Algebra-2: Groups and Rings

Dmitriy Rumynin

January 23, 2008

1©Dmitriy Rumynin 2007
How to use these notes

The lecture notes are split into 4 chapters, further split into 28 sections. Each section will be discussed on a separate lecture. You should still consult these written notes because my planning may not be perfect and some material in a section could be skipped during the lecture. You should still learn it because it could appear on the exam. Each section contains exercises that you should do as a warm up for the assignment problems. Go over them on the support classes.

The recommended book is *Concrete Abstract Algebra* by Lauritzen (£20 on Amazon). It is reasonably priced, mostly relevant and quite thin. To encourage you to read it, I will use one of the exercises from the book as an exam problem. The only irrelevant chapter is chapter 5 on Gröbner basis. It is actually a topic of a year 3 module *Computational Algebraic Geometry*. Nevertheless, some people complained about brevity of exposition, which is a downside of being concise.

One UK-style textbook is *Introduction to Algebra* by Cameron (£30 on Amazon). I have not seen the book itself but the content seems quite relevant. Another book worth mentioning is *Algebra* by Artin (£60 on Amazon but you can get a used one for £20). This one will have all details you need and much more than you can bear. Amazingly, most of professional algebraists started with this book and absolutely love it. BTW, my first book was *Algebra* by van der Waerden (£25 for each volume on Amazon) but it appears that most of the mathematicians who hate Algebra in their later life have started with it.

Another alternative is to get two books: one for rings and one for groups. Virtually any pair of books will cover all the topics in these lecture notes, although some interaction between subjects will be missing.

If you see any errors, misprints, oddities of my English, send me an email. Also write me if you think that some bits require better explanation. If you want to contribute by writing a proof, an example, a valuable observation, please, do so and send them to me. Just don’t use WORD. Send them as text files with or without LATEX: put all the symbols you want me to latex between $$. All the contributions will be acknowledged and your name will be covered with eternal sh/fame.

Vista sections are not covered by the exam. These are food for further contemplation or can be used for the second year essays. Too bad that you have already written them!!
I would like to thank second year students of 2007 Rupesh Bhudia, Iain Embrey, Alexander Illingworth, Matthew Hutton, Philip Jackson, Sebastian Jorn, Karl Pountney, Jack Shaw-Dunn, Gareth Speight and Mohamed Swed who noticed various mistakes.
## Contents

1 Basics 7  
1.1 Groups and subgroups ........................................ 7  
1.2 Symmetric groups, rings and subrings ..................... 12  
1.3 Isomorphisms and direct products ............................ 20  
1.4 Cyclic groups, fields and units ............................. 25  
1.5 Equivalence relations and cosets ............................ 30  
1.6 Lagrange’s theorem and applications ...................... 35  
1.7 Generators and dihedral groups ............................. 40  
1.8 Relations and groups of order up to 7 ..................... 44  

2 Homomorphisms 47  
2.1 Homs, Images and Kernels .................................... 47  
2.2 Normal Subgroups .............................................. 54  
2.3 Ideals ............................................................. 59  
2.4 Quotients and homomorphisms ................................ 64  
2.5 More isomorphism theorems ................................... 67  

3 Group action on sets 71  
3.1 Actions, Orbits and Stabilisers .............................. 71  
3.2 Fixed Points and Quotients ................................... 76  
3.3 Conjugacy classes ................................................ 79  
3.4 Conjugacy classes in alternating groups .................... 82  
3.5 Symmetries ....................................................... 86  

4 Factorisation 91  
4.1 Divisibility ...................................................... 91  
4.2 UFD-s ............................................................. 95  
4.3 Primes in Some Rings ......................................... 98
4.4 Gaussian Primes .............................................. 101
4.5 Fractions ...................................................... 103
4.6 Gauss’ Lemma ............................................... 107
4.7 Polynomial Factorisation ................................. 110
4.8 Polynomial Quotients .................................... 113
4.9 Cyclic Vector Spaces ................................... 116
4.10 Idempotents and discrete Fourier transformation . 120
Chapter 1

Basics

1.1 Groups and subgroups

1.1.1 Executive Summary

We define groups and subgroups. We establish their elementary properties. We learn how to define a group by a multiplication table. We also establish various examples of groups.

1.1.2 Definition of a group

Definition. A group is a set $G$ together with a binary operation $\circ : G \times G \to G$ that satisfies the following properties:

(i) (Closure) For all $g, h \in G$, $g \circ h \in G$;
(ii) (Associativity) For all $g, h, k \in G$, $(g \circ h) \circ k = g \circ (h \circ k)$;
(iii) There exists an element $e \in G$ such that:
   (a) (Identity) for all $g \in G$, $e \circ g = g$; and
   (b) (Inverse) for all $g \in G$ there exists $h \in G$ such that $h \circ g = e$.

(Actually Property (i) does not really need stating, because it is implied by the fact that $\circ : G \times G \to G$ is a binary operation on $G$. But it is traditionally the first of the four group axioms, so we have included it here!)

The number of elements in $G$ is called the order of $G$ and is denoted by $|G|$. This may be finite or infinite.

An element $e \in G$ satisfying (iii) of the definition is called an identity element of $G$, and for $g \in G$, an element $h$ that satisfies (iii)(b) of the definition ($h \circ g = e$) is called an inverse element of $g$. 

7
CHAPTER 1. BASICS

We shall immediately prove two technical lemmas, which are often included as part of the definition of a group. These two proofs need not be memorised!

Lemma 1.1.1 Let $G$ be a group, let $e \in G$ be an identity element, and for $g \in G$, let $h \in G$ be an inverse element of $G$. Then $g \circ e = g$ and $g \circ h = e$.

Proof: We have $h \circ (g \circ e) = (h \circ g) \circ e = e \circ e = e = h \circ g$. Now let $h'$ be an inverse of $h$. Then multiplying the left and right sides of this equation on the left by $h'$ and using associativity gives $(h' \circ h) \circ (g \circ e) = (h' \circ h) \circ g$. But $(h' \circ h) \circ (g \circ e) = e \circ (g \circ e) = g \circ e$, and $(h' \circ h) \circ g = e \circ g = g$, so we get $g \circ e = g$.

We have $h \circ (g \circ h) = (h \circ g) \circ h = e \circ h = h$, and multiplying on the left by $h'$ gives $(h' \circ h) \circ (g \circ h) = h' \circ h$. But $(h' \circ h) \circ (g \circ h) = e \circ (g \circ h) = g \circ h$ and $(h' \circ h) = e$, so $g \circ h = e$. 

Lemma 1.1.2 Let $G$ be a group. Then $G$ has a unique identity element, and any $g \in G$ has a unique inverse.

Proof: Let $e$ and $f$ be two identity elements of $G$. Then, $e \circ f = f$, but by Lemma 1.1.1, we also have $e \circ f = e$, so $e = f$ and the identity element is unique.

Let $h$ and $h'$ be two inverses for $g$. Then $h \circ g = h' \circ g = e$, but by Lemma 1.1.1 we also have $g \circ h = e$, so

$$h = e \circ h = (h' \circ g) \circ h = h' \circ (g \circ h) = h' \circ e = h'$$

and the inverse of $g$ is unique. 

Definition. A group is called abelian or commutative if it satisfies the additional property:

(Commutativity) For all $g, h \in G$, $g \circ h = h \circ g$.

We shall now proceed to change notation!

The groups in this course will either be:

- Multiplicative groups, where we omit the $\circ$ sign ($g \circ h$ becomes just $g h$), we denote the identity element by 1 rather than by $e$, and we denote the inverse of $g \in G$ by $g^{-1}$; or
- Additive groups, where we replace $\circ$ by $+$, we denote the identity element by 0, and we denote the inverse of $g$ by $-g$. 

1.1. GROUPS AND SUBGROUPS

If there is more than one group around, and we need to distinguish between the identity elements of $G$ and $H$ say, then we will denote them by $1_G$ and $1_H$ (or $0_G$ and $0_H$).

Additive groups will always be commutative, but multiplicative groups may or may not be commutative. The default will be to use the multiplicative notation.

The proof of the next lemma is not in the lecture. Try proving it yourself before reading my proof. From now on, this result will be used freely and without explicit reference.

Lemma 1.1.3 Let $g,h$ be elements of the multiplicative group $G$. Then $(gh)^{-1} = h^{-1}g^{-1}$.

Proof: Let us confirm by a calculation that $h^{-1}g^{-1}$ is the inverse of $gh$. Indeed, $(h^{-1}g^{-1}) \cdot (gh) = h^{-1}(g^{-1} \cdot g)h = h^{-1}h = e$. □

1.1.3 Examples – Numbers

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ or indeed the elements of any field form a group under addition. We sometimes denote these by $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, etc.

Now let $K$ be any field (we will define a field later), such as $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$, and let $K^* = K \setminus \{0\}$. Then $K^*$ is a group under multiplication. But note that $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ is not a group under multiplication, because most elements do not have multiplicative inverses.

All of these groups are abelian.

1.1.4 Example – Klein four group

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

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>1</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>1</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>a</td>
<td>1</td>
</tr>
</tbody>
</table>

However, if the group is infinite or finite but large, the multiplication table approach is not quite practical. For instance, a famous big monster group has nearly $10^{52}$ elements. Do you think it is a good idea to write its multiplication table? However, this group can be explicitly described as a subgroup of a larger group, which can be well understood.
1.1.5 Definition of a subgroup

**Definition.** A subset $H$ of a group $G$ is called a *subgroup* of $G$ if it forms a group under the same operation as that of $G$.

**Lemma 1.1.4** If $H$ is a subgroup of $G$, then the identity element $1_H$ of $H$ is equal to the identity element $1_G$ of $G$.

**Proof:** Clearly, $1_H \cdot 1_H = 1_H$. Multiplying by the inverses in $G$ gives $1_H^{-1}$ gives desired $1_H = 1_G$. This lemma implies that $1_G \in H$, in particular, $H$ is non-empty. Indeed, the empty set is not a subgroup because it is not a group. The identity axiom fails!

**Proposition 1.1.5** Let $H$ be a nonempty subset of a group $G$. Then $H$ is a subgroup of $G$, if and only if

(i) $h_1, h_2 \in H \Rightarrow h_1 h_2 \in H$; and

(ii) $h \in H \Rightarrow h^{-1} \in H$.

**Proof:** $H$ is a subgroup of $G$ if and only if the four group axioms hold in $H$. Two of these, 'Closure', and 'Inverses', are the conditions (i) and (ii) of the lemma, and so if $H$ is a subgroup, then (i) and (ii) must certainly be true. Conversely, if (i) and (ii) hold, then we need to show that the other two axioms, 'Associativity' and 'Identity' hold in $H$. Associativity holds because it holds in $G$, and $H$ is a subset of $G$. Since we are assuming that $H$ is nonempty, there exists $h \in H$, and then $h^{-1} \in H$ by (ii), and $hh^{-1} = 1 \in H$ by (i), and so 'Identity' holds, and $H$ is a subgroup.

**Proposition 1.1.6** Let $H$ be a nonempty subset of a group $G$. Then $H$ is a subgroup of $G$, if and only if $h, g \in H \Rightarrow hg^{-1} \in H$.

**Proof:** Let us build on Proposition 1.1.5. If its condition holds then $g^{-1} \in H$ and, consequently, $hg^{-1} \in H$.

On the other hand if $h, g \in H \Rightarrow hg^{-1} \in H$ then $h^{-1} = (hh^{-1})h^{-1} \in H$. Hence, $h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H$.

**Corollary 1.1.7** The intersection of any set of subgroups of $G$ is itself a subgroup of $G$.

**Proof:** Let $X = \{H\}$ be a set of subgroups of $G$ and $T = \cap_{H \in X} H$. If $h, g \in T$ then $h, g \in H$ for all $H \in X$. By Proposition 1.1.6, $hg^{-1} \in H$ for all $H \in X$ and consequently to its intersection $T$. 


1.1.6 Examples – Trivial Subgroups

There are two standard subgroups of any group \( G \): the whole group \( G \) itself, and the trivial subgroup \( \{1\} \) consisting of the identity alone. Subgroups other than \( G \) are called proper subgroups, and subgroups other than \( \{1\} \) are called nontrivial subgroups.

1.1.7 Elementary Properties – the Cancellation Laws

Proposition 1.1.8 Let \( G \) be any group, and let \( g, h, k \in G \). Then

(i) \( gh = gk \Rightarrow h = k \); and
(ii) \( hg = kg \Rightarrow h = k \).

Proof: For (i), we have \( gh = gk \Rightarrow g^{-1}gh = g^{-1}gk \Rightarrow h = k \), and (ii) is proved similarly by multiplying by \( g^{-1} \) on the right. \( \square \)

1.1.8 Exercises

(i) Prove the lemmas in Section 1.1.5.

(ii) What is the intersection of the subgroups \( \mathbb{R}^* \) and \( \{z \mid |z| = 1\} \) of the multiplicative group of the complex numbers \( \mathbb{C}^* \)?
CHAPTER 1. BASICS

1.2 Symmetric groups, rings and subrings

1.2.1 Executive Summary

We discuss our first example of a non-abelian group and its subgroup. We proceed, similarly to groups, to define rings and subrings and establish their elementary properties.

1.2.2 Symmetric and alternating groups

Let \( X \) be any set, and let \( \text{Sym}(X) \) denote the set of permutations of \( X \); that is, the bijections from \( X \) to itself. Then \( \text{Sym}(X) \) is a group under composition of maps. It is known as the symmetric group on \( X \).

The proof that \( \text{Sym}(X) \) is a group uses results from Foundations. Note that the composition of two bijections is a bijection, and that composition of any maps obeys the associative law. The identity element of the group is just the identity map \( X \to X \), and the inverse element of a map is just its inverse map.

Let us recall the cyclic notation for permutations. If \( a_1, \ldots, a_r \) are distinct elements of \( X \), then the cycle \( (a_1, a_2, \ldots, a_r) \) denotes the permutation of \( \phi \in \text{Sym}(X) \) with

(i) \( \phi(a_i) = a_{i+1} \) for \( 1 \leq i < r \).
(ii) \( \phi(a_r) = a_1 \), and
(iii) \( \phi(b) = b \) for \( b \in X \setminus \{a_1, a_2, \ldots, a_r\} \).

When \( X \) is finite, any permutation of \( X \) can be written as a product (= composite) of disjoint cycles. Note that a cycle \( (a_1) \) of length 1 means that \( \phi(a_1) = a_1 \), and so this cycle can (and normally is) omitted.

For example, if \( X = \{1, 2, 3, 4, 5, 6, 7, 8\} \) and \( \phi \) maps 1, 2, 3, 4, 5, 6, 7, 8 to 5, 8, 6, 4, 3, 1, 2, 7, respectively, then \( \phi = (1, 5, 3, 6)(2, 8, 7) \), where the cycle (4) of length 1 has been omitted. We will denote the identity permutation in cyclic notation by \( () \).

Remember that a composite \( \phi_2 \phi_1 \) of maps means \( \phi_1 \) followed by \( \phi_2 \), so, for example, if \( X = \{1, 2, 3\} \), \( \phi_1 = (1, 2, 3) \) and \( \phi_2 = (1, 2) \), then \( \phi_1 \phi_2 = (1, 3) \), whereas \( \phi_2 \phi_1 = (2, 3) \). This example shows that \( \text{Sym}(X) \) is not in general a commutative group. (In fact it is commutative only when \( |X| \leq 2 \).)

The inverse of a permutation can be calculated easily by just reversing all of the cycles. For example, the inverse of \( (1, 5, 3, 6)(2, 8, 7) \) is \( (6, 3, 5, 1)(7, 8, 2) \), which is the same as \( (1, 6, 3, 5)(2, 7, 8) \). (The cyclic representation is not
The following properties of Sym($X$) were studied in Linear Algebra in connection with the definition of the determinant. Let $G = \text{Sym}(X)$ be the symmetric group on the finite set $X$. A cycle of length two is called a transposition. Since an arbitrary cycle like $(1, 2, 3, \ldots, n)$ can be written as a product of transpositions (for example, $(1, 2, 3, \ldots, n) = (1, 2)(2, 3)(3, 4)\ldots(n-1, n)$), we have:

**Lemma 1.2.1** Any permutation on $X$ can be written as a product of transpositions.

A permutation is called even if it is a product of an even number of transpositions, and odd if it is a product of an odd number of transpositions. In order for this to make much sense, we do need to prove the following:

**Proposition 1.2.2** No permutation is both even and odd.

We will discuss a proof of this proposition later on in this course (see examples in section 2.1.2).

Let $\text{Alt}(X)$ be the set $H$ of all even permutations in $\text{Sym}(X)$. It is non-empty since the identity permutation is in $\text{Alt}(X)$. Finally, by Proposition 1.1.6 if $g = \sigma_1\ldots\sigma_{2k}, h = \pi_1\ldots\pi_{2m} \in \text{Alt}(X)$, are both even where $\sigma_i$ and $\pi_i$ are transpositions then

$$gh^{-1} = (\sigma_1\ldots\sigma_{2k})(\pi_1\ldots\pi_{2m})^{-1} = (\sigma_1\ldots\sigma_{2k})(\pi_{2m}\ldots\pi_1) \in \text{Alt}(X),$$

proving that $\text{Alt}(X)$ is a subgroup known as the alternating group of $X$.

Notice that a cycle of odd length is a product of an even number of transpositions, and a cycle of even length is a product of an odd number of transpositions. This makes it easy to decide whether a given permutation in cyclic notation is even or odd (but it is also easy to make mistakes!).

### 1.2.3 Definition of a ring

**Definition.** A ring is a set $R$ together with two binary operations $+, \cdot : R \times R \to R$ that satisfy the following properties:

(i) (Group under addition) $(R, +)$ is an abelian group.
(ii) (Associativity) For all $a, b, c \in R$, $(ab)c = a(bc)$;
(iii) (Distributivity) For all $a, b, c \in R$, $(a+b)c = ac+bc$ and $a(b+c) = ab+ac$. 
(iv) (Identity) There exists an element $1 \in R$ such that for all $a \in R$, $1a = a1 = a$.

As in the usual arithmetic, multiplication takes precedence over addition.

The identity element in a ring behaves slightly differently from the identity element in the group. As a start, $1a = a$ does not formally imply $a1 = a$. Nevertheless, the identity is unique.

**Lemma 1.2.3** Let $R$ be a ring. Then $R$ has a unique identity element.

**Proof:** Let 1 and $1'$ be two identity elements of $R$. Then, $1 = 11' = 1'$. □

Besides, various books will treat the identity axiom differently. Some would skip this axiom identity axiom all together. This would allow the following degenerate example to be called a ring. Take an abelian group $A$ and define $xy = 0_A$ for all $x, y \in A$. The multiplication is identically zero!! If such things show up in the course, we would call them rings without identity. There are some meaningful examples of them in the exercises to this section.

What happens if $1 = 0$?

**Lemma 1.2.4** Let $R$ be a ring such that $0 = 1$. Then $R = \{0\}$.

**Proof:** For all $x$, $x = x1 = x0 = 0$. □

The ring $\{0\}$ a ring is called the zero ring. It is not a useful ring. All other rings will be called nonzero rings.

**Definition.** A ring $R$ is commutative if it satisfies

(v) (Commutativity) For all $a, b \in R$, $ab = ba$.

### 1.2.4 Examples – Numbers

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative rings under usual addition and multiplication. Quaternions $\mathbb{H}$, which you will see in exercises, is a ring, which is no longer commutative.

Another important example coming from number is the ring of residues modulo $n$. Pick a positive integer $n$. Then $\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$ with multiplication and addition coming from usual ones modulo $n$. For instance, in $\mathbb{Z}_6$, $4 + 5 = 3$ (residue of 9 modulo 6), $4 \cdot 5 = 2$ (residue of 20 modulo 6), $4 \cdot 3 = 0$ (residue of 12 modulo 6).

### 1.2.5 Examples – Matrices

If $R$ is a ring then the set $M_n(R)$ of $n \times n$-matrices with coefficients in $R$ is another ring. The multiplication and addition is the same as you have
learnt in linear algebra: \((a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})\) and \((a_{ij}) \cdot (b_{ij}) = (\sum_k a_{ik} b_{kj})\).
Watch out for the order of multipliers if the ring \(R\) is no longer commutative!!
For the zero ring \(R\), the ring \(M_n(R)\) is also zero. For a non-zero ring \(M_n(R)\) is commutative if and only if \(R\) is commutative and \(n = 1\).

### 1.2.6 Examples – Polynomials

Let \(R\) be a ring, \(X_1, \ldots, X_k\) independent variables. The polynomials in \(X_i\)-s with coefficients in \(R\) form the polynomial ring \(R[X_1, \ldots X_n]\) under the usual addition and multiplication of polynomials.

A multi-index notation is a convenient way to describe addition and multiplication in the polynomial rings. A multi-index \(\alpha = (\alpha_1, \ldots, \alpha_n)\) is an \(n\)-tuple of non-negative integers. They can be added and compared component-wise. A monomial is written as \(X_1^{\alpha_1} \cdot \cdots \cdot X_n^{\alpha_n}\). A polynomial is a linear combination of monomials \(\sum_{\alpha} r_{\alpha} X^\alpha\) with \(r_{\alpha} \in R\), all zero except finitely many. The \((\sum_{\alpha} r_{\alpha} X^\alpha) + (\sum_{\alpha} t_{\alpha} X^\alpha) = \sum_{\alpha} (r_{\alpha} + t_{\alpha}) X^\alpha\) and \((\sum_{\alpha} r_{\alpha} X^\alpha) \cdot (\sum_{\alpha} t_{\alpha} X^\alpha) = \sum_{\alpha} (\sum_{\beta \leq \alpha} r_{\beta} t_{\alpha - \beta}) X^\alpha\).

Observe that \(R[X_1, \ldots X_n]\) is commutative if and only if \(R\) is commutative.

### 1.2.7 Definition of a subring

**Definition.** A subset \(S\) of a ring \(R\) is called a subring of \(R\) if it forms a ring under the same operation as that of \(R\) with the same identity element.

The identity element in the rings gives us a trouble again. It is possible for a subset to be a ring under the same operations but with different identity element. For example, let \((R, +) = K_4 = \{0, a, b, c\}\) be the Klein four group under addition. This is why we use 0 instead of 1. Now we define multiplication by

\[
a \cdot a = a, \ b \cdot b = b, \ a \cdot b = b \cdot a = 0.
\]

I leave it to the next lecture to show that this is indeed a ring. All we want to notice at this point is that its identity is \(c\), for instance,

\[
c \cdot b = (a + b) \cdot b = a \cdot b + b \cdot b = 0 + b = b
\]

Thus, \(S = \{0, a\}\) is a ring with identity \(a\) but not a subring since \(c\) is not in \(S\).

See an exercise to this section for an example. We don’t even give a name to such things. As a logician would put it, *we consider rings with identity in the signature*, whatever it means.
Proposition 1.2.5 Let $S$ be an abelian subgroup of a ring $R$. Then $S$ is a subring of $R$, if and only if

(i) $a_1, a_2 \in S \Rightarrow a_1 a_2 \in S$; and

(ii) $1_R \in S$.

Proof: $S$ is an abelian subgroup of $R$, closed under the multiplication and containing the identity. Thus, $S$ has two operations and identity for multiplication. All ring axioms of $S$ easily follow from the corresponding axioms of $R$. \hfill \Box

Lemma 1.2.6 The intersection of any set of subrings of $R$ is itself a subring.

1.2.8 Example – complex numbers as matrices

The ring of complex numbers $\mathbb{C}$ is a subring of $M_2(\mathbb{R})$. By $i$ we denote the imaginary unit. Then we identify $\alpha + \beta i = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$.

Actually we have to be more careful because this subring and set $\mathbb{C}$ are not actually equal but isomorphic. The precise statement should be The ring of complex numbers $\mathbb{C}$ is isomorphic to a subring of $M_2(\mathbb{R})$. But this is a topic of the next lecture.

1.2.9 Exercises

(i) If $X$ is finite, what is the order of $\text{Sym}(X)$ and $\text{Alt}(X)$ as a function of $|X|$?

(ii) Let $G = \text{Sym}(X)$ again, and let $Y$ be a subset of a set $X$. Show that the subset $G_Y$ of $G$ defined by $G_Y = \{ g \in G \mid g(y) \in Y \text{ and } g^{-1}(y) \in Y \text{ for all } y \in Y \}$ is a subgroup of $G$.

If $X$ is finite, what is the order of $G_Y$ as a function of $|Y|$ and $|X|$?

(iii) Consider a ring $R$ without identity element. Define $\hat{R} = R \times \mathbb{Z}$ with operations given by $(r, n) + (s, m) = (r + s, n + m)$ and $(r, n) \cdot (s, m) = (rs + mr + ns, mn)$. Prove that this is a ring.

(iv) Consider the set $C(\mathbb{R}, \mathbb{R})$ of all functions from real numbers $\mathbb{R}$ to real numbers $\mathbb{R}$, continuous at all but finitely many points. Using the fact from Analysis that the sum and the product of two continuous functions is continuous, prove that $C(\mathbb{R}, \mathbb{R})$ is a ring.
Consider the subset $C_c(\mathbb{R}, \mathbb{R})$ of all compactly supported functions, that is, functions that vanish outside some closed interval $[a, b]$. Prove that $C_c(\mathbb{R}, \mathbb{R})$ is closed under addition and multiplication but not a ring under these operations.

Consider the subset $C([0, 1], \mathbb{R})$ of all functions that vanish outside the closed interval $[0, 1]$. Prove that $C([0, 1], \mathbb{R})$ is a ring under addition and multiplication in $C_c(\mathbb{R}, \mathbb{R})$ but not a subring of $C(\mathbb{R}, \mathbb{R})$.

(v) Consider the standard 3-dimensional vector space $V = \mathbb{R}^3$ with operations $\times$ and $\cdot$ of vector and scalar product. The quaternions are elements of a vector space $\mathbb{H} = \mathbb{R} \oplus V$. They are a bit like complex numbers: $\alpha$ is a real part of a quaternion $(\alpha, v)$, and $v$ is its imaginary part. Quaternions with zero real part are called imaginary.

Prove that the quaternions form a ring under the addition in the vector space and the multiplication defined by formula $(\alpha, v) \cdot (\beta, w) = (\alpha \beta - v \cdot w, \alpha w + \beta v + v \times w)$.

Pick an orthonormal basis $I, J, K$ of $V$. Show that the 8 elements $\pm I, \pm J, \pm K, \pm 1_H$ form a group under multiplication and write explicitly the multiplication table in this group. This group is called quaternion group and denoted $Q_8$.

We define the usual norm on $\mathbb{H}$ by $|((\alpha, v))| = \sqrt{\alpha^2 + |v|^2}$. Show that $|((\alpha, v)) \cdot (\beta, w)| = |((\alpha, v))|(\beta, w)|$.

Show that $\mathbb{H} \setminus \{0\}$ is a group under multiplication but $\mathbb{H}$ is not a field.

Show that all elements of norm 1 form a subgroup. Notice that geometrically it is a 3-sphere $S^3$.

Show that $x^2 = -1$ if and only if $x$ is imaginary of norm 1. Such quaternions form a 2-sphere $S^2$.

Consider a map $\pi : S^3 \to S^2$ defined by $\pi(q) = qIq^{-1}$ for all $q \in S^3$. Show that the inverse image $\pi^{-1}(I)$ is 1-sphere $S^1$.

In fact, $\pi$ is surjective with all inverse images being $S^1$ (you don’t need to prove it). This is called Hopf fibration and it is a very nice way to imagine what $S^3$ looks like.
1.2.10 Vista: from multiplication tensors to superstring theory

Vista sections are not assessed or examined in any way. Skip to the next section if you are allergic to nuts or psychologically fragile!!

While multiplication table is good idea for finite rings, there is a similar way to describe certain types of rings using tensors. Start with a vector space $R$ over reals. The addition will be usual addition in the vector space.

Now pick elements $e_i \in R$ constituting a basis of $R$ as a vector space. We define multiplication for basis elements

$$e_i \cdot e_j = \sum_k m_{i,j}^k e_k \quad (1.1)$$

for uniquely determined $m_{i,j}^k \in \mathbb{R}$. These numbers are called structure constants. Together they form a $(2,1)$-tensor on the vector space $R$.

We extend this formula by bilinearity, so the multiplication in $R$ is distributive. Notice that if $a = \sum_i \alpha_i e_i, \ b = \sum_j \beta_j e_j, \ c = \sum_k \gamma_k e_k$ then

$$(ab)c = \sum_{i,j,k} \alpha_i \beta_j \gamma_k (e_i \cdot e_j) \cdot e_k, \ a(bc) = \sum_{i,j,k} \alpha_i \beta_j \gamma_k e_i \cdot (e_i \cdot e_k).$$

This implies that it is sufficient to check associativity on the basis,

$$(e_i \cdot e_j) \cdot e_k = \sum_s m_{i,j}^s e_s \cdot e_k = \sum_{s,t} m_{i,j}^s m_{s,k}^t e_t.$$ 

Similarly,

$$e_i \cdot (e_j \cdot e_k) = \sum_s m_{j,k}^s e_i \cdot e_s = \sum_{s,t} m_{j,k}^s m_{i,s}^t e_t.$$ 

Thus, associativity is equivalent to the system of quadratic equations on the structure constants

$$\sum_s m_{i,j}^s m_{s,k}^t = \sum_s m_{j,k}^s m_{i,s}^t \quad (1.2)$$

for all possible $i, j, k, s$.

At the end we should not forget to ensure an identity element $1_R = \sum_i u_i e_i$. Usually, it is rather straightforward if $1_R$ exists.

Let us try to get multiplication coefficients in a very naive way. Let $U$ be an open subset of $\mathbb{R}^n$. Let us pick a three times differentiable function $\Phi : U \to \mathbb{R}$ and a point $y \in U$. 


We try to make $R$ into a ring via formula (1.1) with

$$m^k_{i,j} = \frac{\partial^3 \Phi}{\partial x_i \partial x_j \partial x_k}(y).$$

We do want this multiplication to be associative. The equation (1.2) becomes rewritten as

$$\sum_s \frac{\partial^3 \Phi}{\partial x_i \partial x_j \partial x_s}(y) \frac{\partial^3 \Phi}{\partial x_s \partial x_k \partial x_t}(y) = \sum_s \frac{\partial^3 \Phi}{\partial x_j \partial x_k \partial x_s}(y) \frac{\partial^3 \Phi}{\partial x_i \partial x_s \partial x_t}(y).$$

Should you require now to obtain an associative multiplication at every point $y \in U$, you end up with a system of non-linear third order differential equations for each $i, j, k, t$

$$\sum_s \frac{\partial^3 \Phi}{\partial x_i \partial x_j \partial x_s}(y) \frac{\partial^3 \Phi}{\partial x_s \partial x_k \partial x_t}(y) = \sum_s \frac{\partial^3 \Phi}{\partial x_j \partial x_k \partial x_s}(y) \frac{\partial^3 \Phi}{\partial x_i \partial x_s \partial x_t}(y).$$

(1.3)

Why do I tell you all this about differential equations? By the same reason I do Maths: because it is exciting! System (1.3) is known as WDVV-equation in modern physics. It is an equation for potential in Superstring Theory. It is not known how to solve WDVV-equation in general. It is an important problem in modern physics.
CHAPTER 1. BASICS

1.3 Isomorphisms and direct products

1.3.1 Executive Summary

Algebraic structures like rings and groups are rarely equal but often isomorphic. We discuss the notion of the isomorphism. After this we talk about direct products and notice some cool isomorphisms between them. As a tool we introduce the notion of order.

1.3.2 Isomorphisms

Later on, we shall be considering the more general case of homomorphisms, but for now we just introduce the important special case of isomorphisms.

Definition. An isomorphism \( \phi : G \rightarrow H \) between two groups \( G \) and \( H \) is a bijection from \( G \) to \( H \) such that \( \phi(g_1g_2) = \phi(g_1)\phi(g_2) \) for all \( g_1, g_2 \in G \). Two groups \( G \) and \( H \) are called isomorphic if there is an isomorphism between them. In this case we write \( G \cong H \).

The reason this is so important is that isomorphic groups are considered to be essentially the same group – \( H \) can be obtained from \( G \) simply be relabelling the elements of \( G \).

The ring isomorphism is defined the same way.

Definition. An isomorphism \( \phi : R \rightarrow T \) between two rings \( R \) and \( T \) is a bijection from \( R \) to \( T \) such that \( \phi(r_1r_2) = \phi(r_1)\phi(r_2) \) and \( \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) \) for all \( r_1, r_2 \in R \). Two rings \( R \) and \( T \) are called isomorphic if there is an isomorphism between them. In this case we write \( R \cong T \).

In section 1.2.8, we saw that the ring of complex numbers \( \mathbb{C} \) is isomorphic to a subring of \( M_2(\mathbb{R}) \). Here is our first example of a group isomorphism.

