Warwick Mathematics Exchange

MA249

Algebra II

2023, May 23rd

Desync, aka The Big Ree

Contents

Introduction

In *Algebra II*, we study the algebraic structures of groups and rings. We previously defined quotient groups for abelian groups in MA136 *Intro to Abstract Algebra*, but we now extend this to general groups using the notion of normal subgroups. We then prove the isomorphism theorems for general groups, before proving the corresponding theorems for rings.

Disclaimer: I make *absolutely no guarantee* that this document is complete nor without error. In particular, any content covered exclusively in lectures (if any) will not be recorded here. This document was written during the 2022 academic year, so any changes in the course since then may not be accurately reflected.

Notes on formatting

New terminology will be introduced in *italics* when used for the first time. Named theorems will also be introduced in *italics*. Important points will be **bold**. Common mistakes will be underlined. The latter two classifications are under my interpretation. YMMV.

Content not taught in the course will be outlined in the margins like this. Anything outlined like this is not examinable, but has been included as it may be helpful to know alternative methods to solve problems.

The table of contents above, and any inline references are all hyperlinked for your convenience.

Scalars are written in lowercase italics, c, or using Greek letters.

Vectors are written in lowercase bold, $\mathbf{v}$, or rarely overlined, $\overleftrightarrow{v}$, where more contrast or clarity is required.

Matrices are written in uppercase bold, $\mathbf{A}$.

Note: transformations represented by matrices may be written in just italics, as functions often are, i.e., $s(\mathbf{v}) = \mathbf{A}\mathbf{v}$.

History

First Edition: 2023-05-15[*]
Current Edition: 2023-05-18

Authors

This document was written by R.J. Kit L., a maths student. I am not otherwise affiliated with the university, and cannot help you with related matters.

Please send me a PM on Discord @Desync#6290, a message in the WMX server, or an email to Warwick.Mathematics.Exchange@gmail.com for any corrections. (If this document somehow manages to persist for more than a few years, these contact details might be out of date, depending on the maintainers. Please check the most recently updated version you can find.)

If you found this guide helpful and want to support me, you can buy me a coffee!

(Direct link for if hyperlinks are not supported on your device/reader: ko-fi.com/desync.)

[*] Storing dates in big-endian format is clearly the superior option, as sorting dates lexicographically will also sort dates chronologically, which is a property that little and middle-endian date formats do not share. See ISO-8601 for more details. This footnote was made by the computer science gang.

0.1 Glossary of Common Groups & Sets

- D_n (the *dihedral group*) - the group of isometries on a regular n-gon. $|D_n| = 2n$.
- $\mathbb{Z}/n\mathbb{Z}$ - set of integers mod n under addition, or possibly multiplication if n is prime[*].
- Nth roots of unity - solutions of $z^n = 1$ over the complex numbers under multiplication, sometimes denoted U_n, though this is non-standard notation.
- $\mathbb{S}^1$ or $\mathbb{T}$ (the *circle group*) - the set of complex numbers with magnitude 1 under multiplication.
- $\mathrm{Map}(X)$ - the set of functions from a set, X, to itself.
- $\mathrm{Sym}(X)$ - the group of bijections from a set X to itself, isomorphic to S_n.
- S_n (the *symmetric group*) - the group of permutations of n points. $|S_n| = n!$.
- A_n (the *alternating group*) - the group of even permutations of n points. $|A_n| = \frac{n!}{2}$.
- $M_{m\times n}(\mathbb{R})$ is the group of matrices with real entries. $M_{m\times n}(\mathbb{Z})$, etc., are defined similarly.
- $GL_n(\mathbb{R})$ (the *general linear group*) is the group of $n \times n$ matrices with non-zero determinants and real entries, under matrix multiplication.
- $SL_n(\mathbb{R})$ (the *special linear group*) is the group of $n \times n$ matrices with unit determinant and real entries, under matrix multiplication.
- $SL_2(\mathbb{Z})$ (the *modular group*) is the group of 2×2 matrices with unit determinant and integer entries, under matrix multiplication.
- $SO_n(\mathbb{R})$ (the *special orthogonal group*) is the group of $n \times n$ rotation matrices under matrix multiplication.

1 Review

A *group*, $(G,*)$ is a set, G, equipped with a binary operation, $* : G \times G \to G$, that obeys the following axioms:

- $\forall a,b \in G, a * b \in G$ (closure);
- $\forall a,b,c \in G, a * (b * c) = (a * b) * c$ (associativity);
- $\exists e \in G$ such that $\forall a \in G, a * e = e * a = a$ (existence of identity);
- $\forall a \in G, \exists (a^{-1}) \in G$ such that $a * (a^{-1}) = (a^{-1}) * a = e$ (existence of inverses).

We can also write id_G for the identity for clarity (and also to mark which group the identity is from). If the operation is additionally commutative, that is, $\forall a,b \in G, a * b = b * a$, then the group is *abelian.*

Example.

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, any ring R, and any field K form an (abelian) group under addition.
- The set of non-zero elements of a field K, $K^* = K \setminus \{0_K\}$, forms a group under multiplication.

We define multiplicative notation for groups as follows:

- The group operation is omitted, so $a * b$ is written as ab;
- The identity is often written as 1 or 1_G, instead of e or id;

[*] The groups $(\mathbb{Z}n/\mathbb{Z},+)$ and $(\mathbb{Z},+_n)$ are technically slighly different, though they are isomorphic. The set underlying the first group contains congruence classes with modularity built into the elements themselves, while the set underlying the second group is just the integers, and the modularity is built into the operation instead.

- If $n \in \mathbb{N}$, then $a^n = \underbrace{a * a * \cdots * a}_{n}$;
- If $n = 0$, $a^n = 1_G$;
- If n is a negative integer, $a^n = (a^-n)^{-1}$;
- $(a^{-1})^n = a^{-n}$;
- $(a^m)^n = a^{mn}$;
- $(a^m)(a^n) = a^{m+n}$;
- If the group is abelian, $(ab)^n = (a^n)(b^n)$.

Abelian groups are more commonly written in additive notation:

- The group operation is written as $+$;
- The identity is often written as 0 or 0_G, instead of e or id;
- If $n \in \mathbb{N}$, then $na = \underbrace{a + a + \cdots + a}_{n}$;
- If $n = 0$, $na = 0_G$;
- The inverse of g is written as $-g$ instead of g^{-1}.
- If n is a negative integer, $na = -n(-a)$;
- $n(-a) = -na$;
- $n(ma) = (m \times n)a$;
- $(ma) + (na) = (m + n)a$;
- If the group is abelian, $n(a + b) = na + nb$.

1.1 Basic Properties

Theorem (Cancellative Property)**.** *Let G be a group and let a,b,$g \in G$. Then,*

(i) $ga = gb \to a = b$;

(ii) $ag = bg \to a = b$.

Proof. For (i),

$$\begin{aligned} ga &= gb \\ g^{-1}(ga) &= g^{-1}(gb) && \text{[Existence of inverses]} \\ (g^{-1}g)a &= (g^{-1}g)b && \text{[Associativity]} \\ \mathrm{id}_G\, a &= \mathrm{id}_G\, b \\ a &= b && \text{[Identity]} \end{aligned}$$

(ii) is proved similarly by right multiplying by g^{-1}. ■

In future proofs, we will omit brackets and not explicitly refer to associativity to save space.

Lemma (Uniqueness of Identity)**.** *The identity of a group is unique.*

Proof. Suppose e and f are identities of a group, G. $ef = e$, as f is the identity. But $ef = f$, as e is also the identity, so $ef = e = f$, so $e = f$ and the identity is unique. ■

Lemma (Uniqueness of Inverse)**.** *Every element of a group has a unique inverse.*

Proof. Suppose a and b are both inverses of g, so $ga = \mathrm{id}_G = gb$. By the cancellative property, $a = b$. ■

Lemma (Two-Sided Identity)**.** *If e_ℓ is a left identity for a group G – that is, $e_\ell g = g$ for all $g \in G$ – and e_r is a right identity for G, then $e_\ell = e_r = \mathrm{id}_G$.*

Proof. $e_\ell e_r = e_r$ as e_ℓ is a left identity, and $e_\ell e_r = e_\ell$ as e_r is a right identity, so $e_\ell = e_\ell e_r = e_r = \mathrm{id}_G$. ■

Lemma (Two-Sided Inverse)**.** *If ℓ is a left inverse for an element g – that is, $\ell g = \mathrm{id}_G$ – then ℓ is the (two-sided) inverse of g. Similarly, if r is a right inverse for g, then it is a (two-sided) inverse of g.*

Proof. $\ell g = \mathrm{id}_G$ as ℓ is a left inverse of g, so,

$$\begin{aligned} \ell g &= \mathrm{id}_G \\ \ell g &= g^{-1} g \\ \ell g g^{-1} &= g^{-1} g g^{-1} \\ \ell &= g^{-1} \end{aligned}$$

As the choice of ℓ was arbitrary, all left inverses of g are equal. The proof for right inverses is similar. ■

Theorem (Distribution of Inverse)**.** *For all a,$b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof.

$$\begin{aligned} (ab)^{-1}ab &= \mathrm{id}_G \\ (ab)^{-1}abb^{-1} &= \mathrm{id}_G\, b^{-1} \\ (ab)^{-1}a &= b^{-1} \\ (ab)^{-1}aa^{-1} &= b^{-1}a^{-1} \\ (ab)^{-1} &= b^{-1}a^{-1} \end{aligned}$$

■

1.2 Order

Let $(G, *\,)$ be a group. The cardinality of the underlying set G is called the *order* of the group, denoted $|G|$.

Let $g \in G$. The *order* of g, denoted $|g|$ or $o(g)$ is the least integer $n > 0$ such that $g^n = \mathrm{id}_G$. If no such n exists, then g has *infnite order* and we write $|g| = \infty$.

Note that if g has infinite order, then $g^i \neq g^j$ for all $i \neq j$, or else if $g^i = g^j$ for some $i < j$, then $g^{j-i} = \mathrm{id}_G$ by the cancellative property, so the order of g divides $j - i$ and is hence finite. Similarly, if g has finite order n, then $g^i \neq g^j$ for all $i \neq j \in [0,n]$.

Lemma 1.1. *$|g| = 1$ if and only if $g = \mathrm{id}_G$.*

Proof. $\mathrm{id}_G^1 = \mathrm{id}_G$. Conversely, for all $\mathrm{id}_G \neq g \in G$, $g^1 = g \neq \mathrm{id}_G$. ■

Lemma 1.2. *If $|g| = n$, then $g^k = 1$ if and only if $n|k$.*

Proof. Suppose $n \nmid k$, so $k = qn + r$ for some $q,r \in \mathbb{N}$ with $0 < r < n$ (by the division algorithm). Then,

$$\begin{aligned} g^k &= g^{qn+r} \\ &= (g^n)^q g^r \\ &= \mathrm{id}_G^q \, g^r \\ &= g^r \end{aligned}$$

and since $0 < r < n$, $g^r \neq g^n = \mathrm{id}_G$.

Conversely, suppose $n|k$ so $k = qn$. Then,

$$\begin{aligned} g^k &= g^{qn} \\ &= (g^n)^q \\ &= \mathrm{id}_G^q \\ &= \mathrm{id}_G \end{aligned}$$

■

Theorem 1.3. *For every $g \in G$, $|g|$ divides $|G|$.*

Proof. Follows from Lagrange's theorem (§ 1.10). ■

Theorem 1.4. *If $|G| = n$, then $g^n = 1$ for all $g \in G$.*

Proof. Let a be the order of g, so $g^a = 1$. By Lagrange's theorem, a divides n, so $n = ab$ for some integer b. So, $g^n = g^{ab} = (g^a)^b = 1^b = 1$. ■

1.3 Morphisms

A *homomorphism* between two groups $(G, *\,)$ and $(H, \cdot\,)$ is a function $\phi : G \to H$ such that $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a,b \in G$.

