Hoofdstuk 2

Deelgroepen en normaaldelers

2.1 Wat is een deelgroep?

Definitie 2.1. Een deelverzameling H van een groep $G, \circ$ is een deelgroep van G als en slechts als H niet leeg is en $H, \circ$ zelf een groep is.

We noteren : $H \leq G$. We noemen G en $\{e\}$ onechte of triviale deelgroepen van G. De andere deelgroepen noemt men echte deelgroepen.
Het neutraal element van de deelgroep is hetzelfde als het neutraal element van de groep en het symmetrische element van een element van de deelgroep is het symmetrische element van dit element in de groep.
Om na te gaan of een bepaalde deelverzameling een deelgroep is kan je ook gebruik maken van volgende criteria:

Stelling 2.2. *H is een deelgroep van G als en slechts als*

$$H \neq \emptyset, H.H \subseteq H \text{ en } H^{-1} \subseteq H$$

Bewijs. Als H een deelgroep is van G dan is H natuurlijk gesloten voor de groepsbewerking en voor het inverse neming. Omgekeerd geldt de associativiteit omdat alle elementen van H ook in G zitten waar de associativiteit geldt. Omdat H niet leeg is bestaat er een $x \in H$, en dus is ook $x^{-1} \in H$. Maar dan is ook $x.x^{-1} = e \in H$. Dus is H een groep en geldt er dat $H \leq G$. $\square$

Gevolg 2.3. *Als H eindig is volstaat het dat H gesloten is voor de groepsbewerking want als $o(a) = n$ dan is $a^{-1} = a^{n-1} \in H$.*

Stelling 2.4. *H is een deelgroep van G als en slechts als*

$$\forall a, b \in H : a.b^{-1} \in H$$

Bewijs. Als H een deelgroep is van G, is H gesloten voor de groepsbewerking en het inverse neming en geldt $\forall a, b \in H : a.b^{-1} \in H$. Omgekeerd, neem $a = b$ en we krijgen dat $e \in H$. Ook is $a.b = a.(b^{-1})^{-1} \in H$, dus is H een deelgroep van G. □

2.2 Enkele eigenschappen

Stelling 2.5. *De doorsnede van twee deelgroepen is een deelgroep.*

Bewijs. Stel $A \leq G, B \leq G$ en $x, y \in A \cap B$. Dan behoren x en y ook tot A en is $xy^{-1} \in A$. Maar x en y zitten ook in B en dus ook $xy^{-1} \in B$. Bijgevolg is $xy^{-1} \in A \cap B$ en is $A \cap B \leq G$. □

Stelling 2.6. *De vereniging van twee deelgroepen A en B van G is een deelgroep van G als en slechts als $A \subset B$ of $B \subset A$.*

Bewijs. Als $A \subset B \Rightarrow A \cup B = B \leq G$. Omgekeerd: stel $A \cup B \leq G$. Neem $a \in A$ en $b \in B$, dan zijn $a, b \in A \cup B$ en dus is $ab^{-1} \in A \cup B$. Dit betekent dat $ab^{-1} \in A$ of $ab^{-1} \in B$. Hieruit volgt dat $b^{-1} \in A$ of $a \in B$. Omdat A een deelgroep is betekent dit dat $b \in A$ of $a \in B$, met andere woorden $A \subset B$ of $B \subset A$. □

Voor twee niet lege deelverzamelingen A en B van G definieert men $A.B = \{ab \text{ met } a \in A \text{ en } b \in B\}$. We noemen deze verzameling het product van A en B. Het is duidelijk dat $(A.B)^{-1} = B^{-1}.A^{-1}$. Als $A = \{a\}$, dan noteren we aB in plaats van $A.B$. En voor $g \in G$ noteren we met $B^g = g^{-1}Bg$ de toegevoegde verzameling van B. Als U een deelgroep is van G, dan is $U.U = U = U^{-1}$.

Stelling 2.7. *Het product HK van 2 deelgroepen H en K van G is een deelgroep van G als $HK = KH$.*

Bewijs. Neem $h_1k_1, h_2k_2 \in H.K$, dan is $h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. Nu is $k_1k_2^{-1}h_2^{-1} \in K.H = H.K$, dus bestaat er een $h_3k_3 \in H.K$ zodat $k_1k_2^{-1}h_2^{-1} = h_3k_3$. Bijgevolg is $h_1k_1(h_2k_2)^{-1} = h_1(h_3k_3) = (h_1h_3)k_3 \in H.K$, en dus is $H.K \leq G$. □

Stelling 2.8. *Als H en K deelgroepen zijn van G, dan is:*

$$|HK| = \frac{|H|.|K|}{|H \cap K|}$$

Bewijs. We definiëren de relatie $(h_1, k_1)R(h_2, k_2) \Leftrightarrow h_1k_1 = h_2k_2$ in de verzameling van alle koppels $H \times K$. Dit is een equivalentie relatie en het aantal klassen is juist $|HK|$. Omdat $h_1k_1 = h_2k_2 \leftrightarrow h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$. Dan bestaat er een element d van $H \cap K$ zodat $h_1 = h_2d$ en $k_2 = dk_1$. Elke equivalentieklasse van de relatie R bevat bijgevolg $|H \cap K|$ elementen en daaruit volgt het gestelde. □

