Algebra-2: Groups and Rings

Dmitriy Rumynin*

January 6, 2011

How to use these notes

The lecture notes are split into 27 sections. Each section will be discussed in one lecture, making every lecture self-contained. This means that the material in a section may be reshuffled or even skipped for the lecture, although the numeration of propositions will be consistent. The remaining (up to 3) lectures will be spent on revisions and exercises including past exams.

These written notes is an official curriculum: anything in them except vistas can appear on the exam. Each section contains exercises that you should do. To encourage you doing them, I will use some of the exercises in the exam.

Vista sections are not assessed or examined in any way. Skip them if you are allergic to nuts or psychologically fragile! The vistas are food for further contemplation. A few of them are sky blue, but most are second year material that we don't have time to cover. You are encouraged to expand one of them into your second year essay.

The main recommended book is *Concrete Abstract Algebra* by Lauritzen. It is reasonably priced (£25 new, £11 used on Amazon), mostly relevant (except chapter 5) and quite thin. The downside of the book is brevity of exposition and some students prefer more substantial books. An excellent UK-style textbook is *Introduction to Algebra* by Cameron (from £17 on Amazon). Another worthy book is *Algebra* by Artin (£75 on Amazon for the new edition but you can get older editions for around £45). This one will have all details you need and much more than you can bear. Most of algebraists I asked have started with this book and absolutely love it. A similarly priced (and better according to some) alternative to Artin is

Abstract Algebra by Dummit and Foote (£55). My own first book was *Algebra* by van der Waerden (£30 for each volume on Amazon) but it appears that most of the mathematicians who hate Algebra in their later life have started with it.

An alternative strategy 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. If you think that some bits require better explanation, write me as well. All the contributions will be acknowledged. 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, Mohamed Swed and Jason Warnett for valuable suggestions how to improve these lecture notes.

Contents

1 Groups and subgroups

We define groups and establish their elementary properties. We learn how to define a group by a multiplication table and how to build new groups by using direct products and subgroups.

1.1 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.

We shall immediately prove two technical lemmas, which are often included as part of the definition of a group.

Lemma 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 1.2 *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, 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 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 gh), 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 $-g$.

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 1.3 *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, $(h^{-1}g^{-1}) \cdot (gh) = h^{-1}(g^{-1} \cdot g)h = h^{-1}h = e$. □

1.2 Examples – from Algebra-1

Actually, you already know a plenty of examples of groups from Algebra-1. A vector space V is an additive group under addition.

Finitely generated abelian groups are defined using generators and relations in Algebra-1. One particular group is $< x | nx = 0 >$, the cyclic group of order n. We denote the cyclic group C_n and always write in the default multiplicative notation, so that $C_n =< x | x^n = 1 >$. The infinite cyclic group is denoted by C_∞.

1.3 Direct product of groups

In Algebra-1, you have used the operation of direct product of abelian groups. In particular, the fundamental theorem of finitely generated abelian groups presented any such group as a product of cyclic ones.

Direct product of any groups is defined in the same way. It is a useful method of building 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}).

1.4 Multiplication Table

A convenient way to describe a group is by writing its *multiplication table.* For instance, the Klein four group $K_4 =< a, b|a^2, b^2 >$ is the set $\{1, a, b, c = ab\}$ with the multiplication table:

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

However, if the group is infinite or finite but large, the multiplication table approach is not quite practical. For instance, the famous *big monster group* has approximately 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.

1.5 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 1.4 *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 $1_h^{-1} \cdot 1_h \cdot 1_h = 1_h^{-1} \cdot 1_h$ 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 1.5 *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 1.6 *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 1.5. 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, $h_1h_2 = h_1(h_2^{-1})^{-1} \in H$. □

Corollary 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 1.6, $hg^{-1} \in H$ for all $H \in X$ and consequently to its intersection T. □

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.

1.7 Elementary Properties – the Cancellation Laws

Proposition 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. □

1.8 Exercises

(i) Prove that elements of the form $(g, 1_H)$ form a subgroup in $G \times H$.

(ii) Suppose G is a group, $x_1, \dots x_n \in G$. Prove that if $x_1x_2 \cdots x_n = 1$ then $x_2x_3 \cdots x_nx_1 = 1$.

(iii) Give an example showing that a union of subgroups is not necessarily a subgroup.

(iv) 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 $H = \cup_{n=1}^{\infty} G_n$ is a subgroup.

1.9 Vista: other products of groups

The direct products are not the only products of groups available. Its close relative is a semidirect product. You can twist direct and semidirect product by a cocycle to get twisted and crossed products. There are also bycrossed products and knit products. Amazingly enough, all of them are various group structures on the set $G \times H$ for a pair of groups.

If you are willing to consider more general sets, I have further products up my sleeve. If you can solve Rubik's cube, you have an experience with wreath product! It is used to build Rubik's cube group out of two symmetric and two abelian groups. Topologists use free products, HNN-extensions and amalgams. Any of these constructions could be a nice topic for a second year essay.

2 Rings and subrings

We define rings. We establish that each ring gives two groups: additive and multiplicative. We also discuss methods of obtaining new rings from old ones.

2.1 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 2.1 *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.* A natural question is whether 1 should be different from 0.

Lemma 2.2 *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 $a, b \in R$, $ab = ba$.

2.2 Examples – Numbers

Standard number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative rings under usual addition and multiplication. Quaternions $\mathbb{H}$, which you will see later in the term, 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).

2.3 Matrices over a ring

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 $n = 1$.

2.4 Polynomials over a ring

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 $X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n}$. 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 $R[X_1, \dots X_n]$ is commutative if and only if R is commutative.

2.5 Subrings

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 a different identity element (see section 2.9 for an example). As a logician would put it, *we consider rings with identity in the signature.*

Proposition 2.3 *Let S be an abelian subgroup of a ring R. Then S is a subring of R, if and only if*

(i) $a_1, a_2 \in S \Rightarrow a_1a_2 \in S$*; 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. □

Lemma 2.4 *The intersection of any set of subrings of R is itself a subring.*

2.6 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 can define a complex number $\alpha + \beta i$ as the matrix $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$.

Actually we have to be more careful because one may choose a different definition of $\mathbb{C}$, for instance as a set of formal symbols $\alpha + \beta i$ or pairs (α, β) with suitably defined operations. Then the subring and $\mathbb{C}$ are no longer equal but rather *isomorphic.* The precise statement should be that the ring of complex numbers $\mathbb{C}$ is isomorphic to a subring of $M_2(\mathbb{R})$. Isomorphisms is a topic of the next lecture.

2.7 Additive and multiplicative group of a ring

A ring R gives rise to *its additive group* R^+. As a set $R^+ = R$, and the addition is the same. All what happens is that the multiplication and the unit are completely forgotten. For instance, the additive group $\mathbb{Z}_n^+$ is the cyclic group of order n, usually denoted C_n in the multiplicative notation. Similarly, the additive group $\mathbb{Z}_n^+$ is the infinite cyclic group C_∞.

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 2.5 *All the units in a ring R form a group under multiplication.*

PROOF: Let us denote $R^\times$ the set of all units in R. The product on $R^\times$ is associative because the product on R is associative. The identity element of $R^\times$ 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 $R^\times$ is called *the group of units of the ring R* or *the multiplicative group of R*. For example, the multiplicative group $M_n(R)^\times$ of the matrix ring $M_n(R)$ is called *the general linear group* and denoted $GL_n(R)$.

2.8 Fields

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

Let us look at some familiar rings. For integers, $\mathbb{Z}^\times = \{\pm 1\} \neq \mathbb{Z} \setminus \{0\}$, so $\mathbb{Z}$ is not a field. For complex numbers, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$, so $\mathbb{C}$ is a field. For the zero ring, $\mathbb{Z}_1^\times = \{0\} \neq \mathbb{Z} \setminus \{0\} = \emptyset$, so $\mathbb{Z}_1$ is not a field. Thus, a field has at least two distinct elements $0 \neq 1$.

2.9 Direct product of rings

Direct products of rings are very similar to direct products of groups.

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 $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$, $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$ 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 $R \times S$.

2.10 Exercises

(i) Which of the rings $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_8$ are fields?

(ii) Prove that $\mathbb{Z}_n$ is a field if and only n is prime.

(iii) Find R^+ and $R^\times$ for the direct product ring $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(iv) What is the intersection of the subgroups $\mathbb{R}^\times$ and $\{z \mid |z| = 1\}$ of the multiplicative group of the complex numbers $\mathbb{C}^\times$?

(v) Consider a ring R without identity element. Define $\widehat{R} = R \times \mathbb{Z}$ 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.

(vi) An element $p \in R$ such that $p^2 = p$ is called *an idempotent*. Prove that a field contains exactly two distinct idempotents.

(vii) Describe all idempotents in $M_2(\mathbb{R})$.

(viii) 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.

(ix) Which of the following subsets form a subring of $C(\mathbb{R}, \mathbb{R})$: smooth functions $C^\infty(\mathbb{R}, \mathbb{R})$, compactly supported functions $C_c(\mathbb{R}, \mathbb{R})$, polynomial functions $f(X)$ such that $f'(0) = 0$?

(x) Let $V = U \oplus W$ be three vector spaces over $\mathbb{R}$ such both V and U are of countable dimension. We consider the ring $R = L_{\mathbb{R}}(V)$ of all linear maps $V \to V$ with the composition of maps as a multiplication. Choose a linear isomorphism $f : V \to U$ that becomes an element of R now. Prove that there infinitely many $x \in R$ such that $xf = 1_R$.

Conclude that f is not a unit and there is no $y \in R$ such that $fy = 1_R$.

2.11 Vista: pass rings

Besides the ring of commutative polynomials $R[X_1, \ldots X_n]$ there is also a ring of noncommutative polynomials $R < X_1, \ldots X_n >$. Inside this ring $X_1X_2 \neq X_2X_1$. This ring is of crucial importance in Physics and Engineering as its elements are *tensors*!

The general algebraic object is the tensor ring of a bimodule. Importance subclass are *pass algebras* or *quiver algebras*[1]. Its elements are formal linear combinations of passes in a directed graph (quiver). The product of two passes is its concatenation if one pass ends where the other one starts or zero if not. For instance, $R < X_1, \ldots X_n >$ is the pass algebra of the graph with 1 vertex and n loops at this vertex.

3 Isomorphisms and symmetric groups

Algebraic structures like rings and groups are rarely equal but often isomorphic. We discuss the notion of isomorphism[2] an apply it to symmetric

[1] see http://www.amsta.leeds.ac.uk/˜pmtwc/quivlecs.pdf for more info

[2] Later on in Section 9, we shall be considering the more general notion of *a homomorphism*

groups.

3.1 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* $\phi : G \to H$ between two groups G and H is a bijection from G to H such that $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ 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 $G \cong H$.

Isomorphic groups may be 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 in the same way.

Definition. An *isomorphism* $\phi : R \to T$ between two rings R and T is a bijection from R to T such that $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$ 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 2.6, 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. The groups $C_2 \times \mathbb{R}^+$ and $\mathbb{R}^\times$ are isomorphic. To write it explicitly, it is convenient to think of C_2 as its isomorphic group $\mathbb{Z}^\times = \{1, -1\}$. The map $\phi : C_2 \times \mathbb{R}^+ \to \mathbb{R}^\times$ defined by $\phi(\varepsilon, x) = \varepsilon e^x$ is an isomorphism.

The isomorphism $\phi : C_2 \times \mathbb{R}^+ \to \mathbb{R}^\times$ illustrates the fact that often it is important that isomorphic groups (or rings) are not equal. Restricted to a subgroup ϕ is an exponential function : $e^x : \mathbb{R} \mapsto \mathbb{R}_{>0}$. You won't get far in your analysis exam if you think of it as an equality!

3.2 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 $|g|$, 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 3.1 $|g| = 1 \Leftrightarrow g = 1$.

Lemma 3.2 *If* $|g| = n$ *then, for* $x \in \mathbb{Z}$, $g^x = 1 \Leftrightarrow n|x$.

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

3.3 Symmetric groups

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

The proof that $\mathrm{Sym}(X)$ 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 $\phi \in X$ 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 ϕ 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 ϕ_1 followed by ϕ_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 $\mathrm{Sym}(X)$ 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 unique: $(a_1, a_2, \ldots, a_r) = (a_2, a_3, \ldots, a_r, a_1)$, etc.)

Proposition 3.4 *Let X and Y be two sets with $|X| = |Y|$. Then the groups $\mathrm{Sym}(X)$ and $\mathrm{Sym}(Y)$ of all permutations of X and Y are isomorphic.*

PROOF: Let $\psi : X \to Y$ be a bijection. The map $\mathrm{Sym}(X) \to \mathrm{Sym}(Y)$ defined by $f \mapsto \psi f \psi^{-1}$ is an isomorphism. □

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

3.4 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 3.3.

(iii) If X is finite, what is the order of $\mathrm{Sym}(X)$ as a function of $|X|$?

(iv) Now let n be a positive integer, $H_n = \{z \in \mathbb{C} \mid z^n = 1\}$. Prove that H_n is a subgroup of $\mathbb{C}^\times$, isomorphic to C_n.

(v) A matrix $M \in GL_n(R)$ is *a permutation matrix* if in each row and column $n-1$ entries are 0_R and the remaining entry is 1_R. Prove that permutation matrices form a subgroup of $GL_n(R)$ isomorphic to S_n.

3.5 Vista: linear groups

A group G is called linear if it is isomorphic to a subgroup of $GL_n(F)$ for some field. A few things could prevent a group from being linear. For instance, $\mathrm{Sym}(X)$ is not linear if X is infinite. Observe that $\mathrm{Sym}(X)$ has at least countably many commuting (i.e. $xy = yx$) elements of order 2. Let us assume that $1 + 1 \neq 0 \in F$ which implies that any matrix of order 2 can be diagonalised. Now finitely many diagonalisable commuting matrices can be simultaneously diagonalised. But $GL_n(F)$ can accommodate at most $2^n - 1$ diagonal matrices of order 2.

There are other obstacles. In 1902 Burnside proved that a finitely generated linear periodic[3] must be finite. In 1964 Golod and Shafarevich con-

[3] periodic mean every element has finite order

structed an infinite finitely generated periodic group[4]. These groups cannot be linear by Burnside's theorem.

Given an infinite group, it can be a non-trivial challenge to establish whether it is linear. For instance, it was a long standing problem whether the braid group[5] is linear. It was solved affirmatively in 2000 by Warwick mathematician Daan Krammer.

4 Generators, cyclic groups, quaternionic group

We discuss generators of groups. We put on sound footing the discussion about cyclic groups. We use them in Diffie-Hellman Key Exchange. We finish with introducing the group Q_8.

4.1 Generators

Let G be a group, H its subgroup.

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

This means that every element of H can be written as an expression like $g_2^2 g_2^{-1} g_1 g_4 g_3^{-1} g_1 g_2^{-1}$ 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.

We write $< g_1, g_2, \ldots, g_r \ldots >$ for the subgroup generated by elements g_i. If $< g_1, g_2, \ldots, g_r \ldots >= G$, we say that they generate the group. A group G is called *finitely generated* if it can be generated by at least one finite set.

Examples. 1. $\mathbb{Z}^+ =< -1 >$, indeed each $n \in \mathbb{Z}$ can be written as $(-n)(-1)$. Also, $\mathbb{Z}^+ =< 2, 3 >$, indeed each $n \in \mathbb{Z}$ can be written as $n3 - n2$. However, $\mathbb{Z}^+ \neq< 2 >= 2\mathbb{Z}$, since only even numbers are additive powers of 2.

2. The following property of S_n was established in Linear Algebra in connection with the definition of the determinant. 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 conclude that any permutation on X can be written as a product of transpositions. Let us state this fact in the language of generators.

[4] see http://www.jstor.org/pss/2324085 which contains an easier than Golod-Shafarevich's example

[5] its wiki http://en.wikipedia.org/wiki/Braid_group is quite good

Lemma 4.1 *S_n is generated*[6] *by all transpositions.*

3. You have seen in Linear Algebra that any invertible matrix is a product of elementary matrices. This means that the group $\mathrm{GL}_n(K)$ for a field K is generated by elementary matrices.

4.2 Cyclic Groups

Definition. A group G is called *cyclic*, if it is generated by one element. A cyclic subgroup of G is a subgroup $< g >$ generated by any $g \in G$.

Essentially, a cyclic group G consists of the integral powers of a single element. In other words, there exists an element g in G with the property that, for all $h \in G$, there exists $x \in \mathbb{Z}$ with $g^x = h$. We call the element g *a cyclic generator* of G.

We have already seen cyclic groups $C_n = \mathbb{Z}_n^+$ and $C_\infty = \mathbb{Z}^+$ in Section 1.2. Are there any other cyclic groups? Let us look at generators first.

Lemma 4.2 *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 3.2 to conclude that the set $\{g^m \mid m \in \mathbb{Z}\}$ contains exactly k elements. The second statement follows. $\square$

Let us use the additive notation to describe generators in the cyclic groups we know. The group $\mathbb{Z}^+$ has infinitely many elements of infinite order but only two generators: 1 and -1. An element $x \in \mathbb{Z}_n^+$ is a generator if and only it has order n, i.e., the smallest positive integer m such that $n|mx$ is n. This means that x is a generator if and only if x and n are coprime. The number[7] of possible generators of $\mathbb{Z}_n^+$ is denoted $\varphi(n)$. The function $\varphi : \mathbb{N} \to \mathbb{N}$ is called *Euler's totient function.* We will compute it in Section 12.2.

The following fact is an easy corollary of Lemma 4.2, which we state for future reference. Its proof is left as an exercise.

[6] In fact there are much smaller generating sets for S_n, see the exercise below.

[7] it is equal to the number of coprime numbers to n between 0 and $n-1$ as we have just proved

Proposition 4.3 *The order $|g|$ of an element $g \in G$ is equal to the order $| < g > |$ of the cyclic subgroup $< g >$ generated by g.*

Now we are ready to establish an identification test for an infinite cyclic group.

Proposition 4.4 *Let G be a group of infinite order generated by an element g. Then $G \cong \mathbb{Z}^+$.*

PROOF: Observe that $G = \{g^x \mid x \in \mathbb{Z}\}$. We saw in Subsection 3.2 that the elements g^x of G are distinct for distinct $x \in \mathbb{Z}$, and so the map $\phi : \mathbb{Z}^+ \to G$ defined by $\phi(k) = g^k$ for all $k \in \mathbb{Z}^+$ is a bijection, and it is easily checked to be an isomorphism. □

Thus, any two infinite cyclic groups are isomorphic. This means that the notation C_∞ is unambiguous. The following identification test for C_n means that the notation C_n is unambiguous.

Proposition 4.5 *Let G be a group of order n generated by an element g. Then $G \cong \mathbb{Z}_n^+$.*

PROOF: Cyclicity of G means that $G = \{g^x \mid x \in \mathbb{Z}\}$. By Proposition 4.3, $|g| = n$. By Lemma 3.2, $g^x = g^y$ if and only if $1 = g^{x-y}$ if and only if $n|(x-y)$. Thus, $G = \{g^x \mid x \in \mathbb{Z}_n\}$ and the map $\phi : \mathbb{Z}_n^+ \to G$ defined by $\phi(k) = g^k$ for all $k \in \mathbb{Z}_n^+$ is a bijection. It is easily checked to be an isomorphism. □

4.3 Diffie-Hellman key exchange

Let us consider Alice and Bob who want to communicate secretly over insecure channel listened to by Eve. Alice and Bob want to exchange a secret key over the channel and to encode all future communications with their secret key. This is not a spy novel, this happens every time you use your credit card on Internet.

Amazingly enough, the elegant, yet most efficient solution uses cyclic subgroups. Over the channel, Alice and Bob agree on a group G and an element $g \in G$. 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.

Eavesdropping Eve has access to a, b, g, G. To compute K she needs exponents m or n and there is no (known) way of finding them quickly. In the standard implementationthe group G is $\mathbb{Z}_p^\times$ where p is a large prime (approximately 1000 binary bits or so), We will prove later (Corollary 21.4) that $\mathbb{Z}_p^\times \cong C_{p-1}$. Known sneaky ways of finding n and m will need prime factorisation of $p-1$, which is known to be computationally hard.

Suppose a computer can make one group multiplication in G every microsecond (10^{-6} seconds). How long will it take to compute g^n? If $n = 2m$ is even, one uses $g^n = g^m \cdot g^m$. If $n = 2m+1$ is odd, one uses $g^n = g^m \cdot g^m \cdot g$. Hence, one computes 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, one needs at most 2000 multiplications. Thus, Alice and Bob will make their computations in at most 2 milliseconds ($2 \cdot 10^{-3}$ seconds).

Let us consider how Eve can try to break the key in the most straightforward way. She needs to solve the equation $g^n = a$ in n that can be done compute all $|g|$ powers of g until she hits a. Repeating $g^x = gg^{x-1}$, every power requires one multiplication. As $|g| \approx 2^{1000}$, Eve needs at most $2^{1000} = (2^{10})^{100} \approx (10^3)^{100} = 10^{300}$ multiplications, that can be done in at most 10^{294} seconds. It is worse mentioning at this point that 10^8 seconds constitute approximately 3 years, so Eve would need to wait for 3×10^{286} years for the code to be broken.

4.4 Pauli's matrices and quaternionic group

The following matrices in $GL_2(\mathbb{C})$ are known as Pauli's matrices (we use i to denote the imaginary unit):

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

In Physics they are used to describe spin, but we will need their scalar multiples in the inverse order:

$$I = i\sigma_z = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ J = i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ K = i\sigma_x = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Definition. The quaternionic group Q_8 is $< I, J, K >$, the subgroup of $GL_2(\mathbb{C})$, generated by I, J and K.

Notice that $K = IJ$ and Q_8 is actually generated by I and J. The following proposition describes the group structure completely.

Proposition 4.6 *Q_8 has 8 elements*

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad -1 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad -I = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},$$
$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad -J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad -K = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

and its multiplication table is

	1	-1	I	$-I$	J	$-J$	K	$-K$
1	1	-1	I	$-I$	J	$-J$	K	$-K$
-1	1	-1	$-I$	I	$-J$	J	$-K$	K
I	I	$-I$	-1	1	K	$-K$	$-J$	J
$-I$	$-I$	I	1	-1	$-K$	K	J	$-J$
J	J	$-J$	$-K$	K	-1	1	I	$-I$
$-J$	$-J$	J	K	$-K$	1	-1	$-I$	I
K	K	$-K$	J	$-J$	$-I$	I	-1	1
$-K$	$-K$	K	$-J$	J	I	$-I$	1	-1

PROOF: Computing with matrices, we need to establish that $I^2 = J^2 = -1$ and $IJ = K$ and $JI = -K$. Using matrices, we observe that -1 is a scalar matrix so it commutes with any other matrix: $(-1)X = X(-1) = X$.

To locate all the elements we start with $1, I, J, K \in Q_8$, then $-1 = I^2 \in Q_8$, then $-I = (-1)I, -J = (-1)J, -K = (-1)K \in Q_8$. To show that it is indeed all of Q_8, we have to prove that these 8 matrices are closed under multiplication (closeness under inverses follows because they have finite order). We do this by filing the multiplication table. So far we know the part of the table:

	1	-1	I	$-I$	J	$-J$	K	$-K$
1	1	-1	I	$-I$	J	$-J$	K	$-K$
-1	1	-1	$-I$	I	$-J$	J	$-K$	K
I	I	$-I$	-1	1	K	$-K$		
$-I$	$-I$	I	1	-1	$-K$	K		
J	J	$-J$	$-K$	K	-1	1		
$-J$	$-J$	J	K	$-K$	1	-1		
K	K	$-K$						
$-K$	$-K$	K						

The rest follows from the following formal calculations: $IK = I(IJ) = I^2J = -J$, $KI = (-JI)I = -JI^2 = J$, $JK = J(-JI) = -J^2I = I$, $KJ = (IJ)J = IJ^2 = -I$, and $K^2 = (-JI)(IJ) = -JI^2J = J^2 = -1$. □

The group Q_8 is called quaternionic because of the obvious connection with quaternions. We postpone the discussion about it until we introduce quaternions in Section 27. But we need an identification test for the group.

Proposition 4.7 *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: 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 $a^4 = 1$ and $b^4 = (a^2)^2 = 1$, $a^{-1} = a^3$ and $b^{-1} = b^3$, so any element of G is a product of several a and b. Furthermore, we can use the equation $ba = a^{-1}b = a^3b$ to move all occurrences of a in the product to the left of the expression, so that $G = \{a^k b^l \mid k, l \in \mathbb{Z}\}$. Since $z = a^2 = b^2$ commute with both a and b (indeed, $zb = b^3 = bz$ and the same for a) and $z^2 = a^4 = 1$, we get a description $G = \{1, a, b, ab, z, za, zb, zab\}$ with all the elements distinct since $|G| = 8$.

An isomorphism $\phi : G \to Q_8$ is uniquely determined by $\phi(a) = I$ and $\phi(b) = J$, for instance, $\phi(z) = \phi(a^2) = \phi(a)^2 = -1$ and $\phi(ab) = \phi(a)\phi(b) = K$. One way to finish the proof now is to fill out the multiplication table of G and see that they are the same.

A more elegant way is to observe that we filled the multiplication table of Q_8 formally starting with relations: $I^2 = J^2 = -1$, $IJ = K$, $JI = -K$ and $(-1)X = X(-1) = X$ and, without explicitly mentioning $(-1)^2 = 1$. In G we know the same relations: $a^2 = b^2 = z$, $ba = a^{-1}b = a^3b = zab$, z commutes with everything, and $z^2 = 1$. Hence, we are bound to arrive at the same multiplication table. □

4.5 Exercises

(i) Prove that $< g_1, g_2, \ldots, g_r >$ is equal to the intersection of all subgroups containing every g_i.

(ii) Is $\mathbb{Q}^+$ a finitely generated group? Justify your answer.

(iii) Prove an improved version of Lemma 4.1: S_n is generated $n-1$ transpositions $(k, k+1)$ for $1 \leq k \leq n-1$.

(iv) Prove Proposition 4.3.

(v) Prove that Q_8 has 6 elements of order 4 and one element of order 2.

(vi) Prove that any subgroup of a cyclic group is cyclic itself.

4.6 Vista: free groups

In Algebra-1 you have seen the free abelian group $Ab < X >$ on a set X. It consists of all formal $\mathbb{Z}$-linear combinations of elements of X. Similarly to this idea, there is a free (nonabelian) group on a set X. Let us consider (finite) words in alphabet $\{x, x^{-1} \mid x \in X\}$. For instance, the empty word $\emptyset$, $xx^{-1}y^{-1}y$, $xxxx$ are all words but x^2 is not. A word w is *irreducible* if words xx^{-1} or $x^{-1}x$ are not subwords of w. Now the free group $Gr < X >$ consists of all irreducible words in the alphabet. The multiplication is concatenation followed by reduction, for instance the product of $xyzx^{-1}$ and $xz^{-1}y$ is not $xyzx^{-1}xz^{-1}y$ since it is not irreducible but its reduction xyy.

If $|X| = n$, one writes F_n for $Gr < X >$. We have seen a couple of them: F_0 is the trivial group C_1, F_1 is the infinite cyclic group C_∞. The next group F_2 is brand new and exciting. Its algebraic properties are crucial to establishing the Banach-Tarski paradox[8] where one cuts a 3-sphere into 4 disjoint pieces and makes two identical 3-spheres by combining 2 pairs of pieces.

5 Orthogonal and dihedral groups

We introduce orthogonal groups and pinpoint the structure of $O_2(\mathbb{R})$. We introduce the dihedral group as a subgroup of $O_2(\mathbb{R})$. We also realize it as a subgroup of the symmetric group.

5.1 Orthogonal matrices

We recall that the transpose of a matrix $A = (a_{i,j}) \in M_n(R)$ is the matrix $A^T = (b_{i,j})$ where $b_{i,j} = a_{j,i}$.

