MA4H8: Ring Theory

Luke Collins*
maths.com.mt/notes

Version 0.1† (1st October, 2019)

It's the job that's never started
as takes longest to finish.

— J.R.R. Tolkien
The Lord of the Rings

Contents

*Based on lectures given by Prof Charudatta Hajarnavis (academic year 2019–2020) at the Mathematical Institute, University of Warwick.

†If you find any mathematical, grammatical or typographical errors whilst reading these notes, please let the author know via email: luke.collins@warwick.ac.uk.

Notation and Terminology

Rings and modules are denoted by capital letters such as R and M. Small Latin or Greek letters such as x, f or ϕ denote members of a set or functions. Ideals are denoted using Fraktur letters such as $\mathfrak{a}$ or $\mathfrak{p}$. The set of natural numbers is denoted by $\mathbb{N}$, the set of integers by $\mathbb{Z}$, the set of rational numbers by $\mathbb{Q}$, the set of real numbers by $\mathbb{R}$, the set of complex numbers by $\mathbb{C}$ and the empty set by $\emptyset$.

A function f with domain A and codomain B is written $f\colon A \to B$. The image of $x \in A$ under f is denoted by $f(x)$ or sometimes by fx. A function f is *injective* if for all $x, y \in A$, $f(x) = f(y) \Rightarrow x = y$. If f is injective, we write $f\colon A \hookrightarrow B$. A function f is *surjective* if for all $y \in B$, there exists $x \in A$ such that $f(x) = y$. If f is surjective, we write $f\colon A \twoheadrightarrow B$. A function f is a *bijection* if it is both an injection and a surjection. If f is bijective, we write $f\colon A \xhookrightarrow{\sim} B$.

If $f\colon A \to B$ is a function and $S \subseteq A$, the *restriction* of f to S, denoted by $f \restriction S$, is the function $(f \restriction S)\colon S \to B$ defined by $(f \restriction S)(x) = f(x)$ for all $x \in S$.

The set of functions from A to B is denoted B^A, so that $f\colon A \to B$ if and only if $f \in B^A$.

We generalise the notation of functions and ring operations to sets in the obvious way. In particular, if f is a function, A and B are sets, and x is an element of a ring, then we have the following:

- $A + B = \{a + b : a \in A \text{ and } b \in B\}$,
- $A - B = \{a - b : a \in A \text{ and } b \in B\}$,[1]
- $x + A = \{x + a : a \in A\}$ and $A + x = \{a + x : a \in A\}$,
- $xA = \{xa : a \in A\}$ and $Ax = \{ax : a \in A\}$,
- $f(A) = \{f(a) : a \in A\}$ (also written fA).

For instance, with these conventions, we have that $f\colon A \to B$ is surjective if and only if $f(A) = B$, and the set of even integers is $2\mathbb{Z}$. Notice that we do not list AB here, this particular notation will be defined differently than "the obvious way" (see section 1.5).

If $f\colon A \to B$ is a function, we also denote the *image* $f(A)$ by $\operatorname{im} f$.

[1] We use $A \setminus B$ for set difference.

1 Basics

A *ring* is a triple $(R, +, \cdot)$, where R is a non-empty set, $+, \cdot : R \times R \to R$ are two binary operations, termed "addition" and "multiplication" respectively, and the following properties hold:

I. for all $a, b \in R$, $a + b \in R$, (Closure under $+$)

II. for all $a, b, c \in R$, $a + (b + c) = (a + b) + c$, (Associativity under $+$)

III. there exists $0 \in R$ s.t. for all $a \in R$, $a + 0 = a$, (Identity for $+$)

IV. for all $a \in R$, there exists $-a \in R$ s.t. $a + (-a) = 0$, (Inverses for $+$)

V. for all $a, b \in R$, $a + b = b + a$, (Commutativity under $+$)

VI. for all $a, b \in R$, $a \cdot b \in R$, (Closure under $\cdot$)

VII. for all $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, (Associativity under $\cdot$)

VIII. for all $a, b, c \in R$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, (Left distributivity)

IX. for all $a, b, c \in R$, $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$. (Right distributivity)

I and VI are obvious from the definition of $+$ and $\cdot$, we state them here for emphasis. Observe that I–V imply that $(R, +)$ is an abelian group. We also have the following optional properties:

A. there exists $1 \in R$ s.t. for all $a \in R$, $a \cdot 1 = 1 \cdot a = a$, (Identity for $\cdot$)

B. for all $a \in R \setminus \{0\}$, there exists $a^{-1} \in R$ s.t. $a \cdot a^{-1} = a^{-1} \cdot a = 1$, (Inverses for $\cdot$)

C. for all $a, b \in R$, $a \cdot b = b \cdot a$. (Commutativity under $\cdot$)

A ring satisfying A is called a *unital ring* or a *ring with* 1, a ring satisfying A and B is called a *division ring*, a ring satisfying C is called a *commutative ring*, and a ring satisfying all three properties is called a *field*.

Notation. We relax the triple notation $(R, +, \cdot)$, simply referring to the corresponding ring as "the ring R". We also relax the multiplication notation $a \cdot b$ to simple juxtaposition of the symbols: ab. The sum $a + (-b)$ is written $a - b$, and $a + (b + c)$ is written $a + b + c$, which is unambiguous by associativity under $+$; similarly $a(bc)$ is written abc. In commutative rings, the product ab^{-1} is written $\frac{a}{b}$. Sometimes, when dealing with multiple rings, we subscript the operations and identity elements for clarity, e.g., we write $a +_R b$, $a \cdot_R b$, 0_R and 1_R to emphasise that these correspond to the operations and identities of the ring R.

Let us begin by sating some basic properties which follow immediately from the ring axioms.

Proposition 1.1. *Let R be a ring. Then the following properties hold.*

(i) *The identity $0 \in R$ is unique,*

(ii) *Given $a \in R$, the inverse $-a$ is unique,*

(iii) *$-(-a) = a$ for all $a \in R$,*

(iv) *$a \cdot 0 = 0 \cdot a = 0$ for all $a \in R$,*

(v) *$a(-b) = (-a)b = -ab$ for all $a, b \in R$,*

(vi) *$(-a)(-b) = ab$ for all $a, b \in R$,*

(vii) *for all $a, b, x \in R$, $a + x = b + x \implies a = b$,*

(viii) *$a(b - c) = ab - ac$ for all $a, b, c \in R$,*

(ix) *$-(a + b) = -a - b$ and $-(a - b) = -a + b$ for all $a, b \in R$,*

(x) *if R is a unital ring, then $1 \in R$ is unique,*

(xi) *if R is a unital ring, then $(-1)a = a(-1) = -a$ for all $a \in R$ and $(-1)(-1) = 1$,*

(xii) *if R is a division ring, then given $a \in R$, the inverse a^{-1} is unique,*

(xiii) *if R is a division ring, then $(ab)^{-1} = b^{-1}a^{-1}$ for all $a, b \in R$.*

Proof. We prove (i) as an example, the rest follow similarly from the axioms by straightforward arguments.

