

CDM

Permutations and Groups, II

Klaus Sutner

Carnegie Mellon University

Fall 2009

Outline

- 1 Some Groups
- 2 Subgroups and Homomorphisms
- 3 Group Representations
- 4 Congruences
- 5 The Word Problem

Implementing Groups

So how do we actually compute in a group? Let's focus on the finite case, for which there always is a brute-force solution – at least in principle.

Definition

Given a finite group $\mathcal{G} = \langle G, * \rangle$ the **Cayley table** or **multiplication table** of \mathcal{G} is an G by G matrix with entries in G : the entry in position (a, b) is $a * b$.

It is usually safe to assume that the group elements are represented by integers, so the size of Cayley table is $\Theta(n^2)$ using a uniform cost function.

That's OK for small n but not for larger ones.

More importantly, Cayley tables tend to shed little light on the structure of the group, all you have is a pile of data.

Small Groups

- $n = 1$: trivial group $\{1\}$

- $n = 2$: \mathbb{Z}_2

$$\begin{array}{cc} 1 & a \\ a & 1 \end{array}$$

- $n = 3$: \mathbb{Z}_3

$$\begin{array}{ccc} 1 & a & b \\ a & b & 1 \\ b & 1 & a \end{array}$$

$$n = 4$$

• \mathbb{Z}_4

1	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>b</i>	<i>c</i>	1
<i>b</i>	<i>c</i>	1	<i>a</i>
<i>c</i>	1	<i>a</i>	<i>b</i>

Kleinsche Vierergruppe

1	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	1	<i>c</i>	<i>b</i>
<i>b</i>	<i>c</i>	1	<i>a</i>
<i>c</i>	<i>b</i>	<i>a</i>	1

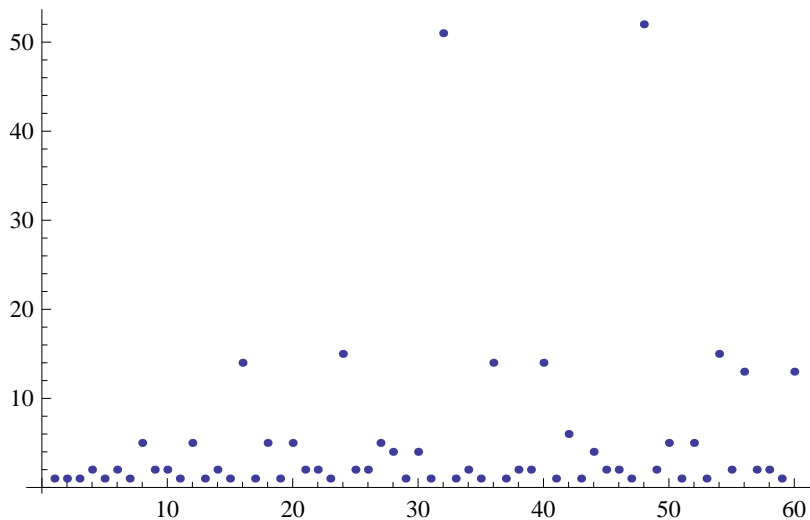
$$n = 5, 6$$

- $n = 5$: \mathbb{Z}_5
- $n = 6$: $\mathbb{Z}_6, \mathbb{S}_3$
- $n = 7$: \mathbb{Z}_7
- $n = 8$: 5 groups

It gets to be a bit tedious to write down these Cayley tables. Here is a count of the number of finite groups of size n for $n \leq 60$.

Note that the outliers at $n = 32$ and $n = 48$.

Counting Finite Groups



Cyclic Groups

A group G is **cyclic** if there is some element $a \in G$ such that

$$G = \{ a^i \mid i \in \mathbb{Z} \}$$

In this case a is called a **generator**.

If G is a finite cyclic group we have

$$G = \{ a^i \mid 0 \leq i < k \}$$

where k is the order of a (which is the size of G).

Note that in any finite group G and for any $a \in G$ the subgroup $\{ a^i \mid 0 \leq i < k \}$ is cyclic (with generator a).

Cyclic Groups are Boring

Up to isomorphism there is only one cyclic group of order k , and it is isomorphic to $\langle \mathbb{Z}_k, +, 0 \rangle$. A generator is 1.

Note that there are other generators, though: ℓ is a generator iff $\gcd(\ell, k) = 1$.

All cyclic groups are commutative.

