Tillägg till föreläsning 3 (11/9/01)

Sats 3.1 *Låt $n, k \geq 0$ vara heltal. Antalet lösningar till*

$$x_1 + x_2 + \cdots + x_k = n, \tag{1}$$

där de x_i är icke-negativa heltal, är $\begin{pmatrix} n+k-1 \\ k-1 \end{pmatrix}$.

BEVIS : Vi inför symbolerna $\cdot$, $|$, som ska kallas för 'dot' och 'dash' resp. Notera att den binomiala koefficienten $\begin{pmatrix} n+k-1 \\ k-1 \end{pmatrix}$ är lika med antalet ord som kan bildas ut av n stycken 'dots' och $k-1$ stycken 'dashes'. För varje sådant ord innehåller $n+k-1$ symboler totalt, och ordet bestäms unikt av vilka $k-1$ av de $n+k-1$ positionerna som har en 'dash'.

Vi skall nu beskriva en 1-1 korrespondens mellan dessa ord och lösningarna till (1). Tag ett godtyckligt ord W alltså, och ansluta därtill k-tuplet $(x_1, x_2, ..., x_k)$, där

$x_1 =$ antalet 'dots' innan den första 'dash',
$x_2 =$ antalet 'dots' mellan den första och andra 'dashes',
$x_3 =$ antalet 'dots' mellan den andra och tredje 'dashes',
. ...
. ...
. ...
$x_k =$ antalet 'dots' efter den sista 'dash'.

Eftersom det finns n stycken 'dots' totalt i W, då är $(x_1, ..., x_k)$ en lösning till (1). Det är klart att olika ord ger olika k-tupel, och att varje lösning till (1) anslutas till något ord. Då har vi den efterlängtade 1-1 korrespondensen och beviset är slut.

Sats 3.2 *Låt $n \geq 0$ vara ett heltal. Då gäller att*

$$\begin{pmatrix} 2n \\ n \end{pmatrix} = \sum_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix}^2. \tag{2}$$

BEVIS : Den VL av (2) är antalet n-element delmängder till $\{1, ..., 2n\}$. Låt $\mathcal{A}$ beteckna samlingen av alla dessa n-element mängder. Vi skall nu visa hur

man får dela upp $\mathcal{A}$ i n stycken mindre samlingar, $\mathcal{A}_1, ..., \mathcal{A}_n$, så att

$$\#(\mathcal{A}_k) = \left(\begin{array}{c} n \\ k \end{array} \right)^2. \tag{3}$$

Detta skall räcka till att bevisa (2). Så vad är $\mathcal{A}_k$ då ?

Ju, först splittra mängden $\{1, ..., 2n\}$ i två halvar, $H_1 := \{1, ..., n\}$ och $H_2 := \{n+1, ..., 2n\}$. Låt då $\mathcal{A}_k$ bestå av alla n-element mängder som innehåller k element från H_1 och $n-k$ från H_2. Då är varje mängd X i samlingen $\mathcal{A}_k$ av formen

$$X = X_1 \sqcup X_2,$$

där X_1 är en k-element delmängd till H_1 och X_2 är en $(n-k)$-element delmängd till H_2. Vi har alltså $\left(\begin{array}{c} n \\ k \end{array} \right)$ möjligheter för X_1 och $\left(\begin{array}{c} n \\ n-k \end{array} \right)$ möjligheter för X_2. Enligt multiplikationprincipen har vi då totalt

$$\left(\begin{array}{c} n \\ k \end{array} \right) \times \left(\begin{array}{c} n \\ n-k \end{array} \right) = \left(\begin{array}{c} n \\ k \end{array} \right) \times \left(\begin{array}{c} n \\ k \end{array} \right) = \left(\begin{array}{c} n \\ k \end{array} \right)^2$$

möjligheter för X, som bevisar (3) och därmed hela satsen.