Suppose 0 is not unique, i.e., there are $0, 0' \in R$ such that $a + 0 = 0 + a = 0$ and $a + 0' = 0' + a = 0'$ for all $a \in R$, and $0 \neq 0'$. In particular, $0 = 0 + 0' = 0'$, i.e., $0 = 0'$, a contradiction. □

Examples 1.2. We give some examples of rings.

(i) $(\{0\}, +, \cdot)$ where $0 + 0 \stackrel{\text{def}}{=} 0$ and $0 \cdot 0 \stackrel{\text{def}}{=} 0$ is a trivial example of a ring, and is also a field. This is usually called the zero ring, denoted by 0.

(ii) The set $\mathbb{Z}$ of integers with usual addition and multiplication is a commutative unital ring. It is not a division ring since only ± 1 have multiplicative inverses.

(iii) Let n be a positive integer. Then the set $n\mathbb{Z}$ with the usual addition and multiplication is a commutative ring, but is not unital when $n \neq 1$.

(iv) The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$, each equipped with their usual addition and multiplication operations, are examples of fields.

(v) The set $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ with addition and multiplication modulo 5 is a field.

(vi) The set $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with addition and multiplication modulo 6 is a commutative unital ring, but *not* a field (e.g. $2 \in \mathbb{Z}_6$ has no multiplicative inverse).

(vii) The set $\mathbb{Q}^{2\times 2}$ of 2×2 matrices with entries in $\mathbb{Q}$ equipped with the usual addition and multiplication of matrices is a ring with $1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, but it is not a commutative nor a division ring (e.g. $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ has no inverse).

(viii) The set $\mathbb{R}[x]$ of polynomials in x with coefficients in $\mathbb{R}$, equipped with the usual addition and multiplication of polynomials, is a commutative unital ring (1 is the polynomial $p(x) = 1$), but it is not a division ring.

(ix) The set $C(\mathbb{R})$ of continuous functions from $\mathbb{R}$ to $\mathbb{R}$ with addition $f+g$ and multiplication fg defined by $(f+g)(x) \stackrel{\text{def}}{=} f(x)+g(x)$ and $(fg)(x) \stackrel{\text{def}}{=} f(x)g(x)$ for all $x \in \mathbb{R}$ is a commutative ring but not a division ring (not all continuous functions have a multiplicative inverse in $C(\mathbb{R})$).

1.1 Ideals and Homomorphisms

Let R be a ring, and let $S \subseteq R$ be a non-empty subset. Then the set S is said to be a *subring* of R if $(S, +_R \restriction S, \cdot_R \restriction S)$ is a ring.

Proposition 1.3. *Let R be a ring, and let $\emptyset \neq S \subseteq R$. Then S is a subring if and only if $a - b, ab \in S$ for all $a, b \in S$.*

Proof. The necessary condition is obvious, we prove the sufficient condition. Pick $b \in S$. Then $b - b = 0 \in S$, so we have the additive identity in S. Consequently, we also have $0 - b = -b \in S$, which gives additive inverses by the arbitrariness of b. Finally, for any $a \in S$, we have $a - (-b) = a + b \in S$, so we have closure under addition. Closure under multiplication is given, and the remaining ring properties are hereditary so S inherits them. □

Definition 1.4 (Ideal)**.** Let R be a ring, and let $\mathfrak{a}$ be a subring of R. Then $\mathfrak{a}$ is said to be a *right ideal* of R, denoted by $\mathfrak{a} \lhd_r R$, if $\mathfrak{a}$ absorbs all right products with its elements, i.e., $\mathfrak{a}r \subseteq \mathfrak{a}$ for all $r \in R$.

Similarly, $\mathfrak{a}$ is said to be a *left ideal* of R, denoted by $\mathfrak{a} \lhd_\ell R$, if $\mathfrak{a}$ absorbs all left products with its elements, i.e., $r\mathfrak{a} \subseteq \mathfrak{a}$ for all $r \in R$.

The subring $\mathfrak{a}$ is said to be a *two-sided ideal*, or simply, an *ideal*, denoted by $\mathfrak{a} \lhd R$, if both $\mathfrak{a} \lhd_r R$ and $\mathfrak{a} \lhd_\ell R$.

Examples 1.5. (i) Trivially, $\{0\} \lhd R$ and $R \lhd R$.

(ii) Let n be a positive integer. Then $n\mathbb{Z}$ is an ideal of the ring $\mathbb{Z}$.

(iii) The set of all polynomials in $\mathbb{R}[x]$ which are divisible by $x^2 + 1$ is an ideal of $\mathbb{R}[x]$.

(iv) The set of all functions f in $C(\mathbb{R})$ such that $f(0) = 0$ is an ideal of $C(\mathbb{R})$.

(v) Consider the set $R = \{0, 1\} \times \{0, 1\}$, with operations $(a, b) +_R (c, d) \stackrel{\text{def}}{=} (a+c, b+d)$ and $(a, b) \cdot_R (c, d) \stackrel{\text{def}}{=} (ac, bd)$ modulo 2. It is straightforward to check that this is a commutative ring with $1_R = (1, 1)$. The subset $S = \{(0, 0), (1, 1)\}$ is a subring but not an ideal, since $(1, 0) \cdot (1, 1) = (1, 0) \notin S$.

Let R be a ring and let $\mathfrak{a} \lhd R$. A *coset* is a subset of R of the form $x + \mathfrak{a}$ for some $x \in R$. In particular, $x + \mathfrak{a}$ is called the coset of x in R with respect to $\mathfrak{a}$. It is straightforward to check that two cosets $x + \mathfrak{a}$ and $y + \mathfrak{a}$ are equal if and only if $x - y \in \mathfrak{a}$, and that this is an equivalence relation on R with the distinct cosets being the corresponding equivalence classes. The set of all cosets of R with respect to an ideal $\mathfrak{a}$ is denoted by $R/\mathfrak{a}$, i.e.,

$$R/\mathfrak{a} = \{x + \mathfrak{a} : x \in R\}.$$

We can make this into a ring as follows. Define addition and multiplication by $(x + \mathfrak{a}) +_{R/\mathfrak{a}} (y + \mathfrak{a}) \stackrel{\text{def}}{=} (x + y + \mathfrak{a})$ and $(x + \mathfrak{a}) \cdot_{R/\mathfrak{a}} (y + \mathfrak{a}) \stackrel{\text{def}}{=} (xy + \mathfrak{a})$. It is a good exercise to check that these operations are well-defined, i.e., they are not dependent on which x and y are chosen to represent the corresponding coset.

