

Foundations of finite group theory for a (future) computer

N. J. Wildberger
School of Mathematics
UNSW Sydney 2052

December 2, 2003

Prologue

Good morning, Daisy. In 2027, your Development Committee approached me with a curious proposal. You, a ‘dynamic AI system’, were soon to be launched, and to demonstrate your capability to discover new mathematics with a minimum of instruction, they wanted a beginner’s course in elementary group theory (meant for a computer, of course). You were going to absorb the material and immediately start doing research.

They claim that your capacity to comprehend written English, and familiarity with basic mathematics, is that of a good second year undergraduate. But your ability to assimilate and compute is astounding. After all, you trounced Deep Blue ten minutes after learning the rules for chess.

GenghisV, one of the main gurus on the project, explained what was required.

“This beauty is a whiz. Give her the main definitions, I/O specifications, and general directions—then we’ll let’er rip. Getting *her* to do *human* mathematics is not so much the point, since GAP and MAGMA already do that very well. Mathematics *by* a computer *for* a computer is the goal here.”

“That’s what we got with classical logic in one of her training sessions, where she devoured, almost instantaneously, all the exercises we had found, and started churning out new stuff.”

“What do you mean by *I/O specifications*? And why don’t you give her some group theory books?” I asked.

“Computers can’t easily work with abstract objects unless definitions are tied down with conventions for input and output,” he replied. “For example, the term ‘graphics file’ is vague, whereas ‘gif file’ or ‘jpeg file’ is precise. It’s a concept mathematicians should take more seriously.”

“You define a group to be a particular kind of multiplication table. So a computer will, by default, expect groups to be input and output as multiplication tables. When subsequently groups are discussed in terms of generators

and relations, or physical symmetries, or abstract operators, the computer gets confused. She looks for software to convert these forms into the one agreed upon in the definition, because she wants to *work* with objects, not just talk about them.”

“To put it another way, when you say ‘Let G be a group’, you are presumably initiating a thought experiment. But the subsequent development of that experiment will be, or ought to be, dependent on the *form* you have in mind for that unknown group. In the absence of a convention for this form, what does the phrase mean?”

“Please make sure your basic definitions are completely concrete, that is, understandable by a computer. But don’t worry about programming her, or organizing the subject in some kind of computer style.”

“In fact, forget about the way us AI systems work. Daisy programs herself. Arranges her internal structures in a spooky way which even we don’t understand, and is *smarter* than you can probably even imagine. Just explain to her the most important ideas, as you see them, and let her discover the rest.”

“And keep the following in mind. An hour after you teach *her* group theory, she’ll be teaching *you* group theory.”

Overview

So I took the job, and the result is this object-oriented course. May I begin with a brief overview, even though it won’t make a lot of sense till you have absorbed the terms and perused the literature? (It may help human readers at least).

The usual introduction to group theory starts out with the main definitions and some examples, typically the symmetric groups S_n , groups arising from symmetries of familiar two and three dimensional objects, and groups of matrices. It then goes on to a discussion of subgroups, Lagrange’s theorem, homomorphisms and quotient groups. This is followed by material on conjugacy classes, actions, generators and relations, and solvability. The course often ends with the Sylow theorems.

In a second course, or perhaps a related course in linear algebra, there is a treatment of the classification of finite abelian groups and duality, and the extension of these ideas to the non-commutative setting, involving character theory and representations. The latter subject is quite important in applications.

This course is unorthodox. The order of topics is dramatically different from the above, there are very few examples, and the treatment of many areas is non-standard, even heretical. Some of the usual material is not included.

The order of topics is different because I want to address right away the two problems which I feel are at the heart of the subject, which are: ‘How do you tell if two given groups are *isomorphic*?’ and ‘How do you find the *character table* of a given group?’ I want you thinking about these issues as soon as possible.

There are very few examples because you are in a much better position to generate them than I am. Most of the groups I know are of a particular geometric

or algebraic kind, and really rather unrepresentative. This reflects the human inability to process large amounts of information unless it is presented to us geometrically (that is, visually). Not having such a limitation, you should find it relatively easy to generate explicitly millions, even billions, of groups, and subsequently perform all manners of empirical investigations on them.

The treatment is non-standard because I am influenced by two theories which shed a lot of light on group theory. One is the theory of *multisets*, as expounded in [W1]. The other is the theory of *hypergroups*, which developed in the 1970's and provides a unified arena to investigate objects which have been studied under a plethora of different names. These include generalized translation operators, pseudo-groups, Hecke algebras, hypercomplex systems, paragroups, superselection sectors, Bose-Mesner algebras, Racah-Wigner algebras, centralizer algebras, table algebras, association schemes, and fusion rules of conformal field theories. For an introduction and explicit references, see [BI], [BH], [W3] and [OW].

I will show that with the right attitude towards multisets, hypergroup theoretic ideas can be introduced into group theory in a direct and elementary way. This allows us to get to the heart of the subject even in a first course, without resorting to group algebras.

Finally a word or two about *programs*. To me, a program is a finite collection of explicit instructions that takes an input of a specified kind and yields an output of a specified kind. A 'program' that does not always halt is like a 'theorem' which is not always true. Neither interests us. Obtaining bounds on running times of programs in terms of sizes of inputs is a valuable goal.

I will suggest that you develop particular programs, usually to count something or other. These Exercises and Problems are necessarily somewhat open ended, with the latter very difficult, at least for me.

Definitions, specifications and examples

Let G be a finite set of specified mathematical objects. That means that G is given to us, either explicitly, as in the ordered set $G_1 = \{1, 2, 3, 4\}$, or the (unordered) set $G_2 = \{\square, \triangle, \nabla\}$, or indirectly via a program. Clearly both of us could write a program to list the elements of

$$G_3 = \{n \mid n = 1, 2, \dots, 10^{100}\}$$

while I would have no idea how to proceed with

$$G_4 = \{n \in \{5, 6, \dots, 10^{10}\} \mid \exists k, l \in \{5, 6, \dots\}, n^5 k^2 - n l^8 = k^7 + l^3 + 1\}$$

so to me the latter has only been *described*, not *specified*.

A **multiplication program** on G is a program that inputs ordered pairs $[x, y]$ from G and outputs a single element from G , denoted either by $x \cdot y$ or xy . A multiplication program on G is **associative** if $(xy)z = x(yz)$ for all $x, y, z \in G$, **commutative** if $xy = yx$ for all $x, y \in G$, and has an **identity** if

there exists a distinguished element e of G such that $ex = xe = x$ for all $x \in G$. If a multiplicative program on G has an identity e , then it also has **inverses** if for each element $x \in G$ there exists an element $y \in G$ with $xy = yx = e$.