Proposition 1.3.1 Let \( X \) and \( Y \) be two sets with \( |X| = |Y| \). Then the groups \( \text{Sym}(X) \) and \( \text{Sym}(Y) \) of all permutations of \( X \) and \( Y \) are isomorphic.

Proof: Let \( \psi : X \rightarrow Y \) be a bijection. The map \( \text{Sym}(X) \rightarrow \text{Sym}(Y) \) defined by \( f \mapsto \psi f \psi^{-1} \) is an isomorphism. \( \square \)

The notation \( \text{Sym}(n) \) or \( S_n \) is standard for the symmetric group on a set \( X \) with \( |X| = n \). By default, we take \( X = \{1, 2, 3, \ldots, n\} \).

Corollary 1.3.2 Let \( X \) and \( Y \) be two finite sets with \( |X| = |Y| \). Then the groups \( \text{Alt}(X) \) and \( \text{Alt}(Y) \) of even permutations of \( X \) and \( Y \) are isomorphic.
As with Sym\((X)\), the isomorphism type of Alt\((X)\) depends only on \(|X|\), and the notation Alt\((n)\) or \(A_n\) is standard for the alternating group on a set \(X\) of size \(n\).

### 1.3.3 Why not equalities?

There are circumstances where it is important that isomorphic groups (or rings) are not equal. Consider the exponential function \(f : \mathbb{R} \to \mathbb{R}_0, f(x) = e^x\). It is a bijection. The domain of this function is a group under addition, while the range is a group under multiplication, and \(f(x + y) = f(x)f(y)\). Hence it is a group isomorphism but you cannot say that these two groups are equal. Just try to convince your bank manager that these two groups are isomorphic when you hit the overdraft limit.

### 1.3.4 Elementary Properties – Orders of Elements

First some more notation. In a multiplicative group \(G\), we define \(g^2 = gg\), \(g^3 = ggg\), \(g^4 = gggg\), etc. Formally, for \(n \in \mathbb{N}\), we define \(g^n\) inductively, by \(g^1 = g\) and \(g^{n+1} = gg^n\) for \(n \geq 1\). We also define \(g^0\) to be the identity element \(1\), and \(g^{-n}\) to be the inverse of \(g^n\). Then \(g^{x+y} = g^x g^y\) for all \(x, y \in \mathbb{Z}\).

In an additive group, \(g^n\) becomes \(ng\), where \(0g = 0\), and \((-n)g = -(ng)\).

**Definition.** Let \(g \in G\). Then order of \(g\), denoted by \(o(g)\) or by \(|g|\), is the least \(n > 0\) such that \(g^n = 1\), if such an \(n\) exists. If there is no such \(n\), then \(g\) has infinite order, and we write \(|g| = \infty\).

Note that if \(g\) has infinite order, then the elements \(g^x\) are distinct for distinct values of \(x\), because if \(g^x = g^y\) with \(x < y\), then \(g^{y-x} = 1\) and \(g\) has finite order.

Similarly, if \(g\) has finite order \(n\), then the \(n\) elements \(g^0 = 1, g^1 = g, \ldots, g^{n-1} = g^{-1}\) are all distinct, and for any \(x \in \mathbb{Z}\), \(g^x\) is equal to exactly one of these \(n\) elements. Proofs of the next three lemmas are left as exercises for the reader.

**Lemma 1.3.3** \(|g| = 1 \iff g = 1\).

**Lemma 1.3.4** If \(|g| = n\) then, for \(x \in \mathbb{Z}\), \(g^x = 1 \iff n|x\).

(Recall notation: for integers \(x, y\), \(x|y\) means \(x\) divides \(y\).

The following result is often useful. It is the first manifestation of the principle that isomorphic groups have the same algebraic properties.
Lemma 1.3.5 If $\phi : G \to H$ is an isomorphism, then $|g| = |\phi(g)|$ for all $g \in G$.

1.3.5 Direct product of groups

Using direct products one can obtain new groups from already known ones.

**Definition.** Let $G$ and $H$ be two (multiplicative) groups. We define the direct product $G \times H$ of $G$ and $H$ to be the set $\{(g, h) \mid g \in G, \ h \in H\}$ of ordered pairs of elements from $G$ and $H$, with the obvious component-wise multiplication of elements $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$ for $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

It is straightforward to check that $G \times H$ is a group under this operation. Note that the identity element is $(1_G, 1_H)$, and the inverse of $(g, h)$ is just $(g^{-1}, h^{-1})$.

Notice that both $G$ and $H$ are (isomorphic to) subgroups of $G \times H$. $G$ becomes a subgroup of elements of the form $(g, 1_H)$ and $H$ becomes a subgroup of elements of the form $(1_G, h)$.

If the groups are additive, then it is sometimes called the direct sum rather than the direct product, and written $G \oplus H$. For instance, in Linear Algebra you used to talk about direct sums of vector spaces.

1.3.6 Direct product of rings

Direct products can be used with rings.

**Definition.** Let $R$ and $S$ be two rings. We define the direct product $R \times S$ of $R$ and $S$ to be the set $\{(r, s) \mid r \in R, \ s \in S\}$ of ordered pairs of elements from $R$ and $S$, with the obvious component-wise addition and multiplication $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$, $(r_1, s_1)(r_2, s_2) = (r_1r_2, s_1s_2)$ for $r_1, r_2 \in R$ and $s_1, s_2 \in S$.

It is straightforward to check that $R \times S$ is a ring under these operations. Note that the identity element is $(1_R, 1_S)$ but $R$ and $S$ are not subrings of $R \times S$, in general. Indeed, $R$ can be thought of as elements of the form $(r, 0_S)$ but it does not contain the identity element of $R \times S$.

As a matter of fact, the ring in the last lecture whose additive group is $K_4$ is the direct product $Z_2 \times Z_2$. 
1.3.7 Direct products of residue rings

We would like to make the following observation about the residue rings, which is a version of the Chinese Remainder Theorem, which we will prove later in the course. For now, we will use the following fact that you must have learnt in Foundations (if not, we will prove it later on as well): integers \( m \) and \( n \) are coprime (have no common prime divisors) if and on if there exist integers \( a \) and \( b \) such that \( am + bn = 1 \).

**Proposition 1.3.6** The rings \( \mathbb{Z}_m \times \mathbb{Z}_n \) and \( \mathbb{Z}_{mn} \) are isomorphic if and only if \( m \) and \( n \) are relatively prime.

**Proof:** The “only if” bit follows from Lemma 1.3.5. If \( m \) and \( n \) are not relatively prime then their least common multiple \( l = \text{lcm}(m,n) \) is less than \( mn \). The abelian additive groups are not isomorphic because \( |1| = mn \) in \( (\mathbb{Z}_{mn},+) \) but for any element \( (a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n \), we have \( l(a,b) = (la,lb) = 0 \), so no element of \( \mathbb{Z}_m \times \mathbb{Z}_n \) has order \( mn \).

If \( m \) and \( n \) are coprime then there exist integers \( a,b \) such that \( am + bn = 1 \).

Let \( (x)_n \) be the residue of \( x \mod n \). We define \( \phi : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n \) by \( \phi(x) = ((x)_m,(x)_n) \). It is obvious that \( \phi(x+y) = \phi(x) + \phi(y) \) and \( \phi(xy) = \phi(x)\phi(y) \).

It remains to show that \( \phi \) is a bijection. We do it by writing the inverse map explicitly: \( \phi^{-1}(y,z) = (amz + bny)_{mn} \). Since both sets have the same cardinality \( nm \), it suffices to observe that \( \phi((amz + bny)_{mn}) = (((amz + bny)_{mn})_m,((amz + bny)_{mn})_n) = ((amz + bny)_m, (amz + bny)_n) = ((bny)_m, (amz)_n) = (y,z) \) with the last equality ensured by \( (bn)_m = 1 = (am)_n \) since \( am + bn = 1 \).

Using induction on \( k \), one derives the following corollary.

**Corollary 1.3.7** If \( n = p_1^{a_1} \cdots p_k^{a_k} \) is a decomposition of \( n \) into a product of distinct primes then \( \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}} \) as rings.

1.3.8 Exercises

(i) Show that the relationship between groups of being isomorphic satisfies the conditions of an equivalence relation; that is, \( G \cong G, G \cong H \Rightarrow H \cong G \), and \( G \cong H, H \cong K \Rightarrow G \cong K \).

(ii) Prove Lemma 1.3.5.

(iii) Show that \( \mathbb{Q}_8 \) is isomorphic to a subgroup of \( GL(2, \mathbb{C}) \). By \( i \) we denote the imaginary unit. The isomorphism is constructed using Pauli’s matrices:
1 ↦ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I ↦ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad -1 ↦ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad -I ↦ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},
J ↦ \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad K ↦ \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \quad -J ↦ \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \quad -K ↦ \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.

(iv) Show that \( \mathbb{H} \) is isomorphic to a subring of \( M_2(\mathbb{C}) \).
1.4 Cyclic groups, fields and units

1.4.1 Executive Summary

There are two main topics: cyclic groups and units. As a byproduct we define fields. We also discuss units in some specific rings.

1.4.2 Cyclic Groups

Definition. A group $G$ is called cyclic, if it consists of the integral powers of a single element. In other words, $G$ is cyclic if there exists an element $g$ in $G$ with the property that, for all $h \in G$, there exists $x \in \mathbb{Z}$ with $g^x = h$.

The element $g$ is called a generator of $G$.

The most familiar examples of cyclic groups are additive groups rather than multiplicative. The group $(\mathbb{Z}, +)$ of integers under addition is cyclic, because every integer $x$ is equal to $x1$, and so 1 is a generator. Notice that $-1$ is also a generator. The additive group $(\mathbb{Z}_n, +)$ of residues mod $n$ is also cyclic with the generator 1. Again any other residue $x$ is equal to $x1$. However, it can have a number of generators, which is clarified in the following lemma, whose proof has been omitted in class.

Lemma 1.4.1 In an infinite cyclic group, any generator $g$ has infinite order. In a finite cyclic group of order $n$, generators are exactly elements of order $n$.

Proof: Let $G$ be a cyclic group, $g \in G$ a generator. If $|g| = k < \infty$ then $g^m = g^{m+k} = g^{m+tk}$ for all $t, m \in \mathbb{Z}$. Hence, $g^m = g^{(m)_k}$ and $\{g^m \mid m \in \mathbb{Z}\}$ contains at most $k$ elements. This proves the first statement.

For the second statement, we use Lemma 1.3.4 to conclude that the set $\{g^m \mid m \in \mathbb{Z}\}$ contains exactly $k$ elements. The second statement follows.

Proposition 1.4.2 Any two infinite cyclic groups are isomorphic. For a positive integer $n$, any two cyclic groups of order $n$ are isomorphic.

Proof: If $G$ and $H$ are infinite cyclic groups with generators $g$ and $h$, then $G = \{g^x \mid x \in \mathbb{Z}\}$ and $H = \{h^x \mid x \in \mathbb{Z}\}$. We saw in Subsection 1.3.4 that the elements $g^x$ of $G$ are distinct for distinct $x \in \mathbb{Z}$, and so the map $\phi : G \rightarrow H$ defined by $\phi(g^x) = h^x$ for all $x \in \mathbb{Z}$ is a bijection, and it is easily checked to be an isomorphism.

If $G$ and $H$ are finite cyclic groups of order $n$, then $G = \{g^x \mid x \in \mathbb{Z}_n\}$ and $H = \{h^x \mid x \in \mathbb{Z}_n\}$ and the map $\phi : G \rightarrow H$ defined by $\phi(g^x) = h^x$ for all $x \in \mathbb{Z}_n$ is an isomorphism.
We denote a cyclic group of order $m$ by $C_m$. Since any two such groups are isomorphic, this notation is effectively unambiguous.

1.4.3 Units

**Definition.** An element $x$ of a ring $R$ is called a unit if there exists an element $x' \in R$ such that $xx' = x'x = 1_R$.

**Lemma 1.4.3** All the units in a ring $R$ form a group under multiplication.

**Proof:** Let us denote $R^*$ the set of all units in $R$. The product on $R^*$ is associative because the product on $R$ is associative. The identity element of $R^*$ is $1_R$ and the inverse of $x$ is $x'$.

In particular, $x'$ is unique and will be denoted $x^{-1}$ to be consistent with the rest of the notation. The group $R^*$ is called the group of units of the ring $R$.

1.4.4 Definition of a field

**Definition.** A field is a commutative ring $K$ such that $K^* = K \setminus \{0\}$. A subfield is subring of a field, which is a field under the same operations.

Let us look at some familiar rings. For integers, $\mathbb{Z}^* = \{\pm 1\} \neq \mathbb{Z} \setminus \{0\}$, so $\mathbb{Z}$ is not a field. For complex numbers, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, so $\mathbb{C}$ is a field. For the zero ring, $\mathbb{Z}_1^* = \{0\} \neq \mathbb{Z} \setminus \{0\} = \emptyset$, so $\mathbb{Z}_1$ is not a field. This seems strange but there are reasons not to consider the zero ring a field. Thus, a field has at least two distinct elements $0 \neq 1$.

1.4.5 Units in residues rings

We are in a position to understand units in the residue rings completely.

**Lemma 1.4.4** $x \in \mathbb{Z}_n^*$ if and only if $x$ and $n$ are coprime.

**Proof:** If $x$ and $n$ are not coprime then $d = \gcd(x, n) > 1$. Hence $d$ divides $xy$ for all $y \in \mathbb{Z}_n$. Hence $xy$ is never 1 and $x$ is not a unit.

If $x$ and $n$ are coprime (have no common prime divisors) then there exist integers $a$ and $b$ such that $ax + bn = 1$ (in $\mathbb{Z}$). This implies that $x$ is a unit with $x^{-1} = (a)_n$ in $\mathbb{Z}_n$. 

Notice that the order of $m$ in the additive group $(\mathbb{Z}_n, +)$ is $n/\gcd(m, n)$. Hence, Lemma 1.4.4 tells us that $\mathbb{Z}_n^*$ is exactly the set of elements of order $n$ in the additive group. By Lemma 1.4.1, $\mathbb{Z}_n^*$ is exactly the set of generators in the additive group.

The following corollary describes which of the residues rings are fields.
1.4. CYCLIC GROUPS, FIELDS AND UNITS

Corollary 1.4.5 \( \mathbb{Z}_m \) is a field if and only if \( m \) is prime.

Proof: Every divisor of \( m \) will be a non-unit in \( \mathbb{Z}_m \). So \( \mathbb{Z}_m \) is not a field unless \( m \) is prime. If \( m \) is prime it is a field by Lemma 1.4.4. \( \square \)

Definition. The Euler function \( \varphi: \mathbb{N} \to \mathbb{N} \) is defined as \( \varphi(m) = |\mathbb{Z}_m^*| \).

By Lemma 1.4.4, \( \varphi(m) \) is equal to the number of integers between 1 and \( m - 1 \), coprime with \( m \). According to our discussion above, \( \varphi(m) \) is equal to the number of generators of the cyclic group \( C_m \). The following lemma allows us to compute the Euler function explicitly.

Lemma 1.4.6 If \( R \) and \( S \) are rings, the groups \( (R \times S)^* \) and \( R^* \times S^* \) are isomorphic.

Proof: Both groups are subsets of the ring \( R \times S \). Let us observe that these subsets are equal: \((r, s) \in (R \times S)^* \) if and only if \( \exists (a, b) \in R \times S \) \( (a, b)(r, s) = (1, 1) \) if and only if \( \exists a \in R, b \in S \) \( ar = 1, bs = 1 \) if and only if \( r \in R^* \) \& \( s \in S^* \) if and only if \( (r, s) \in R^* \times S^* \). The required isomorphism is the identity map, which clearly preserves the multiplication. \( \square \)

Corollary 1.4.7 If \( m \) and \( n \) are coprime then \( \varphi(mn) = \varphi(m)\varphi(n) \)

Proof: It follows immediately from lemmas 1.3.6 and 1.4.6 \( \square \)

Corollary 1.4.8 If \( m = p_1^{a_1} \cdots p_k^{a_k} \) where \( p_i \) are distinct primes then \( \varphi(m) = \prod_{i=1}^{k} (p_i^{a_i} - p_i^{a_i-1}) \).

Proof: By corollary 1.4.7, \( \varphi(m) = \prod_{i=1}^{k} \varphi(p_i^{a_i}) \). By Lemma 1.4.6, \( m \in \mathbb{Z}_p^{a_i} \) is a unit if and only if \( m \) is coprime to \( p_i^{a_i} \). The latter is equivalent to not being divisible by \( p_i \). The residues divisible by \( p_i \) are of the form \( xp_i \) for some \( x \), so there are exactly \( p_i^{a_i-1} \) of them. Hence \( \varphi(p_i) = p_i^{a_i} - p_i^{a_i-1} \) finishing the proof. \( \square \)

1.4.6 Units in matrix rings

I have had little time to cover this section in class but you know all this already from your Linear Algebra class.

Definition. The group of units in \( M_n(R) \) is called the general linear group and denoted \( \text{GL}_n(R) \).

This group exists for any ring \( R \). You have studied it in Linear Algebra, at least for \( R = \mathbb{C} \) and \( R = \mathbb{R} \). A crucial tool for these studies is the
The determinant possesses the standard properties for any commutative ring $R$. In particular,

**Lemma 1.4.9** Let $R$ be a commutative ring, $A \in M_n(R)$. Then $A \in \text{GL}_n(R)$ if and only if $\det(A) \in R^*$.

**Proof:** The only if part follows from the multiplicativity of determinant. If $AB = I$ then $1 = \det(AB) = \det(A) \det(B)$. The if part is immediate using row decomposition into the minors. If $M = (A_{i,j})$ is the matrix of minors then the row decomposition says that $AM^T = \det(A)I$. Hence, $A^{-1} = \det(A)^{-1}M^T$. \hfill $\square$

For instance, $\text{GL}_n(\mathbb{Z})$ consists of integer matrices with determinant $\pm 1$ or $\text{GL}_n(K)$ for a field $K$ consists of matrices with nonzero determinant.

**Definition.** For a commutative ring $R$, the special linear group $\text{SL}_n(R) = \{A \in M_n(R) | \det(A) = 1\}$.

**Lemma 1.4.10** Let $R$ be a commutative ring. Then $\text{SL}_n(R)$ is a subgroup of $\text{GL}_n(R)$.

Notice that if the ring is no longer commutative the definition of the determinant does not work. Say $n = 2$, which of the following would be the determinant: $a_{11}a_{22} - a_{12}a_{21}$, $a_{11}a_{22} - a_{21}a_{12}$, $a_{22}a_{11} - a_{12}a_{21}$, or $a_{22}a_{11} - a_{21}a_{12}$? All these elements could be distinct and none of them will do the job as a determinant.

There are other distinguished subgroups of $\text{GL}_n(R)$, namely orthogonal, symplectic and unitary, which will be defined in the exercises.

**1.4.7 Exercises**

(i) Let $n$ be a positive integer number. Let $H_n = \{z \in \mathbb{C} | z^n = 1\}$. Show that $H_n$ is a subgroup of the multiplicative group of the complex numbers. Prove that $H_n$ is a cyclic group of order $n$.

(ii) Compute the group of units in the polynomial ring $K[X_1, \ldots, X_n]$ where $K$ is a field.

(iii) Prove Lemma 1.4.9 (Hint: use cofactors or minors.)
(iv) Prove Lemma 1.4.10

(v) Let $A \in M_n(R)$ where $R$ is a commutative ring. Recall that a transposed matrix is defined by $(a_{ij})^T = (a_{ji})$. Let us define $O_n(R, A) = \{X \in \text{GL}_n(R) | XAX^T = A\}$. Show that $O_n(R, A)$ is a subgroup of $\text{GL}_n(R)$.

Explain where you have used the commutativity of $R$.

The group $O_n(R, A)$ is a generalised orthogonal group. Choosing particular $A$ will give you orthogonal, Lorentzian and symplectic groups. For instance, $A = I$, the identity matrix, gives the usual orthogonal group.

(vi) Let $R$ be a ring with involution $\ast$, the latter is an abelian group isomorphism from $R$ to $R$ such that $(ab)^\ast = b^\ast a^\ast$ for all $a, b \in R$ (examples of such are complex conjugation on $\mathbb{C}$ or $\mathbb{H}$ or the identity map on a commutative ring). We define a conjugate matrix by $(a_{ij})^\ast = (a_{ji}^\ast)$. The generalised unitary group (as a set) is $U_n(R, A) = \{X \in \text{GL}_n(R) | XAX^* = A\}$ for some $A \in M_n(R)$. Show that $U_n(R, A)$ is a subgroup of $\text{GL}_n(R)$.

(vii) Let $U$ be the group of quaternions of norm 1 under multiplication. Show that $\mathbb{H}^*$ is isomorphic to $U \times (\mathbb{R}, +)$.
1.5 Equivalence relations and cosets

1.5.1 Executive Summary
We define equivalence relations and equivalence classes. We introduce cosets, an important example of equivalence classes.

1.5.2 Binary Relations
Let $X$ be a set.

**Definition.** A binary relations on $X$ is a subset $R$ of $X \times X$.

We write $xRy$ whenever $(x, y) \in R$. For instance, let $X = \mathbb{R}$. The relation greater is a subset $\{(x, y) \in \mathbb{R}^2 | x > y\}$.

There is a certain shift of paradigm when we talk about binary relations in this way. This abstract approach can be pushed to other objects, for instance, binary operations! We can think of a multiplication on a group $G$ as a subset $\{(a, b, c) \in G^3 | ab = c\}$ of $G^3$.

**Definition.** Let $R$ be a binary relation on a set $X$. We say that $R$ is

(i) **symmetric** if $\forall x, y \in X \ xRy \implies yRx$;

(ii) **reflexive** if $\forall x \in X \ xRx$;

(iii) **transitive** if $\forall x, y \in X \ xRy \ & \ yRz \implies xRz$.

For instance, the relation greater is transitive but neither reflexive, nor symmetric.

1.5.3 Equivalence Relations
The binary relation equal is reflexive, transitive and symmetric. The following definition generalises this situation.

**Definition.** A binary relation is an equivalence relation if it is reflexive, transitive and symmetric.

You already saw the following examples of non-trivial equivalence relations in Linear Algebra and Foundations. We are not going to check here that these are indeed equivalence relations. This easily follows from the material later in the course. Example 1 is the equivalence relation given by cosets of $n\mathbb{Z}$ in Section 1.5.4. The later three examples are coming from group actions in Section 3.1.1

**Examples.** 1. Let $X = \mathbb{Z}$, $n \in \mathbb{Z}$, $n \neq 0$. We say that $x \sim_n y$ if $n$ divides $x - y$. This equivalence relation, called congruent modulo $n$, appear in Foundations.
2. Let $X = F^{n \times m}$ be the set of all $n \times m$-matrices over a field $F$. The equivalence relation *equivalent* appears in Linear Algebra. Let us recall that $A \sim B$ if and only if $A$ and $B$ have the same rank if and only if $A$ can be transformed to $B$ by elementary row and column transformations if and only if there exist $P \in \text{GL}_n(F)$, $Q \in \text{GL}_m(F)$ such that $PAQ = B$ if and only if $A$ and $B$ represent the same linear map $f : F^m \to F^n$ in different bases of the two vector spaces.

3. Let $X = F^{n \times n}$ be the set of all $n \times n$-matrices over a field $F$. The equivalence relation *similar* appears in Linear Algebra. Let us recall that $A \sim B$ if and only if $A$ and $B$ have the same Jordan normal form if and only if there exists $P \in \text{GL}_n(F)$ such that $PAP^{-1} = B$ if and only if $A$ and $B$ represent the same linear map $f : F^n \to F^n$ in different bases of the vector space.

4. Let $X = S(\mathbb{R}^{n \times n})$ be the set of all symmetric $n \times n$-matrices over the real numbers $\mathbb{R}$. This equivalence relation without a special name appears in Algebra-1. In this relation $A \sim B$ if and only if $A$ and $B$ have the same signature if and only if there exists $P \in \text{GL}_n(F)$ such that $PAP^T = B$ if and only if $A$ and $B$ represent the same quadratic form $q : \mathbb{R}^n \to \mathbb{R}$ in different bases of the two vector spaces.

**Definition.** Given an equivalence relation $R$ on $X$ and $a \in X$, the equivalence class of $a$ is the following set $[a] = \{ x \in X \mid xRa \}$.

**Proposition 1.5.1** The following are equivalent for $a, b \in X$ and an equivalence relation $R$:

(i) $a \in [b]$;

(ii) $[a] = [b]$;

(iii) $aRb$.

**Proof:** (iii) implies (i) by definition of $[b]$.

Assume (i). Then $aRb$, hence $bRa$ by symmetricity. Pick an arbitrary $x \in [a]$ so that $xRa$. Using transitivity, $xRb$, hence $x \in [b]$. We proved that $[a] \subseteq [b]$. Pick an arbitrary $x \in [b]$ so that $xRb$. Using transitivity, $xRb$, hence $x \in [a]$. We proved that $[a] = [b]$.

Finally assume (ii). Then $a \in [a] = [b]$ and $aRb$. \[\Box\]

**Corollary 1.5.2** Two equivalence classes $[a]$ and $[b]$ are either equal or disjoint. Hence, the equivalence classes form a partition of $X$.

**Proof:** If $[a]$ and $[b]$ are not disjoint, then there exists an element $c \in [a] \cap [b]$. So by Proposition 1.5.1 $[a] = [c] = [b]$. \[\Box\]
Corollary 1.5.3 The equivalence relation can be uniquely recovered from its partition into equivalence classes.

Proof: This follows immediately from Proposition 1.5.1 as \( aRb \) if and only if they belong to the same class.

Finally, we define the quotient set \( X/R \) as a collection of equivalence classes. We will see the further usefulness of this later on but here are the first three examples which you already saw in various subjects.

Examples. 1. Let \( \sim_n \) be the congruence modulo \( n \) we saw in examples today. The quotient set \( \mathbb{Z}/\sim_n \) is the ring \( \mathbb{Z}_n \) of residues modulo \( n \).

2. Let \( X \) be the set of all Cauchy sequences in \( \mathbb{Q} \). Recall that a sequence \( (a_n) \) is Cauchy if for any \( \varepsilon > 0 \) there exists \( N \) such that \( |a_m - a_n| < \varepsilon \) for all \( m, n > N \). Two Cauchy sequences \( (a_n) \) and \( (b_n) \) are equivalent if their difference \( a_n - b_n \) tends to zero. The significance of this equivalence relation is that the quotient set \( X/\sim \) is the set of real numbers.

3. Various function spaces in analysis also quotient sets where one identifies functions different by a “negligible” function. For instance, let \( X \) be the set of all function \( f : [0, 1] \to \mathbb{R} \) such that the Lebesgue integral \( \int_0^1 |f(x)|^2 \, dx \) is well-defined and finite. Two functions \( f \) and \( g \) in \( X \) are equivalent if \( \int_0^1 |f(x) - g(x)|^2 \, dx = 0 \). The quotient set \( X/\sim \) is the \( L^2 \) space \( L^2([0, 1], \mathbb{R}). \)

1.5.4 Cosets

Given a group \( G \) and a subgroup \( H \), we define a binary relation \( \sim_H \) on \( G \). We set \( x \sim_H y \) if there exists \( h \in H \) such that \( x = hy \). Notice that for \( G = \mathbb{Z} \) and \( H = n\mathbb{Z} \), this is the congruence modulo \( n \).

Proposition 1.5.4 The relation \( \sim_H \) is an equivalence relation. Moreover, \( x \sim_H y \) if and only if \( xy^{-1} \in H \).

Proof: Since \( x = 1 \cdot x \) the relation is reflexive. If \( x = hy \) then \( y = h^{-1}x \), so the relation is symmetric. If \( x = hy \) and \( y = gz \) then \( y = hgz \), so the relation is transitive.

The last statement follows from the fact that \( x = hy \) if and only if \( h = xy^{-1} \). If \( x = hy \) then \( y = h^{-1}x \), so the relation is symmetric.

We are particularly interested in equivalence classes under this equivalence relation. Clearly, \( [g] = Hg = \{hg \mid h \in H \} \).

Definition. Let \( g \in G \). Then the right coset of \( g \) is the equivalence class \( Hg \). Similarly, the left coset \( gH \) is the subset \( \{gh \mid h \in H \} \) of \( G \).
Note. The left cosets are equivalence classes of the left equivalence relation $x^{-1}y \in H$.

Note. In the case of additive groups, we denote the coset by $H + g$ rather than by $Hg$.

Example. Let $G = S_3$ be the symmetric group. Then $G$ consists of the 6 permutations $(1,2,3), (1,3,2), (1,2), (1,3), (2,3)$, where $(1)$ represents the identity permutation.

Let us first choose $H = \{(), (1,2,3), (1,3,2)\}$ to be the cyclic subgroup generated by $a = (1,2,3)$. If we put $b = (2,3)$, then we find that $Hb = \{(1,2), (1,3), (2,3)\}$. In fact any right coset of $H$ is equal to either $H$ itself or to $Hb = G \setminus H$. Furthermore, $bH = Hb$, and indeed $Hg = gH$, for all $g \in G$, so the right and left cosets are the same in this example.

Now let us choose $H = \{(), (2,3)\}$ to be the cyclic subgroup generated by $b = (2,3)$. With $a = (1,2,3)$, we have $Ha = \{(1,2,3), (1,3)\}$ and $Ha^2 = \{(1,3,2), (1,2)\}$, but $aH = \{(1,2,3), (1,2)\}$ and $a^2H = \{(1,3,2), (1,3)\}$, so the right and left cosets are not the same in this case.

The following two corollaries are immediate consequences of Corollary 1.5.2 and Proposition 1.5.4

**Corollary 1.5.5** Two right cosets $Hg_1$ and $Hg_2$ of $H$ in $G$ are either equal or disjoint.

**Corollary 1.5.6** The right cosets of $H$ in $G$ partition $G$.

### 1.5.5 Exercises

(i) Find a binary relation on the set $\mathbb{R}$ that is both reflexive and transitive but not symmetric.

(ii) Find a binary relation on the set $\mathbb{R}$ that is both symmetric and transitive but not reflexive.

(iii) Find a binary relation on the set $\mathbb{R}$ that is both reflexive and symmetric but not transitive.

(iv) Describe and draw the cosets of $\mathbb{R}$ in $\mathbb{C}$.

(v) Describe and draw the cosets of $\mathbb{R}^+$ in $\mathbb{C}^*$.

(vi) Describe and draw the cosets of $H = \{z \in \mathbb{C}||z| = 1\}$ in $\mathbb{C}^*$. 
(vii) Consider solutions of a homogeneous system of linear equations: \( H = \{ X \in \mathbb{R}^m | AX = 0 \} \). Show that \( H \) is a subgroup.

Now consider solutions of a non-homogeneous system of linear equations: \( W = \{ X \in \mathbb{R}^m | AX = B \} \). Show that \( W \) is a coset of \( H \).
1.6 Lagrange’s theorem and applications

1.6.1 Executive Summary

We prove Lagrange’s theorem. Using it, we start our journey into classification of groups.

1.6.2 Lagrange’s Theorem

We have already observed that cosets form a partition of the group $G$.

**Proposition 1.6.1** If the subgroup $H$ is finite, then all right cosets have exactly $|H|$ elements.

**Proof:** Since $h_1g = h_2g \Rightarrow h_1 = h_2$ by the cancellation law, it follows that the map $\phi : H \rightarrow Hg$ defined by $\phi(h) = hg$ is a bijection, and the result follows. \qed

Of course, all of the above results apply with appropriate minor changes to left cosets.

Corollary 1.5.6 and Proposition 1.6.1 together imply:

**Theorem 1.6.2** (Lagrange’s Theorem) Let $G$ be a finite group and $H$ a subgroup of $G$. Then the order of $H$ divides the order of $G$.

**Definition.** The number of distinct right cosets of $H$ in $G$ is called the index of $H$ in $G$ and is written as $|G : H|$.

If $G$ is finite, then we clearly have $|G : H| = |G|/|H|$.

**Proposition 1.6.3** Let $G$ be a finite group. Then for any $g \in G$, the order $|g|$ of $g$ divides the order $|G|$ of $G$.

**Proof:** Let $|g| = n$. The powers $\{g^x \mid x \in \mathbb{Z}\}$ of $g$ form a subgroup $H$ of $G$, and we saw in Subsection 1.3.4 that the distinct powers of $g$ are $\{g^x \mid 0 \leq x < n\}$. Hence $|H| = n$ and the result follows from Lagrange’s Theorem. \qed

1.6.3 Groups of Order up to 5

A large part of group theory consists of classifying groups with various properties. This means finding representatives of the isomorphism classes of groups with these properties. As an application, we can now immediately classify all finite groups whose order is prime.
Proposition 1.6.4 Let $G$ be a group having prime order $p$. Then $G$ is cyclic; that is, $G \cong C_p$.

