2011–12–20

Lecturer: Bengt E W Nilsson

Three parts in this course: finite groups, infinite groups, and Lie algebras. Finite groups: can be used to solve polynomial equations. We can prove that it is possible to solve all quartic and cubic equations, and that there is no general solution to fifth-order polynomial equations — prove it, using finite groups.

Definition: Group G, elements $g_i \in G$. Axioms:

1. Closure under composition. (An abstract operation you can do with the elements.)
2. Associativity.
3. $\exists$ a (unique) unit element e.
4. $\exists$ an inverse g^{-1} for any $g \in G$. (The inverse is also unique.)

Recall: $\mathrm{SL}(2,\mathbb{Z})$ means:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a,b,c,d \in \mathbb{Z}, \quad \det(g) = 1.$$

The S of $\mathrm{SL}(2,\mathbb{Z})$ means $\det(g) = 1$; the L means matrix, the 2 of $\mathrm{SL}(2,\mathbb{Z})$ means 2×2 matrices, and $\mathbb{Z}$ is the integers.

Closure: yes. Associativity: naturally. Unit element: unit matrix. What about inverse? Works too.

Example: $\mathbb{Z}$ under multiplication? Not a group. (The inverse of 2, for instance, is not an integer.)

Example: $\mathbb{Z}$ under addition? OK.

Example: $\mathbb{N}^* = \mathbb{Z}^+$? Not a group.

Example: SU(2). This describes spin in quantum mechanics. This is a continuous group:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a,b,c,d \in \mathbb{C}, \quad U^\dagger U = \mathbb{1}, \quad \det(U) = 1.$$

Claim:

$$U = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}, \quad \text{with } \det(U) = a\,\bar{a} + b\bar{b} = 1.$$

Then

$$U^\dagger = \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} \quad \Rightarrow \quad U^\dagger U = \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix} \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Check $U_1 U_2 \equiv U_3 \in \mathrm{SU}(2)$ for any U_1 and U_2: OK!

Put

$$\begin{cases} a = x_1 + \mathrm{i}\, x_2 \\ b = x_3 + \mathrm{i}\, x_4 \end{cases}, \quad \text{then} \quad \det(U) = 1 \Longleftrightarrow x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1.$$

This is the equation for the three-sphere S^3 embedded in $\mathbb{R}^4$. So $\mathrm{SU}(2) \approx S^3$. This group is a manifold. In this case SU(2) is *connected*: you can go from any point to any other by a path; and *simply connected:* any loop is contractible to a point.

(Compare loops on a torus: some loops are contractible, but there are loops that are not contractible — not simply connected.)

Example: SU(2) is related to SO(3), which is the group of rotations in $\mathbb{R}^3$. SU(2) $\approx S^3$, but SO(3) $\approx \mathbb{R}\mathrm{P}^3$ is like a half-sphere with opposite points identified. $\mathbb{R}\mathrm{P}^3$ is not simply connected.

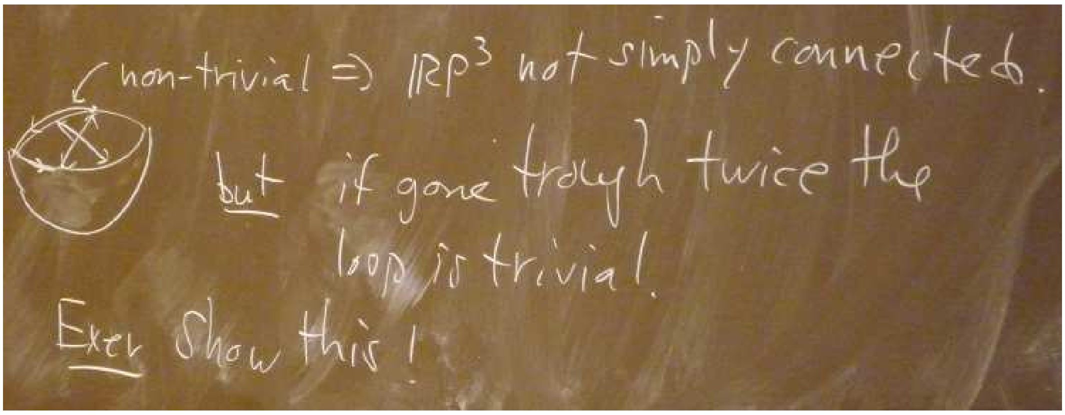
non-trivial ⇒ ℝP³ not simply connected.
but if gone trough twice the loop is trivial.
Exer Show this!