Definition 1.6 (Quotient ring)**.** Let R be a ring, and let $\mathfrak{a} \triangleleft R$. The ring $R/\mathfrak{a}$ with the operations described above is called the *quotient ring of R modulo $\mathfrak{a}$*.

The zero element of $R/\mathfrak{a}$ is $0_R+\mathfrak{a} = \mathfrak{a}$, and if R has 1, then the multiplicative identity of $R/\mathfrak{a}$ is $1_R + \mathfrak{a}$.

Proposition 1.7. *Let R be a ring and let $\mathfrak{a} \triangleleft R$. Then $\mathfrak{b}^* \triangleleft R/\mathfrak{a}$ if and only if $\mathfrak{b}^* = \mathfrak{b}/\mathfrak{a}$ for some $\mathfrak{a} \subseteq \mathfrak{b} \triangleleft R$.*

Proof. If $\mathfrak{b}^* \triangleleft R/\mathfrak{a}$, define $\mathfrak{b} \stackrel{\text{def}}{=} \{x \in R : x + \mathfrak{a} \in \mathfrak{b}^*\}$. Then

$$\mathfrak{b}/\mathfrak{a} = \{x + \mathfrak{a} : x \in \mathfrak{b}\} = \{x + \mathfrak{a} : x \in R \text{ and } x + \mathfrak{a} \in \mathfrak{b}^*\} = \mathfrak{b}^*.$$

Conversely, if $\mathfrak{b}^* = \mathfrak{b}/\mathfrak{a}$ where $\mathfrak{a} \subseteq \mathfrak{b} \triangleleft R$, then

$$\begin{aligned} \mathfrak{b}^*(R/\mathfrak{a}) = \{(x + \mathfrak{a})(R/\mathfrak{a}) : x \in \mathfrak{b}\} &= \{xy + \mathfrak{a} : x \in \mathfrak{b} \text{ and } y \in R\} \\ &\subseteq \{z + \mathfrak{a} : z \in \mathfrak{b}\} \qquad (\mathfrak{b} \triangleleft R) \\ &= \mathfrak{b}^*, \end{aligned}$$

and similarly $(R/\mathfrak{a})\mathfrak{b}^* \subseteq \mathfrak{b}^*$, so $\mathfrak{b}^*$ is an ideal of $R/\mathfrak{a}$. □

Example 1.8. Let $R = \mathbb{Z}$ and $\mathfrak{a} = 6\mathbb{Z}$, so

$$R/\mathfrak{a} = \mathbb{Z}/6\mathbb{Z} = \{6\mathbb{Z}, 1 + 6\mathbb{Z}, 2 + 6\mathbb{Z}, 3 + 6\mathbb{Z}, 4 + 6\mathbb{Z}, 5 + 6\mathbb{Z}\}.$$

If we consider $\mathfrak{b}^* \stackrel{\text{def}}{=} \{6\mathbb{Z}, 2 + 6\mathbb{Z}, 4 + 6\mathbb{Z}\}$, it is not hard to see that $\mathfrak{b}^* \triangleleft R/\mathfrak{a}$. Indeed, if we take $\mathfrak{b}$ to be as in the proof, we get $\mathfrak{b} = \{x : x+6\mathbb{Z} \in \mathfrak{b}^*\} = 2\mathbb{Z}$. Indeed, $2\mathbb{Z}/6\mathbb{Z} = \{6\mathbb{Z}, 2 + 6\mathbb{Z}, 4 + 6\mathbb{Z}\} = \mathfrak{b}^*$.

Definition 1.9 (Homomorphism)**.** Let R and S be rings. A function $\phi\colon R \to S$ such that

$$\phi(x + y) = \phi(x) + \phi(y) \qquad \text{and} \qquad \phi(xy) = \phi(x)\phi(y)$$

for all $x, y \in R$ is said to be a *homomorphism* of R into S.

Examples 1.10. (i) The map $\phi\colon R \to S$ defined by $\phi(x) \stackrel{\text{def}}{=} 0_S$ for all $x \in R$ is trivially a homomorphism.

(ii) The identity $\iota\colon R \to S$ defined by $\iota(x) \stackrel{\text{def}}{=} x$ for all $x \in R$ is also a homomorphism.

(iii) $\phi\colon \mathbb{Z} \to \mathbb{Z}_n$ defined by $\phi(m) \stackrel{\text{def}}{=} m \bmod n$ is a homomorphism.

(iv) $\phi\colon \mathbb{C} \to \mathbb{C}$ defined by $\phi(z) \stackrel{\text{def}}{=} \bar{z}$ is a homomorphism.

(v) Let R be a ring, and $\mathfrak{a} \triangleleft R$. Then $\sigma\colon R \to R/\mathfrak{a}$ defined by $\sigma(x) \stackrel{\text{def}}{=} x + \mathfrak{a}$ for all $x \in R$ is a homomorphism from R onto $R/\mathfrak{a}$, called the *natural* (or sometimes *canonical*) *homomorphism*.

We can deduce some straightforward facts about homomorphisms.

Notation. Let R be a ring, and let $f\colon X \to R$ be a function. Then the set $\{x \in X : f(x) = 0\}$ is denoted by $\ker f$ and is called the *kernel* of f.

Proposition 1.11. *Let R, S be rings, and let $\phi\colon R \to S$ be a homomorphism. Then*

(i) $\phi(0_R) = 0_S$,

(ii) $\phi(-a) = -\phi(a)$ *for all* $a \in R$,

(iii) $\ker\phi \triangleleft R$,

(iv) $\operatorname{im}\phi$ *is a subring of* S,

(v) $\phi\colon R \hookrightarrow S$ *if and only if* $\ker\phi = \{0_S\}$.

Proof. We prove (i) as an example, the rest follow similarly by straightforward arguments.

Let $x \in R$. Then $\phi(x) = \phi(x+0) = \phi(x)+\phi(0)$, and similarly $\phi(x) = \phi(0)+\phi(x)$. Since 0_S is unique (proposition 1.1), it follows that $\phi(0) = 0_S$. □

Definition 1.12 (Isomorphism)**.** Let R, S be rings, and let $\phi\colon R \hookrightarrow\!\!\!\!\rightarrow S$ be a bijective homomorphism. Then ϕ is said to be an *isomorphism*, and the rings R and S are said to be *isomorphic*, denoted by $R \simeq S$.

Clearly $\simeq$ is an equivalence relation since the identity $\iota\colon R \to R$ is a bijective homomorphism from R to itself; if $\phi\colon R \to S$ is a bijective homomorphism, then so is $\phi^{-1}\colon S \to R$; and finally if $\phi\colon R \to S$ and $\varphi\colon S \to T$ are isomorphisms, then so is $\varphi \circ \phi\colon R \to T$.

