ALGEBRA 1

Concrete Abstract Algebra: From Numbers to Gröbner Bases

Niels Lauritzen

Contents

1 Numbers

1.1 Natural numbers and integers

In order to construct our number system, we define the natural numbers, $\mathbb{N}$, and the integers, $\mathbb{Z}$, where

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$$
$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

implying that $\mathbb{N} \subset \mathbb{Z}$. In order to construct these as ordered sets, we define the greater than- or equal and greater than operator, let $X, Y \in \mathbb{Z}$ then we define

$$X \leq Y \iff X - Y \in \mathbb{N} \quad \text{and} \quad X < Y \iff X \neq Y \text{ and } X \leq Y$$

Giving us the usual number ordering

$$\cdots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \cdots$$

Definition 1.1.1: First element

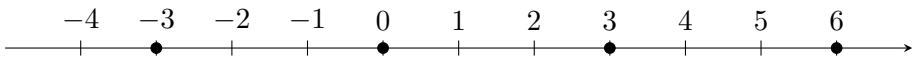
Let $s \in S$ where $S \subseteq \mathbb{Z}$, then s is the unique first element in S if $\forall x \in S, s \leq x$.

Example 1.1.1 Suppose that $S = \{1, 2, 3, 4, \ldots\}$, then $\forall x \in S, 1 \leq x$, making 1 the first element of the set.

It is immediately obvious that every nonempty subset of $\mathbb{N}$ must have a first element (due to it having a concrete lower bound), we call this property being well-ordered.

1.2 Modular arithmetic

Imagine that every multiple of 3 is marked on the axis of integers



then any integer can be expressed by the closest left multiple of 3 and the amount of you have to travel right to reach it. We call the amount you walk to the right the remainder following division by 3.

Example 1.2.1 Suppose we are observing multiples of 3, then

$$5 = 3 \times 1 + 2 \qquad 7 = 3 \times 2 + 1$$

As such 5 has remainder 2 with respect to 3 and and 7 has remainder 1 with respect to 3.

Theorem 1.2.1: Uniqueness of remainder

Let $d \in \mathbb{Z}$ where $d > 0$, then $\forall x \in \mathbb{Z}$ there exists a unique remainder $r \in \mathbb{N}$ such that

$$x = qd + r$$

where $q \in \mathbb{Z}$ and $0 \leq r < d$.

Proof. Assume that $x = q_1 d + r_1$ and $n = q_2 d + r_2$ where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 < d$ then

$$\begin{aligned} q_1 d + r_1 = q_2 d + r_2 &\implies q_1 d - q_2 d = r_2 - r_1 \\ &\implies d(q_1 - q_2) = r_2 - r_1 \end{aligned}$$

as we are assuming that $r_1 \neq r_2$, we let r_2 be larger than r_1, which implies that $r_2 - r_1 = md$ where $m = q_1 - q_2$, but this contradicts that $r_2 - r_1 \leq r_2 < d$. To prove the existence of r, we let $M = \{x - qd \mid q \in \mathbb{Z}\}$, then $M \cap \mathbb{N} \neq \emptyset$, whereby r must be the first element in $M \cap \mathbb{N}$, as such $\exists q, r = x - qd$, where $0 \leq r < d$. If $r \geq d$ then $r > r - d \geq 0$ and $r - d = x - (q+1)d \in M \cap \mathbb{N}$, contradicting that r is the first element in $M \cap \mathbb{N}$. □

Definition 1.2.1: Divisor

Suppose that $a = bc$ where $a, b, c \in \mathbb{Z}$, then we call c a divisor of a, which we write as $c \mid a$.

Definition 1.2.2: Remainder

If $x, d \in \mathbb{Z}$ where $d > 0$ we let $[x]_d$ be the unique remainder from Theorem 1.1.

1.3 Congruences

Definition 1.3.1: Congruence

Let $a, b, c \in \mathbb{Z}$ then a, b are called congruent modulo c if $c \mid b - a$, denoted $a \equiv b \mod c$, which can be simply stated as them having the same remainder when divided by c.

Proposition 1.3.1: Congruence

Let $c \in \mathbb{Z}$ where $c > 0$ then:

(i) $a \equiv [a]_c \mod c$

(ii) $a \equiv b \mod c \iff [a]_c = [b]_c$

for $a, b \in \mathbb{Z}$.

Proof. We know that $\exists q \in \mathbb{Z}, a = qc + [a]_c$ by Theorem 1.1, whereby

$$\begin{aligned} a = qc + [a]_c &\implies a - [a]_c = qc \\ &\implies c \mid a - [a]_c = qc \end{aligned}$$

proving (i). We now define $b = q'c + [b]_c$ for some $q' \in \mathbb{Z}$, then

$$a - b = (q - q')c + [a]_c - [b]_c$$

whereby $c \mid a - b \iff c \mid [a]_c - [b]_c$ which as $0 < [a]_c, [b]_c < c \implies [a]_c = [b]_c$ proving (ii). □

Example 1.3.1 The integers 29 and 14 can be written as $29 = 5 \times 5 + 4$ and $14 = 5 \times 2 + 4$, as they both have the same remainder

$$[29]_5 = [14]_5 = 4 \iff 29 \equiv 14 \mod 5$$

Proposition 1.3.2: Congruence of sum and product

Suppose that $x_1 \equiv x_2 \mod d$ and $y_1 \equiv y_2 \mod d$ then:

(i) $x_1 + y_1 \equiv x_2 + y_2 \mod d$

(ii) $x_1y_1 \equiv x_2y_2 \mod d$

for $x_1, x_2, y_1, y_2 \in \mathbb{Z}$.

Proof. Since d divides $x_1 - x_2$ and $y_1 - y_2$, it must also divide the sum of the two

$$d \mid x_1 - x_2 + y_1 - y_2 \implies d \mid x_1 + y_1 - (x_2 + y_2)$$

proving (i). Similarly we recognize that

$$x_1y_1 - x_2y_2 = x_1(y_1 - y_2) + y_2(x_1 - x_2)$$

And as x_1, y_2 are factors of terms we know to be divisible by d, so must their products be, and by (i) also their sum, proving (ii). □

Example 1.3.2 We wish to determine the remainder of 12^{11} divided by 21. We split the exponent using binary expansion

$$11 = 2^3 + 2^1 + 2^0 = 2^3 + 2 + 1$$

From this it follows that $\left[12^{11}\right] = \left[\left[12^{2^3}\right]\left[12^2\right]\left[12\right]\right]$. As such we compute

$$\begin{aligned}
\left[12^1\right] &= 12 \\
\left[12^2\right] &= 18 \\
\left[12^{2^2}\right] = \left[(12^2)^2\right] &= \left[12^2\left[12^2\right]\right] = [18 \times 18] = 9 \\
\left[12^{2^3}\right] = \left[\left(12^{2^2}\right)^2\right] &= \left[\left[12^{2^2}\right]\left[12^{2^2}\right]\right] = [9 \times 9] = 18
\end{aligned}$$

Which lets us compute the remainder as

$$\left[12^{11}\right] = [[18 \times 18] \times 12] = [9 \times 12] = 3$$

1.4 Greatest common divisor

Definition 1.4.1: Divisor set

Let $D = \{d \in \mathbb{N} \mid d \mid n\}$ be the set of natural divisors of $n \in \mathbb{Z}$, we call D the divisor set of n and denote it $\text{div}(n)$.

