Group theory

Abstract group theory
English summary
Notes by Jørn B. Olsson
Version 2007

---

b.. *what wealth, what a grandeur of thought may spring from what slight beginnings.* (H.F. Baker on the concept of groups)

CONTENT:

1. On normal and characteristic subgroups. The Frattini argument

G1 - 2007-version.

This continues the notes from the courses Matematik 2AL and Matematik 3 AL. (Algebra 2 and Algebra 3). The notes about group theory in Algebra 3 are written in English and are referred to as GT3 in the following.

Content of Chapter 1

Definition of normal and characteristic subgroups (see also GT3, Section 1.12 for details)

$Aut(G)$ is the automorphism group of the group G and $Aut_i(G)$ the subgroup of inner automorphisms of G.

(1A) Theorem: (Important properties of $\trianglelefteq$ and *char*) This is Lemma 1.98 in GT3.

(1B) Remark: See GT3, Exercise 1.99.

If M is a subset of G, then $\langle M\rangle$ denotes the subgroup of G generated by M. See GT3, Remark 1.22 for an explicit desciption of the elements of $\langle M\rangle$.

(1C): *Examples and remarks on certain characteristic subgroups.* If the subset M of G is "closed under automorphisms of G", ie.

$$\forall \alpha \in Aut(G)\ \ \forall m \in M: \ \ \alpha(m) \in M,$$

then $\langle M\rangle$ *char* G.

Examples of subsets which are closed under automorphisms include (p is a prime number)

- $\mathcal{E}(G) = \{m \in G \mid |m|\ finite\}$
- $\mathcal{P}_p(G) = \{m \in G \mid m\ is\ a\ p-element\}$
- $\mathcal{D}_p(G) = \{m \in G \mid |m| finite,\ p \nmid |m|\}$
- $\mathcal{K}(G) = \{m \in G \mid \ \exists\ a, b \in G : m = [a, b]\}$.

Here $[a,b] = aba^{-1}b^{-1}$ is the commutator of a and b. Note, that $\langle \mathcal{K}(G) \rangle = G'$, G's commutator group. (See GT3).

If G is abelian, then $\mathcal{E}(G)$ is exactly G's *torsion subgroup* G_T. In this case we actually have $\mathcal{E}(G) = \langle \mathcal{E}(G) \rangle$.

If G is a finite group with a normal p–Sylow subgroup P, then

$$P = \mathcal{P}_p(G).$$

(See GT3, Exercise 1.119).

This also shows that *if $P \trianglelefteq G$ is a p–Sylow subgroup, then P char G.*

We use some of the above remarks to prove the next theorem.

A group G is called *elementary abelian*, if G is abelian and there is a prime p, s.t. $x^p = 1$ for all $x \in G$. The definition of a solvable group is given in GT3, Section 1.18..

(1D) Theorem: *Let N be a minimal normal subgroup in the finite solvable group G. Then N is elementary abelian.*

Proof: ...

The Frattini argument

If H, $P \subseteq G$ are subgroups, then

$$N_H(P) = \{h \in H \mid hPh^{-1} = P\}$$

is called P's *normalizer in* H. This is a subgroup of H and $P \trianglelefteq N_G(P)$. Moreover $P \trianglelefteq G \Leftrightarrow N_G(P) = G$.

If H and K are subgroups of G, then their "product" $HK = H \cdot K$ is the subset

$$HK = \{g \in G \mid \exists h \in H, k \in K : \ g = hk\}.$$

(Se Chapter 2 and `GT3`, Section 1.6 for details.)

(1E) Theorem: (Frattini argument) *Let G be finite, $H \trianglelefteq G$. Let P be a p–Sylow subgroup in H. Then*

$$G = HN_G(P).$$

Proof: See eg. D Gorenstein: Finite groups, Theroem 1.3.7, p. 12

We may use the Frattini argument to prove

(1F) Theorem: *Let P be a p–Sylow subgroup in G. Let K be a subgroup in G, satisfying $N_G(P) \subseteq K$. Then $K = N_G(K)$.*

Proof: ...

2. On products of subgroups

G2 - 2007-version

If H and K are subgroups of G, we define

$$HK = H \cdot K = \{g \in G | \exists h \in H,\ k \in K : g = hk\}.$$

For results on HK, see GT3, Section 1.5 and 1.6, especially Lemma 1.39 and Theorem 1.40.

(2A) Theorem: *Let H and K be subgroups of the finite group G.*

(1) *The subset HK satisfies*

$$|HK| = |H|\ |K|/|H \cap K|.$$

In particular

$$|HK| \ \mid\ |H|\ |K|.$$

(2) *We have*

$$|G : H \cap K| \ \leq |G : H|\ |G : K|.$$

(3) *If HK is a subgroup of G, we have*

$$|G : H \cap K| \ \mid\ |G : H|\ |G : K|.$$

Proof: (1) See GT3, Lemma 1.39.

(2) As $HK \subseteq G$ we have $|HK| \leq |G|$ and then (1) shows, that

$$|H|\ |K|/|H \cap K| \leq |G|.$$

Divide this with $|H||K|$ and multiply by $|G|$ to get (2).

(3) is proved analandously, using that we now know that $|HK| \mid |G|$, since HK is a subgroup. □

(2B) Theorem: *If H and K are subgroups of subgroups of the finite group G and if $(|G : H|,\ |G : K|) = 1$, then $G = HK$.*

Proof: We show $|G| \mid |HK|$. As $|HK| \leq |G|$ we then get $|HK| = |G|$, ie. $G = HK$. Let p be a prime, $p \mid |G|$. Then $p \nmid |G : H|$ or $p \nmid |G : K|$, by

assumption. We then get that either H or K contains en p–Sylow group P of G. We get $|P| \mid |H| \mid |HK|$ or $|P| \mid |K| \mid |HK|$ by (2A). In any case $|P| \mid |HK|$. As p was arbitrary we get $|G| \mid |HK|$, as desired. □

Definition: Let $|G| = p^a m$, $(p, m) = 1$. A subgroup M of G with $|M| = m$ is called a *p–(Sylow) complement* in G. (M is a *p'–Hall subgroup*. See chapter 3.) The set of p–Sylow subgroups i G is denoted $Syl_p(G)$.

(2C) Corollary: *If $P \in Syl_p(G)$ and if M is a p–Sylow complement in G, then*

$$G = PM, \quad P \cap M = \{1\}.$$

Proof: Apply (2B) with $H = P$, $K = M$ to show $G = PM$. As $(|P|, |M|) = 1$ we get trivially $P \cap M = \{1\}$. □

Remarks: 1. A group G need not contain a p–Sylow complement. However if $P \in Syl_p(G)$, $P \trianglelefteq G$, then G contains a p–Sylow complement. This is a special case of the Schur–Zassenhaus Theorem in Chapter 3.
2. Generally we call the subgroup K of G a *complement* to the subgroup M, if we have

$$G = MK \quad \textit{and} \quad M \cap K = \{1\}.$$

(2D) Theorem: *Let H and K be subgroups of the finite group G. If the least common multiple (lcm) of $|H|$ and $|K|$ is $|G|$ then $HK = G$.*

Proof: Analandous to (2B). □

(2E) Theorem: *Let $|G| = {p_1}^{a_1} \cdots {p_r}^{a_r}$, where $p_i \neq p_j$, $i \neq j$ are primes. Let $I \subseteq \{1, \ldots, r\}$, such that for all $i \in I$ we have that G has a p_i–Sylow complement K_i. Then $|\bigcap_{i \in I} K_i| = \prod_{j \notin I} {p_j}^{a_j}$.*

Proof: Induction by $|I|$. For $|I| = 1$ we use the definition. Assume that the Theorem is shown for subsets $I' \subseteq I$, $I' \neq I$. Let $I = I^* \cup \{k\}$, $k \notin I^*$. Let $K^* = \bigcap_{i \in I^*} K_i$. By the induction hypothesis $|K^*| = {p_k}^{a_k} \prod_{j \notin I} {p_j}^{a_j}$. As $|K_k| = \prod_{j \neq k} {p_j}^{a_j}$ we get, that lcm $(|K^*|, |K_k|) = |G|$. By (2A) $|G| = |K^*|\,|K_k| / |\bigcap_{i \in I} K_i|$. The result follows by an easy calculation. □

Here is another application of (2A):

(2F) Theorem: *Let G be finite and $Q \subseteqq N \trianglelefteq G$. Let p be a prime. Then*

$$Q \in Syl_p(N) \Leftrightarrow \exists P \in Syl_p(G) : Q = P \cap N.$$

Proof: $\Rightarrow$ Let $Q \in Syl_p(N)$. Then in particular Q is a p–subgroup in G. Choose by Sylow's 2. Theorem, $P \in Syl_p(H)$, such that $Q \subseteq P$. Now $P \cap N$ is a p–subgroup of N, containing Q. As Q is a p–Sylow group in N, we get $Q = P \cap N$.
$\Leftarrow$ Let $P \in Syl_p(G)$, and put $Q = P \cap N$. We have by (2A)

$$|N : Q| = |N : P \cap N| = |N| \Big/ |P \cap N| = |NP|/|P| = |NP : P|$$

which divides $|G : P|$. As $P \in Syl_p(G)$ we get $p \nmid |G : P|$, and therefore $p \nmid |N : Q|$. As Q is a p–subgroup in N, we get $Q \in Syl_p(N)$ $\square$

(2G) Theorem: *Let G be finite, $N \trianglelefteq G$. Assume that K is a p–Sylow complement in G. Then $N \cap K$ et p–Sylow complement in N, and KN/N is a p–Sylow complement in G/N.*
Proof: ... $\square$

We may also use the above results to extend the claims of (1C). The next Theorem is about $\langle \mathcal{D}_p(G) \rangle$ in (1C).

(2H) Theorem: *Let G be finite, p a prime and $D := \langle g \in G \mid p \nmid |g| \rangle$. Then D is a characteristic subgroup of G and D is the smallest normal subgroup in G whose index in G is a power of p.*

Proof: By (1C) D *char* G. In particular $D \trianglelefteq G$. Let $P \in Syl_p(G)$. We claim $DP = G$. If $q \neq p$ is a prime and $q \mid |G|$, then D contains a q-Sylow subgroup Q of G, since all $g \in Q$ satisfy $p \nmid |g|$. Thus $DP = G$ (eg. by (2D)). Then $|G : D| = |P : P \cap D|$ a power of p.

Assume now that $N \trianglelefteq G$ and that $|G : N|$ is a power of p. We want to show $D \subseteq N$. It suffices to show that if $g \in G$, $p \nmid |g|$, then $g \in N$. Consider the coset $\bar{g} = gN$ as an element in the factor group $\bar{G} = G/N$. As $|\bar{g}| \mid |g|$ and $p \nmid |g|$ we get $p \nmid |\bar{g}|$. Thus $|\bar{g}|$ has on the one hand an order prime to p, and on the other hand a p-power order, since $\bar{G}$ has p-power order. We get $|\bar{g}| = 1$, ie. $g \in N$. $\square$

The subgroup D in (2H) is denoted $O^p(G)$, as mentioned in (1C). It is one of four characteristic subgroups of a finite group G, associated to a given prime p.

Let p be a prime. A p-group is a group of p-power order. A p'-group is a group of order prime til p. Correspondingly we define p- and p'-elements. The following is only of interest when $p \mid |G|$. We define

- $O^p(G)$ is the smallest normal subgroup in G, whose *index* $|G : O^p(G)|$ is a power of p.
- $O_p(G)$ is the largest normal subgroup i G, whose *order* $|O_p(G)|$ is a power of p (p-subgroup).
- $O^{p'}(G)$ is the smallest normal subgroup in G, whose *index* $|G : O^{p'}(G)|$ is prime til p.
- $O_{p'}(G)$ is the largest normal subgroup i G, whose *order* $|O_{p'}(G)|$ is prime til p (p'-subgroup).

You of course need to convince yourself that these subgroups are well defined. What is meant by smallest/largest? It could be by with respect to their order (number of elements) or with respect to the inclusion order. As we shall see for these subgroups it does not matter which order relation we choose.

Let us mention, that if $p \nmid |G|$, then the only p-element in $|G|$ is the identity element 1. In that case $O^p(G) = O_{p'}(G) = G$ and $O_p(G) = O^{p'}(G) = \{1\}$. How does this fit with Theorem (2M) below?

If H and K are subgroups of G and at least one of them is a normal subgroup in G, then HK is again a subgroup, as we have seen. We may then apply all of Theorem (2A). If H and K are both normal, then so is HK and $H \cap K$ is again normal. If for example $|G : H|$ and $|G : K|$ are both prime to p, then from Theorem (2A)(3) we get, that $|G : H \cap K|$ is prime to p. Thus also the intersection of *all* normal subgroups in G, of index prime to p is a normal subgroup with the same property. This subgroup is then $O^{p'}(G)$. Correspondingly you may argue with the other subgroups. For example HK is a normal p'-subgroup of G, if both H and K are, since $|HK| \mid |H|\,|K|$, by (2A)(1). Thus the product of *all* such subgroups is normal p'-subgroup, ie. it is $O_{p'}(G)$.

We now have:

(2I) Theorem: *The subgroup $O^p(G)$ may be described in the following equivalent ways*

(1) $O^p(G) = \bigcap_{\{A \trianglelefteq G |\ |G:A|\ isa\ p-power\}} A$

(2) $O^p(G) = \langle g \in G \mid g\ p' - element \rangle$

(3) $O^p(G) = \langle Q \mid Q \in \bigcup_{\{q\ prime\ \neq\ p\}} Syl_q(G) \rangle$

(4) $O^p(G) = \langle Q \mid Q\ p' - subgroup\ of\ G \rangle$

(2J) Theorem: *The subgroup $O^{p'}(G)$ may be described in the following equivalent ways*

(1) $O^{p'}(G) = \bigcap_{\{A \trianglelefteq G\ \mid\ p\ \nmid\ |G:A|\}} A$

(2) $O^{p'}(G) = \langle g \in G \mid g\ p - element \rangle$

(3) $O^{p'}(G) = \langle P\ | P \in Syl_p(G) \rangle$

(4) $O^{p'}(G) = \langle P\ | P\ p - subgroup\ of\ G \rangle$

(2K) Theorem: *The subgroup $O_p(G)$ may be described in the following equivalent ways*

(1) $O_p(G) = \langle A \trianglelefteq G\ | A\ er\ p - subgroup \rangle$

(2) $O_p(G) = \bigcap_{P\ \in\ Syl_p(G)} P$

(2L) Theorem: *The subgroup $O_{p'}(G)$ may be described in the following way*

(1) $O_{p'}(G) = \langle A \trianglelefteq G\ | A\ p' - subgroup \rangle$

Proof of the Theorems: That the groups are described by the property (1) follows from Theorem (2A), as explained above in the cases $O^{p'}(G)$ and $O_{p'}(G)$.

Proof for (2I): In Theorem (2H) it is shown that (1) and (2) are equivalent. Let $X = \langle Q \mid Q \in \bigcup_{\{q\ prime\ \neq\ p\}} Syl_q(G) \rangle$. As the elements in each of the generating subgroups Q for X consists of p'-elements, (2) shows that $X \subseteq O^p(G)$. On the other hand $X \trianglelefteq G$, as the set of generating subgroups Q is closed under conjugation. As X contains q-Sylow groups of G for all primes $q \neq p$, no prime $q \neq p$ can divide $|G : X|$. Thus $|G : X|$ is a power of p and thus $O^p(G) \subseteq X$. It is easily seen that the descriptions in (2) are (4) eqvivalent. (Why?)

Proof of (2J): *This is an exercise.*

Proof of (2K): Let $X = \bigcap_{P \in Syl_p(G)} P$. Assume that $A \trianglelefteq G$ is a p-group. Let $P \in Syl_p(G)$. Then the subgroup AP also has p-power order by (2A). As P er en Sylow group we get $AP = P$, ie. $A \subseteq P$. Thus $A \subseteq X$. By (1) we see that $O_p(G) \subseteq X$. Since the set of p-Sylow groups is closed under conjugation we have $X \trianglelefteq G$. Thus $X \subseteq O_p(G)$. $\square$

You may of course combine $O^p, O^{p'}, O_p, O_{p'}$. For example $O^p(O^{p'}(G))$ is $O^p(H)$, where $H = O^{p'}(G)$. This subgroup is also denoted $O^{pp'}(G)$. You may then continue with $O^{p'pp'}(G)$, etc. and get smaller subgroups of G. If we at some time reach the triviel subgroup $\{1\}$, we call G p-solvable. Analandously you may consider subgroups like $O_{p'p}(G)$, defined as follows: $O_{p'p}(G)/O_p(G) = O_{p'}(G/O_p(G))$ Clearly $O^{p'}(O^{p'}(G)) = O^{p'}(G)$ and $O^p(O^p(G)) = O^p(G)$.

(2M) Theorem:

(1) We have $O_{p'}(G) \subseteq O^p(G)$ and $O_p(G) \subseteq O^{p'}(G)$.

(2) $O_{p'}(G) = O^p(G) \Leftrightarrow G$ has a normal p-complement.

(3) $O_p(G) = O^{p'}(G) \Leftrightarrow G$ has a normal p-Sylow group.