If G has an associative multiplication program, then if an identity exists, it is unique, and if in addition inverses exist, they are also unique. An associative multiplication program on G which has an identity and inverses is called a **group**. We say simply that ' G is a group'. If the multiplication program of a group G is commutative, then G is a **commutative group**. The **order** of a group G is the number of elements of G , denoted $|G|$.

To *specify* a group G , we should specify both the underlying set G and the multiplication program on G . This may be done directly, by listing in some fashion all the elements of G and giving an explicit table for the multiplication program, or indirectly, by providing programs that will output the elements of G and the results of multiplications.

Example 1 Let $G = \{1, 2, 3, 4\}$ with multiplication program given by the following table, where by convention the element in row i and column j is the group element $i \cdot j$.

$i \cdot j$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

This is an example of a commutative group which has been directly specified.

Example 2 Let $G = \{n \mid n = 1, 2, \dots, 10^{100}\}$ with multiplication program given by the formula

$$i \cdot j = i + j - 1 \pmod{10^{100}}.$$

This is another example of a commutative group. It has been indirectly specified by a program.

Example 3 Let S_n be the set of permutations of $\{1, 2, \dots, n\}$, with a typical permutation of the form $\sigma = [\sigma(1) \sigma(2) \dots \sigma(n)]$, the identity $e = [12 \dots n]$, and the multiplication defined by composition

$$(\sigma_1 \cdot \sigma_2)(k) = \sigma_1(\sigma_2(k)).$$

This definition hovers between a description and a specification, since a modicum of programming skill, but not much more, is required to list all $n!$ elements and the multiplication program explicitly for any given n .

Example 4 Let $G = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ with multiplication table

$i \cdot j$	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	4	3	12	10	11	9	8	6	7	5
3	3	4	1	2	8	11	10	5	12	7	6	9
4	4	3	2	1	9	7	6	12	5	11	10	8
5	5	9	12	8	6	1	3	10	11	4	2	7
6	6	11	7	10	1	5	12	4	2	8	9	3
7	7	10	6	11	4	9	8	1	3	12	5	2
8	8	12	9	5	11	3	1	7	6	2	4	10
9	9	5	8	12	7	4	2	11	10	1	3	6
10	10	7	11	6	2	12	5	3	1	9	8	4
11	11	6	10	7	3	8	9	2	4	5	12	1
12	12	8	5	9	10	2	4	6	7	3	1	11

This is a directly specified non-commutative group. It is usually referred to in the literature as A_4 , the set of even permutations of a 4-set. The particular multiplication table above comes from listing these permutations in the following order.

$$[1234], [2143], [3412], [4321], [2314], [3124], \\ [2431], [4132], [3241], [4213], [1342], [1423].$$

For each x in a group G we denote its inverse by x^{-1} . Associativity further implies that for any integer n , x^n is well defined, where

$$\begin{aligned} x^0 &= e \\ x^n &= xx \cdots x \text{ (} n \text{ times) if } n > 0 \\ x^n &= x^{-1}x^{-1} \cdots x^{-1} \text{ (} m \text{ times) if } n = -m < 0. \end{aligned}$$

For elements x, y of a group G , define the element xyx^{-1} to be the **conjugate** of x by y . A subset C of G of the form $\{xyx^{-1} \mid y \in G\}$ is called a **conjugacy class**. The conjugacy classes form a partition of G .

A non-empty subset $H \subseteq G$ with the property that $xy \in H$ and $x^{-1} \in H$ for all $x, y \in H$ is a **subgroup** of G . For finite groups, which is all we deal with here, the first of these conditions implies the second. A subgroup H which is a union of conjugacy classes is a **normal** subgroup. A group G which contains no normal subgroups except for $\{e\}$ and G itself is **simple**.

A group G is **cyclic** if there is an element x in G such that every element has the form x^n for some integer n . In such a case x is called a **generator** for G . Cyclic groups are necessarily commutative. A subset S of a group G **generates** G if every element of G is a product of elements of S . A group is a **p -group** for some prime p if $|G|$ is a power of p .

Having established all this terminology, it is time for our first exercise.

Exercise 1 Write a program which determines if a specified multiplication program is a group, and subsequently checks if this group is commutative.

Implicit in this exercise are some interesting issues. How many checks are required to verify associativity in an arbitrary multiplication program? More generally, how much *information* is there in the multiplication program of a group? How much information is required to determine commutativity? The following result, an extension of Cayley's theorem, may help with these kinds of questions. It is surely known, but perhaps not well-known.

Theorem 1 *An $n \times n$ multiplication table with an identity on a set G is a group if and only if its rows form a subgroup of the group of permutations of G .*

Proof. Suppose, by possibly relabelling the elements, that $G = \{1, 2, \dots, n\}$. Then the group of permutations of G is S_n . Let σ_i denote the i -th row of the multiplication table, so that $\sigma_i[j] = k$ if and only if $i \cdot j = k$.

Suppose that G is a group. Since $i \cdot j = i \cdot k$ implies that $j = k$, each row σ_i contains each element of G exactly once, so is an element of S_n . We thus write $\sigma_i[j] = \sigma_i(j)$ as the effect of the bijection σ_i on the element j . For two rows σ_i and σ_j we compute the product in S_n as follows

$$(\sigma_i \cdot \sigma_j)(k) = \sigma_i(\sigma_j(k)) = \sigma_i(j \cdot k) = i \cdot (j \cdot k) = (i \cdot j) \cdot k = \sigma_{i \cdot j}(k)$$

for arbitrary k which shows that the product of two rows is a row. It follows that the rows form a subgroup of S_n .

Conversely suppose that the rows of the multiplication table for G form a subgroup of S_n and that 1 is the identity. We first check associativity. For fixed i and j and variable k ,

$$i \cdot (j \cdot k) = \sigma_i(\sigma_j(k)) = (\sigma_i \cdot \sigma_j)(k) = \sigma_{i \times j}(k) = (i \times j) \cdot k$$

for some element $i \times j$ of G . To show that $i \times j = i \cdot j$, let $k = 1$. To check inverses, for every i the row σ_i contains 1 so there is some element j such that $i \cdot j = 1$. There is then also an element k such that $j \cdot k = 1$, and so $1 = (j \cdot (i \cdot j)) \cdot k = (j \cdot i) \cdot (j \cdot k) = j \cdot i$. Thus i has inverse j . ■

There are some common subgroups of a group G that occur frequently. The **center** of G is the normal subgroup defined by

$$Z = \{x \in G \mid xy = yx \ \forall y \in G\}.$$

The **commutator** subgroup of G is the smallest subgroup containing all **commutators** of the form $xyx^{-1}y^{-1}$. Others can be found in standard texts.

