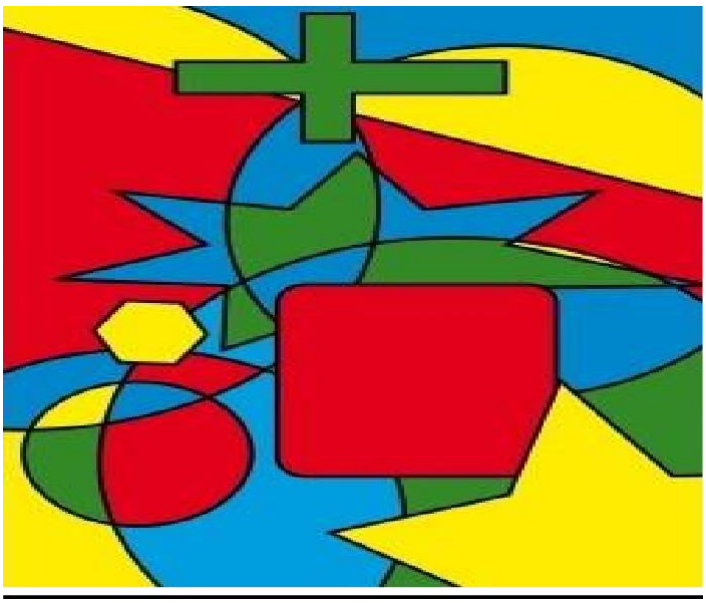
BCS405A

Discrete Mathematical Structures

(For the 4th Semester Computer Science and Engineering Stream)



Module 5

INTRODUCTION TO GROUP THEORY

Content

Groups:

- Definitions, properties,
- Homomrphisms,
- Isomorphisms,
- Cyclic Groups,
- Cosets, and Lagrange's Theorem.

Coding Theory and Rings:

- Elements of CodingTheory,
- The Hamming Metric,
- The Parity Check, and Generator Matrices.

Group Codes:

- Decoding with Coset Leaders,
- Hamming Matrices.

Rings and Modular Arithmetic:

- The Ring Structure – Definition and Examples,

GROUPS

Introduction:

Definitions, Examples, and Elementary Properties:

In m athematics, a **discrete group** is a group *G* equipped with the discrete topology. With this topology *G* becomes a topological group. A **discrete subgroup** of a topological group *G* is a subgroup *H* whose relative topology is the discrete one. For example, the integers, **Z**, form a discrete subgroup of the reals, **R**, but the rational numbers, **Q**, do not.

Any group can be given the discrete topology. Since every map from a discrete space is continuous, the topological homomorphisms between discrete groups are exactly the group homomorphisms between the underlying groups. Hence, there is an isomorphism between the category of groups and the category of discrete groups. Discrete groups can therefore be identified with their underlying (non-topological) groups. With this in mind, the term **discrete group theory** is used to refer to the study of groups without topological structure, in contradistinction to topological or Lie group theory. It is divided, logically but also technically, into finite group theory, and infinite group theory.

There are some occasions when a topological group or Lie group is usefully endowed with the discrete topology, 'against nature'. This happens for example in the theory of the Bohr com pactification, and in group cohomology theory of Lie groups.

Properties:

Since topological groups are homogeneous, one need only look at a single point to determine if the group is discrete. In particular, a topological group is discrete if and only if the singleton containing the identity is an open set.

A discrete group is the same thing as a zero-dimensional Lie group (uncountable discrete groups are not second-co untable so authors who require Lie groups to satisfy this axiom do not regard these groups as Lie groups). The identity component of a discrete group is just the trivial subgroup while the group of components is isomorphic to the group itself.

Since the only Hausdorff topology on a finite set is the discrete one, a finite Hausdorff topological group must necessarily be discrete. It follows that every finite subgroup of a Hausdorff group is discrete.

A discrete subgroup *H* of *G* is co compact if there is a compact subset *K* of *G* such that *HK* = *G*.

Discrete normal subgroups play an important role in the theory of covering groups and locally isomorphic groups. A discrete normal subgroup of a connected group G necessarily lies in the center of G and is therefore abelian.

Other properties:

- every discrete group is totally disconnected
- every subgroup of a discrete group is discrete.
- every quotient of a discrete group is discrete.
- the product of a finite number of discrete groups is discrete.
- a discrete group is compact if and only if it is finite.
- every discrete group is locally compact.
- every discrete subgroup of a Hausdorff group is closed.
- every discrete subgroup of a compact Hausdorff group is finite.

Examples:

- Frieze groups and wallpaper groups are discrete subgroups of the i sometry group of the Euclidean plane. Wallpaper groups are cocompact, but Frieze groups are not.

- A space group is a discrete subgroup of the i sometry group of Euclidean space of some dimension.
- A crystallographic group usually means a cocompact, discrete subgroup of the isometries of some Euclidean space. Sometimes, however, a crystallographic group can be a cocompact discrete subgroup of a n ilpotent or solvable Lie group.
- Every triangle group T is a discrete subgroup of the isometry group of the sphere (when T is finite), the Euclidean plane (when T has a $\mathbf{Z} + \mathbf{Z}$ subgroup of finite index), or the hyperbolic plane.

Fuchsian groups are, by definition, discrete subgroups of the isometry group of the hyperbolic plane.

o A Fuchsian group that preserves orientation and acts on the upper half-plane model of the hyperbolic plane is a discrete subgroup of the Lie group

o A Fuchsian group that preserves orientation and acts on the upper half-plane model of the hyperbolic plane is a discrete subgroup of the Lie PSL(2,**R**), the group of orientation preserving isometries of the upperhalf-plane model of the hyperbolic plane.

A Fuchsian group is sometimes considered as a s pecial case of a Kleinian group, by embedding the hyperbolic plane isometrically into three dimensional hyperbolic space and ex tending the group action on the plane to the whole space.

The modular group is PSL(2,**Z**), thought of as a discrete subgroup of PSL(2,**R**). The modular group is a lattice in PSL(2,**R**), but it is not cocompact.
Kleinian groups are, by definition, discrete subgroups of the isometry group of hyperbolic 3-space. These include quasi- Fuchsian groups.
A Kleinian group that preserves orientation and acts on the upper half space model of h yperbolic 3-space is a discrete s ubgroup of the Lie group PSL(2,**C**), the group of o rientation preserving isometries of the upper half- space model of h yperbolic 3-space.
A lattice in a Lie group is a discrete subgroup such that the Haar measure of thequotient space is finite.

Group homomorphism:

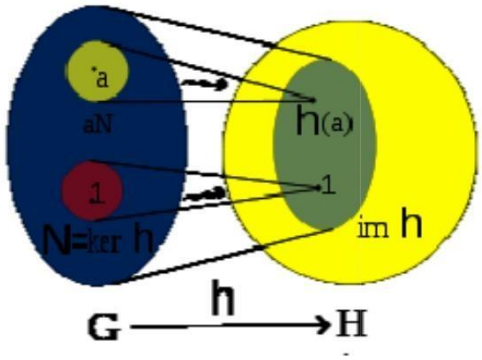


Image of a Group homomorphism(**h**) from **G**(left) to **H**(right). The smaller oval inside **H** is the image of **h**. **N** is the kernel of **h** and **aN** is a coset of **h**.

In mathematics, given two groups $(G, *)$ and $(H, \cdot)$, a **group homomorphism** from $(G, *)$ to $(H, \cdot)$ is a function $h : G \to H$ such that for all u and v in G it holds that

$$h(u * v) = h(u) \cdot h(v)$$

where the group operation on the left hand side of the equation is that of G and on the right hand side that of H.

From this property, one can deduce that h maps the identity element e_G of G to the identity element e_H of H, and it also maps inverses to inverses in the sense that

$$h(u^{-1}) = h(u)^{-1}.$$

Hence one can say that h "is compatible with the group s tructure".

Older notations for the homomorphism $h(x)$ may be x_h, though this may be confused as an index or a general subscript. A more recent trend is to write group homomorphisms on the right of their arguments, omitting brackets, so that $h(x)$ becomes simply $x\,h$. This approach is especially prevalent in areas of group theory where automata play a role, since it accords better with the convention that automata read words from left to right.