Definition. A matrix is $A = \in M_n(R)$ is *orthogonal* if it is invertible and $A^{-1} = A^T$.

We denote the set of orthogonal matrices by $O_n(R)$. This set is of interest only if the coefficient ring R is commutative.

Lemma 5.1 *If R is commutative then $O_n(R)$ is a subgroup of $GL_n(R)$.*

PROOF: Clearly, $O_n(R)$ is non-empty ($I \in O_n(R)$) and closed under inverses ($(A^{-1})^T = (A^T)^T = A = (A^{-1})^{-1}$). By the two-step test (Proposition 1.5), it suffices to establish that $AB \in O_n(R)$ whenever $A, B \in O_n(R)$. Thus, $(AB)^{-1} = B^{-1}A^{-1} = B^TA^T = (AB)^T$ finishes the proof. □

Notice that the very last equality $B^TA^T = (AB)^T$ requires commutativity of R. If R is not commutative, it breaks down even for 1×1-matrices.

The entries of the identity matrix $I = (\delta_{i,j})$ are called Dirak delta-symbol. In other words, $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ otherwise.

Lemma 5.2 *Let F be a field, $A \in M_n(F)$ with columns $c_1, c_2 \ldots c_n$. Then $A \in O_n(F)$ if and only if $c_i^T c_j = \delta_{i,j}$ for all i and j.*

PROOF: Notice that $c_i^T c_j$ is the (i,j)-entry of A^TA. Thus, $c_i^T c_j = \delta_{i,j}$ is equivalent to $A^TA = I$. It remains to notice that this implies (Linear Algebra) that A is invertible and $A^{-1} = A^{-T}$. □

It is worse pointing out that Lemma 5.2 holds for $A \in M_n(R)$ where R is a commutative ring. Unfortunately, we are not ready to prove it in

[8] Its wiki http://en.wikipedia.org/wiki/Banach-Tarski_paradox is quite good

this generality. We lack the standard properties of the determinants for matrices over commutative rings, i.e. multiplicative property $\det(AB) = \det(A)\det(B)$ and the minor formula $AM(A) = M(A)A = \det(A)I$ where $M(A)$ is the matrix of minors in A. Notice that the latter imply that $A \in GL_n(R)$ if and only if $\det(A) \in R^\times$.

5.2 Orthogonal group of size 2 over real numbers

We would like to pinpoint the structure of the group $O_2(\mathbb{R})$. Let us consider the following two matrices

$$R_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \text{ and } S_\alpha = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} .$$

Proposition 5.3 $O_2(\mathbb{R}) = \{S_\alpha, R_\alpha \mid \alpha \in \mathbb{R}\}$.

Proof: The matrices S_α and R_α belong to $O_2(R)$ by the direct matrix calculation (or by Lemma 5.2). In the opposite direction, if $X \in O_2(R)$, by Lemma 5.2, its columns c_1, c_2 form an orthonormal basis of $O_2(R)$. Any length 1 vector in $\mathbb{R}^2$ has a form $v_\alpha = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}$ for some $\alpha \in \mathbb{R}$. Let $c_1 = v_\alpha$ for some fixed α. Then either $c_2 = v_{\alpha+\pi/2}$ and $X = R_\alpha$ or $c_2 = v_{\alpha-\pi/2}$ and $X = S_\alpha$. □

It follows from the proof that S_α is never equal to R_β. Another way to observe this is by computing determinants: $\det(S_\alpha) = -1$ while $\det(R_\alpha) = 1$. Let us now describe these transformations geometrically. Observe, using standard trigonometric identities, that

$$R_\alpha v_\beta = \begin{pmatrix} \cos\alpha\cos\beta - \sin\alpha\sin\beta \\ -\sin\alpha\cos\beta + \cos\alpha\sin\beta \end{pmatrix} = \begin{pmatrix} \cos(\alpha+\beta) \\ \cos(\alpha+\beta) \end{pmatrix} = v_{\alpha+\beta} ,$$

hence R_α is a clockwise rotation by α. Similarly,

$$S_\alpha v_\beta = \begin{pmatrix} \cos\alpha\cos\beta + \sin\alpha\sin\beta \\ \sin\alpha\cos\beta - \cos\alpha\sin\beta \end{pmatrix} = v_{\alpha-\beta} .$$

In particular, $R_\alpha v_{\alpha/2} = v_{\alpha/2}$ and $R_\alpha v_{\alpha/2+\pi/2} = v_{\alpha/2-\pi/2} = -v_{\alpha/2+\pi/2}$. Hence, it is a reflection across the line spanned by $v_{\alpha/2}$. Using these calculations, one can now write the multiplication table for $O_2(\mathbb{R})$:

	R_β	S_β
R_α	$R_{\alpha+\beta}$	$S_{\alpha+\beta}$
S_α	$S_{\alpha-\beta}$	$R_{\alpha-\beta}$

Observe that rotations form a subgroup $SO_2(\mathbb{R})$ (called special orthogonal group) that looks suspiciously similar to $\mathbb{R}^+$, indeed, $R_\alpha R_\beta = R_{\alpha+\beta}$. There is a natural map $R : \mathbb{R}^+ \to SO_2(\mathbb{R})$ that sends α to R_α, which is not an isomorphism, because $R_\alpha = R_\beta$ whenever $\alpha - \beta = 2n\pi$ for some $n \in \mathbb{Z}$. The map R is an example of a homomorphism, a concept discussed in Section 9.

5.3 Dihedral group

Let $n \in \mathbb{N}$ with $n \geq 2$. The dihedral group D_{2n} is the group generated by S_0 and $R_{2\pi/n}$. Unfortunately, some books denote this group by D_n and others by D_{2n}, which can be confusing! We prefer D_{2n} because it tells us the number of its elements:

Lemma 5.4 *The order of D_{2n} is $2n$ and all its elements are $S_{2k\pi/n}$, $R_{2k\pi/n}$ for $k \in \mathbb{Z}$, $0 \leq k \leq n-1$.*

Proof: Using the multiplication table, we can easily find elements $R_{2k\pi/n} = R^k_{2\pi/n}$ and $S_{2k\pi/n} = R_{2k\pi/n} S_0 = R^k_{2\pi/n} S_0$ in $D_{2n} =< R_{2\pi/n}, S_0 >$.

Let $G = \{S_{2k\pi/n}, R_{2k\pi/n}\}$. It remains to observe that G a subgroup. G is obviously nonempty. G is closed under inverse because $R^{-1}_{2k\pi/n} = R_{2(n-k)\pi/n}$ and $S^{-1}_{2k\pi/n} = S_{2k\pi/n}$. Finally, G is closed under multiplication because $G = \{S_{2k\pi/n}, R_{2k\pi/n} \mid k \in \mathbb{Z}\}$ and $2k\pi\mathbb{Z}$ is a subgroup of $\mathbb{R}^+$ (look at the multiplication table). □

In fact, it is convenient at this point to denote rotations $a^k = R_{2k\pi/n}$ where $a \in \mathbb{Z}_n$. If we denote the reflection $b = S_0$, a typical reflection becomes $a^k b = S_{2k\pi/n}$ and multiplication table in D_{2n} could be written using addition in $\mathbb{Z}_n$:

	a^l	$a^l b$
a^k	a^{k+l}	$a^{k+l}b$
$a^k b$	$a^{k-l}b$	a^{k-l}

We need a recognition test for the dihedral group.

Proposition 5.5 *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 $b^2 = 1$, $a^{-1} = a^{n-1}$ and $b^{-1} = b$, so any element of G is a product of several a and b. 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 $0 \leq l < 2$. 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 $0 \leq k < n$. Now formally we recover the multiplication table of G that turns out to be the same as of D_{2n}:

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

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

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

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

Hence $\phi(a^k b^l) = a^k b^l$ is the required isomorphism (from G to D_{2n} or in the opposite direction - it does not matter). □

5.4 Dihedral group as a subgroup of symmetric group

Let $n \in \mathbb{N}$ with $n \geq 2$ and let P be a regular n-sided polygon in the plane whose vertices are $v_k = v_{2k\pi/n}$, $k \in \mathbb{Z}$. It is clear from the formulas $S_\alpha v_\beta = v_{\alpha-\beta}$ and $R_\alpha v_\beta = v_{\alpha+\beta}$ in the previous section that $XP = P$ for any $X \in D_{2n}$. In fact, the opposite is true: if $XP = P$ for some $X \in O_2(\mathbb{R})$ then $X \in D_{2n}$. Thus, D_{2n} is the group of symmetries of a regular n-gon.

It is instructive to stop thinking of P as a 2-dimensional figure. Let us think of P as a set of its vertices. This allows us to think of D_{2n} as a subgroup of S_n. More precise, for each $X \in D_{2n}$ there exists a unique $\sigma_X \in S_n$ such that $Xv_k = v_{\sigma_X(k)}$. For instance, $\sigma_a = (1, 2, 3, \ldots, n)$ rotates the vertices counterclockwise. Similarly, b is the reflection through the bisector of P that passes through the vertex $v_0 = v_n$. Then b interchanges the vertices v_1 and v_{n-1} that are adjacent to v_n, and similarly it interchanges v_2 and v_{n-2}, v_2 and v_{n-3}, etc., so we have $\sigma_b = (1, n-1)(2, n-2)(3, n-3)\ldots$. For example, when $n = 5$, $b = (1, 4)(2, 3)$ and when $n = 6$, $b = (1, 5)(2, 4)$. Notice the difference between the odd and even cases. When n is odd, b fixes no vertex other than v_0, but when n is even, b fixes one other vertex, namely $v_{n/2}$. We summarize this discussion in the following proposition.

Proposition 5.6 *The function $X \mapsto \sigma_X$ is an isomorphism from D_{2n} to a subgroup of S_n.*

5.5 Exercises

(i) Verify the multiplicative property $\det(AB) = \det(A)\det(B)$ and the minor formula $AM(A) = M(A)A = \det(A)I$ for 2×2-matrices over a commutative ring.

(ii) Let R be a commutative ring. Prove that $A \in GL_2(R)$ if and only if $\det(A) \in R^\times$.

(iii) Compute the order of the general linear groups $GL_2(\mathbb{Z}_2)$ and $GL_2(\mathbb{Z}_4)$.

(iv) Compute the order of the orthogonal groups $O_2(\mathbb{Z}_2)$ and $O_2(\mathbb{Z}_4)$.

(v) What is the subgroup of $O_2(\mathbb{R})$ generated S_α and S_0?

(vi) Prove that D_4 is isomorphic to K_4.

(vii) Prove that D_6 is isomorphic to S_3.

(vii) Prove that D_8 has 5 elements of order 2 and 2 elements of order 4. Conclude that D_8 is not isomorphic to Q_8.

(viii) 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,c> := Group < a,b,c | a^k, b^l, c^m, a*b*c >; G; Order(G);** for some particular $k \geq l \geq m \geq 2$. Determine experimentally by running the code which of these groups are finite.

5.6 Vista: defining relations and Burnside's problem

The equations $\{a^n = 1,\, b^2 = 1,\, ba = a^{-1}b\}$ are called *defining relations* for D_{2n}. One formally writes $D_{2n} = Gr < a, b \mid a^n = b^2 = 1, ba = a^{-1}b >$. This is a great way of describing groups. Roughly it means that D_{2n} is the largest group generated by two elements a and b that satisfy these equations. More precisely, it means that D_{2n} is a quotient group of the free group $F_2 = Gr < a, b \mid \emptyset >$ by a subgroup determined by these relations. Another example of a group determined by relations is von Dyck group $D_{k,l,m} = Gr < a, b, c \mid a^k = b^l = c^m = abc = 1 >$ with which you worked in the last exercise. Working out properties of a group from its presentation by generators and relations is far from straightforward: apart from MAGMA there packages GAP and SAGE that can help you with it. In Warwick Derek Holt is actively involved with them and has actually written a code for many of the functions.

Here is your another chance to get immediate recognition as a mathematical genius on par Galois, Gauss and Perelman. The group $B(n, m) = Gr < x_1, x_2, \ldots x_n \mid w^m = 1 >$ is know as Burnside group. By w here I mean all possible words in a and b. By Proposition 7.6, $B(n, 2)$ is abelian, of order 2^n. Using MAGMA, you can observe that $B(2, 3) \cong Gr < a, b \mid a^3 = b^3 = (ab)^3 = (ab^2)^3 = 1 >$ has order 27.

What is about $B(2, 5)$? Beware that your laptop is not of big help here.

If this group is finite, it has exactly 5^{34} (approximately 6×10^{23}) elements. But I would bet that it is infinite. If any betting agency accepts, please, let me know.

This problem is known as Burnside's problem[9]. In 1984, E. Zelmanov received Fields Medal for proving that $B(k,n)$ admits a unique maximal finite quotient $B_0(k,n)$. This was known as restricted Burnside's problem. In particular, the order of $B_0(2,5)$ is 5^{34}.

6 Equivalence relations and cosets

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

6.1 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.

6.2 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 have already seen the following examples of non-trivial equivalence relations. It is a good exercise to check the axioms but we will not do it here.

[9] Gupta, On groups in which every element has finite order. Amer. Math. Monthly 96 (1989), 297–308 is an accessible source. This is the first maths paper I have read.

Examples. 1. Let $X = \mathbb{Z}$, $n \in \mathbb{Z}$, $n \neq 0$. We say that $x \equiv_n y$ if n divides $x - y$. This equivalence relation, called *congruent modulo n*, appear in Foundations.

2. We say that $x \sim y \in \mathbb{R}^+$ if $R_x = R_y \in SO_2(\mathbb{R})$. Clearly, $x \sim y$ if and only if $x - y \in 2\pi\mathbb{Z}$.

3. 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 $P \in \mathrm{GL}_n(F)$, $Q \in \mathrm{GL}_m(F)$ 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.

4. 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 $P \in \mathrm{GL}_n(F)$ 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.

5. 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 $P \in \mathrm{GL}_n(F)$ 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 6.1 *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. □

Corollary 6.2 *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 6.1 $[a] = [c] = [b]$. □

Corollary 6.3 *The equivalence relation can be uniquely recovered from its partition into equivalence classes.*

PROOF: This follows immediately from Proposition 6.1 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. 6. Let $\equiv_n$ be the congruence modulo n we saw in examples today. The quotient set $\mathbb{Z}/\equiv_n$ is the ring $\mathbb{Z}_n$ of residues modulo n.

7. 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 relations is that the quotient set $X/\sim$ is the set of real numbers.

8. 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 $L^2([0, 1], R)$.

6.3 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 6.4 *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. □

Similarly to $x \sim_H y$, there is an equivalence relation $x\ _H\!\sim y$. We say that $x\ _H\!\sim y$ if and only if $xh = y$ for some $h \in H$ if and only if $x^{-1}y \in H$.

Definition. Let $g \in G$, $H \leq G$. The *right coset* of H containing g is the equivalence class ${}_H[g]$ of $\sim_H$. Similarly, the *left coset* is the equivalence class $[g]_H$ of $_H\!\sim$

The rightness of a right coset is the position of g with respect to H. Notice that ${}_H[g] = \{hg \mid h \in H\} = Hg$. In fact, Hg is the standard notation used in most of the books. We will use both notations since they are convenient in different situations.

Similarly, $[g]_H$ is the left coset $gH = \{gh \mid h \in H\}$. If H and the side are clear from the context, we just write $[g]$. In the case of additive groups, the standard notation becomes $H + g$ rather than Hg but we may still use $[g]$.

Example. If V is a vector space and W is a subspace, the cosets of W are affine subspaces $v + W$ parallel to W.

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 () 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 ${}_H[b] = Hb = \{(1,2), (1,3), (2,3)\}$. In fact any right coset of H is equal to either H itself or to ${}_H[b] = Hb = G \setminus H$. Furthermore, $[b]_H = {}_H[b]$, and indeed ${}_H[g] = [g]_H$, 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 ${}_H[a] = Ha = \{(1,2,3), (1,3)\}$ and ${}_H[a^2] = \{(1,3,2), (1,2)\}$, but $[a]_H = aH = \{(1,2,3), (1,2)\}$ and $[a^2]_H = a^2H = \{(1,3,2), (1,3)\}$, so the right and left cosets are not the same in this case.

The following two corollaries are immediate consequences of Corollary 6.2 and Proposition 6.4

Corollary 6.5 *Two right cosets ${}_H[g_1]$ and ${}_H[g_2]$ of H in G are either equal or disjoint.*

Corollary 6.6 *The right cosets of H in G partition G.*

6.4 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 $\mathbb{R}^\times$ in $\mathbb{C}^\times$.

(vi) Describe and draw the cosets of $H = \{z \in \mathbb{C} | |z| = 1\}$ in $\mathbb{C}^\times$.

(vii) 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.

(viii) 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.

(iX) 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.

6.5 Vista: groupoids

The notion of groupoid is a common generalisation of a group and an equivalence relation. If one develops the theory of groupoids first, then one can say that a group is a groupoid with one object and an equivalence relation is a groupoid where homs have at most one element. Find out more by exploring references on its wiki http://en.wikipedia.org/wiki/Groupoid

7 Lagrange's theorem and applications

We prove Lagrange's theorem. Using it, we classify groups of order 4 and groups of exponent 2. We also prove some number theoretic facts.

7.1 Lagrange's Theorem

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

Proposition 7.1 *If the subgroup H is finite, then all right cosets have exactly $|H|$ elements.*

PROOF: Since $h_1 g = h_2 g \Rightarrow h_1 = h_2$ by the cancellation law, it follows that the map $\phi : H = {}_H[1] \to {}_H[g]$ defined by $\phi(h) = hg$ is a bijection, and the result follows. □

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

Corollary 6.6 and Proposition 7.1 together imply:

Theorem 7.2 (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 7.3 *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 3.2 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. □

We finish with the following technical lemma for future use.

Lemma 7.4 *If $x, y \in G$ then $|y| = |xyx^{-1}|$ for all $g \in G$.*

PROOF: It follows immediately from Lemma 3.3 and the fact that $g \mapsto xgx^{-1}$ is an isomorphism $G \to G$. □

7.2 Groups of prime order

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 7.5 *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 7.3, so $|g| = p$. But then G must consist entirely of the powers g^k $(0 \leq k < p)$ of g, so $G \cong C_p$ by Proposition 4.4. □

7.3 Groups of exponent 2

The exponent of a group G is the least common multiple of orders of its elements. In other words, it is the smallest n such that $x^n = 1$ for all $x \in G$. We will not use this notion much but we need the following description of groups of exponent 2.

Proposition 7.6 *Let G be group where every element has order 2 or 1. Then $G \cong (C_2)^n$ and $|G| = 2^n$ for some $n \in \mathbb{N}$.*

PROOF: Since $x^2 = y^2 = (yx)^2 = 1$ for all $x, y \in G$, $xy = y^2xyx^2 = y(yx)(yx)x = yx$, so the group is abelian. Moreover, it has a natural structure of a vector space of $\mathbb{Z}_2$: $1 \cdot x = x$ and $0 \cdot x = 1_G$ for all $x \in G$. Since G is finite, it admits a finite basis (as a vector space over $\mathbb{Z}_2^n$) and the statement follows. □

Proposition 7.6 gives a method for classifying groups of order 4:

Proposition 7.7 *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 3.3: 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 7.3 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 and $G \cong C_2 \times C_2 = K_4$ by Proposition 7.6. □

7.4 Euler's theorem and Fermat's little theorem

If we use Lagrange's theorem to multiplicative groups of some finite rings, we arrive at some celebrated number theoretical facts. Let us first describe the group.

Lemma 7.8 *Let $x \in \mathbb{Z}_n$. Then $x \in \mathbb{Z}_n^{\times}$ 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 then x generates $\mathbb{Z}_n^{+}$ as discussed in Section 4.2. Thus, there exists $m \in \mathbb{Z}$ such that $mx = 1 \in \mathbb{Z}_n^{+}$ or $mx = an + 1$ in $\mathbb{Z}$. Let $k = (m)_n$, the residue of m modulo n. This means that $kx = bn + 1$ in $\mathbb{Z}$ and $kx = 1$ in $\mathbb{Z}_n^{\times}$. □

Once again we came across he function $\varphi : \mathbb{N} \to \mathbb{N}$ is called the Euler's totient function $\varphi : \mathbb{N} \to \mathbb{N}$, introduced in Section 4.2. This time $|\mathbb{Z}_n^{\times}| = \varphi(n)$. We will derive a formula for $\phi(n)$ in Section 12.2

Corollary 7.9 *$\mathbb{Z}_m$ 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 7.8. □

We are ready for Euler's theorem.

Theorem 7.10 (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, $b \in \mathbb{Z}_n^\times$. By Proposition 7.3, $|b|$ divides $\varphi(n)$. Hence $b^{\varphi(n)} = 1$ in $\mathbb{Z}_n^\times$. 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 7.11 *(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. □

7.5 Exercises

(i) The following groups have order 4: $\mathbb{Z}_5^\times$, $\mathbb{Z}_8^\times$, $\mathbb{Z}_{10}^\times$, $\mathbb{Z}_{12}^\times$. Determine whether each of them is K_4 or C_4.

(ii) Find an explicit isomorphism between $\mathbb{Z}_5^\times$ and $\mathbb{Z}_{10}^\times$.

(iii) Let $n \in \mathbb{N}$ be odd. Find an explicit isomorphism between $\mathbb{Z}_n^\times$ and $\mathbb{Z}_{2n}^\times$. Conclude that $\varphi(2n) = \varphi(n)$.

(iv) Prove that in a finite abelian group G, $\prod_{x \in G} x = \prod_{|x|=2} x$.

(v) Use exercise (iv) to prove Wilson's theorem: a prime p divides $(p-1)! + 1$.

(vi) Prove that any two countable groups of exponent 2 are isomorphic.

7.6 Vista: Sylow's Theorem

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. 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.

8 Normal subgroups

We introduce normal subgroups. Using these tools, we classify groups of order up to 8.

8.1 Normal Subgroups

We need the notion of normal subgroup to carry on.

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

The standard notation for "H is a normal subgroup of G" is $H \lhd G$ or $H \unlhd G$. ($H \lhd G$ 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 7.1, 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.

4. More generally, $SO_2(\mathbb{R})$ is a normal subgroup of $O_2(\mathbb{R})$. From its multiplication table, one coset consists of rotations R_α and another coset consists of reflections S_α.

In examples 3 and 4, the normal subgroup has index 2, for instance, $H = \{1, a, a^2\}$ and $|G|/|H| = 6/3 = 2$ in example 3.

Proposition 8.1 *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 6.6, 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 $H \lhd G$. □

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

Proposition 8.2 *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 $H \unlhd G$, 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 $g^{-1}hg = \overline{g}h\overline{g}^{-1}$ where $\overline{g} = g^{-1}$), so, putting $h' = g^{-1}hg$, we have $hg = gh' \in gH$, and so $Hg \subseteq gH$. Thus $gH = Hg$, and $H \unlhd G$. □

8.2 Groups of order 8

Proposition 8.3 *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: By Proposition 7.3, nonidenity elements of G may have order 2, 4 and 8. If all non-identity elements have order 2, then $G \cong C_2 \times C_2 \times C_2$ by Proposition 7.6.

Otherwise, there is an element $a \in G$ of order 4, for instance, if $|x| = 8$ then $a = x^2$ is of order 4. By Proposition 8.1, $N =< a >= \{1, a, a^2, a^3\}$ is a normal subgroup. Pick any $b \in G \backslash N$. Since $bab^{-1} \in N$ and $|bab^{-1}| = |a| = 4$ by Lemma 7.4, bab^{-1} must be either a or a^{-1}.

Also we cannot have $b^2 \in Nb$, as this would imply $b^2 = nb$ for some $n \in N$ and $b = n \in N$. Hence, $b^2 \in N$ since $G = N \cup Nb$.

Before we analyse eight possibilities, we observe that G is generated by a and b since $< a, b >$ properly contains N, hence, it has index strictly less then 2. In particular, this implies that $bab^{-1} = a$ makes G abelian while $bab^{-1} = a^3$ makes it nonabelian.

Let us assume $bab^{-1} = a^3$ and analyse four nonabelian possibilities:

(i) $b^2 = 1$, then $G \cong D_8$ by Proposition 5.5,

(ii) $b^2 = a$ is impossible as this means that $a^3 = bab^{-1} = bb^2b^{-1} = b^2 = a$,

(iii) $b^2 = a^2$, then $G \cong Q_8$ by Proposition 4.7

(iv) $b^2 = a^3$ is impossible as this means that $a = (a^3)^3 = b^6$ and $a^3 = bab^{-1} = bb^6b^{-1} = b^6 = a$.

Let us finally assume $bab^{-1} = a$ and analyse four abelian possibilities using the matrix technique from Algebra-1:

(i) $b^2 = 1$, then G is a quotient of $Ab < x, y \mid 4x, 2y >= C_4 \times C_2$, as they both have the same order, $G \cong C_4 \times C_2$,

(ii) $b^2 = a$, then G is a quotient of $Ab < x, y \mid 4x, x - 2y >$, reducing the matrix $\begin{pmatrix} 4 & 1 \\ 0 & -2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 4 & 1 \\ 8 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & 1 \\ 8 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 8 & 0 \\ 0 & 1 \end{pmatrix}$ gives $Ab < x, y \mid 8x, y >\cong C_8$, hence $G \cong C_8$ by the order equality, and

(iii) $b^2 = a^2$, then G is a quotient of $Ab < x, y \mid 4x, 2x - 2y >$, reducing the matrix $\begin{pmatrix} 4 & 2 \\ 0 & -2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 4 & 0 \\ 0 & -2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}$ gives $Ab < x, y \mid 4x, 2y >= C_4 \times C_2$, hence $G \cong C_4 \times C_2$ by the order equality,

(iv) $b^2 = a^3$, then G is a quotient of $Ab < x, y \mid 4x, 3x - 2y >$, reducing the matrix $\begin{pmatrix} 4 & 3 \\ 0 & -2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 3 \\ 2 & -2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 3 \\ 0 & -8 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix}$ gives $Ab < x, y \mid x, 8y >\cong C_8$, hence $G \cong C_8$ by the order equality.

□

It is worse pointing out why these five groups of order 8 are nonisomorphic. Three of them are abelian, two are nonabelian. The nonabelian D_8 and Q_8 have different number of elements of order 2: 5 and 1 correspondingly. The abelian are distinct by the fundamental theorem of abelian groups from Algebra-1. Alternatively, you can just count the number of elements of order in each of them.

8.3 Groups of order $2p$

Let p be a prime. We know two groups of order $2p$: the cyclic group C_{2p} and the dihedral group D_{2p}. It is worse pointing out what happens at small primes. If $p = 2$ then $D_4 \cong K_4$ is abelian, non-isomorphic to C_4. If $p = 3$ then D_6 is nonabelian, isomorphic to the symmetric group S_3.

Proposition 8.4 *Let G be group of order $2p$. Then $G \cong C_{2p}$ or $G \cong D_{2p}$.*

Proof: By Proposition 7.3 the orders of elements $g \in G$ can be 1,2,p or $2p$. If there is a g with $|g| = 2p$, then $G \cong C_{2p}$, so assume not. If all elements had order 1 or 2, then, by Proposition 7.6, $|G| = 2^m$, hence $p = 2$ and $G \cong K_4 \cong D_4$.

Hence we assume that there is an element a of order p. Then the subgroup $H =< a >= \{1, a, a^2 \dots a^{p-1}\}$ has index 2 in G, so normal by Proposition 8.1. Choose $b \in G \setminus H$. Under assumptions we made the order of b is 2 or p. If $|b| = p$ then the size of the union $< b > \cup < a >$ is $1+2(p-1) = 2p-1$ because $< b > \cap < a >= \{1\}$. Hence there exists $c \in G \setminus (< b > \cup < a >)$ and $< c >$ must be $\{1, c\}$ since there are no more elements left. In particular, $|c| = 2$. If $|b| = 2$ then we set $c = b$. In both cases we have found $c \in G \setminus H$ with $c^2 = 1$.

