

Group Theory I
Lecture Notes for MTH 912
F18

Ulrich Meierfrankenfeld

December 12, 2018

Contents

1	Group Actions	5
1.1	Groups acting on sets	5
1.2	Direct and Semidirect Products	10
1.3	Complements	15
1.4	Frobenius Groups	22
1.5	Imprimitive action	28
1.6	Wreath products	30
1.7	Multi-transitive action	34
2	Hypercentral and Hypocentral Groups	37
2.1	Hypercentral Groups	37
2.2	The Frattini subgroup	46
2.3	Finite p -groups with cyclic maximal subgroups	49
2.4	Hypoabelian groups	55
3	π-separable groups and Hall πsubgroups	63
3.1	The Theorem of Schur-Zassenhaus	63
3.2	π -separable and π -solvable groups	64
3.3	Sylow π - and Hall π -subgroups	66
4	Subnormal subgroups and near-components	73
4.1	Join of Subnormal Subgroups	73
4.2	Near-components	73
A	Set Theory	81
A.1	Ordinals	81

Chapter 1

Group Actions

1.1 Groups acting on sets

Definition 1.1.1. An action of a group G on set Ω is a function

$$\begin{aligned}\bullet: \Omega \times G &\rightarrow \Omega \\ (\omega, g) &\mapsto \omega^g\end{aligned}$$

such that

- (i) $\omega^1 = \omega$ for all $\omega \in \Omega$.
- (ii) $(\omega^x)^y = \omega^{xy}$ for all $\omega \in \Omega, x, y \in G$.

A G -set is a pair $(\Omega, \bullet)$, where $\bullet$ is an action of G on Ω .

Example 1.1.2. Let G be a group, H a subgroup of G and Ω a set. Each of the following are actions.

(a)

$$\begin{aligned}\text{RM: } G \times G &\rightarrow G \\ (a, b) &\mapsto ab\end{aligned} \quad (\text{action by right multiplication})$$

(b)

$$\begin{aligned}\text{LM: } G \times G &\rightarrow G \\ (a, b) &\mapsto b^{-1}a\end{aligned} \quad (\text{action by left multiplication})$$

(c)

$$\begin{aligned}\text{Conj: } G \times G &\rightarrow G \\ (a, b) &\mapsto b^{-1}ab\end{aligned} \quad (\text{action by left conjugation})$$

(d)

$$\begin{aligned}\text{RM: } G/H \times G &\rightarrow G \\ (Ha, b) &\mapsto Hab\end{aligned} \quad (\text{action by right multiplication})$$

(e)

$$\begin{aligned} \text{Nat: } \Omega \times \text{Sym}(\Omega) &\rightarrow \Omega \\ (\omega, \pi) &\mapsto \omega\pi \end{aligned} \quad (\text{natural action})$$

Definition 1.1.3. Let $\bullet$ be an action of the group G on the set Ω . Let $g \in G$, $\omega \in \Omega$, $H \subseteq G$ and $\Delta \subseteq \Omega$.

- (a) $\Delta^g := \{\omega^g \mid \omega \in \Delta\}$.
- (b) $\omega^H = \{\omega^h \mid h \in H\}$.
- (c) $C_H^\bullet(\Delta) := \{h \in H \mid \omega^h = \omega \text{ for all } \omega \in \Delta\}$.
- (d) $C_H^\bullet(\omega) = \{h \in H \mid \omega^h = \omega\}$. (So $C_H^\bullet(\omega) = C_H^\bullet(\{\omega\})$. We will often write $H_\omega^\bullet$ for $C_G^\bullet(\omega)$).
- (e) $C_\Delta^\bullet(g) = \{\delta \in \Delta \mid \delta = \delta^g\}$.
- (f) $C_\Delta^\bullet(H) = \{\delta \in \Delta \mid \delta = \delta^h \text{ for all } h \in H\}$.
- (g) $N_H^\bullet(\Delta) := \{h \in H \mid \Delta^h = \Delta\}$.
- (h) Δ is called H -invariant if $\Delta = \Delta^h$ for all $h \in H$.

Remark 1.1.4. Let $\bullet$ be an action of the group G on the set Ω .

- (a) Let $P(\Omega)$ be the set of subsets of Ω . Then

$$\bullet_{P(\Omega)}: P(\Omega) \times G \rightarrow P(\Omega), \quad (\Delta, g) \mapsto \Delta^g$$

is action of G on $P(\Omega)$.

- (b) Let $H \leq G$ and let Δ be an H -invariant subset of Ω . Then

$$\bullet_{H, \Delta}: \Delta \times H \rightarrow \Delta, \quad (\omega, h) \mapsto \omega^h$$

is action of H on Δ .

- (c) If there is no doubt about the action $\bullet$, we will often omit the superscript $\bullet$ in $C_H^\bullet(\omega)$, $N_H^\bullet(\Delta)$ and so on.

Lemma 1.1.5. Let $\bullet$ be an action of the group G on the set Ω , $g \in G$, $H \subseteq G$ and $\Delta \subseteq \Omega$.

- (a) If $H \leq G$, then $C_H(\Delta) \leq N_H(\Delta) \leq H$.
- (b) $C_H(\Delta)^g = C_{H^g}(\Delta^g)$.
- (c) Define

$$\phi_g: \Omega \rightarrow \Omega, \quad \omega \mapsto \omega^g$$

and

$$G^{\bullet\Omega} = \{\phi_g \mid g \in G\}.$$

Then the function

$$\phi: G \rightarrow \text{Sym}(\Omega), \quad g \mapsto \phi_g$$

is a well-defined homomorphism of groups with

$$\text{Ker}\phi = C_G^\bullet(\Omega) \quad \text{and} \quad \text{Im}\phi = G^{\bullet\Omega}.$$

In particular, $C_G^\bullet(\Omega)$ is a normal subgroup of G , $G^{\bullet\Omega}$ is a subgroup of $\text{Sym}(\Omega)$ and $G/C_G^\bullet(\Omega) \cong G^{\bullet\Omega}$.

Proof. Readily verified. As an example we prove (b). Let $h \in G$. Then

$$\begin{aligned}
& h \in C_H(\Delta)^g \\
\iff & h^{g^{-1}} \in C_H(\Delta) \\
\iff & \omega^{h^{g^{-1}}} = \omega \text{ for all } \omega \in \Delta \text{ and } h^{g^{-1}} \in H \\
\iff & \omega^{ghg^{-1}} = \omega \text{ for all } \omega \in \Delta \text{ and } h \in H^g \\
\iff & (\omega^{gh} = \omega^g \text{ for all } \omega \in \Delta \text{ and } h \in H^g \\
\iff & (\omega^g)^h = \omega^g \text{ for all } \omega \in \Delta \text{ and } h \in H^g \\
\iff & \mu^g = \mu \text{ for all } \mu \in \Delta^g \text{ and } h \in H^g \\
\iff & h \in C_{H^g}(\omega^g)
\end{aligned}$$

Hence $C_H(\Delta)^g = C_{H^g}(\Delta^g)$ □

Definition 1.1.6. Let G be a group and let Ω_1 and Ω_2 be G -sets. Let $\alpha : \Omega_1 \rightarrow \Omega_2$ be a function.

(a) α is called G -equivariant if

$$\omega^g \alpha = (\omega \alpha)^g$$

for all $\omega \in \Omega$ and $g \in G$.

(b) α is called a G -isomorphism if α is G -equivariant bijection.

(c) Ω_1 and Ω_2 are called G -isomorphic if there exists a G -isomorphism from Ω_1 to Ω_2 .

Definition 1.1.7. Let G be a group acting on a non-empty set Ω .

(a) We say that G acts transitively on Ω if for all $a, b \in \Omega$ there exists at least one $g \in G$ with $a^g = b$.

(b) We say that G acts semiregularly on Ω if for all $a, b \in \Omega$ there exists at most one $g \in G$ with $a^g = b$.

(c) We say that G acts regularly on Ω if for all $a, b \in \Omega$ there exists exactly one $g \in G$ with $a^g = b$, that is if G acts transitively and semiregularly on Ω .

Example 1.1.8. (a) The action of the group G on G by right multiplication is regular.

(b) The natural action of $\text{Sym}(\Omega)$ on the set Ω is transitive. If $|\Omega| \geq 3$, this action is not semiregular.

Lemma 1.1.9. Suppose that the group G acts transitively on the set Ω and let $\omega \in \Omega$. View G/G_ω as a G -set via right multiplication. Then the map

$$\begin{aligned}
\phi : G/G_\omega & \rightarrow \Omega \\
G_\omega g & \mapsto \omega^g
\end{aligned}$$

is a well-defined G -isomorphism. In particular, $|\Omega| = |G/G_\omega|$.

Proof. Let $g, h \in G$. Then the following statements are equivalent:

$$\begin{aligned}
\omega^g &= \omega^h \\
\omega^{gh^{-1}} &= \omega \\
gh^{-1} &\in G_\omega \\
G_\omega g &= G_\omega h
\end{aligned}$$

The forward direction shows that ϕ is injective and the backward direction shows that ϕ is well-defined. Since G is transitive on Ω , ϕ is surjective. Note that

$$((G_\omega g)h)\phi = (G_\omega(gh))\phi = \omega^{gh} = (\omega^g)^h = ((G_\omega g)\phi)^h$$

and so ϕ is G -equivariant. □

Definition 1.1.10. Let G be a group and $L \leq G$.

- (a) A supplement to L in H is a subgroup K of G with $G = LK$.
- (b) A complement to L in G is a supplement K to L in G with $L \cap K = 1$.

Proposition 1.1.11. Let G be a group acting on a set Ω , H a subgroup of G and $\omega \in \Omega$.

- (a) (**Frattini Argument**) If H acts transitively on Ω , then $G = G_\omega H$.
- (b) If H acts semi-regularly on Ω , then $G_\omega \cap H = 1$.
- (c) If H acts regularly on Ω , then H is a complement to G_ω in G .

Proof. (a) Let $g \in G$. Since H acts transitively on Ω , $\omega^g = \omega^h$ for some $h \in H$. Hence $gh^{-1} \in G_\omega$ and $g = (gh^{-1})h \in G_\omega H$.

(b) Let $h \in G_\omega \cap H$. Then $\omega^h = \omega = \omega^1$ and so $h = 1$ by definition of semi-regular.

(c) Since H acts regularly on Ω if and only if it acts transitively and semi-regularly, (c) follows from (a) and (b). □

Definition 1.1.12. Let G be a group acting on the set Ω .

- (a) Let $\omega \in \Omega$. The ω^G is called the orbit of G on Ω containing ω . Ω/G denotes the set of orbits of G on Ω .
- (b) Let $a, b \in \Omega$. We say that a is G -equivalent to b if $b = a^g$ for some $g \in G$, that is, if $b \in a^G$.

Remark 1.1.13. Let $(\Omega_i)_{i \in I}$ be a family of G -sets. Then the disjoint union $\uplus_{i \in I} \Omega_i (= \bigcup_{i \in I} \Omega_i \times \{i\})$ is a G -set via $(\omega, i)^g = (\omega^g, i)$ for all $g \in G, i \in I$ and $\omega \in \Omega_i$.

Lemma 1.1.14. Let G be a group acting on set Ω .

- (a) G -equivalent is an equivalence relation. Its equivalence classes are the orbits of G on Ω . In particular, the orbits of G on Ω form a partition of Ω .
- (b) Let Δ be a set of representatives for the orbits of G on Ω (that is $\Delta \subseteq \Omega$ and $|\Delta \cap O| = 1$ for each orbit O of G on Ω). Then Ω and $\uplus_{\omega \in \Delta} G/G_\omega$ are isomorphic G -sets. In particular,

$$|\Omega| = \sum_{\omega \in \Delta} |G/G_\omega| \quad (\text{Orbit equation})$$

Proof. (a) Since $\omega = \omega^1$, the relation is reflexive. If $a, b \in \Omega$ with $a^g = b$, then $b^{g^{-1}} = a$ and the relation is symmetric. If $a^g = b$ and $b^h = c$, then $a^{gh} = c$ and the relation is transitive. ω^G is the set of elements which are G -equivalent to ω and so is the equivalence class of G -equivalent containing ω .

(b) Since each elements of ω lies in exactly on orbits of G on Ω and since each orbit contains exactly one element of Δ we have

$$\Omega = \bigsqcup_{\omega \in \Delta} \omega^G$$

Observe that G acts transitively on ω^G and so by 1.1.9 $\omega^G \cong G/G_\omega$ as a G -set. So (b) holds. $\square$

Lemma 1.1.15. *Let G be a group acting on a non-empty set Ω .*

- (a) *G acts semiregularly on Ω if and only if $G_a = 1$ for all $a \in \Omega$.*
- (b) *G acts transitively on Ω if and only if there exists $a \in \Omega$ such that for all $b \in \Omega$ there exists $g \in G$ with $a^g = b$.*
- (c) *G acts regularly on Ω if and only if there exists $a \in \Omega$ such that for all $b \in \Omega$ there exists a unique $g \in G$ with $a^g = b$.*

Proof. (a) Suppose that G acts semiregularly on Ω and let $a \in \Omega$. Then (1.1.11)(b) shows that $G \cap G_a = 1$ and so $G_a = 1$.

Suppose now that $G_a = 1$ for all $a \in \Omega$. Let $b \in \Omega$ and suppose that $b = a^g = a^h$ for $a \in \Omega$ and $g, h \in G$. Then $a^{gh^{-1}} = a$, $gh^{-1} \in G_a = 1$ and $g = h$. So G acts semiregularly on Ω .

(b) The forward direction is obvious. If $a^G = \Omega$, then Ω is an orbit for G on Ω . Thus any two elements of Ω are G -equivalent and so G act transitively on Ω .

(c) The forward direction is obvious. Suppose now that $a \in \Omega$ and for each b there exists a unique $g \in G$ with $a^g = b$. For $b = a$ we see that $G_a = 1$. Thus $G_b = G_{a^g} = G_a^g = 1$. Now (b) shows that G acts transitively and (a) shows that G acts semiregularly on Ω . So G acts regularly on Ω . $\square$

Definition 1.1.16. *Let G be a group acting on a set Ω . We say that G acts faithfully on G if $C_G(\Omega) = 1$.*

Remark 1.1.17. *G acts faithfully on Ω if and only if the homomorphism*

$$\phi: G \rightarrow \text{Sym}(\Omega), \quad g \mapsto \phi_g$$

from (1.1.5)(c) is injective. In particular, if G acts faithfully, then G is isomorphic to the subgroup $G^{\bullet\Omega}$ of $\text{Sym}(\Omega)$.

Lemma 1.1.18. *Let G be a group acting on a set Ω . Then the function*

$$\Omega \times G/C_G(\Omega) \rightarrow \Omega, (\omega, C_G(\Omega)g) \mapsto \omega^g$$

is a well-defined, faithful action of $G/C_G(\Omega)$ on Ω .

Proof. Readily verified. $\square$

Lemma 1.1.19. *Let G be a group. Then the following are equivalent:*

- (a) *All subgroups of G are normal in G .*
- (b) *Whenever G acts transitively on a set Ω , then $G/C_G(\Omega)$ acts regularly on Ω .*

Proof. Let Ω be a set on which G acts transitively and put $\overline{G} = G/C_G(\Omega)$. Note that $\overline{G}_\omega = \overline{G}_\omega$ for all $\omega \in \Omega$. Observe that

(*) $\overline{G}$ acts regularly on Ω iff $\overline{G}_\omega = 1_{\overline{G}}$, and iff $G_\omega = C_G(\Omega)$ for all ω in Ω .

(a) $\implies$ (b): Suppose that all subgroups of G are normal in G . Then $G_\omega = G_\omega^g = G_{\omega^g}$. Since G acts transitively on G this gives $G_\omega = G_\mu$ for all $\mu \in \Omega$ and so

$$C_G(\Omega) = \bigcup_{\mu \in \Omega} G_\mu = G_\omega.$$

Thus (*) shows that $\overline{G}$ act regularly on G .

(b) $\implies$ (a): Suppose $G/C_G(\Omega)$ acts regularly on Ω for each transitive G -sets Ω . Let $H \leq G$ and put $\Omega = G/H$. Let $\omega = H$ and note that $\omega \in \Omega$ and $G_\omega = H$ and by (*) $G_\omega = C_G(\Omega)$. Thus $H = C_G(\Omega)$ and since $C_G(\Omega)$ is a normal subgroup of G , H is normal in G . $\square$

1.2 Direct and Semidirect Products

Definition 1.2.1. Let $(G_i)_{i \in I}$ be a family of groups.

(a) $\times_{i \in I} G_i$ denotes the set of function $f : I \rightarrow \bigcup_{i \in I} G_i$ with $if \in G_i$ for all $i \in I$. We view $\times_{i \in I} G_i$ as a group via

$$i(fg) = if \cdot ig$$

for all $f, g \in \times_{i \in I} G_i$ and $i \in I$. $\times_{i \in I} G_i$ is called the (external) direct product of $(G_i)_{i \in I}$.

(b) For $f \in \times_{i \in I} G_i$ define $\text{supp}(f) = \{i \in I \mid if \neq 1\}$.

(c)

$$\bigoplus_{i \in I} G_i := \{f \in \times_{i \in I} G_i \mid \text{supp}(f) \text{ is finite}\}.$$

Note that $\bigoplus_{i \in I} G_i$ is a subgroup of $\times_{i \in I} G_i$. $\bigoplus_{i \in I} G_i$ is called the (external) direct sum of $(G_i)_{i \in I}$.

Definition 1.2.2. Let G be group and let $(G_i)_{i \in I}$ be a family of subgroup of G . For $J \subseteq I$ define $G_J = \langle G_j \mid j \in J \rangle$. Then G is called the internal direct sum of $(G_i)_{i \in I}$ provided that

(i) $G = G_I$,

(ii) $G_i \trianglelefteq G$ for all $i \in I$, and

(iii) $G_i \cap G_{I \setminus \{i\}} = 1$ for all $i \in I$.

Definition 1.2.3. Let I be an ordered set, G a group and $f \in \bigoplus_{i \in I} G$. Then

$$\prod_{i \in I} if := i_1 f \cdot i_2 f \cdot \dots \cdot i_n f$$

where $i_1, i_2, \dots, i_n \in I$ with

$$\text{supp}(f) = \{i_1, \dots, i_n\} \quad \text{and} \quad i_1 < i_2 < \dots < i_n$$

Lemma 1.2.4. *Let I be an ordered set and $(G_i)_{i \in I}$ be a family of groups. Define $G := \bigoplus_{i \in I} G_i$ and for $J \subseteq I$ define $G_J = \{f \in G \mid \text{supp}(f) \subseteq J\}$. Put $G_i^* = G_{\{i\}}$. For $i \in I$ and $g \in G_i$ define*

$$\begin{aligned} g_i : I &\rightarrow \bigcup_{i \in I} G_i \\ j &\mapsto \begin{cases} 1 & \text{if } j \neq i \\ g & \text{if } j = i \end{cases} \end{aligned}$$

- (a) *Let $J \subseteq I$ and $f \in G_J$. Then $f = \prod_{j \in J} (jf)_j$.*
- (b) *Let $i \in I$. Then the function $G_i \rightarrow G_i^*, g \mapsto g_i$ is an isomorphism of groups.*
- (c) *Let $J \subseteq I$. Then $G_J \trianglelefteq \times_{i \in I} G_i$, $G_J \trianglelefteq G$ and $G_J = \langle G_j^* \mid j \in J \rangle$*
- (d) *G is the internal direct sum of $(G_i^*)_{i \in I}$.*

Proof. (a) Define $h := \prod_{j \in I} (jf)_j$ and let $i \in I$.

$$ih = \prod_{j \in J} i(jf)_j$$

Note that $i(jf)_j = 1$ if $i \neq j$ and $i(jf)_j = jf = if$ if $i = j$.

Suppose $i \in J$. Then there exists a unique $j \in J$ with $i = j$ (namely i). Thus $ih = if$.

Suppose $i \notin J$, then there does not exist any $j \in I$ with $i = j$. Thus $ih = 1$. Since $f \in G_J$ we have $\text{supp}(f) \subseteq J$. Thus $i \notin \text{supp}(f)$ and so $if = 1$. Thus again $ih = if$.

We proved that $ih = if$ for all $i \in I$ and so $h = g$.

(b) Let $g, h \in G_i$ and $j \in I$ with $j \neq i$. By definition of g_i we have $hg_i = 1$. Hence $\text{Supp}(g_i) \subseteq \{i\}$ and so $g_i \in G_i^*$. Thus the function is well-defined. Moreover

$$j(g_i h_i) = jg_i \cdot jh_i = 1 \cdot 1 = 1 = j(gh)_i \quad \text{and} \quad i(g_i h_i) = ig_i \cdot ih_i = gh = i(gh)_i$$

Thus $g_i h_i = (gh)_i$ and the function is a homomorphism.

If $g_i = h_i$, then $g = ig_i = ih_i = h$ and so the function is injective.

Let $f \in G_i^*$. By (a) applied with $J = \{i\}$ we have $f = (if)_i$ and so the function is surjective.

(c) Let $e, f \in G_J$, $h \in \times_{i \in I} G_i$ and $i \in I \setminus J$. Then $ie = if = 1$ and so

$$if^{-1} = (if)^{-1} = 1, \quad i(ef) = ie \cdot if = 1, \quad if^h = i(h^{-1}fh) = ih^{-1} \cdot 1f \cdot ih = (ih)^{-1} \cdot 1 \cdot (ih) = 1$$

Hence f^{-1}, ef and f^h all are contained in G_J . Thus G_J is a subgroup of G and $G_J \trianglelefteq \times_{i \in I} G_i$. So also $G_J \trianglelefteq G$.

Let $j \in J$ and $g \in G_j^*$. Then $\text{supp}(g) \subseteq \{j\} \subseteq J$ and so $g \in G_J$. Thus $G_j^* \leq G_J$ and since G_J is a subgroup of G , also $\langle G_j^* \mid j \in J \rangle \leq G_J$.

Now let $f \in G_J$. By (a) $f = \prod_{j \in J} (jf)_j$. As $(jf)_j \in G_j^*$ we conclude that $G_J \leq \langle G_j^* \mid j \in J \rangle$. Thus $G_J = \langle G_j^* \mid j \in J \rangle$ and (a) is proved

(d) By (c) $G = G_I = \langle G_i^* \mid i \in I \rangle$ and $G_i^* = G_{\{i\}} \trianglelefteq G$. If $g \in G_i^* \cap G_{I \setminus \{i\}}$ then $\text{supp}(g) \subseteq \{i\} \cap I \setminus \{i\} = \emptyset$ and so $g = 1$. Thus

$$G_i^* \cap \langle G_j^* \mid j \in I \setminus \{i\} \rangle = G_i^* \cap G_{I \setminus \{i\}} = 1$$

and so all three conditions on the internal direct sum hold. $\square$

Lemma 1.2.5. *Let G be group, I an ordered set and $(G_i)_{i \in I}$ a family of subgroup of G .*

(a) *G is the internal direct sum of $(G_i)_{i \in I}$ if and only if the function*

$$\phi: \bigoplus_{i \in I} G_i \rightarrow G, \quad f \mapsto \prod_{i \in I} i f$$

is isomorphism of groups.

(b) *Suppose that G is the internal direct sum of $(G_i)_{i \in I}$. Then $[G_i, G_j] = G_i \cap G_j = 1$ for all $i, j \in I$ with $i \neq j$. In particular, the function ϕ in (a) is independent of the ordering on I .*

Proof. Let $G^* = \times_{i \in I} G_i$ and define $G_i^* \leq G^*$ as in Lemma 1.2.4. Observe that $G_i^* \phi = G_i$.

Suppose first that ϕ is an isomorphism of groups. By (1.2.4)(d) we know that G^* is the internal direct sum of $(G_i^*)_{i \in I}$. As ϕ is an isomorphism and $G_i^* \phi = G_i$ we conclude that G is the internal direct sum of $(G_i)_{i \in I}$.

Suppose next that G is the internal direct sum of $(G_i)_{i \in I}$. Let $i, j \in I$ with $i \neq j$. Then both G_i and G_j are normal in G and so

$$[G_i, G_j] \leq G_i \cap G_j \leq G_i \cap G_{I \setminus \{i\}} = 1$$

It follows that $g_i g_j = g_j g_i$ for any $g_i \in G_i, g_j \in G_j$. This implies that ϕ is independent of ordering on I . Moreover, for any $f, g \in G^*$:

$$(fg)\phi = \prod_{i \in I} i(fg) = \prod_{i \in I} (if \cdot ig) = \prod_{i \in I} if \cdot \prod_{i \in I} ig = f\phi \cdot g\phi$$

So ϕ is an homomorphism. Let $f \in \text{Ker} \phi$ and $j \in I$. Then

$$1 = f\phi = \prod_{i \in I} if = \left(\prod_{i < j} if \right) \cdot jf \cdot \left(\prod_{i > j} if \right)$$

and so

$$jf = \left(\prod_{i < j} if \right)^{-1} \cdot 1 \cdot \left(\prod_{i > j} if \right)^{-1} \in G_{I \setminus \{j\}}$$

Since $jf \in G_j$ and $G_j \cap G_{I \setminus \{j\}} = 1$ we conclude that $jf = 1$ for all $j \in I$. Thus $f = 1$ and so f is injective. Observe that $G_i = G_i^* \phi \leq \text{Im} \phi$ for all $i \in I$. Since ϕ is a homomorphism we know that $\text{Im} \phi$ is a subgroup of G . Hence

$$G = G_I = \langle G_i \mid i \in I \rangle \leq \text{Im} \phi$$

and so ϕ is surjective. □

Definition 1.2.6. *Let G and H be groups. An actions of G on H is an action $\cdot$ of G on the set H such that*

$$(ab)^g = a^g b^g$$

for all $a, b \in H$ and $g \in G$.

Remark 1.2.7. (a) Let G be the group acting on the group H and $g \in G$. Then function

$$\phi_g: H \rightarrow H, \quad h \mapsto h^g$$

automorphism of H . Moreover,

$$\phi: G \rightarrow \text{Aut}(H), \quad g \mapsto \phi_g$$

is a homomorphism of groups and $G^{\bullet H}$ is a subgroup of $\text{Aut}(H)$.

(b) Let G and H be groups and

$$\phi: G \rightarrow \text{Aut}(H), \quad g \mapsto \phi_g$$

be a homomorphism of groups. Then

$$\bullet: H \times G \rightarrow H, \quad (h, g) \mapsto h\phi_g$$

is an action of G on the group H .

Example 1.2.8. Let G be a group and N a normal subgroup of G .

(a) $N \times G \rightarrow N, (n, g) \rightarrow g^{-1}ng$ is an action of G on the group N .

(b) $G \times G \rightarrow G, (h, g) \rightarrow hg$ is not an action of G on the group G (unless $G = 1$).

(c) $G \times \text{Aut}(G) \rightarrow G, (g, \alpha) \rightarrow g\alpha$ is an action of $\text{Aut}(G)$ on the group G .

Definition 1.2.9. Let L be a group and let H and G be subgroups of L . Then L is called the internal semidirect product of H by G , provided that H is normal in L , and G is a complement to H in L .

Lemma 1.2.10. Let the group L be the internal direct product of H by G .

(a) G acts on the group H by conjugation.

(b) The function $\tau: G \times H \rightarrow L, (g, h) \mapsto gh$ is bijection.

(c) $(g_1h_1)(g_2h_2) = (g_1g_2)(h_1^{g_2}h_2)$ for all $g_1, g_2 \in G, h_1, h_2 \in H$.

Proof. (a) is obvious.

Let $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

(b) Observe that $\text{Im } \tau = GH$ and since G is complement to H in L , we have $L = GH$. So τ is surjective. If $g_1, g_2 \in G$ and $h_1, h_2 \in H$ with $g_1h_1 = g_2h_2$, then $g_2^{-1}g_1 = h_1h_2^{-1} \in G \cap H = 1$. So $g_1 = g_2$ and $h_1 = h_2$.

(c)

$$(g_1h_1)(g_2h_2) = g_1g_2g_2^{-1}h_1g_2h_2 = (g_1g_2)(h_1^{g_2}h_2)$$

□

The previous lemma leads to the following definition.

Definition 1.2.11. Let G be a group acting on the group H . Then $G \ltimes H$ is the set $G \times H$ together with the binary operation

$$\begin{aligned} (G \times H) \times (G \times H) &\rightarrow (G \times H) \\ ((g_1, h_1), (g_2, h_2)) &\mapsto (g_1g_2, h_1^{g_2}h_2) \end{aligned}$$

$G \ltimes H$ is called the external direct product of H by G .

Lemma 1.2.12. *Let G be a group acting on the group H and put $G^* = \{(g, 1) \mid g \in G\}$ and $H^* = \{(1, h) \mid h \in H\}$.*

- (a) $G \ltimes H$ is a group.
- (b) The function $G \rightarrow G \ltimes H, g \rightarrow (g, 1)$ is an injective homomorphism with image G^* .
- (c) The function $H \rightarrow G \ltimes H, h \rightarrow (1, h)$ is an injective homomorphism with image H^* .
- (d) $(1, h)^{(g, 1)} = (1, h^g)$ for all $g \in G, h \in H$.
- (e) $G \ltimes H$ is the internal semidirect product of H^* by G^* .

Proof. (a) Clearly $(1, 1)$ is an identity. We have

$$\begin{aligned} ((g_1, h_1)(g_2, h_2))(g_3, h_3) &= (g_1 g_2, h_1^{g_2} h_2)(g_3, h_3) = (g_1 g_2 g_3, (h_1^{g_2} h_2)^{g_3} h_3) = \\ &= (g_1 g_2 g_3, (h_1^{g_2})^{g_3} h_2^{g_3} h_3) = (g_1 g_2 g_3, h_1^{g_2 g_3} h_2^{g_3} h_3) = (g_1, h_1)(g_2 g_3, h_2^{g_3} h_3) = (h_1, g_1)((h_2, g_2)(h_3, g_3)) \end{aligned}$$

and so the multiplication is associative.

We have

$$\begin{aligned} (g, h)(x, y) &= (1, 1) \\ \iff gx = 1 \text{ and } h^x y &= 1 \\ \iff x = g^{-1} \text{ and } y &= (h^x)^{-1} \\ \iff x = g^{-1} \text{ and } y &= (h^{g^{-1}})^{-1} \end{aligned}$$

Thus $(g^{-1}, (h^{g^{-1}})^{-1})$ is an inverse of (g, h) .

(b) Since for any $g \in G$, the map $H \rightarrow H, h \rightarrow h^g$ is a homomorphism, we have $1^g = 1$. Thus $(g_1, 1)(g_2, 1) = (g_1 g_2, 1^{g_2}) = (g_1 g_2, 1)$.

(c) $(1, h_1)(1, h_2) = (1, h_1^1 h_2) = (1, h_1 h_2)$.

(d) $(1, h)^{(g, 1)} = (g^{-1}, 1)(1, h)(g, 1) = (g^{-1}, h)(g, 1) = (g^{-1} g, h^g) = (1, h^g)$.

(e) Clearly $G^* \cap H^* = 1$. Since $(g, 1)(1, h) = (g, h)$, $G \ltimes H = G^* H^*$ and so G^* is a complement to H^* in $G \ltimes H$. By (d), G^* normalizes H^* and so H^* is normal in $G^* H^* = G \ltimes H$. $\square$

Example 1.2.13. Consider $H = C_2 \times C_2$ and $G = \text{Aut}(H)$. So G acts on the group H . Note that $G \cong \text{Sym}(3)$. We claim that $G \ltimes H$ is isomorphic to $\text{Sym}(4)$. Note that $\text{Sym}(4)$ has

$$H^* := \{1, (12)(34), (13)(24), (14)(23)\}$$

as a normal subgroup and $H^* \cong C_2 \times C_2$. Observe that H^* acts regularly on $\Omega = \{1, 2, 3, 4\}$ and so by 1.1.11, $G^* := \text{Sym}(4)_4$ is a complement to H^* in $\text{Sym}(4)$. Also $G^* \cong \text{Sym}(3) \cong \text{Aut}(H^*)$ and $C_{G^*}(H^*) = 1$. So G^* acts faithfully on H^* . Thus $\text{Sym}(4)$ is the internal semidirect product of H^* by G^* . Hence using Exercise 2 on Homework 1,

$$\text{Sym}(4) = G^* H^* \cong G^* \ltimes H^* \cong G \ltimes H.$$

1.3 Complements

Lemma 1.3.1 (Modular Law). *Let G be a group and let A , B and U be subsets of G .*

- (a) *Suppose that $UB \subseteq U$ and $UB^{-1} \subseteq U$. Then $U \cap AB = (A \cap U)B$.*
- (b) *Suppose that $B \subseteq U \leq G$. Then $U \cap AB = (A \cap U)B$.*
- (c) *Suppose that $B \subseteq U \leq G = AB$. Then $U = (A \cap U)B$.*

Proof. (a) Let $u \in U \cap AB$. Then $u = ab$ for some $a \in A$ and $b \in B$. Since $UB^{-1} \subseteq U$, we have $a = ub^{-1} \in U$. Thus $a \in A \cap U$ and so $u = ab \in (A \cap U)B$. Hence $U \cap AB \subseteq (A \cap U)B$. Conversely, $(A \cap U)B \subseteq UB \cap AB \subseteq U \cap AB$.

(b) Since U is a group and $B \subseteq U$ we have $UU \subseteq U$ and $B^{-1} \subseteq U$. Thus $UB \subseteq U$ and $UB^{-1} \subseteq U$. So (b) follows from (a).

(c) If $G = AB$, then $U = U \cap AB$ and (c) follows from (b). □

Lemma 1.3.2. *Let G be a group, $H, K_1, K_2 \leq G$ with $G = K_1H$ and $K_2 \cap H = 1$.*

- (a) $G = HK_1$.
- (b) *If $K_1 \leq K_2$, then $K_1 = K_2$.*
- (c) $K_1^G = K_1^H$. *In particular, K_1 and K_2 are conjugate under G if and only if they are conjugate under H .*

Proof. (a) Note that $L^{-1} = L$ for any group L . So

$$G = G^{-1} = (K_1H)^{-1} = H^{-1}K_1^{-1} = HK_1$$

(b) Since $K_1 \leq K_2$ and $G = HK_1$, the Modular Law (1.3.1)(c) implies $K_2 = (K_2 \cap H)K_1$. As $K_2 \cap H = 1$ we get $K_1 = K_2$.

(c) Let $g \in G$. Since $G = K_1H$ we know that $g = k_1h$ with $k_1 \in K_1$ and $h \in H$. So $K_1^g = K_1^{kh} = K_1^h$. □

Definition 1.3.3. *Let G be a group, $H \leq G$ and $T \subseteq H$. Then T is called a transversal to H in G if the function $T \rightarrow G/H, t \mapsto Ht$ is a bijection.*

Remark 1.3.4. *Let G be a group, $H \leq G$ and $T \subseteq H$. Then the following statements are equivalent:*

- (a) T is a transversal to H in G .
- (b) $|L \cap T| = 1$ for each $L \in G/H$.
- (c) The function $H \times T \rightarrow G, (h, t) \mapsto ht$ is a bijection.

Lemma 1.3.5. *Let G be a group and $U \leq G$. Let $\mathcal{A}$ be the set of transversals to U in G .*

- (a) G acts on $\mathcal{A}$ by right multiplication.
- (b) $N_G(U)$ acts on $\mathcal{A}$ by conjugation.
- (c) $N_G(U)^{\text{op}}$ acts on $\mathcal{A}$ by left multiplication.

Proof. Let $T \in \mathcal{A}$, $X \in G/U$, $g \in G$ and $h \in N_G(U)$.

(a): $|Tg \cap X| = |(Tg \cap X)g^{-1}| = |T \cap Xg^{-1}| = 1$, where the latter holds since Xg^{-1} is a coset of U and T is a transversal.

(b) Observe that X^h is a coset of U (indeed if $X = Uh$ then $X^h = U^h g^h = Ug^h$. So also $X^{h^{-1}}$ is a coset and $|T^h \cap X| = |(T^h \cap X)^{h^{-1}}| = |T \cap X^{h^{-1}}| = 1$.

(c) By (a) $Th \in \mathcal{A}$ and then by (b) $(Th)^{h^{-1}} \in \mathcal{A}$. As $(Th)^{h^{-1}} = hThh^{-1} = hT$, (c) holds. □

Lemma 1.3.6. *Let G be a group, $U \leq G$ and $H \leq U$. Let S be transversal to H in U and let T a transversal to U in G . Then ST is a transversal to H in G , and the function $S \times T \rightarrow ST$, $(s, t) \rightarrow (s, t)$ is a bijection.*

Proof. Since S and T are transversals, the functions

$$H \times S \rightarrow U, (h, s) \rightarrow hs, \quad \text{and} \quad U \times T \rightarrow G, (u, t) \rightarrow ut$$

are bijections. It follows that the function

$$H \times S \times T \rightarrow G, (h, s, t) \mapsto hst$$

is bijection. But then also the functions

$$S \times T \rightarrow ST, (s, t) \mapsto st, \quad \text{and} \quad H \times ST, (h, r) \mapsto hr$$

must be bijections. □

Lemma 1.3.7. *Let G be a group and $H, E, F \leq G$ with $E \leq F$.*

(a) *E is a supplement to H in G if and only if F is a supplement to H in G and E is a supplement to $H \cap F$ in F .*

(b) *E is a complement to H in G if and only if F is a supplement to H in G and E is a complement to $H \cap F$ in F .*

Proof. (a) Suppose $G = HE$. Since $E \leq F$ we get $G = HE \leq HF$ and so $G = HF$. Also $E \leq F \leq G = H$ and the modular gives $F = (H \cap F)E$.

Suppose that $G = HF$ and $F = (H \cap F)E$. Then $G = HF = H(H \cap F)E = HE$.

(b) Since $E \leq F$ we have $H \cap E = H \cap (F \cap E) = (H \cap F) \cap E$. Hence $H \cap E = 1$ if and only if $(H \cap F) \cap E = 1$. Together with (a) this gives (b). □

Lemma 1.3.8. *Let G be a group, and let $K, H, U \leq G$ with $H \leq U \leq G = HK$*

(a) *The function*

$$\alpha: G/U \rightarrow K/(U \cap K), \quad X \mapsto X \cap K$$

is a well defined bijection with inverse

$$\beta: K/U \cap K \rightarrow G/U, \quad Y \mapsto HY$$

(b) *Let $T \subseteq K$. Then T is a transversal to $U \cap K$ in K if and only if T is a transversal to U in G .*

Proof. All applications of 1.3.1 in this proof will be to G^{op} rather than G .