In areas of mathematics where one considers groups endowed with additional structure, a *homomorphism* sometimes means a map which respects not only the group structure (as above) but also the extra structure. For example, a homomorphism of topological groups is often required to be continuous.

The category of groups

If $h : G \to H$ and $k : H \to K$ are group homomorphisms, then so is $k \circ h : G \to K$. This shows that the class of all groups, together with group homomorphisms as morphisms, forms a category.

Types of homomorphic maps

If the homomorphism h is a bijection, then one can show that its inverse is also a group homomorphism, and h is called a *group isomorphism*; in this case, the groups G and H are called *is omorphic*: they differ only in the notation of their elements and are identical for all p ractical purposes.

If h: $G \to G$ is a group h omomorphism, we call it an *endomorphism* of G. If furthermore it is bijective and hence an isomorphism, it is called an *automorphism*. The set of all automorphisms of a group G, with functional composition as operation, forms itself a group, the *automorphism group* of G. It is denoted by Aut(G). As an example, the automorphism group of ($\mathbf{Z}$, +) contains only two elements, the identity transformationand multiplication with -1; it is isomorphic to $\mathbf{Z}/2\mathbf{Z}$.

An **epimorphism** is a surjective homomorphism, that is, a homomorphism which is *onto* as a function. A **monomorphism** is an injective homomorphism, that is, a homomorphism which is *one-to-one* as a function.

Homomorphisms of abelian groups

If G and H are abelian (i.e. commutative) groups, then the set Hom(G, H) of all group homomorphisms from G to H is itself an abelian group: the sum $h + k$ of two homomorphisms is defined by

$$(h + k)(u) = h(u) + k(u) \quad \text{for all } u \text{ in } G.$$

The commutativity of H is needed to prove that $h + k$ is again a group homomorphism. The addition of homomorphisms is compatible with the composition of homomorphisms in the following sense: if f is in Hom(K, G), h, k are elements of Hom(G, H), and g is in Hom(H,L), then

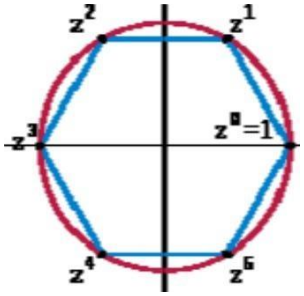
$$(h + k) \circ f = (h \circ f) + (k \circ f) \quad \text{and} \quad g \circ (h + k) = (g \circ h) + (g \circ k).$$

This shows that the set End(G) of all endomorphisms of an abelian group forms a ring, the *endomorphism ring* of G. For example, the endomorphism ring of the abelian group consisting of the direct sum of m copies of $\mathbf{Z}/\mathbf{nZ}$ is isomorphic to the ring of m-by-m matrices with entries in $\mathbf{Z}/n\mathbf{Z}$. The above compatibility also shows that the category of all abelian groups with group ho momorphisms forms a preadditive category; the existence of direct sums and well-behaved kernels makes this category the prototypical example of an abelian category.

Cyclic group

In group theory, a **cyclic group** is a group that can be generated by a single element, in the sense that the group has an element g (called a "generator" of the group) such that, when written multiplicatively, every element of the group is a power of g (a multiple of g when the notation is additive).

Definition



The six 6th complex roots of unity form a cyclic group under multiplication. z is a primitive element, but z^2 is not, because the odd powers of z are not a power of z^2.

A group G is called cyclic if there exists an element g in G such that $G = \langle g \rangle = \{ g^n \mid n \text{ is an integer} \}$. Since any group generated by an element in a group is a subgroup of that group, showing that the only subgroup of a group G that contains g is G itself suffices to show that G is cyclic.

For example, if $G = \{ g^0, g^1, g^2, g^3, g^4, g^5 \}$ is a group, then $g^6 = g^0$, and G is cyclic. In fact, G is essentially the same as (that is, isomorphic to) the set { 0, 1, 2, 3, 4, 5 } with addition modulo 6. For example, 1 + 2 = 3 (mod 6) cor responds to $g^1 \cdot g^2 = g^3$, and 2 + 5 = 1 (mod 6) corresponds to $g^2 \cdot g^5 = g^7 = g^1$, and so on. One can use the isomorphism φ defined by $\varphi(g^i) =$ i.

For every positive integer n there is exactly one cyclic group (up to isomorphism) whose order is n, and there is exactly one infinite cyclic group (the integers under addition). Hence, the cyclic groups are the simplest groups and they are completely classified.

The name "cyclic" may be m isleading: it is possible to generate infinitely many elements and not form any literal cycles; that is, every g^n is distinct. (It can be said that it has one infinitely long cycle.) A group generated in this way is called an **infinite cyclic group**, and is isomorphic to the additive group of integers **Z**.

Furthermore, the circle group (whose elements are uncountable) is *not* a cyclic group—a cyclic group always has countable elements.

Since the cyclic groups are abelian, they are often written additively and denoted $\mathbf{Z}_n$. However, this notation can be problematic for number theorists because it conflicts with the usual notation for p-adic number rings or localization at a prime ideal. The quotient notations $\mathbf{Z}/n\mathbf{Z}$, $\mathbf{Z}/n$, and $\mathbf{Z}/(n)$ are standard alternatives. We adopt the first of these here to avoid the collision of notation. See also the section Subgroups and notation below.

One may write the group multiplicatively, and denote it by C_n, where n is the order (which can be ∞). For example, $g^3g^4 = g^2$ in C_5, whereas $3 + 4 = 2$ in $\mathbf{Z}/5\mathbf{Z}$.

Properties

The fundamental theorem of cyclic groups states that if G is a cyclic group of order n then every subgroup of G is cyclic. Moreover, the order of any subgroup of G is a divisor of n and for each positive divisor k of n the group G has exactly one subgroup of order k. This property characterizes finite cyclic groups: a group of order n is cyclic if and only if for every divisor d of n the group has at most one subgroup of order d. Sometimes the e quivalent s tatement is used: a group of order n is cyclic if and only if for every divisor d of n the group has exactly one subgroup of order d.

Every finite cyclic group is i somorphic to the group { [0], [1], [2], ..., [n - 1] } of integers modulo n under addition, and any infinite cyclic group is isomorphic to $\mathbf{Z}$ (the set of all integers) under addition. Thus, one only needs to look at such groups to understand the properties of cyclic groups in general. Hence, cyclic groups are one of the simplest groups to study and a number of nice p roperties are known.

Given a cyclic group G of order n (n may be infinity) and for every g in G,

- G is abelian; that is, their group operation is com mutative: $gh = hg$ (for all h in G). This is so since $g + h \bmod n = h + g \bmod n$.
- If n is finite, then $g^n = g^0$ is the identity element of the group, since $kn \bmod n = 0$ for any integer k.
- If $n = \infty$, then there are exactly two elements that generate the group on their own: namely 1 and -1 for $\mathbf{Z}$
- If n is finite, then there are exactly $\varphi(n)$ elements that generate the group on their own, where φ is the Euler totient function
- Every subgroup of G is cyclic. Indeed, each finite subgroup of G is a group of { 0,

1, 2, 3, ... m - 1} with addition m odulo m. And each infinite subgroup of G is $m\mathbf{Z}$ for some m, which is bijective to (so is omorphic to) **Z**.

- G_n is isomorphic to $\mathbf{Z}/n\mathbf{Z}$ (factor group of **Z** over $n\mathbf{Z}$) since $\mathbf{Z}/n\mathbf{Z} = \{0 + n\mathbf{Z}, 1 + n\mathbf{Z}, 2 + n\mathbf{Z}, 3 + n\mathbf{Z}, 4 + n\mathbf{Z}, ..., n - 1 + n\mathbf{Z}\}$ $\{0, 1, 2, 3, 4, ..., n - 1\}$ under addition modulo n.

More generally, if d is a divisor of n, then the number of elements in $\mathbf{Z}/n$ which have order d is $\varphi(d)$. The order of the residue class of m is n / gcd(n,m).