Proof: (1) As $p \nmid |O_{p'}(G)|$ (2I)(4) shows that $O_{p'}(G) \subseteq O^p(G)$. The other inclusion in (1) follows from (2J)(4).

(2) $\Rightarrow$: Assume $O_{p'}(G) = O^p(G) = K$. We claim that K is a normal p-complement in G. Write $|G| = p^a m$, with $p \nmid m$. It follows from (2I)(3), that $m \mid |O^p(G)| = |K|$. As K also equals $O_{p'}(G)$, which is a p'-group, we have $m = |K|$. Thus K is a normal p-complement.

$\Leftarrow$: If K is a normal p-complement in G, we easily get $K = O^p(G) = O_{p'}(G)$.

(3) Write again $|G| = p^a m$. If $O_p(G) = O^{p'}(G) = P$, then P is a normal p-Sylow group in G : As $|G : O^{p'}(G)| \mid m$, we have $p^a \mid |O^{p'}(G)| = |P|$. Since $P = O_p(G)$ is a p-group, we get $|P| = p^a$. Conversely, if P is a normal p-Sylow group in G, then $P = O_p(G) = O^{p'}(G)$. $\square$

The last part of this chapter is a preparation for later chapters.

Definition: Let M be a subgroup in G. A subset $X \subseteq G$ is called a (left) transversal to M in G if $G = \dot{\bigcup}_{x \in X} xM$. Thus X contains exactly one element

from every coset of M in G. Remark that $G = XM$ and $|X| = |G : M|$. If M has a complement in G, then this complement is also a transversal to M in G. We later need the following:

(2N) Theorem: *Let $N \subseteq M \subseteq G$ be subgroups. If X is a transversal for M in G and Y a transversal for N in M, then XY is a transversal for N in G.*

Proof: We have $M = \dot{\bigcup}_{y\in Y} yN$ and $G = \dot{\bigcup}_{x\in X} xM$, whence

$$G = \dot{\bigcup}_{x\in X} xM = \dot{\bigcup}_{x\in X} x(\dot{\bigcup}_{y\in Y} yN) = \dot{\bigcup}_{t\in XY} tN.$$

You may also consider right transversals to a subgroup of G. $X \subseteq G$ is a right transversal to the subgroup $M \subseteq G$ if $G = \dot{\bigcup}_{x\in X} Mx$.

In analandy with (2N) we have

(2O) Theorem: *Let $N \subseteq M \subseteq G$ be subgroups. If X is a right transversal for M in G and Y a right transversal for N in M, then YX is a right transversal for N in G.* □

Remarks: 1°. X is a (left) transversal to M in $G \Leftrightarrow X^{-1}$ is a right transversal to M in G, since we have $(xM)^{-1} = Mx^{-1}$.

2°. If $M \trianglelefteq G$, then a right transversal X to M in G is also a left transversal and vice versa. If the subgroup M is *not* normal in G, then you may always find a left transversal til M in G, which is *not* a right transversal to M in G. (Exercise).

3. Hall subgroups and complements

G3 - 2007-version

We consider only *finite* groups in the Chapter. Let G be a finite group.

Definition: A subgroup H of G is called a *Hall subgroup*, if it satisfies

$$(|H|\,,\ |G:H|) = 1\ ,$$

ie. H's *order* is relatively prime to its *index* in G. (Philip Hall 1904–1982).

Clearly any p–Sylow group of a finite group is also a Hall subgroup. Also the trivial subgroups $\{1\}$ and G of G are Hall subgroups.

Let π be an arbitrary set of primes. If n is a natural number we write $n = {p_1}^{a_1} \cdots {p_k}^{a_k}$, where $p_1, \cdots, p_k$ are different primes, and $a_1, \cdots, a_k \in \mathbb{N}$. We define

$$n_\pi = \prod_{\{i|p_i \in \pi\}} {p_i}^{a_i} \quad , \quad n_{\pi'} = n/n_\pi\ .$$

(Thus if $n = 60$, $\pi = \{2, 3\}$, then $n_\pi = 12$, $n_{\pi'} = 5$.) Remark, that if $\tilde{\pi}$ is the set of primes, which are *not* in π, then $n_{\pi'} = n_{\tilde{\pi}}$. We define $n_\varnothing = 1$.

A π–*Hall subgroup* in the group G is a subgroup of order $|G|_\pi$. For example the p–Sylow groups are also π–Hall subgroups, where $\pi = \{p\}$. A π'–Hall subgroup in G is a subgroup of order $|G|_{\pi'}$.

Eksemple: The alternating group A_5 has *no* $\{3, 5\}$–Hall subgroup. Such a subgroup should have order 15. Every group of order 15 is cyclic. (`GT3`). But clearly A_5 (or S_5) does not contain an element of order 15. (Look at the cycle–structure of such an element).

Remark: If M is a π–Hall subgroup of G and there exist also a π'–Hall subgroup N i G, then N is a complement to M in G. (See the previous Chapter).

Generally Sylow's Theorems may thus not be extended to statements about the existence of Hall subgroups. But a famous Theorem of Philip Hall shows that Sylow's Theorems *may* be extended to arbitrary Hall subgroups, if we assume that G is solvable, and that they may *only* be extended in this way, when G is solvable.

(3A) Theorem: (P. Hall) *Let G be a* solvable *group. Assume that $|G| = nm$, where $(n, m) = 1$. Then:*

(1) G contains a Hall subgroup of order m;

(2) Any two Hall subgroups of order m i G are conjugate in G;

(3) A subgroup of G, whose order divides m is contained in a Hall subgroup of order m.

Remark: There is also a statement on the number of Hall subgroups of G of order m (corresponding to Sylow's 3. Theorem.) The statement is that this number is a product of factors a_i, where for each a_i there exists a prime divisor $p_i|m$, st.

$$a_i \equiv 1 \pmod{p_i} \ ,.$$

We do not prove this although it is not difficult.

Proof of (3A): See eg. M. Hall: Theory of groups, p. 141-143

Now we show that the statements of Theorem (3A) are only fulfilled solvable groups. The proof of this is based on the following Theorem, which may be proved using representation theory. There is also a purely group theoretic proof for the Theorem, which is quite complicated and we omit it.

(3B) Theorem: (Burnside) *Let G be a finite group of order $p^a q^b$, where p and q are primes. Then G is solvable.*

Proof: Omitted! □

We need also the following result.

(3C) Lemma: *Assume that $|G| = p^a q^b m$, where p and q are different primes, $a, b \in \mathbb{N}$ and $(p, m) = (q, m) = 1$. Assume in addition that G contains subgroups H, A and B, satisfying*

(1) $|H| = p^a q^b$;

(2) $A \neq G$, $|G : A| \mid p^a$;

(3) $B \neq G$, $|G : B| \mid q^b$.

Then G is not simple.

Proof ...

We can now show

(3D) Theorem: *Assume that the finite group G has a p-complement for all primes p with $p \mid |G|$. Then G is solvable.*

Remark: A p–complement is a π'–Hall subgroup, where $\pi = \{p\}$ and is also called a "p'–Hall subgroup" (like a p–Sylow group is a "p–Hall subgroup"). Thus (3D) has the following consequence.

(3E) Corollary: *Assume the the group G has en Hall subgroup of order m for enhver factorization $|G| = mn$, $(m, n) = 1$ of G's order. Then G is solvable.*

Proof of (3D): See eg. M. Hall: Theory of groups, p. 144-145

By Hall's Theorem a group G contains only π–Hall subgroups for all choices of the set of primes π, when G is solvable. But a non-solvable group may under certain conditions contain Hall subgroups for special choices of π. An example of this is Burnside's Theorem on the existence of a normalt p–complement (shown in Chapter 6). Here we prove the Schur–Zassenhaus Theorem, stating that if G has a *normal* π–Hall subgroup, then this has complement (not necessarily normal) which is then a π'–Hall subgroup in G. First we show the Theorem under a stronger assumption.

It should be mentioned that the method of proof for (3F) and the later Theorem (3I) er "cohomolandical" and the map t in the proofs is a "2-cocycle". You may find much more about cohomolandy theory for groups in many books, for example B. Huppert: *Endliche Gruppen I.*

(3F) Theorem: (Schur) *Let M be en normal abelian Hall subgroup i G. Then there exists a complement N til M i G.*

Proof: See eg. D Gorenstein: Finite groups p. 221-224

Next we show that the condition of M being abelian is not necessary in (3F), and get the Schur–Zassenhaus–Theorem. (Issai Schur 1875–1941, Hans Zassenhaus 1912–1991. Schur proved (3F) which ie really the hard part, and Zassenhaus then proved (3G) on the basis of (3F)).

Theorem (3G): (Schur–Zassenhaus Theorem) *Let M be a normal Hall subgroup in G of order m. Then there exists a complement N to M in G.*

Proof: See eg. D Gorenstein: Finite groups p. 221-224

(3H) Corollary: *If $P \in Syl_p(G)$, then P has complement K in $N_G(P)$, such that*

$$N_G(P) = PK \ .$$

($N_G(P)$ is a semidirect product of P and K. See the next Chapter).

Proof: P is a normal Hall subgroup in $N_G(P)$. Apply (3G). □

Remark: In continuation of (3G) you my ask whether two complements to M in G are conjugate in G. This is the case, but we cannot prove it here. You may prove without much difficulty that if $M \trianglelefteq G$ is a Hall subgroup, and *if either M or G/M is solvable*, then all complementer to M in G are conjugate in G. (See for example Theorem 6.2.1 i D. Gorensteins book *Finite Groups*). In 1963 Feit and Thompson proved that any finite group of odd order is solvable. But if $M \trianglelefteq G$ is a Hall subgroup, then $(|G : M|, |M|) = 1$ and thus $|G : M|$ or $|M|$ must be odd. Thus according to Feit–Thompson, either G/M or M be must be solvable. Feit–Thompson's proof is more than 250 pages long (Pacific Journal of Mathematics (1963)). There is a monandraph which treats an essential part of the proof (H. Bender–G. Glauberman: *Local analysis for the odd–order theorem*).

The next quite remarkable theorem does not appear to have anything to do with Theorem (3F), but the proofs are quite similar. They have the existence of a normal abelian subgroup of G in common and both are contained in a more general Theorem of Gaschütz, see for example Hauptsatz 17.4 i Huppert: *Endliche Gruppen I*, p. 121.

(3I) Theorem: (Gaschütz) *Let M be a normal abelian p-subgroup in G. Let P be a p-Sylow group in G. The following statements are equivalent*

(i) M has a complement in P

(ii) M has a complement in G.

Proof: See Kurzweil-Stellmacher: The theory of finite groups, p. 73-76.

4. Semidirect products - theory and examples

G4 - 2007-version

This chapter extends `GT3`, Chapter 1.19 considerably.

Let G be a group, and A a subgroup of then automorphism group $Aut(G)$. We form a new group called $G \rtimes A$, (the *semidirect product of G with/by A*). The underlying set is $G \times A$. The composition is defined by

$$(g, \varphi)(g', \psi) = (g\varphi(g'), \varphi\psi)$$

for $g, g' \in G$, $\varphi, \psi \in A$.

It is easily calculated that the associative law is fulfilled. The neutral/unit element is $(1, 1)$, and the inverse element to (g, φ) is $(\varphi^{-1}(g^{-1}), \varphi^{-1})$, since

$$(g, \varphi)(\varphi^{-1}(g^{-1}), \varphi^{-1}) = (g\varphi(\varphi^{-1}(g^{-1})), \varphi\varphi^{-1}) = (gg^{-1}, \varphi\varphi^{-1}) = (1, 1).$$

In particular $G \rtimes Aut(G)$ is called *the holomorph* of G and denoted $Hol(G)$. We are not going to discuss the holomorph of groups here.

Assume that G ans H are groups, and that there exists a homomorphism $\alpha : H \to Aut(G)$. We form a new group called $G \rtimes_\alpha H$ (the *semidirect product of G by H, relative to α*). The underlying set is $G \times H$, and the composition is defined by

$$(g, h)(g', h') = (g\alpha(h)(g'), hh').$$

(You may here consider "conjugation of g' by h", ie. $hg'h^{-1}$ in this group is being replaced by $\alpha(h)(g')$. (For elements in an *arbitrary* group we know that $ghg'h' = g(hg'h^{-1})hh'$.)

In $G \rtimes_\alpha H$ again $(1, 1)$ is the neutral element, and the inverse element to (g, h) is $(\alpha(h^{-1})(g^{-1}), h^{-1})$, since

$$\begin{aligned}(g, h)(\alpha(h^{-1})(g^{-1}), h^{-1}) &= (g\alpha(h)(\alpha(h^{-1})(g^{-1})), hh^{-1}) \\ &= (g(\alpha(h)\alpha(h^{-1}))(g^{-1}), hh^{-1}) = (g\alpha(1)(g^{-1}), hh^{-1}) \\ &= (gg^{-1}, hh^{-1}) = (1, 1).\end{aligned}$$

We used here that α is a homomorphism.

Special cases: (1) If $H \subseteq Aut(G)$ and α is the embedding of H in $Aut(G)$, them the two above constructions coincide. Therefore the first is a special case of the second.

(2) If $\alpha : H \to Aut(G)$ is defined by $\alpha(h) = 1$ (the identity), then $G \rtimes_\alpha H = G \times H$ is the usual direct product.

If α is clear from the context we often just write $G \rtimes H$ instead of $G \rtimes_\alpha H$.

You may want to *realize a given group as a semidirect product*:
On the one hand we have: If $X = G \rtimes_\alpha H$ is a semidirect product, then

$$G^* = \{(g,1) \mid g \in G\}, H^0 = \{(1,h) \mid h \in H\}$$

are subgroups of X. The maps

$$g \mapsto g^* = (g,1)\ ,\ h \mapsto h^0 = (1,h)$$

are obviously isomorphisms between G and G^* and between H and H^0.

Clearly $X = G^*H^0$ and $G^* \cap H^0 = \{(1,1)\}$. Furthermore $G^* \trianglelefteq X$, which is easily seen from the multiplication formula and the formula for inverse elements. If $g^* = (g,1) \in\ G^*$ and $h^0 = (1,h) \in H^0$, then

$$h^0 g^* (h^0)^{-1} = (1,h)(g,1)(1,h^{-1}) = (\alpha(h)(g),h)(1,h^{-1}) = (\alpha(h)(g),1) = (\alpha(h)(g))^*$$

On the other hand we may consider the following situation: Assume that Y is a group with subgroups G and H, which satisfy

$$G \trianglelefteq Y\ ,\ Y = GH.$$

Then Y may be "connected" with a semidirect product of G by H: For $h \in H$ we let $\alpha(h)$ be the restriction of the inner automorphism κ_h of Y to G. We thus have

$$\alpha(h)(g) = hgh^{-1} \ \text{ for } h \in H,\ g \in G.$$

Then α *is* a homomorphism from H to $Aut(G)$, and we may therefore form $X = G \rtimes_\alpha H$.

How are X and Y related? Here is the answer:

(4A) Theorem: *Let $Y = GH$ and $X = G \rtimes_\alpha H$ be as above. Then*

$$\rho(g,h) = gh$$

defines a surjective *group homomorphism from X to Y. We have*

$$G \cap H = \{1\} \Leftrightarrow \rho \ \text{ is an isomorphism.}$$

Proof: Let $g, g' \in G$, $h, h' \in H$. We have

$$\begin{aligned}
\rho((g,h)(g',h')) &= \rho(g\alpha(h)(g'), hh') \qquad \text{(multiplication in } X) \\
&= \rho(g(hg'h^{-1}), hh') \qquad \text{(definition of } \alpha(h)) \\
&= g(hg'h^{-1})hh' \qquad \text{(definition of } \rho) \\
&= ghg'h' \qquad \text{(cancel } h^{-1}h) \\
&= \rho(g,h)\rho(g',h') \qquad \text{(definition of } \rho)
\end{aligned}$$

Thus ρ is a homomorphism, and since $Y = GH$ it is clear that ρ is surjective. If $G \cap H = \{1\}$ we see that

$$\rho(g,h) = 1 \Leftrightarrow gh = 1 \Rightarrow g = h^{-1} \in G \cap H = \{1\} \Rightarrow g = h = 1 \ ,$$

so that ρ is injective in this case. If $G \cap H \neq \{1\}$ then $\rho(x, x^{-1}) = 1$ when $x \neq 1$, $x \in G \cap H$, so that ρ is *not* injective. $\square$

The above Theorem shows that when $G \cap H = \{1\}$, then Y yields an "inner" characterization of et semidirect product.

An *example* of a group Y realized as a semidirect product, is

$$Y = S_n, \quad G = A_n, \quad H = \langle (1,2) \rangle \quad n \geq 2.$$

Another example we have seen is the result of (3G). If G has a normal Hall subgroup M, then there exists a complement L to M in G. Thus G is a semidirect product of M with L.

Let us consider various other examples.

(4B) Example: *Dihedral groups.* If $G = \langle g \rangle$ is a cyclic group, then the map $\iota : g \mapsto g^{-1}$ is an automorphism of G. In this situation $G \rtimes \langle \iota \rangle$ is a dihedral group. If $|G| = n \leq \infty$, we denote $G \rtimes \langle \iota \rangle$ by D_n. We then have that $|D_n| = 2n$. The group D_n is generated by two elements $(g, 1)$ and $(1, \iota)$. Let us remark that $|(1,\iota)| = |(g,\iota)| = 2$ since $(g,\iota)^2 = (g\iota(g), 1) = (gg^{-1}, 1) = 1$. As D_n is generated by (g,ι) and $(1,\iota)$, we see that a dihedral group is generated by 2 elements of order 2 (so-called "involutions").