Proof: Let $g \in G$ with $1 \neq g$. Then $|g| > 1$, but $|g|$ divides $p$ by Proposition 1.6.3, so $|g| = p$. But then $G$ must consist entirely of the powers $g^k$ $(0 \leq k < p)$ of $g$, so $G$ is cyclic. 

This result and Proposition 1.6.5 provide a classification of all groups of order less than 6. We shall deal with groups of order 6 in the near future. Recall that we already know two groups of order 4: the cyclic group $C_4$ and the Klein four group $K_4 \cong C_2 \times C_2$.

Proposition 1.6.5 There are two groups of order 4 up to an isomorphism: $C_4$ and $K_4$.

Proof: These two groups are non-isomorphic by Lemma 1.3.5: $C_4$ has an element of order 4 but $K_4$ hasn’t.

Now if $G$ is a group of order 4, then by Proposition 1.6.3 its non-identity elements have order 2 or 4. If $G$ admits an element $a$ of order 4, then elements $1, a, a^2, a^3$ are distinct and $G = \{1, a, a^2, a^3\}$ is a cyclic group.

If $G$ has no such element, all non-identity elements have order 2. As in the homework problem, $G$ is abelian in this case and admits a vector space structure over the field $\mathbb{Z}_2$. Choosing a basis, forces an isomorphism $G \cong C_2 \times C_2 \cong K_4$.

1.6.4 Euler’s theorem and Fermat’s little theorem

The following property of Euler’s function (defined in 1.4.5) is of interest.

Theorem 1.6.6 (Euler’s Theorem) Let $a$ and $n$ be coprime integers. Then $n | (a^{\varphi(n)} - 1)$.

Proof: Let $b = (a)_n$ be the residue. Since the numbers are coprime, $b \in \mathbb{Z}_n^\ast$. By Proposition 1.6.3, the $|b|$ divides $\varphi(n)$. Hence $b^{\varphi(n)} = 1$ in the group $\mathbb{Z}_n^\ast$. Consequently, $a^{\varphi(n)} - 1 = (a^{\varphi(n)} - b^{\varphi(n)}) + (b^{\varphi(n)} - 1)$ is divisible by $n$ in $\mathbb{Z}$.

The following fact follows easily.

Corollary 1.6.7 (Fermat’s little theorem) Let $p$ be a prime number, $a$ an integer. Then $p | (a^p - a)$.

Proof: Notice that $a^p - a = a(a^{p-1} - 1) = a(a^{\varphi(p)} - 1)$. If $p | a$ then the divisibility comes from the first multiplicand. If not it comes from the second one by Euler’s theorem.
1.6.5 Applications of Group Theory to Computer Security

Have you ever wondered what happens with your credit card number when you send a payment over the Internet? Why is it secure? In fact, there is not a mathematical proof that the method used is secure. Such proof would be a negative solution to the $P = NP$-problem which is one of the so called millenium problems, each worth a prize of one million dollars. It is needless that a positive solution could worsen hundreds times more, so if you have one, let us keep it a secret. As far as industry is concerned as the system has never been broken, it is good enough.

Let us suppose we have a group $G$ and a computer that can make one group multiplication every microsecond ($10^{-6}$ seconds). How long will it take to compute $g^n$? If $n = 2m$ is even, we can use $g^n = g^m \cdot g^m$. If $n = 2m + 1$ is odd, we can use $g^n = g^m \cdot g^m \cdot g$. Hence, we can compute $g^n$ using between $\log_2 n$ and $2 \log_2 n$ operations. If $n \approx 2^{1000}$, i.e. has 1000 digits in binary representation, we need at most 2000 multiplications, so we can compute the power in 2 milliseconds ($2 \cdot 10^{-3}$ seconds). On the other hand, if we need to find the order of $g$ then we need to compute all $|g|$ powers until we hit 1. If $|g| \approx 2^{1000}$, we need at most $2^{100} = (2^{10})^{100} \approx (10^3)^{100}$ multiplications, so we can compute the order in $10^{294}$ seconds, which is longer the age of the universe. Of course, if we know something about the group then it can take a bit shorter. So the group should be secure, whatever it means.

1.6.6 Diffie-Hellman Key Exchange

This is the simplest, yet the most efficient and mostly used solution. Alice and Bob exchange secret key over a public channel. After that they can encode the communications with their secret key.

Over a public channel, Alice and Bob agree on a group $G$ and an element $g \in G$ to use. Alice secretly picks a power $n$, computes $a = g^n$ and sends $a$ to Bob over the channel. Bob secretly picks a power $m$, computes $b = g^m$ and sends $b$ to Alice.

The key $K = a^m = b^n = g^{mn}$ is now available to both Bob and Alice.

Now if Eve evesdrops then she accesses $a, b, g, G$. But to compute $K$ she needs exponents $m$ or $n$ and there is no way of finding them quickly as we have observed. The group $G$ is typically $\mathbb{Z}_p^*$ where $p$ is a large prime (approximately 1000 binary bits or so).
1.6.7 RSA

This one is more fun mathematically. Suppose that you run a website so popular with customers, that every minutes thousands of customers are queueing up to pay you with their credit card. The key exchange with each of them will slow you down and you need an asymmetric keys solution instead. You need two keys: a private key used and known only to you and a public key that you would give to any customers, including hackers trying to compromise the system. Another industrial application of asymmetric keys is the PGP system but let’s get to the mathematics of it.

The source of the keys are two large (approximately 1000 bits or so) primes \( p \) and \( q \). The public key consists of the product \( n = pq \) and the exponent \( e \) such that \( \gcd(e, \varphi(n)) = 1 \). Popular choices of public exponent are \( 65537 = 2^{16} + 1 \) or \( 17 = 2^4 + 1 \). The private key consists of the private exponent \( d \) such that \((ed)\varphi(n) = 1\). This number is precomputed once and stored.

The public key is available to anybody shopping online. The credit card number is padded with bits upfront to form a message \( m \). Padding ensures the security condition \( m^e \gg n \) but making sure \( m \) is not divisible by \( p \) an \( q \), usually by \( p > m < q \). The encoded message \( x = (m^e)_n \) is send over the Internet. The choice of public exponent usually enables fast calculation. For instance, \( m^{65537} \) is computed using 17 multiplications.

The vendor receives the message and decrypts it by \( m = (m^ed)_n = (x^d)_n \) with the first equality thanks to Euler’s theorem. It is a bit more computation intensive as the number \( d \) tend to be large.

A hacker can easily collect the following ingredients: \( x, e, n \). To get to the credit card number \( m \), the hacker needs \( d \) or \( \varphi(n) \). He(she) will need either to decompose \( n \) into the product of \( p \) and \( q \) or compute \( \varphi(n) \) by any other means. The problem is that with such a large \( n \), it is going to take thousands of years!! Mathematicians know at least one way to do it faster by using quantum computers. (Un)Fortunately, nobody knows how to build quantum computers.

1.6.8 Exercises

(i) Prove that, if \( |G : H| \) is finite, then \( |G : H| \) is also equal to the number of distinct left cosets of \( H \) in \( G \). This is clear if \( G \) is finite, because both numbers are equal to \( |G|/|H| \), but it is not quite so easy if \( G \) is infinite.
(ii) Let $H$ be a subgroup of a group $G$ and let $Hg$ be a right coset of $H$ in $G$. Prove that the set $\{k^{-1} \mid k \in Hg\}$ is a left coset of $H$ in $G$, and deduce that there is a bijection between the sets of left and right cosets of $H$ in $G$.

(iii) Explain how to compute $m^{65537}$ using 17 multiplications.

(iv) Explain why the security condition $m^e \gg n$ is necessary.

1.6.9 Vista

Let us ask the inverse question to Lagrange’s theorem. Suppose $n$ divides $|G|$. Does $G$ admit a subgroup of order $n$. The answer to this naive question is no and we are going to see an example later in the course. However, there is a partial positive answer if $n$ is a prime power. It is given by a series of 4 Sylow’s theorems. Read about them in Lauritzen (section 2.10.4). Unfortunately, we don’t have enough time to cover them in this course. You can learn about them in the third year Group Theory or you can write your second year essay on this topic.

1.6.10 Vista-2

Read more about prime numbers and their factorisation in Lauritzen. There is some money to be made. The RSA challenge will pay you money for factoring one of the numbers of the form $pq$, they have set as challenges. See http://www.rsasecurity.com/rsalabs/node.asp?id=2093

Besides, it is all related to the P=NP problem, one of the millennium problems with one million dollars prize money. See http://en.wikipedia.org/wiki/Complexity_classes_P_and_NP

Finally, if you do have a way of decomposing large numbers, you have a chance of becoming the top criminal of the century by compromising all secure Internet traffic with payment information.
1.7 Generators and dihedral groups

1.7.1 Executive Summary

We introduce generators and observe them in action in a new family of groups, called dihedral groups.

1.7.2 Generators

Definition. The elements \{g_1, g_2, \ldots, g_r\} of a group G are said to generate G (or to form a set of generators for G) if every element of G can be obtained by repeated multiplication of the g_i and their inverses.

This means that every element of G can be written as an expression like \(g_2^{-1}g_1g_4g_3^{-1}g_1g_2^{-1}\) in the \(g_i\) and \(g_i^{-1}\), which is allowed to be as long as you like. Such an expression is also called a word in the generators \(g_i\).

Examples. 1. A group is cyclic if and only if it can be generated by a single element.

2. We have seen in Lemma 1.2.1 that any permutation in the symmetric groups Sym(X) can be written as a product of transpositions. So the set of all transpositions generates Sym(X). (In fact there are much smaller generating sets for Sym(X), see the exercise below.)

3. You have seen in Linear Algebra that the group \(\text{GL}_n(K)\) for a field \(K\) is generated by elementary matrices.

1.7.3 Dihedral groups

Let \(n \in \mathbb{N}\) with \(n \geq 2\) and let \(P\) be a regular \(n\)-sided polygon in the plane. The dihedral group \(D_{2n}\) is the group of the isometries of the plane preserving \(P\). Examples of such are

(i) \(n\) rotations through the angles \(2\pi k/n\) (\(0 \leq k < n\)) about the centre of \(P\); and

(ii) \(n\) reflections about lines that pass through the centre of \(P\), and either pass through a vertex of \(P\) or bisect an edge of \(P\) (or both).

Unfortunately, some books denote this group by \(D_n\) and others by \(D_{2n}\), which can be confusing! We shall use \(D_{2n}\).

To analyse these groups, it will be convenient to number the vertices in order \(1, 2, \ldots, n\), and to regard the group elements as permutations of these vertices. For instance, immediately we can observe that we have listed all the elements.
Lemma 1.7.1 The order of $D_{2n}$ is $2n$ and all its elements ($n$ rotations and $n$ reflections) are listed above.

Proof: As 1 and 2 are adjacent vertices, an isometry $\phi$ is uniquely determined by the vertices $\phi(1)$ and $\phi(2)$. The vertex $\phi(1)$ could be any of $n$ vertices and $\phi(2)$ could be any of 2 vertices adjacent to $\phi(1)$. Thus, $|D_{2n}| = 2n$ and we have listed $2n$ elements of $D_{2n}$. It is clear that they are all distinct. □

To be mathematically rigorous, we have defined $D_{2n}$ as a subgroup of the orthogonal group $O_2(\mathbb{R})$ (note that these are precisely isometries preserving the origin) but by looking at the permutations of vertices, we are switching to a subgroup of $S_n$ isomorphic to $D_{2n}$.

Let us go back to elements of $D_{2n}$. The $n$ rotations are the powers $a^k$ for $0 \leq k < n$, where $a = (1, 2, 3, \ldots, n)$ is a rotation through the angle $2\pi/n$.

Let $b$ be the reflection through the bisector of $P$ that passes through the vertex 1. Then $b$ interchanges the vertices 2 and $n$ that are adjacent to 1, and similarly it interchanges 3 and $n-1$, 4 and $n-2$, etc., so we can have $b = (2, n)(3, n-1)(4, n-2)\ldots$. For example, when $n = 5$, $b = (2, 5)(3, 4)$ and when $n = 6$, $b = (2, 6)(3, 5)$. Notice that there is a difference between the odd and even cases. When $n$ is odd, $b$ fixes no vertex other than 1, but when $n$ is even, $b$ fixes one other vertex, namely $(n+2)/2$.

Now we can see, either geometrically or by multiplying permutations, that the $n$ reflections of $P$ are the elements $a^kb$ for $0 \leq k < n$. (Remember that $ab$ means first do $b$ and then do $a$.) Thus we have

$$G = \{a^k | 0 \leq k < n\} \cup \{a^kb | 0 \leq k < n\}$$

(†).

In other words, $a$ and $b$ generated $D_{2n}$.

Again, the odd and even cases are slightly different. When $n = 5$, $b, ab, a^2b, a^3b, a^4b$ are equal to $(2, 5)(3, 4), (1, 2)(3, 5), (1, 3)(4, 5), (1, 4)(2, 3), (1, 5)(2, 4)$ respectively, which are the reflections through the bisectors of $P$ through vertices $1, 4, 2, 5, 3$. When $n = 6$, we have $b = (2, 6)(3, 5), a^2b = (1, 3)(4, 6), a^4b = (1, 5)(2, 4)$, which are reflections through bisectors of $P$ passing through two vertices, whereas $ab = (1, 2)(3, 6)(4, 5), a^3b = (1, 4)(2, 3)(5, 6), a^5b = (1, 6)(2, 5)(3, 4)$, which are reflections through lines that bisect two edges of $P$.

In all cases, we have $ba = a^{n-1}b$ (= $a^{-1}b$); this is the reflection that interchanges vertices $i$ and $n+1-i$ for $1 \leq i \leq n$. This equation, together with $a^n = 1$ and $b^2 = 1$ enable us to calculate the full multiplication table of
G with the elements written as they are in the expression (†) above, because they enable us to perform any of the four basic types of products. In a certain sense, these relations are defining relations for the group $D_{2n}$.

Let us work out $ba^k = a^{n-1}b a^{k-1} = a^{n-1}b a^{k-1}b = a^{n-k}b (= a^{-k}b)$ for $0 \leq k < n$.

(i) $(a^k)(a^l) = a^{k+l}$ $(k + l < n)$ or $a^{k+l-n}$ $(k + l \geq n)$;

(ii) $(a^k)(a'b) = a^{k+l}b$ $(k + l < n)$ or $a^{k+l-n}b$ $(k + l \geq n)$;

(iii) $(a^kb)(a') = a^k a^{n-l}b = a^{k+n-l}b$ $(k \leq l)$ or $a^{k-l}b$ $(k \geq l)$;

(iv) $(a^kb)(a'b) = a^k a^{n-l}bb = a^{k+n-l}b$ $(k \leq l)$ or $a^{k-l}b$ $(k \geq l)$.

Let us write out the full multiplication table in the case $n = 6$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>a</th>
<th>a^2</th>
<th>a^3</th>
<th>a^4</th>
<th>a^5</th>
<th>b</th>
<th>ab</th>
<th>a^2b</th>
<th>a^3b</th>
<th>a^4b</th>
<th>a^5b</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>a</td>
<td>a^2</td>
<td>a^3</td>
<td>a^4</td>
<td>a^5</td>
<td>b</td>
<td>ab</td>
<td>a^2b</td>
<td>a^3b</td>
<td>a^4b</td>
<td>a^5b</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a^2</td>
<td>a^3</td>
<td>a^4</td>
<td>a^5</td>
<td>1</td>
<td>ab</td>
<td>a</td>
<td>a^2b</td>
<td>a^3b</td>
<td>a^4b</td>
</tr>
<tr>
<td>a^2</td>
<td>a^2</td>
<td>a</td>
<td>a^2</td>
<td>a^3</td>
<td>a^4</td>
<td>a^5</td>
<td>1</td>
<td>a</td>
<td>a^2b</td>
<td>a^3b</td>
<td>a^4b</td>
<td>a^5b</td>
</tr>
<tr>
<td>a^3</td>
<td>a^3</td>
<td>a</td>
<td>a^2</td>
<td>a^3</td>
<td>a^4</td>
<td>a^5</td>
<td>1</td>
<td>a</td>
<td>a^3b</td>
<td>a^4b</td>
<td>a^5b</td>
<td>b</td>
</tr>
<tr>
<td>a^4</td>
<td>a^4</td>
<td>a^5</td>
<td>1</td>
<td>a</td>
<td>a^2</td>
<td>a^3</td>
<td>a^4</td>
<td>a^5b</td>
<td>b</td>
<td>ab</td>
<td>a^2b</td>
<td>a^3b</td>
</tr>
<tr>
<td>a^5</td>
<td>a^5</td>
<td>1</td>
<td>a</td>
<td>a^2</td>
<td>a^3</td>
<td>a^4</td>
<td>1</td>
<td>a^5b</td>
<td>b</td>
<td>ab</td>
<td>a^2b</td>
<td>a^3b</td>
</tr>
<tr>
<td>b</td>
<td>ab</td>
<td>ab</td>
<td>a</td>
<td>a</td>
<td>a^2</td>
<td>a^3</td>
<td>1</td>
<td>a</td>
<td>a^5</td>
<td>a^4</td>
<td>a^3</td>
<td>a</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a^2</td>
<td>a^3</td>
<td>1</td>
<td>a</td>
<td>a^5</td>
<td>a^4</td>
<td>a^3</td>
<td>a</td>
</tr>
<tr>
<td>a^2</td>
<td>a^2</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a^2</td>
<td>1</td>
<td>a</td>
<td>a^5</td>
<td>a^4</td>
<td>a^3</td>
<td>a</td>
</tr>
<tr>
<td>a</td>
<td>a^2b</td>
<td>a^2b</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>1</td>
<td>a</td>
<td>a^5</td>
<td>a^4</td>
<td>a^3</td>
<td>a</td>
</tr>
<tr>
<td>b</td>
<td>a^2b</td>
<td>a^2b</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>1</td>
<td>a</td>
<td>a^5</td>
<td>a^4</td>
<td>a^3</td>
<td>a</td>
</tr>
<tr>
<td>a</td>
<td>a^3b</td>
<td>a^3b</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>1</td>
<td>a</td>
<td>a^5</td>
<td>a^4</td>
<td>a^3</td>
<td>a</td>
</tr>
<tr>
<td>a^2</td>
<td>a^3b</td>
<td>a^3b</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>1</td>
<td>a</td>
<td>a^5</td>
<td>a^4</td>
<td>a^3</td>
<td>a</td>
</tr>
<tr>
<td>a</td>
<td>a^4b</td>
<td>a^4b</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>1</td>
<td>a</td>
<td>a^5</td>
<td>a^4</td>
<td>a^3</td>
<td>a</td>
</tr>
<tr>
<td>a^2</td>
<td>a^4b</td>
<td>a^4b</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>1</td>
<td>a</td>
<td>a^5</td>
<td>a^4</td>
<td>a^3</td>
<td>a</td>
</tr>
<tr>
<td>a</td>
<td>a^5b</td>
<td>a^5b</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>a</td>
<td>1</td>
<td>a</td>
<td>a^5</td>
<td>a^4</td>
<td>a^3</td>
<td>a</td>
</tr>
</tbody>
</table>

and in general, using residues

<table>
<thead>
<tr>
<th>$a^l$</th>
<th>$a^l b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a^k$</td>
<td>$a^{(k+l)n}$</td>
</tr>
<tr>
<td>$a^k b$</td>
<td>$a^{(k+n-1)n}$</td>
</tr>
<tr>
<td>$a^{(k-1)n} b$</td>
<td>$a^{(k-1)n}$</td>
</tr>
</tbody>
</table>

### 1.7.4 Exercises

(i) Show that $S_n$ is generated by $n-1$ transpositions $(1, 2), (2, 3), \ldots, (n-2, n-1), (n-1, n)$.

(ii) Prove that $D_4$ is isomorphic to $K_4$.

(iii) Prove that $D_6$ is isomorphic to $S_3$. 

(iv) The centre of a group $G$ is defined by $Z(G) = \{ x \in G | \forall y \in G \ xy = yx \}$. Show that the centre is an abelian subgroup.

Compute the centre of $D_{2n}$, $n \geq 1$.

(v) Go to the online Magma calculator http://magma.maths.usyd.edu.au/calc/ and play around with groups. For instance, try the code

\[ G<a,b> := \text{Group} < a, b | a^{30}, b^2, a*b = b*a^{-1} >; G; \text{Order}(G); \]
1.8 Relations and groups of order up to 7

1.8.1 Executive Summary

We discuss relations. These become a crucial tool when we extend the classification of groups up to order 7.

1.8.2 Relations

We shall be needing some techniques to prove isomorphisms between groups satisfying various properties. The following results provide methods of doing this for certain families of groups.

Proposition 1.8.1 Let $G$ be a group of order $2n$ generated by two elements $a$ and $b$ that satisfy the equations $a^n = 1$, $b^2 = 1$ and $ba = a^{-1}b$. Then $G \cong D_{2n}$.

Proof: Since $G$ is generated by $a$ and $b$, any element of $G$ can be written as a product of the generators $a$, $b$, $a^{-1}$, $b^{-1}$. Since $a^n = 1$ and $b^2 = 1$, we can always replace $a^{-1}$ by $a^{n-1}$ and $b^{-1}$ by $b$, so we can assume that only $a$ and $b$ appear in this product. Furthermore, we can use the equation $ba = a^{-1}b = a^{n-1}b$ to move all occurrences of $a$ in the product to the left of the expression, and we end up with a word in the form $a^k b^l$. Using $a^n = b^2 = 1$ again, we can assume that $0 \leq k < n$ and $0 \leq b < 2$. This leaves us with precisely $2n$ different words $a^k b^l$, and since we are told that $|G| = 2n$, these words must all represent distinct elements of $G$. We have now shown that $G = \{a^k \mid 0 \leq k < n\} \cup \{a^k b \mid 0 \leq k < n\}$, exactly as in $D_{2n}$.

Using $ba = a^{-1}b$ twice, we get $ba^2 = (ba)a = a^{-1}ba = a^{-1}a^{-1}b = a^{-2}b$, and similarly $ba^k = a^{-k}b$ for all $k \geq 0$, and since $a^{-k} = a^{n-k}$, we have $ba^k = a^{n-k}b$ for $0 \leq k < n$. We saw in Subsection 1.7.3, that these equations, together with $a^n = 1$ and $b^2 = 1$ allow us to deduce the whole of the multiplication table of $D_{2n}$. Hence any group satisfying the hypotheses of this proposition has corresponding elements and the same multiplication as $D_{2n}$, and so it is isomorphic to $D_{2n}$.

The equations $\{a^n = 1, b^2 = 1, ba = a^{-1}b\}$ are called defining relations for $D_{2n}$, which means roughly that $D_{2n}$ is the largest group generated by two elements $a$ and $b$ that satisfy these equations. We shall not go into the general theory of defining relations in this course, but we shall give two more examples.
Consider the direct product $C_m \times C_n$ of cyclic groups of orders $m$ and $n$, which has order $mn$. Let $c$ and $d$ be generators of $C_m$ and $C_n$, and let $a = (c, 1)$ and $b = (1, d)$. Then we can easily check that $a^m = 1$, $b^n = 1$ and $ab = ba$.

**Proposition 1.8.2** Let $G$ be a group of order $mn$ generated by two elements $a$ and $b$ that satisfy the equations $a^m = 1$, $b^n = 1$ and $ba = ab$. Then $G \cong C_m \times C_n$.

**Proof**: By a similar argument to that used in the proof of Proposition 1.8.1, we can show that any element of $G$ can be written as $a^k b^l$ with $0 \leq k < m$, $0 \leq l < n$, and hence deduce that $G = \{a^k b^l \mid 0 \leq k < m, 0 \leq l < n\}$.

From $ba = ab$, we deduce $b^l a^k = a^k b^l$ for $k, l \geq 0$, and the defining relations now enable us easily to deduce the complete multiplication table of $G$. The result follows.

Later on we will use the following proposition to identify the quaternion group. Recall that $Q_8$ consists of 6 imaginary quaternionic units $\pm I, \pm J, \pm K$ as well as two extra elements $\pm 1$.

**Proposition 1.8.3** Let $G$ be a group of order 8 generated by two elements $a$ and $b$ that satisfy the equations $a^4 = 1$, $b^2 = a^2$ and $ba = a^{-1} b$. Then $G \cong Q_8$.

**Proof**: Notice that $b^4 = (b^2)^2 = (a^2)^2 = 1$. By pushing $b$ to the right, $G = \{a^k b^l \mid 0 \leq k < 3, 0 \leq l < 1\}$. An isomorphism $\phi : G \rightarrow Q_8$ is uniquely determined by $\phi(a) = I$ and $\phi(b) = J$. Details of checking that this is an isomorphism, which can be done by working out multiplication table of $G$, are left to the reader.

**1.8.3 Groups of Order up to 7**

We already know that there is a single group of order 7: $C_7$. Hence we concentrate on classification of groups of order 6. We have seen two examples so far, the cyclic group $C_6$ and the dihedral group $D_6$. Note that the symmetric group $S_3$ is isomorphic to $D_6$. Since $D_6$ is nonabelian (or, alternatively, since it has no element of order 6), these two groups cannot be isomorphic to each other. We shall now prove that they are the only examples.

**Proposition 1.8.4** Let $G$ be group of order 6. Then $G \cong C_6$ or $G \cong D_6$. 
Proof: By Proposition 1.6.3 the orders of elements \( g \in G \) can be 1, 2, 3 or 6. If there is a \( g \) with \( |g| = 6 \), then \( G \cong C_6 \), so assume not. If all elements had order 1 or 2, then (as in the homework 1) \( |G| = 2^n \), which is impossible. Hence there is an element \( a \) of order 3. Then the subgroup \( H = \{ 1, a, a^2 \} \) has index 2 in \( G \). Choose \( b \in G \setminus H \). Then \( G = H \cup Hb = H \cup bH \) are both disjoint unions. Hence \( bH = \{ b, ba, ba^2 \} = Hb = \{ b, ab, a^2b \} \).

Let us assume that \( G \) has no element of order 6. What can \( b^2 \) be? \( b^2 = b, ab \) or \( a^2b \) all lead to contradictions by the cancellation law (Proposition 1.1.8). If \( b^2 = a \) or \( a^2 \) on the other hand, then \( b \) has order 6, and \( G \cong C_6 \). Let us assume that \( b^2 = 1 \).

Now \( a \) and \( b \) generate \( G \). Which element of \( Hb \) is \( ba \)? Clearly, \( ba \neq b \) by the cancellation laws (Proposition 1.1.8).

If \( ba = ab \) then by Propositions 1.8.2 and 1.3.6, \( G \cong C_3 \times C_2 \cong C_6 \).

If \( ba = a^2b = a^{-1}b \) then by Proposition 1.8.1, \( G \cong D_6 \). \( \square \)

1.8.4 Exercises

(i) Let \( X \) be a subset of a group \( G \). Let \( < X > \cap_{X \subseteq H < G} H \). Show that \( H \) is the smallest subgroup of \( G \) containing \( X \). This subgroup \( < X > \) is called the subgroup generated by \( X \).

Show that \( < X > \) consists of words in elements of \( X \).

(ii) Prove Proposition 1.8.3

1.8.5 Vista: Burnside’s problem

Here is your another chance to get immediate recognition as a mathematical genius on par Galois, Gauss and Perelman. Is the group \( B(2, 5) \) generated by \( a \) and \( b \) with defining relations \( w^5 = 1 \) finite or infinite? By \( w \) I mean all possible words in \( a \) and \( b \). So the group \( G \) is largest possible group generated by \( 2 \) elements with all nontrivial elements of order 5.

Beware that your laptop is not of big help here. If this group is finite, it has exactly \( 5^{34} \) (approximately \( 6 \times 10^{23} \)) elements. But I would bet that it is infinite. If any betting agency accepts (they do accept similar bets, for instance, on discovering Higgs particles before 2010), please, let me know.

In 1984, E. Zelmanov received Fields Medal for proving that for \( k \) and \( n \), there exists the largest finite group generated by \( k \) elements such that each element in degree \( n \) is 1. This is known as restricted Burnside’s problem.
Chapter 2
Homomorphisms

2.1 Homs, Images and Kernels

2.1.1 Executive Summary
We introduce the notion of a homomorphism, its image and its kernel.

2.1.2 Definition and examples of homomorphisms

Definition. Let $G, H$ be groups, $R, S$ rings. A group homomorphism $\phi$ from $G$ to $H$ is a function $\phi : G \rightarrow H$ such that $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. A ring homomorphism $\phi$ from $R$ to $S$ is a function $\phi : R \rightarrow S$ such that $\phi(1_R) = 1_S$, $\phi(r_1r_2) = \phi(r_1)\phi(r_2)$, and $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ for all $r_1, r_2 \in R$.

Notice that the ring homomorphism requires an extra condition concerning the identity. For instance, the natural map $R \rightarrow R \times S, r \mapsto (r, 0_S)$ is not a ring homomorphism. Such surprises don’t happen with groups.

Lemma 2.1.1 Let $\phi : G \rightarrow H$ be a homomorphism. Then $\phi(1_G) = 1_H$ and $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.

Proof: (Recall that $1_G$ and $1_H$ are the identity elements of $G$ and $H$.) Let $\phi(1_G) = h$. Then

$$1_H h = h = \phi(1_G) = \phi(1_G 1_G) = \phi(1_G) \phi(1_G) = hh,$$

so $h = 1_H$ by the cancellation law. Similarly, if $g \in G$ and $\phi(g) = h$, then

$$\phi(g^{-1}) \phi(g) = \phi(g^{-1}g) = \phi(1_G) = 1_H = h^{-1}h = \phi(g)^{-1} \phi(g).$$
so \( \phi(g^{-1}) = \phi(g)^{-1} \) by the cancellation law.

In some sources the words *monomorphism* and *epimorphism* are used to describe injective and surjective homomorphisms.

We have already discussed isomorphisms that are just bijective homomorphisms.

**Examples.** 1. If \( H \) is a subgroup of \( G \), then the map \( \phi : H \to G \) defined by \( \phi(h) = h \) for all \( h \in H \) is an injective homomorphism. It is an isomorphism if \( H = G \).

2. Similarly, if \( R \) is a subring of \( S \), then the map \( \phi : R \to S \) defined by \( \phi(h) = h \) for all \( h \in R \) is an injective homomorphism. It is an isomorphism if \( R = S \).

3. If \( G \) is an abelian group and \( r \in \mathbb{Z} \), then \((gh)^r = g^r h^r\) for all \( g, h \in G \), so the map \( \phi : G \to G \) defined by \( \phi(g) = g^r \) is a homomorphism.

**Warning.** This only works when \( G \) is abelian.

4. If \( V \) and \( W \) are vector spaces over the same field \( F \) then they are abelian groups as well. Any linear map \( \psi : V \to W \) is a group homomorphism.

**Warning.** The opposite is true only for very special fields (for instance, \( \mathbb{Q} \)). Otherwise, consider the complex conjugation \( x \mapsto x^* \), \( \mathbb{C} \to \mathbb{C} \). It is a group homomorphism but not a linear map of vector spaces over \( \mathbb{C} \), although it is a linear map of vector spaces over \( \mathbb{R} \).

5. Let \( R \) be a commutative ring of characteristic \( p \), that is, \( px = 0 \) for any \( x \in R \) where \( p \) is a prime number. The ring \( R \) admits a Frobenius homomorphism, \( F : R \to R \) defined by \( F(x) = x^p \). The tricky part of being a homomorphism is the preservation of addition. The identity \((x+y)^p = x^p + y^p \) is sometimes called *freshman’s dream binomial formula*. It holds because the commutativity of \( x \) and \( y \) implies that

\[
(x + y)^p = x^p + y^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} x^k y^{p-k}
\]

and all binomial coefficients in the sum are divisible by \( p \).

6. Let \( k \) be a fixed element of a group \( G \). Then, for \( g, h \in G \), we have \( kghk^{-1} = kgk^{-1}khk^{-1} \), so the map \( \phi : G \to G \) defined by \( \phi(g) = kgk^{-1} \) is a homomorphism. In fact it is an isomorphism, because \( kgk^{-1} = khk^{-1} \Rightarrow g = h \) by the cancellation laws, and each \( h \in G \) is equal to \( \phi(k^{-1}hk) \). Notice that if \( G \) is abelian, then whatever \( k \) we choose, we always get \( \phi(g) = g \) for all \( g \) so, these examples are only interesting for nonabelian groups.
We can deduce the following result from Proposition 1.3.5.

**Proposition 2.1.2** If $g, k$ are elements of a group $G$, then $g$ and $kgk^{-1}$ have the same order.

The elements $g$ and $kgk^{-1}$ are called *conjugate* elements. We shall be come back to study this relationship later on.

7. Similarly for a ring $R$, pick $k \in R^*$. The map $\phi : R \to R$ defined by $\phi(r) = krk^{-1}$ is a homomorphism. It is an isomorphism for the same reason as in groups.

8. Let $G = \{1, a, b, c\}$ be a Klein Four Group. Define $\phi : G \to G$ by $\phi(1) = 1, \phi(a) = b, \phi(b) = c, \phi(c) = a$. Then it is straightforward to check that $\phi$ is an isomorphism.