Als S een deelverzameling is van G, dan bestaat er een minimale deelgroep van G die S omvat. Deze deelgroep kan gevonden worden door de doorsnede te bepalen van alle deelgroepen van G die S omvatten. Deze minimale deelgroep noemt men de *deelgroep voortgebracht door* S en men noteert: $\langle S \rangle$. Elk element van $\langle S \rangle$ is het product van elementen uit S en hun inverse.
Als $\langle S \rangle = G$, dan noemt men S een *voortbrengende verzameling van* G . Elk element van S noemt men een voortbrengend element of generator van G.
Als $S = \{a\}$, noteert men de deelgroep voortgebracht door S als $\langle a \rangle$. We noemen deze deelgroep de *cyclische deelgroep* van G voorgebracht door a. Een *cyclische groep* is een groep met 1 voortbrengend element. Elke eindige groep heeft minstens 1 cyclische deelgroep.

In de verzameling van alle deelgroepen van een groep G, kan men enige structuur brengen door ze te ordenen volgens de relatie $\cdots \subset \cdots$. Alzo vormt de verzameling deelgroepen van G een *tralie*, dit is een geordende verzameling waarin elk tweetal elementen een kleinste bovengrens en een grootste ondergrens heeft.

2.3 Nevenklassen

Definitie 2.9. H een deelgroep van G en $g \in G$.
De linkernevenklasse van g ten opzichte van H is de verzameling:

$$gH = \{gh : h \in H\}$$

De rechternevenklasse van g ten opzichte van H is de verzameling:

$$Hg = \{hg : h \in H\}$$

Als H een deelgroep is van G, definiëren we de volgende relatie in G:

$$a_1 \sim a_2 \Leftrightarrow a_1^{-1}a_2 \in H$$

Stelling 2.10. *De relatie $\sim$ is een equivalentierelatie in G.*

Bewijs. Omdat $a_1^{-1}a_1 = e \in H$ is $\sim$ reflexief. Als $a_1 \sim a_2$ is $a_1^{-1}a_2 \in H \Rightarrow (a_1^{-1}a_2)^{-1} \in H \Rightarrow a_2^{-1}a_1 \in H \Rightarrow a_2 \sim a_1$. De relatie is dus symmetrisch. Als $a_1 \sim a_2$ en $a_2 \sim a_3$, dan is $(a_1^{-1}a_2)(a_2^{-1}a_3) \in H \Rightarrow a_1^{-1}a_3 \in H \Rightarrow a_1 \sim a_3$. Dus er is transitiviteit en bijgevolg is de relatie $\sim$ een equivalentierelatie. $\square$

De equivalentierelatie $\sim$ verdeelt G in equivalentieklassen. Deze klassen zijn juist de linkernevenklassen ten opzichte van H. Als men de relatie $\sim$ definieert als $a_1 \sim a_2 \Leftrightarrow a_1a_2^{-1} \in H$, dan zijn de equivalentieklassen de rechternevenklassen ten opzichte van H.

Definitie 2.11. Als H een deelgroep is van G dan is de *index* van H in G, genoteerd als $[G : H]$, het aantal linkernevenklassen ten opzichte van H in G.
De verzameling linkernevenklassen ten opzichte van H in G noemt men de *quotiëntverzameling* van G modulo H, genoteerd als G/H.

Stelling 2.12. *Het aantal linkernevenklassen ten opzichte van H is gelijk aan het aantal rechternevenklassen ten opzichte van H.*

Bewijs. Definieer $f : \{aH : a \in G\} \to \{Ha : a \in G\} : aH \longmapsto Ha^{-1}$. De functie f is injectief want $f(aH) = f(bH) \Rightarrow Ha^{-1} = Hb^{-1} \Rightarrow a^{-1}(b^{-1})^{-1} \in H \Rightarrow a^{-1}b \in H \Rightarrow aH = bH$. Bovendien is f surjectief, want voor elke rechternevenklasse Ha bestaat er een linkernevenklasse $a^{-1}H$ waarvoor geldt dat $f(a^{-1}H) = H(a^{-1})^{-1} = Ha$. Dus is f bijectief en zijn er evenveel linkernevenklassen als rechternevenklassen. □

Gevolg 2.13. *De index van H in G is dus eveneens het aantal rechternevenklassen ten opzichte van H.*

Stelling 2.14. *Lagrange: G eindig en $H \leq G$, dan is*

$$[G : H] = \frac{\#G}{\#H}$$

Bewijs. Door de sudoku eigenschap bevat elke linkernevenklasse ten opzichte van H evenveel elementen als H en omdat de linkernevenklassen een partitie vormen is het aantal elementen van G gelijk aan het aantal linkernevenklassen vermenigvuldigd met het aantal elementen van H. □

Gevolg 2.15. *De orde van een deelgroep is dus steeds een deler van de orde van de groep. Omgekeerd is het niet zo dat voor elke deler van de orde van G er een deelgroep bestaat met die orde.*

Definitie 2.16. Als H een deelgroep is van G, dan is de deelverzameling S van G een linkertransversaal van H in G als S juist 1 element bevat van elke linkernevenklasse van H.