On the other hand a group generated by 2 involutions is isomorphic to a dihedral group. This is seen as follows. Assume that $D = \langle x, y \rangle$, where $x^2 = y^2 = 1$, $x \neq y$. We then have that $x^{-1} = x$ and $y^{-1} = y$. Put $g = xy$.

Then $G := \langle g \rangle$ is cyclic and $D = \langle g, y \rangle$. Furthermore $ygy^{-1} = yxyy^{-1} = yx = y^{-1}x^{-1} = (xy)^{-1} = g^{-1}$. Thus conjugation by y correponds to the map ι above.

When $n \in \mathbb{N}$, $n \geq 3$, then D_n may be realized as a subgroup of S_n, if we consider the subgroups

$$D_n^* = \langle (1, 2, \cdots, n), \quad \tau = (1, n)(2, n-1)\cdots \rangle$$

of S_n. If $G = \langle (1, 2, \cdots, n) \rangle$, $H = \langle \tau \rangle$ then $D_n^* = GH$ and $G \trianglelefteq D_n^*$, $G \cap H = \{1\}$, since

$$\tau(1, 2, \cdots, n)\tau^{-1} = (n, n-1, \cdots, 2, 1) = (1, 2, \cdots, n)^{-1}.$$

It is the clear that $D_n \cong D_n^*$ (use (4A)). We also have that $D_3^* \cong S_3$, as they have the same order. Let us remark that for $n = 4$ we have $|D_4^*| = 8$, so that D_4^* is a 2–Sylow group in S_4, (and also in S_5. Why?).

The definition may be extended to the case where G is an abelian group. The map $\iota : g \mapsto g^{-1}$, $G \to G$, is still an automorphism of G, so you may form a "di-abelian" group $G \rtimes \langle \iota \rangle$ of order $2|G|$. In the following we do not distinguish between the abstract group D_n and the concrete permutation group D_n^*.

(4C) Example: *Permutation matrices and monomial groups.*

If R is a commutative ring with unit element 1, $n \in \mathbb{N}$, then the set of invertible $n \times n$–matrices with coefficients from R form a group called $GL(n, R)$ $(= \{A \in R_n^n \mid \det A \text{ invertible in } R\})$. When $\pi \in S_n$ we define a matrix $P(\pi) \in R_n^n$ by

$$P(\pi) = [a_{ij}] \quad \text{where} \quad a_{ij} = \delta_{i\pi(j)}$$

(δ is "Kronecker delta"). Clearly $P(\pi)$ has exactly one element $\neq 0$ in each column and in each row. Repeated application of the column rule for determinants show that $\det P(\pi) = \pm 1$, so that $P(\pi) \in GL(n, R)$.

If $\pi, \rho \in S_n$ we have $P(\pi)P(\rho) = P(\pi\rho)$: Let $P(\pi)P(\rho) = [c_{ij}]$; then

$$c_{ij} = \sum_k \delta_{i\pi(k)}\delta_{k\rho(j)} \neq 0 \Leftrightarrow$$

$$\text{There exists a } k \text{ such that } \quad k = \rho(j) \quad \text{and} \quad \pi(k) = i$$

$$\Leftrightarrow \pi\rho(j) = i,$$

ie. $c_{ij} = \delta_{i\pi\rho(j)}$. This means that P is a *homomorphism* from S_n to $GL(n,R)$. Clearly P is injective so we may consider S_n as a subgroup of $GL(n,R)$.

A matrix on the form $P(\pi)$, $\pi \in S_n$ is called a $(n \times n-)$ *permutation matrix*. We have:

$$\det P(\pi) = sign(\pi), \qquad (\pi\text{'s sign})$$

$$P(\pi)^t = P(\pi^{-1}) \quad \text{for all } \pi \in S_n.$$

Both claims are proved by expressing π as a product of transpositions (ie. permutations on the form (i,j)): The permutation matrix $P((i,j))$ is obtained from the unit matrix E_n by interchanging the i'th and the j'te column. Thus $\det P(\tau) = -1$, when τ is a transposition. Clearly we also have $P(\tau) = P(\tau)^t$, when τ is a transposition. If $\pi = \tau_1\tau_2\cdots\tau_k$, where all τ_i are transpositions then

$$det(P(\pi)) = \prod_{i=1}^{n} det(P(\tau_i)) = (-1)^k = sign(\pi)$$

and

$$P(\pi)^t = [P(\tau_1)\cdots P(\tau_k)]^t = P(\tau_k)^t\cdots P(\tau_i)^t$$
$$= P(\tau_k)\cdots P(\tau_1) = P(\tau_k\cdots\tau_1) = P(\pi^{-1}).$$

A permutation matrix consists of zeros except exactly one 1 in each row and each column. You may now replace the numbers 1 in a permutation matrix $P(\pi)$, $\pi \in S_n$ by n elements from a given group G. If $g_1, g_2, \ldots, g_n \in G$, $\pi \in S_n$ we put

$$P(g_1, \ldots, g_n; \pi) = (\delta_{i\pi(j)}g_i).$$

This is of course no longer an element in $GL(n,R)$, but a "formal" matrix with elements from the set $G \cup \{0\}$ (when we define that $\delta_{ii}g = g$, $\delta_{ij}g = 0$ for $i \neq j$). If then G is a group and A a subgroup of S_n we put

$$Mon(G,A) = \{P(g_1,\cdots,g_n;\pi) \mid g_i \in G \ \ \pi \in A\},$$

a set of "G–monomial" matrices.

If in addition we define that $0 + g = g + 0 = g$ for $g \in G$, then G's composition and the usual rule for matrix multiplication induces a composition on $Mon(G,A)$. If we "multiply" the matrices

$$P(g_1,\cdots,g_n;\pi) \quad \text{and} \quad P(h_1,\cdots,h_n;\rho)$$

and use the rules mentioned above we get a matrix $[c_{ij}]$, where

$$c_{ij} = \sum_k \delta_{i\pi(k)} g_i \delta_{k\rho(j)} h_k = \delta_{i\pi\rho(j)} g_i h_{\rho(j)} = \delta_{i\pi\rho(j)} g_i h_{\pi^{-1}(i)}$$

so that

$$P(g_1, \cdots, g_n; \pi) P(h_1, \cdots, h_n; \rho) = P(g_1 h_{\pi^{-1}(1)}, \cdots, g_n h_{\pi^{-1}(n)}; \pi\rho).$$

Using this "matrix multiplication" $Mon(G, A)$ becomes a group with $P(1, \cdots, 1; (1))$ as neutral element and where

$$P(g_1, \cdots, g_n; \pi)$$

has

$$P(g_{\pi(1)}^{-1}, \cdots, g_{\pi(n)}^{-1}; \pi^{-1})$$

as inverse element. We call $Mon(G, A)$ a (G–)*monomial group.*

Now $Mon(G, A)$ is an "inner" semidirect product of the normal subgroup

$$G^* = \{P(g_1, \cdots, g_n; (1)) \mid g_i \in G, i = 1, 2, \cdots, n\},$$

(which is isomorphic to $\underbrace{G \times \cdots \times G}_{n}$) with the subgroup $A^* = \{P(1, \cdots, 1; \pi) \mid \pi \in A\}$ (which is isomorphic to A.)

(4D) Example: Let us look at the monomial group $Mon(G, A)$ (as a semidirect product) from the"outside".

If $A \subseteq S_n$ and $G^* = \underbrace{G \times \cdots \times G}_{n}$ $(= G^n)$, we may define a homomorphism $\alpha : A \to Aut(G^*)$ by

$$\alpha(\pi)(g_1, \cdots, g_n) = (g_{\pi^{-1}(1)}, \cdots, g_{\pi^{-1}(n)}).$$

It may look odd that the map $\beta : A \to Aut(G^*)$ given by

$$\beta(\pi)(g_1, \cdots, g_n) = (g_{\pi(1)}, \cdots, g_{\pi(n)})$$

is *not* a homomorphism. The connection between α and β is that $\alpha(\pi) = \beta(\pi^{-1})$, so that if one of the maps is a homomorphism, then the other is an *antihomomorphism.* That α is a homomorphis is seen as follows:

Assume that $\pi, \rho \in A$. Let

$$\alpha(\rho)(g_1, \cdots, g_n) = (h_1, \cdots, h_n)$$

$$\alpha(\pi)(h_1, \cdots, h_n) = (k_1, \cdots, k_n).$$

By definition $h_i = g_{\rho^{-1}(i)}$ and $k_i = h_{\pi^{-1}(i)}$ for $i = 1, \cdots, n$. We then get that $k_i = h_{\pi^{-1}(i)} = g_{\rho^{-1}(\pi^{-1}(i))} = g_{(\pi\rho)^{-1}(i)}$. Thus

$$\alpha(\pi) \circ \alpha(\rho)(g_1, \cdots, g_n) = (k_1, \cdots, k_n)$$

$$= (g_{(\pi\rho)^{-1}(1)}, \cdots, g_{(\pi\rho)^{-1}(n)}) = \alpha(\pi\rho)(g_1, \cdots, g_n),$$

ie. $\alpha(\pi) \circ \alpha(\rho) = \alpha(\pi\rho)$. Only when A is abelian, β will be a homomorphism.

We may now define an isomorphism φ

$$G^* \rtimes_\alpha A \overset{\varphi}{\cong} Mon(G, A)$$

by $\varphi(g_1, \cdots, g_n; \pi) = P(g_1, \cdots, g_n; \pi)$. The multiplication in $G^* \rtimes A$ is

$$(g_1, \cdots, g_n; \pi)(h_1, \cdots, h_n; \rho) = (g_1 h_{\pi^{-1}(1)}, \cdots, g_n h_{\pi^{-1}(n)}; \pi\rho).$$

It is necessary but not very "nice" that you have to apply π^{-1} on the indices of the h_i's. This may be avoided by "interchanging " G and A, as we do in the next example.

(4E) Example: (*Wreath product, Kransprodukt*). As in (4D) $A \subseteq S_n$ and $G^* = \underbrace{G \times \cdots \times G}_{n}$. We define a composition on $A \times G^*$ by

$$(\pi; g_1, \cdots, g_n)(\rho; h_1, \cdots, h_n) = (\pi\rho; g_{\rho(1)} h_1, \cdots, g_{\rho(n)} h_n).$$

Then $A \times G^*$ is a group with $((1); 1, \cdots, 1)$ as a neutral element, and $(\pi; g_1, \cdots, g_n)$ has $(\pi^{-1}; h_1, \cdots, h_n)$ as inverse element, where $h_i = g^{-1}_{\pi^{-1}(i)}$.

This group is called the *wreath productet of G by A*, and denoted $G \wr A$.

Now $G \wr A$ may also by realized by "monomial" matrices, and

$$G \wr A \simeq Mon(G, A).$$

If $(\pi; g_1, \cdots, g_n) \in G \wr A$ we put

$$P^*(\pi; g_1, \cdots, g_n) = (\delta_{i\pi(j)} g_j).$$

The only difference between this and $P(g_1, \cdots, g_n; \pi)$ is that "g_i" is replaced by "g_j". If we "multiply" $P^*(\pi; g_1, \cdots, g_n)$ and $P^*(\rho; h_1, \cdots, h_n)$ we get $P^*(\pi\rho; g_{\rho(1)}h_1, \cdots, g_{\rho(n)}h_n)$ so that P^*–matrices form a group $Mon^*(G, A)$, which is isomorphic to $G \wr A$.

We have now using G and A constructed four groups, two "matrix groups" $Mon(G, A)$ and $Mon^*(G, A)$, and two "abstract" groups $G^* \rtimes_\alpha A$ (i (4D)) and $G \wr A$ here. We have shown that

$$G^* \rtimes_\alpha A \simeq Mon(G, A) \quad \text{and at} \quad G \wr A \simeq Mon^*(G, A).$$

To complete the picture we want to show that

$$G^* \rtimes_\alpha A \simeq G \wr A.$$

First a Remark.

(4F) Remark: *The "opposite" group.* If G ia an arbitrary group we may form its opposite group G^{op}, as follows. The underlying set is G's elements, and the composition $\circ$ i G^{op}, is given by

$$g \circ h = hg$$

(where we have used the composition in G on the right hand side!) It is clear that G^{op} is a group with the same neutral element and same inverse elements. Moreover the map $\iota : g \mapsto g^{-1}$ is an *isomorphism* between G and G^{op}, since

$$\iota(gh) = (gh)^{-1} = h^{-1}g^{-1} = \iota(h)\iota(g) = \iota(g) \circ \iota(h).$$

(4G) Theorem: *Let $G \wr A$ and $G^* \rtimes_\alpha A$ be as before. By*

$$\psi : (\pi; g_1, \cdots, g_n) \mapsto (g_1^{-1}, \cdots, g_n^{-1}; \pi^{-1})$$

is defined an isomorphism between $G \wr A$ and $(G^* \rtimes_\alpha A)^{op}$. Thus we also have

$$G \wr A \simeq G^* \rtimes_\alpha A.$$

Proof: We have

$$\psi(\pi; g_1, \cdots, g_n) \circ \psi(\rho; h_1, \cdots, h_n) = (h_1^{-1}, \cdots, h_n^{-1}; \rho^{-1})(g_1^{-1}, \cdots, g_n^{-1}, \pi^{-1})$$

$$= (h_1^{-1}g_{\rho(1)}^{-1}, \cdots, h_n^{-1}g_{\rho(n)}^{-1}; \rho^{-1}\pi^{-1}) = \psi(\pi\rho; g_{\rho(1)}h_1, \cdots, g_{\rho(n)}h_n) =$$
$$\psi((\pi; g_1, \cdots, g_n)(\rho; h_1, \cdots, h_n)).$$

□

It is easy to find wreath products as subgroups in symmetric groups:

(4H) Remark: *If $G \subseteq S_m$ and $A \subseteq S_n$, then $G \wr A$ is (isomorphic to) a subgroup of S_{mn}.*

Proof: Let $(\pi; g_1, \cdots, g_n) \in G$, and consider

$$P^*(\pi; g_1, \cdots, g_n) = [\delta_{i\pi(j)}g_j].$$

If replace g_j by $P(g_j)$, then $P^*(\pi; P(g_1), \cdots, P(g_n))$ becomes a $mn \times mn$–permutation matrix. □

(4I) Example: *(of (4H))* Let $m = 3$, $n = 2$, $\pi = (1, 2, 3) \in S_3$, $g_1 = (1, 2)$, $g_2 = (1)$, $g_3 = (1, 2) \in S_2$ such that $P^*(\pi; P(g_1), P(g_2), P(g_3)$ should be a 6×6-permutation matrix. Let us calculate this and the correponding permutation. First we consider the permutation matrix $P(\pi)$

$$P(\pi) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

by (4C). In this matrix we replace the 1 in the j'th column by the 2×2-matrix $P(g_j)$ $j = 1, 2, 3$ and the 0's by 2×2-zero matrices

$$P^*(\pi; P(g_1), P(g_2), P(g_3)) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

This is a 6×6-permutation matrix. The corresponding permutation ρ is calculated by considering the position of the 1 in the various columns. We get

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

(Here for example $\rho(1) = 4$ because the 1 in the first column is in row 4). Thus

$$\rho = (1, 4, 6)(2, 3, 5).$$

Another way of calculating ρ is as follows: Consider g_1 as a permutation of $\{1, 2\}$, g_2 as a permutation of $\{3, 4\}$ and g_3 as a permutation of $\{5, 6\}$. Then $g_1g_2g_3 = (1, 2)(3)(4)(5, 6) = (1, 2)(5, 6)$. Next you consider $\pi = (1, 2, 3)$ as a permutation $\Delta(\pi)$ of 6 which permutes the sets $\{1, 2\}$, $\{3, 4\}$, $\{5, 6\}$ by $1 \to 3 \to 5 \to 1$ and $2 \to 4 \to 6 \to 2$, ie.

$$\Delta(\pi) = (1, 3, 5)(2, 4, 6).$$

For the product $\Delta(\pi)g_1g_2g_3$ we then get

$$(1, 3, 5)(2, 4, 6)(1, 2)(5, 6) = (1, 4, 6)(2, 3, 5),$$

the same permutation ρ as before! (Writing Δ in front of π, ie. $\Delta(\pi)$ means intuitively that we are dealing with a "duplicartion" of π. If $\rho = (1, 3) \in S_3$ then $\Delta(\rho) = (1, 5)(2, 6)$.)

(4J) Remark: *If G is finite, and $A \subseteq S_n$, then $|G \wr A| = |G|^n|A|$.*

(4K) Exaeple: (*Sylow groups in the symmetric groups S_{p^a}*).