Multiplicative Subgroup

Recall

$$\mathbb{Z}_n^* = \{x < n \mid \gcd(x, n) = 1\}$$

Example

Here is the Cayley table for \mathbb{Z}_{20}^* .

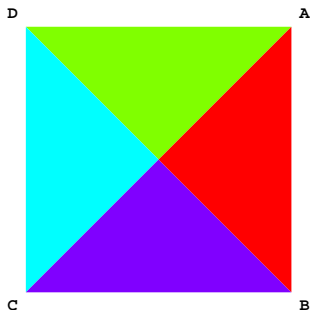
1	3	7	9	11	13	17	19
3	9	1	7	13	19	11	17
7	1	9	3	17	11	19	13
9	7	3	1	19	17	13	11
11	13	17	19	1	3	7	9
13	19	11	17	3	9	1	7
17	11	19	13	7	1	9	3
19	17	13	11	9	7	3	1

Note the subgroup $\{1, 3, 7, 9\}$ in the top-left corner.

Dihedral Groups

Recall the tic-tac-toe counting problem from above. To handle this and similar problems we need to deal with symmetries in the plane.

More precisely, consider the square with four vertices in positions $(\pm 1, \pm 1)$.



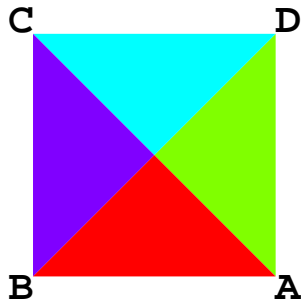
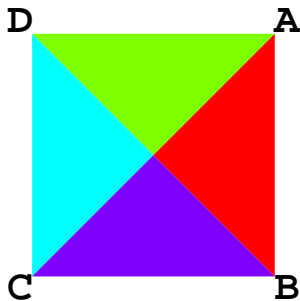
What are the rigid motions of the plane that leave the square unchanged in the sense that they place the square on top of itself?

Dihedral Groups, II

Your geometric intuition should tell you the following:

The motions that leave the square unchanged are precisely:

- Rotations around the origin by multiples of $\pi/2$
There are essentially only 4 of these, including the trivial one.
- Reflections along the axes and diagonals.
There are 4 of these.



Dihedral Groups, III

These motions naturally form a group: composition of motions is associative, the identity motion is admissible, every motion is reversible, and the composition of two admissible motions is again admissible.

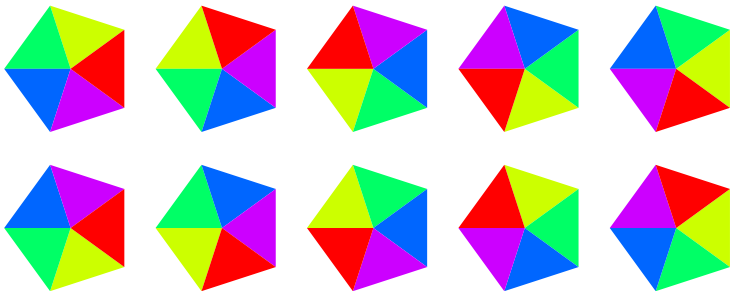
This group is called a **dihedral group** D_4 .

If we replace the square by a regular n -gon we obtain D_n : a group consisting of n rotations and n reflections.

Another tempting generalization is to 3-dimensional space (replace square by cube), but we won't pursue this here.

Pentagon

The symmetries of a pentagon, given by D_5 .



An Isomorphism

Proposition

The symmetric group on 3 points is isomorphic to the dihedral group D_3 .

Proof.

First note that both groups have size 6, so there is a chance the claim might be correct.

The permutations $f = (1, 2)$ and $g = (1, 2, 3)$ (in cycle notation) generate \mathbb{S}_3 , so we only need to find their counterparts in D_3 .

f corresponds to a reflection and g corresponds to a rotation.

□

Exercise

Check the details in the last argument. Why can this line of reasoning not be used to show that \mathbb{S}_n is isomorphic to D_n in general?

- Some Groups

② Subgroups and Homomorphisms

- Group Representations
- Congruences
- The Word Problem

Subgroups

Definition

Consider a group $\langle A, \cdot \rangle$. A **subgroup** of A is a set $B \subseteq A$ such that $\langle B, \odot \rangle$ is a group, where \odot is the restriction of \cdot to B .

