Algebra 4: Groups and Rings

by Ivan Noden
based on lectures by Yusra Naqvi

Contents

1 Basics of Groups

1.1 Group Definition

The study of groups comprises the majority of this course. In essence, groups are algebraic structures that encode notions of symmetry and generalise the structure of many algebraic objects we are familiar with including the integers, symmetries of a polygon, permutations of a set and more.

Definition 1.1 (Group)**.** A group is a pair $(G, *)$ consisting of a set G and a binary operation $* : G \times G \to G$ such that:

(i) $*$ is associative.

(ii) There exists some element $e \in G$ such that $g * e = e * g = g$ for all $g \in G$. We call this element the identity of G.

(iii) For all $g \in G$ there exists some $h \in G$ such that $g * h = h * g = e$. We call h the inverse of g and denote it g^{-1}

For notational convenience, we often write gh when we mean $g * h$. Occasionally $g + h$ will be used if it makes more sense in context. We will also tend to just use the set G when we mean $(G, *)$. Throughout these notes, we use e to denote the identity element of a group even when this is not explicitly stated. If we wish to distinguish between the identity of a group G and the identity of a group H, we will denote them by e_G and e_H respectively.

Example 1.2 (Integers, Reals, etc.)**.** The sets $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$ all form groups under the binary operation of addition. Moreover, $\mathbb{R}^\times$ (that is $\mathbb{R} \setminus \{0\}$), is also a group under multiplication. The same can be said for $\mathbb{Q}^\times$ and $\mathbb{C}^\times$ but not $\mathbb{Z}^\times$ as elements other than ± 1 have no multiplicative inverse.

Example 1.3 (Symmetries of a Polygon)**.** Consider a triangle. If we rotate or flip the triangle along the bisector of one of its angles then the triangle looks the same. Since it looks the same, we can rotate or flip again, or undo the rotation or flip we just did. We can also do nothing which keeps everything the same. This all means that the symmetries of a triangle form a group (associativity is obvious). We call this group D_6. More generally, the group D_{2n} is the group of symmetries of an n-sided polygon. We will go into more detail on this group, including giving a more concrete description, later.

Example 1.4 (Bijections and Permutations)**.** Let A be a set. We denote the set of all bijections of A as $\mathrm{Bij}(A)$. Since the composition of two bijections is a bijection; bijections are invertible; the identity map is a bijection; and function composition is associative, the set $\mathrm{Bij}(A)$ forms a group under composition.

In particular, if we consider the set $A = \{1, \dots, n\}$ for some $n \in \mathbb{N}$ then an bijection of A is simply a permutation of the integers from 1 to n. The group of these bijections is denoted S_n.

Definition 1.5 (Abelian Group)**.** We say a group, G, is abelian if its binary operation is commutative. That is if $gh = hg$ for all $g, h \in G$.

We now recall some basic properties of groups. These are provided without proof.

Proposition 1.6. *Let G be a group and $g, h \in G$. Then:*

(i) The identity element of G is unique.

(ii) The inverse of g is unique.

(iii) $(g^{-1})^{-1} = g$

(iv) $(gh)^{-1} = g^{-1}h^{-1}$

1.2 Cayley Tables

Cayley tables allow us to visualise the structure of a given group. We order the elements of a group G and write them across the top and down the side of a table, filling in the entries of the table with the product of the corresponding row and column headers. This is a generalisation of the multiplication grids we learn in school.

One of the main aims of this course is to classify what kinds of groups are possible given how many elements it has. Cayley tables can help answer that question as we can consider all the possible ways of filling out a Cayley table whilst ensuring we satisfy the requirements of being a group. To help us with fulfilling this condition, we use the following lemma:

Lemma 1.7. *Every group element appears exactly once in each row and column of a Cayley table*

Proof. Note that this Lemma is equivalent to saying that, given $g \in G$, for all $h \in G$, there exists $f_1, f_2 \in G$ such that $f_1 g = g f_2 = h$ and f_1, f_2 are unique.

Let $f_1 = hg^{-1}$ and $f_2 = g^{-1}h$, then note $f_1 g = g f_2 = h$ as required.

Now suppose there exists $f_1' \in G$ such that $f_1' g = h$, then $h = f_1' g = f_1 g$ so multiplying by g^{-1} on the right gives $f_1' = f_1$. Thus f_1 is unqiue. A similar argument holds for f_2. □

We can know use this lemma to construct all possible Cayley tables of a few small sizes.

Example 1.8 (One Element)**.** Consider a group $G = \{e\}$. Then clearly the only possible Cayley table is

	e
e	e

We call this group the trivial group and its only element is the identity.

Example 1.9 (Two Elements)**.** Consider a group $G = \{e, x\}$. Note that x must have an inverse and so $xx = e$ is forced. This means there is only one possible Cayley table:

	e	x
e	e	x
x	x	e

Example 1.10 (Three Elements)**.** Consider a group $G = \{e, x, y\}$. Applying Lemma 1.7, we find there can only be one possible Cayley table:

	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Example 1.11 (Four Elements)**.** Consider a group $G = \{e, x, y, z\}$. The possible Cayley tables for this group require more thought but it does not take long to figure out that there are only two possible Cayley tables that fulfill the conditions of Lemma 1.7.

	e	x	y	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

	e	x	y	z
e	e	x	y	z
x	x	z	e	y
y	y	e	z	x
z	z	y	x	e

We can check that these two tables describe two fundamentally different groups by comparing the inverses of elements. For instance, the first table tells us that $x^{-1} = x$ while the second says $x^{-1} = y$.

1.3 Order

The notion of order gives a concept of size to both a group and its elements. Before we define what we mean by order, we need some pre-requisites.

Definition 1.12 (Exponentiation)**.** Let G be a group, $g \in G$ and $n \in \mathbb{N}$.We define:

(i) $g^n = \overbrace{g \dots g}^{n \text{ times}}$.

(ii) $g^0 = e$.

(iii) $g^{-n} = (g^{-1})^n$.

Proposition 1.13 (Properties of Exponents)**.** *Let G be a group, $g \in G$ and $m, n \in \mathbb{Z}$. Then:*

(i) $g^m g^n = g^{mn}$.

(ii) $(g^n)^{-1} = g^{-n} = (g^{-1})^n$.

(iii) $(g^m)^n = g^{mn} = (g^n)^m$

Definition 1.14 (Generation)**.** Let G be a group and $g \in G$. We call the set $\{g^n : n \in \mathbb{Z}\}$ the set generated by g and denote it $\langle g \rangle$. If $\langle g \rangle = G$ then we say G is generated by g. If there is such an element that generates G, we say that G is cyclic.

We are now able to define what we mean by order.

Definition 1.15 (Order)**.** The order of a group G is the size of the set of elements in G, denoted $|G|$. The order of an element $g \in G$ is the size of the set generated by g and is denoted $\mathrm{ord}(g)$. If $\langle g \rangle$ is infinite then we write $\mathrm{ord}(g) = \infty$.

Often, an alternative definition of the order of an element is given and is encapsulated in the next proposition.

Proposition 1.16. *Let $g \in G$ and let k be the smallest positive integer such that $g^k = e$. If such an integer exists,* $\mathrm{ord}(g) = k$. *Otherwise* $\mathrm{ord}(g) = \infty$.

Proof. Recall that the order of g is the size of the set $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. Note that if k is the smallest positive integer such that $g^k = e$ then, for $r \in \{1, \dots, k-1\}$, we have that $g^{k+r} = g^r \neq e$. Also, for any $m \in \mathbb{N}$ with $m > k$ such that $g^m \neq e$, we have that

$g^m = g^{k+r} = g^r$ for some $r \in \{1, \dots, k-1\}$. Therefore there are $k-1$ non-identity elements in $\langle g \rangle$ and hence $\mathrm{ord}(g) = k$.

If no such k exists, clearly $\langle g \rangle$ is infinite as required. □

Proposition 1.17 (Properties of Order)**.** *Let G be a group and $g \in G$. Let $n = \mathrm{ord}(g)$. Then:*

(i) If $|G|$ is finite then so is n.

(ii) Let $k \in \mathbb{Z}$, then $g^k = e$ if and only if $n \mid k$.

(iii) Let $k \in \mathbb{Z}$, then $\mathrm{ord}(g^k) = \frac{n}{\gcd(n,k)}$.

(iv) Let $i, j \in \mathbb{Z}$, then $g^i = g^j$ if and only if $i \equiv j \mod n$

Proof. The proof of *(i)* is trivial.

For *(ii)*, let $k \in \mathbb{Z}$ and first suppose $g^k = e$. Then, by Proposition 1.16, $k > n$ so we can apply the division algorithm. That is, we know there exist unique $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $k = qn + r$. So $g^k = g^{qn+r} = (g^n)^q g^r = g^r = e$ since $g^n = e$. However, from Proposition 1.16, we know n is the smallest positive integer such that $g^n = e$ and thus the fact that $g^r = e$ and $0 \leq r < n$ implies that $r = 0$. Therefore $k = qn$, that is n divides q. The reverse implication is trivial since $g^{an} = (g^n)^a = e^a = e$ for all $a \in \mathbb{Z}$.

For *(iii)*, let $k \in \mathbb{Z}$, $d = \gcd(n, k)$ and $o = \mathrm{ord}(g)$. By Bezout's Lemma, there exist $a, b \in \mathbb{Z}$ such that $an + bk = d$. Also, there exists some $s \in \mathbb{Z}$ such that $k = sd$.

Note that $(g^k)^{n/d} = (g^{sd})^{n/d} = (g^n)^s = e$ so, by *(ii)*, we know o divides $\frac{n}{d}$. Also, $g^{ko} = (g^k)^o = e$ so, again by *(ii)*, we know n divides $ko = sdo$ or, equivalently, $\frac{n}{d}$ divides so. However, since $\gcd(n, k) = d$ we know that $\gcd(n/d, k/d) = \gcd(n/d, s) = 1$ and thus $\frac{n}{d}$ dividing so must mean $\frac{n}{d}$ divides o. If two integers divide each other, they must be equal so $\frac{n}{d} = o$ as required.

The proof of *(iv)* is similar to that of *(ii)*. The full details are left as an exercise to the reader.

□

1.4 Subgroups

Definition 1.18. Let $H \subseteq G$. We say $(H, *)$ is a subgroup of $(G, *)$, written $H \leq G$, if $(H, *)$ is a group. We call a subgroup H proper if $H \neq G$ and $H \neq \{e\}$

To check if a subset H of G is a subgroup, we need only check that H is non-empty, closed under addition and closed under inverses. This is because associativity naturally follows from G being a group and the existence of the identity follows from the product of an element and its inverse still being in H. All of this can be streamlined into what is called the 'one-step check.'

Proposition 1.19 (One-Step Check)**.** *Let G be a group and H a non-empty subset of G. Then H is a subgroup of G if, for all $g, h \in H$ we have that $gh^{-1} \in H$.*

We now consider some examples of subgroups.

Example 1.20 (Subgroups of Integers)**.** Consider the group of $\mathbb{Z}$ under addition. Then the set of all even integers E forms a subgroup of $\mathbb{Z}$. However, the set of all odd integers O does not, this is because O is not closed under addition as two odd integers add to an even integer. Also O does not contain the identity element 0.

Example 1.21 (Union and Intersection)**.** If we let G be a group and H and K be subgroups of G then $H \cap K$ is also a subgroup of G.

To see this, first note that H and K both contain the identity element and hence so does $H \cap K$. Now, consider $x, y \in H \cap K$. Since H and K are closed under products and inverses, the fact that $x, y \in H$ implies $xy^{-1} \in H$ and similarly we know $xy^{-1} \in K$. Therefore, $xy^{-1} \in H \cap K$ so, by Proposition 1.19, $H \cap K$ must be a subgroup.

Compare this to the set $H \cup K$. If this were a subgroup then for all $h \in H$ and $k \in K$ we have that $hk \in H \cup K$. Thus hk is in at least one of H or K. Without loss of generality, assume it is in H. Note that h^{-1} is also in H so $h^{-1}hk = k \in H$. This therefore means that $K \subseteq H$. If we assumed $hk \in K$ then instead we'd find $H \subseteq K$. Since the reverse implications is clearly also true, this means that $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.

Recall from Definition 1.14 that a group G is cyclic if there exists an element $g \in G$ such that $\langle g \rangle = G$. Cyclic groups will come up often in this course, particularly as we can have a cyclic group of any order we like. They also have a number of nice properties, including one concerning their subgroups.

Proposition 1.22 (Subgroups of Cyclic Groups)**.** *Let G be a cyclic group and H a subgroup of G. Then H is cyclic.*

Proof. Let $g \in G$ be such that $G = \langle g \rangle$, then any element of G, and hence any element of H, can be written as a power of g. So if we let $h \in H$ then there exists $k \in \mathbb{Z}$ such that $g^k = h$. Let n be the smallest positive integer such that $g^n \in H$. By the division algorithm, we know there exist unique $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $k = qn + r$. See that $g^k(g^n)^{-q} = g^{k-qn} = g^r \in H$. However, n is the smallest positive integer such that $g^n \in H$ and $0 \leq r < n$ so it must be that $r = 0$. As a result, $h = g^k = (g^n)^q$, that is an arbitrary element of H can be written as a power of g^n. Since all powers of g^n must be in H, this shows that $H = \langle g^n \rangle$ and hence H is cyclic. □

1.5 Group Homomorphisms

In general, a homomorphism is a map that preserves a certain algebraic structure so, as you may guess, a group homomorphism preserves the structure of a group.

Definition 1.23 (Group Homomorphism)**.** Let $(G, *)$ and $(H, \star)$ be groups. A group homomorphism is a map $\varphi : G \to H$ such that, for all $a, b \in G$, we have that $\varphi(a*b) = \varphi(a)\star\varphi(b)$.

Proposition 1.24 (Properites of Homomorphisms)**.** *Let G and H be groups and $\varphi : G \to H$ be a homomorphism. Let $g \in G$. Then the following hold:*

(i) $\varphi(e_G) = e_H$.

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(iii) $\varphi(g^k) = \varphi(g)^k$ *for all* $k \in \mathbb{Z}$.

(iv) If $\operatorname{ord}(g) = n$ *then* $\operatorname{ord}(\varphi(g))$ *divides* n.

Proof. For *(i)*, note that $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$. Multiplying on either side by $\varphi(e_G)^{-1}$ shows us that $\varphi(e_G) = e_H$.

For *(ii)*, note that $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_G) = e_H$ and hence $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Statement *(iii)* simply follows from inductively applying the definition of a homomorphism along with statements *(i)* and *(ii)* for non-positive powers.

For *(iv)*, let $n = \operatorname{ord}(g)$. Then $\varphi(g)^n = \varphi(g^n) = \varphi(e_G) = e_H$ so $\operatorname{ord}(\varphi(g))$ divides n by Proposition 1.17. □

As we tend to do with maps, we often consider the kernel (the set of elements which map to the identity) and the image of a homomorphism. In particular, we often utilise the more general facts that, for a homomorphism $\varphi : G \to H$ where G and H are groups, φ is injective if and only if $\ker\varphi = \{e_G\}$ and φ is surjective if and only if $\operatorname{im}\varphi = H$. Also worthy of note is the fact that the above proposition tells us that $\ker\varphi$ is a subgroup of G and $\operatorname{im}\varphi$ is a subgroup of H. For now, a thorough proof of these claims is left as an exercise for the reader but the former claim will be revisited further down the line with added importance.

Definition 1.25 (Group Isomorphism)**.** Let G and H be groups and $\varphi : G \to H$ a homomorphism. We say φ is an isomorphism if it is bijective. If such a map exists, we say G and H are isomoprhic and write $G \cong H$. Note that the inverse of φ is also an isomoprhism and so it is also true that $H \cong G$.

If two groups are isomorphic they have the same structure and can almost be considered the same group but with relabelled elements and hence properties such as being abelian and the number of elements of each order are the same across isomoprhic groups. This notion adds more rigour to what we were aiming to do in Section 1.2 on Cayley tables where we tried to determine how many tables of a given size were possible. With our newly defined language, we can reformulate our aim as classifying groups of a given order upto isomorphism. In that section we already showed there was only one group of each order less than 4 and two groups of order 4 upto isomorphism. Much of the rest of our discussion on groups will have the aim of classifying groups of higher orders.

We can begin doing so by recalling a throwaway comment made earlier, that we can find a cyclic group of any given order. In fact, all cyclic groups of the same order are isomorphic. The intuitive justification of this is that elements in a cyclic group can be written as powers of a single generating element. By relabeling this element, we can get any other cyclic group we desire. More precisely, if G and H are cylic groups of the same order generated by g and h respectively then the map $\varphi : G \to H$ defined such that $\varphi(g^n) = h^n$ for all $n \in \mathbb{Z}$ is an isomorphism. Due to this fact, we often talk of *the* cyclic group of order n for some $n \in \mathbb{N}$. This group is denoted C_n and there is an even easier way of checking when a group is isomorphic to this one.

Proposition 1.26. *Let* G *be a group and let* $n = |G|$. *If there exists an element* $g \in G$ *such that* $\operatorname{ord}(g) = n$ *then* $G \cong C_n$.

Proof. Let $g \in G$ be such that $\operatorname{ord}(g) = n$. Then $\langle g \rangle$ has n distinct elements. Clearly, $\langle g \rangle$ is a subgroup of G. However $|\langle g \rangle| = |G| = n$ so it must be that $G = \langle g \rangle$. We know $\langle g \rangle$ is cyclic and hence G must be too. Therefore $G \cong C_n$. □

We saw in Example 1.4 that bijections on a set form a group under composition. For similar reasons, the set isomorphisms between a group and itself also forms a group under composition.

Definition 1.27 (Automorphism)**.** Let G be a group. An automorphism of G is an isomorphism from G to G. The set of all automorphisms of G is denoted $\mathrm{Aut}(G)$ and it forms a group under composition.

Another reason we take keen interest in cyclic groups is because their automorphisms are relatively simple.