Let p be a prime. If $n \in \mathbb{N}$ we let $\nu_p(n)$ be the largest non negative number such that $p^{\nu_p(n)} \mid n$. For example $\nu_3(72) = 2$ as $72 = 3^2 \cdot 8$. Let us consider $\nu_p(|S_{p^a}|)$, $a \geq 1$. We have $\nu_p(|(S_{p^a}|) = \nu_p(p^a!)$. It is clear that p^{a-1} among the numbers $1, \cdots, p^a$ are divisible by p, namely $p, 2p, \cdots, p^{a-1}p$. Moreover p^{a-2} are divisible by p^2 (if $a \geq 2$), namely $p^2, 2p^2, \cdots, p^{a-2}p^2$. By continuing with p^3 etc. we get

$$\nu_p(p^a!) = p^{a-1} + p^{a-2} + \cdots + 1 = (p^a - 1)/(p - 1).$$

For $a = 1$, a p–Sylow group in S_p is cyclic, generated by for example $(1, 2, \cdots, p)$, ie. $\simeq \mathbb{Z}_p$. By (4J) $|\mathbb{Z}_p \wr \mathbb{Z}_p| = p^{p+1}$. Thus $\mathbb{Z}_p \wr \mathbb{Z}_p$ has the same order as a p–Sylow group in S_{p^2}. This is generalized: Let us inductively define the group X_a by $X_1 = \mathbb{Z}_p$, $X_a = X_{a-1} \wr \mathbb{Z}_p$. Using induction over a we see that X_a is isomorphic to a subgroup of S_{p^a} (use (4H)) and that $\nu_p|X_a| = \nu_p(|S_{p^a}|) = \nu_p(p^a!)$ (use (4J)), such that the p–Sylow group of S_{p^a} is an iterated wreath product of a cyklic groups of order p. Let us

consider a concrete realization of the p–Sylow group i S_{p^2}. This group has an elementary abelian subgroup of order p^p, namely

$$\langle(1,2,\cdots,p)\rangle \times \langle(p+1,\cdots,2p)\rangle \times \cdots \times \langle(\cdots,p^2)\rangle.$$

This corresponds to the subgroup $G \times \cdots \times G$ in the generel case. The group A becomes in this example the group generated by

$$\langle(1,p+1,2p+1,\cdots,(p-1)p+1)(2,p+2,\cdots,(p-1)p+2)\cdots(p,2p,\cdots,p^2)\rangle$$

In the case $p = 2$ the 2–Sylow group of S_4 is generated by $(1,2)$ and $(1,3)(2,4)$. The group "$G\times G$" becomes $\langle(1,2)\rangle\times\langle(3,4)\rangle$ and $A = \langle(1,3)(2,4)\rangle$. If we go to S_8 its 2–Sylow group is generated by

$$(1,2), \quad (1,3)(2,4) \quad \text{and} \quad (1,5)(2,6)(3,7)(4,8).$$

Think about this! How does it look in S_{16}? Notice that each of these elements is a "duplication" of the previous one in the same way as in (4I)!

(4L) Remark: You can show that the p–Sylow group in S_n, n arbitrary, may be described as follows:

Write n "p–adically", ie.

$$n = a_0 + a_1, p + \cdots + a_k p^k, \quad \text{where} \quad 0 \leq a_i \leq p-1.$$

Then in S_n the p–Sylow group is isomorphic to

$$X_1^{a_1} \times X_2^{a_2} \times \cdots \times X_k^{a_k},$$

where ${X_i}^{a_i} = \underbrace{X_i \times \cdots \times X_i}_{a_i}$ and X_i is as in the previous example.

We remind about the definition of *centralizer* (`GT3`). If $a \in G$, then a's centralizer in G is the subgroup

$$C_G(a) = \{g \in G \ \ |ga g^{-1} = a\}.$$

Correpondingly $C_G(X)$ is defined for a subset X of G.

(4M) Example: The wreath product also plays a rôle in the description of centralizers of elements in symmetric groups. We consider only the case of

"homocyclic" elements, ie. elements which is a product of cycles of the same length.

Let $k, \ell \in \mathbb{N}$ and assume that $\kappa \in S_{k\ell}$ is a product of k disjoint cycles of the same length ℓ. We explain that

$$C_{S_{k\ell}}(\kappa) \cong \mathbb{Z}_\ell \wr S_k,$$

where $\mathbb{Z}_\ell$ ís a cyclic group of order ℓ.

We assume that

$$\kappa = (a_{11}, a_{12}, \cdots, a_{1\ell})(a_{21}, a_{22}, \cdots, a_{2\ell}) \cdots (a_{k1}, a_{k2}, \cdots, a_{k\ell}),$$

where the a_{ij}'s are different numbers between 1 and $k\ell$. When $\varphi \in S_{k\ell}$

$$\varphi\kappa\varphi^{-1} = (\varphi(a_{11}), \varphi(a_{12}), \cdots, \varphi(a_{1\ell})) \cdots (\varphi(a_{k1}), \varphi(a_{k2}), \cdots, \varphi(a_{k\ell})).$$

Therefore $\varphi \in C(\kappa) = C_{S_{k\ell}}(\kappa)$ if and only if the sets of cycles

$$\{(a_{11}, a_{12}, \cdots, a_{1\ell}), \cdots, (a_{k1}, a_{k2}, \cdots, a_{k\ell})\}$$

and

$$\{(\varphi(a_{11}), \varphi(a_{12}), \cdots, \varphi(a_{1\ell})), \cdots, (\varphi(a_{k1}), \varphi(a_{k2}), \cdots, \varphi(a_{k\ell}))\}$$

are identical. This means that if $\varphi \in C(\kappa)$ and we know $\varphi(a_{i1})$, then also $\varphi(a_{i2}), \cdots, \varphi(a_{i\ell})$ are determined since the order in cycles must be respected: If $\varphi(a_{i1}) = a_{i'j'}$ where $1 \leq i' \leq k$ and $1 \leq j' \leq \ell$, then also

$$(*) \quad \varphi(a_{ij}) = a_{i'(j'+j-1)} \quad \text{for} \quad 1 \leq j \leq \ell,$$

where the second index is calculated modulo ℓ. An element $\varphi \in C(\kappa)$ is thus completely determined by

$$\varphi(a_{11}), \varphi(a_{21}), \cdots, \varphi(a_{k1}).$$

As $a_{11}, a_{21}, \cdots, a_{k1}$ are all in different cycles i κ, then also $\varphi(a_{11}), \varphi(a_{21}), \cdots, \varphi(a_{k1})$ must be in different cycles.

On the other hand every choice of $\varphi(a_{11}), \varphi(a_{21}), \cdots, \varphi(a_{\ell 1})$ in different cycles yields an element in $C(\kappa)$ using $(*)$ above.

Given $\pi \in S_k$ we may in particular define its "duplication element" $\Delta(\pi) \in C(\kappa)$ by

$$(**) \quad \Delta(\pi)a_{i1} = a_{\pi(i)1} \quad 1 \leq i \leq k.$$

(By $(*)$ we also have $\Delta(\pi)a_{ij} = a_{\pi(i)j}$ for all i, j).

Let now $\varphi \in C(\kappa)$ be determined by

$$(***) \quad \varphi(a_{i1}) = a_{\pi(i)t_i} \quad \text{for} \quad 1 \leq i \leq k.$$

Here $1 \leq t_i \leq \ell$ for all i. As $\varphi(a_{11}), \cdots, \varphi(a_{k1})$ are different cycles, π is a permutation of $1, \cdots, k$, ie. $\pi \in S_k$. By definition of $\Delta(\pi^{-1})$ we then get from $(**)$ and $(***)$

$$\Delta(\pi^{-1})\varphi(a_{i1}) = a_{it_i}.$$

It is clear that $\Delta(\pi^{-1}) = \Delta(\pi)^{-1}$, since Δ is a homomorphism $S_k \to C(\kappa)$. Let us put $\psi = \Delta(\pi^{-1})\varphi = \Delta(\pi)^{-1}\varphi$. We then have

$$\psi(a_{i1}) = a_{it_i} \quad \text{for} \quad 1 \leq i \leq k.$$

Let us denote the cycles in κ by $z_1, \cdots, z_k$, ie.

$$z_i = (a_{i1}, a_{i2}, \cdots, a_{i\ell}).$$

As disjoint cycles are permutable it is clear that $z_i \in C(\kappa)$ for all i. Thus also the element ψ' defined by

$$\psi' = z_1^{t_1-1} z_2^{t_2-1} \cdots z_k^{t_k-1} \in C(\kappa).$$

Now for $1 \leq i \leq k$

$$\begin{aligned} \psi'(a_{i1}) &= z_i^{t_i-1}(a_{i1})u \qquad \text{(why?)} \\ &= a_{it_i} \qquad \text{(why??)} \end{aligned}$$

We conclude that $\psi = \psi'$ and get that

$$\varphi = \Delta(\pi) \cdot z_1^{t_1-1} \cdots z_k^{t_k-1}.$$

If we define a map

$$\alpha : \mathbb{Z}_k \wr S_k \to C(\kappa)$$

by

$$\alpha(\pi; s_1, \cdots, s_k) = \Delta(\pi) \cdot z_1^{s_1} \cdots z_k^{s_k},$$

where the s_i's are calculated modulo $\ell = |z_i|$, then α is surjective by the above. It is easy to see that α is a homomorphism, and that the kernel of α is triviel. Thus α is an isomorphism.

In conclusion we can say that if you want to consider $G \wr A$, where $G \subseteq S_m$ and $A \subseteq S_n$ as a subgroup of S_{mn}, you let the n copies of G in $G^* = G \times \cdots \times G$ (n gange) operate on pairwise disjoint subsets of $\{1, \cdots, mn\}$, where each of these subsets have m elements. By "duplication" the elements of A are blown up to permute the n disjoint subsets, on which the G's operate.

On subgroups in a direct product

We describe a method so that you may in principle determine *all* subgroups of the direct product of two groups. This parametrization of the subgroups is usually not found in textbooks on group theory although it is fairly simple.

Let G and H be groups and $X = G \times H$ the direct product of G and H. Consider the following set of 5-tuples:

$$\mathcal{U}(G,H) = \{(G_1, G_2, H_1, H_2, \varphi)\}$$

where $G_2 \trianglelefteq G_1 \subseteq G$ are subgroups in G, $H_2 \trianglelefteq H_1 \subseteq H$ subgroups in H, and φ is a group isomorphism $\varphi : G_1/G_2 \to H_1/H_2$.

If $T = (G_1, G_2, H_1, H_2, \varphi) \in \mathcal{U}(G,H)$ we put

$$U_T = \{(g,h) \in G \times H \mid g \in G_1, h \in H_1 \text{ and } \varphi(gG_2) = hH_2\}.$$

Here we consider gG_2 (hH_2) as an element in G_1/G_2 (H_1/H_2).

(4N) Theorem: *The map $T \to U_T$ is a bijection between the sets $\mathcal{U}(G,H)$ and the set of subgroups of $G \times H$.*

Proof: We first remark that if $T \in \mathcal{U}(G,H)$, then U_T *is* a subgroup of $G \times H$: If (g,h), $(g_1,h_1) \in U_T$ we have $\varphi(gG_2) = hH_2$ and $\varphi(g_1^{-1}G_2) = h_1^{-1}H_2$, since φ is a homomorphism. Thus we get that

$$\varphi(gg_1^{-1}G_2) = \varphi(gG_2)\varphi(g_1^{-1}G_2) = hH_2h_1^{-1}H_2 = hh_1^{-1}H_2$$

ie. $(gg_1^{-1}, hh_1^{-1}) = (g,h)(g_1,h_1)^{-1} \in U_T$.

It is also clear that if $T, T' \in \mathcal{U}(G,H)$ and $T \neq T'$ (ie. if at least one of the five "coordinates" in T and T' is different), then $U_T \neq U_{T'}$.

Let now U be a subgroup of $G \times H$. We show that there exists $T \in \mathcal{U}(G,H)$, such that $U = U_T$. Put

$$G_1 = \{g \in G \mid \text{ There exists } h \in H, \text{ så } g,h) \in U\}$$

$$G_2 = \{g \in G \mid (g,1) \in U\}$$

$$H_1 = \{h \in H \mid \text{ There exists } g \in G, \text{ så } (g,h) \in U\}$$

$$H_2 = \{h \in H \mid (1,h) \in U\}.$$

It is clear that G_1, G_2 are subgroups of G, and H_1, H_2 are subgroups of H and $G_2 \subseteq G_1$, $H_2 \subseteq H_1$.

Assume now that $h \in H_1$, $x \in H_2$. Choose $g \in G$, such that $(g,h) \in U$. We also have $(1,x) \in U$ so that

$$(g,h)(1,x)(g,h)^{-1} = (1, hxh^{-1}) \in U,$$

ie. $hxh^{-1} \in H_2$. Thus $H_2 \trianglelefteq H_1$ (and analogously $G_2 \trianglelefteq G_1$).

Assume that $g \in G$, and that $h, h_1 \in H$ both satisfy $(g,h) \in U$, $(g,h_1) \in U$. By definition of H_1 we get $h, h_1 \in H_1$. Furthermore $g \in G_1$. We have $(g,h)^{-1}(g,h_1) = (1, h^{-1}h_1) \in U$ so that $h^{-1}h_1 \in H_2$. Thus $hH_2 = h_1H_2$. We see that $\psi : g \mapsto hH$ defines a map from $G_1 \to H_1/H_2$. It is clear that this map is a homomorphism. If $x \in \ker(\psi)$, there exists a $h_2 \in H_2$, such that $(x, h_2) \in U$. As $(1, h_2) \in U$ (because $h_2 \in H_2$) we get $(x, 1) \in U$, ie. $x \in G_2$. It is also easily seen that ψ is surjective.

By the first isomorphism Theorem for groups ψ induces an isomorphism $\varphi : G_1/G_2 \to H_1/H_2$ and we then get that $U = U_T$, where

$$T = (G_1, G_2, H_1, H_2, \varphi) \in \mathcal{U}(G,H)$$

.

(4O) Remark: Let $(G_1, G_2, H_1, H_2, \varphi) = T \in \mathcal{U}(G,H)$ as above. We than have

$$|U_T| = |G_1||H_2| = |G_2||H_1|,$$

if the groups are finite. (Why?)

(4P) Remark: A special class of subgroups of $G \times H$ are those on the forme $G_1 \times H_1$, G_1 subgroup in G, H_1 subgroup in H. The corresponding $T \in \mathcal{U}(G,H)$ is then

$$(G_1, G_1, H_1, H_1, 1).$$

A generalization of (4N) to a direct product of three or more subgroups is much more complicated than you might expect!

5. Subgroups and Verlagerung

G5 - 2007-version

Some parts of this Chapter are also discussed in GT3, Chapter 1.16.

(5A) Remark: Let us consider a wreath product $G \wr A$ as in (4E). The map

$$(\pi; g_1, \cdots, g_n) \mapsto \pi$$

is a en homomorphism from $G \wr A$ onto A with G^* as a kernel. But generally none of the following maps are homomorphisms.

$$(\pi; g_1, \cdots, g_n) \mapsto g_i \qquad (G \wr A \to G)$$

$$(\pi; g_1, \cdots, g_n) \mapsto (g_1, \cdots, g_n) \qquad (G \wr A \to G^*)$$

$$(\pi; g_1, \cdots, g_n) \mapsto g_1 g_2 \cdots g_n \qquad (G \wr A \to G).$$

The first two maps may only be homomorphisms when $A = \{(1)\}$ which is uninteresting. However the third map may be a homomorphism, when G is abelian. This may be generalized as follows:

Assume that $N \trianglelefteq G$, and that G/N is abelian. Consider the map

$$p_{G/N} : G \wr A \to G/N$$

defined by

$$p_{G/N}(\pi; g_1, \cdots, g_n) = g_1 g_2 \cdots g_n N \ .$$

Then $p_{G/N}$ *is* a surjective homomorphism. We remark that

$$g_1 \cdots g_n N = (g_1 N) \cdots (g_n N) \ ,$$

and as G/N is abelian, we get for each $\rho \in S_n$ that

$$g_1 N \cdots g_n N = g_{\rho(1)} N \cdots g_{\rho(n)} N = g_{\rho(1)} \cdots g_{\rho(n)} N \ .$$

Therefore

$$\begin{aligned} & p_{G/N}((\pi; g_1, \cdots, g_n)(\rho; h_1, \cdots, h_n)) \\ &= p_{G/N}(\pi\rho; g_{\rho(1)} h_1, \cdots, g_{\rho(n)} h_n) \\ &= g_{\rho(1)} h_1 \cdots g_{\rho(n)} h_n N \end{aligned}$$

$$= (g_1 \cdots g_n N)(h_1 \cdots h_n N) \quad \text{(see above)}$$
$$= p_{G/N}(\pi; g_1, \cdots, g_n) p_{G/N}(\rho; h_1, \cdots, h_n) \ .$$

(5B) Notation: Let H be a subgroup in the group G of finite index $|G : H| = n$. Let $T = \{g_1, \cdots, g_n\}$ be a transversal til H i G (See Chapter 2),

$$(*) \qquad G = \dot{\bigcup_{g_i \in T}} g_i H.$$

Let $x \in G$. By $(*)$ there exists for $1 \leq i \leq n$ a uniquely determined integer $\alpha_x^T(i) \in \{1, \cdots, n\}$, and a uniquely determined element $h_{xi}^T \in H$ such that

$$x g_i = g_{\alpha_x^T(i)} h_{xi}^T \ .$$

□

Let us try to replace T by another transversal $T' = \{g_1 \widetilde{h}_1, \cdots, g_n \widetilde{h}_n\}$ where $\widetilde{h}_i \in H$, and for $x \in G$ compare α_x^T with $\alpha_x^{T'}$, and h_{xi}^T with $h_{xi}^{T'}$. We have

(5C) Lemma: *In the above notation we have*

$$\alpha_x^T = \alpha_x^{T'} .$$

(Thus we put, independently of the choice of T,

$$\alpha_x^T = \alpha_x).$$

Moreover

$$h_{xi}^{T'} = \widetilde{h}_{\alpha_x(i)}^{-1} h_{xi}^T \widetilde{h}_i \ .$$

Proof: If $x g_i \in g_j H$ we also have that $x g_i \widetilde{h}_i \in g_j H$. Thus, by definition,

$$\alpha_x^T(i) = j = \alpha_x^{T'}(i) \ ,$$

ie. $\alpha_x^T = \alpha_x^{T'}$. As $x g_i = g_{\alpha_x(i)} h_{xi}^T$, we get

$$x(g_i \widetilde{h}_i) = g_{\alpha_x(i)} h_{xi}^T \widetilde{h}_i$$
$$= (g_{\alpha_x(i)} \widetilde{h}_{\alpha_x(i)})(\widetilde{h}_{\alpha_x(i)}^{-1} h_{xi}^T \widetilde{h}_i) \ ,$$

and thus

$$h_{xi}^{T'} = \widetilde{h}_{\alpha_x(i)}^{-1} h_{xi}^{T} \widetilde{h}_i \ .$$

□

(5D) Theorem *Let notation be as in (5B) and (5C). Then the map*

$$\alpha_{G/H} : x \to \alpha_x$$

is a homomorphism $G \to S_n$ (called the permutation repræsentationen of G on the cosets of H) *with kernel*

$$K = \bigcap_{g \in G} gHg^{-1} \ .$$

Proof: Let $x \in G$. We first show that $\alpha_x \in S_n$. It is clear that $\alpha_x : \{1, \cdots, n\} \to \{1, \cdots, n\}$ so we need only show that α_x is injective: If $\alpha_x(i) = j = \alpha_x(i')$ then $xg_i \in g_j H$ and $xg_{i'} \in g_j H$, so that

$$g_i^{-1} g_{i'} = (xg_i)^{-1}(xg_{i'}) \in H \ .$$

This means $g_i H = g_{i'} H$, ie. $i = i'$.