This is always written $\langle B, \cdot \rangle$, no one bothers to distinguish between the full group operation \cdot and the restriction \odot . Note, though, that the group operation may be much easier to compute in the subgroup.

Example

- $\langle \mathbb{Q}, + \rangle$ is a subgroup of $\langle \mathbb{R}, + \rangle$.
- $\langle \mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{Q}, + \rangle$.
- $\langle 2\mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{Z}, + \rangle$.
- $\{1\}$ is the **trivial** subgroup of any group (written multiplicatively).

Testing Subgroups

Lemma

Let A be a group and $\emptyset \neq B \subseteq A$.

Then B is a subgroup of A if, and only if, $x, y \in B$ implies $x^{-1} \cdot y \in B$.

If the group is finite then it suffices that $x, y \in B$ implies $x \cdot y \in B$.

Proof.

The first part follows easily from the definition.

For the second part note that B must contain 1: as a finite semigroup B must contain an idempotent, which must be the identity in A . The map

$$B \rightarrow B, x \mapsto b \cdot x$$

is a permutation of B for each $b \in B$ (injective implies surjective in the finite case). But then for some $x \in B$: $1 = b \cdot x$ so we have closure under inverses.

□

Homomorphisms

A map from one group to another is mostly interesting if it preserves structure.

Definition

Suppose G and H are groups. A function $f : G \rightarrow H$ is a **(group) homomorphism** if

$$f(x \cdot y) = f(x) * f(y)$$

Here \cdot is the operation in G , and $*$ the operation in H .

If the function f is in addition injective then it is an **monomorphism**.

If the function f is in addition surjective then it is an **epimorphism**.

If the function f is in addition bijection then it is an **isomorphism**.

Usually one simply writes $f(xy) = f(x)f(y)$ and does not explicitly display the two different group operations.

Basic Properties

Proposition

Let $f : G \rightarrow H$ be homomorphism.

Then $f(1_G) = 1_H$ and $f(x^{-1}) = f(x)^{-1}$.

Example

- $f : G \rightarrow H, f(x) = 1$, is a homomorphism.
- $f : G \rightarrow G, f(x) = x$ is an isomorphism.
- $f : \mathbb{Z} \rightarrow \mathbb{Z}_m, f(x) = x \bmod m$ is an epimorphism.
- $\log : \mathbb{R}^+ \rightarrow \mathbb{R}$ is a isomorphism from $\langle \mathbb{R}^+, \cdot, 1 \rangle$ to $\langle \mathbb{R}, +, 0 \rangle$.

As the last example show, one does not always want to identify isomorphic groups. In fact, the whole purpose of logarithms is to translate multiplication into addition.

Kernels

Definition

The **kernel** of a homomorphism $f : G \rightarrow H$ is defined as

$$\ker f = \{ x \in G \mid f(x) = 1 \}.$$

Hence

$$f(x) = f(y) \iff y^{-1}x \in \ker f$$

This is slightly different from the kernel relations in combinatorics, but close enough to warrant the same name.

Note that f is injective (a monomorphism) iff the kernel is trivial: $\ker f = 1$.

Proposition

The kernel of a homomorphism is always a subgroup.

Cayley's theorem

Theorem (Cayley)

Every group is isomorphic to a subgroup of a permutation group.

Proof. Let $\mathcal{A} = \langle A, \cdot \rangle$ be a group, and let \mathbb{S}_A be the full permutation group over A . Define a map

$$\begin{aligned}\varphi : \mathcal{A} &\rightarrow \mathbb{S}_A \\ \varphi(a)(x) &= x \cdot a\end{aligned}$$

Then φ is a homomorphism: $\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$. Moreover, φ is mono: the kernel is just $1 \in A$. Hence, the range of φ is a subgroup of \mathbb{S}_A that is isomorphic to \mathcal{A} . □

Note that this representation is not too helpful computationally: each permutation in \mathbb{S}_A has the same size as A .

- Some Groups
- Subgroups and Homomorphisms
- ③ Group Representations
 - Congruences
 - The Word Problem

Representing Dihedral Groups

For simplicity, here is the special case D_4 .

- 1: identity
- $\alpha, \alpha^2, \alpha^3 = \alpha^{-1}$: rotations
- $\beta, \alpha^2\beta$: reflections along axes
- $\alpha\beta, \alpha^3\beta$: reflection along diagonals

You have to check that this is geometrically correct.

