UMD 403: Undergraduate Algebra

Patrick Brosnan

March 5, 2026

Chapter 1

Preliminaries

1.1 Overview

In Chapter 1, I set up some notation, introduce the well-ordered property of the natural numbers and, as an application of the well-ordered property, I also prove the Fundamental Theorem of Arithmetic (Theorem 1.8). The first proof I give is Zermelo's direct proof, which uses only the well-ordered property avoiding Euclid's Lemma (Lemma 1.9. As such, I think it is a good example of how powerful the well-ordered property can be. On the other hand, as the usual proof using Euclid's Lemma is nice too, I give the standard proof in Section 1.5.

1.2 Notation and Well-Ordered Property

Let's write $\mathbb{N} = \{0, 1, 2, \ldots\}$ for the set of natural numbers and $\mathbb{P} = \{1, 2, 3, \ldots\}$ for the set of positive natural numbers. Write $\mathbb{Z}$ for the set of all integers.

Definition 1.1. If a and b are integers, we write $a|b$ and say that a *divides* b if there exists an integer c such that $b = ac$. If $a|b$, then a is called a *divisor* of b, and b is called a *multiple* of a.

Proposition 1.2. *Suppose a, b, c, x and y are all integers.*

1. *If $a|b$ and $b|c$, then $a|c$.*
2. *If $a|b$ and $a|c$, then $a|(xa + yb)$.*

Proof. Exercise. □

Axiom 1.3 (Well-ordered property of $\mathbb{P}$)**.** *Any nonempty subset S of $\mathbb{P}$ has a smallest element.*

Remark 1.4. As Gallian points out in his text, Axiom 1.3 is pretty much equivalent to the principle of mathematical induction.

Definition 1.5. A *prime number* is a positive integer p, which has exactly two positive divisors. An integer $n > 1$, which is not prime is said to be *composite*.

Proposition 1.6. *Suppose $n \in \mathbb{P}$.*

1. *n is prime if and only if it has exactly two positive divisors. Moreover, when n is prime, the two positive divisors are exactly 1 and n itself.*
2. *n is composite if and only there exist positive integers a and b, both less than n, such that $n = ab$.*

Proof. Exercise. □

Let's say that a prime factorization of an integer $n \in \mathbb{P}$ is a list $[p_1, p_2, \ldots, p_r]$ of prime numbers such that

1. $p_1 \leq p_2 \leq \cdots \leq p_r$, and
2. $n = p_1 \ldots p_r$.

We allow the empty list [] of prime numbers with the convention that the product of the empty list is 1. Under this convention, 1 has a prime factorization (it's just empty).

We say that a positive integer n has a unique prime factorization if any two prime factorizations of n are equal. Explicitly, this means that, if $[p_1, \ldots, p_r]$ and $[q_1, \ldots, q_s]$ are both prime factorizations of n, then $r = s$ and $p_i = q_i$ for all $i = 1, \ldots, r$.

Finally, note that if $[p_1, \ldots, p_r]$ is any list of primes satisfying (2) above, we can sort it to get a list of primes satisfying (1) as well. We'll do that below (possibly sometimes without even mentioning it).

1.3 Existence

Proposition 1.7. *Every $n \in \mathbb{P}$ has a prime factorization.*

Proof. Suppose not. Then the set S of positive integers not having a prime factorization is nonempty. So, by the well-ordered axiom, Axiom 1.3, there exists a smallest element $n \in S$. We've seen that 1 has a prime factorization, namely, the empty list or primes []. So $n > 1$. Obviously, n can't be prime: otherwise $[n]$ would be a prime factorization of n. As $n > 1$ and n is not prime, n must be composite. Therefore $n = ab$ with $1 < a \leq b < n$. As n is, by assumption, the smallest positive integer without a prime factorization, a and b both have prime factorizations $[p_1, \ldots, p_r]$ and $[q_1, \ldots, q_s]$ respectively. So

$$n = (p_1 p_2 \cdots p_r)(q_1 q_2 \cdots q_s).$$

Sorting the list $[p_1, \ldots, p_r, q_1, \ldots, q_s]$ to arrange the elements in order, we get a prime factorization of n. As this contradicts our assumption that n is the smallest integer without a prime factorization, Proposition 1.7 is proved. □

1.4 Uniqueness

Theorem 1.8 (Fundamental Theorem of Arithmetic)**.** *Every $n \in \mathbb{P}$ has a unique prime factorization.*

Proof. We've already proved the existence of a prime factorization. So, now, we only have to prove uniqueness. As in the proof of existence, we work by contradiction using the Axiom 1.3. So suppose Theorem 1.8 is not true. Then there is a positive integer n with two distinct prime factorizations. So, by Axiom 1.3, we can find a smallest such positive integer n.

It's easy to see that [] is the only prime factorization of 1. (The point is that, $x, y > 1 \Rightarrow xy > 1$.) So $n > 1$, and n has two distinct prime factorizations $p = [p_1, \ldots, p_r]$ and $q = [q_1, \ldots, q_s]$, and, by switching p and q if necessary, we can assume $p_1 \leq q_1$.

First assume $p_1 = q_1$. Then $a := p_2 \cdots p_r = q_2 \cdots q_s < n$. So, by the minimality of n, a has a unique prime factorization. Therefore, $[p_2, \ldots, p_r] = [q_2, \ldots, q_s]$. But then, obviously, $[p_1, \ldots, p_r] = [q_1, \ldots, q_s]$ as $p_1 = q_1$, and this contradicts the assumption that p and q were two distinct prime factorizations of n.

Therefore, we must have $p_1 < q_1$. So set $m := (q_1 - p_1)q_2 \cdots q_s$. Then $1 \leq m < n$. By the minimality of n, m has a unique prime factorization. My strategy is to get a contradiction by showing that, in fact, m has two distinct prime factorizations.

First, let $u = [u_1, \ldots, u_t]$ be a (possibly empty) prime factorization of $q_1 - p_1$. If $p_1 = u_i$ for some i, then $p_1 | (q_1 - p_1)$ and, since $q_1 = p_1 + (q_1 - p_1)$, this implies that $p_1 | q_1$. But as $1 < p_1 < q_1$ and q_1 is prime, this is impossible. So, we see that p_1 cannot be equal to any of the u_i. And p_1 is not equal to any of the q_i either as $p_1 < q_1 \leq q_i$ for all i. So, by sorting the list $[u_1, \ldots, u_t, q_2, \ldots, q_s]$, we get a prime factorization of m in which p_1 does not appear.

On the other hand, we have

$$\begin{aligned} m &= (q_1 - p_1)q_2 \ldots q_s \\ &= q_1 q_2 \ldots q_s - p_1 q_2 \ldots q_s \\ &= n - p_1 q_2 \ldots q_s \\ &= p_1 p_2 \ldots p_r - p_1 q_2 \ldots q_s \\ &= p_1(p_2 \ldots p_r - q_2 \ldots q_s). \end{aligned}$$

So, as $\ell := p_2 \ldots p_r - q_2 \ldots q_s \in \mathbb{P}$, we can factor ℓ into primes and this gives rise to a prime factorization of m containing p_1. Therefore, m has two distinct prime factorizations, one not containing p_1 and one containing p_1. As $m < n$, this contradicts the minimality of n and prove the theorem. □

1.5 Euclid's Lemma and the more standard uniqueness proof

The usual proof of the Fundamental Theorem is based on the following result, which Gallian calls Euclid's Lemma.

Lemma 1.9 (Euclid's Lemma)**.** *Suppose p is a prime number and $a, b \in \mathbb{Z}$. If $p|ab$, then p divides either a or b.*

I'll prove this in class. Here's a (pretty obvious) corollary.