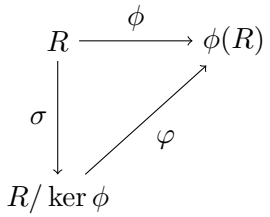

FIGURE 1: Diagram of the first isomorphism theorem, $\phi = \sigma \circ \varphi$

Example 1.13. $\mathbb{Z}_6 = \{0, \ldots, 5\}$ with addition and multiplication modulo 5 and $\mathbb{Z}/6\mathbb{Z}$ are isomorphic, with isomorphism $\phi(x) \stackrel{\text{def}}{=} x + 6\mathbb{Z}$.

In algebra, we work mainly up to isomorphism, i.e., algebraic structures which are isomorphic are considered equivalent for all intents and purposes, such as $\mathbb{Z}_6$ and $\mathbb{Z}/6\mathbb{Z}$ in example 1.13. Indeed, the difference between isomorphic rings is superficial, in the sense that, even though their elements are different, the way they interact additively and multiplicatively is preserved. In this way, an isomorphism can be considered simply a "relabelling" of the elements of the ring.

1.2 The Isomorphism Theorems

Given a ring R, what are the possible homomorphic images of R, i.e., what are the possible rings $\phi(R)$ for different homomorphisms $\phi\colon R \to S$? Surely this would depend on the codomain S? Surprisingly, the answer to the last question is no: all the information about the image of R under a homomorphism is contained in R itself.

Theorem 1.14 (First isomorphism theorem)**.** *Let R be a ring, and let $\phi\colon R \to S$ be a homomorphism. Then $\phi(R) \simeq R/\ker\phi$.*

(Notice $R/\ker\phi$ exists by proposition 1.11.)

Proof. Define $\varphi\colon R/\ker\phi \to \phi(R)$ by $\varphi(x + \ker\phi) \stackrel{\text{def}}{=} \phi(x)$, which is well-defined since if $x + \ker\phi = y + \ker\phi$, then $x - y \in \ker\phi$, i.e., $\phi(x - y) = \phi(x) - \phi(y) = 0$, i.e., $\phi(x) = \phi(y)$. It is straightforward to check that φ is an isomorphism. □

The remaining two so-called "isomorphism theorems" are straightforward applications of the first isomorphism theorem.

Theorem 1.15 (Second isomorphism theorem)**.** *Let R be a ring with subring S and ideal $\mathfrak{a}$. Then*

$$S/(S \cap \mathfrak{a}) \simeq (S + \mathfrak{a})/\mathfrak{a}.$$

Proof. Let $\sigma\colon R \to R/\mathfrak{a}$ be the natural homomorphism $\sigma(x) \stackrel{\text{def}}{=} x + \mathfrak{a}$, and let $\sigma' \stackrel{\text{def}}{=} \sigma \restriction S$. Clearly σ' is also a homomorphism, with $\sigma'(S) = \sigma(S) = (S + \mathfrak{a})/\mathfrak{a}$ and $\ker \sigma' = S \cap \mathfrak{a}$. Apply the first isomorphism theorem. □

Theorem 1.16 (Third isomorphism theorem)**.** *Let R be a ring with ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that $\mathfrak{a} \subseteq \mathfrak{b}$. Then*

$$\frac{R/\mathfrak{a}}{\mathfrak{b}/\mathfrak{a}} \simeq R/\mathfrak{b}.$$

(Notice that $\mathfrak{b}/\mathfrak{a} \lhd R/\mathfrak{a}$ by proposition 1.7, so $(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$ exists.)

Proof. Define $\phi\colon R/\mathfrak{a} \to R/\mathfrak{b}$ by $\phi(x + \mathfrak{a}) \stackrel{\text{def}}{=} x + \mathfrak{b}$. It is easy to check that ϕ is a well-defined homomorphism, with $\ker \phi = \mathfrak{b}/\mathfrak{a}$. Apply the first isomorphism theorem. □

1.3 Special Kinds of Rings

In a ring R, a *divisor of zero* is an element $x \neq 0$ such that $xy = 0$ for some $y \neq 0$. A ring with no divisors of zero is called a *domain*. If, in addition, the ring is commutative, then we call it an *integral domain*.

Examples 1.17. (i) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all integral domains. On the other hand, $\mathbb{Z}_6 = \{0, \ldots, 5\}$ is not a domain, since $2 \cdot 3 = 0$.

(ii) The set $\mathbb{Q}^{2\times 2}$ of 2×2 matrices with entries in $\mathbb{Q}$ is not a domain, since e.g., $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -1 \\ -1 & 1 \end{smallmatrix}\right) = 0$.

(iii) The set $\mathbb{H}$ (after Hamilton), called the set of *quaternions*, is a number system which generalises of the complex numbers, with three imaginary units i, j, and k rather than one, so that each $z \in \mathbb{H}$ is of the form $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{R}$. The behaviour of these new units is characterised by the equations

$$i^2 = j^2 = k^2 = ijk = -1.$$

In particular, $\mathbb{H}$ is not commutative (e.g., $ij = -ji$). It is an example of a domain which is not an integral domain.

Proposition 1.18. *Every field is an integral domain.*

Proof. Let k be a field, let $a, b \in k$ be non-zero and suppose $ab = 0$. Then a^{-1} exists, so we can divide by a to get that $b = 0$, a contradiction. □

Proposition 1.19. *Every finite integral domain is a field.*

Proof. Let R be a finite integral domain, and for all $b \in R$, define $\phi_b \colon R \to R$ by $\phi_b(a) \stackrel{\text{def}}{=} ab$. It is easy to check that because R is finite, ϕ_b is a bijection for all b. Now for each $b \in R$, define $1_b \stackrel{\text{def}}{=} {\phi_b}^{-1}(b)$. It is easy to see that $1_b b = b 1_b = b$, and that in fact, $1_b = 1_c$ for any $b, c \in R$ (so $1 \stackrel{\text{def}}{=} 1_b$ does not actually depend on b). Next, for each $b \in R$, define $b^{-1} \stackrel{\text{def}}{=} {\phi_b}^{-1}(1)$. It is easy to see that $bb^{-1} = b^{-1}b = 1$. Thus we have identity and inverses, so R is a field. □

For $n \in \mathbb{N}$, let nx denote

$$\underbrace{x + \cdots + x}_{n \text{ times}}.$$

Then the *characteristic* of a ring R is the smallest $n \in \mathbb{N}$ such that $nx = 0$ for all $x \in R$. If such an n exists, we say R has *finite characteristic* and denote it by $\operatorname{char}(R) = n$. In no such n exists, we say that R has *characteristic zero*, and write $\operatorname{char}(R) = 0$.