This is clear for the rotations α^i , but the reflections require a little check. In particular it is not clear that there is a single reflection β such that all others can be expressed in terms of β and rotations.

Exercise

Check the details.

Simplification Rules

Now for the important part: we don't need the multiplication table, since we can just "multiply" these words over the alphabet $\{\alpha, \beta\}$.

$$\alpha^2 \cdot \alpha^3 \beta = \alpha^5 \beta = \alpha \beta$$

Here we have used the first of the following simplification rules:

- $\alpha^4 = 1$,
- $\beta^2 = 1$,
- $\alpha\beta = \beta\alpha^3 = \beta\alpha^{-1}$.

As is customary in this context, we have written 1 to express the empty word.

Note that this group is not commutative.

The General Case

What is the structure of a dihedral group D_n in general?

Exactly the same, we only need to replace 4 by n . No extra work is needed.

- $\alpha^n = 1$,
- $\beta^2 = 1$,
- $\alpha\beta = \beta\alpha^{n-1} = \beta\alpha^{-1}$.

Very elegant.

Exercise

Check that this description holds in general for all n . Make sure to distinguish between even and odd n .

Normal Form

It follows that every element can be written in the form

$$\alpha^i \quad \text{or} \quad \beta\alpha^i$$

where $0 \leq i < n$.

- The α^i are all the pure rotations.
- The $\beta\alpha^i$ are all the combined rotations cum reflection along a particular axis, which produces arbitrary reflections.

To multiply two elements, we concatenate the words and then apply the simplification rules until we are back in normal form.

Simplification in D_4

Here is an example of how this simplification process works:

$$\alpha\alpha\beta\beta\beta\alpha\beta\alpha$$

$$\alpha\alpha\beta\alpha\beta\alpha$$

$$\alpha\beta\alpha^{-1}\alpha\beta\alpha$$

$$\alpha\beta\beta\alpha$$

$$\alpha^2$$

It is not clear that application of the rules in a different order could not produce a different result, but one can prove that one always gets to the same normal form.

Finitely Presented Groups

Hence we can describe the dihedral group D_n very compactly by

$$\langle \alpha, \beta; \alpha^n = 1, \beta^2 = 1, \alpha\beta = \beta\alpha^{-1} \rangle$$

This means: there are two special elements α and β , and all the other elements can be obtained from these two by arbitrary combinations subject to the rules indicated.

Again, there is no need for a multiplication table of size $(2n)^2$.

We can just form products of α 's and β 's and apply the simplification rules given.

Another Example

Here is just one other example of a finitely presented group. There are $n - 1$ generators g_1, g_2, \dots, g_{n-1} and the relations are

$$\begin{aligned}g_1^2 &= 1 \\(g_i g_{i+1})^3 &= 1 \quad \text{for } i < n - 1 \\(g_i g_j)^2 &= 1 \quad \text{for } j < i - 1\end{aligned}$$

Note how it is entirely unclear what the size of this group is, or what its properties might be. It requires a bit of effort to establish the following characterization.

Lemma

The group defined by these rules is (isomorphic to) the symmetric group on n points. Hint: figure out what the g_i are.

- Some Groups
- Subgroups and Homomorphisms
- Group Representations
- ④ Congruences
 - The Word Problem

Subgroups and Partitions

To explain more carefully how the last construction works we need to consider good equivalence relation on groups. This will also be crucial for applications to counting.

Definition

Suppose G is a finite group. Fix a subgroup H of G , let $a \in G$. Define

$$\begin{aligned}x \sim_H y &\iff x^{-1}y \in H \\ a \cdot H &= \{ a \cdot b \mid b \in H \}\end{aligned}$$

\sim_H is the **equivalence induced by H** . The sets $a \cdot H$ are the **(left) cosets** of H in G , and the number of such cosets is the **index** of H in G , written **$[G : H]$** .

One can define right cosets in an analogous way.

Example 1

Let G be the integers under addition and $H = m\mathbb{Z}$. Then

$$\begin{aligned}x \sim y &\iff y - x \in m\mathbb{Z} \\ &\iff x = y \pmod{m}\end{aligned}$$

H is the kernel of the epimorphism $x \mapsto x \bmod m$.

Example 2

Let G be the group of all permutations on $[n]$. Define

$$f(x) = \begin{cases} 0 & \text{if } x \text{ is even,} \\ 1 & \text{otherwise.} \end{cases}$$

Then f is homomorphism from G to the additive group \mathbb{Z}_2 .