Proposition 1.28. *Let C_n be a cyclic group of order n and $r \in \mathbb{N}$. The map $\phi_r : C_n \to C_n$ defined by $\phi_r(x) = x^r$ is a homomorphism and is an automorphism if and only if* $\gcd(n, r) = 1$.

Proof. Let $x \in C_n$ be the generator of C_n. We can therefore write any element of C_n as a power of x. To check this map is a homomorphism, we simply calculate $\phi_r(x^j x^i) = \phi_r(x^{i+j}) = \phi_r(x)^{i+j} = x^{r(i+j)} = x^{ri}x^{rj} = \phi_r(x^i)\phi_r(x^j)$ for all $i, j \in \mathbb{Z}$. Thus ϕ_r is a homomorphism

For this map to be an isomorphism, $\phi_r(x)$ should generate the image of ϕ_r. By Proposition 1.26, it is enough for $\phi_r(x) = x^r$ to have order n. From Proposition 1.17, we know the order of x^r is given by $\frac{n}{\gcd(n,r)}$ which equals n if and only if $\gcd(n, r) = 1$. □

Automorphisms of cyclic groups will come up quite regularly and, in this context, we will continue to use ϕ_r to refer to the map constructed above without restating its definition.

Now that we understand what automorphisms of cyclic groups look like, we can understand what the group of automorphisms itself looks like. To do so, we call upon a common group used in number theory: $\mathbb{Z}_n^\times$. This is the group of residue classes modulo n which have multiplicative inverses, that is residue classes $\overline{a}$ such that there exists another residue class $\overline{b}$ where $\overline{ab} = \overline{1}$. Residue classes have this property if and only if the integers representing it are coprime to n so there is a clear relationship between this group and $\mathrm{Aut}(C_n)$.

Proposition 1.29. *Let C_n be a cyclic group of order n. Then* $\mathrm{Aut}(C_n) \cong \mathbb{Z}_n^\times$. *In particular, if $p \in \mathbb{N}$ is prime then $C_p \cong C_{p-1}$.*

Proof. We define the map $\psi : \mathrm{Aut}(C_n) \to \mathbb{Z}_n^\times$ by $\psi(\phi_r) = \overline{r}$. To show this is a homomorphism, consider $\phi_r, \phi_s \in \mathrm{Aut}(C_n)$and note $(\phi_r \circ \phi_s)(x) = \phi_r(x^s) = x^{rs} = \phi_{rs}(x)$ so $\psi(\phi_r \circ \phi_s) = \overline{rs} = \psi(\phi_r)\psi(\phi_s)$. Thus ψ is a homomorphism.

To show ψ is a bijection, first consider $\ker \psi$ and suppose $\phi_r \in \mathrm{Aut}(C_n)$ is such that $\psi(\phi_r) = \overline{1}$ (that is suppose $\phi_r \in \ker \psi$). This is only possible if $r \equiv 1 \mod n$ so, by Proposition 1.17, this means $\phi_r(x) = x^r = x$ for all $x \in C_n$ and so ϕ_r is the identity map. Thus the kernel of ψ is trivial and hence ψ is injective. Surjectivity follows from the fact that $\phi_r \in \mathrm{Aut}(C_n)$ if and only if r is coprime to n and $\overline{r} \in \mathbb{Z}_n^\times$ if and only if r is coprime to n. Hence ψ is also surjective and so is an isomorphism. Therefore $\mathrm{Aut}(C_n) \cong \mathbb{Z}_n^\times$.

Now let $p \in \mathbb{N}$ be prime. By the above, $C_p \cong \mathbb{Z}_p^\times$. Since every integer which is not a multiple of p is coprime to p, there are $p-1$ residue classes modulo p and hence $|\mathbb{Z}_p^\times| = p-1$. Moreover, from number theory, we know there exist primitive roots modulo p, these primitive roots are each generators of $\mathbb{Z}_p^\times$. Thus $\mathbb{Z}_p^\times \cong C_{p-1}$.

□

1.6 Group Presentations

During this course, we want to try and classify all the groups of given orders however we have already seen that isomorphic groups can be written and interprted in many different ways. In order to write down our classifications, we want a way of describing these groups in the most abstract terms possible. To do so, we use group presentations.

Definition 1.30 (Group Presentation)**.** A group presentation consists of a set of generators S and of relations between these generators R. It defines a group G to be the largest group such that every element of G can be written as a product of elements of S and their inverses subject to the relations R. We write $G = \langle S \mid R \rangle$.

Typically, relations are products of elements of S that are equivalent to the identity element however they can be rewritten to make them easier to understand.

Example 1.31 (Cyclic Group Presentation)**.** We know the group C_n is generated from one element, call it x. The only relation in this group is the fact that $x^n = e$. We can therefore write $C_n = \langle x \mid x^n = e \rangle$

Example 1.32 (Dihedral Group Presentation)**.** Recall that in Example 1.3 we gave an informal description of the group of symmetries of an equilateral triangle. In more abstract terms, this group is isomorphic to the dihedral group of order 6 which we write as $D_6 = \langle f, r \mid f^2 = r^3 = e,\, r^{-1}f = fr \rangle$. To see how this is related to symmetries of a triangle, consider the isomorphism which sends the rotation of angle $\frac{\pi}{3}$ about the centre to r and sends the reflection through the bisector of the top corner to f.

More generally, the symmetry group of the regular n-sided polygon is isomorphic to the group $D_{2n} = \langle f, r \mid f^2 = r^n = e,\, r^{-1}f = fr \rangle$.

2 Lagrange's Theorem

Before we can begin classifying groups, we need to understand more about their properties. If we are able to find further restrictions placed on what can and can't be a group we should be able to better determine what different groups of a given order can look like. One important example of this kind of property is Lagrange's Theorem. Before we get to this though, we must first develop some knowledge of cosets.

2.1 Cosets

Definition 2.1 (Coset)**.** Let G be a group and $H \subseteq G$ a subgroup. For all elements $g \in G$ we define the left coset of H by g to be the set $gH = \{gh : h \in H\}$ and the right coset of H by g is the set $Hg = \{hg : h \in H\}$.

In general, we will consider left cosets more often simply as a convention. Most of the results we prove with left cosets can easily be transferred to a result about right cosets. The proposition below is an example of this.

Proposition 2.2 (Size of Cosets)**.** *Let G be a group and $H \subseteq G$ a subgroup. Then, for all $g \in G$, we have $|gH| = |H|$.*

Proof. Let $g \in G$. Define the map $\lambda : H \to gH$ such that $\lambda(h) = gh$, we will show that λ is a bijection. By the definition of gH, λ is surjective. Now, suppose $\lambda(a) = \lambda(b)$ for some $a, b \in H$. Then $ga = gb$ which implies $a = b$ so λ is injective. Therefore λ is bijective and hence $|H| = |gH|$. □

Definition 2.3 (Set of Cosets)**.** Let G be a group and $H \subseteq G$ a subgroup. The set of all left cosets of H is denote $G/H = \{gH : g \in G\}$. Similarly, the set of all right cosets is denoted $H\backslash G$.

Since the notation for sets of cosets ($H\backslash G$ and H/G) can easily be confused with that used for set difference ($G \setminus H$), from now on we will denote the set difference as $G - H$.

Definition 2.4 (Index)**.** Let G be a group and $H \subseteq G$ a subgroup. The number of left cosets of H in G is called the index of H in G. We denote it $[G\colon H]$. Note that $[G\colon H] = |G/H|$.

2.2 Lagrange's Theorem

The reason we are concerned with cosets is they allow us to form an equivalence relation on the set of elements in a group. Before we get to that, we briefly recall what an equivalence relation is.

A relation $\sim$ is used to denote when a property between two elements, x and y, of a set, S, holds. When this is the case, we write $x \sim y$. We say a relation is an equivalence relation if it is reflexive ($x \sim x$ for all $x \in S$), symmetric ($x \sim y$ implies $y \sim x$), and transitive ($x \sim y$ and $y \sim z$ implies $x \sim z$). If the relation is an equivalence relation, we can then create subsets of S containing elements which are related to each other, these susbets are called equivalence classes and have the important property that each element of S belongs to exactly one equivalence class. This allows us to break up S into the union of disjoint equivalence classes.

Lagrange's Theorem applies this notion to groups and we do so using cosets.

Proposition 2.5. *Let G be a group and $H \subseteq G$ a subgroup. Define a relation $\sim$ on G where, for $x, y \in G$, we have $x \sim y$ if and only if $x^{-1}y \in H$. Then $\sim$ is an equivalence relation and the corresponding equivalence classes are left cosets.*

Proof. In order to show this relation is an equivalence relation, we must show it is reflexive, symmetric and transitive. Let $x, y, z \in G$. For reflexivity, note $xx^{-1} = e \in H$ so $x \sim x$. For symmetry, suppose $x \sim y$. Then $x^{-1}y \in H$ and so is its inverse, $(x^{-1}y)^{-1} = y^{-1}x \in H$ so $y \sim x$. Finally, for transitivity, suppose $x \sim y$ and $y \sim z$. Then $x^{-1}y, y^{-1}z \in H$ and hence so is their product, $x^{-1}yy^{-1}z = x^{-1}z \in H$. Thus $x \sim z$. Therefore $\sim$ is an equivalence relation.

Now, for $g \in G$, let $[g]$ denote the equivalence class given by this relation. Let $x \in [g]$ then $x^{-1}g = h$ for some $h \in H$. Thus $e = g^{-1}xh$ and so $x = gh^{-1}$. Thus $x \in gH$ and so $[g] \subseteq gH$. To show the reverse inclusion, let $x \in gH$, then $x = gh$ for some $h \in H$. Thus $x^{-1}g = h^{-1} \in H$ so $x \sim g$. Thus $x \in [g]$ and so $gH \subseteq [g]$. Therefore $gH = [g]$. □

Now that we have developed our knowledge of cosets, the proof of Lagrange's Theorem is fairly straighforward.

Theorem 2.6 (Lagrange's Theorem)**.** *Let G be a finite group and $H \subseteq G$ a subgroup. Then $|H|$ divides $|G|$.*

Proof. We define the relation $\sim$ on G such that $x \sim y$ if and only if $x^{-1}y \in H$. By Proposition 2.5, this is an equivalence relation. Thus G can be written as the disjoint union of equivalence classes. Let $a_i \in G$ for $i \in \{1, \dots, r\}$ be representatives of these equivalence classes where $r \in \mathbb{N}$ is such that all equivalence classes are represented by some a_i and that none are related pairwise. Note that such an r exists since G is finite.

We can then write $G = \bigcup_{i=1}^{r}[a_i]$ where $[a_i]$ is the equivalence class a_i belongs to. We also know from Proposition 2.5 that $[a_i] = a_iH$ so $G = \bigcup_{i=1}^{r} a_iH$. Since these equivalence classes are disjoint, $|G| = \sum_{i=1}^{r} |a_iH| = r|H|$ (the last equality follows from Proposition 2.2).

This proves that $|H|$ divides $|G|$ and, moreover, $|G| = r|H|$ where r is the number of left cosets of H, that is the index of H in G. □

2.3 Consequences of Lagrange's Theorem

Lagrange's Theorem is often most useful when applied to elements of groups. We can do this since, for all elements g in a group G, the set $\langle g \rangle$ is a subgroup of G. Noticing this, the following corollary becomes trivial.

Corollary 2.6.1 (Lagrange's Theorem for Elements)**.** *Let G be a finite group and $g \in G$. Then* $\text{ord}(g)$ *divides $|G|$.*

Using this fact, we are able to make our first major progression into classifying groups.

Theorem 2.7 (Groups of Prime Order)**.** *Let $p \in \mathbb{N}$ be prime and G be a group of order p. Then $G \cong C_p$.*

Proof. Let $g \in G$. Then, by Corollary 2.6.1, $\text{ord}(g)$ divides p. Since p is prime, $\text{ord}(g) \in \{1, p\}$. However, only the identity element of G has order 1 and so, since $|G| > 1$, there must be an element of G with order p.

Therefore, by Proposition 1.26, we have that $G \cong C_p$. □

Lagrange's Theorem can also tell us about the subgroups of groups of prime order.

Proposition 2.8. *Let G be a group of prime order. Then G has no non-trivial proper subgroups.*

Proof. Any subgroup of G must have an order dividing $|G|$ which is prime, meaning the order of the subgroup is either 1 or $|G|$. Therefore the subgroup is either trivial or G itself. □

We can also provide a partial converse of Lagrange's Theorem when it comes to cyclic groups.

Proposition 2.9. *Let G be a cyclic group of order n. Then, for all $d \in \mathbb{N}$ that divide n, there exists a subgroup of G of order d.*

Proof. Let g be a generator for G. Since d divides n, there exists $k \in \mathbb{N}$ such that $n = dk$ and thus $(g^k)^d = e$. We claim d is in fact the order of g^k.

To see this, assume the opposite and suppose there exists $r \in \mathbb{N}$ with $r < d$ such that $(g^k)^r = e$. This would imply n divides rk but $n = dk$ so $rk < n$, a contradiction. Thus d is the smallest positive integer such that $(g^k)^d = e$ and hence $\operatorname{ord}(g^k) = d$.

Therefore the subgroup $\langle g^k \rangle$ of G is a subgroup of order d. □

3 Quotient Groups and Normal Subgroups

We now move on to considering when the set of cosets of a subgroup is itself a group. The reason for this is the coset an element is in can indicate to us some of the properties of that element and if these properties are all we care about then it would be much simpler to consider a group made up of cosets instead of the group as a whole. For example, cosets of the subgroup $n\mathbb{Z}$ in $\mathbb{Z}$ (the subgroup of multiples of n) categorise integers by how 'close' they are to being a multiple of n. Doing this would require some valid way of defining the product of cosets (e.g. something like $aH * bH = (ab)H$) regardless of which representative of the coset was chosen. For this, we turn to the idea of a congruence relation.

3.1 Congruence Relations

Definition 3.1. A congruence relation on a group G is an equivalence relation $\sim$ on G such that, for all $a_1, a_2, b_1, b_2 \in G$, we have that $a_1 \sim a_2$ and $b_1 \sim b_2$ implies $a_1 b_1 \sim a_2 b_2$.

Since being in the same coset of a subgroup defines an equivalence relation, we can see that, if we are able to choose subgroups where this equivalence relation is in fact a congruence relation, we should be able to define a product of cosets without worrying about which representatives are chosen.

To motivate which kinds of subgroups we may want to consider, we first show the following proposition.

Proposition 3.2. *Let $\sim$ be a congruence relation on a group G. Then the set $H = \{g \in G : g \sim e\}$ is a subgroup of G satsifying $gHg^{-1} = \{ghg^{-1} : h \in H\} \subseteq H$ for all $g \in G$.*

Proof. Note that $e \sim e$ so $e \in H$, thus H is non-empty. Now let $a, b \in H$. Then $a \sim e$ and $a^{-1} \sim a^{-1}$ so $a^{-1}a = e \sim a^{-1}e = a^{-1}$. Thus $a^{-1} \in H$. Also, $a \sim e$ and $b \sim e$ so $ab \sim ee = e$ and thus $ab \in H$. Therefore H is a subgroup.

Now let $g \in G$. Then for all $h \in H$, we have $h \sim e$ so $ghg^{-1} \sim geg^{-1} = e$ and thus $ghg^{-1} \in H$. Therefore $gHg^{-1} \subseteq H$. □

3.2 Normal Subgroups

Definition 3.3. Let G be a group and $H \subseteq G$ a subgroup. We say H is normal in G if H is closed under conjugation, that is, for all $g \in G$, we have $gHg^{-1} \subseteq H$. Sometimes this is denoted by $H \triangleleft G$.

As hinted at in the previous proposition, we will soon see that normal subgroups are the kind of subgroups we need in order to have a well-defined product on its cosets. Before showing this, let us first try and understand normal subgroups themselves further.

Example 3.4 (Orientation-Preserving Symmetries)**.** Consider the group $D_6 = \langle r, f \mid f^2 = r^3 = e,\, r^{-1}f = fr\rangle$ and the subgroup $\langle r\rangle$. You can quite easily verify algebraically that this subgroup is normal but there is a more intuitive reasoning. If you imagine D_6 as the group of symmetries of an equilateral triangle with r representing a rotation and f a reflection, it seems clear that a conjugation of any rotation is still a rotation.

More generally we can consider the group of symmetries of any regular polygon or polyhedron. We can split elements of these groups into two categories, those that reverse orientation (informally those that involve some kind of reflection) and those that preserve it. The subgroup of orientation-preserving symmetries is normal since conjuagting one of these symmetries either continues to preserve the orientation or reverses it, preserves it, then reverse it again, ultimately preserving the orientation.

Example 3.5 (Centre of a Group)**.** Let G be a group. The centre of G is the set $Z(G) = \{x \in G :\ xg = gx, \text{ for all}\, g \in G\}$, that is the set of elements that commute. The centre of G forms a normal subgroup.

To see this, first note that clearly $e \in Z(G)$. Now let $x, y \in Z(G)$ and $g \in G$. Then $gxy = xgy = xyg$ so $xy \in Z(G)$. Moreover, $gx^{-1} = (x^{-1}x)gx^{-1} = x^{-1}gxx^{-1} = x^{-1}g$ so $x^{-1} \in G$ and thus $Z(G)$ is a subgroup. To see that it is normal, simply note that $gxg^{-1} = gg^{-1}x = x$ so $gxg^{-1} \in Z(G)$.

To more easily check if a subgroup is normal, there are a few equivalent characterisations we can check for.

Proposition 3.6. *Let G be a group and $H \subseteq G$ be a subgroup. Then the following are equivalent:*

(i) H is normal in G

(ii) $gHg^{-1} = H$ for all $g \in G$

(iii) $gH = Hg$ for all $g \in G$

Proof. We first show that *(i)* implies *(ii)*.

We know $gHg^{-1} \subseteq H$ for all $g \in G$. So we need to show $H \subseteq gHg^{-1}$. Let $h \in H$ and note $h = g(g^{-1}hg)g^{-1}$ and $g^{-1}hg \in H$. Thus $h \in gHg^{-1}$, meaning $H \subseteq gHg^{-1}$ and thus $gHg^{-1} = H$.