Sats 3.3 *Låt $n \geq 0$ vara ett heltal. Då gäller att*

$$2^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right). \tag{4}$$

BEVIS : Koefficienten $\left(\begin{array}{c} n \\ k \end{array} \right)$ är antalet k-element delmängder till $\{1, ..., n\}$. Om vi summerar över k, från 0 till n, då räknas VARJE delmängd till $\{1, ..., n\}$ precis en gång. Det kvarstår därför att bevisa att $\{1, ..., n\}$ har totalt 2^n delmängder. Vi gör detta genom att beskriva en 1-1 korrespondens mellan delmängderna och binära ord av längd n. Enligt multiplikationsprincipen, är antalet sådana ord exakt 2^n, eftersom vi har två möjligheter (0 eller 1) för varje position, och n positioner totalt.

Tag nu ett ord W. Antag att W har en etta i k stycken positioner, säg positioner $x_1, ..., x_k$ där $1 \leq x_1 < ... < x_k \leq n$, och en nolla i de kvarstående positionerna. Anslut då till W, k-element mängden $\{x_1, ..., x_k\}$, som är en

delmängd till $\{1, ..., n\}$. Det är klart att till olika ord anslutas olika mängder, och att varje delmängd till $\{1, ...n\}$ anslutas till något ord. Då har vi den efterlängtade 1-1 korrespondensen, och beviset är därmed slut.

OBS! Ekv. (4) kan också deriveras genom att sätta $x = y = 1$ i Binomialsatsen. Se dina föreläsningsanteckningar.

Sats 3.4 *Låt X vara en ändlig, icke-tom mängd. Då är det totala antalet delmängder till X bestående av ett jämnt antal element lika med det totala antalet delmängder bestående av ett udda antal element.*

BEVIS : Det räcker att betrakta mängderna $\{1, ..., n\}$, för $n \geq 1$. Låt J_n (resp. U_n) beteckna det totala antalet delmängder till $\{1, ..., n\}$ bestående av ett jämnt (resp. udda) antal element. Vi skall visa att, för alla $n \geq 1$,

$$J_n = U_n = J_{n-1} + U_{n-1} = 2^{n-1}.$$

Betrakta J_n. Låt A vara en delmängd till $\{1, ..., n\}$ som har ett jämnt antal element. Det finns J_n möjligheter för A enligt definitionen. Antingen $n \in A$ eller $n \notin A$. Om $n \in A$ då är $A = \{n\} \sqcup A^*$, där A^* är en delmängd till $\{1, ..., n-1\}$ som har ett element mindre än A, därför ett udda antal element. Enligt definitionen, finns det U_{n-1} möjligheter för A^*. Om $n \notin A$, där är A själv en delmängd till $\{1, ..., n-1\}$, med ett jämnt antal element, så enligt definitionen finns det J_{n-1} möjligheter för A.

Då finns det totalt $J_{n-1} + U_{n-1}$ möjligheter för A, som bevisar att $J_n = J_{n-1} + U_{n-1}$.

En liknande argument (som lämnas till läsaren), visar att $U_n = J_{n-1} + U_{n-1}$. Slutligen, att $J_n = U_n = 2^{n-1}$ följer då från att $\{1, ..., n\}$ har totalt 2^n delmängder (se beviset av Sats 3.3).

OBS! I termer av binomiska koefficienter, Sats 3.4 är ekvivalent med ekvationen

$$\sum_{k=0}^{n} (-1)^k \begin{pmatrix} n \\ k \end{pmatrix} = 0. \tag{5}$$

Denna ekvation kan också verifieras genom att sätta $x = 1$, $y = -1$ i Binomialsatsen. Se övning 5.27 och dina föreläsningsanteckningar.

Sats 3.5 *Låt $n \geq 0$ vara ett heltal. Då gäller att*

$$3^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) 2^k. \tag{6}$$

BEVIS : Vi påstår at båda ledar av (6) ger antalet ternära ord (dvs, ord i de tre symbolerna $0, 1$ och 2) av längd n.