We will first show

(*) Let $k \in K$. Then $Uk \cap K = (U \cap K)k$.

Indeed, $\{k\} \subseteq K \leq G$ and so (1.3.1)(b) gives $U\{k\} \cap K = (U \cap K)\{k\}$.

(a) Let X be a coset of U in G and $g \in G$. Then $X = Ug$. Note that $H^{-1}X = HX \subseteq UX = UUg = Ug = X$ and so (1.3.1)(a) gives $X = X \cap HK = H(X \cap K)$. In particular, there exists $k \in X \cap K$. Since $k \in X$ and X is a coset of U , we get $X = Uk$. Thus $X \cap K = Uk \cap K \stackrel{(*)}{=} (U \cap K)k$. Hence $X \cap K$ is indeed a coset of $U \cap K$ in K , so α is well defined. Moreover, from $X = H(X \cap K)$ we see that $\alpha \circ \beta$ is the identity on G/U .

Now let $Y \in K/U \cap K$. Then $Y = (U \cap K)k$ with $k \in K$ and so $HY = H(U \cap K)k = Uk$. Thus KY is a coset of U in G , and β is well defined. Moreover,

$$HY \cap K = Uk \cap H \stackrel{(*)}{=} (U \cap K)y = Y$$

and so $\beta \circ \alpha$ is the identity on $K/U \cap K$. Hence β is an inverse of α and (a) is proved.

(b) T is a transversal to U in G if and only if $|T \cap X| = 1$ for all $X \in G/U$. Since $T \subseteq K$, this holds if and only if $T \cap (X \cap K) = 1$ for all $X \in G/U$. By (a), the latter is equivalent to $|T \cap Y| = 1$ for all $Y \in K/U \cap K$ and so equivalent to T being a transversal to $U \cap K$ in U . $\square$

Lemma 1.3.9. Let G be a group and let M, H, U be subgroups of G with $H' \leq M \leq H \leq U$. Let $\mathcal{A}$ be the set of transversals in G to U . Fix $Z \in \mathcal{A}$ and let $\mathcal{B}$ be the set of transversals $R \in \mathcal{A}$ with $R \subseteq HZ$. For $R, S \in \mathcal{B}$ define

$$(R|S) := \prod_{\substack{(r,s) \in R \times S \\ Ur = Us}} Mrs^{-1}$$

Then for all $R, S, T \in \mathcal{B}$,

- (a) $M \trianglelefteq H$ and H/M is abelian.
- (b) For each $r \in R$ there exists a unique $s \in S$ with $Ur = Us$.
- (c) Let $(r, s) \in R \times S$. Then $Ur = Us \iff rs^{-1} \in H \iff Hr = Hs$.
- (d) $R|S$ is an element of H/M and independent of the order of multiplication.
- (e) $(R|R) = M = 1_{H/M}$.
- (f) $(R|S)(S|T) = R|T$.
- (g) $(R|S)^{-1} = S|R$.
- (h) The relation $\sim$ on $\mathcal{B}$ defined by $R \sim S$ if $R|S = 1_{H/M}$ is an equivalence relation.

Proof. (a) Since $H' \leq M$, we have $[M, H] \leq M$ and so $M \trianglelefteq H$. Also $(H/M)' = H'M/M = M/M$ and so H/M is abelian.

(b) This holds since S is a transversal to R in S .

(c) Suppose $Ur = Us$. Since both R and S are contained in HZ there exist $h_1, h_2 \in H$ and $z_1, z_2 \in Z$ with $r = h_1z_1$ and $s = h_2z_1$. Note that $h_i \in H \subseteq U$. So $U = Uh_i$ and

$$Uz_1 = Uh_1z_1 = Ur = Us = Uh_2z_2 = Uz_2.$$

Since Z is a transversal to U , this implies $z_1 = z_2$. Thus

$$rs^{-1} = (h_1 z_1)(h_2 z_2)^{-1} = h_1(z_1 z_2^{-1})h_2^{-1} = h_1 h_2^{-1} \in H$$

If $rs^{-1} \in H$, then clearly $Ur = Us$. If $Ur = Us$, then also $Ur = UHr = UHs = Us$.

Now let $(r, s, t) \in R \times S \times T$ with $Ur = Us$ and $Us = Ut$.

(d) Since $Ur = Us$, (c) gives $rs^{-1} \in H$, so $R|S \in H/M$. Since H/M is abelian, the product is independent of the order of multiplication.

(e) Follows from $Ur = Ur$ and $rr^{-1} = 1$.

(f) Note that $Ur = Ut$, so t is the unique element of T with $Ur = Ut$. Also $(rs^{-1})(st^{-1}) = rt^{-1}$ and so (f) holds.

(g) From (f) and (e) we have $(R|S)(S|R) = (R|R) = 1_{H/M}$.

(h) By (e) $R|R = 1_{H/M}$, so $\sim$ is reflexive. If $R|S = 1_{H/M}$, then by (g),

$$(S|R) = (R|S)^{-1} = 1_{H/M}^{-1} = 1_{H/M}.$$

So $\sim$ is symmetric. If $R \sim S$ and $S \sim T$, then by (f),

$$R|T = (R|S)(S|T) = 1_{H/M} \cdot 1_{H/M} = 1_{H/M}$$

and so $\sim$ is transitive. □

Lemma 1.3.10. *Retain the notation from 1.3.9 except define*

$$R|S := \prod_{\substack{(r,s) \in R \times S \\ Ur = Us}} Mr^{-1}s$$

Assume in addition that $M = 1$, $H \trianglelefteq G$ and A is a complement to H in U . Let $R, S \in \mathcal{B}$ and $g \in G$.

(a) *If $(r, s) \in R \times S$ with $Ur = Us$, then $r^{-1}s \in H$.*

(b) *The conclusion of 1.3.9 hold with the new definition of $(R|S)$.*

(c) *There exists a unique $g^* \in HZ$ with $Ag = Ag^*$.*

For $D \subseteq G$ define $D^ := \{d^* \mid d \in D\}$ and for $D * g := (Rg)^*$.*

(c) *Let $D \in \mathcal{A}$. Then D^* is the unique element of $\mathcal{B}$ with $AD = AD^*$.*

(d)

$$* : \mathcal{B} \times G \rightarrow \mathcal{B}, \quad (R, g) \mapsto (Rg)^*$$

is a well-defined action of G on $\mathcal{B}$.

(e) *$(R * g|S * g) = (R|S)^g$. In particular, $\sim$ invariant is under the action of G on $\mathcal{B}$ via $*$.*

(f) *Suppose that $m := |G/U|$ is finite and let $h \in H$. Then $(R|S * h) = (R|S)h^m$. In particular, $R \sim (S * h)$ if and only if $h^m = (S|R)$.*

Proof. (a) Since $Ur = Us$, (1.3.9)(c) gives $Hr = Hs$. As $H \trianglelefteq G$ this implies $rH = sH$. Hence $r^{-1}s \in H$.

(b) In view of (a) the same arguments as in 1.3.9 now give (b).

(c) Since A is a complement to H in U , the function

$$A \times H \rightarrow U, \quad (a, h) \rightarrow ah$$

is a bijection. So H is transversal to A in U . As Z is a transversal to U in G , 1.3.6 shows that HZ is a transversal to A in G . This gives (c).

(c): Let $d \in D$. Then $Ad = Ad^*$ and so also $AD = AD^*$. From $Ad = Ad^*$ we get $UAd = UAd^*$, so $UD = UD^*$ and since D is a transversal to U in G , also D^* is a transversal to U in G . By definition of d^* we have $d^* \in HZ$, so also $D^* \subseteq HZ$ and $D^* \in \mathcal{B}$.

Suppose $AR = AS$. Then for each $r \in R$ there exist $s \in A$ with $r \in As$. Hence $Ar = As$. Note that $r \in R \subseteq HZ$, so $r^* = r$. Now also $s \in HZ$, so $r^* = s$. Hence $r = s \in S$. By symmetry $S \subseteq R$ and so $R = S$.

(d): We will first show that

(+) Let $D \in \mathcal{A}$. Then $D * g \in \mathcal{B}$ and $D * g = D^* * g$.

By 1.3.5 $Dg \in \mathcal{A}$ and so by (c) $(Dg)^* \in \mathcal{B}$, that is $D * g \in \mathcal{B}$. We compute

$$A(D * g) = A(Dg)^* \stackrel{(c)}{=} A(Dg) = (AD)g \stackrel{(c)}{=} (AD^*)g = A(D^*g) \stackrel{(c)}{=} A(D^*g)^* = A(D^* * g)$$

By (c) both $D * g$ and $D^* * g$ are in $\mathcal{B}$, and so the uniqueness assertion in (c) gives $D * g = D^* * g$. Thus (+) holds.

By (c) $R * g \in \mathcal{B}$, so the function in (d) is well-defined. Observe that $g^* = g$ for all $g \in HZ$, so also $R^* = R$. Hence $R * 1 = (R1)^* = R^* = R$. Also for $a, b \in G$.

$$(R * a) * b = (Ra)^* * b \stackrel{(+)}{=} Ra * b = ((Ra)b)^* = (R(ab))^* = R * (ab)$$

So $*$ is indeed an action of G on $\mathcal{B}$.

(e) Let $r \in R$, $s \in S$ and $g \in G$. Since $Ag = Ag^*$ we have $Ug = Ug^*$. Hence

$$Ur = Us \iff Urg = Usg \iff U(rg)^* = U(rs)^*$$

As $R * g = \{(rg)^* \mid r \in R\}$ this implies

$$(++) \quad (R * g \mid S * g) = \prod_{\substack{(\tilde{r}, \tilde{s}) \in (R * g, S * g) \\ U\tilde{r} = U\tilde{s}}} \tilde{r}^{-1} \tilde{s} = \prod_{\substack{(r, s) \in R \times S \\ Ur = Us}} ((rg)^*)^{-1} (sg)^*$$

Assume now that $Ur = Us$. Then by (a) $h := r^{-1}s \in H$. Note that $s = rh$. So

$$(+++) \quad Asg = Arhg = Argh^g = A(rg)^* h^g.$$

Since $H \trianglelefteq G$ we have $h^g \in H$ and $HZ = ZH$. Thus

$$(rg)^* h^g \in HZH = HHZ = HZ$$

and (+++) implies that $(sg)^* = (rg)^* h^g$ and so

$$((rg)^*)^{-1}(sg)^* = h^g = (r^{-1}s)^g$$

Substitution into $(++)$ gives

$$\begin{aligned} (R * g \mid S * g) &= \prod_{\substack{(r,s) \in R \times S \\ Ur = Us}} (r^{-1}s)^g \\ &= \left(\prod_{\substack{(r,s) \in R \times S \\ Ur = Us}} r^{-1}s \right)^g \\ &= (R|S)^g \end{aligned}$$

Thus (e) holds.

(f) Let $h \in H$. Then $Sh \subseteq HZH = HZ$ and so $S * h = (Sh)^* = Sh$. Also for $(r, s) \in R \times S$, $Ush = Uh^{s^{-1}}s = Us$ and so $Ur = Ush$ if and only if $Ur = Us$. Thus

$$\begin{aligned} (R \mid S * h) &= \prod_{\substack{(\tilde{r}, \tilde{s}) \in (R, S * h) \\ U\tilde{r} = U\tilde{s}}} \tilde{r}^{-1}\tilde{s} \\ &= \prod_{\substack{(r,s) \in R \times S \\ Ur = Us}} r^{-1}s h \\ &= \left(\prod_{\substack{(r,s) \in R \times S \\ Ur = Us}} r^{-1}s \right) h^m \\ &= (R|S)h^m \end{aligned}$$

□

Theorem 1.3.11 (Gaschütz). *Let G be a group, H an Abelian normal subgroup of G and $H \leq U \leq G$. Suppose that $m := |G/U|$ is finite and that one of the following holds:*

- (1) *H is finite and $\gcd(|H|, |G/U|) = 1$.*
- (2) *The function $H \rightarrow H, h \mapsto h^m$ is a bijection.*

Then

- (a) *There exists a complement to H in G if and only if there exists a complement to H in U .*
- (b) *Let K_1 and K_2 be complements of H in G . Then K_1 and K_2 are conjugate in G if and only if $K_1 \cap U$ and $K_2 \cap U$ are conjugate in U .*

Proof. Observe first, that if H is finite and $\gcd(|H|, |G/U|) = 1$, then $H \rightarrow H, h \mapsto h^m$ is a bijection. So in any case (2) holds.

(a) ' $\implies$ ': Let K be a complement to H in G . Then by 1.3.8, $K \cap U$ is a complement to H in U .

(b) ' $\implies$ ': Suppose K_1 and K_2 are conjugate in G . Then by (1.3.2)(c), $K_2 = K_1^h$ for some $h \in H$. Since $h \in U$ we get $(K_1 \cap U)^h = K_1^h \cap U^h = K_2 \cap U$ and so $K_1 \cap U$ and $K_2 \cap U$ are conjugate in U .

(a) ' $\Leftarrow$ ': Suppose that there exists a complement A to H in U . Define the set $\mathcal{B}$, the equivalence relation $\sim$ and the action $*$ of G on $\mathcal{B}$ as in 1.3.10. Then by (1.3.10)(f) $\sim$ is invariant under G . Hence Exercise 1 on Homework 1 shows that G acts on the set of equivalence class $\mathcal{B}/\sim$ via

$$\mathcal{B}/\sim \times G \rightarrow \mathcal{B}/\sim, \quad ([R], g) \mapsto [R * g]$$

Let $R, S \in \mathcal{B}$ and $h \in H$. Then (1.3.10)(f) shows that $R \sim S * h$ if and only if $h^m = (S | R)$. As $h \rightarrow h^m$ is a bijection there exists a unique such h . So for each R and S there exists a unique $h \in H$ with $[R] = [S * h]$, that is H acts regularly on $\mathcal{B}/\sim$. Now (1.1.11)(c) shows that $G_{[R]}$ is a complement to H in G .

(b) ' $\Leftarrow$ ': Let K_0 and K_1 be complements to H in G such that $K_0 \cap U$ is conjugate to $K_1 \cap U$ in U . Then $K_1 \cap U = (K_0 \cap U)^u = K_0^u \cap U$ for some $u \in U$.

If K_1 is conjugate to K_0^u in G , then K_1 is also conjugate to K_0 in G . So it suffices to show that K_1 and K_0^u are conjugate in G , and replacing K_0 by K_1 we may assume that $K_1 \cap U = K_0 \cap U$. Put $A = K_0 \cap U$. Then $A = K_i \cap U$ and A is a complement to H in U .

Let $i \in \{0, 1\}$. From (1.3.8)(b) we get:

(*) *Let $L_i \subseteq K_i$. Then L_i is a transversal to A in K_i if and only if L_i is a transversal to U in G .*

Let Z_0 be a transversal to A in K_0 . Since K_1 is a complement to H in G , we have $HK_1 = G$ and so for each $z \in Z$ there exists $k_z \in K_1$ with $Hk_z = K_1 k_z$. Put

$$Z_1 := \{k_z \mid z \in Z_0\}.$$

By (1.3.8)(b) Z_0 is also a transversal to U in G . So we can and will use the notation in 1.3.10 with $Z = Z_0$.

(**) *$Z_i \in \mathcal{B}$ and Z_i is a transversal to A in K_i .*

By choice Z_0 is a transversal to A in K_0 and as already seen, Z_0 is a transversal to U in G . As $Hk_z = Hk_z$ we also have $Uk_z = Uk_z$ and so, since Z_0 is a transversal, also Z_1 is a transversal to U in G . Hence (*) shows that Z_1 is a transversal to A in K_1 . Clearly $Z_0 \subseteq HZ_0$ and since $Hk_z = Hk_z \subseteq HZ_0$ also $Z_i \in HZ_0$. So $Z_i \in \mathcal{B}$.

(***) *Let R_i be transversal to A in K_i . Then $R_i^* = Z_i$*

As Z_i and R_i are transversals to A in K_i we have $AR_i = K_i = AZ_i$. By (*) $R_i \in \mathcal{A}$. Since $Z_i \in \mathcal{B}$, we conclude from (1.3.10)(c) that $Z_i = R_i^*$.

(+) *$K_i = G_{[Z_i]}$.*

Let $g \in K_i$. By (1.3.5)(a) $Z_i g$ is a transversal to A in K_i . Hence (***) shows that $(Z_i g)^* = Z_i$, that is $Z_i * g = Z_i$ and so $K_i \leq G_{[Z_i]}$. As H acts regularly on $\mathcal{B}/\sim$, we know from (1.1.11)(c) that $G_{[Z_i]}$ is a complement to H in G . The same is true for K_i and so (1.3.2)(b) shows that $K_i = G_{[Z_i]}$. Thus (+) holds.

Since H acts transitively on $\mathcal{B}/\sim$ there exists $h \in H$ with $[Z_0 * h] = [Z_1]$. Then

$$K_0^h = G_{[Z_0]}^h = G_{[Z_0 * h]} = G_{[Z_1]} = K_1.$$

and K_0 and K_1 are conjugate under G . □

Remark 1.3.12. In the proof of Gaschütz' Theorem a complement A to H in U is used to find a complement H to H in G . Then $K \cap U$ is a complement to U in H . But these operation are not inverse to each other, that is $K \cap U$ can be different from A and might not even be conjugate to A in U :

Take for example $G = G_1 \times G_2$, where $G_1 = \text{Sym}(4)$ and $G_2 = C_2$. Let $H = \langle (12)(34), (13)(24) \rangle \trianglelefteq G$, $U_1 = H \langle (12) \rangle \in \text{Syl}_2(G_1)$, $U = U_1 \times G_2 \in \text{Syl}_2(G)$ and $A = \langle ((12), 1), ((12)(34), g_2) \rangle$, where $1 \neq g_2 \in G_2$. Then A is a complement to H in U .

Let K be any complement to H in G . Then $K \cap HG_2$ is a complement to H in HG_2 and so has order 2. Since $HG_2 \trianglelefteq G$ we see that $K \cap HG_2$ is normal in K and so is contained in $Z(K)$. Note that HG_2 is abelian, so $K \cap HG_2 \leq Z(HG_2)$. As $KH = G$ we conclude that $K \cap HG_2 \leq Z(G) = G_2$. Thus $G_2 \leq U \cap K$ and since $G_2 \trianglelefteq G$, also $G_2 \leq (U \cap K)^g$ for any $g \in G$. But $G_2 \not\leq A$ and so $A \neq (U \cap K)^g$ for all $g \in G$.

Suppose now that we start with a complement K to H in G , then the proof of '(1.3.11)(b) $\implies$ ' shows that the complement to U in G constructed from the complement $K \cap U$ to H in U , is conjugate to K , as long as one choose the transversal Z to be contained in H .

Theorem 1.3.13 (Schur-Zassenhaus). Let G be a group and H an abelian normal subgroup of G . Suppose that $m := |G/H|$ is finite and that one of the following holds:

- (1) H is finite and $\gcd(|H|, |G/H|) = 1$.
- (2) The function $\alpha : H \rightarrow H, h \rightarrow h^m$ is a bijection.

Then there exists a complement to H in G and any two such complements are conjugate under H .

Proof. Note that the Hypothesis of 1.3.11 is fulfilled with $U = H$. Observe that 1 is a complement to H in U and so there exists a complement to H in G . If K_1 and K_2 are complements to H in G , then $U \cap K_1 = H \cap K_1 = 1 = Y \cap K_2$. So $U \cap K_1$ and $U \cap K_2$ are conjugate in U and we conclude that K_1 and K_2 are conjugate in G . Now (1.3.2)(c) shows that K_1 and K_2 are conjugate under H . $\square$

1.4 Frobenius Groups

Definition 1.4.1. Let G be group, H a subgroup of G and $H \subseteq G$. We say that G is a Frobenius group with complement H if

- (i) $1 \neq H \neq G$, and
- (ii) $H \cap H^g = 1$ for all $g \in G \setminus H$

In this case, the set

$$K_G(H) := G \setminus \bigcup H^{\sharp G} \quad (= \{g \in G \mid g \neq h^l \text{ for all } h \in H^{\sharp}, l \in G\})$$

is called the Frobenius kernel of G with respect to H .

Let G be a finite Frobenius group with complement H and kernel K . Using character theory, Frobenius proved that K is a subgroup of G . Later, H. Bender produced an elementary proof of Frobenius' Theorem, but only in the case where H has even order. The goal of this section is to present Bender's proof.

But first we will rephrase the group-theoretical concept of a Frobenius group in terms of permutation groups.

Definition 1.4.2. Let G be a group acting on a set Ω .

- (a) $K_G(\Omega)$ is the set of all $g \in G$ such that $\langle g \rangle$ acts semiregularly on Ω .

(b) We say that G is a Frobenius group on Ω if

- (i) $|\Omega| \geq 2$ and G acts transitively on Ω .
- (ii) G does not act regularly on Ω .
- (iii) For all $a \in \Omega$, G_a acts semiregularly on $\Omega \setminus \{a\}$.

Lemma 1.4.3. Let G be a group, $H \leq G$ and put $\Omega = G/H$.

- (a) G is a Frobenius group on Ω if and only if G is a Frobenius group with complement H .
- (b) $K_G^\#(H) = \{g \in G \mid C_\Omega(g) = \emptyset\}$.
- (c) If G is Frobenius group with complement H , then $K_G(\Omega) = K_G(H)$.

Proof. Note that

(*) Let $\omega \in \Omega$. Then $\omega = Hl$ for some $l \in G$ and $G_\omega = G_H^l = H^l$.

(a) We

$$|\Omega| \geq 2 \iff |G/H| \geq 2 \iff G \neq H$$

Observe that G acts transitively on Ω . Thus

$$\begin{aligned} & G \text{ does not act regularly on } \Omega. \\ \iff & G \text{ does not act semiregularly on } \Omega \\ \iff & G_\omega \neq 1 \text{ for } \omega \in \Omega \\ \stackrel{(*)}{\iff} & H \neq 1 \end{aligned}$$

Also

$$\begin{aligned} & G_\omega \text{ acts semiregularly on } \Omega \setminus \{\omega\} \\ \stackrel{(1.1.15)(a)}{\iff} & G_\omega \cap G_\mu = 1 \text{ for all } \mu \in \Omega \setminus \{\omega\} \\ \stackrel{(*)}{\iff} & H \cap H^g = 1 \text{ for all } g \in G \setminus H. \end{aligned}$$

(b) Let $g \in G$. Then

$$\begin{aligned} & g \in \bigcup H^G \\ \iff & g \in H^l \quad \text{for some } l \in G \\ \iff & g \in G_{Hl} \quad \text{for some } l \in G \\ \iff & Hl \in C_\Omega(g) \text{ for some } l \in G \\ \iff & C_\Omega(g) \neq \emptyset \end{aligned}$$

(c) Suppose G is a Frobenius group with complement H . Let $g \in G \setminus K_G(H)$. Then by (b) $C_\Omega(g) \neq \emptyset$. So there exists $\omega \in \Omega$ with $g \in G_\omega$. Thus $\langle g \rangle \cap G_\omega \neq 1$ and $\langle g \rangle$ does not act semiregularly on Ω . Hence $g \notin K_G(\Omega)$.

Now let $g \in G \setminus K_G(\Omega)$. Then $\langle g \rangle$ does not act semiregularly on Ω and so $\langle g \rangle \cap G_\omega \neq 1$ for some $\omega \in \Omega$. Hence $1 \neq g^n \in H^k$ for some $n \in \mathbb{Z}, k \in G$. It follows that

$$1 \neq g^n = (g^n)^g \in H^k \cap (H^k)^g = (H \cap H^{g^{k^{-1}}})^k$$

Hence $H \cap H^{g^{k^{-1}}} \neq 1$ and since G is a Frobenius group with complement H we get $g^{k^{-1}} \in H$. Thus $g \in H^k$ and so $g \notin K_G(H)$. $\square$

Lemma 1.4.4. *Let G be a Frobenius group with complement H and kernel K . Put $\Omega = G/H$.*

- (a) $1 \in K$, $K = K^{-1}$ and K is a normal subset of G .
- (b) Let $g \in G \setminus K$. Then $|C_\Omega(g)| = 1$, that is g has a unique fixed-point on Ω .
- (c) $N_G(H) = H$. In particular, $|H^G| = |G/H|$.
- (d) Let M be normal subset of G with $M \subseteq \bigcup H^{\sharp G}$. Then

$$|M| = |G/H| \cdot |M \cap H|$$

- (e) Suppose G is finite. Then $|\Omega| = |G/H| = |K|$ and $|K| \equiv 1 \pmod{|H|}$.

Proof. (a) This follows more or less directly from the definition of K .

(b) Since $g \notin K$ we have $g \neq 1$ and $g \in H^l$ for some $l \in G$. Thus g fixes Hl . Since $H^l (= G_{Hl})$ acts semiregularly on $\Omega \setminus \{Hl\}$ we see that Hl is the only fixed-point of g on Ω .

(c) Clearly $H \leq N_G(H)$. Suppose $g \notin H$, then $H \cap H^g = 1$. As $H \neq 1$ this gives $H \neq H^g$ and so $g \notin N_G(H)$. Thus $H = N_G(H)$. In particular,

$$|G/H| = |G/N_G(H)| = |H^G|.$$

(d) Let $g \in G$. Then $|M \cap H^g| = |(M \cap H^g)^{g^{-1}}| = |M^{g^{-1}} \cap H| = |M \cap H|$. Moreover, $H^g \cap H^l = 1$ for all $g, l \in G$ with $H^g \neq H^l$ and so $(M \cap H^g) \cap (M \cap H^l) = \emptyset$. Hence $\{M \cap L \mid L \in H^G\}$ is a partition of M into $|G/H|$ sets of size $|M \cap H|$. So (d) holds.

(e) Clearly $|\Omega| = |G/H|$. Since H acts semiregularly on $\Omega \setminus \{H\}$, all orbits of H on $\Omega \setminus \{H\}$ are regular and so have size $|H|$. Thus $|\Omega| \equiv 1 \pmod{|H|}$.

Put $M := \bigcup H^{\sharp G}$. Then $M \cap H = H^{\sharp}$ and (d) gives

$$|M| = |G/H| \cdot |M \cap H| = |G/H| \cdot |H^{\sharp}| = |G/H| \cdot (|H| - 1) = |G| - |G/H|$$

Hence

$$|K| = |G \setminus M| = |G| - |M| = |G| - (|G| - |G/H|) = |G/H|.$$

$\square$

Lemma 1.4.5. *Let G be a finite Frobenius group with complement H and kernel K .*

- (a) Let $U \leq G$. Then one of the following holds:

- (1) $H \cap U = 1$.
- (2) $U \leq H$.

(3) U is Frobenius groups with complement $U \cap H$ and kernel $U \cap K$.

(b) Let H_0 be any Frobenius complement of G . Then there exists $g \in G$ with $H^g \leq H_0$ or $H_0 \leq H^g$.

Proof. The proof is by induction on $|G|$.

(a) We may assume that $H \cap U \neq 1$ and $H \not\leq U$. Then $U \neq G$ and $H \cap U \neq U$. If $g \in U \setminus (U \cap H)$, then $g \notin H$ and so $(U \cap H) \cap (U \cap H)^g \leq H \cap H^g = 1$. Thus U is a Frobenius group with complement $U \cap H$ and kernel (say) $\tilde{K}$. Note that $(U \cap K) \cap (U \cap H)^g \leq K \cap H^g = 1$ for all $g \in U$ and so $U \cap K \subseteq \tilde{K}$. Let $u \in U \setminus (U \cap K)$. Then $u \in H^g$ for some $g \in G$. Since $u \neq 1$ we have $U \cap H^g \neq 1$. Suppose that $U \leq H^g$, then $1 \neq U \cap H \leq H^g$ and so $H = H^g$ and $U \leq H$, a contradiction. Hence $U \neq H^g$ and as seen above $U \cap H^g$ is a Frobenius complement of U . As $U \neq G$ we can apply (b) to U and conclude that there exists $v \in U$ with $U \cap H^g \leq (U \cap H)^v$ or $(U \cap H)^v \leq U \cap H^g$. In either case $H^g \cap H^v \neq 1$ and so $H^g = H^v$. Thus $u \in U \cap H^v = (U \cap H)^v$ and so $u \notin \tilde{K}$. Thus $\tilde{K} = U \cap K$ and (a) is proved.

(b) Let K_0 be Frobenius kernel of G with respect to H_0 . Interchanging H and H_0 if necessary we may assume that $|K_0| \leq |K|$.

Put $M := \bigcup H^{\sharp G}$. Then $M \cap K_0$ is a normal subset of G and (1.4.4)(d) shows that

$$|M \cap K_0| = |G/H| \cdot |M \cap K_0 \cap H| = |K| \cdot |K_0^{\sharp} \cap H|$$

As $|K_0| > |K_0^{\sharp}| \geq |M \cap K_0|$ this gives $|K_0| > |K| \cdot |K_0^{\sharp} \cap H|$. Since $|K_0| \leq |K|$ and $|K_0^{\sharp} \cap H|$ is non-negative integer this implies $|K_0^{\sharp} \cap H| = 0$, so $H \cap K_0 = 1$. It follows that $H \cap H_0^g \neq 1$ for some $g \in G$. As $H \cap K_0 = 1$ and H cannot be a Frobenius group with complement $H \cap H_0^g$ and kernel $H \cap K_0$. Also $H \cap H_0^g \neq 1$ and so (a) applied with (H, H_0^g) in place of (U, H) shows that $H \leq H_0^g$.

□

The following trivial observation will be very useful in Bender's proof of Frobenius' Theorem

Lemma 1.4.6. *Let G be a group and s, t elements of order 2 in G . Put $a := st$. Then*

$$a^s = a^t = ts = a^{-1}$$

Proof.

$$a^s = (st)^s = s^{-1}sts = ts = t^{-1}s^{-1} = (st)^{-1} = a^{-1}.$$

□

Theorem 1.4.7. *Let G be a finite Frobenius group with complement H and kernel K . Suppose H has even order. Then K is a normal subgroup of G , and G is the internal semidirect product of K by H .*

Proof. Since H has even order there exists $t \in H$ with $|t| = 2$. We will first show that

(*) $tt^g \in K^{\sharp}$ for all $g \in G \setminus H$.

Let $g \in G$ with $tt^g \notin K^{\sharp}$. We need to prove that $g \in H$. Put $a := tt^g$. If $a = 1$, then $1 \neq t^g = t^{-1} \in H \cap H^g$ and so $g \in H$. So we may assume that $a \neq 1$. Then $a \notin K$ and so there exists $x \in G$ with $a \in H^x$. Hence using 1.4.6

$$a^{-1} \stackrel{1.4.6}{=} a^t \in (H^x)^t = H^{xt}$$

Thus also $a \in H^{xt}$. Hence $1 \neq a \in H^x \cap H^{xt}$. It follows that $t \in H^x$. Thus $1 \neq t \in H \cap H^x$ and so $x \in H$ and $H = H^x$. By 1.4.6 $t^g t = a^{-1} \in H^x$, so the statement $t \in H^x$ applied with the roles of t and t^g interchanged gives $t^g \in H^x = H$. As $t \in H$ we also have $t^g \in H^g$, so $1 \neq t^g \in H \cap H^g$. Hence $g \in H$ and (*) is proved.

Let S be a transversal to H in G with $1 \in S$.

(**) Let $r, s \in S$. Then either $(r = s, t^r = t^s \text{ and } t^r t^s = 1)$ or $(r \neq s, t^r \neq t^s \text{ and } t^r t^s \in K^\sharp)$. In particular, $t^S t^S \subseteq K$ and $tt^S \subseteq K$.

Suppose first that $HS = Hr$. Since S is a transversal then $s = r$ and so $t^r t^s = (t^s)^2 = 1$.

Suppose next that $Hr \neq HS$. Then $sr^{-1} \notin H$ and $(*)$ gives $tt^{sr^{-1}} \in K^\sharp$. Since K is a normal subset of G we have $K^\sharp = K^{\sharp r}$ and so conjugation with r gives $t^r t^s \in K^\sharp$. Then $t^r t^s \neq 1$ and so also $t^r \neq (t^s)^{-1} = t^s$.

(***) $K = tt^S$.

Since $tt^S \subseteq K$ and K is finite we just need to show that $|tt^S| = |K|$. For this $r, s \in S$ with $tt^r = tt^s$. Then $t^s = t^r$ and $(**)$ implies that $r = s$. So $|tt^S| = |S|$. As $|S| = |G/H|$ and by (1.4.4)(e) $|G/H| = |K|$ we get $|tt^S| = |K|$ and $(***)$ holds.

(+) K is normal subgroup of G .

By (1.4.4)(a) we have $1 \in K$, $K = K^{-1}$ and K is a normal subset of G . So we only have to show that K is closed under multiplication:

$$KK = K^{-1}K \stackrel{(**)}{=} (tt^S)^{-1}(tt^S) = (t^S)^{-1}t^{-1}tt^S = t^S t t t^S = t^S t^S \stackrel{(***)}{\subseteq} K$$

Thus (+) is proved.

Note that $K \cap H = 1$ and $|KH| = |K||H| = |G/H||H| = |G|$. Thus $G = HK$ and so G is the internal semidirect product of K by H . $\square$

The next two lemmas will help to produce examples of Frobenius groups.

Lemma 1.4.8. *Let G be a group acting on a set Ω and N a normal subgroup of G acting regularly on Ω . Let $a \in \Omega$. The action of G_a on Ω is isomorphic to the action of G_a on N by conjugation, and the action of G_a on $\Omega \setminus \{a\}$ is isomorphic to the action of G_a on $N^\sharp$.*

Proof. Since N acts regularly on Ω , the function

$$\phi: N \rightarrow \Omega, \quad n \mapsto a^n$$

is a bijection. Let $g \in G_a$ and $n \in N$. Then $a^g = a$ and so also $a^{g^{-1}} = a$. Thus

$$(n^g)\phi = a^{g^{-1}ng} = (a^n)^g = (n\phi)^g$$

and so ϕ is G -equivariant. Observe that $1\phi = a$ and so the lemma holds. $\square$

Lemma 1.4.9. *Let G be the internal semidirect product of K by H . Suppose that $K \neq 1$ and $H \neq 1$. Put $\Omega = G/H$. Then*

- (a) K acts regularly in Ω . In particular, the action of H on $\Omega \setminus \{H\}$ is isomorphic to the action of H on $K^\sharp$ by conjugation.
- (b) $K_G^\sharp(H) = \{hk \mid h \in H, k \in K \setminus \{[h, l] \mid l \in K\}\}$.
- (c) $K \subseteq K_G(H)$.
- (d) $K = K_G(H)$ if and only if $K = \{[h, l] \mid l \in K\}$ for each $h \in H^\sharp$,
- (e) Let $h \in H$. Then $C_\Omega(h) = \{H\}$ if and only if $C_K(h) = 1$.

- (f) G is a Frobenius group with complement H if and only if $C_K(h) = 1$ for all $h \in H^\#$.
- (g) Suppose K is finite. Then G is a Frobenius group with complement H if and only if $K = K_G(H)$.
- (h) $K_G(H)$ is a subgroup of G if and only if $K = K_G(H)$.

Proof. (a) Since K is normal in G and $K \cap H = 1$ we have $K \cap H^g = 1$ for all $g \in G$ and so K acts semiregularly on Ω . Since $G = HK$, K acts transitively on Ω and so the first statement in (a) holds. The second now follows from 1.4.8

(b) Let $g \in G^\#$. Then $g = hk$ with $h \in H$ and $k \in K$. Note that $g \notin K_G(H)$ if and only if $g = a^r$ for some $a \in H^\#$ and $r \in G$. Let $a \in H$ and $r \in G$. Since K is a complement to H in G , there exist uniquely determined $b \in H$ and $l \in K$ with $r = bl$. We compute

$$a^r = a^{bl} = (a^b)^l = a^b(a^b)^{-1}l^{-1}a^bl = a^b[a^b, l]$$

Since $K \trianglelefteq G$ and $l \in K$ we have $[a^b, l] \in K$. Also $a^b \in H$. Thus

$$\begin{aligned} g &= a^r \\ \iff hk &= a^b[a^b, l] \\ \iff h &= a^b \text{ and } k = [a^b, l] \\ \iff a &= h^{b^{-1}} \text{ and } k = [h, l] \end{aligned}$$

Hence $g = a^r$ for some $a \in H$ and $r \in G$ if and only if there exists $l \in K$ with $k = [h, l]$. Indeed, if $k = [h, l]$ with $l \in K$ when $g = a^r$ where $r = h^{b^{-1}}l$ and b is any element of H .

It follows that $g = hk \in K_G(H)$ if and only if $k \neq [h, l]$ for all $l \in K$. Hence (b) holds.

(c) If $h = 1$, then $[h, l] = 1$ for all $l \in K$ and so (b) shows that $k = 1k \in K_G(H)$ for all $k \in K^\#$.

(d) $K_G(H) \subseteq K$ if and only if $hk \notin K_G(H)$ for all $h \in H^\#, k \in K$. By (b) this holds if and only if $K = \{[h, l] \mid l \in K\}$ for all $h \in H^\#$.

(e) By (a) the action of H on $\Omega \setminus H$ is isomorphic to the action of H on $K^\#$. This implies (e).

(f) By (1.4.3)(a) G is a Frobenius groups with complement H if and only if G is a Frobenius group on Ω . Since $K \neq 1$ we have $|\Omega| \geq 2$. Clearly G acts transitively on Ω and since $H \neq 1$, G does not act regularly on Ω . Thus G is a Frobenius group on Ω if and only if H acts semiregularly on $\Omega \setminus \{H\}$. This holds if and only if $C_{\Omega \setminus \{H\}}(h) = \emptyset$ for all $h \in H^\#$ and so by (e) if and only if $C_K(h) = 1$ for all $h \in H^\#$.

(g) Let $h \in H$. Then the function

$$K/C_K(h) \rightarrow \{[h, l] \mid l \in K\}, \quad C_K(h)l \mapsto [h, l]$$

is well-defined bijection. Thus $|K/C_K(h)| = |\{[h, l] \mid l \in K\}|$.

Since K is finite, we have $C_K(h) = 1$ iff $|K/C_K(h)| = |K|$, iff $|\{[h, l] \mid l \in K\}| = |K|$ and iff $\{[h, l] \mid l \in K\} = K$.

