SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Sylows satser och några tillämpningar

av

Salwan Alnakar

2020 - No K11

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Sylows satser och några tillämpningar

Salwan Alnakar

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Håkan Granath

2020

Sammanfattning

Sylows satser, uppkallade efter Ludwig Sylow, är en samling satser som spelar en fundamental roll i teorin för ändliga grupper för att bland annat kunna klassificera grupper av ändliga ordningar. Det här arbetet handlar om att bevisa Sylows satser och tillämpa satserna för att klassificera grupper av vissa ordningar. I arbetet går vi igenom grunderna inom grupper och gruppverkan och använder dess satser och definitioner för att bevisa Sylows satser och ge exempel på några tillämpningar av dem.

Abstract

Sylow's theorems, named after Ludwig Sylow, are a collection of theorems that play a fundamental role in the theory of finite groups in order to be able to classify groups of finite orders, among other things. This paper is about proving Sylow's theorems and applying the theorems to classify groups of certain orders. In the paper we go through the basic theory of groups and group action and use it to prove Sylow's theorems and give examples of some of their applications.

Tack

Jag vill tacka min handledare Håkan Granath, för hans hjälp med värdefulla kommentarer och särskilt sitt tålamod under arbetets gång. Detta har gett mig möjlighet att utveckla och fördjupa mina kunskaper i matematik.

Innehåll

1 Introduktion

Gruppteori är studium av algebraiska strukturer som kallas för grupper, och tillhör den matematiska ämnesgrenen abstrakt algebra som är en ganska ung gren jämfört med andra delområden i matematik och började utformas och utvecklas i början av 1800-talet [7]. Under denna tid besvarade den franska matematikern Évariste Galois frågan ifall det fanns en lösningsformel till algebraiska ekvationer av ordning 5, 6 eller högre. Till sin hjälp använde han ett verktyg som han kallade för ”grupp”. Även om matematikerna hade tidigare funderat på och övervägt det vi idag kallar för grupper, var det dock Galois den första som använde ordet grupp mer formellt och det gjorde honom till en av grundarna inom gruppteori [8]. Under denna tid kom matematiker på att det fanns andra geometrier att upptäcka förutom det som utvecklades av grekerna, och grupper kom att bli ett viktigt hjälpmedel för studier av dessa geometrier. Ungefär vid samma tid höll den tyska matematikern Carl Friedrich Gauss på med att utveckla tekniken av modulär aritmetik som hjälpte honom att lösa några problem inom talteori [9]. Denna teknik om modulär aritmetik delade också likheter med verktyget grupper som användes av Galois. Matematiker försökte generalisera egenskaperna av verktyget grupper och studera och förfina dem så att de ska gälla alla dessa områden. Således föddes teorin om grupper. Så småningom kom man på andra abstrakta koncept som ringar, kroppar, vektorrum osv och dessa formade grenen abstrakt algebra där gruppteori är en central del.

Sylows satser är en samling av tre stycken satser uppkallade efter den norske matematikern Peter Ludwig Sylow (1832-1918). Han föddes och dog i Oslo. Han arbetade som lärare i Halden i 40 år ända fram till 1898, då blev han utnämnd till professor och föreläste vid Oslo universitet nästan ända fram till sin död. Han studerade och sammanställde verken av Niels Henrik Abel inom algebra tillsammans med Sophus Lie [11]. Sylow gav viktiga bidrag till grenen gruppteori men det han är mest känd för är Sylow satserna publicerade år 1872, och de kom att bli av en fundamental betydelse i teorin om ändliga grupper [5]. Sylows satser bygger på och är en generalisering av Cauchys sats. Medan Cauchys sats säger att ifall ett primtal p delar ordningen av en grupp G måste G innehålla ett element av ordning p (och därmed en delgrupp av ordning p) [10], säger Sylows satser att ifall p^k är den högsta potensen av p som delar ordningen av G måste G ha delgrupper av ordning p^k. Sylows satser är också relaterade till Lagranges sats i den mening att de bekräftar existensen av delgrupper vars ordningar är primtalspotenser och ge kännedom om antalet sådana grupper.

Innan vi börjar behandla Sylows satser och dess tillämpningar behöver vi först förstå grunderna inom gruppteori, grupper av olika typer, gruppverkan samt några ytterligare definitioner relaterade till grupper.

2 Grupper

Grupper är abstrakta strukturer som används som verktyg för att beskriva olika matematiska system. I det här kapitlet presenteras de olika typerna av grupper och dess egenskaper samt några viktiga definitioner.

2.1 Grundläggande definitioner

Först definierar vi vad en grupp är för något.

Definition 2.1. *Vi definierar en grupp som en mängd G bestående av element och en binär operator, vanligen betecknat med en asterisk $*$. Gruppen betecknas på följande vis $(G, *)$. En grupp behöver uppfylla följande axiom:*

i *Slutenhet. För varje $x, y \in G$ så gäller det att $x * y \in G$.*

ii *Associativitet. För varje $x, y, z \in G$ så gäller det att $x * (y * z) = (x * y) * z$.*

iii *G har ett enhetselement I. För alla $x \in G$ skall $x * I = I * x = x$.*

iv *Varje element i G har ett inverselement. För varje $x \in G$ existerar det ett $y \in G$ så att $x * y = y * x = I$. Elementet y betecknas x^{-1}.*

Elementen i en grupp behöver så klart inte bara vara siffror, begreppet grupper är ett abstrakt koncept. Framöver kommer gruppen $(G, *)$, om ingen risk för missförstånd finns, att refereras till med G. Dessutom för x, y tillhörande gruppen $(G, *)$ kommer vi ofta använda xy istället för $x * y$, alltså $xy = x * y$.

För att få en bättre förståelse gällande vad en grupp är, kommer först några exempel att presenteras.

Exempel 2.1. Mängden $\mathbb{Z}$ av alla heltal med den binära operationen $+$, betecknat $(\mathbb{Z}, +)$, bildar en grupp. Vi ska se att den uppfyller gruppaxiomen:

i Gruppen är sluten. Om x, y är heltal så är deras summa $x + y$ också ett heltal.

ii Associativitet gäller uppenbart på heltal. Om $x, y, z \in \mathbb{Z}$ så gäller $(x+y)+z = x + (y + z)$.

iii Enhetselementet för gruppen är talet $0 \in \mathbb{Z}$. För varje $x \in \mathbb{Z}$ så gäller att $x + 0 = 0 + x = x$.

iv Till varje $x \in \mathbb{Z}$ existerar det en invers $y \in \mathbb{Z}$ sådan att $x + y = y + x = 0$ där $y = -x$.

Ett ytterligare förtydligande är att framöver när vi skriver elementen i en grupp G, syftar vi på elementen som finns i mängden som bildar gruppen G.

Ett sätt som är illustrativt, särskilt till grupper innehållande mindre antal element, är så kallad Cayleytabell, som har uppfunnits av den engelske matematikern Arthur Cayley. Detta är helt enkelt en multiplikationstabell för grupper. Vi illustrerar hur det fungerar med följande exempel:

Exempel 2.2. Låt G vara gruppen med mängden $\{1, -1, i, -i\}$ och operationen $*$ vara multiplikation. Då har vi Cayleytabellen för gruppen som nedan.

$*$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Vi ska visa att G är en grupp:

i G är sluten. Vi kan se i tabellen att resultatet av multiplikationen av varje x $\in G$ med varje y $\in G$ är ett element i G.

ii Associativitet följer av att vi har multiplikation av komplexa tal.

iii Enhetselementet i gruppen är talet 1. Multiplikation av ett element med 1 ger elementet själv.

iv Varje element i G har en invers. Det kan vara lite svårt att se direkt, men vi räknar upp dem. Talet 1 är sin egen invers, samma sak för talet -1. Imaginära talen i och $-i$ är varandras inverser.

I Cayleytabellen kan vi se flera intressanta egenskaper. Den första intressanta egenskapen är att varje element i gruppen förekommer endast en gång i varje rad och kolumn. Den andra är att tabellen är symmetrisk kring diagonalen. Detta innebär att vi har en så kallad kommutativ grupp, mer information om denna typ av grupp ges i avsnitt 2.2.

Ordningen av en grupp är storleken av dess mängd. Antal element i en grupp G betecknas $|G|$ och kallas för ordningen av G. En grupp kan antingen vara ändlig, dvs innehåller ett begränsat antal element, eller oändlig och innehålla ett oändligt antal element. I uppsatsen kommer vi bara att behandla ändliga grupper. Ordningen för gruppen i Exempel 2.1 är oändlig eftersom mängden heltal är oändlig, medan ordningen för gruppen i Exempel 2.2 är 4, så $|G| = 4$.

I följande definition beskriver vi grupphomomorfism, som är en avbildning mellan två grupper.

Definition 2.2. *En grupphomomorfism* $\theta : G \to H$ *är en funktion från gruppen* $(G, *)$ *till gruppen* $(H, \Diamond)$ *som uppfyller:*

$$\theta(g_1 * g_2) = \theta(g_1) \Diamond \theta(g_2),$$

för alla $g_1, g_2 \in G$.

Grupphomomorfism kräver inte att θ är injektiv och eller surjektiv. En isomorfism däremot är en grupphomomorfism θ som är både injektiv och surjektiv, alltså bijektiv.

Ett annat viktigt begrepp som vi ska definiera är direkt relaterat till definitionen av en grupp.