Figure 1. A non-trivial loop. But if you go through it twice, the loop is trivial.

Exercise: Show this!

Example: U(1): $u \in \mathbb{C}$ such that $|u| = 1 \Rightarrow u = \mathrm{e}^{\mathrm{i}\theta}$.

$$u_1\, u_2 = \mathrm{e}^{\mathrm{i}\theta_1}\, \mathrm{e}^{\mathrm{i}\theta_2} = \mathrm{e}^{\mathrm{i}(\theta_1+\theta_2)} = \mathrm{e}^{\mathrm{i}\theta_3} = u_3.$$

The composition is multiplication. The addition of these u_i's is not in the group. (Not a group under addition: not a vector space). In the exponents, you *can* add the θ_i's, however.

Example: $q \in \mathrm{SU}(2)$: $q =$ unit element in $\mathbb{H}$, in the sense $\sum_i q_i^2 = 1$:

$$q = q_0 + q_1\,\mathrm{i} + q_2\,\mathrm{j} + q_3\,\mathrm{k}:$$

$$\mathrm{i}, \mathrm{j}, \mathrm{k}: \quad \mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1, \quad \mathrm{i}\,\mathrm{j} = \mathrm{k}\ (\text{cyclic i j k}), \quad \mathrm{i}\,\mathrm{j} = -\mathrm{j}\mathrm{i}.$$

Note: In Cartan's classification of Lie groups: A_n, B_n, C_n, D_n...

$$A_1: \quad \mathrm{SO}(3), \mathrm{SU}(2), \mathrm{SL}(2, \mathbb{R}), \mathrm{SL}(2, \mathbb{C})$$

These groups are really the same, if you allow the coefficients to be generally complex.

$\mathrm{SL}(2, \mathbb{C}) \approx \mathrm{SO}(1, 3)$.

$$A_2: \quad \mathrm{SU}(3), \mathrm{SL}(3, \mathbb{R}), ...$$

Finite groups

We will introduce in this context a number of theorems and concepts that have general use in the whole subject. Some will seem very specialised to finite groups, but will come back in everything we do later too. We start by considering an example D_3 (the finite group, not to be confused with the D_3 of the Cartan classification above).

$$D_3 = \{E, A, B, C, D, F\}$$

where E is the unit element. The order $|D_3| = 6$ is the number of elements. We need a multiplication table:

$i\backslash j$	E	A	B	C	D	F
E	E	A	B	C	D	F
A	A	E	D	F	B	C
B	B	F	E	D	C	A
C	C	D	F	E	A	B
D	D	C	A	B	F	E
F	F	B	C	A	E	D

Entry ij is given by $g_{ij} = g_i \cdot g_j$.

Example: $AB = D \neq BA = F$.

This implies that D_3 is non-abelian.

Definition: Abelian means $g_i \cdot g_j = g_j \cdot g_i$ for all g_i, $g_j \in G$. (Named after the Norwegian mathematician Niels Henrik Abel — look him up on Wikipedia.)

The table satisfies *associativity*, which constrains the table a lot. (You can't just dream up any old multiplication table and still satisfy associativity.)

Exercise: D_3 is *generated* by two (non-trivial) elements (called *generators*). Show this!

