ${}_RR$, as you will get to show in the exercises.

Exercises 3.2.

1. If X and Y are sets of the same cardinality (that is, there is a one-to-one function from X onto Y) then any free R-module over X is isomorphic to any free R-module over Y.

2. Let R^n be n-tuples of elements of R, as usual. This is an R-module in the obvious way: $r(x_1, \ldots, x_n) = (rx_1, \ldots, rx_n)$ (dah). This module is usually denoted ${}_RR^n$. Let $e_i = (0, \ldots, 0, 1, 0, \ldots 0)$, 1 in the i^{th} position and $X = \{e_1, \ldots, e_n\}$. Then ${}_RR^n$ is a free R-module over X. In particular, every vector space over a field F is a free F-module. The free abelian group on n generators is isomorphic to $\mathbb{Z}$.

3. Now consider ${}_RR^\omega$. Let $e_i = (0, \ldots, 0, 1, 0, \ldots)$, 1 in the i^{th} position and $X = \{e_1, e_2, \ldots\}$. The submodule generated by X consists of all ω-tuples which are 0 in all but finitely many coordinates (this is called the ***direct sum***). Show this submodule is free over X.

4. Note that the e_i in the exercises above generate ${}_RR^n$ and ${}_RR^\omega$. Also $\sum x_i e_i = \sum y_i e_i$ implies $x_i = y_i$ for all i. Generators of a module that have these properties are called a ***base***. Show that if M has a basis with n elements, then $M \cong {}_RR^n$ and hence is a free R-module.

5. Suppose M_i, $i = 1, \ldots, n$ are submodules of a module M such that the submodule genereated by the M_i's is all of M, that is, $M = M_1 + \cdots + M_n$. Also assume

$$M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_n) = 0$$

for $i = 1, \ldots, n$. Show that M is isomorphic to the direct product (or direct sum, they're the same for finite products) of the M_i's.

Every vector space over a field F has a basis and so is a free F-module. But in general not all modules are free. Also there are rings R such that ${}_RR^n \cong {}_RR^m$ for distinct n and m; see exercise 27 of section 10.3 of Dummit and Foote [1]. But for commutative rings this is not possible:

Theorem 3.3. *If R is commutative, then ${}_RR^n \cong {}_RR^m$ implies $n = m$.*

Proof. See Chapter 3 of Jacobson [4]. □

3.2 Finitely Generated Modules over a PID

Theorem 3.4 (Dedekind)**.** *Let R be a PID. Every submodule of a free R-module is free. If M is free of rank n, then every submodule is free of rank at most n.*

Proof. Jacobson [4] gives an elementary, computational proof of this in the finite rank case. Hungerford [3] proves the full theorem. □

Exercises 3.5.

1. Show that if A is an n-generated module over a PID and B is a submodule of A, then B can be generated by a set with at most n elements.

Let R be a PID and let A and $B \in \mathrm{M}_{m,n}(R)$. A and B are ***equivalent*** if there are invertible matrices $P \in \mathrm{M}_m(R)$ and $Q \in \mathrm{M}_n(R)$ such that $B = PAQ$.

Theorem 3.6. *If $A \in M_{m,n}(R)$, R a PID, the A is equvalent to a diagonal matrix*

$$\mathrm{diag}(d_1, d_2, \ldots, d_r, 0, \ldots, 0).$$

where $d_i \neq 0$ and $d_i \mid d_j$ if $i \leq j$. The d_i's are unique up to associates.

This diagonal matrix is called the ***Smith normal form*** of A. The d_i's are called the ***invariant factors*** of A. In class we will follow the proof given in Jacobson [4].

The uniqueness in the above theorem follows from the relation between the invariant factors and the determinental divisors, which we now define. For $A \in \mathrm{M}_{m,n}(R)$ we define the ***rank*** of A to be the greatest r such that A has an $r \times r$ submatrix with nonzero determinant. Δ_i, the i^{th} ***determinental divisor*** of A is the gcd of the determinants of the $i \times i$ submatrices of A, $i = 1, \ldots, r$. The uniqueness is shown by proving the following.

$$\Delta_i = d_1 \cdots d_i, \quad i = 1, \ldots, r. \tag{3.1}$$

Defining $\Delta_0 = 1$, this can be writen as

$$d_i = \Delta_i / \Delta_{i-1}, \quad i = 1, \ldots, r, \tag{3.2}$$

Note the Laplace expansion theorem implies $\Delta_{i-1} \mid \Delta_i$.