Definition 2.3. *En delgrupp till en grupp* $(G, *)$ *är en grupp* $(H, *)$ *där* H *är en delmängd till mängden* G*, och räkneoperationen på* H *ärvs från gruppen* G *och som är sådan att gruppaxiomen gäller. Notation för att* H *är en delgrupp i* G *är* $H \leq G$.

Nästa sats ger oss ett kriterium för att en delmängd H till en grupp G är en delgrupp till G.

Sats 2.4. *[4, s. 76] Låt* G *vara en grupp och* H *en delmängd i* G*. Då är* H *en delgrupp till* G *om och endast om* H *uppfyller tre villkor. Det första är att det för alla element* $h_1, h_2 \in H$ *så gäller att* $h_1 h_2 \in H$*. Det andra är att enhetselementet* I *till* G *tillhör också* H*. Det tredje och sista är att för ett element* $h \in H$ *så gäller att dess invers* h^{-1} *tillhör* H.

Utifrån Sats 2.4 kan vi inse att till en grupp G existera det alltid minst två delgrupper, nämligen gruppen G själv som delgrupp samt delgruppen $H = \{I\}$ bestående endast av enhetselementet. Det här gäller alla grupper så klart.

Låt H vara en icke tom delmängd i en grupp G. För varje $g \in G$ bildar vi delmängderna $gH = \{gh \mid h \in H\}$ och $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ i G, alltså $gH \subseteq G$ och $gHg^{-1} \subseteq G$.

Sats 2.5. *Låt* H *vara en delgrupp i gruppen* G*. Då har vi att för varje* $g \in G$ *att mängden* gHg^{-1} *också är en delgrupp i* G*. Vidare gäller att ordningen av* gHg^{-1} *är lika med* H.

Bevis. Vi ska visa med hjälp av Sats 2.4 att mängden gHg^{-1} är faktiskt en delgrupp i G.

Enhetselement $I \in G$ eftersom för alla $g \in G$ gäller $I = gg^{-1} = gIg^{-1}$. Därmed är I innehållen i gHg^{-1} då gIg^{-1} är ett element i gHg^{-1}. Låt a, b vara två element i gHg^{-1} som skrivas $a = gh_1g^{-1}$ och $b = gh_2g^{-1}$ för $h_1, h_2 \in H$. Då gäller det, för alla $g \in G$, att $ab = gh_1g^{-1}gh_2g^{-1} = gh_1Ih_2g^{-1} = gh_1h_2g^{-1}$ är också ett element i gHg^{-1}. Slutligen, låt $c = ghg^{-1}$ vara ett element i gHg^{-1} för ett element i $h \in H$. Då gäller att inversen c^{-1} till c kan uttryckas som $c^{-1} = (ghg^{-1})^{-1} = gh^{-1}g^{-1}$ är också ett element i gHg^{-1} där h^{-1} är förstås inversen till h i H.

Till sist, för att visa att $|H| = |gHg^{-1}|$, visar vi att avbildningen $\theta_g : H \to gHg^{-1}$ är bijektiv. Vi visar detta genom att verifiera att $\theta_g(h) = ghg^{-1}$ är både injektiv och surjektiv. För injektion, har vi att för varje $h_1, h_2 \in H$ där $h_1 \neq h_2$ gäller att $\theta_g(h_1) = gh_1g^{-1} \neq gh_2g^{-1} = \theta_g(h_2)$. Att θ är surjektiv är uppenbart. Avbildningen θ är bijektiv och därmed stämmer likheten $|H| = |gHg^{-1}|$. $\square$

Vi ger nu en definition relaterat till skrivsättet gHg^{-1}.

Definition 2.6. *Två delgrupper H_1 och H_2 i en grupp G är konjugerade delgrupper om det finns ett $g \in G$ sådant att $H_2 = gH_1g^{-1}$. Vi säger att H_2 är erhållen från H_1 genom konjugering.*

En central sats inom gruppteori är Lagranges sats.

Sats 2.7. *[4, s. 130] Låt G vara en grupp. Om G har en delgrupp H så måste ordningen av H dela ordningen av G.*

Delgrupper vars ordning är en primtalspotens är lite mer intressanta för oss då Sylows satser behandlar just sådana, dess definition är som följande.

Definition 2.8. *En p-delgrupp till en ändlig grupp G är en delgrupp vars ordning är en potens p^k, där p är ett primtal och k är ett naturligt tal. En p-delgrupp vars ordning är den högsta potensen av p som delar gruppens ordning kallas för en Sylow p-delgrupp.*

Vi har nu gått igenom de grundläggande egenskaperna för en grupp och ska strax gå igenom några olika typer av grupper. Vi börjar med att presentera den enklare typen.

2.2 Kommutativa grupper

En kommutativ grupp, även kallad för abelsk grupp, är en grupp där den kommutativa lagen gäller. I Exempel 2.1 ser vi att G är en abelsk grupp eftersom den kommutativa lagen gäller vid addition av två heltal, för $x, y \in \mathbb{Z}$ gäller att $x + y = y + x$. En intressant egenskap hos en abelsk grupp är att dess Cayleytabell är symmetrisk kring huvuddiagonalen. I Exempel 2.2 är G en sådan grupp.

2.3 Symmetriska grupper

Låt $n > 0$ vara ett heltal. En symmetrisk grupp, betecknat S_n, består av alla permutationer av talen $\{1, 2, \ldots, n\}$. Eftersom det finns $n!$ permutationer av n stycken tal, betyder det att gruppens ordning är $n!$ så $|S_n| = n!$. Vi kan som exempel ta gruppen S_3, den består av permutationer av element i mängden {1,2,3}. Ordningen för gruppen S_3 är $3! = 6$. Gruppens operation, $\circ$, är funktionskomposition då en permutation kan betraktas som en bijektiv funktion från en mängd till sig själv. Innan vi skriver vilka element som S_3 innehåller ska vi gå igenom hur permutationer hanteras inom gruppteori. Det finns flera sätt att representera en permutation på, men ett mycket effektivt är cykelformen. Permutationen som tar 3 till 1, 1 till 2 och 2 till 3 skrivs med cykelnotationen som (312). Permutationen som tar 1 till 1, 2 till 3 och 3 till 2 skrivs (23) där är det konvention att utelämna elementet 1 som avbildas på sig själv, dock är (1)(23) och (23) samma permutation. Därför skrivs enhetselementet i gruppen, som avbildar varje elementet på sig själv, som den tomma parentesen ().

Gruppen S_3 innehåller följande element:

$$S_3 = \{(), (12), (13), (23), (123), (132)\}.$$

Vi ska redogöra hur två element kombineras ur S_3. Låt $\alpha = (23)$ och $\beta = (132)$ vara två permutationer. Vi applicerar permutationen $\alpha \circ \beta$ på var och en av elementen i $\{1, 2, 3\}$, ett element i taget. För element 1 gäller $(\alpha \circ \beta)(1) = \alpha(\beta(1)) = \alpha(3) = 2$. Vidare har vi $(\alpha \circ \beta)(2) = 1$ och får cykeln (12). Sist, $(\alpha \circ \beta)(3) = 3$ och det blir sin egen cykel (3). Vi får två cykler, (12) av längd 2 och (3) av längd 1. Dock skriver vi inte ut cykler av längd 1. Då är kompositionen $\alpha \circ \beta = \alpha\beta = (23)(132) = (12)(3) = (12)$. Följande Cayleytabell för S_3 visar produkten av alla par av permutationer i S_3.

$\circ$	()	(12)	(13)	(23)	(123)	(132)
()	()	(12)	(13)	(23)	(123)	(132)
(12)	(12)	()	(132)	(123)	(23)	(13)
(13)	(13)	(123)	()	(132)	(12)	(23)
(23)	(23)	(132)	(123)	()	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	()
(132)	(132)	(23)	(12)	(13)	()	(123)

Varje element i S_n kan skrivas som en produkt av disjunkta cykler. Ordningens roll har då ingen betydelse, vilket följande exempel illustrerar: Permutationen $\sigma = (134)(25)$ ur S_5 kan också skrivas (25)(134), båda beskriver samma permutation.

Efter att vi har gått igenom symmetriska grupper och beskrivit cykelnotationen, kan vi ta ett exempel på tillämpning av Sats 2.4.

Exempel 2.3. Låt H vara en delmängd till den symmetriska gruppen S_8 där

$$H = \{(), (174)(258), (147)(285), (174)(258)(36), (147)(285)(36), (36)\}.$$

Vi påstår att H är en delgrupp i S_8, men vi ska enbart visa att för en bestämd produkt av två permutationer i H att villkoren i Sats 2.4 gäller. På samma sätt som nedan visar man att villkoren i Sats 2.4 också gäller för resten av produkterna av två permutationer i H, och därmed visar man att H är en delgrupp. Ett fullständigt bevis på att H är en delgrupp i S_8 ges i avsnitt 2.4 om cykliska grupper.

Vi väljer två element $h_1 = (174)(258)$ och $h_2 = (147)(285)(36)$ ur H. Då gäller att $h_1h_2 = (174)(258)(147)(285)(36) = (36)$ som också är ett element i H. Enhetselementet i S_8 är $()$ och vi ser att det också finns i H. Slutligen kan vi välja ett element $h_3 = (174)(258)$ som har elementet $(147)(285) \in H$ som invers då $(174)(258)(147)(285) = ()$.

