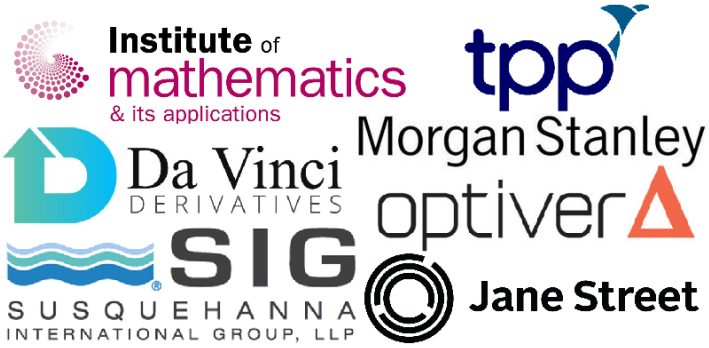
WMS



MA249

Algebra II: Groups and Rings Revision Guide

Written by David McCormick

Contents

1 Groups, Subgroups and Isomorphisms **1**
1.1 Basic Definitions . . . 1
1.2 Subgroups and Direct Products . . . 2
1.3 Isomorphisms . . . 2
1.4 Generators and Relations . . . 3
1.5 Classification of Finite Groups . . . 4

2 Cosets, Quotients Groups and Homomorphisms **4**
2.1 Cosets and Lagrange's Theorem . . . 5
2.2 Quotient Groups and Normal Subgroups . . . 6
2.3 Homomorphisms . . . 7

3 Group Actions and Conjugacy **8**
3.1 Orbits and Stabilizers . . . 8
3.2 Conjugacy . . . 8
3.3 Sylow's Theorems . . . 9

4 Rings, Ideals and Ring Homomorphisms **9**
4.1 Basic Definitions . . . 9
4.2 Subrings and Direct Products . . . 10
4.3 Ideals . . . 10
4.4 Ring Homomorphisms . . . 11
4.5 Quotient Rings and the Isomorphism Theorems . . . 11

5 Domains, Divisibility and Factorisation **12**
5.1 Domains . . . 12
5.2 Divisibility . . . 13
5.3 Examples of Domains . . . 14
5.4 Polynomial Rings . . . 15

DON'T PANIC

Introduction

This revision guide for MA249 Algebra II: Groups and Rings has been designed as an aid to revision, not a substitute for it. Algebra II is a hard module, perhaps harder than you think; success in the exam will require a lot of hard work and a little luck. This revision guide contains almost no proofs, simply for lack of space; most of the proofs are short and sweet and (more importantly) examinable. But with this all said, do not be put off: Algebra II covers a lot of fascinating mathematics and can be a refreshing break from lots of epsilons, deltas and integral signs. Even if algebra is not your thing you might grow to like it (in the same way a hostage might grow to like his kidnapper).

Authors

Originally written by David McCormick, with assistance from Daniel Wood and Tom Boardman, based upon lectures given by Dmitriĭ Rumynin at the University of Warwick, 2007.
Revised for the second edition by David McCormick, based upon lectures given by Derek Holt at the University of Warwick, 2009.
Any corrections or improvements should be entered into our feedback form at http://tinyurl.com/WMSGuides (alternatively email revision.guides@warwickmaths.org).

History

First Edition: May 23, 2007.
Second Edition: May 4, 2009.
Current Edition: January 18, 2020.

1 Groups, Subgroups and Isomorphisms

1.1 Basic Definitions

A *group* is the simplest kind of algebraic structure; essentially a group is a set, together with a "well-behaved" binary operation on that set, which eats two elements of the group and spits out a third. Groups are as crucial to algebra as grapes are to wine. Underestimate them at your peril!

Definition 1.1. A *group* is a set G together with a binary operation satisfying:
(i) For every $g, h \in G$, $g \ h \in G$ (closure[1]).
(ii) For every $g, h, k \in G$, $g \ (h \ k) = (g \ h) \ k$ (associativity).
(iii) There exists $e \in G$ such that $e \ g = g$ for every $g \in G$ (existence of a left identity, e).
(iv) For every $g \in G$ there exists $g' \in G$ such that $g' \ g = e$ (existence of left inverses).
We will usually denote a group by G, although sometimes we may wish to denote it by $(G, \ )$ (especially when we explicitly state what G and are).

Note that we only required the existence of a *left* identity and a *left* inverse: however, it follows from this that the same identity and inverse are also a right identity and a right inverse, and indeed that the identity and inverse are unique.

Lemma 1.2. Let G be a group with an identity element $e \in G$ and let $g' \in G$ be an inverse of $g \in G$. Then $g \ e = g$ and $g \ g' = e$.

Lemma 1.3. Every group G has a unique identity element and every $g \in G$ has a unique inverse.

One very useful property of a group is the *cancellation laws*:

Lemma 1.4. Let G be a group. For any $g, h, k \in G$, $g \ h = g \ k \Rightarrow h = k$ and $h \ g = k \ g \Rightarrow h = k$.

Sometimes, the binary operation is particularly well-behaved that it does not matter what order in which it is performed:

Definition 1.5. A group G is called *abelian* (or *commutative*) if $g \ h = h \ g$ for every $g, h \in G$.

Remark 1.6. For different groups it is often useful to use different notation:

(i) *Multiplicative notation*: We omit the symbol , simply replacing $g \ h$ by gh; we denote the identity element by 1 (rather than by e); and we denote the inverse of an element g by g^{-1}. In multiplicative notation we define g^n by

$$g^n = \underbrace{ggg \cdots g}_{n \text{ times}}$$

for $n \in \mathbb{N}$. We also define g^0 to be the identity element and g^{-n} to be the inverse of g^n. This means that $g^n g^m = g^{n+m}$ for all $n, m \in \mathbb{Z}$.

(ii) *Additive notation*: We replace the symbol by $+$; we denote the identity element by 0; and we denote the inverse of an element g by $-g$. In additive notation we define ng by

$$ng = \underbrace{g + g + \cdots + g}_{n \text{ times}}$$

for $n \in \mathbb{N}$. We also define $0g$ to be the identity element and $-ng$ to be the inverse of ng. This means that $ng + mg = (n+m)g$ for all $n, m \in \mathbb{Z}$.

On the whole we use multiplicative notation; however, if the group is abelian then additive notation is also common.

So far we have only thought of a group as an abstract structure. The point of group theory, however, is to understand as many examples of groups as possible, so we now consider some simple examples.

Examples 1.7. 1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ form a group under addition; we can denote these groups as $(\mathbb{Z}, +)$, etc. Furthermore, define $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$, and analogously $\mathbb{Q}^*$ and $\mathbb{C}^*$. Then $\mathbb{R}^*$ (or $\mathbb{Q}^*$ or $\mathbb{C}^*$) is a group under multiplication. Note that each of these groups is abelian.

[1] Technically this is part of the definition of a binary operation, but it is traditional to state it as the first group axiom.

2. Let X be any set, and let $\mathrm{Sym}(X)$ denote the set of permutations of X, i.e. bijections from $X \to X$. Then $\mathrm{Sym}(X)$ is a group under composition of maps, known as the *symmetric group* on X. When $X = \{1, \ldots, n\}$, we denote $\mathrm{Sym}(X)$ by S_n, and the elements of S_n are permutations.

3. A convenient way to describe a group is by writing its *multiplication table*. For example, the Klein four group is the set $K_4 := \{1, a, b, c\}$ with the multiplication table:

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

By laboriously checking the axioms, we can show that this operation does indeed define a group.

1.2 Subgroups and Direct Products

Having found a number of examples of groups, it is natural to look for ways of constructing new groups from old ones. The easiest construction is to take a subset $H \subseteq G$; if we find that it forms a group under the same operation as G, then we call it a subgroup:

Definition 1.8. Let G be a group. A subset $H \subseteq G$ is a *subgroup* of G, denoted $H \leq G$, if H forms a group under the same operation as G.

For any group G there are two standard subgroups: G itself and the the *trivial* subgroup $\{1\}$. Subgroups other than G are called *proper* subgroups, and subgroups other than $\{1\}$ are called *non-trivial* subgroups.

Lemma 1.9. If H is a subgroup of G, then the identity 1_H of H is equal to the identity 1_G of G.

The following technical result is useful for checking if a subset is a subgroup.

Proposition 1.10. Let H be a non-empty subset of a group G. Then H is a subgroup of G if and only if $hg^{-1} \in H$ for any $h, g \in H$.

Examples 1.11.

1. The set of all even integers, denoted $2\mathbb{Z}$, is a subgroup of $\mathbb{Z}$ under addition, since the sum or difference of any two even integers is again even.