Note that this necessarily requires that $\phi(\mathrm{id}_G) = \mathrm{id}_H$[*] as,

$$\begin{aligned} \mathrm{id}_H \cdot \phi(g) &= \phi(g) \\ &= \phi(\mathrm{id}_G * g) \\ &= \phi(\mathrm{id}_G) \cdot \phi(g) \end{aligned}$$

so $\mathrm{id}_H = \phi(\mathrm{id}_G)$ by the cancellative property.

An injective homomorphism is also called a *monomorphism*, and a surjective homomorphism is called an *epimorphism*.

If the inverse of a homomorphism is a homomorphism, or equivalently, if the homomorphism is a bijection, then it is called an *isomorphism*. If an isomorphism exists between G and H, we say that G and H are *isomorphic*, and we write $G \cong H$ to denote this relation. It is easy to check that isomorphism is an equivalence relation.

Lemma 1.5. *If $\phi : G \to H$ is an isomorphism, then $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.*

[*] In fact, mapping identities to identities is a requirement for homomorphisms between more general objects such as ring homomorphisms (as we will see later), or categorical functors. For groups, identities being preserved just happens to be implied by the operation compatibility requirement, so it is omitted from our definition.

Proof. For all $g \in G$,

$$\begin{aligned} \mathrm{id}_H &= \phi(\mathrm{id}_G) \\ &= \phi(gg^{-1}) \\ &= \phi(g) \cdot \phi(g^{-1}) \end{aligned}$$

so $\phi(g^{-1})$ is the inverse of $\phi(g)$ in H, giving $\phi(g^{-1}) = \phi(g)^{-1}$. ■

Theorem 1.6. *If $\phi : G \to H$ is an isomorphism, then $|g| = |\phi(g)|$ for all $g \in G$.*

Proof. If $|g|$ is infinite, then g^k is distinct for all $k \in \mathbb{Z}$. Then, $\phi(g^k) = \phi(g)^k$ must also be distinct for all $k \in \mathbb{Z}$, so $|\phi(g)|$ is infinite.

Conversely, suppose $n = |g|$ is finite.

$$\begin{aligned} \phi(g)^n &= \phi(g^n) \\ &= \phi(\mathrm{id}_G) \\ &= \mathrm{id}_H \end{aligned}$$

so $|\phi(g)| \leq n = |g|$. Now, let $m = |\phi(g)|$, so

$$\begin{aligned} \phi(g^m) &= \phi(g)^m \\ &= \mathrm{id}_H \\ &= \phi(\mathrm{id}_G) \end{aligned}$$

and since ϕ is an isomorphism, it is injective, so $g^m = \mathrm{id}_G$ and hence $|\phi(g)| = m \leq |g|$. Then,

$$|\phi(g)| \leq |g| \leq |\phi(g)|$$

so $|\phi(g)| = |g|$. ■

1.4 Subgroups

Let $(G,*)$ be a group, and let H be a subset of G. Furthermore, suppose that $(H,*)$ is also a group. $(H,*)$ is then a *subgroup* of $(G,*)$.

To show that a subset $H \subseteq G$ is a subgroup of G, it suffices to show that H is non-empty, is closed under $*$, and that every element has an inverse in H.

Theorem (Two-Step Subgroup Test)**.** *If $(G,*)$ is a group and $H \subseteq G$, then $(H,*)$ is a subgroup of G if and only if,*

(i) $H \neq \emptyset$;

(ii) $a,b \in H \to a * b \in H$;

(iii) $a \in H \to a^{-1} \in H$.

Proof. Every subgroup H clearly fulfils these three conditions for the forward implication.

For the reverse implication, we verify the four axioms. Closure is given by the condition (*ii*), while associativity is inherited from the main group, as the operation in H is just the restriction of the operation in G. The existence of an inverse element follows from condition (*iii*). The existence of the identity element follows from taking a,b to both be the identity in condition (*ii*), or by taking b to be a^{-1}. ■

The test is named the two-step test because H is often assumed to be non-empty, so the first condition need not be checked.

This suggests a shorter test still:

Theorem (One-Step Subgroup Test). *If $(G, *)$ is a group and $H \subseteq G$, then $(H, *)$ is a subgroup of G if and only if,*

1. *$H \neq \emptyset$;*
2. *$a,b \in H \to ab^{-1} \in H$;*

Proof. Every subgroup H clearly fulfils these three conditions for the forward implication.

For the reverse implication, we verify the four axioms. Associativity is again inherited from the main group.

Since H is non-empty, there exists an element $x \in H$. Taking $a = x$ and $b = x$ gives $x * x^{-1} = \mathrm{id}_G \in H$, so the identity element is in H.

Inverses follow from taking $a = \mathrm{id}_G$ and $b = x$, giving $\mathrm{id}_G * x^{-1} = x^{-1} \in H$.

Let $x,y \in H$. Then, as inverses exist, $y^{-1} \in H$, and so we may take $a = x$ and $b = y$, giving $x * (y^{-1})^{-1} = x * y \in H$, and hence H is closed. ■

Theorem 1.7. *The following results hold for all groups:*

(i) The intersection of two subgroups is also a subgroup.

(ii) The union of two subgroups is generally not a subgroup.

(iii) The group itself, G, and the trivial group, $\{\mathrm{id}_G\}$, are always subgroups of G.

Proof. (i) Let $H \leq G$ and $K \leq G$. $\mathrm{id}_G \in H$ and $\mathrm{id}_G \in K$, so $H \cap K$ is non-empty as it also contains id_G. Since $H \leq G$, $xy^{-1} \in H$ for all $x,y \in H$, and similarly for K. Suppose $a,b \in H \cap K$ so $a,b \in H$ and $a,b \in K$. Then, $ab^{-1} \in H$ and $ab^{-1} \in K$, and hence $ab^{-1} \in H \cap K$, so $H \cap K$ is a subgroup by the one-step test. ■

Any subgroup not equal to G is a *proper* subgroup, while any subgroup not equal to $\{\mathrm{id}_G\}$ is a *non-trivial* subgroup.

Let $S \subset G$ be a set of elements of G. $H = \langle S \rangle$ is then defined to be the minimal group that contains all of S. That is, there are no subgroups of H that contain every element of S. S is then called the *generating set* of H, or equivalently, we say that H is *generated* by S.

If $S = \{g\}$ is a singleton set, then $H = \langle S \rangle = \langle g \rangle$ is given by $\{g^n | n \in \mathbb{N}\} = \{\cdots,(g^{-2}),g^{-1},1,g,g^2,g^3,\cdots\}$. If $g \in G$, then $\langle g \rangle$ is a subgroup of G. It is obvious from the definition that $|\langle g \rangle| = |g|$.

1.5 Cyclic Groups

A group G is *cyclic* if there exists an element $g \in G$ such that $G = \{g^n : n \in \mathbb{Z}\}$, and we say that g is a *generator* of G, or that G is *generated* by g. (So cyclic groups are a special case of generated groups from the previous section, where $|S| = 1$.)

A generator is not necessarily unique. For instance, $\mathbb{Z}$ is generated by both 1 and -1, and $\mathbb{Z}/p\mathbb{Z}$ with p prime is generated by every non-identity element.

Lemma 1.8. *In an infinite cyclic group, every generator has infinite order. In a finite cyclic group of order n, every generator has order n.*

We write C_n for the finite cyclic group of order n.

Theorem 1.9. *Every infinite cyclic group is isomorphic to the group of integers under addition.*

Proof. Suppose $(G,\times)$ is an infinite cyclic group with generator g. Define the map $\phi : (\mathbb{Z},+) \to (G, \cdot\,)$ by $n \mapsto g^n$.

$$\begin{aligned}\phi(a+b) &= g^{a+b}\\ &= g^a \cdot g^b\\ &= \phi(a)\cdot\phi(b)\end{aligned}$$

so ϕ is a homomorphism. Then, as G has infinite order, so does g and hence $g^a \neq g^b$ for all $a \neq b$, so ϕ is injective. As G is cyclic, every element can be written in the form g^n for some $n \in \mathbb{Z}$, which is exactly the statement of surjectivity for ϕ. It follows that ϕ is an isomorphism. ■

Corollary 1.9.1. *Any two infinite cyclic groups are isomorphic.*

Proof. As G was arbitrary, all infinite cyclic groups are isomorphic. ■

Theorem 1.10. *Any two cyclic groups of equal order are isomorphic.*

Proof. Let G and H be cyclic groups of finite order k with generators g and h, respectively. Define the map $\phi : G \to H$ by $g^n \mapsto h^n$. This map is clearly bijective by construction.

Let $a,b \in G$. As G is cyclic, $a = g^s$ and $b = g^t$ for some integers s,t.

$$\begin{aligned}\phi(ab) &= \phi(g^s g^t)\\ &= \phi(g^{s+t})\\ &= h^{s+t}\\ &= h^s h^t\\ &= \phi(g^s)\phi(g^t)\\ &= \phi(a)\phi(b)\end{aligned}$$

so ϕ is a homomorphism, and is hence an isomorphism. ■

Theorem 1.11. *Cyclic groups are abelian.*

Proof. Let $G = \langle g \rangle$ and let $a,b \in G$. Then,

$$\begin{aligned}ab &= g^n g^m\\ &= g^{n+m}\\ &= g^{m+n}\\ &= g^m g^n\\ &= ba\end{aligned}$$

by associativity. ■

Theorem 1.12. *If a group G has prime order p, then it is cyclic. That is, $G \cong C_p$.*

Proof. $|G| \geq 2$ as $p \geq 2$ is prime. Let $g \in G \setminus \{\mathrm{id}_G\}$. As $g \neq \mathrm{id}_G$, $|\langle g \rangle| > 1$. By Lagrange's theorem, $|\langle g \rangle|$ divides $|G| = p$, but p is prime, so $|\langle g \rangle| = |G|$, and hence $\langle g \rangle = G$. ■

1.6 Permutation Groups

If X is any set, then the collection of permutations on X has group structure under composition. This group is called the *symmetric group* on X, and is denoted $\mathrm{Sym}(X)$.

It doesn't really matter what the elements of X actually are, since they just label the inputs and outputs of the functions we're interested in, so the structure really only depends on the cardinality of X:

Theorem 1.13. *Suppose $|X| = |Y|$ for two sets X and Y. Then,* $\mathrm{Sym}(X) \cong \mathrm{Sym}(Y)$*.*

We then write $\mathrm{Sym}(n)$ or S_n for the symmetric group on n elements.

1.7 Dihedral Groups

Let P be a regular n-sided polygon in the plane with $n \geq 3$. The collection of isometries on P has group structure under composition. This group is called the *dihedral group* of order $2n$, and is denoted D_n.

These isometries consist of:

(i) n rotations through the angles $2\pi k/n$ for $0 \leq k < n$;

(i) n reflections.

We label the vertices of P in order and consider these isometries as permutations on these vertices. Then, the rotations are the elements a^k, $0 \leq k < n$, where $a = (1,2,\ldots,n)$ is the cyclic permutation corresponding to the rotation by $2\pi/n$, and the reflections are the elements $a^k b$, $0 \leq k < n$, where $b = (2,n)(3,n-1)(4,n-2)\ldots$ is the reflection that passes through the vertex 1.

In all cases, we have $ba = a^{n-1}b = a^{-1}b$, so $ba^k = a^{n-k}b = a^{-k}b$ for $0 \leq k < n$. This allows us to find the full Cayley table of this group expressed in this form as we can then perform any of the four basic types of products:

(i) $(a^k)(a^l) = a^{k+l}$

(ii) $(a^k)(a^l b) = a^{k+l}b$

(iii) $(a^k b)(a^l) = a^k(ba^l) = a^k a^{-l} b = a^{k-l}b$

(iv) $(a^k b)(a^l b) = a^k(ba^l)b = a^k a^{-l} bb = a^{k-l}$

with all exponents taken modulo n.

1.8 Permutation Notation

We write permutations in S_n in *cycle notation.*

Let $A_1,A_2,A_3,\cdots,A_m$ be distinct elements of $\{1,2,\cdots,n\}$. The *cycle*, $(A_1,A_2,A_3,\cdots,A_m)$ means that A_1 is mapped to A_2, A_2 to A_3, $\cdots$, A_{m-1} to A_m and A_m to A_1, and any elements not in the cycle are fixed in place.

