Computational Group Theory

Soria Summer School 2009
Session 1: Basics from group theory

Technische Universiteit
Eindhoven
University of Technology

July 2009 Hans Sterk (sterk@win.tue.nl)

Where innovation starts

Overview

This course focuses on some computational aspects in group theory

- Basics on groups
- Permutation groups
- Coset enumeration
- Mathieu groups

There are other areas where computations with groups come up, such as invariant theory

Some useful literature:

- G. Butler: *Fundamental algorithms for permutation groups*
  Lecture Notes in Computer Science 559 (1991). Springer-Verlag
- Derek F. Holt, Bettina Eick, Eamonn A. O'Brien: *Handbook of computational group theory*
  Chapman & Hall/CRC (2005)
- Arjeh M. Cohen, Hans Cuypers, Hans (Eds.): *Some tapas of computer algebra.* Algorithms and Computation in Mathematics, vol 4 (1999). Springer-Verlag
  (In particular, Chap 8: *Working with finite groups*; Project 6: *The small Mathieu groups*)

Groups

Groups occur in various settings:

- As an abstract ‘computational structure’: a set plus decent multiplication
- As a structure in a range of structures: groups, rings, fields, etc.
- As a means to catch symmetries, like the symmetries of a cube, or a more advanced structure
- As a means to do geometry à la Klein: the (transformation) groups determine the geometry:
  - spherical geometry
  - hyperbolic geometry
  - euclidean geometry
- Also: geometry and other structures inspire group theory
  - Automorphisms of structures like ‘algebraic curves’

Groups

Group: a set G together with an operation $G \times G \longrightarrow G$ such that

- **associativity:** $(a * b) * c = a * (b * c)\ \forall a, b, c \in G$
- **unit element:** there exists $e \in G$ s.t. $e * g = g * e = g\ \forall g \in G$
- **inverse elements:** for every $g \in G$ there is a $g^{-1} \in G$ with $g * g^{-1} = g^{-1} * g = e$

Remarks:

- There is a *unique* unit element:
$$e = e * e' = e'$$
- Inverses are unique, hence the notation g^{-1}
$$h = h * e = h * (g * h') = (g * h) * h' = e * h' = h'$$

(Homo)morphism: $f : G \longrightarrow G'$ s.t.

$$f(gh) = f(g)f(h)$$

Kernel: $\{g \in G \mid f(g) = e\}$; **Image:** $f(G)$

Subgroups and normal subgroups

- **Subgroup** $H < G$:
  a subset which is a group wrt $*$
  - Permutations: $S_3 < S_4$
- **Normal subgroup** $N \triangleleft G$:
  subgroup N s.t. $gN = Ng$ for all $g \in G$, or

$$gng^{-1} \in N \quad \text{for all } g \in G,\ n \in N$$

  - $A_3 < S_3$, where A_n denotes even permutations
  - Kernels of morphisms $f : G \to G'$ of groups

$$\{g \in G \mid f(g) = e_{G'}\}$$

Constructions with groups

- **(Direct) product group $G \times H$:**

$$\{(g,h) \mid g \in G,\, h \in H\}$$

  with coordinatewise multiplication

  – $\mathbf{Z} \times \mathbf{Z}$

- **Semi-direct product $G = N \rtimes H$:**

  – N is a normal subgroup, H a subgroup

  – $G = NH$ and $N \cap H = \{e\}$

  Also from 2 groups N and H and morphism $\phi : H \to \mathrm{Aut}(N)$

$$(n_1, h_1) * (n_2, h_2) = (n_1 \phi_{h_1}(n_2), h_1 h_2)$$

  – Translations, orthogonal transformations within isometries of a euclidean vector space

- **Quotient group:** G/N, where N is a normal subgroup

A semidirect product: isometries of the plane

- V: euclidean plane, 'say', $\mathbf{R}^2$
- Isometry $A : V \to V$ with

$$d(Av, Aw) = d(v, w) \quad \text{for all } v, w \in V$$

  - Translation T_a with $T_a(v) = v + a$
  - Orthogonal linear transformations

$$(Av, Aw) = (v, w) \quad \text{for all } v, w \in V$$

- Subgroup of translations $\mathcal{T}$ is normal:

$$g^{-1}T_a g(v) = g^{-1}(g(v) + a) = v + g^{-1}(a) = T_{g^{-1}(a)}(v)$$

- Every isometry is a composition of a translation and an orthogonal map

Related: Affine linear transformations of an affine space ('vectorspace without origin')