2. Let $\mathrm{Sym}(X)$ be the symmetric group on a finite set X. The set $\mathrm{Alt}(X)$ of *even*[2] permutations in $\mathrm{Sym}(X)$ is a subgroup of $\mathrm{Sym}(X)$, since the composition of two even permutations is again even.

Another way of creating new groups from old groups is to take two groups G and H and form the set of all ordered pairs (g, h), where $g \in G$ and $h \in H$; this is the Cartesian product of G and H, denoted $G \times H$. To make the set $G \times H$ into a group, we simply specify componentwise multiplication:

Definition 1.12. Let G and H be multiplicative groups. The *direct product* of G and H, denoted $G \times H$, is the set $\{(g, h) \mid g \in G, h \in H\}$ with the operation given by $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$.

It is easy to check that $G \times H$ is a group under this operation; the identity is $(1_G, 1_H)$ and the inverse of (g, h) is just (g^{-1}, h^{-1}). If the groups are abelian, it is called the *direct sum* and denoted $G \oplus H$.

1.3 Isomorphisms

Having found some groups, some subgroups, and some direct products, sometimes we will find the same group in different guises. Recall the group $K_4 = \{1, a, b, c\}$, whose multiplication table is denoted by below. Let $C_2 = \{0, 1\}$, with the operation $0 + 0 = 1 + 1 = 0$ and $1 + 0 = 0 + 1 = 1$. The direct product of C_2 with itself is the group $C_2 \times C_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ with the binary operation defined as below.

[2] Recall that a permutation is even if it can be written as the product of an even number of transpositions, e.g. (123) = (13)(12) is even. Similarly a permutation can be odd, but not both.

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

These two tables have the same structure; we have just relabelled the elements, and we can set up a bijection $\phi\colon K_4 \to C_2 \times C_2$ by $1 \mapsto (0,0)$, $a \mapsto (0,1)$, $b \mapsto (1,0)$, $c \mapsto (1,1)$. This means that multiplying any two elements in one group and finding that image gives the same result as finding their images separately and then multiplying them together; we can express this as $\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$ for any $g_1, g_2 \in K_4$. We call K_4 and $C_2 \times C_2$ *isomorphic*, which we define formally as follows:

Definition 1.13. Let $(G, \cdot)$ and $(H, \cdot)$ be groups. A *group isomorphism* is a bijection $\phi\colon G \to H$ such that

$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$$

for every $g_1, g_2 \in G$. Two groups G and H are *isomorphic*, denoted $G \cong H$, if there exists a group isomorphism between them.

We specify a *group* isomorphism because we will meet another type of isomorphism later on. However, until otherwise specified, 'isomorphism' will refer to a group isomorphism.

In order for there to be *any* bijection between two sets, they must have the same "size", i.e. the same number of elements. We call the "size" of a group G the order of G:

Definition 1.14. The *order* of G, denoted $|G|$, is the number of elements of G; we write $|G| = \infty$ if G has infinitely many elements.

Thus if $G \cong H$, we must have $|G| = |H|$; the converse is not true, as we will see later.

Example 1.15. Consider two sets X and Y such that $|X| = |Y|$, and let $\mathrm{Sym}(X)$ and $\mathrm{Sym}(Y)$ be the symmetric groups of X and Y respectively. Then $\mathrm{Sym}(X) \cong \mathrm{Sym}(Y)$. To see this, let $\psi\colon X \to Y$ be any bijection; then the map $\phi\colon \mathrm{Sym}(X) \to \mathrm{Sym}(Y)$, defined by $\phi(f) = \psi f \psi^{-1}$, is an isomorphism, since ϕ is bijective and

$$\phi(fg) = \psi fg\psi^{-1} = \psi f\psi^{-1}\psi g\psi^{-1} = \phi(f)\phi(g).$$

To find if two groups G and H are isomorphic is, in general, difficult, since we must construct an isomorphism between the two groups. Properties which are left invariant under an isomorphism help us to distinguish between genuinely distinct groups. One of the most fundamental properties of a group element is its *order*.

Definition 1.16. Let G be a group. The *order* of an element $g \in G$, denoted $|g|$, is the least positive $n \in \mathbb{N}$ such that $g^n = 1$, if such an n exists. If no such n exists then g has *infinite order*, and we write $|g| = \infty$.

Lemma 1.17. Let G be a group, and let $g \in G$. Then $|g| = 1 \iff g = 1$. Furthermore, if $|g| = n$, then $g^m = 1$ for some $m \in \mathbb{Z}$ if and only if $n \mid m$.

The next lemma tells us that an isomorphism preserves orders of elements, just as it must preserve the order of the group:

Lemma 1.18. Let $\phi\colon G \to H$ be an isomorphism. Then $|g| = |\phi(g)|$ for all $g \in G$.

This is very useful in telling non-isomorphic groups apart; if there is an element of order n in G, but no such element in H, then G and H cannot be isomorphic.

1.4 Generators and Relations

An important example of groups are cyclic groups:

Definition 1.19. A group G is *cyclic* if there exists $g \in G$ such that for every $h \in G$ we have $h = g^n$ for some $n \in \mathbb{Z}$. The element g is a *generator* of G.

Example 1.20. The additive group $(\mathbb{Z}_n, +)$ of residues modulo n is a cyclic group, generated by 1.

Lemma 1.21. In an infinite cyclic group, any generator g has infinite order. In a finite cyclic group of order n, any generator has order n.

Proposition 1.22. Any two infinite cyclic groups are isomorphic. Any two finite cyclic groups with the same order are isomorphic.

We denote a finite cyclic group of order n by C_n and an infinite cyclic group by C_1.

Under most circumstances, one element will not generate the whole group. When we can find a set elements $g_1, \ldots, g_r$ in which we can express every element $g \in G$ as a product of the elements $g_1, \ldots, g_r$, we say $g_1, \ldots, g_r$ generate G:

Definition 1.23 (Generators)**.** The elements $\{g_1, g_2, \ldots, g_r\}$ of a group G are said to *generate* G if every element of G can be obtained by repeated multiplication of g_i and their inverses.

Another important example of a group, which arises naturally geometrically, is the dihedral group:

Definition 1.24. Let P be an n-sided regular polygon in the plane. The *dihedral group* of order $2n$, denoted D_{2n}, is the group of isometries of P.[3]

Let a be the clockwise rotation of angle $2\pi/n$ about the centre of P. It is convenient to number the vertices of P (clockwise, 1 to n) and to consider the isometries of P as permutations of these vertices. So a is the permutation $(1, 2, \ldots, n)$. Similarly, if we let b be the line of symmetry passing through vertex 1, then b is the permutation $(2, n)(3, n-1)(4, n-2)\ldots$.

The n isometric reflections of P are $a^k b$ for $0 \leq k < n$. So $D_{2n} = \{a^k b^l \mid 0 \leq k < n,\ l = 0 \text{ or } 1\}$, and, since $ba = a^{-1}b$, we have $(a^{k_1}b^{l_1})(a^{k_2}b^{l_2}) = a^{k_1 \pm k_2}b^{l_1+l_2}$, where we take $k_1 \pm k_2$ modulo n and $l_1 + l_2$ modulo 2.

In fact, any group of order $2n$ generated by two elements a and b that satisfies $a^n = b^2 = 1$ and $ba = a^{-1}b$, which we write as $\langle a, b \mid a^n = b^2 = 1, ba = a^{-1}b\rangle$, is isomorphic to the dihedral group D_{2n}:

Proposition 1.25. Let $G = \langle a, b \mid a^n = b^2 = 1, ba = a^{-1}b\rangle$. Then $G = D_{2n}$.

We call $a^n = b^2 = 1$ and $ba = a^{-1}b$ *relations* on the group G. We have only really defined D_{2n} for $n > 3$, since a two-sided polygon doesn't make much sense. However, we can think of a two-sided polygon as a line segment in the plane. This has four symmetries: the identity, rotation by π, and two reflections. (These are also the symmetries of a non-square rectangle.) Each of these elements has order 2, so $D_4 = K_4$.

Example 1.26. Our final example of a group is the quaternion group $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ where we define multiplication using $i^2 = j^2 = k^2 = ijk = -1$. This is like the complex numbers, but in four dimensions instead of two. As with the dihedral group, we can show that any group $G = \langle a, b \mid a^4 = 1, b^2 = a^2, ba = a^{-1}b\rangle$ is isomorphic to Q_8.

1.5 Classification of Finite Groups

We classify groups of orders 6 and 8, using the following lemma:

Lemma 1.27. Let G be a group in which $g^2 = 1$ for all $g \in G$. Then G is abelian. Letting a, b be distinct non-identity elements of G, we have that $\{1, a, b, ab\}$ is a subgroup of G of order 4.