Example 1.4.1 A few example are listed:

$$\begin{aligned}\operatorname{div}(12) &= \{1, 2, 3, 4, 6, 12\}\\ \operatorname{div}(28) &= \{1, 2, 4, 14, 28\}\\ \operatorname{div}(32) &= \{1, 2, 4, 8, 16, 32\}\end{aligned}$$

Here an interesting pattern emerges when we determine the intersection of divisor sets:

$$\begin{aligned}\operatorname{div}(12) \cap \operatorname{div}(28) &= \{1, 2\} = \operatorname{div}(2)\\ \operatorname{div}(28) \cap \operatorname{div}(32) &= \{1, 2, 4\} = \operatorname{div}(4)\end{aligned}$$

Indicating that the intersection of divisor sets for some $m, n \in \mathbb{Z}$ form a divisor set for a third number $d \in \mathbb{N}$.

Lemma 1.4.1: Euclid

Let $m, n \in \mathbb{Z}$, then there exists a unique natural number $d \in \mathbb{N}$ such that

$$\operatorname{div}(m) \cap \operatorname{div}(n) = \operatorname{div}(d)$$

Proof. Uniqueness follows from the fact that no two distinct natural numbers have the same divisior sets as it always contains itself. To prove existence of d we assume that $m, n \in \mathbb{N}$, since $\operatorname{div}(x) = \operatorname{div}(-x)$ for $x \in \mathbb{Z}$. We use induction on $\min(m, n)$ where

$$\min(m, n) = m \implies m \leq n \text{ and } \min(m, n) = n \implies m > n.$$

If $\min(m, n) = 0$, we can assume that $n = 0$ whereby $\operatorname{div}(m) \cap \operatorname{div}(n) = \operatorname{div}(m)$ as all numbers divide zero whereby $\operatorname{div}(m) \subset \operatorname{div}(0)$. We now assume that $\operatorname{div}(m) \cap \operatorname{div}(n) = \operatorname{div}(d)$ holds for every $m, n \in \mathbb{N}$ where $\min(m, n) < N$ with $N > 0$.

Using induction, we suppose that $m, n \in \mathbb{N}$ where $\min(m, n) = N$ with $m \geq n = N$. Then we have that $\exists q \in \mathbb{Z}, m = qn + r$ where $0 \leq r < n$ by Theorem 1.2.1, then

$$\operatorname{div}(m) \cap \operatorname{div}(n) = \operatorname{div}(m - qn) \cap \operatorname{div}(n) = \operatorname{div}(r) \cap \operatorname{div}(n)$$

as a number divides m, n if and only if it also divides $m - qn$. By induction

we know that $\operatorname{div}(r) \cap \operatorname{div}(n) = \operatorname{div}(d)$ for some $d \in \mathbb{N}$ since $\min(r, n) = r < n = N$. □

Definition 1.4.2: Greatest common divisor

The unique number $d \in \mathbb{N}$ discussed above is called the greatest common divisor of m, n denoted $d = \gcd(m, n)$.

1.5 Euclidean algorithm

Proposition 1.5.1: Euclid's algorithm

Let $m, n \in \mathbb{N}$, then:

(i) $\gcd(m, 0) = m$ if $m \in \mathbb{N}$.

(ii) $\gcd(m, n) = \gcd(m - qn, n)$ for every $q \in \mathbb{Z}$.

Proof. As $\operatorname{div}(0) = \mathbb{Z} \implies \gcd(m, 0) = \operatorname{div}(m) \cap \operatorname{div}(\mathbb{Z}) = \operatorname{div}(m)$, proving (i). We arrive at (ii) from the fact that

$$\operatorname{div}(d) = \operatorname{div}(m) \cap \operatorname{div}(n) = \operatorname{div}(m - qn) \cap \operatorname{div}(n)$$

being an alternative way to express that $d \mid m, n \iff d \mid m - qn, n$, such that $\gcd(m, n) = \gcd(m - qn, n)$. □

Example 1.5.1 Let $m = 24$ and $n = 14$, then

$$\gcd(24, 14) = \gcd(14, 10) = \gcd(10, 4) = \gcd(4, 2) = \gcd(2, 0) = 2$$

For a more general case with $m \leq n \leq 0$, we let $r_{-1} = m$ and $r_0 = n$, if $r_0 = 0$ then $\gcd(r_{-1}, r_0) = r_{-1}$, if this is not the case however then we define $r_1 = [r_{-1}]_{r_0} \implies \exists q_1, r_1 = r_{-1} - q_1 r_0$, wherby we let $\gcd(r_{-1}, r_0) = \gcd(r_0, r_1)$, repeating until $r_N = 0$ whereby we have that $\gcd(m, n) = r_{N-1}$.

Since m, n share a common factor, it must be possible to construct a linear combination of m, n resulting in said factor.

Example 1.5.2 We wish to determine $\lambda, \mu \in \mathbb{Z}$ such that $24\lambda + 14\mu = 2$, we

do this by determining λ, μ for the remainder in each step of the algorithm

$$\begin{aligned}
24 &= 1 \times 24 + 0 \times 14 \\
14 &= 0 \times 24 + 1 \times 14 \\
10 &= 24 - 14 = 1 \times 24 - 1 \times 14 \\
4 &= 14 - 10 = -1 \times 24 + 2 \times 14 \\
2 &= 10 - 2 \times 4 = 2 \times 24 - 3 \times 14
\end{aligned}$$

Giving us that $\lambda = 2, \mu = -3$.

Definition 1.5.1: Extended Euclidean algorithm

The Euclidean algorithm with the addition demonstrated above for computing λ, μ is called the extended Euclidean algorithm.