By (f) G is a Frobenius groups with complement H iff $C_K(h) = 1$ for all $h \in H^\#$. As just seen this holds if and only if $\{[h, l] \mid l \in K\} = K$ for all $h \in H^\#$, and so by (d) if and only if $K = K_G(H)$.

(h) Suppose that $K_G(H)$ is a subgroup of G . Since $K \leq K_G(H)$ and $G = HK$ we have $K_G(H) = (K_G(H) \cap H)K = 1K = K$. $\square$

Example 1.4.10. (a) Let K be a non-trivial abelian group with no elements of order 2. Let $h \in \text{Aut}(K)$ defined by $k^h = k^{-1}$ for all $k \in K$. Let $H = \langle h \rangle \leq \text{Aut}(K)$ and let G be the semidirect product of K by H . Let $k \in K$. Then $[h, k] = (k^{-1})^h k = k k = k^2$. Hence

$$C_K(h) = \{k \in K \mid k^2 = 1\} = 1 \quad \text{and} \quad \{[h, k] \mid k \in K\} = \{k^2 \mid k \in K\}.$$

Thus (1.4.9)(f) shows that G is a Frobenius group with complement H . Moreover, by (1.4.9)(h) $K_G(H)$ is a subgroup of G iff $K_G(H) = K$ and so by (1.4.9)(d) iff $K = \{[h, k] \mid k \in K\}$, that is iff $K = \{k^2 \mid k \in K\}$.

In particular, the infinite dihedral group is an example of a Frobenius group whose kernel not a subgroup.

- (b) Let $\mathbb{K}$ be a division ring with $|\mathbb{K}| \geq 2$. Let $K = (\mathbb{K}, +)$, $\mathbb{K}^\# = \mathbb{K} \setminus \{0\}$, $H = (\mathbb{K}^\#, \cdot)$ and $H^\# = H \setminus \{1\}$. Then H acts on K via right multiplication. Let $k \in K$ and $h \in H^\#$. Consider true equation $[h, k] = (k^{-1})^h k$ in a group with multiplicative notation. In our context this formula becomes

$$[h, k] = (-k)h + k = k(1 - h)$$

Since $1 - h \neq 0$ we see that $[h, k] = 0$ if and only if $k = 0$. So $C_K(h) = 0$ and (1.4.9)(e) shows that G is a Frobenius group with complement H . Moreover, since $1 - h \neq 0$, for each $l \in K$ there exists $k \in K$ with $l = k(1 - h) = [h, k]$. Hence (1.4.9)(d) gives $K = K_G(H)$. Thus $H \ltimes K$ is a Frobenius group with complement H and kernel K .

1.5 Imprimitve action

Definition 1.5.1. Let G be a group acting on a set Ω .

- (a) A system of imprimitivity for G on Ω is a G -invariant set $\mathcal{B}$ of non-empty subsets of Ω with $A = \biguplus \mathcal{B}$.
- (b) A set of imprimitivity for G on Ω is a non-empty subset B of Ω such that $B = B^g$ or $B \cap B^g = \emptyset$ for each $g \in G$.
- (c) A system of imprimitivity $\mathcal{B}$ for G on Ω is called proper if $\mathcal{B} \neq \{\Omega\}$ and $\mathcal{B} \neq \{\{\omega\} \mid \omega \in \Omega\}$.
- (d) A set of imprimitivity B is called proper if $|B| \geq 2$ and $B \neq \Omega$.
- (e) G acts primitively on G if there does not exist a proper system of imprimitivity for G on Ω

Lemma 1.5.2. Let G be a group acting on a set Ω .

- (a) Let $\mathcal{B}$ be a system of imprimitivity for G on Ω . Any member of $\mathcal{B}$ is a set of imprimitivity for G on Ω . Moreover, $\mathcal{B}$ is proper if and only if $\mathcal{B}$ contains a proper set of imprimitivity.
- (b) Let B be set of imprimitivity for G on Ω . Define

$$\mathcal{B} := \begin{cases} B^G & \text{if } \bigcup B^G = \Omega \\ B^G \cup \{\Omega \setminus \bigcup B^G\} & \text{otherwise.} \end{cases}$$

Then $\mathcal{B}$ is system of imprimitivity for G on Ω . Moreover, $\mathcal{B}$ is proper if and only if either B is proper or $|\Omega \setminus \bigcup B^G| \geq 2$.

(c) G acts primitively on Ω if and only if there does not exist a proper set of imprimitivity for G on Ω .

Proof. (a) Let $g \in G$. Then B, B^g both are contained in $\mathcal{B}$ and so either $B = B^g$ or $B \cap B^g = \emptyset$. Thus B is a set of imprimitivity. Observe $\mathcal{B} \neq \Omega$ iff $B \neq \Omega$ for all $B \in \mathcal{B}$ and iff $B \neq \Omega$ for some $B \in \mathcal{B}$. Also $\mathcal{B} \neq \{\{\omega\} \mid \omega \in \Omega\}$ if and only if $\mathcal{B}$ contains an element B with $|B| \geq 2$. Thus $\mathcal{B}$ is proper if and only if it contains an element B with $|B| \geq 2$ and $B \neq \Omega$.

(b) Clearly $\mathcal{B}$ is G invariant. Since $B = B^g$ or $B \cap B^g = \emptyset$ for all $g \in G$ we have $\Omega = \bigsqcup \mathcal{B}$. $\mathcal{B}$ is proper iff it contains a proper set of imprimitivity, iff B is proper or $\Omega \setminus \bigcup B^G$ is proper and iff B is proper or $|\Omega \setminus \bigcup B^G| \geq 2$.

(c) Suppose G is not imprimitive on Ω iff there exists a proper system of imprimitivity for G on Ω . By (a) and (b) this is the case if and only if there exists a proper set of imprimitivity for G on Ω . $\square$

Lemma 1.5.3. *Suppose G acts primitively on a set Ω . Then either G acts transitively on Ω or $|\Omega| = 2$ and G acts trivially on Ω .*

Proof. Suppose that G does not act transitively on Ω . Let O be an orbit for G on Ω . Then $O \neq \Omega$ and $\{O, \Omega \setminus O\}$ is system of imprimitivity for G on Ω . Since G acts primitively, $|O| = 1 = |\Omega \setminus O|$. Thus $|\Omega| = 2$ and G acts trivially on Ω . $\square$

Lemma 1.5.4. *Let G be a group acting transitively on Ω and let $\omega \in \Omega$. Then the function*

$$H \rightarrow \omega^H$$

is a bijection between the subgroups of G containing G_ω and the sets of imprimitivity of G on Ω containing ω , with inverse

$$\Delta \rightarrow N_G(\Delta).$$

Moreover, ω^H is a proper if and only if $G_\omega \subsetneq H \subsetneq G$.

Proof. Let $H \leq G$ with $G_\omega \leq H$. We will first show that ω^H is indeed a set of imprimitivity. For this let $g \in G$ with $\omega^H \cap \omega^{Hg} \neq \emptyset$. Then there exist $h_1, h_2 \in H$ with $\omega^{h_1} = \omega^{h_2g}$. Hence $h_2gh_1^{-1} \in G_\omega \leq H$ and so also $g \in H$. Thus $Hg = H$ and $\omega^{Hg} = \omega^H$.

Now let Δ be a set of imprimitivity with $\omega \in \Delta$. Let $g \in G_\omega$. Then $\omega = \omega^g \leq \Delta \cap \Delta^g$. Since Δ is a set of imprimitivity this gives $\Delta = \Delta^g$ and so $G_\omega \leq N_G(\Delta)$.

We showed that both of our functions are well-defined. Next we show that they are inverse to each other.

Clearly $H \leq N_G(\omega^H)$. Since $N_G(\omega^H)$ acts on ω^H and H acts transitively on ω^H , the Frattini argument gives $N_G(\omega^H) \leq G_\omega H = H$.

Clearly $\omega^{N_G(\Delta)} \subseteq \Delta$. Let $\mu \in \Delta$. Since G acts transitively on G , $\mu = \omega^g$ for some $g \in G$. Then $\mu = \omega^\epsilon \Delta \cap \Delta^g$ and so $\Delta = \Delta^g$ and $g \in N_G(\Delta)$ and $\mu \in \omega^{N_G(\Delta)}$. Hence $\omega^{N_G(\Delta)} = \Delta$.

We proved that the two functions are inverse to each other and so are bijection. The non-proper sets of imprimitivity containing ω are $\{\omega\}$ and Ω . Since $N_G(\{\omega\}) = G_\omega$ and $N_G(\Omega) = G$ we conclude that ω^H is proper if and only if $H \neq G_\omega$ and $H \neq G$. $\square$

Corollary 1.5.5. *Suppose G acts transitively on Ω and let $\omega \in \Omega$. Then G acts primitively on Ω iff G_ω is a maximal subgroup of G .*

Proof. Since G acts transitively on Ω there exists a proper set of imprimitivity for G on Ω iff there exists a proper set of imprimitivity containing ω . Thus G acts primitively on G if and only if $\{\omega\}$ and Ω are the only sets of imprimitivity containing ω . By 1.5.4, this holds iff G_ω and G are the only subgroups of G containing G_ω and so iff G_ω is a maximal subgroup of G . $\square$

Lemma 1.5.6. *Let G be a group and N a normal subgroup of G . The the set orbits of N on G is system of imprimitivity for G on Ω . This system is proper unless N acts transitively or trivially on Ω .*

Proof. Let O be an orbit for N on G . Let $\omega \in O$ and $g \in G$.

$$O^g = (\omega^N)^g = \omega^{Ng} = \omega^{gN} = (\omega^g)^N$$

and so O^g is an orbit for N on Ω . Thus the set of orbits of N on Ω is G -invariant. Ω is the disjoint union of these orbits and so the orbits indeed form a system of imprimitivity.

The system is proper unless one of the orbits is equal to Ω or all orbits have size 1. So unless N acts transitively on Ω or N acts trivially on Ω . $\square$

Corollary 1.5.7. *Let G be a group acting faithfully and primitively on a set Ω . Then all non-trivial normal subgroups of G act transitively on Ω .*

Proof. Let $1 \neq N \trianglelefteq G$. Since G acts primitively on Ω there does exists a proper system of primitivity for G on Ω . Hence 1.5.6 shows that N acts trivially or transitively on G . As G acts faithfully on G we know that N does not act trivially on Ω . $\square$

1.6 Wreath products

Definition 1.6.1. (a) *Let A and B be sets. Then A^B is the set of functions from B to A .*

(b) *Let H be a group and B a set. We view H^B as group via $b(fg) = (bf)(bg)$ for all $b \in B$ and $f, g \in H^B$.*

(c) *Let G be a group and $g \in G$. Then inn_g is the function*

$$\text{inn}_g : G \rightarrow G, \quad a \mapsto a^g$$

Lemma 1.6.2. *Let G be a group acting on set Ω and let H be a group. For $f \in H^\Omega$ and $g \in G$ define $f^g \in H^\Omega$ via $\omega f^g = \omega^{g^{-1}} f$ for all $\omega \in \Omega$.*

$$H^\Omega \times G \rightarrow H^\Omega, \quad (f, g) \rightarrow f^g$$

is an action of G on the group H^Ω .

Proof. Let $e, f \in H^\Omega$, $\omega \in \Omega$ and $g, h \in G$. Clearly $f^1 = f$. Also

$$\omega f^{gh} = \omega^{(gh)^{-1}} f = (\omega^{h^{-1}})^{g^{-1}} f = \omega^{h^{-1}} f^g = \omega (f^g)^h.$$

Hence $f^{gh} = (f^g)^h$ and G acts on H^Ω . Also

$$\omega (ef)^g = \omega^{g^{-1}} (ef) = (\omega^{g^{-1}} e)(\omega^{g^{-1}} f) = (\omega e^g)(\omega f^g) = \omega (e^g f^g)$$

Thus $(ef)^g = e^g f^g$ and so G acts on the group H^Ω . $\square$

Definition 1.6.3. *Let G be a group acting on set Ω and let H a group. Then $G \wr_\Omega H$ denotes the semidirect product of H^Ω by G with respect to the action defined in 1.6.2*

Lemma 1.6.4. *Let G be a group and H a subgroup of G . Put $\Omega = G/H$ and let S be a transversal to H in G . For $A \in \Omega$ let A_S be the unique element in $A \cap S$.*

(a) Let $g \in G$. Then

$$f_g: \Omega \rightarrow H, \quad A \mapsto (Ag^{-1})_S \cdot g \cdot A_S^{-1}$$

is a well-defined element of H^Ω .

(b)

$$\rho_S: G \rightarrow G \wr_\Omega H, \quad g \mapsto (g, f_g)$$

is a monomorphism of groups.

(c) Let T be a transversal to H in G . Then there exists $b \in G \wr_\Omega H$ with

$$\rho_T = \rho_S \circ \text{inn}_b.$$

Proof. (a) Let $A \in \Omega$. Note that $HA_S = A$. So $H = AA_S^{-1}$ and

$$H(Af_g) = H(Ag^{-1})_S \cdot g \cdot A_S^{-1} = Ag^{-1} \cdot g \cdot A_S^{-1} = AA_S^{-1} = H.$$

Hence $Af_g \in H$ and f_g is well-defined.

(b) Observe first that $G \wr_\Omega H$ is a subgroup of $G \wr_\Omega G$. For $g \in G$, define

$$c_g: \Omega \rightarrow G, \quad A \mapsto g.$$

Then $c_g \in G^\Omega$ and $c_g^h = c_g$ for all $g, h \in G$. It follows that the function

$$c: G \rightarrow G \wr_\Omega G, \quad g \mapsto (g, c_g)$$

is a monomorphism. Note that the function

$$\tau_S: \Omega \rightarrow G, \quad A \mapsto A_S$$

is an element of G^Ω . Write τ for τ_S . Then $(1, \tau)$ is an element of $G \wr_\Omega G$. Let $g \in G$. Then

$$(1, \tau)(g, c_g)(1, \tau)^{-1} = (g, \tau^g c_g)(1, \tau^{-1}) = (g, \tau^g c_g \tau^{-1})$$

and

$$A(\tau^g c_g \tau^{-1}) = A\tau^g \cdot Ac_g \cdot A\tau^{-1} = (Ag^{-1})_\tau \cdot g \cdot (A\tau)^{-1} = (Ag^{-1})_S \cdot g \cdot A_S^{-1} = Af_g$$

So $\tau^g c_g \tau^{-1} = f_g$ and

$$g\rho_S = (g, f_g) = (g, \tau^g c_g \tau^{-1}) = (1, \tau)(g, c_g)(1, \tau)^{-1} = (gc)^{(1, \tau^{-1})}$$

Hence

$$\rho_S = c \circ \text{inn}_{(1, \tau^{-1})}$$

Thus ρ_S is a monomorphism.

(c) We compute

$$\rho_T = c \circ \text{inn}_{(1, \tau_T^{-1})} = c \circ \text{inn}_{(1, \tau_S^{-1})} \circ \text{inn}_{(1, \tau_S)} \circ \text{inn}_{(1, \tau_T^{-1})} = \rho_S \circ \text{inn}_{(1, \tau_S \tau_T^{-1})}$$

Note that

$$H(A\tau_S) = HA_S = A = HA_T = H(A\tau_T)$$

and so

$$A(\tau_S \tau_T^{-1}) = A\tau_S \cdot (A\tau_T)^{-1} \in H$$

Hence $\tau_S \tau_T^{-1}$ is an element of H^Ω . Choosing $b = (1, \tau_S \tau_T^{-1}) \in G \wr_\Omega H$ we see that (c) holds. $\square$

Lemma 1.6.5. *Let G be a group acting on a group H and let Ω be a set such that G and H act on Ω . Suppose that for all $g \in G$, $h \in H$ and ω in Ω ,*

$$((\omega^{g^{-1}})^h)^g = \omega^{h^g}$$

Then $G \ltimes H$ acts on Ω via $\omega^{(g,h)} = (\omega^g)^h$.

Proof. Let $\omega \in \Omega$, $g, \tilde{g} \in G$ and $h, \tilde{h} \in H$.

We have

$$\omega^{(1,1)} = (\omega^1)^1 = \omega$$

and

$$(\omega^{(g,h)})^{(\tilde{g},\tilde{h})} = (((\omega^g)^h)^{\tilde{g}})^{\tilde{h}} = \left(\left(\left(((\omega^g)^{\tilde{g}})^{\tilde{g}^{-1}} \right)^h \right)^{\tilde{g}} \right)^{\tilde{h}} = \left(((\omega^g)^{\tilde{g}})^{h\tilde{g}} \right)^{\tilde{h}} = (\omega^{g\tilde{g}})^{h\tilde{g}\tilde{h}} = \omega^{(g\tilde{g},h\tilde{g}\tilde{h})} = \omega^{(g,h)(\tilde{g},\tilde{h})}$$

and the lemma is proved. $\square$

Lemma 1.6.6. *Let G be a group acting on set A and H a group acting on a set B . Then*

- (a) *G acts on $A \times B$ via $(a,b)^g = (a^g, b)$ and H^A acts on $A \times B$ via $(a,b)^f = (a, b^f)$.*
- (b) *$G \wr_A H$ acts on $A \times B$ via $(a,b)^{(g,f)} = (a^g, b^{a^g f})$.*
- (c) *$\{\{a\} \times B \mid a \in A\}$ is a system of imprimitivity for $G \wr_A H$ on $A \times B$.*

Proof. (a) Obvious.

(b) Let $a \in A, b \in B, g \in G$ and $f \in H^A$. Observe (with the action from (a))

$$((a,b)^g)^f = (a^g, b)^f = (a^g, b^{a^g f})$$

We just need to verify that the hypothesis of 1.6.5 holds for the actions of G and H^B on $A \times B$.

$$\left(((a,b)^{g^{-1}})^f \right)^g = ((a^{g^{-1}}, b)^f)^g = (a^{g^{-1}}, b^{a^{g^{-1}} f})^g = (a, b^{a^{g^{-1}} f})^g = (a, b^{a^g f}) = (a,b)^{f^g}$$

(c): Clearly $A \times B = \bigsqcup_{a \in A} \{a\} \times B$. Moreover for $g \in G$, $(a \times B)^g = a^g \times B$ and for $f \in H^\Omega$, $(a, B)^f = a \times B$. So $\{\{a\} \times B \mid a \in A\}$ is $G \wr_A H$ -invariant. $\square$

Lemma 1.6.7. *Let G be a group and H a subgroup of G . Suppose H acts on set B and put $A := G/H$. Let S be transversal to H in G and $a \in A$ and $g \in G$ let a_S and f_g be as in 1.6.4.*

- (a) *G acts on $A \times B$ via $(a,b)^g = (ag, b^{(ag)f_g})$.*
- (b) *$\{\{a\} \times B \mid a \in A\}$ is a system of imprimitivity for G on $A \times B$.*
- (c) *Let $a \in A, b \in B$ and $g \in G$. Then $(ag)_{f_g} = a_S \cdot g \cdot (ag)_S^{-1}$. In particular, $(a,b)^g = (ag, b^{a_S \cdot g \cdot (ag)_S^{-1}})$.*
- (d) *Put $\tilde{B} := \{H\} \times B$. Then $N_G(\tilde{B}) = H$ and $\tilde{B}$ is a set of imprimitivity for G on $A \times B$.*
- (e) *Put $k = H_S^{-1}$. The function $\lambda : B \rightarrow \tilde{B}, b \rightarrow (H, b^k)$ is an isomorphism of H -sets.*

Proof. (a) By 1.6.4 the function

$$G \rightarrow G \wr_A H. \quad g \rightarrow (g, f_g)$$

is a homomorphism and by (1.6.6)(b) $G \wr_A H$ acts on $A \times B$ via $(a, b)^{(g, f)} = (ag, b^{af})$. Hence (a) holds.

(b) By (1.6.6)(b) $\{\{a\} \times B \mid a \in A\}$ is a system of imprimitivity for $G \wr_A H$ and so also for G .

(c) $(ag)f_g = (agg^{-1})_S \cdot g \cdot (ag)_S$.

(d) As $\{\{a\} \times B \mid a \in A\}$ is a system of imprimitivity, $\{H\} \times B$ is set of imprimitivity for G on $A \times B$, see (1.5.2)(a). Observe that $(\{H\} \times B)^g = \{Hg\} \times B$. Thus $\tilde{B}^g = \tilde{B}$ iff $Hg = H$ and so iff $g \in H$. Hence $N_G(\tilde{B}) = H$.

(e) Put $k = h_S^{-1}$. Let $h \in H$. Then by (c)

$$(H, b)^h = (Hh, b^{H_S \cdot h \cdot (Hh)_S^{-1}}) = (H, b^{k^{-1}hk}) = (H, b^{hk})$$

Thus

$$(b\lambda)^h = (H, b^k)^h = (H, b^{kh^k}) = (H, b^{hk}) = (b^k)\lambda$$

and λ is an isomorphism of H -sets

□

Lemma 1.6.8. *Let G be a group acting on a set Ω , let H a subgroup of G acting on the set B and let $\sigma : B \rightarrow \Omega$ be a H -equivariant function. Put $A := G/H$. Let S be a transversal to H in G and for $a \in A$ let a_S be the unique element in $a \cap S$. Define an action of G on $A \times B$ and the function $\lambda B \rightarrow A \times B$ as in 1.6.7*

(a) *The function*

$$\epsilon : A \times B \rightarrow \Omega, \quad (a, b) \mapsto (b\sigma)^{a_S}$$

is the unique G -equivariant function from $A \times B$ to Ω with $\lambda \circ \epsilon = \sigma$.

(b) *Put $D := \text{Im } \sigma$. Then D is an H -invariant subset of Ω and $\text{Im } \epsilon = \bigcup D^G$.*

(c) *ϵ is injective if and only if each of the following hold: σ is injective, $H = N_G(D)$ and D is a set of imprimitivity for G on Ω .*

Proof. (a) Using (1.6.7)(c) we get

$$(a, b)^g \epsilon = (ag, b^{a_S \cdot g \cdot (ag)_S^{-1}}) \epsilon = \left((b^{a_S \cdot g \cdot (ag)_S^{-1}}) \sigma \right)^{(ag)_S} = \left((b\sigma)^{a_S \cdot g \cdot (ag)_S^{-1}} \right)^{(ag)_S} = (b\sigma)^{a_S g} = ((a, b)\epsilon)^g.$$

So ϵ is G -equivariant. Since $(b\lambda)\epsilon = (H, b^{H_S^{-1}})\epsilon = (b^{H_S^{-1}})^{H_S} \epsilon = b$, we have $\lambda \circ \epsilon = \sigma$.

Suppose now that $\mu : A \times B \rightarrow \Omega$ is G -equivariant with $\lambda \circ \mu = \sigma$. Then

$$(a, b)\mu = (Ha_S, (b^{H_S^{-1}})^{H_S \cdot a_S \cdot (Ha_S)_S^{-1}})\mu = (H, b^{H_S^{-1}})^{a_S} \mu = (b\lambda)^{a_S} \mu = ((b\lambda)\mu)^{a_S} = (b\sigma)^{a_S}.$$

(b) Since S is a transversal to H in G we have $G = HS$. As D is H -invariant this implies that $D^G = D^{AS} = D^S = \{D^{a_S} \mid a \in A\}$. Also

$$\text{Im } \epsilon = \{(a, b)\epsilon \mid (a, b) \in A \times B\} = \{(b\sigma)^{a_S} \mid b \in B, a \in A\} = \{d^{a_S} \mid d \in D, a \in A\} = \bigcup \{D^{a_S} \mid a \in A\} = \bigcup D^G.$$

(c) Suppose first that ϵ is injective. Since λ is injective we conclude that $\lambda \circ \epsilon$ is injective, that is σ is injective.

Let $g \in G$ with $D \cap D^g \neq \emptyset$. Put $a = Hg$. Since D is H -invariant we get $D^{Hs} \cap D^{as} \neq \emptyset$. Hence there exists $b, \tilde{b} \in B$ with $(b\sigma)^{Hs} = (\tilde{b}\sigma)^{as}$. Thus $(H, b)\epsilon = (a, \tilde{b})\epsilon$. As ϵ is injective we get $H = a$. Thus $g \in H$ and so $D = D^g$. In particular, D is a set of imprimitivity for G on Ω . Also if $g \in N_G(D)$, then $D \cap D^g = D \neq \emptyset$ and so $g \in H$. Thus $N_G(D) = H$.

Suppose next that σ is injective, $H = N_G(D)$ and D is a set of imprimitivity for G on Ω . Let $(a, b), (\tilde{a}, \tilde{b}) \in A \times B$ with $(a, b)\epsilon = (\tilde{a}, \tilde{b})\epsilon$. Then

$$(b\sigma)^{as} = (\tilde{b}\sigma)^{\tilde{a}s} \in D^{as} \cap D^{\tilde{a}s}.$$

Then $D \cap D^{\tilde{a}s a_s^{-1}} \neq \emptyset$. Since D is a set of imprimitivity this implies $D = D^{\tilde{a}s a_s^{-1}}$. Thus $\tilde{a}_s a_s^{-1} \in N_G(B) = H$. This gives $H a_s = H \tilde{a}_s$ and so $a = \tilde{a}$. Hence

$$(b\sigma)^{as} = (\tilde{b}\sigma)^{\tilde{a}s} = (\tilde{b}\sigma)^{as}$$

and so also $b\sigma = \tilde{b}\sigma$. As σ is injective we get $b = \tilde{b}$. Thus $(a, b) = (\tilde{a}, \tilde{b})$ and ϵ is injective. $\square$

1.7 Multi-transitive action

Definition 1.7.1. (a) Let Ω be a set and $n \in \mathbb{Z}^+$. Then $\Omega_{\neq}^n = \{(\omega_1, \omega_2, \dots, \omega_n) \in \Omega^n \mid \omega_i \neq \omega_j \text{ for all } 1 \leq i < j \leq n\}$.

(b) Let G be a group acting on a set Ω and $n \in \mathbb{Z}^+$ with $n \leq |\Omega|$. We say that G acts n -transitively on Ω if G acts transitively on $\Omega_{\neq}^n$. (Note here that G acts on Ω^n via $(\omega_1, \omega_2, \dots, \omega_n)^g = (\omega_1^g, \dots, \omega_n^g)$ and $\Omega_{\neq}^n$ is an G -invariant subset of Ω^n).

(c) Let Ω be a set, $n \in \mathbb{N}$ and $\omega = (\omega_1, \dots, \omega_n) \in \Omega^n$. Then $\underline{\omega} = \{\omega_1, \omega_2, \dots, \omega_n\}$.

Lemma 1.7.2. Let G be a group acting on a finite set Ω . Then G acts $|\Omega|$ -transitively on Ω if and only if $G^{\bullet\Omega} = \text{Sym}(\Omega)$.

Proof. Let $\omega, \mu \in \Omega_{\neq}^n$. Then there exists exactly one element $\pi \in \text{Sym}(\Omega)$ with $\omega\pi = \mu$. So $\text{Sym}(\Omega)$ acts $|\Omega|$ -transitively. Conversely suppose G acts $|\Omega|$ -transitively on Ω and let $\pi \in \text{Sym}(\Omega)$. Then there exists $g \in G$ with $\omega^g = \omega\pi$ and so the image of g in $\text{Sym}(\Omega)$ is π . Thus $G^{\bullet\Omega} = \text{Sym}(\Omega)$. $\square$

Example 1.7.3. Let $\mathbb{K}$ be a division ring and V a non-zero vector space over $\mathbb{K}$. Let $\text{GL}_{\mathbb{K}}(V)$ be the group of $\mathbb{K}$ -linear automorphism of V .

- (a) $\text{GL}_{\mathbb{K}}(V)$ acts transitively on $V^{\#}$.
- (b) If $|\mathbb{K}| = 2$ and $\dim_{\mathbb{K}} V \geq 2$, then $\text{GL}_{\mathbb{K}}(V)$ acts 2-transitively on $V^{\#}$.
- (c) If $|\mathbb{K}| = 2$ and $\dim_{\mathbb{K}} V = 2$ then $\text{GL}_{\mathbb{K}}(V)$ acts 3-transitively on $V^{\#}$.
- (d) If $|\mathbb{K}| = 3$ and $\dim_{\mathbb{K}} V = 1$, then $\text{GL}_{\mathbb{K}}(V)$ acts 2-transitively on $V^{\#}$.
- (e) If $\dim_{\mathbb{K}}(V) \geq 2$, then $\text{GL}_{\mathbb{K}}(V)$ acts 2-transitively on the set of 1-dimensional subspace of V .

Lemma 1.7.4. Let $n \in \mathbb{Z}^+$ and G group acting n -transitively on a set Ω .

- (a) G acts m -transitively on Ω for all $1 \leq m \leq n$.
- (b) Let $m \in \mathbb{Z}^+$ with $n + m \leq |\Omega|$ and $\omega \in \Omega_{\neq}^n$. Then G acts $n + m$ -transitively on Ω if and only if G_{ω} acts m -transitively on $\Omega \setminus \underline{\omega}$.

Proof. (a) is obvious.

(b) Define a relation $\sim$ between $\Omega_{\#}^n$ and $\Omega_{\#}^m$ by

$$\omega \sim \mu \iff \underline{\omega} \cap \underline{\mu} = \emptyset$$

Observe that $\sim$ is G -invariant,

$$G_{\#}^{m+n} = \{(\omega, \mu) \mid \omega \in \Omega_{\#}^n, \mu \in \Omega_{\#}^m, \omega \sim \mu\}$$

and, for $\omega \in \Omega_{\#}^n$,

$$(G \setminus \underline{\omega})_{\#}^m = \{\mu \in \Omega_{\#}^m \mid \omega \sim \mu\}$$

Since G acts n -transitively on Ω it acts transitively on $\Omega_{\#}^n$. Now Exercise 7 on Homework 2 shows that G acts transitively on $\{(\omega, \mu) \mid \omega \in \Omega_{\#}^n, \mu \in \Omega_{\#}^m, \omega \sim \mu\}$ if and only if G_{ω} acts transitively on $\{\mu \in \Omega_{\#}^m \mid \omega \sim \mu\}$. It follows that G acts transitively on $G_{\#}^{m+n}$ if and only if G_{ω} acts transitively on $(\Omega \setminus \underline{\omega})_{\#}^m$. So (b) holds $\square$

Lemma 1.7.5. *Let G be the internal semidirect product of K by H . Put $\Omega = G/H$ and let $n \in \mathbb{Z}^+$ with $n < |\Omega|$. Then G acts $n+1$ transitively on Ω if and only if H acts n -transitively on $K^{\#}$.*

Proof. Observe that G acts 1-transitively on Ω . Let $\omega = H \in G/H$. Then $G_{\omega} = h$. Hence by 1.7.4 G acts $n+1$ -transitively on Ω if and only if H acts n -transitively on $\Omega \setminus \{H\}$. By (1.4.9)(a), the action of H on $\Omega \setminus \{H\}$ is isomorphic to the action of H on $K^{\#}$. So the lemma holds. $\square$

Example 1.7.6. Let $\mathbb{K}$ be a field and V a non-zero vector space over $\mathbb{K}$. Let G be the external semidirect product of V by $\text{GL}_{\mathbb{K}}(V)$ and let $\Omega = G/H \times \{1\}$. Then

- (a) G acts 2-transitively on Ω .
- (b) If $|\mathbb{K}| = 2$, then G acts 3-transitively on Ω .
- (c) If $|\mathbb{K}| = 2$ and $\dim_{\mathbb{K}} V = 2$, then G acts 4-transitively on Ω .
- (d) If $|\mathbb{K}| = 3$ and $\dim_{\mathbb{K}} V = 1$, then G acts 3-transitively on Ω .

Proof. This follows from 1.7.3 and 1.7.5. $\square$

Note that in (1.7.6)(c), $|\Omega| = |V| = 4$. Since G acts 4-transitively on Ω we conclude from 1.7.2 that $G \cong \text{Sym}(4)$. So $\text{Sym}(4)$ is isomorphic to the external semidirect product of $\mathbb{F}_2^2$ by $\text{GL}_{\mathbb{F}_2}(\mathbb{F}_2^2)$.

Lemma 1.7.7. *Let $n \in \mathbb{Z}^+$ and G a group acting n -transitively on a finite set Ω . Suppose there exists a normal subgroup N of G acting regularly on Ω . Then $n \leq 4$ and one of the following holds.*

- (1) $n = 1$.
- (2) $n = 2$ and N is an elementary abelian p -group for some prime p .
- (3) $n = 3$ and N is an elementary abelian 2-group.
- (4) $n = |N| = |\Omega| = 3$, N is cyclic and $G^{\bullet\Omega} = \text{Sym}(\Omega) \cong \text{Sym}(3)$.
- (5) $n = |N| = |\Omega| = 4$, N is elementary abelian and $G^{\bullet\Omega} = \text{Sym}(\Omega) \cong \text{Sym}(4)$.

Proof. We may assume that $n \geq 2$. Let $\omega \in \Omega$. As N acts regularly on Ω , 1.1.11 shows that G_ω is complement to N in G . This G is the internal semidirect product of N by G_ω and so as G acts $n - 1$ -transitively on Ω we conclude from 1.7.5 that G_ω acts $n - 1$ -transitively on $N^\#$.

Let p be a prime divisor of $|N|$. Since G_ω acts transitively on $N^\#$ and N has an element of order p , all non-trivial elements of N have order p . Thus N is a p -group and so $Z(N) \neq 1$. Since $Z(N)^\#$ is invariant under G_ω we conclude that $N = Z(N)$ and so N is an elementary abelian p -group. Since N acts regularly on Ω we have $|\Omega| = |N|$.

If $n = 2$ we conclude that (2) holds and if $n = 3$ and $p = 2$, (3) holds. So it remains to consider the cases $n \geq 3$ and p is odd and $n \geq 4$ and p is even.

Suppose $n \geq 3$ and p is odd. Then $C_{G_\omega}(x)$ acts transitively on $N^\# \setminus \{x\}$. Since $x^{-1} \in N^\# \setminus \{x\}$ and $C_{G_\omega}(x)$ fixes x^{-1} we get $N^\# \setminus \{x\} = \{x^{-1}\}$. Thus $N = \{1, x, x^{-1}\}$, $|\Omega| = |N| = 3$ and $n = 3$. By 1.7.2, $G^{\bullet\Omega} = \text{Sym}(\Omega)$ and (4) holds.

Suppose next that $n \geq 4$ and $p = 2$. Let $y \in N \setminus \langle x \rangle$. Then $xy \in N^\# \setminus \{x, y\}$ and $C_{G_\Omega}(\{x, y\})$ acts transitively on $N^\# \setminus \{x, y\}$. Since $C_{G_\Omega}(\{x, y\})$ fixes xy , this implies that $N^\# \setminus \{x, y\} = \{xy\}$. Thus $|\Omega| = |N| = 4$. So also $n = 4$ and by 1.7.2, $G^{\bullet\Omega} = \text{Sym}(\Omega)$. Hence (5) holds in this case. $\square$

Chapter 2

Hypercentral and Hypocentral Groups

2.1 Hypercentral Groups

Lemma 2.1.1. *Let G be a group and a, b, c in G . Then*

$$(a) \quad [a, b] = a^{-1}a^b, \quad a^b = a[a, b] \quad \text{and} \quad ab = ba[a, b]$$

$$(b) \quad [b, a] = [a, b]^{-1} = [a^{-1}, b]^a = [a, b^{-1}]^b.$$

$$(c) \quad [a, bc] = [a, c][a, b]^c.$$

$$(d) \quad [ab, c] = [a, c]^b[b, c]$$

$$(e) \quad [a, b^{-1}, c]^b[b, c^{-1}, a]^c[c, a^{-1}, b]^a = 1$$

Proof. (a) follows immediately from $[a, b] = a^{-1}b^{-1}ab$ and $a^b = b^{-1}ab$.

(b)

$$[b, a] = b^{-1}a^{-1}ba = (a^{-1}b^{-1}ab)^{-1} = [a, b]^{-1},$$

and

$$[a^{-1}, b]^a = a^{-1}(ab^{-1}a^{-1}b)a = b^{-1}a^{-1}ba = [b, a]$$

, Taking inverses on both sides of the last equation and using the formula $[a, b]^{-1} = [b, a]$ gives

$$[b, a^{-1}]^a = [a, b]$$

So switching a and b completes the proof of (b).

$$(c) \quad [a, c][a, b]^c = (a^{-1}c^{-1}ac)c^{-1}(a^{-1}b^{-1}ab)c = a^{-1}c^{-1}b^{-1}abc = [a, bc].$$

$$(d) \quad \text{Take the inverse on both sides of (c) and use the formula } [a, b]^{-1} = [b, a].$$

(e)

$$[a, b^{-1}, c]^b = [a^{-1}bab^{-1}, c]^b = (ba^{-1}b^{-1}ac^{-1}a^{-1}bab^{-1}c)^b = (a^{-1}b^{-1}ac^{-1}a^{-1})(bab^{-1}cb) = (aca^{-1}ba)^{-1}(bab^{-1}cb)$$

Put $x = aca^{-1}ba$, $y = bab^{-1}cb$ and $z = bab^{-1}cb$. Then

$$[a, b^{-1}, c]^b = x^{-1}y$$

Cyclicly permuting a , b and c gives

$$[b, c^{-1}, a]^c = y^{-1}z$$

and

$$[c, a^{-1}, b]^a = z^{-1}x$$

Since $(x^{-1}y)(y^{-1}z)(z^{-1}x) = 1$, (e) holds. □

Lemma 2.1.2. *Let G be a group and let A and B subsets of G .*

- (a) $\langle A^B \rangle = \langle \langle A \rangle^B \rangle$.
- (b) $[A, B] = [B, A]$.
- (c) If $1 \in B$, then $\langle A^B \rangle = \langle A, [A, B] \rangle$.
- (d) If A is a subgroup of G , then $A \leq N_G([A, B])$ and $[A, B] = [A, B^A]$.
- (e) Suppose A is a subgroup of G and $1 \in B$. Then $[A, B] \trianglelefteq A[A, B] = \langle A^B \rangle$
- (f) Suppose A is a subgroup of G . Then $B \leq N_G(A)$ if and only if $[A, B][A, B^{-1}] \leq A$.
- (g) $[\langle A \rangle, B] = \langle [A, B]^{\langle A \rangle} \rangle$.
- (h) $[\langle A \rangle, \langle B \rangle] = \langle [A, B]^{\langle A \rangle \langle B \rangle} \rangle$.
- (i) If A and B are A -invariant, then $[\langle A \rangle, B] = [A, B]$.
- (j) If $a \in G$ with $B^a = B$, then $[a, B] = [\langle a \rangle, B]$.
- (k) $[A, G] = [\langle A^G \rangle, G]$.
- (l) Suppose A and B are subgroups of G . Then $[A, B] \trianglelefteq \langle A, B \rangle = AB[A, B]$ and $[A, B] = [\langle A^B \rangle, B] = [A, \langle B^A \rangle] = [\langle A^B \rangle, \langle B^A \rangle]$.