Corollary 1.10. *Suppose p is a prime number and $a_1, \ldots, a_r$ is a nonempty list of integers. If $p| \prod_{i=1}^{r} a_i$, then there exists $i = 1, \ldots, r$ such that $p|a_i$.*

Proof. Induct on r. It's obvious if $r = 1$, and it is just the statement of Lemma 1.9 when $r = 2$. So assume it holds for r, and let $a_1, \ldots, a_{r+1}$ be a nonempty list of integers such that $p| \prod_{i=1}^{r+1} a_i$. Then, since we know the result when $r = 2$, either $p| \prod_{i=1}^{r} a_i$ or $p|a_{r+1}$. In the first case, we're done by the induction hypothesis. In the second case, it's just obvious that we're done. □

Standard Proof of uniqueness part of Theorem 1.8. As in the first proof, assume, to get a contradiction, that Theorem 1.8 does not hold. Then we can find a positive integer n with two distinct prime factorizations $p = [p_1, \ldots, p_r]$ and $q = [q_1, \ldots, q_s]$. As we noted in the beginning of the first proof, it is easy to see that [] is the unique prime factorization of 1. So $n > 1$. Moreover, using Axiom 1.3 we can assume that n is the smallest positive integer with two distinct prime factorizations, and, by switching p and q if necessary, we can assume that $p_1 \leq q_1$. Then $p_1|n$. So, by Corollary 1.10, $p_1|q_i$ for some i. Since q_i is prime and $p_1 > 1$, this implies that $p_1 = q_i$. So, then $p_1 \leq q_1 \leq q_i = p_1$, and this implies that $p_1 = q_1$. But then $p_2 \cdots p_r = q_1 \cdots q_s$. So, by the minimality of n, $r = s$ and $p_i = q_i$ for all $i = 2, \ldots, r$. So, in fact, $p = q$. This contradicts our assumption that n has two distinct prime factorizations. So the theorem is proved. □

1.6 Attempt at getting the history right

You really shouldn't trust wikipedia, but I looked up some of the history of the Fundamental Theorem of Arithmetic and verified it as carefully as I could using the books I have.

Lemma 1.9 is basically Proposition 30 of Book VII of Euclid. The proof really is very similar to the one Gallian gives, which is basically the one I'll give in class. Euclid never proved or even stated Theorem 1.8. The closest he came is Proposition 14 of Book IX, which says that the smallest positive integer n divisible by primes $p_1, \ldots, p_r$ is not divisible by any other primes.

Apparently, Theorem 1.8 was first stated by Kama al Din al-Farisi, who lived 1267 – 1319.

Gauss gave a proof of uniqueness in Article 16 of his book *Disquisitiones Arithmeticae*. Wikipedia mistakenly claims that Gauss's proof uses modular arithmetic. This isn't true. What Gauss does is this: he notes that, by Euclid's Lemma, if $n > 1$ is an integer with two distinct prime factorizations, then the set of primes appearing in each factorization must be the same, only the values of the positive exponents can possibly be different. So for example, you could conceivably have $n = p_1^{a_1} \cdots p_r^{a_r} = p_1^{b_1} \cdots p_r^{b_r}$, with $b_1 > a_1$. But then $A := n/p_1^{a_1}$ would have two prime factorizations $A = p_2^{a_2} \cdots p_r^{a_r}$ and $A = p_1^{b_1 - a_1} p_2^{b_2} \cdots p_r^{b_r}$, and p_1 would appear in the second prime factorization, but not in the first contradicting Euclid's Lemma.

One last piece of history: The nonstandard proof I gave is given on the Wikipedia page for the Fundamental Theorem of Algebra under the heading "Uniqueness without Euclid's Lemma". It also seems to have been known for quite a long time. Apparently, it is due to Ernst Zermelo (1871 – 1953), who discovered it sometime around 1900 but didn't publish it until 1934.

1.7 The division algorithm with remainder

Theorem 1.11. *Let $n \in \mathbb{Z}$ and let $d \in \mathbb{P}$. Then there there exists integers q and r such that*

1. $n = qd + r$.
2. $0 \leq r < d$.

Moreover, the integers q and r are unique. The integer q is called the quotient *and the integer r is called the remainder. We write* $\mathrm{Mod}(n, d) := r$.

Proof. Let S denote the set of all nonnegative integers, which can be written in the form $n - qd$ with $q \in \mathbb{Z}$.

If $n > 0$, then the set S is obviously nonempty as $n \in S$. If $n = 0$, then, taking $q = -1$, we see that $d \in S$. And, if $n < 0$, then, taking $q = -n$, we see that $-n(1 + d) \in S$.

So we can find a smallest element $r \in S$ and write it in the form $r = n - qd$. By definition, r satisfies (1). On the other hand, if $r \geq d$, then $0 \leq n - qd - d = n - (q + 1)d = r - d < r$, which is a contradiction. So r satisfies (2) as well.

To see uniqueness, suppose $n = q_1 d + r_1 = q_2 d + r_2$ with both (q_1, d_1) and (q_2, r_2) satisfying the properties satisfied by (q, d) in (1) and (2). Without loss of generality, we can assume that $r_1 \leq r_2$. And then we have $0 \leq r_2 - r_1 < d$. Then, since $q1d + r_1 = q_2 d + r_2$, we have that $(q_1 - q_2)d = (r_2 - r_1)$. And since $0 \leq r_2 - r_1 < d$, this implies that $r_2 - r_1 = q_1 - q_2 = 0$ proving the uniqueness of the pair (q, r) in the theorem. □

One of the nice things about the proof of Theorem 1.11 is that it gives an algorithm to compute q and r. It's not a very effective one. But here's what it says in the case that $n > 0$:

1. Set $r = n$ and $q = 0$.

2. If $r < d$, stop. Otherwise, replace r by $r - d$ and q by $q + 1$.

3. Repeat step 2 until you stop.

Another nice thing about the proof is that it stays within integers.

But there's another way to think about the division algorithm if we're willing to use the rational (or even real) numbers.

Definition 1.12. Suppose $x \in \mathbb{R}$. The *floor* $\lfloor x \rfloor$ of x is the largest integer n such that $n \leq x$.

The existence of the floor $\lfloor x \rfloor$ follows from a variant of the well-ordered property of $\mathbb{N}$. (It is also basically obvious.) Moreover, we have

Lemma 1.13. *If $x \in \mathbb{R}$, then $x - 1 < \lfloor x \rfloor \leq x$.*

Proof. Exercise. □

Proposition 1.14. *Suppose $n \in \mathbb{Z}$ and $d \in \mathbb{P}$. Write $n = qd + r$ as in Theorem 1.11. Then $q = \lfloor n/d \rfloor$ and $r = n - qd = n - d\lfloor n/d \rfloor$.*

Proof. From Lemma 1.13, we get that

$$\frac{n}{d} - 1 < \lfloor \frac{n}{d} \rfloor \leq \frac{n}{d}.$$

Multiplying through in the above equation by d and then subtracting the answers from n, we get that

$$0 = n - d\left(\frac{n}{d}\right) \leq n - d\left\lfloor \frac{n}{d} \right\rfloor < n - d\left(\frac{n}{d} - 1\right) = d.$$

So we're done by the uniqueness of q and r in Theorem 1.11. □

1.8 Greatest common divisor and least common multiple

Chapter 2

Binary operations, monoids and groups

2.1 Binary Operations

Definition 2.1. Let M be a set. A *binary operation* on M is a function

$$\cdot : M \times M \to M$$

often written $(x, y) \mapsto x \cdot y$. A pair $(M, \cdot)$ consisting of a set M and a binary operation $\cdot$ on M is called a *magma*.

Example 2.2. Let $M = \mathbb{Z}$ and let $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be the function $(x, y) \mapsto x + y$. Then, $+$ is a binary operation and, consequently, $(\mathbb{Z}, +)$ is a magma.

Example 2.3. Let n be an integer and set $\mathbb{Z}_{\geq n} := \{x \in \mathbb{Z} \,|\, x \geq n\}$. Now suppose $n \geq 0$. Then, for $x, y \in \mathbb{Z}_{\geq n}$, $x+y \in \mathbb{Z}_{\geq n}$. Consequently, $\mathbb{Z}_{\geq n}$ with the operation $(x, y) \mapsto x + y$ is a magma. In particular, $\mathbb{Z}_+$ is a magma under addition.

Example 2.4. Let $S = \{0, 1\}$. There are $16 = 4^2$ possible binary operations $m : S \times S \to S$. Therefore, there are 16 possible magmas of the form (S, m).

Example 2.5. Let n be a non-negative integer and let $\cdot : \mathbb{Z}_{\geq n} \times \mathbb{Z}_{\geq n} \to \mathbb{Z}_{\geq n}$ be the operation $(x, y) \mapsto xy$. Then $\mathbb{Z}_{\geq n}$ is a magma. Similarly, the pair $(\mathbb{Z}, \cdot)$ is a magma (where $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is given by $(x, y) \mapsto xy$).

Example 2.6. Let $M_2(\mathbb{R})$ denote the set of 2×2 matrices with real entries. If

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \text{ and } B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

are two matrices, define

$$A \circ B = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Then $(M_2(\mathbb{R}), \circ)$ is a magma. The operation $\circ$ is called *matrix multiplication*.

Definition 2.7. If $(M, \cdot)$ is a magma, then M is called the *underlying set* and $\cdot$ is called the *binary operation* or sometimes the *multiplication*.