Let now $x, y \in G$. For $1 \leq i \leq n$ we have $yg_i \in g_{\alpha_y(i)} H$, so that $x(yg_i) \in xg_{\alpha_y(i)} H = g_{\alpha_x(\alpha_y(i))} H$. From this we get $\alpha_{xy} = \alpha_x \circ \alpha_y$.

Let $x \in G$. Then

$$\alpha_x = (1) \Leftrightarrow xg_i \in g_i H \ \ for \ \ 1 \leq i \leq n$$

$$\Leftrightarrow x \in g_i H g_i^{-1} \ \ for \ \ 1 \leq i \leq n$$

$$\Leftrightarrow x \in \bigcap_{i=1}^{n} g_i H g_i^{-1} = \bigcap_{g \in G} gHg^{-1} \ .$$

□

(5E) Corollary: *If the group G has a subgroup H of index $|G : H| = n$, then there exists a* normal *subgroup N of G, satisfying*

(i) $|G : N| \ | \ n!$

(ii) $N \subseteq H$.

Proof: As N we may use $\ker\alpha$, where α is as in (5D), since α induces an injective homomorphism from $G/\ker\alpha$ into S_n. Thsu $|G/\ker\alpha| = |G/N| \mid |S_n| = n!$ □

(5F) Example: Let $n \geq 5$. Then the alternating group A_n has no subgroup of index k, when $1 < k < n$. Otherwise the *simple* group A_n would contain a normal subgroup of index $\leq k\,!$ different from A_n, and this is not possible. In particular we see that A_{n-1} must be a maximal subgroup in A_n (of index n). □

(5H) Example: If G has a subgroup H of index 3, then G has also a *normal* subgroup of index 2 or 3. Either $H \trianglelefteq G$ or G has a normal subgroup N with $H \subseteq N$, $|G:N| = 3! = 6$. In that case $G/N \simeq S_3$ which has A_3 as a normal subgroup of index 2. Thus G also has a normal subgroup of index 2. □

(5I) Remark: If we choose $H = \{1\}$ in (5D), and G is finite then $\alpha_{G/H} = \alpha_G$ is a monomorphism $G \to S_{|G|}$, which is called the *regular representation of* G.

(5J) Theorem: *Let the notation be as in (5B) and (5C). By*

$$\mathcal{V}_T(x) = (\alpha_x; h^T_{x1}, \cdots, h^T_{xn})$$

is defined a monomorphism $\mathcal{V}_T : G \to H \wr S_n$.
Proof: Let $x, y \in G$. As $yg_i = g_{\alpha_y(i)} h^T_{yi}$ we get

$$(xy)g_i = x(yg_i) = (xg_{\alpha_y(i)})h^T_{yi} = (g_{\alpha_x(\alpha_y(i))} h^T_{x\alpha_y(i)})h^T_{yi}$$

such that

$$\mathcal{V}_T(xy) = (\alpha_x\alpha_y; h^T_{x\alpha_y(1)}h^T_{y1}, \cdots, h^T_{x\alpha_y(n)}h^T_{yn})$$
$$= (\alpha_x; h^T_{\alpha 1}, \cdots, h^T_{xn})(\alpha_y; h^T_{y1}, \cdots, h^T_{yn}) = \mathcal{V}_T(x)\mathcal{V}_T(y)\ .$$

If $x \in Ker(\mathcal{V}_T)$ then $xg_i = g_i 1$ for all i, ie. $x = 1$. □

(5K) Theorem: *Notation as above. Assume in addition that* $K \trianglelefteq H$ *such that* H/K *is abelian. Then*

$$Ver = p_{H/K} \circ \mathcal{V}_T$$

defines a homomorphism $G \to H/K$ *which is independent of the choice of* T. *It is called* Verlagerung *from* G *to* H/K.

Proof: $\mathcal{V}_T : G \to H \wr S_n$ and $p_{H/K} : H \wr S_n \to H/K$ are homomorphisms, whence Ver is also a homomorphism. If T' is another transversal it must be shown that $p_{H/K} \circ \mathcal{V}_T = p_{H/K} \circ \mathcal{V}_{T'}$. This follws easily from (5C). $\square$

We use the German term "Verlagerung" in these notes. In English textbooks it is often called "transfer".

6. Focal subgroups, Grün's Theorems, Z–groups

G6 - 2007-version

First a couple of general remarks. As usual $G' = [G, G]$ denotes the commutator subgroup of the group G.

(6A) Lemma: *Let H be a subgroup of G. We have*

$$G' \subseteq H \Leftrightarrow H \trianglelefteq G \text{ and } G/H \text{ abelsk} .$$

Proof: Exercise or Chapter 1.18 in GT3 □

(6B) Example: Let us consider the dihedral group D_{20} of order 40 (see (4B)). We write

$$D_{20} = \langle x, y \mid x^{20} = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle .$$

It is easy to see that D_{40}'s commutator group is $D'_{40} = \langle x^2 \rangle$, $|D'_{40}| = 10$. The commutator factor group D_{40}/D'_{40} is Klein's four group $\mathbb{Z}_2 \times \mathbb{Z}_2$. By (6A) the list of normal subgroups $N \triangleleft D_{20}$, with D_{20}/N abelian is as follows:

$$D_{20}, \langle x \rangle, \langle x^2, y \rangle, \langle x^2, xy \rangle, \langle x^2 \rangle .$$

In this list the 1., 3. and 4. group are dihedral groups and the other are cyclic. (Why?)

In this Chapter G is a *finite* group.

A *p–focal* subgroup in G is a p–Sylow group i G'. By (2F) the p–focal subgroups in G are exactly $P \cap G'$, $P \in Syl_p(G)$. In the above Example (6B) the 2-focal subgroup has order 2 and the 5-focal subgroup has order 5. The p–focal subgroups are important because they may under certain circumstances be described "locally" using certain "proper" subgroups in G. This is particularly important in the study of non-abelian simple groups. In such a group $G' = G$, and the p–focal subgroup are exactly the p-Sylow groups in G. Generally we have

(6C) Theorem: *Let $P \in Syl_p(G)$. Then $P/P \cap G'$ is an abelian p–group, and there exists a normal subgroup $K \trianglelefteq G$, such that*

$$G/K \simeq P/P \cap G' .$$

Proof: The factor group G/G' is abelian and contains therefore a p–complement ($= p'$–Hall subgroup) K/G'. As $G' \subseteq K$ we have $K \trianglelefteq G$, and G/K is abelian by (6A). As $|G : K|$ is a power of p we have $G = KP$, eg. by (2B). We get $G/K \simeq P/P \cap K$. It is clear that $P \cap G' \subseteq P \cap K$. As $|K : G'|$ is prime to p then a p–Sylow group for G' is also a p–Sylow group for K. Therefore (2F) shows that $P \cap G' = P \cap K$. Thus $G/K = KP/K \cong P/P \cap K = P/P \cap G'$, as desired. □

If $x, y \in G$ and $H \subseteq G$ is a subgroup we write $x \sim_H y$, if there exists a $h \in H$ so that $hxh^{-1} = y$, and we call x and y *conjugate* i H. It is clear that $\sim_H$ is an equivalence relation on the elements of G. When $x, y \in G$ then $[x, y] = xyx^{-1}y^{-1}$ is x and y's *commutator*. We have $G' = \langle [x, y] \mid x, y \in G \rangle$.

The next Theorem is very useful.

(6D) Theorem: (Generators for focal subgroups) *Let $P \in Syl_p(G)$. Then*

$$P \cap G' = \langle xy^{-1} \mid x, y \in P \ , \ x \sim_G y \rangle \ .$$

Proof D. Gorenstein: Finite groups, 7.3.3-7.3.4

Definition: Let $K \subseteq L \subseteq G$ be subgroups. We say that L *controls fusion in* K, if we have:

$$\forall \ a, b \in K : \quad a \sim_G b \Rightarrow a \sim_L b \ .$$

Here is a simple example of control of fusion:

(6E) Lemma: *If $P \in Syl_p(G)$ is abelian, then $N_G(P)$ controls fusion in P.*

Proof Assume that $a, b \in P, g \in G$ and $gag^{-1} = b$. We then have that $gC_G(a)g^{-1} = C_G(b)$. As P is abelian, we have $P \in Syl_p(C_G(a))$ and $P \in Syl_p(C_G(b))$. By the above we also have

$$gPg^{-1} \in Syl_p(gC_G(a)g^{-1}) = Syl_p(C_G(b)).$$

If we apply Sylows Theorem on the Sylow groups gPg^{-1} and P in $C_G(b)$, we see that there exists $c \in C_G(b)$, such that $gPg^{-1} = cPc^{-1}$. If we then put $n = c^{-1}g$ we see that $n \in N_G(P)$ and $nan^{-1} = b$. □

(6F) Theorem: *If $P \in Syl_p(G)$, and if $L \supseteq P$ controls fusion in P, then*

$$P \cap G' = P \cap L' \ .$$

Proof: By assumption

$$\forall \ x, y \in P : \quad x \sim_G y \Leftrightarrow x \sim_L y \ .$$

Thus by (6D) $P \cap G'$ and $P \cap L'$ have the same generators so that

$$P \cap G' = P \cap L' \ .$$

□

(6G) Corollary: *If $P \in Syl_p(G)$ is abelian then $P \cap G' = P \cap N_G(P)'$.*
Proof: Use (6E) and (6F). □

(6H) Example: Let us check what (6D) means for a 2–Sylow group in S_4 (and in S_5). By (4B)

$$P = \langle (1,2,3,4), (1,4)(2,3) \rangle \in Syl_2(S_4) \ .$$

P is a dihedral group and contains the following elements

$$P = \{(1), (1,2,3,4), (1,4,3,2), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,3), (2,4)\} \ .$$

Of these elements only the following are conjugate in S_4 (and in S_5!)

(i) $(1,2,3,4)$ and $(1,4,2,3) = (1,2,3,4)^{-1}$

(ii) $(1,2)(3,4)$ and $(1,3)(2,4)$ and $(1,4)(2,3)$

(iii) $(1,3)$ and $(2,4)$.

Let $P^* = P \cap (S_4)'$. From (i) and (iii) we get only $(1,3)(2,4)$ as generator in P^*. From (ii) we get $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$, since every element in (ii) is a product of the two other. Thus $P^* = \{(1), (1,3)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, Klein's four group. In S_5 we get the same result!

This example also shows that (6*G*) *is wrong when P is not abelian*: In S_4 there are three 2–Sylow groups, so that $|S_4 : N_{S_4}(P)| = 3$, ie. $N_{S_4}(P) = P$. Therefore

$$P \cap N_{S_4}(P)' = P' = \{(1), (1,3)(2,4)\} \neq P^* = P \cap S_4' \ .$$

Corollary (6G) may be generalized as follows:

(6I) Theorem: (Grün's Theorem) *Let $P \in Syl_p(G)$. We have*

$$P \cap G' = \langle P \cap N_G(P)' \ , \ P \cap g^{-1}P'g \mid g \in G \rangle \ .$$

Remarks: If P is abelian then $P' = \{1\}$ and thus $P \cap g^{-1}P'g = 1$ for all $g \in G$. Therefore $(6I)$ implies $(6G)$. We again have to consider Verlagerung into an abelian factor group of P, and need to choose coset representatives for P in G in a special way. You start by dividing G into *double cosets* modulo P so we need to add some facts about double cosets. This is done generally here.

If H, K are subgroups in G, $g \in G$ we call the subset

$$HgK = \{x \in G \mid \exists h \in H \ , \ k \in K : x = hgk\}$$

a double (H, K)–coset. The double cosets are equivalence classes for the following equivalence relation ${}_H\equiv_K$ on G:

$$g_H \equiv_K g_1 \Leftrightarrow \exists h \in H \ , \ k \in K : g = hg_1k \ .$$

Thus the (H, K) double cosets divide G into disjoint subsets. Contrary to a result on cosets we do *not* have that $|HgK| \ | \ |G|$. In fact

(6J) Theorem: *The double coset HgK is a union of $|H : H \cap gKg^{-1}|$ right cosets to K (and of $|K : K \cap g^{-1}Hg|$ left cosets to H). In particular*

$$|HgK| = |H : H \cap gKg^{-1} \mid \ |K| \ (= |K : K \cap g^{-1}Hg| \ |H|) \ .$$

Proof. Easy direct calculation. You may also prove the result by applying (2A) to the subgroups H and gKg^{-1} of G. □

When $u \in P$, $P \in Syl_p(G)$, $g^* \in G$ we give a description of some coset representatives in Pg^*P which are useful in the calculation of of $Ver(u)$.

(6K) Lemma: *Let $u \in P$, $P \in Syl_p(G)$, $g^* \in G$. There exists $g \in G$, $1 = a_0, a_1, \cdots, a_r \in P$, $t_0, t_1, \cdots, t_r \geq 0$, such that the following is fulfilled:*

(1) $Pg^*P = PgP$.

(2) $PgP = \bigcup_{i=0}^{r} \bigcup_{j=0}^{p^{t_i}-1} u^j a_i g P$.

(3) For all i we have $g^{-1}a_i^{-1}u^{p^{t_i}}a_i g \in P$

(4) For all i we have $g^{-1}u^{p^{t_i}}g \in P$.

(5) $\sum_{i=0}^{r} p^{t_i} = |P : P \cap gPg^{-1}|$.

Proof: Huppert: Endliche Gruppen I, IV.3.4, p. 423.

This is used to prove (6I).

Proof for (6I): Huppert: Endliche Gruppen I, IV.3.4, p. 423.

Let $P \in Syl_p(G)$. $Z(P)$ denotes as usual P's center. The group G is called *p–normal* if:

$$\forall g \in G : gZ(P)g^{-1} \subseteq P \Rightarrow gZ(P)g^{-1} = Z(P).$$

(For example G is p–normal, if P is abelian.)

The next result may be seen as a generalization of (6G) in another direction.

(6L) Theorem: (Grün's 2. Theorem) *Let G be p–normal. Let $P \in Syl_p(G)$ and $H = N_G(Z(P))$. Then $P \cap G' = P \cap H'$.*

Proof: Huppert: Endliche Gruppen I, IV.3.7, p. 425.

The next Theorem is one of the most useful applications of Verlagerung.