This is the abstract, formal definition of D_3. The abstract group D_3 can be realized in many ways:

1. As symmetry operations on an equilateral triangle.

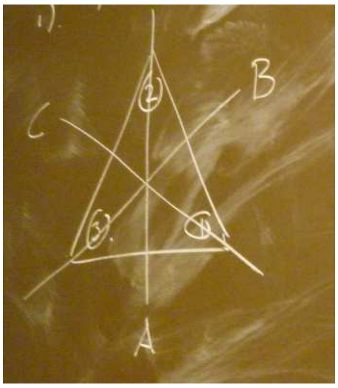

Figure 2. A, B, C are space-fixed axes. 1,2,3 are triangle-fixed corners.

Operations: flips around A, B, C and rotations in the plane by $\frac{2\pi}{3}$ (operation D) and $-\frac{2\pi}{3}$ (operation F). I get back the triangle in the same orientation, but the corners will have moved.

Composition: AB means do first B, then A.

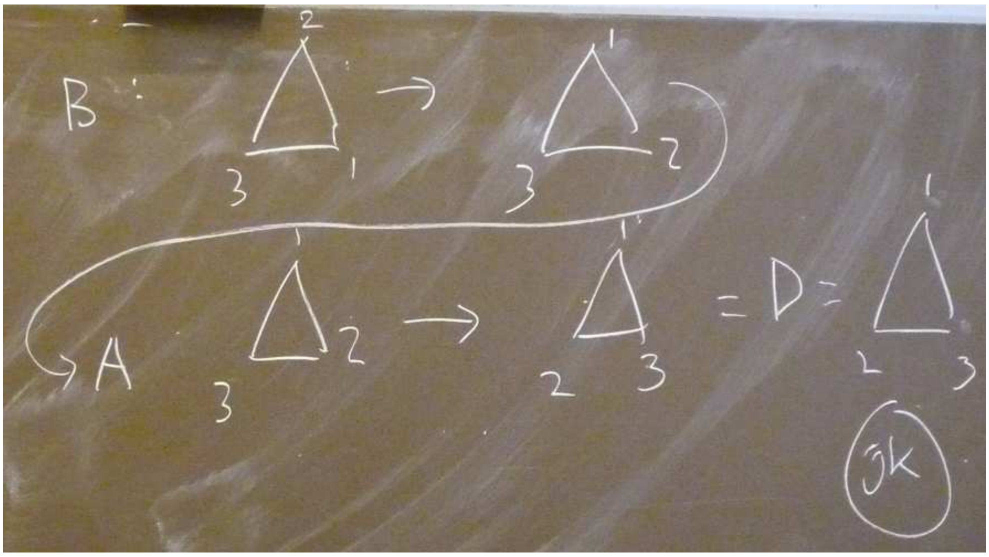

Figure 3. $A\,B = D$

So: Two flips is a rotation. One flip and one rotation is a flip, and two rotations is a rotation.

Exercise: Explain this!

2. Matrix realisation. This we call a *representation*. When we say *representation* in this course, we mean a group in terms of matrices.

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix},$$

$$C = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}, \quad D = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, \quad F = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}.$$

Check: $A\,B = D$: OK.

Note: Also $E = D = F = 1$, $A = B = C = -1$ is a representation! What do we mean by this? If you plug it into the multiplication table it is satisfied. Even all $g_i = 1$ works.

Question: Can we find *all* representations? All matrix relizations of this group?

Definition: If all elements are distinct, then the representation is called *faithful.*

Definition: Isomorphic: one-to-one map.

Example: The abstract D_3 is *isomorphic* to the 2×2 matrix and triangle operations above.

Defintion: If the map is *not* one-to-one, it is *homomorphic.* Examples $\{-1, 1\}$ and $\{1\}$.

Definition: A *representation* is a map Γ from the abstract group into matrices, such that $\Gamma(A)\,\Gamma(B) = \Gamma(A\,B)$ and all group axioms.

Theorem: Rearrangement theorem.

Note: Just saying that multiplying all elements by any given element gives back all elements once.

Proof: Fix A_k, then the set of elements $E\,A_k, A_1 A_k, A_2 A_k, \ldots, A_{|G|} A_k$ will contain any element in G — pick any A_i and for it to appear we use A_r such that $A_r A_k = A_i$. Can this always be done for arbitrary A_i and a fixed A_k? It is always possible — just use $A_r = A_i A_k^{-1} \in G$.