If p is a prime number, then the only group (up to isomorphism) with p elements is the cyclic group C_p or $\mathbf{Z}/p\mathbf{Z}$.

The direct product of two cyclic groups $\mathbf{Z}/n\mathbf{Z}$ and $\mathbf{Z}/m\mathbf{Z}$ is cyclic if and only if n and m are coprime. Thus e.g. $\mathbf{Z}/12\mathbf{Z}$ is the direct product of $\mathbf{Z}/3\mathbf{Z}$ and $\mathbf{Z}/4\mathbf{Z}$, but not the direct product of $\mathbf{Z}/6\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z}$.

The definition immediately implies that cyclic groups have very simple group presentation $C_\infty = \langle x \mid \rangle$ and $C_n = \langle x \mid x^n \rangle$ for finite n.

A primary cyclic group is a group of the form $\mathbf{Z}/p^k$ where p is a prime number. The fundamental theorem of abelian groups states that every finitely generated abelian group is the direct p roduct of finitely many finite primary cyclic and infinite cyclic groups.

$\mathbf{Z}/n\mathbf{Z}$ and **Z** are also commutative rings. If p is a prime, then $\mathbf{Z}/p\mathbf{Z}$ is a finite field, also denoted by $\mathbf{F}_p$ or **GF**(p). Every field with p elements is isomorphic to this one.

The units of the ring $\mathbf{Z}/n\mathbf{Z}$ are the numbers coprime to n. They form a group under multiplication modulo n with $\varphi(n)$ elements (see above). It is written as $(\mathbf{Z}/n\mathbf{Z})^\times$. For example, when $n = 6$, we get $(\mathbf{Z}/n\mathbf{Z})^\times = \{1,5\}$. When $n = 8$, we get $(\mathbf{Z}/n\mathbf{Z})^\times = \{1,3,5,7\}$.

In fact, it is known that $(\mathbf{Z}/n\mathbf{Z})^\times$ is cyclic if and only if n is 1 or 2 or 4 or p^k or 2 p^k for an odd prime number p and $k \geq 1$, in which case every generator of $(\mathbf{Z}/n\mathbf{Z})^\times$ is called a primitive root modulo n. Thus, $(\mathbf{Z}/n\mathbf{Z})^\times$ is cyclic for $n = 6$, but not for $n = 8$, where it is instead i somorphic to the Klein four-group.

The group $(\mathbf{Z}/p\mathbf{Z})^\times$ is cyclic with p - 1 elements for every prime p, and is also written $(\mathbf{Z}/p\mathbf{Z})^*$ because it consists of the non-zero elements. More generally, every *finite*

s ubgroup of the mu ltiplicative group of any field is cyclic.

Examples

In 2D and 3D the symmetry group for *n*-fold rotational symmetry is C_n, of abstract group type Z_n. In 3D there are also other symmetry groups which are algebraically the same, see *Symmetry groups in 3D that are cyclic as abstract group*.

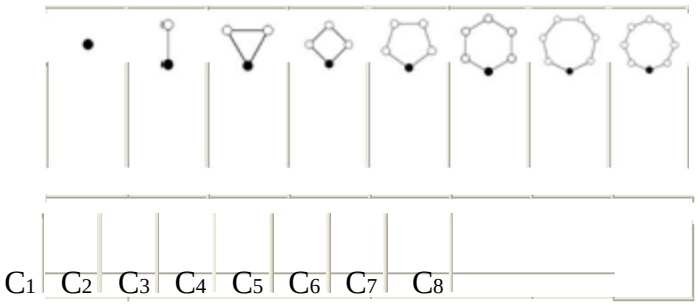
Note that the group S^1 of all rotations of a circle (the circle group) is *not* cyclic, since it is not even countable.

The n^{th} roots of unity form a cyclic group of order *n* under multiplication. e.g., $0 = z^3 - 1 = (z - s^0)(z - s^1)(z - s^2)$ where $s^i = e^{2\pi i / 3}$ and a group of $\{s^0, s^1, s^2\}$ under mul tiplication is cyclic.

The Galois group of every finite field extension of a finite field is finite and cyclic; conversely, given a finite field *F* and a finite cyclic group *G*, there is a finite field extension of *F* whose Galois group is *G*.

Representation

The cycle graphs of finite cyclic groups are all *n*-sided polygons with the elements at the vertices. The dark vertex in the cycle graphs below stand for the identity element, and the other vertices are the other elements of the group. A cycle consists of successive powers of either of the elements connected to the identity element.



The rep resentation theory of the cyclic group is a critical base case for the representation theory of more general finite groups. In the complex case, a representation of a cyclic group d ecomposes into a direct sum of linear c haracters, making the connection between

character theory and repre sentation theory transparent. In the positive ch aracteristic case, the indecomposable repre sentations of the cyclic group form a model and inductive basis for the rep resentation theory of groups with cyclic Sylow subgroups and more generally the representation theory of blocks of cyclic defect.

Subgroups and notation

All subgroups and quotient groups of cyclic groups are cyclic. Specifically, all subgroups of $\mathbf{Z}$ are of the form $m\mathbf{Z}$, with m an integer ≥ 0. All of these subgroups are different, and apart from the trivial group (for $m=0$) all are isomorphic to $\mathbf{Z}$. The lattice of subgroups of $\mathbf{Z}$ is isomorphic to the dual of the lattice of natural numbers ordered by divisibility. All factor groups of $\mathbf{Z}$ are finite, except for the trivial exception $\mathbf{Z}/\{0\} = \mathbf{Z}/0\mathbf{Z}$. For every positive divisor d of n, the quotient group $\mathbf{Z}/n\mathbf{Z}$ has precCSEly one subgroup of order d, the one generated by the residue class of n/d. There are no other subgroups. The lattice of subgroups is thus isomorphic to the set of divisors of n, ordered by divisibility. In particular, a cyclic group is simple if and only if its order (the number of its elements) is prime.

Using the quotient group formalism, $\mathbf{Z}/n\mathbf{Z}$ is a standard notation for the additive cyclic group with n elements. In ring terminology, the s ubgroup $n\mathbf{Z}$ is also the ideal (n), so the quotient can also be written $\mathbf{Z}/(n)$ or $\mathbf{Z}/n$ without abuse of notation. These alternatives do not conflict with the notation for the p-adic integers. The last form is very common in informal calculations; it has the additional advantage that it reads the same way that the group or ring is often described verbally, "Zee mod en".

As a p ractical problem, one may be given a finite subgroup C of order n, generated by an element g, and asked to find the size m of the subgroup generated by g^k for some integer k. Here m will be the smallest integer > 0 such that mk is divisible by n. It is therefore n/m where $m = (k, n)$ is the greatest common divisor of k and n. Put another way, the index of the subgroup generated by g^k is m. This reasoning is known as the **index calculus algorithm**, in number theory.

Endomorphisms

The endomorphism ring of the abelian group $\mathbf{Z}/n\mathbf{Z}$ is isomorphic to $\mathbf{Z}/n\mathbf{Z}$ itself as a ring. Under this isomorphism, the number r corresponds to the endomorphism of $\mathbf{Z}/n\mathbf{Z}$ that maps each element to the sum of r copies of it. This is a bijection if and only if r is

coprime with *n*, so the automorphism group of $\mathbf{Z}/n\mathbf{Z}$ is isomorphic to the unit group $(\mathbf{Z}/n\mathbf{Z})^\times$ (see above).

Similarly, the endomorphism ring of the additive group **Z** is isomorphic to the ring **Z**. Its automorphism group is iso morphic to the group of units of the ring **Z**, i.e. to {-1, +1} $\cong C_2$.

Virtually cyclic groups

A group is called **virtually cyclic** if it contains a cyclic subgroup of finite index (the number of cosets that the subgroup has). In other words, any element in a virtually cyclic group can be arrived at by applying a member of the cyclic subgroup to a member in a certain finite set. Every cyclic group is virtually cyclic, as is every finite group. It is known that a finitely generated discrete group with exactly two *ends* is virtually cyclic

(for instance the product of $\mathbf{Z}/n$ and **Z**). Every abelian subgroup of a Gromov hyperbolic group is virtually cyclic.