Remark 2.8. There is a substantial amount of abuse of notation that goes along with binary operations. For example, suppose $(M, \cdot)$ is a magma and $m, n \in M$. Instead of writing $m \cdot n$ we often omit the $\cdot$ from the notation and write mn as in Example 2.5. Moreover, when referring to a magma $(M, \cdot)$, we often simply refer to the underlying set M and write the binary operation as $(x, y) \mapsto xy$. That way we avoid having to write down a name for the binary operation. So, for example, we say, "let M be a magma" when we should really say, "let $(M, \cdot)$ be a magma." We use this abuse of notation in the following definition.

Definition 2.9. Let M be a magma. We say that M is *commutative* if, for all $x, y \in M$, $xy = yx$. We say that M is *associative* if, for all $x, y, z \in M$, $(xy)z = x(yz)$. An element $e \in S$ is an *identity* element if, for all $m \in M$, $em = me = m$.

Example 2.10. There is another important product on $M_2(\mathbb{R})$ called the *Lie bracket*. It is given by $(A, B) \mapsto [A, B] := A \circ B - B \circ A$. It is *not* associative. To see this, set

$$A = B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Then

$$[[A, B], C] = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

but

$$[A, [B, C]] = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix},$$

We write $\mathfrak{gl}_2(\mathbb{R})$ for the magma consisting of the set $M_2(\mathbb{R})$ equipped with the Lie bracket binary operation.

Remark 2.11. If M is a commutative magma, then sometimes we write the binary operation as $(m, n) \mapsto m + n$. We never use the symbol "+" for a binary operation which is not commutative. Also, if the binary operation is written "+," we never omit it from the notation. For example, while we write 3×5 as $(3)(5)$, we never write $3 + 5$ as $(3)(5)$.

Proposition 2.12. *Let M be a magma. Then there is at most one identity element $e \in S$.*

Proof. Suppose e, f are identity elements. Then $e = ef = f$. □

Remark 2.13. If M is a commutative magma with binary operation $+$ then it is traditional to let the symbol "0" denote the identity element. Otherwise, it is traditional to use the symbol "e" or the symbol "1."

2.1.1 Multiplication Tables

If $M = \{x_1, x_2, \ldots, x_n\}$ is a finite set and "$\cdot$" is a binary operation on M. The *multiplication table* for M is the following $n \times n$-table of elements of M:

$$\begin{pmatrix} x_1x_1 & x_1x_2 & \cdots & x_1x_n \\ x_2x_1 & x_2x_2 & \cdots & x_2x_n \\ \cdots & \cdots & & \cdots \\ x_nx_1 & x_nx_2 & \cdots & x_nx_n \end{pmatrix}$$

Note that M is commutative if and only if the multiplication table is symmetric (in the sense that $x_ix_j = x_jx_i$ for all i, j).

Remark 2.14. The magma $(\mathbb{Z}, +)$ is associative and has 0 as its identity element. The magma $(\mathbb{N}, +)$ is also associative with 0 as its identity element. If $n > 0$, then the magma $(\mathbb{Z}_{\geq n}, +)$ is associative, but does not have an identity element.

The following definition is motivated by computer science.

Definition 2.15. Suppose k is a positive integer and S is a set. A *word of length* k in S is a k-tuple $\mathbf{m} = (m_1, \ldots, m_k)$ of elements of S. If $\mathbf{a} = (a_1, \ldots, a_i)$ and $\mathbf{b} = (b_1, \ldots, b_j)$ are two words of length i and j respectively then the *concatenation* of $\mathbf{a}$ and $\mathbf{b}$ is the word $\mathbf{a}.\mathbf{b} := (a_1, \ldots, a_i, b_1, \ldots, b_j)$.

We write $W_k(S)$ for the set of words of length k in S. So $W_k(S)$ is just equal to the set S^k. We write $W(S) = \cup_{k=1}^{\infty} W_k(S)$ for the union of the sets $W_k(S)$. An element of $W(S)$ is called a *word in* S. Then concatenation is a binary operation

$$W(S) \times W(S) \to W(S) \text{ given by}$$
$$(\mathbf{a}, \mathbf{b}) \mapsto \mathbf{a}.\mathbf{b}.$$

This makes $W(S)$ into a magma, which called the *magma of words in* S.

Definition 2.16. Suppose M is a magma and $\mathbf{m}$ is a word of length $k > 0$ in M. We define a set $P(\mathbf{m})$ of products of $\mathbf{m}$ inductively as follows. If $k = 1$, then $P(\mathbf{m}) = \{m_1\}$. Suppose then inductively that $P(\mathbf{n})$ is defined for every word $\mathbf{n}$ of length strictly less than $\mathbf{m}$. Then $P(\mathbf{n})$ is the set of all products xy where $x \in P(\mathbf{a}), y \in P(\mathbf{b})$ and $\mathbf{n} = \mathbf{a}.\mathbf{b}$.

Theorem 2.17. *Suppose M is an associative magma, and $\mathbf{m} = (m_1, \ldots, m_k)$ is a word in M of length $k > 0$. Then $P(\mathbf{m})$ consists of a single element.*

Proof. We induct on k. For $k = 1$ the theorem is obvious. So suppose that $k > 1$ and the theorem is known for all words of length strictly less than k. Write $\mathbf{h} = (m_1, \ldots, m_{k-1})$ and $\mathbf{t} = m_k$. Then, by induction, $P(\mathbf{h})$ consists of a single element u and $P(\mathbf{t})$ obviously consists of the single element m_k. Since $\mathbf{m} = \mathbf{h}.\mathbf{t}$, $um_k \in P(\mathbf{m})$. Now suppose $z \in P(\mathbf{m})$. By definition, $z = xy$ where $x \in P(\mathbf{a}), y \in P(\mathbf{b})$ with $\mathbf{m} = \mathbf{a} \cdot \mathbf{b}$. Suppose $\mathbf{a} = (m_1, \ldots, m_i)$ and $\mathbf{b} = (m_{i+1}, \ldots, m_k)$. Since $1 \leq i < k$, $P(\mathbf{b})$ consists of a single element. So, setting $\mathbf{b}' = (m_{i+1}, \ldots, m_{k-1})$, we have $y = y'm_k$ where y' is the unique element of $P(\mathbf{b}')$. Then xy' is an element of $P(\mathbf{h})$, so it is equal to u. So, by associativity, we have $z = xy = x(y'm_k) = (xy')m_k = um_k$. □

Definition 2.18. If M is an associative magma and $\mathbf{m} = (m_1, \ldots, m_k)$ is a word in M of length $k > 0$, then we write $\Pi(\mathbf{m})$ or simply $m_1 m_2 \cdots m_k$ for the unique element of $P(\mathbf{m})$.

Exercises

Exercise 2.19. An element l of a magma M is called a *left identity* if, for all $m \in M$, $lm = m$. Similarly, an element r of a magma M is called a *right identity* if, for all $m \in M$, $mr = m$. Suppose M is a magma having a left identity l and a right identity r. Show that $l = r$ and that l is the identity element of the magma.

Exercise 2.20. The cross product on $\mathbb{R}^3$ is the binary operation given by

$$(x_1, y_1, z_1) \times (x_2, y_2, z_2) = (y_1 z_2 - y_2 z_1, z_1 x_2 - z_3 x_1, x_1 y_2 - x_2 y_1).$$

Show that the cross product is neither associative nor commutative. Then show that it has no identity element.

2.2 Monoids and Groups

Definition 2.21. A *monoid* is an associative magma which has an identity element.

Example 2.22. The natural numbers form a monoid under addition. This means that $(\mathbb{N}, +)$ is a monoid. The natural numbers also form a monoid under multiplication: $(\mathbb{N}, \cdot)$ is a monoid. The identity element of $(\mathbb{N}, +)$ is 0 and the idenitity element of $(\mathbb{N}, \cdot)$ is 1.

The default notation is to write 1 for the identity element of a monoid M *unless* the binary operation on M is written as $+$. If the binary operation is written as $+$, the default is to write 0 for the identity element. Occasionally, when the binary operation is not written as $+$, other symbols are used for the identity element. For example, the symbol e is common (but not as common as the symbol 1). When we need to be clear that 1 refers to the identity element of a particular magma M, we sometimes write 1_M. For example, we do this in the next definition.

Proposition 2.23. *Let M be a monoid and $a, b \in M$. Suppose $ab = ba = 1$. Then, for $c \in M$, the following are equivalent.*

1. *$ac = 1$;*
2. *$ca = 1$;*
3. *$b = c$.*

Proof. (iii)$\Rightarrow$ (i) and (iii) $\Rightarrow$ (ii) are both obvious from the hypothesis. To see that (i)$\Rightarrow$ (iii), suppose $ac = 1$. Then $b = b1 = b(ac) = (ba)c = 1c = c$. To see that (ii)$\Rightarrow$ (iii), apply (i)$\Rightarrow$ (iii) to M^{op}. $\square$

Definition 2.24. Let M be a monoid. An element of $m \in M$ is *invertible* if there exists an $n \in M$ such that $mn = nm = 1$. I write $M^\times$ for the set of $m \in M$ such that m is invertible.