9. Recall that $\text{GL}(n, K)$ is the group of invertible $n \times n$ matrices over a commutative ring $K$. By the product of determinants rule, $\det(AB) = \det(A) \det(B)$, it follows that the map $\phi : \text{GL}(n, K) \to K^*$ defined by $\phi(g) = \det(g)$ is a homomorphism.

10. There is an injective group homomorphism $\Omega : S_n \to \text{GL}(n, \mathbb{R})$. In words, $\Omega(\sigma)$ is a linear transformation of $\mathbb{R}^n$ permuting elements of the standard basis $e_i$. In formulas, $\Omega(\sigma)_{i,j} = 1$ whenever $i = \sigma(j)$ and zero otherwise.

    The composition $\det \circ \Omega$ is particularly interesting homomorphism, called sign homomorphism, that allows us to prove Proposition 1.2.2. Since $\sigma^n = 1$ for some $m > 1$, $\det \circ \Omega(\sigma)^m = \det \circ \Omega(\sigma^m) = 1$. There are only two real numbers 1 and $-1$ that have finite order, hence we ha have a homomorphism $\text{sign} : S_n \to \mathbb{C}_2$ which distinguishes odd and even permutations. The former have $\text{sign}(\sigma) = -1$ and the latter satisfy $\text{sign}(\sigma) = 1$.

   Please, note that there is a risk of circular argument here. It all de- pends on how you define determinant!! If you define it algebrai cally by $\det(a_{i,j}) = \sum_{\sigma \in S_n} \text{sign}(\sigma)a_{\sigma(1),1}a_{\sigma(2),2}\ldots a_{\sigma(n),n}$ then you are in real trouble for used determinant to define sign of a permutation and vise versa.

2.1.3 Image

The image $\text{im}(\phi)$ of a homomorphism is just its image as a function, and the following propositions are straightforward to prove.

**Proposition 2.1.3** Let $\phi : G \to H$ be a group homomorphism. Then $\text{im}(\phi)$ is a subgroup of $H$. 
Proposition 2.1.4 Let $\phi : R \to S$ be a ring homomorphism. Then $\text{im}(\phi)$ is a subring of $S$.

2.1.4 Kernels

Definition. Let $\phi : G \to H$ be a homomorphism. Then the kernel $\text{ker}(\phi)$ of $\phi$ is defined to be the set of elements of $G$ that map onto $1_H$; that is,

$$\text{ker}(\phi) = \{ g \mid g \in G, \phi(g) = 1_H \}.$$

In the case of additive group or rings this becomes

$$\text{ker}(\phi) = \{ g \mid g \in G, \phi(g) = 0_H \}.$$

Note that by Lemma 2.1.1 above, $\text{ker}(\phi)$ always contains $1_G$.

Definition. A subgroup $H$ of a group $G$ is called normal in $G$ if the left and right cosets $gH$ and $Hg$ are equal for all $g \in G$.

The following proposition explains the connection between normal subgroups and homomorphisms. Together with Proposition 2.2.6, it says that the set of normal subgroups of $G$ is equal to the set of kernels of group homomorphisms with domain $G$.

Proposition 2.1.5 Let $\phi : G \to H$ be a group homomorphism. Then $\text{ker}(\phi)$ is a normal subgroup of $G$.

Proof: Checking that $K = \text{ker}(\phi)$ is a subgroup of $G$ is straightforward, using Proposition 1.1.5. If $g \in G$ then

$$gK = \phi^{-1}(\phi(g)) = Kg,$$

so $K$ is normal.

Definition. An additive subgroup $I$ of a ring $R$ is called ideal in $R$ if $xI \subseteq I \subseteq Ix$ for any $x \in R$.

Proposition 2.1.6 Let $\phi : R \to S$ be a ring homomorphism. Then $\text{ker}(\phi)$ is an ideal in $R$.

Proof: By Proposition 2.1.5, $K = \text{ker}(\phi)$ is an additive subgroup of $R$. If $r \in K$, $x \in R$ then $\phi(xr) = \phi(x)\phi(r) = O_S \phi(r) = 0_S$. Hence $xr \in K$. Similarly, $rx \in K$ and $K$ is an ideal.
2.1. HOMS, IMAGES AND KERNELS

Examples. 10. For rings $R$, $S$ let us onsider the projection $R \times S \rightarrow S$ given by $(r, s) \mapsto s$. It is a ring homomorphism whose kernel is $R$. Thus, $R$ sitting inside $R \times S$ is an ideal (but not a subring as we saw earlier).

11. Here is an example of a homomorphism from an additive group to a multiplicative group. Let $G = (\mathbb{C}, +)$ and $H = \mathbb{C}^*$, and define $\phi: G \rightarrow H$ by $\phi(g) = \exp(g)$. Then $\phi(g_1 + g_2) = \phi(g_1)\phi(g_2)$, which says that $\phi$ is a homomorphism. In fact $\phi$ is a surjective but not injective. The kernel of $\phi$ is $2\pi i \mathbb{Z}$ since $\exp(x + iy) = \exp(x)(\cos(y) + i \sin(y))$ for $x, y \in \mathbb{R}$.

12. Let $G = H = D_{12}$, the dihedral group of order 12. We saw in Subsection 1.7.3 that $G = \{a^k \mid 0 \leq k < 6\} \cup \{a^kb \mid 0 \leq k < 6\}$. We define $\phi: G \rightarrow H$ by $\phi(a^k) = a^{2k}$ and $\phi(a^kb) = a^{2k}b$ for $0 \leq k < 6$. We claim that $\phi$ is a homomorphism. It seems at first sight as though we need to check that $\phi(gh) = \phi(g)\phi(h)$ for all 144 ordered pairs $g, h \in G$, but we can group these tests into the four distinct types listed in Subsection 1.7.3. We will make free use of the fact that $a^m = 1$ when $6| m$.

(i) $\phi(a^ka') = \phi(a^{k+l})$ or $\phi(a^{k+i-6}) = a^{2(k+l)} = a^{2k}a^{2l} = \phi(a^k)\phi(a')$;

(ii) $\phi(a^k(a'b)) = \phi(a^k)\phi(a'b)$ – this is similar to (i);

(iii) $\phi((a^k)ba') = \phi(a^{k-l}b)$ or $\phi(a^{k-l+6}b) = a^{2(k-l)}b$ or $a^{2(k-l+6)}b = a^{2k}a^{-2l}b = a^{2k}ba^{-2l} = \phi(a^k)\phi(a')$;

(iv) $\phi((a^k)(a'b)) = \phi(a^k)\phi(a'b)$ – this is similar to (iii).

So $\phi$ really is a homomorphism. We can check that the only elements of $G$ with $\phi(g) = 1$ are $g = 1$ and $g = a^3$, so $\ker(\phi) = \{1, a^3\}$, which is the normal subgroup that we considered in Example 3 of Subsection 2.2.5. $\im(\phi)$ consists of the 6 elements $1, a^2, a^4, b, a^2b, a^4b$ of $G$.

In general, if $\phi: G \rightarrow H$ is a homomorphism and $J$ is a subset of $H$, then we define the complete inverse image of $J$ under $\phi$ to be the set $\phi^{-1}(J) = \{g \in G \mid \phi(g) \in J\}$. It is easy to check, using Proposition 1.1.5, that if $J$ is a subgroup of $H$, then $\phi^{-1}(J)$ is a subgroup of $G$.

Here is a final statement, which will be useful later.

Proposition 2.1.7 Let $\phi: G \rightarrow H$ be a homomorphism. Then $\phi$ is injective if and only if $\ker(\phi) = \{1_G\}$ (or $\{0\}$ in the case of rings or additive groups).

Proof: Since $1_G \in \ker(\phi)$, if $\phi$ is injective, then we must have $\ker(\phi) = \{1_G\}$. Conversely, suppose that $\ker(\phi) = \{1_G\}$, and let $g_1, g_2 \in G$ with $\phi(g_1) = \phi(g_2)$. Then $1_H = \phi(g_1)^{-1}\phi(g_2) = \phi(g_1^{-1}g_2)$ (by Lemma 2.1.1), so $g_1^{-1}g_2 \in \ker(\phi)$ and hence $g_1^{-1}g_2 = 1_G$ and $g_1 = g_2$. So $\phi$ is injective. \qed
2.1.5 Exercises

(i) Let $V$ and $W$ be vector spaces over the field $\mathbb{Q}$ of rational numbers. Show that any group homomorphism $\psi : V \rightarrow W$ is a linear map.

(ii) A homomorphism $\phi : A \rightarrow B$ is called an epimorphism if for any pair of homomorphisms $\alpha, \beta : B \rightarrow C$ the equality $\alpha \phi = \beta \phi$ implies that $\alpha = \beta$. Prove that any surjective homomorphism is an epimorphism. Prove that the natural embedding $\mathbb{Z} \rightarrow \mathbb{Q}$ is an epimorphism of rings but not surjective.

(iii) Let $G$ be a Klein Four Group. How many distinct homomorphisms $\phi : G \rightarrow G$ are there? How many of these are isomorphisms?

(iv) Let $\phi : R \rightarrow S$ be a ring homomorphism. Prove that if $K$ is a subring of $S$, then $\phi^{-1}(K)$ is a subring of $R$.

Prove that if $A$ is a subring of $R$, then $\phi(A)$ is a subring of $S$.

Prove that if $I$ is an ideal of $S$, then $\phi^{-1}(I)$ is an ideal of $R$.

Give an example where $J$ is an ideal of $R$ but $\phi(J)$ is not an ideal of $S$.

(v) Describe all distinct group homomorphisms from $C_n$ to $C_m$ and compute their number. Which of them are ring homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$.

2.1.6 Vista

Let $R = \mathbb{C}[x_1, \ldots, x_n]$ be the ring of complex polynomials. All $\mathbb{C}$-linear ring homomorphisms $\phi : \rightarrow R$ are easy to describe. Such a homomorphism gives $n$ polynomials $f_i = \phi(x_i)$. In the other direct, any $n$-tuple of polynomials $f_i$ define a linear ring homomorphism $\phi(F(x_1, \ldots, x_n)) = F(f_1, \ldots, f_n)$.

The fun starts when if we want to decide which of them are isomorphisms and $n \geq 2$. Let us consider the Jacobian of $\phi$:

$$J\phi = (\partial f_i / \partial x_j) \in M_n(R).$$

If $\phi$ is an isomorphism then $\phi \phi^{-1} = I$ where $\phi^{-1}$ is the inverse homomorphism and $I$ is the identity homomorphism given by $f_i = x_i$. By the product rule in Analysis $J\phi J\phi^{-1} = JJ$ but the latter is identity matrix. Hence, $J\phi \in \text{GL}_n(R)$.
and consequently \( \det(J_\phi) \in R^* = \mathbb{C}^* \). Indeed, the units of \( R \) are non-zero polynomials of degree zero (prove it).

It is natural to suggest that the opposite is also true: \( \det(J_\phi) \in R^* \) should imply \( \phi \) being an isomorphism. It should, indeed, but nobody knows how to prove it!! It is one of the famous problems in Algebraic Geometry call Jacobian Conjecture. In my opinion, it narrowly missed the millennium problems list by coming just behind another algebraic geometry problem called Hodge’s Conjecture. Try to think of it and see where the difficulty is.
2.2 Normal Subgroups

2.2.1 Executive Summary

We discuss normal subgroups. We use them to classify groups of order 8. The we define quotient groups.

2.2.2 Normal Subgroups

We recall that a subgroup $H$ of a group $G$ is normal if the left and right cosets $gH$ and $Hg$ are equal for all $g \in G$.

The standard notation for “$H$ is a normal subgroup of $G$” is $H \triangleleft G$ or $H \unlhd G$. ($H \triangleleft G$ is sometimes but not always used to mean that $H$ is a proper normal subgroup of $G$ – i.e. $H \neq G$.)

Examples. 1. The two standard subgroups $G$ and $\{1\}$ of any group $G$ are both normal.

2. Any subgroup of an abelian group is normal.

3. In the example $G = D_6$ in Subsection 1.6.2, we saw that the subgroup $\{((),(1,2,3),(1,3,2)) = \{1, a, a^2\}$ is normal in $G$, but the subgroup $\{((),(2,3)) = \{1, b\}$ is not normal in $G$.

In Example 3, the normal subgroup $H = \{1, a, a^2\}$ has index $|G|/|H| = 6/3 = 2$ in $G$. In fact we have the general result:

**Proposition 2.2.1** If $G$ is any group and $H$ is a subgroup with $|G : H| = 2$, then $H$ is a normal subgroup of $G$.

**Proof:** Assume that $|G : H| = 2$. Then there are only two distinct right cosets of $G$, one of which is $H$, and so by Corollary 1.5.6, the other one must be $G \setminus H$. The same applies to left cosets. Hence, for $g \in G$, if $g \in H$ then $gH = Hg = H$ and if $g \notin H$ then $gH = Hg = G \setminus H$. In either case $gH = Hg$, so $H \triangleleft G$.

So, in Example 6 of Subsection 1.1.5, $\text{Alt}(X)$ is a normal subgroup of $\text{Sym}(X)$.

The following result often provides a useful method of testing a subgroup for normality.

**Proposition 2.2.2** Let $H$ be a subgroup of the group $G$. Then $H$ is normal in $G$ if and only if $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

**Proof:** Suppose that $H \triangleleft G$, and let $g \in G$, $h \in H$. Then $Hg = gH$, and $gh \in gH$, so $gh \in Hg$, which means that there exists $h' \in H$ with $gh = h'g$. Hence $ghg^{-1} = h' \in H$. 
Conversely, assume that $ghg^{-1} \in H$ for all $g \in G$, $h \in H$. Then for $gh \in gH$, we have $ghg^{-1} \in H$, so $gh = h'g$ for some $h' \in H$; i.e. $gh \in Hg$, and we have shown that $gH \subseteq Hg$. For $hg \in Hg$, we have $g^{-1}hg \in H$ (because $g^{-1}hg = g^{-1}gHg^{-1} = g^{-1}$), so, putting $h' = g^{-1}hg$, we have $hg = gh' \in gH$, and so $Hg \subseteq gH$. Thus $gH = Hg$, and $H \leq G$. □

**Example. 4.** Let $G$ be the dihedral group $D_{12}$. Recall from Subsection 1.7.3 that $G = \{1, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\}$ where $a$ and $b$ are the permutations $(1, 2, 3, 4, 5, 6)$ and $(2, 6)(3, 5)$; the full multiplication table of this group is written out in Subsection 1.7.3.

Let $H$ be the cyclic subgroup $\{1, a^3\}$ of order 2 of $G$. We claim that $H$ is normal in $G$. To prove this, we have to show that $ghg^{-1} \in H$ for all $g \in G$, $h \in H$. If $h = 1$, then $ghg^{-1} = gg^{-1} = 1 \in H$, so we only need consider $h = a^3$. Then if $g = a^k$ for $0 \leq k < 5$, we have $ghg^{-1} = a^k a^3 a^{-k} = a^3 \in H$. The remaining case is $g = a^4b$ for $0 \leq k < 5$. From Subsection 1.7.3, we have $ba^3 = a^6 = 3b$ and so $ba^3b^{-1} = a^3$, and then, for any $k$, $(a^k b)a^3(a^k b)^{-1} = a^k ba^3b^{-1}a^{-k} = a^k a^3 a^{-k} = a^3 \in H$, and we have proved that $H \lhd G$.

### 2.2.3 Classification of Groups of Order up to 8

The classification of groups of order 8 takes a little more effort, because there are five isomorphism classes, but it can be done using only the results proved so far.

**Proposition 2.2.3** 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 $Q_8$.

**Proof:** If $G$ has an element of order 8, then it is cyclic ($C_8$), so assume not. If all non-identity elements have order 2, then $G$ is a vector space over $\mathbb{Z}_2$. The dimension must be 3 because $2^3 = 8$. Hence $G \cong C_2 \times C_2 \times C_2$.

Otherwise, there is an element $a \in G$ of order 4, and a normal subgroup $N = \{1, a, a^2, a^3\}$. Let $b \in G \setminus N$, so $G = N \cup Nb$. As in Proposition 1.8.4, we cannot have $b^2 \in Nb$, so $b^2 \in N$. If $b^2 = a$ or $a^3$, then $|b| = 8$, contrary to assumption. Hence $b^2 = 1$ or $a^2$. Since $N$ is normal, $bab^{-1} \in N$. As in Proposition 1.8.4, we cannot have $bab^{-1} = 1$. If $bab^{-1} = a^2$, then $ba^2b^{-1} = bab^{-1}bab^{-1} = a^2 a^2 = 1$, and then $a^2 = b^{-1}b = 1$, contradiction, so $bab^{-1} \not= a^2$, and hence $bab^{-1} = a$ or $a^3$; that is, $ba = ab$ or $ba = a^3b = a^{-1}b$. We now have four possibilities to analyse:

(i) $b^2 = 1$, $ba = ab$. Then $G \cong C_4 \times C_2$ by Proposition 1.8.2.
(ii) $b^2 = a^2$, $ba = ab$. In this case, we have $(ab)^2 = a^2b^2 = a^4 = 1$, so if we replace $b$ by $ab$, then we are back in Case (i), and $G \cong C_4 \times C_2$ again.

(iii) $b^2 = 1$, $ba = a^{-1}b$. $G \cong D_8$ by Proposition 1.8.1.

(iv) $b^2 = a^2$, $ba = a^{-1}b$. $G \cong Q_8$ by Proposition 1.8.3

2.2.4 Quotient Groups

Definition. If $A$ and $B$ are subsets of a group $G$, then we define their product $AB = \{ab \mid a \in A, b \in B\}$.

The definition of quotient groups depends on the following crucial technical result.

Lemma 2.2.4 If $N$ is a normal subgroup of $G$ and $Ng$, $Nh$ are cosets of $N$ in $G$, then $(Ng)(Nh) = Ngh$.

Proof: Let $n_1g \in Ng$ and $n_2h \in Nh$. Then, by normality of $N$, we have $gN = Ng$, and so $gn_2$ is equal to some element $n_3g \in Ng$. Hence $(n_1g)(n_2h) = n_1(gn_2)h = n_1(n_3g)h = (n_1n_3)gh \in Ngh$, which proves $(Ng)(Nh) \subseteq Ngh$. Finally, $ngh = (ng)(1h) \in (Ng)(Nh)$, so $Ngh \subseteq (Ng)(Nh)$, and we have equality.

Proposition 2.2.5 Let $N$ be a normal subgroup of a group $G$. Then the set $G/N$ of right cosets $Ng$ of $N$ in $G$ forms a group under multiplication of sets.

Proof: We have just seen that $(Ng)(Nh) = Ngh$, so we have closure, and associativity follows easily from associativity of $G$. Since $(N1)(Ng) = N1g = Ng$ for all $g \in G$, $N1$ is an identity element, and since $(Ng^{-1})(Ng) = Ng^{-1}g = N1$, $Ng^{-1}$ is an inverse to $Ng$ for all cosets $Ng$. Thus the four group axioms are satisfied and $G/N$ is a group.

Definition. The group $G/N$ is called the quotient group (or the factor group) of $G$ by $N$.

Notice that if $G$ is finite, then $|G/N| = |G : N| = |G|/|N|$. Let us finish with the following fact.

Proposition 2.2.6 Let $N$ be a normal subgroup of a group $G$. Then the map $\phi : G \rightarrow G/N$ defined by $\phi(g) = Ng$ is a surjective group homomorphism with kernel $N$.

Proof: It is straightforward to check that $\phi$ is a surjective group homomorphism, and $\phi(g) = 1_H \Leftrightarrow Ng = N1_G \Leftrightarrow g \in N$, so $\ker(\phi) = N$. □
2.2. NORMAL SUBGROUPS

2.2.5 Examples of Quotient Groups

1. Let $G$ be the infinite cyclic group $(\mathbb{Z}, +)$, and let $N = n\mathbb{Z}$ be its subgroup generated by a fixed positive integer $n$ – let’s take $n = 5$ just to be specific. Now, by using Lemma 1.5.4 (after changing from multiplicative to additive notation!), we see that the cosets $5\mathbb{Z} + k$ and $5\mathbb{Z} + j$ of $N$ in $G$ are equal if and only if $k \equiv j \pmod{5}$. So there are only 5 distinct cosets, namely $N = N + 0$, $N + 1$, $N + 2$, $N + 3$, $N + 4$. It is now clear that $G/N$ is isomorphic to the group $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ (see Subsection 1.4.2) under the correspondence $N + i \to i$ for $0 \leq i < 5$.

2. Now let $G = \langle g \rangle$ be finite cyclic, and suppose that $|g| = lm$ is composite. Let $N$ be the normal subgroup $\langle g^m \rangle$. Using methods of Subsection 1.3.4, we can see that $N$ has order $l$ and consists of the elements $\{g^{mk} \mid 0 \leq k < l\}$. Since all cosets have the form $Ng^k$ for some $k \in \mathbb{Z}$, it is clear that $G/N$ is cyclic and is generated by $Ng$. We can calculate its order as $|G|/|N| = m$. To see this directly, note that (using Lemma 1.5.4 again) $Ng^k = Ng^j \iff g^{k-j} \in N \iff m|(k-j)$, and so the distinct cosets are $Ng^k$ for $0 \leq k < m$. In particular, $(Ng)^m = Ng^m = N1$ is the identity element of $G/N$, and $|Ng| = m$.

3. For a more complicated example, we take Example 4 of Subsection 2.2.2, namely $G = D_{12}$ and $N = \{1, a^3\}$. Then $|G/N| = |G|/|N| = 6$. For $g \in G$, let us denote $Ng$ by $\overline{g}$. (This is a commonly used notation, but you must always keep in mind that $\overline{g} \neq \overline{h}$ does not necessarily imply that $g = h$!) Then, since $a^3 \in N$, we have

$$\overline{a^3} = (Na)^3 = Na^3 = N1 = \overline{1}$$

is the identity of $G/N$. We also have $\overline{b^0} = 1$ and $\overline{ba} = \overline{a^{-1}b}$, because these relations are inherited from the corresponding relations of $G$. Thus $G/N$ is a group of order 6 satisfying the three relations $\overline{a^3} = 1$, $\overline{b^2} = 1$, $\overline{ba} = \overline{a^{-1}b}$, and so by Proposition 1.8.1 $G/N \cong D_6$.

It might be helpful in understanding this example to see the full multiplication table of $G$ again (we saw it already in Subsection 1.7.3), but this time with the elements arranged according to their cosets. Notice that all elements in each $2 \times 2$ block of this table lie in the same coset of $N$ in $G$. We can then see the multiplication table of $G/N$ by regarding these $2 \times 2$ blocks as single elements (i.e. cosets) in the quotient group.
CHAPTER 2. HOMOMORPHISMS

2.2.6 Exercises

(i) A group $G$ is simple if it has exactly two normal subgroups: $G$ and 1. Prove that a simple abelian group is a cyclic group of prime order.

(ii) Let $N \trianglelefteq G$. Prove that the subgroups of $G/N$ are precisely the quotient groups $I/N$, for subgroups $I$ of $G$ that contain $N$.

2.2.7 Vista

Classification of simple finite groups was both a major success and a major tragedy of the 20-th century mathematics. While the theorem is beautiful, the proof has spread over 30,000 journal pages. And up until now we have not got an acceptable proof. You can read more about this topic on wikipedia, search for “Classification of finite simple groups”.

<table>
<thead>
<tr>
<th>$N$</th>
<th>$Na$</th>
<th>$Na^2$</th>
<th>$Nb$</th>
<th>$Nab$</th>
<th>$Na^2b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$a^3$</td>
<td>$a a^4$</td>
<td>$b$</td>
<td>$ab$</td>
<td>$a^2 b$</td>
</tr>
<tr>
<td>$a^3$</td>
<td>1</td>
<td>$a^4$</td>
<td>$a^5$</td>
<td>$a^2$</td>
<td>$a^3 b$</td>
</tr>
<tr>
<td>$a^4$</td>
<td>$a^4$</td>
<td>$a^5$</td>
<td>$a^5$</td>
<td>$b$</td>
<td>$ab$</td>
</tr>
<tr>
<td>$a^5$</td>
<td>$a^4$</td>
<td>$a^2$</td>
<td>1</td>
<td>$a^3$</td>
<td>$a^4 b$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$Nb$</th>
<th>$Nab$</th>
<th>$Na^2b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$b$</td>
<td>$a^2 b$</td>
</tr>
<tr>
<td>$a^3 b$</td>
<td>$a^4 b$</td>
<td>$a^2 b$</td>
</tr>
<tr>
<td>$a^5 b$</td>
<td>$a^4 b$</td>
<td>$a^2 b$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$Na$</th>
<th>$Na^2$</th>
<th>$Nab$</th>
<th>$Na^2b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$a^3$</td>
<td>$a a^4$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a^3$</td>
<td>1</td>
<td>$a^4$</td>
<td>$a^5$</td>
</tr>
<tr>
<td>$a^4$</td>
<td>$a^4$</td>
<td>$a^5$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a^5$</td>
<td>$a^4$</td>
<td>$a^2$</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$Na^2$</th>
<th>$Nab$</th>
<th>$Na^2b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$b$</td>
<td>$a^2 b$</td>
</tr>
<tr>
<td>$a^3 b$</td>
<td>$a^4 b$</td>
<td>$a^2 b$</td>
</tr>
<tr>
<td>$a^5 b$</td>
<td>$a^4 b$</td>
<td>$a^2 b$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$Na$</th>
<th>$Na^2$</th>
<th>$Nab$</th>
<th>$Na^2b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$a^3$</td>
<td>$a a^4$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a^3$</td>
<td>1</td>
<td>$a^4$</td>
<td>$a^5$</td>
</tr>
<tr>
<td>$a^4$</td>
<td>$a^4$</td>
<td>$a^5$</td>
<td>$b$</td>
</tr>
<tr>
<td>$a^5$</td>
<td>$a^4$</td>
<td>$a^2$</td>
<td>1</td>
</tr>
</tbody>
</table>
2.3. Ideals

2.3.1 Executive Summary

We discuss ideals to develop some intuition about them. We introduce Euclidean domains and principal ideal domains and discuss ideals in them.

2.3.2 Ideals and domains

Let us recall that an ideal of a ring $R$ is an additive subgroup satisfying the two properties: $xI \subseteq I$ and $Ix \subseteq I$ for all $x \in R$. For a commutative ring these two properties are the same. For a non-commutative ring, one sometimes introduces left ideals satisfying $xI \subseteq I$ and right ideals satisfying $Ix \subseteq I$.

**Example. 1.** Let $R$ be a non-zero ring, $n \geq 2$. Let $I$ be the set of all matrices in $M_n(R)$ that vanish outside one particular row. Then $I$ is a right ideal but not an ideal. In particular, $I$ is not a left ideal. Likewise, let $J$ be the set of all matrices in $M_n(R)$ that vanish outside one particular column. Then $J$ is a left ideal but not an ideal. In particular, $J$ is not a right ideal.

We won’t take any interest in this course in the left and right ideals. They will be studied in the third year module Rings and Modules.

In this lecture, we will concentrate on principal ideals $(x)$ as these are the easiest ideals to work with. The construction is explained in the following proposition.

**Proposition 2.3.1** Let $R$ be a ring, $x \in R$. The subset

$$(x) = \{ \sum_{k=1}^{n} r_kxs_k | r_k, s_k \in R \}$$

is an ideal in $R$.

**Proof:** The subset is clearly non-empty. The difference of two sums $\sum_{k=1}^{n} r_kxs_k$ is also such a sum. Finally, $a(\sum_{k=1}^{n} r_kxs_k) = \sum_{k=1}^{n} (ar_k)x_k \in (x)$ and $\sum_{k=1}^{n} r_kxs_ka = \sum_{k=1}^{n} r_k(x(s_ka)) \in (x)$. \hfill \Box

**Examples. 2.** If $R$ is commutative $\sum_{k=1}^{n} r_kxs_k = x(\sum_{k=1}^{n} r_kx_k)$, so $(x) = xR = \{xr | r \in R \}.

3. In a noncommutative ring the principal ideals are trickier. For instance, $(E_{1,1}) = M_n(R)$ where $E_{ij}$ is a matrix with all zeroes except a single entry $1_R$.
CHAPTER 2. HOMOMORPHISMS

on the intersection of the $i$-th row and the $j$-th column. The key calculation

$$(r_{ij}) = \sum_{k,l} (r_{k,l}E_{k,1})E_{1,1}E_{1,l}$$

writes an arbitrary matrix $(r_{ij})$ as an element of the principal ideal.

This example shows that the following lemma fails for a non-commutative ring. In the case of commutative rings, the lemma provides a useful characterisation of units.

**Lemma 2.3.2** Let $R$ be a commutative ring, $x \in R$. Then $x \in R^*$ if and only if $(x) = R$.

**Proof:** $x \in R^*$ if and only if $\exists y \ xy = 1_R$ if and only if $1_R \in (x)$ if and only if $(x) = R$. The last forward implication is clear because if $1_R$ belongs to an ideal $I$ then $a = a \cdot 1 \in I$ for all $a \in R$. \hfill $\square$

**Definition.** Two non-zero elements $a, b$ in a ring $R$ such that $ab = 0_R$ are called zero divisors. A domain is a non-zero commutative ring without zero divisors.

There are good reasons not to call the zero ring a domain. Unfortunately, I could not think of a short convenient definition that automatically excludes it. Could you?

The following proposition has a straightforward proof but is useful for producing domains.

**Proposition 2.3.3** (1) A field is a domain.

(2) A subring of a domain is a domain

(3) A polynomial ring over a domain is a domain.

There are several types of domains of particular interest.

### 2.3.3 Euclidean domains and PID-s

**Definition.** A domain $R$ is called a principal ideal domain (abbreviated PID) if any ideal of $R$ is principal.

One convenient way to verify that a domain is a principal ideal domain is via Euclid’s algorithm. The following type of domains allow this.

**Definition.** A euclidean domain is a domain $R$ that admits a norm function $\nu : R \setminus \{0\} \to \mathbb{N}$ such that

(i) $\nu(ab) \geq \nu(b)$ for all $a, b \in R$;
2.3. IDEALS

(ii) \( \nu(ab) = \nu(b) \) if and only if \( a \in R^* \);

(iii) \( \forall a, b \exists q, r \) such that \( a = qb + r \) and either \( r = 0 \) or \( \nu(b) > \nu(r) \).

**Examples. 4.** Integers \( \mathbb{Z} \) form a euclidean domain. The norm function is an absolute value, that is, \( \nu(x) = |x| \). The elements \( q \) and \( r \) in the last property come from the division with a remainder. Notice that already in this case the elements \( q \) and \( r \) are not unique. Let \( a = 13, b = 5 \). Both \( 13 = 5 \cdot 2 + 3 \) and \( 13 = 5 \cdot 3 - 2 \) are acceptable.

5. The ring \( K[X] \) of polynomials in one variable over a field \( K \) is a euclidean domain. The norm function is the degree of a polynomial. Notice that \( K[X]^* \) consists of nonzero constant polynomials that ensures the second part of the definition. The elements \( q \) and \( r \) in the last property come from the polynomial division with a remainder.

6. Gaussian integers \( \mathbb{Z}[i] = \{a + bi \in \mathbb{C} | a, b \in \mathbb{Z} \} \) form a subring of \( \mathbb{C} \). Hence, it is a domain. It is euclidean with the norm function \( \nu(x) = |x|^2 \). The first property is clear. The second property follows from the fact that \( \mathbb{Z}[i]^* = \{1, -1, i, -i \} \), which follows from \( q^{-1} = q^*/|q|^2 \) where \( q^* = \text{Re}(q) - \text{Im}(q)i \) is the conjugate number of \( q \). For the third property choose the Gaussian integer \( q \) nearest to \( a/b \). Observe that \( |q - a/b| \leq 1/\sqrt{2} \). Let \( r = a - qb \). As soon as \( r \neq 0 \), \( \nu(r) = |a - qb|^2 = |q - a/b|^2|b|^2 \leq \nu(b)/2 < \nu(b) \).

The last calculation seems to make sense even for \( r = 0 \). What is about our exclusive disjunction “either . . . or”? The answer to this question is that the function \( \nu \) is not defined at zero, so the last calculation does not make sense. Look at the previous example (Example 5). There is not a way to say what the degree of a zero polynomial is without losing the precious property \( \text{deg}(fg) = \text{deg}(f) + \text{deg}(g) \).

**Theorem 2.3.4** A euclidean domain is a principal ideal domain.

**Proof:** Let \( I \) be an ideal in an euclidean domain \( R \). Choose \( b \in I \setminus \{0\} \) with the smallest possible norm. Obviously, \( (b) \subseteq I \). Let us now prove the opposite inclusion. For an arbitrary \( a \in I \) we can write \( a = bq + r \) with either \( r = 0 \) or \( \nu(b) > \nu(r) \). If \( r \neq 0 \) then \( r = a - bq \in I \) and has a smaller norm than \( b \). This contradiction proves that \( a = bq \in (b) \). \( \Box \)

Rings \( \mathbb{Z}[\alpha] \) for \( \alpha \in \mathbb{C} \) are domains but other properties are harder to predict. We will explain the following examples later in the course. For now you should take my word on them.
Examples. 7. The domain $\mathbb{Z}[\alpha]$ with $\alpha = (1 + \sqrt{-19})/2$ is PID but not euclidean.

