Introduction to Algebra

Shu Sasaki

8th March 2024

1 Introduction

2 Revising bits and bobs from NSF

2.1 Integer division

2.2 GCD and Euclid's algorithm

2.3 Euclid's algorithm extended

2.4 Prime numbers

3 Modular arithmetic

3.1 Equivalence relations and partitions

3.2 Congruence mod n

3.3 Arithmetic with congruence classes

3.4 Modular inverses

4 Algebraic structures

Which is more symmetrical, a scalene triangle or an equilateral triangle? The equilateral triangle has lots of symmetries (reflection and rotation), while the scalene triangle has no symmetry at all. We are capable of sensing, or even quantifying, 'symmetries' (we often find symmetry rather pleasing, evidenced in art, architecture etc.). But what exactly is symmetry?

By a 'symmetry' of an object, we mean an 'action' we perform on the object (e.g. rotating 'r', reflecting 's', etc.) while preserving its structure (e.g. vertices, edges, etc.). For the equilateral triangle, what are all the symmetries?

Let us call the vertices of an equilateral triangle a, b and c clockwise, with a sitting at '12', b at '4' and c at '8' if we fit the triangle in an old-fashioned clock. For ease of reference, let us write this configuration $[a, b, c]$. Rotating $\pi/3$ clockwise changes $[a, b, c]$ into $[c, a, b]$, while reflecting the triangle with respect to the line passing through a and the mid-point of the edge bc turns $[a, b, c]$ into $[a, c, b]$. We call the former 'action' r and the latter s. Playing around this a bit, we should see

that $\{e, r, s, r^2, sr, sr^2\}$ (e denotes 'doing nothing'), subject to conditions such as $r^3 = e, s^2 = e$ and $srs = r^{-1}$, i.e. the composition of actions, s followed by r and then by s, equals $-\pi/3$ rotation represented by r^{-1}, are all possible actions, as there are in total 3! possible configurations$[*, *, *]$ in $\{a, b, c\}$. To sum up, we have completely described the symmetries of an equilateral triangle in terms of rotations and reflections. In fact, this 'labelling of actions' has given a 'structure' to the symmetries– for example, rs is manifestly different from sr!

A group is an axiomatisation/formalisation of 'actions' (we often forget about the 'object') as we have seen in this example.

Why groups? Groups pin down what we intuitively sense as a 'structure' (antithesis of which is 'chaos') and for that reason they are everywhere! Would it be surprising that group theory predicted the existence of many elementary particles before they were found experimentally? Groups theory is also a powerful tool in public-key cryptography and 'conceptually solving' Rubik's Cube?

Representation theory is a subject that aims at describing symmetry in terms of matrices (as we see in linear algebra). This is a subject area very much related to physics, for example.

4.1 Groups

Definition. A group is a set G with an operation $*$ on G satisfying the following axioms:

(G0) If a, b are elements of G, then $a * b$ is an element of G.

(G1) If a, b, c are elements of G, then $a * (b * c) = (a * b) * c$.

(G2) There is an element e in G (called the identity element) such that $a * e = e * a = a$ for every element of G.

(G3) For every element a of G, there exists b in G such that $a * b = b * a = e$. The element b is called the inverse of a.

(G4) If a, b are elements of G, then $a * b = b * a$.

When these five conditions hold, we say $(G, *)$ (or simply G if the operation $*$ is clear from the context) is a commutative/abelian group. By groups, I shall mean abelian groups unless otherwise specified.

Examples.

• $(G, *) = (\mathbb{Q}, +)$ is a group– this is an additive group (where the identity element e is '0' as we know well).

• $(\mathbb{Q} - \{0\}, \times)$ is a group– this is a multiplicative group (where the identity element is '1' as we know well).

• $(\mathbb{Z}, +)$ is an additive group.

• $(\mathbb{Z}, \times)$ is not a group. It seems 1 is a perfect candidate for the identity element (as it does the job in a bigger set $\mathbb{Q}$) but, for example, 2 does not have (multiplicative) inverse, i.e. there is no integer b such that $2 \times b = 1$!

• $(\{\text{The roots of } X^n - 1 \text{ in } \mathbb{C}\}, \times)$ is a multiplicative group (with identity element 1).

• $(\{\text{The roots of } X^n - 1 \text{ in } \mathbb{C}\}, +)$ is not a group.

• $(\{\text{The 2-by-2 invertible matrices with entries in } \mathbb{C}\}, \times)$ is a group but not an abelian group!

• $(\mathbb{Z}_n, +)$ is a group.

• $(\mathbb{Z}_n, \times)$ is not a group. The element $[1]$ satisfies (G2) but Theorem 12 proves that only those $[a]$ with $\gcd(a, n) = 1$ has (multiplicative) inverses, failing (G3).