Note that, by Proposition 2.23, if m is invertible then m has a unique inverse. If M is a commutative and the binary operaiton is written as $(m, n) \mapsto m + n$, then it is traditional to denote let $-m$ denote the inverse of m. Otherwise it is traditional to write m^{-1} for the inverse.

Proposition 2.25. *Suppose M is a monoid. Then*

1. *If $x, y \in M^\times$, then $xy \in M^\times$ with $(xy)^{-1} = y^{-1}x^{-1}$;*
2. *$M^\times$ is a submonoid of M;*
3. *if $m \in M^\times$ then $(m^{-1})^{-1} = m$. Moreover, $(M^\times)^\times = M^\times$, and*
4. *$(M^\times)^\times = M^\times$.*

Proof. Exercise. □

Definition 2.26. A monoid M is a *group* if $M = M^\times$.

From Exercise 2.25, it follows that, if M is a monoid, $M^\times$ is a group.

Example 2.27. Here are the prototypical examples of monoids and groups. Let X be a set. Write $E(X)$ for the set of all functions $f : X \to X$. Equip $E(X)$ with the binary operation $(f, g) \mapsto f \circ g$. Then $E(X)$ is a monoid because composition of functions is associative and $\mathrm{id}_X \circ f = f \circ \mathrm{id}_X = f$ for all $f \in \operatorname{End} X$. Write $A(X)$ for $E(X)^\times$. Then $A(X)$ is called the *automorphism group* of X or the *group of permutations of X*.

Proposition 2.28. *Suppose $f \in E(X)$, where X is a set. Then $f \in A(X)$ if and only if the map $f : X \to X$ is one-one and onto.*

Proof. By definition, a map $f : X \to X$ is in $A(X)$ if and only if there exists a $g : X \to X$ such that $f \circ g = g \circ f = \mathrm{id}_X$. But this condition is equivalent to the condition that f is one-one and onto. □

2.3 Submagmas, submonoids and subgroups

Definition 2.29.

1. Suppose M is a magma and $N \subseteq M$. We say that N is an *submagma* of M if N is closed under the binary operation on M. In other words, N is a submagma if, for all $x, y \in N$, $xy \in N$.
2. Suppose M is a monoid with identity element 1 and $N \subseteq M$. We say N is a *submonoid* if N is a submagma of M and $1 \in N$.
3. Suppose M is a group and $N \subseteq M$. We say that N is a subgroup of M and write $N \leq M$ if N is a submonoid of M, which is closed under the operation of taking inverses. In other words, N is a subgroup if N is a submonoid of M and, for all $x \in N$, $x^{-1} \in N$.

If G is a group and $H \subseteq G$, we say that H is a *proper subgroup* of G and write $H < G$ if $H \leq G$ but $H \neq G$.

Proposition 2.30. *Suppose G is a group and $H \subseteq G$. Then $H \leq G$ if and only if the following three properties hold:*

1. $1 \in H$.
2. $x, y \in H \Rightarrow xy \in H$.
3. $x \in H \Rightarrow x^{-1} \in H$.

Proof. Exercise. Just unravel the defintions in Defintion 2.29. □

Theorem 2.31 (One step subgroup test)**.** *Suppose G is a group and $H \subseteq G$. Then $H \leq G$ if and only if the following two properties hold:*

1. $H \neq \emptyset$.
2. $x, y \in H \Rightarrow xy^{-1} \in H$.

Proof. ($\Rightarrow$) Assume that $H \leq G$. Then (1) holds because $1 \in H$. Moreover, if x, $y \in H$, then $y^{-1} \in H$ by Proposition 2.30(3). So $xy^{-1} \in H$ by Proposition 2.30(2).

($\Leftarrow$) Suppose that H satisfies Theorem 2.31 (1) and (2). Since $H \neq \emptyset$, we can find $h \in H$. Then, by (2), $1 = hh^{-1} \in H$. So H satisfies Proposition 2.30(1). Consequently, if $x \in H$, then $x^{-1} = 1x^{-1} \in H$ by (2). So H satisfies Proposition 2.30(3). Finally, suppose $x, y \in H$. Then $y^{-1} \in H$ by what we've just seen. So, applying (2) again, we see that $xy = x(y^{-1})^{-1} \in H$ showing that H satisfies Proposition 2.30(2). □

Suppose G is a group with identity element e. Then G and $\{e\}$ are both subgroups of G. The subgroup $\{e\}$ is called the *trivial subgroup* of G. We say that G is *the trivial group* if $G = \{e\}$.

2.4 The monoid of subsets of a monoid

Suppose X is a set. We write $\mathcal{P}(X)$ for the set of all subsets of X. The set $\mathcal{P}(X)$ is often called the *power set* of X. If X is a finite set with n elements, then $\mathcal{P}(X)$ has 2^n elements. Because of this we sometimes write 2^X for $\mathcal{P}(X)$ even when X is not finite.

If $(M, *)$ is a magma, we can define a binary operation on the power set $\mathcal{P}(M)$ by setting

$$S * T = \{s * t : s \in S, t \in T\} \tag{2.32}$$

for S, $T \subseteq M$.

Remark 2.33. Usually, we just write ST instead of $S*T$, except when the binary operation $*$ on M is called $+$. In that case, we always write $S + T$.

Proposition 2.34. *Suppose M is a monoid with identity element 1. Then $\mathcal{P}(M)$ with the binary operation defined above is also a monoid with identity element $\{1\}$.*

Proof. Suppose $X \subseteq M$. Then $X\{1\} = \{x1 : x \in X\} = \{x : x \in X\} = X$. And similarly, $\{1\}X = X$. This shows that $\{1\}$ is the (necessarily unique) identity element of the magma $\mathcal{P}(M)$.

On the other hand, if X, Y and Z are subsets of M, then it's easy to see that $X(YZ) = \{xyz : x \in X, y \in Y, z \in Z\} = (XY)Z$. □

Suppose $m \in M$ and $X \subseteq M$. Then we sometimes abuse notation and write $mX = \{m\}X$ and $Xm = X\{m\}$. It should be clear from the context when we do this. Of course, if the binary operation is written as "+," then we write $X + m = X + \{m\}$ or $m + X = \{m\} + X$.

Proposition 2.35. *Suppose $S \subseteq M$ and n is a positive integer. Then $S^n = \{s_1 s_2 \cdots s_n : \forall i, s_i \in S\}$.*

Proof. By definition, $S^0 = \{1\}$ and, for $n > 0$, $S^n = SS^{n-1}$. So $S^1 = S1 = S$.

Now, let's prove the proposition by induction on n starting with $n = 1$. We've already proved the base case. So, suppose that the proposition holds for $n - 1$. Then $S^n = SS^{n-1} = S\{s_2 \cdots s_n : \forall i, s_i \in S\} = \{s_1 s_2 \cdots s_n : \forall i, s_i \in S\}$. □

Now suppose G is a group. If $X \subseteq G$, we write $X^{-1} = \{x^{-1} : x \in X\}$ or, when G is abelian with binary operation written "+," we write $-X = \{-x : x \in X\}$.

2.5 Subgroup generated by a set

In this section, let's let G be a group with identity element e.

Theorem 2.36. *Suppose $(H_i, i \in I)$ is a family of subgroups of G. Then $H := \cap_{i \in I} H_i$ is a subgroup of G.*

Proof. Since $H_i \leq G$ for each i, $e \in H_i$ for each i. Therefore, $e \in H$. Suppose $x, y \in H$. Then $xy^{-1} \in H_i$ for all i. Therefore $xy^{-1} \in H$. □

Remark 2.37. The set I in Theorem 2.36 need not be finite. For example, for each positive integer n set $H_n := n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$. Then $H_n \leq \mathbb{Z}$ for all $n \in \mathbb{P}$. It's easy to see that

$$H := \cap_{n \in \mathbb{P}} H_n = \{0\},$$

the trivial subgroup of $\mathbb{Z}$.

Definition 2.38. Suppose G is a group and S is a subset of G. The subgroup $\langle S \rangle$ of G *generated by* S is the intersection of all subgroups of G containing S.

If $S = \{g_1, \ldots, g_k\}$, we abuse notation and write $\langle g_1, \ldots, g_k \rangle$ for $\langle S \rangle$, which is said to be generated by the elements $g_1, \ldots g_k$. A subgroup of G is called *cyclic* if it can be generated by a single element.