(6M) Theorem: (Burnside) *Let $P \in Syl_p(G)$. If $P \subseteq Z(N_G(P))$, then G has a normal p–complement K.*

Proof: We show that $P \cap G' = \{1\}$, and then the existence of K follows from (6C). Put $N = N_G(P)$. We have that $P \subseteq Z(N)$, and as $P \subseteq N = N_G(P)$ we see that P is abelian. Thus by (6G)

$$(**) \qquad P \cap G' = P \cap N' \ .$$

But $P \cap N'$ may be calculated by (6D). As $P \subseteq Z(N)$ we get for $x, y \in P$ that $x \sim_N y \Leftrightarrow x = y$. By (6D) $P \cap N' = \{1\}$, so that $(**)$ yields $P \cap G' = \{1\}$, as desired. □

In the following we need

(6N) Lemma: *If L is a subgroup of G, then $C_G(L) \trianglelefteq N_G(L)$, and the faktor group $N_G(L)/C_G(L)$ is isomorphic to a subgroup of $Aut(L)$.*
Proof: If $x \in N_G(L)$

$$\alpha_x : \ell \mapsto x\ell x^{-1}$$

defines an automorphism of L. The map $x \to \alpha_x$ is a homomorphism from $N_G(L)$ into $Aut(L)$ with $C_G(L)$ as kernel. □

(6P) Remark: If L is cyclic then $Aut(L)$ is abelian. If L is an elementary abelian p–group of order p^n then L may be considered as a vector space over the field $\mathbb{Z}_p$ with p elements, $dim L = n$. The homomorphismes from the group L to itself "correspond" then to linear maps of the vector space L. It follows that $Aut(L) \simeq GL(n, \mathbb{Z}_p)$, the set of invertible $n \times n$–matrices with coefficients from $\mathbb{Z}_p$.

(6Q) Theorem: *Let p be smallest prime dividing $|G|$. If $P \in Syl_p(G)$ is cyclic, then G has a normal p–complement. In particular a group with a cyclic 2–Sylow group always has a normal 2–complement.*
Proof: By (6N) $N_G(P)/C_G(P)$ is isomorphic to a subgroup of $Aut(P)$. But $Aut(P)$ is an abelian group of order $p^{n-1}(p-1)$, if $|P| = p^n$. (See eg. `GT3`, Chapter 1.13) As $p^n \mid |C_G(P)|$ (because P is abelian) we get $p \nmid |N_G(P) : C_G(P)|$. Now p is the smallest prime divisor of $|G|$, so that $((p-1), |G|) = ((p-1), |N_G(P)|) = 1$. We get that $|N_G(P) : C_G(P)| = 1$, ie. $N_G(P) = C_G(P)$. Thus $P \subseteq Z(N_G(P))$. Apply (6M). □

(6R) Theorem: *A simple group of order 60 is isomorphic to the alternating group A_5.*
Proof. Let G be simple, $|G| = 60$. Choose $P \in Syl_2(G)$, so that $|P| = 4$. Then $|G : N_G(P)| =: n_2(G)$ is the number of 2–Sylow groups in G. We have $n_2(G) | 15 = |G : P|$. By (5E) we have $n_2(G) \geq 5$, so that $n_2(G) \in \{5, 15\}$. If $n_2(G) = 15$, then $P = N_G(P)$ as $|N_G(P)| = \frac{60}{15} = 4$. By (6M) this is impossible. Thus $n_2(G) = |G : N_G(P)| = 5$, and the claim follows from (5E). □

(6S) Lemma: *If $G/Z(G)$ is cyclic, then G is abelian.* (See also `GT3`).
Proof: Exercise

You are reminded that $G^{(i)}$ is the i'th commutator group in G.

$$G^{(0)} = G;\ G^{(1)} = [G, G];\ G^{(i)} = [G^{(i-1)}, G^{(i-1)}]\ .$$

(GT3, Chapter 1.18)

We have $G^{(i)} char G$ for all i, by (1A)(2).

(6T) Theorem: *Assume that $i \geq 1$ and that the factor groups $G^{(i)}/G^{(i+1)}$ and $G^{(i+1)}/G^{(i+2)}$ are both cyclic. Then $G^{(i+1)} = G^{(i+2)}$.*

Proof: The assumptions are independent of what $G^{(0)}, \cdots, G^{(i-1)}$ are, or what $G^{(j)}$ is for $j \geq i+2$. We may therefore assume that $i = 1$, and that $G^{(i+2)} = G^{(3)} = \{1\}$. We then know that $G^{(2)}/G^{(3)} = G^{(2)} = \langle a \rangle$ is cyclic. As $G^{(2)} = G'' = \langle a \rangle \trianglelefteq G$, we have $N_G(\langle a \rangle) = G$. Let $X = C_G(a)$. By (6N) G/Z is isomorphic to a subgroup of $Aut(\langle a \rangle)$. Also $Aut(\langle a \rangle)$ is abelian ((6P)). Thus G/X is abelian. This means that $G' \subseteq X$. We then have

$$G'' = \langle a \rangle \subseteq G' \subseteq X = C_G(a) \ .$$

As $G' \subseteq C_G(a)$, we get $G'' = \langle a \rangle \subseteq Z(G')$. Thus, by an isomorphism theorem,

$$G'/Z(G') \simeq \left(G' \Big/ \langle a \rangle\right) \Big/ \left(Z(G')/\langle a \rangle\right) \ .$$

As $G'/\langle a \rangle = G'/G''$ is cyclic, we get that $G'/Z(G')$ is cyclic. By (6S) G' is abelian, so that $G^{(2)} = (G')' = \{1\}$. Thus $G^{(2)} = G^{(3)} (= \{1\})$, as desired. □

We can now give a description of the finite groups, where *all* Sylow groups are cyclic (for all primes). Such a group is called a *Z-group.* (Z is an abreviation for Zassenhaus. Hans Zassenhaus 1912–1991. (See also Chapter 3)).

(6U) Theorem: *A Z–group is solvable.*

Proof: Let G be a Z–group. The proof is by induction by $|G|$. Let p be the smallest prime divisor in $|G|$. By (6Q) G has a normalt p–complement K. Thus G/K is a (cyclic) p–group, ie. solvable, and K is solvable by the induction hypothesis (See also Theorem (2F), which shows that K is a Z–group). Thus G is solvable. □

(6V) Lemma: *An abelian Z–group is cyclic.*

Proof: Exercise

(6W) Theorem: *A Z–group G is a semidirect product*

$$G = A \rtimes B \ ,$$

where A and B are cyclic.

Proof: G is solvable by (6U). Consider the commutator series

$$G = G^{(0)} \supset G^{(1)} \supset \cdots \supset G^{(k)} = \{1\} \ .$$

The factor groups $G^{(i)}/G^{(i+1)}$ are abelian Z–groups, and thus cyclic by (6V). Then (6T) shows that $G^{(2)} = \{1\}$! We now have that G/G' and G' are cyclic. Let $|G'| = m$, $|G : G'| = n$, so that $|G| = mn$. Let $G' = \langle a \rangle$ and choose $b \in G$ with $G/G' = \langle bG' \rangle$. We have $G = \langle a, b \rangle$. As $\langle a \rangle \trianglelefteq G$, we get $b^{-1}ab = a^r$, where $\langle a^r \rangle = \langle a \rangle$ (so that $(r, m) = 1$). Furthermore

$$a^{-1}b^{-1}ab = a^{r-1} \ .$$

If $X = \langle a^{r-1} \rangle$ then $G/X = \langle aX, bX \rangle$. As $[a, b] \in X$, G/X is abelian, so that $G' \subseteq X$. Hence $G' = X = \langle a^{r-1} \rangle$. Since $|a| = |a^{r-1}|$, we have $(r - 1, m) = 1$. As $G/G' = \langle bG' \rangle$ has order n, we have $b^n \in G'$, say

$$b^n = a^s \ .$$

Then $b^n = b^{-1}b^n b = b^{-1}a^s b = (b^{-1}ab)^s = a^{rs}$, ie. $a^s = a^{rs}$. Therefore $|a| = m \mid (r - 1)s$. As $(m, r - 1) = 1$ we get $m|s$, and as $a^m = 1$ we get $a^s = 1$. Thus $\mathbf{b^n = a^s = 1}$ and $|b| = n$. We can now show $(m, n) = 1$: If $p|m$, $p|n$, p a prime and $m = m_1 p$, $n = n_1 p$, then a^{m_1} and b^{n_1} are elements of order p, and as $\langle a \rangle \cap \langle b \rangle = \{1\}$ we see that $\langle a^{m_1}, b^{n_1} \rangle$ is an abelian group of order p^2, which is not cyclic. This is impossible as G's p–Sylow groups are cyclic. Thus $(m, n) = 1$. □

We have shown that G is a semidirect product of $A = G' = \langle a \rangle$ and $B = \langle b \rangle$. Let us remark that as $(m, n) = 1$, A and B are *Hall subgroups in* G.

In the case where all Sylow groups have prime order there is a stronger statement than (6W):

(6X) Theorem: *Assume that $|G| = p_1 p_2 \cdots p_r$, where $p_1 < p_2 < \ldots < p_r$ are primes. Then*

$$G = A \rtimes B \ ,$$

where there exists an s, $1 \leq s \leq r$ such that

$$|B| = p_1 \cdots p_s \ , \quad |A| = p_{s+1} \cdots p_r \ .$$

7. Groups of a given finite order

G7- 2007-version

This chapter is essentially different from the other chapters. It is inspirered by the pages 203-215 in the book

D.S.Dummitt, R.S. Foote: Abstract algebra, Prentice-Hall 1991.

We illustrate methods to at study finite groups of a given order. You may for instance want to show that such a group cannot be simple.
We use Sylow's Theorems and results from the previous 2 Chapters. First we make a number of Remarks, which might be useful for this type of problems and then we illustrate the methods in a series of examples.

Remarks:

(I) If $P \in Syl_p(G)$, then the number $n_p(G) := |Syl_p(G)|$ of p–Sylow groups of G satisfies

$$n_p(G) = |G : N_G(P)| \quad and \quad n_p(G) \equiv 1 (mod\ p).$$

If G er simple and $p \mid |G|$, then $n_p(G) > 1$, unless G is cyclic of order p.

(This follows from Sylow's Theorem.)

(II) If $P \in Syl_p(G)$ has order p, then G has precisely $(p-1)n_p(G)$ elements of order p.

(We know that as $|P| = p$, none of the $n_p(G)$ p-Sylow groups can have elements $\neq 1$ in common. Each Sylow group contais $(p-1)$ elements $\neq 1$.

This counting argument does *not* work, if $|P| > p$, unless you can show the 2 arbitrary different subgroups $P, P^* \in Syl_p(G)$ satisfy $P \cap P^* = 1$. If this is the case we say that the Sylow groups are TI, ie. "Trivial Intersection." If the p-Sylow groups of G are TI then G contains $(|P|-1)n_p(G)$ elements $\neq 1$ of p-power order.)

(III) If you want to show that the Sylow groups in G are TI (eg. to count p-elements, see (II)), you may do this indirectly by considering a Sylow group intersection $R = P \cap P^* \neq 1$ of *maximal* order where P and

P^* are different. As p-groups are nilpotent (see Chapters 8-9) the subgroup R of P (or P^*) cannot be equal to its own normalizer in P (or P^*.) You then know that $N_G(R)$ *must contain at least* $(p+1)$ *p-Sylow groups*, since the p-subgroups $N_P(R)$ and $N_{P^*}(R)$ of $N_G(R)$ cannot be contained in the same p-Sylow group T of $N_G(R)$, due to the maximality of R. If they were and $T \subseteq U, U \in Syl_p(G)$, then $P = U = P^*$, as $|P \cap U| \geq |N_P(R)| > |R|$ and $|P^* \cap U| \geq |N_{P^*}(R)| > |R|$. Thus there is a chance that $N_G(R)$ may be a very large subgroup of G. See also Remark (XI).

(IV) If G is simple and p is the largest prime dividing $|G|$, then G has no subgroup U of index k, $1 < k < p$.

(If it did then G would have a normal subgroup N $N \subseteq U \subseteq G$, with G/N isomorphic to a subgroup of S_k. (Corollary (5E)) It is clear that $N = 1$. As $p \mid |G|$, but $p \nmid k!$, because $k < p$, we would get a contradiction.)

(V) We may generalize (IV) as follows: If G is a group, we define $s(G) := min\{t \in \mathbb{N} \mid |G| \mid t!\}$. Then we have: If G is simple then G has no subgroup of index k, when $1 < k < s(G)$.

(If it did then G would be isomorphic to a subgroup of S_k, as in (IV). In particular then $|G| \mid k!$, contradicting that $k < s(G)$.)

(VI) Remark (V) may also be improved a little: If G is simple of order ≥ 3 and has a subgroup of index k > 1, then every subgroup of G is isomorphic to a subgroup of the alternating A_k.

(We know that G is isomorphic to a subgroup H of S_k. But actually H must be a subgroup of A_k : If $H \not\subseteq A_k$ then $H \cap A_k$ has index 2 in H. But as H is simple (isomorphic to G) we have a contradiction.)

(VII) If p is an odd prime and $P \in Syl_p(A_k)$ then

$$|N_{A_k}(P)| = \frac{1}{2}|N_{S_k}(P)|.$$

(This follows easily from the Frattini argument in Chapter 1.)

(VIII) If p is an odd prime, $k = p$ eller $k = p + 1$ and $P \in Syl_p(A_k)$ then $|N_{A_k}(P)| = \frac{1}{2}p(p-1)$.

(It is not difficult to see that *in these cases for k* we have $|N_{S_k}(P)| = p(p-1)$. (Exercise.) Then use (VII).)

(IX) Assume that $p < q$ are primes, such that $p \nmid (q-1)$. (We then know that every group of order pq is cyclic). Assume that $P \in Syl_p(G)$ and $Q \in Syl_q(G)$ are both cyclic *of order p and q respectively.* Then

$$p \mid |N_G(Q)| \Leftrightarrow q \mid |N_G(P)|.$$

(If $p \mid |N_G(Q)|$, then $N_G(Q)$ contains a subgroup P^* of order p. Then P^*Q is a subgroup of order pq in G, which then is cyclic. Therefore Q and P^* centralizes each other so that $Q \subseteq C_G(P^*) \subseteq N_G(P^*)$. As P and P^* are conjugate in G, then also $N_G(P)$ and $N_G(P^*)$ are conjugate. We get $q \mid |N_G(P)|$. The other direction is proved analogously.)

(X) You may also 'play primes against each other' in other situations than the one in (IX). Assume that P is a p-subgroup and at the prime q is a divisor in $|N_G(P)|$. You may then look at the number of q-Sylow groups in $N_G(P)$ applying for example (I). If it turns out that $n_q(N_G(P)) = 1$, then $N_G(P) \subseteq N_G(Q)$, where $Q \in Syl_q(N_G(P))$. There my be other subgroups in $N_G(Q)$, eg. if $Q \notin Syl_q(G)$, which may make this subgroup very large. Then you may apply for example (IV)-(VI).

(XI) Assume that $n_p(G) \not\equiv 1(mod\, p^2)$. Then there exist p-Sylow groups P, P^* in G, such that $R = P \cap P^*$ has index p in P and in P^*. In particular then $N_G(R)$ contains at least $(p+1)$ p-Sylow groups.

(This is seen as follows: Choose $P \in Syl_p(G)$. Consider for $P^* \in Syl_p(G)$ the set $\{P^{*x} | x \in P\}$, ie. the set of P-conjugate subgroups to P^*. If $x \in P$ and $P^{*x} = P^*$, then $< P^*, x >= P^* < x >$ is a p-subgroup in G. As P^* is a Sylow group, we have $x \in P^*$, ie. $x \in P \cap P^*$. Therefore the set $\{P^{*x} | x \in P\}$ contains exactly $|P : P \cap P^*|$ Sylow groups. The assumption $n_p(G) \not\equiv 1(mod\ p^2)$ shows then that there exists a p-Sylow group $P^* \neq P$, such that $p^2 \nmid |P : P \cap P^*|$. In that case we put $R = P \cap P^*$. As p-groups are nilpotent (see Chapters 8-9) the subgroup R of P (respectivelt P^*) not be its own normalizer in P (respectively P^*.) Therefore $P, P^* \subseteq N_G(R)$.)