Proposition 1.28. Let G be a group of order 6. Then $G = C_6$ or $G = D_6$.

Proposition 1.29. Let G be a group of order 8. Then G is isomorphic to one of C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8 and Q_8.

2 Cosets, Quotients Groups and Homomorphisms

This section is devoted to the study of *quotient groups*, which are another fundamental way of taking a group and making new groups from it. These are more complicated than subgroups or direct products, but they are very powerful; however, getting your head around the concept can be tricky.

[3] This group is sometimes denoted D_n; we shall always use D_{2n}.

2.1 Cosets and Lagrange's Theorem

Recall the definition of an equivalence relation from MA132 FOUNDATIONS.

Definition 2.1. An *equivalence relation* on a set X is a relation on X such that
1. is reflexive, i.e. for any $x \in X$, x x.
2. is symmetric, i.e. for any $x, y \in X$, x y $\Leftrightarrow$ y x.
3. is transitive, i.e. for any $x, y, z \in X$, if x y and y z then x z.

The *equivalence class* of an element $x \in X$ is the set $[x] = \{y \in X \mid y \quad x\}$.

It is a fundamental fact of equivalence relations that the equivalence classes of on X partition X; that is, every $x \in X$ belongs to exactly one equivalence class.

Let H be a subgroup of a group G. Let us define an equivalence relation on G by g_1 g_2 if there exists $h \in H$ such that $g_1 = hg_2$, i.e. g_1 and g_2 are equivalent if they "differ" by an element of H. Clearly g hg for any $h \in H$; this describes all elements equivalent to g, so the equivalence class of an element g is the set $\{hg \mid h \in H\}$. We call this the right coset of H by g. Analogously, defining g_1 g_2 if there exists $h \in H$ such that $g_1 = g_2 h$, we get the left coset of H by g. We formally define this as follows:

Definition 2.2. Let H G and let $g \in G$. The *right coset* of H by g, denoted Hg, is the subset $\{hg \mid h \in H\}$ of G. The *left coset* of H by g, denoted gH, is the subset $\{gh \mid h \in H\}$ of G.

If G is additive then we denote the (right) coset by $H + g$. Given a subgroup H of a group G, the expression "a right coset of H in G" refers to a coset Hg for some $g \in G$; we may drop "in G" if it is clear what G is. When G is abelian, it is clear that $gH = Hg$ for every subgroup H and every element g; we simply call these *cosets* when G is abelian. It should be clear that all the following results regarding right cosets easily apply to left cosets.

Example 2.3. Consider the integers $\mathbb{Z}$ under addition, and consider the subgroup $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$ for some fixed $n \in \mathbb{N}$. The coset $n\mathbb{Z} + m$ is then the set of all $x \in \mathbb{Z}$ such that x m modulo n. For example, when $n = 3$, the cosets are $3\mathbb{Z}+0 = \{\ldots, \quad 6, \quad 3, 0, 3, 6, \ldots\}$, $3\mathbb{Z}+1 = \{\ldots, \quad 5, \quad 2, 1, 4, 7, \ldots\}$, and $3\mathbb{Z}+2 = \{\ldots, \quad 4, \quad 1, 2, 5, 8, \ldots\}$.

In the previous example, notice that $3\mathbb{Z}+(a+3b) = 3\mathbb{Z}+a$ for any integers a, b. In general, it is true that $k \in Hg$ if and only if $kg^{-1} \in H$, which happens if and only if $Hg = Hk$. This yields the following result:

Proposition 2.4. For a subgroup H G, any two right cosets of H are either equal or disjoint. Hence, the right cosets of H partition G.

In the case when the group is finite, all the right cosets of H have the same number of elements; indeed, they all have $|H|$ elements. This is the key step in proving Lagrange's Theorem:

Theorem 2.5 (Lagrange's Theorem)**.** Let G be a finite group and let H G. Then the order of H divides the order of G.

By taking the cyclic group generated by an element $g \in G$, this yields:

Corollary 2.6. Let G be a finite group. Then the order of any element $g \in G$ divides the order of G.

Definition 2.7. Let H G. The *index* of H, denoted $|G : H|$, is the number of distinct right (or left) cosets of H in G.[4]

Thus, if G is finite, then $|G| = |H||G : H|$.

[4] It doesn't actually matter which type of coset we use, since $xH \mapsto Hx^{-1}$ is a bijection between the set of left cosets of H and the set of right cosets of H.

2.2 Quotient Groups and Normal Subgroups

We move now to quotient groups. Let H be a subgroup of a group G. For each $g \in G$, we form the coset Hg. Consider the set $\{Hg \mid g \in G\}$ of all cosets. Since the cosets of H partition G, every element of G lies in exactly one of the cosets Hg. By dividing G into the cosets of H, we have "quotiented out" the subgroup H. It is an amazing fact that, under certain restrictions on what kind of subgroup H is, *this set of cosets is itself a group*! We call this group the *quotient group* of G by H, and denote it by G/H.

First let us define the product of two subsets of a group:

Definition 2.8. Let A and B be subsets of a group G. The *product* of A and B, denoted AB, is the set $\{ab \mid a \in A,\ b \in B\}$.[5]

We want to define the group operation on the set of cosets by taking their product $(Hg_1)(Hg_2)$. But for this to be well-defined, we require that it is independent of the choice of representative of H; in fact, we have $(Hg_1)(Hg_2) = H(g_1g_2)$, i.e. the product of two cosets is again a coset, and is indeed independent of the choice of elements of H. This will be true if we can "flip" the middle two terms; that is, if $H(g_1H)g_2 = H(Hg_1)g_2$.

When $gH = Hg$ for every $g \in G$, we call H a *normal subgroup* of G. When we quotient G out by a normal subgroup, it doesn't matter whether we partition it using left cosets or right cosets since they will be the same. Every subgroup of an abelian group is normal; however, every subgroup of the Quaternion group Q_8 is normal, but Q_8 is not abelian.

Definition 2.9. A subgroup $H \leq G$ is *normal*, denoted $H \trianglelefteq G$, if $gH = Hg$ for every $g \in G$.

The following equivalent way of defining normal subgroup is often much easier to check.

Proposition 2.10. Let $H \leq G$. Then $H \trianglelefteq G$ if and only if $ghg^{-1} \in H$ for every $g \in G$ and $h \in H$.

One particular case when a subgroup is always normal is very useful:

Lemma 2.11. Let $H \leq G$ be a subgroup of index $|G : H| = 2$. Then H is a normal subgroup of G.

When a subgroup is normal, we define a group operation on the set of cosets $G/H := \{Hg \mid g \in G\}$:

Lemma 2.12. Let $H \trianglelefteq G$ and $g_1, g_2 \in G$. Then $(Hg_1)(Hg_2) = Hg_1g_2$.

Theorem 2.13. Let $H \trianglelefteq G$. Then the set G/H of (right) cosets of H forms a group under multiplication of cosets, where the identity is given by $H1$ and the inverse of Hg is given by Hg^{-1}. We call G/H the *quotient group* of G by H.

Example 2.14 (Residues modulo n)**.** Consider the group $(\mathbb{Z}, +)$. We know that $n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\} \leq \mathbb{Z}$ where $n \in \mathbb{N}$. Now, $n\mathbb{Z} + a = n\mathbb{Z} + b$ if and only if $a - b \in n\mathbb{Z}$, i.e. if and only if $a \equiv b \pmod{n}$. Thus $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z} + 0, n\mathbb{Z} + 1, n\mathbb{Z} + 2, \ldots, n\mathbb{Z} + (n-1)\}$. We can see from this that $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

Example 2.15. Consider the dihedral group $D_8 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$. Since $a^2 = 1$, $H := \{1, a^2\}$ is a subgroup of D_8. For any $g = a^kb^l \in G$, $g1g^{-1} = 1 \in H$ and $ga^2g^{-1} = a^kb^la^{2\,k}b^{-l} = a^{2k-2} \in H$, so H is normal. So the quotient group D_8/H is

$$D_8/H = \big\{\{1, a^2\}, \{a, a^3\}, \{b, a^2b\}, \{ab, a^3b\}\big\}.$$

By mapping each coset $\{1, a^2\} \mapsto 1$, $\{a, a^3\} \mapsto a$, $\{b, a^2b\} \mapsto b$, $\{ab, a^3b\} \mapsto c$, we see that $D_8/H = K_4$.