VL : Vi har tre möjligheter för varje position ($0, 1$ och 2) och n positioner totalt, så enligt multiplikationprincipen finns det 3^n möjliga ord av längd n.

HL : Låt $\mathcal{W}$ beteckna samlingen av alla ternära ord av längd n. Vi skall dela upp $\mathcal{W}$ i n stycken mindre samlingar, $\mathcal{W}_1, ..., \mathcal{W}_n$, så att

$$\#(\mathcal{W}_k) = \left(\begin{array}{c} n \\ k \end{array} \right) 2^k.$$

Detta skall räcka till att bevisa (6). Så vad är $\mathcal{W}_k$ då ?

Ju, $\mathcal{W}_k$ skall bestå av alla ord med $(n-k)$-stycken nollor. För ett sådant ord, finns det $\left(\begin{array}{c} n \\ n-k \end{array} \right)$ val för positionerna av nollorna. Efter att ha placerat nollorna får man sätta antingen en etta eller an tvåa i var en av de kvarstående k positionerna. Enligt multiplikationprincipen, har vi då att

$$\#(\mathcal{W}_k) = \left(\begin{array}{c} n \\ n-k \end{array} \right) 2^k = \left(\begin{array}{c} n \\ k \end{array} \right) 2^k,$$

vilket skulle visas.

OBS! Ekv. (6) kan också deriveras genom att sätta $x = 2$, $y = 1$ i Binomialsatsen. Se övning 5.28 och dina föreläsningsanteckningar.

Tillägg till föreläsning 4 (14/9/01)

Sats 4.1 *Låt a, b vara naturliga tal. Då gäller att SGD(a, b) är det minsta naturliga talet som kan skrivas i formen*

$$ax + by, \tag{7}$$

för något par x, y av heltal (inklusive negativa tal).

BEVIS : Låt d vara det minsta naturliga talet som kan skrivas i formen (7). Låt x_0, y_0 vara heltal så att

$$d = ax_0 + by_0. \tag{8}$$

För att bevisa att $d = \text{SGD}(a, b)$ måste vi visa att

(i) $d|a$.
(ii) $d|b$.
(iii) Om $c|a$ och $c|b$, då $c|d$.

(i) Enligt division algoritmen, finns det ett unikt par q, r av heltal så att $0 \leq q$, $0 \leq r < d$ och

$$a = qd + r. \tag{9}$$

Att $d|a$ är ekvivalent med att $r = 0$. För att visa detta, substituera (8) i (9) som då säger, efter lite manipulation,

$$r = a(1 - qx_0) + b(-qy_0). \tag{10}$$

Ekv. (10) uttrycker r i formen av (7). Men $r \geq 0$ och d, enligt dess definition, är det minsta positiva talet som kan skrivas i denna form. Därför måste ju $r = 0$.

(ii) Samma typ av argument som för (i).

(iii) Låt c vara någon gemensam delare till a och b. Då är c också en delare till $ax_0 + by_0 = d$, v.s.v.

Tillägg till föreläsning 9 (02/10/01)

Hädanefter, använder vi multiplikativ notation $\cdot$ för den binära operationen i en allmän grupp.

DEFINITION 9.1 : En icke-tom delmängd H till en grupp G kallas för en *delgrupp* till G om

(i) för alla $a, b \in H$, så är $ab \in H$; dvs, H är sluten under multiplikationen i G,
(ii) för alla $a \in H$, så är $a^{-1} \in H$.

Proposition 9.1 *Låt $(G, \cdot)$ vara en grupp, och H en delgrupp. Då är $(H, \cdot)$ en grupp.*

BEVIS : Vi måste kolla att $(H, \cdot)$ satisfierar gruppaxiomen. H är sluten under $\cdot$ enligt (i). Gruppoperationen är associativ i hela G, då också i H. Varje element i H har en invers i H, enligt (ii). Det kvarstår att visa existensen av en identitet. Vi påstår att identiteten 1_G av G ligger i H. För H är icke-tom, så det finns minst ett element $a \in H$. Då är $a^{-1} \in H$, enligt (ii). Och då är $1_G = aa^{-1} \in H$, enligt (i).