2.4 Cykliska grupper

Låt G vara en grupp och g ett godtyckligt element i gruppen. Vi betecknar mängden av alla potenser av g, $\{\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, \dots\}$, med $\langle g\rangle$ och det är alltså mängden av alla element som elementet g kan generera. Gruppen G kallas cyklisk om det för något $g \in G$ gäller att $\langle g\rangle = G$. En viktig observation är att $\langle g\rangle$ bildar en delgrupp till G för alla $g \in G$, vi bevisar det i följande sats.

Sats 2.9. *Låt G vara en grupp, för varje $g \in G$ har vi att $\langle g\rangle$ bildar en cyklisk delgrupp till G.*

Bevis. Eftersom $\langle g\rangle$ är en delmängd till G så kan vi använda Sats 2.4 och visa att dess tre villkor är uppfyllda. För det första villkoret låter vi $g^{k_1}, g^{k_2} \in \langle g\rangle$ där $k_1, k_2 \in \mathbb{Z}$. Då gäller det att deras produkt $g^{k_1}g^{k_2} = g^{k_1+k_2}$ är innehållen i $\langle g\rangle$ eftersom $g^{k_1+k_2}$ är en potens av g då $k_1 + k_2 \in \mathbb{Z}$. Till det andra villkoret har vi att g^0 per definition är lika med enhetselementet i G, alltså $g^0 = I$. Och eftersom $g^0 \in \langle g\rangle$ så är enhetselementet I också är innehållen i $\langle g\rangle$. Slutligen för det tredje villkoret, låt $g^k \in \langle g\rangle$. Vi har $(g^k)^{-1} = g^{-k}$ och av det följer att inverselementet g^{-k} till g^k också är innehållen i $\langle g\rangle$. Vi har visat att $\langle g\rangle$ är en delgrupp till G, alltså att $\langle g\rangle \leq G$. □

Nu ska vi definiera vad ordningen av ett element innebär. Det skiljer sig från ordningen av en grupp.

Definition 2.10. *Låt G vara en ändlig grupp. Ordningen av ett element $g \in G$ definieras som ordningen av gruppen $\langle g\rangle$ och betecknas $o(g)$. Vi har alltså att $o(g) = |\langle g\rangle|$.*

En konsekvens av Definition 2.10 och Sats 2.7 är att ordningen av ett element $g \in G$ delar ordningen av G, alltså $|o(g)|$ delar $|G|$. Följande sats uttrycker ordningen av ett element på ett annat men ekvivalent sätt.

Sats 2.11. *[4, s. 87] Låt G vara en ändlig grupp med enhetselementet I och g ett godtyckligt element i gruppen. Ordningen av g, $o(g)$, är det minsta möjliga positiva heltal k som uppfyller ekvationen $g^k = I$.*

I följande exempel ska vi visa att delmängden H från Exempel 2.3 är en cyklisk delgrupp. Exemplet visar också en tillämpning av Sats 2.11.

Exempel 2.4. Låt H vara en delmängd till den symmetriska gruppen S_8 i Exempel 2.3. Då är H en cykliska grupp, alltså $H = \langle h \rangle$ för ett $h \in H$. Låt nämligen $h = (147)(285)(36)$. Vi beräknar potenserna av h.

$$\begin{aligned} h &= (147)(285)(36), \\ h^2 &= (174)(258), \\ h^3 &= (36), \\ h^4 &= (147)(285), \\ h^5 &= (174)(258)(36), \\ h^6 &= (). \end{aligned}$$

Vi ser att $o(h)$ är 6 då $h^6 = ()$. Eftersom h har genererat alla element i H är H en cykliska grupp med generatorn h, alltså $H = \langle h \rangle$. Detta visar påståendet i Exempel 2.3 att H är en delgrupp i S_8.

Sats 2.12. *Låt p vara ett primtal. Alla grupper G av ordning p är cykliska. Vidare har G totalt $p-1$ möjliga generatorer.*

Bevis. Eftersom ordningen för $|G| = p \geq 2$ måste G innehålla minst ett element g som inte är enhetselementet. Vi väljer en sådan $g \in G$ godtyckligt där $g \neq I$. Ordningen av g är lika med ordningen av den cykliska gruppen $\langle g \rangle$, alltså $o(g) = |\langle g \rangle|$. Enligt Sats 2.9 är $\langle g \rangle \leq G$. Enligt Sats 2.7 $|\langle g \rangle| \mid |G|$ och utifrån $o(g) = |\langle g \rangle|$ får vi $o(g) \mid |G|$. Eftersom ordning av G är ett primtal, är ordningen av g antingen 1 eller p, alltså $o(g) = 1$ eller $o(g) = p$. Eftersom g är inte enhetselementet kan dess ordning inte vara 1, så $o(g) = p$. Det här betyder att $\langle g \rangle$ har samma ordning som G och eftersom $\langle g \rangle$ är en delgrupp i G måste $G = \langle g \rangle$. Alltså är G en cyklisk grupp.

Gruppen G har ett enhetselement och $p-1$ icke enhetselement. Vi valde ett godtyckligt icke enhetselement $g \in G$ och visade att det genererar G. Eftersom det finns $p-1$ sådana val av g som inte är enhetselementet har G totalt $p-1$ möjliga generatorer. $\square$

Med hjälp av definitionerna av ordning för ett gruppelement visar vi ett intressant samband mellan cykliska grupper och abelska grupper.

Sats 2.13. *Alla cykliska grupper G är abelska.*

Bevis. Vi antar att $G = \langle g \rangle$ för ett element g i G. Vi väljer godtyckligt två element g_1 och g_2 ur G. Målet är att visa att g_1 och g_2 kommuterar, alltså att $g_1 g_2 = g_2 g_1$. Vi vet att $g_1 = g^a$ och $g_2 = g^b$ för några heltal a och b. Vi ställer upp produkten av elementen g_1 och g_2:

$$g_1 g_2 = g^a g^b = g^{a+b} = g^{b+a} = g^b g^a = g_2 g_1,$$

och vi har därmed visat att G är abelsk. $\square$

En viktig anmärkning är att omvändning till Sats 2.13 inte är sann. Kleins fyrgrupp [6] är en grupp med fyra element som inte uppfyller Sats 2.13. Vi kan exemplifiera den som gruppen K med följande permutationer $\{(), (12)(34), (13)(24), (14)(23)\}$. Dess Cayleytabell är följande.

$\circ$	()	(12)(34)	(13)(24)	(14)(23)
()	()	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	()	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	()	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	()

Vi ser i Cayleytabellen att den är symmetrisk kring diagonalen därför måste K vara abelsk. Från diagonalen ser vi att $o(g) = 2$ för varje $g \in K$ men inte $g = I$, därför kan K inte vara cyklisk.

2.5 Dihedrala grupper

En dihedral grupp, betecknat D_n, med ordningen $2n$ innehåller element som är symmetrier av en regelbunden n-hörning i planet. Gruppen består alltså av n stycken speglingar och n stycken rotationer. Enhetselementet I är inräknat bland de n rotationerna. Gruppoperationen är avbildningssammansättning.

Vi ger en mer konkret beskrivning av dihedrala gruppen D_n för $n \geq 3$. Låt Q vara en regelbunden n-hörning placerad med dess centrum i origo. Låt s vara speglingen längs en symmetrilinje som går igenom origo och ett av hörnen i Q, och låt r vara rotationen kring origo med $\frac{2\pi}{n}$ radianer moturs. Gruppen D_n genereras av $s, r \in D_n$ där följande villkor är uppfyllda:

$$r^n = I, \tag{1}$$

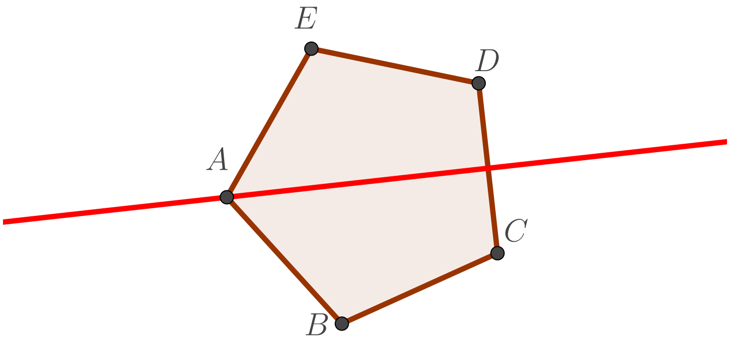
$$s^2 = I, \tag{2}$$

och som vi snart kommer att visa, så gäller även

$$(sr)^2 = srsr = I. \tag{3}$$

Man exekverar som vanligt produkter av s och r från höger till vänster. Alltså exempelvis i ekvation (3) gäller först rotation, spegling, rotation och sist spegling.

Vi ska ge en motivering till att ekvation (3) håller. För enkelhetens skull illustrerar vi med fallet $n = 5$. Följande figur visar en regelbunden 5-hörning



För att visa likheten i (3) räcker det att visa att $srsr$ fixerar två närliggande hörn i 5-hörningen. Speglingen s speglar punkterna tvärs över den röda streckade symmetrilinjen genom punkten A. Rotationen r roterar punkterna $\frac{2\pi}{5}$ radianer moturs. Vi får

$$srsr(A) = srs(r(A)) = srs(B) = sr(s(B)) = sr(E) = s(r(E)) = s(A) = A$$

och

$$srsr(E) = srs(r(E)) = srs(A) = sr(s(A)) = sr(A) = s(r(A)) = s(B) = E,$$

alltså gäller likheten i ekvation (3).