Group isomorphism

In abstract algebra, a **group isomorphism** is a function between two groups that sets up a one-to-one corre spondence between the elements of the groups in a way that respects the given group operations. If there exists an isomorphism between two groups, then the groups are called **isomorphic**. From the standpoint of group theory, isomorphic groups have the same p roperties and need not be distinguished.

Definition and notation

Given two groups $(G, *)$ and $(H, \odot)$, a *group isomorphism* from $(G, *)$ to $(H, \odot)$ is a bijective group homomorphism from *G* to *H*. Spelled out, this means that a group i somorphism is a bijective function $f : G \to H$ such that for all *u* and *v* in *G* it holds that

$$f(u * v) = f(u) \odot f(v)$$

.

The two groups $(G, *)$ and $(H, \odot)$ are isomorphic if an isomorphism exists. This is

written:

$$(G,*) \cong (H,\odot)$$

Often shorter and more simple notations can be used. Often there is no ambiguity about the group operation, and it can be omitted:

$$G \cong H$$

Sometimes one can even simply write $G = H$. Whether such a notation is possible without confusion or ambiguity depends on context. For example, the equals sign is not very suitable when the groups are both subgroups of the same group. See also the examples.

Conversely, given a group $(G, *)$, a set H, and a bijection $f : G \to H$, we can make H a group $(H, \odot)$ by defining

$$f(u) \odot f(v) = f(u * v)$$

.

If $H = G$ and $\odot = *$ then the bijection is an automorphism (*q.v.*)

In tuitively, group theorists view two iso morphic groups as follows: For every element *g* of a group *G*, there exists an element *h* of *H* such that *h* 'behaves in the same way' as *g* (operates with other elements of the group in the same way as *g*). For instance, if *g* generates *G*, then so does *h*. This implies in particular that *G* and *H* are in bijective cor respondence. So the definition of an isomorphism is quite natural.

An i somorphism of groups may equivalently be defined as an i nvertible morphism in the category of groups.

Examples

- The group of all real numbers with addition, $(\mathbb{R},+)$, is isomorphic to the group of all positive real numbers with multiplication $(\mathbb{R}^+,\times)$:

$$(\mathbb{R},+) \cong (\mathbb{R}^+,\times)$$

via the isomorphism

$f(x) = e^x$

(see exponential function).

- The group $\mathbb{Z}$ of integers (with addition) is a subgroup of $\mathbb{R}$, and the factor group $\mathbb{R}/\mathbb{Z}$ is isomorphic to the group S^1 of complex numbers of absolute value 1 (with multiplication):

$$\mathbb{R}/\mathbb{Z} \cong S^1$$

An isomorphism is given by

$$f(x + \mathbb{Z}) = e^{2\pi xi}$$

for every x in $\mathbb{R}$.

The Klein four-group is isomorphic to the direct product of two copies of $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ (see modular arithmetic), and can therefore be written $\mathbb{Z}_2 \times \mathbb{Z}_2$. Another notation is Dih_2, because it is a dihedral group.

- Generalizing this, for all odd n, Dih_{2n} is isomorphic with the direct product of Dih_n and Z_2.

- If $(G, *)$ is an infinite cyclic group, then $(G, *)$ is isomorphic to the integers (with the addition operation). From an algebraic point of view, this means that the set of all integers (with the addition operation) is the 'only' infinite cyclic group.

Some groups can be proven to be isomorphic, relying on the axiom of choice, while it is even theoretically impossible to construct concrete isomorphisms. Examples:

- The group (, +) is isomorphic to the group (, +) of all complex numbers with addition.
- The group (, ·)* of non-zero complex numbers with multiplication as operation is isomorphic to the group S^1 mentioned above.

Properties

- The kernel of an isomorphism from (*G*, *) to (*H*,) , is always $\{e_G\}$ where e_G is the identity of the group (*G*, *)
- If (*G*, *) is isomorphic to (*H*,), and if *G* is abelian then so is *H*.
- If (*G*, *) is a group that is isomorphic to (*H*,) [where *f* is the isomorphism], then if *a* belongs to *G* and has order *n*, then so does *f(a)*.
- If (*G*, *) is a locally finite group that is isomorphic to (*H*,), then (*H*,) is also locally finite.
- The previous examples illustrate that 'group properties' are always preserved by i somorphisms.

Cyclic groups

All cyclic groups of a given order are i somorphic to $\mathbb{Z}_n, +_n$.
Let *G* be a cyclic group and *n* be the order of *G*. *G* is then the group generated by $< x > = \{e,x,...,x^{n-1}\}$. We will show that

$$G \cong \mathbb{Z}_n, +_n$$

Define

$\varphi : G \to \mathbb{Z}_n = \{0, 1, ..., n-1\}$ so that $\varphi(x^a) = a$. Clearly, φ is bijective.

Then

$$\varphi(x^a \cdot x^b) = \varphi(x^{a+b}) = a + b = \varphi(x^a) +_n \varphi(x^b)$$

which proves that $G \cong \mathbb{Z}_n, +_n$

Consequences

From the definition, it follows that any isomorphism $f : G \to H$ will map the identity element of *G* to the identity element of *H*,

$f(e_G) = e_H$

that it will map inverses to inverses,

$$f(u^{-1}) = [f(u)]^{-1}$$

and more generally, *n*th powers to *n*th powers,

$$f(u^n) = [f(u)]^n$$

for all *u* in *G*, and that the inverse map $f^{-1} : H \to G$ is also a group isomorphism.

The relation "being isomorphic" satisfies all the axioms of an equivalence relation. If *f* is an isomorphism between two groups *G* and *H*, then everything that is true about *G* that is only related to the group s tructure can be translated via *f* into a true ditto s tatement about *H*, and vice versa.

Automorphisms

An isomorphism from a group $(G,*)$ to itself is called an automorphism of this group. Thus it is a bijection $f : G \to G$ such that

$$f(u) * f(v) = f(u * v).$$

An au tomorphism always maps the identity to itself. The image under an au tomorphism of a conjugacy class is always a conjugacy class (the same or another). The image of an element has the same order as that element.

The composition of two automorphisms is again an automorphism, and with this operation the set of all automorphisms of a group G, denoted by $\mathrm{Aut}(G)$, forms itself a group, the *au tomorphism group* of G.

For all Abelian groups there is at least the automorphism that replaces the group elements by their inverses. However, in groups where all elements are equal to their inverse this is the trivial automorphism, e.g. in the Klein four-group. For that group all permutations of the three non-identity elements are automorphisms, so the automorphism group is i somorphic to S_3 and Dih_3.

In Z_p for a prime number p, one non-identity element can be replaced by any other, with cor responding changes in the other elements. The automorphism group is isomorphic to Z_{p-1}. For example, for $n = 7$, multiplying all elements of Z_7 by 3, modulo 7, is an automorphism of order 6 in the automorphism group, because $3^6 = 1$ (modulo 7), while lower powers do not give 1. Thus this automorphism generates Z_6. There is one more automorphism with this property: multiplying all elements of Z_7 by 5, modulo 7. Therefore, these two correspond to the elements 1 and 5 of Z_6, in that order or conversely.

The automorphism group of Z_6 is isomorphic to Z_2, because only each of the two elements 1 and 5 generate Z_6, so apart from the identity we can only interchange these.

The automorphism group of $Z_2 \times Z_2 \times Z_2 = \mathrm{Dih}_2 \times Z_2$ has order 168, as can be found as follows. All 7 non-identity elements play the same role, so we can choose which plays the role of (1,0,0). Any of the remaining 6 can be chosen to play the role of (0,1,0). This determines which corresponds to (1,1,0). For (0,0,1) we can choose from 4, which determines the rest. Thus we have $7 \times 6 \times 4 = 168$ automorphisms. They correspond to those of the Fano plane, of which the 7 points correspond to the 7 non-identity elements

The lines connecting three points correspond to the group operation: a, b, and c on one line means a+b=c, a+c=b, and b+c=a. See also general linear group over finite fields.

