Algebra 3
Results in group theory 2

1. september 2005

Below you find a very extensive outline including several proofs of the results on the pages 1.8-1.16 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 and 4. These notes may be also be found on the Internet:

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

Page 1.8

Direct products

- *Definition* of $HK = \{hk | h \in H, k \in K\}$ for subgroups H, K of the group G.

- **Theorem 7:** HK is a subgroup of $G \Leftrightarrow HK = KH$.

- **Theorem 8:** If $H \lhd G$ and K is a subgroup of G then $HK = KH$, so that HK is a subgroup of G.

- **Theorem 9:** If $H \lhd G, K \lhd G, HK = G, H \cap K = \{e\}$ then each element $g \in G$ may be written uniquely as $g = hk$ $(h \in H, k \in K)$ and products are computed "componentwise": $(h_1k_1)(h_2k_2) = (h_1h_2)(k_1k_2)$.

- *Definition.* In the situation of Theorem 9 the group G is called *inner direct product* of H and K. Moreover H, K are called *direct factors* of G.

- *Remark* about inner and outer direct products. The outer direct product of the groups H and K is simply the cartesian product $H \times K$ with componentwise product. Clearly inner and outer direct products of H, K are isomorphic.

Page 1.9

- **Theorem 10:** If a complete group H is a normal subgroup of a group G, then it is a direct factor of G.

Noethers isomorphism theorems

- **Noethers first isomorphism theorem.** Let H, K be subgroups of G, $H \lhd G$. Then $H \cap K \lhd K$ and $HK/H \simeq K/H \cap K$.

Page 1.10

- **Noethers second isomorphism theorem.** Let H be normal in G and κ the canonical homomorphism $\kappa : G \to G/H = G^*$. Then the maps $K \to \kappa(K) \subseteq G^*$ and $K^* \to \kappa^{-1}(K^*)$ yield a $1-1$ correspondence between the subgroups K of G containing H and the subgroups K^* of G^*. This correspondence satisfies $K \lhd G \Leftrightarrow \kappa(K) \lhd G^*$. If $K \lhd G$, then $G/K \simeq G^*/\kappa(K)$. (If $\kappa(K)$ is written K/H, then the isomorphism may be formulated as follows: $G/K \simeq (G/H)/(K/H)$.)

Commutator groups

- *Remark:* For any subset A of a group G there exists a smallest subgroup of G. It is simply the intersection of all subgroups of G which contains A. It is called the subgroup of G generated by A and is often denoted $< A >$ or $\{A\}$. It consists of all elements on the form $s_1^{m_1} s_2^{m_2} \cdots s_n^{m_n}$, where $n \in \mathbb{N}, s_i \in A, m_i \in \mathbb{Z}$, repetitions allowed.

- For elements a, b i a group G the solution $x = aba^{-1}b^{-1}$ to the equation $ab = xba$ is called the *commutator* corresponding to a, b. The subgroup of G generated by all commutators $aba^{-1}b^{-1}$ is called G's *commutator group* and is denoted G' (the *"derived " group*). Clearly an arbitrare automporphism of G maps the set of all commutators into itself. Therefore G' is a characteristic subgroup of G. In particular, $G' \lhd G$.

Page 1.11

- **Theorem 11:** If $H \lhd G$ we have:

$$H \supseteq G' \Leftrightarrow G/H \text{ is abelian.}$$

Thus G' is the smallest normal subgroup of G with abelian factor group.

Proof: $\Rightarrow$: All commutators are in H, ie. $aba^{-1}b^{-1} \in H$ for all $a, b \in G$, whence $\bar{a}\bar{b}\bar{a}^{-1}\bar{b}^{-1} = \bar{e}$ in G/H. (Here $\bar{a}$ denotes a's coset, ie. the image of the element a under the canonical homomorphism. Thus $\bar{a}\bar{b} = \bar{b}\bar{a}$, ie. G/H is abelian.

$\Leftarrow$: Let $a, b \in G$ be arbitrary. Then we have for the corresponding cosets in G/H that $\bar{a}\bar{b} = \bar{b}\bar{a}$, whence $\overline{aba^{-1}b^{-1}} = \bar{e}$. This means $aba^{-1}b^{-1} \in H$. Thus H contains all commutators and we get $H \supseteq G'$.

- *Remark* G abelian $\Leftrightarrow G' = \{e\}$.

Groups of a given finite order.

- We are going to prove some theorems about groups of given order n for certain values of n. In particular we determine all groups af order < 12.

For each $n \in \mathbb{N}$ we have at least one group af order n, the cyclic group $\mathbb{Z}_n$.

For each even number $2n$, $n \geq 3$, we also have at least one non-abelian group of order $2n$, namely the *dihedral group* of order $2n$, which is denoted D_n.