Exercise 2 *Write programs that determine the center, the commutator subgroup, and other important subgroups of a group G .*

Let G and H be groups with identity elements e_G and e_H respectively. The product $G \times H$ is a group with identity element $[e_G, e_H]$ and multiplication

$$[x_1, y_1][x_2, y_2] = [x_1x_2, y_1y_2].$$

Isomorphism, Classification and Invariants

Two groups G and H are **isomorphic** if there exists a bijection $\sigma : G \rightarrow H$ such that

$$\begin{aligned}\sigma(xy) &= \sigma(x)\sigma(y) \\ \sigma(x^{-1}) &= \sigma(x)^{-1}\end{aligned}$$

for all $x, y \in G$, in which case we write $G \simeq H$. The bijection σ will typically be a program.

Here is the first—and perhaps most fundamental—problem in the subject.

Problem 1 Write a program which determines if two given groups G and H are isomorphic.

Classical mathematics manages to generally finesse this issue, by somehow assuming that we can theoretically identify isomorphic objects without prescribing how. It also gets into logical difficulties, rarely acknowledged, by discussion of ‘isomorphism classes’.

There *is* a reasonably simple program that accomplishes the task—just run through all the possible bijections between two groups by brute force and check if any is an isomorphism. There are $n!$ possibly different multiplication programs on a group G of order n , so this is hopelessly inefficient in general.

Therefore an important goal is to develop tools for distinguishing groups. Somewhat informally, an *invariant* is a program that inputs a group and outputs a ‘simpler’, or at least ‘smaller’, mathematical object with the property that isomorphic groups yield identical, or isomorphic, outputs.

There are three families of invariants which arise in a first course—the *order* invariants, the *central* invariants, and the *subgroup* invariants. These will be among our primary tools for studying group theory. Please keep in mind that these are generally going to be programs.

To make some initial contact with the isomorphism problem, let’s suppose that $G = \{1, 2, \dots, n\}$. The multiplication program of G yields an $n \times n$ array, or matrix, whose element in row i and column j is the group element $i \cdot j$. We can equivalently encode this data in the list

$$L = [1 \cdot 1, 1 \cdot 2, \dots, 1 \cdot n, 2 \cdot 1, 2 \cdot 2, \dots, 2 \cdot n, \dots, n \cdot 1, n \cdot 2, \dots, n \cdot n].$$

The objects in L are the numbers $1, 2, \dots, n$, each with multiplicity n . Permutations of the labels for the elements of G will yield generally different lists. Of all such lists, there is exactly one which is minimal in the lexicographical ordering of lists of natural numbers, we call it the **minimal list** of G . This is a canonical invariant of a group G which ‘solves’ the isomorphism problem: two groups are isomorphic if and only if they have the same minimal list. However, finding it seems impractical.

One other important and natural problem is that of *classification*—how do we systematically organize the zoo of groups? Clearly the problem of identifying

isomorphic groups needs to be addressed first, since without it classification becomes far too unwieldy. A simple-minded approach is to list all the groups G of a given order by arranging their minimal lists in increasing (or decreasing) lexicographical order.

Problem 2 Write a program that inputs n and outputs, in some systematic fashion (for example, by the order described above), a complete list, up to isomorphism, of groups G of order n .

Problem 3 Find a multiplication program for each simple group described in the Atlas of Finite Simple Groups [CCNPW].

Remark 1 I should mention that there are a lot of p -groups. For example, up to isomorphism there are roughly 50 billion groups of order less than 1030, and more than 95% of these are groups of order 1024.

Multisets from groups

The next definitions are highly non-standard (be warned!) but are indispensable in this treatment of the subject. Our purpose is develop a language for efficiently compressing the information content of a multiplication table into significantly smaller tables—thus yielding invariants. There will be two basic ways of doing this, by either considering central analysis—the study of conjugacy classes and their algebraic structure, or subgroup analysis—the study of the relationship between a group G and a subgroup H .

First we need just a quick review of positive rational multisets (see [W1]). A **multiset** is an unordered collection of mathematical objects, with repetitions allowed, such as $A = [1_1_2]$ or $B = [3_3]$. Note the convention of square brackets, and the use of spaces, not commas, to separate elements. Square brackets with commas denote lists, as in computer science.

We say A is a 3-multiset, since $|A| = 3$, whereas B is a 2-multiset. Besides the (usual) operations of \cup and \cap , we may also **add** two multisets, by simply combining all elements of both. This allows us to give meaning to expressions like

$$\begin{aligned} 2A &= A + A = 4[1] + 2[2] \\ 3A + 2B &= 6[1] + 3[2] + 2[3]. \end{aligned}$$

More generally we allow rational combinations like $\frac{3}{4}A + \frac{1}{4}B$, which is a 1-multiset. We may also form the direct product $A \times B$ by the rule

$$A \times B = [[a, b] \mid a \in A, b \in B].$$

In the example

$$A \times B = [[1, 3] _ [1, 3] _ [1, 3] _ [1, 3] _ [2, 3] _ [2, 3]].$$

We say A is **from** B , denoted by $A \subseteq B$, if for any object x

$$m_A(x) > 0 \Rightarrow m_B(x) > 0$$

where $m_A(x)$ is the multiplicity of the object x in the multiset A .

If A and B are multisets from a group G , in other words if $A \subseteq G$ and $B \subseteq G$, then define the multisets

$$\begin{aligned} A^{-1} &= [a^{-1} \mid a \in A] \\ AB &= [ab \mid [a, b] \in A \times B]. \end{aligned}$$

In this latter definition of the **product** AB , (not to be confused with the direct product $A \times B$ defined above), we must consider *all* possible products ab with repetitions included. Note that this generally yields a multiset even if A and B are subsets of G , so that AB has here a *different meaning* than in almost all texts in the subject! We see that if A and B are multisets from a group G , then

$$|AB| = |A||B|.$$

It follows that the product of any two 1-multisets from a group G is itself a 1-multiset. That means that 1-multisets act somewhat like ‘generalized group elements’. In special cases the multiplication structure of appropriately chosen 1-multisets forms a useful invariant of a group which is often a key to further study.

An obvious way of creating a 1-multiset from a group G is to take a (non-empty) positive multiset $S \subseteq G$ and form the **associated 1-multiset**

$$s = \frac{S}{|S|}.$$

This will be a convention—general multisets denoted by capitals, and the associated 1-multisets denoted by the corresponding small letter.

Special cases of the product of multisets deserve mention. For $x \in G$ and A a multiset from G ,

$$\{x\}A = [xa \mid a \in A]$$

is the **left translate** of A by x , and

$$A\{x\} = [ax \mid a \in A]$$

is the **right translate** of A by x .