Quotients

$N \lhd G$

- **Left and right cosets**

$$aN = \{an \mid n \in N\}, \quad Nb = \{nb \mid n \in N\}$$

For normal subgroups: $aN = Na$, since $aNa^{-1} = N$

- Quotient as set: $G/N = \{aN \mid a \in G\}$
- Product:

$$(aN) * (bN) = (ab)N$$

This works well since

$$(aN)(bN) = a(Nb)N = abNN = abN$$

Note that the left (resp.) right cosets partition G. If G is finite:

$$|G/N| = |G|/|N|$$

Technische Universiteit Eindhoven University of Technology

Further examples

- $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$,... with addition
- $\mathbf{Z}/n\mathbf{Z}$ (or $\mathbf{Z}_n$) with addition
- $\mathbf{Z}^*$, $\mathbf{Q}^*$,... the invertible elements wrt multiplication
- Likewise: $\mathbf{Z}_8^* = \{1, 3, 5, 7\}$
- Matrix groups, such as
  - The general linear group over a field K

    $$GL_n(K): \quad n \times n \text{ invertible matrices}$$

    wrt to multiplication
  - The special linear group over a field K

    $$SL_n(K) = \{A \in GL_n(K) \mid \det(A) = 1\}$$

  - The orthogonal group over K

    $$O_n(K) = \{A \in GL_n(K) \mid A \cdot A^\top = I\}$$

    $SO_n(K)$: subgroup with extra condition $\det(A) = 1$

Technische Universiteit Eindhoven University of Technology

Details and examples: groups

Presentations: Groups given by generators and relations/relators

$$G = \langle S \mid R \rangle$$

G is the quotient of the free group on S by the normal closure of $\langle R \rangle$

- **Cyclic group** presented in such a way:

  $$G = \langle x \mid x^5 \rangle$$

  Compute with element x, but x^5 can be simplified to the unit element e. In particular, the elements are e, x, x^2, x^3, x^4, so a cyclic group of order 5

- **Coxeter group:**

  $$G = \langle x, y \mid x^2, y^2, (xy)^3 \rangle$$

  A 'concrete' version of it:

  x reflection in the x_1-axis
  y reflection in $x_2 = \sqrt{3}\, x_1$

  Based on the observation that the product of these two reflections is a rotation over 120°.
  Or take permutations: $x = (1, 2)$, $y = (2, 3)$, $xy = (1, 3, 2)$

- **Icosahedral rotation group:** $\langle s, t \mid s^2, t^3, (st)^5 \rangle$

Technische Universiteit Eindhoven University of Technology

Permutation groups

- **Symmetric group** $\mathrm{Sym}(\Omega)$, where Ω is a set: all permutations/bijections of Ω. For $\Omega = \{1, 2, \ldots, n\}$: S_n
- **Special case:** S_n
  - Disjoint cycle notation:
  $$(1, 3, 4)(2, 5) \in S_5$$
  - Product of transpositions:
  $$(1, 3)(2, 3)(3, 5) \in S_5$$
  - The **sign** of a permutation: parity (± 1) of the number of pairs $i < j$ s.t. $\sigma(i) > \sigma(j)$
  - The sign is multiplicative:
  $$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma) \cdot \mathrm{sgn}(\tau)$$
  So a surjective morphism $\mathrm{sgn} : S_n \to \{\pm 1\}$
  - The sign of a (single) transposition is -1
  - $\mathbf{A}_n$: the normal subgroup of even permutations, of index 2 in S_n
- **Permutation group:** subgroup of some $\mathrm{Sym}(\Omega)$

These occur e.g. in symmetries of discrete structures

Technische Universiteit Eindhoven University of Technology

Group actions

Group action: group G acts on set X

$$x^g$$

such that $(x^g)^h = x^{gh}$

- Groups of matrices acting on vector subspaces
- $O_n(\mathbf{R})$ acting on the unit sphere S^{n-1}:

$$\underline{v}A$$

- A group G acting on itself:

$$g^h := g \cdot h$$

  (right multiplication with h)

More on group actions

For a group G acting on Ω:

- **G-orbit of $\omega \in \Omega$:**
$$\omega^G = \{\omega^g \mid g \in G\}$$
- **Stabilizer G_ω**: group elements fixing ω.