The number of elements in the cycle is the *length* of the cycle. A cycle of length 2 is additionally called a *transposition.*

So, in S_5, the cycle of length 3, (1,4,5) would map the ordering [1,2,3,4,5] to [5,2,3,1,4].

Cycles are equivalent up to circular shifts, so, for example, $(1,2,3) = (3,1,2) = (2,3,1)$ as in all 3 cases, the cycle represents the mappings $1 \mapsto 2$, $2 \mapsto 3$, and $3 \mapsto 1$.

Two cycles are *disjoint* if they do not contain any numbers in common. Disjoint cycles additionally commute.

To invert a permutation given as a product of not necessarily disjoint-cycles, reverse each cycle, then reverse the order of cycles.

Example. Let $\rho = (1{,}12{,}7{,}4)(3{,}8{,}10)(9{,}5{,}6{,}2{,}11)$. What is ρ^{-1}?

Reverse the cycles to get $(4{,}7{,}12{,}1)(10{,}8{,}3)(11{,}2{,}6{,}5{,}9)$, then reverse the order of cycles, giving $\rho^{-1} = (11{,}2{,}6{,}5{,}9)(10{,}8{,}3)(4{,}7{,}12{,}1)$.

In this case, the cycles are all disjoint, and therefore commute, so the final step wasn't strictly necessary. However, it is required for inverting non-disjoint cycles.

1.9 The Alternating Group & Transpositions

Theorem 1.14. *Every permutation can be written as a product of transpositions.*

Proof. Every permutation can be written as a product of disjoint cycles, so it suffice to show that cycles can be written as products of transpositions. Then, $(A_1{,}A_2{,}A_3{,}\cdots{,}A_m) = (A_1{,}A_m)\cdots(A_1{,}A_3)(A_1A_2)$ ■

Example.

$$(1{,}2{,}3{,}4{,}5) = (1{,}5)(1{,}4)(1{,}3)(1{,}2)$$

Note that these transpositions are not disjoint, and do not commute. Furthermore, the transposition decomposition of a permutation is not unique.

Every permutation can be written as a product of an even number of transpositions, or an odd number of transpositions, but crucially, not both.

A permutation is *even* if it can be written as a product of an even number of transpositions, and similar for *odd*.

The alternating group $\mathrm{Alt}(X)$ on a set X is the set of even permutations on X under composition. As with $\mathrm{Sym}(X)$, the isomorphism classes of the alternating groups depend only on the cardinality of X, so we write $\mathrm{Alt}(n)$ or A_n for the alternating group on n elements.

A_n is a clearly a subgroup of S_n as we can write $A_n = \{\sigma \in S_n : \sigma \text{ is even}\}$, and it has order $\frac{n!}{2}$.

1.10 Cosets

Let G be a group, H be a subgroup of G, and g be an element of G. The set $gH = \{gh : h \in H\}$ is a *left coset* of H, and $Hg = \{hg : h \in H\}$ is a *right coset* of H. In the case of abelian groups written in additive notation, we denote the coset by $g + H$ rather than gH.

A coset of a subgroup has the same order as the subgroup, as inverses are unique.

Theorem 1.15. *The following statements are equivalent for all $g{,}k \in G$:*

(i) $k \in gH$

(ii) $gH = kH$

(iii) $gk^{-1} \in H$

Corollary 1.15.1. *Two left cosets g_1H and g_2H in G are either equal or disjoint.*

Proof. If g_1H and g_2H are not disjoint, then there exists some element $k \in g_1H \cap g_2H$. But then $g_1H = kH = g_2H$ by the above theorem. ■

Example. $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. What are the left cosets of $2\mathbb{Z}$ in $\mathbb{Z}$?

First, pick an element of $\mathbb{Z}$. Let's pick 0. Add it to every element of $2\mathbb{Z}$:

$$0 + 2\mathbb{Z} = \{\cdots, 0 + (-2), 0 + (0), 0 + (2), \cdots\} = 2\mathbb{Z}$$

so $2\mathbb{Z}$ is a left coset of $2\mathbb{Z}$ in $\mathbb{Z}$.

Now, let's pick 1 and add it to every element of $2\mathbb{Z}$:

$$1 + 2\mathbb{Z} = \{\cdots, 1 + (-2), 1 + (0), 1 + (2), \cdots\}$$

This is distinct from the previous set, so this is a new coset.

Now, if we try 2 or anything else, we'll find that we just land in one of our two previous cosets. In fact, these two cosets partition $\mathbb{Z}$, so we know we have them all. Thus, the left cosets of $2\mathbb{Z}$ in $\mathbb{Z}$ are $2\mathbb{Z}$ and $1 + 2\mathbb{Z}$.

Lemma 1.16. *If H is finite, then all left cosets have exactly $|H|$ elements. That is, $|gH| = |H|$ for all $g \in G$.*

Proof. The map $\phi : H \to gH$ defined by $\phi(h) = gh$ is a bijection by the cancellative property. ■

Let G be a group and H be a subgroup of G. The *index* $[G : H]$ is defined to be the number of left cosets (or right cosets, but not counting both) of H in G.

Example. What is the index $[\mathbb{Z} : 2\mathbb{Z}]$?

In the previous part, we found two cosets, so $[\mathbb{Z} : 2\mathbb{Z}] = 2$.

Theorem (Lagrange)**.** *If H is a subgroup of a group G, then $|G| = [G : H]|H|$.*

Proof. Let H be a subgroup of a group G, and define an equivalence relation R on all pairs of elements $x,y \in G$ such that xRy holds if and only if there exists $h \in H$ such that $x = yh$. Under this equivalence relation, the left cosets of H in G are equivalence classes, and therefore partition G into disjoint sets. The mapping $x \mapsto ax$ is inverted by $y \mapsto a^{-1}y$, and therefore defines a bijection $H \to aH$, so each left coset aH has the same cardinality as H. The number of left cosets is the index, $[G : H]$, so $|G| = [G : H]|H|$, as required. ■

If the index and sizes of each set are interpreted as cardinal numbers, Lagrange's theorem holds even if some of the sets are infinite in size.

Corollary (Lagrange)**.** *The order of any element a of a finite group divides the order of the group. Or equivalently, the order of any subgroup of a group divides the order of the group.*

2 Normal Subgroups

A subgroup N of a group G is *normal* in G if $gN = Ng$ for all $g \in G$, and we write $N \triangleleft G$ to denote this relation.

For any group, G, the trivial subgroup, $\{\mathrm{id}_G\}$, is always a normal subgroup of G. G itself is also always a normal subgroup of G. If these are the only normal subgroups, then G is a *simple* group.

Theorem 2.1. *If H is a subgroup of a group G such that $[G : H] = 2$, then H is normal in G.*

Proof. Since H has index 2, it has exactly two left cosets; H itself, and $G \setminus H$. H also has exactly two right cosets; H, and $G \setminus H$. Thus, the left and right cosets of H coincide and H is normal. ■

We give an alternative characterisation of normal subgroups:

Theorem 2.2. *If H is a subgroup of a group G such that $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$, then H is normal in G.*

That is, a subgroup N of a group G is normal if and only if it is invariant under conjugation (§4.2). That is, the conjugation of any element of N by any element of G is always in N; $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$. For this reason, normal subgroups are also sometimes called *invariant* or *self-conjugate* in G.

This then gives various equivalent conditions for a subgroup to be normal:

- For all $g \in G$, the left and right cosets gN and Ng are equal;
- The set of left and right cosets of N in G are equal;
- N is a union of conjugacy classes of G;
- The image of conjugation of N by any element of G is a subset of N;
- The image of conjugation of N by any element of G is equal to N.

(Some of these will be proved later.)

Theorem 2.3. *Every subgroup of an abelian group is normal.*

Proof. Let H be a subgroup of an abelian group G, and let $g \in G$. Let $x \in gHg^{-1}$ so $x = ghg^{-1}$ for some $h \in H$. Then,

$$\begin{aligned} x &= ghg^{-1} \\ &= hgg^{-1} \\ &= h \\ &\in H \end{aligned}$$

so H is invariant under conjugation by any g and is hence normal. ■

2.1 Direct Products

Let G and H be groups. The *direct product* (*group*) $G \times H$ of G and H is the group on the Cartesian product of G and H,

$$\{(g,h) : g \in G, h \in H\}$$

of ordered pairs of elements from G and H, under the operations of G and H applied componentwise. That is, we define the group operation $\star$ on $G \times H$ to be,

$$(g_1,h_1) \star (g_2,h_2) = (g_1 * g_2, h_1 \cdot h_2)$$

where $*$ is the group operation on G, and $\cdot$ is the group operation on H. The identity element $\mathrm{id}_{G\times H}$ is then given by $(\mathrm{id}_G, \mathrm{id}_H)$, and the inverse of (g,h) is (g^{-1},h^{-1}).

Theorem 2.4. *Any group of order 4 is isomorphic to either C_4 or $C_2 \times C_2$.*

Theorem 2.5. *Any group of order 6 is isomorphic to either C_6 or D_3.*

The *quaternion group* Q_8 is a non-abelian group of order 8, isomorphic to the set of quaternion units (and their inverses) under quaternion multiplication. That is, the set $\{1,i,j,k,-1,-i,-j,-k\}$ where $i^2 = j^2 = k^2 = ijk = -1$.

Theorem 2.6. *Any group of order 8 is isomorphic to either C_8 or $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_4, or Q_8.*

3 Quotient Groups

A *quotient group* or *factor group* is a group obtained by identifying similar elements of a larger group together using an equivalence relation that preserves some of the group structure, with the rest of the structure being "factored" out. For instance, the group of integers under addition modulo n, $(\mathbb{Z}/n\mathbb{Z},+)$ or equivalently, $(\mathbb{Z},+_n)$, can be obtained from the group of integers under addition, $(\mathbb{Z},+)$, by identifying elements that differ by a multiple of n, and defining a group structure that operates on congruence classes rather than individual elements.

Subgroups and quotient groups are dual notions, the two being the primary ways of constructing smaller groups from a larger one. Any normal subgroup has a corresponding quotient group, formed by eliminating the distinction between elements of the subgroups. For any congruence relation on a group G, the equivalence classes of the identity element is always a normal subgroup, N, of the original group, while the other classes are precisely the cosets of that normal subgroup, and the corresponding quotient group is G/N.

The reason why G/N is called a "quotient" group comes from an analogy with division of integers. When dividing 12 by 3, we obtain the answer 4 because we can split a collection of 12 objects into 3 subcollections each containing 4 objects. Quotient groups follow a similar idea, but when "dividing" groups, we end up with another group as the answer rather than a number, because groups have more structure than arbitrary collections of objects.

Lemma 3.1. *Let N be normal in G, and let $g,h \in G$. Then, the product of any element in the coset gN with any element in the coset hN is an element in the coset $(gh)N$.*

Proof. Let $gn_1 \in gN$ and $hn_2 \in hN$. Then, by normality of N, $gN = Ng$, so $n_1h \in Nh$ is equal to some element $hn \in hN$, and hence $(gn_1)(hn_2) = g(n_1h)n_2 = g(hn)n_2 = (gh)(nn_2) \in (gh)N$. ■

If A and B are subsets of a group G, we define their (*internal*) *product* AB to be the set $\{ab : a \in A, b \in B\}$.

Lemma 3.2. *If N is normal in G and gN and hN are cosets of N in G, then $(gN)(hN) = (gh)N$.*

Proof. By the previous lemma, $(gN)(hN) \subseteq (gh)N$. Then, let $n \in N$, so $(gh)n = (g\,\mathrm{id}_G)(hn) \in (gN)(hN)$ and $(gh)N \subseteq (gN)(hN)$. ■

Theorem 3.3. *Let N be normal in G. Then, the set G/N of left cosets gN of N in G forms a group under internal multiplication called the quotient group of G by N.*

Proof. By the previous lemma, $(gN)(hN) = (gh)N$, giving closure, and associativity is inherited from associativity in G. Then, $(1N)(gN) = (1g)N = gN = (g1)N = (gN)(1N)$ for all $g \in G$, so $1N$ is the identity element, and $(g^{-1}N)(gN) = (g^{-1}g)N = 1N$, so $(g^{-1})N$ is the inverse element of gN. ■

Note that if G is finite, then $|G/N| = [G : N] = |G|/|N|$.