For Abelian groups all automorphisms except the trivial one are called outer automorphisms.

———————

Non-Abelian groups have a non-trivial inner automorphism group, and possibly also outer automorphisms.

Coding Theory and Rings

Elements of Coding Theory

Coding theory is studied by various scientific di sciplines — such as info rmation theory, electrical engineering, mathematics, and computer science — for the purpose of designing efficient and reliable data transmission methods. This typically involves the removal of r edundancy and the correction (or detection) of errors in the transmitted data. It also includes the study of the properties of codes and their fitness for a specific application.

Thus, there are es sentially two aspects to Coding theory:

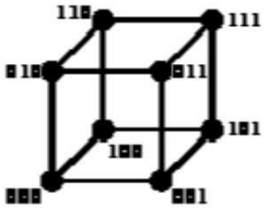
1. Data compression (or, *source coding*)
2. Error correction (or, *channel coding')*

These two aspects may be studied in combination.

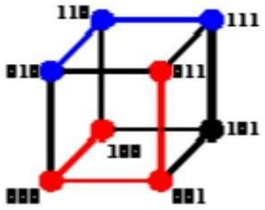
The first, source encoding, attempts to compress the data from a source in order to transmit it more efficiently. This practice is found every day on the Internet where the common "Zip" data compression is used to reduce the network load and make files smaller. The second, channel encoding, adds extra data bits to make the transmission of
data more robust to dis turbances present on the transmission channel. The ordinary user may not be aware of many applications using channel coding. A typical music CD uses the Reed-Solomon code to correct for scratches and dust. In this application the transmission channel is the CD itself. Cell phones also use coding techniques to correct

for the fading and noCSE of high frequency radio transmission. Data modems, t elephone transmissions, and NASA all employ channel coding techniques to get the bits through, for example the turbo code and LDPC codes.

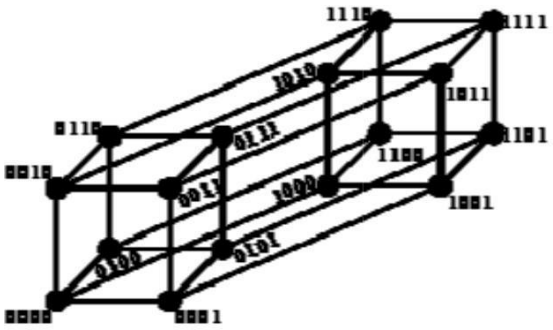
The hamming metric:



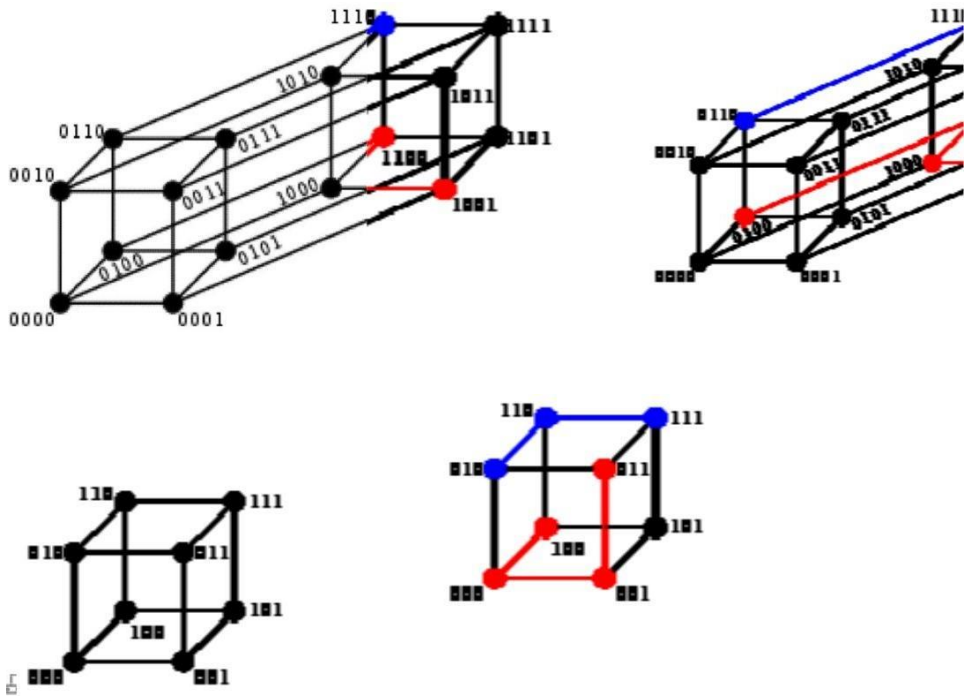
3-bit binary cube for finding Hamming distance



Two example distances: 100->011 has distance 3 (red path); 010->111 has distance 2 (blue path)



4-bit binary h ypercube for finding Hamming distance



Two example dis tances: 0100->1001 has distance 3 (red path); 0110->1110 has distance 1 (blue path)

In information theory, the **Hamming distance** between two strings of equal length is the number of positions at which the corresponding symbols are different. Put another way, it

Parity-check matrix

In coding theory, a **parity-check matrix** of a linear block code **C** is a generator matrix of the dual code. As such, a codeword c is in **C** if and only if the matrix-vector product $\mathbf{H}^{\mathbf{T}}\mathbf{c}=\mathbf{0}$.

The rows of a parity check matrix are parity checks on the codewords of a code. That is, they show how linear combinations of certain digits of each codeword equal zero. For example, the parity check matrix

specifies that for each codeword, digits 1 and 2 should sum to zero and digits 3 and 4 should sum to zero.

Creating a parity check matrix

The parity check matrix for a given code can be derived from its generator matrix (and vice-versa). If the generator matrix for an [*n*,*k*]-code is in standard form

$$G = \begin{bmatrix} I_k | P \end{bmatrix}$$
,

then the parity check matrix is given by

$$H = \begin{bmatrix} -P^T | I_{n-k} \end{bmatrix}$$
,

because

$GH^T = P - P = 0.$

Negation is performed in the finite field mod *q*. Note that if the characteristic of the underlying field is 2 (i.e., 1 + 1 = 0 in that field), as in binary codes, then - *P* = *P*, so the negation is unnecessary.

For example, if a binary code has the generator matrix

$$G = \begin{bmatrix} 10|101 \\ 01|110 \end{bmatrix}$$

The parity check matrix becomes

$$H = \begin{bmatrix} 11|100 \\ 01|010 \\ 10|001 \end{bmatrix}$$

For any valid codeword *x*, *Hx* = 0. For any invalid codeword *r* the syndrome *S* satisfies

$$H\tilde{x} = S$$

Parity check

If no error occurs during transmission, then the received codeword *r* is identical to the t ransmitted codeword *x*:

$$\mathbf{r} = \mathbf{x}$$

The receiver multiplies *H* and *r* to obtain the **syndrome** vector **z**, which indicates whether an error has occurred, and if so, for mul which codeword bit. Performing this tiplication (again, entries modulo 2):

$$\mathbf{z} = \mathbf{Hr} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Since the syndrome *z* is the null vector, the receiver can conclude that no error has occurred. This conclusion is based on the observation that when the data vector is multiplied by **G**, a change of basis occurs into a vector subspace that is the kernel of **H**. As long as nothing happens during transmission, **r** will remain in the kernel of **H** and the mul tiplication will yield the null vector.

Coset

In mathematics, if *G* is a group, *H* is a subgroup of *G*, and *g* is an element of *G*, then

gH = {*gh* : *h* an element of *H*} is a **left coset of *H*** in *G*, and

$Hg = \{hg : h$ an element of H is$\}$ a **right coset of *H*** in G.

Only when H is normal will the right and left cosets of H coincide, which is one definition of normality of a subgroup.