Proof. Let $a \in A$ and $b, c \in B$.

(a) Clearly $\langle A^B \rangle \leq \langle \langle A \rangle^B \rangle$. Note that $\langle A \rangle^b = \langle A^b \rangle \leq \langle A^B \rangle$ and so $\langle \langle A \rangle^B \rangle \leq \langle A^B \rangle$. Thus (a) holds.

(b) Follows from $[a, b]^{-1} = [b, a]$.

(c) Since $a^b = a[a, b] \in \langle A, [A, B] \rangle$ we get $\langle A^B \rangle \leq \langle A, [A, B] \rangle$. As $1 \in B$ we have $a = a^1 \in \langle A^B \rangle$ and so also $[a, b] = a^{-1}a^b \in \langle A^B \rangle$. Thus $\langle A, [A, B] \rangle \leq \langle A^B \rangle$ and (c) holds.

(d) Let $d \in A$. By (2.1.1)(b), $[ad, b] = [a, b]^d[d, b]$ and so $[a, b]^d = [ad, b][d, b]^{-1} \in [A, B]$. Thus $A \subseteq N_G([A, B])$. So the first statement in (d) holds. In particular, $[A, B^a] = [A^a, B^a] = [A, B]^a = [A, B]$ and so $[A, B^A] = [A, B]$ and also the second statement in (d) is proved.

(e) By (d) $A \leq N_G([A, B])$. It follows that $A[A, B]$ is a subgroup of G and

$$[A, B] \trianglelefteq A[A, B] = \langle A, [A, B] \rangle$$

By (c) $\langle A^B \rangle = \langle A, [A, B] \rangle$ and so (e) holds.

(f) Observe that $A^b \subseteq A$ iff $a^b \in A$ for all $a \in A$, iff $a^{-1}a^b \in A$ for all $a \in A$, iff $[a, b] \in A$ for all $a \in A$ and iff $[A, b] \in B$. Also $A^b = A$ iff $A^b \subseteq A$ and $A \subseteq A^{b^{-1}}$, iff $A^b \subseteq A$ and $A^{b^{-1}} \subseteq A$, iff $[A, b] \leq A$ and $[A, b^{-1}] \leq A$. Thus $B \leq N_G(A)$ if and only if $[A, B][A, B^{-1}] \leq A$.

(g) Put $H := \langle [A, B]^{\langle A \rangle} \rangle$. By (e) $\langle A \rangle$ normalizes $[\langle A \rangle, B]$. Since $[A, B] \leq [\langle A \rangle, B]$ we conclude that $H \leq [\langle A \rangle, B]$. Define $D := \{d \in \langle A \rangle \mid [d, B] \leq H\}$. We will show that D is a subgroup of G . Let $d, e \in D$ and b in D . Observe that $\langle A \rangle$ normalizes H . Thus

$$[de, b] = [d, b]^e [e, b] \in H \text{ and } [d^{-1}, b] = ([d, b]^{-1})^{d^{-1}} \in H$$

Hence $de \in D$ and $d^{-1} \in D$. Thus D is a subgroup of G . Since $A \subseteq D \leq \langle A \rangle$, this gives $D = \langle A \rangle$ and so $[\langle A \rangle, B] \leq H$.

(h)

$$[\langle A \rangle, \langle B \rangle] \stackrel{(g)}{=} \langle [\langle A \rangle, B]^{\langle B \rangle} \rangle \stackrel{(g)}{=} \langle \langle [A, B]^{\langle A \rangle} \rangle^{\langle B \rangle} \rangle \stackrel{(a)}{=} \langle [A, B]^{\langle A \rangle \langle B \rangle} \rangle$$

(i) Suppose A and B are A -invariant. Then $[A, B]$ is A -invariant and so also $\langle A \rangle$ -invariant. Thus (i) gives $[\langle A \rangle, B] = \langle [A, B]^{\langle A \rangle} \rangle = [A, B]$.

(j) Follows from (i) applied to $A = \{a\}$.

(h) By (d) $[A, G] = [A^G, G]$. Since G and A^G are A^G -invariant, (i) gives $[A^G, G] = [\langle A^G \rangle, G]$.

(l) By (d) A and B normalizes $[A, B]$. Hence $[A, B] \trianglelefteq \langle A, B \rangle$. By (e) $\langle A^B \rangle = A[A, B]$ and $\langle B^A \rangle = B[A, B]$. Thus $\langle A, B \rangle = \langle A^B \rangle \langle B^A \rangle = A[A, B]B[A, B] = AB[A, B]$.

By (d) $[A, B] = [A, \langle B^A \rangle]$ and so by (g)

$$[A, \langle B^A \rangle] = [A, B^A]^{\langle B^A \rangle} = \langle [A, B]^{\langle B^A \rangle} \rangle$$

Since $[A, B] \trianglelefteq \langle A, B \rangle$ we have $\langle [A, B]^{\langle B^A \rangle} \rangle = \langle [A, B] \rangle = [A, B]$. Thus $[A, \langle B^A \rangle] = [A, B]$. By symmetry $[\langle A^B \rangle, B] = [A, B]$. Observe that $\langle A^B \rangle \trianglelefteq \langle A, B \rangle$. So $\langle A^B \rangle = \langle A^{\langle B^A \rangle} \rangle$ and thus

$$[A, B] = [A, \langle B^A \rangle] = [\langle A^{\langle B^A \rangle} \rangle, \langle B^A \rangle] = [\langle A^B \rangle, \langle B^A \rangle]$$

□

Lemma 2.1.3 (Three Subgroup Lemma). (a) Let G be a group, $N \trianglelefteq G$ and A, B and C subsets of G . Suppose that

$$[[A, B^{-1}], C] \leq N \quad \text{and} \quad [[B, C^{-1}], D] \leq N$$

Then

$$[[C, A^{-1}], B] \leq N$$

(b) Let G be a group and A, B and C subgroups of G with

$$[[A, B], C] = 1 \quad \text{and} \quad [[B, C], A] = 1$$

Then

$$[[C, B], A]$$

Proof. (a) Let $a \in A, b \in B$ and $c \in C$. By (2.1.1)(e)

$$[[a, b^{-1}], c]^b [[b, c^{-1}], a]^c [[c, a^{-1}], b]^a = 1$$

By hypothesis $[[a, b^{-1}], c] \in N$ and $[[b, c^{-1}], a] \in N$. Since $N \trianglelefteq G$ also

$$[[a, b^{-1}], c]^b \in N \quad \text{and} \quad [[b, c^{-1}], a]^c \in N$$

It follows that $[[c, a^{-1}], b]^a \in N$ and since $N \trianglelefteq G$ also $[[c, a^{-1}], b] \in N$.

Put $D = \{[c, a^{-1}] \mid c \in C, a \in A\}$. Then $[d, b] \in N$ for all $d \in D, b \in B$. Hence also $[D, B] \leq N$. Now (2.1.2)(g) gives

$$[\langle D \rangle, B] = \langle [D, B] \rangle \leq \langle N^G \rangle = N$$

Note that $\langle D \rangle = [C, A^{-1}]$ and so indeed $[[C, A^{-1}], B] \leq N$.

(a) Note that $E = E^{-1}$ for any subgroup E of G . Thus (b) follows from (a) applied with $N = 1$. $\square$

Definition 2.1.4. Let G be a group and $A \leq G$. Then $Z(G, A) := \{g \in G \mid [G, g] \leq A\}$.

Note that by (2.1.2)(h), $Z(G, A)$ is a normal subgroup of G .

Lemma 2.1.5. Let G be a group and $A \leq G$.

(a) $Z(G, A) \trianglelefteq G$.

(b) $Z(G, A) = \{g \in G \mid Agh = Ahg \text{ for all } h \in G\}$.

(c) Put $B := \bigcap A^G$. Then $Z(G, A) = Z(G, B)$ and $Z(G, A)/B = Z(G/B)$.

Proof. (a) By (2.1.2)(k)

$$[\langle Z(G, A)^G \rangle, G] = [Z(G, A), G] \leq A$$

Thus $\langle Z(G, A)^G \rangle \leq Z(G, A)$ and so $Z(G, A) \trianglelefteq G$.

(b) By (2.1.2)(j), $[G, g] = [G, \langle g \rangle] = [G, g^{-1}]$. Hence $g \in Z(G, A)$ iff $[G, g] \leq A$, iff $[G, g^{-1}] \leq A$ iff $[h^{-1}, g^{-1}] \in A$ for all $h \in G$, iff $hgh^{-1}g^{-1} \in A$ for all $h \in G$, and iff $Ahg = Agh$ for all $h \in G$.

(c) Observe that a normal subgroup of G is contained in A if and only if it is contained in B . By (2.1.2)(d) $G \leq N_G([G, g])$. Hence $[G, g] \leq A$ if and only if $[G, g] \leq B$. Thus $Z(G, A) = Z(G, B)$. Also $[h, g] \in B$ if and only if $[h, g]B = B$ and so if and only if (in G/B), $[hB, gB] = 1_{G/B}$. It follows that $g \in Z(G, B)$ if and only if $[G/B, gB] = 1_{G/B}$ and so if and only if $gB \in Z(G/B)$. $\square$

Lemma 2.1.6. Let G be a group and $A \leq B \leq G$.

(a) $Z(G, A) \leq Z(G, B)$.

(b) $Z(G, A) \leq N_G(A)$.

(c) If $A \trianglelefteq G$, then $Z(G, B)/A = Z(G/A, B/A)$

Proof. (a): $[Z(G, A), G] \leq A \leq B$.

(b) $[Z(G, A), A] \leq [Z(G, A), G] \leq A$.

(c) $[g, h] \in B$ if and only if $[g, h]A \subseteq B$ and if and only if (in G/A) $[gA, hA] \in B/A$. $\square$

Definition 2.1.7. Let G be a group and α an ordinal. Define the groups $Z_\alpha(G)$ and $L_\alpha(G)$ inductively via

$$Z_\alpha(G) = \begin{cases} 1 & \text{if } \alpha = 0 \\ Z(G, Z_\beta(G)) & \text{if } \alpha = \beta + 1 \text{ for some ordinal } \beta \\ \bigcup_{\beta < \alpha} Z_\beta(G) & \text{if } \alpha \text{ is a limit ordinal} \end{cases}$$

and

$$L_\alpha(G) = \begin{cases} G & \text{if } \alpha = 0 \\ [L_\beta(G), G] & \text{if } \alpha = \beta + 1 \text{ for some ordinal } \beta \\ \bigcap_{\beta \in \alpha} L_\beta(G) & \text{if } \beta \text{ is a limit ordinal} \end{cases}$$

Let z_G be the smallest ordinal α with $Z_\alpha(G) = Z_{\alpha+1}(G)$ and l_G be smallest ordinal α with $L_\alpha(G) = L_{\alpha+1}(G)$. Put $Z_*(G) = Z_{z_G}(G)$ and $L_*(G) = L_{l_G}(G)$. $Z_*(G)$ is called the hypercenter of G and $L_*(G)$ the hypocenter of G .

G is called hypercentral of class z_G if $G = Z_*(G)$ and G is called hypocentral of class l_G if $L_*(G) = 1$.

Example 2.1.8. The hypercenter and hypocenter of D_{2^∞} .

For $k \in \mathbb{N}$ let C_{p^k} be a cyclic group of order p^k and view C_{p^k} has a subgroup of $C_{p^{k+1}}$. Put $C_{p^\infty} = \bigcup_{k=0}^\infty C_{p^k}$. (C_{p^∞} is called the Prüfer group for the prime p . Let $t \in \text{Aut}(C_{p^\infty})$ be defined by $x^t = x^{-1}$ for all $x \in C_{p^\infty}$. Let $D_{p^\infty} = \langle t \rangle \ltimes C_{p^\infty}$.

Observe that for $k \in \mathbb{N} \cup \{\infty\}$, C_{p^k} is a normal subgroup of D_{p^∞} . If k is finite, $D_{p^\infty}/C_{p^k} \cong D_{p^\infty}$. Also $D_{p^\infty}/C_{p^\infty} \cong C_2$.

We will now compute $Z_\alpha(D_{2^\infty})$. Since C_{2^∞} is abelian and t does not centralize C_{2^∞} we have $C_{D_{2^\infty}}(C_\infty) = C_{2^\infty}$. Thus $Z(D_{2^\infty}) \leq C_{2^\infty}$ and $Z(D_{2^\infty}) = C_{C_{2^\infty}}(t)$. $x \in C_{2^\infty}$ is centralized by t if and only if $x^t = x^{-1} = x$ and so iff $x^2 = 1$. Thus $Z(C_{2^\infty}) = C_2$. Let $k \in \mathbb{N}$ and suppose inductively that $Z_k(C_{2^\infty}) = C_{2^k}$. Since $D_{2^\infty}/C_{2^k} \cong D_{2^\infty}$ we get

$$Z(D_{2^\infty}/C_{2^k}) = C_{2^{k+1}}/C_{2^k}$$

and so $Z_{k+1}(C_{2^\infty}) = C_{2^{k+1}}$. Thus

$$Z_{\mathbb{N}}(D_{2^\infty}) = \bigcup_{k \in \mathbb{N}} Z_k(D_{2^\infty}) = \bigcup_{k \in \mathbb{N}} C_{2^k} = C_{2^\infty}$$

Since $D_{2^\infty}/C_{2^\infty}$ is isomorphic to C_2 and so is abelian, we conclude that $Z_{\mathbb{N}+1}(D_{2^\infty}) = D_{2^\infty}$ and so D_{2^∞} is hypercentral of class $\mathbb{N} + 1$.

Since $D_{2^\infty}/C_{2^\infty}$ is abelian, $L_1(D_{2^\infty}) \leq C_{2^\infty}$. Let $x \in C_{2^\infty}$. Then $[x, t] = x^{-1}x^t = x^{-2}$. Since each element of C_{2^k} is the square of an element in $C_{2^{k+1}}$ we conclude that $C_{2^\infty} = [C_{2^\infty}, t] = [C_{2^\infty}, D_{2^\infty}] \leq L_1(D_{2^\infty})$. Thus $L_1(D_{2^\infty}) = C_{2^\infty}$ and

$$L_2(D_{2^\infty}) = [C_{2^\infty}, D_{2^\infty}] = C_{2^\infty} = L_1(D_{2^\infty})$$

So C_{2^∞} is the hypocenter of D_{2^∞} and D_{2^∞} is not hypocentral.

Lemma 2.1.9. Let G be a group and H a subgroup of G with $Z_*(G) \not\leq H$. Let α be the smallest ordinal with $Z_\alpha(G) \not\leq H$. Then $Z_\alpha(G) \leq Z(G, H)$. In particular, $Z(G, H) \not\leq H$ and $H \not\leq N_G(H)$.

Proof. Since $Z_0(G) = 1 \leq H$, we have $\alpha \neq 0$. If α is a limit ordinal, then $Z_\alpha(G) = \bigcup_{\beta < \alpha} Z_\beta(G) \leq H$, a contradiction. Thus $\alpha = \beta + 1$ for some ordinal β . Then $Z_\beta(G) \leq H$ by minimality of α and so

$$Z_\alpha(G) = Z(G, Z_\beta(G)) \leq Z(G, H)$$

□

Lemma 2.1.10. Let G be a group and N a non-trivial normal subgroup of G with $N \leq Z_*(G)$. Then $N \cap Z(G) \neq 1$.

Proof. Since $N \cap Z_*(G) = N \neq 1$ there exists an ordinal α minimal with $N \cap Z_\alpha(G) \neq 1$. Since $Z_0(G) \cap N = 1 \cap N = 1$, $\alpha \neq 0$. If α is a limit ordinal, then $Z_\alpha(G) \cap N = \bigcup_{\beta < \alpha} Z_\beta(G) \cap N = 1$, a contradiction. Thus $\alpha = \beta + 1$ for some ordinal β . Then

$$[Z_\alpha(G) \cap N, G] \leq Z_\beta \cap N = 1$$

and so $Z_\alpha(G) \cap N \leq Z(G)$. □

Lemma 2.1.11. *Let G be a group. Then the following are equivalent:*

- (a) G is hypercentral.
- (b) $Z(G, H) \not\leq H$ for all $H \not\leq G$.
- (c) $Z(G/N) \neq 1$ for all $N \trianglelefteq G$ with $N \neq G$.

Proof. (a) $\implies$ (b): Suppose G is hypercentral and $H \not\leq G$. Then $Z_*(G) = G \not\leq H$ and so by 2.1.9, $Z(G, H) \not\leq H$.

(b) $\implies$ (c): Follows from $Z(G/N) = Z(G, N)/N$.

(c) $\implies$ (a): Let $\alpha = z_G$. Then $Z(G/Z_\alpha(G)) = Z_{\alpha+1}(G)/Z_\alpha(G) = 1$ and so (c) implies that $Z_\alpha(G) = G$. □

Lemma 2.1.12. *Let G be a group and α an ordinal.*

- (a) Let $H \leq G$. Then $Z_\alpha(G) \cap H \leq Z_\alpha(H)$.
- (b) Let $N \trianglelefteq G$. Then $Z_\alpha(G)N/N \leq Z_\alpha(G/N)$.
- (c) Let β be an ordinal. Then $Z_\alpha(G/Z_\beta(G)) = Z_{\beta+\alpha}(G)/Z_\beta(G)$.

Proof. In each case we assume inductively that the statement holds for all ordinals less than α . Note also that all three statements hold for $\alpha = 0$. So we assume that $\alpha \neq 0$.

(a) Suppose $\alpha = \beta + 1$ for some ordinal β . By induction $Z_\beta(G) \cap H \leq Z_\beta(H)$ and by definition $Z_\alpha(G) = Z(G, Z_\beta(G))$ and so $[Z_\alpha(G), G] \leq Z_\beta(G)$. Thus

$$[Z_\alpha(G) \cap H, H] \leq [Z_\alpha(G), G] \cap H \leq Z_\beta(G) \cap H \leq Z_\beta(H)$$

and so $Z_\alpha(G) \cap H \leq Z_\alpha(H)$.

Suppose α is limit ordinal.

$$\begin{aligned} Z_\alpha(G) \cap H &= \left(\bigcup_{\beta \in \alpha} Z_\beta \right) \cap H && \text{-- definition of } Z_\alpha(G) \\ &= \bigcup_{\beta \in \alpha} Z_\beta(G) \cap H \\ &\leq \bigcup_{\beta \in \alpha} Z_\beta(H) && \text{-- by induction} \\ &= Z_\alpha(H) && \text{-- definition of } Z_\alpha(H) \end{aligned}$$

(b) Suppose $\alpha = \beta + 1$ for some ordinal β . By induction $Z_\beta(G)N/N \leq Z_\beta(G/N)$. So

$$[Z_\alpha(G)N/N, G] = [Z_\alpha(G), G]N/N \leq Z_\beta(G)N/N \leq Z_\beta(G/N)$$

and so $Z_\alpha(G)N/N \leq Z_\alpha(G/N)$.

Suppose α is limit ordinal. Then

$$Z_\alpha(G)N/N = \left(\bigcup_{\beta \in \alpha} Z_\beta\right)N/N = \bigcup_{\beta \in \alpha} Z_\beta(G)N/N \leq \bigcup_{\beta \in \alpha} Z_\beta(G/N) = Z_\alpha(G/N)$$

(c) Suppose $\alpha = \gamma + 1$ for some ordinal γ . Then

$$\begin{aligned} Z_{\beta+\alpha}(G)/Z_\beta(G) &= Z_{\beta+(\gamma+1)}/Z_\beta(G) \\ &= Z_{(\beta+\gamma)+1}(G)/Z_\beta(G) && \text{-- definition of } \beta + (\gamma + 1) \\ &= Z(G, Z_{\beta+\gamma}(G))/Z_\beta(G) && \text{-- definition of } Z_{(\beta+\gamma)+1}(G) \\ &= Z(G/Z_\beta(G), Z_{\beta+\gamma}(G)/Z_\beta(G)) && \text{-- (2.1.6)(c)} \\ &= Z(G/Z_\beta(G), Z_\gamma(G/Z_\beta(G))) && \text{-- by induction} \\ &= Z_{\gamma+1}(G/Z_\beta(G)) && \text{-- definition of } Z_{\gamma+1} \\ &= Z_\alpha(G/Z_\beta(G)) \end{aligned}$$

Suppose α is a limit ordinal. Then by (A.1.11)(c) also $\beta + \alpha$ is limit ordinal. We compute

$$\begin{aligned} Z_\alpha(G/Z_\beta(G)) &= \bigcup_{\gamma \in \alpha} Z_\gamma(G/Z_\beta(G)) && \text{-- definition of } Z_\alpha \\ &= \bigcup_{\gamma \in \alpha} Z_{\beta+\gamma}(G)/Z_\beta(G) && \text{-- by induction} \\ &= \bigcup_{\beta \leq \rho \in \beta+\alpha} Z_\rho(G)/Z_\beta(G) && \text{-- (A.1.11)(b)} \\ &= \left(\bigcup_{\beta \leq \rho \in \beta+\alpha} Z_\rho(G) \right) / Z_\beta(G) \\ &= \left(\bigcup_{\rho \in \beta+\alpha} Z_\rho(G) \right) / Z_\beta(G) && \text{-- } Z_\rho(G) \leq Z_\beta(G) \text{ for all } \rho \in \beta \\ &= Z_{\beta+\alpha}(G)/Z_\beta(G) && \text{-- definition of } Z_{\beta+\alpha} \end{aligned}$$

□

Corollary 2.1.13. *Let G be a hypercentral group of class α . Then all sections of G are hypercentral of class at most α .*

Proof. Let A be a section of G , that is $A = H/N$ where $H \leq G$ and $N \trianglelefteq H$. Then $H = H \cap G = H \cap Z_\alpha(G) \leq Z_\alpha(H)$ and so H is hypercentral of class at most α . Thus $A = H/N = Z_\alpha(H)/N = Z_\alpha(H/N)$ and A is hypercentral of class at most α . □

Lemma 2.1.14. *Let G be a hypercentral group and M a maximal subgroup of G . Then $M \trianglelefteq G$ and $G/M \cong C_p$ for some prime p .*

Proof. By 2.1.9 $M \not\leq N_G(M)$. Since M is a maximal subgroups, $N_G(M) = G$. So $M \trianglelefteq G$. Since M is a maximal subgroups of G , G/M has no proper subgroups. Thus $G/M \cong C_p$ for some prime p . □

Lemma 2.1.15. *Let G be a hypercentral group and A a maximal abelian normal subgroup of G . Then $C_G(A) = A$.*

Proof. Since A is abelian, $A \leq C_G(A)$. Suppose that $A < C_G(A)$. Then $C_G(A)/A$ is a non-trivial normal subgroup of the hypercentral group G/A . Thus by 2.1.10

$$Z(G/A) \cap C_G(A)/A \neq 1$$

Hence there exists $b \in C_G(A) \setminus A$ with $bA \in Z(G/Z)$. Then $[b, G] \leq A$ and it follows that $A\langle b \rangle$ is an abelian normal subgroup of G , a contradiction to maximality of A . $\square$

Definition 2.1.16. *Let A and B be subsets of a group G and α an ordinal. Define $[A, B; \alpha]$ inductively via*

$$[A, B; \alpha] = \begin{cases} \langle A^B \rangle & \text{if } \alpha = 0 \\ [[A, B; \beta], B] & \text{if } \alpha = \beta + 1 \text{ for some ordinal } \beta \\ \bigcap_{\beta \in \alpha} [A, B; \beta] & \text{if } \beta \text{ is a limit ordinal} \end{cases}$$

Remark 2.1.17. *Let G be group and $A, B \leq G$.*

- (a) *Let α be an ordinal. Then $[G, G; \alpha] = L_\alpha(G)$.*
- (b) *$[A, B; 1] = [A, B]$.*
- (c) *Let $n \in \mathbb{N}$. Then*

$$[A, B; n] = [\underbrace{[\dots [[A, B], B], \dots], B}_{n\text{-times}}] \quad \text{and} \quad [A, B; n+1] = [[A, B], B; n]$$

Lemma 2.1.18. *Let $n \in \mathbb{N}$, G a group and $H \leq G$. Then $H \leq Z_n(G)$ if and only if $[H, G; n] = 1$.*

Proof. If $n = 0$ both statements say that $H = 1$. Suppose inductively that for all $A \leq G$: $A \leq Z_n(G)$ if and only if $[A, G; n] = 1$. Then

$$H \leq Z_{n+1}(G) \text{ iff } [H, G] \leq Z_n(G) \text{ iff } [[H, G], G; n] = 1 \text{ and iff } [H, G; n+1] = 1. \quad \square$$

Corollary 2.1.19. *Let G be a group and $n \in \mathbb{N}$. Then $G = Z_n(G)$ if and only if $L_n(G) = 1$.*

Proof. We have $G = Z_n(G)$ iff $[G, G; n] = 1$ iff $L_n(G) = 1$. $\square$

Definition 2.1.20. *Let G be a group. G is called nilpotent if $G = Z_n(G)$ for some $n \in \mathbb{N}$. If G is nilpotent the smallest $n \in \mathbb{N}$ with $G = Z_n(G)$ is called the nilpotency class of G .*

Corollary 2.1.21. *Let G be a group and $n \in \mathbb{N}$.*

- (a) *G is nilpotent of class n if and only if G is hypercentral of class n and if and only if G is hypocentral of class n .*
- (b) *Suppose G is nilpotent of class n . Then all sections of G are nilpotent of class at most n .*

Proof. (a): The definition of nilpotent and hypercentral shows that G is nilpotent of class n if and only if G is hypercentral of class n . By 2.1.19 $G = Z_n(G)$ if and only if $L_n(G) = 1$. So G is hypercentral of class n if and only if G is hypocentral of class n .

(b) By (a) G is hypercentral of class n . Hence by 2.1.13 all section of G are hypercentral of class at most n , and so by (a) all section of G are nilpotent of class at most n . $\square$

Lemma 2.1.22. *Let G be group and N normal in G .*

- (a) *Let α and β be ordinals such that $N \leq Z_\alpha(G)$ and G/N is hypercentral of class at most β . Then G is hypercentral of class at most $\alpha + \beta$.*
- (b) *G is hypercentral if and only if $N \leq Z_*(G)$ and G/N is hypercentral.*
- (c) *G is nilpotent if and only if G/N is nilpotent and $N \leq Z_n(G)$ for some $n \in \mathbb{N}$*

Proof. (a) Note that $G/Z_\alpha(G) \cong G/N/Z_\alpha(H)/N$ and so by 2.1.13 $G/Z_\alpha(G)$ is hypercentral of class at most β . Thus

$$G/Z_\alpha(G) = Z_\beta(G/Z_\alpha(G)) \stackrel{(2.1.12)(c)}{=} Z_{\alpha+\beta}(G)/Z_\beta(G)$$

It follows that $G = Z_{\alpha+\beta}(G)$ and (a) holds.

(b) If G is hypercentral, then $N \leq G = Z_*(G)$ and by 2.1.13 G/N is hypercentral.

Now suppose that $N \leq Z_*(G)$ and G/N is hypercentral. Then by (a) shows that G is hypercentral of class at most $z_G + z_{G/N}$.

(c) If G is nilpotent, then $G = Z_n(G)$ for some $n \in \mathbb{N}$. Thus $N \leq Z_n(G)$ and G/N is nilpotent.

If $N \leq Z_n(G)$ and G/N is nilpotent of class m , then by (a), G is hypercentral of class at most $n + m$. Thus G is nilpotent. $\square$

Lemma 2.1.23. *Let $(G_i)_{i \in I}$ be a family of groups and put $G = \times_{i \in I} G_i$.*

- (a) *Let α be an ordinal. Then $Z_\alpha(G) = \times_{i \in I} Z_\alpha(G_i)$.*
- (b) *$z_G = \bigcup_{i \in I} z_{G_i}$.*
- (c) *$Z_*(G) = \times_{i \in I} Z_*(G_i)$.*
- (d) *G is hypercentral if and only if each G_i is hypercentral.*
- (e) *G is nilpotent if and only if each G_i is nilpotent and $\bigcup_{i \in I} z_{G_i}$ is finite.*

Proof. (a) Follows from $Z(G) = \times_{i \in I} Z(G_i)$ and induction on α .

(b) and (c) follows from (a).

(d) follows from (c).

(e) Follows from (d) and (b). $\square$

Definition 2.1.24. *Let π be a set of positive prime integers and G a group.*

- (a) *$\pi(G)$ is the set of prime divisors of order of the elements of finite order in G .*
- (b) *G is called a π -group if all elements of G have finite order and $\pi(G) \subseteq \pi$.*
- (c) *$O_\pi(G)$ is the largest normal π -subgroup of G . ($O_\pi(G)$ exists by Exercise 1 on Homework 4).*
- (d) *π' is the set of all positive primes integers which are not contained in π .*

Lemma 2.1.25. *Let p be a prime and G a finite p -group. Then G is nilpotent.*

Proof. Let $N \triangleleft G$ with $N \neq G$. Then G/N is a non-trivial p -group and so $Z(G/N) \neq 1$. Thus by 2.1.11, G is hypercentral. Since G is finite, z_G is finite and so G is nilpotent. $\square$

Lemma 2.1.26. *Let G be a finite group. Then the following are equivalent:*

- (a) G is nilpotent.
- (b) $H \not\leq N_G(H)$ for all $H \not\leq G$.
- (c) All Sylow subgroups of G are normal in G .
- (d) $G = \times_{p \in \pi(G)} O_p(G)$.
- (e) $G = \times_{i=1}^n G_i$, where G_i is a p_i -subgroup for a prime p_i .

Proof. (a) $\implies$ (b): Since G is nilpotent, then $G = Z_*(G)$ and so $H \not\leq N_G(H)$ by 2.1.9.

(b) $\implies$ (c): Let p be a prime and S be a Sylow p -subgroup of G . Put $H = N_G(S)$ and $L = N_G(H)$. Then $S \in \text{Syl}_p(H)$ and $H \trianglelefteq L$. The Frattini argument gives

$$N_G(H) = L = HN_L(S) = H(N_G(S) \cap L) = H(H \cap L) = H$$

If (b) holds we conclude that $G = H = N_G(S)$ and so $S \trianglelefteq G$.

(c) $\implies$ (d): Suppose all Sylow subgroups of G are normal in G . For each $p \in \pi(G)$ choose $S_p \in \text{Syl}_p(G)$. Then $S_p \trianglelefteq G$ and so $S_p \leq O_p(G)$. As S_p is a maximal p -subgroup of G this gives $O_p(G) = S_p$. Define

$$K_p := \langle O_r(G) \mid r \in \pi(G) \setminus \{p\} \rangle, \quad \text{and} \quad K = \langle O_p(G) \mid p \in \pi(G) \rangle$$

Note that

$$[O_p(G), O_{p'}(G)] \leq O_p(G) \cap O_{p'}(G) = 1 \quad \text{and} \quad K_p \leq O_{p'}(G)$$

Thus $[O_p(G), K_p] = 1 = O_p(G) \cap K_p = 1$ and so

$$K = \times_{p \in \pi(G)} O_p(G)$$

It follows that

$$|K| = \prod_{p \in \pi(G)} |O_p(G)| = \prod_{p \in \pi(G)} |S_p| = |G|$$

and so $G = K$. Thus (d) holds.

(d) $\implies$ (e): Since each $O_p(G)$ is a p -group, (d) implies (e).

(e) $\implies$ (a): By 2.1.25 each G_i is nilpotent. Observe that $\bigcup_{i=1}^n z_{G_i}$ is finite and so 2.1.23 shows that $\times_{i=1}^n G_i$ is nilpotent. Thus G is nilpotent. $\square$

2.2 The Frattini subgroup

Definition 2.2.1. *Let $(S, \leq)$ be a partially ordered set.*

- (a) m is called a largest element of S if $m \in S$ and $s \leq m$ for all $s \in S$.
- (b) m is called a smallest element of S if $m \in S$ and $m \leq s$ for all $s \in S$.

Definition 2.2.2. *Let G be a group. Then $\Phi(G)$ is the largest subgroup of G contained in all maximal subgroups of G . Note here $\Phi(G)$ exists: If G has maximal subgroup, then $\Phi(G)$ is the intersection of the maximal subgroups of G . Otherwise $\Phi(G) = G$.*

$\Phi(G)$ is called the Frattini subgroup of G .

Lemma 2.2.3. *Let G be a group.*

- (a) *Let $H \leq G$. Then $H \leq \Phi(G)$ if and only if $H \leq M$ for all maximal subgroups M of G .*
- (b) *Let $N \trianglelefteq G$. Then $\Phi(G)N/N \leq \Phi(G/N)$.*

Proof. (a) follows directly from the definition of $\Phi(G)$.

(b) Suppose $\overline{M}$ is maximal subgroup of G/N . Then $\overline{M} = M/N$ for some $M \leq G$ with $N \leq M$. As $\overline{M}$ is a maximal subgroup of G/N , we know that M is maximal subgroup of G . Hence $\Phi(G) \leq M$. Thus $\Phi(G)N/N \leq M/N = \overline{M}$ and (a) shows that $\Phi(G)N/N \leq \Phi(G/N)$. $\square$

Lemma 2.2.4. *Let G be a finite group and $H \leq G$. Then $H = G$ if and only if $G = \Phi(G)H$.*

Proof. Suppose $H = G$. Then clearly $G = \Phi(G)H$.

Suppose $H \neq G$. Since G is finite there exists a maximal subgroup M of G with $H \leq M$. Then $\Phi(G) \leq M$ and so $\Phi(G)H \leq M$ and $\Phi(G)H \neq G$. $\square$

Definition 2.2.5. *Let G be a group. Then a generating set for G is a subset H of G with $G = \langle H \rangle$.*

Lemma 2.2.6. *Let G be a finite group and $H \subseteq G$. Then H is a generating set for G if and only if $\{\Phi(G)h \mid h \in H\}$ is a generating set for $G/\Phi(G)$.*

Proof. By 2.2.4 we have $G = \langle H \rangle$ iff $G = \langle H \rangle\Phi(G)$ and so iff $G/\Phi(G) = \langle \Phi(G)h \mid h \in H \rangle$ $\square$

Lemma 2.2.7. *Let G be a finite group.*

- (a) *Let $H \trianglelefteq G$. Then the following statements are equivalent*
 - (a) *H is nilpotent.*
 - (b) *$H\Phi(G)/\Phi(G)$ is nilpotent.*
 - (c) *$H\Phi(G)$ is nilpotent.*

(b) *$\Phi(G)$ is nilpotent.*

(c) *G is nilpotent if and only if $G/\Phi(G)$ is nilpotent.*

Proof. (a) (a:a) $\implies$ (a:b): Suppose H is nilpotent. Then also $H/H \cap \Phi(G)$ is nilpotent. As $H/H \cap \Phi(G) \cong H\Phi(G)/\Phi(G)$ we conclude that $H\Phi(G)/\Phi(G)$ nilpotent.

(a:b) $\implies$ (a:c): Put $\overline{G} = G/\Phi(G)$ and suppose that $\overline{H}$ is nilpotent. Let p be a prime and S be a Sylow p -subgroup of $H\Phi(G)$. Then $\overline{S}$ is a Sylow p -subgroup of $\overline{H}$. Since $\overline{H}$ is nilpotent, 2.1.26 shows that $\overline{S} \trianglelefteq \overline{H}$. So $\overline{H} \leq N_{\overline{G}}(\overline{S})$. Since $H \trianglelefteq G$ we have $\overline{H} \trianglelefteq \overline{G}$ and the Frattini argument shows that

$$\overline{G} = \overline{H}N_{\overline{G}}(\overline{S}) = N_{\overline{G}}(S).$$

Thus $\overline{S} \trianglelefteq \overline{G}$, so also $S\Phi(G) \trianglelefteq G$. Another application of Frattini argument shows that

$$G = N_G(S)S\Phi(G) = N_G(S)\Phi(G).$$

Hence by 2.2.4, $G = N_G(S)$ and so $S \trianglelefteq G$. Now 2.1.26 shows that $H\Phi(G)$ is nilpotent.

(a:c) $\implies$ (a:a): Suppose $H\Phi(G)$ is nilpotent. Then also H is nilpotent.

(b) Note that 1 is nilpotent and $\Phi(G) = 1\Phi(G)$. Thus (a) applied to $H = 1$ shows that $\Phi(G)$ nilpotent.

(c) This is the special case $H = G$ of (a). $\square$

Lemma 2.2.8. *Let p be a prime and A an elementary abelian p -group.*

- (a) $A \cong \bigoplus_{i \in I} C_p$ for some set I .
- (b) Any minimal generating set of A has cardinality $|I|$.
- (c) $\Phi(A) = 1$.

Proof. Observe that A is vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ via $\lambda a = a^n$ for all $a \in A$ and $\lambda = n + \mathbb{Z} \in \mathbb{F}_p$. Let $(a_i)_{i \in I}$ be a $\mathbb{F}_p$ -basis for A .

(a) Observe that $\mathbb{F}_p a_i = \langle a_i \rangle \cong C_p$ and $A = \bigoplus_{i \in I} \mathbb{F}_p a_i$. So (a) holds.

(b) A minimal generating set of the group A is just a basis of the $\mathbb{F}_p$ -space A and so has cardinality $|I|$.

(c) Let $1 \neq a \in A$. Since a can be extended to an $\mathbb{F}$ -basis for A we may assume $a = a_j$ for some $j \in I$. Put $D = \langle a_i \mid i \in I, i \neq j \rangle$. Then $A = \langle a \rangle \times D$. So $|A/D| = p$ and D is a maximal subgroup of A with $a \notin D$. Thus $a \notin \Phi(A)$ and so $\Phi(A) = 1$. $\square$

Lemma 2.2.9. *Let G be a groups and p be a prime. Define*

$$\Phi_p(G) := \langle [x, y], z^p \mid x, y, z \in G \rangle$$

Then

- (a) Let $H \leq G$. Then $\Phi_p(G) \leq H$ if and only if $H \trianglelefteq G$ and G/H is an elementary abelian p -group.
- (b) $\Phi_p(G)$ is the smallest normal subgroup of G such that $G/\Phi_p(G)$ is an elementary abelian p -group.
- (c) $\Phi(G) \leq \Phi_p(G)$.