The subgroup $< a, c >$ properly contains H, hence has index less than 2, hence $G =< a, c >$. Since H is normal, $cac^{-1} = a^n$ for some n. Since $c^2 = 1$, we conclude that $a = ccac^{-1}c^{-1} = ca^nc^{-1} = (cac^{-1})^n = (a^n)^n) = a^{n^2}$. Thus p divides $n^2 - 1 = (n - 1)(n + 1)$. So p must divide either $n - 1$ or $n + 1$.

If p divides $n - 1$, $cac^{-1} = a^n = a$, so G is abelian. If p is odd, then $|ca| = 2p$, contradiction. Hence $p = 2$ and $G \cong Ab < x, y \mid 2x, 2y >\cong K_4$.

If p divides $n + 1$, then $cac^{-1} = a^n = a^{-1}$ and $ca = a^{-1}c$. By Proposition 5.5, $G \cong D_{2p}$. □

8.4 Exercises

(i) Show that $GL_2(\mathbb{Z}_2)$ is a group of order 6 and determine which of the groups in Proposition 8.4 it is isomorphic to.

(ii) Show that $O_2(\mathbb{Z}_3)$ is a group of order 8 and determine which of the groups in Proposition 8.3 it is isomorphic to.

(iii) For a commutative ring R we denote $T_n(R)$ the group of triangular $n \times n$-matrices with coefficients in R, i.e. $T_n(R) = \{(a_{ij}) \in GL_n(R) \mid a_{ij} = 0 \text{ whenever } i > j\}$. Show that $T_3(\mathbb{Z}_2)$ is a group of order 8 and determine which of the groups in Proposition 8.3 it is isomorphic to.

(iv) Let $ST_n(R)$ be the subgroup of $T_n(R)$ of matrices with determinant 1. Show that $T_2(\mathbb{Z}_3)$ is a group of order 6 and determine which of the groups in Proposition 8.4 it is isomorphic to.

(v) Show that $ST_2(\mathbb{Z}_4)$ is a group of order 8 and determine which of the groups in Proposition 8.3 it is isomorphic to.

8.5 Vista: classification of groups

We have advanced quite far in classification of groups. To facilitate the discussion, let $f(n)$ be the number of non-isomorphic groups of order n. We know so far that if p is prime then $f(p) = 1$, $f(2p) = 2$, $f(8) = 5$. Later one, we are going to classify groups of order p^2: they are all abelian, hence $f(p^2) = 2$.

The next interesting order is 12, $f(12) = 5$, only 2 are abelian. Out of 3 nonabelian, we know only D_{12} so far, but we are introducing the two remaining one later in this course, albeit we are not proving that the list is exhaustive. One needs Sylow's theorem to handle 15, $f(15) = 1$. The next number 16 is the first case where I would not know what to do: $f(16) = 14$ and I don't know most of them[10]. The next interesting case is 18: $f(18) = 5$. Four of the groups are straightforward: C_{18}, $C_3 \times C_6$, D_{18}, $C_3 \times D_6$ but the remaining one requires semidirect products. In general, if n have no large prime powers, $f(n)$ is easy to handle. $f(p^3) = 5$ with all 5 groups easy to construct: three are abelian, $UT_3(\mathbb{Z}_p)$ (subgroup of T_3 consisting of matrices with 1 on the main diagonal) and Prime powers[11] behave badly: $f(32) = 51$, $f(64) = 267$, ..., $f(1024) = 49487365422$.

While classifying all finite groups appears hopeless, it may be possible to understand generating functions $\sum_n f(n)z^n$ or $\sum_n f(p^n)z^n$.

9 Homomorphisms

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

[10] although see M. Wild, Groups of order 16 made easy, American Mathematical Monthly, 112 (2005), 20–31.

[11] Check out the book with exciting title *The groups of order 2^n (n equal to 6)* by Hall and Senior.

9.1 Definition and examples of homomorphisms

Definition. Let G, H be groups, R, S rings. A *group homomorphism* ϕ from G to H is a function $\phi : G \to H$ such that $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. A *ring homomorphism* ϕ from R to S is a function $\phi : R \to S$ such that $\phi(1_R) = 1_S$, $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$, 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 $R \to R \times S$, $r \mapsto (r, 0_S)$ is not a ring homomorphism. Such surprises don't happen with groups.

Lemma 9.1 *Let $\phi : G \to H$ 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. The reason for avoiding this terminology is clear from exercises to this discussion. On the other hand, we happily use the word *isomorphism* that describes a bijective homomorphism.

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 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 an element of a group G. Then, for $g, h \in G$, we have $kghk^{-1} = kgk^{-1}khk^{-1}$, so the map $\gamma_k : G \to G$ defined by $\gamma_k(g) = kgk^{-1}$ 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 $\gamma_k(k^{-1}hk)$. Alternatively, we can observe that $\gamma_k^{-1} = \gamma_{k^{-1}}$.

Notice that if G is abelian, then whatever k we choose, we always get $\phi_k(g) = g$ for all k, g so, these example is interesting for nonabelian groups only. We have used γ_k in Lemma 7.4 already.

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

7. Similarly for a ring R, pick $k \in R^\times$. The map $\gamma_k : R \to R$ defined by $\gamma_k(r) = krk^{-1}$ 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 $\phi(1) = 1$, $\phi(a) = b$, $\phi(b) = c$, $\phi(c) = a$. It is straightforward to check that ϕ is an isomorphism.

9. If K is a commutative ring, by the determinant of a product rule, $\det(AB) = \det(A)\det(B)$, it follows that the map $\phi : \mathrm{GL}(n, K) \to K^\times$ defined by $\phi(g) = \det(g)$ is a homomorphism. The determinant of a product rule is subtle to prove: you have seen a proof for a field in Linear Algebra-1. We will not attempt the proof for a general K in this module/

10. There is an injective group homomorphism $\Omega : S_n \to \mathrm{GL}(n, \mathbb{R})$. 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. Since $\sigma^m = 1$ 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 have a homomorphism $\mathrm{sign} : S_n \to \{-1, 1\} \cong C_2$ which distinguishes odd and even permutations. The former have $\mathrm{sign}(\sigma) = -1$ and the latter satisfy $\mathrm{sign}(\sigma) = 1$.

Please, note that there is a risk of circular argument here. It all depends on how you define determinant!! If you define it algebraically by $\det(a_{i,j}) = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) a_{\sigma(1),1} a_{\sigma(2),2} \ldots a_{\sigma(n),n}$ then you are in real trouble since you are using determinant to define sign of a permutation and vise versa. We will break this circle in Section 13.3.

9.2 Image

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

Proposition 9.2 *Let $\phi : G \to H$ be a group homomorphism. Then* $\mathrm{im}(\phi)$ *is a subgroup of H.*

Proposition 9.3 *Let $\phi : R \to S$ be a ring homomorphism. Then* $\mathrm{im}(\phi)$ *is a subring of S.*

9.3 Kernels

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

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

In the case of additive group or rings this becomes

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

Note that by Lemma 9.1 above, $\ker(\phi)$ always contains 1_G.

The following proposition explains the connection between normal subgroups and homomorphisms. Together with Proposition 10.3, it says that the set of normal subgroups of G is equal to the set of kernels of group homomorphisms with domain G.

Proposition 9.4 *Let $\phi : G \to H$ be a group homomorphism. Then* $\ker(\phi)$ *is a normal subgroup of G.*

PROOF: Checking that $K = \ker(\phi)$ is a subgroup of G is straightforward, using Proposition 1.5. If $g \in G$ then

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

so K is normal. □

Examples. 10. Here is an example of a homomorphism from an additive group to a multiplicative group. Let us define $\phi : \mathbb{C}^+ \to \mathbb{C}^\times$ by $\phi(g) = \exp(g)$. Then $\phi(g_1+g_2) = \phi(g_1)\phi(g_2)$, which says that ϕ is a homomorphism. In fact ϕ is a surjective but not injective. The kernel of ϕ is $2\pi i\mathbb{Z}$ since $\exp(x+iy) = \exp(x)(\cos(y) + i\sin(y))$ for $x, y \in \mathbb{R}$.

11. A close relative of example 10 is the homomorphism $R : \mathbb{R}^+ \to O_2(\mathbb{R})$, essentially defined in Section 5.2. Recall that $R(\alpha) = R_\alpha$, the rotation by α matrix. It is a homomorphism since $R_\alpha R_\beta = R_{\alpha+\beta}$. It is neither surjective, nor injective. Its image is $SO_2(\mathbb{R})$ and its kernel $2\pi\mathbb{Z}$.

12. Let $G = H = D_{12}$, the dihedral group of order 12. We saw in Subsection 5.3 that $G = \{a^k \mid 0 \le k < 6\} \cup \{a^k b \mid 0 \le k < 6\}$. We define $\phi : G \to H$ by $\phi(a^k) = a^{2k}$ and $\phi(a^k b) = a^{2k}b$ for $0 \le k < 6$. We claim that ϕ 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 5.3. We will make free use of the fact that $a^m = 1$ when $6|m$.

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

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

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

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

So ϕ 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 10.2. $\mathrm{im}(\phi)$ consists of the 6 elements $1, a^2, a^4, b, a^2b, a^4b$ of G.

In general, if $\phi : G \to H$ is a homomorphism and J is a subset of H, then we define the complete inverse image of J under ϕ to be the set $\phi^{-1}(J) = \{g \in G \mid \phi(g) \in J\}$. It is easy to check, using Proposition 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 9.5 *Let $\phi : G \to H$ be a homomorphism. Then ϕ 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 ϕ 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 9.1), so $g_1^{-1}g_2 \in \ker(\phi)$ and hence $g_1^{-1}g_2 = 1_G$ and $g_1 = g_2$. So ϕ is injective. □

9.4 Exercises

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

(ii) A homomorphism $\phi : A \to B$ is called *an epimorphism* if for any pair of homomorphisms $\alpha, \beta : B \to C$ the equality $\alpha\phi = \beta\phi$ implies that $\alpha = \beta$. Prove that any surjective homomorphism is an epimorphism.

(iii) Prove that the natural embedding $\mathbb{Z} \to \mathbb{Q}$ is an epimorphism of rings but not surjective.

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

(v) Let $\phi : R \to S$ 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.

(vi) Let us consider the following setup. For each natural number n we are given a group G_n and a group homomorphism $\phi_n : G_n \to G_{n+1}$ 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 $\prod_{n=1}^{\infty} G_n$.

(viii) 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 $\phi_n : G_n \to G_{n+1}$ 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^∞}. Prove that C_{p^∞} is isomorphic to H where $H = \{z \in \mathbb{C}^\times \mid \exists n\ z^{p^n} = 1\}$.

(ix) 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 $\mathbb{Z}_m$?

9.5 Vista: Jacobian conjecture

Let $R = \mathbb{C}[x_1, \ldots x_n]$ be the ring of complex polynomials. All $\mathbb{C}$-linear ring homomorphisms $\phi :\to R$ 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 $\phi(F(x_1, \dots x_n)) = F(f_1, \dots f_n)$.

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

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

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

It is natural to suggest that the opposite holds: $\det(J\phi) \in R^\times$ should imply ϕ being an isomorphism. This is one of the famous open problems in Algebraic Geometry called *Jacobian Conjecture*. It has had a good share of false proofs! Try to see where the difficulty[12] is.

10 Quotient groups

We introduce quotient groups and prove the isomorphism theorem. We use it to prove Cayley's theorem.

10.1 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 group depends on the following technical result.

Lemma 10.1 *If N is a normal subgroup of G and $[g] = Ng$, $[h] = Nh$ are cosets of N in G, then $[g][h] = [gh]$.*

PROOF: Let $n_1 g \in [g] = Ng$ and $n_2 h \in [h] = Nh$. By normality of N, $[g] = Ng = gN$, and so gn_2 is equal to some element $n_3 g \in Ng$. Hence $(n_1 g)(n_2 h) = n_1(gn_2)h = n_1(n_3 g)h = (n_1 n_3)gh \in Ngh = [gh]$, which proves $[g][h] \subseteq [gh]$. Finally, $ngh = (ng)(1h) \in (Ng)(Nh)$, so $[gh] = Ngh \subseteq (Ng)(Nh) = [g][h]$, and we have equality. □

We are taking advantage of N being normal and don't distinguish right and left cosets.

[12] read http://sbseminar.wordpress.com/2009/05/27/how-not-to-prove-the-jacobian-conjecture/ before you write one of these http://arxiv.org/abs/0912.1924v1

Proposition 10.2 *Let N be a normal subgroup of a group G. Then the set G/N of cosets $[g] = Ng$ of N in G forms a group under multiplication of sets.*

PROOF: We have just seen that $[g][h] = [gh]$, so we have closure, and associativity follows easily from associativity of G. Since $[1][g] = [1g] = [g]$ for all $g \in G$, $[1]$ is an identity element, and since $[g^{-1}][g] = [g^{-1}g] = [1]$, $[g^{-1}]$ is an inverse to $[g]$ for all cosets $[g]$. 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 10.3 *Let N be a normal subgroup of a group G. Then the map $\phi : G \to G/N$ defined by $\phi(g) = [g]$ is a surjective group homomorphism with kernel N.*

PROOF: It is straightforward to check that ϕ is a surjective group homomorphism, and $\phi(g) = 1_H \Leftrightarrow [g] = [1_G] = N \Leftrightarrow g \in N$, so $\ker(\phi) = N$. □

10.2 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 6.4 (after changing from multiplicative to additive notation!), we see that the cosets $[k] = 5\mathbb{Z}+k$ and $[j] = 5\mathbb{Z}+j$ of N in G are equal if and only if $k \equiv j \pmod 5$. So there are only 5 distinct cosets, namely $[0] = N = N+0$, $[1] = N+1$, $[2] = N+2$, $[3] = N+3$, $[4] = N+4$. It is now clear that G/N is isomorphic to the group $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ (see Subsection 4.2) via the isomorphism $[i] \mapsto i$ 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 3.2, 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 $[g] = Ng$. We can calculate its order as $|G|/|N| = m$. To see this directly, note that (using Lemma 6.4 again) $[g^k] = [g^j] \Leftrightarrow g^{k-j} \in N \Leftrightarrow m|(k-j)$, and so the distinct cosets are $[g^k]$ for $0 \leq k < m$. In particular, $[g]^m = [g^m] = N1$ is the identity element of G/N, and $|[g]| = m$.

3. For a more complicated example, we take Example 4 of Subsection 8.1, namely $G = D_{12}$ and $N = \{1, a^3\}$. Then $|G/N| = |G|/|N| = 6$. Since $a^3 \in N$, we have

$$[a]^3 = [a^3] = Na^3 = N = [1]$$

is the identity of G/N. We also have $[b]^2 = [1]$ and $[b][a] = [a^{-1}][b]$, because these relations are inherited from the corresponding relations of G. Thus G/N is a group of order 6 satisfying the three relations $[a]^3 = 1$, $[b]^2 = 1$, $[b][a] = [a]^{-1}[b]$, and, by Proposition 5.5 $G/N \cong D_6$.

It might be helpful in understanding this example to see the full multiplication table of G (cf. Subsection 5.3), with the elements arranged according to their cosets. Notice that all elements in each 2×2 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 2×2 blocks as single elements (i.e. cosets) in the quotient group.

		N		Na		Na^2		Nb		Nab		Na^2b	
		1	a^3	a	a^4	a^2	a^5	b	a^3b	ab	a^4b	a^2b	a^5b
N	1	1	a^3	a	a^4	a^2	a^5	b	a^3b	ab	a^4b	a^2b	a^5b
	a^3	a^3	1	a^4	a	a^5	a^2	a^3b	b	a^4b	ab	a^5b	a^2b
Na	a	a	a^4	a^2	a^5	a^3	1	ab	a^4b	a^2b	a^5b	a^3b	b
	a^4	a^4	a	a^5	a^2	1	a^3	a^4b	ab	a^5b	a^2b	b	a^3b
Na^2	a^2	a^2	a^5	a^3	1	a^4	a	a^2b	a^5b	a^3b	b	a^4b	ab
	a^5	a^5	a^2	1	a^3	a	a^4	a^5b	a^2b	b	a^3b	ab	a^4b
Nb	b	b	a^3b	a^5b	a^2b	a^4b	ab	1	a^3	a^5	a^2	a^4	a
	a^3b	a^3b	b	a^2b	a^5b	ab	a^4b	a^3	1	a^2	a^5	a	a^4
Nab	ab	ab	a^4b	b	a^3b	a^5b	a^2b	a	a^4	1	a^3	a^5	a^2
	a^4b	a^4b	ab	a^3b	b	a^2b	a^5b	a^4	a	a^3	1	a^2	a^5
Na^2b	a^2b	a^2b	a^5b	ab	a^4b	b	a^3b	a^2	a^5	a	a^4	1	a^3
	a^5b	a^5b	a^2b	a^4b	ab	a^3b	b	a^5	a^2	a^4	a	a^3	1

10.3 The isomorphism theorem

Sometimes it is also called *the first isomorphism theorem*, see the exercises for the second and the third ones.

Theorem 10.4 (Isomorphism theorem for groups) *Let $\phi : G \to H$ be a group homomorphism with the kernel K. Then $G/K \cong \mathrm{im}(\phi)$. More precisely, there is an isomorphism $\overline{\phi} : G/K \to \mathrm{im}(\phi)$ defined by $\overline{\phi}({}_K[g]) = \phi(g)$ for all $g \in G$.*

Proof: The trickiest point to understand in this proof is that we have to show that $\overline{\phi}({}_K[g]) = \phi(g)$ really does define a map from G/K to $\mathrm{im}(\phi)$.

The reason that this is not obvious is that we can have ${}_K[g] = {}_K[h]$ 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 ${}_K[g] = {}_K[h] \Rightarrow g = kh$ for some $k \in K = \ker(\phi)$, and then $\phi(g) = \phi(k)\phi(h) = \phi(h)$.

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

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

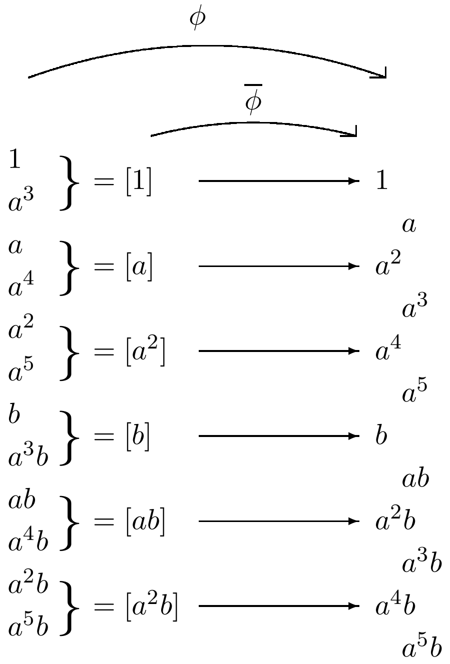
and so $\overline{\phi}$ is a monomorphism by Proposition 9.5. Thus $\overline{\phi} : G/K \to \mathrm{im}(\phi)$ is an isomorphism, which completes the proof. □

A particular value of the first isomorphism theorem is that it tells us the structure of any homomorphism $\phi : G \to H$. Indeed, ϕ is composition of three other homomorphism: the quotient homomorphism $G \to G/\ker(\phi)$, the isomorphism $\overline{\phi}$ and the embedding $\mathrm{im}(\phi) \to H$. For instance, $R : \mathbb{R}^+ \to O_2(\mathbb{R})$ from Example 12 in Section 9 becomes a composition of three maps

$$R : \mathbb{R}^+ \xrightarrow{p} \mathbb{R}^+/2\pi\mathbb{R} \xrightarrow{\psi} SO_2(\mathbb{R}) \xrightarrow{\iota} O_2(\mathbb{R})$$

the quotient map $p(\alpha) = [\alpha]$, the isomorphism $\psi([\alpha]) = R_\alpha$ and the embedding $\iota(T) = T$.

Let us illustrate this theorem using Example 12 from Section 9. 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 ϕ. The elements of $\mathrm{im}\phi$ are printed slightly to the left of those not in $\mathrm{im}(\phi)$ in the codomain column.



10.4 Cayley Theorem

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

Theorem 10.5 (Cayley's Theorem) *Every group G is isomorphic to a permutation group. (That is, to a subgroup of* $\mathrm{Sym}(X)$ *for some set X.) If G is finite, the set X can be chosen finite.*

PROOF: Let $X = G$. Define a homomorphism ϕ by $\phi(x) : y \mapsto xy$. By Theorem 10.4, $G/\ker(\phi)$ is isomorphic to a subgroup of $\mathrm{Sym}(X)$. Let us compute the kernel. If $x \in \ker(\phi)$ then $\phi(x) = Id_G$. Hence, $x = \phi(x)(1) = Id(1) = 1$. So the kernel is trivial and we are done. □

Why don't mathematicians study permutation groups instead of groups? Well, they 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 $\mathrm{Sym}(S_n) = S_{n!}$.

10.5 Exercises

Exercise (iii) below is often referred to as *the second isomorphism theorem*, while exercise (iv) is referred to as *the third isomorphism theorem.*

(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) Prove that if G is a simple group and H is a subgroup of index 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.

(iii) 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.

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

(v) Let $K \subseteq H \subseteq G$, where H and K are both normal subgroups of G. Then $(G/K)/(H/K) \cong G/H$.

10.6 Vista: simple groups

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 acceptably written proof. You can read more about this topic on wikipedia, search for "Classification_of_finite_simple_groups". Currently, mathematicians work on second and third generation proofs. Inna Capdeboscq in Warwick is actively involved in both projects.

If you are thinking of writing an essay, it may be a good idea to describe all simple groups of order up to 1000. Roger Carter used to teach MA4** level module with exactly this topic (and title). Besides 168 cyclic groups of prime order, there are only five nonisomorphic groups: the alternating groups A_5 of order 60 and A_6 of order 360 as well as linear groups $GL_3(\mathbb{F}_2)$ of order 168, $PGL_2(\mathbb{F}_8)$ of order 504 and $PSL_2(\mathbb{F}_{11})$ of order 660. While for the most numbers n, it is relatively easy to show that there is no simple group of order n, numbers 120, 540 and 720 will require special attention[13].

11 Ideals and quotient rings

We introduce ideals and discuss quotient rings. We state, prove and use the isomorphism theorem for rings.

11.1 Ideals

Definition. An additive subgroup I of a ring R is called *an ideal* in R if $xI \subseteq I \supseteq Ix$ for any $x \in R$. One writes $I \trianglelefteq R$.

To clarify the notation, $xI = \{xr \mid r \in I\}$. Thus, for any $r \in I$ both xr and rx must be in I for any $x \in R$. For a commutative ring R these

[13] cf. http://mathoverflow.net/questions/41958/no-simple-groups-of-order-720 and http://sci.tech-archive.net/Archive/sci.math/2006-12/msg07456.html

two properties are the same. For a non-commutative ring, one sometimes introduces *left ideals* satisfying $xI \subseteq I$ and *right ideals* satisfying $Ix \subseteq I$

Examples. 1. Any ring R has two boring ideals: zero ideal $\{0\}$ and the ring R itself.
2. For any $n \in \mathbb{Z}$, the numbers in $\mathbb{Z}$ divisible by n form an ideal $n\mathbb{Z}$. Notice that $1\mathbb{Z} = \mathbb{Z}$ and $0\mathbb{Z} = \{0\}$.
3. 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.*

Proposition 11.1 *Let $\phi : R \to S$ be a ring homomorphism. Then* $\ker(\phi)$ *is an ideal in R.*

PROOF: By Proposition 9.4, $K = \ker(\phi)$ is an additive subgroup of R. If $r \in K$, $x \in R$ then $\phi(xr) = \phi(x)\phi(r) = 0_S\phi(r) = 0_S$. Hence $xr \in K$. Similarly, $rx \in K$ and K is an ideal. □

Example. 4. For rings R, S let us consider the projection $R \times S \to S$ 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).

11.2 Generators of an ideal

Proposition 11.2 *Let R be a ring, $x_1, x_2 \ldots \in R$. The subset $(x_1, x_2 \ldots) = \{\sum_{k,j} r_k x_j s_k | r_k, s_k \in R\}$ is an ideal in R.*

PROOF: The subset is clearly non-empty. Let us clarify that the subset consists of the finite sums. The difference of two sums $\sum_{k,j} r_k x_j s_k$ is also such a sum. Finally, $a(\sum_{k,j} r_k x_j s_k) = \sum_{k,j}(ar_k)x_j s_k \in (x_1, x_2 \ldots)$ and $(\sum_{k,j} r_k x_j s_k)a = \sum_{k,j} r_k x_j (s_k a) \in (x_1, x_2 \ldots)$. □

If $I \trianglelefteq R$ and $I = (x_1, x_2 \ldots)$ we say $x_1, x_2 \ldots$ are generators of the ideal I. If $I = (x_1, x_2 \ldots, x_n)$, I is called *finitely generated.* If $I = (x)$, I is called *principal.* We have already seen the principal ideals $(n) = n\mathbb{Z}$ in $\mathbb{Z}$.

Examples. 5. If R is commutative $\sum_{k=1}^n r_k x s_k = x(\sum_{k=1}^n r_k s_k)$, so $(x) = xR = \{xr | r \in R\}$.
6. In a noncommutative ring the principal ideals are trickier. For instance, $(E_{1,1}) = M_n(R)$ where $E_{i,j}$ is a matrix with all zeroes except a single entry 1_R, 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 11.3 *Let R be a commutative ring, $x \in R$. Then $x \in R^\times$ if and only if $(x) = R$.*

PROOF: $x \in R^\times$ 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 $a \in R$. □

11.3 Quotient rings

The following proposition defines the quotient ring R/I for a ring R and its ideal I.

Proposition 11.4 *The additive cosets of an ideal $I \trianglelefteq R$ form a ring under addition $[a] + [b] = [a + b]$ and multiplication $[a] \cdot [b] = [ab]$.*

PROOF: Recall that the additive cosets are $[a] = a + I$. The form an abelian quotient group R^+/I with zero $[0] = 0 + I = I$. We need to check that the multiplication is well defined: Let $[a] = [x]$ and $[b] = [y]$. This means that $a - x \in I \ni b - y$. Then $ab = ab - ay + ay - xy + xy = a(b - y) + (a - x)y + xy$. Hence $ab - xy \in I$ and $[ab] = I + ab = I + xy = [xy]$.

The ring axioms (associativity, distributivity and unity) follow from the ring axioms of R. For instance, $[1] = 1 + I$ is the unit. □

Example. 7. 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 11.5 *Let I be an ideal of a ring R. Then the map $\phi : R \to R/I$ defined by $\phi(r) = [r]$ is a surjective ring homomorphism with kernel I.*

PROOF: By definition of R/I, ϕ is a ring homomorphism. Since $[x] = \phi(x)$, ϕ is surjective. Finally, $\phi(x) = 0 \Leftrightarrow [x] = I + x = I \Leftrightarrow x \in I$, so $\ker(\phi) = I$. □

11.4 The isomorphism theorem

The following theorem is also called *the first isomorphism theorem*, see the exercises for the second and the third ones.

Theorem 11.6 (Isomorphism theorem for rings) *Let $\phi : R \to S$ be a ring homomorphism with the kernel I. Then $R/I \cong \mathrm{im}(\phi)$. More precisely, there is an isomorphism $\overline{\phi} : R/I \to \mathrm{im}(\phi)$ defined by $\overline{\phi}([x]_I) = \phi(x)$ for all $x \in R$.*

Proof: By Theorem 11.6, $\overline{\phi}$ is a well-defined isomorphism of abelian groups under addition. It remains to see that this is a ring homomorphism, which follows from ϕ being a ring homomorphism. □

Let us look at two examples where the isomorphism theorem is useful.

