Some slides for 21st Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

30-11-2011

S_n

- The same construction makes of S_3 sense for a set with n elements. For instance $M_n = \{1, \ldots, n\}$.
- We have S_n: bijective maps $M_n \to M_n$.
- S_n is a group with the composition of maps and order $n!$
- $\sigma \in S_n$ is a bijection and denoted by

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Let $\sigma \in S_n$. We define M_σ

$$M_\sigma = \{x \in M_n : \sigma(x) \neq x\}$$

We say that $\sigma, \tau \in S_n$ are disjoint if $M_\sigma \cap M_\tau = \emptyset$.

Proposition 2.9.2

Let $\sigma, \tau \in S_n$ be disjoint permutations in S_n. Then $\sigma\tau = \tau\sigma$

A **k-cycle** is a permutation $\sigma \in S_n$ such that for k (different) elements $x_1, \ldots, x_k \in M_n$,

$$\sigma(x_1) = x_2, \;\; \sigma(x_2) = x_3, \;\; , \ldots \sigma(x_{k-1}) = x_k, \;\; , \sigma(x_k) = x_1$$

We denote it by $\sigma = (x_1 x_2 \ldots x_k)$

The k-cycle σ can be represented in k ways:

$$\begin{array}{c} (x_1 x_2 \ldots x_{k-1} x_k), \\ (x_2 x_3 \ldots x_k x_1), \\ \vdots \\ (x_k x_1 \ldots x_{k-2} x_{k-1}) \end{array}$$

- $M_\sigma = \{x_1, \ldots, x_k\}$
- The order of a k-cycle in S_n is k.

- 1-cycle: identity map
- 2-cycle: trasposition. σ transposition: $\sigma^{-1} = \sigma$
- Simple trasposition: a transposition $s_i = (i \;\; i+1)$

Proposition 2.9.5

Let $\sigma \in S_n$ be written as a product of disjoint cycles $\sigma_1 \cdots \sigma_r$. Then the order of σ is the least common multiple of the orders of the cycles $\sigma_1, \ldots, \sigma_r$

Proposition 2.9.6

Every permutation $\sigma \in S_n$ is a product of unique disjoint cycles.

Using bubble sort we saw:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = (2\ 3)(3\ 4)(2\ 3)(1\ 2)$$

We wonder: What is the minimal number of simple transpositions needed for writing a permutation as a product in this way?

Let σ be a permutation. A pair of indices (i, j), where $1 \leq i < j \leq n$, is called an **inversion** of σ if $\sigma(i) < \sigma(j)$. Let

$$I_\sigma = \{(i, j) : 1 \leq i < j \leq n \text{ and } \sigma(i) > \sigma(j)\}$$

denote the set of inversions and $n(\sigma) = |I_\sigma|$ the number of inversions of σ.

Example:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix}$$

Compute: I_σ and $n(\sigma)$

Let σ be a permutation. A pair of indices (i, j), where $1 \leq i < j \leq n$, is called an inversion of σ if $\sigma(i) > \sigma(j)$. Let

$$I_\sigma = \{(i, j) : 1 \leq i < j \leq n \text{ and } \sigma(i) > \sigma(j)\}$$

denote the set of inversions and $n(\sigma) = |I_\sigma|$ the number of inversions of σ.

Example:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix}$$

$I_\sigma = \{(1,2), (1,3), (1,4), (1,5), (1,6), (2,3), (2,6), (4,5), (4,6), (5,6)\}$

$n(\sigma) = 10$

Proposition 2.9.12

The permutation $\sigma \in S_n$ is the identity map if and only if $n(\sigma) = 0$. If σ is not the identity map then there exists $i \in \{1, \ldots, n-1\}$ such that $\sigma(i) > \sigma(i+1)$.

Proof: $\sigma \in S_n$ is the identity map $\Leftrightarrow n(\sigma) = 0$

- If σ identity map, the it has no inversions and $n(\sigma) = 0$.
- If $n(\sigma) = 0$ and σ is not the identity map then there exists a smallest $i \in M_n$ such that $\sigma(i) > i$, but $(i, \sigma^{-1}(i))$ is an inversion.