Theorem 2.39. *Suppose S is a subset of a group G with identity element 1. Set $T = S \cup S^{-1} \cup \{1\}$, and set $H = \cup_{n \geq 0} T^n$. Then $H = \langle S \rangle$.*

Proof. First, let's show that H is a subgroup of G. Clearly, $e \in H$. Suppose $x = g_1 \dots g_r$ and $y = h_1 \dots h_s$ are in H. Then $xy^{-1} = g_1 \dots g_r h_s^{-1} h_{s-1}^{-1} \dots h_1^{-1}$ is of the same form. It follows that $H \leq G$. Clearly, $S \subset H$. So, since $\langle S \rangle$ is the intersection of all subgroups of G containing S, $\langle S \rangle \leq H$.

Suppose K is a subgroup of G containing S. Then any element g of the form $t_1 \dots t_r$ with $t_i \in T$ is in K. Therefore any such element is in $\langle S \rangle$. So $H \leq \langle S \rangle$. Therefore $H = \langle S \rangle$. □

2.6 Powers of elements

Definition 2.40. Suppose M is a monoid with identity element e, $m \in M$ and $k \in \mathbb{N}$. Suppose further that the binary operation on M is written multiplicatively as $(m_1, m_2) \mapsto m_1 m_2$.

We define an element $m^k \in M$ inductively as follows.

1. We set $m^0 = e$.
2. Assuming m^j is already defined for $j \leq k$, we set $m^k = mm^{k-1}$.

So $m^0 = e$, $m^1 = me = m$, $m^2 = mm^1 = mm$, $m^3 = mm^2 = mmm$, etc. Intuitively m^k is just the product of m with itself k times.

Proposition 2.41. *Suppose M is a monoid and $m \in M$ as in Definition 2.40. Let $i, j \in \mathbb{N}$. Then*

1. $m^{i+j} = m^i m^j$.
2. $(m^i)^j = m^{ij}$.

Proof. Exercise. □

Notation 2.42. If the binary operation on M is written additively, then, we write km for m^k.

Now suppose that G is a group with identity element e and binary operation $(g_1, g_2) \mapsto g_1 g_2$.

Definition 2.43. Suppose $g \in G$ and n is a positive integer. We set $g^{-n} := (g^{-1})^n$.

So, now for $g \in G$, we have g^n defined for all integers n.

Proposition 2.44. *Suppose G is a group, $g \in G$ and $i, j \in \mathbb{Z}$. Then*

1. $g^{i+j} = g^i g^j$.
2. $(g^i)^j = g^{ij}$.

Proposition 2.45. *Suppose G is a group and $g \in G$. Then $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.*

Proof. Set $H = \langle g \rangle$. By Theorem 2.39, the elements of H are exactly the element of the form $h = g^{i_1} g^{i_2} \cdots g^{i_k}$ where $i_1, \ldots, i_k \in \{-1, 0, 1\}$. So any such element can be written as $h = g^{i_1 + \cdots i_k}$. This shows that $H \subseteq \{g^n : n \in \mathbb{Z}\}$.

On the other hand, for any $n \in \mathbb{Z}$, we can find a positive integer k and $i_1, \ldots, i_k \in \{-1, 0, 1\}$ such that $n = i_1 + \cdots + i_k$. This shows that $\{g^n : n \in \mathbb{Z}\} \subseteq H$. □

2.7 Subgroups of cyclic groups

The following is a group-theoretic version of the Euclidean algorithm.

Theorem 2.46. *Every subgroup of a cyclic group is cyclic.*

Proof. Suppose $G = \langle g \rangle$ is a cyclic group and $H \leq G$. If $H = \{e\}$, where e denotes the identity element of G, then $H = \langle e \rangle$. So H is cylic. So, from now on, assume that $H \neq \{e\}$.

Set $L := \{n \in \mathbb{Z} : g^n \in H\}$ and set $L^+ := L^+ \cap \mathbb{P}$.

I claim that L^+ is nonempty. To see this, using the assumption that $H \neq \{e\}$, pick $h \in H \setminus \{e\}$. Since $G = \langle g \rangle$, we can find $n \in \mathbb{Z}$ such that $h = g^n$. Moreover, $n \neq 0$, since $g^0 = e$ by definition. So either $n > 0$ or $-n < 0$. If $n > 0$, then $n \in L^+$. Otherwise, $g^{-n} = h^{-1} \in H$. So $-n \in L^+$.

Now, since L^+ is nonempty, it has a smallest element $d \in L^+$ by the well-ordered property of $\mathbb{P}$. I claim that $H = \langle g^d \rangle$. It's clear that $\langle g^d \rangle \leq H$ since $g^d \in H$. So we need to show that $H \leq \langle g^d \rangle$. To see this, pick $h \in H$ and write $h = g^n$ for some $n \in \mathbb{Z}$. Then, using the division algorithm, write $n = qd + r$ for integers q and r with $0 \leq r < d$. We get that $h = g^n = g^{qd+r} = (g^d)^q g^r$. So, as $h, g^d \in H$, $g^r = h(g^d)^{-1} \in H$ as well. By the minimality of d and the fact that $0 \leq r < d$, this then implies that $r = 0$. So $h = (g^d)^q \in \langle g^d \rangle$. Thus, as h was arbitrary, $H = \langle g^d \rangle$ proving the theorem. □

It's worth mentioning the following Corollary.

Corollary 2.47. *Every subgroup of $\mathbb{Z}$ is cyclic. In fact, every subgroup of $\mathbb{Z}$ can be written as $d\mathbb{Z}$ for a unique nonnegative integer d, where here $d\mathbb{Z} = \{dk : k \in \mathbb{Z}\}$.*

Proof. Obvious from the theorem as $\mathbb{Z}$ is cyclic and $d\mathbb{Z} = (-d)\mathbb{Z}$ for $d \in \mathbb{Z}$. □

Proposition 2.48. *Every cyclic group is abelian.*

Proof. Suppose $G = \langle g \rangle$ is cyclic and $x, y \in G$. We can find integers n, m such that $x = g^n$ and $y = g^m$. Then $xy = g^n g^m = g^{n+m} = g^m g^n = yx$. □

Corollary 2.49. *The symmetric group S_3 is not cyclic.*

Proof. The symmetric group S_3 is not abelian. □

2.8 Cyclic Groups and Orders of Elements

For this section G is a group with identity element e.

Definition 2.50. Suppose $g \in G$. Set $K(g) = \{n \in \mathbb{Z} : g^n = e\}$ and set $K^+(g) = K(g) \cap \mathbb{P}$. We say that g has *infinite order* and write $|g| = \infty$ if $K^+(g) = \emptyset$. Otherwise, the *order of* g is the smallest element of $K^+(g)$.

Proposition 2.51. *For each $g \in G$, $K(g) \leq \mathbb{Z}$. Consequently, $K(g) = d\mathbb{Z}$ for some (uniquely defined) nonnegative integer d.*

If $K(g) = \{0\}$, then $d = 0$ and $|g| = \infty$. Otherwise, d is the smallest element of $K^+(g) = d\mathbb{Z} \cap \mathbb{P}$. So $|g| = d$.

Proof. We use the one-step subgroup test. For this, first note that $0 \in K(g)$ as $g^0 = e$ by definition. On the other hand, suppose $n, m \in K(g)$. Then $g^{n-m} = g^n(g^m)^{-1} = ee^{-1} = e$. So $n - m \in K(g)$ as well.

This shows that $K(g) \leq \mathbb{Z}$. The rest follows from Corollary 2.47 and Definintion 2.50. □

Theorem 2.52. *Suppose $g \in G$, and suppose i and j are integers.*

If $|g| = \infty$, then $g^i = g^j \Leftrightarrow i = j$.

If $|g| = d < \infty$, then $g^i = g^j \Leftrightarrow d|i - j$.

Proof. Without loss of generality, we can suppose that $i \leq j$.

First assume that $|g| = \infty$. Then, $K(g) = \{0\}$ by Proposition 2.51. So $g^i = g^j \Rightarrow g^{i-j} = g^i(g^j)^{-1} = e \Rightarrow i - j = 0 \Rightarrow i = j$.

On the other hand, suppose $|g| = d$ for some nonzero integer d. Then, by Proposition 2.51, $K(g) = d\mathbb{Z}$. So $g^i = g^j \Rightarrow g^{i-j} = g^i(g^j)^{-1} = e \Rightarrow i - j \in d\mathbb{Z} \Rightarrow i - j = dk$ for some $k \in \mathbb{Z}$. □

Corollary 2.53. *With the notation as in 2.52, suppose $d = |g| > \infty$ and $i, j \in \mathbb{Z}$. Then $g^i = g^j \Leftrightarrow i \equiv j \pmod{d}$.*

Proof. Obvious. □

Definition 2.54. The order $|G|$ of G is ∞ if G is infinite and the number of elements of G otherwise.