8. The domain $\mathbb{Z}[\alpha]$ with $\alpha = \sqrt{-5}$ is not PID.

2.3.4 Applications

Principal ideals have several applications, which you may have seen already. The idea is always the same. Let us start with the minimal polynomial of a matrix. Let $K$ be a field, $A \in M_n(K)$ a matrix. It defines a ring homomorphism $f_A : K[\alpha] \rightarrow M_n(K)$ by $f_A(\sum_n \alpha_n \alpha^n) = \sum_n \alpha_n A^n$. This ring homomorphism is sometimes called evaluation homomorphism because $f_A(F(\alpha)) = F(A)$. The homomorphism $f_A$ is a linear map from an infinite dimensional vector space to a finite dimensional one. Hence, the kernel is non-zero. Since $K[\alpha]$ the kernel is an ideal $(m_A)$ for some polynomial $m_A \in K[\alpha]$. Multiplying $m_A$ by a scalar does not change the ideal, thus, without loss of generality, $m_A$ is monic (the highest degree term has a coefficient 1). This, $m_A$ is called the minimal polynomial of $A$. The kernel of $f_A$ consists of all polynomials $F(\alpha)$ such that $F(A) = 0$. Thus, $m_A$ is the monic polynomial of minimal degree such that $F(A) = 0$.

In a similar way, a complex number $\alpha \in \mathbb{C}$ a matrix defines an evaluation ring homomorphism $f_\alpha : \mathbb{Q}[\alpha] \rightarrow \mathbb{C}$ by $f_\alpha(F(\alpha)) = F(\alpha)$. The kernel is $(m_\alpha)$. If $m_\alpha = 0$ the number $\alpha$ is called transcendental: it does no satisfy any polynomial with rational coefficients. If $m_\alpha \neq 0$ the number $\alpha$ is called algebraic. Unique monic $m_\alpha$ is called the minimal polynomial of $\alpha$.

The last application of this sort is the characteristic of a ring. Any ring $R$ has a natural homomorphism $f_R : \mathbb{Z} \rightarrow R$ defined by $f_R(n) = n1_R$. The kernel of this homomorphism is $(n)$ for some $n \geq 0$. This number $n$ is the characteristic of $R$.

2.3.5 Exercises

(i) Show that if $R$ is a domain then $R[x_1 \ldots x_n]$ is a domain.

(ii) Prove the rest of Proposition 2.3.3.

(iii) Let $I$ and $J$ be ideals in a ring $R$. Show that $I + J = \{i + j \mid i \in I, j \in J\}$, $IJ = \{\sum_n i_n j_n \mid i \in I, j \in J\}$ and $I \cap J$ are also ideals in $R$.

(iv) Show that the ring $\mathbb{Q}_p$ from problem 3, homework 2 is Euclidean domain.
(v) Prove that the characteristic of a domain is always a prime number.

(vi) Describe all rings of characteristic 1.
2.4 Quotients and homomorphisms

2.4.1 Executive Summary
We start with quotient rings. Then we discuss the first isomorphism theorem. As an application we prove Cayley’s Theorem.

2.4.2 Quotient Rings
The following proposition defines the quotient ring \( R/I \) for a ring \( R \) and its ideal \( I \).

**Proposition 2.4.1** The cosets of an ideal form a ring under the addition in the quotient group and the multiplication \((I + a) \cdot (I + b) = I + ab\).

**Proof**: The only thing required to be proved is well-definedness. All axioms for \( R/I \) follow from the axioms of \( R \). The well-definedness follows from the following calculation. Let \( I + a = I + x \) and \( I + b = I + y \) then \( ab = ab - ay + ay - xy + xy = a(b - y) + (a - x)y + xy \). Hence \( ab - xy \in I \) and \( I + ab = I + xy \).

**Example. 1.** The quotient ring \( \mathbb{Z}/(n) \) is isomorphic to the ring \( \mathbb{Z}/n \) of the residues modulo \( n \). The isomorphism \( \mathbb{Z}_n \to \mathbb{Z}/(n) \) is just \( m \mapsto m + (n) \). Remember that we have never checked formally that \( \mathbb{Z}_n \) is a ring. This would do it. In fact, \( \mathbb{Z}(n) \) should be thought of as the definition of \( \mathbb{Z}_n \).

**Proposition 2.4.2** Let \( I \) be an ideal of a ring \( R \). Then the map \( \phi : R \to R/I \) defined by \( \phi(g) = I + g \) is a surjective ring homomorphism with kernel \( I \).

**Proof**: It is straightforward to check that \( \phi \) is a surjective ring homomorphism. Finally, \( \phi(x) = 0 \iff I + x = I \iff x \in I \), so \( \ker(\phi) = I \).

2.4.3 The First Isomorphism Theorem
**Theorem 2.4.3** (First Isomorphism Theorem for Groups) Let \( \phi : G \to H \) be a group homomorphism with the kernel \( K \). Then \( G/K \cong \text{im}(\phi) \). More precisely, there is an isomorphism \( \overline{\phi} : G/K \to \text{im}(\phi) \) defined by \( \overline{\phi}(Kg) = \phi(g) \) for all \( g \in G \).

**Proof**: The trickiest point to understand in this proof is that we have to show that \( \overline{\phi}(Kg) = \phi(g) \) really does define a map from \( G/K \) to \( \text{im}(\phi) \). The reason that this is not obvious is that we can have \( Kg = Kh \) with \( g \neq h \), and when that happens we need to be sure that \( \phi(g) = \phi(h) \). This is called checking that the map \( \overline{\phi} \) is well-defined. In fact, once you have understood
what needs to be checked, then doing it is quite easy, because \( Kg = Kh \Rightarrow g = kh \) for some \( k \in K = \ker(\phi) \), and then \( \phi(g) = \phi(k)\phi(h) = \phi(h) \).

Clearly \( \text{im}(\overline{\phi}) = \text{im}(\phi) \), and it is straightforward to check that \( \overline{\phi} \) is a homomorphism. Finally,

\[
\overline{\phi}(Kg) = 1_H \iff \phi(g) = 1_H \iff g \in K \iff Kg = K1 = 1_{G/K},
\]

and so \( \overline{\phi} \) is a monomorphism by Proposition 2.1.7. Thus \( \overline{\phi}: G/K \to \text{im}(\phi) \) is an isomorphism, which completes the proof. \( \square \)

Let us illustrate this theorem using Example 11 from Section 2.1. Note that the elements of \( G = D_{12} \) are listed in two separate columns in the diagram, in different orders, once for the domain and once for the codomain of \( \phi \). The elements of \( \text{im}(\phi) \) are printed slightly to the left of those not in \( \text{im}(\phi) \) in the codomain column.

A particular value of the first isomorphism theorem is that it tells us the structure of any homomorphism \( \phi: G \to H \). Indeed, \( \phi \) is composition of three other homomorphism: the quotient homomorphism \( G \to G/\ker(\phi) \), the isomorphism \( \overline{\phi} \) and the embedding \( \text{im}(\phi) \to H \).

**Theorem 2.4.4** (First Isomorphism Theorem for Rings) *Let \( \phi: R \to S \) be a ring homomorphism with the kernel \( I \). Then \( R/I \cong \text{im}(\phi) \). More precisely,
there is an isomorphism $\overline{\phi} : R/I \to \text{im}(\phi)$ defined by $\overline{\phi}(I + x) = \phi(x)$ for all $x \in R$.

PROOF: By Theorem 2.4.4, $\overline{\phi}$ is a well-defined isomorphism of abelian groups under addition. It is straightforward to check that it is a ring homomorphism. \qed

2.4.4 Cayley Theorem

As an application, let us prove Cayley’s theorem.

Theorem 2.4.5 (Cayley’s Theorem) Every group $G$ is isomorphic to a permutation group. (That is, to a subgroup of $\text{Sym}(X)$ for some set $X$.) If $G$ is finite the set $X$ can be chosen finite.

PROOF: Let $X = G$. Define a homomorphism $\phi$ by $\phi(x) : y \mapsto xy$. By Theorem 2.4.4, $G/\ker(\phi)$ is isomorphic to a subgroup of $\text{Sym}(X)$. Let us compute the kernel. If $x \in \ker(\phi)$ then $x = x \cdot 1 = [\phi(x)](1) = 1$. So the kernel is trivial and we are done. \qed

Why don’t mathematicians study premutation groups instead of groups? Well, the do both! Permutation group is not really just a group, but a group embedded in $S_n$, there could be different embeddings. You can consider $S_n$ in $S_n$ or $\text{Sym}(S_n) = S_n!$. 

2.5 More isomorphism theorems

2.5.1 Executive Summary

We prove the second and the third isomorphism theorem. We also consider some applications and computations.

2.5.2 Things as they stand

The other two isomorphism theorems are less important, and are used mainly in more advanced courses. Before we can state the Second Isomorphism Theorem, we need a lemma. Recall from Subsection 2.2.4 that the product of two subsets $A$ and $B$ of $G$ is defined as $AB = \{ab \mid a \in A, b \in B\}$. This is not usually a subgroup of $G$, even when $A$ and $B$ are subgroups (can you find an example to demonstrate this?). However, we have:

**Lemma 2.5.1** If $H$ is any subgroup and $K$ is a normal subgroup of a group $G$, then $HK = KH$ is a subgroup of $G$.

**Proof:** Let $hk \in HK$. Then, by normality of $K$, $hk \in hK = Kh \subseteq KH$ and similarly $KH \subseteq HK$, and we have equality. The product of two elements of $HK$ lies in $HKHK = HHHK = HK$, and the inverse $k^{-1}h^{-1}$ of an element $hk \in HK$ lies in $KH = HK$, so $HK$ is a subgroup of $G$ by Proposition 1.1.5. \hfill \Box

**Theorem 2.5.2** (Second Isomorphism Theorem for Groups) Let $H$ be any subgroup and let $K$ be a normal subgroup of a group $G$. Then $H \cap K$ is a normal subgroup of $H$ and $H/(H \cap K) \cong HK/K$.

**Proof:** Use Proposition 2.2.2 to show that $H \cap K \leq H$. Let $\phi : G \rightarrow G/K$ be the natural map (see Theorem 2.1.5(ii)). Then $\phi(H)$ is the set of cosets $Kh$ for $h \in H$, which together form the subgroup $KH/K = HK/K$ of $G/K$; in other words $\text{im}(\phi_H) = HK/K$. Also $\ker(\phi_H) = H \cap \ker(\phi) = H \cap K$. Now, by applying Theorem 2.4.3 to $\phi_H$, we get $H/(H \cap K) \cong HK/K$. \hfill \Box

**Example.** Let $K$ and $H$ be respectively the subgroups $\{1, a^2, a^4\}$ and $\{1, a^3, b, a^3b\}$ of $G = D_{12}$. Then $K \cong C_3$ and $H$ is a Klein Four Group. $K$ is a normal subgroup: to check this, use Proposition 2.2.2; for example,

$$(a^k b) a^2 (a^k b)^{-1} = a^k ba^2 b^{-1} a^{-k} = a^k a^4 a^{-k} = a^4$$

for all $k \in \mathbb{Z}$. Clearly $H \cap K = \{1\}$ is trivial, and so $H/(H \cap K) \cong H$ is also a Klein Four Group. By direct calculation, we find $HK = G$, so $HK/K = G/K$ is a Klein Four Group.
Let us formulate the second isomorphism theorem for rings now.

**Theorem 2.5.3** (Second Isomorphism Theorem for Rings) Let $S$ be any subring and let $I$ be an ideal in a ring $R$. Then $S \cap I$ is an ideal in $S$ and $S/(S \cap I) \cong S + I/I$.

**Proof**: Using Theorem 2.5.2 for the additive groups, we get an isomorphism $S/(S \cap I) \cong S + I/I$ of the groups under addition which is coming from a group homomorphism $\eta : S \rightarrow S + I/I$, $\eta(s) = s + I$.

It is easy to observe that $S + I$ is a subring and $I$ is an ideal in it. Finally, it remains to observe that $\eta$ is a ring homomorphism that follows from the fact that $\eta$ is a restriction of the quotient homomorphism $R \rightarrow R/I$ to $S$. □

### 2.5.3 Third Isomorphism Theorem

**Theorem 2.5.4** (Third Isomorphism Theorem for Groups) Let $K \subseteq H \subseteq G$, where $H$ and $K$ are both normal subgroups of $G$. Then $(G/K)/(H/K) \cong G/H$.

**Proof**: Define $\phi : G/K \rightarrow G/H$ by $\phi(Kg) = Hg$ for all $g \in G$. As in the proof of Theorem 2.4.3, we need to check that this is well-defined; that is, that $Kg_1 = Kg_2 \Rightarrow \phi(g_1) = \phi(g_2)$. This is easy, because $K \subset H$, so $Kg_1 = Kg_2 \Rightarrow Hg_1 = Hg_2$.

Since $\text{im}(\phi) = G/H$ and $\ker(\phi) = H/K$, the result follows by applying Theorem 2.4.3 to $\phi$. □

Let us do it for the rings now.

**Theorem 2.5.5** (Third Isomorphism Theorem for Rings) Let $I \subseteq J \subseteq R$, where $I$ and $J$ are both ideals in $R$. Then $J/I$ is an ideal in $R/I$ and $(R/I)/(J/I) \cong R/J$.

**Proof**: One just needs to observe that the map $\phi : R/I \rightarrow R/J$ defined by $\phi(I + r) = J + r$ for all $r \in R$ is a ring homomorphism. The rest of the proof is the same as in Theorem 2.5.4. □

### 2.5.4 Chinese Remainder Theorem

The comparisons modulo $n$ in Number Theory become much clearer using quotient rings. We recall that one writes $x \equiv y \pmod{n}$ if $n$ divides $x - y$. In our notation, one can write it as the equality of cosets $x + (n) = y + (n)$.

One can use Proposition 1.3.6 to prove the following theorem but we prefer to give another, more high tech proof using the methods we have just developed.
Theorem 2.5.6 (Chinese Remainder Theorem) Let $n_i, i = 1, \ldots, t$ be natural numbers such that each pair $n_i, n_j, i \neq j$ is coprime. The system of comparisons $x + (n_i) = k_i + (n_i)$ admits a solution in $\mathbb{Z}$. Any two solutions are different by a multiple of $N = n_1 \cdot \ldots \cdot n_t$.

PROOF: Let us consider the homomorphism
\[ \psi : \mathbb{Z} \to \prod_i \mathbb{Z}/(n_i), \quad \psi(x) = (x + (n_1), \ldots, x + (n_t)). \]

It is clearly a ring homomorphism. The kernel consists of all $x$ divisible by all $n_i$. Since they are pairwise coprime, $\ker(\psi) = (N)$. By the first isomorphism theorem, $\mathbb{Z}/N$ is isomorphic to a subring of $\prod_i \mathbb{Z}/(n_i)$. Since both rings have the same number of elements they are isomorphic. Consequently, $\psi$ is surjective.

Now let us analyse what it tells us about the system. The surjectivity of $\psi$ ensures an existence of a solution because the system can be written as a single equation
\[ \psi(x) = (k_1, \ldots, k_t). \]
If $x, x'$ are two solutions of this equation, $x - x' \in \ker(\psi) = (N)$, so their difference is divisible by $N$.

2.5.5 A calculations

Essentially, the main application of the isomorphism theorems is recognition of various groups and rings that appear. Let us look at two examples.

Let $R = \mathbb{Z}[i]/(1 - 2i)$. Let us denote $J = (1 - 2i)$. The homomorphism $\psi : \mathbb{Z} \to R$ is surjective because $1 + J = 2i + J$ implies $i + J = -2 + J$ (by multiplication by $i$). Hence, $a + bi + J = (a - 2b) + J$ is in the image. If $n \in \ker(\psi)$ then $n = (x + yi)(1 - 2i) = (x + 2y) + (y - 2x)i$ for some $x, y \in \mathbb{Z}$. This means that $y = 2x$ and $n = 5x$ Hence, $\ker(\psi) = (5)$ and, by the first isomorphism theorem, $R \cong \mathbb{Z}_5$.

Consider the ring $R_a = \mathbb{R}[x]/(x^2 - a)$ for some $a \in \mathbb{R}$. If $J = (x^2 - a)$ then elements of $R_a$ are $ax + \beta + J$. In the case of $a > 0$, the homomorphism $\mathbb{R}[x] \to \mathbb{R} \times \mathbb{R} x \mapsto (-\sqrt{a}, \sqrt{a})$ gives rise to an isomorphism $R_a \cong \mathbb{R} \times \mathbb{R}$. In the case of $a < 0$, the homomorphism $\mathbb{R}[x] \to \mathbb{C} x \mapsto \sqrt{|a|}i$ gives rise to an isomorphism $R_a \cong \mathbb{C}$.

2.5.6 Exercises

(i) Prove Proposition 1.3.6 using the method of the proof.
(ii) Compute the ring \( \mathbb{Z}[i]/(1 + 3i) \).

(iii) Compute the ring \( \mathbb{Z}[i]/(5 + 3i) \).

(iv) Complete all the details in the last example concerning \( R_a \).

(v) Show that \( R_0, R_1 \) and \( R_{-1} \) are pairwise non-isomorphic rings.
Chapter 3

Group action on sets

3.1 Actions, Orbits and Stabilisers

3.1.1 Definition and Action

Definition. Let $G$ be a group and $X$ a set. An action of $G$ on $X$ is a map $\cdot : G \times X \to X$, which satisfies the properties:

(i) $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G, x \in X$;
(ii) $1_G \cdot x = x$ for all $x \in X$.

Note 1. In this definition, the image of $(g, x)$ under the map $\cdot$ is denoted by $g \cdot x$.

2. We have actually defined a left action of $G$ on $X$. A right action can be defined analogously as a map $X \times G \to X$.

Proposition 3.1.1 Let $\cdot$ be an action of the group $G$ on the set $X$. For $g \in G$, define the map $\phi(g) : X \to X$ by $\phi(g)(x) = g \cdot x$. Then $\phi(g) \in \text{Sym}(X)$, and $\phi : G \to \text{Sym}(X)$ is a homomorphism.

Proof: Property (ii) in the definition says that $\phi(1_G)$ is the identity map $I_X : X \to X$, and then Property (i) implies that $\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = I_X$, and similarly $\phi(g^{-1})\phi(g) = I_X$. So $\phi(g)$ and $\phi(g^{-1})$ are inverse maps, which proves that $\phi(g) : X \to X$ is a bijection. Hence $\phi(g) \in \text{Sym}(X)$, and then Property (i) implies immediately that $\phi$ is a homomorphism. 

The opposite is also true: a homomorphism $\phi : G \to \text{Sym}(X)$ defines an action $g \cdot x = \phi(g)(x)$. In fact, it gives a bijection between the set of actions $G \times X \to X$ and the set of homomorphisms $\phi : G \to \text{Sym}(X)$.
The kernel of an action \( \cdot \) of \( G \) on \( X \) is defined to be the kernel \( K = \ker(\phi) \) of the homomorphism \( \phi : G \to \text{Sym}(X) \) defined in Proposition 3.1.1. So

\[
K = \{ g \in G \mid g \cdot x = x \text{ for all } x \in X \}.
\]

The action is said to be faithful if \( K = \{1\} \). In this case, Theorem 2.4.3 says that \( G \cong G/K \cong \text{im}(\phi) \), which we state as a proposition, which can be thought of as a generalisation of Cayley’s Theorem (Theorem 2.4.5).

**Proposition 3.1.2** If \( \cdot \) is a faithful action of \( G \) on \( X \), then \( G \) is isomorphic to a subgroup of \( \text{Sym}(X) \).

**Examples.** 1. If \( G \) is a subgroup of \( \text{Sym}(X) \), then we can define an action of \( G \) on \( X \) simply by putting \( g \cdot x = g(x) \) for \( x \in X \). This action is faithful.

2. Let \( P \) be a regular hexagon, and let

\[
G = \{1, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\} = D_{12}
\]

be the group of isometries of \( P \). In Subsection 1.7.3, we defined \( a \) and \( b \) to be the permutations \((1, 2, 3, 4, 5, 6)\) and \((2, 6)(3, 5)\) of the set \( \{1, 2, 3, 4, 5, 6\} \) of vertices of \( P \), and so this immediately gives us an action of \( G \) on the vertex set.

There are some other related actions however. We could instead take \( X \) to be the set \( E = \{e_1, e_2, e_3, e_4, e_5, e_6\} \) of edges of \( P \), where \( e_1 \) is the edge joining 1 and 2, \( e_2 \) joins 2 and 3, etc. The map \( \phi \) of the action of \( G \) on \( E \) is then given by \( \phi(a) = (e_1, e_2, e_3, e_4, e_5, e_6) \), \( \phi(b) = (e_1, e_6)(e_2, e_5)(e_3, e_4) \). (Notice that any homomorphism is fully specified by the images of a set of group generators, because the images of all other elements in the group can be calculated from these.) This action is still faithful.

As a third possibility, let \( D = \{d_1, d_2, d_3\} \) be the set of diagonals of \( P \), where \( d_1 \) joins vertices 1 and 4, \( d_2 \) joins 2 and 5, and \( d_3 \) joins 3 and 6. Then map \( \phi \) of the action of \( G \) on \( D \) is defined by \( \phi(a) = (d_1, d_2, d_3) \), and \( \phi(b) = (d_2, d_3) \). This action is not faithful, and its kernel is the normal subgroup \( \{1, a^3\} \) of \( G \) that we have already studied. The image is isomorphic to \( D_6 \).

3. There is a faithful action called the left regular action, which we can define for any group \( G \). Here we put \( X \) to be the underlying set of \( G \) and simply define \( g \cdot x \) to be \( gx \) for all \( g \in G, x \in X \). Conditions (i) and (ii) of the definition obviously hold, so we have defined an action. If \( g \) is in the
kernel $K$ of the action, then $gx = x$ for all $x \in X$, which implies $g = 1$ by the cancellation law, so the action is faithful. From Proposition 3.1.2, we can deduce Cayley’s Theorem (Theorem 2.4.5).

4. $G$ acts on the set of left cosets of a subgroup $H$ by $g \cdot xH = gxH$.

### 3.1.2 Orbits and Stabilisers

**Definition.** Let $\cdot$ be an action of $G$ act on $X$. We define a relation $\sim$ on $X$ by $x \sim y$ if and only if there exists a $g \in G$ with $y = g \cdot x$. Then $\sim$ is an equivalence relation – the proof is left as an exercise. The equivalence classes of $\sim$ are called the **orbits** of $G$ on $X$. In particular, the orbit of a specific element $x \in X$, which is denoted by $G \cdot x$ or by $\text{Orb}_G(x)$ is

$$\{ y \in X \mid \exists g \in G \text{ with } g \cdot x = y \}.$$

In most of the examples that we have seen so far, there is just one orbit, the whole of $X$. Here is an example with two orbits. Let $X$ be a set, and $Y$ a proper nonempty subset of $X$. In Example 7 of Subsection 1.1.5, we defined the subgroup $\text{Sym}(X)_Y$ of $\text{Sym}(X)$ to be $\{ g \mid g \in \text{Sym}(X), g(y) \in Y \text{ and } g^{-1}(y) \in Y \ \forall y \in Y \}$. Denote this subgroup by $G$, and give it the obvious action on $X$ with $g \cdot x = g(x)$ for $g \in G, x \in X$. Then there are two orbits, $Y$ and $X \setminus Y$.

In a similar way, for any partition of $X$, we can can define a subgroup of $\text{Sym}(X)$ having the sets in this partition as the orbits.

**Definition.** Let $G$ act on $X$ and let $x \in X$. Then the stabiliser of $x$ in $G$, which is denoted by $G_x$ or by $\text{Stab}_G(x)$ is $\{ g \in G \mid g \cdot x = x \}$.

The proof of the following proposition is left as an exercise.

**Proposition 3.1.3** Let $G$ act on $X$ and $x \in X$. Then

(i) $\text{Stab}_G(x)$ is a subgroup of $G$;

(ii) $\cap_{x \in X} \text{Stab}_G(x)$ is the kernel of the action of $G$ on $X$.

The next theorem is a very fundamental result in group theory. **Theorem 3.1.4** (The Orbit-Stabiliser Theorem) Let a group $G$ act on $X$, $x \in X$. Then there is a bijection between elements of $\text{Orb}_G(x)$ and left cosets of $\text{Stab}_G(x)$. In particular, $|\text{Orb}_G(x)| = |G : \text{Stab}_G(x)|$.

**Proof:** We consider a function $\psi : G \to X$ defined by $\psi(g) = g \cdot x$
Let $y \in \text{Orb}_G(x)$. Then there exists a $g \in G$ with $g \cdot x = y$. Let $H = \text{Stab}_G(x)$. For an element $g' \in G$, we have

$$g' \cdot x = y \iff g' \cdot x = g \cdot x \iff g^{-1}g' \cdot x = x \iff g^{-1}g' \in H \iff g' \in gH.$$ 

So the elements $g'$ with $g' \cdot x = y$ are precisely the elements of the coset $gH = \psi^{-1}(y)$. Hence, $\psi$ defines a bijection between the set of cosets and the orbit.  

**Examples.** 1. The Hopf fibration from Homework 1 is an example of an action. The sphere $S^3$ is the group of norm 1 quaternions. The sphere $S^2$ is the set of imaginary norm 1 quaternions. The action map $S^3 \times S^2 \to S^2$ is written using the multiplication in the quaternions: $g \cdot x = gxg^{-1}$. By choosing a particular quaternion $I \in S^2$ one gets the fibration $S^3 \to S^2$ by $x \mapsto xIx^{-1}$.

2. Liner Algebra and Advanced Linear algebra is concerned with 3 particular group actions, although this terminology is not used there. The first action has $G = \text{GL}_n(K) \times \text{GL}_m(K)$ and the set of $n \times m$ matrices $X$. Two matrices are equivalent if they can be moved to each other by a sequence of elementary row and column transformations. The elementary transformation is just a multiplication by an elementary matrix, who together generate the general linear group. In our language we consider the action $(g,h) \cdot x = gxh^{-1}$ whose orbits are the equivalence classes. An orbit consists of matrices with a given rank and admits a unique representative in row and column echelon form (also called Smith’s normal form).

3. The second Linear Algebra action has $G = \text{GL}_n(\mathbb{C})$ and $X = M_n(\mathbb{C})$. Two matrices $A$ and $B$ are similar if there exists $q \in G$ such that $qAq^{-1} = B$. In our language we consider the action $g \cdot x = gxg^{-1}$ whose orbits are the similarity classes. An orbit consists of matrices with a given rank and admits a representative in Jordan normal form (if more then one they are related by a permutation of blocks).

4. The last Linear Algebra action has actually two groups $G = \text{GL}_n(\mathbb{R}) \geq H = \text{O}_n(\mathbb{R})$ acting on the same set $X$ of real symmetric $n \times n$ matrices. It appears in the classification of bilinear forms In our language we consider the action $g \cdot x = gxg^T$. A $G$-orbit is determined by the rank and the signature of the form and admits a diagonal representative with 0, ±1 on the diagonal. An $H$-orbit is determined by the eigenvalues and also admits a diagonal representative with the eigenvalues on the diagonal.
3.1.3 Exercises

(i) Prove that \(\sim\), defined in this lecture, is an equivalence relation.

(ii) Check the action axioms in the four examples just above.
3.2 Fixed Points and Quotients

3.2.1 Executive Summary

We introduce the notions of fixed points and quotients. We prove three important formulae related to actions and discuss its applications to combinatorics.

3.2.2 Definitions

We consider a group $G$ acting on a set $X$ in this section.

**Definition.** The quotient set $X/G$ is the set of orbits.

**Example.** Let $X = H$ be a group containing $G$ as a subgroup. The action is by the left multiplication $(g, x) \mapsto gx$. The orbits of this action are right cosets $Gx$. The quotient set is the set of all right cosets. In particular, if $G$ is normal in $H$, the quotient set admits a group structure which we called the quotient group.

**Definition.** Let $T \subseteq G$ be a subset of $G$. The fixed points (or the fixed point set) is defined as $X_T = \{ x \in X | \forall g \in T \ g \cdot x = x \}$. In particular, we are interested in $X^g = X^{(g)}$ for $g \in G$ and $X^G$.

Notice that in the above example $X^g = \emptyset$ unless $g = 1$, in which case $X^1 = X$. Such actions are called fixed points free or simply free.

3.2.3 Formulae

We would like to establish three useful formulae underlining combinatorics of the group action. The first is an immediate consequence of Theorem 3.1.4

**Proposition 3.2.1** (The Orbit-Stabiliser Formula) Let $G$ be a finite group acting on a finite set $X$. The for any $x \in X$

$$|G| = |\text{Orb}_G(x)||\text{Stab}_G(x)|.$$

**Proposition 3.2.2** (The Counting Formula) Let $G$ be a finite group acting on a finite set $X$. Then

$$|X| = |X^G| + \sum_x |G||\text{Stab}_G(x)|$$

where the sum is taken over the representatives of all orbits containing more than 1 element.
3.2. FIXED POINTS AND QUOTIENTS

Proof: $X$ is a disjoint union of orbits. One element orbits form $X^G$. The number of elements in the larger orbits is $\sum_x |\text{Orb}_G(x)| = \sum_x |G|/|\text{Stab}_G(x)|$ using Proposition 3.2.1.

\[ |X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|. \]

Proof: Let $A = \{(g,x) \in G \times X | g \cdot x = x\}$. The formula is obtained by counting the size of $A$ in two different ways. On one hand,

\[ |A| = \sum_{g \in G} |X^g|. \]

On the other hand,

\[ |A| = \sum_{x \in X} |\text{Stab}_G(x)| = \sum_{x \in X} |G|/|\text{Orb}_G(x)| = |G| \sum_{\text{orbits } x \in \text{ an orbit}} 1/|\text{Orb}_G(x)| =
\]

\[ = |G| \sum_{\text{orbits}} 1 = |G||X/G|. \]

□

3.2.4 Applications to Combinatorics

The formulae allow us to do certain calculations. Let us count the number of geometrically distinct colourings of a regular pentagon using $n$ colours. Let us paint the sides of the pentagon, each side into each own paint. Let $S$ be the set of sides. Hence a colouring is a function $f : X \rightarrow \mathbb{Z}_n$, and the set of all colourings $C$ has a cardinality $n^5$.

What are geometrically the same colourings? The group $D_{10}$ acts on $S$. It gives an action on $C$ given by formula: $g \cdot c(s) = c(g^{-1} \cdot s)$ where $g \in D_{10}$, $s \in S$, $c \in C$. Two colourings are geometrically the same if they are in the same $D_{10}$-orbit (or the same $C_5$-orbit if we want rotational symmetry only).

With only rotational symmetry we want to count the number of $C_5$-orbits. Observe that 1 fixes every colouring while a non-trivial rotation fixes only the colourings that use the same colour for each side. Hence, by Burnside’s formula $|C/C_5| = (n^5 + n + n + n + n)/5 = (n^5 + 4n)/5$.

Allowing reflectional symmetry, we want to count the number of $D_{10}$-orbits. Each of 5 reflections fixes colouring that uses 3 colours. Hence, by Burnside’s formula $|C/D_{10}| = (n^5 + 4n + 5n^3)/10$. 
Read an example in Lauritzen where he counts the number of colouring of a regular octagon into 4 white and 4 black colours.

3.2.5 Exercises
(i) Check that the alternative formula \( g \cdot c(s) = c(g \cdot s) \) with \( g \in D_{10}, s \in S, c \in C \) does not define an action but a right action.

(ii) Count the number of geometrically different colourings of a regular heptagon into 4 white and 3 black colours. Do both calculations, with and without reflections.

(iii) Count the number of geometrically different colourings of a regular \( 2p \)-gon (where \( p \) is prime) into \( n \) colours. Do both calculations, with and without reflections.

(iv) Count the number of geometrically different colourings of a regular \( p^2 \)-gon (where \( p \) is prime) into \( n \) colours. Do both calculations, with and without reflections.
3.3 Conjugacy classes

3.3.1 Executive Summary
We apply the set actions to study groups. Each group acts on itself in an interesting way.

3.3.2 Definition
In Example 3 of Subsection 3.1.1, a group $G$ was made to act on the set of its own elements by multiplication on the left; that is, $g \cdot x = gx$ for $g, x \in G$.

There is another important action of $G$ on $X = G$, which is defined by

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

for $g, x \in G$.