S is een linkertransversaal van H als en slechts als $G = SH$ en $st^{-1} \notin H$ voor alle $s \neq t$ in S. Als speciaal geval hiervan noteren we dat wanneer S en H beide deelgroepen zijn van G zodat $G = SH$ en $S \cap H = \{e\}$, dan is S een linkertransversaal van H in G. We noemen S het *complement* van H in G.

2.4 Normale deelgroep of normaaldeler

We kunnen ons afvragen of de groepsbewerking van G een groepsstructuur induceert op de verzameling van alle linkernevenklassen ten opzichte van H. Dan zou $(g_1H).(g_2H) = (g_1.g_2)H$. Dit is enkel zo als voor elk element g van de groep geldt dat: $gH = Hg$, met andere woorden als de linkernevenklassen samenvallen met de rechternevenklassen ten opzichte van H. Vandaar volgende definitie:

Definitie 2.17. H is een normale deelgroep of normaaldeler van G als $H \leq G$ en $\forall g \in G : gH = Hg$. Notatie: $H \trianglelefteq G$.

Definitie 2.18. Een groep G is enkelvoudig als G geen normaaldelers heeft.

Een ander criterium om na te gaan of een deelgroep een normaaldeler is wordt gegeven door:

Stelling 2.19. *H is een normaaldeler van G als en slechts als*

$$H \leq G \text{ en } \forall h \in H, \forall g \in G : ghg^{-1} \in H$$

.

Bewijs. Als H een normaaldeler is van G dan is $\forall g \in G : gH = Hg$. Dus is voor elke $h \in H : gh \in Hg \Rightarrow ghg^{-1} \in H$. Omgekeerd, neem $gh \in gH$. Omdat $ghg^{-1} \in H$ is $gh \in Hg$ en is $gH \subseteq Hg$. Analoog vinden we dat $Hg \subseteq gH$, dus is H een normaaldeler van G. $\square$

Gevolg 2.20. *Een normaaldeler is invariant onder toevoeging met $g \in G$. Met andere woorden: $gHg^{-1} = g^{-1}Hg = H$.*

Gevolg 2.21. *Een deelgroep H is een normaaldeler van G als H de unie is van volledige toevoegingsklassen.*

Gevolg 2.22. *In een abelse groep is elke deelgroep een normaaldeler.*

Als H en N deelgroepen zijn van G, dan weten we dat HN slechts een deelgroep is als $HN = NH$. Onderzoeken we nu verdere eigenschappen van HN:

Stelling 2.23. *Als H een deelgroep is van G en N een normaaldeler is van G , dan is HN een deelgroep van G.*

Bewijs. Neem $h_1n_1, h_2n_2 \in HN$, dan is $(h_1n_1)(h_2n_2)^{-1} = h_1(n_1n_2^{-1}h_2^{-1}) = h_1(nh_2^{-1})$. Omdat N een normaaldeler is van G geldt: $Nh_2^{-1} = h_2^{-1}N$.
Bijgevolg is $(h_1n_1)(h_2n_2)^{-1} = h_1h_2^{-1}n' \in HN$ en dus is HN een deelgroep van G. $\square$

Stelling 2.24. *Als H een deelgroep is van G en N een normaaldeler is van G , dan is N een normaaldeler van HN.*

Bewijs. Neem $hn \in HN$, dan is $hn \in G$ en is $hnN = Nhn$. Bijgevolg is $N \trianglelefteq HN$. $\square$

Stelling 2.25. *Als H en N normaaldelers zijn van G , dan is HN ook een normaaldeler van G.*

Bewijs. Neem $g \in G$, dan is $ghn \in gHN$ en omdat $ghn = (gh)n = (h'g)n = h'(gn) = h'(n'g) = (h'n')g \in HNg$ is $gHN \subseteq HNg$.
Analoog is $HNg \subseteq gHN$ en dus is $gHN = HNg$. Bijgevolg is $HN \trianglelefteq G$. $\square$

We kunnen nu ook G/H uitrusten als een groep.

Stelling 2.26. *Als H een normale deelgroep is van G dan is $G/H, .$ met $g_1H.g_2H = (g_1g_2)H$ een groep.*

Bewijs. De groepsbewerking is associatief want $(g_1H.g_2H).(g_3H) = (g_1g_2H).(g_3H) = (g_1g_2).g_3H = g_1.(g_2g_3)H = (g_1H).(g_2g_3H) = (g_1H).(g_2H.g_3H)$. Het neutraal element is $eH = H$ en $g^{-1}H$ is het symmetrische element van gH. $\square$

Gevolg 2.27. *We noemen G/H nu de quotiëntgroep van G modulo H.*

Gevolg 2.28. *In een abelse groep is elke quotiëntgroep abels.*

De volgende eigenschappen zijn dikwijls nuttig om na te gaan of een bepaalde deelgroep een normaaldeler is zonder rekenwerk.