• $(\mathbb{R}, *)$, where $*$ is defined as $a * b = a^2 b$, is not a group. (G2) fails for this example, i.e., there is no identity element. To see this, suppose that e is an element of $\mathbb{R}$ satisfying (G2). Firstly, $e * e = e$ yields $e^3 = e$. The only real numbers which satisfy this are $0, 1$ or -1. Secondly, for every element a in $\mathbb{R}$, the equality $a * e = e * a = a$ yields $a^2 e = e^2 a = a$. If $e = 0$, then $a = 0$ and this is false (as it says any element a of $\mathbb{R}$ is 0). If $e = 1$, then $a^2 = a$ forcing a to be either 0 or 1. If $e = -1$, then $-a^2 = a$ forcing a to be either 0 or -1.

• $(\mathbb{Z}_{\geqslant 1}, *)$, where $*$ is defined as $a * b = |a - b|$, is not a group. (G1) fails for this example. Indeed, $1 * (2 * 5) = 2$ but $(1 * 2) * 5 = 4$.

• Let S be a non-empty set. Let $\mathrm{Sym}(S)$ be the set of *bijective* functions $a : S \to S$ and $*$ be the composition $\circ$– if a and b are elements of G, then $a \circ b$ is the composite $S \xrightarrow{b} S \xrightarrow{a} S$ sending s to $a(b(s))$. Then $(\mathrm{Sym}(S), \circ)$ is a group.

(G0) If a and b are bijective, so is $a \circ b$. To see $a \circ b$ is injective, suppose $(a \circ b)(s) = (a \circ b)(s')$ for some elements s, s' of S (and aim at proving $s = s'$). By definition, $a(b(s)) = a(b(s'))$. Since a is injective, $b(s) = b(s')$. Since b is injective, $s = s'$ as desired. To prove $a \circ b$ is surjective, let s be an element of S (and aim at finding s'' such that $(a \circ b)(s'') = s$). Since a is surjective, there exists an element s' in S such that $a(s') = s$. Since b is surjective, there exists s'' in S such that $b(s'') = s'$. It then follows that $(a \circ b)(s'') = a(b(s'')) = a(s') = s$ by definition.

(G1) Let a, b, c be elements of $\mathrm{Sym}(S)$ (and aim at proving $a \circ (b \circ c) = (a \circ b) \circ c$). Indeed, $[a \circ (b \circ c)](s) = a((b \circ c)(s)) = a(b(c(s))) = (a \circ b)(c(s)) = [(a \circ b) \circ c](s)$.

(G2) The identity element is the identity map 'id' sending s to s. Then $(a \circ \mathrm{id})(s) = a(\mathrm{id}(s)) = a(s)$ and $(\mathrm{id} \circ a)(s) = \mathrm{id}(a(s)) = a(s)$.

(G3) If a is an element of $\mathrm{Sym}(S)$, then it follows from the surjectivity of a that, for any element s' of S, there exists s in S such that $a(s) = s'$. Note that this s is unique; indeed if r and s are elements of S satisfying $a(r) = s'$ and $a(s) = s'$, then $a(r) = a(s)$ holds. By injectivity of a, we have $r = s$. Granted, we define b to be the map that sends s' in S to the element s of S uniquely defined such that $a(s) = s'$– as is clear from the definition, this is well-defined only because a is bijective to start with. It remains for us to check that b fulfils the role of being the inverse of a. Since $(a \circ b)(s') = a(b(s')) = a(s) = s'$, we see that $a \circ b = \mathrm{id}$. Similarly, since $(b \circ a)(s) = b(a(s)) = b(s') = s$, we see that $b \circ a = \mathrm{id}$. This map b is often written as a^{-1}.

This last example formalises what we previously discussed as 'symmetries of an equilateral triangle' (where S is taken to be the vertices of the triangle and 'rotations' and 'reflections' are bijections). In fact, it underlies the historical development of the group theory:

Non-examinable Examples.

Symmetry groups of regular polygons (e.g. an equilateral triangle).

Symmetry groups of platonic solids.

Galois groups. E. Galois found a way to describe the solutions of a polynomial over $\mathbb{Q}$ in terms of a group. In fact, this was the motivation behind the development of group theory!

I find R. Borcherd's video https://www.youtube.com/watch?v=D908X1JAowY enlightening.

4.2 Elementary properties of groups

Proposition 14. Let $(G, *)$ be a group.

- The identity element of G is unique.
- Each element a of G has a unique inverse (written multiplicatively as a^{-1}).
- If $a * b = a * c$, then $b = c$. Similarly, if $b * a = c * a$, then $b = c$.
- For any a, b in G, then $(a * b)^{-1} = b^{-1} * a^{-1}$.