Lemma 1.5.1: Linear combination exists

Let $m, n \in \mathbb{Z}$, then there exist $\lambda, \mu \in \mathbb{Z}$ such that

$$\lambda m + \mu n = \gcd(m, n).$$

Proof. Let $m, n \in \mathbb{N}$ and $d = \gcd(m, n)$, then the extended Euclidean algorithm will give $\lambda, \mu \in \mathbb{Z}$ such that $\lambda m + \mu n = d$, we now show that

$$(-\lambda)(-m) + \mu n = \lambda m + (-\mu)(-n) = (-\lambda)(-m) + (-\mu)(-n) = d$$

Showing that λ, μ exist for all m, n. □

Definition 1.5.2: Coprime integers

Two integers $a, b \in \mathbb{Z}$ are called relatively prime (or coprime) if

$$\gcd(a, b) = 1.$$

Corollary 1.5.1: Divisor of product of relative prime

Suppose that $a \mid bc$ where $a, b, c \in \mathbb{Z}$ where $\gcd(a, b) = 1$, then $a \mid c$.

Proof. By Lemma 1.5.1 there exists a linear combination $\lambda a + \mu b = 1$, multiplying by c then gives $\lambda ac + \mu bc = c \implies a \mid c$ as a obviously divides the first term and bc by the proposition. □

Corollary 1.5.2: Properties of relative primes

Let $a, b, c \in \mathbb{Z}$ then:

(i) If $\gcd(a, b) = 1$, $a \mid c$ and $b \mid c$ then $ab \mid c$.

(ii) If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$ then $\gcd(a, bc) = 1$.

Proof. By Lemma 1.5.1 there exists a linear combination $\lambda a + \mu b = 1$, since $a, b \mid c$ we can write c as $c = ax = by$ for some $x, y \in \mathbb{Z}$, as such we multiply the linear combination by c, giving

$$c = \lambda ac + \mu bc = \lambda aby + \mu bax = ab(\lambda y + \mu x)$$

proving (i). To prove (ii) we again use Lemma 1.5.7, whereby we get two identities $\lambda_1 a + \mu_1 b = 1$ and $\lambda_2 a + \mu_2 c = 1$ for some $\lambda_1, \mu_1, \lambda_2, \mu_2 \in \mathbb{Z}$, multiplying the two together we have that

$$1 = (\lambda_1 a + \mu_1 b)(\lambda_2 a + \mu_2 c) = (\lambda_1 \lambda_2 a + \lambda_1 \mu_2 c + \mu_1 b \lambda_2)a + (\mu_1 \mu_2)bc$$

Showing that $\gcd(a, bc) = 1$ whereby they are relative primes. □

1.6 Chinese remainder theorem

Example 1.6.1 Consider a number $x < 30$, let a, b, c be rows numbered upwards from zero in the following three tables where the number is located

0	2	4	6	8	10	12	14	16	18	20	22	24	26	28
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29

0	3	6	9	12	15	18	21	24	27
1	4	7	10	13	16	19	22	25	28
2	5	8	11	14	17	20	23	26	29

0	5	10	15	20	25
1	6	11	16	21	26
2	7	12	17	22	27
3	8	13	18	23	28
4	9	14	19	24	29

Take for example $x = 27$, then we find $a = 1, b = 0, c = 2$, in fact, these numbers are all you need to know in order to determine x, this is called the 30-riddle.

Definition 1.6.1: Remainder map

Define

$$\mathbb{Z}/N = \{X \in \mathbb{N} \mid 0 \leq X < N\}$$

For $N \in \mathbb{N}$. If $N = n_1 \times n_2 \times \ldots \times n_t \neq 0$ then we let

$$r : \mathbb{Z}/N \to \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t$$

By the map given by $r(X) = ([X]_{n_1}, \ldots, [X]_{n_t})$. We call this the remainder map.

Example 1.6.2 Suppose that $N = 2 \times 3 \times 5 = 30$ and $x = 27$, then we have that

$$r(27) = ([27]_2, [27]_3, [27]_5) = (1, 0, 2)$$

We recognize this tuple as the values a, b, c for $x = 27$ in the 30-riddle.

Lemma 1.6.1: Bijective remainder map

Suppose that $N = n_1 \times n_2 \times \cdots \times n_t$ where $n_1, n_2 \ldots, n_t \in \mathbb{N} \setminus \{0\}$ and $\gcd(n_i, n_j) = 1$ if $i \neq j$ then

$$r : \mathbb{Z}/N \to \mathbb{Z}/n_1 \times n_2 \times \cdots \times n_t$$

is bijective.

Proof. If $r(X) = r(Y)$ then $[X]_{n_i} = [Y]_{n_i}$ for all $i \in \{1, 2, \ldots, t\}$, implying that $X \equiv Y \mod n_i$ whereby $n_i \mid X - Y$. From Corollary 1.5.2 we know that if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$ then $\gcd(a, bc) = 1$, meaning that if a

number is divisible by several coprimes, it is also divisible by their products, and as such $N \mid X - Y$. Similarly we recognize that $0 \leq X, Y < N$, whereby it is only possible for N to divide $X - Y$ if their sum is equal 0, and as such $X = Y$, implying that each mapping is unique and r is therewfore injective, this implies that r is also surjective as the codomain and domain have the same number of elements, making r injective. □

Theorem 1.6.1: Chinese remainder theorem

Suppose that $N = n_1 \times n_2 \times \cdots \times n_t$ where $n_1, n_2, \ldots, n_t \in \mathbb{Z} \setminus \{0\}$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$. Consider the system of congruences

$$\begin{aligned} X &\equiv a_1 \mod n_1 \\ X &\equiv a_2 \mod n_2 \\ &\vdots \\ X &\equiv a_t \mod n_t \end{aligned}$$

for $a_1, a_2, \ldots, a_t \in \mathbb{Z}$. Then:

(i) The system has a solution $X \in \mathbb{Z}$.

(ii) If $X, Y \in \mathbb{Z}$ are solutions of the system then $X \equiv Y \mod N$. If X is a solution and $Y \equiv X \mod N$ then Y is a solution.