Theorem 3.7 (Cauchy-Binet)**.** *Let R be a commutative ring and let $A \in M_{m,n}(R)$ and $B \in M_{n,k}(R)$, $\alpha = (\alpha_1, \ldots, \alpha_r)$ be a sequence with $1 \leq \alpha_1 < \cdots < \alpha_r \leq m$, $\beta = (\beta_1, \ldots, \beta_r)$ be a sequence with $1 \leq \beta_1 < \cdots < \beta_r \leq k$. For any matrix $C \in Mn, k(R)$, let $C[\alpha, \beta]$ be the $r \times r$ submatrix of C lying at the intersection of the α rows and β columns. Then*

$$\det AB[\alpha, \beta] = \sum_{\gamma} \det A[\alpha, \gamma] \det B[\gamma, \beta,]$$

where the sum is over $\gamma = (\gamma_1, \ldots, \gamma_n)$ with $1 \leq \gamma_1 < \cdots < \gamma_r \leq n$.

Corollary 3.8. *Up to associates, equivalent matrices have the same determinental divisors.*

Proof. If d is the r^{th} determinental divisor of A, the Cauchy-Binet Theorem shows that d divides all determinates of $r \times r$ submatrices PAQ. Hence d divides the r^{th} determinental divisor of PAQ. Since similarity is a symmetric relation, this shows similar matrices have the same determinental divisors, up to associates. □

Note that (3.1) and (3.2) follow from this corollary and from Theorem 3.6. And of course the uniqueness of the invariant factors (the d_i's), and that equivalent matrices have the same invariant factors, up to associates, follow from (3.2). So we only need to prove the first part of Theorem 3.6, which we will do in class.

Since R is a PID each of the invariant factors can be written as

$$d_i = p_1^{e_{i1}} \cdots p_m^{e_{im}}$$

where $p_1, \ldots, p_m$ are distinct primes in R. Since $d_i \mid d_{i+1}$, $e_{ik} \leq e_{i+1,k}$. A prime power $p_k^{e_{ik}}$ with $e_{ik} > 0$ is called an ***elementary divisor*** of A. The ***list of elementary divisors*** is the list of all of them including repeats. For example, suppose $R = \mathbb{Z}$ and $d_1 = 2^3 \cdot 3$, $d_2 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 7$, and $d_3 = 2^4 \cdot 3^3 \cdot 5^5 \cdot 7^2$. Then the list of elementary divisors is

$$2^3, 2^4, 2^4, 3, 3^3, 3^3, 5^2, 5^5, 7, 7^2.$$

The invariant factors can be recovered from the list of elementary divisors and the rank of A. So if the rank of B is four and it has the above list of elementary divisors, then there will be 4 invariant factors. d_4 must be the product of all the highest prime powers: $d_4 = 2^4 \cdot 3^3 \cdot 5^5 \cdot 7^2$. d_3 is the product of the highest remaining prime powers: $d_3 = 2^4 \cdot 3^3 \cdot 5^2 \cdot 7$. And $d_2 = 2^3 \cdot 3$. d_1 is the product of the rest. But there aren't any so it is the product of the empty set: $d_1 = 1$.

Exercise 3.9.

1. Let R be a Euclidean domain and let $\mathrm{SL}_n(R)$ be all $n \times n$ matrices over R with determinant 1. In this exercise you will show that the group $\mathrm{SL}_n(R)$ is generated by the elementary matrices of the first kind (those of the form $I_n + bE_{i,j}$, $i \neq j$i). First note the the elementary transformation used in putting a matrix into Smith Normal Form of the form no $D(u)$ was used. The elementary matrix corresponding to interchanging two rows (or columns) has determinant -1 but if we multiply one of the rows by -1, then the determinant is 1 and this elementary operation (interchanging two rows and multiplying one of them by -1) can be used (in the proof of the Smith Normal Form) instead of just interchanging the rows. You can take this as given—you do not need to write it up.

a. Let u be a unit is R. Show that

$$\begin{bmatrix} 0 & u \\ -u^{-1} & 0 \end{bmatrix}$$

can be written as a product of three elementary matrices of the first kind, each of which has either u or $-u^{-1}$ as its single off-diagonal entry. Note the modified permutation matrix described above is this matrix with $u = 1$.

b. Show that if u is a unit, then

$$\begin{bmatrix} u & 0 \\ 0 & u^{-1} \end{bmatrix}$$

is a product of two matrices from part **a**.

c. Using part **a** and the comments above we see that A can be put into Smith Normal Form using elementary matrices of the first kind. Now use the matrices of part **b** to modify the Smith Normal Form into the identity matrix and show this implies that A is a product of elementary matrices of the first kind.