Proof. (1) If e and e' have properties that $e*a = a*e = a$ and $e'*a = a*e' = a$ for every element a of G, then $e * e' = e'$ (by letting $a = e'$ int the former) and $e * e' = e$ (by letting $a = e'$ in the latter). Combining, $e = e'$. (2) Let b and b' are elements of G has properties that $a * b = b * a = e$ and $a * b' = b' * a = e$. One observes that $b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'$. (3) Let a^{-1} be the inverse of a. It then follows that $a^{-1} * (a * b) = a^{-1} * (a * c)$. The LHS equals $(a^{-1}*a)*b = e*b = b$ and similarly the RHS equals $(a^{-1}*a)*c = e*c = c$. Hence $b = c$, as desired. The second assertion can be proved analogously. (4) The inverse $(a * b)^{-1}$ is the unique element c of G that satisfies $c * (a * b) = (a * b) * c = e$. Firstly, $(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1}*e*b = b^{-1}*b = e$. Secondly, $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = a*a^{-1} = e$. Since $b^{-1} * a^{-1}$ has the properties that uniquely characterise the inverse of $a * b$, we see that $(a * b)^{-1} = b^{-1} * a^{-1}$. □

4.3 Rings

Definition. A ring is a set R which comes equipped with two operations, $+$ (addition) and $\times$ (multiplication), satisfying the following axioms:

(R+0) If a, b are elements of R, then $a + b$ is an element of R.

(R+1) If a, b, c are elements of R, then $a + (b + c) = (a + b) + c$.

(R+2) There is an element 0 in R such that $a+0 = 0+a = a$ for every element of R– the element is sometimes referred to as the additive identity element, or the identity element with respect to $+$/addition.

(R+3) For every element a of R, there exists b in G such that $a + b = b + a = 0$.

(R+4) If a, b are elements of R, then $a + b = b + a$.

(R×0) If a, b are elements of R, then $a \times b$ is an element of R.

(R×1) If a, b, c are elements of R, then $a \times (b \times c) = (a \times b) \times c$.

(R×+) If a, b, c are elements of R, then

$$a \times (b + c) = a \times b + a \times c.$$

(R+×) If a, b, c are elements of R, then

$$(b + c) \times a = b \times a + c \times a.$$

Remark. The first five axioms say that $(G, *) = (R, +)$ is an additive (abelian) group.

Remark. As seen in groups, the operations $+$ and $\times$ are just symbols/names given to operations that satisfy a bunch of conditions that pin down $+$ and $\times$ on $\mathbb{Z}$ (it is precisely for this reason that the symbols '$+$' and '$\times$' are used conventionally). See examples below.

Remark. We often write ab instead of $a \times b$.

Definition. A ring R is said to be a commutative ring if $a \times b = b \times a$ holds for all a, b in R.

Examples.

• $\{0\}$, where 0 is the additive identity element in $\mathbb{Z}$ with addition $0 + 0 = 0$ and $0 \times 0 = 0$, is a (commutative) ring– this is the smallest ring there is.

• Let $(G, *)$ be an abelian group (with identity element e). Define $+$ in terms of $*$; and define $\times$ by $a \times b = e$ for all elements a, b in G. Then $(G, +, \times)$ is a commutative ring.

• $(\mathbb{Z}, +, \times)$ is a commutative ring.

• $(\{\text{The non-negative integers}\}, +, \times)$ is not a ring, because they do not have inverses with respect to $+$.

• $(\{\text{The positive integers}\}, +, \times)$ is not a ring, because there is no additive identity element '0'.

• The set $\mathbb{R}[X]$ of polynomials in one variable X with coefficients in $\mathbb{R}$ is a commutative ring (this may be thought of as infinitely many copies of $\mathbb{R}$). We will revisit this example again, so we will be brief. An element of $\mathbb{R}[X]$ is of the form $f = c_n(f)X^n + c_{n-1}(f)X^{n-1} + \cdots + c_1(f)X + c_0(f)$ and it is said to be a polynomial of degree $n = \deg(f)$ with coefficients $c_n(f), c_{n-1}(f), \ldots c_0(f)$ in $\mathbb{R}$, when c_n is non-zero.

• The set $\mathrm{M}_2(\mathbb{R})$ of n-by-n matrices with entries in $\mathbb{R}$ is a ring but not a commutative ring. More generally, if R is a ring, the set $\mathrm{M}_n(R)$ of n-by-n matrices with entries in R is a (non-commutative) ring.

• $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$ is a commutative ring with addition $(a + b\sqrt{-1}) + (c + d\sqrt{-1}) = (a + c) + (b + d)\sqrt{-1}$ and multiplication $(a + b\sqrt{-1})(c + d\sqrt{-1}) = (ac - bd) + (ad + bc)\sqrt{-1}$. This ring is often referred to as the Gaussian integers (named after F. Gauss). If you are suddenly gripped by the desired to know more, https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf might be enlightening.

• $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a commutative ring with addition $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$ and multiplication $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$.