Note that if G is a finite group and $H \trianglelefteq G$ then $|G/H| = |G : H| = |G|/|H|$. Thus the quotient group G/H is a smaller group than G, and if we can find a normal subgroup H we can "break down" G into H and G/H. If we cannot do this, then G is termed "simple":

Definition 2.16. A group G with $|G| > 1$ is called *simple* if its only normal subgroups are $\{1\}$ and G.

Cyclic groups of prime order p are simple, because their subgroups can only be of order 1 and p. In fact, since every subgroup of an abelian group is normal, any abelian simple group have no non-trivial subgroups of any kind; one can then check that any abelian simple group must be cyclic of prime order.

[5] In additive notation this becomes $A + B = \{a + b \mid a \in A,\ b \in B\}$.

2.3 Homomorphisms

In order to study a general group G, we often want to find a map from G to some known group H which preserves the group structure of G. We can then infer information about G from known properties of H. An isomorphism $\phi\colon G \to H$ is an example of a structure-preserving map; it preserves the structure by requiring $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. If we can find an isomorphism between G and H, then we immediately know everything about G that we knew about H.

We now consider more general structure-preserving maps by removing the requirement that ϕ be a bijection. A bijection is a purely set-theoretic notion; by removing this requirement we have a general structure-preserving map, which we call a *homomorphism*.

Definition 2.17. Let G, H be groups. A *(group) homomorphism* ϕ from G to H is a map $\phi\colon G \to H$ such that $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$.

As above, an isomorphism is a bijective homomorphism. As with isomorphisms, we specify a *group* homomorphism because we will meet another type of homomorphism later on. However, until otherwise specified, 'homomorphism' will refer to a group homomorphism.

Lemma 2.18. Let $\phi\colon G \to H$ be a homomorphism. Then $\phi(1_G) = 1_H$, and $\phi(g^{-1}) = \big(\phi(g)\big)^{-1}$ for every $g \in G$.

Definition 2.19. Let $\phi\colon G \to H$ be a homomorphism. The *image* of ϕ is the set $\mathrm{im}(\phi) := \{h \in H \mid h = \phi(g) \text{ for some } g \in G\}$; i.e. the set of all elements of H mapped to by ϕ. The *kernel* of ϕ is the set $\ker(\phi) := \{g \in G \mid \phi(g) = 1_H\}$, i.e. the set of all elements of G mapped to the identity 1_H.

The following useful technical lemma allows us to easily check if a homomorphism is injective.

Lemma 2.20. Let $\phi\colon G \to H$ be a homomorphism. Then ϕ is injective if and only if $\ker(\phi) = \{e\}$.

If $\phi\colon G \to H$ is a homomorphism, then it is easy to see that $\ker(\phi)$ is a subgroup of G and $\mathrm{im}(\phi)$ is a subgroup of H. More importantly, however, $\ker(\phi)$ is a *normal* subgroup of G:

Proposition 2.21. Let $\phi\colon G \to H$ be a homomorphism. Then $\ker(\phi) \trianglelefteq G$, and $\mathrm{im}(\phi) \leq H$.

Since $K = \ker(\phi)$ is a normal subgroup of G, we can find the quotient group G/K. Let us consider again example 2.15, with $D_8 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$, and $H := \{1, a^2\}$. We showed that $D_8/H = K_4$. Let us define a homomorphism $\phi\colon D_8 \to K_4$ by $\phi(a^k) = 1$ if k is even and a if k is odd, and $\phi(a^kb) = b$ if k is even and c if k is odd. Then $\ker(\phi) = \{1, a^2\} = H$, and $\mathrm{im}(\phi) = K_4$. That is, $G/(\ker(\phi)) = \mathrm{im}(\phi)$: the quotient of a group by the kernel of a homomorphism is isomorphic to the image of the homomorphism:

Theorem 2.22 (First Isomorphism Theorem for Groups)**.** Let $\phi\colon G \to H$ be a homomorphism with kernel K. Then there is an isomorphism $\phi^0\colon G/K \to \mathrm{im}(\phi)$ defined by $\phi^0(Kg) = \phi(g)$ for every $g \in G$.

The next theorem is quite interesting; it tells us that we can think of every group as a subgroup of a permutation group.

Theorem 2.23 (Cayley's Theorem)**.** Let G be a group. Then G is isomorphic to a subgroup of $\mathrm{Sym}(G)$.

The second and third isomorphism theorems are largely technical results. A lecturer once said that the Isomorphism Theorems were all "meaningless statements". However, they are useful in certain circumstances, especially in exams. This is as they not only tell us about groups being isomorphic, but also provide us with natural concrete maps between them.

Theorem 2.24 (Second Isomorphism Theorem for Groups)**.** Let G be a group. If $H \leq G$ and $K \trianglelefteq G$, then $H \cap K \trianglelefteq H$ and $H/(H \cap K) = HK/K$.

The second isomorphism theorem is fairly simple to prove but it allows us to translate the quotient of subgroups into the context of the quotient of cosets, which we can understand much more easily.

Theorem 2.25 (Third Isomorphism Theorem for Groups)**.** Let G be a group where $K, H \trianglelefteq G$ and $K \leq H \leq G$. Then $(G/K)/(H/K) = G/H$.

Corollary 2.26. If G is abelian and $H \leq G$ and $K \leq H$, then $|G : K| = |G : H||H : K|$.

The third is another easy result (just an application of the first really) but again a useful one, allowing us to sort out a rather nasty quotient into a simple one. You can remember it as "the one where you cancel out the 'K's"; just don't forget the inclusions so it makes sense.

3 Group Actions and Conjugacy

In many cases, a group is not merely an abstract set; often a group *acts* on some other set. For instance, the symmetry group of a regular polygon *acts* on the regular polygon by rotating or reflecting it; the general linear group $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by transforming it linearly. We thus define the general case of a group G acting on a set X.

Definition 3.1. Let G be a group and let X be a set. A (*left*) *action*[6] of G on X is a map from $G \quad X \; ! \; X$ such that:
(i) For every $g, h \; 2 \; G$ and $x \; 2 \; X$, $(gh) \quad x = g \quad (h \quad x)$.
(ii) $1 \quad x = x$ for every $x \; 2 \; X$.

Proposition 3.2. Let be an action of a group G on a set X. For $g \; 2 \; G$ define $\phi_g \colon X \; ! \; X$ by $\phi_g(x) = g \quad x$. Then $\phi_g \; 2 \; \mathrm{Sym}(X)$ and the map $\phi \colon G \; ! \; \mathrm{Sym}(X)$, defined by $\phi(g) = \phi_g$, is a homomorphism.

Since any group is isomorphic to a subgroup of $\mathrm{Sym}(X)$ for some suitable set X, we can equate each element g of a group with a permutation $\phi(g)$. The action of g on X is then to apply the permutation $\phi(g)$ to the set X.

Definition 3.3. Let be an action of a group G on a set X. The *kernel*[7] K of is the set $K = \{g \; 2 \; G \; j \; g \quad x = x \text{ for every } x \; 2 \; X\}$. The action is *faithful* if $K = \{1\}$.

3.1 Orbits and Stabilizers

Definition 3.4. Let be an action of a group G on a set X. The *orbit* of an element $x \; 2 \; X$, denoted $\mathrm{Orb}_G(x)$ (or $G \quad x$), is the set $\mathrm{Orb}_G(x) := \{y \; 2 \; X \; j \; y = g \quad x \text{ for some } g \; 2 \; G\}$.

Definition 3.5. The *stabilizer* of an element $x \; 2 \; X$, denoted $\mathrm{Stab}_G(x)$ (or G_x), is the set $\mathrm{Stab}_G(x) := \{g \; 2 \; G \; j \; g \quad x = x\}$.

Proposition 3.6. Let be an action of a group G on a set X. Define a relation on X by $x \quad y$ if and only if $y = g \quad x$ for some $g \; 2 \; G$. Then is an equivalence relation on X. Furthermore, the orbits of X are the equivalence classes of and thus they partition X.

Lemma 3.7. Let be an action of a group G on a set X. Then $\mathrm{Stab}_G(x) \quad G$ for any $x \; 2 \; X$. Furthermore, $\bigcap_{x \, 2 \, X} \mathrm{Stab}_G(x)$ is equal to the kernel of this action.

The following result is of fundamental importance in group theory:

Theorem 3.8 (The Orbit–Stabilizer Theorem)**.** Let be an action of a group G on a set X. Then for any $x \; 2 \; X$, $|\mathrm{Orb}_G(x)| = |G : \mathrm{Stab}_G(x)|$.

3.2 Conjugacy

In addition to acting on a set, a group can act on itself in a particularly useful way.

Definition 3.9. Let G be a group. The action from $G \quad G \; ! \; G$ defined by $g \quad h = ghg^{\;1}$ is called *conjugation*.