Proposition 1.20. *Let R be a unital integral domain. Then* $\operatorname{char}(R)$ *is* 0 *or prime.*

Proof. Suppose R has finite characteristic, and for contradiction, suppose $\operatorname{char}(R) = nm$ with $n, m \geqslant 2$. Then for all $x \in R$,

$$0 = (nm)x = (n1)(mx) = 0.$$

□

1.4 Modules

A module is a generalisation of the notion of a vector space over some field, where we instead draw scalars from a ring.

Definition 1.21 (Module)**.** Let R be a ring, let $(M, +)$ be an abelian group, and let $\circ : M \times R \to M$ be an operation called *scalar multiplication* satisfying the following properties for all $x, y \in M$ and

$r, s \in R$:

(i) $(x + y) \circ r = x \circ r + y \circ r$, (RING ELEMENT DISTRIBUTIVITY)

(ii) $x \circ (r +_R s) = x \circ r + x \circ s$, (SCALAR DISTRIBUTIVITY)

(iii) $x \circ (rs) = (x \circ r) \circ s$. (SCALAR ASSOCIATIVITY)

Then M is called a *right R-module*.

A *left R-module* is defined analogously, with ring elements multiplied on the left rather than on the right.

Notation. Just as we do with ring multiplication, we relax the notation $x \circ r$ to xr, since it is always evident from context which of the two product is being used.

We will write M_R to show that M is a right R-module, and similarly ${}_RM$ to show that M is a left R-module. We will work mainly with right modules, but most results can be adapted to left modules.

Examples 1.22. (i) Every abelian group G is a left $\mathbb{Z}$-module. Indeed, if we define scalar multiplication by

$$ng \stackrel{\text{def}}{=} \begin{cases} \underbrace{g + \cdots + g}_{n \text{ times}} & \text{if } n \geqslant 1 \\ 0_G & \text{if } n = 0 \\ \underbrace{-g - \cdots - g}_{-n \text{ times}} & \text{if } n < 0, \end{cases}$$

it is clear that all the properties hold.

(ii) If we take $M = R$, any ring is trivially a right (or left) R-module over itself, where scalar multiplication is the same as multiplication in R. Moreover, if we take a right ideal $\mathfrak{a} \triangleleft_r R$, this is a right R-module with the same product as R. Similarly, $\mathfrak{b} \triangleleft_\ell R$ is a left R-module.

(iii) Any vector space $V(k)$ over a field k is a left k-module, where scalar multiplication is defined as usual.

(iv) Let R be a ring, and consider the set $M = R^{n \times n}$ of $n \times n$ matrices

with entries from R. Then M is a left R-module if we define

$$rA \overset{\text{def}}{=} \begin{pmatrix} r & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & r \end{pmatrix} A = (r\delta_{ij})_{n\times n} A.$$

Some straightforward properties of modules which follow from the definition:

Proposition 1.23. *Let M be a right R-module. Then for all $r \in R$ and $x \in M$:*

(i) $0_M r = 0_M$,

(ii) $x0_R = 0_M$,

(iii) $(-x)r = x(-r) = -xr$.

Proof. As usual, we prove (i) and leave the rest as exercises.

Indeed, for all $x \in M$, $xr = (x + 0_M)r = xr + 0_M r$, and by uniqueness of the additive identity in a group, $0_M r = 0_M$ follows. □

Definition 1.24 (Unital)**.** Let R be a unital ring, and let M be a right R-module. Then M is said to be *unital* if $1x = x$ for all $x \in M$.

Example 1.25. A unital module over a field k is the same as a k-vector space.

As with rings and vector spaces, we have the notion of a corresponding substructure. A non-empty subset $S \subseteq M_R$ of a right R-module M is said to be a *submodule of M* if S is itself a right R-module of M with the inherited scalar multiplication. An analogous definition applies to left R-modules.

Example 1.26. In view of examples 1.22(iii), we see that every right ideal of a ring R is a submodule of R_R and every left ideal is a submodule of ${}_R R$.

We also state a criteron for submodules in the vein of proposition 1.3.

Proposition 1.27. *Let M_R be a module, and let $\emptyset \neq S \subseteq M_R$. Then S is a submodule of R if and only if $x - y, xr \in S$ for all $x, y \in S$ and $r \in R$.*

The proof is analogous.

Now we go to the notion of quotients of modules. Observe that by definition, a right R-module M is an abelian group. In particular, any submodule S of

M_R is a normal subgroup, so we may form the quotient group M_R/S. This quotient can in turn be made into an R-module by defining

$$(x+S)r \stackrel{\text{def}}{=} xr + S$$

for all $x \in M_R$ and $r \in R$. We leave it as an exercise to check that this is well-defined and that this definition of scalar multiplication does indeed make M_R/S a right R-module. (We define quotients for left R-modules similarly.)

Next we go to the notion of homomorphisms of modules.

Definition 1.28 (Homomorphism)**.** Let M and N be two right R-modules. A function $\phi\colon M \to N$ such that

$$\phi(x+y) = \phi(x) + \phi(y) \qquad \text{and} \qquad \phi(xr) = \phi(x)r$$

for all $x, y \in M$ and $r \in R$ is said to be an *R-homomorphism* of M into N.

Homomorphisms for left R-modules are defined analogously. Just as with homomorphisms of rings, we have the properties outlined in the following proposition.

Proposition 1.29. *Let M, N be right R-modules, and let $\phi\colon M \to N$ be an R-homomorphism. Then*

(i) $\phi(0_M) = 0_N$,

(ii) $\phi(-x) = -\phi(x)$ *for all* $x \in M$,

(iii) $\ker\phi$ *is a submodule of* M,

(iv) $\operatorname{im}\phi$ *is a submodule of* N,

(v) $\phi\colon M \hookrightarrow N$ *if and only if* $\ker\phi = \{0_M\}$.

The proof is identical. We similarly have the notion of R-isomorphism, i.e., a bijective R-homomorphism. If $\phi\colon M \xhookrightarrow{\sim} N$ is an R-isomorphism, we write $M \simeq N$ and say they are *isomorphic*.

Finally, we note that the isomorphism theorems can be adapted to modules, and that their proofs are straightforwardly adapted from those given in section 1.2.

Theorem 1.30 (Isomorphism theorems for modules)**.** *Let M be a right R-module. Then:*

I. *If N is a right R-module and $\phi\colon M \to N$ is an R-homomorphism, then $\phi(M) \simeq M/\ker\phi$.*

II. *If S, T are submodules of M, then $(S+T)/T \simeq S/(S\cap T)$.*

III. *If S, T are submodules of M and $S \subseteq T$, then $(M/S)/(T/S) \simeq M/T$.*

The corresponding theorems for left R-modules are identical.