Example 5 For the group $G = A_4$ defined in Example 4, let $A = [2_3]$ and $B = [6_10_11]$. Then

$$\begin{aligned} A^{-1} &= [2_3] = A \\ B^{-1} &= [5_9_12] \\ AB &= [6_6_7_7_10_11] \\ BA &= [6_7_7_10_11_11] \end{aligned}$$

Order invariants

The main **order invariants** are the **order** of G , namely $|G|$, and the **order multiset** of G defined by

$$\text{ord}(G) = [\text{ord}(x) \mid x \in G]$$

where $\text{ord}(x)$ is the least nonzero natural number n such that $x^n = e$. Clearly if two groups are isomorphic then their orders and order multisets must agree.

Exercise 3 Write a program which outputs the order multiset of a group G .

There are secondary order invariants which one may define, which I have not seen studied. Given x and y in a group G , an ordered pair of integers $[n, m]$ such that $x^n = y^m$ may be called a **period pair** for $[x, y]$. Period pairs for $[x, y]$ form an integral lattice and include the vectors $[\text{ord}(x), 0]$ and $[0, \text{ord}(y)]$. One may associate to this some invariants, the simplest of which is the area $a(x, y)$ of a fundamental domain. Define the **area multiset** of G by

$$a(G) = [a(x, y) \mid x, y \in G].$$

Similarly for a triple of elements x, y, z we can consider **period triples** $[n, m, l]$ satisfying $x^n = y^m = z^l$, an associated **volume multiset** and so on.

For any element x in a group G , the subgroup $\{x^k \mid k = 1, 2, \dots, \text{ord}(x)\}$ is called the **cyclic subgroup** generated by x . Any subgroup of a cyclic group is also cyclic. The set of cyclic subgroups of a group G is a poset under inclusion, which we call the **cyclic subgroup poset** of G . Clearly the period lattice for x and y are closely related to the cyclic subgroups generated by x and y .

More generally we must be attuned to the possibility of counting something at all times in this subject. To this effect, multisets play an important organizational role. For another example, if the number of elements that commute with an element x is $c(x)$ then we may study the multiset

$$[c(x) \mid x \in G].$$

You will be able to define and study many more such order invariants as you proceed with your investigations.

Conjugacy classes and the class hypergroup

Now we come to *central analysis* on a group G . Let C_i be a conjugacy class of G . Then the associated **1-class** is the 1-multiset

$$c_i = \frac{C_i}{|C_i|}.$$

A multiset S from G with the property that $\{x\}S\{x^{-1}\} = S$ for all $x \in G$ will be called **G -invariant**, or **central**. Denoting the conjugacy classes by

$C_0 = \{e\}, C_1, \dots, C_n$, any central multiset is a linear combination of them in the multiset sense, so any central 1-multiset s is a combination

$$s = \sum_{i=0}^n r_i c_i$$

where $r_i \geq 0$ and $\sum_{i=0}^n r_i = 1$.

Since the product of central multisets is central, for each i and j there are positive rational numbers n_{ij}^k summing to 1 such that

$$c_i c_j = \sum_{k=0}^n n_{ij}^k c_k.$$

The coefficient n_{ij}^k is the probability that the product xy is in C_k if x is in C_i and y is in C_j .

The multiplication $c_i \cdot c_j = c_i c_j$ of 1-classes is associative, has identity c_0 , and has a partial notion of inverse: for every c_i there is a unique $c_i^* = c_{i^*}$ with the property that $c_i c_i^*$ contains a non-zero multiple of c_0 , corresponding to the conjugacy class of inverse elements of c_i . We require that the map $c_i \rightarrow c_i^*$ be an involution. This defines a (finite) **hypergroup**.

In terms of the coefficients n_{ij}^k and the map $i \rightarrow i^*$ the definition amounts to the following conditions.

1. $\sum_{k=0}^n n_{ij}^k = 1 \quad \forall i, j$
2. $n_{ij}^k \geq 0 \quad \forall i, j$
3. $\sum_{l=0}^n n_{ij}^l n_{lk}^m = \sum_{l=0}^n n_{il}^m n_{jk}^l \quad \forall i, j, k, m$
4. $n_{0i}^k = n_{i0}^k = \delta_{ik} \quad \forall i, k$
5. $n_{ij}^0 > 0 \Leftrightarrow j = i^* \quad \forall i, j$
6. $n_{ij}^k = n_{j^* i^*}^k \quad \forall i, j, k$

The set

$$K(G) = \{c_0, c_1, \dots, c_n\}$$

with the multiplication and involution defined above is the **class hypergroup** of G .

Why would we consider this seemingly complicated object? There are two good reasons. First of all $K(G)$ is generally much smaller than G , especially if G is highly non-commutative. The monster group M , largest of the sporadic simple groups, has roughly 8×10^{53} elements. Its class hypergroup $K(M)$ has 194 elements, and so its multiplication program contains at most 194^3 rational numbers.

Furthermore, $K(G)$ is always *commutative*, meaning that $c_i c_j = c_j c_i$ for all i, j . Thus classical tools of harmonic analysis, such as characters, the Fourier

transform, Plancherel theorems, Parseval identities, and so on are available. Commutative hypergroups provide us with a powerful extension of abelian harmonic analysis with applications far beyond group theory; to physics, number theory, combinatorics and functional analysis (see [BH],[W2] and the references therein).

Example 6 Let $G = A_4$ with conjugacy classes

$$\begin{aligned} C_0 &= \{[1234]\} \\ C_1 &= \{[2143] _ [3412] _ [4321]\} \\ C_2 &= \{[2314] _ [4132] _ [3241] _ [1423]\} \\ C_3 &= \{[3124] _ [2431] _ [4213] _ [1342]\}. \end{aligned}$$

The multiplication program for the class hypergroup

$$K(A_4) = \{c_0, c_1, c_2, c_3\}$$

is given by the table

$c_i \cdot c_j$	c_0	c_1	c_2	c_3
c_0	c_0	c_1	c_2	c_3
c_1	c_1	$\frac{1}{3}c_0 + \frac{2}{3}c_1$	c_2	c_3
c_2	c_2	c_2	c_3	$\frac{1}{4}c_0 + \frac{3}{4}c_1$
c_3	c_3	c_3	$\frac{1}{4}c_0 + \frac{3}{4}c_1$	c_2

We can see that $c_i^* = c_i$ for all i (in such a case the hypergroup is called **Hermitian**.)

So determination of the 1-class structure constants n_{ij}^k is one of the first and most important tasks to be performed for any group G . Here is my favourite group theory problem.