Example 3.10. Two permutations in $\mathrm{Sym}(X)$ are conjugate (in $\mathrm{Sym}(X)$) if and only if they have the same cycle-type. (However, two permutations in $\mathrm{Alt}(X)$ which have the same cycle type *are not necessarily conjugate in* $\mathrm{Alt}(X)$.)

For conjugation there are special names for the orbits, stabilizers, and kernel.

Definition 3.11. Let G be a group acting on itself by conjugation. The *conjugacy class* of an element $g \; 2 \; G$, denoted $\mathrm{Cl}_G(g)$, is the orbit of g. Two elements of G are *conjugate* if they belong to the same conjugacy class.

This means that two elements $g_1, g_2 \; 2 \; G$ are conjugate if there exists $h \; 2 \; G$ such that $hg_1h^{\;1} = g_2$. In geometric terms, if we consider g_1 and g_2 as transformations of some set X, then if g_1 and g_2 are conjugate they are the same transformation viewed from a different angle. For example, any two rotations are conjugate in the general linear group $GL_n(\mathbb{R})$.

[6] A *right* action can analogously de ned as a map from $X \quad G \; ! \; X$.
[7] Notice that K is in fact the kernel of the homomorphism $\phi \colon G \; ! \; \mathrm{Sym}(X)$ de ned in Proposition 3.2.

Definition 3.12. Let G be a group acting on itself by conjugation. The *centralizer* of an element $g \in G$, denoted $C_G(g)$, is the stabiliser of g; that is $C_G(g) := \{h \in G \mid hgh^{-1} = g\}$.

By definition, $C_G(g)$ is the set of all h such that $hg = gh$; in other words, the centraliser of g is the set of those h which commute with g. When we intersect the stabilizers we get the kernel; this will consist of those elements g which commute with *every* element of G; we call this the centre.

Definition 3.13. The *centre* of G, denoted $Z(G)$, is the kernel of the action of conjugation; that is, $Z(G) = \{h \in G \mid hg = gh \text{ for all } g \in G\}$.

Being able to compute conjugacy classes is important. There are many examples where conjugacy classes help us to analyse the structure of a group. Conjugacy classes also have connections to normal subgroups:

Lemma 3.14. A subgroup $H \leq G$ is normal in G if and only if H is a union of conjugacy classes of G.

By counting the size of its conjugacy classes, this allows us to prove that A_5, the alternating group on five letters, is a simple group which is non-abelian[8].

3.3 Sylow's Theorems

Lagrange's theorem tells us that if H is a subgroup of a finite group G, then $|H|$ divides $|G|$. A natural question is whether the converse holds; that is, if G is a finite group and n is any number which divides $|G|$, is there a subgroup of G of order n? This is true in some special cases; for example, it is true for every finite cyclic group. In general, it is *not* true, and the smallest counterexample is:

Proposition 3.15. A_4 (which has $|A_4| = 12$) has no subgroup of order 6.

However, *Sylow's theorems* provide a partial converse to Lagrange's theorem. In particular, they assert the existence of subgroups of all prime power orders which divide $|G|$.

Definition 3.16. Let G be a finite group and let p be a prime with $|G| = p^n q$, where $p \nmid q$. A subgroup of G of order p^n is called *Sylow p-subgroup* of G.

Theorem 3.17 (Sylow)**.** Let G be a finite group and p a non-trivial prime divisor of $|G|$. Then:
1. There exists at least one Sylow p-subgroup of G.
2. Any two Sylow p-subgroups are conjugate in G.
3. If $1 \leq m \leq n$, any subgroup of G of order p^m is contained in a Sylow p-subgroup of G.
4. The number of Sylow p-subgroups of G is congruent to 1 modulo p.

Corollary 3.18. Let G be a finite group, p be a prime divisor of $|G|$, and P a Sylow p-subgroup of G. Denote $|G|_p$ as the highest power of p dividing $|G|$. Then:
1. $r_p = |G : N_G(P)|$
2. $r_p \| |G|/|G|_p$
3. $P \trianglelefteq G$ if and only if $r_p = 1$

4 Rings, Ideals and Ring Homomorphisms

4.1 Basic Definitions

Rings are a natural extension of groups; instead of one binary operation on a set, we have *two* binary operations. Many definitions and theorems about groups have obvious ring analogies.

Definition 4.1. A *ring* $(R, +, \cdot)$ is a set R with two binary operations $+$ and $\cdot$ which satisfy:
(i) $(R, +)$ is an abelian group.
(ii) $xy \in R$ for every $x, y \in R$ (closure).
(iii) $(ab)c = a(bc)$ for every $a, b, c \in R$ (associativity).
(iv) $(a + b)c = ac + bc$ and $a(b + c) = ab + ac$ for every $a, b, c \in R$ (distributivity).
(v) There exists $1 \in R$ such that $1a = a1 = a$ for every $a \in R$ (existence of multiplicative identity).

[8] Indeed, it is the smallest non-abelian simple group, but the proof of that is beyond the scope of the course.

The operation + is called *addition*, for which we use additive notation. The operation is called *multiplication*, for which we use multiplicative notation. The identity element 0 of $(R, +)$ is called the *additive identity element* of R, while the element $1 \in R$ in (v) is called a *multiplicative identity element* of R; as with a group, this identity is unique. It is routine to show that $0a = a0 = 0$ for every $a \in R$. As with arithmetic, multiplication is dominant over addition, e.g. $a + bc = a + (bc)$.

A simple example of a ring is $\mathbb{Z}$ with the standard operations of addition and multiplication. However, you should not assume that the operations of a ring are necessarily ordinary addition and multiplication; we give them these names simply for convenience. For example, let X be any set and let 2^X be the set of all subsets of X (the power set of X); then 2^X is a ring under the operations of symmetric difference (for addition) and intersection (for multiplication).

If R is a ring such that $0 = 1$, then it is easy to show that $R = \{0\}$. The ring $\{0\}$ is called the *zero ring*. All other rings are called *non-zero rings*.

Definition 4.2. A ring R is called *commutative* if $ab = ba$ for every $a, b \in R$.

Examples 4.3.

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are rings under the usual definitions of addition and multiplication.
2. If R is a ring, then the set $M_n(R)$ of $n \times n$ matrices with coefficients in R is another ring.
3. Let R be a ring and let $x_1, \ldots, x_n$ be independent variables. The set of polynomials $R[x_1, \ldots, x_n]$ in the x_is with coefficients in R is a ring. $R[x_1, \ldots, x_n]$ is commutative if and only if R is commutative.

Since a ring under multiplication does not form a group, we are not guaranteed to have a multiplicative inverse for each element. We call an invertible element a unit:

Definition 4.4. Let R be a ring. An element $x \in R$ is a *unit* if there exists $x' \in R$ such that $xx' = x'x = 1$. The set of units in R is denoted by $R^\times$.

Lemma 4.5. Let R be a ring. Then $R^\times$ is a group under multiplication.

Thus for each $x \in R^\times$, x' is unique; we will denote it by x^{-1}. If every nonzero element in a commutative ring has an inverse, we call the ring a field[9]:

Definition 4.6. A *field* F is a commutative ring such that $F^\times = F \setminus \{0\}$.

For example, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all fields with the standard operations of addition and multiplication.

4.2 Subrings and Direct Products

As with groups, having found a standard stock of rings, we seek ways of creating new rings and, as with groups, we have three principal ways of doing this: subrings, direct products and quotient rings. We examine the first two of these now.

Definition 4.7. Let R be a ring. A subset S of R is a *subring* of R if S forms a ring under the same operations as R, and has the same multiplicative identity element as R; we write $S \leq R$. Similarly, a *subfield* of F is a subring of F which forms a field under the same operations as F.

Definition 4.8. Let R and S be two rings. The *direct product* of R and S, denoted $R \times S$, is the set $\{(r, s) \mid r \in R,\ s \in S\}$ with the operations of addition and multiplication given by $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$ and $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$ respectively.

4.3 Ideals

Ideals are analogous to normal subgroups, and we use them in the same way to construct quotient rings.

Definition 4.9. Let R be a ring. A subgroup I of $(R, +)$ is an *ideal* in R, denoted $I \trianglelefteq R$, if $xI \subseteq I$ and $Ix \subseteq I$ for every $x \in R$.

For non-commutative rings, we can define right and left ideals by taking just the former or latter inclusion respectively. The property $xI, Ix \subseteq I$ is sometimes called the swallowing property. Intuitively, every element x is 'swallowed' by I under multiplication; this allows us to define multiplication in additive cosets.