Vi gör en omskrivning av (3) till $srs = r^{-1}$. Eftersom s har ordning 2, så $s = s^{-1}$, kan vi göra en omskrivning av $srs = r^{-1}$ till $srs^{-1} = r^{-1}$.

Sammanfattningsvis har vi att D_n genereras av elementen r och s, och de uppfyller relationerna

$$s^2 = I, \qquad r^n = I, \qquad srs^{-1} = r^{-1}. \tag{4}$$

För mer detaljer, se [2, s. 170].

2.6 Sidoklasser och kvotgrupper

En förutsättning för att definiera kommande typer av grupper, nämligen normala delgrupper och kvotgrupper, är att först förstå vad en sidoklass är för något.

Definition 2.14. *Låt G vara en grupp och H en delgrupp till G. För $g \in G$ bildar vi mängden gH, alltså $gH = \{gh \mid h \in H\}$, som kallas för vänstersidoklassen till H med avseende på g. På motsvarande sätt bildar vi högersidoklassen till H med avseende på g som Hg, där $Hg = \{hg \mid h \in H\}$.*

Om g är enhetselementet kan man betrakta delgruppen H som en vänstersidoklass gH eller en högersidoklass Hg. Viktigt att lägga märke till är att för icke abelska grupper så spelar det roll på vilken sida vi multiplicerar elementet g med delgruppen. Vi ska gå igenom några egenskaper för sidoklasser. För mer detaljer, se [2, s. 134-136] och [3, s. 80-82].

Låt g_1H, g_2H vara två vänstersidoklasser till en delgrupp H i en grupp G där $g_1, g_2 \in G$. Då gäller det antingen $g_1H = g_2H$ eller $g_1H \cap g_2H = \emptyset$. Två vänstersidoklasser är alltså antingen identiska eller disjunkta. Det här innebär att mängden av alla vänstersidoklasser partitionerar G. Ett element $g \in G$ tillhör alltså endast en vänstersidoklass. Vidare har vi att $|gH| = |H|$ för $g \in G$. En viktig observation är att sidoklasser är inte delgrupper i G då endast H som innehåller enhetselementet. Motsvarande resonemang gäller för högersidoklasserna Hg.

Antalet vänstersidoklasser till H i G betecknas $[G : H]$ och kallas index av H i G. Låt $k = [G : H]$. Eftersom mängden av alla vänstersidoklasser till H partitionerar G samt att alla vänstersidoklasserna är av lika storlek gäller att: $|G| = k|H|$. Vi har alltså förhållandet

$$[G : H] = \frac{|G|}{|H|}.$$

Definition 2.15. *Låt G vara en grupp och N en delgrupp i G. Ifall mängden av alla vänstersidoklasser till N i G är identisk med mängden av alla högersidoklasser till N i G kallas N för en normal delgrupp i G. Vi har alltså $gN = Ng$ för alla $g \in G$. Ekvivalent har vi $g^{-1}Ng = N$ för alla $g \in G$. Att N är normal delgrupp i G betecknas $N \triangleleft G$.*

Vi ger ett exempel på en normal delgrupp i en viss grupp.

Exempel 2.5. Gruppen $N = \{(), (123), (132)\}$ är en delgrupp i S_3. Med hjälp av villkoret i Definition 2.15 ska vi visa att N är en normal delgrupp i S_3.

Först, bildar vi mängden av alla vänstersidoklasser till N, vi kallar den K. Första elementet i K är g_1N där $g_1 = I$ är enhetselementet i G. Andra elementet i K är g_2N där $g_2 = (12) \in S_3$. Med hjälp av avsnitt 2.3 räknar vi snabbt produkten av elementen i S_3 och får att $g_1N = \{(), (123), (132)\}$ och $g_2N = \{(12), (23), (13)\}$. Mängden $K = \{g_1N, g_2N\} = \{\{(), (123), (132)\}, \{(12), (23), (13)\}\}$. Elementen Ng_1 och Ng_2 är alla vänstersidoklasser till N. De är disjunkta och partitionerar hela N. Som kontroll visar vi att indexet av N i S_3 är lika med ordningen av S_3 delat med ordningen av N. Indexet $[S_3 : N] = 2$ och $\frac{|S_3|}{|N|} = \frac{6}{3} = 2$. Alltså $[S_3 : N] = \frac{|S_3|}{|N|}$.

Låt L vara mängden av alla högersidoklasser till N. Den består av elementen $Ng_1 = \{(), (123), (132)\}$ och $Ng_2 = \{(12), (13), (23)\}$. Mängden $L = \{Ng_1, Ng_2\}$. Eftersom mängderna K och L är identiska är N en normal delgrupp i S_3.

Sats 2.16. *[4, s. 194] Låt G vara en grupp och N en normal delgrupp i G. Mängden av alla vänstersidoklasser till N i G bildar en grupp, betecknat G/N. Gruppen G/N kallas kvotgruppen av G med N. Gruppens operation är multiplikation av delmängder (vänstersidoklasser). Mera konkret, låt $g_1N, g_1N \in G/N$, vi har då att $(g_1N)(g_2N) = g_1g_2N$.*

Eftersom N är en normal delgrupp är mängden bestående av högersidoklasser till N i G också en kvotgrupp. Gruppoperationen är multiplikation av högersidoklasser. För Ng_1, Ng_2 i mängden av högersidoklasser är $Ng_1Ng_2 = Ng_1g_2$. Alltså det finns en isomorfi mellan kvotgruppen innehållande vänstersidoklasser och kvotgruppen innehållande högersidoklasser, härav används beteckningen G/N för båda dessa grupper.

Exempel 2.6. Vi betraktar normala delgruppen N i S_3 från Exempel 2.5 för att bilda kvotgruppen S_3/N, enligt Sats 2.16. Vi kan konstatera att

$$S_3/N = \{g_1N, g_2N\} = \{\{(), (123), (132)\}, \{(12), (13), (23)\}$$

är en kvotgrupp av S_3 med N, enligt Sats 2.16. Kvotgruppens ordning är 2 och gruppen S_3/N är därför cyklisk enligt Sats 2.12.

3 Gruppverkan

I det här kapitlet ska vi definiera gruppverkan som är ett viktigt hjälpmedel för att senare kunna bevisa Sylows satser. Vi kommer även att ta upp några ytterligare definitioner och satser som är också nödvändiga för att förstå bevisen av Sylows satser. Vi börjar med den centrala definitionen som är gruppverkan.

Definition 3.1. *Låt G vara en grupp och T en mängd. Gruppen G verkar på mängden T om det existerar en avbildning som till varje $(g, t) \in G \times T$ ordnar ett element $g.t \in T$, sådan att följande två villkor är uppfyllda:*

i) För enhetselementet $I \in G$ gäller att $I.t = t$ för alla $t \in T$.

ii) För alla $g_1, g_2 \in G$ och alla $t \in T$ ska $g_1.(g_2.t) = (g_1 g_2).t$.

Föregående definition är en vänstergruppverkan då G verkar på T från vänster. På motsvarande sätt definieras en högergruppverkan där G verkar på T från höger. Följande notationer $\pi_g(t), g(t), g.t$ är alla lika och syftar på verkan av ett element g på ett element t. Vi kommer dock oftast använda notationen $g.t$. Det ska inte förväxlas med gt som är produkten mellan två element. Vi ska ge ett exempel på gruppverkan.

Exempel 3.1. En grupp G kan verka på en mängd T bestående av alla delgrupper i G genom konjugering. Gruppen G verkar på T enligt

$$g.H = gHg^{-1} \tag{5}$$

för alla $g \in G$ och $H \in T$. Gruppverkan i (5) uppfyller villkoren i Definition 3.1.

3.1 Bana, stabilisator och fixpunktsmängd

Givet en gruppverkan definierar vi några begrepp som ger olika typer av information beroende på det vi söker efter.

Definition 3.2. *En bana av ett element t som tillhör en mängd T under verkan av en grupp G är följande mängd:*

$$\{g.t \mid g \in G\}.$$

Mängden betecknas $\mathrm{Orb}_G(t)$, banan av t under verkan av G. Antalet element i mängden $|\mathrm{Orb}_G(t)|$ kallas längden av banan.

Banan $\mathrm{Orb}_G(t)$ är resultatet av gruppverkan av alla element i G på ett elementet t, och innehåller således element i mängden T. Två banor är antingen disjunkta eller identiska. Mängden av alla banor partitionerar hela mängden T, se [2, s. 203] för bevis.

Definition 3.3. *En stabilisator av ett element t som tillhör en mängd T under verkan av en grupp G är följande mängd:*

$$\{g \in G \mid g.t = t\}.$$

Mängden betecknas $\mathrm{Stab}_G(t)$, stabilisatorn av t under verkan av G.

Stabilisatorn innehåller alla element i G som avbildar elementet t på sig själv. Det existerar alltid ett element i stabilisatorn för varje $t \in T$ eftersom enhetselementet alltid avbildar varje element i T på sig själv. En viktig skillnad mellan en bana och en stabilisator är att den första är en delmängd av T och den andra är en delmängd av G men också en delgrupp i G vilket vi visar i följande sats.

Sats 3.4. *Låt G vara en grupp som verkar på en mängd T. För varje element $t \in T$ är $\operatorname{Stab}_G(t)$ en delgrupp till G.*

Bevis. Eftersom $\operatorname{Stab}_G(t)$ är en delmängd i G kan vi använda Sats 2.4 och visa att dess tre villkor är uppfyllda.