The kernel of f is the subgroup

$$H = \{x \in G \mid x \text{ even}\}$$

Note that $|H| = |G|/2 = n!/2$.

Example 3

Consider the multiplicative group

$$G = \mathbb{Z}_{13}^* = \{1, 2, \dots, 12\}$$

We one can check that $H = \{1, 3, 9\}$ is a subgroup with cosets

$$H = \{1, 3, 9\}, 2H = \{2, 5, 6\}, 4H = \{4, 10, 12\}, 7H = \{7, 8, 11\}$$

The multiplication table for G/H written with canonical representatives is

1	2	4	7
2	4	7	1
4	7	1	2
7	1	2	4

and is isomorphic to the additive group \mathbb{Z}_4 .

Compare to Plain Sets

This should look rather familiar by now: we have used plain functions

$$f : A \rightarrow A$$

to describe equivalence relations on sets (canonical selector function).

Now we use subgroups to describe special equivalence relations on (the carrier sets of the) groups. But these subgroups are all kernels of appropriate homomorphisms.

Of course, not all equivalence relations can be obtained via homomorphisms, but those that are so obtained have particularly good properties.

Exercise

Show that for H the kernel of a homomorphism our definition of \sim_H is the same as in the set case.

Partition Size

Lemma

\sim_H is an equivalence relation on G , and the equivalence classes of \sim_H all have the same size $|H|$.

Proof.

Reflexivity follows from $1 \in H$.

Symmetry since $x^{-1}y \in H$ implies $(x^{-1}y)^{-1} = y^{-1}x \in H$,

Transitivity since $x^{-1}y, y^{-1}z \in H$ implies $x^{-1}z \in H$.

For the second claim note that $[x]_{\sim} = xH$.

But $z \mapsto xz$ is a bijection from H to xH . □

Lagrange's theorem

Theorem (Lagrange)

Let G be a finite group, and H any subgroup of G . Then $|G| = |H| \cdot [G : H]$.

In particular, $|H|$ divides $|G|$.

Note how algebra produces a stronger result here: if we look at arbitrary functions $f : A \rightarrow B$ then any equivalence relation arises as a kernel relation.

But if we consider groups and homomorphisms we get only very special equivalence relations.

This restriction will turn out to be very helpful to answer counting problems such as the tic-tac-toe question from above.

Application

As a special case the order of any group element divides the order (cardinality) of the whole group.

Hence for $n = |G|$, $a \in G$ we have $a^n = 1$.

This provides a simple proof for the famous Euler-Fermat theorem.

Recall that \mathbb{Z}_m^* is the group of elements in \mathbb{Z}_m that have multiplicative inverses.

Also, $\varphi(m)$ is Euler's totient function: $\varphi(m) = |\mathbb{Z}_m^*|$.

Theorem (Euler-Fermat)

The order of $a \in \mathbb{Z}_m^$ divides $\varphi(m)$.*

Congruences

Definition

Suppose G is a group and \sim an equivalence relation on G . \sim is a **congruence** if for all $x, y, u, v \in G$:

$$x \sim y, u \sim v \text{ implies } xu \sim yv.$$

Congruences are very important since they make it possible to define a group structure on the quotient set G/\sim :

$$[x] \cdot [y] = [x \cdot y]$$

Why? Suppose $[a] = [a']$ and $[b] = [b']$. Then our definition makes sense only if $[ab] = [a'b']$.

But that's exactly what the congruence property guarantees.

Congruences and Homomorphisms

Unfortunately, the equivalence relations \sim_H are not congruences in general. We need another condition to get a congruence.

Definition

Let H be a subgroup of G . H is a **normal subgroup** if for all $a \in G$ $aH = Ha$.

Note that in a commutative group any subgroup is normal.

Proposition

If H is a normal subgroup then \sim_H is a congruence.

Proposition

H is the kernel of a homomorphism $f : G \rightarrow G'$ iff H is normal.

Exercise

Prove these propositions.

Example: Chinese Remainder

You know this already. E.g., let p and q be two distinct primes.

$$f : \mathbb{Z} \rightarrow \mathbb{Z}_p \times \mathbb{Z}_q$$
$$f(x) = (x \bmod p, x \bmod q)$$

Then $H = pq\mathbb{Z}$ and the quotient is $\mathbb{Z}/(pq\mathbb{Z}) = \mathbb{Z}_{pq}$.