Examples. 8. Let $R = \mathbb{Z}[i]/(1-2i)$. Let us denote $J = (1-2i)$, its additive cosets $x + J = [x]$. The map $\psi : \mathbb{Z} \to R$, $\psi(n) = [n]$ is obviously a ring homomorphism. It is surjective because $(1-2i)i = i - 2 \in J$ implies $[i] = [-2]$. Hence, $[a+bi] = [a] + b[i] = [a] + b[-1] = [a-2b] = \psi(a-2b)$ is in the image. If $n \in \ker(\psi)$ then $[n] = [0]$ and $n \in J$. This means that $n = (x+yi)(1-2i) = (x+2y) + (y-2x)i$ for some $x, y \in \mathbb{Z}$. Hence, $y = 2x$ and $n = 5x$ Hence, $\ker(\psi) = (5)$ and, by the isomorphism theorem, $R \cong \mathbb{Z}_5$.

9. We want to compute the ring $R_a = \mathbb{R}[x]/(x^2 - a)$ for some $a \in \mathbb{R}$. Every real (or complex) number α defines an evaluation homomorphism $f_\alpha : \mathbb{R}[x] \to \mathbb{R}$, $f_\alpha(F(x)) = F(\alpha)$ (or $f_\alpha : \mathbb{R}[x] \to \mathbb{C}$ correspondingly). The idea is to realize $J = (x^2 - a)$ as the kernel of a suitable evaluation homomorphism.

If $a < 0$, we choose the square root $b = \sqrt{a}$ and consider the homomorphism $f_b : \mathbb{R}[x] \to \mathbb{C}$. It is useful to observe that besides a ring homomorphism f_b is an $\mathbb{R}$-linear map, in particular, its image is an $\mathbb{R}$-vector subspace. Since $f_b(1) = 1(b) = 1$ and $f_b(x) = b$ is imaginary, f_b is surjective. Now $f_b(x^2 - a) = b^2 - a = 0$, hence $x^2 - a \in \ker f_b$. Since the kernel is ideal, $J \subseteq \ker f_b$. It remains to observe that both J and $\ker f_b$ have codimension 2. Hence, $J = \ker f_b$ and $R_a \cong \mathbb{C}$ by the isomorphism theorem, which also tells you explicit isomorphism $\psi = \overline{f_b} : R_a \to \mathbb{C}$, $\psi([F(x)]) = F(b)$.

If $a > 0$, we need two evaluations to cook a ring homomorphism $\psi = (f_{-\sqrt{a}}, f_{\sqrt{a}}) : \mathbb{R}[x] \to \mathbb{R} \times \mathbb{R}$. The same argument will lead to $J = \ker \psi$ and $R_a \cong \mathbb{R} \times \mathbb{R}$.

11.5 Exercises

Exercise (ii) often referred to as *the second isomorphism theorem for rings*, while exercise (iii) is referred to as *the third isomorphism theorem for rings.*

(i) Let I, J be ideals in R. Show that $I \cap J$, $I+J = \{x+y \mid x \in I, y \in J\}$ and $IJ = \{\sum_i x_i y_i \mid x_i \in I, y_i \in J\}$ are all ideals of R and that $IJ \subseteq I \cap J \subseteq I+J$.

(ii) 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 $S/(S \cap I) \cong (S+I)/I$.

(iii) 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 $(R/I)/(J/I) \cong R/J$.

(iv) Compute the ring $\mathbb{Z}[i]/(1+3i)$.

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

(vi) Let $R_a = \mathbb{R}[x]/(x^2 - a)$. Show that R_0, R_1 and R_{-1} are pairwise non-isomorphic rings.

(vii) $R_f = \mathbb{R}[x]/(f(x))$ where $f(x)$ is a quadratic polynomial. Show that R_f is isomorphic to either R_0, or R_1, or R_{-1}.

(viii) 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 $J = \cup_{n=1}^{\infty} I_n$ is an ideal.

11.6 Vista: simple rings

Similarly to a group, a ring R is called *simple* if it contains exactly two ideals 0 and R. In particular, the zero ring is not simple. A field is a simple ring. More generally, $M_n(F)$ is a simple ring if F is a field.

Similarly to groups, one can inquire about classification of simple rings. In groups it is unreasonable to expect to classify *all* simple groups and the right question is to classify *finite* simple groups. Finite simple rings can be classified: they are all $M_n(\mathbb{F}_q)$ where $\mathbb{F}_q$ is a finite field. In fact, there is a more general class of *artinian* rings where simple rings can be classified: they are all $M_n(D)$ where D is a division ring. This result is called Artin-Wedderburn Theorem and is covered in the 3rd year *Rings and Modules.*

12 Chinese remainder theorem

We prove Chinese Remainder Theorem (CRT). We use it to compute Euler's function and for public key encoding.

12.1 CRT, abstract form

Let R be a ring, I_k a set of ideals. For each ideal in the set we have the quotient homomorphism $\psi_k : R \to R/I_k$, $\psi_k(x) = x + I_k$. We can fuse them together into $\psi : R \to \prod_k R/I_k$, $\psi(x) = (x + I_k)$.

Lemma 12.1 *The map $\psi : R \to \prod_k R/I_k$ is a ring homomorphism with a kernel $\cap_k I_k$.*

PROOF: It follows easily from the properties of the quotient maps that ψ is a ring homomorphism. Now $x \in \ker\psi \Leftrightarrow \forall k \; x + I_k = 0 + I_k \Leftrightarrow \forall k \; x \in I_k \Leftrightarrow x \in \cap_k I_k$ □

The isomorphism theorem tells us that there is an induced injective homomorphism of rings $\overline{\psi} : R/\cup_k I_k \to \prod_k R/I_k$. In general, Chinese Remainder Theorem (CRT) is any statement that concludes that $\overline{\psi}$ is an isomorphism. We are going to prove for the ring $\mathbb{Z}$.

Theorem 12.2 (CRT, abstract form) *Let n_i, $i = 1, \ldots t$ be natural numbers such that each pair n_i, n_j, $i \neq j$ is coprime. Let $N = n_1 \cdot \ldots \cdot n_t$. Then $\cap_i(n_i) = (N)$ and the natural map $\overline{\psi} : \mathbb{Z}_N \to \prod_i \mathbb{Z}_{n_i}$ is a ring isomorphism.*

PROOF: The ideal $\cap_i(n_i)$ consists of all k divisible by all n_i. This is equivalent to divisibility by N since n_i are pairwise coprime.

By Lemma 12.1, $\overline{\psi}$ is an injective ring homomorphism. It is an isomorphism since both rings have N elements. □

Theorem 12.2 fails if there are infinitely many ideals (see exercises). On the other hand, it holds for any commutative ring if one replaces coprime generators by *comaximal* ideals. The proof gets much longer and you can follow the proof in the exercises. The noncommutative rings require a completely different statement that you can also find in the exercises.

12.2 Computation of Euler's function

Recall that the Euler totient function $\varphi : \mathbb{N} \to \mathbb{N}$ is defined as $\varphi(m) = |\mathbb{Z}_m{}^\times|$ (cf. Lemma 7.8).

Lemma 12.3 *If R and S are rings, the groups $(R \times S)^\times$ and $R^\times \times S^\times$ are isomorphic.*

PROOF: Both groups are subsets of the ring $R \times S$. Let us observe that these subsets are equal: $(r, s) \in (R \times S)^\times$ 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 $r \in R^\times$ & $s \in S^\times$ if and only if $(r, s) \in R^\times \times S^\times$. The required isomorphism is the identity map, which clearly preserves the multiplication. □

We are ready to compute it now.

Corollary 12.4 *If m and n are coprime then $\varphi(mn) = \varphi(m)\varphi(n)$*

PROOF: It follows immediately from Theorem 12.2 and Lemma 12.3. □

Corollary 12.5 *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 12.4, $\varphi(m) = \prod_{i=1}^{k} \varphi(p_i^{a_i})$. By Lemma 12.3, $m \in \mathbb{Z}_{p_i^{a_i}}$ 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 remainders 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 $\varphi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i-1}$. □

12.3 RSA

Suppose that you run a website so popular with customers, that every minute thousands of customers are queueing up to pay you with their credit cards. 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. More serious industrial application of asymmetric keys is the PGP system, which allows you to exchange messages securely with any number of people on the internet by giving away your public key.

The source of the key is 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 more computationally intensive but doable: d could have up to 1,000,000 binary bits, so x^d may require up to 2,000,000 multiplications.

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, which gives $\varphi(n)$, or compute d directly in the group $\mathbb{Z}_n^\times$ by some other means. With such a large n any known method is going to take thousands of years. Mathematicians know at least one way to do it faster by using *quantum computers*. It is engineers' turn to figure out how to build them.

12.4 CRT, elementary form

We recall that one writes $x \equiv_n y$ if n divides $x - y$. The Chinese Remainder Theorem can be formulated on the level of systems of comparisons.

Theorem 12.6 (CRT, elementary form) *Let $n_i, k_i \in \mathbb{Z}$, $i = 1, \ldots t$ such that each pair n_i, n_j, $i \neq j$ is coprime. The system of comparisons $x \equiv_{n_i} k_i$ admits a solution in $\mathbb{Z}$. Any two solutions are different by a multiple of $N = n_1 n_2 \cdots n_t$.*

Proof: Existence of solution is surjectivity of the natural map $\psi : \mathbb{Z} \to \prod_i \mathbb{Z}/(n_i)$, $\psi(x) = (x + (n_1), \ldots, x + (n_t))$, established in Theorem 12.2 Let $x \in \mathbb{Z}$ be a solution. Now $y \in \mathbb{Z}$ is a solution if and only if $x - y \in \ker \psi$. It remains to notice that $\ker psi = (N)$ by Lemma 12.1

$$\psi : \mathbb{Z} \to \prod_i \mathbb{Z}/(n_i), \quad \psi(x) = (x + (n_1), \ldots, x + (n_t)).$$

□

Our proof of CRT is not constructive. We do not know from the proof how to solve the system of comparisons. On the other hand, one can easily derive a constructive proof from the solution method we are about to describe. The key is the number $N_i = N/n_i = \prod_{k \neq i} n_k$. It is divisible by any n_j, $j \neq i$ and coprime to n_i. So, it is a generator of C_{n_i} inside $\mathbb{Z}_N^+ \cong \prod_j C_{n_j}$.

Let us look at a concrete example. Let us solve $x \equiv_7 6$, $x \equiv_{11} 5$, $x \equiv_{13} 4$. In this case, $N = 7 \cdot 11 \cdot 13 = 1001$ and the generators are $N_1 = 143 \equiv_7 3$, $N_2 = 91 \equiv_{11} 3$, $N_3 = 77 \equiv_{13} 12 \equiv_{13} -1$. In $\mathbb{Z}_7$ we have $6 = 2 \cdot 3$, in $\mathbb{Z}_{11}$ we have $5 = 9 \cdot 3$ and in $\mathbb{Z}_{13}$ we have $4 = 9 \cdot (-1)$. Hence, $x = 2N_1 + 9N_2 + 9N_3 = 2 \cdot 143 + 9 \cdot 91 + 9 \cdot 77 = 286 + 819 + 693 = 1798$ is a solution. Any other other solution is $1798 + 1001k$. In particular. $1798 - 1001 = 797$ is the minimal positive solution.

12.5 Exercises

Exercises (v)-(x) and above take you through two general versions of CRT.

(i) Let p_k be the k-th prime number, $I_k = (p_k)$. Prove that the natural map $\overline{\psi} : \mathbb{Z}/\cap_k I_k \to \prod_k \mathbb{Z}/I_k$ is not an isomorphism. Conclude that CRT fails for infinite sets of ideals.

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

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

(iv) Find the smallest positive x such that $x \equiv_7 3$, $x \equiv_{13} 4$, $x \equiv_{19} 5$.

(v) Let $I, J \trianglelefteq R$. We say that I and J are *comaximal* if $I + J = R$. Prove that the natural map $\overline{\psi} : R/I \cap J \to R/I \times R/J$ is an isomorphism if and only if I and J are comaximal.

(vi) Let $I_1, \ldots I_n$ be a collection of ideal in R. Suppose I_k and $\cap_{j<k} I_j$ are comaximal for each $k = 2, 3, \ldots n$. Using induction, prove that the natural homomorphism $\overline{\psi} : R/\cap_k I_k \to \prod_k R/I_k$ is an isomorphism.

(vii) Let R be commutative, $I, J \trianglelefteq R$. Prove that $(I + J)(I \cap J) \subseteq IJ$.

(viii) Let R be commutative, $I, J \trianglelefteq R$ comaximal. Prove that $I \cap J = IJ$.

(ix) Let R be commutative, I_k, $k = 1, \ldots n$ pairwise comaximal ideals of R. Using induction, prove that I_n and $\cap_{k<n} I_k$ are comaximal.

(x) Let R be commutative, I_k, $k = 1, \ldots n$ pairwise comaximal ideals of R. Prove that the natural map $\overline{\psi} : R/\cap_k I_k \to \prod_k R/I_k$ is an isomorphism.

(xi) Let $I, J \trianglelefteq R$ be comaximal, R commutative. Prove that I^n and J^m are comaximal for all n and m.

12.6 Vista: prime factorisation

Read more about prime numbers and their factorisation in Lauritzen. The now defunct RSA challenge[14] used to pay you money for factoring one of the numbers of the form pq. This is all related to the P=NP problem, one of the millennium problems with one million dollars bounty[15]. You may also want to find out more about quantum computers. Imagine notoriety you can achieve if you find a way of factoring large numbers: you may become the top criminal of the century by compromising all secure internet traffic with payment information.

13 Actions, stabilisers and alternating group

We introduce the notion of actions, and discuss stabilisers. We use to prove that the parity of a permutation is well defined.

13.1 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 $x \in X$.

In this definition, the image of (g, x) under the map $\cdot$ is denoted by $g \cdot x$. If G acts on a set X, we would refer to X as a G-set.

[14] http://www.rsasecurity.com/rsalabs/node.asp?id=2093

[15] http://en.wikipedia.org/wiki/Complexity_classes_P_and_NP

Proposition 13.1 *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 $\phi(g) \in \mathrm{Sym}(X)$, and $\phi : G \to \mathrm{Sym}(X)$ 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 $\phi(g) \in \mathrm{Sym}(X)$, and then Property (i) implies immediately that ϕ is a homomorphism. □

The opposite is also true: a homomorphism $\phi : G \to \mathrm{Sym}(X)$ 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 $\phi : G \to \mathrm{Sym}(X)$ (see exercises and Example 1).

The kernel of an action $\cdot$ of G on X is defined to be the kernel $K = \ker(\phi)$ of the homomorphism $\phi : G \to \mathrm{Sym}(X)$ defined in Proposition 13.1. 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 10.4 says that $G \cong G/K \cong \mathrm{im}(\phi)$, which we state as a proposition, which can be thought of as a generalisation of Cayley's Theorem (Theorem 10.5).

Proposition 13.2 *If $\cdot$ is a faithful action of G on X, then G is isomorphic to a subgroup of* $\mathrm{Sym}(X)$.

Examples. 1. If G is a subgroup of $\mathrm{Sym}(X)$, 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 $P = \{v_i \mid i \in \mathbb{Z}_6\}$ be a regular hexagon, $G =< a = R_{2\pi/6}, b = S_0 >= D_{12}$ its group of isometries. We use notation of Section 5.4 here. The action of G on the vertex set gives a homomorphism $\phi : G \to S_6$ where $\phi(a) = (v_0, v_1, v_2, v_3, v_4, v_5)$ and $\phi(b) = (v_1, v_5)(v_2, v_4)$.

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 v_6 and v_1, e_2 joins v_1 and v_2, etc. The map ϕ 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 v_1 and v_4, d_2 joins v_2 and v_5, and d_3 joins v_3 and v_0. Then map ϕ of the action of G on D is defined by $\phi(a) = (d_1, d_2, d_3)$, and $\phi(b) = (d_1, d_2)$. 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 *regular* action, defined for any group G. The regular G-set X is the set of G as a set. The action $g \cdot x$ is defined 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 13.2, we can deduce Cayley's Theorem (Theorem 10.5).

4. Similarly to the regular G-set, there exists *antiregular* G-set for any group G. The antiregular G-set $X = G$, as a set. The action is defined via $g \cdot x = xg^{-1}$ for all $g \in G$, $x \in X$.

13.2 Stabilisers

Definition. Let X be a G-set, $x \in X$. The stabiliser of x in G, denoted by G_x or $\text{Stab}_G(x)$, is $\{g \in G \mid g \cdot x = x\}$.

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

Proposition 13.3 *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.*

13.3 Action, rings and alternating groups

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.

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

One can define the automorphism group

$$\text{Aut}(R) = \{\phi \in \text{Sym}(R) \mid \phi \text{ is a ring homomorphism}\}.$$

Its elements, isomorphisms $R \to R$, are called *automorphisms.* See Exercise (iii) for an adaptation of Proposition 13.1 to the situation of rings.

Let us consider the action of the symmetric group S_n on the set $R = \mathbb{Z}[X_1, \dots X_n]$ defined by the obvious formula $\sigma \cdot F(X_1, \dots X_n) = F(X_{\sigma(1)}, \dots X_{\sigma(n)})$. For example, if $\sigma = (1,2,3)$ and $F = 1 + X_1 + X_2^3 + X_3X_4$ then $\sigma \cdot X_1 = X_2$, $\sigma \cdot X_2 = X_3$, $\sigma \cdot X_3 = X_1$, $\sigma \cdot X_4 = X_4$ and $\sigma \cdot F = F(X_2, X_3, X_1, X_4) = 1 + X_2 + X_3^3 + X_1X_4$. Let point it out that the action of S_n on the set R is actually an action on the ring R.

Definition. The alternating group A_n is the stabiliser of the Vandermonde polynomial $\Omega = \prod_{i>j}(X_i - X_j) \in \mathbb{Z}[X_1, \dots X_n]$.

We need the following calculation.

Proposition 13.4 *If $\sigma = (i,j)$ is a transposition then $\sigma \cdot \Omega = -\Omega$.*

Proof: Without loss of generality, $i > j$. We represent Ω 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 $\sigma \cdot \omega_1 = X_j - X_i = -\omega_1$. 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, $\sigma \cdot \omega_2 = \omega_2$. The remaining three functions are similar, as they pair X_i and X_j with X_t in one of 3 regions:

$$\omega_3 = \prod_{t>i}(X_t - X_i)(X_t - X_j), \ \sigma \cdot \omega_3 = \prod_{t>i}(X_t - X_j)(X_t - X_i) = \omega_3,$$

$$\omega_4 = \prod_{i>t>j}(X_i - X_t)(X_t - X_j), \ \sigma \cdot \omega_4 = \prod_{i>t>j}(X_j - X_t)(X_t - X_i) = \omega_4,$$

$$\omega_5 = \prod_{t<j}(X_i - X_t)(X_j - X_t)), \ \sigma \cdot \omega_5 = \prod_{t<j}(X_j - X_t)(X_i - X_t) = \omega_5.$$

Since S_n acts on the ring R, $\sigma \cdot \Omega = (s \cdot \omega_1)(s \cdot \omega_2)(s \cdot \omega_3)(s \cdot \omega_4)(s \cdot \omega_5) = -\Omega$. □

Proposition 13.4 allows to describe A_n in the standard terms. We say that a permutation $\sigma \in S_n$ is *even* if it is a product of even number of transpositions and that σ is *odd* if it is a product of odd number of transpositions. Apriori, it is not clear why a permutation cannot be both odd and even.

Corollary 13.5 *Each permutation $\sigma \in S_n$ is either odd or even. The alternating group A_n consists of even permutations in A_n.*

PROOF: Observe that $\Omega \neq -\Omega$ since $2\Omega \neq 0$. If $\sigma = \tau_n \cdots \tau_1$ then $\sigma \cdot \Omega = (-1)^n \Omega$ by Proposition 13.4. Hence, σ is even (odd) if and only if $\sigma \cdot \Omega = \Omega$ ($\sigma \cdot \Omega = -\Omega$ correspondingly). □

The next two corollaries are immediate.

Corollary 13.6 *The sign function* $\mathrm{sign} : S_n \to \mathbb{Z}^\times$ *defined by* $\mathrm{sign}(\sigma) = \frac{\sigma \cdot \Omega}{\Omega}$ *is a well-defined group homomorphism.*

Corollary 13.7 *If* $n \geq 2$ *then* $|A_n| = n!/2$.

PROOF: Since the sign function is a surjective homomorphism, $S_n/A_n \cong \mathbb{Z}^\times \cong C_2$ by the isomorphism theorem. Hence, $|S_n|/|A_n| = 2$ and $|A_n| = n!/2$. □

13.4 Exercises

(i) Let G be a group, X a set. Prove that there is a bijection between the set of actions $G \times X \to X$ and the set of homomorphisms $\phi : G \to \mathrm{Sym}(X)$.

(ii) Prove Proposition 13.3

(iii) Let G be a group, R a ring. Prove that there is a bijection between the set of actions of G on the ring X and the set of homomorphisms $\phi : G \to \mathrm{Aut}(X)$.

(iv) In the case of $n = 2$, express the discriminant Ω^2 via functions $\phi_1 = X_1 + X_2$ and $\phi_2 = X_1X_2$. How does it help to solve quadratic equations?

(v) Let $G = \mathrm{Sym}(X)$, $Y \subseteq X$. 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 $|X|$?

13.5 Vista: Grassmann ring and determinants

The sign function is used to define the determinant. In the opposite direction each $\sigma \in S_n$ defines permutation matrix A_σ and $\mathrm{sign}(\sigma) = \det(A_\sigma)$. There is an alternative way of building two of them together at the expense of using a slightly more exotic ring.

Let K be a commutative ring. The Grassmann ring $S = \Lambda_K < X_1, \ldots X_n >$ as an additive group is a subgroup of the additive group of the polynomial ring $R = K[X_1, \ldots X_n]$. It consists of all polynomials where each X_i enters with degree at most 1. In particular, if K is a field, S is 2^n-dimensional vector space over K.

The multiplication in S is different: it is K-bilinear but on monomials one uses rules $X_iX_j = -X_jX_i$ and $X_i^2 = 0$. The linear group $G = GL_n(K)$ acts on the ring S: $(a_{ij}) \cdot X_k = \sum_i a_{ik} X_i$ extends to a unique ring automorphism. Similarly, S_n acts via $\sigma \cdot X_j = X_{\sigma(j)}$. Now, the key is the top degree element $\Omega = X_1 X_2 \ldots X_n$. It gives both the sign and the determinant by $(a_{ij}) \cdot \Omega = \det(a_{ij})\Omega$ and $\sigma \cdot \Omega = \mathrm{sign}(\sigma)\Omega$.

The Grassmann ring is not commutative in general but always supercommutative. Find out more about superalgebras, supergroups and supervector spaces and how they are used in Physics.

14 Orbits

We introduce the quotient G-set G/H and prove the orbit-stabiliser theorem. We look at Riemann sphere and Hopf fibration.

14.1 Homomorphisms of G-sets

Let X and Y be G-sets. A function $\phi : X \to Y$ is *a homomorphism of G-sets* if $\phi(g \cdot x) = g \cdot \phi(x)$ for all $g \in G$, $x \in X$. A bijective homomorphism will be referred to as *an isomorphism*. The G-sets X and Y are called *isomorphic* if there exists an isomorphism between them.

Examples. 1. For any G-set X and any $x \in X$, *the orbit map* $\beta_x : G \to X$ defined by $\beta_x(g) = g \cdot x$ is a homomorphism from the regular G-set to X. Indeed, $\beta_x(h \cdot g) = \beta_x(hg) = hg \cdot x = h \cdot (g \cdot x) = h \cdot \beta_x(g)$.

2. Let $X = G$ be the antiregular G-set. The orbit map β_1 is the inverse map: $\beta_1(g) = g \cdot 1 = 1g^{-1} = g^{-1}$. Thus, regular and antiregular G-sets are isomorphic.

14.2 Orbits

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.

Definition. 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 $\mathrm{Orb}_G(x)$ is

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

Observe that the orbit $\mathrm{Orb}_G(x)$ is the image of the orbit map β_x.

Similarly, to the general equivalence relations it is instructive to consider *the quotient set* $X/\sim$, i.e. the set of orbits. As the equivalence relation is carried out by G, we denote this quotient set X/G. If there is a single orbit, the action (as well the G-set) is called *transitive*.

Example. 3. Let $X = G$ be the antiregular G-set, H a subgroup of G. We restrict the antiregular action: G is an H-set under the antiregular action: $h \cdot g = gh^{-1}$. The orbits of this action are left cosets $[g]_H = gH$. T he quotient set G/H is the set of all left cosets. In particular, if H is normal in G, the quotient set admits a group structure which we called the quotient group. If H is not necessarily normal, the quotient set G/H still carries an action of G (or a G-set structure): $g \cdot [a]_H = [ga]_H$. The axioms of the action are apparent but one needs to verify that this action is well defined: $[a]_H = [b]_H \implies \exists h \in H\ a = bh \implies ga = gbh \implies g \cdot [a]_H = [ga]_H = [gb]_H = g \cdot [b]_H$. See also exercise (iii).

4. Smith's normal form in Linear Algebra deals with the action of $G = \mathrm{GL}_n(K) \times \mathrm{GL}_m(K)$ on the set $X = K^{n\times m}$ of $n \times m$ matrices: $(g, h) \cdot x = gxh^{-1}$. Observe that $x \in \mathrm{Orb}_G(y)$ if and only if x and y are equivalent if and only if they can be moved one to another by a sequence of elementary row and column transformations if and only if x and y have the same rank. Recall that the elementary transformation is just a multiplication by an elementary matrix, who together generate the general linear group. Thus, $|X/G| = \min(n, m) + 1$ while the Smith's normal form of x is a particularly nice element in $\mathrm{Orb}_G(x)$.

5. Jordan normal form story is slightly more complicated: $G = \mathrm{GL}_n(\mathbb{C})$ acts on $X = M_n(\mathbb{C})$ via $g \cdot x = gxg^{-1}$. Similarly, $x \in \mathrm{Orb}_G(y)$ if and only if x and y are similar if and only if they have the same Jordan form. The set X/G is infinite but its precise structure can be pinpointed.

6. Classification of quadratic forms (over $\mathbb{R}$) involves two groups $G = \mathrm{GL}_n(\mathbb{R}) \geq H = \mathrm{O}_n(\mathbb{R})$ acting on the same set X of real symmetric $n \times n$ matrices: $g \cdot x = gxg^T$. A G-orbit is determined by the rank and the signature of the form and admits a diagonal representative with $0, \pm 1$ on the diagonal. Since there are $r+1$ distinct forms of rank r, $|X/G| = \sum_{r=0}^{n} r+1 = (n+1)(n+2)/2$. Each G-orbit is a union of H-orbits. The latter are determined by the eigenvalues and also admits a diagonal representative with the eigenvalues on the diagonal.

14.3 Orbit-Stabiliser Theorem

The next theorem is fundamental in group theory: it is an analogue of the isomorphism theorem for G-sets.

Theorem 14.1 (The Orbit-Stabiliser Theorem) *Let a group G act on X, $x \in X$, G_x the stabiliser. Then the orbit map β_x defines an isomorphism of G-sets between G/G_x and $\mathrm{Orb}_G(x)$. In particular, $|\mathrm{Orb}_G(x)| = |G : G_x|$.*

PROOF: We consider a function $\psi : G/G_x \to \mathrm{Orb}_G(x)$ defined by $\psi([g]) = \beta_x(g) = g \cdot x$. Let us observe that this is well defined: $[g] = [h] \Longrightarrow \exists a \in G_x\ ga = h \Longrightarrow \psi([h]) = h \cdot x = ga \cdot x = g \cdot (a \cdot x) = g \cdot x = \psi([g])$.