[9] If every nonzero element in a noncommutative ring has an inverse, we call the ring a *division ring* or *skew field*. An example of a skew field is the quaternions.

Definition 4.10. Let R be a ring and $x \in R$. The *principal ideal* generated by x is defined to be $(x) := \{rxs \mid r, s \in R\}$. (It is routine to check that a principal ideal is indeed an ideal.)

That is, an ideal $I \trianglelefteq R$ is a principal ideal if it is generated by a single element $x \in R$.

Lemma 4.11. Let R be a commutative ring, and let $x \in R$. Then $x \in R^\times$ if $(x) = R$.

Example 4.12. Consider the subgroup $n\mathbb{Z} \leq (\mathbb{Z}, +)$, as defined in example 2.14. Take some $nm \in n\mathbb{Z}$. Then for any $x \in \mathbb{Z}$, we have $x(mn) = (mn)x = (xm)n \in n\mathbb{Z}$, by associativity and commutativity. Thus both the left and right cosets $xn\mathbb{Z}$ and $n\mathbb{Z}x$ are subsets of $n\mathbb{Z}$, and so $n\mathbb{Z}$ is a principal ideal in the ring $\mathbb{Z}$. So we can rewrite $n\mathbb{Z}$ as (n).

A kind of ideal which is particularly interesting is a *maximal ideal*:

Definition 4.13. An ideal $I \trianglelefteq R$ is called *maximal* if $I \neq R$, and if J is any ideal of R with $I \subseteq J \subseteq R$, then $I = J$ or $J = R$.

Theorem 4.14. An ideal I of a commutative ring is maximal if and only if R/I is a field.

4.4 Ring Homomorphisms

We define ring homomorphisms analogously to group homomorphisms; we require that it preserves *both* the additive structure and the multiplicative structure, but we must also require that it maps the multiplicative identity to the multiplicative identity.

Definition 4.15. Let R and S be rings. A *ring homomorphism* is a map $\phi\colon R \to S$ such that $\phi(1_R) = 1_S$, $\phi(r_1+r_2) = \phi(r_1)+\phi(r_2)$ and $\phi(r_1r_2) = \phi(r_1)\phi(r_2)$ for every $r_1, r_2 \in R$. A *ring isomorphism* is a bijective homomorphism. R and S are *isomorphic*, denoted $R = S$, if there exists a ring isomorphism $\phi\colon R \to S$.

We may drop the words "group" or "ring" and simply refer to a "homomorphism" or an "isomorphism" if it is clear whether we are dealing with groups or with rings. The following definition and proposition are completely analogous to their group-theoretic counterparts:

Definition 4.16. Let R and S be rings and let $\phi\colon R \to S$ be a homomorphism. The *image* of ϕ, denoted $\mathrm{im}(\phi)$, is the set $\{s \in S \mid s = \phi(r) \text{ for some } r \in R\}$. The *kernel* of ϕ, denoted $\ker(\phi)$, is the set $\{r \in R \mid \phi(r) = 0_S\}$.

Proposition 4.17. Let $\phi\colon R \to S$ be a ring homomorphism. Then $\mathrm{im}(\phi) \leq S$, and $\ker(\phi) \trianglelefteq R$.

Example 4.18. The rings $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ are isomorphic if and only if m and n are coprime.

4.5 Quotient Rings and the Isomorphism Theorems

Just as with groups, we may define the quotient ring R/I when I is an ideal of R.

Proposition 4.19. Let I be an ideal of a ring R. The set R/I of right additive cosets forms a ring under addition $(I + a) + (I + b) = I + (a + b)$ and multiplication $(I + a)(I + b) = I + ab$. We call R/I the *quotient ring* of R by I.

Example 4.20. Consider the ring $\mathbb{Z}$. Then $\mathbb{Z}/(n) = \{(n) + 0, n + 1, \ldots, (n) + n\} \cong \mathbb{Z}_n$.

Notice the similarities between Examples 2.14, 4.12, and 4.20.

The three isomorphism theorems for groups carry over virtually unchanged (including their proofs) to give the three isomorphism theorems for rings.

Theorem 4.21 (First Isomorphism Theorem for Rings)**.** Let $\phi\colon R \to S$ be a ring homomorphism with kernel I. Then there is an isomorphism $\phi'\colon R/I \to \mathrm{im}(\phi)$ defined by $\phi'(I + r) = \phi(r)$ for every $r \in R$.

Theorem 4.22 (Second Isomorphism Theorem for Rings)**.** Let R be a ring. If S is a subring of R and $I \trianglelefteq R$, then $S \setminus I \trianglelefteq R$ and $S/(S \setminus I) = (S + I)/I$

Theorem 4.23 (Third Isomorphism Theorem for Rings)**.** Let R be a ring with $I \subseteq J \subseteq R$ and $I, J \trianglelefteq R$. Then $J/I \trianglelefteq R/I$, and $(R/I)/(J/I) = R/J$.

5 Domains, Divisibility and Factorisation

5.1 Domains

A very useful property of the integers is *divisibility*; but in rings divisibility is, sadly, something of a rarity. One problem with a general ring is that since we are not guaranteed to have a multiplicative identity, we are not guaranteed that $xy = 0 \implies x = 0$ or $y = 0$. For instance, in the matrix ring $M_2(\mathbb{R})$, the matrices $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$ are clearly non-zero, but their product is the zero matrix. When this happens we call x a *zero divisor*, since in some sense it is a non-zero element which divides zero.

Definition 5.1. Let R be a ring. An element $x \in R \setminus \{0\}$ is a *zero divisor* if there exists $y \in R \setminus \{0\}$ such that $xy = 0$ or $yx = 0$.

When there are no zero divisors in a ring, we call the ring an *integral domain*.

Definition 5.2. R is an *integral domain* (or just a *domain*[10]) if it is a non-zero commutative ring which contains no zero divisors.

For divisibility to come even close to making sense, we must work over an integral domain; indeed, when we work over a domain, we have (multiplicative) cancellation laws just like for a group:

Lemma 5.3. If R is a domain, and $a, b, c \in R$, $a \neq 0$, then $ab = ac \implies b = c$ and $ba = ca \implies b = c$.

Examples 5.4. Any field is a domain. Conversely, and more importantly, any finite integral domain is a field. Note also any subring of a domain is a domain, and a polynomial ring over a domain is a domain.

Recall that the integers $\mathbb{Z}$ and the ring of polynomials $F[x]$ over a field F have the *Euclidean algorithm*: given any two integers $a, b \in \mathbb{Z}$ such that $b \neq 0$, we can divide with remainder to find $q, r \in \mathbb{Z}$ such that $a = qb + r$; and given any two polynomials $f, g \in F[x]$ with $g \neq 0$ there exist $q, r \in F[x]$ such that $f = qg + r$. If we can divide with remainder in a domain, we call it a Euclidean domain:

Definition 5.5. Let R be a domain. R is a *Euclidean domain*, abbreviated ED, if R admits a *norm function*; that is, a function $\nu\colon R \setminus \{0\} \to \mathbb{N}$ which satisfies the following properties:

(i) $\nu(ab) \geq \nu(b)$ for every $a, b \in R$.

(ii) For every $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $\nu(b) > \nu(r)$.

Warning. A norm function on a domain is sometimes called a *Euclidean function* or just a *norm*. You should not confuse a norm function on a domain with a norm on a vector space (although, just to add to the confusion, there are some examples where a norm on a vector space is also a norm function on a domain, e.g. example 5.6 below).

Example 5.6. $\mathbb{Z}$ forms a Euclidean domain with the norm function $\nu(n) = |n|$.

Example 5.7. $F[x]$, the ring of polynomials in one variable over a field F, forms a Euclidean domain under the norm function $\nu(p) = \deg(p)$.

Another property that $\mathbb{Z}$ has is that every ideal can be generated by exactly one element, that is, every ideal is a principal ideal. When this holds, we call the domain a principal ideal domain:

Definition 5.8. Let R be a domain. R is a *principal ideal domain*, abbreviated PID, if every ideal in R is a principal ideal.

It turns out that this is a more general notion than a Euclidean domain, in the following sense:

Theorem 5.9. Any Euclidean domain is a principal ideal domain.

Examples 5.10. It turns out that $\mathbb{Z}[\alpha]$ with $\alpha = (1 + \sqrt{-19})/2$ is a PID but not an ED. But not every domain is a PID: $\mathbb{Z}[\sqrt{-5}]$ is *not* a PID.

[10] Some books define a *domain* as a non-zero ring with no zero divisors and an *integral domain* as a commutative domain.