A **coset** is a left or right coset of *some* subgroup in G. Since $Hg = g(g^{-1}Hg)$, the right cosets Hg (of H) and the left cosets $g(g^{-1}Hg)$ (of the conjugate subgroup $g^{-1}Hg$) are the same. Hence it is not meaningful to speak of a coset as being left or right unless one first specifies the underlying subgroup.

For abelian groups or groups written additively, the notation used changes to $g+H$ and $H+g$ respectively.

Examples

The additive cyclic group $\mathbf{Z}_4 = \{0, 1, 2, 3\} = G$ has a subgroup $H = \{0, 2\}$ (isomorphic to $\mathbf{Z}_2$). The left cosets of H in G are

$0 + H = \{0, 2\} = H$

$1 + H = \{1, 3\}$

$2 + H = \{2, 0\} = H$

$3 + H = \{3, 1\}$.

There are therefore two distinct cosets, H itself, and $1 + H = 3 + H$. Note that every element of G is either in H or in $1 + H$, that is, $H \cup (1 + H) = G$, so the distinct cosets of H in G partition G. Since $\mathbf{Z}_4$ is an abelian group, the right cosets will be the same as the left.

Another example of a coset comes from the theory of vector spaces. The elements

(vectors) of a vector space form an Abelian group under vector addition. It is not hard to show that subspaces of a vector space are subgroups of this group. For a vector space *V*, a s ubspace *W*, and a fixed vector *a* in *V*, the sets

$$\{x \in V : x = a + n, n \in W\}$$

are called affine subspaces, and are cosets (both left and right, since the group is Abelian). In terms of geometric vectors, these affine subspaces are all the "lines" or "planes" parallel to the subspace, which is a line or plane going through the origin.

General properties

We have $gH = H$ if and only if g is an element of H, since as H is a subgroup, it must be closed and must contain the identity.

Any two left cosets of H in G are either identical or disjoint — i.e., the left cosets form a partition of G such that every element of G belongs to one and only one left coset.[1] In particular the identity is in precCSEly one coset, and that coset is H itself; this is also the only coset that is a subgroup. We can see this clearly in the above examples.

The left cosets of H in G are the equivalence classes under the equivalence relation on G given by $x \sim y$ if and only if $x^{-1}y \in H$. Similar statements are also true for right cosets.

A **coset representative** is a representative in the equivalence class sense. A set of representatives of all the cosets is called a transversal. There are other types of equivalence relations in a group, such as conjugacy, that form different classes which do not have the properties discussed here. Some books on very applied group theory erroneously identify the conjugacy class as 'the' equivalence class as opposed to a particular type of equivalence class.

Index of a subgroup

All left cosets and all right cosets have the same order (number of elements, or cardinality in the case of an infinite H), equal to the order of H (because H is itself a coset). Furthermore, the number of left cosets is equal to the number of right cosets and is

known as the **index** of H in G, written as $[G : H]$Lagrange's theorem allows us to compute the index in the case where G and H are finite, as per the formula:

$$|G| = [G : H] |H|$$

This equation also holds in the case where the groups are infinite, although the meaning may be less clear.

Cosets and normality

If H is not normal in G, then its left cosets are different from its right cosets. That is, there is an a in G such that no element b satisfies $aH = Hb$. This means that the partition of G into the left cosets of H is a different partition than the partition of G into right cosets of H. (It is important to note that *some* cosets may coincide. For example, if a is in the center of G, then $aH = Ha$.)

On the other hand, the subgroup N is normal if and only if $gN = Ng$ for all g in G. In this

Lagrange's theorem (group theory)

Lagrange's theorem, in the mat hematics of group theory, states that for any finite group G, the order (number of elements) of every subgroup H of G divides the order of G. The theorem is named after Joseph Lagrange.

Proof of Lagrange's Theorem

This can be shown using the concept of left cosets of H in G. The left cosets are the equivalence classes of a certain equivalence relation on G and therefore form a partition of G. Specifically, x and y in G are related if and only if there exists h in H such that $x = yh$. If we can show that all cosets of H have the same number of elements, then each coset of H has precCSEly $|H|$ elements. We are then done since the order of H times the number of cosets is equal to the number of elements in G, thereby proving that the order H divides the order of G. Now, if aH and bH are two left cosets of H, we can define a map $f : aH \to bH$ by setting $f(x) = ba^{-1}x$. This map is b ijective because its inverse is given by $f^{-1}(y) = ab^{-1}y$.

This proof also shows that the quotient of the orders $|G| / |H|$ is equal to the index $[G : H]$

(the number of left cosets of H in G). If we write this statement as

$$|G| = [G : H] \cdot |H|,$$

then, seen as a statement about cardinal numbers, it is equivalent to the Axiom of choice.

Using the theorem

A consequence of the theorem is that the order of any element a of a finite group (i.e. the smallest positive integer number k with $a^k = e$, where e is the identity element of the group) divides the order of that group, since the order of a is equal to the order of the cyclic subgroup generated by a. If the group has n elements, it follows

$$a^n = e.$$

This can be used to prove Fermat's little theorem and its generalization, Euler's theorem. These special cases were known long before the general theorem was proved.

The theorem also shows that any group of prime order is cyclic and simple.

E xistence of subgroups of given order

Lagrange's theorem raCSEs the converse question as to whether every divisor of the order of a group is the order of some subgroup. This does not hold in general: given a finite group G and a divisor d of $|G|$, there does not necessarily exist a subgroup of G with order d. The smallest example is the alternating group $G = A_4$ which has 12 elements but no subgroup of order 6. A *CLT group* is a finite group with the property that for every divisor of the order of the group, there is a subgroup of that order. It is known that a CLT group must be solvable and that every supersolvable group is a CLT group: however there exists solvable groups which are not CLT and CLT groups which are not super solvable.

There are partial converses to Lagrange's theorem. For general groups, Cauchy's theorem guarantees the existence of an element, and hence of a cyclic subgroup, of order any prime dividing the group order; Sylow's theorem extends this to the existence of a s ubgroup of order equal to the maximal power of any prime dividing the group order. For s olvable groups, Hall's theorems assert the existence of a subgroup of order equal to any

unitary divisor of the group order (that is, a divisor coprime to its cofactor).

Group Co des: Deco ding wthi Coset L ead ers, Hamming Matrices

R ings a nd Mod ular Arithmetic: The Ring Structure – Definition and E xampl es, Ring P ro pe rt ies and Sub str uctures, The I ntegers Mod ulo n

In computer science, **group codes** are a type of code. Group codes consist of *n* linear block cod~~es which are~~ subgroups of G^n, where *G* is a finite Abelian group.

A systematic group code *C* is a code over G_n of order defined by $|G|^k$ n - k homomorphisms which determine the parity check bits. The remaining *k* bits are the in formation bits themselves.

Construction

Group codes can be constructed by special generator matrices which resemble generator matrices of linear block codes except that the elements of those matrices are endomorphisms of the group instead of symbols from the code's alphabet. For example, consider the generator matrix

$$G = \begin{pmatrix} \begin{pmatrix} 00 \\ 11 \end{pmatrix} & \begin{pmatrix} 01 \\ 01 \end{pmatrix} & \begin{pmatrix} 11 \\ 01 \end{pmatrix} \\ \begin{pmatrix} 00 \\ 11 \end{pmatrix} & \begin{pmatrix} 11 \\ 11 \end{pmatrix} & \begin{pmatrix} 00 \\ 00 \end{pmatrix} \end{pmatrix}$$

The elements of this matrix are 2*x*2 matrices which are endomorphisms. In this scenario, each codeword can be represented as $g_1^{m_1} g_2^{m_2} \cdots g_r^{m_r}$ where $g_1,...g_r$ are the generators of *G*.

Decoding with Coset leader

In the field of coding theory, a **coset leader** is defined as a word of minimum weight in any particular coset - that is, a word with the lowest amount of non-zero entries. Sometimes there are several words of equal minimum weight in a coset, and in that case,

any one of those words may be chosen to be the coset leader.