It is a homomorphism of G-sets: $\psi(g \cdot [h]) = \psi([gh]) = gh \cdot xg \cdot (h \cdot x) = g \cdot \psi([h])$.

For any $y \in \mathrm{Orb}_G(x)$ there exists a $g \in G$ with $g \cdot x = y$. Hence $\psi([g]) = y$. For an element $g' \in G$, we have

$$g' \cdot x = y \Longleftrightarrow g' \cdot x = g \cdot x \Longleftrightarrow g^{-1}g' \cdot x = x \Longleftrightarrow g^{-1}g' \in G_x \Longleftrightarrow g' \in gG_x.$$

So the elements g' with $\psi(g') = y$ are precisely the elements of the coset gG_x. Hence, ψ is a bijection. □

Examples. 7. In Example 2 of Section 13.1, D_{12} acts transitively on sets P, E and D of vertices, edges and diagonals of the regular hexagon. Let us see what the orbit-stabiliser does for the vertices. Let us pick a vertex v_0. Its stabiliser is $H = \{1, S_0 = b\}$. The quotient set is $D_{12}/H = \{[1]_H, [a]_H, [a^2]_H, [a^3]_H, [a^4]_H, [a^5]_H\}$ with $[a^k]_H = \{a^k, a^k b\}$. Now the orbit-stabiliser theorem gives a bijection $\psi : D_{12}/H \to P$ given explicitly by $\psi([a^k]_H) = a^k \cdot v_0 = v_k$.

If one chooses another point the picture changes slightly. For instance, the stabiliser of v_2 is $A = \{1, S_2 = a^2 b\}$. The quotient set is $D_{12}/A = \{[1]_A, [a]_A, [a^2]_A, [a^3]_A, [a^4]_A, [a^5]_A\}$ with $[a^k]_A = \{a^k, a^{k+2}b\}$. The orbit-stabiliser theorem bijection $\psi' : D_{12}/A \to P$ changes to $\psi'([a^k]_A) = a^k \cdot v_2 = v_{2+k}$.

8. Let F be a field. The projective n-space $X = PF^n$ consists lines Fa in F^{n+1}. The group $G = GL_{n+1}(F)$ acts on X transitively by $A \cdot Fa = F(Aa)$. The action has a kernel $Z \lhd G$ that consists of scalar matrices. The quotient group $PGL_{n+1}(K) = G/Z$, called projective linear group acts faithfully and transitively. The stabiliser of Fe_1 in G is the group of triangular matrices $T_{n+1}(F)$. Thus, we have a bijection between $PGL_{n+1}(K)/T_{n+1}(F)$ and X.

14.4 Exercises

(i) Consider the identity map $I : G \to G$, $I(g) = g$. Show that I is a homomorphism of G-sets from the regular G-set to the antiregular G-set if and only if G is a group of exponent 2.

(ii) Prove that $\sim$, defined in Section 14.2, is an equivalence relation.

(iii) Let X be a $G \times H$-set. Prove that X/H is a G-set with the action $g \cdot [x] = [g \cdot x]$ for all $g \in G$, $[x] \in X/H$. How does it apply to the construction of the quotient set G/H.

(iv) Prove that the stabiliser of $[x]_H \in G/H$ is xHx^{-1}.

(v) Let G be a simple group (i.e. it has exactly two normal subgroups), H its proper subgroup of finite index. Prove that G is finite (hint: what is the kernel of the action on G/H).

(vi) Derive a precise estimate in (v): if $|G : H| = n$ then $|G| \leq n!/2$.

(vii) Prove that the quotient G-sets G/A and G/B are isomorphic if and only if there exists $x \in G$ such that $xAx^{-1} = B$.

(viii) Considering action on $P\mathbb{F}_3^1$, prove that $PGL_2(\mathbb{F}_3)$ is isomorphic to S_4.

14.5 Vista: Riemann Sphere and Mobius Group

In 1872 Klein proposed Erlangen Program where he suggested to classify geometries according to their groups of symmetries. Let us take a look how it works on Riemann Sphere.

The Riemann sphere is the projective 1-space over complex numbers $S^2 = P\mathbb{C}^1$. Geometrically, it is a 2-sphere. It is customary to represent $S^2 = P\mathbb{C}^1$ as a union $\mathbb{C} \cup \{\infty\}$ where a complex number z represents the line $\mathbb{C}\begin{pmatrix} z \\ 1 \end{pmatrix}$ while ∞ represents the line $\mathbb{C}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. In this representation, the natural action of $GL_2(\mathbb{C})$ is given by Mobius transformations

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \cdot z = \frac{\alpha_{11}z + \alpha_{12}}{\alpha_{21}z + \alpha_{22}}.$$

The action of $GL_2(\mathbb{C})$ is not faithful: the kernel consists of scalar matrices $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$. The group $PGL_2(\mathbb{C})$ acting faithfully is called *Mobius group.* The transformations $z \mapsto A\cdot z$ for $A \in GL_2(\mathbb{C})$ are called *Mobius transformations.* Mobius transformations are conformal, i.e. they preserve angles between curves. In fact, $PGL_2(\mathbb{C})$ is the group of all conformal transformations of $P\mathbb{C}^1$ and $PGL_2(\mathbb{C})$ underlines conformal geometry of $P\mathbb{C}^1$.

Recall that a matrix $A = (a_{ij})$ is unitary if and only if $A^{-1} = A^*$ where $A^* = (a_{ji}^*)$ is the conjugate matrix. Unitary matrices form the unitary group $U_n(\mathbb{C})$, while unitary matrices with determinant 1 form the special unitary group $SU_n(\mathbb{C})$. The group $SU_2(\mathbb{C})$ consists of matrices $\begin{pmatrix} \alpha & -\beta^* \\ \beta & \alpha^* \end{pmatrix}$ with $|\alpha|^2 + |\beta|^2 = 1$. Hence geometrically, $SU_2(\mathbb{C})$ is the unit 3-sphere S^3.

The Mobius transformations from $SU_2(\mathbb{C})$ preserve spherical distances. This corresponds to the metric geometry of $P\mathbb{C}^1$ in Klein program. The orbit map $\beta_x : SU_2(\mathbb{C}) \to P\mathbb{C}^1$ is a Hopf fibration $\beta_x : S^3 \to S^2$ with all $\beta_x^{-1}(y)$ being unit spheres.

15 Fixed points

We introduce fixed points. We prove three counting formulae and discuss their applications to combinatorics.

15.1 Fixed points

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.*

15.2 Formulae

We would like to establish three useful formulae underlining combinatorics of the group action. The first is an immediate consequence of Theorem 14.1

Proposition 15.1 (The Orbit-Stabiliser Formula) *Let G be a finite group acting on a finite set X. The for any $x \in X$*

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

Proposition 15.2 (The Counting Formula) *Let G be a finite group acting on a finite set X. Then*

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

where the sum is taken over the representatives of all orbits containing more than 1 element.

PROOF: X is a disjoint union of orbits. One element orbits form X^G. The number of elements in the larger orbits is $\sum_x |\mathrm{Orb}_G(x)| = \sum_x |G|/|\mathrm{Stab}_G(x)|$ using Proposition 15.1. □

Theorem 15.3 (The Burnside Formula) *Let G be a finite group acting on a finite set X. Then*

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

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,

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

$$= |G| \sum_{orbits} 1 = |G||X/G|.$$

□

15.3 Necklaces and bracelets

The formulae allow us to compute necklaces and bracelets. We want to make a necklace of k beads. We have n different types of beads with at least k beads of each type. How many necklaces can we make?

Mathematically, we consider the set P_k of vertices of regular k-gon. The dihedral group D_{2k} acts on P_k. Now we consider the set $X = X_{k,n}$ of all untied necklaces, i.e. functions $F : P_k \to \mathbb{Z}_n$. The dihedral group D_{2k} and its rotation subgroup C_k act on $X_{k,n}$: $(g \cdot F)(v) = F(g^{-1} \cdot v)$ where $g \in D_{2k}$, $F \in X$, $v \in P_k$. The cardinality of $X_{k,n}$ is n^k.

Definition. *A necklace* is a C_k-orbit in $X_{k,n}$. *A bracelet* is a D_{2k}-orbit in $X_{k,n}$.

Let us count bracelets and necklaces for $k = 5$. With necklaces we count the number of C_5-orbits. Observe that 1 fixes every function $f \in X$ while a non-trivial rotation fixes only the constant functions. Hence, by Burnside's formula $|C/C_5| = (n^5 + n + n + n + n)/5 = (n^5 + 4n)/5$.

With bracelets we count the number of D_{10}-orbits. A reflection R fixes functions that are constant on the orbits of the reflection, i.e. $f(Rv) = f(v)$ for each vertex v. A reflection has 3 orbits, there are n^3 such functions. Hence, by Burnside's formula $|C/D_{10}| = (n^5 + 4n + 5n^3)/10$.

Proposition 15.4 *The number of necklaces in $X_{k,n}$ is*

$$N(k,n) = \frac{1}{k} \sum_{t|k} \varphi(d) n^{k/t}$$

and the number of bracelets is

$$B(k,n) = \begin{cases} \frac{1}{2}N(k,n) + \frac{1}{2}n^t & \text{if } k = 2t-1 \text{ is odd} \\ \frac{1}{2}N(k,n) + \frac{1}{4}n^t + \frac{1}{4}n^{t+1} & \text{if } k = 2t \text{ is even} \end{cases}$$

Proof: Pick $g = a^m \in C_k$. If d is the greatest common divisor of m and k, we can write $m = dm'$ with k and m' coprime. It follows that $|g| = k/d$

and when g acts on P_k it has d orbits each of size k/d. Thus, $|X^g_{k,n}| = n^d$. Burnside's formula gives

$$N(k,n) = \frac{1}{k}\sum_{g\in G} n^{k/|g|}$$

Since $g = (a^d)^{m'}$, it follows that $< g > \supseteq < a^d >$. Since $| < g > | = k/d = | < a^d > |$, it follows that $< g > = < a^d >$ and there is a single subgroup $< a^d >$ of order $t = k/d$. It has $\varphi(t)$ elements of order t. Hence, C_k contains $\varphi(t)$ elements of order t for each $t|k$ and the formula for $N(k,n)$ follows.

If $k = 2t-1$ is odd then each reflection fixes one vertex and has further $t-1$ orbits of two vertices each. Hence, $|X^g_{k,n}| = n^t$ for each of k reflections. The formula for $B(2t-1,n)$ follows.

If $k = 2t$ is even then a reflection through a vertex fixes two vertices and has further $t-1$ orbits of two vertices each. Hence, $|X^g_{k,n}| = n^{t+1}$ for t reflections. A reflection through the middle of an edge has t orbits of two vertices each. Hence, $|X^g_{k,n}| = n^t$ for the remaining t reflections. The formula for $B(2t,n)$ follows. □

If the supply of a certain type of beads is limited or any other restrictions is imposed, one can still do the count but one has to deal with a subset of $X_{k,n}$. Some of these situations are covered in exercises and the vista section.

15.4 Exercises

(i) Check that the alternative formula $g\cdot F(v) = F(g\cdot v)$ with $g\in D_{2k}$, $F\in X$, $v\in P_k$ does not define an action.

(ii) Let a group G act on a ring R. Prove that the set of fixed points R^G is a subring.

(iii) Write an explicit formula derived from Proposition 15.4 for the numbers of bracelets and necklaces if $k = p^2$ (p is prime), n is arbitrary.

(iv) Count the number of necklaces and bracelets one can make from 4 identical white and 3 identical black beads. (All the beads are used.)

(v) Count the number of necklaces and bracelets one can make from 4 identical white and 4 identical black beads. (All the beads are used.)

15.5 Vista: aperiodic necklaces

You must have seen the exponential identity

$$1 + \alpha z + \frac{\alpha^2 z^2}{2!} + \frac{\alpha^3 z^3}{2!} + \ldots = \lim_{n\to\infty}(1 + \frac{\alpha z}{n})^n$$

where $\alpha \in \mathbb{R}$, z is a variable. Have you seen its close relative, *the cyclotomic identity*

$$1 + \alpha z + \alpha^2 z^2 + \alpha^3 z^3 + \ldots = \prod_{k=1}^{\infty} (\frac{1}{1-kz})^{A(k,\alpha)}$$

where $A(k,\alpha) = \frac{1}{k}\sum_{t|k} \mu(d)\alpha^{k/t}$ and μ is the Mobius function?

We say that a necklace in $X_{k,n}$ is aperiodic if its stabiliser in C_k is trivial. The function $A(k,n)$ counts the number of aperiodic necklaces. This could be fused together into a nice second year essay as there are several different proofs (http://en.wikipedia.org/wiki/Cyclotomic_identity and http://www.stat.wisc.edu/˜callan/notes/cyclotomic/cyclo.pdf).

16 Conjugacy classes

We use G-action on G to study group theory..

16.1 Definition

In Examples 3 and 4 of Subsection 13.1, a group G was made to act on the set of its own elements by the regular $g \cdot x = gx$ and antiregular actions $g \cdot x = xg^{-1}$ for $g, x \in G$.

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

$$g \cdot x = gxg^{-1} \text{ for } g, x \in G.$$

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 $\mathrm{Cl}_G(g)$ for the orbit of g; that is the conjugacy class containing g. We have seen already in Proposition 7.4 that conjugate elements have the same order.

What is $\mathrm{Stab}_G(g)$ 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 $gfg^{-1} = f$, i.e. commute with g. Hence $G^g = C_G(g)$.

Applying the formulae 15.1, 15.2, 15.3 from the last lecture we get:

Proposition 16.1 *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) $|\mathrm{Cl}_G(g)| = |G|/|C_G(g)|$
(ii) $|G| = |\mathrm{Z}(G)| + \sum_x |G|/|C_G(x)|$
(iii) $|G/G| = \frac{1}{|G|} \sum_{g \in G} |C_G(g)|$

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 $\mathrm{Z}(G)$. So we have

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

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

It is high time that we worked out some examples!

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

2. Q_8 has 5 conjugacy classes: $\{1\}$, $\{-1\}$, $\{\pm I\}$, $\{\pm J\}$, $\{\pm K\}$. Observe that $IJI^{-1} = -J$. Observe also how the formulas work: I has a centraliser of order 4: $< I >$, hence the conjugacy class must have size $8/4 = 2$.

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

16.2 Conjugacy classes in dihedral groups

Using multiplication table of $SO_2(\mathbb{R})$ from Section 5.2, let us draw its conjugation table. We tabulate xyx^{-1} on the intersection of the row containing x and the column containing y:

	R_β	S_β
R_α	R_β	$S_{2\alpha+\beta}$
S_α	$R_{-\beta}$	$S_{2\alpha-\beta}$

The conjugation table for $D_{2n} = \{a^k \mid 0 \leq k < n\} \cup \{a^k b \mid 0 \leq k < n\}$ follows:

	a^l	$a^l b$
a^k	a^l	$a^{2k+l}b$
$a^k b$	a^{-l}	$a^{2k-l}b$

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 $\{a^k b \mid 0 \leq k < n\}$ 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 $a^{n/2} \in \mathrm{Z}(G)$). 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 correspond to the two different types of reflections: those about lines that pass through two vertices of the regular $2k$-gon P and those about lines that bisect two edges of P.

16.3 Classification of groups up to order 11

As an application we extend our classification of groups to the order 11. The only outstanding order is 9.

Proposition 16.2 *A group of order p^n, p is prime has a non-trivial centre.*

PROOF: By Formula (1) of Proposition 16.1, sizes of conjugacy classes are powers of p. By Formula (2) of Proposition 16.1, p must divide $\mathrm{Z}(G)$. Hence, the centre is non-trivial. □

Proposition 16.3 *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 3.3: 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 16.2, $\mathrm{Z}(G) \neq 1$. By Lagrange's Theorem, $|\mathrm{Z}(G)|$ is either p, or p^2. In the latter case G is abelian. Suppose the former case. Pick $x \in G \setminus \mathrm{Z}(G)$ and consider $C_G(x)$. It clearly contains $\mathrm{Z}(G)$ 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 $x \in \mathrm{Z}(G)$.

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 $G \cong C_p \times C_p$. □

16.4 Exercises

(i) Show that the centre of a group is an abelian subgroup.

(ii) Find the centre of D_{2n}.

(iii) Find centraliser of each element of D_{2n}.

(iv) Let p be an odd prime. In the series of the next exercises, we describe conjugacy classes in $GL_2(\mathbb{Z}_p)$. Prove that $|GL_2(\mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$.

(v) Thanks to Jordan normal form, we know that if a matrix $A \in GL_2(\mathbb{Z}_p)$ has an eigenvalue then it is conjugate to one of the matrices

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$$

with $\alpha \neq \beta \in \mathbb{Z}_p$. Compute the centraliser of each of these matrices. Using these computation, list corresponding conjugacy classes and their sizes. Verify that these classes contain $(p-1)p^2(p+1)/2$ elements overall.

(vi) Consider a matrix $A \in GL_2(\mathbb{Z}_p)$ without eigenvalues in $\mathbb{Z}_p$ with characteristic polynomial $z^2 - \alpha z + \beta$. Verify that for a sufficiently general $v \in \mathbb{Z}_p$, A looks like

$$B = \begin{pmatrix} 0 & -\beta \\ 1 & \alpha \end{pmatrix},$$

in the basis v, Av. Compute the centraliser of B and the size of the conjugacy class of A.

(vii) How many conjugacy classes of matrices without eigenvalues are there[16].

16.5 Vista: Sylow's Theorems

The Norwegian mathematician Sylow proved a number of theorems about subgroups of groups of prime power order in 1872. The first Sylow's theorem tells us that if a prime power p^n divides $|G|$ then G has a subgroup of order p^n.

Of particular interest are the maximal prime powers dividing $|G|$. If $|G| = p^n m$ with p and m coprime. The subgroups of order p^n are called Sylow's p-subgroups. The second Sylow's theorem states that any two Sylow's p-subgroups are conjugate.

This tells us that the set of Sylow's p-subgroups is a G-set under conjugation with a single orbit. The stabiliser of a point is the normaliser of the Sylow's subgroup: it contains the group itself. In particular, the number s_p of Sylow's p-subgroups divide m. The first Sylow's theorem tells us that s_p is also 1 modulo p.

[16] It is equal to the number of quadratic equations $z^2 - \alpha z + \beta = 0$ without solutions in $\mathbb{Z}_p$. Every such equation has two distinct solutions in the finite field $\mathbb{F}_{p^2}$ of p^2 elements. This field is unique, so the number of such equations is $(|\mathbb{F}_{p^2}| - |\mathbb{Z}_p|)/2 = (p^2 - p)/2$.

These theorems are very powerful for dealing with finite groups. For instance, let G be a group of order 15. In such a group s_3 should divide 5 and be 1 modulo 3. Hence $s_3 = 1$ and G contains unique normal subgroup of order 3. Similarly, s_5 should divide 3 and be 1 modulo 5. Hence $s_5 = 1$ and G contains unique normal subgroup of order 5. It follows that $G \cong C_3 \times C_5 \cong C_{15}$.

17 Conjugacy classes in S_n and A_n

We describe conjugacy classes in symmetric and alternating groups. We use it to prove that A_5 is simple.

17.1 Conjugacy classes in symmetric groups

Let $G = \mathrm{Sym}(X)$ 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 $fgf^{-1}(f(x_1)) = f(x_2)$. Similarly, we have $fgf^{-1}(f(x_i)) = f(x_{i+1})$ for $1 \leq i < r$ and $fgf^{-1}(f(x_r)) = f(x_1)$. Hence$fgf^{-1}$ has a cycle $(f(x_1), f(x_2), \ldots, f(x_r))$, and we have:

Proposition 17.1 *Given a permutation g in cyclic notation, we obtain the conjugate fgf^{-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 $fgf^{-1} = (3, 7)(4, 6, 2, 1)$.

In general, we say that a permutation has cycle-type $2^{r_2}3^{r_3}\ldots$, 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 $2^2 3^1 5^2$. By Proposition 17.1, 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 $f \in \mathrm{Sym}(X)$ with $fgf^{-1} = h$. 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 17.2 *Two permutations of* $\mathrm{Sym}(X)$ *are conjugate in* $\mathrm{Sym}(X)$ *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.

17.2 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 17.3 *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 $g \in G \backslash H$ such that $gx = xg$. In this case, $\mathrm{Cl}_G(x) = \mathrm{Cl}_H(x)$.
(2) For all $g \in G \setminus H$ such that $gx \neq xg$. In this case, $\mathrm{Cl}_G(x)$ is a union of $\mathrm{Cl}_H(x)$ and $\mathrm{Cl}_H(y)$ for any $y \in \mathrm{Cl}_G(x) \setminus \mathrm{Cl}_H(x)$. Moreover, $|\mathrm{Cl}_G(x)|/2 = |\mathrm{Cl}_H(x)| = |\mathrm{Cl}_H(y)|$.

Proof: By Proposition 8.1, H is normal subgroup of G. Hence, $\mathrm{Cl}_G(x) \subseteq H$.

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 16.1, $|\mathrm{Cl}_G(x)| = |G|/|C_G(x)| \leq 2|H|/2|C_H(x)| = |\mathrm{Cl}_H(x)|$. Hence, $\mathrm{Cl}_G(x) = \mathrm{Cl}_H(x)$.

In the case (2), $C_H(x) = C_G(x)$. Using Proposition 16.1, $|\mathrm{Cl}_G(x)| = |G|/|C_G(x)| = 2|H|/|C_H(x)| = 2|\mathrm{Cl}_H(x)|$. Pick $g \in \mathrm{Cl}_G(x) \setminus \mathrm{Cl}_H(x)$. it suffices to observe that $|\mathrm{Cl}_G(x)|/2 = |\mathrm{Cl}_H(g)|$. But $g = axa^{-1}$ 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 $|\mathrm{Cl}_G(x)| = 2|\mathrm{Cl}_H(g)|$. □

The next lemma is a criterion for normality.

Lemma 17.4 *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 8.2, $H \trianglelefteq G$ if and only if $ghg^{-1} \in H$ for all $g \in G$, $h \in H$. But this is just saying that $H \trianglelefteq G$ if and only if $h \in H \Rightarrow \mathrm{Cl}_G(h) \subset H$, and the result follows. □

For example, consider the subgroup $\{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ 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.

17.3 The Simplicity of A_5

In Subsection 10.1, 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 17.3 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 permutations 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 17.3, $g = (x_1, x_2)(x_3, x_4)(x_5)$ 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 17.5 A_5 *has 5 conjugacy classes, of sizes 1, 15, 20, 12, 12.*

Theorem 17.6 A_5 *is a simple group.*

PROOF: By Lemma 17.4, 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 (7.2). □

17.4 Exercises

(i) Verify that Proposition 17.3 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

17.5 Vista: groups of order 12

This would be too little for a second year essay but you may consider classifying groups up to order 30 for an essay. As far as order 12 is concerned, you already know 4 of the five groups: C_{12}, $C_6 \times C_2$, $D_{12} \cong D_6 \times C_2$, A_4. For the fifth group, consider embeddings $D_6 \leq SO_2(\mathbb{R}) \leq SO_3(\mathbb{R})$ and the surjection $\psi : SU_2(\mathbb{C}) \rightarrow SO_3(\mathbb{R})$ from Vista Section 14.5. The last group BD_{12}, called binary dihedral group, is $\psi^{-1}(D_6)$. It is different from the other four groups because it has a single element of order 2: $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ is the only element of order 2 in $SU_2(\mathbb{C})$.

One can sort them out using Sylow's theorem. By Sylow's theorem, s_2 is either 1 or 3, while s_3 is either 1 or 4. Now Sylow's 2-subgroup could be either C_4 or K_4. You can do the classification by considering the following cases:

$(s_2 = 1, s_3 = 1, C_4)$ the group is $C_3 \times C_4 \cong C_{12}$,
$(s_2 = 1, s_3 = 1, K_4)$ the group is $C_3 \times K_4 \cong C_6 \times C_2$,
$(s_2 = 1, s_3 = 4, C_4)$ no group, C_3 cannot act nontrivially on C_4,
$(s_2 = 1, s_3 = 4, K_4)$ the group is A_4,
$(s_2 = 3, s_3 = 1, C_4)$ the group is BD_{12},
$(s_2 = 3, s_3 = 1, K_4)$ the group is D_{12},
$(s_2 = 3, s_3 = 4)$ no group, Sylow's 3-subgroups contain $(3-1) \cdot 4 + 1 = 9$ elements leaving space only for one Sylow's 2-subgroup.

18 Domains, divisibility and PID-s

Algebra-2 takes a major turn now. We have finished group theory and would like to study ring theory for the rest of the module. We start by discussing divisibility in domains. We introduce and motivate principal ideal domains.

18.1 Domains

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 18.1 *(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.

18.2 Divisibility

We are working in a domain R. Let us try to replicate techniques known to you in Number Theory.

Definition. Let $x, y \in R$ we say that x *divides* y and write $x|y$ if $y = xr$ for some $r \in R$.

The following lemma is obvious.

Lemma 18.2 *The following statements are equivalent for all $x, y \in R$.*

(i) $x|y$.
(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 $x|y$ and $y|x$.

Lemma 18.3 *The following statements are equivalent*
(i) $x \sim y$
(ii) $(y) = (x)$
(iii) There exists $q \in R^{\times}$ *such that* $x = qy$

PROOF: $(i \Longrightarrow iii)$ 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 $q = r \in R^\times$.

The other implications are obvious. □

In $\mathbb{Z}$ divisibility is usual: $x \sim y$ if and only if $x = \pm y$ since $\mathbb{Z}^\times = \{1, -1\}$. 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* $\operatorname{lcm}(x, y)$ is such $l \in R$ that $x|l$, $y|l$, and if $x|z$ and $y|z$ then $l|z$.

Uniqueness of $\operatorname{lcm}(x, y)$ and $\gcd(x, y)$ (up to an associate element) are established in the exercises. Existence is a bit trickier. In general, they may not exist.

18.3 PID-s

Recall that an ideal $I \lhd R$ is principal if $I = (a) = aR$ for some $a \in R$ (see Section 11.2).

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

Example. 1. Integers $\mathbb{Z}$ is PID. Any ideal $I \lhd \mathbb{Z}$ is a subgroup of $\mathbb{Z}^+$ and any subgroup of $\mathbb{Z}$ is cyclic. Hence, $I =< n >$ as an additive group, implying that $I = (n)$ as an ideal.

In the next lecture we will give more examples of PID-s but for now we will use their properties.

Proposition 18.4 *If R is PID then* $\operatorname{lcm}(x, y)$ *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 $(z) \subseteq (x) \cap (y) = (l)$. □

Note that $(x) + (y) = \{rx + sy\}$, hence $\gcd(x, y) = rx + sy$ for some $r, s \in R$ as soon as R is a PID.

18.4 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 R.

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

Proposition 18.5 *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 $q \in R^{\times}$. The domain condition implies that $q = b$. □

Notice that we strategically excluded O_R out of the consideration. If we try to include it, it would be prime but not irreducible causing all sorts of havoc.

Proposition 18.6 *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 18.4. 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. 2. Let $R = \mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$. 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 18.7 $\mathbb{Z}[i\sqrt{5}]$ *is not PID.*

18.5 Exercises

(i) Prove Lemma 18.2.
(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 $\operatorname{lcm}(x, y)$. 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 18.1.
(vi) Show that if R is a domain then $R[x_1 \ldots x_n]$ is a domain.

18.6 Vista: noetherian rings and group rings

A natural generalisation of principal ideal domains are *noetherian domains.* A ring R (not necessarily commutative) is noetherian if every ideal is finitely generated. Hilbert's basis theorem states that $R[X]$ is noetherian whenever R is noetherian. The quotient ring of a noetherian is noetherian (but not a subring, in general). This gives a plenty of examples of noetherian rings.