Proof. If X, Y are solutions then by Lemma 1.6.1 $N \mid X - Y$ and $X \equiv Y \mod N$, the same applies in reverse where $Y \equiv X \mod N$ and $N \mid Y - X$, proving (ii) by showing theyre both solutions. As we know n_i and N/n_j must be relatively prime (N/n_j contains the product of the other coprime terms without n_j) there must exist integers λ_j, μ_j such that

$$\begin{aligned} \lambda_1 n_1 + \mu_1 N/n_1 &= 1 \\ \lambda_2 n_2 + \mu_2 N/n_2 &= 1 \\ &\vdots \\ \lambda_t n_t + \mu_t N/n_t &= 1 \end{aligned}$$

We let $A_j = \mu_j N/n_j$ for $j = \{1, 2, \ldots, t\}$ noticing that $A_j \mod n_j = 1$ and $A_j \mod n_i = 0$ for $i \neq j$, we build a solution from these as

$$X = a_1 A_1 + a_2 A_2 + \cdots + a_t A_t$$

Where we can ignore the first term as it is equal 1 when the other term is equal 0 and vice versa. □

Example 1.6.3 Applying the above on the 30-riddle we have that $n_1 = 2, n_2 = 3, n_3 = 5$, we find $\lambda_i, mu_i \in \mathbb{Z}$ that satisfy

$$\lambda_1 n_1 + \mu_1 N/n_1 = 2\lambda_1 + (2 \times 3 \times 5)/2\mu_1 = 2\lambda_1 + 15\mu_1 = 1$$
$$\lambda_2 n_2 + \mu_2 N/n_2 = 3\lambda_2 + (2 \times 3 \times 5)/3\mu_2 = 3\lambda_2 + 10\mu_2 = 1$$
$$\lambda_3 n_3 + \mu_3 N/n_3 = 5\lambda_3 + (2 \times 3 \times 5)/5\mu_3 = 5\lambda_3 + 6\mu_3 = 1$$

Which has solution $\lambda_1 = -7, \mu_1 = 1, \lambda_2 = -3, \mu_2 = 1, \lambda_3 = -1, \lambda_3 = 1$, giving us $A_1 = 15, A_2 = 10, A_3 = 6$ whereby

$$X = 15a_1 + 10a_2 + 6a_3$$

Is a solution to the system of congruences

$$X \equiv a_1 \mod 2X \qquad \equiv a_2 \mod 3X \equiv a_3 \mod 5$$

And as such we can determine our original number using a_1, a_2, a_3, for $a_1 = 1, a_2 = 0, a_3 = 2$ we find that $X = 15 + 0 + 12 = 27$, and determine the remainder following division by 30 as $[X]_{30} = [27]_{30} = 27$, which is also the number we used in the first example.

---

2 Groups

2.1 Definition

A composition on a set G is a map $\circ : G \times G \to G$. The composition $\circ(g, h)$ is often denoted $g \circ h$ or gh.

Definition 2.1.1: Group

A pair $(G, \circ)$ consisting ofa set G and a composition $\circ : G \times G \to G$ is called a group if it satisfies:

(i) $\forall s_1, s_2, s_3 \in G, s \circ (s_2 \circ s_3) = (s \circ s_2) \circ s_3$, the composition is associative.

(ii) For some $e \in G$, $e \circ s = s$ and $s \circ e = s$, there exists a neutral element.

(ii) For every $s \in G$ there exists an inverse element, t, such that $t \circ s = e$ and $s \circ t = e$.

A group is called abelian if $x \circ y = y \circ x$ for every $x, y \in G$, whilst the number of elements $|G| \in G$ is called the order of G.

An example of a non-abelian group is $(\mathbb{N}, +)$.

Example 2.1.1 The neutral element for $(\mathbb{N}, +)$ would have to be 0, except a problem then occurs as no inverse element would exist (due to us not having negative numbers), as no solution $\in \mathbb{N}$ would exist for $n + t = 0$ where $n, t \in \mathbb{N}$.

To exemplify an abelian group we examine $(\mathbb{Z}, +)$.

Example 2.1.2 The neutral element for $(\mathbb{Z}, +)$ would again have to be 0, but this time we have a well defined inverse element as the equation $n+t = 0$ has solution $t = -n$, both of which being contained in $\mathbb{Z}$, additionally it is abelian as $n + t = t + n$.

Similarly we can look at larger sets such as the rationals and reals, which are abelian in regards to addition, if we look at multiplication instead, we have to exclude 0 from the groups as 1 would have to be the neutral element by (ii), but then no value t exists such that $0 \times t = 1$.

2.2 Groups and congruences

We often times work with $\mathbb{Z}$ instead of $\mathbb{N}$ as we then have an inverse. Given that $\mathbb{Z}$ is a group with composition $+$, we can build new groups tied to the congruence modulo some integer. We define addition on a subset of $\mathbb{Z}$ given by $a + n\mathbb{Z} = \{a + nx \mid n \in \mathbb{Z}\}$ where $a, n \in \mathbb{Z}$.

Example 2.2.1 Let $G = 2 + 3\mathbb{Z}$ and $H = 5 + 3\mathbb{Z}$, then

$$G = \{\ldots, -4, -1, 2, 5, \ldots\}$$
$$H = \{\ldots, -1, 2, 5, 8, \ldots\}$$

We quickly identify that the two sets contain the same elements, and as such we say they are identical.

Proposition 2.2.1: Identical sets

Let $a, b, c \in \mathbb{Z}$ then:

(i) $a + c\mathbb{Z} = b + c\mathbb{Z} \iff a \equiv b \mod c$.

(ii) $(a + c\mathbb{Z}) \cap (b + c\mathbb{Z}) = \emptyset \iff a \not\equiv b \mod c$.

Proof. Let $m \in a + c\mathbb{Z}$, then if $a + c\mathbb{Z} = b + c\mathbb{Z} \implies m \in b + c\mathbb{Z}$. As such for some $x, y \in \mathbb{Z}$ we have $m = a + cx = b + cy \implies a - b = c(y - x)$ meaning that $a \equiv b \mod c$, whereby $a = b + cx \implies a + c\mathbb{Z} = b + cx + c\mathbb{Z} = b + c\mathbb{Z}$ as $x + c \in \mathbb{Z}$, proving (i). Now if $(a + c\mathbb{Z}) \cap (b + c\mathbb{Z}) \neq \emptyset$ there must exists elements $m, x, y \in \mathbb{Z}$ such that $m = a + cx = b + cy \implies a - b = c(y - x)$ whereby $a \equiv b \mod c$ by (i). □

If $c > 0$ then $a + c\mathbb{Z} = b + c\mathbb{Z} \iff [a]_c = [b]_c$. Let $[x]$ be the subset $x + c\mathbb{Z}$, being the set consisting of integers giving remainder x following divison by c.