• If R and S are rings, then the Cartesian product $R \times S = \{(r, s) \mid r \in R, s \in S\}$ is a ring by addition and multiplication on each coordiante.

• The set of all (resp. continuous, resp, differentiable etc.) functions on $\mathbb{R}$ to itself is a ring.

We shall see more examples and will study them in depth.

4.4 Elementary 'additive' properties of rings

Proposition 15. Let $(R, +, \times)$ be a ring.

- There is a unique zero element,

- Any element has a unique additive inverse.
- If $a + b = a + c$, then $b = c$.

Proof. This is proved in Proposition 14 (because $(R, +)$, amongst other thing, is an (additive) abelian group), but we spell out details, just in case.

Suppose that 0 and $0'$ are elements of R satisfying $a + 0 = 0 + a = a$ and $a + 0' = 0' + a = a$ for every element a of R. It suffices to show that $0 = 0'$. Letting $a = 0$ in the former, we obtain $(*)$ $0 + 0' = 0'$; while letting $a = 0$ in the latter, we obtain $(**)$ $0 + 0' = 0$. Combining $(*)$ and $(**)$, we have $0 = 0'$, as desired.

Suppose that b and b' are additive inverses of a, i.e. satisfying $a + b = b + a = 0$ and $a + b' = b' + a = 0$. To see $b = b'$, we observe $b = b + 0 = b + (a + b') = (b + a) + b' = 0 + b' = b'$.

To prove the last assertion, observe that $b = 0 + b = (-a + a) + b = -a + (a + b) = -a + (a + c) = (-a + a) + c = 0 + c = c$. □

Proposition 16. Let R be a ring. For every element a of R, we have $0a = a0 = 0$.

Proof. Since 0 is the additive identity, we have $0 + 0 = 0$ (by letting '$a = 0$' in the definition). Multiplying both sides by a, we get $a(0 + 0) = a0$. The LHS equals $a0 + a0$, while the RHS equals $a0 + 0$ (because 0 is the additive identity!). It therefore follows that $a0 + a0 = a0 + 0$. By Proposition 15, we then deduce that $a0 = 0$. A proof for $0a = 0$ is similar. □

4.5 Elementary 'multiplicative' properties of rings

Definition. Let R be a ring. If R has an element 1 (the multiplicative identity element) such that, for every a in R, we have $a \times 1 = 1 \times a = a$, then we say R is a ring with identity (commonly understood as *multiplicative* identity). The additive identity 0 and the multiplicative identity (if exists) do not have to be distinct.

Examples. Most of rings we have (and will have) seen have identity. To add a few,

- $\{0\}$ is a ring with identity– the additive and multiplicative identities are both 0.
- If R is a ring with identity, $\mathrm{M}_n(R)$ is a ring with identity $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$, where '1' is the identity element of R assured to exist by assumption.
- If R and S are rings with identity, so is $R \times S$ with identity $(1_R, 1_S)$.

Theorem 17. The set $\mathbb{Z}_n$, with addition and multiplication modulo n as defined before, is a commutative ring with identity [1].

Proof. See Chapter 3.

Examples (of rings without identity). It is not very easy to find rings without identity!

- The set of even integers is a ring (with respect to usual $+$ and $\times$) without identity– the set of odd integers is not even a ring!

• Let R be the set of continuous functions $f : \mathbb{R} \to \mathbb{R}$ such that $\int_0^\infty f < \infty$. This is a ring. However, the identity function 1 is not an element of R as $\int_0^\infty 1 = \infty$.

• $(G, *, \times)$ as seen above is not a ring with identity, unless $G = \{e\}$.

Definition. Let R be a ring with identity element 1. An element a in R is called a unit if there is an element b in R such that $ab = ba = 1$. The element b is called the inverse of b, and is written as a^{-1}.

Remark. If R is a ring with identity, an element a is a unit if and only if a has multiplicative inverse. To put it another way,

$$\{\text{units in } R\} = \{\text{elements in } R \text{ with multiplicative inverses}\}.$$

Definition. We will denote by $R^\times$ the units of R.

Examples.

• The units in $\mathbb{Z}$ are exactly $\{-1, 1\}$.

• The units in $M_2(\mathbb{R})$ are exactly the group $GL_2(\mathbb{R})$ of invertible (i.e. non-zero determinant) matrices. In fact, it can be n-by-n for any positive integer n, as well as $\mathbb{R}$ can be replaced by any field (to be defined shortly).

• $\mathbb{Z}[\sqrt{-1}]^\times = \{a + b\sqrt{-1} \mid a^2 + b^2 = 1\} = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$. To see this, observe that $a + b\sqrt{-1}$ is a unit if and only if there exist integers c, d such that $(a + b\sqrt{-1})(c + d\sqrt{-1}) = 1$. Taking the absolute values on both sides, we obtain $(a^2 + b^2)(c^2 + d^2) = 1$. Since $a^2 + b^2 \geqslant 0$, $a^2 + b^2 = 1$.