Lemma 3.4. *If $H \leq G$, then the inclusion map $\phi : H \hookrightarrow G$ defined by $h \mapsto h$ for all $h \in H$ is a homomorphism. If $H = G$, then it is furthermore an (identity) isomorphism.*

3.1 Kernels and Images

Let $\phi : G \to H$ be a group homomorphism. Then, the *kernel* $\ker(\phi)$ of ϕ is the set of elements mapped to id_H. That is,

$$\ker(\phi) = \{g \in G : \phi(g) = \mathrm{id}_H\}$$

The *image* $\mathrm{im}(\phi)$ of ϕ is just its image as a function.

Theorem (Trivial Kernel (Groups))**.** *Let $\phi : G \to H$ be a group homomorphism. Then, ϕ is injective if and only if* $\ker(\phi) = \{\mathrm{id}_G\}$*.*

Proof. Since $\mathrm{id}_G \in \ker(\phi)$, $\phi(\mathrm{id}_G) = \mathrm{id}_H$. If ϕ is injective, then $\ker(\phi) = \{\mathrm{id}_G\}$. Conversely, suppose $\ker(\phi) = \{\mathrm{id}_G\}$. Let g_1,g_inG such that $\phi(g_1) = \phi(g_2)$. Then,

$$\begin{aligned} \mathrm{id}_H &= \phi(g_1)^{-1}\phi(g_1) \\ &= \phi(g_1)^{-1}\phi(g_2) \\ &= \phi(g_1^{-1}g_2) \end{aligned}$$

so $g_1^{-1}g_2 \in \ker(\phi)$, and hence $g_1^{-1}g_2 = \mathrm{id}_G$ and $g_1 = g_2$, so ϕ is injective. ■

Theorem 3.5. *Let $\phi : G \to H$ be a group homomorphism. Then,* $\ker(\phi)$ *is a normal subgroup of G.*

Theorem 3.6. *Let $N \lhd G$ be a normal subgroup. Then the map $\pi : G \to G/N$ defined by $g \mapsto gN$ is a surjective homomorphism with kernel* $\ker(\pi) = N$*.*

Proof. For any a,$b \in G$, $\pi(ab) = (ab)N = (aN)(bN) = \pi(a)\pi(b)$, so π is a homomorphism. Then, for any $gN \in G/N$, $gN = \pi(g)$, so π is surjective. Now, suppose $\pi(g) = \mathrm{id}_{G/N}$. Then,

$$\begin{aligned} \pi(g) &= \mathrm{id}_{G/N} \\ gN &= \mathrm{id}_G N \end{aligned}$$

Since $gN = \mathrm{id}_G N$, ${\mathrm{id}_G}^{-1}g = g \in N$, so $\ker(\pi) = N$. ■

This homomorphism is called the *quotient map*, or *natural* or *canonical* homomorphism from G to G/N.

Theorem 3.7. *Let $\phi : G \to H$ be a group homomorphism. Then,* $\mathrm{im}(\phi)$ *is a (not necessarily normal) subgroup of H.*

Proof. Let h_1,$h_2 \in \mathrm{im}(\phi)$, so there exist g_1,$g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Then,

$$h_1h_2^{-1} = \phi(g_1)\phi(g_2)^{-1} = \phi(g_1g_2) \in \mathrm{im}(\phi)$$

so $\mathrm{im}(\phi)$ is a subgroup by the one-step test. ■

3.2 The Isomorphism Theorems

Theorem (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a homomorphism with kernel* $\ker(\phi) = K$*. Then $G/K \cong$* $\mathrm{im}(\phi)$*, and more precisely, there is a homomorphism $\bar{\phi} : G/K \to$* $\mathrm{im}(\phi)$ *defined by $\bar{\phi}(gK) = \phi(g)$ for all $g \in G$.*

Proof. Clearly, $\mathrm{im}(\bar{\phi}) = \mathrm{im}(\phi)$, so $\bar{\phi}$ is surjective. Now, suppose $gK = hK$, so $gh^{-1} \in K$. Let $k = gh^{-1}$, so $g = kh$. Then, because $k \in K = \ker(\phi)$, $\phi(g) = \phi(k)\phi(h) = \phi(h)$, so $\bar{\phi}$ is a well-defined map.

Let aK,$bK \in G/K$. Then,

$$\begin{aligned} \bar{\phi}\big((aK)(bK)\big) &= \bar{\phi}\big((ab)K\big) \\ &= \phi(ab) \\ &= \phi(a)\phi(b) \\ &= \bar{\phi}(aK)\bar{\phi}(bK) \end{aligned}$$

so $\bar{\phi}$ is a homomorphism.

Finally, suppose $gK \in \ker(\bar{\phi})$, so,

$$\begin{aligned} \bar{\phi}(gK) &= \mathrm{id}_H \\ \phi(g) &= \mathrm{id}_H \end{aligned}$$

so $g \in \ker(\phi) = K$ ■

We restate the theorem with a commutative diagram.

Theorem (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a homomorphism with kernel $\ker(\phi) = K$ and let $\pi : G \to G/K$ be the quotient map. Then, there is an isomorphism $\bar{\phi} : G/K \to \mathrm{im}(\phi)$ such that the following diagram commutes:*

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[dr, "\phi"'] & G/\ker(\phi) \arrow[d, "\bar{\phi}"] \\ & \mathrm{im}(\phi) \end{tikzcd}$$

Proof. Suppose $aK = bK$. Then, $\phi(aK) = \phi(a)\phi(K) = \phi(a)$, and similarly for bK, so $a = b$. The universal property of quotients then yields the unique well-defined map $\bar{\phi} : G/K \to \mathrm{im}(\phi)$ such that the diagram above commutes, and since ϕ and π are surjective, $\bar{\phi} = \phi \circ \pi$ is also surjective. Now, suppose $\pi(g) \in \ker(\bar{\phi})$. Then, from commutativity, $\mathrm{id}_K = \bar{\phi}(\pi(g)) = \phi(g)$, so $g \in \ker(\phi)$, and hence $\ker(\bar{\phi}) = \{\ker(\phi)\}$, so $\bar{\phi}$ is injective. ■

The next two isomorphism theorems are less important, and are used mainly in more advanced group theory.

Theorem (Second Isomorphism Theorem)**.** *Let G be a group, $H \leq G$ be a subgroup, and $K \lhd G$ be a normal subgroup. Then,*

(i) $HK = KH$ is a subgroup of G;

(ii) $H \cap K$ is a normal subgroup of H;

(iii) $H/(H \cap K) \cong HK/K$.

Theorem (Third Isomorphism Theorem)**.** *Let G be a group and let $K \subseteq H \subseteq G$. Suppose K and H are both normal in G. Then,*

(i) K is normal in H;

(ii) H/K is a normal subgroup of G/K;

(iii) $(G/K)/(H/K) \cong G/H$.

4 Group Actions

Many groups we have used so far arise naturally from sets of functions from some set to itself. For instance, $\mathrm{Sym}(X)$ is the set of permutations on a set X; $GL_n(\mathbb{R})$ is the set of endofunctions on $\mathbb{R}^n$; and D_n is the set of isometries on the set of vertices of a regular n-gon. Informally, we'd might say that Sym "acts on" the set X, $GL_n(\mathbb{R})$ "acts on" $\mathbb{R}^n$; and D_n "acts on" the vertices of a regular n-gon. We can formalise this notion with *group actions.*

Let G be a group, and X a set. A (left) *action* of G on X is a map $\cdot : G \times X \to X$ satisfying,

$(A1)$ $\mathrm{id}_G \cdot x = x$ for all $x \in X$;

(*A*2) $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g,h \in G$ and $x \in X$.

Right group actions are defined similarly as maps $X \times G \to X$ satisfying analogous properties, but we will only consider left actions here.

Example.

- $\mathrm{Sym}(X)$ (and any subgroups, such as $\mathrm{Alt}(X)$) acts on X by the map $\rho \cdot x = \rho(x)$.
- $GL_n(\mathbb{R})$ (and any subgroups, such as $SL_n(\mathbb{R})$) acts on $\mathbb{R}^n$ by the matrix multiplication $\mathbf{A} \cdot \mathbf{v} = \mathbf{A}\mathbf{v}$.

In these examples, every element of the group induces a permutation on X, which is an element of $\mathrm{Sym}(X)$. In fact, this is always the case:

Theorem 4.1. *Let $\cdot$ be an action of a group G on a set X. For $g \in G$, define the map $\phi(g) : X \to X$ by $\phi(g)(x) = g \cdot x$. Then, $\phi(g) \in \mathrm{Sym}(X)$, and furthermore, $\phi : G \to \mathrm{Sym}(X)$ is a group homomorphism.*

This suggests an alternative characterisation of group actions as a homomorphism from a group to the symmetric group on some target set.

The *kernel* of an action $\cdot$ of G on X is defined to be the kernel $K = \ker(\phi)$ of the homomorphism $\phi : G \to \mathrm{Sym}(X)$ as defined in the above theorem. That is,

$$K = \{g \in G : g \cdot x = x \text{ for all } x \in X\}$$

If $K = \{\mathrm{id}_G\}$, we say that the action $\cdot$ is *faithful.*

Let $(G, *)$ be a group. Then, taking X to be the set G underlying the group, the left *regular action* of G on itself is the faithful action defined by $g \cdot x = g * x$.

For a faithful action with kernel K, $G \cong G/K$, as the quotient is trivial. Then, the first isomorphism theorem gives $G/K \cong \operatorname{im} \phi \leq \mathrm{Sym}(X)$, so $G \leq \mathrm{Sym}(X)$.

Theorem (Cayley)**.** *Every group is isomorphic to a subgroup of a symmetric group. Specifically, for each $g \in G$, the left-multiplication map $\ell_g : G \to G$ defined by $x \mapsto gx$ is a permutation on G, and the map $G \to \mathrm{Sym}(G)$ defined by $g \mapsto \ell_g$ is an injective homomorphism, thus embedding G into a subgroup of* $\mathrm{Sym}(G)$*.*

4.1 Orbits and Stabilisers

Let $\cdot$ be an action of G on X. Define the relation $\sim$ on $x,y \in X$ by $x \sim y$ if and only if there exists a $g \in G$ such that $y = g \cdot x$. Then, $\sim$ is an equivalence relation, and the equivalence classes are called the *orbits* of G on X. In particular, the orbits of a specific element $x \in X$, denoted by $G \cdot x$ or $\mathrm{Orb}_G(x)$ is,

$$\begin{aligned}\mathrm{Orb}_G(x) &= \{y \in X : (\exists g \in G : g \cdot x = y)\} \\ &= \{g \cdot x : g \in G\}\end{aligned}$$

An action of G on X is *transitive* if there is only a single orbit. Equivalently, an action is transitive if for every $x,y \in X$, there exists $g \in G$ such that $y = g \cdot x$.

Given $g \in G$ and $x \in X$ such that $g \cdot x = x$, we say that x is a *fixed point* of g, or that g *fixes* x. For each $x \in X$, the *stabiliser* (*subgroup*) of G with respect to x, denoted G_x or $\mathrm{Stab}_G(x)$, is the set of elements in G that fix x. That is,

$$\mathrm{Stab}_G(x) = \{g \in G : g \cdot x = x\}$$

This is a subgroup of G, but not necessarily a normal one.