Problem 4 Find a good formula for the 1-class structure constants for the symmetric group S_n .

Character tables

Let's now establish some further central invariants, especially the *character table* of a group. This latter forms the foundation for harmonic analysis on non-abelian groups, with applications to chemistry, physics, and other branches of mathematics, as well as to further development of the subject. Our presentation has its origins in the work of Frobenius [F] and Kawada [K].

Suppose that

$$K(G) = \{c_0, c_1, \dots, c_n\}$$

is the class hypergroup of a group G , with structure equations

$$c_i c_j = \sum_{k=0}^n n_{ij}^k c_k.$$

This can be viewed as a system of $(n + 1)^2$ rational equations in the variables c_i , with the property that the right hand side of each equation is a linear expression, and the left hand side is a quadratic product.

Perhaps the *fundamental computational problem* in the subject is the determination of all complex valued solutions to such a system. That is, we want to replace the variables c_i with complex numbers so that the equations still hold. Almost surely you already possess algorithms (well developed in MAPLE and MATHEMATICA) that will input a system of quadratic/linear equations, and in certain cases, find all solutions. Let's outline the basic idea.

First define a **character** of the commutative hypergroup above to be a complex valued function χ which satisfies

$$\chi(c_i)\chi(c_j) = \sum_{k=0}^n n_{ij}^k \chi(c_k) \quad \forall i, j.$$

There is always at least one character; the constant function

$$\chi_0(c_i) = 1,$$

and for any character χ we must have

$$\chi(c_0) = 1.$$

Example 7 *There are exactly four characters of the hypergroup $K(A_4)$, given by the rows of the following table C (here $\sigma = e^{2\pi i/3}$)*

$\chi_i(c_j)$	c_0	c_1	c_2	c_3
χ_0	1	1	1	1
χ_1	1	$-1/3$	0	0
χ_2	1	1	σ	σ^2
χ_3	1	1	σ^2	σ

It turns out that there are always exactly $(n + 1)$ characters of a finite commutative hypergroup $K = \{c_0, c_1, \dots, c_n\}$. We can find them as follows.

For each element $c_i \in K$, let M_i be the matrix of multiplication by c_i with respect to the ordered basis $\{c_0, c_1, \dots, c_n\}$. The matrices M_i satisfy exactly the same multiplicative relations as the elements c_i , and in particular they mutually commute. Furthermore, they are linearly independent, since if $\sum_i z_i M_i = 0$ then multiplying $\sum_i z_i c_i$ by c_j^* and considering the resulting coefficients of c_0 yields $z_j = 0$.

The matrices M_i can be simultaneously diagonalized by some invertible matrix Q . That is,

$$QM_iQ^{-1} = D_i$$

for some diagonal matrices D_i . The diagonal entries of the matrices D_i are then the characters of K , that is we may define the **hypergroup character table** $C(i, j) = \chi_i(c_j) = D_j(i, i)$. In particular, there are exactly as many characters as conjugacy classes.

It is worth pointing out that in general only *one* of the matrices M_i is required. Suppose that M_1 happens to have distinct eigenvalues. If α_j is one of these, then replacing c_1 with α_j in the $n - 2$ equations for c_1c_2, \dots, c_1c_n yields a system of linear equations in c_2, \dots, c_n which has a unique solution up to a scalar. Substituting into the equation for c_1^2 yields an absolutely unique solution, so this gives us one character, or row of the character table. As α_j runs through the eigenvalues of M_1 , the rows so obtained constitute the full character table.

So the other equations, not involving c_1 , can be viewed as providing additional information to cover the case of eigenvalues of M_1 with multiplicity great than one.

Example 8 For $K(A_4)$, the matrices M_i are

$$\begin{array}{cccc} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 1/3 & 0 & 0 \\ 1 & 2/3 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 0 & 0 & 1/4 \\ 0 & 0 & 0 & 3/4 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} & \begin{bmatrix} 0 & 0 & 1/4 & 0 \\ 0 & 0 & 3/4 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \\ M_0 & M_1 & M_2 & M_3 \end{array}$$

and simultaneous diagonalization of these yields the table of Example 7.

The hypergroup character table C contains much useful information. Its columns furnish us with a *model* of the hypergroup K , in the sense that pointwise multiplication of columns obeys the same structure equations as does hypergroup multiplication, while the rows, being the characters, can also be multiplied pointwise to obtain what turns out (in the case of the class hypergroup of a group) to be a hypergroup structure in complete duality with K , called the **character hypergroup** and denoted $K(G^\wedge)$.

In the particular case when G is itself a commutative group of order n , so that $G = K(G)$, this procedure shows that both G and $G^\wedge = K(G^\wedge)$ are isomorphic to a subgroup of the n -fold product \mathbb{C}^n . In fact it is not hard to see that in this case all the entries of the character table must be n -th roots of unity, so G and G^\wedge are subgroups of products of cyclic groups. (From this one may deduce, with some more work (!) that both G and G^\wedge are themselves isomorphic to products of cyclic groups.)

Weights and orthogonality relations

The character table for a finite commutative hypergroup exhibits some remarkable orthogonality. To describe this, first define the **weight** $\omega(c_i)$ of an element c_i of a hypergroup K to be

$$\omega(c_i) = \frac{1}{n_{ii^*}^0},$$

which in the case of $K(G)$ is just the size of the associated conjugacy class C_i . Define the **weight** $\omega(K)$ of a hypergroup $K = \{c_0, c_1, \dots, c_n\}$ to be

$$\omega(K) = \sum_{i=0}^n \omega(c_i),$$

so that in our case $\omega(K(G)) = |G|$.

For any hypergroup K the rows of the character table, viewed as elements in \mathbb{C}^{n+1} , are orthogonal with respect to the usual Hermitian inner product modified by the weights $\omega(c_i)$, in other words by the inner product

$$\langle a, b \rangle = \frac{1}{\omega(K)} \sum_{i=0}^n a_i \bar{b}_i \omega(c_i),$$

while the columns are similarly orthogonal with respect to the dual weights $\omega(\chi_i)$ of $K(G^\wedge)$. The **weight list**

$$\omega_{K(G)} = [\omega(c_0), \dots, \omega(c_n)]$$

and the **dual weight list**

$$\omega_{K(G^\wedge)} = [\omega(\chi_0), \dots, \omega(\chi_n)]$$

are implicit in the character table, but the orthogonality relations suggest that it is useful to identify them explicitly as important invariants.

Calculating the following five central invariants of a group G is thus a primary task.

Problem 5 Write programs which determine the class hypergroup, the hypergroup character table, the character hypergroup, the weight list, and the dual weight list of a given group G .