Coset leaders are used in the construction of a standard array for a linear code, which can then be used to decode received vectors. For a received vector *y*, the decoded message is *y* - *e*, where *e* is the coset leader of *y*. Coset leaders can also be used to construct a fast decoding strategy. For each coset leader *u* we calculate the syndrome *uH′*. When we receive *v* we evaluate *vH′* and find the matching syndrome. The corresponding coset leader is the most likely error pattern and we assume that *v*+*u* was the codeword sent.

Example

A standard array for an [*n*,*k*]-code is a q^{n-k} by q^k array where:

1. The first row lists all codewords (with the 0 codeword on the extreme left)
2. Each row is a coset with the coset leader in the first column
3. The entry in the i-th row and j-th column is the sum of the i-th coset leader and the j-th codeword.

For example, the [*n*,*k*]-code C_3 = {0, 01101, 10110, 11011} has a standard array as follows:

0 01101 10110 11011

10000 11101 00110 01011

01000 00101 11110 10011

00100 01001 10010 11111

00010 01111 10100 11001

00001 01100 10111 11010

11000 10101 01110 00011

10001 11100 00111 01010

Note that the above is only one possibility for the standard array; had 00011 been chosen as the first coset leader of weight two, another standard array rep resenting the code would have been con structed.
Note that the first row contains the 0 vector and the codewords of C_3 (0 itself being a codeword). Also, the leftmost column contains the vectors of minimum weight enumerating vectors of weight 1 first and then using vectors of weight 2. Note also that each possible vector in the vector space appears exactly once.

Because each possible vector can appear only once in a standard array some care must be taken during cons truction. A s tandard array can be created as follows:

1. List the codewords of *C*, starting with 0, as the first row
2. Choose any vector of minimum weight not already in the array. Write this as the first entry of the next row. This vector is denoted the '**coset leader**'.
3. Fill out the row by adding the coset leader to the codeword at the top of each column. The sum of the i-th coset leader and the j-th codeword becomes the entry in row i, column j.
4. Repeat steps 2 and 3 until all rows/cosets are listed and each vector appears exactly once.

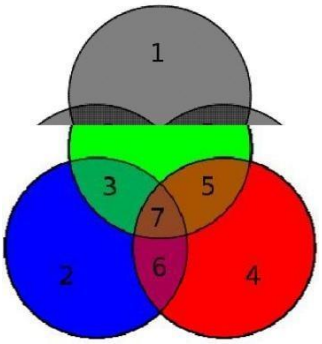
Hamming matrices

Hamming codes can be computed in linear algebra terms through matrices because Hamming codes are linear codes. For the purposes of Hamming codes, two **Hamming matrices** can be defined: the **code generator matrix** and the **parity-check matrix** $\mathbf{H}$:

$$\mathbf{G} := \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and

$$\mathbf{H} := \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$



Bit position of the data and parity bits

As mentioned above, rows 1, 2, & 4 of **G** should look familiar as they map the data bits to their parity bits:

- p_1 covers d_1, d_2, d_4
- p_2 covers d_1, d_3, d_4
- p_3 covers d_2, d_3, d_4

The remaining rows (3, 5, 6, 7) map the data to their position in encoded form and there is only 1 in that row so it is an identical copy. In fact, these four rows are linearly independent and form the identity matrix (by design, not coincidence).

Also as mentioned above, the three rows of **H** should be familiar. These rows are used to compute the **syndrome vector** at the receiving end and if the s yndrome vector is the null

vector (all zeros) then the received word is error-free; if non-zero then the value indicates which bit has been flipped.

The 4 data bits — assembled as a vector — is pre-multiplied by (i.e.,) and taken modulo 2 to yield the encoded value that is transmitted. The original 4 data bits are converted to 7 bits (hence the name "Hamming(7,4)") with 3 parity bits added to ensure even parity using the above data bit coverages. The first table above shows the mapping between each data and parity bit into its final bit position (1 through 7) but this can also be presented in a Venn diagram. The first diagram in this article shows three circles (one for each parity bit) and encloses data bits that each parity bit covers. The second diagram (shown to the right) is identical but, instead, the bit positions are marked.

For the remainder of this section, the following 4 bits (shown as a column vector) will be used as a running example:

$$\mathbf{p} = \begin{pmatrix} d_1 \\ d_2 \\ d_3 \\ d_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Rings and Modular Arithmetic

Ring theory

In mathematics, **ring theory** is the study of rings— algebraic s tructures in which addition and multiplication are defined and have similar properties to those familiar from the integers. Ring theory studies the structure of rings, their representations, or, in different language, modules, special classes of rings (group rings, division rings, universal enveloping algebras), as well as an array of properties that proved to be of interest both within the theory itself and for its applications, such as homological properties and pol ynomial identities.

Commutative rings are much better understood than noncommutative ones. Due to its intimate connections with algebraic geometry and algebraic number theory, which provide many natural examples of co mmutative rings, their theory, which is considered to

be part of commutative algebra and field theory rather than of general ring theory, is quite different in flavour from the theory of their nonco mmutative counterparts. A fairly recent trend, started in the 1980s with the development of noncommutative geometry and with the discovery of quantum groups, attempts to turn the situation around and build the theory of certain classes of noncom mutative rings in a geometric fashion as if they were rings of functions on (non-existent) 'noncommutative spaces'.

Elementary introduction

Definition

Formally, a ring is an Abelian group (R, +), together with a second binary operation * such that for all a, b and c in R,

$$a * (b * c) = (a * b) * c$$

$$a * (b + c) = (a * b) + (a * c)$$

$$(a + b) * c = (a * c) + (b * c)$$

also, if there exists a *mult iplicative identity* in the ring, that is, an element e such that for all a in R,

$$a * e = e * a = a$$

then it is said to be a *ring with unity*. The number 1 is a common example of a unity.

The ring in which e is equal to the additive identity must have only one element. This ring is called the trivial ring.

Rings that sit inside other rings are called subrings. Maps between rings which respect the ring operations are called ring homomorphisms. Rings, together with ring homomorphisms, form a category (the category of rings). Closely related is the notion of ideals, certain subsets of rings which arCSE as kernels of homomorphisms and can serve to define factor rings. Basic facts about ideals, homomorphisms and factor rings are recorded in the i somorphism theorems and in the Chinese remainder theorem.

A ring is called *commutative* if its multiplication is commutative. Commutative rings

resemble familiar number systems, and various definitions for commutative rings are designed to recover properties known from the integers. Commutative rings are also important in algebraic geometry. In co mmutative ring theory, numbers are often replaced by ideals, and the definition of prime ideal tries to capture the essence of prime numbers. Integral domains, non-trivial commutative rings where no two non-zero elements multiply to give zero, generalize another property of the integers and serve as the proper realm to study divisibility. Principal ideal domains are integral domains in which every ideal can be generated by a single element, another property shared by the integers. E uclidean domains are integral domains in which the E uclidean algorithm can be carried out. Important ex amples of co mmutative rings can be constructed as rings of pol ynomials and their factor rings. Summary: Euclidean domain => p rincipal ideal domain => unique factorization domain => integral domain => Com mutative ring.

Non-commutative rings resemble rings of matrices in many respects. Following the model of algebraic geometry, attempts have been made recently at defining non-commutative geometry based on non-commutative rings. Non-commutative rings and associative algebras (rings that are also vector spaces) are often studied via their categories of modules. A module over a ring is an Abelian group that the ring acts on as a ring of endomorphisms, very much akin to the way fields (integral domains in which every non-zero element is invertible) act on vector spaces. Examples of non- commutative

rings are given by rings of square matrices or more generally by rings of endomorphisms of Abelian groups or modules, and by monoid rings.

The congruence relation

Modular ar ithmetic can be handled mathematically by introducing a con gruence relation on the integers that is compatible with the operations of the ring of integers: addition, s ubtraction, and mult iplication. For a positive integer *n*, two integers *a* and *b* are said to be **congruent modulo** *n*, written:

$$a \equiv b \pmod{n},$$

if their dif ference *a* - *b* is an integer multiple of *n*. The number *n* is called the **modulus** of the co ngruence. An equivalent definition is that both numbers have the same remainder when divided by *n*.