Theorem 4.2. *Let G act on X and let $x \in X$. Then, $\bigcap_{x \in X} \mathrm{Stab}_G(x)$ is the kernel of the action of G on X.*

Proof. For any $g \in G$, $g \in \bigcap_{x \in X} \operatorname{Stab}_G(x)$ if and only if $g \cdot x = x$ for all $x \in X$, which is the definition of being in the kernel. ■

Theorem (Orbit-Stabiliser)**.** *Let a finite group G act on X, and let $x \in X$. Then,*

$$|G| = |\operatorname{Orb}_G(x)| \times |\operatorname{Stab}_G(x)|$$

Proof. Let $y \in \operatorname{Orb}_G(x)$, so there exists $g \in G$ such that $y = g \cdot x$, and let $H = \operatorname{Stab}_G(x)$. Now, suppose an element $g' \in G$ satisfies $y = g' \cdot x$. Then,

$$\begin{aligned} g' \cdot x &= y \\ g' \cdot x &= g \cdot x \\ g^{-1}g' \cdot x &= x \end{aligned}$$

so $g^{-1}g'$ fixes x, giving $g^{-1}g' \in \operatorname{Stab}_G(x) = H$. Then, $g' \in gH$, so the elements satisfying $g' \cdot x = y$ are exactly the elements of the coset gH, and as cosets of a set are equal in size, we have $|gH| = |H| = |\operatorname{Stab}_G(x)|$. It follows that for each $y \in \operatorname{Orb}_G(x)$, there are exactly $|\operatorname{Stab}_G(x)|$ elements g' of G such that $g' \cdot x = y$, so the total number of such y must be $|G|/|\operatorname{Stab}_G(x)|$. ■

4.2 Conjugation

Recall that the (left) regular action of a group $(G, *)$ is the action of the group on itself under the group operation, so $g \cdot x = g * x$. Another important action of G on itself is the *conjugation* action defined by,

$$g \cdot x = gxg^{-1}$$

for g,$x \in G$. The orbits of this action are called the *conjugacy classes* of G, and elements in the same conjugacy class are said to be *conjugate* in G. We write $\operatorname{Cl}_G(x)$ for the orbit of x, or equivalently, the conjugacy class containing x. That is,

$$\operatorname{Cl}_G(x) = \{gxg^{-1} : g \in G\}$$

The stabiliser for this action with respect to x is the set of elements $g \in G$ such that $g \cdot x = x$, so,

$$\begin{aligned} g \cdot x &= x \\ gxg^{-1} &= x \\ gx &= xg \end{aligned}$$

so the stabiliser is exactly the set of elements that commute with x. This subgroup is called the *centraliser* of x in G, and is denoted $C_G(x)$. That is,

$$C_G(x) = \{g \in G : gx = xg\}$$

Applying the orbit-stabiliser theorem then yields,

Theorem 4.3. *Let G be a finite group and let $x \in G$. Then,*

$$|G| = |\operatorname{Cl}_G(x)| \times |C_G(x)|$$

The kernel K of this action then consists of the elements that fix, and hence commute with, all elements $g \in G$. This is called the *centre* of G, and is denoted $Z(G)$. So,

$$Z(G) = \{f \in G : fg = gf \text{ for all } g \in G\}$$

Note that $g \in Z(g)$ if and only if $\operatorname{Cl}_G(g) = \{g\}$.

Example. For any abelian group G,

- $Z(G) = G$;
- $C_G(g) = G$;
- $\mathrm{Cl}_G(g) = \{g\}$.

for all $g \in G$.

Example. The symmetric group S_3 has three conjugacy classes that partition its six permutations of three objects:

- Identity ($abc \mapsto abc$);
- Transposing two elements ($abc \mapsto acb$,$abc \mapsto bac$,$abc \mapsto cba$);
- Cyclic permutations of three elements ($abc \mapsto cab, abc \mapsto cab$).

These three classes also correspond to the three ways of transforming a equilateral triangle: identity, reflections and rotations, respectively.

4.3 Conjugacy Classes in Symmetric Groups

Consider two permutations f,$g \in \mathrm{Sym}(X)$. Suppose one of the cycles in g is $(x_1,x_2,\dots,x_r)$, so $g(x_1) = x_2$, $g(x_2) = x_3$, etc. Then, $fg(x_1) = f(x_2)$, so $fgf^{-1}\big(f(x_1)\big) = fg(x_1) = f(x_2)$, and more generally, $fgf^{-1}\big(f(x_i)\big) = f(x_{i+1})$ for i taken modulo r. So, fgf^{-1} has a cycle $(f(x_1),f(x_2),\dots,f(x_r))$. This applies to any cycle in g, so we obtain:

Theorem 4.4. *Given a permutation g as a product of cycles, the conjugate fgf^{-1} of g by f is the permutation given by the same product of cycles with each $x \in X$ replaced with $f(x)$.*

Example. Let $X = \{1,2,3,4,5,6,7\}$, $g = (1,5)(2,4,7,6)$, and $f = (1,3,5,7,2,4,6)$. Then,

$$\begin{aligned} fgf^{-1} &= \big(f(1),f(5)\big)\big(f(2),f(4),f(7),f(6)\big) \\ &= (3,7)(4,6,2,1) \end{aligned}$$

A permutation has *cycle type* $2^{r_2}3^{r_3}4^{r_4}\dots n^{r_n}\dots$ if it has exactly r_i cycles of length i, for $i \geq 2$.

Example. The permutation (1,2,3)(4,5)(6,7)(8,9,10)(11,12,13,14),(15,16) has cycle type $2^3 3^2 4^1$ because it has 3 cycles of length 2, 2 cycles of length 3, and 1 cycle of length 4.

Theorem 4.5. *Two permutations in* $\mathrm{Sym}(X)$ *are conjugate in* $\mathrm{Sym}(X)$ *if and only if they have the same cycle type.*

4.4 Conjugacy Classes in Alternating Groups

Recall that the alternating group A_n is the subgroup of S_n that consists of even permutations. The odd and even permutations partition S_n, so the index of A_n in S_n is 2, so A_n is normal in S_n.

Theorem 4.6. *Let $g \in A_n$. Then, either,*

$$\mathrm{Cl}_{A_n}(g) = \mathrm{Cl}_{S_n}(g)$$

or

$$|\,\mathrm{Cl}_{A_n}(g)| = \frac{1}{2}|\,\mathrm{Cl}_{S_n}(g)|$$

hold.

4.5 Simple Groups

Recall that a non-trivial group G is *simple* if the only subgroups normal in G are G itself, and the trivial group $\{\mathrm{id}_G\}$.

Theorem 4.7. *Cyclic groups of prime order are simple.*

Proof. By Lagrange's theorem, the only possible order of their subgroups are 1 and p. Normality follows from cyclic groups being abelian. ■

In fact, these are the only abelian simple groups possible:

Theorem 4.8. *A simple abelian group is cyclic with prime order.*

Proof. Let G be simple and abelian, and let $g \in G \setminus \{\mathrm{id}_G\}$. If $|g|$ is infinite, then the subgroup generated by g^2 is non-trivial, as it contains $g^2 \neq \mathrm{id}_G$; and proper, as it does not contain g; so G is not simple. If $|g|$ is finite but composite, so $|g| = ab$, then the subgroup generated by g^a is similarly non-trivial and proper, so G is not simple. It follows that $|g|$ is finite and prime, and furthermore, we have $\langle g \rangle = G$, or else $\langle g \rangle$ would be a non-trivial proper subgroup. ■

There are also finite non-abelian groups that are simple. General simple groups have been classified into three main infinite families (with cyclic groups of prime order forming one of the families), and 26 separate groups that do not fit into any of the families, called the *sporadic groups.*

One of the other infinite families of simple groups consists of the alternating groups A_n for $n \geq 5$.

Lemma 4.9. *A subgroup H of a group G is normal in G if and only if H consists of a union of conjugacy classes of G.*

Proof. Recall that H is normal in G if and only if it is invariant under conjugation . That is, $ghg^{-1} \in H$ for all $g \in G$, $h \in H$. But this is just the statement that H is normal in G if and only if $\mathrm{Cl}_G(h) \subseteq H$ for all h. ■

4.6 Sylow's Theorems

One corollary of Lagrange's theorem is that the order of any subgroup H of a finite group G always divides the order of G. One obvious converse question to ask is if a group G has subgroups of all orders that divide $|G|$. This is true for some groups, like finite cyclic grops. However, it is not true in general:

Theorem 4.10. *A_4 has no subgroup of order* 6.

Proof. Suppose A_4 has a subgroup H of order 6. Groups of order 6 must be cyclic or dihedral, and A_4 has no elements of order 6, so $H \cong S_3$, so H must have 3 elements of order 3. Specifically, H must contain the identity element and 3 pairs of transpositions. But then these elements form a subgroup of A_4, so H contains a subgroup of order 4, contradicting Lagrange's theorem. ■

Let G be a finite group of order $p^n m$, where n is the largest power of the prime p that divides $|G|$, so m is not divisible by p. A subgroup of G of order p^n is a *Sylow p-subgroup* of G.

Theorem (Sylow's Theorems)**.** *Let G be a finite group, p a prime, and $|G| = p^n m$, where $p \nmid m$. Then,*

(i) G has a Sylow p-subgroup, and any subgroup of G of order p^a for $1 \leq a \leq n$ is contained in a Sylow p-subgroup of G.

(ii) Any two Sylow p-subgroups of G are conjugate in G. That is, if H and K are Sylow p-subgroups of G, then there exists an element $g \in G$ such that $gHg^{-1} = K$.

(iii) The number r of Sylow p-subgroups of G satisfies $r \equiv 1 \pmod{p}$ and $r|m$.

Let G be a group of order $p^n m$ with $n \geq 1$ and $p \nmid m$. We define $\mathrm{Syl}_p(G)$ to be the set of Sylow p-subgroups of G,

$$\mathrm{Syl}_p(G) = \{H \leq G : |H| = p^n\}$$

and by Sylow's first theorem, this set is always non-empty. It turns out that this set is closed under conjugation:

Lemma 4.11. *If $P \in \mathrm{Syl}_p(G)$ and $g \in G$, then $gPg^{-1} \in \mathrm{Syl}_p(G)$.*

Now, consider the map $\cdot : G \times \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G)$ defined by $g \cdot H = gHg^{-1}$ for $H \in \mathrm{Syl}_p(G)$. The above lemma verifies the correctness of the codomain, but this map can furthermore be shown to be a group action of G on $\mathrm{Syl}_p(G)$. Now, $\mathrm{Orb}_G(P) = \{gPg^{-1} : g \in G\}$, and by Sylow's second theorem, this action is transitive, so,

$$\mathrm{Orb}_G(P) = \mathrm{Syl}_p(G)$$

Then, by the orbit-stabiliser theorem and Lagrange's theorem, we have,

Lemma 4.12. $|\mathrm{Syl}_p(G)|$ *divides* $|G|/|P|$.

Theorem 4.13. *If there is only one Sylow p-subgroup of G, then it is normal in G.*

4.7 Sylow's Theorem and Simple Groups

Theorem 4.14. *There are no simple groups of order* $2\,552$.

Proof. Let G be a group of order $2\,552 = 8 \cdot 11 \cdot 29$.

Take $p = 11$, so $|G| = 11 \cdot (8 \cdot 29) = 11^1 \cdot 232$. The number of Sylow 11-subgroups, r, must divide 232 and satisfy $r \equiv 1 \pmod{11}$. $r = 1$ clearly satisfies the requirements. For other values of r, consider the factorisation $232 = 2^3 \cdot 29$. The factors of 232 are then, 1, 2, 4, 8, $29 \equiv 7$, $58 \equiv 3$, and $116 \equiv 6$, and $232 \equiv 1$, so $r = 232$ is the only other solution.

Now, if G has more than 1 Sylow 11-subgroup, then it must have 232 Sylow 11-subgroups. As 11 is prime, these subgroups must be cyclic, so every non-identity element generates the group. It follows that these subgroups intersect only at the identity element, so each subgroup contributes 10 elements of order 11, so there must be $232 \cdot 10 = 2\,320$ elements of order 11 in G.

Now, take $p = 29$, so $|G| = 29 \cdot (8 \cdot 11) = 29^1 \cdot 88$. By identical arguments as before, the number of Sylow 29-subgroups must be 1 or 88, and again, as 29 is prime, each subgroup must be cyclic, so if there is more than 1 Sylow 29-subgroup, then there are $88 \cdot 28 = 2\,464$ elements of order 28.