Proposition 18. The units of $\mathbb{Z}_n$ are the subset of equivalence classes $[a]$ in $\mathbb{Z}$ represented by integers a such that $\gcd(a, n) = 1$. Furthermore, $|\mathbb{Z}_n| = \phi(n)$.

Proof. See Theorem 12 in Chapter 3.

The following proposition puts together some of the key properties of the multiplicative identity 1.

Proposition 19. Let R be a ring with (multiplicative) identity 1.

- The identity element 1 is unique.
- If 1 is distinct from the additive identity 0, then 0 is NOT a unit.
- 1 is a unit and its inverse is 1 itself.

Proof. (1) This can be proved as in the proof of Proposition 14. Suppose that r and s are elements of R satisfying the properties $ra = ar = a$ and $sa = as = a$ for every element a of R. Letting $a = s$ in the former (resp. $a = r$ in the latter), we obtain $rs = s$ (resp. $rs = r$). Combining, we deduce $r = rs = s$. (2) If 0 were a unit, there exists a say, such that $a0 = 1$. On the other hand, Proposition 16 asserts that $a0 = 0$. This contradicts the assumption that $0 \neq 1$. Hence 0 is not a

unit. (3) $1 \times 1 = 1$, hence 1 is a unit and it is the inverse of itself. $\square$

Proposition 20. Let R be a ring with (multiplicative) identity 1.

- If a is a unit, the inverse of a is unique.
- If a is a unit, then so is a^{-1}– the inverse of a^{-1} is indeed a.
- If a and b are units, then so is ab; and its inverse is $b^{-1}a^{-1}$.

Proof. The assertions are proved as in the proof of Proposition 14. (1) Suppose that b and b' are elements of R such that $ab = ba = 1$ and $ab' = b'a = 1$. It then follows that $b = b \times 1 = b(ab') = (ba)b' = 1 \times b' = b'$ (because $ab' = 1$ and $ba = 1$ by assumption). (2) Since $aa^{-1} = a^{-1}a = 1$, a is the inverse of a^{-1}. (3) Since a (resp. b) is a unit, a^{-1} (resp. b^{-1}) is the unique element of R such that $aa^{-1} = a^{-1}a = 1$ (resp. $bb^{-1} = b^{-1}b = 1$). Then $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b = b^{-1}b = 1$. Also $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$. Therefore, ab is a unit and its inverse is $b^{-1}a^{-1}$ (by the uniqueness established above). $\square$

The frequency with which the proof of Proposition 14 was useful in proving statements in the propositions is suggestive of:

Theorem 21. If $(R, +, \times)$ is a ring with identity, $(R^\times, \times)$ is a group. If, furthermore, $(R, +, \times)$ is commutative, $(R^\times, \times)$ is abelian.

Proof. The last assertion of Proposition 20 shows (G0). (G1) follows by thinking of elements of $R^\times$ as elements of R (and make appeal to (R+1) for R). Since 1 is the (unique) element of R satisfying $1a = a1 = a$ for any element of R, it is certainly the case that $1a = a1 = a$ for any element of $R^\times$ (note that $R^\times$ is a subset of R), hence (G2) holds. The second assertion of Proposition 20 shows (G3). $\square$

We end this section (about rings) by an example and an exercise that I find very instructive. I strongly recommend you study these carefully.

Example. Let $(\mathbb{Z}, +, \times)$ be the ring of integers with usual addition $+$ and multiplication $\times$. Define new addition $\boxplus$:

$$a \boxplus b = a + b + 1$$

and new multiplication

$$a \boxtimes b = a + b + ab$$

in terms of old $+$ and $\times$. Then this is a commutative ring with identity, where the zero identity (the identity element with respect to addition, as prescribed by (R+2)) is -1 and the multiplicative identity is 0!

- (R+0) Since $a + b + 1 \in \mathbb{Z}$, we have $a \boxplus b = a + b + 1 \in \mathbb{Z}$.
- (R+1) On one hand,

$$a \boxplus (b \boxplus c) = a \boxplus (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 1.$$

On the other hand,

$$(a \boxplus b) \boxplus c = (a + b + 1) \boxplus c = (a + b + 1) + c + 1 = a + b + c + 1.$$

Therefore

$$a \boxplus (b \boxplus c) = (a \boxplus b) \boxplus c.$$

- (R+2) (-1) is the identity element with respect to $\boxtimes$. Indeed,

$$a \boxplus (-1) = a + (-1) + 1 = a$$

and

$$(-1) \boxplus a = (-1) + a + 1 = a.$$

[To find the identity, we need to find b in $\mathbb{Z}$ such that $a \boxplus b = a$ holds for any a. By definition, this is equivalent to finding b satisfying $a + b + 1 = a$, i.e. $b + 1 = 0$. Therefore $b = -1$.]