Example 9 You may check that the character hypergroup $K(A_4^\wedge)$ has multiplication table

$\chi_i \cdot \chi_j$	χ_0	χ_1	χ_2	χ_3
χ_0	χ_0	χ_1	χ_2	χ_3
χ_1	χ_1	$\frac{1}{9}\chi_0 + \frac{2}{3}\chi_1 + \frac{1}{9}\chi_2 + \frac{1}{9}\chi_3$	χ_1	χ_1
χ_2	χ_2	χ_1	χ_3	χ_0
χ_3	χ_3	χ_1	χ_0	χ_2

and that the weight list is $\omega_{K(A_4)} = [1, 3, 4, 4]$ while the dual weight list is $\omega_{K(A_4^\wedge)} = [1, 9, 1, 1]$.

By multiplying each row χ_i of the hypergroup character table of the class hypergroup $K(G)$ by the square root of the dual weight $\omega(\chi_i)$ we obtain the **group character table** C' . In other words we define

$$X_i(C_j) = \chi_i(c_j) \sqrt{\omega(\chi_i)}$$

and let $C'(i, j) = X_i(C_j)$. The group character table has the advantage of often having many integral entries, but has the disadvantage of obscuring the symmetry between the class and character hypergroups. Its definition is usually left to a second course in group theory and traditionally involves the deeper notion of a *representation* of a group.

One of the advantages of the approach which we have sketched here is the introduction of character tables *without* representation theory, which was actually Frobenius' original point of view! Recall that the passage from the multiplication table to the character table as I have outlined it involves only counting and solving a quadratic/linear system of equations, or equivalently diagonalizing some matrices.

The weight list $\omega_{K(G)}$ is the list of sizes of the conjugacy classes, while the dual weight list $\omega_{K(G^\wedge)}$ has also the interpretation as the list of squares of the dimensions of the irreducible representations (which we have not defined here).

Example 10 Here is the group character table C' of A_4 .

$X_i(C_j)$	C_0	C_1	C_2	C_3
X_0	1	1	1	1
X_1	3	-1	0	0
X_2	1	1	σ	σ^2
X_3	1	1	σ^2	σ

The next problem is in principal straightforward, since the character tables for simple groups are clearly laid out in the Atlas [CCNPW].

Problem 6 Write multiplication programs for the class hypergroups and character hypergroups of all simple groups.

It is a consequence of the classification of simple groups that a simple group is determined by its group character table, and so by its hypergroup character table. The following fundamental problem probably requires some new insight for its resolution. (The pattern of circles on a simple group, introduced in the next section, might help in this regard.)

Problem 7 Write a program that constructs a simple group from its group or hypergroup character table.

Remark 2 The dual of an arbitrary commutative hypergroup is not always a hypergroup, as negative coefficients can occur. Nevertheless, by enlarging our view to include so-called signed hypergroups, there is a complete duality theory generalizing Pontryagin duality for finite commutative groups. This fact was discovered in the slightly different context of C -algebras by Kawada [K], see [W2] and [OW] for a modern treatment.

Cosets and subgroup analysis

Let's now introduce *subgroup analysis*. Let H be a subgroup of G . A multiset S from G with the property that $\{y\}S = S$ (respectively $S\{y\} = S$) for all $y \in H$ will be called H **left-invariant** (respectively **right-invariant**). A multiset S from G which is both H left-invariant and H right-invariant will be called H **bi-invariant**.

The subgroup H is itself H bi-invariant. For any $x \in G$, the sets $\{x\}H$ and $H\{x\}$ are H right-invariant and H left-invariant respectively and are called **left cosets** and **right cosets** of H respectively. The set of all left cosets of H forms a partition of G , as does the set of all right cosets of H of G . These two partitions of G are equal precisely when H is a normal subgroup of G . Since $|\{x\}H| = |H\{x\}| = |H|$, we deduce

Theorem 2 (Lagrange's Theorem) $|H|$ divides $|G|$ for any subgroup H of a group G .

For any $x \in G$ the multiset $H\{x\}H = [h_1xh_2 | h_1, h_2 \in H]$ is a **double coset** of H . It is H bi-invariant and is an $|H|^2$ -set. In contrast to left and right cosets, a double coset is generally not a set. *Note carefully that at this point our notation diverges from the standard usage of HxH as a set.*

Suppose that the distinct left cosets of H are $H = H_0, H_1, \dots, H_l$. Define the associated **left 1-cosets** by the rule

$$h_j = \frac{H_j}{|H_j|}$$

with $h = h_0$. Now define the **right quotient** of G by H to be

$$G/H = \{h_0, h_1, \dots, h_l\}.$$

Note that G/H is not defined to be a set of cosets, but rather a set of 1-cosets! Since H is a subgroup, we have

$$\begin{aligned} h^2 &= h \\ h^{-1} &= h. \end{aligned}$$

Furthermore, the product of H right-invariant 1-multisets is also an H right-invariant 1-multiset, so there exist rational numbers p_{ij}^k such that

$$h_i h_j = \sum_{k=0}^l p_{ij}^k h_k.$$

This is a product on G/H which shares some of the properties of a hypergroup, for example, it is associative and for fixed i and j the **right quotient structure constants** p_{ij}^k are probabilities. However in general h_0 is a right

identity, that is $h_i h_0 = h_i$ for all i , but not necessarily a left identity. There are inverses but they are not unique, and the product is generally not commutative. Nevertheless, the structure constants p_{ij}^k are computable invariants of the quotient G/H . So any right quotient G/H carries an algebraic structure.

The situation is entirely symmetrical when we interchange all lefts and rights in the above discussion and consider right cosets of H in G and the associated **left-quotient** $H\backslash G$.

In the special case when H is a normal subgroup of G , the left-invariant and right-invariant 1-cosets coincide, and the above product structures coincide and indeed form a group called the **quotient group** and denoted by either G/H or $H\backslash G$. In general the connection between the left-quotients and right-quotients is given by the inverse mapping $x \rightarrow x^{-1}$ that transforms left cosets to right cosets and vice-versa. So the right-quotient and left-quotient structure constants are essentially the same.

In fact there is a simpler and *more fundamental* invariant associated to a subgroup H of a group G which is a hypergroup. A 1-multiset of G of the form

$$a = \frac{H \{x\} H}{|H|^2}$$

will be called a **double 1-coset** of H in G . The double 1-cosets of H in G are either identical or disjoint, and we let

$$H\backslash G/H = \{a_0, a_1, \dots, a_r\}$$

denote the set of all double 1-cosets of H in G , with $a_0 = h_0 = H/|H|$. Then there are rational numbers q_{ij}^k , which again have an interpretation as probabilities, such that

$$a_i a_j = \sum_{k=0}^r q_{ij}^k a_k$$

which makes $H\backslash G/H$ into a bona fide hypergroup which we call the **double coset hypergroup** of H in G . In general $H\backslash G/H$ is not commutative; when it is, (G, H) is known as a **Gelfand pair**.