Proof. (a) Observe that $[H, G] \leq [G, G] \leq \Phi_p(G)$. So if $D \leq H$, then $H \trianglelefteq G$. We therefore may assume that $H \trianglelefteq G$.

Then G/H is elementary abelian iff G/H is abelian and $u^p = 1$ for all $u \in G/H$. This holds if and only if $[x, y] \in H$ and $z^p \in H$ for all $x, y, z \in H$ and iff $\Phi_p(G) \leq H$.

(b) follows immediately from (a).

(c) Put $D := \Phi_p(G)$. By (b) G/D is elementary abelian, so 2.2.8 shows that $\Phi(G/D) = 1$. Hence 2.2.3 gives $\Phi(G)D/D \leq \Phi(G/D) = 1$ and so $\Phi(G) \leq D$. $\square$

Lemma 2.2.10. *Let p be a prime.*

- (a) Let G a (possibly infinite) p -group. Then $\Phi(G) = \Phi_p(G)$ if and only if all maximal subgroups of G are normal in G .
- (b) Let G be finite p -group or a hypercentral p -group. Then $\Phi(G) = \Phi_p(G)$.

Proof. (a) Suppose $\Phi(G) = \Phi_p(G)$ and let M be maximal subgroup of G . Then $\Phi_p(G) = \Phi(P) \leq M$ and (2.2.9)(a) shows that $M \trianglelefteq G$.

Suppose next that all maximal subgroups of G are normal. Let M be a maximal subgroup of P . Then M is normal and so $P/M \cong C_p$. Thus P/M is elementary abelian and so $\Phi_p(G) \leq M$. Hence (2.2.3)(a) shows that $\Phi_p(G) \leq \Phi(G)$. By (2.2.9)(c) $\Phi(G) \leq \Phi_p(G)$, so $\Phi(G) = \Phi_p(G)$.

(b) Any finite p -group is nilpotent and so hypercentral. By 2.1.14 maximal subgroups of hypercentral groups are normal. So (b) follows from (a). $\square$

Lemma 2.2.11. *Let P be a finite p -group and let k the minimal size of a generating set of P . Then $P/\Phi(P) \cong C_p^k$.*

Proof. By 2.2.6 k is also the minimal sizes of a generating set of $P/\Phi(P)$. By 2.2.10, $\Phi(P) = \Phi_p(P)$ and so by 2.2.9 $P/\Phi(P)$ is elementary abelian. Now 2.2.8 shows that $P/\Phi(P) \cong C_p^k$. $\square$

2.3 Finite p -groups with cyclic maximal subgroups

Lemma 2.3.1. *Let p be a prime, $H = \langle h \rangle$ be a cyclic group of order p^n and $B \leq \text{Aut}(H)$ with $|B| = p$. Then there exists $b \in B^\#$ such that one of the following holds:*

- (1) $n \geq 2$ and $h^b = h^{1+p^{n-1}}$.
- (2) $p = 2$, $n \geq 3$ and $h^b = h^{-1}$.
- (3) $p = 2$, $n \geq 3$ and $h^b = h^{-(1+p^{n-1})}$.

Proof. Let $b \in B^\#$. Since $H = \langle h \rangle$ and $|h| = p^n$ there exist $s \in \mathbb{N}$ with $1 \leq s < p^n$ and $h^b = h^s$. Since $b \neq 1$ we have $h^b \neq h^s$. So $s > 1$. Put $l := s - 1$. Then

$$(*) \quad h^b = h^{1+l} = hh^l, \quad [h, b] = h^{-1}h^b = h^l, \quad \text{and} \quad 1 \leq l < p^n - 1$$

Next we show

(**) *Let $r \in \mathbb{N}$ and $m \in \mathbb{Z}^+$ with $l = p^r m$ and $p \nmid m$. Then $r \geq 1$ and $n \geq 2$*

Consider the semidirect product $G = H \rtimes B$ and note that $G/\langle h^p \rangle$ has order p^2 . Thus $G/\langle h^p \rangle$ is abelian. It follows that $h^l = [h, b] \in \langle h^p \rangle$. Hence $p \mid l$ and so $r \geq 1$. Thus $p \leq p^r m = l < p^n - 1$ and so $n \geq 2$.

(*) (*) *Suppose that $r = n - 1$ for all $b \in B^\#$. Then (1) holds for some $b \in B^\#$.*

Note that $p^{n-1}m = p^r m = l < p^n - 1 < p^n = p^{n-1}p$. Thus $1 \leq m < p$ and so there are most $p - 1$ possibilities for m . Observe that the automorphism b is uniquely determined by l and so also by m . Since there are $p - 1$ choices for b in $B^\#$ we conclude $m = 1$ for some choice of b . Thus $l = p^r m = p^{n-1}$ and $b^l = b^{1+l} = b^{1+p^{n-1}}$. So (1) holds for this b .

(+) *Suppose $b \in B^\#$ with $r < n - 1$. Then $p = 2$, $n \geq 3$, $r = 1$, m is odd, $0 \leq 2m < 2^n - 1$ and*

$$h^b = h^{1+2m}.$$

From $r < n - 1$ we get $r + 2 \leq n$ and so $n \geq 3$. We claim that $h^{b^i} = h^{s^i}$ for all $i \in \mathbb{N}$. Indeed this holds for $i = 0$ and if it holds for i , then

$$h^{b^{i+1}} = (h^b)^{b^i} = (h^s)^{b^i} = (h^{b^i})^s = (h^{s^i})^s = h^{s^{i+1}}.$$

Since b has order p , $h = h^{b^p} = h^{s^p}$ and so $h^{s^{p-1}} = 1$. Since $|h| = p^n$ this implies that $p^n \mid s^p - 1$. Recall that $r + 2 \leq n$ and so

$$p^{r+2} \text{ divides } s^p - 1$$

We compute

$$(s^p - 1) = (1 + l)^p - 1 = \sum_{i=1}^p \binom{p}{i} l^i = \sum_{i=1}^p \binom{p}{i} p^{ri} m^i$$

We now consider each of these summands. Recall from (*) that $r \geq 1$.

Suppose $i \geq 3$. Then $ri \geq r + r + r \geq r + 2$ and so p^{r+2} divides $\binom{p}{i} p^{ri} m^i$.

Suppose $i = 1$. Then $\binom{p}{i} p^{ri} m^i = pp^r m = p^{r+1} m$. As p does not divide m this shows that p^{r+2} does not divide $\binom{p}{i} p^{ri}$.

Since p^{r+2} divides $s^p - 1$ we now conclude that p^{r+2} does not divide the only remaining summand $\binom{p}{2} p^{2r} m^2$. Hence p^2 does not divide $\binom{p}{2} p^r$. Thus $r = 1$ and p does not divide $\binom{p}{2}$. Since $\binom{p}{2} = \frac{p}{p-1} 2$ this implies that 2 does not divide $p-1$. So $p-1$ is odd, p is even and $p = 2$. From $r = 1$ and $p = 2$ we get $l = 2m$ with m odd. So $h^b = h^{1+l} = h^{1+2m}$ and (+) is proved.

In view of (**), to prove the lemma, we may assume that $r < n-1$. So (+) holds. In particular, $b = 2$ and so $b^2 = 1$.

Define $\tilde{b}$ in $\text{Aut}(H)$ by $h^{\tilde{b}} = h^{-b}$. Then $h^{\tilde{b}^2} = (h^{-b})^{-b} = (h^b)^b = h$ and so $\tilde{b}^2 = 1$.

Suppose that $\tilde{b} = 1$, then $h = h^{-b}$. Thus $h^b = h^{-1}$ and (2) holds in this case.

Suppose next that $\tilde{b} \neq 1$. By (+) $h^b = h^{1+2m}$ and so

$$h^{\tilde{b}} = h^{-b} = h^{-(1+2m)} = h^{2^n-1-2m} = h^{1+(2^n-2-2m)} = h^{1+2(2^{n-1}-1-m)}$$

Put $\tilde{B} = \langle \tilde{b} \rangle$ and $\tilde{l} = 2(2^{n-1}-1-m)$. Let $\tilde{l} = 2^{\tilde{r}} \tilde{m}$ with $2 \nmid \tilde{m}$. Since m is odd, we know that $2^{n-1}-1-m$ is even. Thus $\tilde{r} \geq 2$. If $\tilde{r} < n-1$ then (+) applied to $\tilde{b}$ shows that $\tilde{r} = 1$, a contradiction. Thus $\tilde{r} = n-1$. As $|\tilde{B}| = p = 2$ we know that $\tilde{b}$ is the only element in $\tilde{B}$. Now (***) shows that (1) holds for $\tilde{b}$. Hence

$$h^{\tilde{b}} = h^{1+p^{n-1}} \quad \text{and so} \quad h^b = h^{-\tilde{b}} = h^{-(1+p^{n-1})}.$$

Thus (3) holds. □

Lemma 2.3.2. *Let G be a group and $A, B \subseteq G$ with $G = \langle B \rangle$.*

- (a) *Suppose that $[a, b] = 1$ for all $a \in A, b \in B$. Then $\langle A \rangle \leq Z(G)$ and $\langle A \rangle \trianglelefteq G$.*
- (b) *Suppose that $[[a, b], c] = 1$ for all $a, b, c \in B$. Then $G' = [B, B] \leq Z(G)$. In particular, $G/Z(G)$ is abelian and G is nilpotent of class at most 2.*

Proof. (a) Note that $B \subseteq C_G(A)$ and since $C_G(A)$ is a subgroup of G we get $G = \langle B \rangle \leq C_G(A)$. Thus $A \leq Z(G)$ and since $Z(G)$ is a subgroup of G we get $\langle A \rangle \leq Z(G)$. In particular, $\langle A \rangle \trianglelefteq G$.

(b) (a) applies to $A = \{[a, b] \mid a, b \in B\}$ shows that $[B, B] \leq Z(G)$ and $[B, B] \trianglelefteq G$. Put $\overline{G} = G/[B, B]$. Then $[\overline{a}, \overline{b}] = 1$ for all $a, b \in B$ and hence (a) shows that $\overline{G} = \langle \overline{B} \rangle \leq Z(\overline{G})$. Thus $\overline{G}' = 1$ and so $G' \leq [B, B] \leq G'$. □

Definition 2.3.3. *Let A, B and C be groups. A function $f : A \times B \rightarrow C$ is called a bihomomorphism of groups if for each $a \in A$ and $b \in B$ the functions*

$$B \rightarrow C, \quad y \mapsto (a, y)f, \quad \text{and} \quad A \rightarrow C, \quad x \mapsto (x, b)f$$

are homomorphisms of groups

Lemma 2.3.4. *Let G be a group of class at most 2.*

- (a) *The function $G \times G \rightarrow G, (a, b) \rightarrow [a, b]$ is a bihomomorphism.*

(b) *The function*

$$\begin{aligned} G/Z(G) \times G/Z(G) &\rightarrow G' \\ (Z(G)a, Z(G)b) &\mapsto [a, b] \end{aligned}$$

is a well-defined bihomomorphism of abelian groups.

Proof. Let $a, b, c, d \in G$.

(a) By (2.1.1)(d)

$$[ab, c] = [a, c]^b [b, c] = [a, b][c, b]$$

and by symmetry $[a, cd] = [a, c][a, d]$. So (a) holds.

(b) By (a) the functions $y \mapsto [a, y]$ and $x \mapsto [x, b]$ are homomorphisms. Also $Z(G)$ is in the kernel of these homomorphisms and so (b) holds. $\square$

Lemma 2.3.5. *Let G be a nilpotent group of class at most 2, let $x, y \in G$ and let $n, m \in \mathbb{Z}$. Put $z := [x, y]$*

(a) $[x^n, y^m] = [x, y]^{nm} = z^{nm}$.

(b) $(yx)^n = y^n x^n z^{\binom{n}{2}}$.

(c) $|z|$ divides $|x|$ and $|y|$.

(d) Let p be an odd prime with $z^p = 1$. Then $(yx)^p = y^p x^p$.

(e) If $|z| = 2$, then $(yx)^2 = y^2 x^2 z$ and $(yx)^4 = y^4 x^4 = (y^2 x^2)^2$.

(f) Let p be an odd prime with $x^p = y^p = 1$. Then $(yx)^p = 1$.

(g) If $x^2 = y^2 = 1$, then $(yx)^2 = z$ and $(yx)^4 = 1$.

Proof. (a) Let $a \in G$. By (2.3.4)(a) the functions $y \mapsto [x^n, y]$ and $x \mapsto [x, y]$ are homomorphisms. Thus

$$[x^n, y^m] = [x^n, y]^n = ([x, y]^n)^m = [x, y]^{nm} = z^{nm}$$

(b) Note that $\binom{n}{0} = 0$ and that $x^0 = 1$ for all $x \in G$. Hence (b) holds for $n = 0$. Suppose true for n . Observe that

$$\binom{n}{2} + n \frac{n(n-1)}{2} + n = \frac{n(n-1) + 2n}{n} = \frac{n(n+1)}{2} = \binom{n+1}{2}$$

and

$$\begin{aligned} (yx)^{n+1} &= (yx)^n yx \\ &= y^n x^n z^{\binom{n}{2}} yx \\ &= y^n (x^n y) x z^{\binom{n}{2}} \\ &= y^n (yx^n [x^n, y]) x z^{\binom{n}{2}} \\ &= y^n y x^n z^n x z^{\binom{n}{2}} \\ &= y^{n+1} x^{n+1} z^{\binom{n}{2} + n} \\ &= y^{n+1} z^{n+1} z^{\binom{n+1}{2}} \end{aligned}$$

Also

$$n^2 - \binom{n}{2} = n^2 - \frac{n(n-1)}{2} = \frac{2n^2 - n(n-1)}{2} = \frac{n(n+1)}{2} = \frac{(-n)(-n-1)}{2} = \binom{-n}{2}$$

and

$$\begin{aligned} (yx)^{-n} &= ((yx)^n)^{-1} \\ &= \left((y^n x^n z^{\binom{n}{2}}) \right)^{-1} \\ &= z^{-\binom{n}{2}} x^{-n} y^{-n} \\ &= y^{-n} x^{-n} [x^{-n}, y^{-n}] z^{-\binom{n}{2}} \\ &= y^{-n} x^{-n} z^{n^2 - \binom{n}{2}} \\ &= y^{-n} x^{-n} z^{\binom{-n}{2}} \end{aligned}$$

So (b) holds for $n+1$ and $-n$ and so for all integers n .

(c) Let $k = |x|$. Then by (a)

$$z^k = [x^k, y] = [1, y] = 1$$

and so $|z|$ divides k . Since $z^{-1} = [y, x]$ this also shows $|z|$ divides $|y|$.

(d) Since p is odd, we know that 2 divides $p-1$. As $\binom{p}{2} = p \frac{p-1}{2}$ this shows that p divides $\binom{p}{2}$. Hence $z^{\binom{p}{2}} = 1$. Thus (d) follows from (b).

(e) Note that $\binom{2}{2} = 1$ and so $z^{\binom{2}{2}} = z$. Also $\binom{4}{2} = 6$. Hence $\binom{4}{2}$ is even and so $z^{\binom{4}{2}} = 1$. Thus (b) gives $(yx)^2 = y^2 x^2 z$ and $(yx)^4 = y^4 x^4$. Also $[x^2, y^2] = z^{2 \cdot 2} = 1$ and so $(x^2 y^2)^2 = (x^2)^2 (y^2)^2 = x^4 y^4$.

(f) Since $x^p = 1$ and (c) shows that $z^p = 1$. Now (d) gives $(yx)^p = x^p y^p = 1$.

(g) Since $x^p = 1$ and (c) shows that $z^2 = 1$. Now (e) gives $(yx)^2 = x^2 y^2 z = z$ and $(yx)^4 = y^4 x^4 = 1$. $\square$

Definition 2.3.6. Let $H = \langle x \rangle$ and $K = \langle y \rangle$ be cyclic groups of order n and m respectively. Let s be an integer with $\gcd(n, s) = 1$ and $s^m \equiv 1 \pmod{n}$. Note that K acts on H via $h^{y^i} = h^{si}$ for all $h \in H$. Let $G = H \ltimes K$ be the semidirect product of H by K with respect to this action.

- (a) Suppose $m = 2$ and $s = -1$. Then G is called the dihedral group of order $2n$ and is denoted by D_{2n} .
- (b) Let $k \in \mathbb{Z}^+$. Suppose that $n = 4k$, $m = 2$ and $s = 2k - 1$. Then G is called the quasi-dihedral group of order $8k$ and is denoted by QD_{8k} .
- (c) Let $k \in \mathbb{Z}^+$. Suppose that $n = 2k$, $m = 4$ and $s = -1$. Note that $z := x^k y^2 \in Z(G)$. Then $G/\langle z \rangle$ is called the quasi-quaternion group of order $4k$ and is denoted by Q_{4k} .
- (d) Let p be a prime and $k \in \mathbb{N}$. Suppose that $n = p^{k+1}$, $m = p$ and $s = 1 + p^k$. Then G is called the quasi-extra group of order p^{k+2} and is denoted by $Q\text{Ext}(p^{k+2})$.

Note that $D_2 \cong C_2$, $D_4 \cong C_2 \times C_2$, $D_8 \cong Q\text{Ext}(8)$, $QD_8 \cong C_4 \times C_2$, $Q_4 \cong C_4$, and $Q\text{Ext}(p^2) \cong C_p \times C_p$.

Theorem 2.3.7. Let p be a prime, P a finite p -group and H a maximal subgroup of P . Suppose that $H = \langle h \rangle$ is cyclic of order p^n . Then exactly one of the following holds:

- (a) There exists $b \in P \setminus H$ with $|b| = p$ and $h^b = h$. In particular, $P \cong C_{p^n} \times C_p$.

- (b) There exists $b \in P \setminus H$ with $|b| = p$ and $h^b = h^{1+p^{n-1}}$. In particular, $P \cong \text{QExt}(p^{n+1})$.
- (c) $p = 2$, $n \geq 3$ and there exists $b \in P \setminus H$ with $|b| = p$ and $h^b = h^{-1}$. In particular, $P \cong D_{2^{n+1}}$.
- (d) $p = 2$, $n \geq 3$ and there exists $b \in P \setminus H$ with $|b| = p$ and $h^b = h^{-(1+p^{n-1})}$. In particular, $P \cong \text{QD}_{2^{n+1}}$.
- (e) There exists $b \in P \setminus H$ with $b^p = h$. In particular, $P \cong C_{p^{n+1}}$.
- (f) $p = 2$, $n \geq 2$ and there exists $b \in P \setminus H$ with $b^2 = h^{p^{n-1}}$ and $h^b = h^{-1}$. In particular, $P \cong Q_{2^{n+1}}$.

Proof. Let $b \in P \setminus H$ with $|b|$ minimal. Since H is a maximal subgroup of P we have $H \trianglelefteq P$ and $|P/H| = p$. Thus $b^p \in H$. Since H is abelian we conclude that the image of B in $\text{Aut}(H)$ as order 1 or b . So if $h^b \neq 1$ we can apply 2.3.1. Hence, after replacing b by b^i for some $0 < i < p$, one of following holds:

- (1) $h^b = h$.
- (2) $n \geq 2$ and $h^b = h^{1+p^{n-1}}$.
- (3) $p = 2$, $n \geq 3$ and $h^b = h^{-1}$.
- (4) $p = 2$, $n \geq 3$ and $h^b = h^{-(1+p^{n-1})}$.

Suppose first that $|b| = p$. Then one of (a), (b), (c) and (d) holds. So we may assume $|b| > p$ and the minimal choice of $|b|$ implies

$$(*) \quad |x| > p \text{ for all } x \in P \setminus H.$$

Recall that $x^p \in H$. If $x^p \notin \langle h^p \rangle$, then $H = \langle x^p \rangle$ and so $P = \langle b \rangle$ and (e) holds. Thus we may assume that $b^p \in \langle h^p \rangle$ and so

$$(**) \quad h_0^p b^p = 1 \text{ for some } h_0 \in H$$

Put $z := [h_0, b]$. If $z = 1$ we get $(h_0 b)^p = h_0^p b^p = 1$, contrary to $(*)$. Thus

$$(***) \quad z \neq 1$$

In particular, (1) does not hold.

Suppose (2) holds. Then $[h, b] = h^{-1} h^{1+p^{n-1}} = h^{p^{n-1}} \in Z(P)$ and so also $z \in \langle h^{p^{n-1}} \rangle \leq Z(P)$.

If p is odd, then (2.3.5)(d) implies that $(h_0 b)^p = h_0^p b^p \stackrel{(**)}{=} 1$, contrary to $(*)$.

Thus $p = 2$ and (2.3.5)(e) implies that $(h_0 b)^4 = (h_0^2 b^2)^2 \stackrel{(**)}{=} 1^2 = 1$. Thus $|h_0 b| = 4$ and the minimal choice of $|b|$ implies that $|b| = 4$. Since $h_0^2 = b^{-2}$ we have $|h_0| = |b| = 4$. Observe that $[h^p, b] = [h, p]^p = (h^{p^{n-1}})^p = 1$. Since $z = [h_0, b] \neq 1$ this implies $h_0 \notin \langle h^p \rangle$ and so $H = \langle h_0 \rangle$. Thus $|H| = 4$, $n = 2$ and $h^b = h^{1+2^{2-1}} = h^3 = h^{-1}$ and (f) holds.

If (3) holds put $u = 1$ and if (4) holds put $u = h^{p^{n-1}}$. In either case $p = 2$, $h^b = h^{-1}u$, $u \in \langle h^{2^{n-1}} \rangle \leq Z(P)$ and $u^2 = 1$. Thus $(h^2)^b = (h^{-1}u)^2 = (h^2)^{-1}$ and so b inverts $\langle h^2 \rangle$. Since $b^2 \in \langle h^2 \rangle$ and b centralizes b^2 , this implies $b^2 = (b^2)^{-1}$ and so $(b^2)^2 = 1$. Since $b^2 \neq 1$, this shows that $|b^2| = 2$ and $|b| = 4$. In particular, b^2 is the unique element of order 2 in H and so $b^2 = h^{2^{n-1}}$.

In case (3) we conclude that (f) holds.

So suppose (4) holds. Then $u = h^{2^{n-1}} = b^2$ and so

$$(hb)^2 = h b h b = h b^2 h^b = h b^2 h^{-1} u = b^2 u = u u = 1$$

a contradiction to $(*)$. □

Lemma 2.3.8. *Let P be a finite 2-group, H a maximal abelian normal subgroups of P and put $H_4 = \{x \in H \mid x^4 = 1\}$. Suppose that*

- (i) H is cyclic.
- (ii) If $x \in P \setminus H$ with $x^2 \in H$, then x inverts H_4 .

Then $|P/H| \leq 2$ and P is a cyclic, dihedral, quasi-dihedral or quasi-quaternion group.

Proof. Since H is maximal abelian normal subgroup of P we know from 2.1.15 that $C_P(H) = H$. If $|H| \leq 2$ we conclude that $P = C_P(H) = H$ is cyclic the lemma holds in this case. So suppose $|H| \geq 4$. Then $H_4 \cong C_4$. It follows that $|\text{Aut}(H_4)| = 2$ and so $|P/C_P(H_4)| \leq 2$.

Let $x \in C_P(H_4)$. Then x does not invert H_4 and so (ii) implies that either $x \in H$ or $x^2 \notin H$. In either case Hx does not have order 2 in $C_P(H_4)/H$. It follows that $C_P(H_4)/H$ has no elements of order 2 and so $C_P(H_4)/H = 1$. Thus $H = C_P(H_4)$ and we conclude that $|P/H| \leq 2$.

If $P = H$, then P is cyclic and the lemma holds. So suppose $H \neq P$. Then H is a maximal subgroup of P , H is cyclic and P is not abelian. Now 2.3.7 shows that either P is a dihedral, quasi-dihedral or quasi-quaternion group or there exists $h \in H$ and $b \in P \setminus H$ with $H = \langle h \rangle$, $|h| = 2^n$, $|b| = 2$ and $h^b = h^{1+2^{n-1}}$. In the latter case b centralizes $\langle h^2 \rangle$. Since $b \notin H = C_P(H)$, we know that b does not centralizes H_2 . Thus $H_4 \not\leq \langle h^2 \rangle$. It follows that $H_4 = H$, so $n = 2$ and $P \cong D_8$. $\square$

Lemma 2.3.9. *Let G be a finite group.*

- (a) *Suppose that G has a unique maximal subgroup M and put $p := |G/M|$. Then p is a prime and G is a cyclic p -group.*
- (b) *Suppose that G has a unique minimal subgroup M and put $p := |M|$. Then p is a prime and either G is a cyclic p -group or $p = 2$ and G is a quasi-quaternion group.*

Proof. (a) Let $x \in G \setminus M$. Then $\langle x \rangle \not\leq M$ and so $\langle x \rangle$ is not contained in any maximal subgroup of G . Since G is finite this gives $\langle x \rangle = G$ and G is cyclic. Let q be a prime with $q \mid |G|$. Then $|G/\langle x^q \rangle| = q$. Thus $\langle x^q \rangle$ is a maximal subgroup of G and so $M = \langle x^q \rangle$. Hence $p = |G/M| = |G/\langle x^q \rangle| = q$. In particular, p is a prime and p is the only prime divisor of $|G|$. So G is a p -group and (a) holds.

(b) Let q be a prime dividing the order $|G|$ and $x \in G$ with $|x| = q$. Then $M = \langle x \rangle$ and so $p = q$. Thus p is a prime and G is a p -group. Let H be a maximal normal abelian subgroup of G . Suppose $H = H_1 \times H_2$ for some non-trivial subgroups H_1 and H_2 of H . Then both H_1 and H_2 contain a minimal subgroups of G . But then $M \leq H_1 \cap H_2$ a contradiction to $H_1 \cap H_2 = 1$. As every finite abelian group is the direct product of cyclic groups we conclude that H is cyclic.

If $G = H$, then G is cyclic and we are done.

So suppose $G \neq H$ and let $a \in G \setminus H$ with $a^p \in H$. Put $Q := H\langle a \rangle$. Note that $|Q/H| = p$ and so H is a cyclic maximal subgroup of Q . Since $M \leq H$, we get $\langle a \rangle \neq M$ and so $|a| \neq p$. As H is a maximal abelian normal subgroup of G , we know from 2.1.15 that $C_G(H) = H$. Hence Q is not abelian and 2.3.7 shows a inverts H and that Q is a quasi-quaternion group. In particular, $p = 2$ and a inverts H_4 . Hence we can apply 2.3.8 and conclude that $|G/H| \leq 2$. Thus $G = Q$ and so G is a quasi-quaternion group. $\square$

Lemma 2.3.10. *Let p be a prime and P a finite p -group all of whose abelian subgroups are cyclic. Then P is cyclic, or $p = 2$ and P is a quaternion group.*

Proof. If $P = 1$, then P is cyclic. So suppose $P \neq 1$. Then also $Z(P) \neq 1$ and there exists $A \leq Z(P)$ with $|A| = p$. Let B be any minimal subgroups of P . Then $|B| = p$ and since $[A, B] = 1$, AB is an abelian subgroup of P . So AB is cyclic and thus has a unique subgroup of order p . Hence $A = B$ and so A is the unique minimal subgroup of P . The lemma now follows from 2.3.9. $\square$

Lemma 2.3.11. *Let p be a prime and P a finite p -group all of whose abelian normal subgroups are cyclic. Then P is cyclic, or $p = 2$ and P is a dihedral, quasidihedral or quaternion group.*

Proof. Let H be a maximal abelian normal subgroup of P . Then H is cyclic and by 2.1.15 $C_P(H) = H$. If $P = H$ we are done. So we may assume that $H \neq P$. Put $H_{p^2} := \{x \in H \mid x^{p^2} = 1\}$. We will show that

(*) $p = 2$ and if $b \in P \setminus H$ with $b^p \in H$, then b inverts H_4 .

Observe that the lemma will follow from 2.3.8 once we proved (*).

Let $b \in P \setminus H$ with $b^p \in H$. Put $Q = H\langle b \rangle$. Let $h \in H$ with $H = \langle h \rangle$ and put $|h| = p^n$. Since $P \neq H = C_P(H)$ we have $n \geq 2$ and b does not centralize h . Note that H is a cyclic maximal subgroups of Q and so we can apply 2.3.7 with Q in place of P . Since $[h, b] \neq 1$, neither Case (a) nor Case (e) holds. In Cases (c) and (f), we see that b inverts H and so (*) holds. In case (d) b inverts $\langle h^2 \rangle$ and $n \geq 3$. Thus $H_4 \leq \langle h^2 \rangle$ and again (*) holds.

It remains to consider Case (d). Then we may choose b such that $|b| = p$ and $h^b = h^{1+p^{n-1}}$. If $p = 2$ and $n = 2$, then h inverts H and (*) holds. So we may assume that $n \geq 3$ if $p = 2$ and aim for a contradiction. For this we show

(**) Put $z := [h, b]$. Then $1 \neq z = h^{p^{n-1}}$, $z^p = 1$ and $z \in Z(P)$.

As $h^b = h^{1+p^{n-1}}$ we have $z = h^{p^{n-1}}$. Since $|h| = p^n$ this implies $z \neq 1$ and $z^p = 1$. In particular, $\langle z \rangle$ is the only subgroup of order p in H , and as $H \trianglelefteq P$, we get $\langle z \rangle \trianglelefteq P$. Hence $1 \neq \langle z \rangle \cap Z(P) = \langle z \rangle$ and so $z \in Z(P)$.

(***) Let $y \in Q \setminus \langle b \rangle \langle h^p \rangle$. Then $y^p \neq 1$.

If $y \in H$, then $y \in \langle h \rangle \setminus \langle h^p \rangle$ and since $h^p \neq 1$ also $y^p \neq 1$. So suppose $y \notin H$. Since $|Q/H| = p$ we get $y^j H = bH$ for some $1 \leq j < p$ and replacing y by y^j we assume that $yH = bH$. Thus $y = bh^i$ for some $0 \leq i < p^n$. Since $y \notin \langle b \rangle \langle h^p \rangle$ we see that p does not divide i . By (**) $z = [h, b] \in Z(P)$ and so 2.3.5 shows that $[h^i, b] = z^i$ and

$$y^p = (bh^i)^p = \begin{cases} b^p h^{ip} = h^{ip} & \text{if } p \text{ is odd} \\ b^p h^{ip} z^i = h^{ip} z^i & \text{if } p = 2 \end{cases}$$

If $p \neq 2$, then $|h| \geq p^2$ and since $p \nmid i$ we get $y^p = h^{ip} \neq 1$. If $p = 2$, then $n \geq 3$ so $y^{p^2} = (h^{ip} z^i)^p = h^{ip^2} (z^p)^i = h^{ip^2} \neq 1$. In either case $y^p \neq 1$ and (***) is proved.

$Q_p := \{x \in Q \mid x^p = 1\}$. Then (***) shows that $Q_p \leq \langle b \rangle \langle h^p \rangle$. Since $[h^p, b] = z^p = 1$ and $b^p = 1$, we have $\langle b \rangle \langle h^p \rangle = \langle b \rangle \times \langle h^p \rangle \cong C_p \times C_{p^{n-1}}$. It follows that $Q_p \cong C_p \times C_p$, so Q_p is abelian but not cyclic.

Since $C_P(H) = H$ we know P/H is isomorphic to a subgroups of $\text{Aut}(H)$. As H is cyclic, $\text{Aut}(H)$ is abelian and so P/H is abelian. Thus $Q/H \trianglelefteq P/H$. Hence also $Q \trianglelefteq P$ and thus $\Omega(Q) \trianglelefteq P$. But this is contradiction since all abelian normal subgroups of P are cyclic. $\square$

2.4 Hypoabelian groups

Definition 2.4.1. Let G be a group.

- (a) $G' = [G, G]$, $G'' = (G')'$. G is called the derived subgroup of G .
- (b) G is called perfect if $G = G'$.

(c) Let α be an ordinal. Define $G^{(\alpha)}$ inductively as follows

$$g^{(\alpha)} = \begin{cases} G & \text{if } \alpha = 0 \\ (G^\alpha)' & \text{if } \alpha = \beta + 1 \\ \bigcap_{\beta < \alpha} G^{(\beta)} & \text{if } \alpha \text{ is a limit ordinal} \end{cases}$$

(d) d_G is the smallest ordinal with $G^{(d_G)} = G^{(d_G+1)}$. $G^{(*)} := G^{(d_G)}$.

(e) $(G^{(\alpha)})_{\alpha \leq d_G}$ is called the derived series of G .

(f) If $G^{(*)} = 1$, then G is called hypoabelian of derived length d_G .

(g) If $G^{(*)} = 1$ and d_G is finite, then G is called solvable of derived length d_G .

Lemma 2.4.2. Let G be a group, $H \leq G$ and α and β ordinals. Then

(a) If $\alpha \geq d_G$, then $G^{(\alpha)} = G^{(*)}$.

(b) $H^{(\alpha)} \leq G^{(\alpha)}$ and $H^{(*)} \leq G^{(*)}$.

(c) If $H \trianglelefteq G$, then $G^{(\alpha)}H/H \leq (G/H)^\alpha$ with equality if α is finite.

(d) $G^{(\alpha+\beta)} = (G^{(\alpha)})^{(\beta)}$.

Proof. (a) If $\alpha = d_G$ this holds by definition of d_G . Induction shows that it holds for all $\alpha \geq d_G$.

(b) Since $H' = [H, H] \leq [G, G] = G'$ this first statement follows by induction on α . Let $\delta = \max(d_G, d_H)$. By (b) $H^{(\delta)} = H^{(*)}$ and $G^{(\delta)} = G^{(*)}$. As $H^{(\delta)} \leq G^{(\delta)}$ this gives $H^{(*)} \leq G^{(*)}$.

(c) By induction on α . If $\alpha = 0$, then both sides are equal to G/H . If $\alpha = \beta + 1$, then using the induction assumption

$$G^{(\alpha)}H/H = [G^{(\beta)}, G^{(\beta)}]H/H = [G^{(\beta)}H/H, G^{(\beta)}H/H] \leq [(G/H)^{(\beta)}, (G/H)^{(\beta)}] = (G/H)^{(\alpha)}$$

with equality if α and so also β is finite.

If α is a limit ordinal, then

$$\begin{aligned} (G^{(\alpha)}H/H &= (\bigcap_{\beta \in \alpha} G^{(\beta)})H/H \leq (\bigcap_{\beta \in \alpha} G^{(\beta)}H)/H = \bigcap_{\beta \in \alpha} G^{(\beta)}H/H \\ &\leq \bigcap_{\beta \in \alpha} (G/H)^{(\beta)} = (G/H)^{(\alpha)} \end{aligned}$$

(d) By induction on β . If $\beta = 0$ both sides are equal to $G^{(\alpha)}$. If $\beta = \gamma + 1$, then

$$G^{(\alpha+\beta)} = G^{(\alpha+(\gamma+1))} = G^{((\alpha+\gamma)+1)} = (G^{(\alpha+\gamma)})' = ((G^{(\alpha)})^{(\gamma)})' = ((G^\alpha)^{(\gamma+1)}) = (G^\alpha)^{(\beta)}$$

If β is a limit ordinal then

$$(G^{(\alpha)})^{(\beta)} = \bigcap_{\gamma < \beta} (G^{(\alpha)})^{(\gamma)} = \bigcap_{\gamma < \beta} G^{(\alpha+\gamma)} = \bigcap_{\alpha \leq \rho < \alpha+\beta} G^{(\rho)} = \bigcap_{\rho < \alpha+\beta} G^{(\rho)} = G^{(\alpha+\beta)}$$

□

Lemma 2.4.3. Let G be a group.

(a) G is perfect if and only if $d_G = 0$ and if and only if $G = G^{(*)}$.

(b) $G^{(*)}$ is largest perfect subgroup of G .

Proof. Note first that $G^{(*)} = G^{(d_G)} = G^{(d_G+1)} = (G^{(d_G)})' = (G^{(*)})'$. So

(*) $G^{(*)}$ is perfect.

(a) G is perfect iff $G = G'$, that is iff $G^{(0)} = G^{(1)}$ and so iff $d_G = 0$. If $d_G = 0$, then $G = G^{(0)} = G^{*d_G} = G^{(*)}$. By (*) $G^{(*)}$ is perfect. So if $G = G^{(*)}$, then G is perfect.

(b) By (a) $G^{(*)}$ is perfect. Let H be a perfect subgroup of G . Then (a) gives $H = H^{(*)}$. By (2.4.2)(b) we have $H^{(*)} \leq G^{(*)}$, so $H \leq G^{(*)}$ and $G^{(*)}$ is indeed the largest perfect subgroup of G . $\square$

Corollary 2.4.4. *Let G be a group. Then the following are equivalent*

- (a) G is hypoabelian.
- (b) G has no non-trivial perfect subgroup.
- (c) G has no non-trivial normal perfect subgroup.
- (d) G has no non-trivial characteristic perfect subgroup.

Proof. (a) $\implies$ (b): If G is hypoabelian, then $G^{(*)} = 1$. By 2.4.3 $G^{(*)}$ is the largest perfect subgroup of G , so all perfect subgroups of G are trivial.

(b) $\implies$ (c): and (c) $\implies$ (d): are both obvious.

(d) $\implies$ (a): Observe that $G^{(*)}$ is a characteristic subgroup of G and by 2.4.3 $G^{(*)}$ perfect. So G has no non-trivial characteristic perfect subgroup, then $G^{(*)} = 1$ and G is hypoabelian. $\square$

Lemma 2.4.5. *Let G be group*

- (a) *If G is hypoabelian of derived length α . Then all subgroups of G are hypoabelian of derived length at most α .*
- (b) *If G is solvable of derived length α then all quotients of G are solvable of derived length at most α .*
- (c) *Let H be a normal subgroups of G . If G/H is hypoabelian of derived length α and H is hypoabelian of derived length β , then G is hypoabelian of derived length at most $\alpha + \beta$.*
- (d) *Let H be a normal subgroups of G . Then G/H is solvable if and only if both H and G/H are solvable.*

Proof. (a) If $G^{(\alpha)} = 1$, then by 2.4.2, $H^{(\alpha)} \leq G^{(\alpha)} = 1$.

(b) Suppose $G^{(\alpha)} = 1$ for a finite ordinal α . Then by 2.4.2, $(G/H)^{(\alpha)} = G^{(\alpha)}H/H = H/H = 1$.