Next we show that *(ii)* implies *(iii)*.

Let $g \in G$ and $x \in gH$. Then there exists $h \in H$ such that $x = gh$. Since $gHg^{-1} = H$ then $ghg^{-1} \in H$. Let $h' = ghg^{-1}$ so then $x = gh = h'g \in Hg$ and thus $gH \subseteq Hg$. Similarly, $Hg \subseteq gH$. Therefore $gH = Hg$.

Finally we show that *(iii)* implies *(i)*.

Let $g \in G$ and $h \in H$. We know $gh \in gH = Hg$ and thus there exists $h' \in H$ such that $gh = h'g$. Therefore $ghg^{-1} = h' \in H$. We then deduce that $gHg^{-1} \subseteq H$ so, by definition, H is normal in G. □

Even with these differing characterisations, it can still be difficult to identify when a group is normal. Therefore we provide some more techniques for spotting them.

Proposition 3.7. *Let G be a group and $H \subseteq G$ a subgroup such that $[G\colon H] = 2$. Then H is normal in G.*

Proof. Let $g \in G$ and $g \notin H$. Then $gH \neq H$ so these are two distinct cosets. Since the index of H in G is 2, we know $G = H \cup gH$ where this union is disjoint and thus $gH = G - H$. Similarly, $Hg \neq H$ so $Hg = G - H = gH$. Therefore H is normal in G. □

Proposition 3.8. *Let G be an abelian group. Then all subgroups of G are normal.*

Proof. Let $H \subseteq G$ be a subgroup. For all $g \in G$ and for all $h \in H$, we have that $ghg^{-1} = gg^{-1}h = h$ and hence $gHg^{-1} \subseteq H$. Therefore H is normal □

The next technique is provided without proof.

Proposition 3.9. *Let G be a group and $p \in \mathbb{N}$ be the smallest prime dividing the order of G. Then if $H \subseteq G$ is a subgroup such that $[G\colon H] = p$ then H is normal.*

3.3 Quotient Groups

We will now use our knowledge of normal subgroups to define a congruence relation that will allow us to, in turn, define a product between cosets.

Proposition 3.10. *Let G be a group and $H \subset G$ a normal subgroup. Define the relation $\sim$ where, for $x, y \in G$, we say $x \sim y$ if and only if $x^{-1}y \in H$ or, equivalently, if $xH = yH$. Then $\sim$ is a congruence relation.*

Proof. Let $a_1, a_2, b_1, b_2 \in G$ be such that $a_1 \sim a_2$ and $b_1 \sim b_2$, so $a_1^{-1}a_2 \in H$ and $b_1^{-1}b_2 \in H$. Since $g^{-1}Hg = H$ for all $g \in G$ then $b_1^{-1}a_1^{-1}a_2b_1 \in H$. We can then see that $(b_1^{-1}a_1^{-1}a_2b_1)(b_1^{-1}b_2) \in H$ and thus $b_1^{-1}a_1^{-1}a_2b_2 = (a_1b_1)^{-1}a_2b_2 \in H$. Therefore $a_1b_1 \sim a_2b_2$ and $\sim$ is a congruence relation. □

Now, if we consider a group G and a normal subgroup H in G, the above proposition tells us that if we have $x, y, z \in G$ such that x and y are in the same coset then xz and yz are in the same coset. This means that $(xH)(zH) = xzH$ is a valid operation to define as taking a product with the same coset will give the same result no matter which representative is chosen. With this established, we can formally define the notion of a quotient group.

Definition 3.11 (Quotient Group)**.** Let G be a group and $H \subseteq G$ a normal subgroup. Define the operation $* : G/H \times G/H \to G/H$ by $aH * bH = abH$. Then $(G/H, *)$ is a group. We call this group the quotient group of G by H.

It may be worth checking that the above does indeed define a group but it follows rather immediately from what we have established previously.

We can now establish one very important way of thinking of normal subgroups, that is as the kernel of a homomorphism. If we let G be a group and H be a normal subgroup of G then we can define the homomorphism $\varphi : G \to G/H$ by $\varphi(g) = gH$ which clearly has H

as its kernel. Thus, normal subgroups are kernels. The proposition below shows that the reverse implication is also true.

Proposition 3.12. *Let G, H be groups and $\varphi : G \to H$ a homomorphism. Then* $\ker\varphi$ *is a normal subgroup of G.*

Proof. Denote $K = \ker\varphi$. We will first show that K is a subgroup.

Let $h, k \in K$. Then $\varphi(hk) = \varphi(h)\varphi(k) = ee = e$ so $hk \in K$. Also, $\varphi(k^{-1}) = \varphi(k)^{-1} = e$ so $k^{-1} \in K$. Hence K is a subgroup of G.

Now let $g \in G$. Then $\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e$ so $gkg^{-1} \in K$. Thus, $gKg^{-1} \subseteq K$ and therefore K is normal in G. □

Using this notion, we can prove the 1st Isomorphism Theorem.

Theorem 3.13 (1st Isomorphism Theorem)**.** *Let G, H be groups and $\varphi : G \to H$ a homomorphism. Then the map $\psi : G/\ker\varphi \to \operatorname{im}\varphi$ given by $\psi(g\ker\varphi) = \varphi(g)$ is an isomorphism and hence $G/\ker\varphi \cong \operatorname{im}\varphi$.*

Proof. For convenience, denote $K = \ker\varphi$.

We first want to show that ψ is a homomorphism. Let $aK, bK \in G/K$. Then $\psi((aK)(bK)) = \psi(abK) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aK)\psi(bK)$. So ψ is a homomorphism.

To show ψ is also bijective, we first show it is injective. To do this, note that if $aK \in \ker\psi$ then $\phi(a) = e$ so $a \in K$ and thus $aK = K$ which is the identity element in G/K. Thus the kernel of ψ is trivial and hence it is injective. Surjectivity follows from the fact that, if $b \in \operatorname{im}\varphi$ then there exists $a \in G$ such that $\varphi(a) = b$ and hence $\psi(aK) = b$. Thus ψ is bijective and hence is an isomorphism.

Therefore $G/\ker\varphi \cong \operatorname{im}\varphi$. □

3.4 Simple Groups

To finish off this section we will briefly take a look at the notion of a simple group.

Definition 3.14 (Simple Group)**.** A group is simple if it has no normal, non-trivial, proper subgroups.

As we have seen, normal subgroups allow us to break a group down into a smaller quotient group so, in some sense, simple groups are groups that can't be broken down any further.

All finite simple groups are known and have been classified although the proof is tens of thousands of pages long and so will not be covered here. However, we have the tools to classify at least one type of simple group: cyclic groups of prime order. To see this, recall that Lagrange's Theorem tells us all subgroups have order dividing the order of the group they are in so groups of prime order can only have two subgroups, that is the trivial group and themselves. Hence they contain no normal, non-trivial, proper subgroups and so are simple.

The other finite simple groups fall into similar categories like this except for the 26 so called sporadic groups which seemingly have no rhyme or reason behind them. The largest of these is the Monster group which has order of magnitude 10^{53}.

4 Direct and Semidirect Products

With quotient groups, we have seen ways in which we can break groups down into smaller ones. We will now look at different ways of combining groups.

4.1 Direct Products

Definition 4.1 (Direct Product)**.** Let $(G, *_G)$ and $(H, *_H)$ be groups. The direct product of these groups is the group on $G \times H$ with the binary operation $(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$ for $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

Direct products are perhaps the simplest ways to build new groups from ones we had before. We have, in fact, come across a direct product previously. If you recall, when looking at Cayley tables we identified two different groups of order 4 (see Example 1.11). We now know one of these had to be C_4, since we can have cyclic groups of any and every order, but the other is in fact the group $C_2 \times C_2$ (Exercise: check this).

We will now briefly look at some properties of direct products.

Proposition 4.2 (Orders in Direct Products)**.** *Let G and H be groups. Let $g \in G$ and $h \in H$. Then the order of (g, h) in $G \times H$ is $\operatorname{lcm}(\operatorname{ord}(g), \operatorname{ord}(h))$.*

Proof. Let $k \in \mathbb{Z}$. Note that $(g, h)^k = (e, h')$ for some $h' \in H$ if and only if $\operatorname{ord}(g)$ divides k. Similarly, $(g, h)^k = (g', e)$ for some $g' \in G$ if and only if $\operatorname{ord}(h)$ divides k. So, $(g, h)^k = (e, e)$ if and only if k is a multiple of both $\operatorname{ord}(g)$ and $\operatorname{ord}(h)$. Since the order of (g, h) is the smallest positive such integer then $\operatorname{ord}(g, h) = \operatorname{lcm}(\operatorname{ord}(g), \operatorname{ord}(h))$. □

Proposition 4.3. *Let $m, n \in \mathbb{N}$. Then $C_m \times C_n \cong C_{mn}$ if and only if $\gcd(m, n) = 1$.*

Proof. Let $a \in C_m$ and $b \in C_n$ be generators of their respective groups. Then $\operatorname{ord}(a, b) = \operatorname{lcm}(m, n)$ by Proposition 4.2. Note that $\operatorname{lcm}(m, n) = mn$ if and only if $\gcd(m, n) = 1$ so (a, b) has order mn if and only if $\gcd(m, n) = 1$. Thus, by Proposition 1.26, $C_m \times C_n$ is cyclic of order mn if and only if $\gcd(m, n) = 1$. □

Not only are direct products good for constructing groups but we can also use them to help classify groups of a given order. In order to do so, we need a method of recognising when a group is a direct product but, for that, we need the following lemma.

Lemma 4.4. *Let G be a group and $H, K \subseteq G$ normal subgroups such that $H \cap K = \{e\}$. Then, for all $h \in H$ and $k \in K$, we have that $kh = hk$.*

Proof. Let $h \in H$ and $k \in K$. Then $kh^{-1}k^{-1} \in H$ since H is normal and hence closed under conjugation. Thus $hkh^{-1}k^{-1} \in H$. Similarly, $hkh^{-1} \in K$ so $hkh^{-1}k^{-1} \in K$. Note then that $hkh^{-1}k^{-1} \in H \cap K = \{e\}$ and therefore $hk = kh$. □

Theorem 4.5 (Direct Product Recognition)**.** *Let G be a group and $H, K \subseteq G$ subgroups such that H and K are normal in G; $H \cap K = \{e\}$; and $G = HK$ (that is every element in G can be written as a product of an element in H and an element in K). Then $G \cong H \times K$.*

Proof. Define the map $\varphi : H \times K \to G$ by $\varphi(h,k) = hk$. Since $G = HK$, this is clearly surjective. Also, note that if $(h,k) \in \ker\varphi$ then $hk = e$ which implies $h = k^{-1} \in K$ but, since $H \cap K = \{e\}$, this means $(h,k) = (e,e)$ so φ is injective. Thus φ is a bijection.

Now we will show φ is a homomorphism. We can do so simply by calculating

$$\begin{aligned}\varphi(h_1,k_1)\varphi(h_2,k_2) &= h_1k_1h_2k_2 \\ &= h_1h_2k_1k_2 \\ &= \varphi(h_1h_2, k_1k_2)\end{aligned}$$

which follows from Lemma 4.4.

Therefore φ is an isomorphism and so $G \cong H \times K$. □

An important thing to note is that the condition $G = HK$ can be changed to $|G| = |H||K|$ if G is finite which is easier to check. This is because $|HK| = |H \times K| = |H||K|$ (Exercise: prove this) and clearly $HK \subseteq G$ so if $|G| = |H|K|$ then $G = HK$.

4.2 Semidirect Products

It can be quite difficult to identify if a group is a direct product because we need to find two normal subgroups. It can be challenging enough to find one so finding two and ensuring they have a trivial intersection is even more so. To ease this restriction we reconsider how we define the product between two elements in the product of a group. For instance, instead of taking $(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2)$ we could instead first map g_2 to a new element dependent on the element h_1 (simply using the same map everytime would not give us a new group). This is the idea behind a semidirect product.

Definition 4.6 (Semidirect Product)**.** Let K and Q be groups. Let $\theta : Q \to \text{Aut}(K)$ be a homomorphism and denote $\theta(q) = \theta_q$. Then $K \times Q$ forms a group under the binary operation defined by $(k_1,q_1)(k_2,q_2) = (k_1\theta_{q_1}(k_2), q_1q_2)$ where $k_1, k_2 \in K$ and $q_1, q_2 \in Q$. We call this group a semidirect product of Q and K and denote it $K \rtimes_\theta Q$ (or $K \rtimes Q$ if θ is obvious).

Example 4.7. We want to describe all possible semidirect products $C_7 \rtimes_\theta C_8$ where $\theta : C_8 \to \text{Aut}(C_7)$ is a homomorphism.

Doing so is a question of finding all potential θ. Thankfully we can use the properties of homomorphisms to narrow down the options. Firstly, note that if y is a generator of C_8 then, to determine θ, we need only know the value of $\theta(y)$. This is since every element of C_8 is y^r for some $r \in \mathbb{Z}$ and $\theta(y^r) = \theta(y)^r$. We can also narrow down options for the value of $\theta(y)$ by noting that $\theta(y^8) = \theta(y)^8 = \theta(e) = \text{id}$, the identity map, and hence the order of $\theta(y)$ must divide 8.

We can further reduce the possibilities of $\theta(y)$ be considering the group $\text{Aut}(C_7)$. Recall that $\text{Aut}(C_7) \cong C_6$, meaning it has order 6 and is cyclic. These facts tell us that $\theta(y)$ must have an order dividing 6 (by Corollary 2.6.1) and hence $\text{ord}(\theta(y)) \in \{1,2\}$. We also know $\theta(y)$ must be a power of a generator of $\text{Aut}(C_7)$, a fact we can use to quickly find elements of the required order.

Recall that elements of $\text{Aut}(C_7)$ have the form $\phi_r : x \mapsto x^r$ and hence a generator of $\text{Aut}(C_7)$ is a map ϕ_r such that for all $i \in \{1,\ldots,6\}$ there exists some $n \in \{1,\ldots,6\}$ such that $rn = i$ as then $\phi_r^n = \phi_i$. Thus, this is the same problem as finding primitive roots modulo 7 so we can use the same tools from number theory to find that ϕ_3 generates $\mathrm{Aut}(C_7)$ as 3 is a primitive root modulo 7.

The importance of this is we now know $\theta(y) = \phi_3^k$ for some $k \in \{1, \ldots, 6\}$ and crucially we know that $\mathrm{ord}(\phi_3^k) = \frac{6}{\gcd(k,6)}$. Clearly, $\theta(y)$ having order one requires $\theta(y) = \mathrm{id}$, the identity map, but for $\mathrm{ord}(\theta(y)) = 2$ we must find k such that $\frac{6}{\gcd(k,6)} = 2$ and thus we can see $\theta(y) = \phi_3^2 = \phi_6$.

If $\theta(y) = \mathrm{id}$ then $\theta = \mathrm{id}$ identically so the semidirect product under this map is no different to the direct product. So $C_7 \rtimes_{\mathrm{id}} C_8 \cong C_7 \times C_8 \cong C_{56}$ (since 7 and 8 are coprime). Note that we denote the map chosen for the semidirect product simply by the value of $\theta(y)$.

More interestingly, if $\theta(y) = \phi_6$ we get the group $C_7 \rtimes_{\phi_6} C_8$ which is fundamentally different group from the direct product. To analyse its behaviour, we let x be a generator for C_7 and note what products between generators give:

- $(x, e)(x, e) = (x\theta_e(x), e) = (x^2, e)$
- $(e, y)(e, y) = (e\theta_y(e), y^2) = (e, y^2)$
- $(x, e)(e, y) = (x\theta_e(e), y) = (x, y)$
- $(e, y)(x, e) = (\theta_y(x), y) = (\phi_6(x), y) = (x^6, y)$

So we can see that this group has two generators, $a = (x, e)$ and $b = (e, y)$ where $a^7 = (x^7, e) = e$, $b^8 = (e, y^8) = e$ and $ba = (e, y)(x, e) = (x^6, y) = a^6 b = a^{-1}b$. Thus $C_7 \rtimes_{\phi_6} C_8 \cong \langle a, b \mid a^7 = b^8 = e,\, a^{-1}b = ba\rangle$. Often this is called the semidirect product via the inverse map since $\phi_6(x) = x^6 = x^{-1}$ and it has this property that $ba = a^{-1}b$.

More generally, to find all semidirect products between cyclic groups we need to find the automorphisms ϕ_r with satisfactory order and we then find that $C_m \rtimes_{\phi_r} C_n \cong \langle a, b \mid a^m = b^n = e,\, a^r b = ba\rangle$.

When considering more general groups, it can be more difficult to characterise their automorphisms. Fortunately, there is one kind of automorphism that comes up repeatedly.

Proposition 4.8. *Let G be a group and $H \subseteq G$ a normal subgroup. For $g \in G$ we define the map $c_g : H \to H$ by $c_g : h \mapsto ghg^{-1}$. Then c_g is an automorphism of H and the map $\theta : G \to \mathrm{Aut}(H)$ where $\theta : g \mapsto c_g$ is a homomorphism.*

Proof. Let $g \in G$ and $h_1, h_2 \in H$. Then $c_g(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = c_g(h_1)c_g(h_2)$ so c_g is a homomorphism. Since H is normal, $\mathrm{im}\, c_g = gHg^{-1} = H$ so c_g is surjective. Suppose now that $h \in \ker c_g$. Then $ghg^{-1} = e$ so $h = g^{-1}g = e$ and thus c_g is injective. This ultimately shows that c_g is an automorphism.

To see that θ is a homomorphism, simply note that, for $a, b \in G$, $c_{ab}(h) = abhb^{-1}a^{-1} = c_a(c_b(h)) = (c_a \circ c_b)(h)$. □

Since every group is a normal subgroup of itself, we see that conjugation is always an automorphism. The reason we prove this theorem for subgroups specifically is that we will use it as a tool for recognising groups as semidirect products. Doing so is much easier than checking if one is a direct product. We formalise this with the next theorem.