Stelling 2.29. *Een deelgroep H met index 2 is altijd een normaaldeler.*

Bewijs. Als H index 2 heeft, dan is $G = H \cup gH$. Omdat $Hg \neq H$ moet $Hg = gH$ en is dus H een normaaldeler van G. □

Stelling 2.30. *Als H de enige deelgroep is van G met orde $|H|$, dan is H een normaaldeler van G.*

Bewijs. De afbeelding $x \to gxg^{-1}$ beeldt de deelgroep H af op de deelgroep gHg^{-1}. De orde van die twee deelgroepen is dezelfde en omdat H de enige deelgroep is van orde $|H|$, moet $H = gHg^{-1}$ en dus is H een normaaldeler van G. □

Eenmaal we de toevoegingsklassen van G bepaald hebben, kunnen we de normaaldelers van G bepalen door die toevoegingsklassen te combineren tot deelgroepen. We moeten natuurlijk altijd de klasse $C(e)$ toevoegen. De klassen die worden toegevoegd moeten altijd per twee worden toegevoegd: $C(a)$ en $C(a^{-1})$.

Als N een normaaldeler is van G, blijkt er een verband te bestaan tussen de deelgroepen van de quotiëntgroep G/N en de deelgroepen van G die N omvatten. Dit resultaat noemen we de correspondentiestelling.

Stelling 2.31. *Er is een bijectief verband tussen de deelgroepen van de quotiëntgroep G/N en de deelgroepen van G die N omvatten. Onder deze correspondentie gaan normaaldelers over in normaaldelers.*

Bewijs. Stel K een deelgroep van G/N en definieer $D = \{g \in G : gN \in K\}$. Het is duidelijk dat D een deelgroep is van G want als $g_1, g_2 \in D$, dan zijn g_1N en G_2N elementen van K en omdat K een deelgroep is zal $(g_1N)(g_2N)^{-1} = g_1g_2^{-1}N \in K$. Bijgevolg is $g_1g_2^{-1}$ een element van D en is D een deelgroep van G. En omdat $\forall n \in N : nN = N \in K$ omvat D de normaaldeler N. Verder is het duidelijk dat $K = D/N$. Want als $x \in D/N$ dan is $x = gN$ met $g \in D$ en dus is $x \in K$. Omgekeerd: als $x \in K$, dan is $x = gN$ en bijgevolg is $x \in D/N$.
Construeer dan volgende afbeelding : $\varphi : D \to D/N$, waarbij D een deelgroep is van G die N omvat. Het is duidelijk dat deze afbeelding surjectief is. Maar ze is ook injectief. Neem twee deelgroepen D_1 en D_2 die N omvatten en $\varphi(D_1) = \varphi(D_2)$, dan bestaan er elementen $d_1 \in D_1$ en $d_2 \in D_2$ waarvoor $d_1N = d_2N \Rightarrow d_1^{-1}d_2 \in N \Rightarrow d_1^{-1}d_2 \in D_1 \Rightarrow d_2 \in D_1$. Dus is D_2 een deel van D_1. Het omgekeerde kunnen we analoog bewijzen, dus is $D_1 = D_2$. Bijgevolg is er een bijectief verband tussen de deelgroepen die N omvatten en de deelgroepen van G/N.
Als D een normaaldeler is van G die N omvat, dan is D/N een normaaldeler van G/N, want $(gN).D/N.(gN)^{-1} = (gN).D/N.(g^{-1}N) = \{gdg^{-1}N\} = D/N$. Hiermee is bewezen dat bij het bijectief verband normaaldelers overgaan in normaaldelers. $\square$

2.5 Het centrum van een groep

Definitie 2.32. Het centrum van een groep G, genoteerd als $Z(G)$, is de verzameling van alle elementen van G die commuteren met alle andere elementen van G.

$$Z(G) = \{x \in G : \forall g \in G : xg = gx\}$$

Gevolg 2.33. *Als G abels is dan is $Z(G) = G$.*

We geven eerst een aantal basiseigenschappen van het centrum van een groep:

Stelling 2.34. *Het centrum van een groep is een normaaldeler van die groep.*

Bewijs. Neem $x, y \in Z(G)$, dan is $\forall g \in G : xy^{-1}g = xgy^{-1} = gxy^{-1}$. Bijgevolg is $xy^{-1} \in Z(G)$ en is $Z(G)$ een deelgroep van G. Neem nu $x \in$

$gZ(G)$, dan is $x = gh = hg \in Z(G)g$. Bijgevolg is $gZ(G) \subseteq Z(G)g$. Analoog is $Z(G)g \subseteq gZ(G)$ en dus is $Z(G)$ een normaaldeler van G. $\square$

Gevolg 2.35. *Het centrum bestaat uit alle toevoegingsklassen van 1 element.*

Stelling 2.36. *Een deelgroep van $Z(G)$ is steeds een normaaldeler van G.*

Bewijs. Stel dat H een deelgroep is van $Z(G)$. Als $h \in H \Rightarrow h \in Z(G)$ en dus is $\forall g \in G : gh = hg$ of $\forall h \in H : h^g = h$. Dit betekent dat H een normaaldeler is van G. $\square$

Omdat $Z(G)$ een normaaldeler is van G, kunnen we de quotiëntgroep $G/Z(G)$ bestuderen. In het algemeen kunnen we weinig zeggen over die quotiëntgroep. Wanneer we echter voorwaarden opleggen aan dit quotiënt kunnen we soms eigenschappen van G afleiden.