- **Theorem 12:** A group of prime order p is cyclic, ie. isomorphic to $\mathbb{Z}_p$.

- **Theorem 13:** There are exactly two (non-isomorphic) groups of orden 4, the cyclic $\mathbb{Z}_4$ and “Kleins Vierergruppe” V_4, which may be realized as the set of matrices on the form $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ with multiplication.

- **Theorem 14:** Let p be an odd prime. There are exactly two (non-isomorphic) groups of $2p$, the cyclic $\mathbb{Z}_{2p}$ and the dihedral group D_p.

Proof: Clearly $\mathbb{Z}_{2p}$ and D_p are non-isomorphic groups of order $2p$.

To show that there are no more groups we prove that there is only one noncyclic group G of order $2p$.

1°. *G has an element of order p.* Otherwise all elements in G would have order 1 or 2, implying that G is abelian. Let $a \neq e$, $a^2 = e$; $A = \{e, a\}$, a subgroup of order 2. $A \lhd G$, since G is abelian. The factor group G/A has order p, ie. G/A is cyclic. Lad $\bar{g}$ be a generator. Thus $\bar{g}^p = \bar{e}$, ie. if $g \in \bar{g}$ then $g \notin A$, $g^p \in A$. Since also $g^2 = e$ we get a contradiction: $g = g^p(g^2)^{-\frac{p-1}{2}} \in A$.

2°. *G has at element of order* 2. Proved analogously or use one of the exercises.

3°. Let a have order p and b order 2. Let $A = \{e, a, \ldots, a^{p-1}\}$ be the cyclic group generated by a. As $[G : A] = 2$, $A \lhd G$ and G/A is cyclic of order 2. Thus $bab^{-1} = a^j$ for some $j, 2 \leq j \leq p-1$. (Note that j cannot be 1, since G is not abelian.) We get $a = b^2ab^{-2} = ba^jb^{-1} = a^{j^2}$. Thus $a^{j^2-1} = 1$, whence

p divides $j^2 - 1 = (j+1)(j-1)$. This implies $p \mid (j+1)$, ie. $j = p-1$. Thus $bab^{-1} = a^{p-1} = a^{-1}$ or $ba = a^{p-1}b$. This relation ensures that there is a unique possiblilty for the multiplications of the elements in G, which are exactly $e, a, a^2, \cdots, a^{p-1}, b, ba, ba^2, \cdots, ba^{p-1}$.

- *Definition:* Let p be a prime. A *p-group* is a group G, whose order is a power of p.

- Description of the *class equation* for a finite group. (See the notes for Algebra 2, or proposition 4.12 in the notes by Milne.) As a consequence we have:

Page 1.13

- **Theorem 15** The center of a of a p-group $\neq \{1\}$ in nontrivial.

- **Lemma:** If $G/Z(G)$ is cyclic, then G is abelian.

Proof: See Milne 4.18.

- **Theorem 16:** If p is a prime There are exactly two non-isomorphic groups of order p^2, the cyclic $\mathbb{Z}_{p^2}$ and the group of diagonal matrices on the form $\begin{pmatrix} e^{\frac{2\pi i a}{p}} & 0 \\ 0 & e^{\frac{2\pi i b}{p}} \end{pmatrix}$, with $a, b \in \mathbb{Z}$. Both of these groups are abelian.

Proof: Milne 4.17.

Page 1.14

- Table of the number of groups of a given order 2-11, determined so far:

Group order	2	3	4	5	6	7	8	9	10	11
Number of gps	1	1	2	1	2	1		2	2	1
Nonabelian	0	0	0	0	1	0		0	1	0

- *The Classification of groups of order 8:* There are 5 groups, 3 abelian and 2 non-abelian.

Abelian: (I) $\mathbb{Z}_8$.

(II) Matrices on the form
$\begin{pmatrix} i^a & 0 \\ 0 & \pm 1 \end{pmatrix}$, with $i = \sqrt{-1}$, $a = 0, 1, 2, 3$.

(III) Matrices on the form

$$\begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \pm 1 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}.$$

Nonabelian:
(IV) The dihedral group D_4.

(V) The quaternion group. (See Appendix to the notes or Milne p. 8)

Page 1.15

Contains a elementary proof of the classification of groups of order 8.

Page 1.16

Completing the list of the number of groups of small order:

Group order	7	8	9	10	11	12	13	14	15	16	17	18	19
Number of gps	1	5	2	2	1	5	1	2	1	14	1	5	1
Nonabelian	0	2	0	1	0	3	0	1	0	9	0	3	0

The proofs for orders 12, 15, 16, 18 are omitted.

• Exercise/Example of three non-abelian and non-ismorphic groups of order 12: D_6, the alternating group A_4 and a group generated by two 2x2 complex matrices A and B.

The rest of page 1.16 and the pages 1.17-1.18 are not in the curriculum.