Here is another chance for you to become a famous algebraist next weekend. All you need to do is to figure out when the group ring is noetherian. Let G be a group, $\mathbb{F}$ a field. The group ring $\mathbb{F}G$ is a vector space with basis E_g, $g \in G$. The multiplication is $\mathbb{F}$-bilinear with $E_g \cdot E_h = E_{gh}$ on the basis elements. When is $\mathbb{F}G$ noetherian?

A group G is called *polycyclic* if it admits a finite chain of subgroups $G_k \leq G$, $k = 0, \ldots n$ such that $G_n = G$, $G_0 = \{1\}$, $G_k \lhd G_{k+1}$ and G_{k+1}/G_k is cyclic for all k. A group G is called *virtually polycyclic* if it has a polycyclic subgroup of finite index. It is known (the level of hard exercise) that if G is virtually polycyclic then $\mathbb{F}G$ is noetherian. It is one of the biggest conjectures in ring theory that the reverse statement holds: is it true that if $\mathbb{F}G$ is noetherian then G is virtually polycyclic.

19 Euclidean domains

First, we discuss what prime elements do on the level of quotient rings. Then we introduce Euclidean domains and give new examples of PID-s.

19.1 Quotient rings and primes

Proposition 19.1 *Let R be a domain. A nonzero element $p \in R$ is prime if and only if $R/(p)$ is a domain.*

PROOF: We write $[x]$ for the coset $x + (p)$. Now $[x] \neq 0$ translates into $p \not| x$. Thus, $[x][y] = 0 \implies [x] = 0 \vee [y] = 0$ translates into the prime element definition $p \mid xy \Longrightarrow p \mid x \vee p \mid y$. □

The following proposition tells us a bit more.

Proposition 19.2 *Let R be a PID. If $p \in R$ is prime then $R/(p)$ is a field.*

Proof: By Proposition 19.1, $R/(p)$ is a domain. We need to find an inverse for a nonzero element $[x] = x + (p) \in R/(p)$. Since $[x] \neq 0$, p does not divide x. Since p is irreducible (Proposition 18.5) and $\gcd(x,p) \mid p$, $\gcd(x,p) = 1$. Since $(x) + (p) = (\gcd(x,p))$, there exist $a, b \in R$ such that $1 = ax + bp$. Hence, $[x]^{-1} = [a]$ in the quotient ring $R/(p)$. □

Proposition 19.2 and Theorem 19.3 tell us how to construct new fields: if F is a field and $f = f(X) \in F[X]$ is irreducible then $F[X]/(f)$ is a field.

19.2 Euclidean domains

Definition. *A euclidean domain* (ED) 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 $a, b \in R$,
(ii) $\nu(ab) = \nu(b)$ if and only if $a \in R^{\times}$,
(iii) $\forall a, b\ \exists q, r$ such that $a = qb + r$ and either $r = 0$ or $\nu(b) > \nu(r)$.

Examples. 1. 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.

2. 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 $K[X]^{\times}$ 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.

It is essential to master the polynomial division with remainder. Dividing by $f(X) = X^n + \sum_{k=0}^{n-1} a_k X^k$, can be done using *a rewriting rule* $X^n \rightsquigarrow -\sum_{k=0}^{n-1} a_k X^k$. For instance, let us divide $X^7 + 1$ by $X^3 - X + 1$. The rewriting rule $X^3 \rightsquigarrow X - 1$. We apply it to the top degree term and write what goes into the result on top:

$$X^7 + 1 \overset{X^4}{\rightsquigarrow} X^4(X-1) + 1 = X^5 - X^4 + 1 \overset{X^2}{\rightsquigarrow} X^2(X-1) - X^4 + 1 = -X^4 + X^3 - X^2 + 1$$

$$\overset{-X}{\rightsquigarrow} -X(X-1) + X^3 - X^2 + 1 = X^3 - 2X^2 + X + 1 \overset{1}{\rightsquigarrow} (X-1) - 2X^2 + X + 1$$

Hence, $X^7 + 1 = (X^4 + X^2 - X + 1)(X^3 - X + 1) + (-2X^2 + 2X)$.

19.3 ED and PID

Theorem 19.3 *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 $a = bq \in (b)$. □

Rings $\mathbb{Z}[\alpha] = \{\sum_k a_k \alpha^k \mid a_k \in \mathbb{Z}\}$ 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. 3. The domain $\mathbb{Z}[(1+\sqrt{-19})/2]$ is PID but not ED.

4. The domain $\mathbb{Z}[\sqrt{-5}]$ is not PID as shown in Section 18.4. Hence, it is not ED either.

5. 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 $q^* = \mathrm{Re}(q) - \mathrm{Im}(q)i$ 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 ν is not defined at zero[17].

19.4 Minimal polynomials

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 $f_A : K[X] \to M_n(K)$ by $f_A(\sum_n \alpha_n X^n) = \sum_n \alpha_n A^n$. This ring homomorphism is sometimes called *evaluation homomorphism* because $f_A(F(X)) = F(A)$. 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 $K[X]$ the kernel is an ideal (m_A) for some polynomial $m_A \in K[X]$. 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

[17] Alternatively, one needs to set $\nu(0) = -\infty$ to keep the precious property $\nu(xy) = \nu(x) + \nu(y)$.

f_A consists of all polynomials $F(X)$ 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 $f_\alpha : \mathbb{Q}[X] \to \mathbb{C}$ by $f_\alpha(F(X)) = F(\alpha)$. The kernel is (m_α). If $m_\alpha = 0$ the number α is called *transcendental*: it does no satisfy any polynomial with rational coefficients. If $m_\alpha \neq 0$ the number α is called *algebraic*. Unique monic m_α is called *the minimal polynomial of* α.

The last application of this sort is *the characteristic of a ring*. Any ring R has a natural homomorphism $f_R : \mathbb{Z} \to R$ 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.

19.5 Exercises

(i) Show that the ring $\mathbb{Q}_p = \{x/p^n \mid x \in \mathbb{Z}\} \leq \mathbb{Q}$, where p is prime, is Euclidean domain.
(ii) Divide $X^8 + X \in \mathbb{Q}[X]$ by $X^4 - X - 1$ with remainder.
(iii) Divide $X^6 - X^5 + 1 \in \mathbb{Q}[X]$ by $X^3 - X^2 + 1$ with remainder.
(iv) Find the minimal polynomial of $(1 + \sqrt{D})/2$ over $\mathbb{Q}$ where D is a square-free integer.
(v) Prove that the characteristic of a domain is always a prime number.
(vi) Describe all rings of characteristic 1.

19.6 Vista: $\sqrt{-19}$ and quadratic integers

You may be left surprised by the lack of details why $\mathbb{Z}[(1+\sqrt{-19})/2]$ is non-euclidean PID. It is actually easy to see that the usual norm $\nu(x) = |x|^2$ fails axiom (iii) of Euclidean domain. It is slightly harder to see a certain weaker version of axiom (iii). This weaker axiom still ensures that an ideal I is generated by a smallest non-zero element. It is somewhat trickier to show that $\mathbb{Z}[(1+\sqrt{-19})/2]$ has no other euclidean norm[18].

It is more interesting to try to understand what is so special about $\sqrt{-19}$. Let $D \neq 1$ be a square-free integer. The quadratic field $\mathbb{Q}[\sqrt{D}]$ has a natural subring $\mathcal{O}_D$ of all algebraic integers. Observe that if $D \equiv_4 1$ then $\mathcal{O}_D = \mathbb{Z}[(1+\sqrt{D})/2]$, and $\mathcal{O}_D = \mathbb{Z}[\sqrt{D}]$, otherwise. Which of these rings are ED or PID? The following statements summarize what is known about imaginary (i.e. $D < 0$) quadratic integers:

(i) $\nu(x) = |x|^2$ is Euclidean norm on $\mathcal{O}_D$ if and only if $D \in \{-1, -2, -3, -7, -11\}$,
(ii) $\mathcal{O}_D$ is PID if and only if $D \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$,

[18] O. A. Campoli, The American Mathematical Monthly, Vol. 95 (9), 1988, pp. 868–871 contains full details and elementary treatment

(iii) if $D \in \{-19, -43, -67, -163\}$ then $\mathcal{O}_D$ is not PID.

Less is known about real ($D > 1$) quadratic integers:

(i) $\mathbf{u}(x) = |x|^2$ is Euclidean norm on $\mathcal{O}_D$ if and only if $D \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$,

(ii) for $D < 100$, $\mathcal{O}_D$ is PID if and only if $D \in \{2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 46, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94, 97\}$,

(iii) it is conjectured by Gauss (open as of 2010) that there are infinitely many PID-s among $\mathcal{O}_D$,

(iv) if extended Riemann's hypothesis holds, then $\mathcal{O}_D$ is PID implies that $\mathcal{O}_D$ is ED.

Thus, $\mathcal{O}_{-19}$ is the "smallest" PID, not ED!

If you want to know more, you should consider taking MA3A6, *Algebraic Number Theory* where you will learn that all $\mathcal{O}_D$ are all *Dedekind domains* and a certain finite group, called *the ideal class group* of $\mathcal{O}_D$, controls whether $\mathcal{O}_D$ is PID (this group must be trivial)!

20 Unique factorisation domains

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.

20.1 Factorisation

Definition. A domain R is FD[19] (*factorisation domain*) if each $x \in R \setminus (R^\times \cup \{0\}$ admits a factorisation $x = r_1 \cdot r_2 \cdots r_n$ where r_i are irreducible elements.

An FD R is UFD[20] (*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 20.1 *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

[19] You won't find this notion in the literature as it follows from being noetherian.

[20] Don't' confuse with UFO.

another factorisation $ab = xr \cdot s_1 \cdots s_t$. 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, $r_1 = qs_i$ for some unit q. Now we use the induction assumption on $(qr_1) \cdot r_2 \cdots r_{n-1} = s_1 \cdots s_{i-1} \cdot s_{i+1} \cdots s_m$. □

20.2 Principal ideals give unique factorisation

Theorem 20.2 *A PID is a UFD.*

Proof: Using Propositions 18.6 and 20.1, 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 $I = \cup_{n=1}^{\infty} (y_n)$ 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.

20.3 Exercises

(i) A ring is *noetherian* if every ideal is finitely generated. Prove that R is noetherian if and only if every ascending chain of ideals in R terminates.

(ii) Prove that every noetherian domain is FD.

(iii) Prove that $(2, X) \lhd \mathbb{Z}[X]$ is not principal

20.4 Vista: the birth of ring theory

The ring theory appeared as a result of an accident, Lame's 1847 mistake (see http://www.mathpages.com/home/kmath447.htm). Let $\omega_p = \exp(2\pi i/p)$ where $p > 2$ is a prime number. Lame has essentially proved that if $\mathbb{Z}[\omega_p] = \{\sum_{i=0}^{p-1} a_i\omega^i \in \mathbb{C} \mid a_i \in \mathbb{Z}\}$ is a UFD then the Fermat Last Theorem holds for p, i.e. the equation $x^p + y^p = z^p$ have no nontrivial integral solutions. Lame has not given enough thought to the issue and just used the UFD property of $\mathbb{Z}[\omega_p]$. Kummer has corrected this mistake and given a criterion in terms of Bernoulli numbers for $\mathbb{Z}[\omega_p]$ to be UFD. A prime p is called *regular* (correspondingly *irregular*) if $\mathbb{Z}[\omega_p]$ 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.

The ring $\mathcal{O}_{-3} = \mathbb{Z}[\omega_3]$ is called Eisenstein integers. If you were thinking about Gaussian primes for your second year essay, consider switching to Eisenstein primes.

21 Polynomials over fields

We study $F[X]$ over a field F. Our knowledge of this ring leads to a number of nontrivial observations about the field F itself.

21.1 Remainder theorem

Proposition 21.1 (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 $0 = f(a) = r$. □

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 $F(a) = 0$.

When we want to classify primes in a ring R, we are after *a complete lists of primes*, which means that each element on the list is prime and any other prime is associate to exactly one prime on the list. For example, $X + a \sim bX + ab$ and we list just one of them.

Proposition 21.2 *If F is an algebraically closed field then $\{X - a \mid a \in F\}$ is a complete list of primes in $F[X]$.*

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 $F[X]^\times = F^\times$. Hence, $X - a$ is associate only to $bX - ab$ for all $b \in F^\times$.

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 21.1, $X - a$ divides f. Hence, f is associate to $X - a$. □

21.2 Finite subgroups of fields

Theorem 21.3 *Let F be a field. A finite subgroup of $F^\times$ is cyclic.*

Proof: Suppose $G \leq F^\times$ 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 21.4 *$\mathbb{Z}_p^\times$ is a cyclic group of order $p-1$.*

21.3 Imaginary units in finite fields

Imaginary unit $i \in \mathbb{C}$ is a 4-th primitive root of unity, i.e., $i^4 = 1$ while $i^2 = -1 \neq 1$. In a general field F, a primitive n-th root of unity is an element $a \in F^\times$ of order n. An imaginary unit is a 4th primitive root of unity.

Proposition 21.5 *$\mathbb{Z}_p$ admits a primitive n-th root of unity if and only if $p \equiv_n 1$.*

PROOF: By Corollary 21.4, $\mathbb{Z}_p^\times \cong C_{p-1}$. It admits an element of order n if and only if $n \mid (p-1)$. In particular, if $n \mid (p-1)$ and t is a generator of $\mathbb{Z}_p^\times$ then $t^{(p-1)/n}$ has order n. □

The following corollary gives as a polynomial prime.

Corollary 21.6 *X^2+1 is prime in $\mathbb{Z}_p[X]$ if and only if $p \equiv_4 3$.*

PROOF: If $p = 2$, then $X^2+1 = (X+1)^2$ is not prime. If $p \equiv_4 1$, then $X^2+1 = (X+i)(X-i)$ is not prime where $i \in \mathbb{Z}_p$ is an imaginary unit. If $p \equiv_4 3$, then X^2+1 is prime because any decomposition of $X^2+1 = (aX-b)(cX-d)$ gives an imaginary unit b/a. Indeed, $(b/a)^2+1 = (ab/a-b)(cb/a-d) = 0$, so that $(b/a)^2 = -1 \neq 1$. □

21.4 Algebraic closure

The following two theorems will neither be proved, nor examined in this module because this would lead too far from the material we study. *Algebraic closure of a field F* is an algebraically closed field $\overline{F}$ which contains F as a subring so that each $a \in \overline{F}$ is algebraic over F.

Theorem 21.7 (Existence and uniqueness of algebraic closure) *Every field admits an algebraic closure. If $\overline{F}$ and $\widetilde{F}$ are two algebraic closures of F then there exists a ring isomorphism $\psi : \overline{F} \to \widetilde{F}$ such that $\psi(x) = x$ for all $x \in F$.*

In MA3D5 Galois Theory you will learn a standard proof via Zorn's lemma. Zorn's Lemma is equivalent to the axiom of choice. Play with website http://consequences.emich.edu that deals with various consequences of the axiom of choice. In particular, Axiom of Choice is form 1, existence of $\overline{F}$ is form 69, uniqueness of $\overline{F}$ is form 233, and Ultrafilter Theorem (a more high-tech way of proving Theorem 21.7) is form 14.

Theorem 21.8 (The fundamental theorem of algebra) $\overline{\mathbb{C}} = \mathbb{C}$

In other words, complex numbers form an algebraically closed field. There are numerous proofs using Algebra, Analysis or Topology including the one done in Foundations along the lines of the original Gauss' argument. My two favourite proofs are via Liouville's Theorem (MA3B8 Complex Analysis) or Open Mapping Theorem

21.5 Derivatives and square-free elements

If R is a domain, $r \in R$ is *square-free* if r is not a unit and if $x^2 \mid r$ then r is a unit. I don't know how to determine whether $r \in \mathbb{Z}$ is square-free except as to decompose r into primes and see.

Let $D : F[X] \to F[X]$ be an F-linear map defined on the monomials by $D(X^n) = nX^{n-1}$. You must have recognized the usual derivative except that we do them over any field and do not use limits. We denote $D(f) = f'$ to play on our usual intuition.

Proposition 21.9 *If* $f \in F[X]$ *and* $\gcd(f, f') = 1$ *then* f *is square-free.*

PROOF: Suppose $h^2|f$, then $f = gh^2$.

Let us observe the product rule: $(ab)' = ab' + a'b$. On monomials $(X^nX^m)' = (n+m)X^{n+m-1} = X^n(X^m)' + (X^n)'X^m$. By biliniearity it holds for any $a, b \in F[X]$.

Now $f' = (gh^2)' = g(hh)' + g'h^2 = (2gh' + g'h)h$. Hence $h|\gcd(f, f') = 1$ forcing h to be a unit. □

Amazingly enough, the inverse statement actually fails. Let $F = \mathbb{Z}_p(t)$ be the field of rational functions with coefficients in $\mathbb{Z}_p$. Consider $f(X) = X^p - t$. One can use Eisenstein's criterion (Proposition 24.4 and example 1 afterwards) to show that $f(X)$ is prime and consequently square-free. On the other hand, $f' = pX^{p-1} - 0 = 0$, so $\gcd(f, f') = f$.

What actually happens is that $f(X) = (X - \sqrt[p]{t})^p$ but the element[21] $\sqrt[p]{t}$ is not in F. However, the following holds true while the proof is left as an exercise.

Corollary 21.10 *Let* $f \in F[X]$ *be a polynomial of degree* n. *Then* $\gcd(f, f') = 1$ *if and only if* f *has* n *distinct roots in* $\overline{F}$.

21.6 Exercises

(i) Let F be a field, $f = f(X) \in F[X]$ irreducible. Prove that $X + (f) \in F[X]/(f)$ is a root of the polynomial $f(X)$.

(ii) Improve Theorem 21.3 by showing that any two subgroups in $F^\times$ of order N are equal.

[21] The key word is *separable* here.

(iii) Prove that $\{X - a, X^2 + bX + c \mid a, b, c \in \mathbb{R},\ b^2 - 4c < 0\}$ is a complete list of primes in $\mathbb{R}[X]$.
(iv) For which p is $X^2 + X + 1$ prime in $\mathbb{Z}_p[X]$?
(v) For which p is $X^2 - X + 1$ prime in $\mathbb{Z}_p[X]$?
(vi) For which p is $X^2 + X + 2 \in \mathbb{Z}_p[X]$ square free?
(vii) For which p is $X^p + X + 1 \in \mathbb{Z}_p[X]$ square-free?
(viii) Prove that if $f \in F[X]$ is square-free and F is algebraically closed then $\gcd(f, f') = 1$.
(ix) Prove Corollary 21.10 .

21.7 Vista: Artin's conjecture

Let $D > 1$ be a square-free integer. Let $S(D)$ be the set of primes p such that $|[D]| = p-1$ where $[D] = D+(p) \in \mathbb{Z}_p^\times$. Emil Artin conjectured in 1927 that this set was infinite. A positive answer follows from Generalised Riemann Hypothesis (which you should never confuse with Extended Riemann Hypothesis). Find out more in M. Ram Murty, Mathematical Intelligencer 10 (4), 1988, 59-67.

22 Gaussian primes

We classify primes in $\mathbb{Z}[i] = \mathbb{Z}[\omega_4] = \mathcal{O}_{-1}$ and derive some consequences.

22.1 Preliminary observations

Primes in $\mathbb{Z}[i]$ are called *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 22.1 *If $x \in \mathbb{Z}[i]$ and $\nu(x)$ is prime then x is gaussian prime.*

Proof: Using Proposition 20.1 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 22.2 *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 22.1. Finally, $x^* = x^{-1} \cdot \nu(x) = (y/p) \cdot p = y$. □

Proposition 22.3 *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. Thus, $n = \nu(q) \mid \nu(p_j) = p_j^2$. □

Proposition 22.4 $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} \cong C_4$.

22.2 Gaussian primes

Lemma 22.5 *For each $p \in \mathbb{Z}$ we have an isomorphism of rings $\mathbb{Z}[i]/(p) \cong \mathbb{Z}_p[X]/(X^2+1)$.*

PROOF: Since $\mathbb{Z}[i] \cong \mathbb{Z}[X]/(X^2+1)$ both rings are quotient rings of of $\mathbb{Z}[X]$. It remains to notice that the kernel of both natural maps $\mathbb{Z}[X] \to \mathbb{Z}[i]/(p)$ and $\mathbb{Z}[X] \to \mathbb{Z}_p[X]/(X^2+1)$ is (p, X^2+1). Thus, both rings are isomorphic to $\mathbb{Z}[X]/(p, X^2+1)$. □

Using this technical lemma, we are ready to tackle the main theorem.

Theorem 22.6 *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 nonassociate gaussian primes q and q^* such that $p = qq^*$.*

PROOF: By Proposition 19.1, a prime $p \in \mathbb{Z}$ is a gaussian prime if and only if $\mathbb{Z}[i]/(p) \cong \mathbb{Z}_p[X]/(X^2+1)$ (Lemma 22.5) is a domain. By Corollary 21.6, this is equivalent to $p \equiv_4 3$.

Now using Proposition 22.3, we can distinguish the two cases for a gaussian prime q. In the first case, q is 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 and p is forced to be 3 modulo 4.

In the second case, q is a gaussian prime such that $p = \nu(q)$ is a prime. As $x \mapsto x^*$ is a ring automorphism, q^* is also a prime. Thus we observe two primes q, q^* such that $p = qq^* = \nu(q)$. As p is not gaussian prime, p is forced to be 1 or 2 modulo 4.

Now $q = x + yi \sim q^* = x - yi$ if and only if $|x| = |y|$ or $x = 0$ or $y = 0$. The latter two cases are impossible and in the former case, we must have $|x| = |y| = 1$. Thus, we get 4 associate primes $\pm 1 \pm i$ and $p = \nu(1+i) = 1^2 + 1^2 = 2$.

If p is 1 modulo 4, we get two groups of associate primes $\{q = x+yi, -y+xi, -x-yi, y-xi\}$ and $\{q^* = x-yi, y+xi, -x+yi, -y-xi\}$. The primes in the different groups are not associate. □

22.3 Applications

Corollary 22.7 (Fermat) *Every prime p congruent 1 modulo 4 is a sum of two integer squares in a unique way.*

PROOF: Theorem 22.6 provides existence: $p = qq^*$ for a prime $q = x + iy$, hence $p = qq^* = x^2 + y^2$. 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 $\mathbb{Z}[i]$. □

Corollary 22.8 *$n \in \mathbb{N}$ is a sum of integer squares if and only if n is not divisible by any prime congruent 3 modulo 4.*

Corollary 22.9 *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 $p_0 = 2$, $q_0 = 1 + i$, $p_j = q_j q_j^*$ 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. □

22.4 Exercises

(i) Prove Proposition 22.4.

(ii) Prove Corollary 22.8

(iii) Decompose 20, 30, 91 and 1001 into a product of gaussian primes.

(iv) Compute $\gcd(8 + 6i, -1 + 3i)$

22.5 Vista: primes in arithmetic progressions

You may notice that there are infinitely many primes congruent 3 modulo 4. The proof is straightforward (hint: $x = 4p_1 \cdot p_2 \cdots p_n - 1$) and no gaussian primes are required. Dirichlet has proved in general that an arithmetic progression $a+nb$ with coprime a and b contains infinitely many primes. You can find the original paper online[22], although I doubt that it was Dirichlet who submitted it. This result is a cornerstone not only in Number Theory but also in Representation Theory and Harmonic Analysis.

23 Fractions and Gauss lemma

We introduce the field of fractions and prove Gauss' Lemma.

[22] http://arxiv.org/abs/0808.1408

23.1 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 23.1 *If R is a domain then $Q(R)$ is a field under the operations*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \ \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

and $\pi : R \to Q(R)$, $\pi(r) = r/1$ 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 π 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

$$adyw + bcyw = bdxw + bdyu.$$

Rewriting it, we get

$$adyw - bdxw = bdyu - bcyw.$$

This obviously holds because

$$adyw - bdxw = dw(ay - bx) = 0 \text{ and } bdyu - bcyw = by(du - cw) = 0.$$

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

$$(\frac{a}{b}+\frac{c}{d})+\frac{e}{f} = \frac{ad+bc}{bd}+\frac{e}{f} = \frac{adf+(bcf+bde)}{bdf} = \frac{a}{b}+\frac{cf+de}{df} = \frac{a}{b}+(\frac{c}{d}+\frac{e}{f}).$$

The commutativity of addition is easier:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{c}{d} + \frac{a}{b}.$$

The zero and the additive inverse are usual: $0 = 0/1$ and $-(a/b) = (-a)/b$ with all the checks routine. The associativity of multiplication is straightforward

$$(\frac{a}{b}\cdot\frac{c}{d})\cdot\frac{e}{f} = \frac{ac}{bd}\cdot\frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b}\cdot\frac{ce}{df} = \frac{a}{b}\cdot(\frac{c}{d}\cdot\frac{e}{f})$$

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 $(a/b)^{-1} = b/a$ 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:

$$(\frac{a}{b}+\frac{c}{d})\cdot\frac{e}{f} = \frac{ad+bc}{bd}\cdot\frac{e}{f} = \frac{ade+bce}{bdf} = \frac{ade}{bdf}+\frac{bce}{bdf} = \frac{a}{b}\cdot\frac{e}{f}+\frac{c}{d}\cdot\frac{e}{f}.$$

The map is a ring homomorphism because $\pi(1_R) = 1/1 = 1_Q$,

$$\pi(xy) = \frac{xy}{1} = \frac{x}{1}\cdot\frac{y}{1} = \pi(x)\cdot\pi(y),\ \pi(x+y) = \frac{x+y}{1} = \frac{x}{1}+\frac{y}{1} = \pi(x)+\pi(y).$$

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.

3. $Q(\mathbb{Z}[\alpha]) = \mathbb{Q}(\alpha)$

23.2 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 23.2 *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 $\widehat{g} = ag \in R[X] \ni \widehat{h} = bh$ and $f = \widehat{g}\widehat{h}$.*

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 $a_1 g(X)$, $a = a_1/a_2 \in Q(R)$. We define $\widetilde{g} = ag \in R[X]$. Similarly, $\widetilde{h} = bh \in R[X]$. Notice that $\widetilde{g}$ and $\widetilde{h}$ are primitive. Consequently,

$$f = \frac{u}{v}\widetilde{g}\widetilde{h} \text{ and } vf = u\widetilde{g}\widetilde{h}$$

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 $\widehat{q} = u\widetilde{g}$ and $\widehat{h} = v^{-1}\widetilde{h}$. 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

$$\pi : R[X] \to R/(p)[X],\ \pi(\sum_k a_k X^k) = \sum_k (a_k + (p))X^k.$$

Since $\pi(v) = 0$, we conclude that

$$0 = \pi(v)\pi(f) = \pi(u)\pi(\widetilde{g})\pi(\widetilde{h}).$$

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, $\pi(\widetilde{g}) \neq 0 \neq \pi(\widetilde{h})$ because these polynomials are primitive. □

23.3 Exercises

(i) Prove that the relation $\sim$ on the W is an equivalence relation.
Let R be a commutative ring, $S \subset R$ *a denominator set*, that is, a subset closed under multiplication, containing 1. 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.*
(ii) Show that if R is a domain, $p \in R$ is prime then $S = R \setminus (p)$ is a denominator set.
(iii) Describe $Q_S(\mathbb{Z})$ where $S = \mathbb{Z} \setminus (p)$ for some prime p.
(iv) Describe $Q_S(\mathbb{Z})$ where $S = \{p^n \mid n \in \mathbb{Z}\}$ for some prime p.
(v) Determine the kernel of the natural homomorphism $R \to Q_S(R)$, $r \mapsto r/1$. In particular, show that the kernel is the whole ring R if and only if $0 \in S$.

23.4 Vista: fractions over ED

A subtle algebraic property of fractions over ED is useful in Analysis, namely for integration and interpolation. If R is ED then any element of

$Q(R)$ can be represented as

$r+\sum_j \frac{r_j}{p_j^{n_j}}$ where $r, r_j, p_j \in R$, $n_j \in N$, p_j are pairwise non-associate prime.