Example 2.2.2 Let $c = 3$ then $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$, where

$$[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

Using this we can add subsets $[x], [y] \in \mathbb{Z}/c\mathbb{Z}$ by defining $[x] + [y] = [x + y]$, as we by Proposition 1.3.2(i) have that if $[x] \equiv [x']$ and $[y] \equiv [y']$ then $[x + y] = [x' + y']$, using this we check whether $(\mathbb{Z}/c\mathbb{Z}, +)$ forms a group. Since associativity holds for $(\mathbb{Z}, +)$, we have that

$$\begin{aligned}([x] + [y]) + [z] &= [x + y] + [z] = [(x + y) + z] \\ &= [x + (y + z)] = [x] + [y + z] = [x] + ([y] + [z])\end{aligned}$$

similarly, we have that 0 is the neutral element as

$$[x] + [0] = [x + 0] = [x]$$

whilst there also exists an inverse by $-x$ as

$$[x] + [-x] = [x - x] = [0].$$

This group is also abelian as $[x] + [y] = [x + y] = [y + x] = [y] + [x]$. In the case that c is 0 then $\mathbb{Z}/0\mathbb{Z} = \{x + 0\mathbb{Z}\} = \{x\} = \mathbb{Z}$, where addition is obviously defined.

2.2.1 Composition table

Definition 2.2.1: Composition table

Given a finite group $\{e, g_1, \ldots, g_r\}, \cdot)$ the composition is often shown using a composition table:

$\circ$	e	g_1	$\cdots$	g_j	$\cdots$	g_r
e	e	g_1	$\cdots$	g_j	$\cdots$	g_r
g_1	g_1	$g_1 \circ g_1$	$\cdots$	$g_1 \circ g_j$	$\cdots$	$g_1 \circ g_r$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
g_i	g_i	$g_i \circ g_1$	$\cdots$	$g_i \circ g_j$	$\cdots$	$g_i \circ g_r$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
g_r	g_r	$g_r \circ g_1$	$\cdots$	$g_r \circ g_j$	$\cdots$	$g_r \circ g_r$

Example 2.2.3 The composition table for the previously computed group $(\mathbb{Z}/3\mathbb{Z}, +)$ is given by

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

2.3 Associativity

Suppose that S is a set with a multiplicative group mapping $(x, y) \to xy$. As it is a group, associativity holds, an expression like $s_1 s_2 \dots s_n$ for $n > 2$ isnt valid for this composition, as it only takes in two element, however we can reduce the expression to contain only two elements by repeatedly multiplying sets of two elements.

Example 2.3.1 Consider the sequence $s_1 s_2 s_3 s_4$ in the previous composition, we can calculate this in 5 different ways

$$s_1(s_2(s_3 s_4))$$
$$s_1((s_2 s_3)s_4)$$
$$(s_1(s_2 s_3))s_4$$
$$((s_1 s_2)s_3)s_4$$
$$(s_1 s_2)(s_3 s_4)$$

Determining whether at set is associative is difficult, except for one case: when S is the set of maps from a set X to itself where composition is defined as usual, meaning that fg is $(fg)(x) = f(g(x))$ for $f, g \in S$ and $x \in X$. In which case $f(gh) = (fg)h$ since $(f(fg))(x) = ((fg)h)(x)$ for all $x \in X$:

$$(f(gh))(x) = f((gh)(x)) = f(g(h(x)))$$
$$(f(g)h)(x) = (fg)(h(x)) = f(g(h(x)))$$

2.4 Example of non-abelian group

Example 2.4.1 Let $X = \{1, 2, 3\}$ and G be the set of all bijective maps $X \to X$, then G is a group with the usual composition of maps as composition. Here the neutral element of G will be the identity map $X \to X$, the inverse of some map $f : X \to X$ is the inverse map $f^{-1} : X \to X$, and

the composition of maps is associative, we can list the elements of G as

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad b = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & 2 \end{pmatrix}$$
$$c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

where for example $c : X \to X$ is the map given by $c(1) = 3, c(2) = 2, c(3) = 1$. Compositions are simple to find, as we can apply associativity, finding for example that $ab(x) = a(b(x))$ implying that $a(b(1)) = a(1) = 2, a(b(2)) = a(3) = 3, a(b(3)) = a(2) = 1$, also showing that $ab = f$. The composition table is given by

$\circ$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	d	e	f	a	c
c	c	f	d	e	b	a
d	d	b	c	a	f	e
f	f	c	a	b	e	d

This group is known as the symmetric group S_3 and is non-abelian, as $ab \neq ba$.

2.5 Uniqueness of neutral and inverse

Suppose that $e, e' \in G$ are neutral elements of G, then $e = e'e = e'$, and as such $e' = e$. Similarly to every $g \in G$ there can only be one inverse element g^{-1}, let $g^{-1\prime}$ be a second inverse element satisfying $g^{-1\prime}g = e$, then $g^{-1\prime}g = e = g^{-1}g$, then by multiplying both sides by $g^{-1\prime}$ we have that $g^{-1\prime} = (g^{-1}g)g^{-1\prime} = g^{-1}(gg^{-1}) = g^{-1}$.

Definition 2.5.1: Inverse element

Let $g \in G$ be an element of a group, then we let $g^{-1} \in G$ denote the unique inverse element of g.

2.6 Multiplication by $g \in G$ is bijective

Let G be a group and $g \in G$, then a map $\varphi : G \to G$ given by $\varphi(x) = gx$ is bijective, we prove this by providing the inverse map $\lambda : G \to G$ given by

$\lambda(x) = g^{-1}x$. Then $\lambda(\varphi(x)) = g^{-1}(gx) = (g^{-1}g)x = ex = x$. proving that $\lambda = \varphi^{-1}$, as the inverse exists, φ must be bijective.

2.7 Subgroups and cosets

Definition 2.7.1: Subgroup

A subgroup of a group G is a non-empty subset $H \subseteq G$ such that the composition of G makes H into a group, i.e., H is a subgroup of G if and only if:

(i) $e \in H$.

(ii) $x^{-1} \in H$ for all $x \in H$.

(iii) $xy \in H$ for all $x, y \in H$.

Example 2.7.1 Observe group S_3 from Example 2.4.1, here $\{e, a\}$ and $\{e, f, d\}$ are subgroups of S_3 by the composition table.

$\circ$	e	d	f
e	e	d	f
d	d	f	e
f	f	e	d

$\circ$	e	a
e	e	a
a	a	e

We recall from previous chapters that $(\mathbb{Z}, +)$ forms a group, in the context of groups the uniqueness of the remainder following divison results in

Proposition 2.7.1: Subgroups of $\mathbb{Z}$

Let H be a subgroup of $(\mathbb{Z}, +)$ then:

$$H = d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\} = \{\ldots - 2d, -d, 0, d, 2d, \ldots\}$$

for a unique $d \in \mathbb{N}$.