Example 11 Let $G = A_4$ and $K = \{1_2\}$. Then $K\backslash G/K = \{a_0, a_1, a_2, a_3\}$ where

$$\begin{aligned} a_0 &= \frac{1}{2} [1_2] & a_1 &= \frac{1}{2} [3_4] \\ a_2 &= \frac{1}{4} [5_8_9_12] & a_3 &= \frac{1}{4} [6_7_10_11] \end{aligned}$$

The multiplication table is

$a_i \cdot a_j$	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_2	a_3
a_2	a_2	a_2	a_3	$\frac{1}{2}a_0 + \frac{1}{2}a_1$
a_3	a_3	a_3	$\frac{1}{2}a_0 + \frac{1}{2}a_1$	a_2

This is obviously commutative, so (G, K) is a Gelfand pair. The character table is

$\chi_i(a_j)$	a_0	a_1	a_2	a_3
χ_0	1	1	1	1
χ_1	1	-1	0	0
χ_2	1	1	σ	σ^2
χ_3	1	1	σ^2	σ

The similarity with the group character table in this case is largely accidental.

Problem 8 Given a group G and a subgroup H , (write a program to) find the structure constants p_{ij}^k and q_{ij}^k above and determine if (G, H) is a Gelfand pair.

Circles: Translates of conjugacy classes

A translate of a conjugacy class in G will be called a **circle** (this is not a usual definition). More particularly, a translate of the i -th conjugacy class C_i will be called an i -**circle**. Since $\{x\}C_i = C_i\{x\}$ for any $x \in G$ and any conjugacy class C_i , it is unnecessary to specify left or right translate. We will say that the circle $\{x\}C_i$ has **colour** i and **centre** x , both of which may not be unique.

Example 12 Let

$$G = S_3 = \{[123], [213], [132], [321], [231], [312]\}$$

with conjugacy classes

$$\begin{aligned} C_0 &= \{[123]\} \\ C_1 &= \{[213] _ [132] _ [321]\} \\ C_2 &= \{[231] _ [312]\}. \end{aligned}$$

Then of course every element is a 0-circle trivially; furthermore

$$\{[123]\}C_1 = \{[231]\}C_1 = \{[312]\}C_1 = C_1$$

and

$$\{[213]\}C_1 = \{[132]\}C_1 = \{[321]\}C_1 = \{[123] _ [231] _ [312]\}$$

so there are only two 1-circles and their centres are not unique. There are six distinct 2-circles, each with a unique centre, namely

$$\begin{aligned} \{[123]\}C_2 &= \{[231] _ [312]\} \\ \{[231]\}C_2 &= \{[123] _ [312]\} \\ \{[312]\}C_2 &= \{[123] _ [231]\} \\ \{[213]\}C_2 &= \{[132] _ [321]\} \\ \{[321]\}C_2 &= \{[213] _ [132]\} \\ \{[132]\}C_2 &= \{[213] _ [321]\}. \end{aligned}$$

Example 13 For $G = A_4$ the class structure equations reveal that a circle may have more than one colour: C_2 and C_3 are translates of each other so each is both a 2-circle and a 3-circle.

Restricting to simple groups, the situation is much more regular than the above examples might lead us to suspect.

Theorem 3 Let G be a finite non-commutative simple group. Then every circle in G has a unique colour and a unique centre. Every point $x \in G$ lies on precisely $|C_i|$ i -circles, and so lies on a total of $|G|$ circles.

Proof. Let C_i, C_j be two distinct conjugacy classes of G . We first show that no translate of C_i can be simultaneously a translate of C_j . If $H_i = \{z \in G \mid \{z\}C_i = C_i\}$ then H_i is a subgroup of G and is normal. It cannot be all of G unless G is trivial, in which case there are not two distinct conjugacy classes. Thus $H_i = \{e\}$ since G is simple. Now suppose that $\{x\}C_i = \{y\}C_j$ for some $x, y \in G$, or equivalently that $\{z\}C_i = C_j$ for some z . Conjugating by $w \in G$, we see that $\{wzw^{-1}\}C_i = C_j$. But then $\{z^{-1}wzw^{-1}\}C_i = C_i$ and so by the previous remark $z^{-1}wzw^{-1} = e$. Since w is arbitrary, z is in the centre of G and so $z = e$. But this is impossible since C_i and C_j are distinct.

For the second claim, note that the statement is true for $x = e$ since the centers of the i -circles on which e lies are exactly the elements of the class C_i^* of inverses of the elements of C_i , which has $|C_i|$ elements. Since the family of i -circles is invariant under translation, every point $x \in G$ lies on precisely $|C_i|$ i -circles, and so on a total of $|G|$ circles. ■

Returning to a general group G , its circles are related to the structure constants n_{ij}^k of the class hypergroup $K(G) = \{c_0, c_1, \dots, c_n\}$.

Theorem 4 For any conjugacy classes C_i, C_j, C_k of G and $z \in C_i$,

$$|\{z\}C_j \cap C_k| = |C_j|n_{ij}^k.$$

Proof. Suppose that the product $C_i C_j$ contains C_k a total of N_{ij}^k times, necessarily an integer. Then since $c_i = C_i/|C_i|$,

$$\frac{N_{ij}^k |C_k|}{|C_i| |C_j|} = n_{ij}^k.$$

Of course $|\{z\}C_j \cap C_k| = |\{xzx^{-1}\}C_j \cap C_k|$ for any x , so that counting in different ways yields

$$|C_i| |\{z\}C_j \cap C_k| = N_{ij}^k |C_k|.$$

Combining, we get the required equality. ■

In particular we see that $|C_j|n_{ij}^k$ is always a positive integer, which in turn allows further deductions, such as the following.

Corollary 1 If C_i and C_j are conjugacy classes of G whose orders are relatively prime, then $C_i C_j$ is a multiple of a single conjugacy class.

Proof. In this case n_{ij}^k is both an integer and a probability for each k , so must be either 0 or 1. ■

Remark 3 *The pattern of circles on a group is an interesting geometrical object, closely connected to the subject of association schemes (see for example [BI]). If we could recover the circle pattern of a simple group from the character table, we could hope to recover G from its action, on the left and right, as symmetries of the circle pattern.*

Relations and isomorphism theorems

So far we have been focusing on individual groups, their conjugacy classes and their subgroups. Now we consider possible relations between two or more groups. The following treatment is more general than usual, though I leave most of the proofs to you.