Proof: If σ is not the identity map then there exists $i = 1, \ldots, n-1$ such that $\sigma(i) > \sigma(i+1)$.

- If σ is a permutation satisfying $\sigma(1) < \cdots < \sigma(n)$ then σ has to be the identity map, since $n(\sigma) = 0$.

Lemma 2.9.13

Let $s_i \in S_n$ be a simple transposition and $\sigma \in S_n$. Then

$$n(\sigma s_i) = \begin{cases} n(\sigma)+1 & \text{if } \sigma(i) < \sigma(i+1), \\ n(\sigma)-1 & \text{if } \sigma(i) > \sigma(i+1), \end{cases}$$

Proof: Assume $\sigma(i) < \sigma(i+1)$

- $(i, i+1)$ is an inversion for σs_i since $(i, i+1)$ is not an inversion for σ.
- Consider
$$\begin{array}{rcl} \varphi : I_\sigma & \to & I_{\sigma s_i} \setminus \{(i, i+1)\} \\ (k, l) & \mapsto & (s_i(k), s_i(l)) \end{array}$$
- We should prove that φ is bijective:
  - If $(k, l) \in I_\sigma$ then $s_i(k) < s_i(l)$. It is clear for every k, l, excepting $k = i$ and $l = i+1$, but we assumed $(i, i+1) \notin I_\sigma$
  - We have that $(s_i(k), s_i(l)) \in I_{\sigma s_i}$ since $(k, l) \in I_\sigma$
  - If $(k, l) \in I_{\sigma s_i} \setminus \{(i, i+1)\}$ then $(s_i(k), s_i(l)) \in I_\sigma$.

Lemma 2.9.13

Let $s_i \in S_n$ be a simple transposition and $\sigma \in S_n$. Then

$$n(\sigma s_i) = \begin{cases} n(\sigma) + 1 & \text{if } \sigma(i) < \sigma(i+1), \\ n(\sigma) - 1 & \text{if } \sigma(i) > \sigma(i+1), \end{cases}$$

Proof: Assume $\sigma(i) > \sigma(i+1)$

- $(\sigma s_i)(i) < (\sigma s_i)(i+1)$ since $\sigma(i) > \sigma(i+1)$
- Then $n((\sigma s_i)s_i) = n(\sigma s_i) + 1$ by previous slide.
- And $\sigma s_i s_i = \sigma$, hence $n(\sigma) = n(\sigma s_i) + 1$ and the result holds

Proposition 2.9.14

Let $\sigma \in S_n$. Then

1. σ is a product of $n(\sigma)$ simple transpositions
2. $n(\sigma)$ is the minimal product of simple transpositions needed in writing σ as a product of simple transpositions.

Proof of (1) by induction on $n(\sigma)$:

- For $n(\sigma) = 0$, σ is the identity map and it is the empty product of simple transpositions
- Assume we can write a transposition τ with $n(\tau) = n - 1$ as product of transpositions
  - If $n(\sigma) \neq 0$, we may find $i \in \{1, \ldots, n-1\}$ such that $\sigma(i) > \sigma(i+1)$ (by prop. 2.9.12)
  - Then $n(\sigma s_i) = n(\sigma) - 1$ by lemma 2.9.13.
  - By induction, $\tau = \sigma s_i$ can be written as the product of $n - 1$ transpositions.
  - Then, $\sigma = \tau s_i$ is a product of $n(\sigma)$ transpositions.

Proposition 2.9.14

Let $\sigma \in S_n$. Then

1. σ is a product of $n(\sigma)$ simple transpositions
2. $n(\sigma)$ is the minimal product of simple transpositions needed in writing σ as a product of simple transpositions.

Proof: $\ell(\sigma)$ is the minimal number of simple transpositions needed in writing σ as a product of simple transpositions.