Det första villkoret är uppfyllt eftersom $\operatorname{Stab}_G(t)$ är inte tom och innehåller alltid minst enhetselementet I då $I.t = t$ medför att $I \in \operatorname{Stab}_G(t)$. Låt $g_1, g_2 \in stab_G(t)$. Enligt definitionen av gruppverkan gäller $(g_1g_2).t = g_1.(g_2.t)$. Enligt definitionen av stabilisatorn är $g_2.t = t$ och det medför $(g_1g_2).t = g_1.(g_2.t) = g_1.(t)$. Eftersom $g_1.(t) = t$ är $(g_1g_2).t = t$ så $g_1g_2 \in \operatorname{Stab}_G(t)$.

För det tredje villkoret gällande ett inverselement, låt g vara ett godtyckligt element i $\operatorname{Stab}_G(t)$. Det innebär $g.t = t$. Vi låter g^{-1} verka på båda sidorna om ekvationen. Vi får då $g^{-1}.(g.t) = g^{-1}.t$. Enligt definitionen av gruppverkan är vänsterledet $g^{-1}.(g.t) = (g^{-1}g).t = I.t = t$. Det medför att högerledet $g^{-1}.t = t$ och det innebär $g^{-1} \in \operatorname{Stab}_G(t)$. □

Vi ska nu definiera en slags stabilisator för gruppverkan genom konjugering.

Definition 3.5. *Låt G vara en grupp och T mängden av alla delgrupper i G. Låt G verkan på T genom konjugering. För $H \in T$ är mängden*

$$\operatorname{Stab}_G(H) = \{g \in G \mid g.H = gHg^{-1} = H\}$$

en delgrupp i G. Delgruppen kallas för normalisatorn till H i G och betecknas $N_G(H)$.

Följande sats kallas för Bana-Stabilisator satsen och spelar en viktig roll inom gruppverkan. Den beskriver förhållandet mellan längden av banan av ett element och ordningen av stabilisatorn av samma element.

Sats 3.6. *[3, s. 219] Låt G vara en grupp som verkar på en mängd T. För $t \in T$ har vi banan $\operatorname{Orb}_G(t)$ och stabilisatorn $\operatorname{Stab}_G(t)$. Då gäller det att:*

$$|\operatorname{Orb}_G(t)| = [G : \operatorname{Stab}_G(t)] = \frac{|G|}{|\operatorname{Stab}_G(t)|}.$$

Ett tredje begrepp vi kan få relaterat till gruppverkan är fixpunktsmängder.

Definition 3.7. *Låt G vara en grupp som verkar på en mängd T. För varje $g \in G$ får vi en mängd*

$$T_g = \{t \in T \mid g.t = t\}.$$

Mängden T_g kallas fixpunktsmängden till elementet g och består av alla element t som är fixa under verkan av g.

Vi ska ge en ytterligare definition av fixpunktsmängder som omfattar alla element i en viss grupp och inte ett specifikt element.

Definition 3.8. *Låt G vara en grupp som verkar på en mängd T. Mängden*

$$T_G = \{t \in T \mid g.t = t \text{ för alla } g \in G\}$$

kallas fixpunktsmängden till G.

Vi presenterar ett exempel för att visa hur begreppen banan, stabilisatorn och fixpunktsmängden hänger ihop givet en gruppverkan.

Exempel 3.2. Låt H vara en delgruppen till den symmetriska gruppen S_8 i Exempel 2.4 och T mängden $\{1, 2, 3, 4, 5, 6, 7, 8\}$. Låt H verka på T enligt $h.t = ht$ för alla $h \in H$ och alla $t \in T$.

Vi börjar med begreppet bana och beräknar banan av elementet 1. För $t = 1$ är $\mathrm{Orb}_H(1) = \{1, 7, 4\}$. Stabilisatorn av samma element 1 är $\mathrm{Stab}_H(1) = \{(), (36)\}$. Vi väljer slutligen ett element h, t.ex $h = (174)(258)$ och beräknar dess fixpunktsmängd. Fixpunktsmängden till h blir $T_{(174)(258)} = \{3, 6\}$.

Som kontroll på att vi har räknat rätt, att ordningen av banan och stabilisatorn stämmer, använder vi Sats 3.6. Ordningen av $\mathrm{Stab}_H(1)$ är 2 och ordningen av H är 6. Vi får $\dfrac{|H|}{|\mathrm{Stab}_{H(1)}|} = \dfrac{6}{2} = 3$, vilket är ordningen av $\mathrm{Orb}_H(1)$, så det stämmer.

Följande sats beskriver ett samband mellan ordningen av en grupp och ordningen av dess fixpunktsmängd. Satsens användning kommer senare i uppsatsen bland annat i beviset av Sylows andra sats.

Sats 3.9. *[4, s. 267] Låt G vara en p-grupp som verkar på en mängd T, och låt T_G vara fixpunktsmängden till G, då gäller: $|T| \equiv |T_G| \pmod{p}$.*

3.2 Kommutatordelgruppen

Vi ska nu ta upp en definition och två satser som vi kommer att använda oss av i kapitlet om tillämpningar.

Definition 3.10. *Låt G vara en grupp där a, b är två element i G. Elementet $aba^{-1}b^{-1}$ kallas för kommutatorn av a och b, och betecknas $[a, b]$.*

Följande sats beskriver vad som händer när vi samlar ihop alla dessa kommutatorer.

Sats 3.11. *[4, s. 223] Låt G vara en grupp och låt G' beteckna mängden av alla ändliga produkter av kommutatorer i G. Då är G' en normal delgrupp i G som kallas för kommutatordelgruppen i G.*

Ett förtydligande till föregående sats är att kommutatordelgruppen G' i G genereras av alla kommutatorer i gruppen G.

Sats 3.12. *[4, s. 224] Låt G vara en grupp med G' som dess kommutatordelgrupp. Vidare låt N vara en normal delgrupp i G och vi får då G/N som en kvotgrupp. Kvotgruppen G/N är abelsk om och endast om kommutatordelgruppen G' är en delgrupp till N, alltså $G' \leq N$.*

4 Sylows satser

I den här delen ska vi bevisa Sylows tre satser. Vi kommer också att ta upp något konkret exempel för att förenkla förståelsen av bevisen till respektive sats.

4.1 Sylows första sats

Sylows första sats ger en garanti för existensen av en Sylow p-delgrupp i en ändlig grupp G, givet vissa villkor. Beviset jag visar här utgår ifrån beviset av den tyska matematikern Helmut Wielandt. I beviset framgår tillämpning av gruppverkan. Jag har gjort beviset delvis tydligare och enklare att förstå. I beviset kommer vi ta hjälp av Bana-Stabilisator satsen, se Sats 3.6.

Innan vi bevisar första satsen behöver vi ett väsentligt resultat om primtal och binomialkoefficient som följande lemma ger.

Lemma 4.1. *Om p är ett primtal och $p \nmid m$ då gäller: $p \nmid \binom{p^k m}{p^k}$.*

Bevis. Vi kan expandera binomialkoefficienten för att få ett bättre förståelse.

$$\binom{p^k m}{p^k} = \frac{(p^k m)!}{p^k!(p^k m - p^k)!} = \frac{p^k m(p^k m-1)\cdots(p^k m - p^k + 1)(p^k m - p^k)!}{p^k(p^k-1)\cdots(p^k - p^k + 1)(p^k m - p^k)!}$$

$$= \frac{p^k m(p^k m-1)\cdots(p^k m - j)\cdots(p^k m - p^k + 1)}{p^k(p^k-1)\cdots(p^k - j)\cdots(p^k - p^k + 1)}$$

$$= m \cdot \frac{(p^k m - 1) \cdots (p^k m - j) \cdots (p^k m - p^k + 1)}{(p^k - 1) \cdots (p^k - j) \cdots (p^k - p^k + 1)}.$$

Vi vet redan att m inte är delbart med p och för att visa att andra faktorn inte är det heller gör vi först en omskrivning till

$$\binom{p^k m}{p^k} = m \cdot \prod_{j=1}^{p^k - 1} \frac{p^k m - j}{p^k - j}.$$

Betrakta nu en faktor

$$\frac{p^k m - j}{p^k - j}. \tag{6}$$

Vi gör en omskrivning av j för att visa att täljaren i (6) inte delas av p när (6) har förkortats så långt som möjligt. Låt $j = p^n q$ där $p \nmid q$ och $n < k$, (vi har fortfarande att $0 < p^n q \leq p^k - 1$). Vi får:

$$\frac{p^k m - j}{p^k - j} = \frac{p^k m - p^n q}{p^k - p^n q} = \frac{p^{k-n} - q}{p^{k-n} m - q}.$$

Alla p faktorer tar ut varandra och vi ser direkt att sista bråket inte är delbart med p. $\square$

Nu är vi redo att bevisa Sylows första sats.

Sats 4.2. *Om G är en ändlig grupp med ordningen $p^k m$ där p är ett primtal, $k, m \in \mathbb{N}$ och $p \nmid m$, då har G en Sylow p-delgrupp av ordning p^k.*

Bevis. Först låter vi S beteckna mängden av delmängder av G med p^k element, alltså $S = \{T \subseteq G : |T| = p^k\}$ består av delmängder av storlek p^k där själva elementen i delmängderna kommer från gruppen G. Antalet element i mängden är således lika med binomialkoefficienten $\binom{p^k m}{p^k}$. Lemma 4.1 ger att $p \nmid |S|$.