One can show that f is an epimorphism (this requires a little argument).

Hence \mathbb{Z}_{pq} is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_q$.

So?

Hence we can either compute

- with one number modulo pq , or
- with two numbers, one modulo p and the other modulo q .

\mathbb{Z}_{pq} and $\mathbb{Z}_p \times \mathbb{Z}_q$ are isomorphic, but computationally there is a difference. This can be exploited sometimes to fake high-precision computations with small word sizes.

Also note that the correctness proof for RSA more or less requires the product representation.

Word Processing in Groups

Recall our clever description for dihedral groups:

$$\langle \alpha, \beta; \alpha^n = 1, \beta^2 = 1, \alpha\beta = \beta\alpha^{-1} \rangle$$

We can also think of α and β as pure letters, say, a and b for clarity. Then there is a homomorphism from the monoid of all words over $\{a, b\}$ to the group

$$\eta : \{a, b\}^* \rightarrow G$$

which is given by $f(a) = \alpha$ and $f(b) = \beta$. The word equations

$$a^n = 1, b^2 = 1, ab = ba^{n-1}$$

describe the kernel K of f .

Quotients, Again

In other words, for any $w \in \{a, b\}^*$ we have $f(w) = 1$ iff w can be reduced to 1 (if you prefer: the empty word) by repeated application of the rewrite rules.

The quotient of the monoid $\{a, b\}^*$ by K is isomorphic to the group G .

Algebraically, there is no difference between G and the quotient structure: exactly the same equations hold in both.

The great advantage of this representation is that we can easily manipulate words, but may not have a direct handle on the group elements (even for dihedral groups where we can handle the group elements the word representation is computationally easier).

Automatic Groups

In fact, we can use finite state machines to perform operations on the words representing group elements.

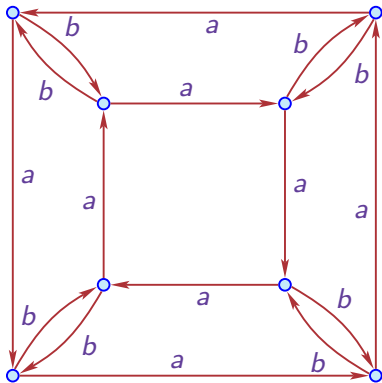
For example, we might try to find a FSM M_1 that, given a word w over $\{a, b\}$ determines whether $f(w) = 1$.

Likewise, we can have machines for multiplication. This is technically a little tricky since we need two words as input (and cannot simply read first u and then v ; rather, we must read both words simultaneously using a product alphabet).

Groups that can be described by finite state machines have a particularly good structure and are well understood.

Example: D_4

The minimal DFA that checks identity in D_4 .



Interpretation:
 inner states: α^i
 outer states: $\alpha^i\beta$

Any state can be chosen as
 initial and final state.

Digression: Counting Identities

How many words over $\{a, b\}^*$ of length n are there that denote the identity in D_4 ?

This may seem like a hard problem, but given the DFA one can easily experiment. Here is a census for words up to length 12:

n	0	1	2	3	4	5	6	7	8	9	10	11	12
#	1	0	1	0	4	0	16	0	64	0	256	0	1024

The conjecture is now obvious: for length $2n > 0$ there are 2^{2n-2} words that denote the identity.

Exercise

Prove this conjecture.

Constructing Groups

We started from a concrete group, and found a nice description for it. But we can also go backwards and start with a description (assuming that we really describe a group).

For example, what is the group described by

$$G = \langle a; a^6 = 1 \rangle$$

Here the reduced elements are of the form $\{1, a, aa, aaa, aaaa, aaaaa\}$.

So we get the none other than the cyclic group \mathbb{Z}_6 .

Exercise

Give a representation for $\mathbb{Z}_n \times \mathbb{Z}_m$.

Exercise

Give a representation for the full permutation group on n points.

- Some Groups
- Subgroups and Homomorphisms
- Group Representations
- Congruences
- ⑤ The Word Problem

Putting Things Together

Here is a slightly more general problem: suppose we want to generate a group H that is given implicitly by some finite representation

$$H = \langle g_1, \dots, g_k ; E_1, \dots, E_l \rangle$$

where the E_i are equations using the generators such as $g_1^2 = 1$, $g_2g_3 = g_3g_2$ and so on.

In principle, there is a simple algorithm: we start with the identity element, and keep multiplying what we already have by the generators. Multiplication $y = x * g$ is done by concatenating words, and then simplifying according to the rewrite rules E_i .