Theorem 4.9 (Semidirect Product Recognition)**.** *Let G be a group and $K, Q \subseteq G$ subgroups such that K is normal in G; $K \cap Q = \{e\}$; and $G = KQ$ (or $|G| = |K||Q|$ if G is finite). Then $G \cong K \rtimes_\theta Q$ where $\theta : Q \to \mathrm{Aut}(K)$ is defined by $\theta(q) = c_q$.*

Proof. Since K is normal in G, it is true that $c_q \in \mathrm{Aut}(K)$ for all $q \in Q$ and that θ a homomorphism, this follows from Proposition 4.8. Now, define $\psi : K \rtimes_\theta Q \to G$ by $\psi(k, q) = kq$. We will show ψ is an isomorphism. First, note that, since $G = KQ$, ψ is surjective. To show injectivity, let $k_1, k_2 \in K$ and $q_1, q_2 \in Q$ be such that $\psi(k_1, q_1) = \psi(k_2\ q_2)$, that is $k_1q_1 = k_2q_2$. So $k_2k_1^{-1} = q_1q_2^{-1} \in K \cap Q$ but $K \cap Q = \{e\}$ so $k_1 = k_2$ and $q_1 = q_2$, that is $(k_1, q_1) = (k_2, q_2)$. Thus ψ is injective and hence ψ is a bijection.

We now show ψ is a homomorphism. Simply write

$$\begin{aligned}\psi((k_1, q_1)(k_2, q_2)) &= \psi(k_1\theta_{q_1}(k_2), q_1, q_2)\\ &= k_1\theta_{q_1}(k_2)q_1q_2\\ &= k_1q_1k_2q_1^{-1}q_1q_2\\ &= k_1q_1k_2q_1\\ &= \psi(k_1, q_1)\psi(k_2, q_2).\end{aligned}$$

Therefore ψ is an isomorphism and so $G \cong K \rtimes_\theta Q$ □

We will show the benefit this theorem has to our cause of classifying groups in a moment but first it is important we note that different homomorphisms can give rise to the same semidirect product and, in general, it is not always easy to determine when two are isomorphic. This means that we often have to resort to hands-on methods (think comparing orders of elements, whether a group is abelian etc.) to see if we get fundamentally different groups. Thankfully, we sometimes have a tool we use to make this process a little simpler.

Proposition 4.10. *Let K and Q be groups. Let $f \in \mathrm{Aut}(Q)$ and $\theta : Q \to \mathrm{Aut}(K)$ be a homomorphism. Denote $\mu = \theta \circ f$. Then $K \rtimes_\mu Q \cong K \rtimes_\theta Q$*

Proof. First we check that $\mu = \theta \circ f$ is indeed a valid homomorphism. If $q \in Q$ then $f(q) = q'$ for some $q' \in Q$ so $\mu(q) = \theta(q') \in \mathrm{Aut}(K)$. Thus μ is a map from Q to $\mathrm{Aut}(K)$. To check that μ is a homomorphism, we write

$$\begin{aligned}\mu(q_1q_2) &= \theta(f(q_1q_2))\\ &= \theta(f(q_1)f(q_2))\\ &= \theta(f(q_1))\theta(f(q_2))\\ &= \mu(q_1)\mu(q_2).\end{aligned}$$

So $\mu : Q \to \mathrm{Aut}(K)$ is a homomorphism as required.

Now define $\lambda : K \rtimes_\mu Q \to K \rtimes_\theta Q$ by $\lambda : (k, q) \mapsto (k, f(q))$. Since $f \in \mathrm{Aut}(Q)$, this is a bijection with inverse $\lambda^{-1} : (k, q) \mapsto (k, f^{-1}(q))$. Now observe

$$\begin{aligned} \lambda((k_1, q_1)(k_2, q_2)) &= \lambda(k_1\mu_{q_1}(k_2), q_1q_2) \\ &= \lambda(k_1\theta_{f(q_1)}(k_2), q_1q_2) \\ &= (k_1\theta_{f(q_1)}(k_2), f(q_1)f(q_2)) \\ &= (k_1, f(q_1))(k_2, f(q_2)) \\ &= \lambda(k_1, q_1)\lambda(k_2, q_2). \end{aligned}$$

So λ is an isomorphism and therefore $K \rtimes_\mu Q \cong K \rtimes_\theta Q$. □

Example 4.11. Consider $C_7 \rtimes_{\phi_2} C_3$ and $C_7 \rtimes_{\phi_4} C_3$.

Suppose $x \in C_3$ generates C_3. Consider the homomorhpism $\theta : C_3 \to \text{Aut}(C_7)$ where $\theta(x) = \phi_2$. If we take $f \in \text{Aut}(C_3)$ where $f : x \mapsto x^2$ then $(\theta \circ f)(x) = \theta(x^2) = \theta(x)^2 = \phi_2^2 = \phi_4$. Therefore, by Proposition 4.10, $C_7 \rtimes_{\phi_2} C_3 \cong C_7 \rtimes_{\phi_4} C_3$.

4.3 Groups of Order 8 or Less

We now have the tools available to classify all groups of order less than 8 (and some of even higher orders). We already know the only group of order 1 is the trivial group and the only groups of orders $2, 3, 5$ and 7 are the cyclic groups (by Theorem 2.7. We also used Cayley tables to find that C_4 and $C_2 \times C_2$ were the only groups of order 4. Now we can use what we know about products of groups to classify all groups of order 6 and 8.

Theorem 4.12 (Groups of order $2p$)**.** *Let $p \in \mathbb{N}$ be an odd prime and G a group such that $|G| = p$. Then $G \cong C_{2p}$ or $G \cong D_{2p}$*

Proof. We first want to show an element of order p exists. If there is an element s of order $2p$ then s^2 has order p. If not, aiming for a contradiction, suppose no element of order p exists. Then for all $g \in G$ it must be that $g^2 = e$ (by Lagrange's theorem). This would mean that, for all $a, b \in G$ we have $b^{-1}a^{-1} = ba$ but $(ab)^2 = e$ so $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. Thus G must be abelian. So, if we let $x, y \in G$ such that x, y are non-trivial and $x \neq y$, then $\{e, x, y, xy\}$ is a subgroup of G but clearly this subgroup has order 4, contradicting Lagrange's theorem. So there must exist $h \in G$ such that $\text{ord}(h) = p$.

Let $H = \langle h \rangle \cong C_p$ and let $k \in G - H$. Denote $K = \langle k \rangle$. Then $|H \cap K|$ divides $|H|$ and $H \cap K \neq H$. Thus it must be that $|H \cap K| = 1$ and so $H \cap K = \{e\}$. From this we see that $|HK| = |H||K| = \text{ord}(k)p \leq |G|$. However, we know $\text{ord}(k) \in \{2, p\}$ but $p^2 > |G|$ so $\text{ord}(k) = 2$. Thus $|HK| = |G|$ and, since $HK \subseteq G$, this implies $G = HK$.

See that H is normal since it has index 2, thus we have all the conditions to show that $G \cong H \rtimes_\theta K \cong C_p \rtimes_\theta C_2$ where $\theta : C_2 \to \text{Aut}(C_p)$. Note that $\theta(k)^2 = \text{id}$ so $\theta(k) = \text{id}$ or $\theta(k) = \phi_{-1}$. Thus G is isomorphic to one of $C_p \rtimes_{\text{id}} C_2 \cong C_p \times C_2 \cong C_{2p}$ or $C_p \rtimes_{\phi_{-1}} C_2 = \langle a, b \mid a^p = b^2 = e, a^{-1}b = ba \rangle \cong D_{2p}$. □

This theorem now tells us that there are two groups of order 6, C_6 and D_6 (note that D_6 is the smallest non-abelian group). It also tells us what the groups of order 10, 202 and 1046 but sadly not over order 8. That we must tackle head on.

To shorten notation, we will quickly introduce the group Q_8, the group of quarternions, which has two equivalent presentations: $\langle x, y \mid x^4 = e,\, y^2 = x^2,\, yx = x^3y\rangle$ (the one we will use for ease of classification) and $\langle i, j, k \mid i^2 = j^2 = k^2 = ijk\rangle$ (the one that comes from the definition of quarternions more generally).

Theorem 4.13 (Groups of Order 8)**.** *The groups of order* 8 *are* C_8*,* $C_4 \times C_2$*,* $C_2 \times C_2 \times C_2$*,* D_8 *and* Q_8*.*

Proof. Let G be a group of order 8. If G has an element of order 8 then $G \cong C_8$ and we are done. If it does not then, by Lagrange's Theorem, every non-trivial element of G has order 2 or 4. We thus consider two cases.

Suppose G has no elements of order 4. Then $g^2 = e$ for all $g \in G$ then G is abelian (see proof of Theorem 4.12) and so $H = \{e, a, b, ab\}$ is a subgroup of G for any $a, b \in G$. Let $k \in G - H$ and let $K = \langle k\rangle$. Since G is abelian, H and K are both normal by Proposition 3.8. Also, $H \cap K = \{e\}$ and $|G| = |H||K|$, meaning $G \cong H \times K$ (by Theorem 4.5). Clearly $K \cong C_2$ and H is a group of order 4 where all its elements have order 2, so $H \cong C_2 \times C_2$. Therefore $G \cong C_2 \times C_2 \times C_2$.

Now suppose G has no element of order 4, call it q and let $Q = \langle q\rangle$. We once again split into two cases. First, suppose there exists $r \in G - Q$ with order 2 and let $R = \langle r\rangle$.

Since Q has index 2, it is normal. Also, $|G| = |Q||R|$ and, by construction, $Q \cap R = \{e\}$. So, by Theorem 4.9, $G \cong Q \rtimes_\theta R \cong C_4 \rtimes_\theta C_2$ where $\theta : C_2 \to \mathrm{Aut}(C_4)$. Note that $\theta(r)^2 = \mathrm{id}$ so $\theta(r) \in \{\mathrm{id}, \phi_{-1}\}$. Thus, either $G \cong C_4 \rtimes_{\mathrm{id}} C_2 \cong C_4 \times C_2$ or $G \cong C_4 \rtimes_{\phi_{-1}} C_2 \cong D_8$.

We now consider the final case where Q is as before but all elements of $G - Q$ have order 4. Let $s \in G - Q$ and note that s^2 has order 2 so $s^2 \in Q$ but only q^2 has order 2 in Q so $s^2 = q^2$. Also, see that $sq \notin Q$ since that would mean $sqq^{-1} = s \in H$, a contradiction. Thus, as Q has index 2, $sq \in Hs = \{s, qs, q^2s, q^3s\}$. Clearly $sq \neq s$ since $q \neq e$. If $sq = qs$ then $(sq)^2 = sqsq = ssqq = q^4 = e$, since $s^2 = q^2$, but this contradicts the fact that $sq \in G - Q$ and so has order 4. Similarly, if $sq = q^2s$ then $sq^2 = q^2sq = q^4s = s$, implying $q^2 = e$, contradicting the fact that q has order 4. This means that $sq = q^3s$. We thus have a group with two generators q and s, both with order 4 and having the properties that $q^2 = s^2$ and $sq = q^3s$. Therefore $G \cong \langle q, s \mid q^4 = e,\, q^2 = s^2,\, sq = q^3s\rangle \cong Q_8$.

□

5 Sylow Theorems

As we have seen, a good general approach for classifying groups of a given order is identifying normal subgroups. The Sylow Theorems are very powerful theorems with many applications, one of them being identifying such subgroups.

5.1 p-Groups

Definition 5.1 (p-Group)**.** Let $p \in \mathbb{N}$ be prime and $m, s \in \mathbb{N}$ with $m, s \geq 1$. If G is a group such that $|G| = p^m$ then G is called a p-group. If $H \subseteq G$ is a subgroup where $|H| = p^s$ then H is called a p-subgroup.

The Sylow Theorems make claims about specific kinds of p-subgroups which we call Sylow p-subgroups.

Definition 5.2 (Sylow p-subgroup)**.** Let $p \in \mathbb{N}$ be prime and G a group such that p divides $|G|$. Then if $H \subseteq G$ is a subgroup of order the highest power of p dividing $|G|$ we say H is a Sylow p-subgroup. That is if $|G| = kp^n$ with $k, p \in \mathbb{N}$, $n \geq 1$ and p not a divisor of k then if $|H| = p^n$ it is called a Sylow p-subgroup. The set of all Sylow p-subgroups of G is denoted $\mathrm{Syl}_p(G)$ and often $|\mathrm{Syl}_p(G)|$ is denoted n_p.

5.2 Sylow Theorems

There are three Sylow theorems. The first tells us that Sylow p-subgroups always exists (when p divides the order of G. The second tells us that Sylow p-subgroups of the same order are conjugate to each other. The third gives us a restriction on how many Sylow p-subgroups there are.

One important use of these is then to find cases when there is exactly one Sylow p-subgroup. Since it must be conjugate to another of the same order, it has to be conjugate to itself and is therefore normal.

We will now state these theorems but omit the proof.

Theorem 5.3 (Sylow's 1st Theorem)**.** *Let $p \in \mathbb{N}$ be prime and $n, k \in \mathbb{N}$ be such that $n \geq 1$ and p does not divide k. Let G be a group such that $|G| = kp^n$. Then $\mathrm{Syl}_p(G) \neq \emptyset$ or, equivalently, $n_p \geq 1$.*

Theorem 5.4 (Sylow's 2nd Theorem)**.** *Let $p \in \mathbb{N}$ be prime and $n, k \in \mathbb{N}$ be such that $n \geq 1$ and p does not divide k. Let G be a group such that $|G| = kp^n$ and let $P \in \mathrm{Syl}_p(G)$. Let $m \in \mathbb{N}$ be such that $1 \leq m \leq n$ and $H \subseteq G$ a subgroup of order p^m. Then there exists $g \in G$ such that $gHg^{-1} \subseteq P$. In particular, if $H \in \mathrm{Syl}_p(G)$ then H is conjugate to P.*

Theorem 5.5 (Sylow's 3rd Theorem)**.** *Let $p \in \mathbb{N}$ be prime and $n, k \in \mathbb{N}$ be such that $n \geq 1$ and p does not divide k. Let G be a group such that $|G| = kp^n$. Then $n_p \equiv 1 \mod p$ and n_p divides k.*

Combining these theorems together gives us the statement that, for $p \in \mathbb{N}$ prime with $n, k \in \mathbb{N}$ where $n \geq 1$ and p does not divide k, if there does not exist $a \in \mathbb{N}$ such that $a \equiv 1 \mod p$ and a divides k then any group of order kp^n has a normal subgroup of order p^n.

However, note that we do not need to necessarily use Theorem 5.4 to show such subgroups are normal since, if H a subgroup of G and $g \in G$, then gHg^{-1} is also a subgroup and $|gHg^{-1}| = |H|$ so, if H is the only subgroup of its order, we must have $gHg^{-1} = H$.

5.3 Applications

Example 5.6 (Groups of Order 15)**.** Let G be a group of order 15.

By Theorem 5.3, there exists some $H \in \mathrm{Syl}\,3(G)$ and some $K \in \mathrm{Syl}_5(G)$. By Theorem 5.5, $n_3 \equiv 1 \mod 3$ and $n_3 \mid 5$ and thus $n_3 = 1$. Similarly, $n_5 \equiv 1 \mod 5$ and $n_5 \mid 3$, thus $n_5 = 1$. So H and K are unique subgroups of order 3 and 5 respectively and hence are normal by Theorem 5.4. Since H and K have co-prime orders, by Lagrange's theorem, $H \cap K = \{e\}$. Also, $|G| = |H||K| = 15$. From this we can see that $G = H \times K$. However, since groups of prime order are cyclic, this means that $G \cong C_3 \times C_5$ and, since 3 and 5 are co-prime, we therefore have $G \cong C_{15}$.

Example 5.7 (Groups of Order 21)**.** Let G be a group of order 21.

By Theorem 5.3 and Theorem 5.5, we have $n_7 \geq 1$, $n_7 \equiv 1 \mod 7$ and $n_7 \mid 3$. Thus $n_7 = 1$. Let $K \leq G$ be the unique subgroup of order 7, it follows that $K \lhd G$ and $K \cong C_7$. By Theorem 5.3, there exists some $Q \in \mathrm{Syl}_3(G)$. Note that $Q \cong C_3$. Since they have co-prime orders, $K \cap Q = \{e\}$. Also note that $|G| = |K||Q| = 21$ so we find that $G \cong C_7 \rtimes_\theta C_3$ for some $\theta : C_3 \to \mathrm{Aut}(C_7)$.

To identify all posible semidirect products, let $C_7 = \langle x \rangle$ and $C_3 = \langle y \rangle$. To have a valid homomorphism we need $\theta(y)^3 = \mathrm{id}$. Since $\mathrm{Aut}(C_7) = \langle \phi_3 \rangle \cong C_6$ (as 3 is a primitive root modulo 7), it must be that $\theta(y) \in \{\mathrm{id}, \phi_3^2 = \phi_2, \phi_3^4 = \phi_4\}$. However, if we take $f \in \mathrm{Aut}(C_3)$ where $f : y \mapsto y^2$ then we can see that ϕ_4 and ϕ_2 give isomorphic groups (see Example 4.11). Thus G is either $C_7 \rtimes_{\mathrm{id}} C_3 = C_7 \times C_3 \cong C_{21}$ or $C_7 \rtimes_{\phi_2} C_3 \cong \langle xy \mid x^7 = y^3 = e,\, x^2 y = yx \rangle$.

6 Group Actions

6.1 Definition

We will briefly move away from the aim of classifying groups to look at group actions. Recall when we first came across the group D_{2n}, we initially described it as the group of symmetries of a regular n-sided polygon but moved away from that definition to a more abstract one based on a group presentation. While this was useful to help us talk about the group in a more general way and identify it as a semidirect product, removing some of the concreteness and specifity can obscure some properties of the group that seem far more obvious and intuitive when we understand it as a group of symmetries. Group actions aim to reverse this process, taking an abstract group and interpreting it as group of symmetries, making it much easier to understand how the group behaves.