Theorem 2.55. *Suppose $G = \langle g \rangle$ is cyclic.*

1. *If $|g| = \infty$, then $|G| = \infty$ and all the elements g^i with $i \in \mathbb{Z}$ are distinct.*
2. *If $|g| = d < \infty$, then $|G| = d$ and $G = \{e, g, \ldots, g^{d-1}\}$. In other words, every element of G has the form g^r for some unique integer r satisfying $0 \leq r < d$.*

Proof. (1) follows directly from Theorem 2.52.

To see (2), suppose $h \in G$. Since $G = \langle g \rangle$, we have $h = g^i$ for some $i \in \mathbf{Z}$. Then, using the division algorithm, we can write $i = qd + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < d$. Then $i \equiv r \pmod{d}$. So $h = g^r$ as well. Thus, $h \in \{e, g, \ldots, g^{d-1}\}$.

On the other hand, if $g^i = g^j$ with $0 \leq i \leq j < d$, then $d|j - i$ by Theorem 2.52. So $i = j$. □

Lemma 2.56. *Suppose n and m are integers which are not both 0, and set $d = \gcd(n, m)$. Then $\gcd(n/d, m/d) = 1$.*

Proof. Since n and m are not both 0, $d \neq 0$. So suppose $e|(n/d)$ and $e|(m/d)$. Then $ed|n$ and $ed|m$. So, by the definition of the gcd, $ed|d$. but this iplies that $e|1$. So $e = \pm 1$. And this shows that $\gcd(n/d, m/d) = 1$. □

Theorem 2.57. *Suppose $G = \langle g \rangle$ is a cyclic group and $i \in \mathbb{Z}$.*

1. *If $|g| = \infty$, then*
$$|g^i| = \begin{cases} \infty, & i \neq 0; \\ 1, & i = 0. \end{cases}$$
2. *If $|g| = n < \infty$, then*
$$|g^i| = \frac{n}{\gcd(n, i)}.$$

Proof. (1) Exercise.

(2) Suppose $|g| = n < \infty$. Then, by Proposition 2.51, $K(g) = n\mathbb{Z}$. So $g^k = e \Leftrightarrow n|k$. Consequently, $(g^i)^k = g^{ik} = e \Leftrightarrow n|ik$. Seting $d = \gcd(n, i)$, we see that $n|ik \Leftrightarrow (n/d)|(i/d)k$. But $\gcd(n/d, i/d) = 1$. So this happens if and only if $(n/d)|k$. Consequently, $K(g^i) = (n/d)\mathbb{Z}$. So $|g^i| = n/d$. □

2.9 Centralizers and Center

Fix a magma M with binary operation $(x, y) \mapsto xy$.

Definition 2.58. The centralizer of a subset $S \subseteq M$ is the set $C(S)$ of all elements $x \in M$, which commute with all elements of S. So, explicitly,
$$C(S) = \{x \in M : \forall s \in S, xs = sx\}.$$

Notation 2.59. If $s \in S$, then, by abuse of notation, we set $C(s) = C(\{s\})\}$. So, expicitly, $C(s) = \{x \in M : xs = sx\}$.

Lemma 2.60. *Suppose $S \subseteq T \subseteq M$. Then $C(T) \subseteq C(S)$.*

Proof. Obvious (by reading the definition). □

Lemma 2.61. *Suppose $S, T \subseteq M$. Then the following are equivalent:*

1. *$S \subseteq C(T)$.*
2. *$T \subseteq C(S)$.*
3. *For all $s \in S$ and $t \in T$, $st = ts$.*

Proof. Exercise. □

Lemma 2.62. *Suppose S is a nonempty subset of M. Then $C(S) = \cap_{s \in S} C(s)$.*

Proof. Obvious (once you understand the definition and the abuse of notation). □

Theorem 2.63. *Suppose $S \subseteq M$*

1. *If M is associative, then $C(S)$ is a submagma of M.*
2. *If M is a monoid, then $C(S)$ is a submonoid of M.*
3. *If M is a group, then $C(S)$ is a subgroup of M.*

Proof. (1) Suppose $x, y \in C(S)$ and $s \in S$. Then $(xy)s = x(ys) = x(sy) = (xs)y = (sx)y = s(xy)$.

(2) Since we already know that $C(S)$ is a submagma of M, we just need to show that $e \in C(S)$, where e denotes the identity element of M. For that, pick $s \in S$ and note that $es = se$ by definition.

(3) Since we already know that $C(S)$ is a submonoid of M, we just need to show that $x \in C(S) \Rightarrow x^{-1} \in C(S)$. For that, pick $s \in S$. Then $x^{-1}s = x^{-1}se = x^{-1}sxx^{-1} = x^{-1}xsx^{-1} = esx^{-1} = sx^{-1}$. So we're done. □

Definition 2.64. The *center* of a group G is the set of elements, which commute with all elements of G. In other words,

$$Z(G) := \{a \in G : ax = xa \text{ for all } x \in G\}.$$

Proposition 2.65. *If G is a group, then $Z(G) = C(G)$. In other words, the center of G is just the centralizer of G itself viewed as a subset of G.*

Proof. Obvious from the definitions. □

Corollary 2.66. *The center $Z(G)$ of a group G is a subgroup of G.*

Proof. Obvious. □

Proposition 2.67. *Suppose G is a group and $S \subseteq G$. Then $C(S) = C(\langle S \rangle)$.*

Proof. Since $S \subseteq \langle S \rangle$, it's clear from Lemma 2.60 that $C(\langle S \rangle) \leq C(S)$. So we just need to prove that $C(S) \leq C(\langle S \rangle)$.

To see this, suppose $h \in C(S)$. Then $S \subseteq C(h)$. But, since $C(h) \leq G$ and $\langle S \rangle$ is the smallest subgroup of G containing S, this implies that $\langle S \rangle \leq C(h)$. But this, in turn, implies that $h \in C(\langle S \rangle)$. So, as h was arbitrary, $C(S) \leq C(\langle S \rangle)$. □

Corollary 2.68. *Suppose $S \subseteq G$ is a set of commuting elements. In other words, suppose that, for all $s, t \in S$, $st = ts$. Then the subgroup $\langle S \rangle$ is abelian.*

Proof. By assumtion, $S \subseteq C(S)$. And $C(S) = C(\langle S \rangle)$ by Proposition 2.67. So $S \subseteq C(\langle S \rangle)$. But this implies that $\langle S \rangle \leq C(\langle S \rangle)$, which directly implies that $\langle S \rangle$ is abelian. □

Example 2.69. Let $G = \mathbf{GL}_2(\mathbb{R})$, the group of invertible 2×2 matrices with integer coefficients, and let J be the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Let's compute the centralizeer $C(J)$ of J. Suppose X is the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then

$$XJ = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$$
$$JX = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}.$$

So we see that

$$C(J) = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a^2 + b^2 \neq 0 \right\}. \tag{2.70}$$

Exercise 2.71. Show that the center of $\mathbf{GL}_2(\mathbb{R})$ consists of the set of diagonal matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

with $a \neq 0$.

2.10 Partitions of sets and equivalence relations

In this section S is a set.

Definition 2.72. A *relation* on S is a subset $R \subseteq S \times S$. An *equivalence relation* on S is a relation on S with the following properties:

1. For all $s \in S$, $(s, s) \in R$.
2. For all $s, t \in S$, $(s, t) \in R \Rightarrow (t, s) \in R$.
3. For all $s, t, u \in S$, $(s, t) \in R$ and $(t, u) \in R \Rightarrow (s, u) \in R$.

Properties (a), (b) and (c) are respectively called the *reflexive*, *symmetric* and *transitive* properties.

If R is a relation on S, then we often write xRy for $(x, y) \in R$. One equivalence relation that exists on any set is equality. Explicitly, this is the relation $R = \{(x, x) : x \in S\}$.

Proposition 2.73. *Suppose T is a set and $f : S \to T$ is a map. Set $K(f) = \{(x, y) \in S : f(x) = f(y)\}$. Then $K(f)$ is an equivalence relation on S.*

Proof. Exercise. □

Definition 2.74. A *partition* of S is a set P of disjoint, nonemtpy subsets of S whose union is S itself.

Proposition 2.75. *Suppose T is a set and $f : S \to T$ is a map which is onto. Then $P(f) = \{f^{-1}(t) : t \in S\}$ is a partition of S.*

Proof. Since f is onto, each of the sets $f^{-1}(t)$ for $t \in S$ is nonempty. If $t_1 \neq t_2$, then $f^{-1}(t_1) \cap f^{-1}(t_2)$ is obviously empty. So the sets in P are disjoint. And, for every $s \in S$, we have $s \in f^{-1}(f(s))$. So the union of the sets in $P(f)$ is all of S. □

Definition 2.76. Suppose P is a partition of S. Then, by definition, for every $s \in S$, there exists a unique subset $U \in P$ such that $s \in U$. Write $\pi_P(s) := U$. Then we have a surjective map $\pi_P : S \to P$.