For example,

$$38 \equiv 14 \pmod{12}$$

because 38 - 14 = 24, which is a multiple of 12. For positive *n* and non-negative *a* and *b*, congruence of *a* and *b* can also be thought of as asserting that these two numbers have the same remainder after dividing by the modulus *n*. So,

$$38 \equiv 2 \pmod{12}$$

because both numbers, when divided by 12, have the same remainder (2). E quivalently, the fractional parts of doing a full division of each of the numbers by 12 are the same: 0.1666... (38/12 = 3.1666..., 2/12 = 0.1666...). From the prior definition we also see that their difference, $a - b = 36$, is a whole number (integer) multiple of 12 ($n = 12$, 36/12 = 3).

The same rule holds for negative values of *a*:

$$-3 \equiv 2 \pmod{5}.$$

A remark on the notation: Because it is common to consider several congruence relations for different moduli at the same time, the modulus is incorporated in the notation. In spite of the ternary notation, the congruence relation for a given modulus is binary. This would have been clearer if the notation $a \equiv_n b$ had been used, instead of the common traditional notation.

The properties that make this relation a congruence relation (respecting addition, s ubtraction, and mult iplication) are the following.

If

$$a_1 \equiv b_1 \pmod{n}$$

and

$$a_2 \equiv b_2 \pmod{n},$$

then:

- $(a_1 + a_2) \equiv (b_1 + b_2) \pmod{n}$
- $(a_1 - a_2) \equiv (b_1 - b_2) \pmod{n}$
- $(a_1 a_2) \equiv (b_1 b_2) \pmod{n}$.

Multiplicative group of integers modulo n

In modular arithmetic the set of congruence classes relatively prime to the modulus *n* form a group under multiplication called the **multiplicative group of integers modulo *n***. It is also called the group of **primitive residue classes modulo *n*.** In the theory of rings, a branch of abstract algebra, it is described as the group of units of the ring of integers modulo *n*. (Units refers to elements with a multiplicative inverse.)

This group is fundamental in number theory. It has found applications in cryptography, integer factorization, and primality testing. For example, by finding the order (ie. the size) of the group, one can determine if *n* is prime: *n* is prime if and only if the order is *n* - 1.

Group axioms

It is a straightforward exercCSE to show that under multiplication the congruence classes (mod *n*) which are relatively prime to *n* satisfy the axioms for an abelian group.
Because $a \equiv b \pmod{n}$ implies that $\gcd(a, n) = \gcd(b, n)$, the notion of congruence classes (mod *n*) which are relatively prime to *n* is well- defined.

Since $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$ implies $\gcd(ab, n) = 1$ the set of classes relatively prime to *n* is closed under multiplication.

The natural mapping from the integers to the congruence classes (mod *n*) that takes an integer to its congruence class (mod *n*) is a ring homomorphism. This implies that the class containing 1 is the unique multiplicative identity, and also the associative and commutative laws.

Given *a*, $\gcd(a, n) = 1$, finding *x* satisfying $ax \equiv 1 \pmod{n}$ is the same as solving $ax + ny = 1$, which can be done by Bézout's lemma.

Notation

The ring of integers (mod *n*) is denoted $\mathbb{Z}/(n)$ or (i.e., the ring of integers modulo the ideal $n\mathbf{Z} = (n)$ consisting of the multiples of *n*) or by $\mathbb{Z}_n$. Depending on the author its group of units may be written $(\mathbb{Z}/n\mathbb{Z})^*$, $(\mathbb{Z}/n\mathbb{Z})^\times$, $U(\mathbb{Z}/n\mathbb{Z})$, or $E(\mathbb{Z}/n\mathbb{Z})$ (for German *Einheit* = unit) or similar notations. This article uses

Structure

Powers of 2

Modulo 2 there is only one relatively prime congruence class, 1, so $(\mathbb{Z}/2\mathbb{Z})^\times \cong \{1\}$ is trivial.

Modulo 4 there are two relatively prime congruence classes, 1 and 3, so $(\mathbb{Z}/4\mathbb{Z})^\times \cong C_2$, the cyclic group with two elements.

Modulo 8 there are four relatively prime classes, 1, 3, 5 and 7. The square of each of these is 1, so $(\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2$, the Klein four-group.

Modulo 16 there are eight relatively prime classes 1, 3, 5, 7, 9, 11, 13 and 15. $\{\pm 1, \pm 7\} \cong C_2 \times C_2$ is the 2-torsion subgroup (ie. the square of each element is 1), so is not cyclic. The powers of 3, {1,3,9,11} are a subgroup of order 4, as are the powers of 5, {1,5,9,13}. Thus $(\mathbb{Z}/16\mathbb{Z})^\times \cong C_2 \times C_4$.

The pattern shown by 8 and 16 holds[1] for higher powers 2^k, $k > 2$: $\{\pm 1, 2^{k-1} \pm 1\} \cong C_2 \times C_{2^{k-2}}$ is the 2-torsion subgroup (so $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is not cyclic) and the powers of 3 are a subgroup of order 2^{k-2}, so $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong C_2 \times C_{2^{k-2}}$.

Powers of odd primes

For powers of odd primes p^k the group is cyclic:[2] $(\mathbb{Z}/p^k\mathbb{Z})^\times \cong C_{p^{k-1}(p-1)} \cong C_{\varphi(p^k)}$.

General composite numbers

The Chinese remainder theorem[3] says that if $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots,$ then the ring $\mathbb{Z}/n\mathbb{Z}$ is the direct product of the rings corresponding to each of its prime power factors:

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2}\mathbb{Z} \times \mathbb{Z}/p_3^{k_3}\mathbb{Z} \ldots$$

Similarly, the group of units $(\mathbb{Z}/n\mathbb{Z})^\times$ is the direct p roduct of the groups corresponding to each of the prime power factors:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{k_2}\mathbb{Z})^\times \times (\mathbb{Z}/p_3^{k_3}\mathbb{Z})^\times \ldots .$$

Order

The order of the group is given by Euler's totient function: $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n).$ This is the product of the orders of the cyclic groups in the direct product.

Exponent

The exponent is given by the Carmichael function λ(*n*), the least common multiple of the orders of the cyclic groups. This means that if *a* and *n* are relatively prime,

$$a^{\lambda(n)} \equiv 1 \pmod{n}.$$

Generators

$(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $\varphi(n) = \lambda(n).$ This is the case precCSEly when *n* is 2, 4, a power of an odd prime, or twice a power of an odd prime. In this case a generator is called a **primitive root modulo n**.

Since all the $(\mathbb{Z}/n\mathbb{Z})^\times,$ *n* = 1, 2, ..., 7 are cyclic, another way to state this is: If *n* < 8 then $(\mathbb{Z}/n\mathbb{Z})^\times$ has a primitive root. If *n* ≥ 8 $(\mathbb{Z}/n\mathbb{Z})^\times$ has a primitive root unless *n* is divisible by 4 or by two distinct odd primes.

In the general case there is one generator for each cyclic direct factor.

Table

This table shows the structure and generators of for small values of *n*. The generators are not unique (mod *n*); e.g. (mod 16) both {-1, 3} and {-1, 5} will work. The generators are listed in the same order as the direct factors.

$\varphi(20) = 8$ $(\mathbb{Z}/20\mathbb{Z})^\times$

For example take *n* = 20. means that the order of is 8 (i.e. there are 8 numbers less than 20 and coprime to it); λ(20) = 4 that the fourth power of any number relatively prime to 20 is ≡ 1 (mod 20); and as for the generators, 19 has order 2, 3 has order 4, and every member of $(\mathbb{Z}/20\mathbb{Z})^\times$ is of the form $19^a \times 3^b$, where *a* is 0 or 1 and *b* is 0, 1, 2, or 3.

The powers of 19 are {±1} and the powers of 3 are {3, 9, 7, 1}. The latter and their negatives (mod 20), {17, 11, 13, 19} are all the numbers less than 20 and prime to it. The fact that the order of 19 is 2 and the order of 3 is 4 implies that the fourth power of every member of $\mathbb{Z}_{20}^\times$ is ≡ 1 (mod 20).