Example: $SO_3(\mathbf{R})$ acts on S^2

- Orbit of $\omega \in S^2$ is S^2 itself
- Stabilizer of $(0,0,1)$: rotations around z-axis, which is a S^1.

Some words on GAP

GAP: Groups, algorithms, programming

- A free system for computational discrete algebra
- Designed for studying groups, rings, vector spaces, algebras, ...

Sample commands

- Introduce permutations:

```
s:=(1,2); t:=(2,3);
```

- Action of $(1, 2, 3)$ on 1:

```
1^(1,2,3);
```

- Introduce a group:

```
s3:=Group(s,t);
```

- Compute the order of an element:

```
Order(s);
```

- Compute the order of the group:

```
Order(s3);
```


Technische Universiteit Eindhoven University of Technology

Elementary algorithms: basics on S_n

Algorithms to compute with basic permutations:

- Write a permutation as a product of disjoint cycles
  - If $2, 3, 1, 5, 4$ are the images of $1, 2, 3, 4, 5$, then you
  - first trace to what cycle 1 belongs: $(1, 2, 3)$
  - Then look at what happens to 4: $(4, 5)$
- Write a permutation as a product of transpositions
  - For instance using $(a_1, a_2, \ldots, a_k) = (a_k, a_{k-1})(a_{k-1}, a_{k-2}) \cdots (a_2, a_1)$
- Determine the sign of a permutation
  - Use the multiplicative property of the sign

Technische Universiteit Eindhoven University of Technology

Elementary algorithms: list of elements

From generator set S to a list of elements

- Start: $\{e\} \cup S$
- Append for each pair (g, h) of elements in list so far: gh if gh not yet in.

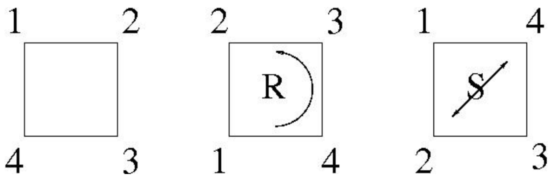
Of course, efficiency is an issue.

Improvements:

- Consider only products $g * s$ with g in list and $s \in S$
- Use subgroups $H_i = \langle S_i = \{s_1, \ldots, s_i\}\rangle$. Then construct elements of H_i from those of H_{i-1} by adding whole cosets:
  - Input: $G = \langle S \rangle$ and list of elements of H_{i-1}
  - Output: list of elements of H_i
  - Start: Coset-Reps:=$\{e\}$
  - For each $g \in$Coset-Reps, do the following:
  - for every generator $s \in S_i$: if $gs \notin$ list, then append gs to Coset-Reps, and coset $H_{i-1}gs$ to list, etc.

Technische Universiteit Eindhoven University of Technology

An example: the square



Elements: $e, r, r^3, r^3, s, rs, r^2s, r^3s$, $G = \langle s, r \rangle$, subgroup $H = \{e, s\}$

- The list starts with e, s and coset representative e
- Take the next generator r, not in $\{e, s\}$, so add the coset $\{r, sr = r^3s\}$ to the list:

  $$\text{list} \; : e, s, r, r^3s$$

  The Coset-Rep becomes $\{e, r\}$
- Next we check products of elts of Coset-Rep and generators s and r:

  $$e * s = s \text{ not new}, \;\; r * s = \;\text{ new}$$

  So add rs and add the coset $\{rs, srs = r^3\}$:

  $$\text{list} \; : e, s, r, r^3s, rs, r^3$$

  with Coset Rep = $\{e, r, rs\}$
- And one more coset to add.

Some exercises

1) Show that the 'factors' $G \times \{e_H\}$ and $\{e_G\} \times H$ are normal subgroups of the direct product $G \times H$.

2) If $G = \langle x, y \mid x^2, y^2(xy)^3 \rangle$, show that $|G|$ is at most 6, straight from the presentation.

3) Use a picture to write down symmetries of an equilateral triangle.

4) For the symmetries of the square $G = \langle s, r \rangle$ list the elements using the above algorithm but now with generators r (rotation) and s (reflection) in that order, and starting from the list of elements of the subgroup $\langle r \rangle$.