Proof. If $d = 0 \implies H = \{0\}$ Assume $H \neq \{0\}$, then $N \cap H$ contains a smallest natural number $d > 0$ as the first positive non-zero entry is always d given that $d \neq 0$. Let $H = d\mathbb{Z}$, then $-d \in H$ by definition as $d \in H$, H being a subgroup. Similarly, the set must be closed under addition, and as such $d + d, d + d + d, d + d + d + d, \ldots \in H$ (and the same for negative d),

showing that all $nd \in H$ for $n \in \mathbb{Z}$, whereby $d\mathbb{Z} \subseteq H$. Suppose now that $m \in H$, division with remainder gives that $m = qd + r$ where $0 \leq r < d$. Since H is a subgroup, $m, d, -qd, r \in H$, but as $d > r \in \mathbb{N} \geq 0$, r can only be 0 whereby $m = qd \implies H = d\mathbb{Z}$. □

Let H be a subgroup of G and $g \in G$, then the subsets

$$gH = \{gh \mid h \in H\} \subseteq G \qquad Hg = \{hg \mid h \in H\} \subseteq G$$

Are called the left- and right cosets respectively. The set of left cosets of H is denoted G/H whilst the set of right cosets of H is denoted $H \setminus G$.

Example 2.7.2 Let $G = (\mathbb{Z}, +), H = 3\mathbb{Z}$, then

$$\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$$

As we are working modulo 3 the sets $1 + 3\mathbb{Z} = 4 + 3\mathbb{Z} = 1 + 3n + 3\mathbb{Z}$ for $n \in \mathbb{Z}$, as such two subgroups of H of G, $g_1H = g_2H$ does not necessarily imply that $g_1 = g_2$.

Example 2.7.3 Let $H = \{e, a\}S_3$, then all left- and right cosets of H can be listed using the composition table as

$$\begin{aligned} eH &= \{ee, ea\} = \{e, a\} & He &= \{ee, ae\} = \{e, a\} \\ aH &= \{ae, aa\} = \{a, e\} & Ha &= \{ea, aa\} = \{a, e\} \\ bH &= \{be, ba\} = \{b, d\} & Hb &= \{eb, ab\} = \{b, f\} \\ cH &= \{ce, ca\} = \{c, f\} & Hc &= \{ec, ac\} = \{c, d\} \\ dH &= \{de, da\} = \{d, b\} & Hd &= \{ed, ad\} = \{d, c\} \\ fH &= \{fe, fa\} = \{f, c\} & Hf &= \{ef, af\} = \{f, b\} \end{aligned}$$

We quickly recognize that these are either equal or disjoint, for the right cosets we have $H = eH = aH, bH = dH, cH = fH$ whilst for the left cosets $H = He = Ha, Hb = Hd, Hc = Hf$, meaning that we can write the sets of cosets as $G/H = \{H, bH, cH\}$ and $G \setminus H = \{H, Hb, Hc\}$.

Lemma 2.7.1

Let H be a subgroup of a group G and let $x, y \in G$, then:

(i) $x \in xH$.

(ii) $xH = yH \iff x^{-1}y \in H$.

(iii) If $xH \neq uH$ then $xH \cap yH = \emptyset$.

(iv) The map $\varphi : H \to xH$ given by $\varphi(h) = xh$ is bijective.

Proof. x is obviously contained in xH as $x = xe$, proving (i). If $xH = yH$ then there exists an $h \in H$ such that $xh = ye = y$, making $y = xh$ and thereby $yH \subseteq xH$, similarly, by the previous equality it follows that $x = yh^{-1}$ whereby we also have $xH \subseteq xH$, which is satisfied if and only if $xH = yH$, proving (ii). Now let $z \in xH \cap yH$, then $z = xh_1 = yh_2$, for some $h_1, h_2 \in H$, then there must exist h_1 such that $xh_1 = yh_2 \implies x^{-1}y \in H$, which by (ii) shows that $xH = xY$, whereby (iii) holds. We let $\lambda(h) = x^{-1}h$, whereby $\lambda(\varphi(h)) = x^{-1}xh = (x^{-1}x)h = eh = h$, proving that the inverse exists whereby it must be bijective. □

Corollary 2.7.1

Let H be a subgroup of G, then

$$G = \bigcup_{g \in G} gH$$

and if $g_1H \neq g_2H$, then $g_1H \cap g_2H = \emptyset$.

Proof. By the proposition we have that $g_1H \neq g_2H$, as such by Lemma 2.7.1(iii) their intersection is the empty set. □

Theorem 2.7.1: Lagrange

If $H \subseteq G$ is a subgroup of a fionite group G, then

$$|G| = |G/H||H|$$

Meaning that the order of a subgroup divides the order of the group.

Proof. Let gH be a coset in G/H, by Lemma 2.7.1(iv) the map $\varphi : G \to gH$ is bijective, and as such $|H| = |gH|$. Now as $G = \bigcup_{i \in G} g_i H$, the order of $|G|$ must be the order of $|H|$ multiplied by the amount of cosets, whereby $G = |G/H||H|$ implying that $|H|$ divides $|G|$. □

Definition 2.7.2: Index

The number of cosets $|G/H|$ is called the index of $H \in G$, denoted $[G : H]$.

3 Exercises

3.1 Chapter 1 FIX 13

Exercise 1 Let s be the first element of $S \subseteq Z$, assume that s_1 also be the first element of S, then if follows that $\forall x \in S, s \leq s_1 \leq x$, however as x is all elements in S, it must also be able to take on the values s, s_1, giving us the inequalities $s \leq s_1 \leq s_1$ and $s \leq s_1 \leq s$, which is only satisfied if $s = s_1$ and as such it must be unique.

Exercise 2 We recall that $x = qd + r \implies r = x - qd$, as such $x - qd$ is the remainder following division of x by d, meaning that $0 \leq r < d$, and as $d > 0$, the set of possible remainders must always contain at least $\{0\}$, meaning that $M \cap \mathbb{N} \neq \emptyset$.