It is easy to check that conditions (i) and (ii) of the definition hold, so this does indeed define an action. This action is called conjugation. The orbits of the action are called the conjugacy classes of $G$, and elements in the same conjugacy class are said to be conjugate in $G$. So $g, h \in G$ are conjugate if and only if there exists $f \in G$ with $h = fgf^{-1}$. We will write $\text{Cl}_G(g)$ for the orbit of $g$; that is the conjugacy class containing $g$. We have seen already in Proposition 2.1.2 that conjugate elements have the same order.

What is $\text{Stab}_G(g)$ for this action? By definition it consists of the elements $f \in G$ for which $f \cdot g = g$; that is, $fgf^{-1} = g$, or equivalently $fg = gf$. In other words, it consists of those $f$ that commute with $g$. It is called the centraliser of $g$ in $G$ and is written as $C_G(g)$. Notice that the fixed point set of $g$ also consists of all $f$ such that $gf^{-1} = f$, i.e. commute with $g$. Hence $G^g = C_G(g)$.

By applying the formulae from the last lecture (3.2.1, 3.2.2, and 3.2.3) we get:

The kernel $K$ of the action consists of those $f \in G$ that fix and hence commute with all $g \in G$. This is called the centre of $G$ and is denoted by $Z(G)$. So we have

$$Z(G) = \{ f \in G \mid fg = gf \ \forall g \in G \}.$$ 

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

It is high time that we worked out some examples!

**Example.** 1. Let $G$ be an abelian group. Then $Z(G) = G$, $C_G(g) = G$ and $\text{Cl}_G(g) = \{ g \}$ for all $g \in G$.

2. $Q_8$ has 5 conjugacy classes: $\{ 1 \}$, $\{ -1 \}$, $\{ \pm I \}$, $\{ \pm J \}$, $\{ \pm K \}$. 


3. The conjugacy classes in $\text{GL}_n(F)$ have been studied in *Linear Algebra* and *Algebra-I*. Two matrices are in the same conjugacy class if and only if they are similar.

**Proposition 3.3.1** Let $G$ be a finite group, $g \in G$. The following three formulae hold, in the second one the summation is taken over representatives of all conjugacy classes, not in the centre.

(i) $|\text{Cl}_G(g)| = |G|/|C_G(g)|$

(ii) $|G| = |Z(G)| + \sum_x |G|/|C_G(x)|$

(iii) $|G/G| = \frac{1}{|G|} \sum_{g \in G} |C_G(g)|$

### 3.3.3 Conjugacy classes in dihedral groups

Let $G = \{a^k \mid 0 \leq k < n\} \cup \{a^kb \mid 0 \leq k < n\}$ be the dihedral group $D_{2n}$. Then of course, as always, $\text{Cl}_G(1) = \{1\}$. To compute the remaining classes, we calculate $fgf^{-1}$ in the four cases, when $f$ and $g$ have the form $a^k$ ($1 \leq k < n$) and $a^kb$ ($0 \leq k < n$). Since $b^2 = 1$, we have $b = b^{-1}$, so we shall always substitute $b$ for $b^{-1}$ in our calculations.

(i) $f = a^l$, $g = a^k$: $fgf^{-1} = g$.

(ii) $f = a^lb$, $g = a^k$: $fgf^{-1} = ba^kb = a^{-k} = g^{-1}$.

(iii) $f = a^l$, $g = a^kb$: $fgf^{-1} = a^{k+l}ba^{-l} = a^{k+l}a^l = a^{k+2l}b$.

(iv) $f = a^lb$, $g = a^kb$: $fgf^{-1} = a^lba^kbba^{-l} = a^lba^{k-l} = a^l a^{l-k} = a^{2l-k}b$.

The cases when $n$ is odd and even are different. Suppose first that $n$ is odd. Then, by (i) and (ii), $a$ and $a^{-k} = a^{n-k}$ are conjugate for all $k$, and we have the distinct conjugacy classes $\{a^k, a^{n-k}\}$ for $1 \leq k \leq (n-1)/2$, all of which contain just two elements. By (iii), we see that $b$ is conjugate to $a^{2l}b$ for $0 \leq l < n$, and when $n$ is odd, this actually includes all elements $a^l b$ for $0 \leq l < n$. (For example, $ab = a^{2l}b$ with $l = (n+1)/2$.) So the set $\{a^l b \mid 0 \leq l < n\}$ forms a single conjugacy class. Geometrically, this is not surprising, because these $n$ elements are all reflections that pass through one vertex and the centre of the polygon $P$ of which $G$ is the group of isometries.

Now suppose that $n$ is even. Then, when $k = n/2$, we have $a^k = a^{-k}$, and so $\{a^{n/2}\}$ is a conjugacy class of size 1 (and hence $a^{n/2} \in Z(G)$). We also have the classes $\{a^k, a^{n-k}\}$ of size 2 for $1 \leq k \leq (n-2)/2$. In this case, the reflections $a^k b$ split up into two conjugacy classes of size $n/2$, namely $\{a^{2k}b \mid 0 \leq k < n/2\}$ and $\{a^{2k+1}b \mid 0 \leq k < n/2\}$. Geometrically these
3.3. CONJUGACY CLASSES

Correspond to the two different types of reflections: those about lines that pass through two vertices of $P$ and those about lines that bisect two edges of $P$.

3.3.4 Applications to Group Theory (Classification of groups up to order 11)

As an application we extend our classification of groups to the order 11. Since 11 is done, we need to concentrate on orders 9 and 10.

Proposition 3.3.2 A group of order $p^n$, $p$ is prime has a non-trivial centre.

Proof: By Formula (1) of Proposition 3.3.1, sizes of conjugacy classes are powers of $p$. By Formula (2) of Proposition 3.3.1, $p$ must divide $Z(G)$. Hence, the centre is non-trivial.

Proposition 3.3.3 Let $p$ be a prime number. There are two groups of order $p^2$ up to an isomorphism: $C_p \times C_p$ and $C_{p^2}$.

Proof: These two groups are non-isomorphic by Lemma 1.3.5: $C_{p^2}$ has an element of order $p^2$ but $C_p \times C_p$ hasn’t.

Let us start by proving that $G$ of order $p^2$ is abelian. By Proposition 3.3.2, $Z(G) \neq 1$. By Lagrange’s Theorem, $|Z(G)|$ is either $p$, or $p^2$. In the latter case $G$ is abelian. Suppose the former case. Pick $x \in G \setminus Z(G)$ and consider $C_G(x)$. It clearly contains $Z(G)$ and $x$. Thus $|C_G(x)|$ is bigger than $p$, hence it is $p^2$. Thus $C_G(x) = G$. It is a contradiction as we conclude $x \in Z(G)$.

If $G$ admits an element $a$ of order $p^2$, $G$ is a cyclic group.

If $G$ has no such element, all non-identity elements have order $p$. As in the homework problem, $G$ admits a vector space structure over the field $\mathbb{Z}_p$.

Choosing a basis, forces an isomorphism $G \cong C_p \times C_p$.

Proposition 3.3.4 Let $p$ be a prime number. There are two groups of order $2p$ up to an isomorphism: $D_{2p}$ and $C_{2p}$.

3.3.5 Exercises

(i) Find all centralisers and the centre in $D_{2n}$.

(ii) Prove Proposition 3.3.4
3.4 Conjugacy classes in alternating groups

3.4.1 Executive Summary

3.4.2 Conjugacy classes in symmetric groups

Let $G = \text{Sym}(X)$ and let $f, g \in G$. Let us write $g$ in cyclic notation, and suppose that one of the cycles of $g$ is $(x_1, x_2, \ldots, x_r)$. Then $g(x_1) = x_2$, and so $fg(x_1) = f(x_2)$ and hence $f^{-1}(f(g(x_1))) = f(x_2)$. Similarly, we have $f^{-1}(f(x_i)) = f(x_{i+1})$ for $1 \leq i < r$ and $f^{-1}(f(x_r)) = f(x_1)$. Hence $fg^{-1}$ has a cycle $(f(x_1), f(x_2), \ldots, f(x_r))$, and we have:

**Proposition 3.4.1**
Given a permutation $g$ in cyclic notation, we obtain the conjugate $fg^{-1}$ of $g$ by replacing each element $x \in X$ in the cycles of $g$ by $f(x)$.

For example, if $X = \{1, 2, 3, 4, 5, 6, 7\}$, $g = (1, 5)(2, 4, 7, 6)$ and $f = (1, 3, 5, 7, 2, 4, 6)$, then $f^{-1} = (3, 7)(4, 6, 2, 1)$.

In general, we say that a permutation has cycle-type $2^23^3 \ldots$, if it has exactly $r_i$ cycles of length $i$, for $i \geq 2$. So, for example,

$$(1, 15)(2, 4, 6, 8, 7)(5, 9)(3, 11, 12, 13, 10)(14, 15, 16)$$

has cycle-type $2^23^15^2$. By Proposition 3.4.1, conjugate permutations have the same cycle-type, and conversely, it is easy to see that if $g$ and $h$ have the same cycle-type, then there is an $f \in \text{Sym}(X)$ with $f^{-1} = h$. For example, if $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $g = (1, 5, 9)(2, 4, 6, 8)(7, 10)$ and $h = (1, 5)(2, 10, 9)(3, 6, 8, 7)$, then we can choose $f$ to map $1, 5, 9, 2, 4, 6, 8, 7, 10, 3$ to $2, 10, 9, 3, 6, 8, 7, 1, 5, 4$, respectively, so $f = (1, 2, 3, 4, 6, 8, 7)(5, 10)$. ($f$ is not unique; can you find some other possibilities?) Hence we have:

**Proposition 3.4.2**
Two permutations of $\text{Sym}(X)$ are conjugate in $\text{Sym}(X)$ if and only if they have the same cycle-type.

For example, $S_3$ has three conjugacy classes, corresponding to cycle-types $1, 2^1, 3^1$, and $S_4$ has five conjugacy classes, corresponding to cycle-types $1, 2^1, 2^2, 3^1, 4^1$. 

3.4.3 Conjugacy classes in subgroups

If \( H \) is a subgroup of \( G \), the conjugacy classes of \( H \) are obviously subsets of conjugacy classes of \( G \). We would like to make two observations on their interaction.

**Proposition 3.4.3** Let \( G \) be a finite group, \( H \) its subgroup of index 2, \( x \in H \). One of the following two mutually exclusive statements holds.

1. There exists \( g \in G \setminus H \) such that \( gx = xg \). In this case, \( \text{Cl}_G(x) = \text{Cl}_H(x) \).
2. For all \( g \in G \setminus H \) such that \( gx \neq xg \). In this case, \( \text{Cl}_G(x) \) is a union of \( \text{Cl}_H(x) \) and \( \text{Cl}_H(y) \) for any \( y \in \text{Cl}_G(x) \setminus \text{Cl}_H(x) \). Moreover, \(|\text{Cl}_G(x)|/2 = |\text{Cl}_H(x)| = |\text{Cl}_H(y)|\).

**Proof:** By Proposition 2.2.1, \( H \) is normal subgroup of \( G \). Hence, \( \text{Cl}_G(x) \subseteq H \).

In the case (1), \( C_H(x) \) is a proper subgroup of \( C_G(x) \). Hence, by Lagrange's theorem \(|C_G(x)| \geq 2|C_H(x)|\). Using Proposition 3.3.1, \(|\text{Cl}_G(x)| = |G|/|C_G(x)| \leq 2|H|/2|C_H(x)| = |\text{Cl}_H(x)|\). Hence, \( \text{Cl}_G(x) = \text{Cl}_H(x) \).

In the case (2), \( C_H(x) = C_G(x) \). Using Proposition 3.3.1, \(|\text{Cl}_G(x)| = |G|/|C_G(x)| = 2|H|/|C_H(x)| = 2|\text{Cl}_H(x)|\). Pick \( g \in \text{Cl}_G(x) \setminus \text{Cl}_H(x) \). It suffices to observe that \(|\text{Cl}_G(x)|/2 = |\text{Cl}_H(g)|\). But \( g = aax^{-1} \) for some \( a \in G \). Consequently, \( C_H(g) = aC_H(x)a^{-1} \). In particular, \(|C_H(g)| = |aC_H(x)a^{-1}|\) and the calculation above shows that \(|\text{Cl}_G(x)| = 2|\text{Cl}_H(g)|\).

The next lemma is an criterion for normality.

**Lemma 3.4.4** A subgroup \( H \) of a group \( G \) is normal in \( G \) if and only if \( H \) consists of a union of conjugacy classes of \( G \).

**Proof:** By Proposition 2.2.2, \( H \leq G \) if and only if \( ghg^{-1} \in H \) for all \( g \in G \), \( h \in H \). But this is just saying that \( H \leq G \) if and only if \( h \in H \Rightarrow \text{Cl}_G(h) \subseteq H \), and the result follows.

For example, consider the subgroup \( \{(1), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} \) of \( S_4 \). This is the union of the conjugacy classes of \( S_4 \) containing elements of cycle-types 1 and \( 2^2 \), and so it is a normal subgroup. Incidentally, since this subgroup lies in \( A_4 \), it is also normal in \( A_4 \), and so \( A_4 \) is not simple.

3.4.4 The Simplicity of \( A_4 \)

In Subsection 2.2.4, we defined a group \( G \) to be simple if its only normal subgroups are \( \{1\} \) and \( G \), and we saw that the only abelian simple groups are the cyclic groups of prime order. There are also infinitely many finite nonabelian simple groups. These were eventually completely classified into
a number of infinite families, together with 26 examples known as sporadic
groups, that do no belong to an infinite family. The work on this proof went
on for decades, the completion was announced in 1981 but a complete proof
is yet to appear.

One of the infinite families of finite nonabelian simple groups consists of
the alternating groups $A_n$ for $n \geq 5$. The aim of this section will be to prove
that $A_5$ is simple.

The conjugacy classes of $A_n$ can be described using Proposition 3.4.3 We
need is for $A_5$. The classes of $S_5$ correspond do cycle-types $1, 2^1, 2^2, 3^1, 2^1 3^1, 4^1, 5^1$, and of these, the permutations of cycle-types $1, 2^2, 3^1$ and $5^1$ are even per-
mutations and hence lie in $A_5$.

There is 1 permutation of cycle-type 1, 15 of type $2^2$, 20 of type $3^1$, and
24 of type $5^1$, making 60 elements in total.

The problem is that these are classes in $S_n$, and two permutations could
conceivably be conjugate in $S_n$ but not in $A_n$, in which case the corresponding
class would split up into more than one conjugacy class in $A_n$.

In fact, the 15 permutations of cycle-type $2^2$ forms a single class in $A_n$.
Using Proposition 3.4.3, $g = (x_1, x_2)(x_3, x_4)(x_5)$ commutes with $h = (x_1, x_2)$.

Similarly, the 20 permutations of cycle-type $3^1$ are all conjugate in $A_n$,
because $g = (x_1, x_2, x_3)(x_4)(x_5)$ commutes with $h = (x_4, x_5)$.

However, for the cycle-type $5^1$, if $g = (1, 2, 3, 4, 5)$ does not commute with
odd permutations. The size of its conjugacy class is $4! = 24$, so the size of
its centraliser is $120/24 = 5$. It already commutes with $1, g, g^2, g^3, g^4$, so it
cannot commute with anything else.

Alternatively, you can argue that 24 does not divide $|A_5| = 60$, so the
$S_5$-conjugacy class must split into two $A_5$-conjugacy classes.

Summing up, we have:

**Lemma 3.4.5** $A_5$ has 5 conjugacy classes, of sizes 1, 15, 20, 12, 12.

**Theorem 3.4.6** $A_5$ is a simple group.

**Proof:** By Lemma 3.4.4, a normal subgroup $N$ of $A_5$ would be a union of
conjugacy classes of $A_5$. But no combination of the numbers 1, 15, 20, 12,
12 that contains 1 adds up to a divisor of 60 other than 1 or 60, and so the
result follows by Lagrange’s Theorem (1.6.2).
3.4. CONJUGACY CLASSES IN ALTERNATING GROUPS

3.4.5 Exercises

(i) Verify that Proposition 3.4.3 holds for $C_n$ inside $D_{2n}$. Find precisely which conjugacy classes in $D_{2n}$ split into two and which one don’t.

(ii) Show that if a permutation $f \in A_n$ contains an independent cycle of even length then $f$ commutes with an odd permutation.

(iii) Show that if a permutation $f \in A_n$ contains two independent cycles of the same length then $f$ commutes with an odd permutation.

(iv) Show that if a permutation $f \in A_n$ contains independent cycles pairwise distinct odd length then $f$ does not commutes with odd permutations.

(v) Count the number of conjugacy classes in $S_n$ and $A_n$ for $1 \leq n \leq 9$. Compute the sizes of the conjugacy classes.
3.5 Symmetries

3.5.1 Executive Summary

We finally prove that the sign of a permutation is well-defined. To this we need to introduce actions of groups on rings and algebras. Then we discuss group actions on other structures.

3.5.2 Actions on rings

When a group $G$ acts on a set $X$ with additional structure, we usually want the bijections $x \mapsto g \cdot x$ to preserve this structure.

Definition. Let $G$ be a group and $R$ a ring. An action of $G$ on the ring $R$ is an action on the set $\cdot : G \times R \to R$ such that $x \mapsto g \cdot x$ is a ring homomorphism.

Notice that since the action of $g$ is a bijection, this ring homomorphism must be a ring isomorphism. We recall explicitly the properties of a homomorphism.

1. $g \cdot (ab) = (g \cdot a)(h \cdot b)$ and $g \cdot (a+b) = (g \cdot a) + (h \cdot b)$ for all $g \in G$, $a, b \in R$;
2. $g \cdot 1_R = 1_R$ for all $g \in G$.

Let us define $\text{Aut}(R) = \{ \phi \in \text{Sym}(R) \mid \phi \text{ is a ring homomorphism} \}$. Its elements, isomorphisms with itself, are called automorphisms. The following is an adaptation of Proposition 3.1.1 to the situation of rings.

Proposition 3.5.1 $\text{Aut}(R)$ is a subgroup of $\text{Sym}(R)$. Moreover, if a group $G$ acts on a ring $R$ then the image of the natural homomorphism $\phi : G \to \text{Sym}(R)$ lies in the subgroup $\text{Aut}(R)$.

Proof: Using Proposition 1.1.5, it suffices to check that if $\phi$ and $\psi$ are ring automorphisms then so are $\phi^{-1}$ and $\phi \psi$.

The second part of the proposition follows immediately from the definition of the action on a ring. \hfill \Box

Let us make another elementary observation. We are not going to use it, hence no proof is given.

Proposition 3.5.2 Let a group $G$ act on a ring $R$. The set of fixed points $R^G$ is a subring.

The elements of $R^G$ are often called invariants or $G$-invariants.
3.5.3 Algebras

Some of the rings we introduced, such as $M_n(F)$ or $F[X]$, are not only
rings but also vector spaces over a field $F$. The following abstract definition
captures this situation.

**Definition.** An algebra is a pair $(R, F)$ such that $F$ is a field, $R$ is both a
ring and a vector space over $F$ such that these two structures share the same
addition and $\alpha(ab) = (\alpha a)b = a(\alpha b)$ for all $\alpha \in F, a, b \in R$.

**Example.** The quaternions $\mathbb{H}$ form naturally an algebra over real numbers,
that is, an algebra $(\mathbb{H}, \mathbb{R})$. However, they don’t form an algebra over complex
numbers. If $1, I, J, K$ is the standard basis of $\mathbb{H}$, we can try naively $(a + bi) \cdot h = ah + bIh$ for all $a + bi \in C, h \in H$. But the algebra axiom fails as
$i(JK) = II = -1 \neq 1 = J(-J) = J(iK)$.

The next proposition sheds some light on the nature of algebra structures.
Let us recall that the centre of a ring $R$ is $Z(R) = \{a \in R | \forall x \in R \ xa = ax\}$. It is a subring of $R$.

**Proposition 3.5.3** Let $R$ be a ring, $F$ a field. There is a bijection between
the set $A = \{(R, F) | (R, F) \text{ is an algebra}\}$ of algebra structures and the set
$B$ of algebra homomorphisms from $F$ to $Z(R)$.

**Proof:** We construct inverse bijections $\alpha : A \to B$ and $\beta : B \to A$. An
element of $A$ is a function $\star F \times R \to R$ defining a vector space structure and
satisfying axiom. We define the homomorphism $\phi = \alpha(\star)$ by $\phi(f) = f \star 1_R$.
From now on we reserve the notation for arbitrary elements $f, \tilde{f} \in F, r, \tilde{r} \in R$.
The image of $\phi$ lies in $Z(R)$ because of the algebra axiom: $\phi(f)r = (f \star 1)r = f \star (1 \cdot r) = f \star (r \cdot 1) = r \cdot (f \star 1) = r\phi(f)$. Two axioms of a homomorphism
follow from the vector space axioms: $\phi(f + \tilde{f}) = (f + \tilde{f}) \star 1 = f \star 1 + \tilde{f} \star 1 = \phi(f) + \phi(\tilde{f})$ and $\phi(1_F) = 1_F \star 1_R = 1_R$. The third axiom follows from the
algebra conditions: $\phi(f \tilde{f}) = (f \tilde{f}) \star 1 = f \star (\tilde{f} \star 1) = f \star (1 \cdot \phi(\tilde{f})) = (f \star 1) \cdot \phi(\tilde{f}) = \phi(f) \phi(\tilde{f})$. Hence, $\alpha$ is well-defined.

Now let us see that a function $\beta$, where $\beta(\phi) = \star$ is defined by $f \star r = \phi(f)r$, is well-defined. The vector space axioms follow from the homomorphism properties of $\phi$: $(f + \tilde{f}) \star (r + \tilde{r}) = \phi((f + \tilde{f})(r + \tilde{r})) = \phi(f) + \phi(\tilde{f}) + \phi(\tilde{f}) + \phi(\tilde{f}) = f \star r + f \star \tilde{r} + \tilde{f} \star r + \tilde{f} \star \tilde{r}$ and $(f \tilde{f}) \star r = \phi(f \tilde{f}) \star r = \phi(f) \phi(\tilde{f})r = f \star (\tilde{f} \star r)$. Finally the first part of the algebra axiom follows
from associativity $f \star (\tilde{f} \star r) = (f \tilde{f}) \star r = (f \star \tilde{f}) \star r$ and the second part follows
from the fact that the image lies in the centre: $(\phi(f)r)\tilde{r} = (aa)b = a(ab)$.
CHAPTER 3. GROUP ACTION ON SETS

It remains to show by calculation that these two functions are inverses of each others. To see that \( \alpha(\beta(\phi)) = \phi \) we apply it to \( f \in F \). Then 
\[
\alpha(\beta(\phi))(f) = (\beta(\phi))(f, 1_R) = \phi(f)1_R = \phi(f).
\]
To see that \( \beta(\alpha(\star)) = \star \) we apply it to \( (f, r) \in F \times R \). Then 
\[
\beta(\alpha(\star))(f, r) = \alpha(\star)(f) \cdot r = (f \star 1)r = f \star (1r) = f \star r.
\]

An algebra homomorphism from \( A = (R, F) \) to \( B = (S, F) \) where both algebras are over the same field \( F \) is just a ring homomorphism from \( R \) to \( S \) which is also a linear map. An action of a group \( G \) on an \( F \)-algebra \( A = (R, F) \) is an action on the the ring \( R \) such that the action map \( x \mapsto g \cdot x \) is an algebra homomorphism for each \( g \in G \).

The example of primary interests is the polynomial algebra \( A = (R, F) \) with \( R = F[X_1, \ldots X_n] \) over a field \( F \). \( A \) is an \( F \)-algebra under the usual multiplication by a scalar. The symmetric group \( S_n \) acts on the algebra \( A \) by permuting variables, namely, \( \sigma \star \Phi(X_1, \ldots X_n) = \Phi(X_{\sigma(1)}, \ldots X_{\sigma(n)}) \). For instance, if \( \Phi = X_1^2 \) then 
\[
(1, 2, 3) \star \Phi = \Phi(X_2, X_3, X_1, X_4, \ldots) = X_2^2 - X_1.
\]
Invariants of this action include power functions \( \Pi_k = X_1^k + X_2^k + \ldots + X_n^k \), \( k \geq 0 \) as well as elementary symmetric functions \( \Sigma_k, 1 \leq k \leq n \) defined as the coefficients of the polynomial
\[
(Z + X_1)(Z + X_2) \cdots (Z + X_n) = Z^n + \Sigma_1 Z^{n-1} + \ldots + \Sigma_n Z^{n-t} + \ldots + \Sigma_n
\]
In fact, any invariant is a polynomial in elementary symmetric functions but we don’t need this rather deep theorem.

3.5.4 Sign Function

Let a group \( G \) act on an algebra \( (R, F) \). An element \( r \in R \) is called a semiinvariant if \( G \cdot r \subseteq Fr \), in other words, for any \( g \in G \) there exists \( \alpha \in F \) such that \( g \cdot r = \alpha r \).

Proposition 3.5.4 Let \( r \in R \) be a nonzero semiinvariant for an action of a group \( G \) on an algebra \( (R, F) \). Then the formula \( g \cdot r = \phi(g)r \) defines a group homomorphism \( \phi : G \to F^* \).

Proof: The formula defines a function \( \phi : G \to F^* \). It remains to see that this is a homomorphism. \( \phi(gh)r = gh \cdot r = g \cdot (h \cdot r) = g \cdot \phi(h)r = \phi(g)\phi(h)r \).

As \( r \neq 0 \) and \( F^* \) is abelian, the statement follows.

By finding an appropriate semiinvariant we can establish the sign function and parity of permutations.
3.5. SYMMETRIES

Corollary 3.5.5 The function \( \text{sign} : S_n \to \{\pm 1\} \) defined by \( \text{sign}((i, j)) = -1 \) is a well-defined group homomorphism.

Proof: We consider the action of the symmetric group \( S_n \) on the algebra \( (\mathbb{R}[X_1, \ldots, X_n], \mathbb{R}) \). The function \( \Omega = \prod_{i>j}(X_i - X_j) \in \mathbb{R}[X_1, \ldots, X_n] \) is a semi-invariant because for \( \sigma \in S_n \) the function \( \sigma \cdot \Omega = \prod_{i>j}(X_{\sigma(i)} - X_{\sigma(j)}) \) contains either \( X_i - X_j \) or \( X_j - X_i = -(X_i - X_j) \) for each pair \( i > j \). Hence \( \sigma \cdot \Omega = \pm \Omega \).

Let \( \text{sign} : S_n \to \mathbb{R}^* \) be the corresponding group homomorphism. Since \( S_n \) is a finite group, every element in the image has a finite order. The only elements of finite order in \( \mathbb{R}^* \) are \( \pm 1 \). Hence it is a homomorphism \( \text{sign} : S_n \to \{\pm 1\} \cong \mathbb{Z}_2 \).

It remains to compute \( \text{sign}(s) \) for \( s = (i, j), \ i > j \). To this we represent \( \Omega \) as a product of 5 functions \( \Omega = \omega_1 \omega_2 \omega_3 \omega_4 \omega_5 \) and compute all the actions separately. First \( \omega_1 = X_i - X_j \) and \( s \cdot \omega_1 = X_j - X_i = -\omega_1 \). Then

\[
\omega_2 = \prod_{t>s, t\neq i, t\neq j, s\neq i, s\neq j} (X_t - X_s)
\]

in which no \( X_i \) or \( X_j \) appear. Consequently, \( s \cdot \omega_2 = \omega_2 \). The remaining three functions are similar, as they pair \( X_i \) and \( X_j \) with \( X_t \) in one of 3 regions:

\[
\omega_3 = \prod_{t>i} (X_t - X_i)(X_t - X_j), \quad s \cdot \omega_3 = \prod_{t>i} (X_t - X_j)(X_t - X_i) = \omega_3,
\]

\[
\omega_4 = \prod_{i>t>j} (X_i - X_t)(X_t - X_j), \quad s \cdot \omega_4 = \prod_{i>t>j} (X_j - X_t)(X_t - X_i) = \omega_4,
\]

\[
\omega_5 = \prod_{t<j} (X_i - X_t)(X_j - X_t), \quad s \cdot \omega_5 = \prod_{t<j} (X_j - X_t)(X_t - X_i) = \omega_5.
\]

Consequently, \( s \cdot \Omega = (s \cdot \omega_1)(s \cdot \omega_2)(s \cdot \omega_3)(s \cdot \omega_4)(s \cdot \omega_5) = -\Omega \) proving that \( \text{sign}(s) = -1 \). \( \square \)

3.5.5 Exercises

(i) Show that the function \( \Omega^2 \) is invariant.

(ii) In the case of \( n = 2 \), express \( \Omega^2 \) via elementary symmetric functions. How does it help to solve quadratic equations?

(iii)
3.5.6 Vista: Galois Theory, Erlangen Problem and Physics

Read about all these things on Internet. Groups take their origin in Galois theory where groups control solutions of algebraic equations. In Erlangen Problem of Klein groups are groups of symmetries of various geometries controlling underlying geometries. In Physics, symmetries are omnipresent leading to conservation laws.
Chapter 4

Factorisation

4.1 Divisibility

4.1.1 Executive Summary

We study divisibility in a domain. We introduce prime elements in the two natural ways but arrive at two different notions.

4.1.2 Basic Definitions

We are working in a domain \( R \) in this lecture. We already know two types of domains: euclidean (ED) and principal ideal (PID).

Definition. Let \( x, y \in R \) we say that \( x \) divides \( y \) and write \( x \mid y \) if \( y = xr \) for some \( r \in R \).

The following lemma is obvious.

Lemma 4.1.1 The following statements are equivalent for all \( x, y \in R \).

(i) \( x \mid y \).

(ii) \( y \in (x) \).

(iii) \( (x) \supseteq (y) \).

Definition. Let \( x, y \in R \). We say that \( x \) and \( y \) are associate (write \( x \sim y \)) if both \( x \mid y \) and \( y \mid x \).

Lemma 4.1.2 The following statements are equivalent
(i) \( x \sim y \)

(ii) \( (y) = (x) \)

(iii) There exists \( q \in R^* \) such that \( x = qy \)

**Proof**: \((i \Rightarrow iii)\) It is clear if \( x = 0 \). Without loss of generality we may assume that \( x \neq 0 \neq y \). There exist \( r, t \in R \) such that \( x = ry \) and \( y = tx \). Then \( x = ry = r(tx) \) and \( (1 - rt)x = 0 \). Because \( R \) is a domain, \( 1 - rt = 0 \) and \( q = r \in R^* \).

The other implications are obvious. \( \square \)

In \( \mathbb{Z} \) all the divisibility is usual. Notice that \( x \sim y \) if and only if \( x = \pm y \).

In a general domain, divisibility properties are invariant under the equivalence relation of being associate. In other words, if \( x \) satisfies a certain divisibility property then so is any such \( y \) that \( x \sim y \). For instance, it is easy to observe (and left as an exercise) that any two greatest common divisors are associate.

**Definition.** Let \( x, y \in R \). The greatest common divisor \( \gcd(x, y) \) is such \( d \in R \) that \( d|x, d|y \), and if \( z|x \) and \( z|y \) then \( z|d \). The least common multiple \( \text{lcm}(x, y) \) is such \( l \in R \) that \( x|l, y|l \), and if \( x|z \) and \( y|z \) then \( l|z \).

Uniqueness (up to an associate element) are established in the exercises. Existence is a bit trickier. It may not exist in an arbitrary domain.

**Proposition 4.1.3** If \( R \) is PID then \( \text{lcm}(x, y) \) and \( \gcd(x, y) \) exist for any pair of elements \( x, y \in R \).

**Proof**: Pick \( d, l \in R \) such that \( (d) = (x) + (y) \) and \( (l) = (x) \cap (y) \). We claim that \( d \) is the greatest common divisor and \( l \) is the least common multiple. Indeed, \( (x) \subseteq (d) \supseteq (y) \) and whenever \( (x) \subseteq (z) \supseteq (y) \) it follows that \( (z) \supseteq (x) + (y) = (d) \). Similarly, \( (x) \supseteq (l) \subseteq (y) \) and whenever \( (x) \supseteq (z) \subseteq (y) \) it follows that \( (z) \subseteq (x) \cap (y) = (l) \). \( \square \)

Note that \( (x) + (y) = \{rx + sy\} \), hence \( d = rx + sy \) for some \( r \) and \( s \).

### 4.1.3 Prime and Irreducible Elements

There are two different ways to say what a prime number is. We are going to see that these lead to two different notions in an arbitrary domain.

**Definition.** Let us consider \( r \in R \setminus (R^* \cup \{0\}) \). We say that \( r \in R \) is **irreducible** if and \( r = ab \) implies that \( a \in R^* \) or \( b \in R^* \). We say that \( p \in R \) is **prime** if \( p \in R \setminus R^* \) and \( p|xy \) implies that \( p|x \) or \( p|y \).
Proposition 4.1.4 A prime element $r$ is irreducible.

Proof: Let $p = ab$. Then $p|a$ or $p|b$ since $p|p = ab$. Without loss of generality, $p|a$. Hence $p \sim a$ and $p = aq$ with $q \in R^*$. The domain condition implies that $q = b$. □

Proposition 4.1.5 If $R$ is a PID, an irreducible element $r$ is prime.