There are two equivalent ways of defining a group action. We will give both of these but we will primarily use the first. The latter is more common however which is why it is provided here.

Definition 6.1 (Group Action)**.** Let G be a group, X a set and $\mathrm{Bij}(X)$ the group of bijections/permutations on X. An action of G on X is a homomorphism $\varphi : G \to \mathrm{Bij}(X)$. For convenience, we write $g \cdot x$ to mean $\varphi(g)(x)$ when the action is clear.

A group action, therefore, is simply a way of associating elements of a group with symmetries of a set such that the group structure is maintained. An alternative definition is as follows.

Definition 6.2. Let G be a group and X a set. An action of G on X is a function $\varphi : G \times X \to X$ such that $\varphi(e, x) = x$ for all $x \in X$ and $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$ for every $g, h \in G$ and every $x \in X$. In condensed notation, we require $e \cdot x = x$ and $g \cdot (h \cdot x) = gh \cdot x$.

To illustrate one of the simplest ways group actions can make tricky questions seem obvious can be seen by considering the group D_{14} (or any D_{2n}). Recall that $D_{14} = \langle x, y \mid x^7 = y^2 = e,\, x^{-1}y = yx \rangle$. How can we prove that $x \neq y$? It would be difficult and time consuming to try and prove this using the relations given in the group presentation but one very easy way is to understand D_{14} as acting on a heptagon where x corresponds to a rotation and y to a reflection. Then clearly $x \neq y$. Below is a more complex example.

Example 6.3. Consider the group A_4, that is the group of even permutations of four elements which we saw in Algebra 1, acting on the vertices of a regular tetrahedron (triangular based pyramid) T as follows. Label the vertices of the terahedon 1, 2, 3 and 4 then, for $\sigma \in A_4$, σ acts on these vertices by rotating T as dictated by the permutation. For instance, the action of $(1\,2)(3\,4)$ would send the vertex labelled 1 to the one labelled 2 and vice versa and simialrly for 3 and 4.

We choose the group A_4 rather than S_4 as these permuations correspond to valid rotations of T. However, we could choose S_4 to act on T in the same way and then some of these actions would describe reflective symmetries as well.

Also note that each element of A_4 corresponds to a different rotation and that each rotation has a corresponding permuatation in A_4. Thus the homomorphism that induces our action is in fact an isomorphism and hence the rotational symmetry group of T is isomorphic to the group A_4.

Definition 6.4 (Faithful Action)**.** Let G be a group, X a set and $\varphi : G \to \mathrm{Bij}(X)$ a homomorphism describing an action of G on X. If φ is injective, that is if every element of G gives a different permutation of X, then we say the action is faithful.

Definition 6.5 (Trivial Action)**.** Let G be a group, X a set and $\varphi : G \to \mathrm{Bij}(X)$ a homomorphism describing an action of G on X. We say the action is trivial if $g \cdot x = x$ for all $g \in G$ and all $x \in X$, that is if $\ker \phi = G$.

6.2 Finding Subgroups

Recall that a group action is a homomorphism from a group to the group of permutations of a set. If an action is unfaithful then the kernel of this homomorphism is non-trivial. So, since we know kernels are normal subgroups, the kernal of an unfaithful, non-trivial action is a non-trivial, proper, normal subgroup. Also note that this means that all non-trivial actions of a simple group are faithful.

Example 6.6. Let G be the group of symmetries of a cube, this group is isomorphic to $C_2 \times S_4$.

Now consider G acting on the line segments connecting opposite faces of a cube. This action is unfaithful and its kernel can be generated by the three reflections in planes containing two of the line segments. Each reflection has order 2 and thus the kernel is isomorphic to $C_2 \times C_2 \times C_2$ and hence this isomorphic to a normal subgroup of $C_2 \times S_4$.

Also recall that whenever we have a homomorphism, not only do we know its kernel is a normal subgroup but that, by Theorem 3.13, its image is the quotient group of its kernel. Thus group actions can also help us identify quotient groups.

Example 6.7. Let G be the group of rotation symmetries of a cube, this group is isomorphic to S_4.

Now consider G acting on two tetrahedra inscribed inside a cube such that the vertices of the tetrahedra intersect vertices of the cube. Then any rotation of the cube about one of its diagonals keeps the tetrahedra in the same position and so G acts unfaithfully on this set. Since each tetrahedron can only take up one of two positions, the group of permutations of the tetrahedra is $S_2 \cong C_2$.

Therefore $G \cong S_4$ has a quotient group isomorphic to C_2.

6.3 Orbits and Stabilisers

Definition 6.8 (Orbit)**.** Let G be a group acting on a set X. The orbit of $x \in X$ is the set of elements that G sends x to. We write $G \cdot x = \{g \cdot x : \; g \in G\}$.

If we let a group G act on a set X and we define the relation $\sim$ by saying, for $x, y \in X$, $x \sim y$ if and only if $g \cdot x = y$ then it is not difficult to see that this is an equivalence relation. Importantly, the corresponding equivalence classes are orbits and thus we can write X as the disjoint union of orbits.

This is useful as different actions can give us quite useful orbits and this shows that these orbits partition the set in a disjoint manner. For instance, consider the group G acting on itself by conjugation, that is, for $g, h \in G$, we define $g \cdot h = ghg^{-1}$. Then the orbit of h is called the conjugacy class of h. Elements in the same conjugacy class share many properties, for instance they all have the same order (since $(ghg^{-1})^n = gh^n g^{-1}$).

We can also consider a group G and a normal subgroup $H \subseteq G$. If we let H act on G by left multiplication, that is for $h \in H$ and $g \in G$ we define $h \cdot g = hg$, then the orbit of g is the right coset Hg. Thus we see again that cosets partition a group.

Definition 6.9 (Stabiliser)**.** Let G be a group acting on a set X. The stabiliser of $x \in X$ is the set of elements in G that fix x. We write $G_x = \{g \in G : \; g \cdot x = x\}$.

Proposition 6.10 (Stabilisers are Subgroups)**.** *Let G be a group acting on the set X. Then for all $x \in X$, we have that G_x is a subgroup of G.*

Proof. Fix $x \in X$. Since $e \cdot x = x$ then $e \in G_x$. Now let $g, h \in G_x$ then $g \cdot x = x$ so $hg \cdot x = h \cdot (g \cdot x) = h \cdot x = x$ so $hg \in G_x$. Also $g^{-1}g \cdot x = e \cdot x = x$ and $g^{-1}g \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$ so $g^{-1} \cdot x = x$. Therefore G_x is a subgroup. □

Some points in the set have every element of the group as a stabiliser, these points are unchanged under the action of the group and hence are called fixed points.

Definition 6.11 (Fixed Point)**.** Let G be a group acting on a set X. We say $x \in X$ is a fixed point if $g \cdot x = x$ for all $g \in G$. Equivalently, $G_x = G$ and $G \cdot x = \{x\}$. We denote the set of all fixed points X^G.

To see the connection between orbits and stabilisers, consider a cube and think of how to count the number of rotational symmetries it has. One way may be to consider just one face and realise there 6 faces it can go to, then a face adjacent to it has 4 places to go to which fixes the rotation. Thus there are $6 \cdot 4 = 24$ rotational symmetries. Similarly, there are 8 places a vertex can go and 3 places an adjacent vertex can go to fix the rotation, giving $8 \cdot 3 = 24$ rotations. We can rephrase this as saying the orbit of a face (under the action of the symmetry group) is all faces of the cube so has size 6. Once the position of the first face is chosen, there are 4 rotations that keep it in place, that is the stabiliser of the face has size 4. We then reason that the size of the symmetry group is the size of the orbits multiplied by the size of the stabilisers. The idea is this should work regardless of whether we consider the group acting on faces or vertices or anything else.

Theorem 6.12 (Orbit-Stabiliser Theorem)**.** *Let G be a group acting on a set X and let $x \in X$. If G and X are finite then $|G| = |G \cdot x||G_x|$. If G or X is infinite, then $G/G \cdot x$ and $G \cdot x$ are in bijection.*

Proof. Define the map $\varphi : G/G_x \to G \cdot x$ by $\varphi : gG_x \mapsto g \cdot x$. To see that this is a well-defined and injective function, consider the following chain of implications for $g, h \in G$

$$\begin{aligned} gG_x = hG_x &\iff g^{-1}h \in G_x \\ &\iff g^{-1}h \cdot x = x \\ &\iff h \cdot x = g \cdot x \\ &\iff \varphi(h) = \varphi(g) \end{aligned}$$

To show surjectivity, let $y \in G \cdot x$. Then there exists some $g \in G$ such that $y = g \cdot x$ so $\varphi(gG_x) = y$. This shows that φ is a bijection and thus the statement follows. □

This theorem is very powerful, to illustrate this, we provide an alternative proof of Lagrange's theorem.

Theorem 6.13 (Lagrange's Theorem)**.** *Let G be a group and $H \subseteq G$ a subgroup. Then $|H|$ divides $|G|$.*

Proof. Let H act on G by right multiplication, that is, for $h \in H$ and $g \in G$, define $h \cdot g = gh$. Then, for any $g \in G$, we have $H \cdot g = \{gh : h \in H\} = gH$. Recall that $|gH| = |H|$. Then, by Theorem 6.12, $|G| = |H \cdot g||H_g| = |H||H_g|$ and therefore $|H|$ divides $|G|$. □

6.4 The Class Equation

If we let G be a finite group acting on a finite set X then we can write X as the disjoint union of orbits. So there exist $x_i \in X$, where $i \in \{1, \ldots, n\}$ for some $n \in \mathbb{N}$, such that $|X| = \sum_{i=1}^{n} |G \cdot x_i|$. Note that if x_i is a fixed point then $|G \cdot x_i| = 1$. Since we can reorder them, we may assume that there exists $m \in \{1, \ldots, n\}$ such that, for $i < m$, we have $x_i \in X^G$. We thus have

$$|X| = |X^G| + \sum_{i=m}^{n} |G \cdot x_i|.$$

This is called the class equation.

Theorem 6.14 (Fixed Point Congruence)**.** *Let $p \in \mathbb{N}$ be prime and G a non-trivial group with $|G| = p^k$ for some $k \in \mathbb{N}$. Let X be a finite set and let G act on X. Then $|X| \equiv |X^G| \mod p$.*

Proof. Let $\{x_1, \ldots, x_n\}$, for some $n \in \mathbb{N}$, be elements of X such that $X = \bigcup_{i=1}^{n} G \cdot x_i$ is disjoint. Let $m \in \{1, \ldots, n\}$ be such that, after relabelling of $\{x_1, .., x_n\}$, if $i < m$ then x_i is a fixed point. Applying Theorem 6.12 to the class equation we get $|X| = |X^G| + \sum_{i=m}^{n} \frac{|G|}{|G_{x_i}|}$. Since $|G| = p^k$ and G_{x_i} is a subgroup, it must be that $|G_{x_i}| = p^{r_i}$ where $r_i \in \{0, 1, \ldots, k-1\}$. Therefore, reducing mod p, we get $|X| \equiv |X^G| \mod p$ as required. □

The class equation and fixed point congruence can be of particular use when we let G act on itself by conjugation. Then $X^G = Z(G)$, the centre of G (that is the elements in G which commute), and the $|G \cdot x_i|$ are distinct conjugacy classes with more than one element. To see the importance of this, consider the following corollary.

Corollary 6.14.1. *If G is a group with order a prime power then $Z(G)$ is non-trivial.*

Proof. Let $p \in \mathbb{N}$ be prime and G a group with order a power of p. Let G act on itself by conjugation so the fixed points are $Z(G)$. By Theorem 6.14, $|G| \equiv |Z(G)| \mod p$ and so, since p divides $|G|$, $|Z(G)| \equiv 0 \mod p$. However, $Z(G)$ always contains the identity so $|Z(G)| \neq 0$. Therefore $|Z(G)| \geq p$ and hence is non-trivial. □

Since the centre of a group is a normal subgroup (see Example 3.5), we can use this fact to identify some groups which are never simple.

Corollary 6.14.2. *Let $p \in \mathbb{N}$ be prime and $n \in \mathbb{N}$ with $n > 1$. Then any group of order p^n is not simple.*

Proof. Let G be a group of order p^n. By Corollary 6.14.1, $Z(G)$ is non-trivial. We consider two cases.

If $Z(G) \neq G$ then it is a non-trivial, proper, normal subgroup and hence G is not simple.

Now, suppose $Z(G) = G$. Then G is abelian and hence any of its subgroups are normal (by Proposition 3.8). To construct a proper subgroup, suppose there exists $g \in G$ such that $\text{ord}(g) = p^k$ for some $k \in \mathbb{N}$ with $k > 1$. Then clearly $\text{ord}(g^{p^{k-1}}) = p$ so $\langle g^{p^{k-1}} \rangle$ is a proper, non-trivial normal subgroup and so G is not simple. If no such g exists then, by Lagrange's Theorem, all non-identity elements must have order p and so each generate a non-trivial, proper, normal subgroup. Thus G is not simple. □

6.5 Classifying Groups with Actions

As we have seen, group actions can tell us a lot about the structure of a group and thus can help us with our goal of classifying groups of a given order. One very helpful tool to aid us in this venture which we can now prove is Cauchy's Theorem. This is, in some sense, a weaker form of Theorem 5.3 but requires far fewer conditions to be met allowing us to very easily find subgroups of prime order.

Theorem 6.15 (Cauchy's Theorem)**.** *Let G be a group and $p \in \mathbb{N}$ a prime divisor of the order of G. Then G contains an element of order p and hence a cyclic subgroup of order p.*

Proof. Let n denote the order of G and $p \in \mathbb{N}$ a prime divisor of n. We construct the set X to contain all p-tuples of elements in G such that the product of these elements is the identity. That is $X = \{(g_1, \dots, g_p) : \ g_i \in G \,\text{for all}\, i \in \{1, \dots, p\} \,\text{and}\, g_1 \cdots g_p = e\}$.

Note that if we are given any $g_1, \dots, g_{p-1} \in G$ then there is a unique element of X containing all these elements of g. To see this, take $g_p = (g_1 \cdots g_{p-1})^{-1}$. Then $g_1 \cdots g_p = e$ and hence $(g_1, \dots, g_p) \in X$. Since we have n choices for each of these $p - 1$ elements and the last one is fixed, we can see that $|X| = n^{p-1}$.

Now consider the group C_p, with generator $y \in C_p$, acting on the set X such that $y^k \cdot (g_1, \dots, g_p) = (g_{k+1}, \dots, g_p, g_1, \dots, g_k)$ for $k \in \{0, \dots, p-1\}$. For instance, $y \cdot (g_1, \dots, g_p) = (g_2, \dots, g_p, g_1)$. Note that fixed points of this action are tuples where every element is the same, that is fixed points have the form $(g, \dots, g)$ where $g \in G$ is such that $g^p = e$. Thus the order of such a g is 1 or p.

Clearly, $e \in X^{C_p}$ by this reasoning so $|X^{C_p}| \geq 1$. By the fixed points congruence (Theorem 6.14), we know $|X| \equiv |X^{C_p}| \mod p$ but $|X| = n^{p-1}$ and n is a multiple of p. It thus follows that $|X^{C_p}|$ is a multiple of p and therefore, since $|X^{C_p}| \geq 1$, we know $|X^{C_p}| \geq p$.

Since only one element can be the identity, this means that there are at least $p-1$ elements of G of order p, each of which generate a cyclic subgroup of order p. □

This theorem is very effective at classifying subgroups as often we aim to find cyclic subgroups and use these to identify a group as some semidirect product. This would have made some of our previous classifications, like that of groups of order $2p$, much easier. We illustrate this technique in the next example.

Example 6.16 (Groups of order 20)**.** We will classify all groups of order 20 which contain an element of order 4.

Let G be a group of order 20 such that there exists an element $h \in G$ where $\mathrm{ord}(h) = 4$. Denote $H = \langle h \rangle$ and see that H is a subgroup of G and $H \cong C_4$.

There is no element in H with order 5 (since elements in H have even order) but 5 is a prime divisor of $|G|$ and so, by Cauchy's Theorem, G must contain an element of order 5.

It therefore must be that there exists $k \in G - H$ such that $\mathrm{ord}(k) = 5$. Let $K = \langle k \rangle \in \mathrm{Syl}_5(G)$. By the third Sylow Theorem, $|\mathrm{Syl}_5(G)| \equiv 1 \mod 5$ and $|\mathrm{Syl}_5(G)|$ divides $|G| = 20$ which is only possible if $|\mathrm{Syl}_5(G)| = 1$. Thus K is the only subgroup of order 5 and so K is normal in G.

Now note that $|G| = |H||K| = 20$ and $H \cap K = \{e\}$ (since $|H|$ and $|K|$ are coprime) so $G = K \rtimes_\theta H$ where $\theta : H \to \mathrm{Aut}(K)$ is a homomorphism.

To find which homomorphisms are possible, we use the fact that $H = \langle h \rangle \cong C_4$ and $K = \langle k \rangle \cong C_5$. From this we see that $\theta(h)^4 = \mathrm{id}$ must hold, however, since $\mathrm{Aut}(C_5) \cong C_4$, every element of $\mathrm{Aut}(C_5)$ has order that divides 4 and thus satisfies this condition. We can narrow down the possibilities slightly as we can let $f \in \mathrm{Aut}\, H$ be given by $f : h \mapsto h^3$ and see that, if $\theta(h) = \phi_2$ then $(\theta \circ f) = \theta(h)^3 = \phi_2^3 = \phi_3$. Thus the homomorphisms defined by $\theta(h) = \phi_2$ and $\theta(h) = \phi_3$ will produce isomorphic semidirect products.

This allows us to find the possible semi-direct products:

$$G = K \rtimes_{\mathrm{id}} H = K \times H \cong C_5 \times C_4 \cong C_{20}$$

or

$$G = K \rtimes_{\phi_2} H \cong \langle a, b \mid a^5 = b^4 = e,\, a^2 b = ba \rangle$$

or

$$G = K \rtimes_{\phi_4} H \cong \langle a, b \mid a^5 = b^4 = e,\, a^4 b = ba \rangle.$$

Since the direct product is abelian and the others aren't we know it is not isomoprhic to either $K \rtimes_{\phi_2} H$ or $K \rtimes_{\phi_4} H$. To see that these are not isomorphic to each other, we must consider how many elements there are of order 2.