And here are the Examples:

Example 1: *A group G of order $132 = 2^2 \cdot 3 \cdot 11$ is not simple.*

Proof: If you want to make the assumption that G is simple lead to a contradiction, you may here 'count elements'. It is usually good to start with the largest prime. Remark that if G is simple, then $n_p(G) \neq 1$ for $p = 2, 3, 11$. As $n_{11}(G) \mid 12$, we egt $n_1 1(G) = 12$, so G has $12 \cdot 10 = \mathbf{120}$ elements of order 11 by (I). As $n_3(G) \geq 4$, G has at least $4 \cdot 2 = \mathbf{8}$ element´s of order 3 by (I). In total you have at least **128** elements of order 11 and 3 in G. Only 4 elements remains. Among these 4 elements must be all elements in all 2-Sylow groups in G. We get $n_2(G) = 1$, a contradiction . □

Example 2: *A group G of order $p^2 \cdot q$, where p and q are primes, is not simple: Either a p-Sylow group or a q-Sylow group is normal in G.*

Proof: Assume that $n_p(G) > 1$, ie. that a p-Sylow group P is not normal. We get $n_p(G) = q$, so that $|N_G(P)| = p^2$. This shows that $N_G(P) = P$, and as P is abelian (as any group of prime square order is), we get $P \subseteq Z(N_G(P))$. Theorem (6M) shows that G har et *normalt* p-complement, which then must have order q.
Alternatively you may by elementary number theoretic considerations show that vise, at $n_p(G) > 1 \Rightarrow n_q(G) = 1$. □

Example 3: *A group G of order $3393 = 3^2 \cdot 13 \cdot 29$ is not simple.*

Proof: This and the next 2 examples use 'subgroups of small index'. If G is simple, G cannot contain a subgroup U of index $1 < k < 29$, by (IV). But $n_3(G) = 13$, as all other divisors $\neq 1$ of $13 \cdot 31$ are not congruent to 1 (mod 3). Thus the 3-Sylow-normalizer must have index 13, by (I), contradiction. The idea in this example may often be used. □

Example 4: *A group G of order $396 = 2^2 \cdot 3^2 \cdot 11$ is not simple.*

Proof: Assume G simple. As 12 is the only divisor > 1 of $2^2 \cdot 3^2$, which is congruent to 1 modulo 11, we have $n_{11}(G) = 12$. G and its subgroups are thus isomorphic to subgroups of A_{12}, by (IV). If $P \in Syl_{11}(G)$, we have $|N_G(P)| = 33 = 3 \cdot 11$. But A_{12} (or even S_{12}) has no subgroup of order 33. Such a subgroup had to be cyclic, as any group of order 33 er cyclic. An element of order 33 in a symmetric group needs at least 11+3=14 elements to operate on. Here we could alternatively use (VIII). □

Example 5: *A group G of order $224 = 2^5 \cdot 7$ is not simple.*

Proof: Assume G simple. We get $n_2(G) = 7$, so that G is isomorphic to a subgroup of A_7, by (VI). But $2^5 \nmid |A_7|$. $\square$

Example 6: *A group G of order $4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$ is not simple.*

Proof: Assume G simple. By (I) we have $n_7(G) = 15$ and $n_{13}(G) = 105 = 3 \cdot 5 \cdot 7$. If $P \in Syl_7(G)$ and $Q \in Syl_{13}(G)$ we get $|N_G(P)| = 4095/15 = 3 \cdot 7 \cdot 13$ and $|N_G(Q)| = 4095/105 = 3 \cdot 13$. This contradicts (IX). $\square$

Example 7: *A group G of order $351 = 3^4 \cdot 13$ is not simple.*

Proof: Assume G simple. Let $P \in Syl_3(G)$. We have that $n_3(G) = 13$ by (I), so that $n_3(G) \not\equiv 1 \pmod{3^2}$. By (XI) there exists $P^* \in Syl_3(G)$, so that $R = P \cap P^*$ has order 3^3. Let $X = N_G(R)$. Then X contains at least 2 3-Sylow groups, namely P and P^*. Thus $|P|$ is a proper divisor of $|X|$, since otherwise $P = X$. We get $X = G$, so that $R \lhd G$, a contradiction. $\square$

Example 8: *A group G of order $2205 = 3^2 \cdot 5 \cdot 7^2$ is not simple.*

Proof: Assume G simple. We get $n_7(G) = 15 \not\equiv 1 \pmod{7^2}$. Choose by (XI) $P, P^* \in Syl_7(G)$, so that $R = P \cap P^*$ has order 7. Thus we have for $X = N_G(R)$ that $n_7(X) > 1$. As $n_7(X) \mid 45 = |G : P|$, we get $n_7(X) = n_7(G) = 15$. Thus X contains *all* 7-Sylow groups from G. As G is generated by these we get $X = G$, a contradiction. $\square$

8. The Frattini subgroup. Nilpotent groups. The Fitting subgroup

G8 - 2007-version

Let G be a group. The subgroup $M \subseteq G$, $M \neq G$, is called *maximal* in G, if there is *no* subgroup K satisfying $M \subset K \subset G$. $Max(G)$ denotes the set of maximal subgroup in G. If $G \neq \{1\}$ is a finite group, then $Max(G) \neq \varnothing$, and we put

$$\Phi(G) = \bigcap_{M \in Max(G)} M.$$

We call $\Phi(G)$ *The Frattini(sub)group* in G. If $M \in Max(G)$ and $\alpha \in Aut(G)$, then also $\alpha(M) \in Max(G)$. Thus $\Phi(G)$ *char* G and in particular $\Phi(G) \trianglelefteq G$. If $G = \{1\}$ we put $\Phi(G) = \{1\}$.

It turns out that $\Phi(G)$ has a connection with "*non-generators*" for G:

If $X \subseteq G$, then as in Chapter 1 $\langle X \rangle$ is the subgroup of G generated by X, ie. the *smallest* subgroup i G, containing X. If $\langle X \rangle = G$, we call X a *generating set* for G.

Consider elements $g \in G$ satisfying:

$$\forall \ X \subseteq G \ : \ \langle X, g \rangle = G \Rightarrow \langle X \rangle = G \ .$$

Such elements are called *non-generators,* becuse they are *superfluous* in all generating sets for G.

Let $I(G) = \{g \in G \mid g \ \ is\ non-generator\}$.

(8A) Theorem: *Let G be a finit group. Then*

$$\Phi(G) = I(G) \ .$$

Remark: This Theorem also holds when G is infinite.

Proof: ...

(8B) Theorem: *Let G be a finite group. Let $P \in Syl_p(\Phi(G))$. Then $P \trianglelefteq G$.*

Proof: We apply the Frattini argument (1E) on $\Phi(G) \trianglelefteq G$ and get

$$G = \Phi(G) \cdot N_G(P) \ .$$

Using (8A) we see

$$G = \langle \Phi(G), N_G(P) \rangle = \langle I(G), N_G(P) \rangle = \langle N_G(P) \rangle = N_G(P) \ ,$$

ie. $P \trianglelefteq G$. □

Remark: This shows that when G is finite then all Sylow groups in the group $\Phi(G)$ are normal in G and therefore also in $\Phi(G)$. This actually means that $\Phi(G)$ is an (inner) direct product of its Sylow groups (ie. a finite *nilpotent* group, see Theorem (8J)).

We give in the following a description of nilpotent groups. Here the group G is not necessarily finite.

When H and K are subsets of G, then

$$[H, K] = \langle [h, k] \mid h \in H \ , \ k \in K \rangle$$

is the subgroup of G generated by all commutators of elements from H and K. As usual $Z(G)$ is the center of the group G.

It is easily seen that

$$H \ char \ G \ \ , \ \ K \ char \ G \Rightarrow [H, K] \ \ char \ G$$

because the automorphisms of G then "mix" the generators for $[H, K]$, see Chapter 1.

(8C) Lemma: *Let $K \trianglelefteq G$ and $K \subseteq H \subseteq G$. Then*

$$[H, G] \subseteq K \Leftrightarrow H/K \subseteq Z(G/K) \ .$$

Proof: We have

$$[H, G] \subseteq K \Leftrightarrow \forall h \in H \ \forall g \in G : [h, g] \in K$$

$$\Leftrightarrow \forall \overline{h} \in H/K \ , \ \forall \overline{g} \in G/K : [\overline{h}, \overline{g}] = \overline{1}$$

$$\Leftrightarrow H/K \subseteq Z(G/K) \ .$$

□

(8D) Lemma: *Let $\varphi : G \to H$ be a surjective homomorphism. Then*

$$\varphi(Z(G)) \subseteq Z(H) \ .$$

Proof: Let $a \in Z(G)$, $h \in H$. We show that $[\varphi(a), h] = 1$. As φ is surjektive there exists a $g \in G$ such that $\varphi(g) = h$. Then $[a, g] = 1$, as $a \in Z(G)$ and thus

$$1 = \varphi([a, g]) = [\varphi(a), \varphi(g)] = [\varphi(a), h] \ .$$

□

In connection with the definitione of nilpotent group *central series* are important.

Definition: We definere two series of subgroups of an arbitrary group G: The *lower central series* for G

$$G = L_1(G) \supseteq L_2(G) \supseteq \cdots \supseteq L_c(G) \supseteq \cdots$$

is defined by

$$L_1(G) = G \ , \ L_i(G) = [L_{i-1}(G), G] \quad for \ \ i \geq 2 \ .$$

the *upper central series* for G

$$\{1\} = Z^0(G) \subseteq Z^1(G) \subseteq \cdots \subseteq Z^c(G) \subseteq \cdots$$

is defined by

$$Z^0(G) = \{1\} \ , \ Z^i(G)/Z^{i-1}(G) = Z\left(G/Z^{i-1}(G)\right) \ \ for \ \ i \geq 2 \ .$$

(In particular $Z^1(G) = Z(G)$.)

(8E) Examples: (1) Let $G = S_4$. We have $Z(G) = \{1\}$, and thus $Z^0(G) = Z^1(G) = Z^2(G) = \cdots = \{1\}$. We have that $G' = A_4$. Furthermore $[G', G] = [A_4, S_4] = A_4$, since for example $[(1,2,3),(1,3,2,4)] = (1,2,4)$ and $[(1,2,3),(2,3,4)] = (1,4)(2,3)$ generate A_4. Therefore

$$L_1(G) = S_4 \ , \ L_2(G) = L_3(G) = \cdots = A_4 \ .$$

(2) Let $G = D_8$, a dihedral group of order 16.

$$G = \langle x, y \mid x^8 = y^2 = 1 \, , \ y^{-1}xy = x^{-1} \rangle \ .$$

Here we have $Z(G) = \langle x^4 \rangle$ and that $G/Z(G) \cong D_4$. The group D_4 has also et center of order 2, so we get

$$Z(G/\langle x^4 \rangle) = \langle x^2 \rangle / \langle x^4 \rangle \ .$$

Now $G/\langle x^2\rangle$ is a four group. We get

$$Z^0(G) = \{1\}\ ,\ Z^1(G) = \langle x^4\rangle\ ,\ Z^2(G) = \langle x^2\rangle$$

$$Z^i(G) = G \quad for \quad i \geq 3.$$

Furthermore $G' = \langle x^2\rangle$ (as we have seen earlier). Now $[G', G] = \langle [x^2, y]\rangle = \langle x^4\rangle$ and $[\langle x^4\rangle, G] = 1$, da $x^4 \in Z(G)$. We get

$$L_1(G) = G\ ,\ L_2(G) = \langle x^2\rangle\ ,\ L_3(G) = \langle x^4\rangle$$

$$L_i(G) = \{1\} \quad for \quad i \geq 4\ .$$

The first example shows that den lower (respectively upper) central series need not finish in $\{1\}$ (respectively G). In the second example we had $Z^2(G) = G$ and $L_3(G) = \{1\}$. The connection is explained here:

(8F) Theorem: *For any group G and any $m \geq 0$ we have*

$$Z^m(G) = G \Leftrightarrow L_{m+1}(G) = \{1\}\ .$$

Furthermore in this case we have

$$(*) \quad L_{i+1}(G) \subseteqq Z^{m-i}(G) \quad for \quad alle\ i$$

Proof: ...

Definition: A group G is called *nilpotent* if there exists an $m \geq 0$ such that $Z^m(G) = G$. The smallest integer m with $Z^m(G) = G$ is called the *nilpotency class* of G. We then say that G is *nilpotent of class m*.

Remark: $G = \{1\}$ is nilpotent of class 0. A group $G \neq \{1\}$ is nilpotent of class 1, if and only if it is abelian. A non-abelian group G is nilpotent of klasse 2 if and only if $G' \subseteq Z(G)$. (Why?)

(8F) Theorem: *Assume that G is nilpotent.*

(1) Any subgroup of G is nilpotent.

(2) If $N \trianglelefteq G$, then G/N is nilpotent.

Proof: (1) Let $U \subseteq G$ be subgroup. From the definition we get easily

$$L_i(U) \subseteq L_i(G) \quad for\ all\ \ i \geq 1$$

(use induction on i). As G is nilpotent, we get $L_m(G) = 1$ for some $m \geq 1$. Then also $L_m(U) = \{1\}$.

(2) It is easily seen from the definition that

$$L_i(G/N) = L_i(G)N/N \quad for\ all\ \ i \geq 1\ .$$

Thus if $L_m(G) = 1$, then also $L_m(G/N) = 1$, and thus G/N is nilpotent. □

(8G) Remark: If $G = S_3$, $N = A_3$, then both G/N and N are abelian (and thus nilpotent), but G is *not* nilpotent. ($L_n(G) = A_3$ for $n \geq 2$.) Thus *the group S_3 is solvable, but not nilpotent.*

(8H) Theorem: *Assume that G is nilpotent, and that $H \subset G$ is a subgroup $\neq G$. Then $H \neq N_G(H)$.*

Proof: Assume that $L_m(G) = \{1\}$. As $L_1(G) = G$ and $H \neq G$, there exists an i, $1 \leq i \leq m-1$ such that $L_{i+1}(G) \subseteq H$, but $L_i(G) \nsubseteq H$. Then

$$[L_i(G), H] \subseteq [L_i(G), G] = L_{i+1}(G) \subseteq H\ .$$

But the inclusion $[L_i(G), H] \subseteq H$ means that $L_i(G) \subseteq N_G(H)$. (Why?) As $L_i(G) \nsubseteq H$, we get $N_G(H) \neq H$. □

(8I) Theorem: *If G and H are nilpotent, then also $G \times H$ is nilpotent.*

Proof: Show by induction that

$$L_i(G \times H) \subseteq L_i(G) \times L_i(H) \quad for\ \ i \geq 1.$$

□

Remark: *A finite p-group is nilpotent.* This follows from the fact that any finite p-group $\neq \{1\}$ has a center $\neq \{1\}$. (See Theorem (9D) below or Chapter 1.11 in `GT3`).

(8J) Theorem: *For a finite group G the following conditions are equvivalent:*

(1) G is nilpotent.

(2) For all subgroups $H \neq G$ we have $N_G(H) \neq H$.

(3) For alle primes p G has a normal p-Sylow group.

(4) G er et direct product of its Sylow groups.

Proof:(1) $\Rightarrow$ (2). Use (8H).

(2) $\Rightarrow$ (3). Let $P \in Syl_p(G)$. Put $H = N_G(P)$. By (1F) we have $H = N_G(H)$, so that from the assumption (2) we get $H = G$, ie. $P \trianglelefteq G$.

(3) $\Rightarrow$ (4). If $p \neq q$ are primes and $P \in Syl_p(G)$, $Q \in Syl_q(G)$, then $[P, Q] \subseteq P \cap Q = \{1\}$, as $P \trianglelefteq G$, $Q \trianglelefteq G$. Thus the elements in P and Q are permutable. As every element may in a unique way be written as a product of permutable elements of prime power order (see Remark below), we get (4).

(4) $\Rightarrow$ (1) follows from the Remark above and (8I). □

Remark: Assume that $g \in G$, $|g| = mn$ where $(m, n) = 1$. Write $1 = km+\ell n$, where $k, \ell \in \mathbb{Z}$. Then $g = g^{km} \cdot g^{\ell n}$, where g^{km} has order n and $g^{\ell n}$ has order m. If $g = xy$, $|x| = n$, $|y| = m$ and $xy = yx$, then $g^{km} = x^{km}y^{km} = x^{km}$, since $y^{km} = (y^m)^k = 1$. Thus $g^{km}x^{-1} = x^{km-1} = x^{-\ell n} = (x^n)^{-\ell} = 1$, as $x^n = 1$. We get $g^{km}x^{-1} = 1$ or $x = g^{km}$. Analogously we see that $y = g^{\ell n}$. (See also Chapter 1.15 in `GT3`.)

We return to the Frattini group $\Phi(G)$ of a group. From (8B) and (8J) we get

(8K) Theorem: *Let G be finite. Then $\Phi(G)$ is a nilpotent and characteristic subgroup of G.* □

Finally we consider the *Fitting subgroup* of a finite group G. In the rest of this Chapter we thus consider only *finite groups*.

(8L) Lemma: *Assume that H and K are normal nilpotent subgroups of the group G. Then also HK is a normal nilpotent subgroup of G.*

Proof: It is clear that $HK \trianglelefteq G$. Let p be a prime, $P_1 \in Syl_p(H)$, $P_2 \in Syl_p(K)$. By (8J) er $P_1 \trianglelefteq H$, so that by one of the Remarks in (1C) $P_1 char H$. We get $P_1 char H \trianglelefteq HK$, so that $P_1 \trianglelefteq HK$. Analogously $P_2 \trianglelefteq HK$ so that $P_1P_2 \trianglelefteq HK$. It is easily seen that $P_1P_2 \in Syl_p(HK)$. Thus in HK all Sylow groups are normal, so that HK is nilpotent by (8J). □

(8M) Theorem: *Let*

$$F(G) = \langle H \mid H \trianglelefteq G\,,\ H \ \ nilpotent \rangle\ .$$

Then $F(G)$ is a characteristic nilpotent subgroup of G, containing all nilpotent normal subgroups of G. $F(G)$ is called the Fitting group *of G.*

Proof: If $H \trianglelefteq G$ is nilpotent and $\alpha \in Aut(G)$, then $\alpha(H) \trianglelefteq G$ and $\alpha(H) \simeq H$ is nilpotent. Therefore $F(G)$ *char* G, by (1C). That $F(G)$ is nilpotent is easily seen from (8L). □

The next Theorem may look rather technical, but it is useful in various connections:

(8N) Theorem: *Let $M \in Max(G)$. Put $L = \bigcap_{x \in G} xMx^{-1}$, so that L is the largest normal subgroup of G contained in M. Put $\overline{G} = G/L$, and let $\overline{F} = F(\overline{G})$.*

If $\overline{F} \neq \overline{1}$, then the following holds:

(1) $\overline{F}$ is a minimal normal subgroup in $\overline{G}$.