5.2 Divisibility

We now define divisibility in a ring:

Definition 5.11. Let R be a domain and let $x, y \in R$. We say x *divides* y, denoted $x \mid y$, if $y = xr$ for some $r \in R$.

It is easy to check that $x \mid y \iff y \in (x) \iff (y) \subseteq (x)$, and these other properties are often easier to work with than the definition itself. Since we can always multiply x and r by a unit and its inverse respectively, divisibility only makes sense up to multiplication by a unit. We thus define:

Definition 5.12. x and y are *associate*, denoted $x \sim y$, if $x \mid y$ and $y \mid x$.

It is again easy to check that $x \sim y$ if and only if $(x) = (y)$, if and only if there exists $q \in R^\times$ such that $x = qy$. For example, two integers $x, y \in \mathbb{Z}$ are associate if and only if $x = \pm y$; two polynomials $f, g \in F[x]$ are associate if and only if there is a constant $a \in F^\times$ such that $f = kg$.

This allows us, just as in the integers, to define highest common factors and lowest common multiples:

Definition 5.13. Let R be a domain and $x, y \in R$.

The *greatest common divisor* or *highest common factor* of x and y, denoted $\gcd(x, y)$ or $\mathrm{hcf}(x, y)$, is that $d \in R$ such that $d \mid x$, $d \mid y$, and if $z \mid x$ and $z \mid y$ then $z \mid d$.

The *lowest common multiple* of x and y, denoted $\mathrm{lcm}(x, y)$, is that $m \in R$ such that $x \mid m$, $y \mid m$, and if $x \mid z$ and $y \mid z$ then $m \mid z$.

Any two greatest common divisors must divide each other, and hence are associate; the same is true of lowest common multiples. Thus $\gcd(x, y)$ and $\mathrm{lcm}(x, y)$, if they exist, are unique up to associates. In an arbitrary domain, they do not necessarily exist, but in a PID they do:

Proposition 5.14. If R is a PID then $\mathrm{lcm}(x, y)$ and $\gcd(x, y)$ exist for any pair of elements $x, y \in R$.

Generalising the notion of prime numbers in $\mathbb{Z}$ leads to two distinct concepts in a general domain, *prime* elements and *irreducible* elements:

Definition 5.15. Let R be a domain, and let $r \in R \setminus (R^\times \cup \{0\})$; that is r is neither zero nor a unit.

r is *irreducible* if $r = ab$ implies that $a \in R^\times$ or $b \in R^\times$.

r is *prime* if $r \mid ab$ implies that $r \mid a$ or $r \mid b$.

Suppose r is prime, and $r = ab$. Then $r \mid a$ or $r \mid b$, since $r \mid r = ab$; suppose w.l.o.g. that $r \mid a$. As $a \mid r$ also, we have $r \sim a$, so $r = aq$ for some $q \in R^\times$. Since R is a domain, this means that $q = b$, i.e. $b \in R^\times$. Hence we have proved:

Proposition 5.16. Any prime element of a domain is irreducible.

In general, an irreducible element need not be prime. But an irreducible element of a PID *is* prime:

Proposition 5.17. If R is a PID, then any irreducible element of R is prime[11].

Example 5.18. For example, in $\mathbb{Z}[\sqrt{5}]$, we have $6 = 2 \cdot 3 = (1 + \sqrt{5})(1 - \sqrt{5})$. It is relatively easy to show that each of 2, 3, $1 + \sqrt{5}$ and $1 - \sqrt{5}$ are irreducible but *not* prime. (In fact, this proves that $\mathbb{Z}[\sqrt{5}]$ is not a PID.)

The final, and most general, form of a domain in which we can "divide nicely" is a unique factorisation domain.

Definition 5.19. A domain R is a *factorisation domain*, abbreviated FD, if every $x \in R \setminus (R^\times \cup \{0\})$ has a *factorisation* $x = r_1 r_2 \cdots r_n$ where the r_i are irreducible elements. A domain R is a *unique factorisation domain*, abbreviated UFD, if R is a FD where for any two factorisations $x = r_1 r_2 \ldots r_n = s_1 s_2 \ldots s_m$, $m = n$ and there exists $\sigma \in S_n$ such that $r_i \sim s_{\sigma(i)}$ for every i.

We can use the distinction between irreducible and prime to test if a FD is a UFD:

[11] The proof of this result is rather tricky.

Proposition 5.20. For a FD R, R is a UFD if and only if every irreducible element of R is prime.

The reason we say a UFD is the most general is that every PID is a UFD:

Theorem 5.21. Every principal ideal domain is a unique factorisation domain.

Examples 5.22. $\mathbb{Z}[x]$ is a UFD, but not a PID, since the ideal $(2, x) = \{2a + xb \mid a, b \in \mathbb{Z}[x]\}$ is not principal. $\mathbb{Z}[\sqrt{-5}]$ is a FD, but not a UFD (since it is not a PID).

We saw in proposition 5.14 that lowest common multiples and greatest common divisors exist in a PID. In fact, they exist in any UFD:

Proposition 5.23. If R is a UFD then $\operatorname{lcm}(x, y)$ and $\gcd(x, y)$ exist for any pair of elements $x, y \in R$.

In summary:

$$\text{ED} \Rightarrow \text{PID} \Rightarrow \text{UFD}$$

while the opposite implications do not hold.

5.3 Examples of Domains

As with most things in mathematics, an example is worth a thousand theorems. So, here goes!

5.3.1 Gaussian Integers

The ring $\mathbb{Z}[i]$ is known as the ring of *Gaussian integers*; it is the polynomials in i, but since $i^2 = 1$ we have $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. There are four units in $\mathbb{Z}[i]$, namely $1, \quad i$. With the norm $\nu(x) = |x|^2$, $\mathbb{Z}[i]$ is a Euclidean domain; hence irreducibles and primes are the same. We now study its primes:

Proposition 5.24. If $x \in \mathbb{Z}[i]$ and $\nu(x)$ is prime (in $\mathbb{Z}$) then x is a Gaussian prime, i.e. a prime in $\mathbb{Z}[i]$.

Proposition 5.25. Let $p \in \mathbb{Z}$ be prime. Then either p is a Gaussian prime or $p = x\bar{x}$ where x is a Gaussian prime (and $\bar{x}$ is the complex conjugate of x).

Proposition 5.26. Let $q \in \mathbb{Z}[i]$ be a Gaussian prime. Then either $\nu(q)$ is a prime or the square of a prime.

Theorem 5.27. The prime elements in $\mathbb{Z}[i]$ are obtained from the prime elements in $\mathbb{Z}$ as follows:

1. $p = 2$ gives rise to a Gaussian prime such that $2 \quad q^2$.
2. For every prime $p \in \mathbb{Z}$ such that $p \quad 3 \pmod 4$, p is a Gaussian prime.
3. For every prime $p \in \mathbb{Z}$ such that $p \quad 1 \pmod 4$, p gives rise to two conjugate Gaussian primes q and $\bar{q}$ such that $p = q\bar{q}$.

Corollary 5.28 (Fermat)**.** The prime 2 and every prime congruent to 1 modulo 4 is the sum of positive integer squares in a unique way.

Fermat's theorem[12] allows us to show that an integer can be expressed as the sum of two integer squares if and only if it is of the form $n^2 p_1 \quad p_k$, where $n \in \mathbb{Z}$ and p_i are distinct positive primes in $\mathbb{Z}$ each equal to 2 or congruent to 1 (mod 4). Fermat's theorem also allows us to show there are infinitely many primes congruent to 1 (mod 4).

5.3.2 Fractions

In this section we introduce fractions as an abstract algebraic concept, rather than as differently sized slices of cake. Let R be a domain and let $W = R \quad (R \setminus \{0\}) = \{(x, y) \in R \quad R \mid y \neq 0\}$. Then we see that W admits an equivalence relation $\quad$ defined by $(a, b) \quad (c, d)$ if and only if $ad = bc$. An equivalence class (a, b) under $\quad$ is called a *fraction* and is denoted by $\frac{a}{b}$. We let $Q(R)$ denote set of all equivalence classes of $\quad$ on W.

Proposition 5.29. If R is a domain then $Q(R)$ is a field under the operations

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \qquad \text{and} \qquad \frac{a}{b} \quad \frac{c}{d} = \frac{ac}{bd}.$$

Furthermore, the map $\pi\colon R \to Q(R)$ defined by $\pi(r) = \frac{r}{1}$ is an injective ring homomorphism.

We call $Q(R)$ the *field of fractions* of a domain R. For example, $Q(\mathbb{Z}) = \mathbb{Q}$, and $Q(\mathbb{Z}[i]) = \mathbb{Q}[i]$. Also, $Q(F[x])$ is the field of *rational functions* p/q where $p, q \in F[x]$ and $q \neq 0$; $\mathbb{Q}(F[x])$ is commonly denoted $F(x)$ (note that $F(x)$ and $F[x]$ are thus different!).