1.5 Direct Sums and Set Products

Let $\mathscr{A} = \{\mathfrak{a}_\gamma : \gamma \in \Gamma\}$ be an arbitrary collection of ideals of a ring R. Their *sum*, denoted by $\sum \mathscr{A}$ or $\sum_{\gamma\in\Gamma} \mathfrak{a}_\gamma$, is the set

$$\textstyle\sum \mathscr{A} \stackrel{\text{def}}{=} \{\sum_{\gamma\in\Gamma'} a_\gamma : a_\gamma \in \mathfrak{a}_\gamma,\ \Gamma' \subseteq \Gamma \text{ and } |\Gamma'| < \infty\},$$

i.e., the set of all possible *finite* sums of members of the $\mathfrak{a}_\gamma$'s. If the index set Γ is finite, equal to $\{1,\dots,n\}$ say, then this is just $\mathfrak{a}_1 + \cdots + \mathfrak{a}_n$, coinciding with ordinary addition of sets.

Definition 1.31 (Direct sum)**.** The sum $\sum \mathscr{A}$ is said to be an (*internal*) *direct sum* if for each $x \in \sum \mathscr{A}$, there is precisely one way to write $x = a_1 + \cdots + a_n$ with each $a_i \in \mathfrak{a}_{\gamma_i}$ for some $\{\gamma_1,\dots,\gamma_n\} \subseteq \Gamma$. If the sum is direct, it is denoted by $\bigoplus \mathscr{A}$ or $\bigoplus_{\gamma\in\Gamma} \mathfrak{a}_\gamma$, and if Γ is finite, equal to $\{1,\dots,n\}$ say, we write $\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$.

An important result which allows us to determine when a sum is direct is the following.

Proposition 1.32. *Let $\mathscr{A} = \{\mathfrak{a}_\gamma : \gamma \in \Gamma\}$ be an arbitrary collection of ideals of a ring R. Then $\sum \mathscr{A}$ is direct if and only if*

$$\mathfrak{a}_{\gamma_0} \cap \Big(\sum_{\substack{\gamma\in\Gamma\\ \gamma\neq\gamma_0}} \mathfrak{a}_\gamma\Big) = \{0\}$$

for all $\gamma_0 \in \Gamma$.

Proof. Suppose $\sum \mathscr{A}$ is direct, and fix $\gamma_0 \in \Gamma$. Clearly $0 \in \mathfrak{a}_\gamma$ for all $\gamma \in \Gamma$ since they are ideals, therefore $0 \in \mathfrak{a}_{\gamma_0} \cap (\sum_{\gamma\neq\gamma_0} \mathfrak{a}_\gamma)$. Now suppose $x \in \mathfrak{a}_{\gamma_0} \cap (\sum_{\gamma\neq\gamma_0} \mathfrak{a}_\gamma)$, and $x \neq 0$. Then x can be expressed as the "sum" $x = a_0$

where $a_0 \stackrel{\text{def}}{=} x$ and (trivially) each $a_i \in \mathfrak{a}_{\gamma_i}$ for some i (namely $i = 0$), but also as some different finite sum of terms $x = a_1 + \cdots + a_n$ where each $a_i \in \mathfrak{a}_{\gamma_i}$ since $x \in \sum_{\gamma \neq \gamma_0} \mathfrak{a}_\gamma$, contradicting that the sum is direct. It follows that $\mathfrak{a}_{\gamma_0} \cap (\sum_{\gamma \neq \gamma_0} \mathfrak{a}_\gamma) = \{0\}$, and $\gamma_0 \in \Gamma$ was arbitrary.

Conversely, if we have $\mathfrak{a}_{\gamma_0} \cap (\sum_{\gamma \neq \gamma_0} \mathfrak{a}_\gamma) = \{0\}$ for every $\gamma_0 \in \Gamma$, suppose $x \in \sum \mathscr{A}$ can be expressed as a finite sum in two different ways, $x = \sum_{\gamma \in \Gamma_1} a_\gamma$ and $x = \sum_{\gamma \in \Gamma_2} b_\gamma$ where each $a_\gamma, b_\gamma \in \mathfrak{a}_\gamma$ and both $\Gamma_1, \Gamma_2 \subseteq \Gamma$ are finite. Define $a_\gamma \stackrel{\text{def}}{=} 0$ for $\gamma \in \Gamma_2 \smallsetminus \Gamma_1$, and similarly $b_\gamma \stackrel{\text{def}}{=} 0$ for $\gamma \in \Gamma_1 \smallsetminus \Gamma_2$. Then

$$x = \sum_{\gamma \in \Gamma'} a_\gamma = \sum_{\gamma \in \Gamma'} b_\gamma \implies \sum_{\gamma \in \Gamma'} (a_\gamma - b_\gamma) = 0$$

where $\Gamma' = \Gamma_1 \cup \Gamma_2$. Now $a_\gamma - b_\gamma \in \mathfrak{a}_\gamma$ for all $\gamma \in \Gamma'$. Pick $\gamma_0 \in \Gamma'$, then

$$\mathfrak{a}_{\gamma_0} \ni a_{\gamma_0} - b_{\gamma_0} = \sum_{\gamma \in \Gamma' \smallsetminus \{\gamma_0\}} (a_\gamma - b_\gamma) \in \sum_{\gamma \in \Gamma' \smallsetminus \{\gamma_0\}} \mathfrak{a}_\gamma \subseteq \sum_{\gamma \neq \gamma_0} \mathfrak{a}_\gamma,$$

which implies that $a_{\gamma_0} = b_{\gamma_0}$. Since γ_0 was arbitrary, we have that $a_\gamma = b_\gamma$ for all $\gamma \in \Gamma'$, so the "two ways" of writing x as a sum are the same, a contradiction. □

Let $\mathscr{R} = \{R_\gamma : \gamma \in \Gamma\}$ be an arbitrary collection of rings. The (*external*) *direct sum* of the rings in $\mathscr{R}$ is the set

$$\bigoplus \mathscr{R} = \bigoplus_{\gamma \in \Gamma} R_\gamma \stackrel{\text{def}}{=} \{(r_\gamma)_{\gamma \in \Gamma} : r_\gamma \in R_\gamma\}$$

of "sequences" where the γ component is in R_γ. If Γ is finite, equal to $\{1, \ldots, n\}$ say, we write $R_1 \oplus \cdots \oplus R_n$. Defining addition and multiplication on R component-wise, we get that R is a ring. Moreover, we see that the set $\mathfrak{a}_{\gamma_0} \stackrel{\text{def}}{=} \{(r_\gamma)_{\gamma \in \Gamma} : r_{\gamma_0} \in R_{\gamma_0}$ and $r_\gamma = 0$ for $\gamma \neq \gamma_0\}$ is an ideal of R isomorphic to R_{γ_0} (by projection). It is not hard to see that R is the internal direct sum of these $\mathfrak{a}_\gamma$'s.