Stelling 2.37. *Als G een eindige groep is en $G/Z(G)$ is cyclisch, dan is G abels.*

Bewijs. Als $a, b \in G$, dan is $a = g^p z_1$ en $b = g^q z_2$. Hierbij zijn z_1 en z_2 elementen van het centrum en is $gZ(G)$ het voortbrengende element van $G/Z(G)$. Maar dan is $a.b = g^p z_1.g^q z_2 = g^{p+q} z_1 z_2 = g^{p+q} z_2 z_1 = g^q z_2.g^p z_1 = b.a$ en dus is G een abelse groep. $\square$

Gevolg 2.38. *Het is eigenlijk ironisch: $G/Z(G)$ is nooit een niet-triviale cyclische groep. Want als $G/Z(G)$ wel niet-triviaal cyclisch zou zijn is G abels en is $G = Z(G)$ en dus is $G/Z(G) = \{e\}$. Bijgevolg zou $G/Z(G)$ wel triviaal cyclisch zijn.*

Toch kunnen we dit resultaat gebruiken om iets te zeggen over het centrum.

Stelling 2.39. *Een niet-abelse groep met orde pq, met p en q priem, heeft triviaal centrum.*

Bewijs. De orde van $G/Z(G)$ moet een deler zijn van pq, dus $G/Z(G)$ heeft orde $1, p, q$ of pq. Als de orde $1, p$ of q is dan is $G/Z(G)$ cyclisch en zou G abels moeten zijn. Dus heeft $G/Z(G)$ orde pq en is $Z(G) = \{e\}$. $\square$

2.6 De commutator deelgroep

Definitie 2.40. De commutator deelgroep of afgeleide groep van een groep G, genoteerd als $G' = [G, G]$, is de deelgroep voorgebracht door alle commutatoren, dit wil zeggen alle elementen van de vorm $[g, h] = ghg^{-1}h^{-1}$.

Definitie 2.41. Voor twee deelverzamelingen X en Y van G, noteert men $[X, Y]$ voor de groep voortgebracht door de elementen $[x, y]$ met $x \in X$ en $y \in Y$.

Definitie 2.42. Een groep is perfect als $G = G'$.

Een willekeurig element van G' is het product van commutatoren. Het is niet noodzakelijk dat het product van commutatoren terug een commutator is.We geven nu een paar basiseigenschappen:

Stelling 2.43. $[g, h]^{-1} = [h, g]$.

Bewijs. $[g, h]^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = [h, g]$. □

Stelling 2.44. *Als H en K deelgroepen zijn van G, dan is*

$$[H, K] = [K, H]$$

Bewijs. Neem een willekeurig element $[h, k]$ van $[H, K]$, dan is $[h, k] = [k, h]^{-1} \in [K, H]$. Bijgevolg is $[H, K]$ een deelverzameling van $[K, H]$. De omgekeerde redenering verloopt analoog. □

Stelling 2.45. $\forall x, yz \in G : [x, yz] = [x, y] \,.\, [x, z]^{y^{-1}}$

Bewijs.

$$\begin{aligned}
[x, yz] &= xyzx^{-1}(yz)^{-1} \\
&= xyzx^{-1}z^{-1}y^{-1} \\
&= (xyx^{-1}y^{-1})y(xzx^{-1}z^{-1})y^{-1} \\
&= [x, y] \,.\, [x, z]^{y^{-1}}
\end{aligned}$$

$\square$

Stelling 2.46. $\forall x, yz \in G : [xz, y] = [z, y]^{x^{-1}} \,.\, [x, y]$

Bewijs.

$$\begin{aligned}
[xz, y] &= xzy(xz)^{-1}y^{-1} \\
&= xzyz^{-1}x^{-1}y^{-1} \\
&= x(zyz^{-1}y^{-1})x^{-1}(xyx^{-1}y^{-1}) \\
&= [z, y]^{x^{-1}} \,.\, [x, y]
\end{aligned}$$

$\square$

Stelling 2.47. *Als G abels is dan is $G' = \{e\}$.*

Bewijs. Omdat $[g, h] = ghg^{-1}h^{-1} = g.g^{-1}.h.h^{-1} = e$ is $G' = \{e\}$. $\square$

Gevolg 2.48. *Voor twee deelverzamelingen X en Y van G geldt dan dat $[X, Y] = \{e\}$ als en slechts als $xy = yx$ voor alle $x \in X$ en $y \in Y$.*