(c) We have $G^{(\alpha)}H/H \leq (G/H)^{(\alpha)} = 1$ and so $G^{(\alpha)} \leq H$. Thus

$$G^{(\alpha+\beta)} = (G^{(\alpha)})^{(\beta)} \leq H^{(\beta)} = 1.$$

(d) Follows from (b) and (c). $\square$

Definition 2.4.6. *Let I be a set, F a group and $\alpha : I \rightarrow F$ a function. Then F is called a free group on I with respect to α provided that for all sets I , all groups G and all functions $\beta : I \rightarrow G$ there exists a unique homomorphism of groups $\gamma : F \rightarrow G$ with $\beta = \alpha \circ \gamma$.*

In the next example we will use (without proof) the following facts about free groups.

Remark 2.4.7. (a) Let I be a set. Then exists a group F with $I \subseteq F$ and F is a free group on I with respect to $\text{id}_{I,F}$.

(b) Subgroups of free groups are free groups.

(c) Let F be a free group on the set I then $F/F' \cong \bigoplus_{i \in I} F$. In particular, $F \neq F'$ unless $F = 1$.

(d) Any group is isomorphic to quotient of a free group.

Example 2.4.8. (a) All free groups are hypoabelian.

(b) Every group is the quotient of a hypoabelian group.

(c) Quotients of hypoabelian groups are not necessarily hypoabelian.

Proof. (a) Let F free group and $H \leq F$. By (2.4.7)(a) H is a free and so by (2.4.7)(c) $H \neq H'$ unless $H = 1$. So F does not have any non-trivial perfect subgroups and 2.4.4 implies that F is hypoabelian.

(b) By (2.4.7)(d) any groups is isomorphic to a quotient of a free group. By (a) free groups are hypoabelian, and so (b) holds.

(c) Since non-trivial perfect groups exist, this follows from (b). $\square$

Definition 2.4.9. Let G be a group and $H \leq G$. A series from H to G is a set $\mathcal{S}$ of subgroups of G such that

(i) $G \in \mathcal{S}$.

(ii) $H \in \mathcal{S}$ and $H \leq S$ for all $S \in \mathcal{S}$.

(iii) If $S, T \in \mathcal{S}$, then $S \leq T$ or $T \leq S$.

(iv) If $\mathcal{D}$ is non-empty subset of $\mathcal{S}$, then both $\bigcup \mathcal{D}$ and $\bigcap \mathcal{D}$ are in $\mathcal{S}$.

(v) Let $T \in \mathcal{S}$. Define $T^- := \bigcup \{B \in \mathcal{S} \mid B \not\leq T\}$ if $T \neq H$ and $T^- = H$ if $T = H$. Then $T^- \trianglelefteq T$ for all $T \in \mathcal{S}$.

Definition 2.4.10. Let G be a group, $H \leq G$ and $\mathcal{S}$ a series from H to G .

(a) G is called simple if $G \neq 1$ and G has no nontrivial proper normal subgroups.

(b) A factor of $\mathcal{S}$ is a group T/T^- where $T \in \mathcal{S}$ with $T \neq T^-$.

(c) $\mathcal{S}$ is called normal if $T \trianglelefteq G$ for all $T \in \mathcal{S}$.

(d) $\mathcal{S}$ is called subnormal if $|\mathcal{S}|$ is finite.

(e) $\mathcal{S}$ is called a composition series from H to G if each factor of $\mathcal{S}$ is a simple group.

(f) $\mathcal{S}$ is a chief series from H to G if it is normal and, for each factor F of $\mathcal{S}$, 1 and F are the only G -invariant subgroups of F .

(g) A (subnormal) series of G is a (subnormal) series from 1 to G .

Definition 2.4.11. A subgroup H of the group G is called subnormal, and we write $H \trianglelefteq G$ if there exists a subnormal series from H to G .

Example 2.4.12. (a) Let G be a group and $H \leq G$. Then any subnormal series from H to G is of the form $G_i, 0 \leq i \leq n$ with

$$H = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G$$

The factors are G_i/G_{i-1} , $1 \leq i \leq n$.

(b) Let $G = (\mathbb{Z}, +)$ and $H = 0$. For $i \in \mathbb{Z}^+$ let n_i be a positive integer. Define $G_0 = \mathbb{Z}$ and inductively $G_i := n_i G_{i-1} = n_1 n_2 \dots n_i \mathbb{Z}$. Then $\mathcal{S} = \{G_i \mid i \in \mathbb{N}\} \cup \{0\}$ is a series with factors $G_{i-1}/G_i \cong C_{n_i}$ $i \in \mathbb{Z}^+$. If each n_i is a prime, $\mathcal{S}$ is a composition series. If p is a prime with $n_i = p$ for all i , then all factors of $\mathcal{S}$ are isomorphic to C_p . Choosing different primes we see that distinct composition series can have non-isomorphic factors.

(c) Let p be a prime. Then

$$1 \leq C_p \leq C_{p^2} \leq \dots \leq C_{p^k} \leq C_{p^{k+1}} \leq \dots C_{p^\infty}$$

is a composition series for C_{p^∞} with factors isomorphic to C_p . Note here that $C_{p^\infty}^- = \bigcup_{k \in \mathbb{N}} C_{p^k} = C_{p^\infty}$.

(d) $1 \triangleleft \text{Alt}(n) \triangleleft \text{Sym}(n)$, is a normal and subnormal series for $\text{Sym}(n)$. If $n \neq 4$, this is also composition series and a chiefseries for $\text{Sym}(n)$.

(e)

$$1 \triangleleft \langle (12)(24) \rangle \triangleleft \langle (12)(34), (13)(24) \rangle \triangleleft \text{Alt}(4) \triangleleft \text{Sym}(4)$$

is a chiefseries but not a compositions series for $\text{Sym}(4)$. The factors are isomorphic to $C_2 \times C_2$, C_3 and C_2 .

(f)

$$1 \triangleleft \langle (12)(34), (13)(24) \rangle \triangleleft \text{Alt}(4) \triangleleft \text{Sym}(4)$$

is a compositions series for $\text{Sym}(4)$. Since $\langle (12)(34) \rangle$ is not normal in $\text{Sym}(4)$, this is not a normal series and so also not a chiefseries. The factors are isomorphic to C_2 , C_2 , C_3 and C_2 .

(g) Let G be a groups. Then $\{1, G\}$ is a series for G , called the trivial series.

(h) Let G be a simple group. Then the trivial series is a composition series and a chiefseries for G . It is the only chiefseries for G , but there are example of simple groups which have non-trivial series Note here that only G^- is guaranteed to be normal in G , but G^- might be equal to G . But this shows that a simple groups cannot have a non-trivial descending series.

Lemma 2.4.13. Let G be a group, $H, K \leq G$ and $\mathcal{S}$ a series from H to K . Put $\mathcal{T} = \{K \cap S \mid S \in \mathcal{S}\}$. Then $\mathcal{T}$ is a series from $K \cap H$ to K and the factors of $\mathcal{T}$ are the groups

$$K \cap S / K \cap S^- \cong (K \cap S) S^- / S^-,$$

where $S \in \mathcal{S}$ with $K \cap S \neq K \cap S^-$. In particular, every factor of $\mathcal{T}$ is isomorphic to a subgroup of a factor of $\mathcal{S}$.

Proof. Since $H \in \mathcal{S}$, $H \cap K \in \mathcal{T}$ and since $G \in \mathcal{S}$, $K = K \cap G \in \mathcal{T}$. As $H \leq S$ for all $H \in \mathcal{S}$, $H \cap K \in H \cap S$ for all $H \cap S \in \mathcal{T}$. Since $\mathcal{S}$ is totally ordered also $\mathcal{T}$ is totally ordered with respect to inclusion.

Let $\mathcal{D}$ be a non-empty subset of $\mathcal{T}$ and put $\mathcal{E} := \{S \in \mathcal{S} \mid K \cap S \in \mathcal{D}\}$. Then $\mathcal{D} = \{K \cap S \mid S \in \mathcal{E}\}$.

Thus

$$\bigcap_{S \in \mathcal{E}} \mathcal{D} = \bigcap_{S \in \mathcal{E}} K \cap S = K \cap \bigcap_{S \in \mathcal{E}} S \in \mathcal{T} \text{ and } \bigcup_{S \in \mathcal{E}} \mathcal{D} = \bigcup_{S \in \mathcal{E}} K \cap S = K \cap \bigcup_{S \in \mathcal{E}} S \in \mathcal{T}$$

Thus $\mathcal{T}$ is closed under unions and intersections.

Let $T \in \mathcal{T}$ and define $S := \bigcap \{R \in \mathcal{S} \mid K \cap R = T\}$. Then $K \cap S = T$.

Let $R \in \mathcal{S}$. We will show that

$$(*) \quad R \not\leq S \text{ if and only if } K \cap R \not\leq T.$$

As $\mathcal{S}$ and $\mathcal{T}$ are totally ordered the negations of $R \not\leq S$ and $K \cap R \not\leq T$ are $S \leq R$ and $T \leq K \cap R$, respectively. Hence it suffices to show that

$$S \leq R \iff T \leq K \cap R.$$

Suppose $S \leq R$. Then $T = K \cap S \leq K \cap R$. Suppose next that $K \cap R \leq T$.

$$K \cap (S \cap R) = (K \cap S) \cap R = T \cap R = T$$

and so $S \leq S \cap R$ by definition of S . Thus $S \leq R$. Thus $(*)$ holds. It follows that

$$\begin{aligned} T^- &= \bigcup \{U \in \mathcal{T} \mid U \not\leq T\} = \bigcup \{K \cap R \mid R \in \mathcal{S}, K \cap R \not\leq T\} \\ &= \bigcup \{K \cap R \mid R \in \mathcal{S}, R \not\leq S\} = K \cap \bigcup \{R \mid R \in \mathcal{S}, R \not\leq S\} = K \cap S^- \end{aligned}$$

Since $S^- \trianglelefteq S$ we get $T^- = K \cap S^- \trianglelefteq K \cap S = T$. Thus $\mathcal{T}$ is a series from $K \cap H$ to H . Also

$$T/T^- = (K \cap S)/(K \cap S^-) = (K \cap S)/(K \cap S) \cap S^- \cong (K \cap S)S^-/S^- \leq S/S^-$$

Given any R in $\mathcal{S}$ with $T = K \cap R$ and $K \cap R^- \neq K \cap R$. Then $S \leq R$ by definition of S . Suppose for a contradiction that $R \neq S$. Then $S \not\leq R$ and so $S \leq R^-$. Thus

$$K \cap R = T = K \cap S \leq K \cap R^- \leq K \cap R$$

and so $K \cap R^- = K \cap R$, contrary to the choice of R . Thus $R = S$ and the factors are exactly as claimed. $\square$

Lemma 2.4.14. *Let G be a group and let*

$$\mathcal{S}: \quad 1 = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G_n = G$$

a subnormal series for G .

(a) *Let $N \trianglelefteq G$ and put $\overline{G} = G/N$. Then*

$$\overline{\mathcal{S}}: \quad \overline{1} = \overline{G_0} \trianglelefteq \overline{G_1} \trianglelefteq \overline{G_2} \trianglelefteq \dots \trianglelefteq \overline{G_{n-1}} \trianglelefteq \overline{G_n} = \overline{G}$$

is a subnormal series of $\overline{G}$ with factors

$$\overline{G_i}/\overline{G_{i-1}} \cong G_i/G_{i-1}/(G_i \cap N)G_{i-1}/G_{i-1}$$

where $1 \leq i \leq n$ with $G_i \neq (G_i \cap N)G_{i-1}$. In particular, each factor of $\overline{\mathcal{S}}$ is isomorphic to a quotient of a factor of $\mathcal{S}$.

(b) Let $A \leq G$ and $B \trianglelefteq A$. Put $\bar{A} = A/B$. Then

$$\bar{\mathcal{T}}: \quad \bar{1} = \overline{A \cap G_0} \trianglelefteq \overline{A \cap G_1} \trianglelefteq \overline{A \cap G_2} \trianglelefteq \dots \trianglelefteq \overline{A \cap G_{n-1}} \trianglelefteq \overline{A \cap G_n} = \bar{A}$$

is a subnormal series for $\bar{A}$ with factors

$$\overline{A \cap G_i} / \overline{A \cap G_{i-1}} \cong (A \cap G_i)G_{i-1} / G_{i-1} / (B \cap G_i)G_{i-1} / G_{i-1}$$

where $1 \leq i \leq n$ with $(A \cap G_i)G_{i-1} \neq (B \cap G_i)G_{i-1}$. In particular, each factor of $\bar{\mathcal{T}}$ is isomorphic to a section of a factor of $\bar{\mathcal{T}}$.

Proof. (a) Just observe that

$$\begin{aligned} \overline{G_i / G_{i-1}} &= G_i N / N / G_{i-1} N / N \\ &\cong G_i N / G_{i-1} N \\ &\cong G_i / (G_i \cap G_{i-1} N) \\ &= G_i / (G_i \cap N) G_{i-1} \\ &\cong G_i / G_{i-1} / (G_i \cap N) G_{i-1} / G_{i-1} \end{aligned}$$

(b) Just apply (a) to the subnormal series

$$\mathcal{T}: \quad 1 = A \cap G_0 \trianglelefteq A \cap G_1 \trianglelefteq G_2 \trianglelefteq \dots \trianglelefteq A \cap G_{n-1} \trianglelefteq A \cap G_n = A$$

of A and the normal subgroups B of A . □

Lemma 2.4.15. *Let G be a group and A and B subgroups of G such that A normalizes B . Suppose that A is solvable of derived length α and B hypoabelian of derived length β . Then AB is hypoabelian of derived length at most $\alpha + \beta$. In particular, if A and B are solvable, so is AB .*

Proof. Note that $AB/B \cong A/A \cap B$ and so AB/B is solvable of derived length at most α . Thus by (2.4.5)(c), AB is hypoabelian of derived length at most $\alpha + \beta$. □

Lemma 2.4.16. *Let A and B be normal nilpotent subgroups of the group G . Then AB is nilpotent of class at most $z_A + z_B$.*

Proof. Put $x = z_A$ and $y = z_B$ and $k = x + y - 1$. The proof is by induction on $x + y$.

Suppose $x = 0$. Then $A = 1$ and so $AB = B$. Hence AB is nilpotent of class z_B and the lemma holds.

So we may assume that $x > 0$ and by symmetry, also $y > 0$. Note that $Z(A) \trianglelefteq G$, $A/Z(A)$ is nilpotent of class $z_{A/Z(A)} = z_A - 1 = x - 1 < x$ and $BZ(A)/Z(A)$ is nilpotent of class at most $z_B = y$. Thus by induction $AB/Z(A)$ is nilpotent of class at most $(x - 1) + y$. Since $k = x + y - 1 = (x - 1) + y$, we conclude from 2.1.19 that $L_k(AB/Z(A)) = 1$. Thus $\mathcal{L}_k(AB) \leq Z(A)$, and by symmetry also $L_k(AB) \leq Z(B)$. It follows that $L_k(AB) \leq Z(A) \cap Z(B) \leq Z(AB)$ and so

$$L_{k+1}(AB) = [L_k(AB), AB] \leq [Z(AB), AB] = 1.$$

Another application of 2.1.19 now shows that $Z_{k+1}(AB) = 1$, so AB is nilpotent of class at most $k + 1$. As $k + 1 = x + y = z_A + z_B$ the lemma is proved. □

Chapter 3

π -separable groups and Hall π subgroups

3.1 The Theorem of Schur-Zassenhaus

Theorem 3.1.1 (Schur-Zassenhaus). *Let G be a finite group and K a normal subgroup of G such that $\gcd(|K|, |G/K|) = 1$. Then there exists a complement to K in G . If in addition, K or G/K is solvable¹, then all such complements are conjugate.*

Proof. We will first prove the existence of a complement. Let H be a subgroup of G minimal with respect to $G = HK$. Put $A = H \cap K$. By Homework 3, $A \leq \Phi(H)$. By (2.2.7)(b) $\Phi(H)$ is nilpotent and so also A is nilpotent. Put $\bar{H} = H/A'$. Note that $|\bar{A}|$ divides $|K|$ and that

$$|\bar{H}/\bar{A}| = |H/A| = |H/H \cap K| = |HK/K| = |G/K|$$

Thus $\gcd(|\bar{H}/\bar{A}|, |\bar{A}|) = 1$. Observe that $\bar{A}$ is abelian and so by Gaschütz' Theorem implies that there exist complement $\bar{U}$ to $\bar{A}$ in $\bar{H}$. Let U be the inverse image of $\bar{U}$ in H . Since $\bar{H} = \bar{U}\bar{A}$ and $\bar{U} \cap \bar{A} = 1$ we get $H = UA$ and $U \cap A = A'$. As $A \leq \Phi(H)$ we conclude that $H = U$ and so $A' = U \cap H = H \cap K = A$. Thus $l_A = 0$ and since A is nilpotent we get $A = L_0(A) = L_{l_A}(A) = 1$. Hence H is a complement to K in G .

Suppose K or G/K is solvable and let H_1 and H_2 be complements to K in G . We need to show that H_1 and H_2 are conjugate in G .

Suppose that K is solvable and put $\bar{G} = G/K'$. Then $\bar{K}$ is abelian and $\bar{H}_i$ is a complement to $\bar{K}$ in $\bar{G}$. As $\gcd(|K|, |G/K|) = 1$ we have $\gcd(|\bar{K}|, |\bar{G}/\bar{K}|) = 1$ and so by Gaschütz' Theorem there exists $g \in G$ with $\bar{H}_1^g = \bar{H}_2$. Then $K'H_1^g = K'H_2$ and H_1^g and H_2 are complement to K' in $K'H_2$. By induction on the derived length of K we know that H_1^g and H_2 are conjugate in $K'H_2$. Hence H_1 and H_2 are conjugate in G .

Suppose next that G/K is solvable. If $G = K$ then $H_1 = H_2 = 1$. So suppose $G \neq K$. As G/K is solvable we conclude $G/K \neq (G/K)'$. Hence $G \neq G'K$ and there exists a maximal subgroup M of G with $KG' \leq M$. Then $M \trianglelefteq G$ and so $|G/M| = p$ for some prime. Since $K \leq M$ and H_i is a complement to K in G we know from 1.3.8 that $M \cap H_i$ is a complement to K in M . Induction on $|G|$ shows that $(M \cap H_1)^g = M \cap H_2$ for some $g \in M$. Replacing H_1 by H_1^g we may assume that $M \cap H_1 = M \cap H_2$. Put $D = \langle H_1, H_2 \rangle$. Since $M \trianglelefteq G$ we have $M \cap H_i \trianglelefteq H_i$ and so $M \cap H_1$ is normal in D . Note that

$$|\bar{H}_i| = |H_i M / M = G/M| = p$$

Since $|\bar{H}_i|$ divides $|H_i|$ this implies that p divides $|H_i|$. Since H_i is a complement to K in H , we have $|H_i| = |G/K|$ and so $\gcd(|K|, |H_i|) = 1$. Thus p does not divide $|K|$. Observe that

¹Since K or G/K has odd order, the Feit-Thompson odd order theorem asserts that this assumption is always fulfilled

$$\overline{D}/\overline{H_i} = |D/(M \cap H_i)|/|H_i/(M \cap H_i)| = |D/H_i|$$

and

$$|K| = |G/H_i| = \frac{|G|}{|H_i|} = \frac{|D||G/D|}{|H_i|} = |D/H_i| \cdot |G/D| = |\overline{D}/\overline{H_i}| \cdot |G/D|$$

Thus $|\overline{D}/\overline{H_i}|$ divides $|K|$ and so p does not divide $|\overline{D}/\overline{H_i}|$. Hence $\overline{H_i}$ is a Sylow p -subgroup of $\overline{D}$. It follows that $\overline{H_1}^d = \overline{H_2}$ for some $d \in D$ and then $H_1^d = H_2$. So H_1 and H_2 are indeed conjugate in G . $\square$

3.2 π -separable and π -solvable groups

A class $\mathcal{D}$ is a statement $\Phi(x)$ involving a variable x . Let a be an object. We say that a is a member of $\mathcal{D}$ (or that $\mathcal{D}$ contains a) and write $a \in \mathcal{D}$ if $\Phi(a)$ is true.

Definition 3.2.1. A class of groups is a class $\mathcal{D}$ such that

- (i) All members of $\mathcal{D}$ are groups.
- (ii) $\mathcal{D}$ contains a trivial group.
- (iii) If $G \in \mathcal{D}$ and H is a group isomorphic to G , then $H \in \mathcal{D}$.

Definition 3.2.2. Let $\mathcal{D}$ be class of group and G a group.

- (a) A section of G is a group A/B where $A \leq G$ and $B \trianglelefteq A$.
- (b) G is a $\mathcal{D}$ -group if $G \in \mathcal{D}$.
- (c) $\mathcal{D}$ is closed under subgroups (quotients, sections), if any subgroup (quotient, section) of a $\mathcal{D}$ -group is a $\mathcal{D}$ -group.
- (d) $\mathcal{D}$ is closed under normal product, if AB is a $\mathcal{D}$ -group whenever A and B are normal $\mathcal{D}$ -subgroups of a group G .
- (e) G is called $\mathcal{D}$ -separable if there exists a subnormal series for G all of whose factors are $\mathcal{D}$ -groups. $\mathcal{D}_{\text{sep}}$ denotes the class of $\mathcal{D}$ -separable groups.
- (f) $\mathcal{D}(G)$ is the subgroup of G generated by all the subnormal $\mathcal{D}$ -subgroups of G .

Lemma 3.2.3. Let $\mathcal{D}$ a class of groups.

- (a) $(\mathcal{D}_{\text{sep}})_{\text{sep}} = \mathcal{D}_{\text{sep}}$, that is if G is a group with a subnormal series all of whose factors are $\mathcal{D}$ -separable, then also G is $\mathcal{D}$ -separable.
- (b) Suppose $\mathcal{D}$ is closed under subgroups (quotients, sections). Then also $\mathcal{D}_{\text{sep}}$ is closed under subgroup (quotient, section).
- (c) Any non-trivial $\mathcal{G}$ -separable group has a nontrivial subnormal $\mathcal{D}$ -subgroup, that is $\mathcal{D}(G) \neq 1$.

Proof. (a) Let $\mathcal{S}$ be a subnormal series all of whose factors are $\mathcal{D}$ -groups. Let H/H^- , $H \in \mathcal{S} \setminus \{1\}$, be factor of $\mathcal{S}$. Then there exists a subnormal series $\mathcal{S}_H$ of H/H^- whose factors are $\mathcal{D}$ -groups. Define

$$\mathcal{T}_H := \{K \leq H \mid H^- \leq K, K/H^- \in \mathcal{S}_H\} \quad \text{and} \quad \mathcal{T} := \bigcup_{H \in \mathcal{S} \setminus \{1\}} \mathcal{T}_H.$$

Then $\mathcal{T}$ is a subnormal series of G . Moreover, if K/K^- is factor of $\mathcal{T}$, then there exists $H \in \mathcal{S}$ with $K, K^- \in \mathcal{T}_H$. Hence K/K^- is isomorphic to the factor $K/H^- / K^-/H^-$ of $\mathcal{S}_H$. Thus K/K^- is a $\mathcal{D}$ -group and so G is $\mathcal{D}$ -separable.

(b) Let G be a $\mathcal{D}$ -separable group and $\mathcal{S}$ a subnormal series of G all of whose factors are $\mathcal{D}$ -groups. Also let R be a subgroup (quotient, section) of G . Then by 2.4.13 ((2.4.14)(a), (2.4.14)(b)) there exists a subnormal series $\overline{\mathcal{T}}$ of R all of whose factors are isomorphic to a subgroup (quotient, section) of a factor of $\mathcal{S}$. As the factors of $\mathcal{S}$ are $\mathcal{D}$ -groups and $\mathcal{D}$ is closed under subgroups (quotients, sections), we conclude that all factors of R are $\mathcal{D}$ -groups. Hence R is $\mathcal{D}$ -separable.

(c) follows immediately from the definition of $\mathcal{D}$ -separable. $\square$

Lemma 3.2.4. *Let $\mathcal{D}$ a class of groups and G a finite group. Suppose $\mathcal{D}$ is closed under normal products. Then $\mathcal{D}(G)$ is the largest subnormal $\mathcal{D}$ -subgroup of G .*

Proof. Since G is finite, there exists maximal subnormal $\mathcal{D}$ -subgroups A_1 and A_2 of G . Observe that we just need to show that $A_1 = A_2$. If $G = A_2$, then $A_1 \leq A_2$ and so $A_1 = A_2$ by maximality of A_1 . So we may assume that $G_1 \neq A_1$ and $G_2 \neq A_2$. Let $i \in \{1, 2\}$. Since $A_i \trianglelefteq G$ there exists $G_i \triangleleft G$ with $A_i \trianglelefteq G_i$. By induction on $|G|$ we know that $\mathcal{D}(G_i)$ is the largest subnormal $\mathcal{D}$ -subgroup of G_i . It follows that $A_i \leq \mathcal{D}(G_i) \trianglelefteq G$ and the maximality of A_i implies that $A_i = \mathcal{D}(G_i)$. Hence A_i is a characteristic subgroup of G and $G_i \triangleleft G$ we get $A_i \trianglelefteq G$. Since $\mathcal{D}$ is closed under normal products we conclude $A_1 A_2$ is a $\mathcal{D}$ -subgroup of G . As $A_1 A_2 \trianglelefteq G$ the maximality of A_1 and A_2 implies that $A_1 = A_1 A_2 = A_2$. $\square$

Corollary 3.2.5. *Let π be a set of primes and G a finite group. Then G has a largest subnormal π -subgroup $O_\pi(G)$.*

Proof. Just observe that the class of finite π -groups is closed under normal products. So 3.2.5 follows from 3.2.4. $\square$

Definition 3.2.6. *Let G be a group. Then $F(G)$ is the subgroup generated by the nilpotent subnormal subgroups of G and $\text{Sol}(G)$ is the groups generated by the solvable subnormal subgroups of G . $F(G)$ is called the Fitting subgroup of G .*

Corollary 3.2.7. *Let G be a finite group. Then $\text{Sol}(G)$ is the largest solvable subnormal subgroup of G and $F(G)$ is the largest nilpotent subnormal subgroup of G .*

Proof. By 2.4.15 and 2.4.16, respectively, the class of solvable groups and the class of nilpotent groups is closed under normal products. Hence from 3.2.4 shows that G has a largest solvable and a largest nilpotent subnormal subgroup. So the Corollary holds. $\square$

Definition 3.2.8. *Let π be a set of primes and G a group.*

- (a) $\mathcal{G}_\pi$ is the class of π -groups and $\mathcal{G}_{\text{Sol}}$ is the class of solvable groups.
- (b) G is called π -separable if G is $\mathcal{G}_\pi \cup \mathcal{G}_{\pi'}$ -separable.
- (c) G is called π -solvable if G is a $(\mathcal{G}_\pi \cap \mathcal{G}_{\text{Sol}}) \cup \mathcal{G}_{\pi'}$ -separable

Lemma 3.2.9. *Let π be a set of primes.*

- (a) *The class of π -separable groups and the class of π -solvable groups are both closed under sections.*
- (b) *$(\mathcal{G}_{\text{Sol}})_{\text{sep}} = \mathcal{G}_{\text{Sol}}$, that is any group, which has a subnormal series with solvable factors, is solvable.*
- (c) *Any π -subgroup of a π -solvable group is solvable.*
- (d) *Let G be a finite solvable group. Then G is π -solvable.*
- (e) *Let G be non-trivial finite π -separable group. Then $O_{\pi}(G) \neq 1$ or $O_{\pi'}(G) \neq 1$.*

Proof. (a) Observe that the class π -groups and the class of solvable groups are both closed under sections. By (3.2.3)(b) if a class $\mathcal{D}$ is closed under section, so is $\mathcal{D}_{\text{sep}}$. Thus (a) holds.

(b) Let $1 = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{n-1} \triangleleft G$ be a subnormal series of the group G all of whose factors are solvable. By induction on n we see that G_{n-1} is solvable. As also G/G_{n-1} is solvable we conclude that G is solvable, see (2.4.5)(d).

(c) Let G be a π -solvable subgroup and H a π -subgroup of G . Since H is a π -group no non-trivial section of H is a π' -group. On the other hand, by (a) H is π -solvable and so H has a subnormal series each of whose factors is solvable or a π' -group. It follows that all factors are solvable and (b) shows that H is solvable.

(d) Let $\mathcal{S}$ be a composition series of G and let F be factor of G . Then F is simple. As G is solvable also F is solvable. Hence $F' \neq F$ and so $F' = 1$. So F is abelian and since F is simple, $|F| = p$, a prime. Then $p \in \pi$ or $p \in \pi'$ and so F is a π - or a π' -group.

(e) Note that G is $\mathcal{G}_{\pi} \cup \mathcal{G}_{\pi'}$ -separable. Hence by (3.2.3)(c) there exists a non-trivial subnormal $\mathcal{G}_{\pi} \cup \mathcal{G}_{\pi'}$ -subgroup L of G . Then either L is a π -group or L is a π' -group. Hence $L \leq O_{\pi}(G)$ or $L \leq O_{\pi'}(G)$ and (e) holds. $\square$

Lemma 3.2.10. *Let π be a set of primes and G a finite π -separable group with $O_{\pi'}(G) = 1$. Then $C_G(O_{\pi}(G)) \leq O_{\pi}(G)$.*

Proof. Put $D := C_G(O_{\pi}(G))$ and $C := O_{\pi}(D)$. Then C is a normal π -subgroups of G and so $C \leq O_{\pi}(G)$. It follows that $[C, D] = 1$, so $C \leq Z(D)$. Let $E \leq D$ with $C \leq D$ and $E/C = O_{\pi'}(D/C)$. Then E/C is a π' -group and C is normal abelian π' -subgroup of E . By Gaschütz Theorem 1.3.11 there exists a complement K to C in E . Note that $K \cong E/C$ and so K is π' -group. From $C \leq Z(E)$ we see that K is normalized by C , and of course also by K . Thus $K \trianglelefteq CK = E$. As $E \trianglelefteq G$ this gives $K \trianglelefteq G$. Hence K is subnormal π -subgroup of G , so $K \leq O_{\pi'}(G) = 1$. Hence $E = C$ and so $O_{\pi'}(D/C) = 1$. Since $C = O_{\pi}(C)$, also $O_{\pi}(D/C) = 1$. Note that D/C is section of the π -separable group G , and so by 3.2.9 also D/C is π -separable. If $D/C \neq 1$, then (3.2.9)(e) shows that $O_{\pi}(D/C) \neq 1$ or $O_{\pi'}(D/C) = 1$, a contradiction. Thus $D/C = 1$ and so $D = C \leq O_{\pi}(G)$. $\square$

3.3 Sylow π - and Hall π -subgroups

Definition 3.3.1. *Let G be a group and π a set of prime. of G .*

- (a) *A Sylow π -subgroup of G is a maximal π -subgroup of G . $\text{Syl}_{\pi}(G)$ is the set of Sylow π -subgroups of G .*
- (b) *A π -subgroup H of G is called a Hall π -subgroup of G if, for all $p \in \pi$, H contains a Sylow p -subgroup of G . $\text{Hall}_{\pi}(G)$ is the set of Hall π -subgroups of G .*

Lemma 3.3.2. *Let G be a group and π a set of primes. Then every π -subgroups of G is contained in a Sylow π -subgroup of G . In particular, G has a Sylow π -subgroup.*

Proof. Let $\mathcal{D}$ be a set of π -subgroups of G which is totally ordered with respect to inclusion. Then $\bigcup \mathcal{D}$ is a π -subgroup of G . So the lemma follows from Zorn's lemma. $\square$

Lemma 3.3.3. *Let G be a finite group, π a set of primes and H a subgroup of G . Then H is a Hall π -subgroup of G if and only if $|H| = |G|_\pi$ and if and only if H is π -group and $|G/H|_\pi = 1$.*

Proof. Let p be a prime. By Sylow's Theorem for finite groups, the Sylow p -subgroups of G are exactly the subgroups of order $|G|_p$. Hence H contains a Sylow p -subgroup of G if and only if $|H|_p = |G|_p$. Note that

$$|H|_\pi = \prod_{p \in \pi} |H|_p \quad \text{and} \quad |G|_\pi = \prod_{p \in \pi} |G|_p$$

and so $|H|_\pi = |G|_\pi$ if and only if $|H|_p = |G|_p$ for all $p \in \pi$. It follows that $|H|_\pi = |G|_\pi$ if and only if H contains a Sylow p -subgroup of G for each $p \in \pi$. Also H is a π -group if and only if $|H| = |H|_\pi$.

Thus H is a π -Hall subgroup of G iff $|H| = |H|_\pi$ and $|H|_\pi = |G|_\pi$, and so iff $|H| = |G|_\pi$. Since $|G| = |G/H| \cdot |H|$, the latter holds iff $|G/H|_{\pi'} = 1$ and $|H|_\pi = |G|_\pi$. $\square$

Lemma 3.3.4. *Let G be a group and π a set of primes.*

- (a) *If the Sylow π -subgroups of G are conjugate in G , then all Sylow π -subgroups of G are Hall π -subgroups.*
- (b) *If G is finite, then all Hall π -subgroups of G are Sylow π -subgroups.*

Proof. (a) Let H be Sylow π -subgroup of G , let $p \in \pi$ and let S a Sylow p -subgroup of G . Then S is contained in a Sylow π -subgroup R of G . By assumption $R^g = H$ for some $g \in G$ and so S^g is a Sylow p -subgroups of G contained in H . Thus H is a Hall π -subgroup of G .

(b) By 3.3.3 any Hall π -subgroup of G has order $|G|_\pi$. On the other hand, any the order of any π -subgroup of G divides $|G|_\pi$. So any Hall π -subgroup of G is a maximal π -subgroup of G , that is a Sylow π -subgroup of G . $\square$

Example 3.3.5. Sylow p' -subgroup and Hall p' -subgroups of $\text{Sym}(p)$.

Let p be a prime, $G = \text{Sym}(p)$ and $I = \{1, 2, \dots, p\}$. Let $H \leq G$. We claim that $p \nmid |H|$ if and only if H acts transitively on I . Suppose first that $p \nmid |H|$. Then H has a subgroup K of order p . The size of any non-trivial of K on I divides p and so is equal to p . Thus K , and so also H , acts transitively on I . Conversely, if H acts transitively on I , then $p = |I| = |H/H_i|$ for $i \in I$ and so $p \nmid |H|$.

This proves the claim. It follows that H is a p' subgroup of H if and only if H does not act transitively on I , and so if and only if $H \leq N_G(J)$ for some proper, non-empty subset of J if I .

Next we show that $H \in \text{Syl}_{p'}(G)$ if and only if $H = N_G(J)$ for some $\emptyset \neq J \subset I$.

Suppose first that $H \in \text{Syl}_{p'}(G)$. Then $H \leq N_G(J)$, $\emptyset \neq J \subset I$, and the maximality of H implies that $H = N_H(J)$.

Suppose next that $H = N_G(J)$ for some $\emptyset \neq J \subset I$. Let L be a p' -subgroup of G with $H \leq L$. Then $L \leq N_H(K)$ for some $\emptyset \neq K \subset I$. So also $H \leq N_H(K)$ and so since only orbits of H on I are J and $I \setminus J$, we get $K = J$ or $K = I \setminus J$. In either case we get $N_G(K) = H$. So $L \leq K$ and $K = L$. Thus H is a maximal π -subgroup of G , that is $H \in \text{Syl}_{p'}(G)$.

It remains determine the Hall p' -subgroups of G . Observe that $|G|_{p'} = p!_{p'} = (p-1)!$ and so H is a Hall p' subgroups of G if and only if $|H| = (p-1)!$. Since Hall-subgroups are Sylow subgroups, we just have to determine all $\emptyset \neq J \subset I$ with $|N_G(J)| = (p-1)!$. Let $|J| = k$. Since

$$N_G(J) = \text{Sym}(J) \times \text{Sym}(I \setminus J),$$

we have $|N_G(J)| = k!(p-k)!$. Hence $N_G(J)$ is Hall p' -subgroup of G if and only if

$$\begin{aligned} & (p-1)! = k!(p-k)! \\ \iff & \frac{(p-1)!}{k!(p-k)!} = 1 \\ \iff & \prod_{i=1}^{k-1} \frac{p-k+i}{1+i} = 1 \quad (*) \end{aligned}$$

Observe that $p-k+i \geq 1+i$ with equality if and only if $p-k=1$. Hence $(*)$ holds if and only if either $k=1$ (and so $k-1=0$ and the product in $(*)$ is an empty product), or $k=p-1$ (and so $p-k=1$). Note that $|J|=1$ if and only if $|I \setminus J|=p-1$. Thus there exists exactly one conjugacy class of Hall p' -subgroups of G , namely the subgroups $N_G(J)$, $J \subset I$ with $|J|=1$.

Note that for $p \geq 5$, there exist subsets $K \subseteq I$ with $1 < |K| < p-1$ and so G has more than one conjugacy class of Sylow p' -subgroups.

Example 3.3.6. Sylow and Hall subgroups of $\text{Sym}(5)$

Let $G = \text{Sym}(5)$ and note that $|G| = 5! = 2^3 \cdot 3 \cdot 5$. Let π be a non-empty proper subset of $\{2, 3, 5\}$ and let $S \in \text{Syl}_\pi(G)$.

Suppose first that $\pi = \{p\}$. Then the Hall π subgroups are exactly the Sylow π subgroups and are conjugate in G . If $p=2$, the $|S| = 2^3$ and $S \cong D_8$. If $p=3$ or 5 , the $|S| = p$ and so $S \cong C_p$.

Suppose next that $\pi = \{2, 3\} = \pi(G) \cap 5'$. Then by 3.3.5 S is isomorphic to $\text{Sym}(3) \times \text{Sym}(2)$ or $\text{Sym}(4)$ with $S \in \text{Hall}_\pi(G)$ if $S \cong \text{Sym}(4)$. Thus there exists a Hall π -subgroup, G acts transitively on $\text{Hall}_\pi(G)$, but does not act transitively on $\text{Syl}_\pi(G)$.

Suppose that finally that $\pi = \{q, 5\}$ with $q \in \{2, 3\}$.