Example 2.77. Suppose $S = \{1, 2, 3\}$ and $P = \{\{1, 2\}, \{3\}\}$. Then $\pi_P(1) = \pi_P(2) = \{1, 2\}$ and $\pi_P(3) = \{3\}$.

Definition 2.78. Suppose R is an equivalence relation on S and $s \in S$. The *equivalence class* of s is $[s]_R = \{t \in S : tRs\}$. We write $S/R = \{[s]_R : s \in S\}$.

Lemma 2.79. *Suppose R is an equivalence relation on S, and s, $t \in S$. Then $s \in S$. So, in particular, $[s] \neq \emptyset$. Moreover, the following are equivalent:*

1. *sRt.*
2. *$[s] = [t]$.*
3. *$[s] \cap [t] \neq \emptyset$.*

Proof. Since sRs by reflexivity, $s \in [s]$. We do the rest of the proof by going around the circle of implications.

(1)⇒(2): Supose $u \in [s]$. Then uRs. So, since sRt, transitivity implies that uRt. So $u \in [t]$. That shows that $[s] \subseteq [t]$. But then, by symmetry, we get that tRs. So the same argument proves that $[t] \subseteq [s]$.

(2)⇒(3): Obvious from the fact that $[s] \neq \emptyset$.

(3)⇒(2): Suppose $u \in [s] \cap [t]$. Then uRs and uRt. So, by symmetry, sRu. And, then, by transitivity, sRt. □

Corollary 2.80. *Suppose R is an equivalence relation on S. Then S/R is a partition of S.*

Proof. Since $s \in [s]$, the sets in S/R are nonemtpy and their union is S. Moreover, they are disjoint by Lemma 2.79(3). So, by definition, they form a partition of S. □

Theorem 2.81. *Write* Equiv *for the set of equivalence relations on S, and write* Part *for the set of partitions of S.*

1. *If R is an equivalence relation on S, then $K(\pi_{S/R}) = R$.*

2. *If P is a partition of S, then $S/K(\pi_P) = P$.*

Consequently, the map Equiv $\to$ Part *given by $R \mapsto S/R$ sets up a one-one correspondence between equivalence relations on S and partitions of S. The inverse of this map is the map $P \mapsto K(\pi_P)$.*

Proof. (a) Suppose R is an equivalence relation. Then $(s,t) \in K(\pi_{S/R}) \Leftrightarrow [s] = [t]$. By Lemma 2.79, this happens if and only if sRs. So, it follows that $K(\pi_{S/R}) = R$.

(b) Exercise. □

2.11 Cosets and Lagrange's Theorem

In this section, G is a group with identity element e and $H \leq G$ is a subgroup.

Definition 2.82. A *left coset* of H is a subset of G of the from gH. A *right coset* of H is a subset of the form Hg. We write G/H for the set of all left cosets of G, and we write $H\backslash G$ for the set of all right cosets of G. An element of a left (or right) coset is called a *coset representative*.

Note that $H = eH = He$ is always both a left and right coset of H. We call it the *trivial coset*.

Lemma 2.83. *For g_1, $g_2 \in G$, write $g_1 L g_2$ if $g_1 \in g_2 H$. Then $g_1 L g_2 \Leftrightarrow g_1^{-1} g_2 \in H$. Moreover, L is an equivalence relation on G and, for each $g \in G$, $[g]_L = gH$.*

Proof. Pick g_1 and $g_2 \in G$. Then $g_1 L g_2 \Leftrightarrow g_1 \in g_2 H \Leftrightarrow g_1 = g_2 h$ for some $h \in H \Leftrightarrow g_1^{-1} g_2 = h$ for some $h \in H \Leftrightarrow g_1^{-1} g_2 \in H$.

To see that L is an equivalence relation, first note that, as $H \leq G$, for all $g \in G$, $e = g^{-1} g \in H$. This shows that L is reflexive.

To see that L is symmetric, suppose $g_1 L g_2$. Then $g_1^{-1} g_2 \in H$. But this implies that $g_2^{-1} g_1 = (g_1^{-1} g_2)^{-1} \in H$ as well. So $g_1 L g_1$.

To see that L is transitive, suppose that $g_1 L g_2$ and $g_2 L g_3$. Then $g_1^{-1} g_2$ and $g_2^{-1} g_3$ are both in H. But this implies that $g_1^{-1} g_3 = (g_1^{-1} g_2)(g_2^{-1} g_3) \in H$.

Given this, by definition $[g]_L = \{x \in G : xLg\} = \{x \in G : x \in gH\} = gH$. □

Corollary 2.84. *The set G/H of left cosets of H form a partition of G.*

Proof. Obvious from Lemma 2.83 and the fact that equivalence classes of an equivalence relation form a partition. □

Definition 2.85. The *index* $[G : H]$ of H in G is the number of left cosets of H in G. We write $[G : H] = \infty$ if that number is infinite.

Lemma 2.86. *Suppose $g \in G$. Then the map $f : H \to gH$ given by $f(h) = gh$ sets up a one-one correspondence between H and the left-coset gH.*

Proof. Trivial. □

Corollary 2.87. *Every left coset gH of H has the same cardinality. More precisely, for any $g \in G$, we have $|gH| = |H|$.*

Proof. Sets in one-one correspondence have the same cardinality by definition. □

Theorem 2.88. *We have $|G| = [G : H]|H|$.*

Proof. Let's prove this when G is finite. (The general proof requires explaining what we mean by the product of infinite sets, but is essentially the same.)

The set G/H is a partition of G into $[G : H]$ subsets each having cardinality $|H|$. □

Corollary 2.89. *Suppose $|G| < \infty$. Then*

1. *The order $|H|$ of any subgroup $H \leq G$ divides $|G|$.*
2. *The order $|g|$ of any element $g \in G$ divides $|G|$.*

Proof. (1) Obvious from Theorem 2.88.

(2) Suppose $g \in G$ and set $H = \langle g \rangle$. If $|g| = \infty$, then all the elements g^i for $i \in \mathbb{Z}$ are distinct by Theorem 2.55(1). So H is infinite, which contradicts the assumption that G is finite.

So we can assume that $|g| = d < \infty$, and then $|H| = d$ by Theorem 2.55(2). So d divides $|H|$ by (1). □

Corollary 2.90. *Any group of prime order is cyclic. In fact, if G is a group of prime order than G is generated by any nonidentity element.*

Proof. Suppose $|G| = p$ is a prime number. Then $|G| > 1$. So there exists a nonidentity element $g \in G$. So $|g| > 1$, but $|g||p$. It follows that $|g| = p$. So $|\langle g \rangle| = p$. So G is cyclic. □

2.12 Order of product of subgroups

In this section G is a group with identity element e, and H and K are two subgroups of G.

Theorem 2.91. *Suppose H and K are finite. Then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Warning 2.92. *In some important cases, $HK \leq G$. But often it is not. (We'll see examples.)*

Remark 2.93. Properly interpretted, Theorem 2.91 is also true when H and K are infinite.

Proof of Theorem 2.91. Let $H \times K$ denote the Cartesian product of H and K. For each $h \in H$ and $k \in K$, $hk \in HK$. So we can define a function $f : H \times K \to HK$ by setting $f(h,k) = hk$. Clearly, f is onto. So, by Proposition 2.75, $P(f) = \{f^-(g) : g \in HK\}$ is a partition of $H \times K$.

I claim that, for each $g \in HK$, $|f^{-1}(g)| = |H \cap K|$. To see this, pick $h \in H$ and $k \in K$ such that $g = hk$. Then, for $u \in H \cap K$, $hu \in H$, $u^{-1}k \in K$ and $f(hu, u^{-1}k) = hk = g$. So we can define a map $\phi : H \cap K \to f^{-1}(g)$ by setting $\phi(u) = (hu, u^{-1}k)$.

I claim that ϕ is both one-one and onto. To see that ϕ is one-one, suppose $u_1, u_2 \in H \cap K$ and $\phi(u_1) = \phi(u_2)$. Then $u_1 = h^{-1}hu_1 = h^{-1}hu_2 = u_2$.

