Department of Mathematics
Prof. Dr. Christian Herrmann
Dipl.-Math. Frederick Magata
Dr. Abdelhadi Es-Sarhir

TECHNISCHE UNIVERSITÄT DARMSTADT

27. April 2006

Linear Algebra II (MCS), SS 2006, Exercise 2

Groupwork

G 5 Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 3 & 7 & 4 & 8 & 1 & 2 & 9 & 5 \end{pmatrix}$.

(i) Determine the canonical decomposition of σ into disjoint cycles.

(ii) Give a decomposition of σ into transpositions.

(iii) What is the sign of σ?

G 6 (i) What is the order of S_n for $n \in \mathbb{N}$?

(ii) What is the order of A_n for $n \in \mathbb{N}$, $n \geq 2$?

(iii) A group is called *cyclic*, if it is generated by a single element. For which $n \in \mathbb{N}$ is S_n cyclic?

G 7 The *order* $\operatorname{ord}(g)$ of a group element $g \in G$ is the cardinality of the cyclic subgroup generated by g. Let $\sigma \in S_n$ and $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_m$ its canonical decomposition into pairwise disjoint cycles. Show that

$$\operatorname{ord}(\sigma) = \operatorname{lcm}(\operatorname{ord}(\sigma_1), \ldots, \operatorname{ord}(\sigma_m)),$$

where $\operatorname{lcm}(\ldots)$ denotes the least common multiple of the elements in parentheses.

G 8 (i) Is there an element of order 7 in S_5?

(ii) Is there an element of order 8 in S_5?

(iii) Locate an element of maximum order in S_5.

G 9 (i) What is the inverse of the cycle $(a_0, \ldots, a_{s-1})$?

(ii) Let $\sigma = (a_0, \ldots, a_5)$ be a proper cycle, i.e. $\sigma \neq \mathrm{id}$. For which $m \in \mathbb{Z}$ is σ^m a proper cycle, too?

Homework

H 4 Show that for every $\sigma \in S_n,\ n \in \mathbb{N}$ and every cycle $(a_0, \ldots, a_{s-1})$, $s \leq n$ we have

$$\sigma(a_0, \ldots, a_{s-1})\sigma^{-1} = (\sigma(a_0), \ldots, \sigma(a_{s-1})).$$

H 5 Show in each case that S_n is generated by the given set of cycles:

(i) All transpositions.

(ii) The transpositions $(1,2), (1,3), \ldots, (1,n)$.

(iii) The transpositions $(1,2), (2,3), \ldots, (n-1,n)$.

(iv) The elements $(1,2), (2, \ldots, n)$ (only for $n \geq 2$).

(v) The elements $(1,n), (1, \ldots, n)$.

(Hint: Use **H 4** and induction.)

Linear Algebra II (MCS), SS 2006, Exercise 2, Solution

Groupwork

G 5 Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 3 & 7 & 4 & 8 & 1 & 2 & 9 & 5 \end{pmatrix}$.

(i) Determine the canonical decomposition of σ into disjoint cycles.

(ii) Give a decomposition of σ into transpositions.

(iii) What is the sign of σ?

(i) $\sigma = (1,6)(2,3,7)(5,8,9)$.

(ii) Since $(a_0, a_1, \dots a_r) = (a_0, a_1)(a_1, \dots, a_r)$, *we have:* $\sigma = (1,6)(2,3)(3,7)(5,8)(8,9)$.

(iii) $\operatorname{sign}(\sigma) = (-1)^5 = -1$.

G 6 (i) What is the order of S_n for $n \in \mathbb{N}$?

(ii) What is the order of A_n for $n \in \mathbb{N}$, $n \geq 2$?

(iii) A group is called *cyclic*, if it is generated by a single element. For which $n \in \mathbb{N}$ is S_n cyclic?

(i) $|S_n| = n!$.

(ii) By definition, A_n is the kernel of the sign homomorphism, which we call the even elements. That is, A_n consists of those elements, which can be written as an even number of transpositions. The product of two even or two odd permutations is even again, and the product of an odd permutation with an even one, or vice versa, gives an odd permutation. A given transposition τ is an odd element. Left multiplication by τ (as multiplication with any element) defines a bijection of S_n. By the previous remark, we thus have that the set of even elements is mapped bijectively onto the set of odd elements. Hence $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

(iii) For $n = 0, 1, 2$ it is easily verified that S_n is cyclic. For $n \geq 3$ however, S_n is not even abelian. For instance $(1,2)(2,3) = (1,2,3)$, but $(2,3)(1,2) = (1,3,2)$. Hence S_n is not cyclic for $n \geq 3$.

G 7 The *order* $\operatorname{ord}(g)$ of a group element $g \in G$ is the cardinality of the cyclic subgroup generated by g. Let $\sigma \in S_n$ and $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_m$ its canonical decomposition into pairwise disjoint cycles. Show that

$$\operatorname{ord}(\sigma) = \operatorname{lcm}(\operatorname{ord}(\sigma_1), \dots, \operatorname{ord}(\sigma_m)),$$

where $\operatorname{lcm}(\dots)$ denotes the least common multiple of the elements in parentheses.

Since the cycles σ_i in the decomposition of σ are pairwise disjoint, they commute. Therefore, we have $\mathrm{id} = \sigma^q = \sigma_1^q \cdot \ldots \cdot \sigma_m^q$ *for some $q \in \mathbb{N}$ if and only if* $\sigma_1^q = \cdots = \sigma_m^q = \mathrm{id}$. *This implies our claim.*

G 8 (i) Is there an element of order 7 in S_5?