Proof: This proof is quite tricky (at least for me personally) and we have to use the fact that $R$ is PID twice. Let $r$ be irreducible, $r|ab$. The element $\tilde{a} = \gcd(r, a)$ exists by Proposition 4.1.3. Then $r = \tilde{a}t$ for some $t \in R$. Since $r$ is irreducible, $\tilde{a}$ or $t$ is a unit. We consider both cases.

Let $t$ be unit. Then $r \sim \tilde{a}$ and it must divide $a$.

Now let $\tilde{a}$ be a unit. Using the description of the greatest common divisor in a PID, $(\tilde{a}) = (1) = (a)+(r)$. Hence, $1 = xa + yr$ for some $x, y \in R$. Finally, $r$ divides $xab = (1 - yr)b = b - yrb$. Hence, $b = (b - yrb) + ybr \in (r)$. □

Example. Let $R = \mathbb{Z}[i \sqrt{5}]$. In this ring, $6 = 2 \cdot 3 = (1 + i \sqrt{5})(1 - i \sqrt{5})$. We claim that 2 is irreducible but not prime.

2 does not divide $1 \pm i \sqrt{5}$ because $2x = 1 \pm i \sqrt{5}$ implies that $x = 1/2 \pm i \sqrt{5}/2$, which is not an element of $R$. Hence, 2 is not prime.

Let us show that 2 is irreducible. If $2 = ab$ with $a = x + yi \sqrt{5}$, $b = s + ti \sqrt{5} \in R$ then $4 = \|a\|^2 \|b\|^2 = (x^2 + 5y^2)(s^2 + 5t^2)$. Clearly, $\|a\|^2, \|b\|^2 \in \mathbb{N}$. If $\|a\|^2 = 1$ then $a^{-1} = a^*/\|a\|^2 = x - yi \sqrt{5} \in R$ and $a$ is a unit in $R$. Similarly, if $\|a\|^2 = 4$ then $\|b\|^2 = 1$ and $b$ is a unit in $R$. Finally, $\|a\|^2 = 2$ leads to a contradiction. Indeed, $\|a\|^2 = x^2 + 5y^2 = 2$ leads to $(x + (5))^2 = 2 \in \mathbb{Z}_5$ which is impossible.

Corollary 4.1.6 $\mathbb{Z}[i \sqrt{5}]$ is neither PID, nor Euclidean.

The next proposition was not in the lecture. This fact has been added because of its convenience for future references.

Proposition 4.1.7 Let $R$ be a domain. A nonzero element $p \in R$ is prime if and only if $R/(p)$ is a domain.

4.1.4 Exercises

(i) Prove Lemma 4.1.1.

(ii) Let $d$ and $d'$ be both the greatest common divisor $\gcd(x, y)$. Prove that $d$ and $d'$ are associate.
(iii) Let \( l \) and \( l' \) be both the least common multiple \( \text{lcm}(x, y) \). Prove that \( l \) and \( l' \) are associate.

(iv) Let \( p \) be prime. Show that if \( p|a_1 \cdot a_2 \cdots a_n \) then \( p \) divides \( a_i \).

(v) Prove Proposition 4.1.7.
4.2 UFD-s

4.2.1 Executive Summary

We introduce the notion of factorisation (into irreducible elements) and its uniqueness. We go on to prove a deep and difficult theorem that every PID admits a unique factorisation.

4.2.2 Unique Factorisation

**Definition.** A domain $R$ is FD (factorisation domain) if each $x \in R \setminus (R^* \cup \{0\})$ admits a factorisation $x = r_1 \cdot r_2 \cdots r_n$ where $r_i$ are irreducible elements.

An FD $R$ is UFD (unique factorisation domain) if for any two factorisations of an element $x = r_1 \cdot r_2 \cdots r_n = s_1 \cdot s_2 \cdots s_m$ (all $r_i$ and $s_i$ are irreducible), $m = n$ and there exists $\sigma \in S_n$ such that $r_i \sim s_{\sigma(i)}$ for all $i$.

**Proposition 4.2.1** Let $R$ be an FD. Then $R$ is a UFD if and only if every irreducible element is prime.

**Proof:** For the only if part we consider an irreducible element $x$ such that $x | ab$. Factorising $a = r_1 \cdots r_k$ and $b = r_{k+1} \cdots r_n$, we get a factorisation $ab = r_1 \cdots r_n$. On the other hand, $ab = xy$. Factorising $y = s_1 \cdots s_t$, we get another factorisation $ab = x r \cdot s_1 \cdots s_t$. By the UFD property, $x$ is associate to $r_i$ for some $i$. If $i \leq k$ then $x | a$. If $i > k$ then $x | b$.

The if part follows by a standard induction on $n$, the length of one of factorisations $x = r_1 \cdot r_2 \cdots r_n = s_1 \cdot s_2 \cdots s_m$. If $n = 1$ then $x = r_1$ is irreducible and everything follows. If we are done for $n - 1$, we observe that $r_n | s_1 \cdot s_2 \cdots s_m$. Since $r_n$ is prime it divides some $s_i$. Hence, $r_1 = q s_i$ for some unit $q$. Now we use the induction assumption on $(qr_1) \cdot r_2 \cdots r_{n-1} = s_1 \cdots s_{i-1} \cdot s_{i+1} \cdots s_m$. \qed

**Theorem 4.2.2** A PID is a UFD.

**Proof:** Using Propositions 4.1.5 and 4.2.1, it suffices to show that $R$ is FD. We have to factorise an arbitrary $x \in R \setminus (R^* \cup \{0\})$. If $x$ is irreducible then we are done. If not we can write $x = x_{1,1} \cdot x_{1,2}$ where $x_{1,i}$ are not units.

We are going to repeat this step over and over again. The step $n+1$ starts with $x = x_{n,1} \cdot x_{n,2} \cdots x_{n,k}$ where none of $x_{n,i}$ are units. If $x_{n,i}$ is irreducible for all $i$, we have arrived to factorisation of $x$. We terminate the process. If not pick all of $x_{n,i}$ which are not irreducible, write them as a product of two non-units $x_{n,i} = x_{n+1,j} \cdot x_{n+1,i+1}$. In this case, we write $x = x_{n+1,1} \cdot x_{n+1,2} \cdots x_{n+1,t}$ and continue with the process.
If this process terminates for all \( x \), we are done: \( R \) is FD. Now suppose the process does not terminate for some particular \( x \) and we are after some sort of contradiction. The process goes on forever and produces a set of decompositions \( x = x_{n,1} \cdot x_{n,2} \cdots x_{n,k} \), one decomposition for each natural number \( n \). The latter statement seems to be obvious but there is a set theoretic issue: we use recursion, which is some sort of induction, to construct a set. Why can we do? The answer is because of Recursion Theorem in Set Theory. Let us not get any further into this now.

The next step requires some abstract thinking. To facilitate it, think of all this decompositions as a binary tree. The root of the tree is the element \( x \). The nodes at level \( n \) are elements \( x_{n,i} \) for all \( i \). If \( x_{n,i} \) is irreducible, it does not have any upward edges. If \( x_{n,i} = x_{n+1,j} \cdot x_{n+1,i+1} \), it has two upward edges going to \( x_{n+1,j} \) and \( x_{n+1,i+1} \). Since the process has not terminated, the tree is infinite. This means there is an infinite path in this tree starting from the root and going upward. Let \( y_n = x_{n,i} \) be the element of this infinite path at level \( n \). In particular, \( y_0 = x \). Observe that \( \ldots y_{n+1} | y_n \ldots y_1 | y_0 \).

We have done all this hard work to obtain the ascending chain of ideals \( \ldots (y_{n+1}) \supset (y_n) \ldots (y_1) \supset (y_0) \) with all the inclusions proper. The trick is that their union \( I = \bigcup_{n=1}^\infty (y_n) \) is an ideal. This is true because all of the ideal conditions could be checked at one particular \( (y_n) \) (do the exercises below if you have difficulties with it). Since \( R \) is a PID, \( I = (d) \) for some particular \( d \in R \). Then \( d \in (y_n) \) for some \( n \). This implies that \( I = (d) \subseteq (y_n) \). Consequently, \( I = (d) = (y_n) = (y_{n+1}) = \ldots = (y_{n+i}) \) that contradicts all the ideal inclusions being proper.

**Examples.**

1. All our ED-S \( \mathbb{Z}, \mathbb{Z}[i], F[X] \) are UFD-s.

2. \( \mathbb{Z}[i\sqrt{5}] \) is FD but not UFD. We have seen that it is not UFD since \( 6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}) \) are two distinct factorisations. We won’t prove in this course that this ring is FD.

3. \( \mathbb{Z}[X] \) is UFD, which will be proved later, but not PID. \((2) + (X)\) is not principal.

4. The birth of Ring Theory is generally associated to the following Lame’s 1847 mistake (see http://www.mathpages.com/home/kmath447.htm ). Let \( \omega = \exp(2\pi i/p) \) where \( p > 2 \) is a prime number. Lame has essentially proved that if \( \mathbb{Z}[\omega] = \{ \sum_{i=0}^{p-1} a_i \omega^i \in \mathbb{C} \mid a_i \in \mathbb{Z} \} \) is a UFD then the Fermat Last Theorem holds for \( p \), i.e. the equation \( x^p + y^p = z^p \) have no integral solutions. Lame has not given enough thought to the issue and just used the UFD property of \( \mathbb{Z}[\omega] \). Kummer has corrected this mistake and given
a criterion in terms of Bernoulli numbers for \( \mathbb{Z}[\omega] \) to be UFD. A prime \( p \) is called \textit{regular} (correspondingly \textit{irregular}) if \( \mathbb{Z}[\omega] \) is UFD (correspondingly not UFD). Looking at small primes, it appears that all are regular. In fact, the first irregular prime is 37; then 59, 67, 101, 103, 131, 149 are irregular. On the other hand, it has been proved that there are infinitely many irregular primes. It is expected that irregular primes constitute about 39% of all the primes but it is still an open problem whether there are infinitely many of them.

4.2.3 Exercises

(i) Given an example showing that a union of subgroups is not necessarily a subgroup.

(ii) Let \( G \) be a group with a subgroup \( G_i \) for each natural \( i \). Prove that if \( G_i \subseteq G_{i+1} \) then the union \( H = \bigcup_{n=1}^{\infty} G_n \) is a subgroup.

(iii) Let \( R \) be a ring with an ideal \( I_i \) for each natural \( i \). Prove that if \( I_i \subseteq I_{i+1} \) then the union \( J = \bigcup_{n=1}^{\infty} I_n \) is an ideal.

(iv) Let us consider the following setup. For each natural number \( n \) we are given a group \( G_n \) and a group homomorphism \( \phi_n : G_n \rightarrow G_{n+1} \). Prove that

\[
G_\infty = \{(x_1, x_2, \ldots) \in \prod_{n=1}^{\infty} G_n | \forall i \phi_i(x_i) = x_{i+1}\}
\]

is a subgroup of \( \prod_{n=1}^{\infty} G_n \).

(v) Let \( p \) be a prime number. Let \( G_n = C_{p^n} \) be the cyclic group of order \( p^n \) with a generator \( x_n \). We define \( \phi_n : G_n \rightarrow G_{n+1} \) by \( \phi(x_n^a) = x_{n+1}^{pa} \). Using the above construction we obtain a group \( G \), called a quasicyclic group and usually denoted \( C_{p^\infty} \). Now let \( H = \{z \in \mathbb{C} | \exists n \in \mathbb{N} \; z^{p^n} = 1\} \). Show that \( H \) is a subgroup of the multiplicative group of the complex numbers. Prove that \( H \) is isomorphic to \( C_{p^\infty} \).

4.2.4 Vista

There are a number of things you can read or do your second year project about. When \( p = 3 \) the ring \( \mathbb{Z}[\omega] \) is called Eisenstein integers. You can read about Eisenstein prime. The ring \( \mathbb{Z}[\alpha] \), where \( \alpha \) is an algebraic integer is an exciting topic as well. For instance, you can find out when \( \mathbb{Z}[i\sqrt{n}] \) is a UFD. You can also read more about Bernoulli numbers.
4.3 Primes in Some Rings

4.3.1 Executive Summary
We discuss prime elements in $F[X]$ and $\mathbb{Z}[i]$.

4.3.2 Polynomial Primes
We will be talking about $F[X]$, the polynomial ring over a field $F$ throughout this section. We start with the following easy observation.

**Proposition 4.3.1 (Remainder Theorem)** Let $f = f(X) \in F[X]$. If $f(a) = 0$ for some $a \in F$ then $X - a$ divides $f$.

**Proof**: Divide $f(X)$ by $X - a$ with a remainder:

$$f(X) = g(X)(X - a) + r.$$ 

Notice that $r$ must have degree less than 1, so $r \in F$ (a constant polynomial). Substituting $X = a$, we arrive at $0 = f(a) = r$. $\square$

**Definition.** A field $F$ is **algebraically closed** if for any $f(X) \in F[X]$ of degree at least 1 there exists $a \in F$ such that $F(a) = 0$.

In all consequent theorems, we are after a complete lists of prime elements, with each prime listed once, up to the equivalence of being associate. For example, $X + a \sim bX + ab$ and we list just one of them. Notice that we don’t state this uniqueness in the statement of the theorem but as a matter of aesthetics our lists always satisfy this property.

**Proposition 4.3.2** If $F$ is an algebraically closed field then the primes in $F[X]$ are $X - a$, as $a$ runs over $F$.

**Proof**: The element $X - a$ is irreducible because any of its divisors must have degree 1 or 0. If it is 0, the divisor is a unit. If it is 1, the divisor is associate to $X - a$.

To show that they are pairwise non-associate, notice that $F[X]^* = F^*$. $X - a$ is associate only to $bX - ab$ for all $b \in F^*$.

Finally, if we have a prime $f \in F[X]$ then $f$ has degree at least 1. Since $F$ is algebraically closed, there is $a \in F$ such that $f(a) = 0$. By Proposition 4.3.1, $X - a$ divides $f$. Hence, $f$ is associate to $X - a$. $\square$

The following theorem will neither be proved, nor examined in this course. You can learn it taking Complex Analysis next year. There are numerous proofs using Algebra, Analysis or Topology. The latter two techniques are usually superior.
4.3. PRIMES IN SOME RINGS

Theorem 4.3.3 (The fundamental theorem of algebra) The field of complex number \( \mathbb{C} \) is algebraically closed

You should prove the next proposition yourself. It is an excellent exercise but we won’t use in this course.

Proposition 4.3.4 The primes in \( \mathbb{R}[X] \) are \( X - a \) and \( X^2 + bX + c \) for all possible \( a, b, c \in \mathbb{R} \) with \( b^2 - 4c < 0 \).

Theorem 4.3.5 Let \( F \) be a field. Then any finite subgroup of \( F^* \) is a cyclic group.

**Proof**: Suppose \( G \leq F^* \) is not cyclic of order \( N \). By the classification of finite abelian groups (from Algebra-1), \( G \) is isomorphic to \( C_{m_1} \times \ldots \times C_{m_n} \), a product of cyclic groups of orders \( n_1 | n_2 | \ldots | n_m \) and \( N = n_1 \cdot n_2 \cdots n_m \). Since \( (x_1, \ldots, x_m)^n = (x_1^n, \ldots, x_m^n) \in C_{m_1} \times \ldots \times C_{m_n} \), we deduce that \( g^n = 1 \) for any \( g \in G \) where \( n = n_m < N \). This provides \( F(X) = X^n - 1 \) with \( N \) roots, hence with \( N > n \) pairwise non-associate prime divisors \( X - a \) for each \( a \in G \). This contradicts the UFD condition for \( F[X] \).

The following corollary is immediate.

Corollary 4.3.6 \( \mathbb{Z}_p^* \) is a cyclic group of order \( p - 1 \).

4.3.3 Gaussian Primes

We will study primes in \( \mathbb{Z}[i] \). We will call them gaussian primes. Let us recall that \( \nu(x) = |x|^2 \). It is useful to remember that if \( x|y \) in \( \mathbb{Z}[i] \) then \( \nu(x)|\nu(y) \) in \( \mathbb{Z} \).

Proposition 4.3.7 If \( x \in \mathbb{Z}[i] \) and \( \nu(x) \) is prime then \( x \) is gaussian prime.

**Proof**: Using Proposition 4.2.1 and the fact that \( \mathbb{Z}[i] \) is a UFD, it suffices to check irreducibility of \( x \). Suppose \( y|x \). Hence, \( \nu(y)|\nu(x) = p \) in \( \mathbb{Z} \) that forces \( \nu(y) \) to be \( p \) or \( 1 \). If \( \nu(y) = p \) then \( y \) is associate to \( x \). If \( \nu(y) = 1 \) then \( y \) is a unit.

Proposition 4.3.8 Let \( p \in \mathbb{Z} \) be a prime. Then either \( p \) is gaussian prime or \( p = xx^* \) where \( x \) is a gaussian prime.

**Proof**: We obtain a proof by turning around the previous proof. If \( p \) is not gaussian prime, there exists a gaussian prime \( x \) such that \( p = xy \) and neither \( x \), nor \( y \) is a unit. Hence, \( \nu(x)\nu(y) = \nu(p) = p^2 \). This forces \( \nu(x) = \nu(y) = p \), which makes \( x \) and \( y \) prime by Proposition 4.3.7. Finally, \( x^* = x^{-1} \cdot \nu(x) = (y/p) \cdot p = y \).
Proposition 4.3.9 Let \( q \in \mathbb{Z}[i] \) be a gaussian prime. Then either \( \nu(q) \) is a prime or a square of a prime.

Proof: Let \( n = \nu(q) = qq^* \). Take decomposition of \( n \) into primes in \( \mathbb{Z} \), say \( n = p_1 \cdots p_t \). Then \( q|p_j \) in \( \mathbb{Z}[i] \) for some \( j \). This ensures the statement. \( \square \)

Theorem 4.3.10 The prime elements in \( \mathbb{Z}[i] \) are obtained from the prime elements \( \mathbb{Z} \). Each prime \( p \in \mathbb{Z} \), congruent 3 modulo 4 is a gaussian prime. The prime \( p = 2 \) gives rise to a gaussian prime \( q \) such that \( 2 \sim q^2 \). Each prime \( p \in \mathbb{Z} \) congruent 1 modulo 4 gives rise to two conjugate gaussian primes \( q \) and \( q^* \) such that \( p = qq^* \).

4.3.4 Exercises

(i) Prove Proposition 4.3.4.

4.3.5 Vista

The first proof of the fundamental theorem of algebra was given by Gauss in 1799. It was his Ph.D. thesis. You can learn more about the theorem and various proof at http://www.cut-the-knot.org/does-you-know/fundamental2.shtml.
4.4 Gaussian Primes

4.4.1 Executive Summary

We prove Theorem 4.3.10 and two corollaries.

4.4.2 Things as they stand

PROOF: Using Proposition 4.3.9, we can distinguish the two cases. Let $q$ be a gaussian prime such that $p = \nu(q)$ is a prime. Then $p$ gives rise to two primes $q, q^*$ such that $p = qq^* = \nu(q)$.

Let $q$ be a gaussian prime such that $p^2 = \nu(q)$ for a prime $p$. Hence, $q|p$ in $\mathbb{Z}[i]$. Pick $s \in \mathbb{Z}[i]$ such that $p = qs$. Then $|s| = |p|/|q| = 1$ and $s$ is a unit ($s^{-1} = s^*/|s|^2$). Hence $q$ is associate to $p$ (Remember that $\mathbb{Z}[i]^* = \{ \pm 1, \pm i \}$). Then $p$ gives rise to two primes $q, q^*$ such that $p = qq^* = \nu(q)$.

It remains to see that everything is controlled by the residue modulo 4. If $p = qq^*$ and $q = x + yi$ then $p = qq^* = x^2 + y^2$. Since $1^2 = 1, 2^2 = 0, 3^2 = 1$ in $\mathbb{Z}_4$, every prime in $\mathbb{Z}$, congruent to 3 modulo 4 cannot be represented as $qq^*$. Thus, it must be prime in $\mathbb{Z}[i]$ as well.

Let us explain $p = 2 = 1^2 + 1^2 = (1 - i)(1 + i)$. By Proposition 4.3.7, $1 \pm i$ are gaussian primes. Since $\mathbb{Z}[i]$ is UFD, these are the only two primes with norm 2. Notice that $1 - i = -i \cdot (1 + i) \sim 1 + i$.

It remains to prove that a prime $p$, congruent to 1 modulo 4 is not gaussian prime. Thanks to Proposition 4.1.7, it suffices to show that the ring $R = \mathbb{Z}[i]/(p)$ is not a domain. Notice that $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2 + 1)$. By the third isomorphism theorem, used twice $R \cong \mathbb{Z}[X]/(p, X^2 + 1) \cong \mathbb{Z}_p[X]/(X^2 + 1)$.

Thanks again to Proposition 4.1.7, it remains to show that the polynomial $f(X) = X^2 + 1 \in \mathbb{Z}_p[X]$ is reducible. For this we need to find $a \in \mathbb{Z}_p$ such that $X - a$ divides $f(X)$ or, by Proposition 4.3.1, $f(a) = a^2 + 1 = 0$. The latter condition means that $a^2 = -1 \neq 1$ (p is odd) or that the element $a \in \mathbb{Z}_p$ has order order 4. By Corollary 4.3.6, $\mathbb{Z}_p$ is a cyclic group of order $p - 1$. If $t$ is its generator then $t^{(p-1)/4}$ has order 4.

\[ \text{Corollary 4.4.1 (Fermat) Every prime congruent 1 modulo 4 is a sum of integer squares in a unique way.} \]

PROOF: Theorem 4.3.10 provides existence. If $p = x^2 + y^2 = a^2 + b^2$ then $p = (x + iy)(x - iy) = (a + ib)(a - ib)$ are two prime decompositions in $\mathbb{Z}[i]$. Everything follows from the UFD property of $\mathbb{Z}[i]$.

\[ \text{Corollary 4.4.2 There are infinitely many primes congruent 1 modulo 4.} \]
Proof: Suppose there are only finitely many of them in \( \mathbb{Z} \), say \( p_1, \ldots, p_n \). Let \( p_0 = 2 \), \( q_0 = 1 + i \), \( p_j = q_jq_j^* \) a prime decomposition of \( p_i \). Let us consider a prime decomposition of \( x = 2p_1 \cdot p_2 \cdots p_n + i \in \mathbb{Z}[i] \). No prime \( p \in \mathbb{Z} \), congruent 3 modulo 4 divides \( x \) because \( x/p \) has \( 1/p \) as the coefficient at \( i \), so it is not in \( \mathbb{Z}[i] \). Hence, one of the gaussian primes \( q_j \) (if it is \( q_j^* \), swap the notation between \( q_j \) and \( q_j^* \)) divides \( x \). Hence, \( p_j = \nu(q_j)\nu(x) = 4p_1^2 \cdot p_2^2 \cdots p_n^2 + 1 \), which is a contradiction since \( x \) has residue 1 modulo all \( p_j \). \( \square \)
4.5 Fractions

4.5.1 Executive Summary

This lecture is really boring. We have to introduce the field of fractions. To lighten it up we discuss fractions over euclidean domains and discuss Lagrange’s polynomial.

4.5.2 Fields of Fractions

Let $R$ be a domain. We consider the set $W = R \times (R \setminus \{0\}) = \{(x, y) \in R \times R | y \neq 0\}$. It admits an equivalence relation where $(a, b) \sim (c, d)$ whenever $ad = bc$. I leave it as an exercise to show that this is, indeed, an equivalence relation. An equivalence class of $(a, b)$ is called a fraction and denoted $a/b$. Let $Q = Q(R)$ be the set of all the equivalence classes on $W$.

**Proposition 4.5.1** If $R$ is a domain then $Q(R)$ is a field under the operations

$$
\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},
$$

and $\pi : R \rightarrow Q(R), \pi(r) = r/1$ is an injective ring homomorphism.

**Proof**: We have to show that these operations are well-defined. Then we have to establish all the axioms of a field. Finally we have to show that $\pi$ is an injective ring homomorphism.

To show that the operations are well defined, we need to notice that the denominators of the results are non-zero because $R$ is a domain. It remains to prove that the result is independent of the representative of the equivalence class. Given $a/b = x/y$ and $c/d = u/w$, we need to show that $ac/bd = xu/yw$ and $ad + bc/bd = xw + yu/yw$. The first equality requires $acyw = bdxu$ that easily follows from $ay = bx$ and $cw = du$. The second equality requires

$$
adyw + bcyw = bdwx + bdyu.
$$

Rewriting it, we get

$$
adyw - bdwx = bdyu - bcyw.
$$

This obviously holds because

$$
adyw - bdwx = dw(ay - bx) = 0 \text{ and } bdyu - bcyw = by(du - cw) = 0.
$$
The list of axioms of the field is long and we have to go and check them all. But we are in a good shape because we know that the operations are well-defined, so we can use our usual intuition about fractions. The associativity of addition is probably the hardest axiom to check

\[
\left( \frac{a}{b} + \frac{c}{d} \right) + \frac{e}{f} = \frac{ad + bc}{bd} + \frac{e}{f} = \frac{adf + (bcf + bde)}{bdf} = \frac{a}{b} + \frac{cf + de}{df} = \frac{a}{b} + \left( \frac{c + e}{d} \right).
\]

The commutativity of addition is easier:

\[
\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{c + a}{d + b}.
\]

The zero and the additive inverse are usual: \(0 = 0/1\) and \(-\left(\frac{a}{b}\right) = \left(-\frac{a}{b}\right)\) with all the checks routine. The associativity of multiplication is straightforward

\[
\left( \frac{a}{b} \cdot \frac{c}{d} \right) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a}{b} \cdot \left( \frac{c}{d} \cdot \frac{e}{f} \right)
\]

as well as the commutativity:

\[
\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{c}{d} \cdot \frac{a}{b}.
\]

The unity and the multiplicative inverse are usual: \(1 = 1/1\) and \(\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}\) with all the checks routine. It is worth noticing though why \(a \neq 0\). Indeed, \(a = 0\) if and only if \(a \cdot 1 = b \cdot 0\) if and only \(a/b = 0/1 = 0\). Finally, we have to check distributivity but it suffices to do it on one side only because the multiplication is commutative:

\[
\left( \frac{a}{b} + \frac{c}{d} \right) \cdot \frac{e}{f} = \frac{ad + bc}{bd} \cdot \frac{e}{f} = \frac{ade + bce}{bdf} = \frac{ad}{bd} + \frac{bce}{bdf} = \frac{a}{b} \cdot \frac{e}{f} + \frac{c}{d} \cdot \frac{e}{f}.
\]

The map is a ring homomorphism because \(\pi(1_R) = 1/1 = 1_Q\),

\[
\pi(xy) = \frac{xy}{1} = \frac{x}{1} \cdot \frac{y}{1} = \pi(x) \cdot \pi(y), \quad \pi(x + y) = \frac{x + y}{1} = \frac{x}{1} + \frac{y}{1} = \pi(x) + \pi(y).
\]

Finally, \(x\) is in the kernel if and only if \(x/1 = 0/1\) if and only if \(x \cdot 1 = 0 \cdot 1\) if and only if \(x = 0\).

**Definition.** \(Q = Q(R)\) is called the field of fractions of a domain \(R\).

**Examples.**

1. \(Q(\mathbb{Z}) = \mathbb{Q}\).
2. \(Q(F[X]) = F(X)\), the field of rational functions in one variable \(X\).
4.5. FRACTIONS

4.5.3 Fractions of ED-s

The following proposition is useful in Analysis. One uses it for integration and interpolation.

**Proposition 4.5.2** If \( R \) is ED then any element of \( Q(R) \) can be represented as
\[
r + \sum_j r_j/p_j^{n_j}
\]
where \( r, r_j, p_j \in R, \ n_j \in N, \ p_j \) are pairwise non-associate prime elements.

**Examples.**
1. \( 5/6 = 1/1 + 1/3 \).
2. \( 101/24 = 4 + 5/24 = 4 + 1/3 - 1/8 \).
3. Here is a typical computation of the integral of a rational function
\[
\int \frac{X+1}{X^3 + X} \, dX
\]
Hence, \( b = c = 1, \ a = -1 \) and
\[
\int \frac{X+1}{X^3 + X} \, dX = \int \left( \frac{-X+1}{X^2+1} + \frac{1}{X} \right) \, dX = -\frac{1}{2} \int \frac{dX^2}{X^2+1} + \int \frac{dX}{X^2+1} + \int \frac{dX}{X} =
\]
\[
= -\frac{1}{2} \ln(X^2 + 1) + \arctan(X) + \ln(X) + C
\]

4. Let \( f = (X - a_1) \cdots (X - a_n) \in \mathbb{C}[X] \) where \( a_j \neq a_k \) for \( j \neq k \) and \( g \in \mathbb{C}[X] \) of degree less than \( n \). Trying to guess the coefficients, we write
\[
g = \sum_{j=1}^{n} \frac{t_j}{X - a_j}
\]
and
\[
g(X) = \sum_{k=1}^{n} \frac{t_j f(X)}{X - a_j} = \sum_{k=1}^{n} \frac{t_j (X - a_1) \cdots (X - a_{j-1}) \cdots (X - a_{j+1}) \cdots (X - a_n)}{X - a_j}.
\]
Substituting \( X = a_j \) we get the answer,
\[
g(a_j) = t_j (a_j - a_1) \cdots (a_j - a_{j-1}) (a_j - a_{j+1}) \cdots (a_j - a_n) = t_j f'(a_j) \quad \text{or} \quad t_j = \frac{g(a_j)}{f'(a_j)}.
\]
Turning this calculation around gives Lagrange’s interpolation polynomial, that is, given \( a_j \) and \( s_j \) we use \( f = (X - a_1) \cdots (X - a_n) \) and \( t_j = s_j/f'(a_j) \) to define the interpolation polynomial

\[
g(X) = \sum_{k=1}^{n} t_j (X - a_1) \cdots (X - a_{j-1}) \cdot (X - a_{j+1}) \cdots (X - a_n)
\]

\[
= \sum_{k=1}^{n} s_j \frac{(X - a_1) \cdots (X - a_{j-1}) \cdot (X - a_{j+1}) \cdots (X - a_n)}{(a_j - a_1) \cdots (a_j - a_{j-1}) \cdot (a_j - a_{j+1}) \cdots (a_j - a_n)}.
\]

It will be the polynomial of the smallest possible degree such that \( g(a_j) = s_j \).

### 4.5.4 Exercises

(i) Prove that the relation \( \sim \) on the \( W \) is an equivalence relation.

(ii) Let \( R \) be a commutative ring, \( S \subset R \) a denominator set, that is, a subset closed under multiplication, containing 1, but not 0. Repeat the construction of the ring of fractions starting with the set \( W = R \times S \). The resulting ring \( Q_S(R) \) is called the partial ring of fractions.

(iii) Show that if \( R \) is a domain, \( p \in R \) is prime then \( S = R \setminus \{p\} \) is a denominator set.

(iv) Describe \( Q_S(\mathbb{Z}) \) where \( S = \mathbb{Z} \setminus \{p\} \) for some prime \( p \).

(v) Describe \( Q_S(\mathbb{Z}) \) where \( S = \{p^n \mid n \in \mathbb{Z}\} \) for some prime \( p \).

(vi) Prove Proposition 4.5.2
4.6 Gauss’ Lemma

4.6.1 Executive Summary

It is another boring lecture dealing with proofs of Gauss’ Lemma and some of its applications.

4.6.2 Gauss Lemma

We are concerned with the polynomial ring $R[X]$ over a UFD $R$.

Definition. A polynomial $f(X)$ is called monic if the coefficient of the highest degree term is 1. It is called primitive if the greatest common divisor of all the coefficients of $f(X)$ together is 1.

Theorem 4.6.1 Let $R$ be a UFD with a field of fractions $Q = Q(R)$. If $f = gh \in R[X]$ for some $g, h \in Q[X]$ then there exist $a, b \in Q$ such that $\hat{g} = ag \in R[X]$ and $\hat{h} = bh$ and $f = \hat{g}\hat{h}$.

Proof: Let $a_1$ be the least common multiple of all the denominators of the coefficients of $g(X)$, $a_2$ the greatest common divisor of all the coefficients of $a_1g(X)$, $a = a_1/a_2 \in Q(R)$. We define $\hat{g} = ag \in R[X]$. Similarly, $\tilde{h} = bh \in R[X]$. Notice that $\hat{g}$ and $\tilde{h}$ are primitive. Consequently,

$$f = u\tilde{gh} \text{ and } vf = u\hat{gh}$$

for some $u, v \in R$. Moreover, the greatest common divisor of $u$ and $v$ is 1.