Proposition 9.2 *I en ändlig grupp, (i) är ett tillräckligt villkor för att en delmängd ska vara en delgrupp.*

BEVIS : Så låt G vara en ändlig grupp och H en sluten delmängd. Låt $a \in H$. Vi måste visa att $a^{-1} \in H$. Eftersom G är ändlig, kan inte alla positiva potenserna $a^n (n > 0)$ av a vara olika element i G. Därför måste det finnas $n > m > 0$ så att $a^n = a^m$, som antyder att $a^{n-m-1} = a^{-1}$. Men $a^{n-m-1} = a \cdot a \cdot ... \cdot a$ ($n - m - 1$ gånger) är ett element av H, eftersom H är sluten under multiplikation, v.s.v.

OBS! Prop. 9.2 kan inte utvidgas till oändliga grupper. Till exempel, tag $G = (\mathbf{Z}, +)$ och $H = \mathbf{N}$. Då är H sluten under multiplikation, men inte en delgrupp till $\mathbf{Z}$.

EXEMPEL 9.1 : Låt G vara en grupp, $a \in G$. Låt H vara delmängden av G som består av alla potenser av a, både positiva och negativa, tillsammans med $a^0 = 1$. Då är det klart att H är en delgrupp till G. Den kallas

för den *cyckliska delgruppen genererad av* a, och betecknas $< a >$.

DEFINITION 9.2 : En grupp G kallas för *cyklisk* om det kan genereras av ett enda element, dvs om det finns $a \in G$ så att $G = < a >$. Ett sådant element kallas för en *generator* av G.

OBS! Notera att en cyklisk grupp är abelsk.

EXEMPEL 9.2 : Man ser lätt att de additiva grupperna $\mathbf{Z}$ och $\mathbf{Z}/n\mathbf{Z}$, för alla $n > 0$, är cykliska och genererade av 1. För varje primtal p är det också sant att den multiplikativa gruppen $(\mathbf{Z}/p\mathbf{Z})^\times$ är cyklisk. För p udda är till och med grupperna $(\mathbf{Z}/p^n\mathbf{Z})^\times$ cykliska, för alla $n > 0$. Tyvärr kan vi inte bevisa dessa fakta i denna kurs, men se Exempel 9.4(i) nedan. Notera också att att

(i) det är inte så lätt att ange en explicit generator av gruppen $(\mathbf{Z}/p\mathbf{Z})^\times$, för ett givet p. Man kan bevisa att minst $1/\log_2 p$ av talen $2, ..., p-1$ är generatorer, men hur de är distribuerade i intervallen $[0, p-1]$ är inte helt klart. En konsekvens av den så kallade *Riemann hypotesen* skulle vara att det finns en konstant $C > 0$ så att, för varje $p > 0$, det finns en generator av $(\mathbf{Z}/p\mathbf{Z})^\times$ som är mindre än $C(\log_2 p)^6$!! Vidare, om man har en generator av $(\mathbf{Z}/p\mathbf{Z})^\times$, så finns det en lätt formel för generatorer av $(\mathbf{Z}/p^n\mathbf{Z})^\times$, för alla $n > 1$. Se också Exempel 9.4(ii) nedan.

(ii) gruppen $(\mathbf{Z}/2^n\mathbf{Z})^\times$ är inte cyklisk för $n \geq 3$, men "nästan" - se anmärkning 9.1 nedan. För allmäna n, utom prim potenser, brukar $(\mathbf{Z}/n\mathbf{Z})^\times$ inte vara cyklisk heller - se Prop. 9.3(iii) och Exempel 3.35 i boken.

DEFINITION 9.3 : Om G är en ändlig grupp, då kallas antalet element i G för *ordningen* av G, och betecknas $|G|$ eller $o(G)$. Om G är oändlig, då säger man att G har *oändlig ordning* och skriver $o(G) = \infty$. Om H är en delgrupp till en ändlig grupp G, då kallas kvotet $o(G)/o(H)$ för *indexen* av H i G, och betecknas $(G : H)$. Vi skall se senare (Sats 9.6) att indexen av en delgrupp är alltid ett heltal.