Nu ska vi låta gruppen G verka på mängden S enligt följande: För varje $g \in G$ och $T \in S$ har vi: $g.T = gT$.

Givet gruppverkan kan vi betrakta banorna $\mathrm{Orb}_G(T) = \{g.T \mid g \in G\}$ för $T \in S$. Vi tar reda på alla dessa banor. Eftersom summan av alla banors längder, $|\mathrm{Orb}_G(T)|$, är lika med $|S|$ har vi att p inte delar alla $|\mathrm{Orb}_G(T)|$ eftersom det skulle betyda att p delar $|S|$ vilket vore en motsägelse.

Vi låter $\mathrm{Orb}_G(T_1) = \{T_1, T_2, \ldots, T_u\} \subseteq S$ vara en bana för något $T_1 \in S$, sådan att $p \nmid u$, alltså p delar inte längden, u, av banan. Vi betecknar banan med S_0, alltså

$S_0 = \mathrm{Orb}_G(T_1)$. Vi betraktar nu samma gruppverkan, fast på en delmängd till S. Gruppen G verkar på delmängden $S_0 \subseteq S$ enligt följande: För varje $g \in G$ och $T \in S_0$ har vi: $g.T = gT$. Givet gruppverkan betraktar vi $\mathrm{Stab}_G(T_1)$ och betecknar den med H

$$H = \mathrm{Stab}_G(T_1) = \{g \in G \mid g.T_1 = T_1\}, \tag{7}$$

stabilisatorn av T_1 under verkan av G. Stabilisatorn H är en delgrupp i G enligt Sats 3.4.

Med hjälp av Sats 3.6 har vi $|G| = u|H|$, det är utifrån den likheten vi ska försöka visa att $|H| = p^k$. Enligt förutsättningen i satsen måste p^k dela $|G|$, och vi vet sedan tidigare att $p \nmid u$, därför måste p^k dela $|H|$. Eftersom p^k delar $|H|$ måste $p^k \leq |H|$.

Enligt (7) gäller att för varje $h \in H$ är $h.T_1 = T_1$, eftersom det är det som stabilisatorn, H, gör är att avbilda element på sig själva. Vi definierar en ny gruppverkan. Gruppen H verkar på mängden T_1 enligt följande: För varje $h \in H$ och $t \in T_1$ har vi: $h.t = ht$.

Givet gruppverkan och ett element $t \in T_1$ betraktar vi $\mathrm{Stab}_H(t) = \{h \in H \mid h.t = t\}$, vi betecknar den gruppen H_t. Vi påminner om att både H och T_1 är delmängder till gruppen G. Stabilisatorn H_t innehåller endast enhetselementet I eftersom det är endast det elementet som avbildar t på sig själv. Därför har vi $|H_t| = 1$. Vi har också givet gruppverkan banan $\mathrm{Orb}_H(t) = \{h.t \mid h \in H\}$, som är en delmängd av mängden T_1. Vi har $|T_1| = p^k$ enligt tidigare, så $|\mathrm{Orb}_H(t)|$ kan inte vara större än p^k, alltså $|\mathrm{Orb}_H(t)| \leq p^k$.

När vi använder Sats 3.6 på nytt har vi följande likhet $|H| = |\mathrm{Orb}_H(t)| \cdot |H_t|$ som leder till att $|H| = |\mathrm{Orb}_H(t)| \leq p^k$. Vi påminner att vi sedan tidigare i beviset har olikheten $p^k \leq |H|$ och tillsammans med den sista olikheten $|H| \leq p^k$ får vi att $|H| = p^k$. Alltså är H en Sylow p-delgrupp i G med ordningen p^k. $\square$

Vi går nu igenom ett exempel för att förtydliga processen av beviset. Vi ska konkretisera beviset av satsen genom att visa steg för steg att den symmetriska gruppen S_3 har Sylow 2-delgrupper.

Exempel 4.1. Gruppen S_3 med gruppoperationen funktionskomposition har följande element, $S_3 = \{(), (12), (13), (23), (123), (132)\}$. Vi primtalsfaktoriserar ordningen av S_3, så $|S_3| = 6 = 2 \cdot 3$. Enligt Sylows första sats måste gruppen S_3 innehålla Sylow 2-delgrupper och Sylow 3-delgrupper. Vi ska visa i det här exemplet fallet $p = 2$, så målet är att följa bevisets resonemang av att S_3 har minst en delgrupp H av ordning 2.

Vi följer helt enkelt beviset steg för steg. Vi börjar med att bilda mängden S som består av 2-element-delmängder av mängden S_3. Antalet element i S är binomialkoefficenten $\binom{6}{2} = 15$. Således blir

$$\begin{aligned}S =&\{\{(), (12)\}, \{(), (13)\}, \{(), (23)\}, \{(), (123)\}, \{(), (132)\},\\&\{(12), (13)\}, \{(12), (23)\}, \{(12), (123)\},\\&\{(12), (132)\}, \{(13), (23)\}, \{(13), (123)\}, \{(13), (132)\},\\&\{(23), (123)\}, \{(23), (132)\}, \{(123), (132)\}\}.\end{aligned}$$

Lemma 4.1 ger att $2 \nmid |S|$. Vi låter gruppen S_3 verkar på mängden S enligt följande: För varje $g \in S_3$ och $T \in S$ har vi $g.T = gT$.

Givet gruppverkan kan vi betraktar banorna $\operatorname{Orb}_{S_3}(T) = \{g.(T) \mid g \in S_3\}$ för $T \in S$. Vi beräknar alla banor givet gruppverkan. Vi tar hjälp av Cayleytabellen för S_3 i avsnitt 2.3 för att underlätta beräkningen av banorna under S_3:s verkan på S. Vi får fyra olika banor:

$$\begin{aligned}\operatorname{Orb}_{S_3}(T_1) &= \{\{(13), (123)\}, \{(), (12)\}, \{(23), (132)\}\},\\ \operatorname{Orb}_{S_3}(T_2) &= \{\{(23), (123)\}, \{(12), (132)\}, \{(), (13)\}\},\\ \operatorname{Orb}_{S_3}(T_3) &= \{\{(12), (123)\}, \{(13), (132)\}, \{(), (23)\}\},\\ \operatorname{Orb}_{S_3}(T_4) &= \{\{(), (123)\}, \{(12), (23)\}, \{(13), (12)\},\\ &\qquad \{(23), (13)\}, \{(123), (132)\}, \{(132), ()\}\}.\end{aligned}$$

Följande $T_1 = \{(13), (123)\}, T_2 = \{(23), (123)\}, T_3 = \{(12), (123)\}$ och $T_4 = \{(), (123)\}$ är element i mängden S. Alla dessa fyra banor bildar en partition av mängden S och därför är summan av banornas längder lika med $|S|$. Vi har alltså att

$$|S| = |\operatorname{Orb}_{S_3}(T_1)| + |\operatorname{Orb}_{S_3}(T_2)| + |\operatorname{Orb}_{S_3}(T_3)| + |\operatorname{Orb}_{S_3}(T_4)| = 15.$$

Vårt $p = 2$ delar inte längden av varje sådan bana eftersom då skulle summan av alla fyra banornas längder, alltså $|S|$, dela 2 vilket vore en motsägelse enligt Lemma 4.1.

Vi väljer nu en bana bland dessa fyra vars längd inte är delbar med 2. Banan $\operatorname{Orb}_{S_3}(T_3) \subseteq S$ är en sådan, vi betecknar den med B (den motsvarar S_0 i beviset). Vi har samma gruppverkan fast på en delmängd till S. Gruppen S_3 verkar på delmängden $B \subseteq S$ enligt följande: För varje $g \in G$ och $T \in B$ har vi: $g.T = gT$. Givet gruppverkan beräknar vi $\operatorname{Stab}_{S_3}(T_3)$ och betecknar den med H

$$H = \operatorname{Stab}_{S_3}(T_3) = \{g \in G \mid g.T_3 = T_3\},$$

stabilisatorn av T_3 under verkan av S_3. Vi får att $H = \{(), (13)\}$. Vi konstaterar direkt att H är en Sylow 2-delgrupp i S_3.

Ett annat val av bana, t.ex banan $\mathrm{Orb}_{S_3}(T_1)$, hade gett oss att $H = \{(), (23)\}$. Banan $\mathrm{Orb}_{S_3}(T_2)$ hade gett $H = \{(), (12)\}$. Dessa tre stycken är nämligen alla Sylow 2-delgrupper i S_3. De är dessutom cykliska enligt Sats 2.12.

4.2 Sylows andra sats

Sylows andra sats säger att vilka två Sylow p-delgrupper som helst är konjugerade delgrupper. I beviset kommer vi använda oss av Sats 3.9 och Sats 2.5.

Sats 4.3. *Låt G vara en ändlig grupp med ordningen $p^k m$, som i Sylows första sats. Låt P_1 och P_2 vara två Sylow p-delgrupper i G, då är P_1 och P_2 konjugerade delgrupper i G.*

Bevis. Att P_1 och P_2 är två konjugerade delgrupper betyder, enligt Definition 2.6, att det finns ett $g \in G$ sådant att $P_1 = gP_2g^{-1}$. Målet är att finna ett sådant g.

Låt T vara mängden av alla vänstersidoklasser xP_1 till P_1, alltså $T = \{xP_1 \mid x \in G\}$. Vi låter gruppen P_2 verkar på mängden T enligt följande:
$y.(xP_1) = yxP_1$ för alla $y \in P_2$ och $xP_1 \in T$.