⇒ Any element will occur. ⇒Each element occurs once. □

Implication: Any subset of n different elements will map under multiplication by an arbitrary element, to n different elements (not in general the same as in the first subset).

DEFINITION: If a subset H of G satisfies the group axioms, it is called a subgroup.

EXAMPLE: Any element $x\in G$ generates a *cyclic* subgroup: $\{x, x^2, x^3, ..., x^n = E\}$ where n is the order of the subgroup, which is abeliean.

D_3: $x=A$: $\{A, A^2=E\}$. Here $n=2$.

$x=D$: $\{D, D^2=F, D^3=E\}$. Here $n=3$.

Cosets

Let $H=\{E, B_2, B_3, ..., B_{h=|H|}\}$ be a subgroup of $G=\{E, A_2, A_3, ..., A_{g=|G|}\}$. Then Hx for any given $x\in G$ is the set $\{E x, B_2 x, ..., B_h X\}$ is a *right coset.*

Now, if $x\in H$ then $H x = H$, according to the rearrangement theorem for H, but if $x\notin H$, then Hx is not a group, since E is not in $H x$. In fact H and Hx are disjoint as sets if $x\notin H$.

Proof. Assume the opposite. $B_i\in H$, $x\notin H$, $B_j\in H$. $B_i x = B_j$.

But then $x=B_i^{-1}B_j\in H$. Contradiction! □

Thus: Two cosets $H x_1$ and $H x_2$ are either identical as sets or disjoint.

Proof. A common element exists: $B_i x = B_j y \Rightarrow B_i(x y^{-1}) = B_j \Rightarrow x y^{-1}\in H \Rightarrow H(x y^{-1}) = H \Rightarrow H x = H y$. So if one common element exists, then the two cosets are identical. □

Hence: G can be divided into a set of disjoint sets.

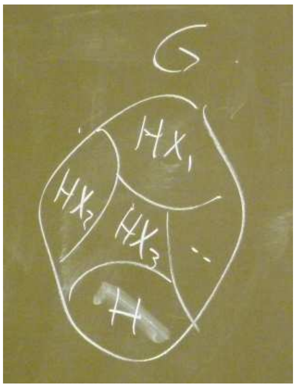

Figure 4.

So $G=H\cup H x_1\cup\cdots\cup H x_l$ where $l\in\mathbb{Z}$. This means that $g=h l$. Lagrange's theorem. l is called the *index* of H in G.

If $|G|=g$ is prime, you cannot split it into subgroup.

EXAMPLE: order $=6=3\times 2$.

1. subgroup with $h=3, l=2$.

2. subgroup with $h=2$, $l=3$.

Classes and invariant subgroups

Two elements A and B in G are *conjugate* to each other if $A = X B X^{-1}$ for some $X \in G$.

If A is conjugate to B and B to C, then A is conjugate to C.

All mutually conjugate elements belong to a set, called a class. And the group G can hence be divided into a number of disjoint classes.

Exercise: Why is the rearrangement theorem not useful here?

Denote classes by $\mathcal{C}_i$ and thus $G = \bigcup_i \mathcal{C}_i$. But also $\mathcal{C}_i \mathcal{C}_j = \sum_k {c_{i j}}^k \mathcal{C}_k$.

Example: D_3:

$$\mathcal{C}_1 = \{E\}, \quad \mathcal{C}_2 = \{A, B, C\}, \quad \mathcal{C}_3 = \{D, F\}.$$

$A = X B X^{-1}$ for some $X \in G$.

Now consider: Invariant subgroups.

Definition: A subset H such that H is a group *and* $x H x^{-1} = H$ for all $x \in G$ is called an *invariant subgroup* (also called *normal subgroup* and *normal divisor*).

H consists of a set of complete classes.

Definition: G is *simple* if the only invariant subgroups of G is $\{E\}$ and G itself.

Definition: *Factor group:* $= \{$elements $=$ cosets on an invariant subgroup $H\} = G/H$. It is a group if H is invariant.