(ii) Is there an element of order 8 in S_5?

(iii) Locate an element of maximum order in S_5.

(i) No. 7 is not a divisor of $5! = 120$. Another reason is (iii).

*(ii) No. You cannot find three pairwise disjoint transpositions or a transposition and a three-cycle disjoint from it (compare with **G 7**).*

(iii) The element $(1,2)(3,4,5)$ has order 6. This is an element of maximum order by arguments similar to those in (ii).

G 9 (i) What is the inverse of the cycle $(a_0, \dots, a_{s-1})$?

(ii) Let $\sigma = (a_0, \dots, a_5)$ be a proper cycle, i.e. $\sigma \neq \mathrm{id}$. For which $m \in \mathbb{Z}$ is σ^m a proper cycle, too?

(i) The inverse is $(a_{s-1}, \dots, a_0)$, which is the same as $(a_0, \dots, a_{s-1})^{s-1}$.

(ii) *We have* $\sigma^2 = (a_0, a_2, a_4)(a_1, a_3, a_5)$, $\sigma^3 = (a_0, a_3)(a_1, a_4)(a_2, a_5)$, $\sigma^4 = (a_0, a_4, a_2)(a_1, a_5, a_3)$ *and* $\sigma^5 = (a_0, a_5, a_4, a_3, a_2, a_1)$. *For an arbitrary* $m \in \mathbb{Z}$ *with* $\sigma^m = \mathrm{id}$, *there is a* $k \in \mathbb{Z}$ *such that* $0 < m - k \cdot 6 < 6$ *and* $\sigma^m = \sigma^{m-k\cdot 6}$. *Hence, up to an integer multiple of* 6, *the only valid values for* m *are* 1 *and* 5.

Homework

H 4 Show that for every $\sigma \in S_n$, $n \in \mathbb{N}$ and every cycle $(a_0, \dots, a_{s-1})$, $s \le n$ we have

$$\sigma(a_0, \dots, a_{s-1})\sigma^{-1} = (\sigma(a_0), \dots, \sigma(a_{s-1})).$$

For every $k = 0, \dots, s-2$ *we have*

$$(\sigma(a_0 \dots a_{s-1})\sigma^{-1})(\sigma(a_k)) = (\sigma(a_0 \dots a_{s-1}))(a_k) = \sigma(a_{k+1}),$$

and $(\sigma(a_0 \dots a_{s-1})\sigma^{-1})(\sigma(a_{s-1})) = \sigma(a_0)$.
For every $\sigma(x) \in \{\sigma(1), \dots, \sigma(n)\} \setminus \{\sigma(a_0), \dots, \sigma(a_{s-1}))\}$, *we clearly have*

$$(\sigma(a_0 \dots a_{s-1})\sigma^{-1})(\sigma(x)) = \sigma(x).$$

It hence follows that $(\sigma(a_0 \dots a_{s-1})\sigma^{-1}) = (\sigma(a_0) \dots \sigma(a_{s-1}))$.

H 5 Show in each case that S_n is generated by the given set of cycles:

(i) All transpositions.
(ii) The transpositions $(1,2), (1,3), \dots, (1,n)$.
(iii) The transpositions $(1,2), (2,3), \dots, (n-1,n)$.
(iv) The elements $(1,2), (2,\dots,n)$ (only for $n \ge 2$).
(v) The elements $(1,n), (1,\dots,n)$.

(Hint: Use **H 4** and induction.)

(i) *This follows from the canonical decomposition of a permutation into pairwise disjoint cycles and the fact that* $(a_0, a_1, \dots a_r) = (a_0, a_1)(a_1, \dots, a_r)$.

(ii) *By (i) it suffices to generate all transpositions by the special transpositions* $(1,2), (1,3), \dots, (1,n)$. *Using* ***H 4*** *we have for any transposition* (a,b), $a \ne b$ *that* $(a,b) = (1,a)(1,b)(1,a)$.

(iii) *Using* $(1,k) = (1,k-1)(k-1,k)(1,k-1)$ *and induction over* k, *we can generate every* $(1,k)$ *out of* $(1,2), (2,3), \dots, (k-1,k)$. *By (ii), we therefore can generate all of* S_n *out of these elements.*

(iv) *Using* $(1,k) = (2,\dots,n)(1,k-1)(n,\dots,2)$ *for* $k = 2, \dots, n$ *and induction over* k, *we can generate every* $(1,k)$ *out of* $(1,2), (2,\dots,n)$. *By (ii), we therefore can generate all of* S_n *out of these elements.*

(v) *Using* $(1,2) = (1,\dots,n)(1,n)(n,\dots,1)$ *and* $(k,k+1) = (1,\dots,n)(k-1,k)(n,\dots,1)$ *for* $k = 2, \dots, n-1$ *and induction over* k, *we can generate every* $(k,k+1)$ *out of* $(1,n), (1,\dots,n)$. *By (iii), we therefore can generate all of* S_n *out of these elements.*

Due to the holidays 'Maifeiertag' on 1.5.2006 and 'Pfingstmontag' on 5.6.2006, lectures will instead take place on thursday of the respective week in room S1 03/123:
Thu. 4.5.2006 8:00 am - 9:40 am room S1 03/123
Thu. 8.6.2006 8:00 am - 9:40 am room S1 03/123

Information concerning this course can be found in the internet at:

`http://www.mathematik.tu-darmstadt.de/lehrmaterial/SS2006/LAII_MCS`