If G and H are groups, then a subgroup R of the product group $G \times H$ will here be called a **group relation between G and H** . Note that the order of G and H matters; interchanging the order of all ordered pairs in R yields the **transpose group relation R^T** between H and G .

A **homomorphism** from a group G to a group H is a map $\varphi : G \rightarrow H$ satisfying for all $x, y \in G$

$$\varphi(xy) = \varphi(x)\varphi(y).$$

Perhaps you have already been pre-programmed to think of homomorphisms, not relations, as the natural objects of study in algebra. In that case, note that given a homomorphism φ from G to H we may define a group relation R between G and H by the rule

$$R = \{[x, \varphi(x)] \mid x \in G\}.$$

If R is a group relation between G and H , then define the **image** and the **transpose image** of R respectively by

$$\text{im}(R) = \{y \in H \mid [x, y] \in R \text{ for some } x \in G\}$$

$$\text{im}^T(R) = \{x \in G \mid [x, y] \in R \text{ for some } y \in H\}.$$

These are subgroups of H and G respectively. If both $\text{im}^T(R) = G$ and $\text{im}(R) = H$ then we define R to be **full**. The next problem is deep, and generalizes aspects of representation theory.

Problem 9 *Write a program that inputs an ordered pair of groups and finds all full group relations between them.*

If R is a group relation between G and H , then define the **kernel** and the **transpose kernel** of R respectively by

$$\ker(R) = \{x \in G \mid [x, e_H] \in R\}$$

$$\ker^T(R) = \{y \in H \mid [e_G, y] \in R\}$$

where e_H and e_G are the identities in H and G respectively. More generally, for any $x \in G$ and $y \in H$ define

$$\begin{aligned} R^y &= \{x \in G \mid [x, y] \in R\} \\ R_x &= \{y \in H \mid [x, y] \in R\} \end{aligned}$$

so that

$$\begin{aligned} \ker(R) &= R^{e_H} \\ \ker^T(R) &= R_{e_G}. \end{aligned}$$

Then R_x is both a left coset and a right coset of $\ker^T(R)$ for all $x \in \text{im}^T(R)$, and R^y is both a left coset and a right coset of $\ker(R)$ for all $y \in \text{im}(R)$, so that $\ker(R)$ and $\ker^T(R)$ are normal subgroups of $\text{im}^T(R)$ and $\text{im}(R)$ respectively.

Theorem 5 *If R is a group relation between groups G and H , then*

$$\text{im}^T(R) / \ker(R) \simeq \text{im}(R) / \ker^T(R).$$

Given a group relation R between groups G and H , we may associate to each $x \in \text{im}^T(R)$ the 1-multiset $r(x) = r_x = R_x / |R_x|$ in H . In that case, the homomorphism equation

$$r(xy) = r(x)r(y)$$

applies, showing that a group relation can be viewed as a (partially defined) homomorphism which is allowed to have 1-multisets as values.

If R is a group relation between G and H satisfying $\text{im}^T(R) = G$ and $\ker^T(R) = e_H$, then R determines a homomorphism φ from G to H by the rule

$$[x, \varphi(x)] \in R.$$

In this case the theorem reduces to

$$G / \ker(R) \simeq \text{im}(R).$$

Then R and R^T both determine homomorphisms if and only if R determines an isomorphism.

We consider a useful example. Suppose G is a group with normal subgroups K and L , which have associated 1-multisets k and l respectively. Define a group relation R between the groups G/K and G/L by the rule that $[\{a\}k, \{b\}l] \in R$ if and only if $\{a\}k \cap \{b\}l$ is non-empty.

Let's first check that this makes sense. Since K and L are normal, $\{a\}k = k\{a\}$ and $\{b\}l = l\{b\}$ for any $a, b \in G$. Thus if $x_1 \in \{a_1\}k \cap \{b_1\}l$ and $x_2 \in \{a_2\}k \cap \{b_2\}l$, then $x_1x_2 \in \{a_1\}k\{a_2\}k = \{a_1a_2\}kk = \{a_1a_2\}k$. Similarly $x_1x_2 \in \{b_1b_2\}l$; thus R is indeed a group relation.

Now $kl = lk$ because both are G -invariant, and so $(kl)^2 = kl$. This implies that kl is the associated 1-multiset to a normal subgroup M (which is usually denoted by KL in the literature) containing both K and L .

It is not hard to see that $\ker(R) = M/K$ and $\ker^T(R) = M/L$ so the above theorem yields the equation

$$\frac{G/K}{M/K} \simeq \frac{G/L}{M/L}.$$

In the special case when K is a subgroup of L (and so a normal subgroup of L), we get $M = L$ and the following isomorphism theorem.

Theorem 6

$$\frac{G/K}{L/K} \simeq G/L.$$

Problem 10 *Show that this theorem extends to general (non-normal) subgroups by developing a theory of quotients for the ‘hypergroup-like’ objects G/H .*

Acknowledgement 1 *I would like to thank Peter Donovan, Hendrik Grundling and David Harvey for useful comments and discussions.*

References

- [BI] E. Bannai and T. Ito, Algebraic combinatorics I—Association Schemes, Benjamin and Cummings, Menlo Park, 1984.
- [BH] W. R. Bloom and H. Heyer, Harmonic analysis of probability measures on hypergroups, de Gruyter Studies in Mathematics, Vol. 20, Walter de Gruyter, Berlin, 1995.
- [CCNPW] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, Atlas of Finite Groups, Clarendon Press, Oxford, 1985.
- [F] G. Frobenius, *Über Gruppencharaktere, Gesammelte Abhandlungen*, Vol. 111, Springer-Verlag, pp. 1–37.
- [K] Y. Kawada, *Über den Dualitätssatz der Charaktere nichtcommutativer Gruppen*, Proc. Phys. Math. Soc. Japan **24** (3) (1942), 97–109.
- [OW] N. Obata and N. J. Wildberger, *Generalized hypergroups and orthogonal polynomials*, Nagoya Math. J. **142** (1996), 67–93.
- [W1] N. J. Wildberger, A new look at multisets, preprint, 2003.
- [W2] N. J. Wildberger, *Duality and Entropy for finite commutative hypergroups and fusion rule algebras*, J. London Math. Soc. **56** (2) (1997), 275–291.
- [W3] N. J. Wildberger, *Finite commutative hypergroups and applications from group theory to conformal field theory*, In Applications of Hypergroups and Related Measure Algebras, Proc. Seattle 1993 Conference, Contemporary Math. **183** (1995), 413–434.