Nu kan vi bestämma fixpunktsmängden till P_2, enligt Definition 3.8, givet gruppverkan: $T_{P_2} = \{xP_1 \in T \mid y.xP_1 = xP_1 \text{ för alla } y \in P_2\}$. Enligt Sats 3.9 har vi att

$$|T| \equiv |T_{P_2}| \pmod{p}. \tag{8}$$

Antalet element i mängden T av vänstersidoklasser till P_1 i G är lika med index av P_1 i G, betecknat $[G : P_1]$, och det i sin tur är lika med $\dfrac{|G|}{|P_1|} = \dfrac{p^k m}{p^k} = m$, så

$$|T| = [G : P_1] = \frac{|G|}{|P_1|} = m. \tag{9}$$

Utifrån (9) har vi att p inte kan vara en delare i $|T|$. Att $|T| \not\equiv 0 \pmod{p}$ medför att $|T_{P_2}| \not\equiv 0 \pmod{p}$ heller enligt (8). Det här leder till att T_{P_2} inte kan vara en tom mängd och måste därför innehålla minst ett element, låt oss kalla det för xP_1.

Gruppverkan av gruppen P_2 på elementet xP_1 ger:

$$y.(xP_1) = xP_1, \tag{10}$$

som är ekvivalent med

$$yxP_1 = xP_1, \tag{11}$$

för alla $y \in P_2$. Vi multiplicerar båda leden av (11) med elementet $x^{-1} \in G$ från vänster sida och får

$$x^{-1}yxP_1 = P_1. \tag{12}$$

Detta är ekvivalent med att $x^{-1}yx \in P_1$ för alla $y \in P_2$. Utifrån det får vi att $x^{-1}P_2x$ är en delgrupp i P_1, så $x^{-1}P_2x \leq P_1$.

Eftersom P_1 och P_2 båda är Sylow p-delgrupper så är ordningen av de två lika $|P_1| = |P_2|$. Och enligt Sats 2.5 har vi $|x^{-1}P_2x| = |P_2|$. Sätter vi ihop båda dessa två samband får vi att $|P_1| = |x^{-1}P_2x|$ och eftersom alla element i $x^{-1}P_2x$ är innehållande i P_1 måste $x^{-1}P_2x = P_1$. Vi har därmed funnit vårt sökta $g = x^{-1}$. □

Som en konsekvens av satsen får vi att en Sylow p-delgrupp, kalla den för P, i en grupp G är en normal delgrupp om och endast om P är den enda Sylow p-delgruppen i G.

4.3 Sylows tredje sats

I den tredje satsen av Sylow tar vi reda på mera information om antalet Sylow p-delgrupper. Satsen säger att antalet Sylow p-delgrupper i en grupp G delar ordningen av gruppen G samt att antalet Sylow p-delgrupper är kongruent med 1 modulo p. Med hjälp av Sylow sats två och tre kan vi exempelvis i vissa fall få veta ifall Sylow p-delgruppen är en normal delgrupp eller inte.

I beviset använder vi gruppverkan genom konjugering av delgrupper. Dessutom utnyttjar vi Sats 3.9 samt Sylows första och andra sats i beviset.

Sats 4.4. *Låt G vara en ändlig grupp med ordningen $p^k m$ där p är ett primtal, $k, m \in \mathbb{N}$ och $p \mid m$. Då gäller två saker: antalet Sylow p-delgrupper, betecknat n_p, i G är kongruent med 1 modulo p och vidare gäller att n_p delar m, vilket speciellt betyder att n_p delar gruppens ordning.*

Bevis. Vi delar upp beviset i två delar. Vi börjar med att bevisa den första delen, att

$$n_p \equiv 1 \pmod{p}. \tag{13}$$

Vi låter S vara mängden av alla Sylow p-delgrupper i G. Då är kardinaltalet för S lika med n_p. Vi väljer en godtycklig Sylow p-delgrupp ur S och kallar den för P. Vi låter P verka, genom konjugering av delgrupper, på S enligt följande:

$$g.H = gHg^{-1}$$

för alla $g \in P$ och $H \in S$.

Till gruppverkan ovan bildar vi fixpunktsmängden till P som

$$S_P = \{H \in S \mid g.H = gHg^{-1} = H \text{ för alla } g \in P\}. \tag{14}$$

Vi har enligt Sats 3.9 att $|S| \equiv |S_P| \pmod p$. Det här är ett viktigt förhållande där vi ska försöka visa att $|S_P| = 1$ och då följer (13) av att $|S| = n_p$ och $S_P = 1$.

Vi noterar att S_P är en icke tom mängd, gruppen $P \in S_p$ eftersom $gPg^{-1} = P$ för alla $g \in P$. Mängden S_P innehåller element från mängden S och vi väljer ett godtyckligt sådant element H. Ekvation (14) liknar Definition 3.5 av normalisatorn $N_G(H)$ till en delgrupp H i en grupp G. Normalisatorn $N_G(H)$ består av alla element i G som uppfyller likheten $gHg^{-1} = H$. Av ekvation (14) framgår det att om $H \in S_P$ så uppfyller samtliga element $g \in P$ likheten $gHg^{-1} = H$. Detta leder till P är en delgrupp i normalisatorn $N_G(H)$. Delgruppen H är också en delgrupp till sin egen normalisatorn $N_G(H)$. Vi vet redan att både P och H är Sylow p-delgrupper i G och eftersom båda också är delgrupper till $N_G(H)$ är de också Sylow p-delgrupper i $N_G(H)$.

Enligt Sats 4.3 har vi att delgrupperna P och H är konjugerade till varandra i $N_G(H)$. Enligt definitionen av normalisatorn har vi att H är en normal delgrupp till $N_G(H)$ och det medför att H måste vara den enda Sylow p-delgruppen i $N_G(H)$. Därför kan vi inte ha flera Sylow p-delgrupper i $N_G(H)$, alltså är $H = P$. Eftersom vi tidigare valde H godtyckligt i S_P innebär detta att fixpunktsmängden S_P innehåller endast ett element, så $|S_P| = 1$, vilket är det vi önskade komma fram till.

Nu ska vi bevisa den andra delen av satsen, n_p delar m.

Vi låter återigen S vara mängden av alla Sylow p-delgrupper i G och $P \in S$. Vi låter gruppen G verka på S genom konjugering av delgrupper enligt följande: För varje $g \in G$ och $P \in S$ har vi: $g.P = gPg^{-1}$. Då Sats 4.3 säger att alla Sylow p-delgrupper är konjugerade innerbär det att det bara kan finnas en bana i S under G. Vi väljer ett godtyckligt $P \in S$, då gäller:

$$n_p = |S| = |\operatorname{Orb}_G(P)| = \frac{|G|}{|G_P|} \tag{15}$$

där G_P är stabilisatorn av P under G. Från (15) får vi att n_p delar $|G| = p^k m$. Eftersom $p \nmid n_p$ enligt (13), gäller $n_p \mid m$ vilket skulle bevisas. $\square$

Exempel 4.2. Vi illustrerar Sylow p-delgrupper för gruppen S_3 med ordningen $|S_3| = 6 = 2 \cdot 3$. Från Exempel 2.5 vet vi att S_3 har en normal delgrupp av ordning 3 och det måste betyda att S_3 endast har en Sylow 3-delgrupp. Antalet Sylow

3-delgrupper, betecknat n_3, är alltså lika med 1. I Exempel 4.1 tog vi reda på alla Sylow 2-delgrupper i S_3. Antalet Sylow 2-delgrupper, betecknat n_2, är alltså lika med 3. Vi har $n_2 = 3$ och $n_3 = 1$.

Vi har att n_2 uppfyller $n_2 \equiv 1 \pmod 2$ och $n_2 \mid 3$ samt n_3 uppfyller $n_3 \equiv 1 \pmod 3$ och $n_3 \mid 2$. Både n_2 och n_3 stämmer därför med Sylows tredje sats.

5 Tillämpningar

Nu kommer vi till den tredje delen av uppsatsen där vi med hjälp av Sylows satser ska kunna bestämma karaktären av grupper av vissa ordningar.

5.1 Några grupper av liten ordning

Som en första tillämpning av Sylows satser ska vi visa att alla grupper G av ordning 15 är cykliska. Vi formulerar påståendet som följande sats.

Sats 5.1. *Alla grupper G av ordning 15 är cykliska.*

Bevis. Vi primtalsfaktoriserar gruppens ordning först, så $|G| = 15 = 3 \cdot 5$. Vårt mål är att visa att det existerar minst ett element $g \in G$ som har ordning 15, eftersom det då betyder att g genererar gruppen G. Med hjälp av Sats 4.2 har vi att det existerar Sylow 3-delgrupper och Sylow 5-delgrupper. Vi låter n_3 och n_5 beteckna antal Sylow 3-delgrupper respektive Sylow 5-delgrupper. Från Sats 4.4 har vi att n_3 måste uppfylla $n_3 \equiv 1 \pmod 3$ och $n_3 \mid 5$ samt att n_5 måste uppfylla $n_5 \equiv 1 \pmod 5$ och $n_5 \mid 3$ vilket resulterar i att n_3 och n_5 måste vara lika med 1. Som en konsekvens av Sats 2.4 vet vi att varje grupp har de triviala delgrupperna, delgruppen med endast enhetselementet och gruppen själv. Vi vet också enligt Sats 2.7 att elements ordningen delar gruppens ordning, så de möjliga elements ordningarna är 1, 3, 5 och 15. Nu ska vi bestämma hur många element i G som har var och en av dessa ordningar.