Exercise 3 From Proposition 1.3.1(i) we have that

$$\begin{aligned} a &\equiv [a] \mod N \\ b &\equiv [b] \mod N \end{aligned}$$

Then by Proposition 1.3.2(ii) we can write the remainder of their product as

$$ab \equiv [a][b] \mod N$$

Whereby we from Proposition 1.3.1(ii) have that

$$[ab] = [[a][b]]$$

Exercise 4 We split 2^{340} into smaller exponents as

$$2^8 + 2^6 + 2^4 + 2^2 \implies 2^{340} = 2^{2^8} 2^{2^6} 2^{2^4} 2^{2^2}$$

from which it follows that $\left[2^{340}\right] = \left[\left[2^{2^8}\right]\left[2^{2^6}\right]\left[2^{2^4}\right]\left[2^{2^2}\right]\right]$. Whereby we can compute the remainders of the smaller terms with respect to $N = 341$:

$$\begin{aligned}
[2] &= 2 \\
\left[2^{2^2}\right] &= [2 \times 2] = 4 \\
\left[2^{2^2}\right] = \left[\left(2^2\right)^2\right] &= [4 \times 4] = [16] = 16 \\
\left[2^{2^3}\right] = \left[\left(2^{2^2}\right)^2\right] &= [16 \times 16] = [256] = 256 \\
\left[2^{2^4}\right] = \left[\left(2^{2^3}\right)^2\right] &= [256 \times 256] = 64 \\
\left[2^{2^5}\right] = \left[\left(2^{2^4}\right)^2\right] &= [64 \times 64] = 4 \\
\left[2^{2^6}\right] = \left[\left(2^{2^5}\right)^2\right] &= [4 \times 4] = 16 \\
\left[2^{2^7}\right] = \left[\left(2^{2^6}\right)^2\right] &= [16 \times 16] = 256 \\
\left[2^{2^8}\right] = \left[\left(2^{2^7}\right)^2\right] &= [256 \times 256] = 64
\end{aligned}$$

Allowing us to compute the remainder as

$$\left[2^{340}\right] = \left[\left[64^2 \times 16^2\right]\right] = [[64 \times 64]\,[16 \times 16]] = [4 \times 256] = [1024] = 1$$

Exercise 6 i) 2 divides every term except $10^0 a_0$ as $\forall n \in \mathbb{N}\backslash\{0\}, \text{div}(10^n) \supseteq \{2, 5, 10\}$, as such $a \equiv a_0 \mod 2$, whereby 2 must divide a_0 for the expression to be divisible by 2.

ii) We have $\forall n \in \mathbb{N}\backslash\{0, 1\}, \text{div}(10^n) \supseteq \{2, 4, \ldots, 100\}$, as such $a \equiv a_0 + 10^1 a_1 \mod 4 \equiv a_0 + 2a_1 \mod 4$, whereby $4 \mid a_0 + 2a_1$ for a to be divisible by 4.

iii) We have $\forall n \in \mathbb{N} \setminus \{0, 1, 2\}, \text{div}(10^n) \supseteq \{2, 4, 8, \ldots, 1000\}$, as such $a \equiv a_0 + 10^1 a_1 + 10^2 a_2 \mod 4 \equiv a_0 + 2a_1 + 4a_2 \mod 4$, whereby $4 \mid a_0 + 2a_1 + 4a_2$ for a to be divisible by 4.

iv) We have that $\forall n \in \mathbb{N} \setminus \{0\}, \text{div}(10^n) \supseteq \{2, 5, 10\}$, as such $a \equiv a_0 \mod 5$ implying that $5 \mid a_0$ for a to be divisible by 5.

v) We first show that 9 and 10 are relatively prime using Euclids algorithm $\gcd(10, 9) = \gcd(9, 1) = \gcd(1, 0) = 1$, as such 9 never divides any factor of 10, and as such must divide all $a_n \in a$ for the expression to be divisible.

vi)

vii)

Exercise 8 By Proposition 1.3.2(ii) we can express $[4^n]_3$ as $[[4]_3^n]_3$, this simplifies immediately as $[4]_3 = 1$ whereby $\forall n \in \mathbb{N}, [[4]_3^n]_3 = [1]_3 = 1$. By Proposition 1.3.1(i) we can then express the remainder of the difference $4^n - 1$ as $[4^n]_3 - [1]_3 = 1 - 1 = 0$, whereby $4 \mid 4^n - 1$.

Exercise 12 We use the extended Euclidean algorithm with $m = 89$ and $n = 55$, as such we write the system of equations

$$\begin{aligned}
89 &= 89 \\
55 &= 55 \\
34 &= 89 - 55 = 89 \times 1 - 55 \times 1 \\
21 &= 55 - 34 = 89 \times (-1) + 55 \times 2 \\
13 &= 34 - 21 = 2 \times 89 - 55 \times 3 \\
8 &= 21 - 13 = 89 \times (-3) + 55 \times 5 \\
5 &= 13 - 8 = 89 \times 5 - 55 \times 8 \\
3 &= 8 - 5 = 89 \times (-8) + 55 \times 13 \\
2 &= 5 - 3 = 89 \times 13 + 55 \times (-21) \\
1 &= 3 - 2 = 89 \times (-21) + 55 \times 34
\end{aligned}$$

whereby $\lambda = -21, \mu = 34$. By Chinese remainder theorem we let $X = 34 \times 7 = 238$, and take the remainder following division by 55 as $[238]_{55} = 18$, as such $x = 18n$ for any $n \in \mathbb{Z}$.

Exercise 13 Suppose that $\lambda N + \mu M = d$, then we can let $d = 0$ and solve, finding that $\lambda_1 N + \mu_1 M = 0 \implies \lambda_1 = \frac{-\mu_1 M}{N}$, then when μ_1 is a nonzero multiple of N, it cancels out the denominator, and we get a corresponding integer value for λ_1, since the sum of these equal 0, we can add any factor thereof with no repercussions to the equality, and find that $\lambda N + \mu M + n(\lambda_1 N + \mu_1 M) = \underbrace{(\lambda + n\lambda_1)}_{\lambda'} N + \underbrace{(\mu + n\mu_1)}_{\mu'} M = d$.

Exercise 17 We solve the system of congruences

$$\begin{aligned}
X &\equiv 2 \mod 3 \\
X &\equiv 3 \mod 5
\end{aligned}$$

for X. As $\gcd(3,5) = 1$ we make use of Chinese remainder theorem with $N = 3 \times 5 = 15$, and establish the system of equations

$$\lambda_1 \times 3 + \mu_1 \times 5 = 1 \implies \lambda_1 = 7, \mu_1 = -4 \implies A_1 = -20$$
$$\lambda_2 \times 5 + \mu_2 \times 3 = 1 \implies \lambda_2 = 5, \mu_2 = -8 \implies A_2 = -24$$

giving us that $X = -40 - 72 = -112$, we take modulo 15 finding that $X \equiv -112 \mod 15 \equiv 8 \mod 15$, as 8 is not odd, we add 15, giving us that $X = 23$ is the smallest odd natural number solution to the system of congruences.