Let M be an R-module, N a submodule of M and $a \in M$. The ***annihilator*** of a is $\operatorname{ann} a = \operatorname{ann}_R a = \{r \in R : ra = 0\}$; $\operatorname{ann}_R N = \{r \in R : rN = 0\}$. The ***torsion submodule*** of M is $\operatorname{tor} M = \{m \in M : \operatorname{ann} a \neq 0\}$. The reader can show $\operatorname{ann} a$ is a left ideal of R, $\operatorname{ann} N$ is a two-sided ideal of R and $\operatorname{tor} M$ is a submodule. Also show that $R/\operatorname{ann} a \cong Ra$. M is a ***torsion module*** if $\operatorname{tor} M = M$ and M is ***torsion free*** if $\operatorname{tor} M = 0$. When R is a PID, $\operatorname{ann} a = (r)$, for some r and we say a has ***order*** r. Of course any associate of r is also "the" order of a. Note that in an abelian group, thought of as a $\mathbb{Z}$-module, order agrees with the usual nottion except an element of order n also has order $-n$.

Theorem 3.10. *A finitely generated torsion free module over a PID is free.*

We will prove this in class following Hungerford [3].

Theorem 3.11. *If M is a finitely generated module over a PID R, then $M = \operatorname{tor} M \oplus F$, where F is a finitely generated free R-module.*

Proof. Let $T = \operatorname{tor} M$. Then M/T is torsion free: if $a + T \in M/T$ and $r(a + T) = T$ then $ra \in T$. But this implies $sra = 0$ for some $s \neq 0$ in R. But then $a \in \operatorname{tor} M = T$, and so $a + T = T$. Of course M/T is finitely generated since M is. By Theorem 3.10, M/T is free. Let $x_1, \ldots, x_k$ be a free generating set, that is, a basis for M/T and let $\varphi : M \twoheadrightarrow M/T$ be the natural homomorphism. Choose $y_i \in M$ with $\varphi(y_i) = x_i$. Let F be the submodule of M gnerated by the y_i's. Let $\psi : M/T \to M$ be the homomorphism that extends $\psi(x_i) = y_i$. Note $\varphi(\psi(x_i)) = \varphi(y_i) = x_i$ and so $\varphi \circ \psi$ is the identity homomorphism on M/T. So $F \cong M/T$ and thus is free.

If $m \in M$ let $a = \psi(\varphi(m)) \in F$. Since $\varphi \circ \psi$ is the identity, $\varphi \circ \psi \circ \varphi = \varphi$. This implies $\varphi(m - a) = 0$, and so $m - a \in T$. Thus

$$m = a + (m - a) \in F + T$$

It is easy to verify that $F \cap T = 0$. Thus $M = F \oplus T$, as desired. □

Let M be a torsion module over a PID R. For p a prime in R let

$$M(p) = \{a \in M : p^i a = 0, \text{ for some } i\}.$$

$M(p)$ is called the ***p-primary*** component of M.

Theorem 3.12. *Let M be a torsion module over a PID R. Then $M(p)$ is a submodule of M and there is a set S of primes in R such that $M = \bigoplus_{p \in S} M(p)$. If M is finitely generated and $M(p) \neq 0$ for $p \in S$ then S is finite.*

Proof. That $M(p)$ is a submodule is left as an exercise.

We can take S to be an SDR (system of distict representatives) of the set of all primes in R under the equivalence relation "p is an associate of q".

Let $a \in M$ and let r be the order of a so that $\operatorname{ann} a = (r)$. Since R is s UFD, we can write $r = up_1^{n_1} \cdots p_k^{n_k}$ for distinct primes in S, $n_i > 0$ and u a unit. Let $r_i = r/p_i^{n_i}$. Note $r_1, \ldots, r_k$ are relatively prime. Since R is a PID, this implies $1 = s_1 r_1 + \cdots + s_k r_k$. Thus

$$a = s_1 r_1 a + \cdots + s_k r_k a.$$

Since $p_i^{n_i} s_i r_i a = s_i r a = 0$, $s_i r_i a \in M(p)$. Hence $a \in \sum_{p \in S} M(p)$.