Det är endast enhetselementet som har ordningen 1. Eftersom vi endast har en delgrupp av ordning 3 så existerar det bara 2 element med ordning 3, det tredje elementet i delgruppen måste ju vara enhetselementet. Vi har också endast en delgrupp av ordning 5 och därmed finns det 4 element av ordning 5. Antal element som är kvar i G är 8 stycken, alla har ordning 15.

Vi har lyckats visa att det finns åtminstone ett element som kan generera gruppen G och därför är gruppen cyklisk. $\square$

På liknande sätt ska vi visa att alla grupper av ordning 51 är cykliska. Resultatet här kommer vi använda senare i avsnitt 5.2 med grupper av större ordning.

Sats 5.2. *Alla grupper G av ordning 51 är cykliska.*

Bevis. Vi primtalsfaktorisera gruppens ordning först, så $|G| = 51 = 3 \cdot 17$. Med hjälp av Sats 4.2 existerar det n_3 Sylow 3-delgrupper och n_{17} Sylow 17-delgrupper. Från Sats 4.4 har vi att $n_3 \equiv 1 \pmod{17}$ och $n_3 \mid 17$ samt att $n_{17} \equiv 1 \pmod{3}$ och $n_{17} \mid 3$ vilket resulterar i att n_3 och n_{17} är lika med 1. De möjliga ordningar som elementen g i gruppen G kan ha måste dela G:s ordning förstås, de är 1, 3, 17 och 51. Nu kan vi bestämma antal element i G som har dessa ordningar, på samma sätt som i beviset av Sats 5.1. Vi presenterar resultatet i följande tabell.

o(g)	antal
1	1
3	2
17	16
51	32

Vi ser direkt utifrån tabellen att G innehåller element g som genererar gruppen. □

5.2 Grupper av ordning 2p

Vi tar ett exempel där gruppens ordning är lite mer generell, alltså med en variabel.

Sats 5.3. *Låt G vara en grupp med ordningen $2p$ där p är ett udda primtal. Då är G antingen en cyklisk grupp eller isomorf med dihedrala gruppen D_p.*

Bevis. Vi har en grupp G med ordningen $|G| = 2 \cdot p$, med $p > 2$.

Enligt Sylows första sats har vi Sylow 2-delgrupper och Sylow p-delgrupper. Med hjälp av Sylows tredje sats ska vi bestämma antalet sådana grupper. Antalet Sylow 2-delgrupper betecknas n_2. Då gäller $n_2 \mid p$ vilket ger $n_2 = 1$ eller $n_2 = p$. Antalet Sylow p-delgrupper betecknas n_p. Då gäller $n_p \mid 2$ och $n_p \equiv 1 \pmod{p}$ vilket ger $n_p = 1$. Vi får två fall: i) $n_2 = 1$, $n_p = 1$. ii) $n_2 = p$, $n_p = 1$.

Fall i). De möjliga ordningar som elementen g i gruppen G kan ha måste dela $|G|$, så de är 1, 2, p och $2p$. De enda delgrupperna i G, förutom de triviala, är Sylow 2-delgrupper och Sylow p-delgrupper. Nu kan vi som vi tidigare visat i Sats 5.1, bestämma antal element i G som har dessa ordningar. Vi presenterar resultatet i tabellen nedan.

o(g)	antal
1	1
2	2
p	$p-1$
$2p$	$p-1$

Eftersom antalet element av ordning $2p$ är $p-1>0$ är G cyklisk.

Fall ii). Låt $H=\langle a\rangle$ vara Sylow p-delgruppen för något $a\in H$ och låt $K=\langle b\rangle$ vara en Sylow 2-delgrupp. Vi har att $|\langle a\rangle|=p$ och $|\langle b\rangle|=2$. Gruppen H är en normal delgrupp, så vi har $bHb^{-1}=H$. Vi definierar en grupphomomorfi $\varphi: H\to H$ där

$$\varphi(x)=bxb^{-1} \tag{16}$$

för $x\in H$. Vi betraktar den sammansatta funktionen $\varphi\circ\varphi$ och får

$$\varphi\circ\varphi(x)=\varphi(\varphi(x))=b(bxb^{-1})b^{-1}=IxI^{-1}=x. \tag{17}$$

I (17) är $bb=I$ och $b^{-1}b^{-1}=I^{-1}=I$ eftersom ordningen för b är ju 2. Från (17) får vi att $\varphi\circ\varphi=I$, det avbildar alla element på sig själva. Låt

$$\varphi(a)=a^k \tag{18}$$

för något $k\in\mathbb{Z}$. Ekvationerna (17) och (18) ger

$$a=\varphi(\varphi(a))=\varphi(a^k)=(\varphi(a))^k=a^{k^2} \tag{19}$$

och vi får att $a=a^{k^2}$. Eftersom ordningen av a är ett primtal gäller $a=a^{k^2}$ om och endast om $k^2\equiv 1 \pmod p$. Vi förenklar ekvationen till $k^2-1\equiv 0 \pmod p$ och med hjälp av konjugatregeln får vi $(k-1)(k+1)\equiv 0 \pmod p$.

Detta leder till att $p\mid(k-1)(k+1)$ så $p\mid(k-1)$ eller $p\mid(k+1)$. Vi får $k\equiv\pm1$ (mod p) och det innebär att vi måste undersöka två fall, $k=1$ eller $k=-1$. För $k=1$ sätter vi samman (16) och (18) och får $\varphi(a)=a$, alltså $bab^{-1}=a$ och det är ekvivalent med $ba=ab$. Det här är en motsägelse då K inte är en normal delgrupp.

För $k=-1$ sätter vi samman (16) och (18) och får $\varphi(a)=a^{-1}$, alltså

$$bab^{-1}=a^{-1}. \tag{20}$$

Vi jämför nu med beskrivningen av den dihedrala gruppen i avsnitt 2.5 och jämför relationen mellan elementen a,b och elementen s,r. Vi har

$$a^p=I, \qquad b^2=I. \tag{21}$$

Vi ser att vi har likheter mellan ekvationerna (20), (21) och ekvationerna (4), se avsnitt 2.5. Vi ser att grupperna har precis samma struktur, och är alltså isomorfa. □

5.3 Grupper av lite större ordning

Nu ska vi undersöka grupper av lite större ordningar, vi tar en ordning där antalet primtalsfaktorer är 3 stycken istället för 2 som i våra tidigare fall.

Sats 5.4. *Alla grupper G av ordning 255 är abelska.*

Bevis. Vi primtalsfaktoriserar gruppens ordning, så $|G| = 255 = 3 \cdot 5 \cdot 17$. Vi låter n_{17} och n_5 beteckna antal Sylow 17-delgrupper respektive Sylow 5-delgrupper. Med hjälp av Sats 4.4 har vi att $n_{17} \equiv 1 \pmod{17}$ och $n_{17} \mid 15$ vilket ger $n_{17} = 1$ samt $n_5 \equiv 1 \pmod 5$ och $n_5 \mid 51$ vilket ger $n_5 = 1$.

Vi vet nu alltså att gruppen G har en normal delgrupp P av ordning 17 och en normal delgrupp Q av ordning 5. Vi definierar nu kvotgrupperna G/P och G/Q, vilkas ordningar är index för P respektive index för Q, så $|G/P| = \dfrac{255}{17} = 15$ och $|G/Q| = \dfrac{255}{5} = 51$.

Enligt Sats 5.1 och Sats 5.2 är G/P och G/Q cykliska grupper och enligt Sats 2.13 är de också abelska grupper. Eftersom G/P och G/Q är abelska följer det enligt Sats 3.12 att både normalgrupperna P och Q innehåller kommutatordelgruppen G', alltså $G' \leq P$ och $G' \leq Q$. Därför måste ordningen för G' vara en delare i både $|P|$ och $|Q|$ och den enda gemensamma delaren till $|P|$ och $|Q|$ är 1. Detta innebär att ordningen av G' är 1 och G' innehåller således endast enhetselementet I.

Att $G' = \{I\}$ leder till att det för varje kommutator $aba^{-1}b^{-1}$ där $a, b \in G$ gäller att $aba^{-1}b^{-1} = I$. Det innebär att G är abelsk, eftersom det betyder att alla element $a, b \in G$ kommuterar, dvs uppfyller $ab = ba$. I och med det får vi att G är abelsk. □

Referenser

[1] Norman L. Biggs, *Discrete Mathematics*, OUP Oxford, 2002

[2] Norman J. Bloch, *Abstract Algebra with Applications*, Prenrice-Hall, 1987

[3] John R. Durbin, *Modern Algebra An Introduction - 4th ed*, John Wiley & Sons Inc, 2000

[4] Per-Anders Svensson, *Abstrakt Algebra*, Studentlitteratur AB, 2001

[5] Wikipedia, Sylow theorems, (hämtad 2020-04-28)

[6] Wikipedia, Klein four-group, (hämtad 2020-04-27)

[7] Wikipedia, Abstract algebra, (hämtad 2019-10-02)

[8] Wikipedia, Évariste Galois, (hämtad 2019-10-02)

[9] Wikipedia, Carl Friedrich Gauss, (hämtad 2019-10-02)

[10] Wikipedia, Cauchy's theorem (group theory), (hämtad 2020-04-28)

[11] Wikipedia, Peter Ludwig Mejdell Sylow, (hämtad 2020-04-28)