(2) $\overline{F}$ is an elementary abelian p-group.

(3) $C_{\overline{G}}(\overline{F}) = \overline{F}$.

(4) $\overline{F} \cap \overline{M} = 1$ (where $\overline{M} = M/L$).

(5) $|G : M| = p^n$ for a suitable n.

Proof: We assume that $\overline{F} \neq \overline{1}$, such that $\overline{F}$ is a normal nilpotent subgroup $\neq \overline{1}$ in $\overline{G}$. Therefore also $Z(\overline{F}) \neq \{\overline{1}\}$. Let $p \mid |Z(\overline{F})|$ and put $\overline{P} = \{\overline{x} \in Z(\overline{F}) \mid \overline{x}^p = \overline{1}\}$. We have $\overline{P}$ *char* $Z(\overline{F})$ as the elements in $\overline{P}$ are permuted by automorphisms of $Z(\overline{F})$. $\overline{P}$ is abelian as $\overline{P} \subseteq Z(\overline{F})$, and therefore it is an elementary abelian p-group. We get $\{\overline{1}\} \neq \overline{P}$ *char* $Z(\overline{F})$ *char* $\overline{F} = F(\overline{G})$ *char* $\overline{G}$. As $\overline{P} \trianglelefteq \overline{G}$, $\overline{P}\,\overline{M}$ is a subgroup of $\overline{G}$ containing $\overline{M} \in Max(\overline{G})$.

But $\overline{P} \not\subseteq \overline{M}$: If $\overline{P} \subseteqq \overline{M}$, then $\overline{P}$'s inverse image in G (called P) is a normal subgroup in G, contained in M. As L is the largest normal subgroup in G contained in M we get $P \subseteq L$, and thus $\overline{P} = P/L = \{\overline{1}\}$, a contradiction. As $\overline{P} \not\subseteq \overline{M}$ and $\overline{M}$ is maximal in G we get $\overline{G} = \overline{P}\,\overline{M}$. Then we get (5) using (2A).

Put $\overline{C} := C_{\overline{G}}(\overline{P})$. As $\overline{P} \subseteq Z(\overline{F})$ we get $\overline{F} \subseteq \overline{C}$. As $\overline{P} \trianglelefteq \overline{G}$ we get $\overline{C} \trianglelefteq \overline{G}$ so that $\overline{C} \cap \overline{M} \trianglelefteq \overline{M}$. As $\overline{P}$ centralizes $\overline{C}$, and therefore also $\overline{C} \cap \overline{M}$, we have $\overline{P} \subseteq N_{\overline{G}}(\overline{C} \cap \overline{M})$. We get $\overline{C} \cap \overline{M} \trianglelefteq \overline{G}$ as $\overline{G} = \overline{P}\,\overline{M}$. In inverse image of $\overline{C} \cap \overline{M}$ in G is a normal subgroup of G, contined in M. As before we get $\overline{C} \cap \overline{M} = \{\overline{1}\}$. But $\overline{P} \subseteq \overline{F} \subseteq \overline{C}$, and as $\overline{P}\,\overline{M} = \overline{G}$, we get $\overline{P}\,\overline{M} = \overline{F}\,\overline{M} = \overline{C}\,\overline{M} = \overline{G}$.

As $\overline{P} \cap \overline{M} \subseteq \overline{F} \cap \overline{M} \subseteqq \overline{C} \cap \overline{M} = \{\overline{1}\}$ we get from (2A), that $|\overline{P}| = |\overline{F}| = |\overline{C}| = |\overline{G} : \overline{M}|$! Thus $\overline{P} = \overline{F} = \overline{C}$. As $\overline{P}$ is elementary abelian and $\overline{F} = \overline{C}$ we get (1) and (2). As $\overline{C} = \overline{F}$ we get (3) and (4). □

(8O) Corollary: *If G is a solvable group and $M \in Max(M)$, then $|G : M|$ is a prime power.*

Proof: Let $L = \bigcap_{x \in G} xMx^{-1}$ be as in (8N). As G is solvable, $\overline{G} = G/L$ is also solvable. Therefore $F(\overline{G}) \neq \{1\}$, since for example a minimal normal subgroup in $\overline{G}$ is abelian and therefore nilpotent (see (1D)). Thus (1)–(5) in (8N) holds in this situation. By (5) $|G : M|$ is a prime power. □

The technical Theorem (8N) plays also a rôle in the following interesting result describing connections between the Frattini group and the Fitting group in a finite group:

(8P) Theorem: *Let G be finite. Put $\Phi = \Phi(G)$, $F = F(G)$. We have*

(1) $[F, F] \subseteq \Phi \subseteq F$.

(2) $F/\Phi = F(G/\Phi)$.

Proof: As $\Phi \trianglelefteq G$ and Φ is nilpotent ((8K)) we get that $\Phi \subseteq F$. To show that $[F, F] \subseteq \Phi$ we choose $M \in Max(G)$, and put $L = \bigcap_{x \in G} xMx^{-1}$ as in (8N). Since $xMx^{-1} \in Max(G)$ for all $x \in G$, we must have $\Phi \subseteq L$ by definition of Φ. Put $\overline{G} = G/L$ and $F(\overline{G}) = K/L$, where then $K \trianglelefteq G$ is the invere image of $F(\overline{G})$ in G.

We have $F \subseteq K$: By an isomorphism Theorem $F/F \cap L \cong FL/L$. Therefore FL/L is a normal nilpotent subgroup in $\overline{G}$, as $F/F \cap L$ is nilpotent by (8F) (2). We get that $FL/L \subseteq K/L$, ie. $F \subseteq K$. By (8N) K/L is abelian (also if $F(\overline{G}) = 1$, ie. $K = L$!) As $FL/L \subseteq K/L$ FL/L is abelian; therefore $[F, F] \subseteq [FL, FL] \subseteqq L$, (see (6A)).

This holds for all intersections L of conjugate maximal subgroups. Let $M_1, M_2, \cdots, M_t$ be a set of representatives for the G-conjugacy classes of maximal subgroups. Put $L_i = \bigcap_{x \in G} xM_ix^{-1}$. Then $\Phi = L_1 \cap L_2 \cap \cdots \cap L_t$. By the above $[F, F] \subseteq L_i$ for all i. We get $[F, F] \subseteq \Phi$. Thus (1) is proved.

We put $\widetilde{G} = G/\Phi$ and $F(\widetilde{G}) = H/\Phi$, where H is the inverse image of $F(\widetilde{G})$ in G. Then $F \subseteq H$ because F/Φ (by (8F)(2)) is a nilpotent normal subgroup in $G/\Phi = \widetilde{G}$, ie. $F/\Phi \subseteq H/\Phi$. To show the inclusion $H \subseteqq F$ we show that H is nilpotent. Let $P \in Syl_p(H)$. Then $P\Phi/\Phi \in Syl_p(\widetilde{G})$, and

therefore $P\Phi/\Phi \trianglelefteq G/\Phi$ by (8J), ie. $P\Phi \trianglelefteq G$. As $\Phi \subseteq H$ and $P \in Syl_p(H)$, we get $P \in Syl_p(P\Phi)$. By the Frattini argument (1E) we get $G = P\Phi N_G(P) = \Phi P N_G(P) = \Phi N_G(P) = N_G(P)$, as Φ consists of "non-generators", (8A). Therefore $P \trianglelefteq G$, and in particular $P \trianglelefteq H$. We get that H is nilpotent by (8F), as desired. □

Our last result in this chapter is about solvable groups:

(8Q) Theorem: *Let G be finite and solvable. Then*

$$C_G(F(G)) \subseteq F(G) .$$

Proof: Put $F := F(G)$, $C := C_G(F)$. Assume that $C \not\subseteq F$. We seek a contradiction. We have that $Z(F) = C \cap F \subset C$. Choose a normal series for G, including the groups C and $C \cap F$ with (elementary) abelian factors (see (1D)),

$$\{1\} = G_t \subset G_{t-1} \subset \cdots \subset G_{s+1} = C \cap F \subset \cdots \subset G_r = C \subseteq \cdots \subseteq G_1 = G .$$

As $F \neq 1$ is nilpotent we have $G_{s+1} = C \cap F = Z(F) \neq \{1\}$. Therefore $G_s \neq G_{s+1}$. (Remark that $s + 1 > 1$ since otherwisw $G_{s+1} = G$, a contradiction). As G_s/G_{s+1} is abelian we have $[G_s, G_s] \subseteq G_{s+1} = Z(F)$. Since furthermore $G_s \subseteq G_r = C = C_G(F)$ we get

$$[[G_s, G_s], G_s] \subseteqq [Z(F), C_G(F)] = \{1\} .$$

Thus G_s is *nilpotent*, ie. $G_s \subseteq F = F(G)$. We get $G_s \subseteq C \cap F$ (as $G_s \subseteq G_r = C$), a contradiction. □

9. Finite p–groups

G9 - 2007-version

In this chapter we consider (better late that never) *finite* groups of p-power order, ie. p-groups.

(9A) Theorem: *Let P be a p-group, $\{1\} \neq N \trianglelefteq P$. Then $N \cap Z(P) \neq \{1\}$. In particular $Z(P) \neq \{1\}$.*

Proof: As $N \trianglelefteq P$, N is a union of conjugacy classes in P. Let $\{1\} = K_1, K_2, \cdots, K_r$ be the P–conjugacy classes contained in N. If $x_i \in K_i$, then $|K_i| = |P : C_P(x_i)|$. We know that

$$(*) \quad |N| = |K_1| + |K_2| + \cdots + |K_r| = 1 + |K_2| + \cdots + |K_r| \ .$$

If we for all $2 \leq i \leq r$ have $C_P(x_i) \neq P$, then $p| \ |K_i| = |P : C_P(x_i)|$ for all i, $2 \leq i \leq r$. This means by $(*)$, that $p \mid \ |N| - 1$. As $p \mid \ |N|$, because $N \neq 1$, this is a contradiction. Thus there is an $i \neq 1$ with $C_P(x_i) = P$. Then $x_i \in N \cap Z(P)$ and $x_i \neq 1$. □

(9B) Corollary: *If $N \trianglelefteq P$ and $|N| = p$, then $N \subseteq Z(P)$.* □

(9C) Corollary:

(1) If $|P| = p^2$, then P is abelian.

(2) If P is non–abelian then $p^2 \mid \ |P : Z(P)|$.

Proof: (1) By (9A) $Z(P) \neq 1$, so that $|P/Z(P)| \leq p$. Thus $P/Z(P)$ ic cyclic, so that $P = Z(P)$ by (6S). (2) follows also from (6S). We have that $|P : Z(P)| \neq 1$, and if $|P : Z(P)| = p$ then $P/Z(P)$ is cyclic, contradiction. □

(9D) Theorem: *A p-group is nilpotent.*

Proof: Let $P \neq 1$ be a p-group. By (9A) $Z^1(P) = Z(P) \neq \{1\}$. If $Z^1(P) \neq P$ then $P/Z^1(P) \neq \{1\}$, a p-group. By (9A)

$$Z(P/Z^1(P)) = Z^2(P)/Z^1(P) \neq 1 \ ,$$

so that $|Z^2(P)| > |Z^1(P)|$. If $Z^2(P) = P$, then P is nilpotent. Otherwise $|Z^3(P)| > |Z^2(P)|$, etc. Finally we get $Z^m(P) = P$ for a suitable $m \geq 1$. □

(9E) Corollary: *Let $U \neq P$ be a subgroup in then p-group P. Then*

$$U \subset N_P(U) \ .$$

Proof: Use (9D) and (8H). □

(9F) Theorem: *Let* $|U| = p^a$, $U \subset P$.

(1) There exists a subgroup V *in* P *satisfying* $U \trianglelefteq V$, $|V| = p^{a+1}$.

(2) If $U \trianglelefteq P$, *then also* V *may bechosen as normal i* P.

Proof: Let $Q = N_P(U)$, so that $U \trianglelefteq Q$, $U \neq Q$ (by (9E)). Choose an element $\overline{x}$ of order p in $Z(Q/U)$. ($\overline{x}$ exists by (9A), as $Q/U \neq \{1\}$).

The inverse image V of $\langle \overline{x} \rangle$ in Q has the properties $U \subseteq V$, $|V : U| = |\langle \overline{x} \rangle| = |\overline{x}| = p$, and $V \trianglelefteq Q$ as $\langle \overline{x} \rangle \trianglelefteq \overline{Q} = Q/U$.

Thus $|V| = |V : U|\ |U| = p|U| = p^{a+1}$ and $U \trianglelefteq V$, as $V \subseteq N_P(U) = Q$. This shows (1). As furthermore $V \trianglelefteq Q$, we see that if $U \trianglelefteq P$, then $Q = P$ and then $V \trianglelefteq P$ showing (2). □

(9G) Corollary: *If* $|P| = p^n$ *then* P *contains a en (normal) subgroup* N *med* $|N| = p^a$ *for* $1 \leq a \leq n$. □

(9H) Corollary: *Let* $M \subseteq P$, $|P| = p^n$. *We have*

$$M \ \textit{maximal subgroup in } P$$

$$\Updownarrow$$

$$|M| = p^{n-1} \ .$$

If M *is maximal in* P, *then* $M \trianglelefteq P$.

Proof: $\Uparrow$ is triviel. $\Downarrow$ follows easily from (9F) (1). The last statement follows from the first and (9E). □

Let us now consider the Frattini group $\Phi(P)$ of G (see Chapter 8). $Max(P)$ denotes again the set of maximal subgroups in P.

(9I) Theorem: *The factor group* $P/\Phi(P)$ *is an elementary abelian* p*–group.*

Proof: If $M \in Max(P)$, then $P/M \cong \mathbb{Z}_p$ by (9H). In particular

(i) $P' \subseteq M$

and

(ii) For all $x \in P$ we have $x^p \in M$ (since $\overline{x} = xM$ has order 1 or p in G/M).

As (i) and (ii) hold for all $M \in Max(P)$ we get from the definition of $\Phi(P) = \bigcap_{M \in Max(P)} M$ that

(iii) $P' \subseteq \Phi(P)$

(iv) For all $x \in P$ $x^p \in \Phi(P)$.

Then (iii) shows that $P/\Phi(P)$ is abelian (see (6A)), and (iv) shows that for all $\overline{x} \in P/\Phi(P)$ we have $\overline{x}^p = 1$. Thus $P/\Phi(P)$ is elementary abelian. □

(9J) Theorem: *Let $x_1, \cdots, x_k \in P$. In the above notation we have*

$$\langle x_1, \cdots, x_k \rangle = P$$

$$\Updownarrow$$

$$\langle \overline{x}_1, \cdots, \overline{x}_k \rangle = \overline{P} \ ,$$

where $\overline{x}_i$ is the image of x_i in the Frattini factor group $\overline{P} = P/\Phi(P)$.

Proof: $\Downarrow$ er trivial.

$\Uparrow$: Assume $\langle \overline{x}_1, \cdots, \overline{x}_k \rangle = \overline{P}$. Put

$$U := \langle x_1, \cdots, x_k, \Phi(P) \rangle \subseteq P \ .$$

We claim that $U = P$. If $x \in P$ then by assumption and (9I) we may write

$$\overline{x} = \overline{x}_1{}^{a_1} \cdots \overline{x}_k{}^{a_k} \ \ \textit{where} \ \ 0 \leq a_i \leq p-1 \ ,$$

ie.

$$\overline{x} = \overline{x_1{}^{a_1} \cdots x_k{}^{a_k}}$$

or $u := x(x_1{}^{a_1} \cdots x_k{}^{a_k})^{-1} \in \Phi(P)$. But then

$$x = x_1{}^{a_1} \cdots x_k{}^{a_k} u \in \langle x_1, \cdots, x_k, \Phi(P) \rangle = U \ .$$

We have shown $P = \langle x_1, \cdots, x_k, \Phi(P) \rangle$. From (8A) we then get $P = \langle x_1, \cdots, x_k \rangle$, as desired. □

(9K) Theorem: (Burnside) *Assume that $|P : \Phi(P)| = p^r$.*

(i) Each generating set for P contains at least r elements.

(ii) A generating set for P with s elements may be "contracted" to a generating set for P with r elements (by deleting some of the s elements).

(iii) In particular there exists a generating set for P with r elements.

Proof: We need (9J) and some linear algebra! The "contraction" theorem for finite-dimensional vector spaces states that a set of spanning vectors for the vector space may be reduced to a basis by removing some of the vectors.

Now $P/\Phi(P)$ is an elementary abelian group of order p^r, and may thus be considered as a vector space of dimension r over the field $\mathbb{Z}_p$ med p elementer. (See (6P)). If $\langle x_1, \cdots, x_s \rangle = P$, then $\langle \overline{x}_1, \cdots, \overline{x}_s \rangle = \overline{P}$ and therefore $\{\overline{x}_1, \cdots, \overline{x}_s\}$ is a generating set of vectors for the vector space $\overline{P}$. Therefore it contains at least $r = \dim \overline{P}$ elements. This shows (i). (ii) follows from the contraction theorem for vector spaces and (9J), and then (iii) is trivial. $\square$