- (R+3) The inverse of a with respect to $\boxplus$ is $-a - 2$. Indeed,

$$a \boxplus (-a - 2) = a + (-a - 2) + 1 = -1$$

and

$$(-a - 2) \boxplus a = (-a - 2) + a + 1 = -1.$$

[To find the inverse of a, we need to find b such that $a \oplus b = -1$ (since -1 is the identity with respect to $\boxplus$!) for example. This is equivalent to $a + b + 1 = -1$, i.e., $b = -a - 2$.]

- (R+4)

$$a \boxplus b = a + b + 1 = b + a + 1 = b \boxplus a.$$

- (R×0) Since $a + b + ab \in \mathbb{Z}$, we have $a \boxtimes b = a + b + ab \in \mathbb{Z}$.

- (R× 1) On one hand,

$$a \boxtimes (b \boxtimes c) = a \boxtimes (b + c + bc) = a + (b + c + bc) + a(b + c + bc).$$

On the other hand,

$$(a \boxtimes b) \boxtimes c = (a + b + ab) \boxtimes c = (a + b + ab) + c + (a + b + ab)c.$$

It follows from (R+4), (R×1), (R×+) and (R+×) for $(\mathbb{Z}, +, \times)$ that

$$a \boxtimes (b \boxtimes c) = (a \boxtimes b) \boxtimes c.$$

- (R×+) On one hand,

$$a \boxtimes (b \boxplus c) = a \boxtimes (b + c + 1) = a + (b + c + 1) + a(b + c + 1).$$

On the other hand,

$$(a \boxtimes b) \boxplus (a \boxtimes c) = (a + b + ab) \boxplus (a + c + ac) = (a + b + ab) + (a + c + ac) + 1.$$

It then follows from (R+4), (R×+) and (R+×) for $(\mathbb{Z}, +, \times)$ that

$$a \boxtimes (b \boxplus c) = (a \boxtimes b) \boxplus (a \boxtimes c).$$

- (R+×) On one hand,

$$(b \boxplus c) \boxtimes a = (b + c + 1) \boxtimes a = (b + c + 1) + a + (b + c + 1)a.$$

On the other hand,

$$(b \boxtimes a) \boxplus (c \boxtimes a) = (b + a + ba) \boxplus (c + a + ca) = (b + a + ba) + (c + a + ca) + 1.$$

It then follows from (R+4), (R×+) and (R+×) for $(\mathbb{Z}, +, \times)$ that

$$(b \boxplus c) \boxtimes a = (b \boxtimes a) \boxplus (c \boxtimes a).$$

- $(\mathbb{Z}, \boxplus, \boxtimes)$ is commutative. Since $(\mathbb{Z}, +, \times)$ is a commutative ring,

$$a \boxtimes b = a + b + ab = b + a + ba = b \boxtimes a.$$

- The multiplicative identity with respect to $\boxtimes$ is 0. Indeed,

$$a \boxtimes 0 = a + 0 + a0 = a$$

and

$$0 \boxtimes a = 0 + a + 0a = a.$$

[To find this, we need to find b in $\mathbb{Z}$ such that $a \boxtimes b = a$ holds for every a. This is equivalent to finding b satisfying $a + b + ab = a$, i.e. $b(1 + a) = 0$, holds for every a. Therefore $b = 0$.]

The units of $(\mathbb{Z}, \boxplus, \boxtimes)$ are $\{0, -2\}$. To see this, we need to find integers a (and b) such that $a \boxtimes b = 0$, i.e. $a + b + ab = 0$. This is equivalent to $(a + 1)(b + 1) = -1$. Therefore, $(a + 1, b + 1)$ is either $(1, -1)$ or $(-1, 1)$. In other words, (a, b) is either $(0, -2)$ or $(-2, 0)$.

The following exercise taught me a lot about rings and abelian groups. I strongly recommend you have a go at it. This is another example of constructing a (commutative) ring out of (abelian) groups.

Exercise. Let $(G, *)$ is an abelian group with identity e. Given an element g in G and a positive integer n, we write ng to mean $g * \cdots * g$, where g is repeated n times, for brevity. Show that the set $R = \mathbb{Z} \times G$ of ordered pairs (n, g) of elements n in $\mathbb{Z}$ and g in G is a commutative ring with identity $(1, e)$ under the addition

$$(n, g) \boxplus (n', g') = (n + n', g * g')$$

and multiplication

$$(n, g) \boxtimes (n', g') = (nn', ng * n'g).$$

The units of $(R, \boxplus, \boxtimes)$ are $\{\pm 1\} \times G$.