To see that ϕ is onto, suppose $(h_1, k_1) \in f^{-1}(g)$. Then $h_1 \in H$, $k_1 \in K$ and $h_1k_1 = g = hk$. It follows that $h^{-1}h_1 = kk_1^{-1}$. But then $u := h^{-1}h_1 = kk_1^{-1} \in H \cap K$. And $\phi(u) = (hu, u^{-1}k) = (hh^{-1}h_1, k_1k^{-1}k) = (h_1, k_1)$. As (h_1, k_1) was an arbitrary element of $f^{-1}(g)$, this proves that $\phi : H \cap K \to f^{-1}(g)$ is onto.

Since ϕ is one-one and onto, $|f^{-1}(g)| = |H \cap K|$ for every $g \in HK$. So $P(f)$ partitions $H \times K$ into $|HK|$ sets each of size $|H \cap K|$. It follows that $|H||K| = |H \times K| = |HK||H \cap K|$. So Theorem 2.91 is proved. □

Example 2.94. Let $G = S_3$ and let $H = \langle\sigma\rangle$, $K = \langle\tau\rangle$ where

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Then $|H| = |\sigma| = 2 = |\tau| = |K|$. So $H = \{e, \sigma\}$, $K = \{e, \tau\}$ and $H \cap K = \{e\}$. Therefore, by Theorem 2.91, we see that $|HK| = 4$. As $4 \nmid 6 = |G|$, Lagrange's theorem shows that HK is not a subgroup of G. And, in fact, since $|HK| > |G|/2$, it follows that the smallest subgroup of G containting HK is G itself. Therefore $G = \langle\sigma, \tau\rangle$.

Chapter 3

Basic group theory

3.1 Homomorphisms

We start with the official definitions.

Definition 3.1. 1. Suppose M and N are magmas. A *magma homomorphism* from M to N is a map $f : M \to N$ such that, for all $x, y \in M$, $f(xy) = f(x)f(y)$.

2. Suppose M and N are monoids with identity elements e_M and e_N. A *monoid homomorphism* from M to N is a monoid homomorphism $f : M \to N$ with the additional property that $f(e_M) = e_N$.

3. Suppose M and N are groups. A *group homomorphism* from M to N is a monoid homomorphism with the additional property that, for all $x \in M$, $f(x^{-1}) = f(x)^{-1}$.

4. A magma (resp. monoid, resp. group) homomorphism f is said to be a magma (resp. monoid, resp. group) *isomorphism* if it is one-one and onto.

5. A magma (resp. monoid, resp. group) homomorphism $f : M \to M$ is called a magma (resp. monoid, resp. group) *endomorphism*.

6. A magma (resp. monoid, resp. group) isomorphism $f : M \to M$ is called a magma (resp. monoid, resp. group) *automorphism*.

We are mostly going to be interested in group homomorphisms, isomorphisms and (sometimes) automorphisms. The following Proposition is helpful in this regard.

Proposition 3.2. *Suppose G and H are groups and $f : G \to H$ is a magma homomorphism. Then f is a group homomorphism as well. In other words, a map $f : G \to H$ is a group homomorphism if and only if for all $x, y \in G$, $f(xy) = f(x)f(y)$.*

Proof. Suppose G and H are groups and $f : G \to H$ is a magma homomorphism. Write e_G (resp. e_H) for the identity element of G (resp. H). Then $f(e_G) = f(e_G)e_H = f(e_G)(f(e_G)f(e_G)^{-1}) = (f(e_G)f(e_g))f(e_G)^{-1} = f(e_G)f(e_G)^{-1} = e_H$. So $f : G \to H$ is a monoid homomorphism.

On the other hand, suppose $g \in G$. Then

$$\begin{aligned} f(g^{-1}) &= f(g^{-1})e_H = f(g^{-1})f(g)f(g)^{-1} \\ &= f(g^{-1}g)f(g)^{-1} = f(e_G)f(g)^{-1} = e_H f(g)^{-1} = f(g)^{-1} \end{aligned}$$

So f is a group homomorphism. □

Example 3.3. The analogue of Proposition 3.2 is not true for monoids. In other words, there are examples of monoids M and N with identity elements e_M and e_N respectively and magma homomorhisms $f : M \to N$ such that $f(e_M) \neq e_N$.

In fact, here's an easy example. Let $N = \{0, 1\}$ with the binary operation $*$ given by setting $0 * 0 = 0 * 1 = 1 * 0 = 0$ and $1 * 1 = 1$. It's not hard to check directly that N is associative. So it is a monoid with identity element 1. The subset $M = \{0\}$ is a submagma. In other words, it is closed under the binary operation. But, according to Definition 2.29, it is not a submonoid because it does not contain the identity element 1 of M.

Write $f : N \to M$ for the inclusion map given by $f(0) = 0$. Then f is a magma homomorphism, but it is not a monoid homomorphism.

If S is any set, we write id_S for the map $\mathrm{id}_S : S \to S$ given by $\mathrm{id}_S(s) = s$. This map, which is called the *identity map* is trivial, but it is also fundamental.

Recall that a map of sets $f : S \to T$ is a bijection if and only if there exists an inverse function $g : T \to S$ such that $f \circ g = \mathrm{id}_T$ and $g \circ f = \mathrm{id}_S$. The inverse function g is then unique and is usually written as $f^{-1} : T \to S$. It follows directly that, in this case, $f^{-1} : T \to S$ is also a bijection.

Proposition 3.4. *1. If M is magma (resp. monoid, resp. group) then* $\mathrm{id}_M : M \to M$ *is a magma (resp. monoid, resp. group) endomorphism.*

2. Suppose M and N are magmas and $f : M \to N$ is a magma isomorphism. Then the inverse function $f^{-1} : N \to M$ is also a magma isomorphism.

3. Suppose M and N are monoids and $f : M \to N$ is a monoid isomorphism. Then the inverse function $f^{-1} : N \to M$ is also a monoid isomorphism.

4. Suppose M and N are groups and $f : M \to N$ is a group isomorphism. Then the inverse function $f^{-1} : N \to M$ is also a group isomorphism.

Proof. (1) Exercise. (It's basically obvious.)

(2) Suppose $f : M \to N$ is a bijection of magmas, and $n_1, n_2 \in N$. Set $m_i := f^{-1}(n_i)$ for $i = 1, 2$ so that $f(m_i) = n_i$.

$$\begin{aligned} f^{-1}(n_1 n_2) &= f^{-1}(f(m_1)f(m_2)) = f^{-1}(f(m_1 m_2)) = m_1 m_2 \\ &= f^{-1}(m_1)f^{-1}(m_2). \end{aligned}$$

So $f^{-1} : N \to M$ is a homomorphism of magmas. As it is a bijetion, it is also an isomorphism of magmas.

(3) Suppose $f : M \to N$ is a bijection of monoids with e_M (resp. e_N) the identity element of M (resp. N). Then $f^{-1} : N \to M$ is a magma isomorphism by (2). And $f(e_M) = e_N$, which implies that $f^{-1}(e_N) = e_M$. So $f^- : N \to M$ is also a monoid homomorphism. As it is a bijection, it is also a monoid isomorphism.

(4) This follows directly from (2) and Proposition 3.2. □

Example 3.5. Write $\mathbb{R}_+ := (0, \infty) = \{x \in \mathbb{R} : x > 0\}$. It's easy to see that $(\mathbb{R}_+, *)$ is a group where $*$ is the usual multiplication. Then let $G = (\mathbb{R}, +)$, and let $H = (\mathbb{R}_+, *)$. From Calculus, we know that $\exp(x + y) = \exp(x)\exp(y)$ and $\exp(x) > 0$ for all x. So the map $\exp : G \to H$ is a group homomorphism.

Here I introduced the symbols G and H to make it absolutely clear what the binary operations are, but usually, I would express this more directly by saying that $\exp : \mathbb{R} \to \mathbb{R}_+$ is a group homomorphism. (The assumption is that the reader can see that addition is the only obvious binary operation that makes $\mathbf{R}$ into a group and multiplication is the only obvious binary operation that makes $\mathbb{R}_+$ into a group.)

In fact, $\exp : \mathbb{R} \to \mathbb{R}_+$ is an isomorphism of groups with inverse $\log : \mathbb{R}_+ \to \mathbb{R}$.

Proposition 3.6. *The composition $S \circ T : G \to K$ of two group homoorphisms $T : G \to H$ and $S : H \to K$ is a group homomorphism. (And similarly for magma and monoid homomorhisms).*

Proof. Let's prove it for group homomorphisms. So suppose $T : G \to H$ and $S : H \to K$ are group homomorphisms and $x, y \in G$. Then $(S \circ T)(xy) = S(T(xy)) = S(T(x)T(y)) = S(T(x))S(T(y)) = (S \circ T)(x)(S \circ T)(y)$. So, by Proposition 3.2, we're done.

The same proof (of course) works for magma homomorphisms, and the proof for monoid homomorphisms is easy (and left to the reader). □