As soon as we prove that $v$ is unit in $R$ we conclude by setting $\hat{q} = u\tilde{g}$ and $\tilde{h} = v^{-1}\tilde{h}$. Let us suppose that it is not a unit. Then there exists a prime element $p \in R$ that divides $v$. Let us consider a ring homomorphism

$$\pi : R[X] \to R/(p)[X], \pi(\sum_k a_kX^k) = \sum_k (a_k + (p))X^k.$$ 

Since $\pi(v) = 0$, we conclude that

$$0 = \pi(v)\pi(f) = \pi(u)\pi(\tilde{g})\pi(\tilde{h}).$$

As $R/(p)[X]$ is a domain, one of the multiplicands must be zero. This is a contradiction. First, $\pi(u) \neq 0$ since $p$ does not divide $u$ because $u$ and $v$ have no common prime divisors. Second, $\pi(\tilde{g}) \neq 0 \neq \pi(\tilde{h})$ because these polynomials are primitive.

We formulate two corollaries and prove them together.
**Corollary 4.6.2** If $R$ is UFD then there are two kinds of primes in $R[X]$: prime elements in $R$; primitive elements in $R[X]$ that are prime in $\mathbb{Q}[X]$.

**Corollary 4.6.3** If $R$ is UFD then $R[X]$ is UFD.

**Proof:** It immediately follows from Theorem 4.6.1 that all elements listed in Corollary 4.6.2 are irreducible. We proceed to prove both corollaries together.

Let us establish that any $f \in R[X]$ can be factorised into the elements listed in Corollary 4.6.2. We can factorise $f = f_1 \cdots f_n$ in $\mathbb{Q}[X]$. Getting rid of denominators and common divisors of numerators, we get $f = a\tilde{f}_1 \cdots \tilde{f}_n$ for some $a \in \mathbb{Q}, \tilde{f}_j = a_jf_j$ primitive in $R[X]$. Factorising $a$ in $R$, we arrive at the required factorisation of $f$. Thus, every irreducible element of $R[X]$ is associate to one of the elements listed in Corollary 4.6.2.

Now we proceed to prove that this factorisation is unique. Let us consider two factorisations

$$f = p_1 \cdots p_k f_1 \cdots f_n = q_1 \cdots q_l g_1 \cdots g_m \in R[X], \quad p_j, q_j \in R, \quad f_j, g_j \notin R$$

into irreducible elements. Without loss of generality $f_j, g_j$ are primitive. Using the UFD property of $\mathbb{Q}[X]$, $n = m$ and $f_j$ associate to $g_{\sigma(j)}$ for some permutation $\sigma$. Since $R[X]$ is a domain, we can cancel all associate elements, so

$$\alpha p_1 \cdots p_k = \beta q_1 \cdots q_l \in R$$

for some units $\alpha, \beta \in R^*$. Using the UFD property of $R$ establishes the uniqueness of the factorisation.

Finally, by Proposition 4.2.1, all the elements listed in Corollary 4.6.2 are prime.

The following two corollaries provide examples of UFD-s that are not PID-s.

**Corollary 4.6.4** If $F$ is a field then $F[X_1, \ldots, X_n]$ is UFD.

**Proof:** We proceed by induction on $n$. If $n = 1$ then $F[X]$ is ED, hence PID, hence UFD. If we have proved it for $n - 1$ we observe that

$$F[X_1, \ldots, X_n] \cong F[X_1, \ldots, X_{n-1}][X_n]$$

is also UFD by Corollary 4.6.3.

**Corollary 4.6.5** $\mathbb{Z}[X_1, \ldots, X_n]$ is UFD.
4.6.3 Exercises

(i) Prove Corollary 4.6.5

(ii) Prove that $F[X_1,\ldots,X_n]$ is not PID if $n > 1$.

(iii) Prove that $\mathbb{Z}[X_1,\ldots,X_n]$ is not PID.
CHAPTER 4. FACTORISATION

4.7 Polynomial Factorisation

4.7.1 Executive Summary

We discuss some examples of irreducible polynomials. We also discuss the quotient ring of the polynomial ring by an ideal generated by a single polynomial.

4.7.2 Eisenstein’s Criterion

As we know the irreducibility of polynomials is the same over $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$. However, determining whether a particular polynomial is irreducible is often subtle. The following is a powerful tool for producing some of examples.

**Proposition 4.7.1** (Eisenstein’s Criterion) Let $R$ be a UFD,

$$f(X) = \sum_{k=0}^{n} a_k X^k \in R[X].$$

We assume that there exists a prime $p \in R$ such that $p$ divides all $a_k$ for $k < n$ but does not divide $a_n$ and $p^2$ does not divide $a_0$. If the greatest common divisor of all the coefficients is 1 then $f(X)$ is irreducible in $R[X]$.

**Proof:** A factorisation with one polynomial of zero degree is impossible because the coefficients have no common divisors. Suppose

$$f(X) = \sum_{k=0}^{n} a_k X^k = (\sum_{k=0}^{m} b_k X^k)(\sum_{k=0}^{t} c_k X^k)$$

with both polynomials of non-zero degree. Then $a_k = \sum_{r+s=k} b_r c_s$ for all $k$. Since $p | a_0 = b_0 c_0$, it divides either $b_0$ or $c_0$ but not both since $p^2$ does not divide $a_0$. Without loss of generality, $p$ divides $b_0$ but not $c_0$.

This serves as a basis of induction. We prove that $p$ divides $b_j$ for each $0 \leq j \leq m < n$. Suppose we have done for all $j < l$. Then

$$b_l c_0 = a_l - (b_{l-1} c_1 + b_{l-2} c_2 + \ldots).$$

Since $p$ divides every term in the right hand side, it divides $b_l c_0$. Since it does not divide $c_0$, it divides $b_l$.

Hence, $p$ divides $a_n = b_n c_l$ which is a contradiction. \qed

Notice that if $f(X)$ admits $p$ as in Eisenstein’s criterion but its coefficients are not relatively prime then $f(X)$ is not irreducible in $R[X]$ but irreducible in $Q[X]$ where $Q = Q(R)$. 
4.7. POLYNOMIAL FACTORIZATION

Examples. 1. If $p$ is prime in $R$ then $X^n + p$ is prime in $R[X]$ for any $n$.

2. If $p$ is prime in $\mathbb{Z}$ then $f(X) = X^{p-1} + X^{p-2} + \ldots + 1$ is prime in $\mathbb{Z}[X]$. Consider the shift automorphism

$$sh_{-1} : \mathbb{Z}[X] \to \mathbb{Z}[X], \quad sh_{-1}(g) = g(X + 1)$$

Since this is a ring automorphism, $f$ is prime if and only if $sh_{-1}(f)$ is prime. Now notice that

$$sh_{-1}(f) = ((X + 1)^p - 1)/(X + 1 - 1) = X^p + \sum_{k=1}^{p-1} \frac{p^l}{k!(p-k)!} X^k.$$

is irreducible by Eisenstein’s criterion.

3. If $n$ is not prime in $\mathbb{Z}$ then $f(X) = X^{n-1} + X^{n-2} + \ldots + 1$ is not irreducible. It is a product of cyclotomic polynomials

$$f = \prod_{k \mid n} \Phi_k, \quad \Phi_k = \prod_{0 < d < k, \gcd(d,k) = 1} (X - e^{2\pi id/k}).$$

One can show $\Phi_k$ is irreducible but we won’t do it here. It is an interesting fact that an early version of a manual for the computer system Maple has stated that all coefficients of $\Phi_k$ are $\pm 1$ and 0. The smallest counterexample is $\Phi_{105}$.

4.7.3 Ring Structure

We are interested in the various structures on the polynomial quotients. The following proposition is useful. Notice the similarity with Proposition 4.1.7.

**Proposition 4.7.2** Let $R$ be a PID. If $p \in R$ is prime then $R/(p)$ is a field.

**Proof:** By Proposition 4.1.7, $R/(p)$ is a domain. We need to find an inverse for a nonzero element $x + (p) \in R/(p)$. Since $x + (p) \neq 0$, $p$ does not divide $x$. Since $p$ is prime, $\gcd(x,p) = 1$. Since $(x) + (p) = (\gcd(x,p))$, there exist $a, b \in R$ such that $1 = ax + bp$. Hence, $(x + (p))^{-1} = a + (p)$ in the quotient ring $R/(p)$. \hfill $\Box$

Proposition 4.7.2 tells us how to construct new fields when we know an interesting irreducible polynomial $f$. The field $F[X]/(f)$ has a structure we can easily understand. Let $n$ be the degree of $f$. We consider the vector space $F[X]_{<n}$ of polynomials of degree less than $n$. The natural map $\pi :$
$F[X]_{<n} \to F[X]/(f)$ defined by $\pi(g) = g + (f)$ is an isomorphism of vector spaces. This describes the additive structure on $F[X]/(f)$.

The multiplicative structure is slightly more involved. To multiply two polynomials $g, h \in F[X]_{<n}$ is the same as to compute $\pi^{-1}(\pi(g)\pi(h))$. The latter is obviously the residue of $gh$ modulo $f$. Finding the residue can be done using a rewriting rule $X^n \sim -\sum_{k=0}^{n-1} a_k X^k$.

For example, the polynomial $f(X) = X^8 + X^5 + X^4 + X^3 + 1$ is irreducible in $\mathbb{Z}_2$. The field $\mathbb{Z}_2[X]/(f)$ is the Galois field of 256 elements. To compute a product there we do

$$(X^5+1)(X^5+X^2) = X^{10} + X^7 + X^5 + X^2 \sim X^2(X^5 + X^4 + X^3 + 1) + X^7 + X^5 + X^2 = X^6$$

Hence,

$$(X^5 + 1 + (f)) \cdot (X^5 + X^2 + (f)) = X^6 + (f).$$

### 4.7.4 Exercises

(i) Use Eisenstein’s criterion to produce 6 new irreducible polynomials in $\mathbb{Z}[X]$.

(ii) Prove that the cyclotomic polynomial $\Phi_k$ has integer coefficients.

(iii) Pick up two of your favourite polynomials in $\mathbb{Z}[X]$ and find the greatest common divisor.

(iv) Pick up $f, g, h$, three of your favourite polynomials in $\mathbb{Z}[X]$ and compute $(g + (f)) \cdot (h + (f)) \in \mathbb{Z}/(f)$. 
4.8 Polynomial Quotients

Version: 1.03

4.8.1 Executive Summary

We discuss some examples of irreducible polynomials. We also discuss the quotients by them.

4.8.2 Ring Structure

Proposition 4.8.1 Let $F$ be a field, $f = f(X) \in F[X]$ an irreducible polynomial. The field $F[X]/(f)$ contains a root of the polynomial $f(X)$.

Proof: The root of $f(X)$ in $F[X]/(f)$ is $a = X + (f)$. Indeed, if $f(X) = \sum_{k=0}^{n} a_k X^k$, then

$$f(a) = \sum_{k=0}^{n} a_k (X^k + (f)) = (\sum_{k=0}^{n} a_k X^k) + (f) = f + (f) = 0.$$ 

The fields $F[X]/(f)$ are examples of algebraic extensions that you will be studying in the third year Galois Theory. The next corollary establishes an existence of a special extension, called a splitting field of $f(X)$.

Corollary 4.8.2 For any field $F$ and a polynomial $f \in F[X]$ there exists a field $K$ such that

(i) $K$ contains $F$ as subring;

(ii) $K$ is finite-dimensional as a vector space over $F$;

(iii) the polynomial $f(X)$ factorises into linear polynomials in $K[X]$.

Proof: We proceed by induction on $n$, the degree of $f$. If $n = 1$ there is nothing to prove: just take $K = F$.

Let us assume now that we have proved it for $n - 1$. There exists a field $L \geq F$ such that $L$ contains a root $\alpha$ of $f$ and $L$ is a finite-dimensional vectors space over $F$ by Proposition 4.8.1. Now using the induction assumption for $f(X)/(X - \alpha)$ and $L$, we arrive at the required field $K$. It remains to notice that $\dim_F K = \dim_F L \cdot \dim_L K < \infty$ as proved in the exercises.

The following application is noteworthy.
Corollary 4.8.3 For any field $F$, and a matrix $A \in M_n(F)$, there exists a field $K$ such that

(i) $K$ contains $F$ as subring;

(ii) $K$ is finite-dimensional as a vector space over $F$;

(iii) the matrix $A$ has an eigenvector in $K^n$ and a Jordan normal form in $M_n(K)$

Proof: Straightforward by using Corollary 4.8.2 to the characteristic polynomial of $A$ and the theorem from Algebra-I about existence of Jordan normal form.

We will need the Chinese Remainder Theorem for polynomials, which we are about to establish. In this form the Chinese Remainder Theorem holds in any PID but not UFD. You can establish this in the exercises.

Theorem 4.8.4 (Chinese Remainder Theorem for polynomials) Let $F$ be a field, $f \in F[X]$. If $f = q_1^{a_1} \cdots q_n^{a_n}$ is an irreducible factorisation in $F[X]$ then $\phi(h + (f)) = (h + (q_1^{a_1}), \ldots, h + (q_n^{a_n}))$ is a ring isomorphism between $F[X]/(f)$ and $F[X]/(q_1^{a_1}) \times \ldots \times F[X]/(q_n^{a_n})$.

Proof: The proof resembles the proof of Theorem 2.5.6. The ring homomorphism

$$
\psi : F[X] \rightarrow \prod_i F[X]/(q_i^{a_i}), \quad \psi(h) = (h + (q_1^{a_1}), \ldots, h + (q_n^{a_n})).
$$

has the kernel consists of all $h(X)$ divisible by all $q_i^{a_i}$, that is, the ideal $(f)$. By the 1-st isomorphism theorem $\phi$ is an isomorphism between $F[X]/(f)$ and the image of $\psi$. It remains to notice that the rings invloved are algebras over $F$. Both $\phi$ and $\psi$ are linear maps of vector spaces over $F$, hence algebra homomorphism. As $\phi$ is an injective linear map from $F[X]/(f)$ to $F[X]/(q_1^{a_1}) \times \ldots \times F[X]/(q_n^{a_n})$, both of which have the same dimension equal to the degree of $f$, $\phi$ is an isomorphism.

4.8.3 Exercises

(i) Let us consider fields $F \leq K \leq L$, containing each other as subrings. A field can be considered as a vector space over any subfield, that is a subring which is a field itself, using the field multiplication. Prove that $\dim_F L = \dim_F K \cdot \dim_K L$. 


(ii) Let $I_1, \ldots, I_n$ be a collection of ideals in a ring $R$. $\phi : R \to \prod_j R/I_j$, $\phi(x) = (x + I_1, \ldots, x + I_n)$.

(iii) Prove the Chinese Remainder Theorem for any PID. (Hint: follow the method of Proposition 1.3.6.)

(iv) Consider $X, Y \in \mathbb{C}[X, Y]$. Show that the Chinese Remainder Theorem fails for them. (Hint: show that $\mathbb{C}[X, Y]/(XY)$ has no non-identity idempotents (see the next lecture).)

4.9 Cyclic Vector Spaces

4.9.1 Executive Summary
We discuss cyclic vector spaces and give their characterisation.

4.9.2 Polynomial Quotient as a Vector Space
We are working with vector spaces over a field $F$. The vector space $V = F[X]/(f)$ has a canonical linear map $T$ given by multiplication by $X$, that is,
$$T(h + (f)) = Xh + (f).$$
Let us write the matrix of $T$ in the standard basis $X^k + (f)$, $k = n - 1, n - 2, \ldots, 1, 0$. where $f = X^n + \sum_{k=0}^{n-1} \alpha_k X^k$. Then
$$T(X^k + (f)) = X^{k+1} + (f)$$
is a basis element unless $k = n - 1$, in which case
$$T(X^{n-1} + (f)) = X^n + (f) = \sum_{k=0}^{n-1} -\alpha_k X^k + (f).$$
Consequently, the matrix of $T$ is
$$A = \begin{pmatrix}
-\alpha_{n-1} & 1 & 0 & \cdots & 0 & 0 \\
-\alpha_{n-2} & 0 & 1 & \cdots & 0 & 0 \\
& \vdots & & \ddots & \vdots & \\
-\alpha_1 & 0 & 0 & \cdots & 0 & 1 \\
-\alpha_0 & 0 & 0 & \cdots & 0 & 0
\end{pmatrix}.$$

4.9.3 Definition of a Cyclic Vector Space
The following is an abstract definition flowing naturally from the previous observation.

**Definition.** A pair $(V, T)$ where $V$ is a finite-dimensional vector space over the field $F$, $T \in E(V)$ is called a cyclic vector space if there exists a polynomial $f(X) \in F[X]$ and a linear bijection $\psi : F[X]/(f) \to V$ such that $\psi(hX + (f)) = T(\psi(h + (f)))$ for all $h \in F[X]$. 
In other words, we are saying that there exists a basis of $V$ in which $T$ is given by a Sylvester matrix

$$A = \begin{pmatrix}
-\alpha_{n-1} & 1 & 0 & \cdots & 0 & 0 \\
-\alpha_{n-2} & 0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
-\alpha_1 & 0 & 0 & \cdots & 0 & 1 \\
-\alpha_0 & 0 & 0 & \cdots & 0 & 0
\end{pmatrix}.$$}

Essentially, we want to characterise linear maps that can be given by such matrices. We start with the following technical lemma.

**Lemma 4.9.1** If $F$ is an infinite field then a vector space over $F$ is not a union of finitely many proper subspaces.

**Proof:** Suppose that this is not true and a vector space $V = \bigcup_{i=1}^n W_i$. We can assume that $W_1 \not\subset \bigcup_{i=2}^n W_i$ because otherwise $V = \bigcup_{i=2}^n W_i$ and we can work with this union instead.

Thanks to this assumption, there exists $a \in W_1$ such that $a \not\in W_i$, for all $i \neq 1$. Besides there exists $b \in W \setminus W_1$ (all subspaces are proper), so $b \not\in W_1$. Let us consider all vectors of the form $a + \alpha b$, where $\alpha \in F$. There are infinitely many of them, so there exists $W_j$ containing two vectors from this set, say be $x = a + \alpha b$, $y = a + \beta b \in W_j$, and $\alpha \neq \beta$.

If $j = 1$, then $(\alpha - \beta)^{-1}(x - y) = b \in W_1$. Contradiction.

If $j \neq 1$, then $(\alpha - \beta)^{-1}(\alpha y - \beta x) = a \in W_j$. Contradiction again. \hfill $\square$

Let us recall that a minimal polynomial of a linear map $T$ is such $\mu_T$ that $(\mu_T)$ is the kernel of the homomorphism

$$\pi_T : F[X] \to E(V), \quad \pi(h(X)) = h(T)$$

where $E(V)$ be the ring of all linear transformations $V \to V$. Notice that $E(V)$ is isomorphic to $M_n(F)$ upon a choice of basis in $V$. If $\chi_T(X) = \det(T - X)$ is the characteristic polynomial then by Cayley-Hamilton’s Theorem from Algebra-I, $\pi_T(\chi_T) = \chi_T(T) = 0$. Consequently, $\mu_T$ divides $\chi_T$.

Let us generalise it a bit. Having picked $v \in V$, we construct a linear map

$$\pi_v : F[X] \to V, \quad \pi_v(h(X)) = [\pi(T)](v).$$

Let us generalise it a bit. Having picked $v \in V$, we construct a linear map

$$\pi_v : F[X] \to V, \quad \pi_v(h(X)) = [\pi(T)](v).$$
Proposition 4.9.2 The kernel of \( \pi_v \) is a non-zero ideal.

**Proof:** Since \( \pi_v \) is a linear map, its kernel is a vector subspace. Since \( F[X] \) is infinite-dimensional but \( V \) is finite-dimensional, it is a non-zero subspace. It remains to check that this is an ideal. If \( h \in \ker(\pi_v) \) then \( \pi_v(fh) = f(T)(h(T)(v)) = f(T)(0) = 0 \), hence \( fh \in \ker(\pi_v) \). \( \square \)

We define the **minimal polynomial** of \( T \) at \( v \) as such \( \mu_{v,T} \) that \((\mu_{v,T})\) is the kernel of \( \pi_v \). Notice that \( \mu_{v,T} \) divides \( \mu_T \).

Theorem 4.9.3 Let the field \( F \) be infinite, \( V \) a finite-dimensional vector space over \( F \), \( T : V \to T \) a linear map. \((V,T)\) is a cyclic vector space if and only if \( \mu_T \sim \chi_T \).

**Proof:** The only if part is quite clear. Let \( V = F[X]/(f) \) be of dimension \( n \), which is also the degree of \( f \). Since \( \mu_T(T)(1 + (f)) = \mu_T(X) + (f) \). This means that \( f \) divides \( \mu_T \). Hence, the degree of \( \mu_T \) is \( n \). This forces \( \mu_T \sim \chi_T \).

The if part follows as soon as we can find \( v \in V \) such that \( \mu_{v,T} = \mu_T \). Indeed, we define \( f = \mu_T \) and the linear bijection is given by

\[
\psi : F[X]/(f) \to V, \quad \psi(h + (f)) = [h(T)](v). 
\]

It is a well-defined linear map since \( f(T)(v) = 0 \). It follows from \( \mu_{v,T} = \mu_T \) that this linear map is injective. Indeed, if \( \psi(h + (f)) = 0 \) if and only if \( h(T)(v) = 0 \) if and only if \( \mu_{v,T} = \mu_T = f \) divides \( h \) if and only if \( h + (f) = 0 \).

It is a linear bijection because it is a linear map between vector spaces of the same dimension with a zero kernel. Finally, \( \psi(hX + (f)) = [hX(T)](v) = T(h(T)(v)) = T(\psi(h + (f))) \).

To find such \( v \) we factorise the minimal polynomial \( \mu_T = q_1^{\alpha_1} \cdots q_m^{\alpha_m} \) where \( q_i \) are primes in \( F[X] \). Let \( f_i(X) = \mu_T(X)/q_i(X) \). The linear map \( f_i(T) \) is non-zero as \( f_i \) is a proper divisor of the minimal polynomial. Then by Lemma 4.9.1 there exists such \( v \in V \) that does not lie in the kernel of any \( f_i(T) \). As \( f_i(T)(v) \neq 0 \), \( \mu_{v,T} = \mu_T \). \( \square \)

Observe that, in general, the minimal polynomial is defined to be monic, but the highest degree coefficient of the characteristic polynomial is \((-1)^n\). As part of the proof, we may conclude that the characteristic polynomial of a Sylvester matrix \( A \) is \((-1)^n(X^n + \sum \alpha_nX^n)\).

Theorem 4.9.3 holds as stated over a finite field as well but it needs a subtler proof. I gave a complete proof while teaching it in 2007 but it took me 3 lectures so I decided to make a lazy proof instead. For large finite fields it is proved in exercises.
4.9. CYCLIC VECTOR SPACES

4.9.4 Linear Recursive Sequences

Sylvester matrices naturally appear in the study of linearly recursive sequences. Let us look at a sequence \( z_i \in F \) defined by a linear recursion

\[
z_0 = a_0, \ z_1 = a_1, \ldots, z_{n-1} = a_{n-1}; \quad z_m = \sum_{i=0}^{n-1} \beta_i z_{m-n+i}, \quad m \geq n \tag{4.1}
\]

where the scalars \( \beta_i, a_i \in F, i = 0, 1 \ldots n - 1 \) are given upfront. The most famous example of a linear recursive sequence is Fibonacci numbers

\[
z_0 = 0, \ z_1 = 1; \quad z_m = z_{m-1} + z_{m-2}, \quad m \geq 2.
\]

Let us introduce a sequence of vectors in \( v_m \in F^{m,1} \) and a matrix \( B \in M_n(F) \):

\[
v_m = \begin{pmatrix}
z_{m+n-1} \\
z_{m+n-2} \\
\vdots \\
z_{m+2} \\
z_{m+1} \\
z_m
\end{pmatrix}, \quad a = \begin{pmatrix}
a_{n-1} \\
a_{n-2} \\
\vdots \\
a_2 \\
a_1 \\
a_0
\end{pmatrix}, \quad B = \begin{pmatrix}
\beta_{n-1} & \beta_{n-2} & \cdots & \beta_2 & \beta_1 & \beta_0 \\
1 & 0 & \cdots & 0 & 0 & 0 \\
0 & 1 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & 0 & 0 \\
0 & 0 & \cdots & 0 & 1 & 0
\end{pmatrix}.
\]

If we can find an explicit formula for \( v_m \) then we can find an explicit formula for \( z_m \). On the other hand recursive relations (4.1) are equivalent to a single relation

\[
v_0 = a, \quad v_m = Bv_{m-1}
\]

that results in an explicit answer

\[
v_m = B^m a.
\]

Notice that the transposed matrix \( B^T \) is the matrix of the multiplication by \( X \) in \( F[X]/(f) \) where \( f = X^n - \sum_{k=0}^{n-1} \beta_k X^k \). So by reverting to rows instead of columns the resemblance becomes even clearer:

\[
v_0 = a, \quad v^T_m = v^T_{m-1} B^T.
\]

4.9.5 Exercises

(i) Let \( F \) be a field of \( q \) elements. Show that every vector space over \( F \) of dimension at least 2 is a union of \( q + 1 \) proper subspaces.

(ii) Let \( F \) be a field of \( q \) elements. Show that no vector space over \( F \) is a union of \( q \) proper subspaces.

(iii) Prove Theorem 4.9.3 if the dimension of \( V \) is smaller or equal than \( q \).
4.10 Idempotents and discrete Fourier transformation

4.10.1 Executive Summary

We study the cyclic vector spaces, understand a role of idempotents and discuss Fourier transformation.

4.10.2 Eigenvectors in cyclic vector spaces

We consider the cyclic vector space \( V = F[X]/(f) \) with its canonical linear map \( T \) given by \( T(h + (f)) = Xh + (f) \), where \( f \) has degree \( n \). We are interested in eigenvectors of \( T \). As we know already the eigenvalues of \( T \) are roots of \( f(X) \) and \( f \) is both minimal and characteristic polynomial of \( T \). The following proposition is immediate from linear algebra but we provide a proof to emphasise some of the ideas involved.

**Proposition 4.10.1** \( V \) admits a basis of eigenvectors of \( T \) if and only if \( f(X) \) admits \( n \) distinct roots in the field \( F \).

**Proof:** Let \( V \) admits a basis of eigenvector and \( \alpha_1, \ldots, \alpha_k \) are the eigenvalues without repetitions. Hence, \( \prod_i (X - \alpha_i) \) is the minimal polynomial of \( T \). By Theorem 4.9.3, \( f(X) \) is a minimal polynomial. This forces \( n = k \) and all \( \alpha_1, \ldots, \alpha_k \) being roots of \( f(X) \).

Now let \( f(X) = (X - \alpha_1) \ldots (X - \alpha_n) \) with all the roots distinct. By Chinese Remainder Theorem (Theorem 4.8.4), the natural homomorphism \( \phi : F[X]/(f) \to \prod_i F[X]/(X - \alpha_i) \) is an algebra isomorphism. Let \( e_i = (0, \ldots, 0, 1 + (X - \alpha_i), 0, \ldots, 0) \). Let us prove that \( \phi^{-1}(e_i) \) is an eigenvector with eigenvalue \( \alpha_i \): \( \phi(X\phi^{-1}(e_i)) = (0, \ldots, 0, X + (X - \alpha_i), 0, \ldots, 0) = (0, \ldots, 0, \alpha_i + (X - \alpha_i), 0, \ldots, 0) = \alpha_i e_i \). Consequently, \( X\phi^{-1}(e_i) = \alpha_i \phi^{-1}(e_i) \). \( \square \)

4.10.3 Idempotents

Let \( R \) be a ring. An idempotent is an element \( e \) of a ring \( R \) such that \( e^2 = e \).

Any ring has two trivial idempotents 1 and 0. All other idempotents are called non-trivial. We have just seen examples of such.

**Proposition 4.10.2** The elements \( E_i = \phi^{-1}(e_i) \) defined in Proposition 4.10.1 satisfy the following properties
4.10. IDEMPOTENTS AND DISCRETE FOURIER TRANSFORMATION

(i) \( \sum_{j=1}^{n} E_j = 1; \)

(ii) \( E_j \cdot E_j = E_j; \)

(iii) If \( i \neq j \) then \( E_i \cdot E_j = 0; \)

**Proof:** It is obvious for \( e_i \)-s, hence it is true for \( E_i \)-s because \( \phi \) is a ring isomorphism. \( \square \)

To get a better feel of non-trivial idempotents, let us state their characterisation in matrix rings.

**Proposition 4.10.3** Let \( F \) be a field, \( e^2 = e \in M_n(F) \) an idempotent. Then there exists an invertible matrix \( Q \) such that \( QeQ^{-1} = \begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix} \) where \( I \) is the identity matrix and \( 0 \) is the zero matrix.

In other words, idempotents in matrix rings are projection operators.

4.10.4 Fourier Transformation

The change of basis in \( F[X]/(f) \) from the standard basis \( X^k + (f) \) to the idempotent basis \( E_k \) is called Discrete Fourier Transformation. Let us understand why.

To define a usual Fourier transformation we need to fix a group homomorphism \( \kappa : (\mathbb{R}, +) \to \mathbb{C}^* \). Typically, \( \kappa(x) = e^{-2\pi i x} \). Given a function \( f(x) : \mathbb{R} \to \mathbb{C} \) we define its Fourier transform as a function \( \hat{f}(\omega) = \int_{-\infty}^{\infty} f(x)\kappa(\omega x)dx \). At this point, we have to get worried about existence of the integral but we are not as this is Algebra, not Analysis. As soon as one fixes all the convergence issues, the Fourier transform is an invertible linear transformation on some infinite dimensional vector space with the inverse Fourier transform given by

\[
 f(x) = \frac{1}{2\pi} \int_{-\infty}^{\infty} \hat{f}(\omega)\kappa^{-1}(\omega x)d\omega
\]

where \( \kappa^{-1}(x) = e^{2\pi i x} \). This formula admits an interpretation, fundamental to applied sciences. A signal function \( f(x) \) is represented as a combination of waves \( \kappa^{-1}(\omega x) \) for various frequencies \( \omega \in \mathbb{R} \). When function \( f(x) \) is periodic, say \( f(x+T) = f(x) \), the spectrum becomes discrete, that is, \( \hat{f}(\omega) = 0 \) unless \( \omega \in 2\pi i/T\mathbb{Z} \) and the integral degenerates into Fourier series, which may be
more familiar to you

\[ f(x) = \frac{1}{2\pi} \sum_{n=-\infty}^{\infty} \hat{f}(2\pi in/T) e^{2\pi inx/T} \]

This way or another, the functions \( e^{\omega x} \) are in the heart of what is going on and they are eigenvectors of the infinitesimal time-shift operator \( d/dx \), what a funny way to name a derivative!

To get to a discrete version of this, we have to sample the signal \( f(x) \) at \( n \) points \( k\epsilon, \ k \in \mathbb{Z}_n \). In other words, as we are trying to process the signal on a computer we record only \( n \) values \( f_k = f(k\epsilon) \). So we are dealing with a finite-dimensional vector spaces \( \mathbb{C}^n \), that admits a natural basis \( e_k, \ k \in \mathbb{Z}_n \) (signals with value 1 at \( k\epsilon \) and 0 elsewhere). A discrete time shift operator is the cyclic permutation \( \Theta(e_k) = e_{k+1} \). It makes \( \mathbb{C}^n \) into a cyclic vector space \( \mathbb{C}[X]/(F) \) where \( F = X^n - 1 \). An explicit linear isomorphism is \( e_k \mapsto X^k + (F) \) and \( \Theta \) corresponds to multiplication by \( X \). Eigenvectors of \( \Theta \) are discrete waves and the change of basis from monomials to eigenvectors is a discrete version of the Fourier transformation. Let us write eigenvectors explicitly.

**Proposition 4.10.4** Let \( w = e^{2\pi i/n} \). Then the eigenvalues of \( \Theta \) are \( w^k, \ k \in \mathbb{Z}_n \) and the eigenvector corresponding to \( w^k \) is \( h_k = \sum_i w^{-kt} e_t \)

**Proof:** As \( F \) is the characteristic polynomial of \( \Theta \), it suffices to check that \( F(w^k) = w^{nk} - 1 = 1 - 1 = 0 \). These are \( n \) distinct root of a degree \( n \) polynomial. It remains to check the eigenvector \( \Theta(h_k) = \sum_i w^{-kt} e_{t+1} = w^k \sum_i w^{-k(1+t)} e_{t+1} = w^k h^k \). \( \square \)

Draw them (or only their real part): they do look like waves.

### 4.10.5 Exercises

(i) Prove Proposition 4.10.3.

(ii) Take \( V = \mathbb{R}[X]/(X^6 - 1) \). Draw the elements of the standard basis.

The idempotents live in the bigger ring \( \mathbb{C}[X]/(X^6 - 1) \). Draw the real and the imaginary parts of idempotents.

### 4.10.6 Vista

Read more about Discrete Fourier Transformation on the net, for instance, on http://ccrma.stanford.edu/~jos/mdft/mdft.html
And they lived happily ever after . . .