- $n(\sigma) \geq \ell(\sigma)$ by (1)
- We prove $n(\sigma) = \ell(\sigma)$ by induction on $\ell(\sigma)$
- $\ell(\sigma) = 0$, trivial
- For $\ell(\sigma) > 0$:
  - We can find a simple transposition s_i such that $\ell(\sigma s_i) = \ell(\sigma) - 1$
  - Thus, $\ell(\sigma s_i) = n(\sigma s_i)$ by induction
  - Hence $\ell(\sigma) \geq n(\sigma)$

The sign of a permutation $\sigma \in S_n$ is

$$\operatorname{sgn}(\sigma) = (-1)^{n(\sigma)}$$

A permutation with sign 1 is called even and with sign -1 is called odd.

Proposition 2.9.16

The sign

$$\begin{array}{rcl} \operatorname{sgn} : S_n & \to & \{-1, 1\} \\ \sigma & \mapsto & \operatorname{sgn}(\sigma) \end{array}$$

of a permutation is a group homomorphism (the composition for $\{-1, 1\}$ is multiplication).

Actually, $(\{-1, 1\}, \cdot)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}, +)$.

$$\begin{array}{rcl} \mathrm{sgn} : S_n & \to & \{-1, 1\} \\ \sigma & \mapsto & \mathrm{sgn}(\sigma) \end{array}$$

Proof sgn is a group homomorphism:

- We have to prove $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)$ for $\sigma, \tau \in S_n$
- Assume that τ is a simple transposition: $n(\sigma s_i) = n(\sigma) \pm 1$ (lemma 2.9.13). Thus $\mathrm{sgn}(\sigma s_i) = -\mathrm{sgn}(\sigma)$.
- Then $\mathrm{sgn}(\sigma s_i) = \mathrm{sgn}(\sigma)\mathrm{sgn}(s_i)$, because $n(s_i) = 1$.
- By previous proposition τ is a product of simple transpositions, apply the previous proof several times

The set of even permutations in S_n is denoted A_n and called the alternating group

- A_n is a normal subgroup of S_n, since A_n is the kernel of sgn.
- By isomorphism theorem:

$$S_n/A_n \xrightarrow{\sim} \{-1, 1\}$$

- Then $|A_n| = |S_n|/2 = n!/2$
- How do we compute $\operatorname{sgn}(\sigma)$ of a permutation?
- By computing the sign of a k-cycle

Lemma 2.9.8

Suppose that $\tau = (i_1 i_2 \ldots i_k)$ is a k-cycle and σ a permutation in S_n. Then $\sigma(i_1 i_2 \ldots i_k)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\ldots\sigma(i_k))$

Proposition 2.9.17

Let $n \geq 2$. A transposition $\tau = (i\ j) \in S_n$ is an odd permutation. The sign of an r-cycle $\sigma = (x_1 \ldots x_r) \in S_n$ is $(-1)^{r-1}$.

Proof: A transposition $\tau = (i\ j) \in S_n$ is an odd permutation

- Consider a permutation $\eta \in S_n$ such that $\eta(1) = i$ and $\eta(2) = j$
- $-1 = \mathrm{sgn}(1\ 2) = \mathrm{sgn}(\eta(1\ 2)\eta^{-1}) = \mathrm{sgn}((\eta(1)\ \eta(2)) = \mathrm{sgn}(\tau)$.

Proof $\mathrm{sgn}((x_1 \ldots x_r)) = (-1)^{r-1}$

- $(x_1 \ldots x_r) = (x_1\ x_2)(x_2\ x_3)\ldots(x_{r-1}\ x_r)$
- $(x_1 \ldots x_r)$ is the product of $r-1$ transpositions and the result holds

Lemma 2.9.18

Every permutation in A_n is a product of 3-cycles if $n \geq 3$.

Proof:

- A permutation in A_n is product of an even number of transpositions
- $(a\ b)(c\ d) = (a\ d\ c)(a\ b\ c)$
- $(a\ b)(b\ c) = (a\ b\ c)$

Simple groups

A group G is called simple if $\{e\}$ and G are the only normal subgroups of H. Otherwise G is called solvable.

Examples:

- $\mathbb{Z}/p\mathbb{Z}$, with p prime.
- A_n, for $n \geq 5$ (Theorem 2.9.19).

Simple finite groups form the building blocks for all finite groups.

Feit and Thomson's theorem: the order of a non-abelian finite simple group must be even.

In 2004: classification of simple groups, 18 families and 26 exceptions. See wikipedia.