[12] Note that this is neither Fermat's Little Theorem nor Fermat's Last Theorem!

5.3.3 Number Fields

An interesting property of PIDs is the following:

Lemma 5.30. An ideal (a) in a PID R is maximal if and only if a is irreducible.

Since an ideal I is maximal if and only if R/I is a field, an irreducible element $a \in R$ gives rise to a field $R/(a)$. In particular, consider the PID $F[x]$ of polynomials with coefficients in a field F, and let $f \in F[x]$ be irreducible; then $F[x]/(f)$ is a field. The case $F = \mathbb{Q}$ is particularly important:

Definition 5.31. An element $\alpha \in \mathbb{C}$ is *algebraic* (over $\mathbb{Q}$) if there exists $f \in \mathbb{Q}[x]$ with $\deg f > 0$ such that $f(\alpha) = 0$. If no such f exists, α is called *transcendental*.

For example, $\sqrt{2}$, $\sqrt{5}$, $\sqrt[3]{3}$ are all algebraic, but π and e are transcendental. In fact, the set of all algebraic numbers $\mathbb{A} := \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic}\}$ is a field.

More importantly, however, if we take just one algebraic number $\alpha \in \mathbb{C}$, we can define a homomorphism $\mathbb{Q}[x] \to \mathbb{C}$ by sending the polynomial $f \mapsto f(\alpha)$. When f is algebraic, $\ker\phi$ is non-empty, and so $\ker\phi = (f)$ for some polynomial $f \in \mathbb{Q}[x]$; by convention we take f to be the unique polynomial of least degree whose leading coefficient is 1 (the *minimal polynomial* of α). By the First Isomorphism Theorem, $\operatorname{im}\phi = \mathbb{Q}[x]/(f)$; as we saw above, $\operatorname{im}\phi$ is a field, thus it is a subfield of $\mathbb{C}$; we denote it by $\mathbb{Q}[\alpha]$.

5.4 Polynomial Rings

We now consider polynomial rings; we first consider the Euclidean domain $F[x]$ for some field F. We wish to assess divisibility in $F[x]$. By dividing with remainder, we may easily show that:

Theorem 5.32 (Remainder Theorem)**.** Let $f \in F[x]$. Then $f(a) = 0$ for some $a \in F$ if and only if $x - a$ divides f.

Corollary 5.33. A polynomial of degree d in $F[x]$ has at most d roots.

For certain fields F, we can factorise every $F[x]$ into linear factors. This is characterised by every polynomial having a root; when it happens we say the field is *algebraically closed*:

Definition 5.34. Let F be a field. F is *algebraically closed* if for every $f \in F[x]$ of degree at least 1 there exists $a \in F$ such that $f(a) = 0$.

Proposition 5.35. If a field F is algebraically closed, then the irreducibles in $F[x]$ are $x - a$ where a is any element of F.

The field $\mathbb{C}$ of complex numbers is algebraically closed, so the irreducible polynomials are exactly those $x - a$ with $a \in \mathbb{C}$. But the field $\mathbb{R}$ of real numbers is not algebraically closed, since $x^2 + bx + c$ has no roots if $b^2 - 4c < 0$; nonetheless it is a good exercise to show that any irreducible in $\mathbb{R}[x]$ must be either a linear polynomial $x - a$ for some $a \in \mathbb{R}$, or a quadratic $x^2 + bx + c$ for some $b, c \in \mathbb{R}$ with $b^2 - 4c < 0$.

However, it is much more difficult to test whether a polynomial in $\mathbb{Q}[x]$ is irreducible, and there is easy-to-remember necessary and sufficient condition for this. It turns out that irreducibility in $\mathbb{Q}[x]$ is connected closely with irreducibility in $\mathbb{Z}[x]$; to that end, we now study the ring of polynomials $R[x]$ of a general domain R. First, we note the following easy but very useful properties of $R[x]$:

Lemma 5.36. If R is an integral domain, then $R[x]$ is also an integral domain. Moreover, an irreducible element of R remains irreducible in $R[x]$, and the units in R and $R[x]$ are the same.

We will henceforth assume that R is a UFD, since things can break (and in quite strange ways) if it is not. We know that, in a UFD, greatest common divisors exist. A particularly useful type of polynomial is when the gcd of the coefficients is 1:

Definition 5.37. A polynomial $f \in R[x]$ is *primitive* if the greatest common divisor of all the coefficients of f together is 1.

It can be shown that the product of two primitive polynomials is primitive. This allows us to show that a primitive polynomial is irreducible over $R[x]$ if and only if it irreducible as a polynomial in $Q[x]$, where $Q = Q(R)$ is the field of fractions of R:

Theorem 5.38 (Gauss' Lemma)**.** Let R be a UFD with field of fractions $Q = Q(R)$. Then a primitive polynomial in $R[x]$ is irreducible if and only if it is irreducible in $Q[x]$.

Corollary 5.39. If R is a UFD, then there are two kinds of irreducibles in $R[x]$: irreducible elements in R, and primitive elements in $R[x]$ that are irreducible in $Q[x]$.

This allows us to show that if R is a UFD, then so is $R[x]$:

Theorem 5.40. If R is a UFD, then $R[x]$ is a UFD.

By repeatedly applying this theorem, we find that:

Corollary 5.41. If R is a UFD, then $R[x_1, \ldots, x_n]$ is a UFD.

Example 5.42. Theorem 5.40 tells us that $\mathsf{Z}[x]$ is a UFD; we saw in examples 5.22 that it is not a PID.

We have seen that the irreducibility of polynomials is the same over $\mathsf{Z}[x]$ and $\mathsf{Q}[x]$. However, determining whether a particular polynomial is irreducible is often subtle, and the following is a powerful tool to help us:

Proposition 5.43 (Eisenstein's Criterion)**.** Let R be a UFD and $f(x) = \sum_{k=0}^{n} a_k x^k$. If there exists a prime $p \in R$ such that $p \mid a_k$ for all $k < n$, but $p \nmid a_n$ and $p^2 \nmid a_0$, and the greatest common divisor of all the coefficients is 1, then $f(x)$ is irreducible in $R[x]$.

5.4.1 Cyclotomic polynomials

As a final application, we consider the complex n^{th} roots of unity; this will lead to some very interesting irreducible polynomials in $\mathsf{Z}[x]$. For $n \in \mathsf{N}$, let $\zeta_n := e^{2\pi i/n}$ be a complex n^{th} root of unity. The n powers $1 = \zeta_n^0, \zeta_n^1, \ldots, \zeta_n^{n-1}$ make up all of the n^{th} roots of unity. This allows us to factorise $x^n - 1 = \prod_{i=0}^{n-1}(x - \zeta_n^i)$ in $\mathsf{C}[x]$.

We call an n^{th} root of unity *primitive* if it is not an m^{th} root of unity for any $m < n$. The primitive roots are thus the elements of order n in the cyclic group of comprising the n^{th} roots of unity. The following lemma is thus obvious:

Lemma 5.44. Let $n > 0$, and for $0 \leq i < n$ define[13] $d_i := \gcd(n, i)$. Then ζ_n^i has order n/d_i, and so it is a primitive $(n/d_i)^{\text{th}}$ root of unity. In particular, ζ_n^i is a primitive n^{th} root of unity if and only if $d_i = 1$.

For each integer $n > 0$, we define the n^{th} *cyclotomic polynomial* to be

$$\Phi_n(x) := \prod_{\substack{0 \leq i < n \\ \gcd(i,n)=1}} (x - \zeta_n^i).$$

We note that $\deg(\Phi_n) = \phi(n)$, where $\phi(n) := |\{i : 0 \leq i < n, \gcd(i, n) = 1\}|$ is Euler's phi-function. Observe that in particular, for p prime, we have $\Phi_p(x) = (x^p - 1)(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$. It is easy to prove (by induction) that:

Proposition 5.45. For each $n \geq 0$, $\Phi_n(x)$ has coefficients in Z and leading coefficient 1.

It is a very useful fact that cyclotomic polynomials are irreducible!

Theorem 5.46. Φ_n is irreducible in $\mathsf{Z}[x]$ for all $n > 0$.

The proof for prime n uses Eisenstein's criterion applied to $\Phi_n(x+1)$. In general, however, the proof uses formal derivatives of polynomials.

[13] Recall that $\gcd(n, 0) = n$ for any $n > 0$.

This guide would not be possible without our wonderful sponsors: