

Algebra 3

Results in group theory 3

12. september 2005

Below you find a very extensive outline of the results covered in the lectures of the second week. It includes several proofs of the results on the pages 1.18-1.30 of the Danish book recommended for the course: Chr. U. Jensen: Klassisk Algebra (Mat 3AL), 2004 which may be downloaded from the Internet:

<http://www.math.ku.dk/noter/>

The reader may find a fairly thorough exposition of most of the results mentioned below in the lecture notes by J. Milne, especially Sections 1, 3, 4 and 6. These notes may be also be found on the Internet:

<http://www.jmilne.org/math/CourseNotes/math594g.html>

Page 1.18

Permutation groups

- Let Ω be an arbitrary set ($\neq \emptyset$) and $S(\Omega)$ the set of all bijective maps of Ω onto Ω . Using composition of maps $S(\Omega)$ is a group. If Ω is finite, eg. $\Omega = \{1, 2, \dots, n\}$ then $S(\Omega)$ is *the symmetric group* S_n .

A *permutation group on Ω* is simply a subgroup of $S(\Omega)$.

- *Definition:* A permutation group G on Ω is called *transitive*, if for arbitrary (a, b) , $a, b \in \Omega$ there exists $\sigma \in G$ st. $\sigma(a) = b$.

- *Definition.* A permutation group G on Ω is called *doubly transitive*, if for arbitrary $a, b, c, d \in \Omega$ $a \neq b$ and $c \neq d$ there exists $\sigma \in G$ st. $\sigma(a) = c$ og $\sigma(b) = d$.

- *Remark.* Clearly doubly transitive \Rightarrow transitive.

- Any group is realizable as a permutation group. We have:

Cayley's theorem: Let G be an arbitrary group. Then there exists an injective homomorphism φ of G onto a transitive subgroup of $S(G)$. In particular, any group of finite order n is isomorphic to a transitive subgroup of the symmetric group S_n .

Proof: For $g \in G$ let φ_g be the following element in $S(G)$:

$$\varphi_g(x) = g \circ x, \quad x \in G.$$

Then φ_g is a bijective map on G , ie. φ_g is a well defined element in $S(G)$. The associativity of group multiplication shows that

$$\varphi_{g_1 \circ g_2} = \varphi_{g_1} \circ \varphi_{g_2}.$$

Thus φ is a homomorphism of G into $S(G)$.

Furthermore

$$\ker(\varphi) = \{g \in G \mid \varphi_g = Id_G\} = \{g \in G \mid g \circ x = x \forall x \in G\} = \{e\}.$$

Thus φ is injective. The image of G by φ is a transitive subgroup in $S(G)$. Indeed, if $a, b \in G$ are arbitrary, then $\varphi_g(a) = b$ for $g = ba^{-1}$.

• A generalization of Cayley's theorem for finite groups is sometimes useful:

Let H be a subgroup of G of index $[G : H] = n$, $n \in \mathbb{N}$, and let $G = \bigcup_{i=1}^n g_i H$ be the decomposition of G into disjoint right cosets wrt. H . Let us assume $g_1 = e$.

Page 1.19

For each $g \in G$ we have that $G = \bigcup_{i=1}^n gg_i H$ is another decomposition of G into disjoint right cosets wrt. H . Thus

$$\begin{pmatrix} g_1 H & g_2 H & \cdots & g_n H \\ gg_1 H & gg_2 H & \cdots & gg_n H \end{pmatrix}$$

is a permutation of the cosets $g_i H$, $1 \leq i \leq n$, and may thus be seen as an element in the symmetric group S_n . We define a map $\rho : G \rightarrow S_n$ by

$$\rho g = \begin{pmatrix} g_1 H & g_2 H & \cdots & g_n H \\ gg_1 H & gg_2 H & \cdots & gg_n H \end{pmatrix}$$

and write $gg_i H = g_{\rho(g)(i)}$, $1 \leq i \leq n$.

In analogy with the proof of Cayley's theorem it is easily seen that ρ is a homomorphism and that $\rho(G)$ is a transitive subgroup of S_n . The order of $\rho(G)$ is then divisible by n (why?)

• For the kernel of ρ we have

$$\ker(\rho) = \bigcap_{i=1}^n g_i H g_i^{-1} \subseteq H \text{ and } \ker(\rho) \triangleleft G \text{ with } G/\ker(\rho) \simeq \rho(G).$$

Clearly $\ker(\rho)$ is the largest normal subgroup of G , which is contained in H .

- *Remark:* If $H = \{e\}$ we obtain Cayley's theorem.

- Some theorems about doubly transitive permutation groups:

- **Theorem 18.** Let $N \neq \{e\}$ be a normal subgroup in a doubly transitive permutation group G on Ω . Then N is transitive.

Proof Let $a, b \in \Omega$, $a \neq b$. We want to find $\sigma \in N$ with $\sigma(a) = b$. As $N \neq \{e\}$ there exists $c \neq d$ in Ω with $\bar{\sigma}(c) = d$ for some $\bar{\sigma} \in N$. As G is doubly transitive, there exists $\tau \in G$ with $\tau(c) = a$, $\tau(d) = b$. Then $\tau \bar{\sigma} \tau^{-1}(a) = b$. Since $N \triangleleft G$ we get $\tau \bar{\sigma} \tau^{-1} \in N$ ie. $\tau \bar{\sigma} \tau^{-1}$ may be used as σ . □

- **Definition:** Let G be a permutation group on Ω . When $a \in \Omega$ we call $G_a = \{\sigma \in G \mid \sigma(a) = a\}$ G 's *stabilizer* in Ω . (G_a is clearly subgroup of G .)

- **Theorem 19:** Let G be doubly transitive on Ω , where $|\Omega| > 1$. Then G_a is a maximal subgroup in G , ie. There are no subgroups lying properly between G_a and G .

Proof: Let H be a subgroup of G satisfying $G_a \subset H$. We want to show $H = G$. Since $G_a \neq H$ we may find $\tau \in H$ with $\tau(a) = b$, $b \neq a$. Let ρ be arbitrary in G . We show $\rho \in H$. Let $\rho(a) = c$. If $c = a$ then $\rho \in G_a \subset H$ and we are done. We may thus assume $c \neq a$. As G is doubly transitive, there exists $\sigma \in G$ with $\sigma(a) = a$, $\sigma(b) = c$. Thus $\sigma \in G_a$. Now $\sigma\tau(a) = c$ implies $\rho^{-1}\sigma\tau(a) = a$, ie. $\rho^{-1}\sigma\tau \in G_a \subseteq H$. As $\sigma, \tau \in H$, we get $\rho \in H$, as desired.

Page 1.20

- The proof of the following criteria for simplicity is omitted:

Theorem 20: Let G be doubly transitive on Ω ($|\Omega| > 1$). Then G is a simple group, if

(i) $G = G'$ (Here G' is the commutator subgroup of G).

(ii) There exists $a \in \Omega$ st. G_a contains a normal abelian subgroup K satisfying

$$G = \langle \sigma K \sigma^{-1} \mid \sigma \in G \rangle$$

Pages 1.21-1.24

These pages covers the elementary theory of permutations in the symmetric groups S_n . (most of which has also been covered in the course Algebra 2) This includes:

- Any permutation may be decomposed uniquely into a product of disjoint cycles. (Proposition 4.22 in Milne).
- Any permutation is a product of transpositions. (Corollary 4.23 in Milne).
- The center of the symmetric group S_n is trivial for $n \geq 3$.
- The alternating group S_n is simple for $n \geq 5$. (Theorem 4.29 in Milne).
- If $n \geq 5$ then the only non-trivial normal subgroup of S_n is A_n . (Corollary 4.33 in Milne).

Pages 1.24-1.30

These pages covers normal series in groups and solvable and nilpotent groups. All material from these pages may be found in Milne's Chapter 6, pages 62-68.

For a treatment of Schreier's refinement theorem and the Zassenhaus Lemma (pages 1.25-1.26) the reader is also referred to some lecture notes of Tara L. Smith, see

<http://math.uc.edu/~tsmith/Math610/compseries.pdf>