Stelling 2.49. *Als H en K deelgroepen zijn van G, dan is $[K, H]$ een deelgroep van H als en slechts als H invariant is voor toevoeging met elementen uit K.*

Bewijs. Als $[K,H]$ een deelgroep is van H is $[k,h] = khk^{-1}h^{-1} \in H$ en dus is $khk^{-1} \in H$. Bijgevolg is H invariant voor toevoeging van elementen uit K. Stel omgekeerd dat H invariant is voor toevoeging van elementen uit K. Omdat $[K,H]$ gedefinieerd werd als de groep voortgebracht door de commutatoren, volstaat het aan te tonen dat $[k,h] \in H$. Maar $[k,h] = (khk^{-1})h^{-1}$ en dit zit duidelijk in H. □

Gevolg 2.50. *Als N en M normaaldelers zijn van G, dan is $[N,M]$ een deelgroep van $N \cap M$.*

Stelling 2.51. *Als H en K deelgroepen zijn van G, dan is $[H,K]$ een normaaldeler van de groep voortgebracht door $H \cup K$.*

Bewijs. Neem $h, h' \in H$ en $k, k' \in K$. Dan moeten we bewijzen dat $[H,K]^{h'^{-1}}$ en $[H,K]^{k'^{-1}}$ in $[H,K]$ liggen. Maar $[h,k]^{h'^{-1}} = [hh',k]\,[h',k]^{-1} \in [H,K]$ en $[h,k]^{k'^{-1}} = [h,k']^{-1}\,[h,kk'] \in [H,K]$. Hiermee is het gestelde bewezen. □

Stelling 2.52. *De commutator deelgroep van een groep is een normaaldeler van die groep.*

Bewijs. Nu is $g\,[x,y]\,g^{-1} = gxyx^{-1}y^{-1}g^{-1} = (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})$ $(gy^{-1}g^{-1}) = [gxg^{-1}, gyg^{-1}]$. Het toegevoegde van een commutator is dus ook een commutator. Op dezelfde manier kan men bewijzen dat het toegevoegde van een product van commutatoren terug een product van commutatoren is, bijgevolg is G' een normale deelgroep van G. □

Stelling 2.53. *G/G' is abels.*

Bewijs. We moeten aantonen dat $gG'.hG' = hG'.gH'$ of dat $ghG' = hgG'$ of $g^{-1}h^{-1}ghG' = G'$. Maar $g^{-1}h^{-1}gh = [g^{-1}, h^{-1}] \in G'$. Hieruit volgt het gestelde. □

We noemen G/G' de *abelisatie* van G.

Stelling 2.54. *Als H een normaaldeler is van G dan is G/H abels als en slechts als G' een deelgroep van H.*

Bewijs. Als G/H abels is, geldt $\forall x, y \in G : xH.yH = yH.xH$. Hieruit volgt dat $x^{-1}y^{-1}xy = [x^{-1}, y^{-1}] \in H$. Dus is elke commutator een element van H en daaruit volgt dat $G' \leq H$.
Omgekeerd als G' een deelgroep is van H dan is $g_1H.g_2H = g_1g_2H = g_2g_1(g_1^{-1}g_2^{-1}g_1g_2)H = g_2g_1H = g_2H.g_1H$ en dus is de quotiëntgroep G/H abels.

□

Gevolg 2.55. *De commutator deelgroep is de unieke kleinste normale deelgroep van G waarvoor de quotiëntverzameling G/G' abels is.*

Stelling 2.56. *Als A en B normaaldelers zijn van G met $A \cap B = \{e\}$, dan zal elk element van A commuteren met elk element van B.*

Bewijs. Neem $a \in A$ en $B \in B$, dan is $[a, b] = (a^{-1}b^{-1}a)b \in B$ want B is een normaaldeler. Maar omdat ook A een normaaldeler is, is $[a, b] = a^{-1}(b^{-1}ab) \in A$. Wegens de veronderstelling is dus $[a, b] = e$ en dus commuteren a en b. □

2.7 De centralisator

Definitie 2.57. De centralisator van een element a van een groep G is de verzameling van al de groepselementen die commuteren met a. Notatie: $C_G(a)$ of $Z(a)$.

$$C_G(a) = Z(a) = \{g \in G : g.a = a.g\}$$

Het begrip centralisator kan ook voor een deelverzameling S worden gedefinieerd als de verzameling van alle groepselementen die commuteren met alle elementen van de deelverzameling.
Dus:

$$C_G(S) = Z(S) = \{g \in G : \forall s \in S : g.s = s.g\}$$

.