DEFINITION 9.4 : Låt G vara en grupp och $a \in G$. *Ordningen* av a är det minsta positiva talet n så att $a^n = 1$, och betecknas $|a|$ eller $o(a)$. Om det finns inget sådant n, då säger man att a har *oändlig ordning* och skriver $o(a) = \infty$.

EXEMPEL 9.3 : (i) I varje grupp har identiteten ordning 1.

(ii) $o(\mathbf{Z}) = \infty$ och varje icke-noll element i $\mathbf{Z}$ har oändlig ordning.
(iii) $o(\mathbf{Z}/n\mathbf{Z}) = n$. Elementet [1] har ordning n, men elementet [2] har ordning $n/2$ när n är jämnt.

Proposition 9.3 *Låt G vara en grupp, $a \in G$.*

(i) För ett heltal N, då gäller att $a^N = 1$ omm $o(a)|N$.
(ii) Ordningen av a är lika med ordningen av den cykliska delgruppen som genereras av a.
(iii) Låt nu G vara en ändlig grupp. Då har varje element i G en ändlig ordning av högst $o(G)$, och G är cyklisk omm det finns ett element $a \in G$ så att $o(a) = o(G)$.

Bevis : (i) Notera att om $o(a) = \infty$ då finns det inget N så att $a^N = 1$, som är konsistent med vad (i) säger. Antag nu att a har ändlig ordning, lika med t säg. Låt $N > 0$. Enligt division algoritm, finns det heltal q, r, med $o \leq r < t$ så att $N = qt + r$. Då har vi att

$$a^N = a^{qt+r} = (a^t)^q \cdot a^r = a^r. \tag{11}$$

Eftersom t är det minsta positiva talet så att $a^t = 1$, så följer det från (11) att $a^N = 1$ omm $r = 0$, dvs omm $t|N$, v.s.v.

(ii) Låt $n > m > 0$ vara ett par av positiva heltal. Då, m.h.a. (i), har vi att

$$a^n = a^m \Leftrightarrow a^{n-m} = 1 \Leftrightarrow o(a) < \infty \text{ och } o(a) \mid n - m. \tag{12}$$

Om $o(a) = \infty$ då medför (12) att inga två positiva potenser av a är lika, så att $< a > = \infty$ också. Om $o(a) = t < \infty$, då medför (11) och (12) att

$$< a > = \{1, a, ..., a^{t-1}\},$$

dvs att dessa t element är olika, och att varje potens av a är lika med ett av dem. Då har vi att $o(< a >) = t$ också i det här fallet.

Obs! Argumentet i detta bevis borde påminna er om första delen av vårt bevis av Eulers sats.

Exempel 9.4 (i) Låt $G = (\mathbf{Z}/7\mathbf{Z})^\times$. Då är G cyklisk av ordning $\phi(7) = 6$

och genererad av [3]. Vi har $[3]^1 = [3]$, $[3]^2 = [2]$, $[3]^3 = [6]$, $[3]^4 = [4]$, $[3]^5 = [5]$ och $[3]^6 = [1]$.

(ii) Låt $n \geq 3$. Gruppen $(\mathbf{Z}/2^n\mathbf{Z})^\times$ har ordning $\phi(2^n) = 2^{n-1}$. Gruppen har inget element av ordning 2^{n-1}, alltså är inte cyklisk. Men man kan visa att [5] har ordning 2^{n-2} (se inlämningsuppgift 2), så gruppen är, på något sätt, nästan cyklisk. Se också Korollarium 9.7 nedan.

ANMÄRKNING 9.1 : (a) Given en ändlig grupp G vars ordning är känd, och ett slumpmässigt valt $a \in G$, kan det vara väldigt svårt att beräkna $o(a)$. Om faktoriseringen av $o(G)$ är också känd då blir problemet mycket lättare pga Korollarium 9.7 nedan, men, som vi vet, verkar ju faktorieringen av ett heltal att vara ett väldigt knepigt problem också.