Conversely, any internal direct sum $\bigoplus_{\gamma \in \Gamma} \mathfrak{a}_\gamma$ can be seen as the external direct sum of the rings $\mathfrak{a}_\gamma$. Therefore, in practice, there is no need to distinguish between the two kinds of direct sums—this is why we use the same notation!

In an analogous way, we define the internal/external direct sums of modules in the following way. Let $\mathcal{S} = \{S_\gamma : \gamma \in \Gamma\}$ be an arbitrary collection of

submodules of a right R-module M. Their *sum*, denoted by $\sum \mathcal{S}$ or $\sum_{\gamma\in\Gamma} S_\gamma$, is the set

$$\sum \mathcal{S} \stackrel{\text{def}}{=} \{\textstyle\sum_{\gamma\in\Gamma'} x_\gamma : x_\gamma \in S_\gamma,\ \Gamma' \subseteq \Gamma \text{ and } |\Gamma'| < \infty\},$$

i.e., the set of all possible *finite* sums of members of the S_γ's. It is straightforward to check that this is a submodule of M. The sum $\sum \mathcal{S}$ is said to be an (*internal*) *direct sum* if for each $x \in \sum \mathcal{S}$, there is precisely one way to write $x = x_1 + \cdots + x_n$ with each $x_i \in S_{\gamma_i}$ for some $\{\gamma_1, \ldots, \gamma_n\} \subseteq \Gamma$. If the sum is direct, it is denoted by $\bigoplus \mathcal{S}$ or $\bigoplus_{\gamma\in\Gamma} S_\gamma$, and if Γ is finite, equal to $\{1, \ldots, n\}$ say, we write $S_1 \oplus \cdots \oplus S_n$.

An analogous result to proposition 1.32 holds here:

Proposition 1.33. *Let $\mathcal{S} = \{S_\gamma : \gamma \in \Gamma\}$ be an arbitrary collection of submodules of a right R-module M. Then $\sum \mathcal{S}$ is direct if and only if $S_{\gamma_0} \cap (\sum_{\gamma\neq\gamma_0} S_\gamma) = \{0\}$ for all $\gamma_0 \in \Gamma$.*

The external direct product of a collection $\mathscr{M} = \{M_\gamma : \gamma \in \Gamma\}$ of right R-modules is the set $\bigoplus \mathscr{M} = \bigoplus_{\gamma\in\Gamma} M_\gamma \stackrel{\text{def}}{=} \{(x_\gamma)_{\gamma\in\Gamma} : x_\gamma \in M_\gamma\}$. This can be made into a right R-module by defining addition and scalar multiplication component-wise.

Analogously to rings, the internal and external direct sums of modules are isomorphic, so there is no need to make any notational distinction between them.

Now we discuss the product of subsets.

Definition 1.34 (Product of Sets)**.** Let M be a right R-module, let $N \subseteq M$ and $T \subseteq R$. Then the *product* of these sets is denoted by NT and is defined

$$NT \stackrel{\text{def}}{=} \{ \sum_{\substack{n\in N'\\ t\in T'}} nt : N' \subseteq N,\ T' \subseteq T \text{ and } |N|, |T| < \infty\}.$$

In particular, NT is not simply $\{nt : n \in N, t \in T\}$, but the set of *all finite sums* of terms of this form, so that we always have closure under addition.

Observe that if $\mathfrak{a} \lhd_r R$, then $N\mathfrak{a}$ is a submodule of M_R.

If, in particular, we put $M = R$, the definition also applies, so for $S, T \subseteq R$, we have $ST = \{s_1t_1 + \cdots + s_nt_n : s_i \in S, t_i \in T\}$. Moreover, for $S \subseteq R$, we

use the notation S^n for the set $\{\sum_{j=1}^{n} s_{1,j} \cdots s_{n,j} : s_{i,j} \in S \text{ and } n \in \mathbb{N}\}$, i.e., all possible finite sums of products of n terms from S.[2]

Remark 1.35. Let M be a right R-module, and let $\mathfrak{a} \lhd R$. In general, M might not be a right $R/\mathfrak{a}$-module, but it can be given a right $R/\mathfrak{a}$ structure if the product $M\mathfrak{a} = \{0\}$. In this case, define scalar multiplication by

$$xr = x(r + \mathfrak{a})$$

for all $x \in M$, $r \in R$. It is easy to check that this is an $R/\mathfrak{a}$-module, and that by this definition, the submodules of M as an R-module and as an $R/\mathfrak{a}$-module are the same.

An important instance of this is $\mathfrak{a}^{n+1}/\mathfrak{a}^n$, which is a right R-module.

1.6 Endomorphism Rings

Let M be a right R-module. A homomorphism $\phi\colon M \to M$ is said to be an *R-endomorphism*. The set $\{\phi \in M^M : \phi \text{ is an } R\text{-endomorphism}\}$ of all R-endomorphisms of M is denoted by $\mathrm{End}_R(M)$, or just $\mathrm{End}(M)$.

If for $\phi, \varphi \in \mathrm{End}(M)$, we define $\phi + \varphi$ by $(\phi + \varphi)(x) \stackrel{\text{def}}{=} \phi(x) + \varphi(x)$ and $\phi\varphi$ by $(\phi\varphi)(x) \stackrel{\text{def}}{=} \phi(x)\varphi(x)$, it is not hard to see that $\mathrm{End}(M)$ is a ring with these operations. Also, if $M_1 \simeq M_2$ as modules, then $\mathrm{End}(M_1) \simeq \mathrm{End}(M_2)$ as rings.

Proposition 1.36. *Let R be a ring with 1. Then $R \simeq \mathrm{End}(R_R)$.*

Proof. Associate each $x \in R$ with the map $\lambda_x\colon R \to R$ defined by $\lambda_x(r) = xr$ for all $r \in R$. It is straightforward to check that $\lambda_x \in \mathrm{End}(R)$ for all $x \in R$, and that $\Phi\colon R \to \mathrm{End}_R(R)$ defined by $\phi(x) = \lambda_x$ is a ring isomorphism. □

Remark 1.37. The above proposition is where our decision to work with right modules, write the maps on the left and follow the natural order of composition of maps has come into play. Viewing R as a left module, we obtain

$$R^{\mathrm{op}} \simeq \mathrm{End}({}_R R),$$

as rings. Whether one opts to work with R or R^{op} is a matter of choice and taste. If we wish to work with left modules while writing our maps on the left but still want to avoid R^{op} then a way out is as follows: define the

[2] Not to be confused with Cartesian product of sets which, if need be, will be written explicitly as $S \times S$.

product $\phi\psi$ by $(\phi\psi)(r) = \psi(\phi(r))$ for all $r \in R$. (This is the same as writing the maps on the right and following the natural order.) You will find in the literature that some people make this choice as well.