Example

$\langle a ; a^n = 1 \rangle$ will produce the elements $a, a^2, \dots, a^{n-1}, 1$, in this order.

Generating the Dihedral Group

Suppose we use two generators a and b and the three rules

$$a^4 = 1, b^2 = 1, ab = ba^3.$$

Then our algorithm will produce the elements

$$1, a, b, aa, baaa, ba, aaa, baa$$

in the given order.

Some Problems

In general, the group H will be infinite, so the algorithm may not terminate. E.g., think about

$$H = \langle a; - \rangle$$

There is one generator, but no simplification rules at all.

This should produce (a group isomorphic to) \mathbb{Z} , rather than just a semigroup. At present, our algorithm fails in this sense (apart from not terminating).

The solution is to add inverses to the generators:

For every letter g also include another letter \bar{g} and the rules

$$g\bar{g} = \bar{g}g = 1$$

Enlarging the Alphabet

Then for the enlarged alphabet

$$\Sigma = \{g_1, \dots, g_k, \bar{g}_1, \dots, \bar{g}_k\}$$

we have a homomorphism (of monoids)

$$\eta : \Sigma^* \rightarrow H$$

that evaluates the words over Σ to the corresponding group elements according to the defining relations. Needless to say

$$\eta(\bar{g}) = \eta(g)^{-1}.$$

Exercise

Explain why it is not necessary to enlarge the alphabet whenever H is finite.

More Word Processing

Another problem is that the simplification may not be so easy: for this algorithm to work we need to be able to check if a newly generated word u represents the same group element as some already encountered word v .

Since witnesses are not unique in general, to check equality we will need some kind of normal form, some canonical way to write u and v in terms of the generators. We could agree that the length-lex minimal word is the right normal form, but how do we compute this particular representation?

Our only hope is to check whether

$$uv^{-1} \text{ somehow simplifies to } 1$$

using the given rewrite rules. Note that it is convenient to have formal inverses for this approach.

The Word Problem

Problem:	Word Problem
Instance:	Generators A , rewrite rules R and a word w in Σ^*
Question:	Can w be simplified to 1, using the given rules?

Theorem (Novikov, Boone, Britton)

The Word Problem is undecidable in general.

In fact, the Word Problem remains undecidable for some fixed A and R .

But as we have seen, for some sufficiently simple groups the word problem can even be handled by a finite state machine.

Opening the Flood Gates

The proof ideas for this theorem were then used to show that just about any question about a finitely presented group G turns out to be undecidable.

- **Word Problem:** Given a word w , does it denote 1?
- **Finiteness:** Is G finite?
- **Commutativity:** Is G commutative?
- **Cyclicity:** Is G cyclic?
- **Isomorphism:** Given two such groups, are they isomorphic?

Of course, special cases are decidable. But in general finitely presented groups are too complicated to be handled computationally.

A Bizarre Result

Here is a result that shows how atrociously complicated finitely presented groups can be.

Theorem (Novikov)

There is a finitely presented group that contains an isomorphic copy of every finitely presented group.

This sounds utterly impossible at first glance: there are only countably many finitely presented groups and they can surely be wrapped up into a single group. But why should that group be finitely presented itself?

But, Novikov's theorem is a consequence of computability theory and a result in group theory: a finitely generated group is isomorphic to a subgroup of a finitely presented one if, and only if, it is recursively presented (replace finitely many equations with a semi-decidable set of equations).

Practical Computing in Groups

There is still a lot that can be computed effectively and even efficiently in groups, though some of the algorithms are quite sophisticated (and incorporate a lot of group theory knowledge).

An excellent public domain package for computational group theory is GAP, available at

`http://www-gap.dcs.st-and.ac.uk/~gap`

Rather large groups such as the group of motions of Rubik's Cube can easily be handled easily by GAP.

There is even a group at CUNY (Baumslag) that tries to implement an interactive system that can be used to solve undecidable problems in group theory – at least in some cases.

Summary

- Groups are a natural generalization of permutation together with composition.
- The idea to study abstract groups is one of the big breakthroughs of 19th century mathematics.
- Some basic computations in finite groups can be carried out efficiently and there are excellent system to do these computations.
- However, in general essentially all questions about finitely presented groups turn out to be undecidable. The word problem is the classical example.
- We will use permutation groups to tackle counting problems.