Assume that $5 \nmid |S|$. By Sylow's Theorem the number of Sylow 5-subgroups of H is $1 \pmod{5}$ and divides 3 if $q=3$ and 8 if $q=2$. Thus H has a unique Sylow 5-subgroup F . Hence $H \leq N_G(S)$. Since G has six Sylow 5-subgroups we have know that $|G/N_G(F)| = 6$ and so $|N_G(F)| = 20 = 4 \cdot 5$. If $q=2$ we get $N_G(S)$ is a π -subgroup of G and so $S = N_G(F)$ and $|S| = 20$. If $q=3$, the $N_G(F)|_\pi = 5$ and so $S = F \cong C_5$.

Assume that $5 \nmid |S|$. Then S is a q -groups and so S is a Sylow q -subgroup.

So if $\pi = \{3, 5\}$ then

$$\text{Syl}_\pi(G) = \text{Syl}_3(G) \cup \text{Syl}_5(G)$$

and if $\pi = \{2, 5\}$, then

$$\text{Syl}_\pi(G) = \text{Syl}_2(G) \cup \{N_G(F) \mid F \in \text{Syl}_5(G)\}$$

In both cases, $\text{Hall}_\pi(G) = \emptyset$ and G does not acts transitively on $\text{Syl}_\pi(G)$.

Example 3.3.7. Sylow $\{2, 3\}$ -subgroups of $GL_3(2)$.

Let V be a 3-dimensional vector-space over $\mathbb{F}_2$ and $G = \text{GL}_{\mathbb{F}_2}(V)$. Then $|V^\#| = 7$ and the number of basis of V is $7 \cdot 6 \cdot 4$. Since G acts regularly on the set of bases of V we get

$$|G| = 2^3 \cdot 3 \cdot 7$$

For $i = 1, 2$ let $\mathcal{P}_i$ be the set of i -dimensional subspaces of V . Since G acts transitively on bases it also acts transitively on $\mathcal{P}_i$. $\mathcal{P}_1 = \{\{0, v\} \mid v \in V^\#\}$ and so $|\mathcal{P}_1| = 7$. Also $\mathcal{P}_2 = \{\{0, a, b, a+b\} \mid a, b \in V^\#, a \neq b\}$ and so $|\mathcal{P}_2| = \frac{7 \cdot 6}{3 \cdot 2} = 7$.

Let $U_i \in \mathcal{P}_i$. Then $|G/N_G(U_i)| = |\mathcal{P}_i|$ and so $|N_G(U_i)| = \frac{|G|}{7} = 2^3 \cdot 3$. Thus $N_G(U_i)$ is a Hall $\{2, 3\}$ - and a Sylow- $\{2, 3\}$ -subgroup of G . We will now show that these are the only Hall $\{2, 3\}$ - and Sylow- $\{2, 3\}$ -subgroup of G .

Let $H \in \text{Syl}_{2,3}(G)$. Then H divides $2^3 \cdot 3$ and since the length of any orbit of H on $V^\#$ divides $|H|$ the possible length of orbits of H on V are

$$1, 2, 3, 4, \text{ and } 6$$

Suppose first that H has fixed a vector $a \in V^\#$. Put $U_1 = \{0, a\} \in \mathcal{P}_1$. Then $H \leq N_G(U_1)$. As $N_G(U_1)$ is $\{2, 3\}$ -subgroup of G , the maximality of H implies $H = N_G(U_1)$.

Supposes next that H does not fix non-zero vector, that is H does not have an orbits of length 1 on $V^\#$. Assume that $\{a, b\}$ is an orbit of length 2 of H on $V^\#$. Then H fixes $a+b$, a contradiction. Thus any orbits of H on $V^\#$ has length 3, 4 and 6. As $|V^\#|$ is odd we conclude that H has an orbit of $\{a, b, c\}$ of length 3 on $V^\#$. Then H fixes $a+b+c$ and so $a+b+c = 0$. It follows that $U_2 := \{0, a, b, c\} \in \mathcal{P}_2$ and $H \leq N_G(U_2)$. As above $H = N_G(U_2)$.

We proved that

$$\text{Syl}_{\{2,3\}}(G) = \text{Hall}_{\{2,3\}}(G) = \{N_G(U_1) \mid U_1 \in \mathcal{P}_1\} \cup \{N_G(U_2) \mid U_2 \in \mathcal{P}_2\}$$

In particular, there exist Hall $\{2, 3\}$ -subgroups of G , but G does not acts transitively on $\text{Hall}_{\{2,3\}}(G)$.

Lemma 3.3.8. *Let G be group and π a set of primes. Let $\mathcal{S}$ be non-empty G -invariant subset of $\text{Syl}_\pi(G)$. Then $\text{O}_\pi(G) = \bigcap \mathcal{S} = \bigcap \text{Syl}_\pi(G)$.*

Proof. Clearly $\bigcap \mathcal{S}$ is a normal π -subgroup of G and so

$$\bigcap \mathcal{S} \leq \text{O}_\pi(G)$$

Note that

$$\bigcap \text{Syl}_p(G) \leq \bigcap \mathcal{S}.$$

Let $H \in \text{Syl}_p(G)$ and let N a normal π -subgroup of G . Then NH is a π -group and so $N \leq H$ by maximality of H . Thus

$$\text{O}_\pi(G) \leq \bigcap \text{Syl}_\pi(G).$$

The three displayed inclusion imply the lemma. □

Observe that the preceding lemma provides a new proof that $\text{O}_\pi(G)$ is a π -group.

Lemma 3.3.9. *Let π be a set of primes and G a finite π -separable group. Then G has a Hall π -subgroup.*

Proof. If $G = 1$, then G is a Hall π -subgroup. So suppose $G \neq 1$. Then by (3.2.9)(e) $A := O_\pi(G) \neq 1$ or $B := O_{\pi'}(G) \neq 1$.

Suppose that $A \neq 1$. Note that $A \trianglelefteq G$ and by induction G/A has a Hall π -subgroup H/A . Then

$$|G|_\pi = |G/A|_\pi \cdot |A| = |H/A| \cdot |A| = |A|$$

and so H is a Hall π -subgroup G .

Suppose next that $A = 1$. Then $B \neq 1$. Note that $B \trianglelefteq G$ and by induction G/B has a Hall π -subgroup K/B . Hence $|G/B|_\pi = |K/B|$ and since B is a π -group,

$$|G|_\pi = |G/B|_\pi = |K/B|$$

Moreover, Schur-Zassenhaus 3.1.1 shows that there exists a complement H to B in K . Then

$$|H| = |B/K| = |G|_\pi$$

and so H is a Hall π -subgroup of G . □

Lemma 3.3.10. *Let π be set of primes and G a finite group. Suppose that G is π -solvable and let $\alpha = \pi$ or $\alpha = \pi'$. Then $\text{Syl}_\alpha(G) = \text{Hall}_\alpha(G)$ and G acts transitively on $\text{Syl}_\alpha(G)$.*

Proof. Since G is π -solvable, we see that G is π -separable and so also π' -separable. Thus G is α -separable and 3.3.9 shows that G has a Hall α -subgroup H . Let S be α -subgroup of G . We will show that

(*) $S^g \leq H$ for some $g \in G$.

By 3.3.8 $O_\alpha(G) \leq S \cap H$ and replacing G by $G/O_\alpha(G)$ we may assume that $O_\alpha(G) = 1$. Let $B = O_{\alpha'}(G)$. Since G is α -separable we get $B \neq 1$. Observe that HB/B is a Hall- α -subgroup of G/B and SB/B is α -subgroup of G/B . Hence by induction $S^h \leq HB$ for some $h \in G$. Without loss $S \leq HB$. Since $B \leq BS \leq BH$ we have $BS = B(BS \cap H)$. As S and H are π -groups, but B is a π' -group we get have $B \cap S = 1$ and $B \cap (BS \cap H) \leq B \cap H = 1$. So both S and $BS \cap H$ are complements to B in BS .

If $\alpha = \pi$, then BS/B is a π -subgroup of the π -solvable group G/B and so (3.2.9)(c) shows that BS/B is solvable. If $\alpha = \pi'$, the B is a π -subgroup of the π -solvable group G , and so B is solvable.

In either case we can apply 3.1.1 and conclude that $S^g = H \cap BS$ for some $g \in G$. So $S^g \leq H$ and (*) is proved.

Let $S \in \text{Syl}_\alpha(H)$. By (*) $S^g \leq H$ for some $g \in G$. The maximality of S gives $S = H$. Hence

$$\text{Syl}_\alpha(H) \subseteq H^G \subseteq \text{Hall}_\alpha(H) \subseteq \text{Syl}_\alpha(G)$$

and the lemma is proved. □

Lemma 3.3.11. *Let G be a finite group and A and B subgroups of G with $G = BA$.*

- (a) *If N is an A -invariant subgroup of B , then $\langle N^G \rangle \leq B$.*
- (b) *If π is set of primes with $|G/B|_\pi = 1$, then $\langle O_\pi(A)^G \rangle \leq B$.*

Proof. (a) $\langle N^G \rangle = \langle N^{AB} \rangle = \langle N^B \rangle \leq B$.

(b) As $O_\pi(A) \trianglelefteq A$ we know that $O_\pi(A)(A \cap B)$ is a subgroup of A . Hence $|O_\pi(A)(A \cap B)/A \cap B|$ divides $|A/A \cap B|$. As

$$|O_\pi(A)/O_\pi(A) \cap B| = |O_\pi(A)/O_\pi(A) \cap (A \cap B)| = |O_\pi(A)(A \cap B)/A \cap B|$$

and

$$|A/A \cap B|_\pi = |AB/B|_\pi = |G/B|_\pi = 1$$

we conclude that $|O_\pi(A)/(O_\pi(A) \cap B)|_\pi = 1$. Since $|O_\pi(A)/(O_\pi(A) \cap B)|_\pi$ also divides $|O_\pi(A)|$ and since $O_\pi(A)$ is a π -group we get $|O_\pi(A)B/B|_\pi = 1$. Thus $O_\pi(A) \leq B$. Hence $O_\pi(A)$ is an A -invariant subgroup of G , and so (b) follows from (a). $\square$

Lemma 3.3.12. *Let G be a finite group and π and μ sets of primes with $\pi' \cap \mu' = \emptyset^2$. Let A, B and C be subgroups of G and suppose that*

- (i) $G = AB = AC$.
- (ii) $|G/B|_\pi = 1$ and $|G/C|_\mu = 1$.
- (iii) A, B and C are solvable.

Then G is solvable.

Proof. We may assume without loss that $\text{Sol}(G) = 1$. Since $G = AB$ and $|G/B|_\pi = 1$, we get from (3.3.11)(b) that $\langle O_\pi(A)^G \rangle \leq B$. Since B is solvable we conclude that $\langle O_\pi(A)^G \rangle$ is a solvable normal subgroup of G and since $\text{Sol}(G) = 1$ we get $O_\pi(A) = 1$. By symmetry also $O_\mu(A) = 1$. From $\pi' \cap \mu' = \emptyset$ we have $\pi' \subseteq \mu$. So $O_{\pi'}(A) \leq O_\mu(A) = 1$. On the other hand since A is solvable, we know that A is π -solvable and so also π -separable. If $A \neq 1$ we conclude from (3.2.9)(e) that $O_\pi(A) \neq 1$ or $O_{\pi'}(A) \neq 1$. Thus $A = 1$ and so $G = AB = B$. Hence G is solvable. $\square$

Corollary 3.3.13. *Let G be a finite group and π and μ sets of primes with $\pi' \cap \mu' = 1$. Suppose there exists Hall π - and μ subgroups H_π and H_μ of G , respectively. Then $H_\pi H_\mu = G$ and $H_\pi \cap H_\mu$ is an Hall $\pi \cap \mu$ -subgroup of G .*

Proof. Since H_π and H_μ are Hall subgroups we have $|H_\pi| = |G|_\pi$ and $|H_\mu| = |G|_\mu$. Since $H_\pi \cap H_\mu$ is a $\pi \cap \mu$ subgroup of G we know that $|H_\pi \cap H_\mu| \leq |G|_{\pi \cap \mu}$. Thus

$$|G| \geq |H_\pi H_\mu| = \frac{|H_\pi| \cdot |H_\mu|}{|H_\pi \cap H_\mu|} \geq \frac{|G|_\pi \cdot |G|_\mu}{|G|_{\pi \cap \mu}} = |G|$$

Hence equality holds everywhere and so $|G| = |H_\pi H_\mu|$ and $|H_\pi \cap H_\mu| = |G|_{\pi \cap \mu}$. Thus $G = H_\pi H_\mu$ and $H_\pi \cap H_\mu$ is a Hall $\pi \cap \mu$ -subgroup of G . $\square$

Corollary 3.3.14. *Let G be a finite group. Suppose that for all $i, j \in \{1, 2, 3\}$ with $i \neq j$:*

- (i) π_i is a set of primes.
- (ii) H_i is a solvable Hall π_i -subgroup of G .
- (iii) $\pi'_i \cap \pi'_j = \emptyset$

Then G is solvable.

Proof. Let $k \in \{2, 3\}$. Since H_1 and H_k are Hall π_1 - and π_k -subgroups of G , respectively, and $\pi'_1 \cap \pi'_k = \emptyset$ we can apply 3.3.13 and conclude that $G = H_1 H_k$.

Since H_k is Hall π_k -subgroup of G we have $|G/H_k|_{\pi_k} = 1$. Also H_1, H_2, H_3 are solvable and $\pi'_2 \cap \pi'_3 = \emptyset$. So the hypothesis of 3.3.12 is fulfilled for $A = H_1, B = H_2, C = H_3, \pi = \pi_2$ and $\mu = \pi_3$. Thus G is solvable. $\square$

²i.e $\pi \cup \mu$ is the set of all primes

Definition 3.3.15. Let G be group. A commuting Sylow-system of G is family $(S_p)_{p \in \pi(G)}$ such that for all $p, q \in \pi(G)$, S_p is a Sylow p -subgroup of G and $S_p S_q = S_q S_p$.

Lemma 3.3.16. Let G be a finite group. Then the following are equivalent:

- (a) For each set of primes π , G has a Hall π -subgroup.
- (b) For each prime p , G has a Hall p' -subgroups.
- (c) G has a commuting Sylow-system.

Proof. (a) $\implies$ (b): Obvious.

(b) $\implies$ (c): For a prime p pick a Hall p' -subgroup L_p of G . For π of $\pi(G)$ define.

$$L_\pi = \bigcap_{p \in \pi} L_p$$

with $L_\pi = G$ if $\pi = \emptyset$.

We will show by induction on $|\pi|$ that L_π is a Hall π' -subgroup of G . If $\pi = \emptyset$ this is obvious. So we may choose $p \in \pi$. If $|\pi| = 1$, then $L_\pi = L_p$ is a Hall p' -subgroup of G . So suppose $|\pi| \geq 2$ and define $\mu := \pi \setminus \{p\}$. By induction L_μ is a Hall μ' subgroup of G . Note also that

$$\begin{aligned} L_\pi &= L_\mu \cap L_p \\ \mu' \cap p' &= (\mu \cup \{p\})' = \pi' \\ (\mu')' \cap (p')' &= \mu \cap \{p\} = \emptyset \end{aligned}$$

Hence 3.3.13 shows that L_π is a Hall π' -subgroup of G .

Define $S_\pi = L_{\pi(G) \setminus \pi}$. Since $\pi = (\pi(G) \setminus \pi') \cap \pi(G)$ we see that S_π is a Hall π -subgroup of G . In particular $S_p := S_{\{p\}}$ is a Sylow p -subgroup of G . Let $p \in \pi(G)$ with $p \neq q$ and put $\pi = \{p, q\}$. Then $S_p, S_q \leq S_\pi$ and $S_p \cap S_q = 1$. Thus

$$|S_p S_q| = \frac{|S_p| \cdot |S_q|}{|S_p \cap S_q|} = \frac{|G_p| \cdot |G_q|}{1} = |G_\pi| = |S_\pi|$$

Thus $S_\pi = S_p S_q$ and by symmetry, $S_q S_p = S_\pi$. It follows that $S_p S + q = S_q S_p$ and so $(S_p)_{p \in \pi(G)}$ is a commuting Sylow System for G .

(c) $\implies$ (a): Let $(S_p)_{p \in \pi(G)}$ be a commuting Sylow system. Choose an ordering on $\pi(G)$ and $\pi \subseteq \pi(G)$ define

$$H_\pi = \prod_{p \in \pi} S_p$$

with $H_\pi = 1$ if $\pi = \emptyset$. Suppose inductively that H_π is a π -subgroup of G and let $p \in \pi(G) \setminus \pi$. Th. Since $S_q S_p$ for all $p \in \pi$ we have $H_\pi S_q = S_q H_\pi$

. Hence $H_\pi S_q$ is a $\pi \cup \{q\}$ -subgroups of G . So H_π is a π -subgroup of G . Since it contains a Sylow p -subgroup for each $p \in \pi$, it is a Hall π -subgroup. □

Lemma 3.3.17. Let G be a finite group with a Sylow-system $(S_p)_{p \in \pi(G)}$. Suppose that $S_p S_q$ is solvable for all $p, q \in \pi(G)$. Then G is solvable.

Proof. If $|G|$ has at most two primes divisor, $G = S_p S_q$ for some $p, q \in \mathbb{P}$ and the lemma holds. So suppose p_1, p_2, p_3 are three distinct primes dividing $|G|$. Define $H_i = \prod_{q \in p'_i} S_q$. Then H_i is Hall p'_i -subgroups. By induction on the number of primes divisors, each H_i is solvable. So by 3.3.14, G is solvable. □

Chapter 4

Subnormal subgroups and near-components

4.1 Join of Subnormal Subgroups

Lemma 4.1.1. *Let G be a finite group and $\mathcal{A}$ a set of subnormal subgroups of G . Then $\langle \mathcal{A} \rangle$ is subnormal in G .*

Proof. If $|\mathcal{A}| \leq 1$, the lemma holds. So suppose $|\mathcal{A}| \geq 2$. Choose $A \in \mathcal{A}$ with $|G/A|$ -minimal and let $B \in \mathcal{A}$ with $A \neq B$. The proof is by induction on $|G/A|$ and then on $|\mathcal{A}|$. Assume $|\mathcal{A}| \geq 3$ and put $F := \langle \mathcal{A} \setminus \{B\} \rangle$. By induction on $|\mathcal{A}|$ we get $F \trianglelefteq G$ and then $\langle \mathcal{A} \rangle = \langle F, B \rangle \trianglelefteq G$.

So we may assume that $|\mathcal{A}| = 2$. Then $\langle \mathcal{A} \rangle = \langle A, B \rangle$. Since $A \trianglelefteq G$ there exists a subnormal series

$$A = A_0 \trianglelefteq A_1 \trianglelefteq \dots \trianglelefteq A_{n-1} \trianglelefteq A_n$$

If $n = 0$ then $A = G$ and so $\langle A, B \rangle = G \trianglelefteq G$. So suppose $n \geq 1$. Note that $A^b \trianglelefteq A_{n-1}$ for all $b \in B$ and since $|A_{n-1}/A| < |G/A|$ induction on $|G/A|$ shows that $D := \langle A^B \rangle \trianglelefteq A_{n-1} \trianglelefteq D$.

Suppose that $D \neq A$. Then $|G/D| \leq |G/A|$ and induction on $|G/A|$ shows that $\langle D, B \rangle \trianglelefteq G$. As $\langle A, B \rangle = \langle D, B \rangle$ we are done in this case.

Suppose next that $A = B$ and put $E := \langle A_1, B \rangle$. Then $A \trianglelefteq E$. Also since $|G/A_1| < |G/A|$, induction on $|G/A|$ shows that $E \trianglelefteq G$. As $B \trianglelefteq G$ and $B \leq E$ we have $B \trianglelefteq E$ and so there exists a subnormal series

$$B = B_0 \trianglelefteq B_1 \trianglelefteq \dots \trianglelefteq B_{m-1} \trianglelefteq B_m = E$$

It follows that

$$\langle A, B \rangle = AB = AB_0 \trianglelefteq AB_1 \trianglelefteq \dots \trianglelefteq AB_{m-1} \trianglelefteq AB_m = E \trianglelefteq G$$

and so again $\langle A, B \rangle \trianglelefteq G$. □

4.2 Near-components

Definition 4.2.1. *Let G be a group.*

- (a) $M(G)$ is the subgroup of G generated by the proper normal subgroups of G .
- (b) G is called nearly simple if G is perfect and $G \neq M(G)$.

- (c) A near-component of G is a subnormal, nearly simple subgroup of G .
- (d) G is called quasi-simple, if G is a non-trivial perfect group with $G/Z(G)$ simple.
- (e) A component of G is a subnormal, quasi-simple subgroup of G .
- (f) $\mathcal{N}(G)$ is the set of near-components of G , $\mathcal{N}_*(G)$ is the set of minimal near-components of G and $\mathcal{N}^*(G)$ is the set of maximal near-components of G .
- (g) $\mathcal{E}(G)$ is the set of components of G , $E(G) := \langle \mathcal{E}(G) \rangle$ and $F^*(G) := F(G)E(G)$. $F^*(G)$ is called the generalized Fitting subgroup of G .

Lemma 4.2.2. *Let G be a group.*

- (a) *If $G \neq M(G)$, then $G/M(G)$ is simple.*
- (b) *G is a quasi-simple if and only if G is nearly simple and $M(G) = Z(G)$.*
- (c) *Suppose G is quasi-simple and let $L \trianglelefteq G$ with $L \not\leq M(G)$. Then $L = G$.*
- (d) *$\mathcal{E}(G) \subseteq \mathcal{N}^*(G)$.*

Proof. (a) Let $N/M(G)$ be a normal subgroup of $G/M(G)$. By definition of $M(G)$ either $N \leq M(G)$ or $N = G$. Thus $N/M(G) = 1$ or $N/M(G) = G/M(G)$.

(b) Suppose first that G is quasi-simple and let $N \trianglelefteq G$ with $N \not\leq Z(G)$. Since $G/Z(G)$ is simple, $G = NZ(G)$ and so $G = G' = [G, NZ(G)] = [G, N] \leq N$. Thus $N = G$ and so $M(G) \leq Z(G)$. Since $G = G' \neq 1$, $G \neq Z(G)$ and so also $M(G) \neq G$. Thus G is nearly simple.

Suppose next that G is nearly simple and $M(G) = Z(G)$. By definition of nearly simple, G is perfect and by (a), $G/M(G)$ is simple. Thus $G/Z(G)$ is simple and so G is quasi-simple.

(c) Any proper subnormal subgroup of G is contained in a proper normal subgroup of G , and all proper normal subgroups of G are contained in G . So (c) holds.

(d) Let K be a component of G . Then K is quasi-simple and (b) shows that K is nearly simple. As $K \trianglelefteq G$ this shows that K is near component of G . Let L be a near-component of G with $L \leq K$. By (b) $M(K) = Z(K)$ and since L is not abelian and we get $L \not\leq M(K)$. Now (c) shows that $L = K$. Thus K is a minimal near component of G . $\square$

Lemma 4.2.3. *Let G be a group, $N \trianglelefteq G$ and $L \leq N$.*

- (a) *L is subnormal in N if and only if L is subnormal in G .*
- (b) *L is a near component of N if and only if L is near component of G . In particular, $\mathcal{N}(N) \subseteq \mathcal{N}(G)$.*
- (c) *L is a component of N if and only if L is component of G . In particular, $\mathcal{E}(N) \subseteq \mathcal{E}(G)$ and $E(N) \leq E(G)$.*
- (d) *$F(N) \leq F(G)$ and $F^*(N) \leq F^*(G)$.*

Proof. (a) If $\mathcal{S}$ is a subnormal series from L to N , then $\mathcal{S} \cup \{G\}$ is a subnormal series from N to G . If $\mathcal{T}$ is a subnormal series from L to G , then $\{T \cap N \mid T \in \mathcal{T}\}$ is a subnormal series from N to L .

(b) and (c) follows immediately from (a).

(d) By (a) any nilpotent subnormal subgroup of G is a nilpotent subnormal subgroups of G . Thus $F(N) \leq F(G)$. By (c) we have $E(N) \leq E(G)$, so $F^*(N) \leq F^*(G)$. $\square$

Lemma 4.2.4. *Let G be a finite group and $N \trianglelefteq G$ with G/N perfect.*

- (a) *There exists a smallest subnormal supplement R to N in G .*
- (b) *$R \trianglelefteq G$ and R is perfect.*
- (c) *Let L be a subnormal supplement to N in G . Then $L/L \cap N \cong G/N$ and R is smallest subnormal supplement to $L \cap N$ in L .*
- (d) *Suppose in addition that G/N is simple. Then $M(R) = R \cap N$, $G/N \cong R/M(R)$ and R is the unique near-component of G with $R \not\leq N$.*

Proof. We will first prove:

- (*) *Let L be a supplement to N in G . Then $L/L \cap N \cong G/N$. In particular, $L/L \cap N$ is perfect.*

Since $G = LN$ we have $L/L \cap N \cong LN/N \cong G/N$.

- (**) *Let G_1 and G_2 be normal supplements to N in G . Then also $[G_1, G_2]$ is a normal supplement to N in G .*

Note that $G = NG_1 = NH_2$ and since G/N is perfect we get

$$G = N[G, G] = N[NG_1, NG_2] = N[G_1, G_2].$$

- (***) *L be a subnormal supplement to N in G and $D \leq L$. Then D is a minimal subnormal supplement to $L \cap N$ in L , if and only if D is a minimal subnormal supplement to N in G .*

Since $L \trianglelefteq G$ we know that $D \trianglelefteq G$ if and only if $D \trianglelefteq L$. As $G = NL$ and $D \leq L$, (1.3.7)(a) shows that D is a supplement to $L \cap N$ in L if and only if D is a supplement to N in G . This gives (**).

(a) Let S_1 and S_2 be minimal subnormal supplement to N in G . If $S_1 = G$ we get $S_1 \leq S_2$ and so $S_1 = S_2$. Thus we may assume that $S_i \neq G$ and so there exists $G_i \triangleleft G$ with $S_i \leq G_i$. Put $G_0 := [G_1, G_2]$. Then by (**) G_0 is a normal supplement to N in G . Let $j \in \{0, 1, 2\}$. By (*) $G_j/G_j \cap N$ is perfect and so by induction there exists smallest subnormal supplement R_j to $G_j \cap N$ in G_j . Let $i \in \{1, 2\}$. By (***) applied to (G, G_i, S_i) in place of (G, L, D) we see that S_i is a minimal normal supplement to $G_i \cap N$ in G_i . Thus $S_i = R_i$. By (***) applied to (G_i, G_0, R_0) in place of (G, L, D) we see that R_0 is a minimal normal supplement to $G_i \cap N$ in G_i . Thus $R_0 = R_i$. Hence $S_1 = R_1 = R_0 = R_2 = S_2$. So (a) holds.

(b) Since $N \trianglelefteq G$ and R is uniquely determined by G and N we get $N \trianglelefteq R$. Now (**) shows that $[R, R]$ is normal supplement to N in G and so $R = [R, R]$ by minimality of R .

(c) follows from (*) and (**).

(d) Suppose G/N is simple. We first show

- (+) *$K \trianglelefteq G$. Then $G = KN = G$ if and only if $K \not\leq N$.*

If $KN = G$, then certainly $K \neq N$. If $K \leq N$, then $1 \neq KN/N \trianglelefteq G/N$ and since G/N is simple we get $KN/N = G/N$ and $G = KN$. So (+) holds.

Let K be a proper normal subgroup of R . The minimality of R shows that $G \neq KN$ and this (+) gives $K \leq N$. Thus $M(R) = R \cap N$. By (b) $R/R \cap N \cong G/N$ and so $R/M(R) \cong G/N$. By (b) R is perfect and since $M(R) = R \cap N \neq N$ we see that R is nearly-simple. Hence R is a near component of G with $R \not\leq N$.

Next let K be any near-component of G with $K \not\leq N$. By (+) $G = KN$ and the minimality of R gives $R \leq K \leq G = NR$. It follows that $K = (K \cap N)R$. Since $K \not\leq N$ we know that $K \cap N \neq K$ and so $K \cap N \leq M(K)$. Thus $R \not\leq M(K)$ and since $R \trianglelefteq K$ we get $R = K$. $\square$

Lemma 4.2.5. *Let G be a finite group, K a near-component of G and N a subnormal subgroup of N . Then one of the following holds:*

- (1) $K \leq N$.
- (2) N normalizes K and $[K, N] \leq M(K)$.

Proof. If $N = G$, then (1) holds. So suppose $N \neq G$ and let H be a maximal normal subgroup of G with $N \leq H$. If $K \leq H$, then (1) or (2) holds by induction on $|G|$.

So suppose $K \not\leq H$. Note that G/H is simple. Since $K' = K \not\leq H$ we see that $(G/H)' \neq 1$. Thus $(G/H)' = G/H$, so G/H is perfect. Thus we can apply 4.2.4 with N in place of G . Since $K \not\leq H$ and K is a near component of G , (4.2.4)(d) shows that K is the smallest subnormal supplement to N in G and $K \cap H = M(K)$. By (4.2.4)(b) $K \trianglelefteq G$ and so

$$[K, N] \leq [K, H] \leq K \cap H = M(K)$$

and (2) holds. □

Lemma 4.2.6. *Let K and L be near-components of a finite groups G . Then exactly one of the following holds.*

$$K = L, \quad K \leq M(L), \quad L \leq M(K), \quad [K, L] \leq M(L) \cap M(K)$$

In particular,

$$K \leq L \quad \text{or} \quad [K, L] \leq M(K)$$

Proof. We will first show that one of the four statements hold. We may assume that $K \not\leq M(L)$ and $L \not\leq M(K)$. Suppose that $K \leq L$. Note that $L/M(L)$ is a perfect simple group and so by (4.2.4)(d) there exists a unique near component of L not contained in $M(L)$. Since both K and L are near components of L not contained in $M(L)$ conclude that $K = L$. So suppose $K \not\leq L$. By symmetry we may also assume $L \not\leq K$. Then by 4.2.5 $[K, L] \leq M(K)$ and by symmetry, $[K, L] \leq M(L)$.

So one of the four statements hold.

As $K \neq M(K)$ and $L \neq M(L)$ the first three statement are mutually exclusive.

Suppose one of the first two statement holds. Then $K \leq L$ and so $K = [K, K] \leq [K, L]$ and $[K, L] \not\leq M(K)$. So the fourth statements does not hold.

By symmetry, if the third statement holds, the fourth one does not. □

Lemma 4.2.7. *Let G be a finite group and K a component of G .*

- (a) *Let $N \trianglelefteq G$. Then $K \leq N$ or $[K, N] = 1$.*
- (b) *Let L be a component of G . Then $K = L$ or $[K, L] = 1$.*
- (c) *$[K, \text{Sol}(G)] = [K, F(G)] = 1$. In particular, $[E(G), \text{Sol}(G)] = 1$ and $[E(G), F(G)] = 1$.*

Proof. (a) Suppose $K \not\leq N$. Then by 4.2.5 $[K, N] \leq M(K) = Z(K)$. Thus

$$[[N, K], K] \leq [Z(K), K] = 1 \quad \text{and} \quad [[K, N], K] = [[N, K], K] = 1.$$

So by the Three Subgroup Lemma 2.1.3 $[[K, K], N] = 1$. Since K is perfect, $K = [K, K]$ and so $[K, N] = 1$.

(b) Suppose $[K, L] \neq 1$. Then by (a), $K \leq L$. By symmetry, $L \leq K$ and so $L = K$.

(c) Since $1 \neq K = K'$, K is not solvable. Thus $K \not\leq \text{Sol}(G)$ and so by (a), $[K, \text{Sol}(G)] = 1$. Since $F(G) \leq \text{Sol}(G)$ also $[K, F(G)] = 1$. □

Definition 4.2.8. Let G be a group.

- (a) G is called *nearly-abelian* if $H \leq Z(G)$ for all proper normal subgroups H of G .
- (b) $F^*(G)$ is the subgroup generated by the nearly-abelian subnormal subgroups of G . $F^*(G)$ is called the *generalized Fitting subgroup* of G .
- (c) $E(G)$ is the subgroup generated by the components of G .

Lemma 4.2.9. Let G be a finite group.

- (a) $C_G(F^*(G)) \leq F^*(G)$.
- (b) Suppose G is solvable. Then $E(G) = 1$ and $C_G(F(G)) \leq C_G(\overline{F}(G))$.

Proof. Put $H := C_G(F^*(G))$. Note that $F^*(G)$ and so also H is normal in G .

Suppose for a contradiction that $H \not\leq F^*(G)$ and let K be a subnormal subgroup of H minimal with $K \not\leq F^*(G)$. By minimality of K any proper normal subgroup of K is contained in $F^*(G)$. Thus

$$M(K) \leq K \cap F^*(G) \leq K \cap C(G) = Z(K)$$

Assume that $K = K'$. Then $K \not\leq Z(K)$ and so $M(K) = Z(K)$. Thus 4.2.2 shows that K is quasi-simple and so K is a component of G . Thus $K \leq E(G) \leq F^*(G)$, a contradiction.

Assume that K is not perfect. Then $K' \leq M(K) \leq Z(K)$ and so $K/Z(K)$ is abelian. Hence $K = Z_2(K)$ and K is nilpotent. Thus $K \leq F(G) \leq F^*(G)$, a contradiction.

(b) Suppose G is solvable. Then 2.4.4 shows that G does not have a non-trivial perfect subgroups. So G has no components. It follows that $E(G) = 1$ and so $F^*(G) = F(G)$. Thus (b) follows from (a) $\square$

Definition 4.2.10. A partially ordered set $(I, \leq)$ is called *totally unordered* if $a = b$ for all $a, b \in I$ with $a \leq b$.

Lemma 4.2.11. Let G be a finite group and $\mathcal{K}$ a totally unordered set of near-components of G .

$$E := \langle \mathcal{K} \rangle, \quad M := \langle M(K) \mid K \in \mathcal{K} \rangle \quad \text{and} \quad \overline{E} := E/M$$

Let $K \in \mathcal{K}$ and put

$$K^\perp = \langle \mathcal{K} \setminus \{K\} \rangle M$$

- (a) E is a perfect subnormal subgroup of G .
- (b) $[K, K^\perp] \leq M(K) \leq K$.
- (c) $K \trianglelefteq E$, $M(K) \trianglelefteq E$, $M \trianglelefteq E$ and $K^\perp E$.
- (d) $K \cap M = K \cap K^\perp = M(K)$, $E = KK^\perp$ and $\overline{K} \cong E/K^\perp \cong K/M(K)$. In particular, $\overline{K}$ is a perfect simple group.
- (e) $K^\perp = C_E(K/M(K))$ and $K^\perp$ is the unique maximal normal subgroup of E with $K \not\leq K^\perp$.
- (f)

$$\overline{E} = \bigoplus_{K \in \mathcal{K}} \overline{K} \cong \bigoplus_{K \in \mathcal{K}} K/M(K).$$

- (g) Let R be a near-component of E . Then there exists $L \in \mathcal{K}$ with $R \leq L$. Moreover, either $R = L \in \mathcal{K}$ and $R \not\leq M$ or $R \leq M(L) \leq M$.

(h)

$$\mathcal{K} = \mathcal{N}^*(E) = \{L \in \mathcal{N}(E) \mid N \not\leq M\}$$

- (i) Let N be maximal normal subgroup of E . Then there exists a unique $K_N \in \mathcal{N}(E)$ with $K_N \not\leq N$. Moreover, $K_N \in \mathcal{K}$ and $M \leq N = K_N^\perp$.
- (j) The function $K \mapsto K^\perp$ is a bijection between $\mathcal{K}$ and the set of maximal normal subgroups of E with inverse $N \mapsto K_N$.
- (k) M is the intersection of the maximal normal subgroups of E .

Proof. (a) By 4.1.1 E is subnormal in G . Any group generated by perfect subgroups is perfect and so (a) holds.

(b) and (c): Let $L \in \mathcal{K}$ with $K \neq L$. Since $\mathcal{K}$ is totally unordered we get $K \neq L$ and so 4.2.6 implies

$$[K, L] \leq M(K) \leq M$$

In particular, L normalizes K . It follows that $K \trianglelefteq E$ and since $M(K)$ is a characteristic subgroup of G , also $M(K) \trianglelefteq E$. Thus in turn implies that $M \trianglelefteq E$ and $K^\perp \trianglelefteq E$.

Note that $[K, M(L)] \leq [K, L] \leq L(K)$ and $[K, M(K)] \leq M(K)$. As $M(K) \trianglelefteq E$ this gives $[K, K^\perp] = [K, \langle \mathcal{K} \setminus \{K\} \rangle M \leq M(K)$. So (b) and (c) hold.

(d) Since $[K, K^\perp] \leq M_K$ and $[K, K] = K \not\leq M(K)$ we have $K \neq K^\perp$. Thus $K \cap K^\perp$ is a proper normal subgroup of K , so and so

$$K \cap K^\perp \leq M(K) \leq K \cap M \leq K \cap K^\perp$$

It follows that $K \cap K^\perp = M(K) = K \cap M$. Since $\langle \mathcal{K} \setminus \{K\} \rangle \leq K^\perp \leq E$ we have $E = \langle \mathcal{K} \rangle = \langle K, K^\perp \rangle = KK^\perp$ and then

$$E/K^\perp = KK^\perp/K^\perp \cong K/K \cap K^\perp = K/K \cap M \cong KM/M = \overline{K}$$

Also $K/K \cap M = K/M(K)$. By (4.2.2)(a) $K/M(K)$ is simple and since K is perfect also $K/M(K)$ is perfect. Thus all parts of (d) are proved.

(e) From $[K, K^\perp] = K \not\leq C_E(K/M(K))$ we know that $C_E(K/M(K))$ is a proper normal subgroup of G . By (e) $K^\perp \leq C_E(K/M(K))$. By (d) $E/K^\perp$ simple, so $K^\perp$ is a maximal normal subgroup of E . Thus $K^\perp = C_E(K/M(K))$.

Let N be any normal subgroup of E with $K \not\leq N$. By 4.2.5 $[K, N] \leq M(K)$. Thus $N \leq C_E(K/M(K)) = K^\perp$ and so $K^\perp$ is the unique maximal normal subgroup of E not containing K . Hence (e) is proved.

(f) From $KM \cap K^\perp = (K \cap K^\perp)M = M$ we get $\overline{K} \cap \overline{K}^\perp = 1$. Together with $\overline{E} = \langle \overline{K} \mid K \in \mathcal{K} \rangle$, $\overline{K} \trianglelefteq \overline{E}$ and $\overline{K}^\perp = \langle \overline{L} \mid L \in \mathcal{K} \setminus \{K\} \rangle$, this shows that $\overline{E}$ is the internal direct sum of $\{\overline{K} \mid K \in \mathcal{K}\}$. Thus (f) holds.