4.6 Fields

Definition. A field is a *commutative* ring $(F, +, \times)$ satisfying the axioms

- $(F, +)$ is an additive group (with identity element 0)
- $(F - \{0\}, \times)$ is a multiplicative group (with identity element 1).
- The additive identity '0' (the identity element in the group $(F, +)$) is distinct from the multiplicative identity '1' (the identity element in the group $(F - \{0\}, \times)$).

Perhaps, it might be useful to spell out the field axioms: a field is a set F which comes equipped with addition $\times$ and multiplication+ which satisfy the following:

- It satisfies (R+0) through to (R+4) [which make $(F, +)$ an additive group with additive identity element 0), (R×0), (R×1), (R×+), (R+×) [which make $(F, +, \times)$ a ring]
- For all elements a and b, $a \times b = b \times a$ [which makes $(F, +, \times)$ a commutative ring]
- There exists an element, denoted 1 ,in F such that for every a in F, $1a = a1 = a$ holds– this is often referred to as the (multiplicative) identity element.
- For every a in $F - \{0\}$, there exists an element b in F such that $ab = ba = 1$– in which case, we write a^{-1} for b.
- $0 \neq 1$.

Remark. If $1 = 0$, then $a = 1 \times a = 0 \times a = 0$ (the last equality needs to be justified; see Proposition ?). So the condition $1 \neq 0$ denies any set with one element $\{1 = 0\}$ any chance of being a field.

Remark. By definition,

$$\text{Field} \Rightarrow \text{Ring} \Rightarrow \text{Group}$$

Remark. Groups encapsulate 'symmetry'. Why rings (and not fields)? In general, elements of a ring do not have (multiplicative) inverses and this is not a bad things and this actually makes rings interesting. For example, the division algorithm would be vacuous if everything in $\mathbb{Z}$ had an inverse (i.e. is divisible).

Examples.
• $\mathbb{Q}, \mathbb{R}$ are fields.
• $\mathbb{Z}$ is a ring but not a field. For example, 2 does not have a multiplicative inverse in $\mathbb{Z}$.

Theorem 22. If p is a prime number, then $\mathbb{F}_p = \mathbb{Z}_p$ is a field.

Proof. Firstly, $[0]$ is distinct from $[1]$. If not, p would divide 1 and consequently force p to be 1.

Suppose that $[a]$ is not equal to $[0]$. This means that p does not divide a. It follows that $\gcd(a, p) = 1$ and therefore $[a]$ has multiplicative inverse by Theorem 12. □

The field of complex number is a field. It is worth studying it carefully:

Definition. The set $\mathbb{C}$ of complex numbers is the set of elements of the form $a + b\sqrt{-1}$ where a, b are real numbers.

We define addition and multiplication on $\mathbb{C}$ by

$$(a + b\sqrt{-1}) + (c + d\sqrt{-1}) = (a + c) + (b + d)\sqrt{-1}$$

$$(a + b\sqrt{-1}) \times (c + d\sqrt{-1}) = (ac - bd) + (ad + bc)\sqrt{-1}.$$

Theorem 23. The set $\mathbb{C}$ is a field.

Proof. The non-trivial part of this exercise is to see any non-zero element of $\mathbb{C}$ has a multiplicative inverse. Let $a + b\sqrt{-1}$ is a non-zero element of $\mathbb{C}$– in which case, either a or b is non-zero, and therefore $a^2 + b^2$ is non-zero. It then follows that

$$\frac{a}{a^2 + b^2} + \frac{(-b)}{a^2 + b^2}\sqrt{-1}$$

is a non-zero element of $\mathbb{C}$ and one can check easily

$$(a + b\sqrt{-1}) \left(\frac{a}{a^2 + b^2} + \frac{(-b)}{a^2 + b^2}\sqrt{-1} \right) = 1$$

and

$$\left(\frac{a}{a^2 + b^2} + \frac{(-b)}{a^2 + b^2}\sqrt{-1} \right) (a + b\sqrt{-1}) = 1.$$

□

Remark. We spot the inverse by calculating

$$\frac{1}{a + b\sqrt{-1}} = \frac{(a - b\sqrt{-1})}{(a + b\sqrt{-1})(a - b\sqrt{-1})} = \frac{a}{a^2 + b^2} + \frac{(-b)}{a^2 + b^2}\sqrt{-1}$$

but we should be mindful that the inverse, or rather the symbol, '$\frac{1}{a + b\sqrt{-1}}$' makes sense only if we know that $\mathbb{C}$ is a field– the symbol $\frac{1}{a + b\sqrt{-1}}$ is *defined to be* the (unique) element of $\mathbb{C}$ which yields 1 when multiplied by the non-zero element $a + b\sqrt{-1}$, so without knowing $a + b\sqrt{-1}$ is invertible (i.e. has a multiplicative inverse) in advance, how can we make sense of the element?! It would be a catch 22! if our proof mentions $\frac{1}{a + b\sqrt{-1}}$ at all. To check that $a + b\sqrt{-1}$ is invertible, all we need is to spot an element of $\mathbb{C}$ that does the job and no one asks how we find it. Which is why, in the proof, we are pretending that we magically pull the element $\frac{a}{a^2 + b^2} + \frac{(-b)}{a^2 + b^2}\sqrt{-1}$ out of our hat!