Now, by Sylow's first theorem, there exist Sylow 29 and 11-subgroups. If there are more than one of each, then we have $2\,320$ and $2\,464$ elements of order 11 and 29, respectively. But these values sum to more than $2\,552 = |G|$, so we cannot simultaneously have more than 1 Sylow 29 and 11-subgroups. But then, any lone Sylow p-subgroup is normal, so G is not simple. ■

5 Rings

A *ring* is a triple, $(R, +, \cdot)$, where R is a set and $+$ and $\cdot$ are binary operations $R \times R \to R$ such that,

(R0) R is closed under $\times$;

(R1) R is an abelian group under $+$;

(R2) $\cdot$ is associative on R;

(R3) $\cdot$ left and right distributes over $+$;

(R4) R contains an identity under ×.

or in more detail,

(R0) $\forall a{,}b \in R, a \cdot b \in R$ (closure of $\cdot$);

(R1) $(R{,}{+})$ is an abelian group (additive group);

(R2) $\forall a{,}b{,}c \in R, a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity of $\cdot$);

(R2) $\forall a{,}b{,}c \in R, (a + b) \cdot c = a \cdot c + b \cdot c$ and $a \cdot (b + c) = a \cdot b + a \cdot c$ (left and right distributivity);

(R3) $\exists 1_R \in R$ such that $\forall a \in R, a \cdot 1_R = 1_R \cdot a = a$ (existence of multiplicative identity).

We call the operation denoted by + *addition*, and the operation denoted by × *multiplication* or *product*, regardless of what the operations actually are. We also call the additive identity 0_R the *ring zero*, as it is also the zero element for the multiplication operation.

Triples satisfying only axioms R0 to R3 are sometimes called *rngs* (as in, rings without identity), and in contrast, rings *with* identity are called *unital rings* to distinguish them from rngs. Whenever "ring" is used without qualification, we will assume that it is a unital ring.

$(R, + , \times)$ is furthermore a *commutative ring* if it satisfies

(R5) × is commutative on R.

Note that the "commutative" part of the name "commutative ring" refers to commutativity of multiplication, as commutativity of addition is required in all rings regardless. However, rings notably do *not* require multiplicative inverses.

Example.

- The set $\{0\}$ under the trivial operations $0 + 0 = 0$ and $0 \cdot 0 = 0$ forms the *zero* or *trivial* ring.
- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative rings under their usual addition and multiplication operations.
- $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$ is a commutative ring under addition and multiplication modulo n for all naturals $n \in \mathbb{N}$.
- If R is a ring, the set $R[x]$ of polynomials in indeterminate x and coefficients in R is another ring under the usual addition and multiplication of polynomials.
- If R is a ring, then the set $M_{n\times n}(R)$ of $n \times n$ matrices with entries in R is another ring. Matrix rings are generally non-commutative, and in fact, are commutative if and only if R is the trivial ring, or R is commutative and $n = 1$.

Let $(R, + , \cdot\,)$ be a ring, and let S be a subset of R. Furthermore, suppose that $(S, + , \cdot\,)$ is also a ring. $(S, + , \cdot\,)$ is then a *subring* of $(R, + , \cdot\,)$.

To show that S is a subring of R, it suffices to show that S contains the identity of + and $\cdot$, is closed under + and $\cdot$, and that every element has an inverse in S under +. More symbolically, if R is a ring, then $S \subseteq R$ is a subring if and only if,

- $0_R \in S$ (additive identity);
- $1_R \in S$ (multiplicative identity);
- If $a{,}b \in S$ then $a + b \in S$ (closure under +);
- If $a{,}b \in S$ then $a \cdot b \in S$ (closure under ×);
- If $a \in S$ then $(-a) \in S$ (additive inverses).

Associativity is inherited from the main ring, and you do not have to check for multiplicative inverses.

We can collapse some of these properties together:

Theorem (Subring Test)**.** *If $(R, +, \cdot)$ is a ring and $S \subseteq R$, then $(S, +, \cdot)$ is a subring of R if and only if,*

1. *$(S,+)$ is a subgroup of $(R,+)$;*
2. *$a,b \in S \to ab \in S$;*
3. *$1_R \in S$.*

Proof. The reverse direction is trivial. Conversely, suppose the three conditions above hold for a subset $S \subseteq R$. We verify the ring axioms:

(R0) Closure follows directly from condition 2.

(R1) $(S,+)$ is an abelian group as it is a subgroup of an abelian group by condition 1.

(R2) Associativity is inherited from R as $S \subseteq R$.

(R3) Distributivity is inherited from R as $S \subseteq R$.

(R4) Multiplicative identity follows directly from condition 3.

■

Example.

- $\mathbb{Z}[i] = \{a + bi : a,b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$ called the ring of *Gaussian integers.*
- $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} : a,b \in \mathbb{Z}\right\}$ is a subring of $\mathbb{R}$.
- The set,
$$\left\{\frac{a}{2^n} : a \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0}\right\}$$
is a subring of $\mathbb{Q}$ called the ring of *dyadic rationals.*

These examples show that it can be easier to describe a ring by expressing it as a subring of a different known ring, as we avoid having to define the multiplication and addition operations, and do not have to verify associativity and distributivity.

Theorem 5.1. *The intersection of subrings of a ring R is itself a subring of R.*

5.1 Morphisms

A *(ring) homomorphism* between two rings $(R, +, \cdot)$ and $(S, \oplus, \odot)$ is a function $\phi : R \to S$ that preserves the structure of R. That is,

- $\phi(a + b) = \phi(a) \oplus \phi(b)$;
- $\phi(a \cdot b) = \phi(a) \odot \phi(b)$;
- $\phi(1_R) = 1_S$.

Additive inverses and the additive identity are also part of the preserved structure, but they are not explicitly specified as they follow from these three conditions.

If the inverse of a ring homomorphism is a homomorphism, or equivalently, if the homomorphism is a bijection, then it is called a (ring) isomorphism. If an isomorphism exists between R and S, we say that

R and S are isomorphic (rings), and we write $R \cong S$ to denote this relation. Again, isomorphism is an equivalence relation.

Like with groups, an injective ring homomorphism is also called a *monomorphism*, and a surjective homomorphism is called an *epimorphism.*

Example.

- For each $n \in \mathbb{N}$, the map $x \mapsto x \pmod{n}$ is a ring homomorphism $\mathbb{Z} \to \mathbb{Z}_n$.
- The map $z \mapsto \overline{z}$ is a ring isomorphism $\mathbb{C} \to \mathbb{C}$.
- If R is any ring and S is a subring of R, then for each element $\alpha \in R$, the map $\phi_\alpha : S[x] \to R$ defined by $f \mapsto f(\alpha)$ is a ring homomorphism known as the *evaluation map* (at α).
- If $\phi : R \to S$ is a ring homomorphism, then there is an *induced* homomorphism $\psi : R[x] \to S[x]$, defined by,
-

$$\psi(a_n x^n + \ldots + a_1 x + a_0) = \phi(a_n)x^n + \cdots + \phi(a_n)x + \phi(a_0)$$

Let $\phi : R \to S$ be a ring homomorphism. Then, the *kernel* $\ker(\phi)$ of ϕ is its kernel when treated as a group homomorphism between the additive groups of R and S. That is, the set of elements that are mapped to the additive identity:

$$\ker(\phi) = \{r \in R : \phi(r) = 0_S\}$$

The *image* $\mathrm{im}(\phi)$ of ϕ is just its image as a function.

We have similar results for ring homomorphisms as we had for group homomorphisms:

Theorem (Trivial Kernel (Rings))**.** *Let $\phi : R \to S$ be a ring homomorphism. Then, ϕ is injective if and only if* $\ker(\phi) = \{0_r\}$.

Proof. See § 3.1. ■

Theorem 5.2. *Let $\phi : R \to S$ be a ring homomorphism. Then,* $\mathrm{im}(\phi)$ *is a subring of S.*

Proof. Follows from the subring test. ■

Note that the kernel of a ring homomorphism is *not* necessarily a subring of the target ring. For example, the kernel of the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_n$ is the set $n\mathbb{Z}$, which does not contain 1 for all $n \geq 2$.

Let R and S be rings. The *direct product* (*ring*) $R \times S$ of R and S is the ring on the Cartesian product of R and S,

$$\{(r,s) : r \in R, s \in S\}$$

of ordered pairs of elements from R and S, under the two operations of R and S both applied componentwise. That is,

$$(r_1,s_1) + (r_2,s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1,s_1) \cdot (r_2,s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

where $+$ and $\cdot$ on the left are the ring operations on $R \times S$, and the two $+$ and $\cdot$ operations on the right are the appropriate ring operations on R and S. The multiplicative identity element $1_{R\times S}$ is then given by $(1_R, 1_S)$; the additive identity $0_{R\times S}$ by $(1_R, 1_S)$; and the additive inverse of (r,s) by $(-r, -s)$.

Notice that R and S are not generally isomorphic to subrings of $R \times S$ in general, even under the obvious projection mapping. For instance, R can be thought of as the elements of $R \times S$ of the form $(r,0_S)$, and these elements do indeed define a ring isomorphic to R, but its multiplicative identity element is $(1_R,0_S)$, which is not the identity of $R \times S$, so this ring is not a subring of $R \times S$.

Theorem (Chinese Remainder Theorem)**.** *$Z_n \times Z_m \cong Z_{nm}$ if and only if n and m are coprime.*

By induction, we can extend this result to,

Corollary 5.2.1. *If $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$ is a factorisation of n into k distinct primes, then,*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$$

Theorem 5.3. *Let R be a ring and $a,b \in R$. Then,*

(i) $a \cdot 0 = 0 \cdot a = 0$*;*

(ii) $a \cdot (-1) = (-1) \cdot a = -a$*.*

Proof. For (i),

$$\begin{aligned} a \cdot 0 &= a \cdot (0 + 0) \\ &= a \cdot 0 + a \cdot 0 \end{aligned}$$

so $a \cdot 0 = 0$ by the cancellative property in the group $(R,+)$, and similarly, $0 \cdot a = 0$.

For (ii),

$$\begin{aligned} (-1) \cdot a + 1 \cdot a &= (-1 + 1) \cdot a \\ &= 0 \cdot a \\ &= 0 \end{aligned}$$

so $(-1) \cdot a = -a$ by uniqueness of inverses in the group $(R,+)$, and similarly, $a \cdot (-1) = -a$. ■

Theorem (Uniqueness of Multiplicative Identity)**.** *The multiplicative identity of a ring is unique.*

Proof. Suppose 1 and $1'$ are multiplicative identities of R. Then, $1 = 1 \cdot 1' = 1'$. ■

Theorem (Coinciding Identities)**.** *Let R be a ring, and suppose that the additive and multiplicative identities coincide, so $0 = 1$. Then, R is the trivial ring.*

Proof. For all $a \in R$, $a = a \cdot 1 = a \cdot 0 = 0$. ■

If a ring is not the trivial ring, we also say that it is a *non-zero* ring.

6 Ideals

For an arbitrary ring, $(R, + , \cdot\,)$, let $(R,+)$ be its additive group. A subset $I \subseteq R$ is a *left ideal* in R if,

(I1) $(I,+)$ is a subgroup of $(R,+)$,

(I2) For every $r \in R$ and every $x \in I$, $r \cdot x \in I$, A *right ideal* is defined similarly, with $r \cdot x \in I$ being replaced with $x \cdot r \in I$ in the second requirement, and a *two-sided ideal*, or just *ideal*, is a left ideal that is also a right ideal. If the ring is commutative, then the definitions of left, right and two-sided ideals coincide.

So, an ideal is a subset of the ring that is a group under the ring addition restricted to the subset and absorbs multiplication from one or both sides.