(g) Let R be a near-component of E . Then $R = [R, E] \leq [R, E]$ and so $[R, E] \not\leq M(R)$. Hence there exists $L \in \mathcal{K}$ with $[R, L] \not\leq M(R)$. By 4.2.6 $R \leq L$ or $[R, L] \leq M(R)$, so $R \leq L$. Hence $R \trianglelefteq L$ and so either $R = L$ or $R \leq M(L)$. Thus (g) holds.

(h) By (g) each-component of E is contained in an member of $\mathcal{K}$. As $\mathcal{K}$ is totally unordered, no elements on $\mathcal{K}$ is contained in another element of $\mathcal{K}$. So $\mathcal{K}$ is exactly the set of maximal near components of E . Moreover, by (g) any near component of E not contained in M is contained $\mathcal{K}$, so (h) holds.

(i) Let N be a maximal normal subgroup of E . Then E/N is simple and Since E is perfect, also E/N is perfect. Now (4.2.4)(d) shows there exists a unique near-component K_N of E with $K_N \not\leq N$. By (g), $K_N \leq L$ for some $L \in \mathcal{K}$. As $K_N \not\leq N$ also $L \not\leq N$. Thus L is near-component of with $L \not\leq N$. So $K_N = L$ by

uniqueness of L . Hence $K_N \in \mathcal{K}$. As N is maximal normal subgroup of E with $K_N \not\leq K$, we conclude from (e) that $N = K_N^\perp$.

(j) By (e) $K^\perp$ is maximal normal subgroup of K . Also K a near component of E with $K \not\leq K^\perp$, so $K = K_{K^\perp}$.

If N is a maximal normal subgroup of E , then (i) shows that $K_N \in \mathcal{K}$ and $N = K_N^\perp$. Thus the two functions in (j) are well define and inverse to each other.

(k) By (j) $\{K^\perp \mid K \in \mathcal{K}\}$ is the set of maximal normal subgroups of G . By (f)

$$\overline{E} = \bigoplus_{K \in \mathcal{K}} \overline{K}$$

As $\overline{K^\perp} = \langle \overline{L} \mid L \in \mathcal{K} \setminus \{K\} \rangle$, this implies that $\bigcap_{K \in \mathcal{K}} \overline{K^\perp} = 1$. Since $M \leq K^\perp$ we conclude that $\bigcap_{K \in \mathcal{K}} K^\perp = M$ and so (k) is proved. $\square$

Lemma 4.2.12. *Let G be a finite group and $H \trianglelefteq G$.*

- (a) $\mathcal{N}^*(H)$ is a totally unordered set of near-components of G .
- (b) $\mathcal{N}_*(H)$ is a totally unordered set of near-components of G
- (c) $\mathcal{E}(H)$ is a totally unordered set of near-components of G .
- (d) Let K is a near-component of H . Then K^H is a totally unordered set of near-components of G . In particular, $K \trianglelefteq \langle K^H \rangle$.

Proof. (a) and (b) Just observe that the set of minimal and the set of maximal elements of any partially ordered set is totally unordered.

(d) By (4.2.2)(d) $\mathcal{E}(H) \subseteq \mathcal{N}_*(H)$. As $\mathcal{N}_*(H)$ is totally unordered, so is $\mathcal{E}(H)$.

(c) Let $L, R \in K^H$ with $L \leq R$. Note that $|L| = |K| = |R|$ and so $L = R$. $\square$

Corollary 4.2.13. *Let G be a finite group. Then the function $\mathcal{K} \mapsto \langle \mathcal{K} \rangle$ is a bijection between the set of totally unordered sets of near-components of G and set of perfect subnormal subgroups of G with inverse $H \rightarrow \mathcal{N}^*(H)$.*

Proof. Let $\mathcal{K}$ be totally unordered set of near-components of G . By 4.2.11 $\langle \mathcal{K} \rangle$ is a perfect subnormal subgroup of G and $\mathcal{N}^*(\langle \mathcal{K} \rangle) = \mathcal{K}$.

Next let H be a perfect subnormal subgroup of G . By (4.2.12)(a) $\mathcal{N}^*(H)$ is a totally unordered set of near-components of G . Put $D = \langle \mathcal{N}^*(H) \rangle$ and suppose for a contradiction that $D \neq H$. Note that $D \trianglelefteq H$ and so there exists a maximal normal subgroup N of G with $D \leq N$. As H is perfect, H/N is a perfect simple group. Thus by (4.2.4)(d) there exists component R of H with $R \not\leq N$. Observe that $R \leq K$ for some $K \in \mathcal{N}^*(H)$. Since $R \not\leq N$ also $K \not\leq N$. But $K \leq D \leq N$ a contradiction. Thus $H = D = \langle \mathcal{N}^*(H) \rangle$.

We proved that the two functions are well-defined and inverse to each other. Thus the corollary holds. $\square$

Lemma 4.2.14. *Let G be a finite group and $\mathcal{S}$ a composition series for G .*

- (a) Let $K \in \mathcal{N}(G)$. Then there exists unique $S_K \in \mathcal{S}$ with $K \leq S$ and $S_K \neq S^-$. Moreover, S_K/S_K^- is perfect, $S_K = KS_K^-$ and $K/M(K) \cong S_K/S_K^-$.
- (b) Let S/S^- be a perfect factor of $\mathcal{S}$. Then there exists a unique $K_S \in \mathcal{N}(G)$ with $K_S \leq S$ and $K_S \not\leq S^-$.

- (c) The function $K \mapsto S_K/S_K^-$ in the bijection between $\mathcal{N}(K)$ and set of perfect factors of $\mathcal{S}$ with inverse $S/S^- \mapsto K_S$.

Proof. (a) Since $K \leq G \in \mathcal{S}$ we can choose $S_K \in \mathcal{S}$ minimal with $K \leq S_K$. Then $K \neq S_K^-$ and since $\mathcal{S}$ is totally ordered, S_K is the unique element of $\mathcal{S}$ with $K \leq S_K$ and $K \not\leq S_K^-$. Since $\mathcal{S}$ is a composition series we know that S_K/S_K^- is simple. As $K = K' \leq S'_K$ we have $S'_K \not\leq S_K^-$. It follows that $1 \neq (S_K/S_K^-)' \trianglelefteq S_K/S_K^-$. Thus S_K/S'_K is a perfect simple groups. Note that K is near-component of S_K with $K \not\leq S_K^-$. Hence (4.2.4)(d) shows that K is the smallest subnormal supplement to S_K^- in S_K and that $S_K/S_K^- \cong K/M(K)$.

(b) This follows from (4.2.4)(d).

(c) Let $K \in \mathcal{N}(G)$. By (a) S_K/S_K^- is a perfect factor of $\mathcal{S}$. Also $K \leq S_K$ and $K \not\leq S_K^-$, so $K = K_{S_K}$. Let S/S^- be a perfect factor of $\mathcal{S}$. By (b) $K_S \in \mathcal{N}(G)$. Also $K_S \leq S$ and $K_S \not\leq S^-$, so $S = S_{K_S}$.

Thus the two function are well-defined and inverse to each other. $\square$

Appendix A

Set Theory

A.1 Ordinals

Definition A.1.1. A well-ordering on set S is a relation $<$ such that

- (i) If $a, b \in S$ then exactly one of $a < b$, $a = b$ and $b < a$ holds.
- (ii) If $a, b, c \in S$ with $a < b$ and $b < c$, then $a < c$.
- (iii) If T is a non-empty subset of S , then there exists $t \in T$ with $t < r$ for all $r \in T$ with $r \neq t$.

Lemma A.1.2 (Principal of Induction). Let ' $<$ ' be a well-ordering on the set S . Let $P(x)$ be a statement involving the variable x . Suppose that, whenever $s \in S$ such that $P(t)$ hold for all $t \in S$ with $t < s$, then also $P(s)$ holds. Then $P(s)$ holds for all $s \in S$.

Proof. If not, then set

$$T := \{s \in S \mid P(s) \text{ does not hold}\}$$

is not empty and so has a minimal element s . It follows that $P(t)$ holds for all $t \in S$ with $t < s$. But then $P(s)$ holds and so $s \notin T$, a contradiction. $\square$

Definition A.1.3. An ordinal is a set S such that

- (i) Each element of S is a subset of S .
- (ii) $\in$ is a well-ordering on S .

Example A.1.4. The following sets are ordinals:

$$\begin{aligned}
 0 &:= \emptyset \\
 1 &:= 0 \cup \{0\} = \{0\} &= \{\emptyset\} \\
 2 &:= 1 \cup \{1\} = \{0, 1\} &= \{\emptyset, \{\emptyset\}\} \\
 3 &:= 2 \cup \{2\} = \{0, 1, 2\} &= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
 &\vdots \\
 n+1 &:= n \cup \{n\} = \{0, 1, 2, \dots, n\} \\
 &\vdots
 \end{aligned}$$

and

$$\mathbb{N} := \bigcap \{\alpha \mid 0 \in \alpha, \forall \beta \in \alpha : \beta \cup \{\beta\} \in \alpha\} = \{0, 1, 2, 3, \dots\}$$

Lemma A.1.5. *Let α be an ordinal.*

- (a) *Let $\beta \in \alpha$ and $\gamma \in \beta$. Then $\gamma \in \alpha$.*
- (b) *Define $\alpha + 1 = \alpha \cup \{\alpha\}$. Then $\alpha + 1$ is an ordinal.*
- (c) *Every element of ordinal is an ordinal.*
- (d) *Let β be an ordinal, then exactly one of $\beta \in \alpha, \alpha = \beta$ and $\beta \in \alpha$ holds.*
- (e) *Let β an ordinal. Then $\alpha \in \beta$ if and only if $\alpha \not\subseteq \beta$. In particular, $\alpha \subseteq \beta$ if and only if $\alpha \in \beta$ or $\alpha = \beta$.*
- (f) *Let A be a non-empty set of ordinals. Then $\cap A$ is an ordinal. Moreover, $\cap A \in A$ and $\cap A$ is the minimal element of A .*
- (g) *Let A be a set of ordinals. Then $\cup A$ is an ordinal.*

Proof. (a) Since α is an ordinal and $\beta \in \gamma$ we have $\beta \subseteq \alpha$. As $\gamma \in \alpha$ we get $\gamma \in \alpha$.

(b) Since $\alpha + 1 = \alpha \cup \{\alpha\}$ we have

(*) *Let $x \in \alpha + 1$. Then $x \in \alpha$ or $x = \alpha$.*

Next we show

(**) *Let $x \in \alpha + 1$. Then $x \subseteq \alpha$. In particular, every element of $\alpha + 1$ is a subset of $\alpha + 1$.*

Let $x \subseteq \alpha + 1$. Then $x \in \alpha$ or $x = \alpha$. In the first case, since α is an ordinal we get $x \subseteq \alpha$. In the second case $x = \alpha$ and so again $x \subseteq \alpha$.

(***) *Let $x, y \in \alpha + 1$ with $x \in y$. Then $x \in \alpha$.*

By (**) $y \subseteq \alpha$. Hence $x \in y$ implies $x \in \alpha$.

(+) *Let $x, y \in \alpha + 1$. Then exactly one of $x \in y, y = x$ and $y \in x$ holds.*

Suppose that $x \in y$ and $x = y$. Then $x \in x$, a contradiction to the axioms of set theory.

Suppose $x \in y$ and $y \in x$. Then (***) shows that $x \in \alpha$ and $y \in \alpha$, a contradiction since ' $\in$ ' is ordering on α .

Thus at most one of the three statements hold.

If $x = \alpha$ and $y = \alpha$, then $x = y$. So we may assume that $x \neq \alpha$, so $x \in \alpha$. If $y = \alpha$ we get $x \in y$. If $y \neq \alpha$, then $y \in \alpha$ and since ' $\in$ ' is total ordering on α we get $x \in y, x = y$ or $y \in x$.

(++) *Let $x, y, z \in \alpha + 1$ with $x \in y$ and $y \in z$. Then $x \in z$.*

By (***) $x \in \alpha$ and $y \in \alpha$. If $z = \alpha$, we conclude that $x \in z$. If $z \neq \alpha$, then $z \in \alpha$ and since ' $\in$ ' is a ordering on α we get $x \in z$.

To complete the proof of (b) we need to show every non-empty subset y of $\alpha + 1$ as a minimal element with respect to ' $\in$ '. If $y = \{\alpha\}$, then certainly α is a minimal element of y . So suppose that $y \neq \{\alpha\}$. Since $\alpha + 1 = \alpha \cup \{\alpha\}$ we have $y \subseteq (y \cap \alpha) \cup \{\alpha\}$. Hence $y \cap \alpha \neq \emptyset$. and since ' $\in$ ' is a well-ordering on α , we see that $y \cap \alpha$ has a minimal element m . As $m \in \alpha$ and $y \subseteq (y \cap \alpha) \cup \{\alpha\}$, m is also a minimal element of y .

(c) Let $\beta \in \alpha$. We will first show that any element $\gamma \in \beta$ is a subset of β . By (a) $\gamma \in \alpha$ and so also $\gamma \subseteq \alpha$. Let $\delta \in \gamma$. Then $\delta \in \alpha$. As $\delta \in \gamma$ and $\gamma \in \beta$ and ' $\in$ ' is a transitive relation on α have get $\delta \in \beta$. Thus $\gamma \subseteq \beta$.

Since ' $\in$ ' is a well-ordering on α and β is a subset of α , ' $\in$ ' is also a well-ordering on α .

(d) If $\alpha = \beta$, then $\alpha \notin \beta$ and $\beta \notin \alpha$. If $\alpha \in \beta$, then $\alpha \subseteq \beta$ and since $\alpha \in \alpha$ also $\alpha \notin \beta$. So at most one of the three statements hold.

Fix the ordinal β , and for any ordinal ρ consider the statement:

$P(\rho)$: At least one of $\beta \in \rho$, $\beta = \rho$ and $\rho \in \beta$ holds. holds.

It remains to show that $P(\alpha)$ hold. As $\alpha \in \alpha + 1$ it suffices to show that $P(\rho)$ holds for all $\rho \in \alpha + 1$. By (b), $\alpha + 1$ is well-ordered with respect to ' ϵ '. So by the Principal of Induction we may assume that $P(\rho')$ holds for all $\rho' \in \alpha + 1$ with $\rho' \in \delta$.

Let $\gamma \in \rho$. Since $\rho \in \alpha + 1$, (a) shows that $\gamma \in \alpha + 1$ and so $P(\gamma)$ holds. Thus

$$\gamma \in \beta, \quad \gamma = \beta \quad \text{or} \quad \beta \in \gamma.$$

If $\gamma = \beta$, then as $\gamma \in \rho$, we get $\beta \in \rho$ and $P(\rho)$ holds

If $\beta \in \gamma$, then as $\gamma \in \rho$, we get $\beta \in \rho$ (see (b)) and again $P(\rho)$ holds.

Thus we may assume that $\gamma \in \beta$ for all $\gamma \in \rho$. Thus

$$\rho \subseteq \beta$$

If $\rho = \beta$, then $P(\rho)$ holds. So we may assume that $\rho \neq \beta$. Since $\rho \subseteq \beta$ we conclude that $\beta \setminus \rho$ is a non-empty subset of the ordinal β and so has an minimal (with respect to ' ϵ ') element δ . Let $\eta \in \delta$. Since $\delta \in \beta$, (b) implies that $\eta \in \beta$. Hence $\eta \in \rho$ by the minimal choice of δ . Thus

$$\delta \subseteq \rho.$$

As $\gamma \in \rho$ and $\delta \notin \rho$ we have $\gamma \neq \delta$. As $\gamma \in \rho$ and ρ is an ordinal, $\gamma \subseteq \rho$. As $\delta \notin \rho$ this gives $\delta \notin \gamma$.

We proved $\gamma \neq \delta$ and $\delta \notin \gamma$. As $\delta, \gamma \in \beta$ and that ' ϵ ' is an ordering on the ordinal β we get $\gamma \in \delta$. Thus holds for all $\gamma \in \rho$, so $\rho \subseteq \delta$. As $\delta \subseteq \rho$ this gives $\rho = \delta \in \beta$.

(e) Suppose $\alpha \in \beta$. Then $\alpha \neq \beta$ and since β is an ordinal, $\alpha \subseteq \beta$. So $\alpha \subsetneq \beta$.

If $\alpha \not\subseteq \beta$ we have $\beta \not\subseteq \alpha$. Hence $\alpha \neq \beta$ and since β is an ordinal, $\beta \notin \alpha$. Now (d) gives $\alpha \in \beta$.

(f) Any subset of a well-ordered set is well-ordered. So $\cap A$ is well-ordered with respect to ' ϵ '. Let $x \in \cap A$. Then $x \in a$ for all $a \in A$ and so $x \subseteq a$ for all $a \in A$. Hence $x \subseteq \cap A$. Thus $\cap A$ is an ordinal. If $\cap A \neq a$ for all $a \in A$, then $\cap A \subsetneq a$ and by (e), $\cap A \in a$ for all $a \in A$. Hence $\cap A \in \cap A$, a contradiction to (e).

(g) Let $x \in \cup A$. Then $x \in a$ for some $a \in A$. It follow that $x \subseteq a$ and so also $x \subseteq \cup A$. From (d) and (a) we see ' ϵ ' is a total ordering on $\cap A$.

Let d be a non-empty subset of $\cup A$. Let $x \in d$. Then $x \in a$ for some $a \in A$ and so $d \cap a \neq \emptyset$. Thus $B := \{a \in A \mid d \cap a \neq \emptyset\}$ is a non-empty set of ordinals. By (f), B has a minimal element b . Then $b \cap d$ is a non-empty subset of the ordinal b and so has a minimal element m . Suppose for a contradiction that $x \in m$. As $m \in b$ and b is an ordinal we get $x \in b$. Thus $x \in b \cap d$, a contradiction since $x \in m$ and m is the minimal element of $b \cap d$. We proved that $x \notin m$ and so m is the minimal element of d . It follows that ' ϵ ' is a well-ordering on $\cup A$ and so $\cup A$ is an ordinal. $\square$

Lemma A.1.6. *Let α be an ordinal and put $\beta = \cup \alpha = \cup_{\gamma \in \alpha} \gamma$. Then exactly of the following two statements holds:*

- (1) $\beta \in \alpha$, $\beta \neq \alpha$, β is the maximal element of α and β is the unique ordinal with $\alpha = \beta + 1$.
- (2) $\beta \notin \alpha$, $\beta = \alpha$, α has no maximal element and there does not exists an ordinal δ with $\alpha = \delta + 1$.

Proof. By (A.1.5)(g) β is an ordinal, We will first show

(*) $\beta \subseteq a$. In particular, exactly one of $\beta \in \alpha$ and $\beta = \alpha$ holds.

Just observe that $\gamma \subseteq \alpha$ for all $\gamma \in \alpha$ and so $\bigcup \alpha \subseteq \alpha$.

(**) Let δ be an ordinal. Then $\alpha = \delta + 1$ if and only if δ is a maximal element of α and if and only if $\beta \in \alpha$ and $\beta = \delta$.

Suppose first that $\alpha = \delta + 1$. Then $\alpha = \delta \cup \{\delta\}$. So $\delta \in \alpha$ and if $\gamma \in \alpha$ then $\gamma \in \delta$ or $\gamma = \delta$. Thus δ is maximal element of α .

Suppose next that δ is maximal element of α . Let $\gamma \in \alpha$. Then either $\gamma \in \delta$ or $\gamma = \delta$. In either case $\gamma \subseteq \delta$ and thus $\beta = \bigcup \alpha \subseteq \delta$. As $\delta \in \alpha$ we also have $\delta \subseteq \bigcup \alpha$ and thus $\beta = \delta \in \alpha$.

Suppose finally that $\beta \in \alpha$ and $\beta = \delta$. Let $\gamma \in \alpha$. Then $\gamma \subseteq \beta$ and so either $\gamma \in \beta$ or $\gamma = \beta$. Thus $\gamma \in \beta + 1$ and so $\alpha \subseteq \beta + 1$. By (*) $\beta \subseteq a$ and since $\beta \in \alpha$ we get $\beta + 1 = \beta \cup \{\beta\} \subseteq \alpha$. So $\alpha = \beta + 1 = \delta + 1$.

We now can prove the lemma. By (*) exactly one of $\beta \in \alpha$ and $\beta = \alpha$ holds.

Suppose $\beta \in \alpha$. Then $\beta \neq \alpha$. Moreover, by (**) applied with $\delta = \beta$ we see that β is maximal element of α and that β is the unique ordinal with $\alpha = \beta + 1$.

Suppose $\beta = \alpha$. Then $\beta \notin \alpha$ and (**) shows that α does not have maximal element and there does not exist an ordinal δ with $\alpha = \delta + 1$. $\square$

Definition A.1.7. A limit ordinal is an ordinal α with $\emptyset \neq \alpha = \bigcup \alpha$

Definition A.1.8. Let α and β be ordinals. Define the ordinal $\alpha + \beta$ inductively via

$$\alpha + \beta = \begin{cases} \alpha & \text{if } \beta = 0 \\ (\alpha + \gamma) + 1 & \text{if } \beta = \gamma + 1 \text{ for some ordinal } \gamma \\ \bigcup_{\gamma < \beta} (\alpha + \gamma) & \text{otherwise} \end{cases}$$

Remark A.1.9.

$$0 + \mathbb{N} = \bigcup_{n \in \mathbb{N}} (0 + n) = \mathbb{N}$$

$$1 + \mathbb{N} = \bigcup_{n \in \mathbb{N}} (1 + n) = \mathbb{N}$$

$$\mathbb{N} + 1 = \mathbb{N} \cup \{\mathbb{N}\} \neq \mathbb{N}$$

In particular, addition of ordinals is not commutative and the right cancellation law does not hold.

Lemma A.1.10. Let α , β and γ be ordinals. Then

(a) $\beta < \gamma$ if and only if $\alpha + \beta < \alpha + \gamma$.

(b) $\alpha + \beta = \alpha + \gamma$ if and only if $\beta = \gamma$.

Proof. Suppose first that $\beta < \gamma$. If $\gamma = \delta + 1$ for some ordinal δ , then $\beta \leq \delta$ and so by induction $\alpha + \beta \leq \alpha + \delta$. Since $(\alpha + \gamma) = (\alpha + (\delta + 1)) = (\alpha + \delta) + 1$ and $\alpha + \gamma < (\alpha + \gamma) + 1$ we conclude that $\alpha + \beta < \alpha + \gamma$. So suppose γ is a limit ordinal. Then $\beta + 1 < \gamma$ and so $\alpha + (\beta + 1) \leq \alpha + \gamma$ by the definition of addition. Since $\alpha + \beta < \alpha + (\beta + 1)$ we again have $\alpha + \beta < \alpha + \gamma$.

In general exactly one of

$$\beta < \gamma, \quad \beta = \gamma, \quad \text{and } \gamma < \beta$$

In this cases we conclude

$$\alpha + \beta < \alpha + \gamma, \quad \alpha + \beta = \alpha + \gamma, \quad \text{and } \alpha + \gamma < \alpha + \beta,$$

respectively and so (a) and (b) holds.

□

Lemma A.1.11. (a) *Let α and β be ordinals with $\alpha \leq \beta$, then there exists a unique ordinal δ with $\alpha + \delta = \beta$.*

(b) *Let α and β be ordinals. Then*

$$\{\alpha + \gamma \mid \gamma < \beta\} = \{\rho \mid \alpha \leq \rho < \alpha + \beta\}$$

(c) *Let α be an ordinal and β limit ordinal. Then $\alpha + \beta$ is a limit ordinal.*

Proof. (a) The uniqueness follows from (A.1.10)(b). So it suffices to find an ordinal δ with $\alpha + \delta = \beta$. If $\beta = \alpha$, we can choose $\delta = 0$. Inductively if $\alpha \leq \gamma < \beta$ let γ^* be the unique ordinal with $\alpha + \gamma^* = \beta$. If $\beta = \gamma + 1$ for some ordinal γ , then

$$\alpha + (\gamma^* + 1) = (\alpha + \gamma^*) + 1 = \gamma + 1 = \beta$$

and we can choose $\delta = \gamma^* + 1$.

So suppose β is limit ordinal and put $\delta = \sup_{\alpha \leq \gamma < \beta} \gamma^*$. Note that $\Gamma := \{\gamma \mid \alpha \leq \gamma < \beta\}$ has no maximal element and so by (A.1.10)(a), also $\{\gamma^* \mid \gamma \in \Gamma\}$ has no maximal element. Thus δ is a limit ordinal. Let μ be an ordinal with $\mu < \delta$. Then $\mu \leq \gamma^*$ for some ordinal $\gamma \in \Gamma$. Thus $\rho := \alpha + \mu \leq \alpha + \gamma^* < \beta$. It follows that $\alpha + \mu = \rho = \alpha + \rho^*$ and so $\mu = \rho^*$. Thus $\{\mu \mid \mu < \delta\} = \{\rho^* \mid \rho \in \Gamma\}$. Hence

$$\alpha + \delta = \sup_{\mu < \delta} \alpha + \mu = \sup_{\rho \in \Gamma^*} \alpha + \rho^* = \sup_{\rho \in \Gamma} \rho = \beta$$

where the last inequality holds, since β is a limit ordinal.

(b) If $\gamma < \beta$, then by A.1.10, $\alpha + \gamma < \alpha + \beta$.

Conversely, if $\alpha \leq \rho < \alpha + \beta$, then by (a), $\rho = \alpha + \gamma$ for some ordinal γ . Since $\alpha + \gamma = \rho < \alpha + \beta$, A.1.10 gives $\rho < \beta$.

(c): Since β is a limit ordinal, we have $\beta \neq 0$. Hence $\alpha < \alpha + \beta$ and $\alpha + \beta \neq 0$. Let ρ be an ordinal. We need to show that $\alpha + \beta \neq \rho + 1$.

Suppose $\rho < \alpha$. Then $\rho + 1 \leq \alpha < \alpha + \beta$ and so $\rho + 1 \neq \alpha + \beta$.

Suppose that $\alpha \leq \rho$. Then by (b) there exist ordinal δ with $\rho = \alpha + \delta$. Then

$$\rho + 1 = (\alpha + \delta) + 1 = \alpha + (\delta + 1)$$

Since β is limit ordinal we have $\delta + 1 \neq \beta$ and so (A.1.10)(b) shows that

$$\alpha + (\delta + 1) \neq \alpha + \beta$$

Hence again $\rho + 1 \neq \alpha + \beta$ and so $\alpha + \beta$ is limit ordinal.

□

Lemma A.1.12. *Let α, β, γ be ordinals. Then*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$$

Proof. If $\gamma = 0$, both sides are equal to $\alpha + \beta$. So suppose $\gamma \neq 0$ and that $(\alpha + \beta) + \delta = \alpha + (\beta + \delta)$ for all ordinals $\delta < \gamma$.

Suppose that $\beta = \delta + 1$ for some ordinal δ . Then

$$\begin{aligned}
 (\alpha + \beta) + \gamma &= (\alpha + \beta) + (\delta + 1) \\
 &= ((\alpha + \beta) + \delta) + 1 \\
 &= (\alpha + (\beta + \delta)) + 1 \\
 &= \alpha + ((\beta + \delta) + 1) \\
 &= \alpha + (\beta + (\delta + 1)) \\
 &= \alpha + (\beta + \gamma)
 \end{aligned}$$

Suppose next that γ is a limit ordinal. Then

$$\begin{aligned}
 (\alpha + \beta) + \gamma &= \sup_{\delta < \gamma} (\alpha + \beta) + \delta \\
 &= \sup_{\delta < \gamma} \alpha + (\beta + \delta) \\
 &= \sup_{\beta \leq \rho < \beta + \gamma} \alpha + \rho \\
 &= \sup_{\rho < \beta + \gamma} \alpha + \rho \\
 &= \alpha + (\beta + \gamma)
 \end{aligned}$$

□

Definition A.1.13. Let α and β be ordinals. Then the ordinal $\alpha\beta$ is inductively defined as follows

$$\alpha\beta = \begin{cases} 0 & \text{if } \beta = 0 \\ \alpha\gamma + \alpha & \text{if } \beta = \gamma + 1 \\ \sup_{\gamma < \beta} \alpha\gamma & \text{if } \beta \text{ is a limit ordinal} \end{cases}$$

Observe that $0\alpha = 0$, $1\alpha = \alpha = \alpha 1$ and $\alpha 2 = \alpha + \alpha$. But $2\alpha = \alpha \neq \alpha + \alpha = 1\alpha + 1\alpha$ for any infinite ordinal. So multiplication of ordinals is not commutative and not left distributive.

Lemma A.1.14. Let $\alpha, \sigma, \tilde{\sigma}, \rho, \tilde{\rho}$ be ordinals with $\alpha \neq 0$, $\rho < \alpha$, and $\tilde{\rho} < \alpha$. Then $\alpha\sigma + \rho < \alpha\tilde{\sigma} + \tilde{\rho}$ if and only if $\sigma < \tilde{\sigma}$ or $\sigma = \tilde{\sigma}$ and $\rho < \tilde{\rho}$. Let α, β and γ be ordinals with $\alpha \neq 0$ and $\beta < \gamma$. Then $\alpha\beta < \alpha\gamma$.

Proof. $\implies$: If $\beta \leq \gamma$ the definition of the multiplication of ordinals shows that $\alpha\beta \leq \alpha\gamma$.

Suppose $\sigma < \tilde{\sigma}$, then $\sigma + 1 \leq \tilde{\sigma}$ and so

$$\alpha\sigma + \rho < \alpha\sigma + \alpha = \alpha(\sigma + 1) \leq \alpha\tilde{\sigma} \leq \alpha\tilde{\sigma} + \tilde{\rho}.$$

Suppose $\sigma = \tilde{\sigma}$ and $\rho < \tilde{\rho}$. Then

$$\alpha\sigma + \rho = \alpha\tilde{\sigma} + \rho < \alpha\tilde{\sigma} + \tilde{\rho}.$$

$\impliedby$: Suppose that $\alpha\sigma + \rho < \alpha\tilde{\sigma} + \tilde{\rho}$. By the forward direction with the roles of (σ, ρ) and $(\tilde{\sigma}, \tilde{\rho})$ transposed we neither have $\tilde{\sigma} < \sigma$ nor $\tilde{\sigma} = \sigma$ and $\tilde{\rho} < \rho$. Since $(\rho, \sigma) \neq (\tilde{\rho}, \tilde{\sigma})$ we conclude that either $\sigma < \tilde{\sigma}$ or $\sigma = \tilde{\sigma}$ and $\rho < \tilde{\rho}$. □

Lemma A.1.15. *Let α and β be ordinals with $\alpha \neq 0$. Then there exists unique ordinals σ, ρ with $\beta = \alpha\sigma + \rho$ and $\rho < \beta$. Moreover, if $\tilde{\sigma}$ and $\tilde{\gamma}$ are ordinals with $\tilde{\rho} < \alpha$. Then $\alpha\sigma + \rho < \alpha\tilde{\sigma} + \tilde{\rho}$ if and only if $\sigma < \tilde{\sigma}$ or $\sigma = \tilde{\sigma}$ and $\rho < \tilde{\rho}$.*

Proof. Note that the uniqueness assertion follows from A.1.14. So we just need to prove the existence of σ and ρ . We use induction on β . If $\beta = 0$, choose $\sigma = \rho = 0$.

If $\beta = \gamma + 1$, let $\gamma = \alpha\hat{\sigma} + \hat{\rho}$ with $\hat{\rho} < \alpha$. If $\hat{\rho} + 1 < \alpha$ we can choose $\sigma = \hat{\sigma}$ and $\rho = \hat{\rho} + 1$. If $\hat{\rho} + 1 = \alpha$, then

$$\beta = \gamma + 1 = \alpha\hat{\sigma} + \hat{\rho} + 1 = \alpha\hat{\sigma} + \alpha = \alpha(\hat{\sigma} + 1)$$

So we can choose $\sigma = \hat{\sigma} + 1$ and $\rho = 0$.

Suppose now that β is a limit ordinal.

For $\delta < \beta$, let $\delta = \alpha\sigma_\delta + \rho_\delta$ with $\rho_\delta < \alpha$. Put

$$\hat{\sigma} = \sup_{\delta < \beta} \sigma_\delta.$$

Suppose that $\hat{\sigma} \neq \sigma_\delta$ for all $\delta < \beta$. Then by A.1.14, $\delta < \alpha\hat{\sigma}$ for all $\delta < \beta$ and so $\beta \leq \alpha\hat{\sigma}$. Also $\hat{\sigma}$ is a limit ordinal and if $\epsilon < \hat{\sigma}$, then $\epsilon < \sigma_\delta$ for some $\delta < \beta$. Then $\alpha\epsilon \leq \alpha\sigma_\delta + \rho_\delta = \delta < \beta$ and so by definition of $\alpha\hat{\sigma}$,

$$\alpha\hat{\sigma} = \sup_{\epsilon < \hat{\sigma}} \alpha\epsilon \leq \beta$$

Thus $\beta = \alpha\hat{\sigma}$ and we can choose $\sigma = \hat{\sigma}$ and $\rho = 0$.

Suppose that $\hat{\sigma} = \sigma_\delta$ for some $\delta < \beta$ and let $\Delta = \{\delta < \beta \mid \sigma_\delta = \hat{\sigma}\}$. Put

$$\hat{\rho} = \sup_{\delta \in \Delta} \rho_\delta.$$

By A.1.14, if $\delta < \beta$ with $\sigma_\delta < \hat{\sigma}$, then $\delta = \alpha\sigma_\delta < \alpha\hat{\sigma} \leq \alpha\hat{\sigma} + \hat{\rho}$. It follows that

$$\beta = \sup_{\delta < \beta} \delta = \sup_{\delta \in \Delta} \delta = \sup_{\delta \in \Delta} \alpha\hat{\sigma} + \rho_\delta = \alpha\hat{\sigma} + \sup_{\delta \in \Delta} \rho_\delta = \alpha\hat{\sigma} + \hat{\rho}$$

Since $\rho_\delta < \alpha$ for all $\delta \in \Delta$, $\hat{\rho} \leq \alpha$. If $\hat{\rho} < \alpha$, choose $\sigma = \hat{\sigma}$ and $\hat{\rho} = \rho$. If $\rho = \alpha$ choose $\sigma = \hat{\sigma} + 1$ and $\rho = 0$. $\square$

Lemma A.1.16. *Let α be an ordinal and Δ a non-empty set of ordinals. Then*

$$\alpha \left(\sup_{\delta \in \Delta} \delta \right) = \sup_{\delta \in \Delta} \alpha\delta$$

Proof. Let $\beta = \sup_{\delta \in \Delta} \delta$ and $\gamma = \sup_{\delta \in \Delta} \alpha\delta$. Let $\delta \in \Delta$. Then $\delta \leq \beta$. and so also $\alpha\delta \leq \alpha\beta$. Hence $\gamma \leq \alpha\beta$.

If $\alpha = 0$, both γ and $\alpha\beta$ are equal to zero. So suppose $\alpha \neq 0$. Then by A.1.15 we have $\gamma = \alpha\sigma + \rho$ for some ordinals σ, ρ with $\rho < \alpha$. Since $\alpha\delta \leq \gamma$ we get from A.1.14 that $\delta \leq \sigma$ and so $\beta \leq \sigma$. Thus $\alpha\beta \leq \alpha\sigma + \rho = \gamma$ and so $\gamma = \alpha\beta$. $\square$

Lemma A.1.17. *Let α, β and γ be ordinals. Then*

$$(a) \quad \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma.$$

$$(b) \quad (\alpha\beta)\gamma = \alpha(\beta\gamma).$$

Proof. (a) If $\gamma = 0$ both sides are equal to $\alpha\beta$. Suppose $\gamma = \delta + 1$. Then

$$\begin{aligned}\alpha(\beta + \gamma) &= \alpha(\beta + (\delta + 1)) = \alpha((\beta + \delta) + 1) = \alpha(\beta + \delta) + \alpha = (\alpha\beta + \alpha\delta) + \alpha \\ &= \alpha\beta + (\alpha\delta + \alpha) = \alpha\beta + \alpha(\delta + 1) = \alpha\beta + \alpha\gamma.\end{aligned}$$

Suppose that γ is a limit ordinal. Then also $\beta + \gamma$ is limit ordinal. So

$$\alpha(\beta + \gamma) = \sup_{\delta < \beta + \gamma} \alpha\delta = \sup_{\epsilon < \gamma} \alpha(\beta + \epsilon) = \sup_{\epsilon < \gamma} \alpha\beta + \alpha\epsilon = \alpha\beta + \sup_{\epsilon < \gamma} \alpha\epsilon = \alpha\beta + \alpha\gamma$$

(b) For $\gamma = 0$ both sides are equal to 0. Suppose $\gamma = \delta + 1$. Then

$$(\alpha\beta)\gamma = (\alpha\beta)(\delta + 1) = (\alpha\beta)\delta + \alpha\beta = \alpha(\beta\delta) + \alpha\beta = \alpha(\beta\delta + \beta) = \alpha(\beta(\delta + 1)) = \alpha(\beta\gamma)$$

Suppose γ is a limit ordinal. Hence using A.1.16

$$(\alpha\beta)\gamma = \sup_{\delta < \gamma} (\alpha\beta)\delta = \sup_{\delta < \gamma} \alpha(\beta\delta) = \alpha\left(\sup_{\delta < \gamma} \beta\delta\right) = \alpha(\beta\gamma)$$

□

Lemma A.1.18. *Let α, β be ordinals with $\alpha \neq 0 \neq \beta$. Define an ordering on $\alpha \times \beta$ by $(\rho, \sigma) < (\tilde{\rho}, \tilde{\sigma})$ if $\sigma < \tilde{\sigma}$ or $\sigma = \tilde{\sigma}$ and $\rho < \tilde{\rho}$. Define*

$$\begin{aligned}f: \alpha \times \beta &\rightarrow \alpha\beta \\ (\rho, \sigma) &\rightarrow \alpha\sigma + \rho\end{aligned}$$

Then f is an isomorphism of order sets.

Proof. This follows immediately from A.1.14 and A.1.15

□

Bibliography

- [KS] Hans Kurzweil and Bernd Stellmacher, *The Theory of Finite Groups, An introduction*, Springer, **2004**,