Stelling 2.58. *$Z(S)$ en $Z(a)$ zijn deelgroepen van G.*

Bewijs. Stel $g \in Z(a)$ dus: $a.g = g.a$, dan is ook $a.g^{-1} = g^{-1}.a$ en dus is $g^{-1} \in Z(a)$. Als ook $h \in Z(a)$ is $gh.a = g.ah = a.gh$ en is ook $gh \in Z(a)$. Dus is $Z(a)$ een deelgroep van G. Analoog bewijs voor $Z(S)$. □

Gevolg 2.59. *De centralisator van S is de grootst mogelijke deelgroep van G waarvan de elementen van S in het centrum liggen.*

Gevolg 2.60. *De centralisator van de groep G is het centrum van die groep.*

Gevolg 2.61. *De centralisator van een element uit het centrum van de groep G is die groep zelf.*

Stelling 2.62. *Het aantal elementen in de toevoegingsklasse van a is gelijk aan de index van de centralisator van a in G.*

Bewijs. Neem b, c in dezelfde nevenklasse van $Z(a)$, dan is $bc^{-1} \in Z(a)$. Er bestaat met andere woorden een element z in $Z(a)$ waarvoor $b = cz$. Maar dan is $bab^{-1} = czaz^{-1}c^{-1} = czz^{-1}ac^{-1} = cac^{-1}$. De elementen b en c bepalen hetzelfde element in de toevoegingsklasse van a. Er is dus een eenduidig verband tussen de elementen van de toevoegingsklasse van a en de nevenklassen van $Z(a)$. Hiermee is het gestelde bewezen. □

Gevolg 2.63. *Het aantal elementen in een toevoegingsklasse is een deler van de orde van de groep. Dit volgt rechtstreeks uit vorige stelling en de stelling van Lagrange.*

Nemen we een representant x_i in elke toevoegingsklasse van G, dan is $|G| = \sum_i [G : Z(x_i)]$ en omdat elk element uit het centrum in zijn toevoegingsklasse maar 1 element heeft, krijgen we volgende gelijkheid, die bekend staat als de klassenvergelijking van de groep:

$$|G| = |Z(G)| + \sum_i [G : Z(x_i)]$$

hierbij wordt i genomen over de toevoegingsklassen met meer dan 1 element.

2.8 De normalisator

Definitie 2.64. De normalisator van een deelgroep H van een groep G, genoteerd als $N_G(H)$, is de verzameling van alle elementen g van G waarvoor H invariant is onder toevoeging.

$$N_G(H) = \left\{g \in G : g^{-1}Hg = H\right\}$$

Stelling 2.65. *De normalisator van een deelgroep H van G is een deelgroep van G.*

Bewijs. Neem $x, y \in N_G(H)$ dan is $(xy^{-1})^{-1}H(xy^{-1}) = y(x^{-1}Hx)y^{-1} = yHy^{-1} = (y^{-1})^{-1}Hy^{-1} = H$. Dan is $xy^{-1} \in N_G(H)$ en bijgevolg is $N_G(H) \leq G$. □

Stelling 2.66. *Een deelgroep H is een normaaldeler in zijn normalisator.*

Bewijs. Neem $x \in N_G(H) \Rightarrow x^{-1}Hx = H \Rightarrow Hx = xH$. Bijgevolg is $H \trianglelefteq N_G(H)$. □

Stelling 2.67. *Als H en K deelgroepen zijn van G en H is een normaaldeler van K, dan is $K \leq N_G(H)$.*

Bewijs. Als $x \in K \Rightarrow xH = Hx \Rightarrow x \in N_G(H)$. Dus is $K \subseteq N_G(H)$ en natuurlijk is K dan een deelgroep van $N_G(H)$. □

Gevolg 2.68. *De normalisator van een deelgroep H van G is de grootst mogelijke deelgroep van G waarin H een normaaldeler is.*

2.9 Minimale en maximale deelgroepen

Definitie 2.69. Een niet triviale deelgroep H van G wordt minimaal genoemd als H zelf geen echte deelgroep omvat. Dus:

$$\{e\} < K \leq H \Rightarrow K = H$$

Definitie 2.70. Een niet triviale deelgroep H van G wordt maximaal genoemd als H zelf niet omvat is in een echte deelgroep van G. Dus:

$$H \leq K < G \Rightarrow K = H$$

Stelling 2.71. *Een echte deelgroep H is minimaal als en slechts als $|H|$ een priemgetal is.*

Bewijs. Als $|H|$ priem is, volgt uit de stelling van Lagrange dat H geen echte deelgroep heeft en dus is H minimaal. Als omgekeerd, H minimaal is, moet H cyclisch zijn. Want als $g \neq e \in H$, dan is de deelgroep voortgebracht door g een deelgroep van H. Omdat H minimaal is moet dus $H = \langle g \rangle$. Dan moet $|H|$ een priemgetal zijn. Zo niet heeft $|H|$ een echte deler l en zou de deelgroep voortgebracht door $g^{\frac{|H|}{l}}$ een echte deelgroep zijn van H en dit is, wegens de minimaliteit van H, onmogelijk. $\square$

Definitie 2.72. De Frattini deelgroep $\Phi(G)$ van een groep G is de doorsnede van alle maximale deelgroepen (als er zijn) ofwel is $\Phi(G) = G$ als er geen maximale deelgroepen zijn.

Definitie 2.73. Een normaaldeler H van G is een maximale normaaldeler als er geen normaaldeler K van G bestaat waarvoor $H \trianglelefteq K \trianglelefteq G$.