Try to prove it yourself but let us see some example:

Examples. 1. $5/6 = 1/ + 1/3$.

2. $101/24 = 4 + 5/24 = 4 + 1/3 - 1/8$.

3. Here is a typical computation of the integral of a rational function $\int (X+1)/(X^3+X)\, dX$.

$$\frac{X+1}{X^3+X} = \frac{aX+b}{X^2+1} + \frac{c}{X} = \frac{cX^2+c+aX^2+bX}{X^3+X}$$

Hence, $b = c = 1$, $a = -1$ and

$$\int \frac{X+1}{X^3+X} dX = \int (\frac{-X+1}{X^2+1} + \frac{1}{X}) dX = -\frac{1}{2}\int \frac{dX^2}{X^2+1} + \int \frac{dX}{X^2+1} + \int \frac{dX}{X} =$$

$$= -\frac{1}{2}\ln(X^2+1) + \arctan(X) + \ln(X) + C$$

Does it ring a bell?

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

$$\frac{g}{f} = \sum_{k=1}^{n} \frac{t_j}{X - a_j}$$

and

$$g(X) = \sum_{k=1}^{n} \frac{t_j f(X)}{X - a_j} = \sum_{k=1}^{n} t_j (X - a_1) \cdots (X - a_{j-1}) \cdot (X - a_{j+1}) \cdots (X - a_n).$$

Substituting $X = a_j$ we get the answer,

$$g(a_j) = t_j(a_j - a_1) \cdots (a_j - a_{j-1}) \cdot (a_j - a_{j+1}) \cdots (a_j - a_n) = t_j f'(a_j) \text{ or } t_j = \frac{g(a_j)}{f'(a_j)}.$$

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 $g(a_j) = s_j$.

24 Polynomials over UFD

We discuss polynomials with coefficients in UFD. We prove Eisenstein's criterion and introduce cyclotomic polynomials.

24.1 Corollaries of Gauss' Lemma

The following proposition is a corollary of Gauss' lemma.

Proposition 24.1 *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 $Q[X]$. Moreover, $R[X]$ is UFD.*

PROOF: It immediately follows from Theorem 23.2 that all elements listed are irreducible. Let us establish that any $f \in R[X]$ can be factorised into them, We can factorise $f = f_1 \cdots f_n$ in $Q[X]$. Getting rid of denominators and common divisors of numerators, we get $f = a\widetilde{f_1}\cdots\widetilde{f_n}$ for some $a \in Q$,$\widetilde{f_j} = a_j f_j$ 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 either a prime in R or a primitive element in $R[X]$, prime in $Q[X]$.

Now we proceed to prove that this factorisation is unique. Let us consider two factorisations

$$f = p_1 \cdots p_k f_1 \cdots f_n = q_1 \cdots q_t g_1 \cdots g_m \in R[X],\ p_j, q_j \in R,\ f_j, g_j \notin R$$

into irreducible elements. Without loss of generality f_j, g_j are primitive. Using the UFD property of $Q[X]$, $n = m$ and f_j associate to $g_{\sigma(j)}$ for some permutation σ. Since $R[X]$ is a domain, we can cancel all associate elements:

$$\alpha p_1 \cdots p_k = \beta q_1 \cdots q_t \in R$$

for some units $\alpha, \beta \in R^{\times}$. Using the UFD property of R establishes the uniqueness of the factorisation.

Finally, by Proposition 20.1, every irreducible is prime. □

The following two corollaries provide new examples of UFD-s.

Corollary 24.2 *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 Proposition 24.1. □

Corollary 24.3 $\mathbb{Z}[X_1, \ldots X_n]$ *is UFD.*

24.2 Eisenstein's Criterion

As we have just observes, the irreducibility of polynomials is the same over $R[X]$ and $Q[X]$. However, determining whether a particular polynomial is irreducible is often subtle. The following is a powerful tool for producing some of examples.

Proposition 24.4 (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 $a_n = b_m c_t$ which is a contradiction. □

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 $Q = Q(R)$.

Examples. 1. If p is prime in R then $X^n + p$ is prime in $R[X]$ for any n. In particular, $f(X) = X^p - t$ is prime in $R[X]$ where $R = F[t]$ (F is a field) and, consequently, by Gauss' lemma, prime in $Q[X] = F(t)[X]$. See Section 21.5 where it was used.

2. If p is prime in $\mathbb{Z}$ then $f(X) = X^{p-1} + X^{p-2} + \ldots X + 1$ is prime in $\mathbb{Z}[X]$. Consider the shift automorphism

$$sh_{-1} : \mathbb{Z}[X] \to \mathbb{Z}[X],\ sh_{-1}(g) = g(X+1)$$

Since it is a ring automorphism, f is prime if and only if $sh_{-1}(f)$ is prime. Now

$$sh_{-1}(f) = ((X+1)^p - 1)/(X+1-1) = X^{p-1} + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} X^{k-1}.$$

is irreducible by Eisenstein's criterion as p (but not p^2) divides all the lower coefficients.

24.3 Cyclotomic polynomial

If n is not prime in $\mathbb{Z}$ then $f(X) = X^{n-1} + X^{n-2} + \ldots X + 1$ is no longer irreducible in $\mathbb{Z}[X]$. It is a product of cyclotomic polynomials

$$f = \prod_{k \neq 1, k|n} \Phi_k, \quad \Phi_k = \prod_{0<d\leq k, \gcd(d,k)=1} (X - e^{2\pi i d/k}).$$

Proposition 24.5 *For each n, $\Phi_n(x)$ is monic with coefficients in $\mathbb{Z}$.*

Proof: We proceed by induction on n. If $n = 1$ then $\Phi_1(X) = X - 1$. Let us suppose that Φ_d is monic for $d < n$. By definition,

$$X^n - 1 = \prod_{k|n} \Phi_k = h(X)\Phi_n(X)\ ,$$

where $h(X)$ is the product of all $\Phi_d(X)$ over divisors of n other than n itself. By the inductive hypothesis, $h(X)$ is monic and has coefficients in Z. So $\Phi_n(X)$ is the result of dividing $X^n - 1$ by $h(X)$.

The process of dividing one polynomial by another would consist of rewritings $X^k \rightsquigarrow (X^k - h(X))$ where k is the degree of $h(X)$. Every time αX^m, $\alpha \in \mathbb{Z}$ is rewritten, αX^{m-k} goes to the result and $\alpha X^{m-k}(X^k - h(X))$

appears. Both have integer coefficients, hence the quotient $\Phi_n(X) = (X^n - 1)/h(X)$ is monic with integer coefficients. □

The polynomial Φ_k is actually irreducible in $\mathbb{Z}[X]$ and you can find more about it in the vista section below. It is an interesting fact that an early version of a manual for the computer system Maple has stated that all coefficients of Φ_k are ± 1 and 0. The smallest counterexample is $\Phi_{105}(X) = X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} - X^{40} - X^{39} + X^{36} + X^{35} + X^{34} + X^{33} + X^{32} + X^{31} - X^{28} - X^{26} - X^{24} - X^{22} - X^{20} + X^{17} + X^{16} + X^{15} + X^{14} + X^{13} + X^{12} - X^9 - X^8 - 2X^7 - X^6 - X^5 + X^2 + X + 1$

24.4 Exercises

(i) Prove Corollary 24.3

(ii) Prove that $F[X_1, \dots X_n]$ is not PID if $n > 1$.

(iii) Prove that $\mathbb{Z}[X_1, \dots X_n]$ is not PID.

(iv) Use Eisenstein's criterion to produce 6 new irreducible polynomials in $\mathbb{Z}[X]$.

(v) Compute the cyclotomic polynomial Φ_k for all $k < 16$.

(vi) Pick two of your favourite polynomials in $\mathbb{Z}[X]$ and find the greatest common divisor.

(vii) Let $f = \sum_k \alpha_k X^k \in R[X]$ be monic, R any domain, $I \lhd R$. Show that if $\overline{f} = \sum_k [\alpha_k] X^k \in R/I[X]$ is irreducible then f is irreducible.

24.5 Vista: irreducibility of cyclotomic polynomials

Irreducibility of the cyclotomic polynomial $\Phi_n(X)$ was part of this module last year. You can find it in the lecture notes on Mathstuff and can use it for your essay. The idea is to try to reduce the coefficients modulo some prime p, coprime to n. If $\overline{\Phi}_n(x) \in \mathbb{Z}_p[X]$ is irreducible then so is $\Phi_n(x)$ (Exercise (vii)). Unfortunately, the life is not so simple: $\overline{\Phi}_n(x) \in \mathbb{Z}_p[X]$ is irreducible if and only if $|p + (n)| = \varphi(n)$ in the group $\mathbb{Z}_n^\times$ (prove it as a part of your essay - very good advanced exercise). This means that $\mathbb{Z}_n^\times$ must be cyclic for $\overline{\Phi}_n(x)$ to have a shot at irreducibility. Look at $\mathbb{Z}_{15}^\times \cong \mathbb{Z}_3^\times \times \mathbb{Z}_5^\times \cong C_2 \times C_4$. Hence, $\overline{\Phi}_{15}(x) \in \mathbb{Z}_p[X]$ is not irreducible for any prime p!

The trick is to use several different primes. Look up the details. A beautiful consequences of irreducibility of Φ_n is an elementary proof that there are infinitely many primes which are 1 modulo n.

25 Algebras and division rings

We introduce algebras fusing rings and vector spaces. We discuss division rings and prove little Wedderburn's theorem.

25.1 Algebras, their homomorphisms and ideals

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

It is common to say that A *is an algebra over* F or simply F*-algebra.* Many of the rings we introduced are algebras.

Examples. 1. Any field K is an algebra over any subfield $\mathbb{F} \leq K$.

2. If $\mathbb{F}$ is a field, $M_n(\mathbb{F})$ and $\mathbb{F}[X]$ are algebras over $\mathbb{F}$.

3. If R is an algebra over K and $\mathbb{F} \leq K$ is a subfield then R is an algebra over $\mathbb{F}$.

Algebras have analogues of subrings, ideals and homomorphisms. *A subalgebra* of $(R, \mathbb{F})$ is a subring $S \leq R$, which is also a vector subspace. *An algebra ideal* of $(R, \mathbb{F})$ is an ideal $I \lhd R$, which is also a vector subspace. *An algebra homomorphism* from $A = (R, \mathbb{F})$ to $B = (S, \mathbb{F})$ where both algebras are over the same field $\mathbb{F}$ is an $\mathbb{F}$-linear ring homomorphism from R to S which is also a linear map. Isomorphism theorem holds for algebras.

Proposition 25.1 (Isomorphism theorem for algebras)

> *(i) If* $\phi : (R, \mathbb{F}) \to (S, \mathbb{F})$ *is an algebra homomorphism then* $\ker(\phi)$ *is an algebra ideal of* $(R, \mathbb{F})$ *and* $\mathrm{im}(\phi)$ *is a subalgebra of* $(S, \mathbb{F})$.
>
> *(ii) If* $I \lhd (R, \mathbb{F})$ *is an algebra ideal then the quotient ring* R/I *is an algebra and the quotient map* $R \to R/I$ *is an algebra homomorphism.*
>
> *(iii) Let* $\phi : (R, \mathbb{F}) \to (S, \mathbb{F})$ *be an algebra homomorphism with the kernel* I*. Then* $R/I \cong \mathrm{im}(\phi)$ *as algebras.*

So far the algebras seem to be pretty much as rings. The following examples should raise your alarms.

Examples. 4. Complex numbers $\mathbb{C}$ is a $\mathbb{C}$-algebra in two different ways: $(\mathbb{C}, \mathbb{C})$ with $\alpha \cdot x = \alpha x$ and $(\mathbb{C}, \mathbb{C})'$ with $\alpha \cdot x = \alpha^* x$. They are isomorphic as algebras but the identity map $I(x) = x$ is not an algebra homomorphism. The complex conjugation $x \mapsto x^*$ is an algebra isomorphism.

5. Since $\mathbb{C}$ is a subring of $M_2(\mathbb{R})$, $M_2(\mathbb{R})$ is a $\mathbb{C}$-vector space:

$$(x + yi) \cdot A = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} A$$

but it is not $\mathbb{C}$-algebra: $\alpha(ab) = a(\alpha b)$ fails.

25.2 Algebras and centres

To understand example 5, we need to recall the notion of the centre. *The centre* of a ring R is $Z(R) = \{a \in R \mid \forall x \in R\ xa = ax\}$. Similarly to groups, *the centraliser* of $x \in R$ is $C(x) = C_R(x) = \{a \in R \mid xa = ax\}$.

Proposition 25.2 *Let R be a ring, $x \in R$. Then $C_R(x)$ and $Z(R)$ are subrings of R. If R is an $\mathbb{F}$-algebra, then $C_R(x)$ and $Z(R)$ are subalgebras.*

PROOF: Since $0, 1 \in C(x)$, $C(x)$ is not empty. It is an additive subgroup since $ax = xa$, $bx = xb$ imply that $(a-b)x = ax - bx = xa - xb = x(a-b)$. It is a subring since $ax = xa$, $bx = xb$ imply that $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$. If R is an $\mathbb{F}$-algebra, $C(x)$ is a subalgebra since $ax = xa$, $\alpha \in \mathbb{F}$ imply that $(\alpha a)x = \alpha(ax) = \alpha(xa) = x(\alpha a)$.

All the statements hold for the centre since $Z(R) = \cap_{x\in R} C_R(x)$. □

Centres shed some light on algebra structures (cf. Exercise (vi)).

Proposition 25.3 *Let R be a ring, $\mathbb{F}$ a field. A ring homomorphism $\phi : \mathbb{F} \to R$ defines an $\mathbb{F}$-algebra structure on R by $f \star r = \phi(f)r$, $f \in \mathbb{F}$, $r \in R$.*

PROOF: The vector space axioms follow from the homomorphism properties of ϕ: $(f + \tilde{f}) \star (r + \tilde{r}) = \phi(f + \tilde{f})(r + \tilde{r}) = \phi(f)r + \phi(f)\tilde{r} + \phi(\tilde{f})r + \phi(\tilde{f})\tilde{r} = f \star r + f \star \tilde{r} + \tilde{f} \star r + \tilde{f} \star \tilde{r}$ 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 $f \star (r\tilde{r}) = (\phi(f)r)\tilde{r} = (f \star r)\tilde{r}$ and the second part follows from the fact that the image lies in the centre: $(\phi(f)r)\tilde{r} = (\alpha a)b = a(\alpha b)$. □

Now we are ready to explain mysterious Example 5: $Z(M_2(\mathbb{R})) = \mathbb{R}$, thus the homomorphism $\mathbb{C} \to Z(M_2(\mathbb{R}))$ does not have an image in the centre. In fact, there are no $\mathbb{C}$-algebra structures on $Z(M_2(\mathbb{R}))$ because there are no ring homomorphisms $\mathbb{C} \to \mathbb{R}$ (see Exercises (iii), (iv) and (vi)).

Example. 6. A ring D is *a division ring* if $D^\times = D \setminus \{0\}$. A division ring is not necessarily a field because a field must be commutative while a division ring does not[23]. If $ax = xa$ then $xa^{-1} = a^{-1}axa^{-1} = a^{-1}xaa^{-1} = a^{-1}x$, thus all $C_D(x)$ are division rings too and $Z(D)$ is a field. By Proposition 25.3, a division ring D is a $Z(D)$-algebra. In the next lecture we give an explicit example of a division algebra, which is not a field. But now we will explain where not to look.

25.3 Finite division rings

Let us make a general observation about finite algebras.

[23] Sometimes division rings are called *skew fields*.

Proposition 25.4 *Let $(R, \mathbb{F})$ be an algebra such that R is finite but nonzero. Then $|\mathbb{F}| = p^m$ for some prime p and positive integer m while $|R| = |\mathbb{F}|^k$ for some positive integer k.*

PROOF: Since $\psi : F \to R$, $\psi(f) = f1_R$ is a nonzero ring homomorphism, its kernel must be zero ($\mathbb{F}$ is a field). Thus, $\mathbb{F}$ is finite.

The characteristic of $\mathbb{F}$ (see Section 19.4) must be prime p. Hence $\mathbb{Z}_p$ is a subring of $\mathbb{F}$. Natural action $a \cdot x = ax$, $a \in \mathbb{Z}_p$, $x \in \mathbb{F}$ makes $\mathbb{F}$ into a vector space over $\mathbb{Z}_p$. Since $\mathbb{F}$ is finite, the vector space is finite dimensional, say of dimension m. Hence, $|\mathbb{F}| = |\mathbb{Z}_p^n| = p^n$.

Similarly, if k is the dimension of R over $\mathbb{F}$ then $|R| = |\mathbb{F}^k| = |\mathbb{F}|^k$. □

Now we are ready for little disappointment.

Theorem 25.5 (Little Wedderburn's Theorem) *A finite division ring is a field.*

PROOF: Let R be a finite division ring with centre Z, which is a field and R is a Z-algebra. By Proposition 25.4, $|Z| = q = p^m$ and $|R| = q^k$. It suffices to prove that $k = 1$.

Consider the action of $G = R^\times$ on R by conjugation: $g \cdot x = gxg^{-1}$. The fixed points of this action is the centre Z. The stabiliser $\text{Stab}_G(x)$ consists of all non-zero elements in the centraliser $C_R(x)$ which is a Z-subalgebra of dimension $d(x)$. Thus, the counting formula (Proposition 15.2) gives us that

$$q^k = |R| = |Z| + \sum_x |G|/|\text{Stab}_G(x)| = q + \sum_x \frac{q^k - 1}{q^{d(x)} - 1}$$

where the sum is over representatives of orbits with at least 2 elements, so $d(x) < k$. Thus, the cyclotomic polynomial $\Phi_k(z)$ divides $z^k - 1$ but not $z^{d(x)} - 1$. Let us rewrite the counting formula as

$$q - 1 = (q^k - 1) - \sum_x \frac{q^k - 1}{q^{d(x)} - 1}.$$

The integer $\Phi_k(q)$ divides the right hand side, hence, it divides $q - 1$. We claim that $|\Phi_k(q)| > q - 1$ for $k > 1$. Indeed, if $\xi = e^{2\pi i/k}$ then the set of primitive k-th roots of unity is $\{\xi^t \mid t \in \mathbb{Z}_k^\times\}$. Thus,

$$|\Phi_k(q)|^2 = \prod_t |q - \xi^t|^2 = \prod_t [(q - Re(\xi^t))^2 + Im(\xi^t)^2]$$

and since $|\xi| = 1$, each real part is certainly between -1 and $+1$, so
$q - Re(\xi^t) > q - 1$ unless $Re(\xi^t) = 1$, which happens only if $\xi^t = 1$, which can happens only if $k = 1$. □

25.4 Exercises

(i) Prove Proposition 25.1.

(ii) Prove that any two $\mathbb{F}$-algebra structures on a field $\mathbb{F}$ are isomorphic as algebras.

(iii) Prove that if R is a commutative ring then $Z(M_n(R)) = \{\alpha I_n \mid \alpha \in R\}$.

(iv) Prove that there are no ring homomorphisms $\mathbb{C} \to \mathbb{R}$. (Hint: where should i go?)

(v) Prove that if V is a vector space over a field $\mathbb{F}$ then the set of all linear operators $E_{\mathbb{F}}(V)$ is an $\mathbb{F}$-algebra with $S\dot{T} = ST$ and $\alpha T : v \mapsto \alpha(Tv) = T(\alpha v)$. Prove that $Z(E_{\mathbb{F}}(V)) = \{\alpha I_V \mid \alpha \in \mathbb{F}\}$.

(vi) Let R be a ring, $\mathbb{F}$ a field. Prove that there is a bijection between the set $A = \{(R, \mathbb{F}) \mid (R, \mathbb{F}) \text{ is an algebra }\}$ of algebra structures and the set B of algebra homomorphisms from $\mathbb{F}$ to $Z(R)$.

25.5 Vista: finite fields

To understand finite division rings, it remains to describe finite fields. We already know that a finite field must have p^n elements for some prime power p^n. In fact, for each prime power p^n there exists a unique (up to an isomorphism) field $\mathbb{F}_{p^n}$ of order p^n. Existence follows from Theorem 21.7. Let $\overline{\mathbb{Z}_p}$ be the algebraic closure of $\mathbb{Z}_p$. Then $\mathbb{F}_{p^n}$ is the subset of $\overline{\mathbb{Z}_p}$ that consists of roots of $z^{p^n} - z$. You need the freshman's dream binomial formula (Section 9.1) to prove that $\mathbb{F}_{p^n}$ is a subfield of $\overline{\mathbb{Z}_p}$.

Uniqueness follows from the UFD property of $\mathbb{Z}_p[z]$. Let $f(z)$ be any prime factor of $\Phi_{p^n-1}(z)$ in $\mathbb{Z}_p[z]$. If $\mathbb{F}$ is a field of order p^n then both $z^{p^n} - z$ and $\Phi_{p^n-1}(z)$ split over $\mathbb{F}$ into linear factors. Let $\xi \in \mathbb{F}$ be a primitive root of $\Phi_{p^n-1}(z)$. The evaluation homomorphism $\mathbb{Z}_p[z] \to \mathbb{F}$, $h(z) \mapsto h(\xi)$ gives rise to an isomorphism $\mathbb{Z}_p[z]/(f) \cong \mathbb{F}$, proving that any two subfields are, indeed isomorphic.

26 Quaternions, algebraic properties

We study the algebraic properties of quaternions. As an application we describe Hopf fibration.

26.1 Hamilton quaternions

In Section 4.4 introducing the quaternionic group Q_8, we used the following matrices in $M_2(\mathbb{C})$:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Proposition 26.1 *The $\mathbb{R}$-span of 1, I, J and K is an $\mathbb{R}$-subalgebra of $M_2(\mathbb{C})$.*

PROOF: The space is an $\mathbb{R}$-vector subspace containing 1. It suffices to check that it is closed under multiplication. We have already seen how to multiply these matrices (Proposition 4.6):

	1	I	J	K
1	1	I	J	K
I	I	-1	K	$-J$
J	J	$-K$	-1	I
K	K	J	$-I$	-1

We are done because the multiplication is bilinear: $(\sum_i \alpha_i E_i)(\sum_j \beta_j E_j) = \sum_{i,j} \alpha_i \beta_j E_i E_j$. □

Definition. The Hamilton[24] quaternions $\mathbb{H}$ is the $\mathbb{R}$-algebra described in Proposition 26.1.

Notice that $\mathbb{H}$ is not a $\mathbb{C}$-subalgebra of $M_2(\mathbb{C})$. The $\mathbb{C}$-span of these elements is the whole $M_2(\mathbb{C})$. Moreover, $\mathbb{H}$ is not a $\mathbb{C}$-algebra at all because $Z(\mathbb{H}) = \mathbb{R}$ and there are no ring homomorphisms $\mathbb{C} \to \mathbb{R}$ (see exercises).

26.2 Real and imaginary quaternions

A quaternion $\alpha 1$ is called *real.* A quaternion $\alpha I + \beta J + \gamma K$ is called *imaginary.* Imaginary quaternions form a three-dimensional subspace $\mathbb{H}_0$, while real quaternions form a subalgebra $\mathbb{R}$ of $\mathbb{H}$. For each quaternion $x = \alpha 1 + \beta I + \gamma J + \delta K \in \mathbb{H}$, analogously to complex numbers we define *its conjugate*

$$x^* = \alpha 1 - \beta I - \gamma J - \delta K,$$

its real part

$$Re(x) = (x + x^*)/2 = \alpha 1 \in \mathbb{R},$$

its imaginary part

$$Im(x) = (x - x^*)/2 = \beta I + \gamma J + \delta K \in \mathbb{H}_0,$$

and *its norm*

$$\nu(x) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2.$$

[24] He discovered the quaternions walking along a canal in Dublin. He got so excited that he vandalised the first bridge with the formulas. Brougham Bridge now carries a plaque saying *Here as he walked by on the 16th of October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication $i^2 = j^2 = k^2 = ijk = -1$ & cut it on a stone of this bridge.*

We treat the space of the imaginary quaternions $\mathbb{H}_0$ as the standard 3-space with the standard dot and crossed products:

$$(\alpha I + \beta J + \gamma K) \bullet (\alpha' I + \beta' J + \gamma' K) = \alpha\alpha' + \beta\beta' + \gamma\gamma' \ ,$$

$$(\alpha I + \beta J + \gamma K) \times (\alpha' I + \beta' J + \gamma' K) = (\beta\gamma' - \beta'\gamma)I + (\gamma\alpha' - \gamma'\alpha)J + (\alpha\beta' - \alpha'\beta)K.$$

Theorem 26.2 *If $x = \alpha + a, y = \beta + b \in \mathbb{H}$ with $\alpha, \beta \in \mathbb{R}$ and $a, b \in \mathbb{H}_0$ then $xy = (\alpha\beta - a \bullet b) + (\alpha b + \beta a + a \times b)$.*

PROOF: By $\mathbb{R}$-bilinearity, $xy = \alpha\beta + \alpha b + \beta a + ab$. It remains to write $a = \alpha_1 I + \alpha_2 J + \alpha_3 K$, $b = \beta_1 I + \beta_2 J + \beta_3 K$ and compute the product $ab = -\alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3 + (\alpha_2\beta_3 - \alpha_3\beta_2)I + (\alpha_3\beta_1 - \alpha_1\beta_3)J + (\alpha_1\beta_2 - \alpha_2\beta_1)K = -a \bullet b + a \times b$. □

Let us draw several corollaries.

Corollary 26.3 *If $x \in \mathbb{H}$ then $xx^* = \nu(x)1$.*

PROOF: We write $x = \alpha + a$ with $\alpha \in \mathbb{R}$, $a \in \mathbb{H}_0$. Then $x^* = \alpha - a$ and $xx^* = (\alpha\alpha - a \bullet (-a)) + (\alpha a - \alpha a - a \times a) = \alpha^2 + a \bullet a = \nu(x)1$, using the fact that $a \times a = 0$. □

Corollary 26.4 *If $x, y \in \mathbb{H}$ then $(xy)^* = y^* x^*$.*

PROOF: Again writing $x = \alpha + a$, $y = \beta + b$ with $\alpha, \beta \in \mathbb{R}$, $a, b \in \mathbb{H}_0$, we get $y^* x^* = (\beta\alpha + b \bullet a) + (-\alpha b - \beta a + b \times a) = (xy)^*$, using the fact that $b \times a = -a \times b$. □

Corollary 26.5 *If $x, y \in \mathbb{H}$ then $\nu(xy) = \nu(x)\nu(y)$.*

PROOF: $\nu(xy)1 = xy(xy)^* = xyy^*x^* = x(\nu(y)1)x^* = xx^*\nu(y)1 = \nu(x)\nu(y)$ □

The vector spaces $\mathbb{H}$ and $\mathbb{H}_0$ are euclidean spaces. The euclidean norm of a vector is $||x|| = \sqrt{\nu(x)}$. The inequality $||x|| \cdot ||y|| \geq |x \bullet y|$ is called Schwarz's inequality. It allows us to define the angle between two nonzero vectors as $\theta = \arccos{(x \bullet y / ||x|| \cdot ||y||)}$.

Corollary 26.6 *If $a, b \in \mathbb{H}_0$ and θ is the angle between a and b then $||a \times b|| = ||a|| ||b|| \sin\theta$.*

PROOF: Since $ab = -a \bullet b + a \times b$, $a \bullet b$ is real and $a \times b$ is imaginary, $\nu(ab) = \nu(a \bullet b) + \nu(a \times b) = ||a||^2||b||^2(\cos\theta)^2 + ||a \times b||^2$ and $\nu(ab) = ||a||||b|| = ||a||^2||b||^2(\cos\theta)^2 + ||a||^2||b||^2(\sin\theta)^2$ proving the statement. □

26.3 Multiplicative group of quaternions

$\mathbb{H}$ is not a field because $IJ \neq JI$ but it is a division ring.