Suppose $a \in M(p) \cap \sum_{q \neq p} M(q)$. Then $p^m a = 0$ for some $m \geq 0$ and $a = a_1 + \cdots + a_t$, where $a_i \in M(p_i)$, p_i primes distinct from each other and from p. Let $p_i^{m_i} a_i = 0$ and let $d = p_1^{m_1} \cdots p_t^{m_t}$ and note $da = 0$. Now d and p^m are relatively prime so there exists r, $s \in R$ with $1 = rp^m + sd$. But then $a = rp^m a + sda = 0$, showing $M(p) \cap \sum_{q \neq p} M(q) = 0$. □

Theorem 3.13. *Let M be a finitely generated module over a PID R.*

1. *M is isomorphic to the direct sum of finitely many cyclic modules:*

$$\begin{aligned} M &= R^k \oplus Ra_1 \oplus \cdots \oplus Ra_m \\ &\cong R^k \oplus R/(d_1) \oplus \cdots \oplus R/(d_m) \\ &= R^k \oplus R/\operatorname{ann} a_1 \oplus \cdots \oplus R/\operatorname{ann} a_m \end{aligned}$$

   where the d_i's are nonzero, nonunit elements of R and

$$d_1 \mid d_2 \mid \cdots \mid d_m.$$

2. *M is isomorphic to the direct sum of finitely many primary cyclic modules:*

$$M \cong R^k \oplus R/(p_1^{n_1}) \oplus \cdots \oplus R/(p_t^{n_t})$$

   where $p_1, \ldots p_t$ are (not necessarily distinct) primes and $n_i \geq 1$.

Proof. We will prove the first part in class using the Smith Normal Form. The second part can be derived from the first using Theorem 3.12 and Exercise 3.5. □

The k in this theorem is called the ***free rank*** of M. The d_i's are called the ***invariant factors*** of M and the $p_i^{n_i}$'s are the ***elementary divisors*** of M. These determine M up to isomorphism:

Theorem 3.14. *Let M_1 and M_2 be modules over a PID R.*

1. *$M_1 \cong M_2$ iff they have the same free rank and invariant factors (up to associates).*
2. *$M_1 \cong M_2$ iff they have the same free rank and elementary divisors (up to associates).*

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

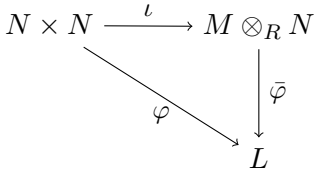
$$\begin{aligned}(m + m', n) - (m, n) - (m', n)\\ (m, n + n') - (m, n) - (m, n')\\ (mr, n) - (m, rn)\end{aligned}$$

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 $\varphi(m, rn) = \varphi(mr, n)$. The natural map $M \times N \to M \otimes_R N$ is balanced and universal for this concept; that is, any balanced map can be factored through this.

Theorem 3.15. *Let M_R and ${}_RN$ be R modules. Let $\iota : M \times N \to M \otimes_R N$ be the natural map. 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:*



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

$$f : M_R \to M'_R \text{ and } g : {}_RN \to {}_RN' \tag{3.3}$$

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 3.15 can be used to show this works.

Theorem 3.16. *Suppose f and g are homomorphism as in* (3.3)*. 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 3.15. □

Another use of Theorem 3.15 is to show that tensor products are associated; 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 3.15.

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

Theorem 3.18. *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 3.17.

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 3.19.

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

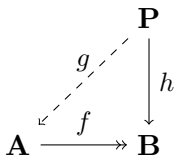
$$\cdots \to X_{n-1} \xrightarrow{\alpha} X_n \xrightarrow{\beta} X_{n+1} \to \cdots$$

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

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0 \tag{3.4}$$

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



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 3.20.

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 3.4 to show that an R module is projective iff it is free. (We only proved Theorem 3.4 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 (3.4) 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 (3.4) 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, $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}$, 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 3.21.

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

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 $\text{char}(R)$. 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 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.

Index