In each, we have that $a^{ri}b = ba^i$ for some $r \in \{2,4\}$ and for all $i \in \mathbb{Z}$. Now, we can write any element of these groups as $a^i b^j$ for some $i,j \in \mathbb{Z}$ so, if an element has order 2 we have that

$$(a^i b^j)(a^i b^j) = a^{i+ir^j} b^{2j} = e$$

which is only possible if $j = 2$ and 5 divides $i + ir^j = i + ir^2$. If $r = 2$, the only possible $i + ir^2 = 5i$ so this holds for any i meaning the elements of order 2 in $K \rtimes_{\phi_2} H$ are $b^2, ab^2, a^2b^2, a^3b^2$ and a^4b^2. However, if $r = 4$ then $i + ir^2 = 17i$ which is only a mutiple of 5 when $i = 0$. Thus the only elements of order 2 in $K \rtimes_{\phi_4} H$ is b^2. Therefore these groups are not isomorphic.

So, if G is a group of order 20 with an element of order 4 then G is isomorphic to either C_{20}, $C_5 \rtimes_{\phi_2} C_4$ or $C_5 \rtimes_{\phi_4} C_4$.

We will finish our study of groups with a final remark on their classification. Notice how most of our methods of classification relied on subgroups of prime order, not only were these subgroups easier to find but they are isomorphic to cyclic groups and so we can easily understand their automorphisms and hence their semidirect products. This means we can quite easily classify groups of very large order as long as they have very few prime divisors but we can struggle with group of relatively small order if they have many prime divisors. This is especially true if a group has order the power of a prime as we have no hope of applying the Sylow Theorems. As a consequence, there tend to be many non-isomorphic groups of order a power of 2 relative to their size. In fact, 99.15% of groups of order 2000 or less have order $1024 = 2^{10}$.

7 Basics of Rings

Recall that $(\mathbb{Z}, +)$ is a group however this does not quite capture all of the structure we are used to with the integers, for that we'd need to include multipliaction as well. However, $\mathbb{Z}$ does not form a group under multiplication as not every element has an inverse. We therefore introduce a new concept, that of rings, to describe this kind of structure.

7.1 Definition and Examples

Definition 7.1 (Ring)**.** A ring $(R, +, \cdot)$ consists of a set R with two binary operations, one denoted addition ("+") and one multiplication ("$\cdot$"), satisfying the following properties:

- $(R, +)$ is an abelian group
- Multiplication is associative
- Multiplication is left and right distributive over addition

We often drop the "$\cdot$" when writing out multiplication. We denote the additive inverse of $a \in R$ by $-a$ and denote addition repeated $n \in \mathbb{N}$ times by na and $-na = n(-a)$. Although this uses additive notation, it follows all of the rules for powers we developed in our study of groups.

This is a rather general definition and often we are concerned with specific types of rings that have added conditions.

Definition 7.2. Let $(R, +, \cdot)$ be a ring. If R has a multiplicative identity we call R a ring with unity. If multiplication in R is commutative, we call R a commutative ring.

Emulating the integers, we denote the additive identity 0 and the multiplicative identity 1.

Be warned, some authors use the term ring to refer specifically to rings with unity, or even commutative rings with unity. Occasionally, some will use the term rng (pronounced "rung") to refer to non-unital rings. For greatest generality we will use the strictest definition.

Example 7.3 (Examples of Rings)**.** Since rings are constructed to emulate the integers, it is no surprise that $\mathbb{Z}$ is a commutative ring with unity under standard addition and multiplication. So are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

An example of a non-commutative ring is that of $n \times n$ matrices with entries from another ring. For instance, the ring of 2×2 matrices with real entries which we denote $M_2(\mathbb{R})$.

For a ring without unity, consider $2\mathbb{Z}$, the ring of even integers. See even numbers are closed under multiplication and addition, this is a (commutative ring) but does not contain 1 so does not have a multiplicative identity.

For a non-commutative ring without unity, we can combine the two previous examples and get $M_2(2\mathbb{Z})$.

7.2 Basic Properties

We now take a look at some basic properties of rings.

Proposition 7.4 (Properties of Rings)**.** *Let R be a ring, $a, b \in R$ and $m, n \in \mathbb{Z}$. Then*

(i) $a0 = 0a = 0$.

(ii) $a(-b) = (-a)b = -(ab)$.

(iii) $(-a)(-b) = ab$.

(iv) $m(ab) = (ma)b = a(mb)$.

(v) $mn(ab) = (ma)(nb)$.

Proof. For *(i)*, note that $a0 = a(0 + 0) = a0 + a0$ and hence $a0 = 0$.

For *(ii)*, note that $a(b - b) = ab + a(-b) = 0$ so $a(-b) = -ab$.

For *(iii)*, use the previous claim to see that $(-a)(-b) = (-(-a))b = ab$.

For *(iv)*, consider the specific case $2(ab) = ab + ab = (a + a)b = (2a)b$. The general case follows the same argument.

For *(v)*, use the previous claim to see that $mn(ab) = m(n(ab)) = m(a(nb)) = (ma)(nb)$. □

If we consider rings with unity, we also have the following property of identities.

Proposition 7.5. *Let R be a non-trivial ring with unity. Then $1 \neq 0$.*

Proof. Aiming for a contradiction, suppose $1 = 0$. Then for all $a \in R$ we have, by Proposition 7.4, $a = a1 = a0 = 0$ implying $R = \{0\}$. However, we assumed R was non-trivial and thus this is a contradiction. □

7.3 Units and Zero Divisors

There are two specific kinds of elements of a ring that are of particular note.

Definition 7.6 (Zero Divisor)**.** Let R be a ring and $a \in R$. We say a is a zero divisor if there exists some $b \in R$ with $b \neq 0$ such that $ab = 0$ or $ba = 0$.

Note that 0 is always a zero divisor. For this reason some authors define a zero divisor to always be non-zero.

Example 7.7. Consider the ring $M_2(\mathbb{R})$ and note that

$$\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix} \begin{pmatrix} 2 & 4 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Thus these two matrices are non-zero zero divisors.

Definition 7.8 (Unit)**.** Let R be a ring with unity and $a \in R$. We say a is a unit if there exists some $b \in R$ such that $ab = ba = 1$. We call b the multiplicative inverse of a and write $b = a^{-1}$. The set of all units is denoted $R^{\times}$.

Note that te set of units form a group under multiplication.

Proposition 7.9 (Units are not Zero Divisors)**.** *Let R be a ring with unity and $u \in R$ a unit. Then u is not a zero divisor.*

Proof. Let $r \in R$ such that $ur = ru = 0$. We want to show $r = 0$.

Since u is a unit, there exists some $u^{-1} \in R$ such that $u^{-1}u = uu^{-1} = 1$. So $u^{-1}ur = r$ and $u^{-1}ur = u^{-1}0 = 0$, implying $r = 0$. Thus u is not a zero divisor. □

7.4 Subrings

Just as we could have subgroups, we can have subrings of a ring.

Definition 7.10 (Subring)**.** Let $(R, +\cdot)$ be a ring and $S \subseteq R$. Then S is a subring if $(S, +, \cdot)$ is a ring. Equivalently, S is a subring if $(S, +)$ is a subgroup of $(R, +)$ and S is closed under mutliplication.

7.5 Ring Homomorphisms

Definition 7.11 (Ring Homomorphism)**.** Let R and S be rings. A ring homomorphism is a map $\varphi : R \to S$ such that, for all $x, y \in R$, we have that $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(xy) = \varphi(x)\varphi(y)$. If φ is bijective then it is an isomorphism.

For rings with unity, often we have the added restriction that unity is preserved.

Definition 7.12 (Unital Ring Homomorphism)**.** Let R and S be rings with unity. A unital ring homomorphism is a ring homomorphism, $\varphi : R \to S$, such that $\varphi(1_R) = 1_S$.

Proposition 7.13 (Properties of Ring Homomorphisms)**.** *Let R and S be rings and $\varphi : R \to S$ a ring homomorphism. Then the following hold:*

(i) $\varphi(0_R) = 0_S$

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

(iii) $\operatorname{im}\varphi$ *is a subring of* S

(iv) $\ker\varphi$ *is a subring of* R

(v) If R *has unity then* $\varphi(1_R)$ *is unity in* $\operatorname{im}\varphi$

Proof. For *(i)*, see that $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$ so $\varphi(0_R) = 0_S$.

For *(ii)*, let $a \in \mathbb{R}$ and note that $\varphi(a - a) = \varphi(0_R) = 0_S$ and $\varphi(a - a) = \varphi(a) + \varphi(-a)$ so $\varphi(a) + \varphi(-a) = 0_S$ meaning $\varphi(-a) = -\varphi(a)$.

For *(iii)*, every element of $\operatorname{im}\varphi$ can be written as $\varphi(r)$ for some $r \in R$ so let $\varphi(a), \varphi(b) \in \operatorname{im}\varphi$ with $a, b \in R$. Then $\varphi(a) + \varphi(b) = \varphi(a + b) \in \operatorname{im}\varphi$. Also, $-\varphi(a) = \varphi(-a) \in \operatorname{im}\varphi$ so $\operatorname{im}\varphi$ is an additive subgroup. Finally, note $\varphi(a)\varphi(b) = \varphi(ab) \in R$ so $\operatorname{im}\varphi$ is closed under multiplication. Therefore $\operatorname{im}\varphi$ is a subring of S.

For *(iv)*, let $a, b \in \ker\varphi$. Then $\varphi(a + b) = \varphi(a) + \varphi(b) = 0_S + 0_S = 0_S$ so $a + b \in \ker\varphi$, also $\varphi(-a) = -\varphi(a) = -0_S = 0_S$ so $-a \in \ker\varphi$, and finally $\varphi(ab) = \varphi(a)\varphi(b) = 0_S 0_S = 0_S$ so $\ker\varphi$ is subring of R.

For *(v)*, suppose R has unity and denote it 1_R. Once again, every element of $\operatorname{im}\varphi$ can be written as $\varphi(a)$ for some $a \in R$. Note that $\varphi(1_R a) = \varphi(1_R)\varphi(a) = \varphi(a)$ so $\varphi(1_R)$ is unity in the subring $\operatorname{im}\varphi$. □

Note that if R and S are rings with unity and $\varphi : R \to S$ is surjective then $\operatorname{im}\varphi = S$ and so $\varphi(1_R) = 1_S$.

7.6 Ring Extensions

To help increase the number of examples of rings we can pull from, we introduce the notion of ring extensions.

Definition 7.14 (Ring Extension)**.** Let R be a ring and $S \subseteq R$ a subring. Let $\alpha_i \in R$ for $i \in \{1, \ldots, n\}$ with $n \in \mathbb{N}$. Then the ring extension $S[\alpha_1, \ldots, \alpha_n]$ is the smallest ring containing S and $\{\alpha_1, \ldots, \alpha_n\}$.

Example 7.15. If we take the ring $\mathbb{R}$ and subring $\mathbb{Q}$ then we can define the ring extension $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} :\ a, b \in \mathbb{Q}\}$. Ring extensions of this kind are used often in number theory.

If we consider the ring $\mathbb{C}$ and the subring $\mathbb{Z}$ then we can define the ring extension $\mathbb{Z}[i] = \{a + bi :\ a, b \in \mathbb{Z},\ i^2 = -1\}$ which is the ring of Gaussian integers.

Polynomials can be thought of as a special case of a ring extension where the elements we extend the ring by are unknown. However, we can also use them to provide an alternative definition to ring extensions. That is, if we let R be a ring and $S \subseteq R$ a subring then, for $\alpha \in R$, the ring extension $S[\alpha] = \{p(\alpha) :\ p \in S[x]\}$.

Since polynomials were covered in detail in Algebra 3, we will not go over them extensively here but will return to them later.

8 Fields and Domains

8.1 Division Ring

We have seen that rings allow us to generalise the notion of being able to add and multiply but often we want to divide as well. If our ring contains units then there is some notion of dividing by them as we can multiply by their inverse. If we can do this to every non-zero element of our ring then we call it a division ring.

Definition 8.1 (Division Ring)**.** Let R be a ring with unity. We say R is a division ring if every non-zero element is a unit, that is $R = R^{\times} \cup \{0\}$.

Example 8.2. Consider the ring of invertible 2×2 matrices union the zero matrix. Since every non-zero element is invertible, this forms a divison ring.

Example 8.3 (Quaternions)**.** Consider the set $\mathbb{H} = \{a + bi + cj + dk : \; a, b, c, d \in \mathbb{R}, \, i^2 = j^2 = k^2 = ijk = -1\}$ with the usual notion of addition and multiplication. This is the ring of quaternions, the ring whose basis elements $(1, i, j, k)$ formed the group Q_8).

If we interpret the complex numbers as a two dimensional vector space with basis 1 and i, representing points in the plane we may be motivated to find something similar for three dimenisons, that is a way of intepreting points in 3D space such that we can multiply and divide any two points. It turns out this is not possible with a three dimensional vector space and four are required, giving rise to the quaternions.

The quaternions are non-commutative but form a division ring.

8.2 Fields

If we take this one step further, we generalise the divison rings we are most familiar with ($\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$) with the notion of a field.

Definition 8.4 (Field)**.** A field is a commutative division ring.

Example 8.5. Let $p \in \mathbb{N}$ be prime. Consider the set $\mathbb{F}_p = \{0, 1, \ldots, p - 1\}$ under modular multiplication and addition. Then this is a finite field of order p.

Whilst we have finite fields, it turns out that any finite division ring must be a field so there are no finite non-commutative division rings.

Definition 8.6 (Characterstic)**.** Let R be a ring with unity. The chartactersitic of R, written $\operatorname{char}(R)$ is the order of the multiplicative identity in the group $(R, +)$.

For instance, the characteristic of $\mathbb{R}$ is infinite and the characteristic of $\mathbb{F}_5$ is 5 since $1 + 1 + 1 + 1 + 1 = 0 \mod 5$.

We often like the categorise fields by their characteristic. For instance, recall in Algebra 3 we often required that we worked in a field where $2 \neq 0$, that is we required the characteristic of the field to be greater than 2.

Characteristics also narrow down the possible order of the field.

Theorem 8.7 (Order of a Finite Field)**.** *Let $\mathbb{F}$ be a finite field with $1 \neq 0$. Then there exists $p \in \mathbb{N}$ prime such that every non-zero element of $\mathbb{F}$ has additive order p. Moreover, $|\mathbb{F}| = p^n$ for some $n \in \mathbb{N}$.*

Proof. Consider the group $(\mathbb{F}, +)$. We first show that all non-zero elements of this group have the same order as 1. To do so, we define the group homomorphism $\varphi_a : \mathbb{F} \to \mathbb{F}$ where $\varphi(x) = ax$ for $a \in \mathbb{F}^\times$. Note that this homomorphism has an inverse, namely $\varphi_{a^{-1}}$, and thus φ_a is an isomorphism. Since isomorphisms preserve order, it follows that $\operatorname{ord}(\varphi_a(1)) = \operatorname{ord}(a) = \operatorname{ord}(1) = \operatorname{char} \mathbb{F}$. Since a is chosen arbitrarily, this is true for all non-zero elements of $\mathbb{F}$.

We now show that $\operatorname{char} \mathbb{F}$ is prime. Denote $|\mathbb{F}| = m$ and note that, since $1 \neq 0$, we have $m \geq 2$. Thus there exists some prime $p \in \mathbb{N}$ such that $p \mid m$ and so, by Cauchy's Theorem, $\mathbb{F}$ must have an element of order p. Since every non-zero element has the same order, this means they all have order p, in particular $\operatorname{ord}(1) = \operatorname{char}(\mathbb{F}) = p$.

We now claim m is a power of p. To see this, suppose there existed a prime $q \in \mathbb{N}$ with $q \neq p$ such that $q \mid m$. By the same argument as above, every element would have order q which is a contradiction. Hence p is the only prime dividing m and therefore $|\mathbb{F}| = p^n$ for some $n \in \mathbb{N}$. □

It turns out that the order of a finite field determines it uniquely, that is all finite fields of the same order are isomorphic. However, we will not prove this here.

Using some knowledge of number theory, we can also make quite a strong claim about subgroups of the group of units of a field.

Theorem 8.8 (Multiplicative Subgroups of Fields are Cyclic)**.** *Let $\mathbb{F}$ be a field. If H is a finite, multiplicative subgroup of $\mathbb{F}^\times$ then H is cyclic.*

Proof. Let $n = |H|$ and fix $d \in \mathbb{N}$ such that d divides n. Let H_d denote the set of elements of order d in H, that is $H_d = \{h \in H : \operatorname{ord}(h) = d\}$. Suppose H_d is non-empty and then let $y \in H_d$. Then $\langle y \rangle$ is a subset of $\{x \in H : x^d = 1\}$ and $|\langle y \rangle| = d$. However, recall from Algebra 3 that $x^d - 1$ has at most d roots in a field and thus $|\{x \in H : x^d = 1\} \leq d$. It therefore must be that $\langle y \rangle = \{x \in H : x^d = 1\}$ and so $H_d \subseteq \langle y \rangle$.

Now, recall the Euler totient function φ where, for $n \in \mathbb{N}$, we define $\varphi(n) = |\{k \in \mathbb{N} : k \leq n \gcd(k, n) = 1\}|$. Since every element of $\langle y \rangle$ is a power of y and, for $r \in \mathbb{N}$, we have $\operatorname{ord}(y^r) = \frac{d}{\gcd(d,r)}$. Generators of $\langle y \rangle$ are elements of order d and thus are of the form y^r where $\gcd(d, r) = 1$. Hence there must be $\varphi(d)$ generators of $\langle y \rangle$. These generators are the elements of H_d so $|H_d| = \varphi(d)$.