Proposition 26.7 *$\mathbb{H}$ is a division ring.*

PROOF: It follows from Corollary 26.3 that $x^{-1} = \nu(x)^{-1}x^*$ for each $x \in \mathbb{H} \setminus \{0\}$. □

Let us analyze the multiplicative group $\mathbb{H}^\times = \mathbb{H}\setminus\{0\}$. Since a quaternion is naturally a matrix:

$$x = \alpha 1 + \beta I + \gamma J + \delta K = \begin{pmatrix} \alpha + \beta i & \gamma + \delta i \\ -\gamma + \delta i & \alpha - \beta i \end{pmatrix},$$

$\mathbb{H}^\times$ is a subgroup of $GL_2(\mathbb{C})$. It has several interesting subgroups on its own. Real quaternions form a subgroup $\mathbb{R}^\times$ that has a further subgroup $\mathbb{R}^\times_+$ of positive real quaternions. Another subgroup is $U(\mathbb{H}) = \{x \in \mathbb{H} \mid \nu(x) = 1\}$.

Proposition 26.8 *$\mathbb{H}^\times \cong \mathbb{R}^\times_+ \times U(\mathbb{H})$.*

PROOF: The multiplication in $\mathbb{H}$ defines a homomorphism $\phi : \mathbb{R}^\times_+ \times U(\mathbb{H}) \to \mathbb{H}^\times$, i.e. $\phi(\alpha, q) = \alpha q$. It is injective because $\alpha q = 1$ imply that $Im(\alpha q) = \alpha Im(q) = 0$, i.e. $q = \beta$ is real. Moreover $\alpha\beta = 1$ while $\alpha > 0$ and $|\beta| = 1$, hence $\alpha = q = 1$.

It is surjective because $q = \nu(q)\nu(q)^{-1}q = \phi(\nu(q), \nu(q)^{-1}q)$. □

Writing a quaternion x as αq, $\alpha \in \mathbb{R}^\times_+$, $q \in U(\mathbb{H})$ is *a polar form of the quaternion.*

26.4 Complex numbers and quaternions

Let us look at elements of order 2 in $\mathbb{H}^\times$.

Proposition 26.9 *The following statements hold for $x \in \mathbb{H}^\times$.*

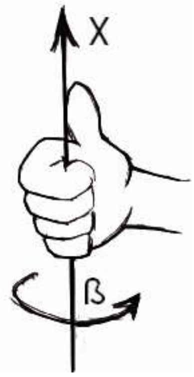
(i) $x^2 \in \mathbb{R}$ if and only if $x \in \mathbb{R} \cup \mathbb{H}_0$.
(ii) $x \in \mathbb{R} \cup \mathbb{H}_0$ if and only if $x^2 \geq 0$.
(iii) $x \in \mathbb{R} \cup \mathbb{H}_0$ if and only if $x^2 \leq 0$.
(iv) $|x| = 2$ if and only if $x = -1$
(v) $|x| = 4$ if and only if $q(x) = 1$ and $x \in \mathbb{H}_0$

PROOF: We write $x = \alpha + a$ with $\alpha \in \mathbb{R}$, $a \in \mathbb{H}_0$. Then $x^2 = (\alpha\alpha - a \bullet a) + (\alpha a + \alpha a + a \times a) = \alpha^2 - a \bullet a + 2\alpha a$, proving (i), (ii) and (iii). Now $x^2 = 1$ if and only if $a = 0$ and $\alpha^2 = 1$. Since $|1| = 1$, -1 is the only element of order 2 in $\mathbb{H}^\times$. Finally $|x| = 4$ if and only if $x^2 = -1$ if and only if $\nu(a) = 1$ and $\alpha = 0$. □

Thus every imaginary quaternion $a \in \mathbb{H}_0$ of norm 1 is an imaginary unit. Imaginary units form a 2-sphere $S^2 \subseteq \mathbb{H}_0$. Each imaginary unit $q \in S^2$ defines a homomorphism $\mathbb{C} \to \mathbb{H}$, $\alpha + \beta i \mapsto \alpha + \beta q$. Thus, in a strange interplay between Algebra and Geometry the set of all homomorphisms from $\mathbb{C}$ to $\mathbb{H}$ is a 2-sphere.

26.5 Hopf fibration

Hopf fibration has been described in Vista Section 14.5. Before we give a simpler description of it, we need to understand 3D-rotations. Let R^x_β be the anticlockwise rotation by the angle β in the plane orthogonal to x:



Lemma 26.10 *If $a = \cos\theta + x\sin\theta$ for some imaginary unit x then $R^x_{2\theta}(w) = awa^{-1}$ for each $w \in \mathbb{H}_0$.*

PROOF: Choose $y, z \in \mathbb{H}_0$ so that x, y, z is a positive oriented orthonormal basis. From Theorem 26.2, it follows that $x^2 = y^2 = z^2 = -1$, $xy = -yx = z$, $yz = -zy = x$ and $zx = -xz = y$.

It suffices to check the proposition on the basis because both parts of the equality $R^x_{2\theta}(w) = awa^{-1}$ are results of linear maps applied to w. Notice that $a^{-1} = \cos\theta - x\sin\theta$. Let us calculate. First, $axa^{-1} = xaa^{-1} = x = R^x_{2\theta}(x)$. Then $aya^{-1} = (\cos\theta + x\sin\theta)y(\cos\theta - x\sin\theta) = (y\cos\theta + z\sin\theta)(\cos\theta - x\sin\theta) = ((\cos\theta)^2 - (\sin\theta)^2)y + (2\cos\theta\sin\theta)z = y\cos 2\theta + z\sin 2\theta = R^x_{2\theta}(y)$ and finally $aza^{-1} = (\cos\theta + x\sin\theta)z(\cos\theta - x\sin\theta) = (z\cos\theta - y\sin\theta)(\cos\theta - x\sin\theta) = ((\cos\theta)^2 - (\sin\theta)^2)z - (2\cos\theta\sin\theta)y = z\cos 2\theta - y\sin 2\theta = R^x_{2\theta}(z)$. □

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: $g \cdot x = gxg^{-1}$. It is well-defined since S^2 is the set of elements of order 4 in $\mathbb{H}^\times$ and $|x| = |gxg^{-1}|$.

Theorem 26.11 *The $U(\mathbb{H})$-set S^2 has one orbit. The stabiliser of $x \in S^2$ is $U(\mathbb{H}) \cup \mathbb{R}(x)$.*

PROOF: If $x, y \in S^2$ then $R^z_{2\theta}(x) = y$ where $z \in \mathbb{H}_0$ is any unit vector orthogonal to both x and y and 2θ is the angle between x and y. By Lemma 26.10, $a \cdot x = axa^{-1} = y$ where $a = \cos\theta + x \sin\theta \in S^3 = U(\mathbb{H})$. Thus, the $U(\mathbb{H})$-set S^2 has one orbit.

To compute the stabiliser of $x \in S^2$, observe that an arbitrary element $a \in U(\mathbb{H})$ can be written as $a = \cos\theta + y \sin\theta$ where $y \in S^2$. By Lemma 26.10, $a \in \mathrm{Stab}(x)$ if and only if $a \cdot x = R^y_{2\theta}(x) = x$. For this to happen we need x and y to be parallel (then $y = \pm x$ and $a \in U(\mathbb{H}) \cup \mathbb{R}(x)$) or $2\theta = 2n\pi$ for some $n \in \mathbb{Z}$ (then $\theta = n\pi$ and $a = \cos n\pi + y \sin n\pi = \pm 1$. □

Geometrically, the stabiliser $U(\mathbb{H}) \cup \mathbb{R}(q)$ is the unit circle in $\mathbb{R}(x) = \mathbb{C}$. Choosing a particular quaternion $x \in S^2$, its orbit map $\beta_x : U(\mathbb{H}) \to S^2$, $\beta_x(g) = gxg^{-1}$ is the Hopf fibration $S^3 \to S^2$: the inverse image $\beta_x^{-1}(y)$ is a coset of the stabiliser $U(\mathbb{H}) \cup \mathbb{R}(x)$, i.e. geometrically a circle.

26.6 Exercises

(i) Prove that $C_{\mathbb{H}}(K) = \mathbb{R} + \mathbb{R}K = \mathbb{R}(K)$.

(ii) Prove that $Z(\mathbb{H}) = \mathbb{R}$.

(iii) Prove that $U(\mathbb{H}) = SU_2(\mathbb{C})$ as subgroups of $GL_2(\mathbb{C})$ (See Vista Section 14.5 for the definition of $SU_2(\mathbb{C})$.

(iv) Prove that $a \times b = (ab - ba)/2$ for all $a, b \in \mathbb{H}_0$.

(v) Using Exercise (iv), prove Jacobi's identity $a \times (b \times c) + b \times (c \times a) + c \times (a \times b) = 0$ for all $a, b, c \in \mathbb{H}_0$.

(vi) Prove Schwarz's inequality $||x|| \cdot ||y|| \geq |x \bullet y|$.

26.7 Vista: from multiplication tensors to superstring theory

We have successfully used a multiplication table to describe quaternionic multiplication. Pushing this through for a general algebra leads to tensors.

Let $(R, \mathbb{F})$ be an algebra. Pick elements $e_i \in R$ constituting a basis of R as a vector space. We define multiplication for basis elements

$$e_i \cdot e_j = \sum_k m^k_{i,j} e_k \tag{1}$$

for uniquely determined $m^k_{i,j} \in \mathbb{F}$. 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

$$(ab)c = \sum_{i,j,k} \alpha^i \beta^j \gamma^k (e_i \cdot e_i) \cdot e_k, \;\; a(bc) = \sum_{i,j,k} \alpha^i \beta^j \gamma^k e_i \cdot (e_i \cdot e_k).$$

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

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

Similarly,

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

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

$$\sum_s m^s_{i,j} m^t_{s,k} = \sum_s m^s_{j,k} m^t_{i,s} \tag{2}$$

for all possible i, j, k, and 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 cook up the structure constants 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 $y \in U$. Structure constants

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

define an $\mathbb{R}$-algebra structure on $\mathbb{R}^n$ via formula (1) as soon as this multiplication is associative and unitary. Equation (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

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

System (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.

27 Quaternions and spinors

Using quaternions, we describe 3D and 4D spinors.

27.1 Exponents of quaternions

In Algebra-I, you have studied matrix exponents. Since $\mathbb{H}$ is an $\mathbb{R}$-subalgebra of $M_2(\mathbb{C})$, one can formally define

$$e^a = \sum_{n=0}^{\infty} \frac{1}{n!} a^n = 1 + a + a^2/2! + \dots$$

While computation of matrix exponents require some subtle techniques such as Jordan forms or Lagrangian interpolation, quaternionic exponents are more straightforward.

Proposition 27.1 (Quaternionic Euler's formula) *If $a = \alpha + \beta x$ for $\alpha, \beta \in \mathbb{R}$ and some imaginary unit $x \in U(\mathbb{H}) \cap \mathbb{H}_0$ then $e^a = e^\alpha(\cos\beta + x \sin\beta)$.*

Proof: Since $a \in \mathbb{R}(x) \cong \mathbb{C}$, all partial sums $\sum_{n=0}^{K} a^n/n!$ belong to $\mathbb{R}(x) \cong \mathbb{C}$ and quaternionic Euler's formula follows from the usual Euler's formula for $\mathbb{R}(x)$. □

Since quaternions do not commute, $e^{a+b} \neq e^a e^b$, in general. On the other hand, if $ab = ba$ then both a and b lie in the same $\mathbb{R}(x)$ and $e^{a+b} = e^a e^b = e^b e^a \in \mathbb{R}(x)$ (cf. exercises (i) and (ii)). Since powers of a single element commute, the usual De Moivre's Formula holds for any $x \in U(\mathbb{H}) \cap \mathbb{H}_0$:

$$(\cos\beta + x \sin\beta)^n = \cos n\beta + x \sin n\beta \ .$$

The following proposition is immediate.

Proposition 27.2 *The element $e^{2\pi x/n}$ has order n in $\mathbb{H}^\times$ for any imaginary unit $x \in U(\mathbb{H}) \cap \mathbb{H}_0$.*

27.2 3D spinors

Let us play more with the action of $U(\mathbb{H})$ on $\mathbb{H}_0$ given by $a \cdot x = axa^{-1}$. In the last lecture we have realized that the orbit map of this action is a Hopf fibration. Now we would like to study the action map.

Theorem 27.3 *The action map $\phi : U(\mathbb{H}) \to SO(\mathbb{H}_0) \cong SO_3(\mathbb{R})$ is a surjective two-to-one group homomorphism.*

Proof: Apriori, the action map is a group homomorphism $\phi : U(\mathbb{H}) \to S(\mathbb{H}_0)$. If $a \in U(\mathbb{H})$ then $a = \cos\theta + x \sin\theta$ for some imaginary unit x and

$R^x_{2\theta}(w) = awa^{-1}$ for each $w \in \mathbb{H}_0$ by Lemma 26.10. Hence, the action map is a group homomorphism $\phi : U(\mathbb{H}) \to SO(\mathbb{H}_0)$.

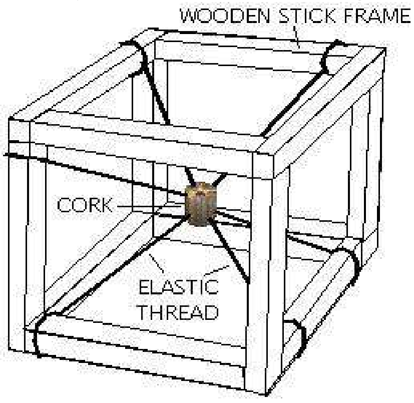
If $A \in SO(\mathbb{H}_0) \cong SO_3(\mathbb{R})$, the characteristic polynomial $\chi_A(z)$ have degree 3, so A has a real eigenvalue λ with an eigenvector v. Since $||Av|| = ||v||$, $|\lambda| = \pm 1$. Moreover, A preserves the orthogonal complement $v^\perp$ and $A|_{v^\perp}$ is orthogonal. If $\lambda = 1$ then $\det(A|_{v^\perp}) = 1$ and $A|_{v^\perp}$ is a rotation. Thus, A is a rotation R^v_θ by some angle θ. If $\lambda = -1$ then $\det(A|_{v^\perp}) = -1$ and $A|_{v^\perp}$ is a reflection. Thus, A has two more eigenvectors, including an eigenvector w with eigenvalue 1. Hence, A is a rotation R^w_π. It follows that $\phi : U(\mathbb{H}) \to SO(\mathbb{H}_0)$ is surjective.

Finally, $a = \cos\theta + x\sin\theta$ is the kernel of ϕ if and only if $R^x_{2\theta}(w) = awa^{-1} = w$ for each $w \in \mathbb{H}_0$ if and only if $2\theta = 2n\pi$ if and only if $\theta = n\pi$ if and only if $a = \pm 1$. □

Using the action homomorphism any $SO_3(\mathbb{R})$-set becomes a $U(\mathbb{H})$-set. The opposite is not true: a $U(\mathbb{H})$-set is an $SO_3(\mathbb{R})$-set if and only if -1 lies in the kernel of the action. *A 3D-spinor* is an element of a $U(\mathbb{H})$-set[25] which is not an $SO_3(\mathbb{R})$-set.

Examples. 1. Any quaternion $x \in \mathbb{H}$ is a spinor. The action is left multiplication in $\mathbb{H}$: $a \cdot x = ax$.

2. Physicists like illustrating the spinors using the following device.

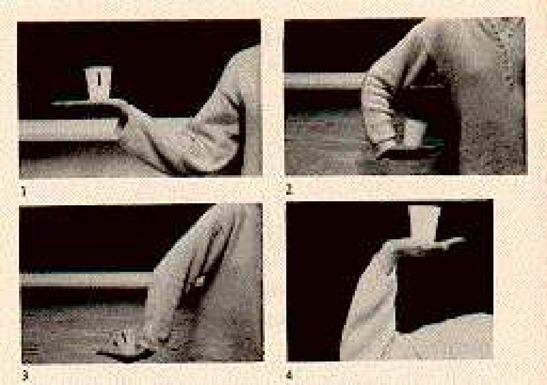


Let A be the set of all positions of this device such that the centre of the cork remains in the centre of the cube. We say that two positions are equivalent if one can be moved to another by adjusting elastic thread only. The quotient set $X = A/\sim$ is a $U(\mathbb{H})$-set: an element a acts on X by

[25] Wikipedia (http://en.wikipedia.org/wiki/Spinor) defines a spinor as an element of a representation, a $U(\mathbb{H})$-vector space rather than merely a $U(\mathbb{H})$-set. This difference is immaterial: a vector space is a set and any set is a subspace of a vector space, the space of formal linear combinations of the elements.

$\phi(a)$ rotating the cork. It is not a $SO_3(\mathbb{R})$-set because a 360-degree rotation tangles the thread. It is less obvious that a 720-degree rotation does not tangle the thread (see http://www.youtube.com/watch?v=O7wvWJ3-t44).

3. A variation of example 2 is Feynman dance:



If we call position 1 x then position 2 is $e^{\pi I/2} \cdot x$, position 3 is $e^{\pi I} \cdot x$ and position 4 is $e^{3\pi I/2} \cdot x$. Observe that the further 180-degrees rotation from position 4 returns everything into position 1, mathematically $e^{\pi I/2} \cdot (e^{3\pi I/2} \cdot x) = x$.

27.3 Binary dihedral group

We have seen that the natural homomorphism $\phi : U(\mathbb{H}) \to SO(\mathbb{H}_0)$ is two-to-one, i.e. the inverse image $\phi^{-1}(A)$ of each point consists of two elements. Any subgroup $G \leq SO_3(\mathbb{R})$ gets its binary analogue $\phi^{-1}(G)$. In particular, *the binary dihedral group* BD_{4n} is the subgroup of $U(\mathbb{H})$, generated by $J = e^{2\pi J/4}$ and $x = e^{\pi I/n}$. Notice that if $n = 4$ then $x = I$ and BD_8 is our old friend the quaternionic group Q_8.

Proposition 27.4 *BD_{4n} is a group of order $4n$ and $\phi(BD_{4n}) \cong D_{2n}$.*

PROOF: All we need to observe is how $\phi(J)$ and $\phi(x)$ act on $J - K$-plane. $\phi(x)$ acts via rotation $R_{2\pi/n}$, while $\phi(J)$ is the reflection fixing J and sending K to $-K$. Thus, $\phi(BD_{4n}) \cong D_{2n}$.

It remains to observe that $-1 = J^2 \in BD_{4n}$. Consequently, $BD_{4n} = \phi^{-1}(\phi(BD_{4n}))$ has order n. □

As $JxJ^{-1} = x^{-1}$ (see Exercise (iii)), $Jx = x^{-1}J$ and every element of BD_{4n} can be written as $x^k J^m$. Since $J^2 = -1 = x^n$, $BD_{4n} = \{x^k, x^k J \mid k \in \mathbb{Z}_n\}$ looking surprisingly similar to D_{4n}. Similarly to Section 5.3, we write the multiplication table of BD_{4n} using addition in $\mathbb{Z}_n$:

	x^l	$x^l J$
x^k	x^{k+l}	$x^{k+l}J$
$x^k J$	$x^{k-l}J$	x^{k-l+n}

Nevertheless, these groups are not isomorphic. For instance, $BD_4 \cong C_4$ while $D_4 \cong K_4$ or $BD_8 \cong Q_8$.

Proposition 27.5 *BD_{4n} is not isomorphic to D_{4n} for any $n \geq 1$.*

PROOF: -1 is the only order 2 element of BD_{4n}, while D_{4n} has at least 2 different reflections. □

Proposition 27.5 gives us the remaining group of order 12: BD_{12} cannot be isomorphic to A_4 either as A_4 has 3 elements of order 2.

27.4 4D spinors

Amazingly 4D-spinors can described in a similar way to 3D-spinors. The group $U(\mathbb{H}) \times U(\mathbb{H})$ on $\mathbb{H}$ by $(a, b) \cdot x = axb^{-1}$. Clearly, these are orthogonal transformations of $\mathbb{H}$.

Theorem 27.6 *The action map $\phi : U(\mathbb{H}) \times U(\mathbb{H}) \to SO(\mathbb{H}) \cong SO_4(\mathbb{R})$ is a surjective two-to-one group homomorphism.*

It is prudent at this stage to stop giving complete proofs. The main issue in this theorem is surjectivity. One can do it in a straightforward way but it is more elegant to argue using (unproved in this module) Coxeter's theorem that any orthogonal transformation in dimension n is a product of at most $n + 1$ reflections. *A reflection* of a euclidean space V is a linear transformation

$$S_x : V \to V, \quad S_x(y) = y - 2\frac{\langle x, y\rangle}{\langle x, x\rangle}x.$$

for some $x \in V \setminus \{0\}$. Reflection S_x fixes the plane $x^\perp$ while sending x to $-x$. In particular, it has determinant -1. Using Coxeter's theorem, elements of $SO(\mathbb{H})$ are products of two or four reflections.

Lemma 27.7 *If $x \in U(\mathbb{H})$ then $S_x(y) = -xy^*x$ for each $y \in \mathbb{H}$.*

One can establish this lemma by a direct calculation. It implies $S_xS_y = \phi(xy, yx)$, proving Theorem 27.6.

Now *4D-spinors* are elements of a $U(\mathbb{H}) \times U(\mathbb{H})$-set, which is not SO_4-set. In contrast to 3D-spinors, quaternions are not 4D-spinors because $(-1, -1)$ acts trivially on $\mathbb{H}$. We have no intention of giving meaningful examples of 4D-spinors. Instead, in preparation to the grand finale, we observe the structure of $SO(\mathbb{H})$. An element $x \in U(\mathbb{H})$ gives rise to *a left scroll* $L_x(y) = xy$ and *a right scroll* $R_x(y) = yx^{-1}$. Right and left scrolls commute: $L_x R_y = R_y L_x$. Finally, every element of $SO(\mathbb{H})$ is a composition of left and right scroll (surjectivity of ϕ in Theorem 27.6).

27.5 Regular polytopes

You probably know that there exists 5 regular polyhedrons (3D-polytopes), often called platonic solids. It is a drastic contrast with regular polygons (2D-polytopes) whom there are infinitely many. What is about regular nD-polytopes? The answer is surprising: if $n \geq 5$ there are 3 regular nD-polytopes, but there are 6 regular 4D-polytopes[26]. Our aim is to sketch construction of the higher dimensional regular polytopes.

Let us start with the three that exist in any dimension. n-hypercube is the easiest one to imagine: its 2^n vertices have coordinates $(\pm 1, \pm 1 \ldots, \pm 1)$. n-hypercube is the convex hull of them.

The next one is n-simplex: it is a convex hull of $n+1$ points. 2-simplex is a regular triangle and 3-simplex is a regular tetrahedron.

The last universal one is n-orthoplex. It is the dual[27] polyhedron of the n-cube. In another language, the $2n$ vertices of n-orthoplex are centres of $n-1$-dimensional faces of an n-cube. The n-orthoplex itself is the convex hull of its vertices. The 4-orthoplex (often called 16-cell) has a particularly nice structure: its vertices are elements of the group $BD_8 = Q_8$!

This gives us an idea take a finite group $G \subseteq U(\mathbb{H})$ and consider its convex hull. The resulting 4-polytope is bound to have a high degree of symmetry: left and right scrolls with respect to the elements of G are symmetries of the resulting polytope. Unfortunately, no other BD_{4n} gives a regular solid. It is instructive to realize why the hull of BD_{16} is not a 4-cube: 2D-faces of a 4-cube are squares while two of the 2-sides of the hull of BD_{16} are octagons.

The key is to find more finite subgroups. One gets them by lifting rotational symmetries of other platonic solids. The first platonic solid is tetrahedron. The group of its rotational symmetric has order 12. Its inverse image in $U(\mathbb{H})$ is called *binary tetrahedral group*:

$$BT =< e^{((I+J+K)\pi/3\sqrt{3})} = \frac{1+I+J+K}{2}, e^{((I-J+K)\pi/3\sqrt{3})}, I >$$

$$\cong < a, b, c \mid a^3 = b^3 = c^2 = abc >$$

[26] Wikipedia has numerous interlinked pages (http://en.wikipedia.org/wiki/Regular_polytope) with a wealth of information related to this lecture.

[27] $X^* = \{v \mid \forall a \in X \mid < a, v > \leq 1\}$

Observe that BT has 24 elements but it is not isomorphic to S_4 (again BT has only 1 element of degree 2). In fact, BT is isomorphic to $SL_2(\mathbb{Z}_3)$. It is more essential for us that the convex hull of BT is a new self-dual regular 4D-polytope, called 24-cell. Self-duality manifests in the fact that it has 24 vertices and 24 3D-faces.

Cube and octahedron are dual of each other. They have the same rotational symmetry group of order 24 (in fact it is isomorphic to S_4). Its inverse image in $U(\mathbb{H})$ is called *binary octahedral group*:

$$BO =< e^{(I\pi/4)} = \frac{1+I}{\sqrt{2}}, e^{((I+J+K)\pi/3\sqrt{3})} = \frac{1+I+J+K}{2}, I >$$

$$\cong < a, b, c \mid a^4 = b^3 = c^2 = abc >$$

This group of order 48 is unusual in many respects. In particular, it has no other notable description as a group. Its convex hull fails to be a regular solid but has some interesting properties.

We are left with icosahedron and dodecahedron, which are dual of each other. Their rotational symmetry group has order 60 (in fact it is isomorphic to S_5). Its inverse image in $U(\mathbb{H})$ is called *binary icosahedral group*:

$$BI =< e^{((I\cos\pi/3 + K\sin\pi/3)\pi/5)}, e^{((I\cos\pi/5 + K\sin\pi/5)\pi/3)}, I >$$

$$\cong < a, b, c \mid a^5 = b^3 = c^2 = abc >$$

This group of order 120 is isomorphic to $SL_2(\mathbb{Z}_5)$. The convex hull of BT is a new regular 4D-polytope, called 600-cell. Its 600 3D-faces are regular tetrahedra.

The remaining regular 4D-polytope is the dual of 600-cell. It is called 120-cell. Its 120 3D-faces are dodecahedra.

27.6 Exercises

(i) Prove that if $ab = ba$ for some $a, b \in \mathbb{H}$ then there exists an imaginary unit $x \in U(\mathbb{H}) \cap \mathbb{H}_0$ such that $a, b \in \mathbb{R}(x)$ (cf. Exercise 26.6(i)).
(ii) Prove that if $AB = BA$ for some $A, B \in M_n(\mathbb{C})$ then[28] $e^{A+B} = e^A e^B$.
(iii) Show that $JxJ^{-1} = x^{-1}$ if $x = e^{\pi I/n}$.
(iv) Prove Lemma 27.7.
(v) Using Lemma 27.7 prove that $S_x S_y = \phi(xy, yx)$.
(vi) Prove that the group of rotational symmetries of a tetrahedron is isomorphic to A_4.

[28] A general formula $e^{A+B} = F(e^A, e^B)$ is called Baker-Campbell-Hausdorff formula.

27.7 Vista

There is no vista for you now: your limit is the sky now.

On a more serious note, if you were thinking of writing an essay[29] on quaternions you, can still do it. You can expand the last section where no proofs were given. You can also discuss integer quaternions or 4-square theorem. Another alternative is to describe quaternions by applying Cayley process to complex numbers. You can apply Cayley process to quaternions to obtain octonions or so called Cayley numbers. They are still a division algebra, albeit nonassociative. Another direction is Clifford algebras and spinors in dimension n.

Certainly, you can write an essay on Physics or Geometry as we have not touched any of those issues.

[29] Consult *On quaternions and octonions* by Conway and Smith or *Regular Polytopes* by Coxeter.