Å andra sidan, brukar det vara betydligt lättare att avgöra om det givna elementet a är en generator av G. Enligt del (ii) av propositionen, gäller det bara att avgöra om $o(a) = o(G)$ eller inte, snarare än att beräkna $o(a)$ exakt. I gruppen $(\mathbf{Z}/p\mathbf{Z})^\times$ till exempel (p ett udda primtal), som vi vet är cyklisk (se Exempel 9.3 ovan), finns det en snabb algoritm för att avgöra om ett givet $a \in \{2, ..., p-1\}$ är en generator - se supplementär kursmaterialen.

(b) För alla de ändliga grupper som har bemöts i denna kurs har gruppordningen varit ganska lätt att beräkna. Men det uppstår situationer där ordningen av gruppen själv (never mind its' elements) är långt från klart. Ett viktigt exempel kommer från en modern form av kryptering som heter ECC (elliptic curve cryptography) - se supplementär kursmaterialen.

Följande resultat sammanfattar de viktigaste egenskaperna hos ändliga cyckliska grupper :

Proposition 9.4 *Låt G vara en cyklisk grupp av ordning $n > 0$, och a en generator av G.*

(i) a^i är en generator av G omm $SGD(i, n) = 1$. Då har G precis $\phi(n)$ olika generatorer.
(ii) För varje positiv delare d av n har G en unik cyklisk delgrupp av index d, som genereras av a^d. G har inga delgrupper utom dessa.

BEVIS : (i) Jag påstår att

$$o(a^i) = \frac{n}{\mathrm{SGD}(n, i)}. \tag{13}$$

För HL är det minsta talet t så att $n|it$. Använd nu Prop. 9.3(i).

(ii) Låt H vara en delgrupp till G. Låt d vara det minsta positiva talet så att $a^d \in H$. Jag påstår att

(a) $d|n$,
(b) $H = < a^d >$,
(c) $(G : H) = d$.

(a) : Vi har att $a^{qd} \in H$ för alla heltal q, eftersom H är sluten under multiplikation och inversion. Låt $r = \text{SGD}(d, n)$. Enligt Euklides algoritm, finns det heltal x, y så att $r = nx + dy$. Då har vi att

$$a^r = a^{nx+dy} = (a^n)^x \cdot a^{dy} = a^{dy} \in H,$$

så $r \geq d$, som medför att $r = d$, dvs att $d|n$.

(b) : Antag att $a^i \in H$ för något $i > 0$. Enligt division algoritmen finns det heltal q, r, med $0 \leq r < d$ så att $i = qd + r \Rightarrow r = i - qd$. Då har vi att $a^r = a^i \cdot a^{-qd} \in H$, som tvingar $r = 0$.

(c) : $o(H) = o(a^d)$, enligt Prop. 9.3(ii). Men, enligt del (i) och (a) är ju $o(a^d) = n/\text{SGD(n,d)} = n/d$. Därför är $(G : H) = o(G)/o(H) = n/\frac{n}{d} = d$, v.s.v.

Exempel 9.5 : I gruppen $\mathbf{Z}/n\mathbf{Z}$ är

$$o([a]) = \frac{n}{\text{SGD}(n, a)}.$$

Vi fortsätter med några exempel till av delgrupper :

Exempel 9.6 : $G = D_n$, r = rotation genom $2\pi/n$, s = spegling genom x-axeln. $< r >$ är en cyklisk delgrupp av index 2 och $< s >$ är en cyklisk delgrupp av index n. För varje delare d av n, så genererar r^d och s en delgrupp H_d av index d. H_d är abelsk omm n är jämnt och $d = n/2$, i vilket fall $H_{n/2}$ är en icke-cyklisk grupp av ordning 4. Varje element i $H_{n/2}$ (utom 1) har ordning 2 (dvs, är en så-kallad *involution*).