Now consider all $d \in \mathbb{N}$ such that d divides n. Then either $|H_d| = 0$ or $|H_d| = \varphi(d)$ so

$$|H| = \sum_{d|n} |H_d| \leq \sum_{d|n} \varphi(d).$$

However, recall (from Number Theory) that $\sum_{d|n} \varphi(d) = n$ and so $|H_d|$ must equal $\varphi(d)$ for all d dividing n. In particular, this means $|H_n| = \varphi(n) \geq 1$ so there exists an element of H with order n. This element then generates H and so H is cyclic. □

8.3 Integral Domains

Clearly, the integers are not a field as the only units are ± 1 and thus we have no notion of division. Despite this, we are still able to simplify equations like $2x = 2y$ or $10x = 25y + 5$ where we seem to divide by an integer. An integral domain (often just called a domain) generalises the properties required to perform this kind of cancellation.

Definition 8.9 (Integral Domain)**.** An integral domain is a commutative ring with unity in which there are no non-zero zero divisors.

Since every non-zero element of a field is a unit and units are not zero divisors, every field is necessarily an integral domain. However so are rings like $\mathbb{Z}$ and polynomials with coefficients in a field.

Proposition 8.10 (Cancellation Law)**.** *Let R be a ring and $a, b, c \in R$ with a not a zero divisor. If $ab = ac$ then $b = c$. Similarly, if $ba = ca$ then $b = c$.*

Proof. Since $ab = ac$ we have that $ab - ac = 0$ and thus $a(b - c) = 0$. However, a is not a zero divisor so $b - c = 0$ and therefore $b = c$. A similar argument holds for the case when $ba = ca$. □

From this, we can see that in an integral domain we can always apply the cancellation law. In fact, the reverse implication also holds.

Theorem 8.11 (Integral Domain Criterion)**.** *Let R be a commutative ring with unity. Then R is an integral domain if and only if, for all $a, b, c \in R$ with $a \neq 0$, whenever $ab = ac$ we have $b = c$.*

Proof. We first assume R is a domain. For $a \in R$, if $a \neq 0$ then a is not a zero-divisor and thus, by Proposition 8.10, $ab = ac$ implies $b = c$ for all $b, c \in R$.

We now assume that, for all $a, b, c \in R$ with $a \neq 0$, we have that $ab = ac$ implies $b = c$. Suppose there exists some $r \in R$ such that $ar = 0$. Then note $a0 = ar = 0$ so, by cancellation, $r = 0$ and thus a is not a zero-divisor. Therefore all non-zero elements of R are not zero divisors and thus R is a domain. □

8.4 Connections Between Domains and Fields

Similar to how all finite division rings are fields, all finite integral domains are fields too.

Proposition 8.12 (Finite Domains are Fields)**.** *Every finite integral domain is a field.*

Proof. Let $R = \{r_1, \dots, r_n\}$ for some $n \in \mathbb{N}$ be a finite domain and let $a \in R$ with $a \neq 0$. We want to show that a is a unit. Take $aR = \{ar_1, \dots, ar_n\}$ and note that, by the cancellation law, for all $i, j \in \{1, \dots, n\}$ with $i \neq j$ we have that $ar_i \neq ar_j$ (as this would imply $r_i = r_j$ which is false). Thus $|aR| = |R|$, implying $aR = R$ since $aR \subseteq R$. So there must exist $i \in \{1, \dots, n\}$ such that $ar_i = 1$, meaning $r_i = a^{-1}$ and a is a unit. Thus R is commutative with all non-zero elements a unit and therefore R is a field. □

Now consider an integral domain which contains a field as a subring, for instance $\mathbb{C}$ contains $\mathbb{R}$ as a subring or the set $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$, which we have seen in Number Theory, that contains $\mathbb{Q}$ as a subring. Note that we can think of each of these as somewhat like a vector space, taking a basis to be $\{1, i\}$ or $\{1, \sqrt{2}\}$ respectively. In turns out that these integral domains are indeed vector spaces and that this holds for any ring containg a field as a subring. Moreover, if this vector space is finite dimensional (as it is in these two cases) it turns out that the integral domain is in fact a field.

Proposition 8.13. *Let R be an integral domain containg a field, $\mathbb{F}$, as a subring. Then R is a vector space over $\mathbb{F}$. Moreover, if $\dim(R)$ is finite then R is a field.*

Proof. To first show that R is a vector space, we recall that a vector space must be an abelian group under addition and must be closed under multiplication by a scalr from the field. Clearly this is the case and all other restrictions on scalar multiplication are satisfied by $\mathbb{F}$ being a subring of R. Thus R is a vector space over $\mathbb{F}$.

Now suppose $\dim(R)$ is finite and let $a \in R$ be such that $a \neq 0$. We want to show that a is a unit, we do so by showing multiplication by a is surjective. Define $\varphi : R \to R$ by $\varphi : r \mapsto ar$. Then for all $r, s \in R$ and $\lambda \in \mathbb{F}$ note that $\varphi(r + \lambda s) = a(r + \lambda s) = ar + a\lambda s = ar + \lambda as = \varphi(r) + \lambda\varphi(s)$. Thus φ is a linear map. Since a is not a zero-divisor (as R is a domain) we have that $\ker \varphi = \{0\}$. By the rank-nullity theorem, this implies $\dim(\operatorname{im} \varphi) = \dim R$. So, since $\operatorname{im} \varphi$ is a subspace of R, it must be that $\operatorname{im} \varphi = R$ and thus φ is surjective. Hence there exists $b \in R$ such that $\varphi(b) = ab = 1$. Therefore a is a unit and so R is a field. □

Example 8.14. We will show $\mathbb{Q}(\sqrt{2})$ is a field.

Clearly $\mathbb{Q}$ is a subring and, since $\mathbb{Q}$ is a field, this means $\mathbb{Q}(\sqrt{2})$ is a vector space. By definition, every element of $\mathbb{Q}(\sqrt{2})$ is a linear combination of 1 and $\sqrt{2}$. Since $\sqrt{2}$ is irrational, clearly 1 and $\sqrt{2}$ are linearly independent and thus $\{1, \sqrt{2}\}$ forms a basis of $\mathbb{Q}(\sqrt{2})$. Therefore $\mathbb{Q}\sqrt{2}$ is finite dimensional and hence must be a field.

9 Ideals

9.1 Definition

When developing an understanding of groups, normal subgroups played a key part. Recall that normal subgroups were kernels of group homomorphisms and allowed us to construct quotient groups. The ring analogue of this is an ideal.

Definition 9.1 (Ideal)**.** Let R be a ring. An ideal $I \subseteq R$ is a subring such that, for all $x \in I$ and all $r \in R$, $rx, xr \in I$

As rings try to generalise the notion of an integer, one way of thinking about ideals is as a generalisation of sets of multiples of an integer.

Example 9.2. In $\mathbb{Z}$, multiples of $n \in \mathbb{Z}$, denoted $n\mathbb{Z}$ are ideals. To see this, let $a \in n\mathbb{Z}$ then $a = nk$ for some $k \in \mathbb{Z}$. If we let $b \in \mathbb{Z}$ then $ab = nbk$ so $ab \in n\mathbb{Z}$.

In fact, these are the only ideals of $\mathbb{Z}$. This is because $(\mathbb{Z}, +)$ is a cyclic group generated by 1 so any subgroup of $(\mathbb{Z}, +)$ must be cyclic and hence generated by an element of $\mathbb{Z}$. However, the group $\langle n \rangle$ is exactly $n\mathbb{Z}$. Since all ideals are rings and hence are additive subgroups, this shows all ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$.

Proposition 9.3. *Let R be a ring with unity and $I \subseteq R$ an ideal. If I contains a unit then $I = R$.*

Proof. Let $u \in I$ be a unit. Then there exists $u^{-1} \in R$ such that $uu^{-1} = 1$ but, since $u \in I$, this must mean $1 \in I$. Now let $r \in R$. Then $r1 = r \in I$ so $R \subseteq I$ but this must mean $I = R$. □

We can equivalently define an ideal as a kernel of a homomorphism but to show these two ideas are equivalent, we first need to develop the idea of quotient rings.

9.2 Quotient Rings

Proposition 9.4 (Quotient Ring)**.** *Let R be a ring and $I \subseteq R$ and ideal. Then the set $R/I = \{r + I : r \in R\}$ is a ring with operations $(a + I) + (b + I) = (a + b) + I$ and $(a + I)(b + I) = ab + I$. We call this ring a quotient ring.*

Proof. The closure and well-definedness of addition follows from the definition of a quotient group.

To prove multiplication is well-defined, suppose $a_1 + I = a_2 + I$ and $b_1 + I = b_2 + I$ for $a_1, a_2, b_1, b_2 \in R$. Recall that this means $a_1 - a_2, b_1 - b_2 \in I$.

Write $a_1b_1 - a_2b_2 = a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2 = a_1(b_1 - b_2) + (a_1 - a_2)b_2$. Since $b_1 - b_2$ and $a_1 - a_2$ are in I, $a_1(b_1 - b_2 + b_2(a_1 - a_2) \in I$ and so $a_1b - 1 - a_2b_2 \in I$. Thus $a_1b_1 + I = a_2b_2 + I$ and so multiplication is well-defined.

Associativy and distributivity is inherited from R. □

We are now able to show that kernels and ideals are one and the same.

Proposition 9.5. *Let R be a ring and $I \subseteq R$. Then I is an ideal if and only if there exists some homomorphism from R of which I is the kernel.*

Proof. We first show that if I is a kernel then it is an ideal. Let φ be a ring homomorphism from R such that $I = \ker \varphi$. Then let $x \in I$ and $r \in R$. See that $\varphi(xr) = \varphi(x)\varphi(r)\varphi(x)0 = 0$ and similarly for $\varphi(rx)$. Thus $xr, rx \in I$ and, since kernels are subrings, I is an ideal.

Now we assume I is an ideal. Consider the homomorphism $\varphi : R \to R/I$ given by $\varphi : r \mapsto r + I$. Then $\varphi(r) = I$ if and only if $r \in I$ so $\ker \varphi = I$. □

9.3 Principal Ideals

Recall that all the ideals of $\mathbb{Z}$ were multiples of some integer. To generalise this idea, we introduce the notion of a generated ideal.

Definition 9.6 (Generated Ideal)**.** Let R be a commutative ring with unity and $a_1, \ldots, a_n \in R$ for some $n \in \mathbb{N}$. The ideal generated by $\{a_1, \ldots, a_n\}$ is the set $\{r_1a_1 + \cdots + r_na_n : r_i \in R \text{for all} i \in \{1, \ldots, n\}\}$. We denote it $(a_1, \ldots, a_n)$.

Proposition 9.7. *Generated ideals are ideals.*

Proof. Let R be a commutative ring with unity and $a_1, \ldots, a_n \in R$ for some $n \in \mathbb{N}$. Denote $A = (a_1, \ldots, a_n)$.

Clearly $0 \in A$ and A is closed under inverses. Let $x, y \in A$. Then for some $\lambda_i, \mu_i \in R$ for $i \in \{1, \ldots, n\}$ we can write $x = \sum_{i=1}^n \lambda_i a_i$ and $y = \sum_{i=1}^n \mu_i a_i$. So $x + y = \sum_{i=1}^n (\lambda_i + \mu_u) a_i \in A$ and thus A is closed under addition. Now, let $r \in R$ and see that $xr = rx = \sum_{i=1}^n (\lambda_i r) a_i \in A$ since R is commutative. Since this holds for all r, this shows that A is both closed under multiplication (so is a subring) and is an ideal. □

The reason we need to consider commutative rings with unity is that the more general definition of an ideal generated by a set A is the interesection of all ideals containing A. Practically, this is quite difficult to work with but is equivalent to the definition given above when considering commutative rings with unity.

Definition 9.8 (Principal Ideal)**.** Let R be a commutative ring with unity and $I \subseteq R$ an ideal. We say I is a principal ideal if there exists $p \in R$ such that $I = (p)$.

Clearly, the ideals of $\mathbb{Z}$ are all principal ideals as they are all multiples of some integer. When this is the case, we call the ring a principal ideal domain.

Definition 9.9 (Principal Ideal Domain)**.** Let R be a domain. We say R is a principal ideal domain (PID) if every ideal in R is a principal ideal.

Example 9.10. If we let $\mathbb{F}$ be a field the $\mathbb{F}[x]$ is a PID.

To see this, consider an ideal $I \subseteq \mathbb{F}[x]$. Let $a \in I$ be a non-zero polynomial of smallest possible degree and let $p \in I$. By Euclidean divison, there exists $q, r \in \mathbb{F}[x]$ with $\deg r < \deg a$ such that $p = aq + r$. Then $r = p - aq \in I$. However, $\deg r < \deg a$ so $r = 0$ as a was chosen to be of least possible degree. Thus $p = aq \in (a)$ so $I \subseteq (a)$. Since $a \in I$ this must mean $I = (a)$ so I is a principal ideal.

9.4 1st Isomorphism Theorem

One useful application of ideals and quotient rings is using them to generate new rings from ones we already know.

Theorem 9.11 (1st Isomorphism Theorem for Rings)**.** *Let R and S be rings and $\varphi : R \to S$ a ring homomorphism. Then $R/\ker\varphi \cong \operatorname{im}\varphi$.*

Proof. Let $\psi : R/\ker\varphi \to \operatorname{im}\varphi$ be given by $\psi : a + \ker\varphi \mapsto \varphi(a)$. Clearly $\psi(\ker\varphi) = \varphi(0) = 0$. Let $a + \ker\varphi, b + \ker\varphi \in R/\ker\varphi$. Then $\psi((a + \ker\varphi) + (b + \ker\varphi)) = \psi((a + b) + \ker\varphi) = \varphi(a + b) = \varphi(a) + \varphi(b)$. Also $\psi(a + \ker\varphi) + \psi(b + \ker\varphi) = \varphi(a) + \varphi(b)$. So ψ is additive. Note $\psi((a + \ker\varphi)(b + \ker\varphi)) = \psi(ab + \ker\phi) = \varphi(ab) = \varphi(a)\varphi(b)$ and also $\psi(a + \ker\varphi)\psi(b + \ker\varphi) = \varphi(a)\varphi(b)$. So ψ is a ring homomorphism.

Now suppose $a + \ker\varphi$ is such that $\psi(a + \ker\varphi) = 0$. Then $\varphi(a) = 0$ so $a \in \ker\varphi$ and $a + \ker\varphi = \ker\varphi$. Thus $\ker\psi$ is trivial and so ψ is injective. Let $c \in \operatorname{im}\varphi$, then there exists $d \in R$ such that $\varphi(d) = c$. Thus $\psi(d + \ker\varphi) = c$ so ψ is surjective. Therefore ψ is an isomorphism and $R/\ker\varphi \cong \operatorname{im}\varphi$. □

Example 9.12 (Complex Numbers)**.** Let $\phi : \mathbb{R}[x] \to \mathbb{C}$ be such that $\phi : p \mapsto p(i)$ where $i^2 = -1$. Then $\ker\varphi = (x^2 + 1)$ and $\operatorname{im}\varphi = \mathbb{C}$ since $a + ib = \varphi(a + bx)$ for all $a, b \in \mathbb{R}$. So $\mathbb{R}[x]/(x^2 + 1) = \mathbb{C}$.

Example 9.13 (Quadratic Rings)**.** Let $\varphi : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{2})$ be given by $\varphi : p \mapsto p(\sqrt{2})$. Then $\ker \varphi = (x^2 - 2)$ and $\operatorname{im} \varphi = \mathbb{Q}(\sqrt{2}$ since $a + b\sqrt{2} = \varphi(a + b\sqrt{2})$ for all $a, b \in \mathbb{Q}$. So $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$.

We will see more examples of generating rings like this later.

10 Prime and Maximal Ideals

10.1 Definition and Examples

A prime ideal mimics the notion of prime numbers. The idea is that if two elements are not in a prime ideal then they're product can't be (similar to how the product of two integers can't have a prime divisor that neither of the original integers had). A maximal ideal mimics the other key aspect of prime numbers, what we more generally call irreducibility. The idea is that a maximal ideal should not be contained in any other ideal, similar to how multiples of a prime aren't all multiples of something else compared to how all multiples of, say, 6 are also all multiples of 3 and 2.

Definition 10.1 (Prime Ideal)**.** Let R be a ring and I a proper ideal of R. We say I is a prime ideal if whenever $ab \in I$, for some $a, b \in R$, then at least one of a or b is in I

Definition 10.2 (Maximal Ideal)**.** Let R be a ring and I a proper ideal of R. We say I is a maximal ideal if any ideal that properly contains I is the whole ring.

Example 10.3 (Prime Ideals)**.** Let $p \in \mathbb{Z}$ be prime. Them (p) is a prime ideal, as we should expect.

The ideal $\{0\}$ is a prime ideal in any integral domain.

The ideal $(x - 3)$ is prime in $\mathbb{R}[x]$. The notion of a prime ideal generalises the other notions of being prime that we've encountered.

In $\mathbb{Z}[x]$, the ideal (p, x) with $p \in \mathbb{Z}$ prime is prime. Think of elements in (p, x) as polynomials with constant terms that are multiples of p. This is then covered by the case of (p) in $\mathbb{Z}$.

Example 10.4 (Maximal ideals)**.** In $\mathbb{Z}$, prime ideals are maximal ideals (we will see that this is true in general for PIDs). For instance, (2) contains all even numbers, any ideal that contains all even numbers has to be (2) or $\mathbb{Z}$ itself.

10.2 Quotients of Prime and Maximal Ideals

Since prime ideals are those in which if two elements aren't in their ideal, their product isn't either, then sending this ideal to zero (that is quotienting by it) will mean we can't mutliply two non-zero elements of the ring and end up with zero. This is the idea behind an integral domain.