Theorem 6.1. *An ideal I of a ring R contains 1_R only when $I = R$.*

Theorem 6.2. *If $\phi : R \to S$ is a ring homomorphism, then $\ker(\phi)$ is an ideal in R.*

Proof. $\ker(\phi)$ is an additive subgroup of R when ϕ is considered as a group homomorphism. Then, if $r \in \ker(\phi)$ and $x \in R$, then,

$$\begin{aligned} \phi(x \cdot r) &= \phi(x) \cdot \phi(r) \\ &= \phi(x) \cdot 0_S \\ &= 0_S \end{aligned}$$

so $x \cdot r \in \ker(\phi)$. Similarly, $r \cdot x \in \ker(\phi)$, so $\ker(\phi)$ absorbs multiplication as well, and is hence an ideal in R. ■

When R is a commutative ring, the subset,

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

consisting of all multiples of a in R is an ideal of R. This ideal is called the *principal ideal* generated by a, and is denoted (a), aR, or Ra.

For an arbitrary ring, the principal ideal (a) is equal to the set of finite sums,

$$\left\{ \sum_{i=1}^{k} r_i a s_i : r_i, s_i \in R \right\}$$

Theorem 6.3. *If R is commutative, then $(a) = R$ if and only if a is a unit of R.*

6.1 Quotient Rings

Ideals are to rings what normal subgroups are to groups in that we can quotient a ring by an ideal to generate another ring, just like how groups can be factored through by a normal subgroup.

Since an ideal I of a ring R is a subgroup of $(R,+)$, we can consider its cosets $I + a$ for $a \in R$. We already know that these form a quotient group under the addition operation defined by,

$$(I + a_1) + (I + a_2) = I + (a_1 + a_2)$$

But to define a ring structure, we also require a multiplication operation.

Theorem (Quotient Ring)**.** *Let I be an ideal of R. Then, the set R/I of cosets $I + a$ of I in R forms a ring under the addition operation in the quotient group, and the multiplication,*

$$(I + a) \cdot (I + b) = I + (a \cdot b)$$

Example. The quotient ring $\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$ is isomorphic to the ring $\mathbb{Z}_n$ of residues modulo n, with the isomorphism $\mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$ given by $x \mapsto x + n\mathbb{Z}$.

Theorem 6.4. *Let I be an ideal of a ring R. Then, the map $\pi : R \to R/I$ defined by $\pi(a) = I + a$ is a surjective ring homomorphism with kernel I called the quotient map.*

Theorem (First Isomorphism Theorem)**.** *Let $\phi : R \to S$ be a homomorphism with kernel* $\ker(\phi) = I$. *Then $R/I \cong \operatorname{im}(\phi)$, and more precisely, there is a homomorphism $\bar{\phi} : R/I \to \operatorname{im}(\phi)$ defined by $\bar{\phi}(I+a) = \phi(a)$ for all $a \in R$.*

6.2 Integral Domains

Let R be a ring, and let $a,b \in R$. If a and b are both non-zero and satisfy $ab = 0$, then a and b are called (*left* and *right*, respectively) *zero divisors.*

A ring R is an (*integral*) *domain* if,

(i) R is commutative;

(ii) R is not the trivial ring;

(iii) R has no zero divisors; that is, if $a,b \in R$, then $a \cdot b = 0 \to (a = 0 \lor b = 0)$.

That is, an integral domain is a non-zero commutative ring in which the product of any two non-zero elements is non-zero.

Example.

- The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are integral domains.
- Subrings of integral domains are also integral domains, so $\mathbb{Z}[i]$ and $\mathbb{Z}\left[\sqrt{2}\right]$ are also integral domains.

Again, it can be easier to describe integral domains as subrings of other known integral domains.

Theorem 6.5. *$\mathbb{Z}_n$ is an integral domain if and only if n is prime.*

Proof. If $n = 1$, then $\mathbb{Z}_n \cong \{0\}$. If $n = ab$ is composite, then $ab = 0$ with $a,b \neq 0$ in Z_n. If n is prime and $a,b \in \mathbb{Z}_n$, then a and b are coprime to n, and hence ab is coprime to n by multiplicativity of gcd, so n does not divide ab, and $ab \neq 0$ in $\mathbb{Z}_n$. ■

6.3 Units

An element, a, of a ring R is a *unit* if it has a two-sided inverse under multiplication. That is, there exists some $b \in R$ such that $a \cdot b = b \cdot a = 1$.

Note that in any non-trivial ring, the additive identity 0_R is not a unit.

The *unit group* of R is the group formed by the set $\{a \in R : a \text{ is a unit in } R\}$ under the ring multiplication operation, denoted R^*.

Example. In $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, every non-zero element, k, has a multiplicative inverse, $\frac{1}{k} \in \mathbb{Q},\mathbb{R},\mathbb{C}$, so the units are the non-zero elements. $\mathbb{Q}^*$, $\mathbb{R}^*$ and $\mathbb{C}^*$ are therefore $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ and $\mathbb{C} \setminus \{0\}$, respectively.

However, in $\mathbb{Z}$, $\frac{1}{k}$ is an integer only for $k = \pm 1$, so the units in $\mathbb{Z}$ are ± 1. $\mathbb{Z}^*$ is therefore $\{-1,1\}$.

In $\mathbb{Z}_n$, an element $a \in \mathbb{Z}_n$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if a and n are coprime (by the Euclidean algorithm and Bézout's identity), so $\mathbb{Z}_n^* = \{a : \gcd(a,n) = 1\}$.

A non-trivial ring R is called a *division ring* if $R \setminus \{0_R\}$ is a group under multiplication. That is, if every non-zero element is a unit, or, if $R \setminus \{0_R\} = R^*$.

A *field* is a commutative division ring. So, in total, $(F, +, \times)$ is a field if,

- $(F,+)$ is an abelian group with additive identity 0_F;
- $(F \setminus \{0_F\},\times)$ is an abelian group with multiplicative identity 1_F;
- $0_F \neq 1_F$ (the *non-degeneracy* condition);

- multiplication distributes over addition.

Example.

- $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields.
- For any prime p, $\mathbb{Z}/p\mathbb{Z}$ is a finite or *Galois* field, sometimes denoted $\mathbb{F}_p$.

Theorem 6.6. *Every field is an integral domain.*

Proof. Let F be a field. Suppose there exist $x,y \in F \setminus \{0\}$ such that $xy = 0$. As F is a field, $x \neq 0$ has a multiplicative inverse x^{-1}, so,

$$\begin{aligned} xy &= 0 \\ x^{-1}xy &= 0 \\ y &= 0 \end{aligned}$$

contradicting the definition of y. ■

Lemma (Cancellative Properties in Domains)**.** *Let R be an integral domain, and let $x,y,c \in R$. If,*

- *$c \neq 0$;*
- *$cx = cy$ or $xc = yc$,*

then $x = y$.

Proof.

$$\begin{aligned} cx &= cy \\ cx - cy &= 0 \\ c(x-y) &= 0 \end{aligned}$$

Since R is a domain, and $k \neq 0$, we must have $x - y = 0$, so $x = y$. The proof for $xc = yc$ is similar. ■

Theorem 6.7. *Every finite integral domain is a field.*

Proof. Let $R = \{0_R = r_0, r_1, r_2, \ldots, r_n\}$ be a finite domain. By the previous lemma, for a fixed $i > 0$, the n products $r_i r_j$ for $1 \leq j \leq n$ are distinct and non-zero, and since there are only n possible values, they all occur exactly once. In particular, this means that $r_i r_j = 1_R$ for some j, so R is a field. ■

Let R be a ring. If there exists a positive integer n such that $nx = 0$ for all $x \in R$, then, then we call the minimal such positive integer the *characteristic* of R. If no such positive integer exists, then the characteristic is 0.

Example.

- $\mathbb{Q}$ and $\mathbb{Z}$ have characteristic 0.
- $\mathbb{Z}_n$ has characteristic n.
- The polynomial ring $R[x]$ has the same characteristic as R.

7 Polynomial Rings

Let $R[x]$ be a polynomial ring over a ring R. If an element $f \in R[x]$ has the form,

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with $a_n \neq 0$, then we define the degree $\deg(f)$ of f to be n, and a_n is the *leading coefficient* of f. If $a_n = 1$, then f is a *monic* polynomial.

Note that non-zero constant polynomials consisting of a single element of R have degree 0, and the degree of the zero polynomial is undefined, although some texts take it to be -1 or $-\infty$.

Theorem 7.1. *If R is an integral domain, then so is $R[x]$.*

Theorem 7.2. *If R is an integral domain, then the units of R and $R[x]$ coincide.*

Note that these properties can fail if R is not an integral domain. For example, $\mathbb{Z}_4$ is not a integral domain as $2 \cdot 2 = 4 \equiv 0$ in $\mathbb{Z}_4$. Then, the polynomial $f = 2x + 1 \in \mathbb{Z}_4[x]$ gives $f \cdot f = 4x^2 + 4x + 1 \equiv 1$, so f is a unit in $\mathbb{Z}_4[x] \setminus \mathbb{Z}_4$.

We can also define polynomial rings in multiple variables. We write $R[x_1, \ldots, x_n]$ for the ring of polynomials in n independent commuting indeterminates $x_1, \ldots, x_n$ with coefficients in R. A *monomial* in this ring is an expression of the form $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, where $a_1, \ldots, a_n$ are non-negative integers, and a *polynomial* in this ring is a linear combination of these monomials with coefficients in R.

Note that we can also build up a polynomial ring in multiple variables as a chain of polynomial rings in single variables. For instance, if $S = R[x_1]$, then $R[x_1, x_2] = S[x_2]$, and so on. By induction on the previous 2 theorems, if R is an integral domain, then $R[x_1, \ldots, x_n]$ is an integral domain and the units of R and $R[x_1, \ldots, x_n]$ coincide.

Lemma 7.3. *$R[x_1, \ldots, x_n]$ is commutative if and only if R is commutative.*

7.1 Polynomial Division

Throughout this section, F will be a field.

Theorem (Polynomial Divison with Remainder)**.** *For any $f, g \in F[x]$ with g non-zero, there exist $q, r \in F[x]$ such that $f = qg + r$, where either $r = 0$ or $\deg(r) < \deg(g)$.*

Theorem (Remainder Theorem)**.** *Let $f = f(x) \in F[x]$. Then, for $a \in F$, $f(a) = 0$ if and only if $(x - a)$ divides f.*

Proof. By the previous proposition,

$$f(x) = g(x)(x - a) + r(x)$$

Since $\deg(x - a) = 1$, $r = 0$ or $\deg(r) < 1$, so $r \in F$ is a constant polynomial. Then,

$$\begin{aligned} f(a) &= g(a)(a - a) + r \\ &= r \end{aligned}$$

■

Corollary 7.3.1. *If $f \in F[x]$ is not the zero polynomial, then $f(a) = 0$ for at most $\deg(f)$ distinct values of $a \in F$. That is, a polynomial of degree d has at most d roots.*

Proof. By induction on $\deg(f)$. If $\deg(f) = 0$, then f is a constant non-zero function, so $f(a) \neq 0$. If otherwise $\deg(f) > 0$ and f has no roots, we are done.

Now, suppose $f(a) = 0$ for some $a \in F$, so $f = g(x - a)$ with with $\deg(g) = \deg(f) - 1$. If we then have $f(b) = 0$, then either $a = b$, or $g(b) = 0$, in which case, there are at most $\deg(f) - 1$ such values of b by the inductive hypothesis. ■

Theorem 7.4. *Let F be a field. Then, all finite subgroups of the unit group F^* are cyclic.*

Corollary 7.4.1. *If p is prime, then the set $\mathbb{Z}_p \setminus \{0\} = \{1,2,\ldots,p\}$, under multiplication modulo p, is a cyclic group of order $p - 1$.*

8 Principal Ideal Domains

The ring R will be an integral domain (and is hence commutative) for this section.

Recall that in a commutative ring, the principal ideals are those of the form $(a) = aR$ for some fixed $a \in R$.

A domain R is a *principal ideal domain* (PID) if every ideal of R is principal.

Theorem 8.1. *For every field F, the polynomial ring $F[x]$ is a principal ideal domain.*

Various familiar properties of divisibility that hold in $\mathbb{Z}$ hold in more general PIDs. But first, we need to extend the notion of divisibility to general integral domains.