Een normaaldeler H is maximaal als G/H enkelvoudig is. Een groep kan meerdere maximale normaaldelers bezitten die verschillend zijn qua structuur en orde. Als G niet enkelvoudig is, heeft G een normaaldeler en dus ook een maximale normaaldeler A. Bijgevolg is G/A enkelvoudig. Nu kan A enkelvoudig zijn. Zoniet bezit A een maximale normaaldeler B zodat A/B enkelvoudig is. Als we dit proces verder zetten zien we dat G een reeks $A, B, \cdots$ van deelgroepen bezit waarvoor $G/A, A/B, \cdots$ allemaal enkelvoudig zijn.

2.10 De stelling van Cauchy

De stelling van Lagrange zegt dat de orde van een element steeds een deler is van de orde van de groep. Het omgekeerde is meestal niet waar: als d een deler is van de orde van een groep, dan bestaat er niet noodzakelijk een element van orde d in die groep. Als d een priemgetal is blijkt de stelling wel te kloppen. Dit resultaat staat bekend als de stelling van Cauchy(1845).

Stelling 2.74. *G een eindige groep en p een priemdeler van $|G|$, dan bevat G een element van orde p of equivalent G bevat een deelgroep van orde p.*

Bewijs. De equivalentie is duidelijk, want elk element a van orde p genereert een deelgroep van orde p, namelijk $\langle a \rangle$ en omdat p priem is bevat elke deelgroep van orde p een element van orde p omdat die deelgroep cyclisch is.
Noteer de orde van G als n. Als $p = n$ dan heeft elk element dat verschilt van het eenheidselement, orde p. We bewijzen de stelling door inductie. Dus veronderstel dus $n > p$ en veronderstel dat de eigenschap klopt voor alle groepen met orde kleiner dan n. We delen het bewijs op in twee delen: G abels of niet abels. Veronderstellen we dus dat G abels is. Omdat de orde van G niet priem is, bezit G een echte normaaldeler H. Bovendien is G/H een groep en is $|H|.|G/H| = n$. Omdat p een priemdeler is van n, moet p ofwel een deler zijn van de orde van H ofwel van de orde van G/H. Maar beide groepen hebben orde kleiner dan n en dus geldt de stelling : er bestaat een element van orde p. Zit dat element in H, dan zit het ook in G en is de stelling bewezen. Als het in G/H zit, bijvoorbeeld $\overline{g}$, wat weten we dan over de orde van g? Stel dat die orde van g gelijk is aan m, dan is $g^m = e \Rightarrow \overline{g}^m = 1 \Rightarrow p$ deelt m, maar dan is $g^{\frac{m}{p}}$ een element van orde p en is de stelling ook bewezen.
Veronderstel nu dat G niet abels is. De redenering blijft dezelfde, alleen is

G/H niet noodzakelijk een groep. Wel is er een deelgroep H en p deelt ofwel de orde van H ofwel de index $[G : H]$. In het eerste geval is de stelling dus bewezen. In het andere geval merken we op dat $Z(G)$ een echte deelgroep is van G en dat ook $Z(g)$ een echte deelgroep is als g geen element is van $Z(G)$. Als p de orde van ofwel $Z(G)$ ofwel $Z(g)$ met $g \notin Z(G)$ deelt is de stelling bewezen. Een ander geval kan gewoon niet voorkomen. Neem immers de klassenvergelijking $|G| = |Z(G)| + \sum_i [G : Z(x_i)]$. Als p nu geen enkel van die $|Z(x_i)|$ deelt, dan deelt het zeker $[G : Z(x_i)]$ en omdat p de orde van G deelt volgt uit de klassenvergelijking dat p de orde van $Z(G)$ deelt. Bijgevolg is de stelling ook bewezen als G niet abels is. □

Bekijken we nu een aantal eenvoudige resultaten die het gevolg zijn van de stelling van Cauchy.

Stelling 2.75. *G een eindige groep en p een priemgetal. De orde van G is een macht van p als en slechts als elk element als orde een macht van p is.*

Bewijs. Als de orde van G een macht van p is, dan heeft elk element als orde een macht van p want de orde van een element deelt de orde van de groep. Veronderstel omgekeerd dat elk element als orde een macht van p heeft en stel dat de orde van G deelbaar is door een priemgetal q verschillend van p. Dan moet, volgens de stelling van Cauchy, G een element hebben van orde q, wat tegen de veronderstelling is. Dus moet de orde van G een macht van p zijn. □

Stelling 2.76. *Als al de elementen, buiten het eenheidselement, dezelfde orde hebben, dan is die orde priem en heeft de groep als orde een macht van dat priemgetal.*

Bewijs. Als de orde van G deelbaar is door twee priemgetallen p en q, dan bevat G,volgens Cauchy, minstens een element van orde p en een element van orde q, wat tegen het gegeven is. Bijgevolg heeft de orde van G slechts 1 priemdeler p en is $|G| = p^n$. Volgens Cauchy is er dan zeker een element van orde p en volgens het gegeven hebben alle andere elementen (behalve het eenheidselement) ook orde p. □