Exercise 18 We show that $\gcd(504, 35, 16) = 1$. We first find $\gcd(504, 35)$ and then $\gcd(\gcd(504, 35), 16)$ as this will give us the shared greatest factor

$$\gcd(504, 35) = \gcd(35, 28) = \gcd(28, 7) = \gcd(7, 0) = 7$$
$$\gcd(16, 7) = \gcd(7, 2) = \gcd(2, 1) = \gcd(1, 0) = 1$$

showing that they are relatively prime and apply Chinese remainder theorem with $N = 504 \times 35 \times 16 = 282240$, we write the system of equations

$$\lambda_1 \times 504 + \mu_1 \times 560 = 1$$
$$\lambda_2 \times 35 + \mu_2 \times 8064 = 1$$
$$\lambda_3 \times 16 + \mu_3 \times 17640 = 1$$

4 Chapter 2

4.1 Chapter 1

Exercise 1 Decide which of the following are groups. List the conditions that are not met in cases where the set is not a group.

a) (2Z,+), the even set of integers with addition.

The set is given by $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$, associativity holds for integer addition, as we are observing addition in the integers the neutral element is 0 as $n + 0 = n$, and an inverse always exists as $x, -x \in 2\mathbb{Z}$. The set is therefore a group.

b) $([-5, 5], +)$ **the set of real numbers between** $-5, 5$ **with addition.**

The set is not closed as for $a, b \in [-5, 5]$ the sum $a+b$ is not always in $[-5, 5]$. Associativity holds for integer addition, similarly the neutral element is 0 as $n + 0 = n$, and an inverse for every element exists as for $x \in [-5, 5]$ the element $-x \in [-5, 5]$ is an inverse, as the set is not closed, it is not a group.

c) $(\mathbb{Z}, \hat{})$**, where the composition is given by** $\mathbf{a\hat{}b = a^b}$ **for** $\mathbf{a, b} \in \mathbb{N}$**.**

Associativity does not hold for exponentiation as $a\hat{}b \neq b\hat{}a$, a neutral element exists as 1, as $a\hat{}1 = a$, but the inverse does not exist as it would for some cases be a fraction not contained in $\mathbb{Z}$, therefore the set does not constitute a group.

d) $(\{\mathbf{e}\}, \cdot)$**, where** $\mathbf{e \times e = e}$**.**

Associativity holds for integer multiplication, similarly we have a neutral element by e, and it is also its own inverse as $e \times e = e$, as such the set forms a group.

e) $\emptyset$**, the empty set with trivial composition.**

Since no elements exist in $\emptyset$ it is impossible for it to be associative as there is nothing to be associative over, similarly a neutral element cannot exist as no elements exist and an inverse lacks for the aforementioned reason.

Exercise 2 Write the composition table for $\mathbb{Z}/5\mathbb{Z}$.

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

Exercise 3 We have seen that $\mathrm{GL}_2(\mathbb{R})$ is non-abelian, use this to show that $\mathrm{GL}_n(\mathbb{R})$ is non-abelian for $n \geq 2$.

We first show that $\mathrm{GL}_n(\mathbb{R})$ for $n \geq 2$ forms a group, we know matrix multiplication is associative, similarly the neutral element exists as the identity matrix I_n, whilst the inverse exists due to the determinant being nonzero by definition, making it satisfy the conditions for a group.

We now show that it is not abelian by counterexample in $n = 2$:

$$AB = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$
$$BA = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

whereby $\mathrm{GL}_n(\mathbb{R})$ for $n \geq 2$ is non-abelian.

Exercise 4 Let G be a group and $g \in G$ be a definite element, show that the mapping $\varphi : G \to G$ given by $\varphi(x) = xg$ is bijective.

Since $\varphi \in G$ there must exist an inverse φ^{-1} such that $\varphi^{-1}(\varphi(x)) = x$, we let $\varphi^{-1}(x) = xg^{-1}$, then $\varphi^{-1}(\varphi(x)) = xgg^{-1} = xe = x$, whereby the function must be bijective as it has an inverse.

Exercise 5 Find all possible composition tables for groups with four elements.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\circ$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Exercise 6 Use the same procedure as in Section 2.1.6, use the result to determine whether an abelian group of order 4 exists.

For the group to be abelian the entries on the diagonal of the composition table (from bottom left to top right) must be the same, this holds for the 4th order composition table given by

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Exercise 7 Check that the composition table in Example 2.1.6 is correct.

Since the composition table contains no rows or columns with the same entry twice, it is correct, similarly we recognize that the diagonal entries are not equivalent, being consistent with G not being abelian.

4.2 Section 2

Exercise 1 Let $(G, \circ)$ be a group, $H \subset G$, and assume that the restriction of $\circ$ to $H \times H$ makes H a group (i.e. H is a subgroup by definition). Show using definition only that:

a) If $\mathbf{e_G}$, $\mathbf{e_H}$ are neutral elements of $\mathbf{G}, \mathbf{H}$ respectively, then $\mathbf{e_H} = \mathbf{e_G}$.

b) If $\mathbf{A} \in \mathbf{H}$ has inverse $\mathbf{b_H} \in \mathbf{H}$ with inverse $\mathbf{b_G} \in \mathbf{G}$, then $\mathbf{b_H} = \mathbf{b_G}$.

Exercise 2 Let $\mathrm{SL}_2(\mathbb{Z})$ be the set of 2×2 matrices with integer entries and determinant 1. Show that matrix multiplication makes this set a group. Is it abelian? Is it finite?

Exercise 3 Let G be a group and let $H \subseteq G$ be a nonempty subset. Show that H is a subgroup if and only if $xy^{-1} \in H$ for all $x, y \in H$.

Exercise 4 Write down all subgroups of $\mathbb{Z}/6\mathbb{Z}$.

Exercise 5 Why does $\mathbb{Z}/7\mathbb{Z}$ have no subgroups other than $[0]$ and itself?

Exercise 6 Let H be a non-empty, finite subset of a (not necessarily finite) group G. Show that if $xy \in H$ holds for all $x, y \in H$ then H is a subgroup. Then give an example showing that this does not hold if H has infinitely many elements.

Exercise 7 Let $\circ$ be an associative composition on a set G. Show that no matter how the brackets are put in the product $s_1 \circ s_2 \circ \cdots \circ s_n$ the result is always equal to $(\ldots((s_1 \circ s_2) \circ s_3)\ldots)$.