Let $x,y \in R$. We say that x *divides* y if $y = xr$ for some $r \in R$, and we write $x|y$ to denote this relation.

Lemma 8.2. *The following statements are equivalent in an integral domains R:*

(i) $x|y$;

(ii) $y \in (x)$;

(iii) $(y) \subseteq (x)$.

Proof. *(i)* → *(ii)*: If $x|y$, then $y = xr$ for some $r \in R$, so $y \in (x) = \{xt : t \in R\}$.

(ii) → *(iii)*: If $y \in (x)$, then $y = xr$ for some $r \in R$, so

$$\begin{aligned}(y) &= \{yt : t \in R\} \\ &= \{(xr)t : t \in R\} \\ &= \{x(rt) : t \in R\} \\ &\subseteq \{xk : k \in R\} \\ &= (x)\end{aligned}$$

(iii) → *(i)* $y \in \{yt : t \in R\} \subseteq \{xr : r \in R\}$, so $y = xr$ for some $r \in R$ and $x|y$. ■

Let $x,y \in R$. If both $x|y$ and $y|x$, then x and y are *associate* in R, and we write $x \sim y$.

Lemma 8.3. *The following statements are equivalent in an integral domains R:*

(i) $x \sim y$;

(ii) $(y) = (x)$;

(iii) *There exists a unit $q \in R$ such that $x = qy$.*

Example.

- In $\mathbb{Z}$, the only units are ± 1, so $x \sim y$ if and only if $|x| = |y|$.
- If F is a field, then the units in $F[x]$ are the non-zero constants, so $x \sim y$ if and only if $x = ay$ for some $a \in F \setminus \{0\}$, so every polynomial is associate to a unique monic polynomial.

Let $x,y \in R$. A *greatest common divisor* $\gcd(x,y)$, also called a *highest common factor*, is an element $d \in R$ such that,

(i) $d|x$ and $d|y$;

(ii) if $k|x$ and $k|y$ for some $k \in R$, then $k|d$.

so a greatest common divisor is a maximal element with respect to the partial ordering induced by divisibility.

A *least common multiple* $\operatorname{lcm}(x,y)$ is an element $m \in R$ such that,

(i) $x|m$ and $y|m$;

(ii) if $x|k$ and $y|k$ for some $k \in R$, then $m|k$.

so a least common multiple is a minimal element, as above. Greatest common divisors and least common multiples are dual notions. Note that $\gcd(0,x) = x$ and $\operatorname{lcm}(0,x) = 0$ for any $x \in R$.

Note that a greatest common divisor is not unique. For example, in $\mathbb{Z}$, 2 and -2 are both greatest common divisors of 4 and 6. Any two greatest common divisors must divide each other, and are hence associate. Similar statements hold for least common multiples. So, gcds and lcms and are unique up to the associate relation.

Proving existence of gcds is more difficult. In arbitrary integral domains, they do not always exist, but in PIDs, they do, and in fact, for the PID $\mathbb{Z}$ this is exactly the statement of Bézout's identity.

Theorem 8.4. *If R is a PID, then $\operatorname{lcm}(x,y)$ and $\gcd(x,y)$ exist for all $x,y \in R$. Furthermore, there exist $r,s \in R$ such that $\gcd(x,y) = rx + sy$.*

8.1 Prime and Irreducible Elements

There are two different ways to characterise prime numbers, but these definitions lead to distinct notions in arbitrary domains.

Let $r \in R \setminus \{0\}$. Then, r is *irreducible* if,

(i) r is not a unit;

(ii) if $r = ab$, then either a or b is a unit.

Let $r \in R \setminus \{0\}$. Then, r is *prime* if,

(i) r is not a unit;

(ii) if $r|ab$, then $r|a$ or $r|b$.

Theorem 8.5. *If R is a domain, then every prime is also irreducible.*

In general, the converse does not hold in an arbitrary integral domain, but it does in a PID.

Theorem 8.6. *If R is a PID, then every irreducible is also prime.*

Together, these theorems show that prime and irreducible elements coincide in PIDs.

An integral domain R is a *factorisation domain* (FD) if each non-unit $x \in R \setminus \{0\}$ admits a factorisation $x = r_1 \cdot r_2 \cdots r_n$, where the r_i are irreducible.

A factorisation domain R is furthermore a *unique factorisation domain* (UFD) if for any two factorisations $\prod_{i=1}^{n} r_i = \prod_{i=1}^{m} s_i = x$ of a non-unit $x \in R \setminus \{0\}$, we have $n = m$, and there exists a permutation $\sigma \in S_n$ such that $r_i \sim s_{\sigma(i)}$ for all i.

Theorem 8.7. *If R is a UFD, then every irreducible is also prime.*

So, prime and irreducible elements also coincide in UFDs.

Lemma 8.8. *A PID is a FD.*

Theorem 8.9. *If R is an FD in which all irreducibles are prime, then R is a UFD. In particular, every PID is a UFD.*

Theorem 8.10. *Any finite collection of elements in a UFD has a* gcd *and an* lcm.

9 Fields

An ideal I of a ring R is *maximal* if $I \neq R$, but if J is any ideal of R such that $I \subseteq J \subseteq R$, then $I = J$, or $J = R$.

Theorem 9.1. *An ideal I in a commutative ring R is maximal if and only if R/I is a field.*

Theorem 9.2. *For $a \neq 0$, the principal ideal (a) in a PID R is maximal if and only if a is irreducible.*

If F is a field, and $f \in F[x]$ has degree $\deg(f) > 0$, then the elements of the quotient ring $F[x]/(f)$ correspond to polynomials in $F[x]$ with degree less than f, where multiplication is done modulo f.

When f is irreducible, the previous two theorems imply that $F[x]/(f)$ is a field. The case $F = \mathbb{Q}$ is particularly important as $\mathbb{Q}[x]/(f)$ is isomorphic to a subfield of $\mathbb{C}$.

An element $\alpha \in \mathbb{C}$ is *algebraic* over $\mathbb{Q}$ if it satisfies a polynomial $f(\alpha) = 0$ for some $f \in \mathbb{Q}[x]$ with $\deg(f) > 0$. An element that is not algebraic is called *transcendental.*

Recall that for any $\alpha \in \mathbb{C}$, the evaluation map $\phi_\alpha : \mathbb{Q}[x] \to \mathbb{C}$, defined by $f \mapsto f(\alpha)$, is a ring homomorphism. Here, there are two cases to consider; whether α is algebraic or not.

If α is transcendental, then there are no polynomials $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$, so $\ker(\phi_\alpha)$ contains only the zero polynomial, and so, by the first isomorphism theorem, we have $\mathrm{im}(\phi_\alpha) \cong \mathbb{Q}[x]$. If α is algebraic, then there exists a non-zero polynomial $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$, so $f \in \ker(\phi_\alpha)$, and since $\ker(\phi_\alpha)$ is an ideal of the PID $F[x]$, $\ker(\phi_\alpha)$ must be a principal ideal, so there is some $m \in F[x]$ such that $\ker(\phi_\alpha) = (m)$.

This polynomial m is not necessarily unique, but any two distinct values must divide each other and thus be associate in $F[x]$. By multiplying by constants, we can assume that m is monic, and this monic polynomial is unique and is called the *minimal polynomial* of α over $\mathbb{Q}$.

Theorem 9.3. *If α is algebraic in $\mathbb{C}$, then there is a unique non-zero irreducible monic polynomial $m \in \mathbb{Q}[x]$ such that $m(\alpha) = 0$.*

By the first isomorphism theorem, we then have,

$$\mathrm{im}(\phi_\alpha) \cong \mathbb{Q}[x]/(f)$$

and since f is irreducible, (f) is a maximal ideal, and hence $Q[x]/(f)$ is a field, so $\mathrm{im}(\phi_\alpha)$ is a subfield of $\mathbb{C}$, denoted $\mathbb{Q}(\alpha)$.

Fields of this type are called *number fields.*

10 Polynomial Fields

A field F is *algebraically closed* if for every $f(x) \in F[x]$ with degree $\deg(f) > 0$, there exists $a \in F$ such that $f(a) = 0$.

Example.

- $\mathbb{C}$ is an algebraically closed field.
- The subfield $\mathbb{A} = \{a \in \mathbb{C} : \exists f \in \mathbb{Q}[x], f(a) = 0\} \subset \mathbb{C}$ of $\mathbb{C}$ of *algebraic numbers* is also an algebraically closed field.

Theorem 10.1. *If F is an algebraically closed field, then the irreducibles in $F[x]$ are exactly the polynomials of degree 1, so each irreducible is associate to $(x - a)$ for a unique $a \in F$.*

10.1 Eisenstein's Criterion

It is difficult to check polynomials in $\mathbb{Z}[x]$ for irreducibility, but *Eisenstein's criterion* provides an sufficient (but not necessary) condition for irreducibility that is often simpler to use.

Let R be a UFD. Then, note that if a non-constant polynomial $f \in R[x]$ is irreducible, its coefficients need to be jointly coprime, as, if a is a non-unit in R that divides all the coefficients of f, then a is a non-unit in $R[x]$ that divides f.

A non-zero polynomial $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ is *primitive* if $\gcd_{0 \leq i \leq n}(a_i) = 1$.

So, any non-zero $f \in \mathbb{R}[x]$ can be written as af_0 where $a \in R$ is the gcd of the coefficients of f and f_0 is primitive.

Theorem (Eisenstein's Criterion)**.** *Let R be a UFD, and let $f = a_n x^n + \cdots a_1 x + a_0 \in R[x]$ be a primitive polynomial. If there exists a prime $p \in R$ such that,*

- $p \nmid a_n$;
- $p \mid a_i$ *for* $0 \leq i < n$;
- $p^2 \nmid a_0$,

or,

- $p^2 \nmid a_n$;
- $p \mid a_i$ *for* $0 \leq i < n$;
- $p \nmid a_0$,

then f is irreducible in $R[x]$.

Example. $3x^3 + 10x^2 + 12x + 2$ is irreducible in $\mathbb{Z}[x]$ as gcd(3,10,12,1) = 1, and Eisenstein's criterion applies with $p = 2$.

10.2 Fields of Fractions

Let R be an integral domain, and define the set,

$$\begin{aligned} W &= R \times (R \setminus \{0\}) \\ &= \{(x,y) \in R \times R : y \neq 0\} \end{aligned}$$

We define an equivalence relation on W by $(a,b) \sim (c,d)$ if and only if $a \cdot d = b \cdot c$. Then, the equivalence classes of an element (a,b) is called a *fraction*, and is denoted $\frac{a}{b}$.

Let $Q(R)$ be the set of equivalence classes of W.

Theorem 10.2. *If R is an integral domain, then $Q(R)$ is a field under the operations,*

$$\frac{a}{b}+\frac{c}{d}=\frac{a\cdot d+b\cdot c}{b\cdot d} \qquad \frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d}$$

and the map $\pi : R \to Q(R)$ defined by $r \mapsto \frac{r}{1}$ is an injective ring homomorphism.

The field $Q(R)$ is called the *field of fractions* of an integral domain R.

Example.

- $Q(\mathbb{Z}) = \mathbb{Q}$
- $Q(F[x])$ is the field of *rational functions* p/q, $p,q \in F[x],q \neq 0$, in one variable x, commonly denoted by $F(x)$.

10.3 Gauss' Lemma

Lemma 10.3. *The product of two primitive polynomials is primitive.*

Theorem 10.4. *Let R be a UFD with a field of fractions $Q = Q(R)$. Then, a primitive polynomial in $R[x]$ is irreducible if and only if it is irreducible in $Q[x]$.*

Lemma 10.5 (Gauss)**.** *A primitive irreducible polynomial in $\mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$.*

Corollary 10.5.1. *If R is a UFD, then there are two distinct types of irreducibles in $R[x]$; irreducible elements in R, and primitive elements in $R[x]$ that are irreducible in $Q[x]$.*

Theorem 10.6. *If R is a UFD, then so is $R[x]$.*