Exempel 9.7[1] : $G = S_n$. En cyklisk permutation $(a_1, ..., a_k)$ har ordning

[1] Historical remark : Galois proved his theorem about non-existence of a 'formula' for

k. Om $\pi \in S_n$ är en produkt av r st. disjunkta cykel av ordningar $k_1, ..., k_r$ resp., då är

$$o(\pi) = MGM(k_1, ..., k_r).$$

För $1 \leq i \leq n$, sätt

$$H_i := \{\pi \in S_n : \pi(i) = i\}.$$

Då är varje H_i en delgrupp av ordning $(n-1)!$ och index n, som kan identifieras med S_{n-1}.

EXEMPEL 9.8 : G någon grupp som helst. Sätt

$$Z(G) := \{z \in G : zg = gz \text{ för alla } g \in G\}.$$

Då är $Z(G)$ en delgrupp av G (se inlämningsuppgift 2) som kallas för *centrum* av G.

I exempel 6 och 7 notera att indexen av varje delgrupp är ett heltal. Dessutom säger Prop. 9.4(ii) att detsamma gäller för en godtycklig delgrupp i en godtycklig ändlig cyklisk grupp. Detta är ingen slump, som vi skall nu bevisa :

OBS! Följande argument borde påminna er om andra delen av vårt bevis av Eulers sats (tag $H = < [a] >$).

Lemma 9.5 *Låt G vara en grupp, H en delgrupp. Inför en relation $\sim$ på G som följer :*

Säg $a \sim b$ om det finns $h \in H$ så att $b = ah$.

Då är $\sim$ en ekvivalens relation på G.

BEVIS :

---

the roots of a 5th degree polynomial equation by reducing the existence of such a formula to the group S_5 having a certain purely group-theoretic property called *solubility*. It is not hard to show that S_n is insoluble iff $n \geq 5$, and hence that there exists no 'formula' for the roots of a polynomial of any degree ≥ 5. For more discussion, see the supplementary course material.

Reflexivitet : $a = a \cdot 1$ och $1 \in H$.

Symmetri : $b = ah \Rightarrow a = bh^{-1}$, och $h \in H \Rightarrow h^{-1} \in H$.

Transitivitet : Antag $b = ah_1$ och $c = bh_2$. Då är $c = (ah_1)h_2 = a(h_1h_2)$ och $h_1, h_2 \in H \Rightarrow h_1h_2 \in H$.

Ekvivalensklassen av $a \in G$ betecknas aH och kallas för den *vänstra komängden* av H som innehåller a. Det är klart från definitionen av $\sim$ att

$$aH = \{ah : h \in H\}. \tag{14}$$

Då säger Lemma 5 att, för två element $a, b \in G$, antingen $aH \cap bH = \phi$ eller $aH = bH$, i vilket fall $b = ah$ för något $h \in H$.

Sats 9.6 (Lagrange) *Låt G vara en ändlig grupp och H en delgrupp till G. Då är $o(H)$ en delare till $o(G)$.*

Bevis : Enligt Lemma 5 är G unionen av parvis disjunkta vänstra komängder av H. Det är klart från (14) att varje komängd har precis $o(H)$ element. Om det finns k st. komängder, då har vi att $o(G) = k \cdot o(H)$, som medför att $o(H)$ delar $o(G)$, v.s.v.

Korollarium 9.7 *Låt G vara en ändlig grupp och $a \in G$. Då gäller att*

(i) $o(a)$ delar $o(G)$.

(ii) $a^{o(G)} = 1$.

Bevis : (i) Tillämpa Sats 9.6 till delgruppen $H = < a >$ och använd Prop. 9.3(ii).

(ii) Följer från del (i) och Prop. 9.3(i).

Korollarium 9.8 *Eulers sats.*

Bevis : Tillämpa Kor. 9.7(ii) till gruppen $G = (\mathbf{Z}/n\mathbf{Z})^{\times}$.