(Subtext) Similarly, it is possible to prove that the set $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ (where addition and multiplication are defined analogously with $\sqrt{2}$ in place of $\sqrt{-1}$) is a field– indeed,

the multiplicative inverse of a non-zero element $a+b\sqrt{2}$ (by assumption, a and b are both non-zero) is

$$\frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a}{a^2-2b^2} + \frac{(-b)}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Note that a^2-2b^2 is never 0. To see this, suppose $a^2-2b^2=0$, i.e. $a^2=2b^2$ (and aim at finding contradiction). Ultimately, we may conclude from the fact that 2 is not a square of rational number (a/b in our case), but how do we formalise this argument?

4.7 Rings that are not fields

We have special names for rings which satisfy some, but not all, of the axioms a field needs to satisfy.

Definition. We say that a ring R with identity is called a division ring/skew field if it satisfies all the axioms except the commutativity of multiplication ($a \times b = b \times a$ for all a, b in R)– a field assumes the set of non-zero elements is an abelian group with respect to $\times$.

The name 'division ring' is justified by the following assertion:

Proposition 24. Let R be a division ring and a is non-zero element of R. If $ab = ac$, then $b = c$.

Proof. Since a is non-zero, it has an inverse a^{-1} in R. Multiplying $ab = ac$ by this, we get $b = c$. □

Example. Let $1, p, q, r$ are symbols subject to the 'multiplicative relations'

- $1p = p1 = p$, $1q = q1 = q$, $1r = r1 = r$
- $p^2 = -1, q^2 = -1, r^2 = -1$
- $pq = r, qp = -r$,
- $qr = p, rq = -p$,
- $rp = q, qr = -q$

The last three set of relations can be more succinctly described via

$$pqr = -1.$$

Indeed, combined with the first three sets of relations, it is possible to recover the last three (Exercise). Let $\mathbb{H}$ (often referred to as Hamilton's quaternions) be the set of elements of the form $c1 + c(p)p + c(q)q + c(r)r$ where $c, c(p), c(q), c(r)$ range over $\mathbb{R}$. In terms of natural addition and multiplication (prescribed by the conditions), $\mathbb{H}$ defines a division ring.

The table of (row)(column) is as follows:

	1	p	q	r
1	1	p	q	r
p	p	-1	r	$-q$
q	q	$-r$	-1	p
r	r	q	$-p$	-1

By assumption, $pq = -qp, qr = -rq, rp = -pr$ and therefore the ring is evidently non-commutative. The multiplicative inverse is 1 (the element of $\mathbb{H}$ given by $(c, c(p), c(q), c(r)) = (1, 0, 0, 0)$).

Let $a = c + c(p)p + c(q)q + c(r)r$ and $b = c - c(p)p - c(q)q - c(r)r$. It then follows that ab is the (non-negative) real number $\mathcal{R} = c^2 + c(p)^2 + c(q)^2 + c(r)^2$ (exercise!). Therefore, if a is non-zero, i.e. $c, c(p), c(q), c(r)$ are not simultaneously 0, then the inverse of a is

$$\frac{b}{\mathcal{R}} = \frac{1}{\mathcal{R}}\left(c - c(p)p - c(q)q - c(r)r\right) = \frac{1}{\mathcal{R}}c - \frac{1}{\mathcal{R}}c(p)p - \frac{1}{\mathcal{R}}c(q)q - \frac{1}{\mathcal{R}}c(r)r \in \mathbb{H}.$$

The element b plays the same role as the complex conjugation in $\mathbb{C}$!

Remark. If you are interested in how complex numbers and Hamilton's quaternions are related, you might find the following paper:

https://maa.org/sites/default/files/pdf/upload_library/22/Allendoerfer/0025570x.di021097.02p0154a.pdf

inspiring.

4.8 Groups, rings and fields from modular arithmetic

The set $\mathbb{Z}_n$ of equivalence classes with respect to 'congruence mod n' is a rich source of non-trivial examples of groups, rings and fields:

- $(\mathbb{Z}_n, +)$ is a group.
- $(\mathbb{Z}_n, +, \times)$ is a commutative ring with identity. There are $\phi(n)$ units in $\mathbb{Z}_n$.
- If n is a prime number p, then $\mathbb{Z}_p = \mathbb{F}_p$ is a field.

4.9 Properties of fields

If you are interested in these, take 'Further topics in algebra (Galois theory)'!.