1.7 Order

Let X be a set with a binary relation $\prec \subseteq X \times X$ such that

(i) if $a \prec b$ and $b \prec c$, then $a \prec c$ for all $a, b, c \in X$,

(ii) for all $a, b \in X$, there exists $c \in X$ such that $a \prec c$ and $b \prec c$.

In other words, $\prec$ is transitive, and every pair of elements has an upper bound. Then X is said to be a *directed* set.

Now, let Y be a set with a binary relation $\preccurlyeq \subseteq Y \times Y$ such that for all $a, b, c \in Y$,

(i) $a \preccurlyeq a$,

(ii) if $a \preccurlyeq b$ and $b \preccurlyeq a$, then $a = b$,

(iii) if $a \preccurlyeq b$ and $b \preccurlyeq c$, then $a \preccurlyeq c$.

In other words, $\preccurlyeq$ is reflexive, antisymmetric and transitive. Then X is said to be a *partially ordered* set, or a *poset*.

Let Y be a poset, and let $A \subseteq Y$. If $u \in Y$ satisfies $a \preccurlyeq u$ for all $a \in A$, then u is said to be an *upper bound* of A. If u is such that $u \preccurlyeq u'$ for all upper bounds $u' \in Y$ of B, then u is said to be the *supremum* of B, denoted $\sup B$. Similarly, if $\ell \preccurlyeq a$ for all $a \in A$, then ℓ is said to be a *lower bound* of A. If ℓ is such that $\ell' \preccurlyeq \ell$ for all lower bounds $\ell' \in Y$ of A, then ℓ is said to be the *infimum* of B, denoted $\inf B$. It is straightforward to check that if they exist, suprema and infima are uniquely determined.

Let Y be a poset. If any subset $\{x, y\} \subseteq Y$ has a supremum and an infimum, then Y is said to be a *lattice*.

Examples 1.38. (i) The set $\mathbb{Z}$ with the usual order $\leqslant$ is a lattice.

(ii) The set $D = \{[-a, a] \times [-b, b] : a, b \in \mathbb{R}\} \subseteq \mathbb{R}^2$ of rectangles in the Euclidean plane centred at the origin is a directed set with the order $\subseteq$.

(iii) Let X be any set, and consider the power set $\wp X$ ordered by $\subseteq$. We have $\sup\{A, B\} = A \cup B$ and $\inf\{A, B\} = A \cap B$.

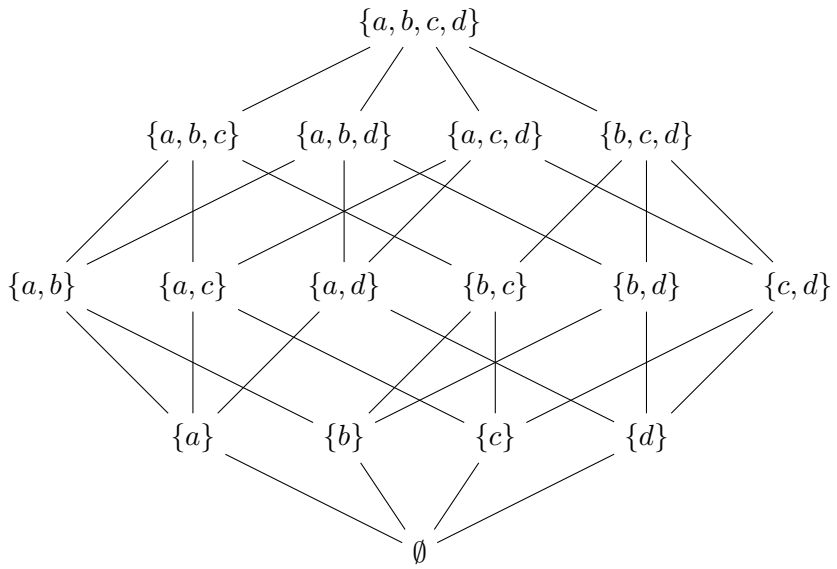

FIGURE 2: Hasse diagram for the lattice $(\wp\{a, b, c, d\}, \subseteq)$.

(iv) Let $n \in \mathbb{N}$, and consider the set D of divisors of n. Then D is a lattice with the order $\mid$ (divides).

Lattices are often visualised using *Hasse* diagrams, see figures 2 and 3 for examples. If you pick any two elements on the same storey of the diagram, the two common edges emanating upward give the supremum, and the two common edges emanating downward give the infimum.

Let X be a partially ordered set. The reason we say X is "partially" ordered is because some elements are not *comparable* (in the Hasse diagram, these are elements on the same "storey"). Two elements $a, b \in X$ are said to be comparable if either $a \preccurlyeq b$ or $b \preccurlyeq a$. If any two elements in a poset are comparable, then the set is said to be *totally ordered*.

Let $m \in A \subseteq X$, where X is a poset. If $m \preccurlyeq a$ implies that $a = m$ for all $a \in A$, then a is said to be a *maximal element* of A.

Theorem 1.39 (Zorn's Lemma)**.** *Let A be a non-empty, partially ordered set. If every totally ordered subset of A has a supremum, then A has a maximal element.*

This important result will be used throughout the course, but we will not prove it here. It turns out that this result is equivalent to (i.e., implies and

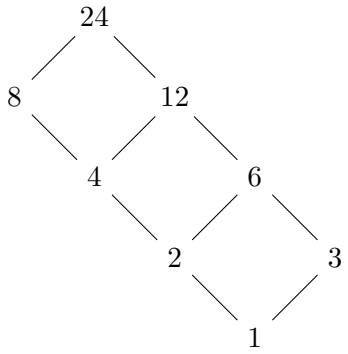

FIGURE 3: Hasse diagram for the lattice of divisors of 24 $(\{1, 2, 3, 4, 6, 8, 12, 24\}, \mid)$.

is implied by) the axiom of choice.

2 Chain Conditions

Let M be a right R-module, and let $\emptyset \neq T \subseteq M$. Then the smallest submodule of M containing T (with respect to inclusion) is said to be the *submodule of M generated by T*. In other words, it is the intersection of all submodules containing T.

By convention, the smallest submodule generated by $\emptyset$ is $\{0\}$.

If a submodule is generated by a singleton set $\{a\}$, then we say it is a *cyclic submodule*. In this case, the submodule equals $\{ar + \lambda a : r \in R \text{ and } \lambda \in \mathbb{Z}\}$, which is the same as aR if R has 1 and M is unital.

2.1 Finiteness Assumption