Proposition 10.5 (Quotient of Prime Ideals)**.** *Let R be a commutative ring with unity and I a proper ideal of R. Then I is a prime ideal if and only if R/I is an integral domain.*

Proof. We first suppose I is a prime ideal. Let $a + I \in R/I$ such that $a + I \neq 0 + I$ (that is $a \notin I$) and let $b + I \in R/I$ be such that $(a + I)(b + I) = 0 + I$. Then $ab + I = 0 + I$, that is $ab \in I$. Since I is prime, this means at least one of a or b is in I but we assumed a wasn't so $b \in I$, or, equivalently, $b + I = 0 + I$. Thus $a + I$ is not a zero-divisor and therefore R/I is an integral domain.

Now suppose R/I is an integral domain. Let $a, b \in R$ such that $ab + I = 0 + I$. Then $ab \in I$. However, we can also write $(a + I)(b + I) = ab + I = 0 + I$ and, since R/I is an integral domain, this means at least one of $a + I$ or $b + I$ is $0 + I$. That is, either $a \in I$ or $b \in I$. Thus I is a prime ideal. □

If we start with a commutative ring with unity and quotient out a maximal ideal then it would follow that we have no proper, non-trivial ideals left. Thus, the ideal generated by each non-zero element in the quotient ring must be the whole ring and hence will contain unity meaning every non-zero element must have an inverse. This is the idea behind a field.

Proposition 10.6 (Quotient of Maximal Ideals)**.** *Let R be a commutative ring with unity and I a proper ideal of R. Then I is a maximal ideal if and only if R/I is a field.*

Proof. Suppose I is a maximal ideal and let $a + I \in R/I$ be such that $a + I \neq 0 + I$ (that is $a \notin I$). Let $(a) + I = \{ar + x : r \in R, x \in I\}$. This is an ideal properly containing I but I is maximal so $(a) + I = R$. Thus $1 \in (a) + I$ but $I \neq R$ so $1 \in (a)$. So there is some $r \in R$ such that $ar = 1$, meaning $(a + I)(r + I) = 1 + I$ and hence $a + I$ is a unit. Therefore R/I is a field.

Now suppose R/I is a field. Let J be an ideal of R such that $I \subsetneq J$, meaning there exists some $r \in J - I$. Since I is a field, there exists some $s + I \in R/I$ such that $(r + I)(s + I) = rs + I = 1 + I$. So $rs - 1 \in I \subsetneq J$ and since $rs \in J$ it must be that $1 \in J$. So J contains unity and hence $J = R$. Therefore I is maximal. □

Note that if R is a commutative ring with unity and I is a maximal ideal the R/I is a field by the above. However, fields are integral domains meaning that I must also be prime. This, in a commutative ring with unity, every maximal ideal is prime.

10.3 Prime and Irreducible Elements

Recall the following definitions.

Definition 10.7 (Prime Element)**.** Let R be a ring with unity and $p \in R$ a non-zero non-unit. We say p is prime if, whenever p divides ab for some $a, b \in R$ we have that p divides at least one of a or b.

Definition 10.8 (Irreducible Element)**.** Let R be a ring with unity and $p \in R$ with $p \neq 1$. We say p is irreducible if whenever $ab = p$ for some $a, b \in R$ then one of a or b is a unit.

Since our motivation for prime and maximal rings was based on the ideas of prime and irreducible elements, it should make sense there are links between the two ideas. For instance, in a commutative ring with unity, a non-trivial principal ideal is prime if and only if it is generated by a prime element. This follows clearly from the definition. We explore some more links between prime and irreducible elements and ideals below.

Proposition 10.9. *If R is a domain then any prime element is irreducible.*

Proof. Suppose p is a prime element of R. Assume $p = ab$ for some $a, b \in R$ where a is not a unit. Since $p \mid ab$, either $p \mid a$ or $p \mid b$ but the latter would imply a is a unit so $p \mid a$. Thus $a = pc$ for some $c \in R$. We can then write $p = pcb$ which cancels to $cb = 1$. Therefore b is a unit and so p is irreducible. □

Proposition 10.10. *Let R be a PID and $p \in R$ a non-zero non-unit. Then the following are equivalent:*

(i) p is prime.

(ii) p is irreducible.

(iii) (p) is maximal.

(iv) (p) is prime.

Proof. We have already shown *(i)* $\implies$ *(ii)*, *(iii)* $\implies$ *(iv)* and *(i)* $\iff$ *(iv)* so we only need to prove *(ii)* $\implies$ *(iii)*.

Suppose $p \in R$ is irreducible. Let J be an ideal of R with $(p) \subsetneq J$. Since we have a PID, $J = (m)$ for some $m \in R$, so $p \in (m)$ and hence $p = rm$ for some $r \in R$. However, p is irreducible so one of r or m is a unit. If r is a unit, $m = r^{-1}p$ so $m \in (p)$, a contradiction. So m must be a unit, then $(m) = R$. Therefore (p) is maximal. □

11 Irreducible Polynomials and Finite Fields

11.1 Motivation

Recall Example 9.12 and Example 9.13 that we constructed fields by taking the quotient of a polynomial ring by the ideal generated by an irreducible polynomial. We showed that this works in general in Proposition 10.6.

The reason we are particularly concerned with doing this with polynomial rings is that irreducible polynomials are those that do not have roots in the field we are working in. However, if we quotient by one of these polynomials, we 'add in' the missing root to the field. That's why $\mathbb{R}[x]/(x^2 + 1)$ gave us the complex numbers.

To use this to generate more fields of use, we will first develop a few tools to help us identify when polynomials are irreducible.

11.2 Polynomials Over Finite Fields

Recall that irreducible polynomials do not have roots in the field we are working in. In a finite field, it is often easy to check if a quadratic is irreducible as we can simply evaluate it at each point in the field and see if it has a root.

Example 11.1. The polynomial $p(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_2$.

To see this, simply note $p(0) = 1$ and $p(1) = 1$ so $p(x)$ has no roots in $\mathbb{F}_2$.

Note that not having roots does not necessarily imply irreduciblity. If we consider $q(x) = (x^2 + x + 1)^2$, the above tells us q has no roots but it is clearly still reducible.

11.3 Polynomials Over Real and Complex Numbers

In these cases we can simply recall facts from Algebra 3.

We know $\mathbb{C}$ is algebraically closed and so every non-constant polynomial has a root. Therefore the only irreducible polynomials are linear.

In $\mathbb{R}[x]$, we know any polynomial with degree greater than 2 is reducible and so the only irreducible polynomials are linear or quadratic with no real roots.

We now move on to the more difficult case of considering polynomials over $\mathbb{Q}$.

11.4 Primitive Polynomials

To help us deduce when polynomials in $\mathbb{Q}[x]$ are irreducible we try and make it into a problem of finding a factorisation over $\mathbb{Z}$. Therefore it makes sense to first consider when factoring over $\mathbb{Z}$ is possible.

Definition 11.2 (Content)**.** Let $a(x) = a_0 + \cdots + a_n x^n \in \mathbb{Z}[x]$. We define the content of a to be $C(a) = \gcd(a_0, \ldots, a_n)$.

Definition 11.3 (Primitive)**.** We say $a \in \mathbb{Z}[x]$ is primitive if $C(a) = 1$.

In general, for all $f \in \mathbb{Z}[x]$, there exists a primitive polynomial $g \in \mathbb{Z}[x]$ such that $f = C(f)g$. Also, note that monic polynomials are always primitive.

Definition 11.4 (Proper Factorisation)**.** Given $f \in \mathbb{Z}[x]$ non-constant, if there exist $g, h \in \mathbb{Z}[x]$ which are non-constant such that $f = gh$ then we say f has a proper factorisation.

Proposition 11.5. *If $f \in \mathbb{Z}[x]$ is primitive then f is irreducible if and only if it has no proper factorisation in $\mathbb{Z}[x]$.*

Proof. Suppose $f \in \mathbb{Z}[x]$ is irreducible. Then whenever $f = gh$, for some $g, h \in \mathbb{Z}[x]$, one of g or h is a unit, that is, g or h is ± 1. Thus f has no proper factorisation.

Now suppose f has no proper factorisation. So whenever $f = gh$, for $g, h \in \mathbb{Z}[x]$, then one of g or h is constant. Since f is primitive, this constant must be ± 1 and therefore f is irreducible. □

11.5 Gauss's Lemma

Gauss's Lemma allows us to transfer the notion of irreducibility over $\mathbb{Z}$ to $\mathbb{Q}$.

Lemma 11.6 (Gauss's Lemma)**.** *The product of two primitive polynomials is primitive.*

Proof. Let f and g be primitive polynomials in $\mathbb{Z}[x]$. Aiming for a contradiction, assume there exists $p \in \mathbb{Z}$ prime such that p divides fg. See that, since every integer not equal to ± 1 is a product of primes, this is in fact enough to assume the converse. Then $fg \in (p)$. Note, however, that (p) is a prime ideal (since p is prime) and so one of f or g is in (p). However these are primitive so this is a contradiction. Therefore fg is primitive □

Theorem 11.7 (Irreducibility Over $\mathbb{Q}$ is Irreducibility Over $\mathbb{Z}$)**.** *Let $f \in \mathbb{Z}$ be primitive. Then f is irreducible in $\mathbb{Z}[x]$ if and only if f is irreducible in $\mathbb{Q}[x]$.*

Proof. Suppose that f is not irreducible in $\mathbb{Z}[x]$. Then f has a proper factorisation in $\mathbb{Z}[x]$ and hence f is not irreducible in $\mathbb{Q}[x]$. Thus irreducible in $\mathbb{Q}[x]$ implies irreducible in $\mathbb{Z}[x]$ by the contrapositive.

Now suppose f is not irreducible in $\mathbb{Q}[x]$. Then there are $a, b \in \mathbb{Q}[x]$ non-units such that $f = ab$. In particular, $\deg a, \deg b \geq 1$. Let n be the product of all denominators of coefficients of a and b. Then $nf = gh$ for some $g, h \in \mathbb{Z}[x]$ with $\deg a = \deg g$ and $\deg b = \deg h$. So $nf = C(g)C(h)g_1h_1$ where $g = C(g)g_1$ and $h = C(h)h_1$ with g_1 and h_1 primitives. Thus $nC(f) = C(g)C(h)C(g_1h_1)$ which implies $n = C(g)C(h)$ since f, g_1 and h_1 are primitive and hence so is g_1h_1 by Lemma 11.6. Therefore $f = g_1h_1$ is a proper factorisation over $\mathbb{Z}[x]$. Thus irreducible in $\mathbb{Q}[x]$ implies irreducible in $\mathbb{Z}[x]$ by the contrapositive. □

11.6 Eisenstein's Criterion

Now we know that we can easily check if a polynomial in $\mathbb{Q}[x]$ is irreducible by mutliplying it by some integer that makes it a polynomial in $\mathbb{Z}[x]$ and seeing if it is irreducible over $\mathbb{Z}$. The question then is how to easily check when a polynomial is irreducible over the integers. The answer is Eisenstein's Criterion.

Theorem 11.8 (Eisenstein's Criterion)**.** *Let $f(x) = a_0 + \ldots + a_nx^n \in \mathbb{Z}[x]$ where $n = \deg f$ with $n \geq 1$. Suppose there exists $p \in \mathbb{Z}$ prime such that $p \mid a_i$ for all $i \in \{0, 1, \ldots, n-1\}$; $p \nmid a_n$; and $p^2 \nmid a_0$. Then f has no proper factorisation in $\mathbb{Z}[x]$ and hence is irreducible in $\mathbb{Q}[x]$.*

Proof. Aiming for a contradiction, we assume f does have a proper factorisation. Then there exists some $g, h \in \mathbb{Z}[x]$ such that $f = gh$ where $\deg g = m$, $\deg h = k < n$. Write $g(x) = b_0 + \ldots + b_mx^m$ and $h(x) = c_0 + \ldots + c_kx^k$. Since $p \mid a_0$ and $p^2 \nmid a_0$, writing $a_0 = b_0c_0$ tells us that exactly one of b_0 or c_0 is divisible by p. Without loss of generality, assume that $p \mid b_0$ and $p \nmid c_0$. Additionally, since $p \nmid a_n$ and $a_n = b_nc_n$, we know $p \nmid b_m$. Let $r \in \{0, \ldots, m\}$ be the smallest integer such that $p \nmid b_r$. Expanding out the product, we find $a_r = b_0c_r + b_1c_{r-1} + \ldots + b_rc_0$. Note that all of these terms are divisible by p except for b_rc_0. Thus $p \nmid a_r$ but, since $r < n$, this is a contradiction. Therefore f has no proper factorisation in $\mathbb{Z}[x]$ and hence is irreducible in $\mathbb{Q}[x]$. □

Example 11.9. If we let $f(x) = 3x^4 + 15x^2 + 10x \in \mathbb{Q}[x]$ then we can apply Eisenstein's criterion with $p = 5$ to see f has no proper factorisation over $\mathbb{Z}$ and therefore is irreducible over $\mathbb{Q}$.

Let $f(x) = x^4 + 1 \in \mathbb{Q}[x]$. We can't immediately apply Eisenstein's criterion but if we let $g(x) = f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$ we can apply Eisenstein's criterion to g with $p = 2$ and see g is irreducible. Since f not being irreducible would imply g is not irreducible, this must mean f is irreducible.

Example 11.10 (Cyclotomic Polynomials)**.** Let $\Phi_n(x)$ denote the nth cyclotomic polynomial, that is the monic polynomial with degree $\varphi(n)$ (the Euler totient of n) whose roots are the primitive nth roots of unity.

If $p \in \mathbb{Z}$ is prime then $\Phi_p(x) = x^{p-1} + \ldots + x + 1$ is irreducible in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

To see this, recall $x^p - 1 = (x-1)\Phi_p(x)$. We can substitute $x \mapsto x+1$ to get $(x+1)^p - 1 = x\Phi_p(x+1)$ and then, by the binomial expansion, we get

$$\begin{aligned}\Phi_p(x+1) &= \frac{1}{x}\sum_{r=1}^{p}\binom{p}{r}x^r \\ &= x^{p-1} + \sum_{r=1}^{p-1}\binom{p}{r}x^{r-1}.\end{aligned}$$

Note that, for $r \in \{1, \ldots, p-1\}$, we have $p \mid \binom{p}{r}$. Furthermore $p^2 \nmid \binom{p}{1} = p$ and $p \nmid 1$. So, by Eisenstein's criterion, $\Phi_p(x+1)$ has no proper factorisation in $\mathbb{Z}[x]$ and, since it is primitive, irreducible in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. The same applies to $\Phi_p(x)$

Before we look at taking the quotient of irreducibles in $\mathbb{Q}[x]$, we will explore the concept in finite fields.

11.7 Finite Fields

Recall that $x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$ (see Example 11.1). Therefore $(x^2 + x + 1)$ is a maximal ideal and so $\mathbb{F}_2/(x^2 + x + 1) = F$ is a field. Let us denote $a + (x^2 + x + 1) \in F$ by $\overline{a}$. Then we can use Euclid's algorithm to write $a(x) = (x^2 + x + 1)p(x) + r(x)$ for some $q, r \in \mathbb{F}_2[x]$ with $\deg r < 2$, that is with r linear. Now since $(x^2 + x + 1)$ is an ideal, $(x^2 + x + 1)p(x) \in (x^2 + x + 1)$ so $a + (x^2 + x + 1) = r + (x^2 + x + 1)$. Thus $\overline{a} = \overline{r}$ and so each coset in F has a linear representative. Since we are in $\mathbb{F}_2$, the only linear polynomials are 0, 1, x and $x + 1$. So $F = \{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\}$. We have therefore constructed a finite field with four elements, that is $F \cong \mathbb{F}_4$.

If we consider $\overline{x}$ in particular note that it represents the coset $x + (x^2 + x + 1)$ and so $\overline{x}^2 = x^2 + (x^2 + x + 1)$ but this must have a linear representative. Note that we can write $x^2 = x^2 + x + 1 + x + 1$ so $\overline{x^2} = \overline{x+1}$. Also note $\overline{x} + \overline{1} = \overline{x+1}$ and so $\overline{x}^2 + \overline{x} + \overline{1} = 2\overline{x+1} = 0$ (since $2 = 0$). Therefore $\overline{x}$ is a root of $x^2 + x + 1$.

We can therefore write F as the set $\{x + y\alpha :\ x, y \in \mathbb{F}_2,\ \alpha^2 + \alpha + 1 = 0\}$.

More generally if we let $p \in \mathbb{Z}$ be prime and consider an irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree n then $\mathbb{F}_p/(f)$ is a finite field of order p^n and we can write it in the form $\mathbb{F}_p/(f) \cong \{x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} :\ x_0, \ldots, x_{n-1} \in \mathbb{F}_p,\ f(\alpha) = 0\}$.

11.8 Extending Rationals

We can do the same process with rational polynomials. Recall, from Example 11.9, that $x^4 + 1$ is irreducible over $\mathbb{Q}$ and so, by a similar argument as above, we can take the quotient ring $\mathbb{Q}[x]/(x^4 + 1) \cong \{a + b\alpha + c\alpha^2 + d\alpha^3 :\ a, b, c, d \in \mathbb{Q},\ \alpha^4 = -1\}$.

11.9 Links to Galois Theory

If we extend a field by quotienting out a maximal ideal we can consider maps which fix the original field but alter the 'added' elements. For example, if we took $F = \mathbb{F}_2/(x^2 + x + 1) \cong \{x + y\alpha :\ x, y \in \mathbb{F}_2\, \alpha^2 = \alpha + 1\}$ we could consider automorphisms $\varphi : F \to F$ such that $\varphi(x) = x$ for all $x \in \mathbb{F}_2$.

We have already seen such a map before. Consider $\mathbb{R}[x]/(x^2+1) \cong \{x + yi : \; x, y \in \mathbb{R}, \, i^2 = -1\} \cong \mathbb{C}$ and the map $\varphi : \mathbb{C} \to \mathbb{C}$ where $\varphi(x + iy) = x - iy$. This is the conjugation map and, as we have seen from complex analysis, such a map preserves much of the structure of the field.

Galois Theory generalises this idea and studies these kinds of maps over more general field extensions. Doing so allows us to turn many questions abour fields into questions about this group of automorphisms. This makes problems such as proving no quintic equation exists possible.